

Dell EMC SmartFabric OS10 User Guide

Release 10.5.0

注意、小心和警告

 **注:** “注意”表示帮助您更好地使用该产品的重要信息。

 **小心:** “小心”表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。

 **警告:** “警告”表示可能会导致财产损失、人身伤害甚至死亡。

Chapter 1: 更改历史记录	28
Chapter 2: 系统	30
出厂安装 OS10 的交换机	30
登录	31
检查 OS10 版本	31
OS10 升级	32
检查 OS10 许可证	38
重新安装许可证	39
未安装操作系统的交换机	39
卸载现有操作系统	40
下载 OS10 映像	40
使用 ONIE 进行安装	41
登录	43
安装 OS10 许可证	44
交换机部署选项	46
手动 CLI 配置	46
ZTD - 自动交换机部署	46
Ansible 自动交换机调配	46
远程访问	46
配置管理 IP 地址	47
配置管理路由	47
配置用户名和密码	48
Chapter 3: CLI 基本信息	49
CONFIGURATION 模式	50
检查设备状态	50
命令帮助	51
候选配置	52
复制正在运行的配置	54
还原启动配置	55
重新加载系统映像	56
筛选 show 命令	56
常见 OS10 命令	56
boot	56
commit	57
configure	57
copy	57
delete	59
dir	59
discard	60
do	60
end	61
exit	61

hostname.....	61
license.....	62
lock.....	62
management route.....	63
move.....	63
no.....	63
ping.....	64
ping6.....	65
reload.....	67
show boot.....	67
show candidate-configuration.....	68
show environment.....	69
show inventory.....	70
show ip management-route.....	70
show ipv6 management-route.....	71
show license status.....	71
show running-configuration.....	72
show startup-configuration.....	74
show system.....	75
show version.....	77
start.....	77
系统.....	77
system-cli disable.....	78
system-user linuxadmin disable.....	78
system identifier.....	78
terminal.....	79
traceroute.....	79
unlock.....	80
username password role.....	80
write.....	81
Chapter 4: 高级 CLI 任务.....	82
命令别名.....	82
多行别名.....	83
别名.....	85
别名（多行）.....	86
默认值（别名）.....	86
说明（别名）.....	87
行（别名）.....	87
show alias.....	87
批处理模式.....	88
batch.....	89
Linux shell 命令.....	89
使用 OS9 命令.....	91
feature config-os9-style.....	92
Chapter 5: 零接触部署.....	93
ZTD DHCP 服务器配置.....	94
ZTD 调配脚本.....	95

ZTD CLI 批处理文件.....	95
ZTD 后脚本.....	96
ZTD 命令.....	97
reload ztd.....	97
show ztd-status.....	97
ztd cancel.....	98
Chapter 6: OS10 调配.....	99
使用 Ansible.....	99
示例：使用 Ansible 配置 OS10 交换机.....	100
Chapter 7: SmartFabric 服务.....	103
SmartFabric 服务特性.....	103
适用于分支和主干的 SmartFabric 服务.....	103
适用于 PowerEdge MX 的 SmartFabric 服务.....	104
适用于分支和主干的 SmartFabric 服务.....	105
SmartFabric 服务组件.....	106
SmartFabric 服务逻辑实体.....	107
上行链路.....	107
上行链路绑定选项.....	108
生成树注意事项.....	108
集成设备的动态加入.....	108
静态加入的服务器.....	109
非集成设备的静态加入.....	109
在交换机上启用 SmartFabric 服务.....	109
使用 GUI 启用 SmartFabric 服务.....	110
SmartFabric 服务图形用户界面.....	110
配置 SmartFabric 服务初始设置.....	111
更新默认结构、交换机名称和描述向导.....	111
为外部网络连接向导创建上行链路.....	111
分解交换机端口向导.....	113
配置跳转主机向导.....	113
更新网络配置向导.....	113
将服务器板载连接到结构向导.....	114
编辑默认结构设置向导.....	114
结构操作和生命周期管理.....	114
SmartFabric 命令.....	115
smartfabric l3fabric enable.....	115
show smartfabric cluster.....	115
show smartfabric cluster member.....	116
show smartfabric details.....	116
show smartfabric networks.....	117
show smartfabric nodes.....	118
show smartfabric personality.....	118
show smartfabric uplinks.....	119
show smartfabric validation-error.....	119
Chapter 8: SmartFabric Director.....	121
在交换机上启用 SmartFabric Director 模式.....	121

支持 SmartFabric Director.....	121
gRPC 网络管理接口代理.....	121
使用 SmartFabric Director 的生命周期管理.....	123
SmartFabric Director 命令.....	124
switch-operating mode.....	124
gnmi-security-profile.....	125
show switch-operating-mode.....	125
show sfd status.....	125
Chapter 9: 系统管理.....	126
系统横标.....	126
登录横标.....	126
MOTD 横标.....	126
系统横标命令.....	127
用户会话管理.....	128
用户会话管理命令.....	128
Telnet 服务器.....	129
Telnet 命令.....	130
简单网络管理协议.....	131
SNMP 安全模式和级别.....	131
MIB.....	131
SNMPv3.....	132
配置 SNMP.....	133
SNMP 命令.....	136
示例：配置 SNMP.....	144
系统时钟.....	145
时区和 UTC 偏离参考.....	146
系统时钟命令.....	162
网络时间协议.....	164
启用 NTP.....	164
转播.....	165
源 IP 地址.....	165
身份验证.....	166
示例 NTP 配置.....	167
NTP 命令.....	169
动态主机配置协议.....	174
数据包格式和选项.....	175
DHCP 服务器.....	176
自动地址分配.....	176
主机名称解析.....	177
手动绑定条目.....	178
DHCP 中继代理.....	179
查看 DHCP 信息.....	180
系统域名和列表.....	180
DHCP 侦听.....	181
DHCP 命令.....	197
DHCP 侦听命令.....	202
DNS 命令.....	208
IPv4 DHCP 限制.....	209

Chapter 10: 接口	211
以太网接口	211
统一端口组	211
Z9264F-ON port-group profiles	213
S5200F-ON 交换机上的端口组	214
L2 模式配置	221
L3 模式配置	221
光纤通道接口	222
配置波长	223
管理接口	224
管理接口	224
VLAN 接口	224
用户配置的默认 VLAN	225
VLAN 扩展配置文件	225
环回接口	226
端口通道接口	227
创建端口通道	227
添加端口成员	227
最小链路数	228
分配端口通道 IP 地址	228
卸下或禁用端口通道	228
负载均衡流量	229
更改哈希算法	229
配置接口范围	229
交换机端口配置文件	230
S4148-ON 系列端口配置文件	231
S4148U-ON 端口配置文件	232
在接口上配置协商模式	233
配置分解模式	234
分解自动配置	235
重置默认配置	236
转发纠错	237
节能以太网	238
启用节能以太网	238
清除 EEE 计数器	238
查看 EEE 状态/统计信息	239
EEE 命令	240
查看接口配置	242
数字光学监控	245
启用 DOM 和 DOM 陷阱	246
接口命令	247
channel-group	247
default interface	247
default vlan-id	249
description (Interface)	250
duplex	250
enable dom	251
enable dom traps	251
feature auto-breakout	251

fec.....	252
interface breakout.....	252
interface ethernet.....	253
interface loopback.....	253
interface mgmt.....	253
interface null.....	254
interface port-channel.....	254
interface range.....	254
interface vlan.....	255
link-bundle-utilization.....	255
mode.....	255
mode l3.....	256
mtu.....	257
negotiation.....	257
port mode Eth.....	258
port-group.....	259
profile.....	259
scale-profile vlan.....	260
show discovered-expanders.....	260
show interface.....	261
show interface transceiver “Tunable wavelength”.....	262
show inventory media.....	262
show link-bundle-utilization.....	264
show port-channel summary.....	264
show port-group.....	265
show switch-port-profile.....	266
show system.....	266
show unit-provision.....	267
show vlan.....	267
shutdown.....	268
speed (光纤通道)	268
speed (管理)	269
switch-port-profile.....	269
switchport access vlan.....	271
switchport mode.....	271
switchport trunk allowed vlan.....	271
unit-provision.....	272
wavelength.....	272

Chapter 11: PowerEdge MX 以太网 I/O 模块.....	273
运行模式.....	273
更改操作模式.....	274
限制.....	275
I/O 模块上的端口组.....	275
双密度 QSFP28 接口.....	275
虚拟端口.....	277
单密度 QSFP28 接口.....	280
面向服务器的接口.....	281
更换 SmartFabric 中的 MX 以太网 IO 模块.....	282
部署说明.....	283

更换 SmartFabric 中的 IOM.....	283
Chapter 12: 光纤通道.....	287
以太网光纤通道.....	288
配置 FIP 侦听.....	288
术语.....	290
虚拟结构.....	290
光纤通道分区.....	292
以太网上的 F_Port.....	294
将 FCoE 流量固定到端口通道的特定端口.....	294
VLT 网络上的 FSB 配置示例.....	296
VLT 网络上的 FC 交换机配置示例.....	298
非 VLT 网络上的 FSB 配置示例.....	300
非 VLT 网络上的 FC 交换机配置示例.....	301
多跳 FIP 侦听桥.....	303
配置说明.....	303
配置多跳 FSB.....	303
验证多跳 FSB 配置.....	309
多跳 FSB 配置示例.....	311
配置指导准则.....	324
NPIV 代理网关级联.....	324
在 FCoE 中支持未标记的 VLAN.....	327
F_Port 命令.....	327
fc alias.....	327
fc zone.....	327
fc zoneset.....	328
feature fc.....	328
member (别名)	328
member (zone).....	329
成员 (分区集)	329
show fc alias.....	330
show fc interface-area-id mapping.....	330
show fc ns switch.....	330
show fc zone.....	331
show fc zoneset.....	332
zone default-zone permit.....	333
zoneset activate.....	333
NPG 命令.....	333
fc port-mode F.....	333
feature fc npg.....	334
show npg devices.....	334
F_Port 和 NPG 命令.....	335
clear fc statistics.....	335
fcoe	335
name.....	336
show fc statistics.....	336
show fc switch.....	336
show running-config vfabric.....	337
show vfabric.....	337
vfabric.....	338

vfabric (interface).....	338
vlan.....	338
FIP 侦听命令.....	339
feature fip-snooping.....	339
fip-snooping enable.....	339
fip-snooping fc-map.....	340
fip-snooping port-mode.....	340
FCoE 命令.....	340
clear fcoe database.....	341
clear fcoe statistics.....	341
fcoe-pinned-port.....	341
fcoe max-sessions-per-enodemac.....	342
fcoe priority-bits.....	342
lldp tlv-select dcbxp-appln fcoe.....	342
show fcoe enode.....	343
show fcoe fcf.....	343
show fcoe pinned-port.....	343
show fcoe sessions.....	344
show fcoe statistics.....	344
show fcoe system.....	345
show fcoe vlan.....	345
Chapter 13: 第 2 层.....	346
802.1X.....	346
端口身份验证.....	347
EAP over RADIUS.....	348
配置 802.1X.....	348
启用 802.1X.....	348
身份重新传输.....	349
故障静默期.....	350
端口控制模式.....	351
重新验证端口.....	352
配置超时.....	352
802.1X 命令.....	353
远端故障检测.....	357
全局启用 FEFD.....	359
启用接口上的 FEFD.....	359
Reset FEFD err-disabled interface.....	360
显示 FEFD 信息.....	360
FEFD 命令.....	360
链路聚合控制协议.....	363
模式.....	363
配置.....	363
接口.....	364
速率.....	365
配置示例.....	365
LACP 回退.....	368
LACP 命令.....	371
链路层发现协议.....	377
可选的 TLV.....	378

基本 TLV.....	379
组织特定的 TLV.....	379
介质端点查找.....	381
网络连接设备.....	381
LLDP-MED 功能 TLV.....	381
网络策略 TLV.....	382
定义网络策略.....	383
数据包计时器值.....	383
禁用和启用 LLDP.....	384
在管理端口上禁用和启用 LLDP.....	384
通告 TLV.....	385
网络策略通告.....	389
快速启动重复计数.....	389
查看 LLDP 配置.....	389
相邻代理通告.....	390
生存时间.....	392
VLT 域中的通告管理地址 TLV.....	392
LLDP 命令.....	393
介质访问控制.....	404
静态 MAC 地址.....	404
MAC 地址表.....	405
清除 MAC 地址表.....	405
MAC 命令.....	406
生成树协议.....	408
EdgePort.....	408
生成树扩展.....	408
从 BPDU 防护违规中恢复.....	410
MAC 刷新优化.....	411
调试配置.....	412
为快速状态转移设置生成树链接类型.....	412
常见的 STP 命令.....	412
Rapid per-VLAN spanning-tree plus.....	418
快速生成树协议.....	426
多个生成树.....	433
虚拟 LAN.....	444
默认 VLAN.....	445
创建或移除 VLAN.....	445
访问模式.....	447
中继模式.....	447
分配 IP 地址.....	448
查看 VLAN 配置.....	449
VLAN 命令.....	450
端口监控.....	451
本地端口监控.....	451
远程端口监控.....	452
封装的远程端口监控.....	454
基于流的监控.....	455
VLT 上的远程端口监控.....	456
端口监控命令.....	458

Chapter 14: 第 3 层	462
虚拟路由和转发	462
配置管理 VRF	462
配置非默认 VRF 实例	464
VRF 配置	466
查看 VRF 实例信息	470
静态路由泄漏	470
VRF 命令	474
双向转发检测	480
BFD 会话状态	480
BFD 三向握手	481
BFD 配置	482
全局配置 BFD	482
BFD for BGP	483
BFD for OSPF	487
适用于静态路由的 BFD	491
BFD 命令	493
边界网关协议	499
会话和对等	499
路由反射器	500
多协议 BGP	500
属性	501
选择条件	501
权重和本地首选项	502
复合鉴别器	502
来源	502
AS 路径和下一跳	503
最佳路径选择	503
更多路径支持	504
通告成本	504
4 字节 AS 编号	504
AS 编号迁移	504
正常重新启动	505
配置边界网关协议	505
启用 BGP	506
禁用 ASN 值的通知	508
配置双堆栈	508
配置管理距离	509
对等模板	510
邻居故障切换	513
配置密码	514
快速外部故障切换	516
被动对等	517
本地 AS	518
AS 编号限制	518
重新分发路由	519
其他路径	520
MED 属性	520
本地首选项属性	521

权重属性.....	522
启用多路径.....	522
路由映射筛选器.....	522
路由反射器群集.....	523
聚合路由.....	524
联盟.....	524
路由抑制.....	525
计时器.....	526
邻居软重新配置.....	526
重新分发 iBGP 路由到 OSPF.....	527
调试 BGP.....	530
BGP 命令.....	530
同等成本多路径.....	560
负载均衡.....	560
最大 ECMP 组和路径.....	564
ECMP 命令.....	564
IPv4 路由.....	568
分配接口 IP 地址.....	568
配置静态路由.....	569
地址解析协议.....	570
IPv4 路由命令.....	570
IPv6 路由.....	575
启用或禁用 IPv6.....	575
IPv6 地址.....	576
无状态自动配置.....	577
邻居查找.....	578
重复地址查找.....	579
静态 IPv6 路由.....	579
IPv6 目标无法访问.....	580
IPv6 逐跳选项.....	580
查看 IPv6 信息.....	580
IPv6 命令.....	581
首先打开最短路径.....	591
自治系统区域.....	591
区域、网络和邻居.....	592
路由器类型.....	592
指定和备份指定的路由器.....	593
链路状态通告.....	594
路由器优先级.....	594
最短路径优先限制.....	595
OSPFv2.....	596
OSPFv3.....	626
对象跟踪管理器.....	646
接口跟踪.....	646
主机跟踪.....	647
设置跟踪延迟.....	648
对象跟踪.....	648
查看跟踪对象.....	648
OTM 命令.....	649
基于策略的路由.....	651

用于匹配路由映射的访问列表.....	652
设置地址以匹配路由映射.....	652
将路由映射分配给接口.....	652
查看 PBR 信息.....	653
基于策略的按 VRF 的路由.....	653
按 VRF 配置 PBR.....	653
PBR 和 VLT.....	654
配置示例.....	657
跟踪路由可访问性.....	658
使用 PBR 允许和阻止特定流量.....	659
查看 PBR 配置.....	660
PBR 命令.....	660
虚拟路由器冗余协议.....	663
配置.....	663
创建虚拟路由器.....	664
组版本.....	665
虚拟 IP 地址.....	665
配置虚拟 IP 地址.....	665
在 VRF 中配置虚拟 IP 地址.....	666
设置组优先级.....	667
身份验证.....	668
禁用抢占.....	668
通告间隔.....	669
接口/对象跟踪.....	670
配置跟踪.....	670
VRRP 命令.....	671
Chapter 15: 多播.....	676
重要事项.....	676
配置多播路由.....	676
未知的多播泛洪控制.....	677
启用多播泛洪控制.....	678
多播命令.....	678
多播侦听泛洪限制.....	678
互联网组管理协议.....	679
标准合规性.....	679
重要事项.....	679
支持的 IGMP 版本.....	679
查询间隔.....	680
最后成员查询间隔.....	680
最长响应时间.....	680
IGMP 即时离开.....	680
选择 IGMP 版本.....	681
查看已启用 IGMP 的接口和组.....	681
IGMP 侦听.....	682
IGMP 命令.....	683
多播侦听器发现协议.....	693
MLD 侦听.....	693
MLD 侦听命令.....	695
协议独立多播.....	701

PIM 术语.....	701
标准合规性.....	702
PIM-SM.....	702
PIM-SSM.....	702
为 S、G 条目配置到期计时器.....	703
Configure static rendezvous point.....	703
使用 BSR 机制配置动态 RP.....	704
配置指定的路由器优先级.....	706
PIM 命令.....	706
PIM-SM 示例配置.....	717
PIM-SSM 示例配置.....	721
多播 VRF 配置示例.....	726
VLT 多播路由.....	734
多播路由表同步.....	734
IGMP 消息同步.....	735
出口掩码.....	735
跨区 VLAN.....	735
部署注意事项.....	735
示例：跨区 L3 VLAN IIF.....	735
示例：方形 VLT 拓扑中的主动-主动 PIM.....	743
VLT 多播路由显示命令.....	774
Chapter 16: VXLAN.....	775
VXLAN 概念.....	775
VXLAN 即 NVO 解决方案.....	776
配置 VXLAN.....	776
在 VTEP 上配置源 IP 地址.....	776
配置 VXLAN 虚拟网络.....	777
配置 VLAN 标记的访问端口.....	778
配置未标记的访问端口.....	778
在虚拟网络之间启用覆盖路由.....	779
通告 VXLAN 源 IP 地址.....	781
配置 VLT.....	781
L3 VXLAN 路由扩展.....	782
VTEP 上的 DHCP 中继.....	783
查看 VXLAN 配置.....	784
VXLAN MAC 地址.....	786
VXLAN 命令.....	788
hardware overlay-routing-profile.....	788
interface virtual-network.....	788
ip virtual-router address.....	789
ip virtual-router mac-address.....	789
member-interface.....	789
nve.....	790
remote-vtep.....	790
show hardware overlay-routing-profile mode.....	791
show interface virtual-network.....	791
show nve remote-vtep.....	792
show nve remote-vtep counters.....	792
show nve vxlan-vni.....	792

show virtual-network.....	793
show virtual-network counters.....	793
show virtual-network interface counters.....	794
show virtual-network interface.....	794
show virtual-network vlan.....	795
show vlan (virtual network).....	795
source-interface loopback.....	795
virtual-network.....	796
virtual-network untagged-vlan.....	796
vxlan-vni.....	796
VXLAN MAC 命令.....	797
clear mac address-table dynamic nve remote-vtep.....	797
clear mac address-table dynamic virtual-network.....	797
show mac address-table count extended.....	798
show mac address-table count nve.....	798
show mac address-table count virtual-network.....	799
show mac address-table extended.....	800
show mac address-table nve.....	800
show mac address-table virtual-network.....	801
示例：VXLAN 和静态 VTEP.....	802
BGP EVPN for VXLAN.....	814
BGP EVPN 与静态 VXLAN 比较.....	814
VXLAN BGP EVPN 操作.....	815
为 VXLAN 配置 BGP EVPN.....	817
VXLAN BGP EVPN 路由.....	820
BGP EVPN 和 VLT.....	821
VXLAN BGP 命令.....	822
VXLAN EVPN 命令.....	825
示例：VXLAN 和 BGP EVPN.....	830
示例：VXLAN BGP EVPN — 多 AS 拓扑.....	851
示例：VXLAN BGP EVPN — 集中化 L3 网关.....	872
示例：VXLAN BGP EVPN — 带有非对称 IRB 的边界分支网关.....	874
控制器调配的 VXLAN.....	877
配置控制器调配的 VXLAN.....	878
从 VMware vCenter 配置和控制 VXLAN.....	881
示例：具有控制器配置的 VXLAN.....	884
VXLAN 控制器命令.....	888
 Chapter 17: UFT 模式.....	 894
配置 UFT 模式.....	895
IPv6 扩展前缀路由.....	896
UFT 命令.....	896
hardware forwarding-table mode.....	896
hardware l3 ipv6-extended-prefix.....	897
show hardware forwarding-table mode.....	897
show hardware forwarding-table mode all.....	898
show hardware l3.....	898
 Chapter 18: 安全性.....	 899

AAA 身份验证.....	899
用户重新身份验证.....	900
密码强度.....	900
简单密码检查.....	901
隐匿密码.....	901
基于角色的访问控制.....	902
分配用户角色.....	902
引导加载程序保护.....	902
Linux 管理员用户配置.....	903
AAA 身份验证.....	904
RADIUS 身份验证.....	904
RADIUS over TLS 身份验证.....	906
TACACS+ 身份验证.....	906
未知用户角色.....	907
SSH 服务器.....	908
虚拟终端行 ACL.....	909
限制 SNMP 访问.....	909
启用 AAA 核算.....	909
启用用户锁定.....	910
限制并发登录会话.....	910
启用登录统计信息.....	911
权限级别.....	911
配置权限级别.....	912
配置启用密码.....	912
审核日志.....	913
安全命令.....	914
aaa accounting.....	914
aaa authentication login.....	915
aaa re-authenticate enable.....	915
boot protect disable username.....	916
boot protect enable username password.....	916
clear logging audit.....	916
crypto ssh-key generate.....	917
disable.....	917
enable.....	917
enable password priv-lvl.....	918
ip access-class.....	918
ip radius source-interface.....	919
ip tacacs source-interface.....	919
ipv6 access-class.....	919
ip ssh server challenge-response-authentication.....	920
ip ssh server cipher.....	920
ip ssh server enable.....	921
ip ssh server hostbased-authentication.....	921
ip ssh server kex.....	921
ip ssh server mac.....	922
ip ssh server password-authentication.....	923
ip ssh server port.....	923
ip ssh server pubkey-authentication.....	923
ip ssh server vrf.....	924

line vty.....	924
logging audit enable.....	924
login concurrent-session limit.....	925
login-statistics enable.....	925
mac address-table static.....	925
password-attributes.....	926
password-attributes max-retry lockout-period.....	926
privilege.....	927
radius-server host.....	927
radius-server host tls.....	928
radius-server retransmit.....	929
radius-server timeout.....	929
radius-server vrf.....	929
service obscure-password.....	930
service simple-password.....	930
show boot protect.....	930
show crypto ssh-key.....	931
show ip ssh.....	931
show mac address-table count.....	932
show logging audit.....	932
show login-statistics.....	933
show privilege.....	933
show running-configuration privilege.....	934
show users.....	934
system-user linuxadmin disable.....	934
system-user linuxadmin password.....	935
tacacs-server host.....	935
tacacs-server timeout.....	936
tacacs-server vrf.....	936
username password role.....	936
username sshkey.....	937
username sshkey filename.....	938
userrole inherit.....	939
X.509v3 证书.....	939
X.509v3 概念.....	940
公钥基础设施.....	940
管理 CA 证书.....	940
证书吊销.....	942
请求并安装主机证书.....	944
自签名证书.....	946
安全配置文件.....	948
群集安全.....	949
X.509v3 命令.....	951
示例：使用 X.509v3 证书配置 RADIUS over TLS.....	961
Chapter 19: OpenFlow.....	963
OpenFlow 逻辑交换机实例.....	963
OpenFlow 控制器.....	964
OpenFlow 版本 1.3.....	964
端口.....	964

流表.....	964
组表.....	965
计量表.....	965
指令.....	965
操作集.....	965
操作类型.....	966
计数器.....	966
OpenFlow 协议.....	967
OpenFlow 使用案例.....	980
配置 OpenFlow.....	980
建立 TLS 连接.....	981
OpenFlow 命令.....	982
controller.....	982
dpid-mac-address.....	983
in-band-mgmt.....	983
max-backoff.....	984
mode openflow-only.....	984
openflow.....	984
probe-interval.....	985
protocol-version.....	985
rate-limit packet_in.....	986
show openflow.....	986
show openflow flows.....	987
show openflow ports.....	987
show openflow switch.....	989
show openflow switch controllers.....	989
switch.....	990
仅限 OpenFlow 模式的命令.....	990
Chapter 20: 访问控制列表.....	993
IP ACL.....	993
MAC ACL.....	993
控制平面 ACL.....	994
控制平面 ACL 限定符.....	994
IP 片段处理.....	995
L3 ACL 规则.....	995
为筛选器分配序列号.....	996
删除 ACL 规则.....	997
L2 和 L3 ACL.....	997
分配和应用 ACL 筛选器.....	998
入口 ACL 筛选器.....	998
出口 ACL 筛选器.....	999
VTY ACL.....	999
SNMP ACL.....	1000
清除访问列表计数器.....	1000
IP 前缀列表.....	1000
路由映射.....	1000
匹配路由.....	1002
设置条件.....	1002
Continue 子句.....	1003

基于 ACL 流的监控.....	1003
启用基于流的监控.....	1004
查看 ACL 表利用率报告.....	1005
已知行为.....	1006
ACL 日志记录.....	1006
重要事项.....	1007
ACL 命令.....	1007
clear ip access-list counters.....	1007
clear ipv6 access-list counters.....	1007
clear mac access-list counters.....	1008
deny.....	1008
deny (IPv6).....	1009
deny (MAC).....	1009
deny icmp.....	1010
deny icmp (IPv6).....	1010
deny ip.....	1011
deny ipv6.....	1011
deny tcp.....	1012
deny tcp (IPv6).....	1012
deny udp.....	1013
deny udp (IPv6).....	1014
description.....	1014
ip access-group.....	1015
ip access-list.....	1015
ip as-path access-list.....	1015
ip community-list standard deny.....	1016
ip community-list standard permit.....	1016
ip extcommunity-list standard deny.....	1017
ip extcommunity-list standard permit.....	1017
ip prefix-list description.....	1017
ip prefix-list deny.....	1018
ip prefix-list permit.....	1018
ip prefix-list seq deny.....	1018
ip prefix-list seq permit.....	1019
ipv6 access-group.....	1019
ipv6 access-list.....	1020
ipv6 prefix-list deny.....	1020
ipv6 prefix-list description.....	1020
ipv6 prefix-list permit.....	1021
ipv6 prefix-list seq deny.....	1021
ipv6 prefix-list seq permit.....	1021
mac access-group.....	1022
mac access-list.....	1022
permit.....	1022
permit (IPv6).....	1023
permit (MAC).....	1024
permit icmp.....	1024
permit icmp (IPv6).....	1025
permit ip.....	1025
permit ipv6.....	1026

permit tcp.....	1026
permit tcp (IPv6).....	1027
permit udp.....	1027
permit udp (IPv6).....	1028
remark.....	1029
seq deny.....	1029
seq deny (IPv6).....	1030
seq deny (MAC).....	1030
seq deny icmp.....	1031
seq deny icmp (IPv6).....	1032
seq deny ip.....	1032
seq deny ipv6.....	1033
seq deny tcp.....	1033
seq deny tcp (IPv6).....	1034
seq deny udp.....	1035
seq deny udp (IPv6).....	1036
seq permit.....	1036
seq permit (IPv6).....	1037
seq permit (MAC).....	1037
seq permit icmp.....	1038
seq permit icmp (IPv6).....	1039
seq permit ip.....	1039
seq permit ipv6.....	1040
seq permit tcp.....	1040
seq permit tcp (IPv6).....	1041
seq permit udp.....	1042
seq permit udp (IPv6).....	1043
show access-group.....	1043
show access-lists.....	1044
show acl-table-usage detail.....	1046
show ip as-path-access-list.....	1049
show ip community-list.....	1049
show ip extcommunity-list.....	1049
show ip prefix-list.....	1050
显示日志记录访问列表.....	1050
路由映射命令.....	1050
continue.....	1050
match as-path.....	1051
match community.....	1051
match extcommunity.....	1051
match interface.....	1052
match ip address.....	1052
match ip next-hop.....	1052
match ipv6 address.....	1053
match ipv6 next-hop.....	1053
match metric.....	1053
match origin.....	1054
match route-type.....	1054
match tag.....	1054
route-map.....	1055

set comm-list add.....	1055
set comm-list delete.....	1055
set community.....	1056
set extcomm-list add.....	1056
set extcomm-list delete.....	1056
set extcommunity.....	1057
set local-preference.....	1057
set metric.....	1057
set metric-type.....	1058
set next-hop.....	1058
set origin.....	1059
set tag.....	1059
set weight.....	1059
show route-map.....	1060

Chapter 21: 服务质量.....1061

配置服务质量.....	1061
入口流量类别.....	1063
数据流量类别.....	1063
控制平面监察.....	1067
出口流量类别.....	1072
监察流量.....	1073
标记流量.....	1073
颜色流量.....	1074
修改数据包字段.....	1074
整形流量.....	1074
带宽分配.....	1075
严格优先级队列.....	1076
速率调整.....	1077
缓冲区管理.....	1077
配置入口缓冲区.....	1078
配置出口缓冲区.....	1079
深度缓冲区模式.....	1080
拥塞规避.....	1081
风暴控制.....	1083
RoCE 实现更快的访问和无损连接.....	1083
在交换机上配置 RoCE.....	1083
RoCE for VXLAN over VLT.....	1084
缓冲区统计信息跟踪.....	1093
端口到端口管道和 MMU 映射.....	1094
QoS 命令.....	1099
bandwidth.....	1099
buffer-statistics-tracking.....	1099
class.....	1099
class-map.....	1100
clear qos statistics.....	1100
clear qos statistics type.....	1100
control-plane.....	1101
control-plane-buffer-size.....	1101
flowcontrol.....	1102

hardware deep-buffer-mode.....	1102
match.....	1102
match cos.....	1103
match dscp.....	1103
match precedence.....	1104
匹配队列.....	1104
match vlan.....	1105
mtu.....	1105
pause.....	1105
pfc-cos.....	1106
pfc-max-buffer-size.....	1106
pfc-shared-buffer-size.....	1107
pfc-shared-headroom-buffer-size.....	1107
police.....	1107
policy-map.....	1108
priority.....	1108
priority-flow-control mode.....	1108
qos-group dot1p.....	1109
qos-group dscp.....	1109
qos-map traffic-class.....	1109
qos-rate-adjust.....	1110
queue-limit.....	1110
queue bandwidth.....	1111
queue qos-group.....	1111
queue qos-group (Z9332F-ON).....	1111
random-detect (interface).....	1112
random-detect (queue).....	1112
random-detect color.....	1112
random-detect ecn.....	1113
random-detect ecn.....	1113
random-detect pool.....	1113
random-detect weight.....	1114
service-policy.....	1114
set cos.....	1114
set dscp.....	1115
set qos-group.....	1115
shape.....	1115
show class-map.....	1116
show control-plane buffers.....	1116
show control-plane buffer-stats.....	1117
show control-plane info.....	1118
show control-plane statistics.....	1119
show hardware deep-buffer-mode.....	1120
show interface priority-flow-control.....	1120
show qos interface.....	1121
show policy-map.....	1121
show qos control-plane.....	1122
show qos egress buffers interface.....	1122
show qos egress buffer-statistics-tracking.....	1122
show qos egress buffer-stats interface.....	1123

show qos headroom-pool buffer-statistics-tracking.....	1124
show qos ingress buffers interface.....	1124
show qos ingress buffer-statistics-tracking.....	1125
show qos ingress buffer-stats interface.....	1125
show qos maps.....	1126
show qos maps (Z9332F-ON).....	1127
show qos port-map details.....	1128
show qos-rate-adjust.....	1133
show qos service-pool buffer-statistics-tracking.....	1133
show qos system.....	1134
show qos system buffers.....	1134
show qos wred-profile.....	1135
show queuing statistics.....	1136
system qos.....	1137
trust dot1p-map.....	1137
trust dscp-map.....	1138
trust-map.....	1138
wred.....	1138

Chapter 22: 虚拟链路中继..... 1140

术语.....	1141
VLT 域.....	1141
VLT 互连.....	1141
正常 LACP 和 VLT.....	1142
配置 VLT.....	1144
配置生成树协议.....	1145
创建 VLT 域.....	1148
配置 VLTi.....	1149
配置 VLT MAC 地址.....	1149
配置延迟还原计时器.....	1150
配置 VLT 对等节点存活检查.....	1150
配置 VLT 端口通道.....	1154
配置 VLT 对等路由.....	1155
配置 VRRP 主动-主动模式.....	1155
通过 eVLT 在数据中心之间迁移虚拟机.....	1156
查看 VLT 信息.....	1159
VLT 命令.....	1160
backup destination.....	1160
delay-restore.....	1160
discovery-interface.....	1161
peer-routing.....	1161
peer-routing-timeout.....	1161
primary-priority.....	1162
show running-configuration vlt.....	1162
show spanning-tree virtual-interface.....	1162
show vlt.....	1164
show vlt backup-link.....	1165
show vlt mac-inconsistency.....	1165
show vlt mismatch.....	1166
show vlt role.....	1169

show vlt vlt-port-detail.....	1169
vlt-domain.....	1170
vlt-port-channel.....	1170
vlt-mac.....	1170
vrrp mode active-active.....	1171
Chapter 23: 上行链路故障检测.....	1172
配置上行链路故障检测.....	1173
VLT 上的上行链路故障检测.....	1175
UFD VLT 的示例配置.....	1176
UFD 命令.....	1178
clear ufd-disable.....	1178
defer-time.....	1178
downstream.....	1179
downstream auto-recover.....	1179
downstream disable links.....	1179
enable.....	1180
name.....	1180
show running-configuration uplink-state-group.....	1180
show uplink-state-group.....	1181
uplink-state-group.....	1182
upstream.....	1182
Chapter 24: 聚合数据中心服务.....	1183
优先级流控制.....	1183
PFC 配置说明.....	1183
配置 PFC.....	1186
PFC 命令.....	1189
增强的传输选择.....	1192
ETS 配置说明.....	1192
配置 ETS.....	1192
ETS 命令.....	1195
数据中心桥接交换.....	1195
DCBX 配置说明.....	1196
配置 DCBX.....	1196
DCBX 命令.....	1199
互联网小型计算机系统接口.....	1202
iSCSI 配置说明.....	1203
配置 iSCSI 优化.....	1203
VLT 上的 iSCSI 同步.....	1205
iSCSI 命令.....	1206
聚合网络 DCB 示例.....	1209
Chapter 25: sFlow.....	1216
启用 sFlow.....	1216
最大标头大小配置.....	1217
收集器配置.....	1218
轮询间隔配置.....	1219
采样率配置.....	1219

源接口配置.....	1220
查看 sFlow 信息.....	1221
sFlow 命令.....	1222
sflow collector.....	1222
sflow enable.....	1222
sflow max-header-size.....	1223
sflow polling-interval.....	1223
sflow sample-rate.....	1223
sflow source-interface.....	1224
show sflow.....	1224
Chapter 26: 遥测.....	1226
遥测术语.....	1226
YANG 塑形的遥测数据.....	1226
配置遥测.....	1228
查看遥测配置.....	1229
遥测命令.....	1232
debug telemetry.....	1232
destination.....	1232
destination-group (subscription-profile).....	1232
destination-group (telemetry).....	1233
enable.....	1233
encoding.....	1233
sensor-group (subscription-profile).....	1234
sensor-group (telemetry).....	1234
sensor-path.....	1235
show telemetry.....	1235
source interface.....	1238
subscription-profile.....	1238
telemetry.....	1238
transport.....	1239
示例：配置流式遥测.....	1239
Chapter 27: RESTCONF API.....	1241
配置 RESTCONF API.....	1241
RESTCONF API 的 CLI 命令.....	1242
rest api restconf.....	1242
rest https cipher-suite.....	1242
rest https server-certificate.....	1242
rest https session timeout.....	1243
RESTCONF API 任务.....	1243
查看 CLI 命令的 XML 结构.....	1244
RESTCONF API 示例.....	1245
Chapter 28: OS10 故障处理.....	1247
诊断工具.....	1247
引导分区和映像.....	1248
监控进程.....	1248
LED 设置.....	1249

数据包分析.....	1249
端口适配器和模块.....	1250
测试网络连接.....	1250
查看解决方案 ID.....	1251
查看诊断.....	1253
诊断命令.....	1254
恢复 Linux 密码.....	1261
恢复 OS10 用户名密码.....	1262
还原出厂默认设置.....	1264
SupportAssist.....	1265
重要事项.....	1265
配置 SupportAssist.....	1265
设置公司名称.....	1266
设置联系信息.....	1267
安排活动.....	1267
查看状态.....	1268
国家/地区名称和代码的列表.....	1269
SupportAssist 命令.....	1276
支持套装.....	1285
事件通知.....	1286
generate support-bundle.....	1286
系统监控.....	1287
系统事件和警报.....	1287
系统日志记录.....	1289
通过 TLS 的系统日志记录.....	1290
查看系统日志.....	1292
环境监控.....	1292
链路套装监控.....	1293
警报命令.....	1293
日志记录命令.....	1299
登录 OS10 设备.....	1304
常见问题.....	1305
安装.....	1305
硬件.....	1306
配置.....	1306
安全性.....	1306
第 2 层.....	1306
第 3 层.....	1306
系统管理.....	1307
访问控制列表.....	1307
服务质量.....	1307
监控.....	1307

Chapter 29: 支持资源..... 1309

更改历史记录

下表概述了本指南从以前的 OS10 版本到 10.5.0.3 版本的更改。有关新功能的详细信息，请参阅相应的章节。

表. 1: 10.5.0.3 中的新功能

版本	日期	功能部件	说明
A03	2019-12-06	在交换机上启用 SmartFabric 服务	使用 OS10 CLI 启用或禁用 OS10 交换机中的 SmartFabric 服务。
		SmartFabric 服务图形用户界面	在分支和主干拓扑中形成的第 3 层结构中，方便白天部署配置和管理交换机。
		禁用 ASN 值的通知	配置系统以修改收到的 BGP 路由的 AS_PATH 属性，并禁用预置全局配置的 AS 编号。

表. 2: 10.5.0.1P1 中的新功能

版本	日期	功能部件	说明
A02	2019-10-07	优先级流控制	- 为 Z9332F-ON 配置流量类别到队列映射 - 查看默认流量类别到队列映射的格式。
		queue qos-group (Z9332F-ON)	配置不同流量类别的流量类型到不同队列的映射。
		show qos maps (Z9332F-ON)	显示 dot1p 到流量类别、DSCP 到流量类别以及流量类别到设备中的队列映射的 QoS 映射配置。

表. 3: 10.5.0.1 中的新功能

版本	日期	功能部件	说明
A01	2019-09-17	SmartFabric 中的 MX 以太网 IO 模块更换	更换属于 SmartFabric 的以太网 I/O 模块 (IOM)。
		SmartFabric 服务模式 CLI 支持： - NTP - SupportAssist - 日志记录 - 系统时钟 - 安全性 - F_Port 命令	使用 SmartFabric OS10 CLI 配置以下协议或服务： - NTP - SupportAssist - 日志记录 - SNMP - 系统时钟 - 安全性 - FC 分区
		SmartFabric 服务 show 命令	使用 show 命令可查看 SmartFabric 相关的配置信息。
		SmartFabric 服务模式下的未标记 VLAN 支持	在 SmartFabric 服务模式下为 FCoE 上行链路和 FCoE 支持的服务器端口（这是 FCoE VLAN 的一部分）使用任何未标记的 VLAN。
		使用 SmartFabric Director 的生命周期管理	GNMI 代理处理来自 SmartFabric Director 服务器的映像升级或降级请求。服务器可以使用 Google Network 操作接口 (gNOI) API 调用将这些请求发送到 gNMI 代理。
		gRPC 网络管理接口代理	使用 gNMI 协议和 Openconfig Yang 模型支持 OS10 设备配置的新接口。支持通过 gNOI 协议在 OS10、遥测代理配置、

表. 3: 10.5.0.1 中的新功能 (续)

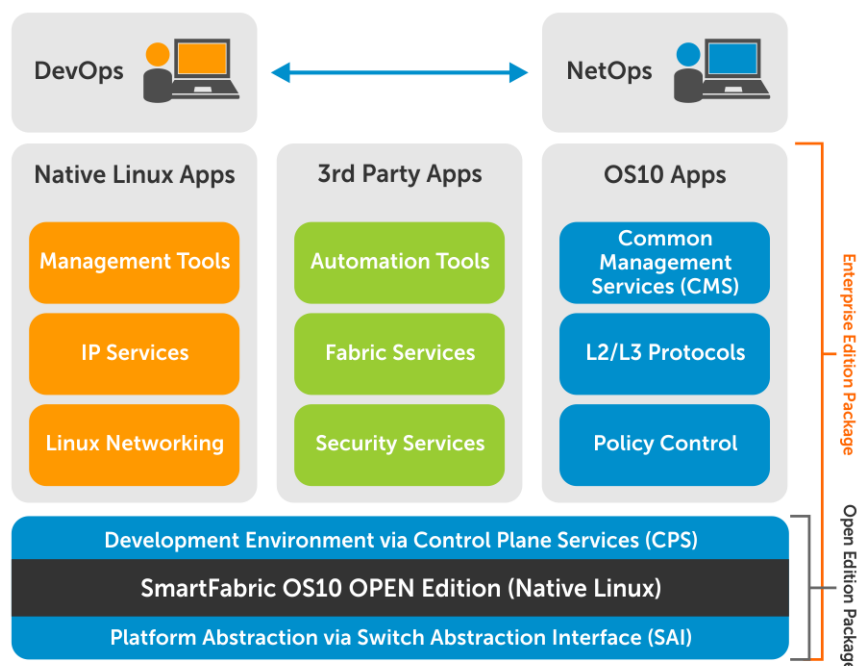
版本	日期	功能部件	说明
			OS10 生命周期管理 (LCM) 上创建、读取、更新和删除 (CRUD) 操作。
		VLT 域中的 TLV 管理地址	发送与 VLT 对等主机上的管理地址 TLV 对应的虚拟地址。
		默认主机名称	使用模块插槽格式设置默认主机名称。
		SmartFabric 服务模式下的 VLT 备份链路	VLT 对等节点存活检查将在 SmartFabric 服务模式下自动配置。

表. 4: 10.5.0.0 中的新功能

版本	日期	功能部件	说明
A00	2019-08-09	VLT 多播路由	在 VLT 域上配置 IPv4 网络的多播路由。
		DHCP 侦听	监控 DHCP 消息并阻止不受信任或流氓 DHCP 服务器。
		使用 BSR 机制配置动态 RP	自动发现多播网络中给定多播组的集合点 (RP)。
		- VXLAN - 多-AS - 集中第 3 层网关路由 - 边界分支网关	- 在 BGP EVPN 环境中使用多 AS 系统。 - 在集中式网关拓扑中配置路由 - 在边界分支拓扑中配置路由
		系统事件和警报	使用严重性配置文件更改事件的严重性。
		证书吊销	验证发证 CA 是否尚未撤销对等证书。
		将 iBGP 路由重新分发到 OSPF	重新分发使用内部 BGP 到 OSPF 学习的路由。
		端口到端口管道和 MMU 映射	有关使用相同端口管道的接口进行入口和出口以获得最佳性能的建议。
		配置 openflow	为 IPv4 和 IPv6 网络上的 OpenFlow 配置多个控制器。
		NPIV 代理网关级联	在融合网络适配器 (CNA) 或光纤通道主机总线适配器 (FC HBA) 和 FCoE 转发器 (FCF) 交换机之间将两台交换机作为 NPIV 代理网关 (NPIV) 进行连接。
		隐匿密码	在 show 命令输出中隐匿密码，以使文本字符不显示。
		RADIUS 身份验证	指定一个接口，其 IP 地址用作 RADIUS 服务器的用户身份验证的源 IP 地址。
		简单密码检查	关闭默认的强密码检查，并配置更简单的密码（无限制）。
		SupportAssist	对适用于企业系统 SupportAssist 的新更新。
		系统时钟	配置夏令时配置。
		通过 TLS 的系统日志记录	使用传输层安全 (TLS) 协议将已记录的系统消息加密发送至 syslog 服务器。
		VLAN 名称 TLV	使用 LLDP PDU 中的 VLAN 名称将 OS10 配置为通告 TLV。

系统

Dell EMC SmartFabric OS10 是支持多种体系结构和环境的网络操作系统 (NOS)。SmartFabric OS10 解决方案允许多层分散化的网络功能。SmartFabric OS10 在 CLI、SNMP 和 REST 接口上捆绑了行业标准管理、监控及 L2 和 L3 网络堆栈。用户可以选择自己的第三方网络、监控、管理和编排应用程序。为了开发可扩展的 L2 和 L3 网络，SmartFabric OS10 在单个二进制图像中提供模块化和分散解决方案。



SmartFabric OS10 关键功能

- 传统网络操作集成的标准网络功能、接口和脚本功能
- 通过交换机抽象接口 (SAI) 的基于标准的切换硬件抽象
- 通过控制面服务 (CPS) 的普遍、无限制的开发人员环境
- 第 2 层交换和第 3 层路由协议，带有集成的 IP 服务、服务质量、可管理性和自动化功能
- 通过在具有独特 VLT 功能的两个 DC 内扩展 L2 VLAN，提高 VM 移动性区域
- 使用批处理和别名简化配置管理的编程 API 和 CLI 自动化
- 数据中心桥接的聚合网络支持，具有优先级流控制 (802.1Qbb)、ETS (802.1Qaz)、DCBx 和 iSCSI TLV

要求

- 已启用开放网络安装环境 (ONIE) 的 Dell EMC 设备
- 要安装：将 SmartFabric OS10 软件映像存储在服务器上 (HTTP、FTP、SCP、SFTP、TFTP) 或通用串行总线 (USB) 介质
- 要配置：设置远程访问 SmartFabric OS10 交换机 — 请参阅[远程访问](#)。

后续步骤：确定启用 Dell EMC ONIE 的交换机是否已安装出厂 OS10 或未安装操作系统。转至[出厂安装 OS10 的交换机](#)或[未安装操作系统的交换机](#)。

受支持的平台：有关您的 SmartFabric OS10 版本当前支持的 Dell EMC 交换机的列表，请参阅 *SmartFabric OS10 Release Notes*。SmartFabric OS10 Release Notes 存储在具有 SmartFabric OS10 软件更新的 Dell Digital Locker 中 ([DDL](#)) 中。

出厂安装 OS10 的交换机

交换机可能附带出厂加载的 OS10 Enterprise Edition。OS10 升级可从 Dell Digital Locker ([DDL](#)) 下载。出厂加载的 OS10 映像包含永久许可证。

在出厂安装的 OS10 交换机上，您可以在登录后执行以下任务：

- 检查 OS10 版本。
- 升级 OS10 映像。
- 重新安装许可证。

如果在交换机上预安装了 OS10，则默认情况下启用零接触部署 (ZTD)。您可以将 ZTD 配置为安装新的 OS10 映像。有关如何自动执行交换机部署的详细信息，请参阅[零接触部署](#)。

注：如果在引导至 ONIE：Install OS 模式后除了出厂安装的 OS10 映像，不必重新安装即可。

MX 以太网 I/O 模块

在 Dell EMC PowerEdge MX 以太网 I/O 模块上，OS10 出厂安装在 MX9116n 结构交换引擎和 MX5108n 以太网交换机上。MX7116n 结构扩展模块不支持 OS10 和用作连接到结构交换引擎的非托管以太网中继器。

登录

使用串行线缆将终端仿真程序连接到交换机上的控制台串行端口。串行端口设置为 115200 波特率、8 数据位和无奇偶校验。

要登录到 OS10 交换机，请启动并等待系统执行开机自检 (POST)。输入 `admin` 作为默认用户名和用户密码。

首次登录 OS10 后更改 `admin` 的默认密码。系统将保存新密码以供将来登录。通过 CLI 更改密码后，使用 `write memory` 命令保存配置。例如：

```
OS10 login: admin
Password: admin
Last login: Sat Oct  6 00:25:33 UTC 2018 on ttyS0
Linux OS10 4.9.110 #1 SMP Debian 4.9.110-3+deb9u4 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

-----
-*          Dell EMC  Network Operating System (OS10)          *-
-*                                                         *-
-* Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved.  *-
-*                                                         *-
-----

This product is protected by U.S. and international copyright and
intellectual property laws. Dell EMC and the Dell EMC logo are
trademarks of Dell Inc. in the United States and/or other
jurisdictions. All other marks and names mentioned herein may be
trademarks of their respective companies.

OS10# configure terminal
% Error: ZTD is in progress(configuration is locked).
OS10# ztd cancel
OS10# configure terminal
OS10(config)# username admin password alpha404! role sysadmin
OS10(config)# exit
OS10# write memory
```

检查 OS10 版本

Dell EMC 建议您将工厂加载的 OS10 升级到最新的 OS10 版本。

- 要检查当前版本的 OS10 映像，请使用 `show version` 命令。
- 要检查可下载的 OS10 版本，请按照 [OS10 升级 > 下载 OS10](#) 中的过程进行升级。

检查 OS10 版本

```
OS10# show version
```

```
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2019 by Dell Inc. All Rights Reserved.
OS Version: 10.5.0.0
Build Version: 10.5.0.270
Build Time: 2019-07-29T23:35:01+0000
System Type: S4148F-ON
Architecture: x86_64
Up Time: 1 day 00:54:13
```

OS10 升级

要升级 OS10 映像，请先下载并解压缩新的 OS10 二进制映像（如[下载 OS10 映像](#)中所述）。然后，将二进制映像文件复制到本地服务器，然后按照[安装 OS10 升级](#)中的步骤进行操作。

注：要将 Dell EMC ONIE 交换机从 OS9 或另一个网络操作系统 (NOS) 升级到 OS10，请按照[未安装操作系统的交换机](#)中的步骤进行操作。

下载 OS10 映像以进行升级

注：对于 MX 系列以太网 I/O 模块，OS10 更新打包戴尔升级包 (DUP)，并且可以从 www.dell.com/support/ 下载。有关如何下载 DUP 文件以及升级 MX9116n 和 MX5108n 交换机上 OS10 的信息，请参阅 *Dell EMC SmartFabric OS10 Release Notes—Release 10.5.0*。

要升级现有的 OS10 映像，请首先从 DDL 下载新的 OS10 Enterprise Edition 映像。

1. 使用您的帐户凭据登录到 [DDL](#)。
2. 找到您的授权 ID 和订单编号的条目，然后选择产品名称。
3. 选择“Product”页上的 **Available Downloads** 选项卡。
4. 选择要下载的 OS10 Enterprise Edition 映像，然后单击 **Download**。
5. 阅读戴尔终端用户许可协议，然后滚动到协议末尾并单击 **Yes, I agree**。
6. 选择如何下载软件文件，然后单击 **Download Now**。
7. 下载 OS10 Enterprise Edition 映像后，打开 tar 文件的包装并将 OS10 二进制映像存储在本地服务器上。要打开 tar 文件的包装，请遵循以下指导准则：
 - 从 tar 文件中提取 OS10 二进制文件。例如，要打开 Linux 服务器上的 tar 文件或从 ONIE 提示符中解压缩，请输入：

```
tar -xf tar_filename
```

注：某些 Windows 的解压缩应用程序会在提取 tar 文件的内容时插入额外的回车 (CR) 或换行符 (LF)。额外的 CR 和 LF 可能会损坏下载的 OS10 二进制映像。如果您使用基于 Windows 的工具解压缩 OS10 二进制文件，请关闭此选项。例如，在 WinRAR 中的“高级选项”选项卡下，取消选择 tar 文件智能 CR/LF 转换功能。

- 通过在映像文件上使用 md5sum 命令为下载的 OS10 二进制文件生成校验和。确保生成的校验和与从 tar 文件中提取的映像 MD5 文件中的校验和相匹配。

```
md5sum image_filename
```

8. 请按照[安装 OS10 升级](#)中的步骤进行操作。

安装 OS10 升级

下载并解压缩新 OS10 二进制映像后，如[下载 OS10 映像](#)中所述，请执行以下步骤：

注：在 VLT 配置程序中的 OS10 映像升级过程中，当 VLT 设备运行不同的软件版本时，在 VLT 设备上不能进行任何配置更改。请确保将两个设备升级到相同的版本，然后再进行任何配置更改。

注：在 MX 系列 I/O 模块上，按照 *Dell EMC SmartFabric OS10 Release Notes—Release 10.5.0* 中的说明，在下方的 DUP 文件中安装 OS10 升级。

1. （可选）在 EXEC 模式下将当前运行的配置备份到启动配置。

```
OS10# copy running-configuration startup-configuration
```

2. 在 EXEC 模式下备份启动配置 startup.xml)。

```
OS10# copy config://startup.xml config://backup_filepath
```

3. 在 EXEC 模式下，使用 `image download server-filepath/filename` 命令从本地服务器下载新 OS10 二进制映像；例如：

```
OS10# image download sftp://admin:passwd@10.1.1.1/home/admin/images/OS10EE.bin
```

4. (可选) 在 EXEC 模式下查看当前的软件下载状态。

```
OS10# show image status
```

5. 在 EXEC 模式下使用 `image install file-url` 命令在待机分区中安装 OS10 映像，其中 `filename` 是在步骤 3 中通过 `image download` 命令下载的映像文件的名称；例如：

```
OS10# image install image://OS10EE.bin
```

注： OS10 有两个分区：A 和 B。一个分区处于活动状态，这是当前运行的版本，在下次系统重新加载时用作正在运行的软件。另一个分区仍保持备用状态，即安装软件升级的分区。

`image install` 命令将下载的映像安装到备用分区。如果活动分区包含任何经过修改的文本文件或已安装的自定义软件包，则这些文件在待机分区中将不可用。在下载映像后，备份修改的文件并重新安装软件包。

注： 在 MX9116n 结构交换引擎和 MX5108n 以太网交换机上，如果使用 DUP 文件安装 OS10 映像，则所有固件组件都会进行升级。固件升级存储为挂起安装，直到您重新加载交换机为止。要查看固件升级的内容，请使用 `show image firmware` 命令。

6. (可选) 在 EXEC 模式下查看软件安装的状态。

```
OS10# show image status
```

7. 将下一次引导分区更改为将下载的 OS10 映像存储在 EXEC 模式下的备用分区。

```
OS10# boot system standby
```

8. (可选) 在 EXEC 模式中验证下一个引导分区已更改为待机状态；例如：

```
OS10# show boot
Current system image information:
=====
Type          Boot Type      Active              Standby              Next-Boot
-----
Node-id 1 Flash Boot      [B] 10.5.0.0        [A] 10.5.0.0        [B] active
```

```
OS10# show boot detail
Current system image information detail:
=====
Type:                      Node-id 1
Boot Type:                  Flash Boot
Active Partition:           B
Active SW Version:           10.5.0.0
Active SW Build Version:     10.5.0.270
Active Kernel Version:       Linux 4.9.168
Active Build Date/Time:      2019-07-29T23:35:01Z
Standby Partition:          A
Standby SW Version:          10.5.0EX
Standby SW Build Version:     10.5.0EX.252
Standby Build Date/Time:     2019-07-27T17:31:55Z
Next-Boot:                   active[B]
```

9. 在 EXEC 模式下的备用分区中重新加载新软件映像。

```
OS10# reload
```

10. 在 EXEC 模式下使用 `show version` 命令，以验证下载的 OS10 映像是否安装为当前运行的版本。正在运行的 OS10 映像位于活动分区中。

```
OS10# show version
Dell EMC Networking OS10 Enterprise
```

```
Copyright (c) 1999-2019 by Dell Inc. All Rights Reserved.
OS Version: 10.5.0.0
Build Version: 10.5.0.270
Build Time: 2019-07-29T23:35:01+0000
System Type: S4148F-ON
Architecture: x86_64
Up Time: 1 day 00:54:13
```

安装固件升级

您可能需要升级 OS10 交换机上的固件组件，而无需升级 OS10 映像。要在单独的操作中升级固件组件：

1. 在 EXEC 模式下使用 `image download server-filepath/firmware-filename` 命令从服务器下载 OS10 固件文件；例如：

```
OS10# image download http://10.11.8.184/tftpboot/users/regr//neteng/okelani/files
/new/onie-firmware-x86_64-dellemc_s5200_c3538-r0.3.40.5.1-9.bin
```

2. 在 EXEC 模式下使用 `image install firmware-file-url` 命令安装 OS10 固件文件，其中 `firmware-file` 是在步骤 1 中下载的固件文件的名称；例如：

```
OS10# image install image://onie-firmware-x86_64-dellemc_s5200_c3538-r0.3.40.5.1-9.bin
```

要查看挂起的固件升级，请使用 `show image firmware` 命令。要取消固件安装并移除所有待处理的固件升级，请使用 `image cancel` 命令。

3. 在 EXEC 模式下重新加载交换机。

```
OS10# reload
```

升级命令

boot system

设置用于下一次重新引导的引导分区。

语法	<code>boot system {active standby}</code>
参数	• <code>active</code> — 将正在运行的分区重置为下一个引导分区。 • <code>standby</code> — 将备用分区设置为下一引导分区。
默认	活动
命令模式	EXEC
使用情况信息	使用此命令可配置在引导时用于重新加载软件的 OS10 映像的位置。使用 <code>show boot</code> 命令查看配置的下一个引导映像。此命令会立即应用，不需要 <code>commit</code> 命令。
示例	<pre>OS10# boot system standby</pre>
支持的版本	10.2.0E or later

image cancel

取消正在进行的映像或固件文件下载。

语法	<code>image cancel</code>
参数	无
默认	未配置
命令模式	EXEC

使用情况信息	<code>image cancel</code> 命令会从服务器（例如正在进行的 OS10 二进制映像或固件升级）取消文件下载。映像下载完成后，该命令不起作用。命令还将移除交换机上所有待处理的固件升级。
示例	<pre>OS10# image cancel</pre>
支持的版本	10.2.0E or later

image copy

将活动分区中的整个映像复制到备用分区（镜像映像）。

语法	<code>image copy active-to-standby</code>
参数	<code>active-to-standby</code> — 输入将活动分区中的整个映像复制到备用分区（镜像映像）。
默认	未配置
命令模式	EXEC
使用情况信息	将正在运行的活动软件映像复制到备用映像位置。
示例	<pre>OS10# image copy active-to-standby</pre>
支持的版本	10.2.0E or later

image download

将新的软件映像或固件文件下载到本地文件系统。

语法	<code>image download file-url</code>
参数	<code>file-url</code> — 输入映像文件的 URL： <code>ftp://userid:passwd@hostip:/filepath</code> — 输入要从远程 FTP 服务器复制的路径。 <code>http[s]://hostip:/filepath</code> — 输入要从远程 HTTP 或 HTTPS 服务器复制的路径。 <code>scp://userid:passwd@hostip:/filepath</code> — 输入要从远程 SCP 文件系统复制的路径。 <code>sftp://userid:passwd@hostip:/filepath</code> — 输入要从远程 SFTP 文件系统复制的路径。 <code>tftp://hostip:/filepath</code> — 输入要从远程 TFTP 文件系统复制的路径。 <code>usb://filepath</code> — 输入要从 USB 文件系统复制的路径。
默认	未配置
命令模式	EXEC
使用情况信息	<code>image download</code> 命令用于将映像文件下载到 <code>image</code> 目录。使用 <code>dir image</code> 命令可显示 <code>image</code> 目录的内容。OS10 SW 映像文件很大，并且会占用大量的磁盘空间。Dell EMC Networking 建议您通过使用 <code>delete</code> 命令从 <code>image</code> 目录中删除不必要的图像文件；例如： <pre>delete image://OS10EE-10.2.0.bin</pre> 使用 <code>show image status</code> 命令查看下载进度。 使用 <code>scp</code> 和 <code>sftp</code> 选项时，请始终输入绝对文件路径（而不是相对于用户帐户主目录的路径）。例如： <pre>image download sftp://dellos10:password@10.1.1.1/home/dellos10/images/PKGS_OS10EE-10.4.3.bin</pre>
示例	<pre>OS10# image download sftp://dellos10:adminTo%40%20@10.1.1.1/home/dellos10/images/PKGS_OS10-Enterprise-10.4.0E.55-installer-x86_64.bin</pre>
支持的版本	10.2.0E or later

image install

从以前下载的文件或远程位置安装新的映像或固件文件。

语法	image install file-url
参数	- file-url — 映像或固件文件的位置： - ftp://userid:passwd@hostip:/filepath — 输入要从远程 FTP 服务器安装的路径。 - http[s]://hostip:/filepath — 输入要从远程 HTTP 或 HTTPS 服务器安装的路径。 - scp://userid:passwd@hostip:/filepath — 输入要从远程 SCP 文件系统安装的路径。 - sftp://userid:passwd@hostip:/filepath — 输入要从远程 SFTP 文件系统安装的路径。 - tftp://hostip:/filepath — 输入要从远程 TFTP 文件系统安装的路径。 - image://filename — 输入要用于从本地文件系统安装映像的路径。 - usb://filepath — 输入要用于从 USB 文件系统安装映像的路径。
默认	全部
命令模式	EXEC
使用情况信息	使用 show image status 命令可查看安装进度。
示例	<pre>OS10# image install ftp://10.206.28.174:/PKGS_OS10-Enterprise-10.4.0E.55-installer-x86_64.bin</pre>
支持的版本	10.2.0E or later

show boot

显示引导分区相关的信息。

语法	show boot [detail]
参数	detail — (可选) 输入以显示详细信息。
默认	未配置
命令模式	EXEC
使用情况信息	使用 boot system 命令为下一次重新引导设置引导分区。
示例	<pre>OS10# show boot Current system image information: ===== Type Boot Type Active Standby Next-Boot ----- Node-id 1 Flash Boot [B] 10.5.0.0 [A] 10.5.0.0 [B] active</pre>
示例 (详细信息)	<pre>OS10# show boot detail Current system image information detail: ===== Type: Node-id 1 Boot Type: Flash Boot Active Partition: B Active SW Version: 10.5.0.0 Active SW Build Version: 10.5.0.270 Active Kernel Version: Linux 4.9.168 Active Build Date/Time: 2019-07-29T23:35:01Z Standby Partition: A Standby SW Version: 10.5.0EX Standby SW Build Version: 10.5.0EX.252 Standby Build Date/Time: 2019-07-27T17:31:55Z Next-Boot: active[B]</pre>
支持的版本	10.2.0E or later

show image firmware

显示所有待处理的固件升级和过去的固件升级的状态。

语法	show image firmware
参数	无
默认	未配置
命令模式	EXEC
使用情况信息	如果安装的是 OS10 固件文件，则固件升级将存储为待定安装，直到您重新加载交换机为止。要查看固件升级的内容，请使用 show image firmware 命令。如果没有可用的挂起或过期的固件升级，则在 show 命令输出中将不会显示任何条目。

示例	<pre>OS10# show image firmware Upgrade State: pending reload (staged) Pending Firmware Upgrade(s) # Name Version Date ----- 1 onie-firmware-x86_64-dellemc_mxseries-r0.3.35.5.1-17.bin 3.35.5.1 2019-03-25 15:19:19 2 cpld-fw-mx5108n-r1.5.4.1.bin 1.5.4.1 2019-03-25 15:19:19 3 bios-20190225-xt-3.34.8.10a.bin 3.34.8.10 2019-03-25 15:19:19 Past Firmware Upgrade(s) Name Version Result ----- onie-firmware-x86_64-dellemc_mxseries-r0.3.35.5.1-15.bin 3.35.5.1 Success onie-updater-x86_64-dellemc_mxseries-r0 3.35.1.1 Success</pre> <pre>OS10# show image firmware Pending Firmware Upgrade(s) ===== # Name Version Date ----- ----- Past Firmware Upgrade(s) ===== Name Version Result ----- onie-firmware-x86_64-dellemc_s5200_c3538-r0.3.40.5.1-6. 3.40.5.1-6 Success onie-updater 3.40.1.1-5 Fail onie-updater-x86_64-dellemc_s5200_c3538-r0.3.40.1.1-6 3.40.1.1-6 Fail</pre>

支持的版本 10.5.0 or later

show image status

显示映像传输和安装信息。

语法	show image status

参数	无
默认	未配置
命令模式	EXEC
使用情况信息	在较低版本的 OS10 中，image install 命令可能会显示为冻结状态，并且不会显示当前的映像状态。复制 SSH 或 Telnet 会话，然后重新输入 show image status 命令以查看当前状态。

示例	<pre> OS10# show image status Image Upgrade State: install ===== File Transfer State: idle ----- State Detail: Completed: No error Task Start: 2019-01-03T17:37:49Z Task End: 2019-01-03T17:38:04Z Transfer Progress: 100 % Transfer Bytes: 489894821 bytes File Size: 489894821 bytes Transfer Rate: 31657 kbps Installation State: install ----- State Detail: In progress: Installing Task Start: 2019-01-03T17:38:04Z Task End: 0000-00-00T00:00:00Z </pre>

支持的版本	10.2.0E or later

show version

显示软件版本信息。

语法	show version
参数	无
默认	未配置
命令模式	EXEC
使用情况信息	无

示例	<pre> OS10# show version Dell EMC Networking OS10 Enterprise Copyright (c) 1999-2019 by Dell Inc. All Rights Reserved. OS Version: 10.5.0.0 Build Version: 10.5.0.270 Build Time: 2019-07-29T23:35:01+0000 System Type: S4148F-ON Architecture: x86_64 Up Time: 1 day 00:54:13 </pre>

支持的版本	10.2.0E or later

检查 OS10 许可证

要检查预安装的 OS10 许可证的状态，请使用 show license status 命令。出厂安装的 OS10 映像使用永久许可证运行。永久许可证允许您在 120 天试用期内运行 OS10。有关详情，请参阅您的设备随附的设置指南。

查看许可证状态

<pre> OS10# show license status System Information ----- </pre>

```

Vendor Name       : DELL EMC
Product Name      : S4148F-ON
Hardware Version  : X01
Platform Name     : x86_64-dell_s4100_c2338-r0
PPID             : TW09H9MN282987130026
Service Tag       : 9531XC2
Product Base      :
Product Serial Number:
Product Part Number :
License Details
-----
Software          : OS10-Enterprise
Version           : 10.5.0EX
License Type       : PERPETUAL
License Duration   : Unlimited
License Status     : Active
License location   : /mnt/license/9531XC2.lic
-----

```

重新安装许可证

OS10 Enterprise Edition 在出厂时已加载 OS10 的设备上运行永久许可证。在交换机上预安装了许可证文件。如果许可证已损坏或被删除，您必须从购买者帐户下的 DDL 下载许可证，并重新安装许可证。

1. 使用您的帐户凭据登录到 [DDL](#)。
2. 使用授权 ID 和订单号查找硬件产品名称。
3. 检查 [Products](#) 页面的 [Assigned To](#) 字段中是否显示设备服务编号。
4. 单击 **Key Available for Download**。
5. 选择如何接收许可证密钥 — 通过电子邮件或下载到本地设备。
6. 单击**提交**。
7. 保存许可证 .zip 文件，然后按照[安装许可证](#)中的说明安装许可证。

未安装操作系统的交换机

如果 Dell EMC 已启用 ONIE 的交换机未安装默认操作系统，您可以从 Dell Digital Locker 下载 OS10 软件映像，并使用 ONIE 进行安装。此外，在以下情况下在 Dell EMC ONIE 设备上安装 OS10：

- 您可以从 OS 9 或任何第三方操作系统转换交换机。
- 您可以从 Dell EMC 退回材料授权 (RMA) 接收更换设备。

您下载的 OS10 映像具有 120 天试用许可证，并且需要在试用期结束后运行永久许可证。有关详细信息，请参阅设备随附的安装指南和以下常见问题解答：

- [常见问题](#)
- [我的帐户常见问题](#)

要在未安装操作系统的 Dell EMC ONIE 交换机上安装 OS10 映像并延长 OS10 许可证，请执行以下操作：

1. （可选）如果在交换机上安装了不同的操作系统（如 OS 9 或第三方操作系统），请卸载现有操作系统 — [卸载现有操作系统](#)。
2. [下载 OS10 映像](#)
3. [使用 ONIE 安装 OS10](#)
4. [登录到交换机](#)
5. [下载并安装 OS10 许可证](#)

相关 ONIE 说明文件

有关使用 ONIE 的其他信息，请参阅：

- [ONIE 用户指南](#)
- [ONIE — 在交换机上手动加载 DNOS](#)

将 OS9 升级到 OS10

当您从 OS9 交换机升级到 OS10 时，第一步是使用 ONIE 引导菜单上的 **ONIE: Uninstall OS** 选项卸载 OS9。卸载选项将删除 OS9 配置和所有磁盘分区。在卸载 OS9 之后，请遵循未安装操作系统的 ONIE 交换机的步骤 — 请参阅[下载 OS10 映像](#)、[使用 ONIE 安装](#)以及[安装 OS10 许可证](#)。

RMA 更换

更换交换机无需安装操作系统或许可证。如果收到更换交换机，则必须将更换交换机的服务编号 (STAG) 分配给 DDL 中的 SW 权利并安装 OS10 软件和许可证。

要下载 OS10 Enterprise Edition 和许可证，请遵循未安装操作系统的 ONIE 交换机的步骤 — 请参阅[下载 OS10 映像](#)、[使用 ONIE 安装](#)以及[安装 OS10 许可证](#)。

卸载现有操作系统

 **小心:** 要在运行 OS9 或其他第三方操作系统的交换机上安装 OS10，必须先卸载现有操作系统。卸载将删除交换机配置和所有磁盘分区。

要在 Dell EMC ONIE 交换机上卸载 OS9 或第三方操作系统，请引导交换机并观察要显示的 ONIE 引导菜单。立即使用箭头键滚动星号并选择 ONIE: Uninstall OS 选项以避免默认情况下交换机引导至 ONIE: Install OS。

```
+-----+
| ONIE: Install OS          |
| ONIE: Rescue              |
| *ONIE: Uninstall OS      |
| ONIE: Update ONIE        |
| ONIE: Embed ONIE         |
| ONIE: Diag ONIE          |
+-----+
```

ONIE 卸载过程完成后，交换机将引导至 ONIE: Install OS 模式。

下载 OS10 映像

如果您是在销售单点订购之后购买 OS10 Enterprise Edition 映像，则您购买的 OS10 允许在所有权 90 天内下载发布的软件映像。完成订单后，您将收到一封电子邮件通知，其中包含软件授权 ID、订单号和指向该 DDL 的链接。

要延长软件授权的下载期，您必须在硬件上拥有 Dell EMC ProSupport 或 ProSupport Plus 合同。将软件权限绑定到交换机服务编号，使其与支持合同保持一致：

 **注:** 在 10.5.0.1 和更高版本中，MX 系列以太网 I/O 模块支持 OS10。OS10 映像打包为戴尔升包 (DUP)，并且可以从 www.dell.com/support/ 下载。有关如何下载 DUP 文件以及 MX9116n 和 MX5108n 交换机上 OS10 的信息，请参阅 *Dell EMC SmartFabric OS10 Release Notes—Release 10.5.0*。

1. 使用您的帐户凭据登录到 [DDL](#)。
2. 找到您的授权 ID 和通过电子邮件发送的订单编号，然后选择产品名称。
3. 在 **Product** 页面上，“Product”产品选项卡上的 Assigned To 字段为空。单击 **Key Available for Download**。
4. 在 Bind to 和 Re-enter ID 字段中输入您购买了 OS10 Enterprise Edition 的设备服务编号。此步骤将软件权利绑定到交换机的服务编号。
5. 选择如何接收许可证密钥：通过电子邮件或下载到本地设备。
6. 单击 **Submit** 以下载许可证 .zip 文件。
7. 选择 **Available Downloads** 选项卡。
8. 选择要下载的 OS10 Enterprise Edition 版本，然后单击 **Download**。
9. 阅读戴尔终端用户许可协议。滚动到协议的末尾，然后单击 **Yes, I agree**。
10. 选择如何下载软件文件，然后单击 **Download Now**。
11. 下载 OS10 Enterprise Edition 映像后，打开 tar 文件的包装并将 OS10 二进制映像存储在本地服务器上。要打开 tar 文件的包装，请遵循以下指导准则：
 - 从 tar 文件中提取 OS10 二进制文件。例如，要打开 Linux 服务器上的 tar 文件或从 ONIE 提示符中解压缩，请输入：

```
tar -xf tar_filename
```

- 通过在映像文件上运行 md5sum 命令，为下载的 OS10 二进制映像生成校验和。确保生成的校验和与从 tar 文件中提取的映像 MD5 文件中的校验和相匹配。

```
md5sum image_filename
```

12. 按照[使用 ONIE 安装](#)中的步骤进行操作，并[安装 OS10 许可证](#)以安装 OS10 Enterprise Edition 映像和许可证。

使用 ONIE 进行安装

 **小心:** 使用 ONIE 安装 OS10 或另一个操作系统会擦除交换机上的所有配置。配置置不可恢复。在进行操作系统更新或更改之前，备份交换机上的所有配置和已安装的可。将交换机配置的定期备份存到交换机。

如果您购买仅限 ONIE 的交换机或要更换现有操作系统，请按照 [下载 OS10 映像](#) 中的说明下载 OS10 映像。然后，使用基于 ONIE 的自动查找或手动安装来安装 OS10 软件映像：

- **自动安装** — ONIE 发现网络信息，包括动态主机配置协议 (DHCP) 服务器、连接到映像服务器，并自动下载和安装映像。
- **手动安装** — 如果 DHCP 服务器不可用或您使用 USB 介质安装 OS10 软件映像，请手动配置您的网络信息。

系统设置程序

安装之前，请验证系统是否连接正确：

- 将串行线缆和终端仿真程序连接到控制台串行端口 — 串行端口设置为 115200 波特率、8 数据位和无奇偶校验。
- 将管理端口连接到网络以便通过网络下载映像。要找到控制台端口和管理端口，请参阅特定于平台的 [安装指南](#)，网址：www.dell.com/support。

安装 OS10

对于启用了 ONIE 的交换机，请转至 ONIE 引导菜单。启用了 ONIE 的交换机通过预加载的诊断程序（诊断）和 ONIE 软件进行引导。

```
+-----+
|*ONIE: Install OS
| ONIE: Rescue
| ONIE: Uninstall OS
| ONIE: Update ONIE
| ONIE: Embed ONIE
| ONIE: Diag ONIE
+-----+
```

- 安装操作系统 — 引导至 ONIE 提示符，并使用自动查找流程安装 OS10 映像。当 ONIE 安装新的操作系统映像时，将删除之前安装的映像和 OS10 配置。
- 修复 — 引导至 ONIE 提示符，并启用 OS10 映像或 ONIE 更新的手动安装。
- 卸载操作系统 — 删除所有磁盘分区的内容，包括 OS10 配置（ONIE 和诊断除外）。
- 更新 ONIE — 安装新的 ONIE 版本。
- 嵌入 ONIE — 格式化磁盘并安装 ONIE。
- EDA 诊断 — 运行系统诊断程序。

ONIE 进程安装 OS10 映像并随后在 ONIE: Install OS 模式重新引导交换机（默认）时，ONIE 将获得系统的所有权并保持安装模式（ONIE 安装模式为粘滞），直至 OS10 映像再次成功安装。要出于安装以外的任何原因从 ONIE 引导交换机，请从 ONIE 引导菜单中选择 ONIE: Rescue 或 ONIE: Update ONIE 选项。

 **小心:** 在自或手 OS10 安装期，如果出情况，致安装失，并且上存在有的操作系， Uninstall OS 以清除分区。如果仍然存在，系 Dell EMC 技支持。

自动安装

您可以在启用了 ONIE Dell EMC 的设备上自动安装 OS10 映像。此过程称为零接触安装。在设备引导至 ONIE: Install OS 后，ONIE 自动查找将按照以下步骤查找安装程序文件，并使用第一种成功的方法：

1. 使用从引导加载程序传递的静态配置的路径。
2. 在本地连接的设备上搜索文件系统，如 USB。
3. 从 DHCPv4 服务器搜索确切的 URL。
4. 根据 DHCP 的响应搜索不精确的 URL。
5. 搜索 IPv6 邻居。
6. 启动 TFTP 瀑布。

ONIE 自动查找进程会查找存储的软件映像，下载并安装它，然后使用新映像重新引导设备。自动发现将重复，直至成功安装软件映像并重新引导交换机。

ONIE 查找 — 使用情况信息

- 所有 ONIE 自动查找方法仅下载并运行受支持的默认文件名，例如 onie-installer。开放网络安装环境网站中介绍了所需的文件名和搜索顺序，网址为 [查找和执行](#)。有关详细信息，请参阅 [Dell EMC 支持站点](#) 上的 *Open Networking Hardware Diagnostic Guide*。

- 如果您使用的是 DHCPv4 服务器，ONIE 自动查找会从 DHCP 服务器和 DHCP 选项获取域名服务器 (DNS) 的主机名称、域名、管理接口 IP 地址和 IP 地址。它还会使用 ONIE 服务器的默认 DNS 搜索 SCP、FTP 或 TFTP 服务器。DHCP 选项不用于提供服务器 IP。
- 如果您使用的是 USB 存储设备，ONIE 仅在 FAT 或 EXT2 文件系统中搜索 OS10 映像。

示例：OS10 自动安装

1. 在 TFTP 服务器上，使用 `mv image-name default-filename` 命令将 OS10 映像重命名为支持的安装程序文件名，例如 `onie-installer`。

```
mv PKGS_OS10-Base-10.3.1B.144-installer-x86_64.bin onie-installer
```

2. 启动交换机的 ONIE：Install 模式以安装 OS10 映像。

```
Starting: discover... done.
ONIE:/ # Info: eth0: Checking link... up.
Info: Trying DHCPv4 on interface: eth0
ONIE: Using DHCPv4 addr: eth0: 10.10.10.17 / 255.0.0.0
Info: eth1: Checking link... down.
ONIE: eth1: link down. Skipping configuration.
ONIE: Failed to configure eth1 interface
ONIE: Starting ONIE Service Discovery
Info: Fetching tftp://10.10.10.2/onie-installer-x86_64-dellemc_s4148fe_c2338 ...
Info: Fetching tftp://10.10.10.2/onie-installer-dellemc_s4148fe_c2338 ...
Info: Fetching tftp://10.10.10.2/onie-installer-x86_64-bcm ...
Info: Fetching tftp://10.10.10.2/onie-installer-x86_64 ...
Info: Fetching tftp://10.10.10.2/onie-installer ...
ONIE: Executing installer: tftp://10.10.10.2/onie-installer
...
...
...
Press <DEL> or <F2> to enter setup.
Welcome to GRUB!

GNU GRUB version 2.02~beta2+e4a1fe391
OS10-B
EDA-DIAG
ONIE Booting `OS10-A'
Loading OS10 ...

[ 3.883826] kvm: already loaded the other module
[ 3.967628] dummy-irq: no IRQ given. Use irq=N
[ 3.973212] mic_init not running on X100 ret -19
[ 3.980168] esas2r: driver will not be loaded because no ATTO esas2r devices were
found
[ 4.021676] mtdoops: mtd device (mtddev=name/number) must be supplied
[ 5.092316] i8042: No controller found
[ 5.108356] fmc_write_eeprom fake-design-for-testing-f001: fmc_write_eeprom: no
busid passed, refusing all cards
[ 5.120111] intel_rapl: driver does not support CPU family 6 model 77
[ 4.226593] systemd-fsck[493]: OS10-SYSROOT1: clean, 23571/426544 files,
312838/1704960 blocks
Debian GNU/Linux 8 OS10 ttyS0
Dell EMC Networking Operating System (OS10)
OS10 login:
```

手动安装

如果不使用 OS10 映像的基于 ONIE 的自动安装，并且 DHCP 服务器不可用，则可以手动安装映像。配置管理端口并提供软件映像文件以开始安装。

1. 将 OS10 软件映像保存在 SCP/TFTP/FTP 服务器上。
2. 接通交换机电源并选择 ONIE Rescue 以进行手动安装。
3. 停止 DHCP 查找。

```
$ onie-discovery-stop
```

4. 配置管理端口上的 IP 地址，其中 `x.x.x.x` 表示内部 IP 地址。配置管理端口后，答复为 `up`。

```
$ ifconfig eth0 x.x.x.x netmask 255.255.0.0 up
```

5. 在设备上安装软件。安装命令从指定的 SCP、TFTP 或 FTP URL 访问 OS10 软件，创建分区，验证安装并重新启动。

```
$ onie-nos-install image_url
```

例如，输入

```
ONIE:/ # onie-nos-install ftp://a.b.c.d/PKGS_OS10-Enterprise-x.x.xx.bin
```

其中，`a.b.c.d` 表示要从中下载映像文件的位置，而 `x.x.xx` 表示要安装的软件版本编号。

OS10 安装程序映像会创建多个分区，包括 OS10-A 和 OS10。安装完成后，交换机会自动重新启动，并从 OS10-A 加载 OS10，默认情况下将成为活动分区。OS10-B 将成为备用分区。

要使用 USB 驱动器手动安装：

您可以使用 USB 设备手动安装 OS10 软件映像。验证 USB 设备是否支持 FAT 或 EXT2 文件系统。有关以 FAT 或 EXT2 格式来格式化 USB 设备的说明，请参阅随附的 Windows 文档以了解 FAT 格式或参阅随附的 Linux 文档以了解 FAT 或 EXT2 格式。

1. 将 USB 存储设备插入交换机上的 USB 存储端口。
2. 打开交换机的电源以使用 ONIE: Rescue 选项自动引导。
3. (可选) 如果设备引导至 ONIE: Install，请停止 ONIE 查找。

```
$ onie-discovery-stop
```

4. 在系统上创建 USB 装载位置。

```
$ mkdir /mnt/media
```

5. 识别 USB 驱动器的路径。

```
$ fdisk -l
```

6. 将 USB 介质插入设备的 USB 端口。

```
$ mount -t vfat usb-drive-path /mnt/media
```

7. 从 USB 安装软件，其中 `/mnt/media` 指定 USB 分区的装载路径。

```
$ onie-nos-install /mnt/media/image_file
```

ONIE 自动查找进程会查找指定 USB 路径下的映像文件，加载软件映像并重新引导交换机。有关详情，请参阅 [ONIE User Guide](#)。

登录

使用串行线缆将终端仿真程序连接到交换机上的控制台串行端口。串行端口设置为 115200 波特率、8 数据位和无奇偶校验。

要登录到 OS10 交换机，请启动并等待系统执行开机自检 (POST)。输入 `admin` 作为默认用户名和用户密码。

首次登录 OS10 后更改 `admin` 的默认密码。系统将保存新密码以供将来登录。通过 CLI 更改密码后，使用 `write memory` 命令保存配置。例如：

```
OS10 login: admin
Password: admin
Last login: Sat Oct  6 00:25:33 UTC 2018 on ttyS0
Linux OS10 4.9.110 #1 SMP Debian 4.9.110-3+deb9u4 x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```



```
-----
-*          Dell EMC  Network Operating System (OS10)          *-
-*                                                         *-
-* Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved.   *-
-*                                                         *-
-----

This product is protected by U.S. and international copyright and
intellectual property laws. Dell EMC and the Dell EMC logo are
trademarks of Dell Inc. in the United States and/or other
jurisdictions. All other marks and names mentioned herein may be
trademarks of their respective companies.

OS10# configure terminal
% Error: ZTD is in progress(configuration is locked).
OS10# ztd cancel
OS10# configure terminal
OS10(config)# username admin password alpha404! role sysadmin
OS10(config)# exit
OS10# write memory
```

安装 OS10 许可证

如果在出厂时在您的交换机上加载了 OS10，则无需安装 OS10 许可证。如果您下载试用版 OS10，OS10 将附带 120 天试用许可证。要继续不间断使用，请购买并安装永久许可证，以避免在 120 天后每 72 小时重新引导 OS10 设备。

安装 OS10 并登录后，请安装永久许可证，以便在试用期到期后运行 OS10 Enterprise Edition。OS10 许可证安装在 `/mnt/license` 目录中。

1. 从 DDL 下载 `License.zip` 文件，如[下载 OS10 映像](#)中所述。
2. 打开 zip 文件，并在 Dell 文件夹中找到许可证文件。将许可证文件复制到本地或远程工作站。
3. 在 EXEC 模式下从工作站安装许可证文件。

```
license install {ftp: | http: | localfs: | scp: | sftp: | tftp: | usb:} filepath/
filename
```

- `ftp://userid:passwd@hostip/filepath` — 从远程 FTP 服务器复制。
- `http://hostip/filepath` — 从远程 HTTP 服务器复制。
- `http://hostip` — 将请求发送到远程 HTTP 服务器。
- `localfs://filepath` — 从本地文件目录安装。
- `scp://userid:passwd@hostip/filepath` — 从远程 SCP 服务器复制。
- `sftp://userid:passwd@hostip/filepath` — 从远程 SFTP 服务器复制。
- `tftp://hostip/filepath` — 从远程 TFTP 服务器复制。
- `usb://filepath` — 从连接到交换机上 USB 存储端口的存储设备上的文件目录进行安装。
- `filepath/filename` — 输入存储许可证文件的目录路径。

 **注：**通 VRF 例安装可，OS10 支持某些文件方法。参下表，了解默认、管理和非默认 VRF 例中支持的文件方法。

表. 5: 使用 VRF 安装许可证

文件传输方法	默认 VRF	管理 VRF ¹	非默认 VRF
FTP	是	是	否
HTTP	是	是	否
localfs	是	是	是
SCP	是	是	否
SFTP	是	是	否
TFTP	是	是	否
USB	是	是	是

¹在配置管理 VRF 以用于 OS10 许可证安装之前，请删除管理接口上的所有 IP 地址。

安装许可证 — SCP

```
OS10# license install scp://user:userpwd@10.1.1.10/0A900Q2-NOSEnterprise-License.xml
License installation success.
```

安装许可证 — localfs

请按照以下步骤从本地文件目录安装许可证：

1. 将许可证文件从 FTP 服务器位置复制到系统上的主目录。

```
OS10# copy ftp://admin:admin@10.11.95.101//home/admin/LADF/0A900Q2-NOSEnterprise-
License.XML home://7B900Q2-NOSEnterprise-License.XML
```

2. (可选) 使用 `show copy-file status` 命令检查文件复制的状态。

```
OS10# show copy-file status
File Transfer State:   idle
-----
State Detail:         idle
Task Start:           2019-02-15T00:46:35Z
Task End:              2019-02-15T00:46:36Z
Transfer Progress:    100 %
Transfer Bytes:        3795 bytes
File Size:             3795 bytes
Transfer Rate:         8 kbps
```

3. 验证许可证是否存在于系统的主目录中。

```
OS10# dir home

Directory contents for folder: home
Date (modified) Size (bytes) Name
-----
2019-02-15T00:47:25Z 3795 0A900Q2-NOSEnterprise-License.XML
```

4. 输入 `license install` 命令以及在步骤 1 中下载许可证的主目录位置的路径。

```
OS10# license install localfs://home/admin/0A900Q2-NOSEnterprise-License.XML
[ 5784.994389] EXT4-fs error (device dm-0): ext4_has_uninit_itable:3039: comm
CPS_API_instanc: Inode table for bg 0 marked as needing zeroing
License installation success.
```

使用管理 VRF 安装许可证

```
OS10(config)# ip vrf management
OS10(conf-vrf)# interface management
OS10(conf-vrf)# exit
OS10(config)# ip sftp vrf management
OS10(config)# exit
OS10# license install sftp://user:userpwd@10.1.1.10/0ANNX42-NOSEnterprise-License.xml

License installation success.
```

验证许可证安装

```
OS10# show license status

System Information
-----
Vendor Name       :   DELL EMC
Product Name      :   S4148F-ON
Hardware Version  :   X01
Platform Name     :   x86_64-dell_s4100_c2338-r0
PPID              :   TW09H9MN282987130026
Service Tag       :   9531XC2
Product Base      :
Product Serial Number:
Product Part Number :
License Details
-----
```

```
Software      : OS10-Enterprise
Version       : 10.5.0.0
License Type  : PERPETUAL
License Duration: Unlimited
License Status : Active
License location: /mnt/license/9531XC2.lic
-----
```

许可证安装失败故障处理

如果安装失败，将显示一条错误消息。

```
License installation failed
```

1. 验证本地或远程许可证位置的安装路径。
2. 在远程服务器上检查日志以查找 FTP 或 TFTP 文件传输失败的原因。
3. 从交换机对远程服务器执行 ping 操作 — 使用 [ping](#) 和 [traceroute](#) 命令测试网络连接。如果 ping 操作失败，请检查以下内容：
 - 如果可以通过管理路由访问远程服务器，请检查是否已正确配置管理路由。
 - 如果可以通过前面板端口访问远程服务器，请检查是否存在静态或动态路由。
 - 如果 ping 操作成功，并且 FTP 或 TFTP 登录到远程服务器没有注册响应，请检查传输路径中是否存在阻止传输协议的防火墙。
4. 在与交换机相同的子网上安装具有许可证文件的服务器。
5. 确保服务器已启动并且正在运行。

交换机部署选项

登录 OS10 后，您可以配置交换机：

- 通过使用命令行接口手动配置
- 通过使用零接触部署 (ZTD) 自动配置
- 通过将自定义脚本与 Ansible 配合使用自动配置

手动 CLI 配置

使用 OS10 命令行界面输入命令以监控和配置 OS10 交换机。通过执行基本和高级 CLI 任务（[CLI 基础知识](#)和[高级 CLI 任务](#)）来设置您的交换机。然后根据您在网络中部署交换机的方式继续使用其他配置设置。有关详细的配置和 CLI 信息，请参阅相应的章节。

ZTD - 自动交换机部署

使用零接触部署自动执行 OS10 交换机部署，包括：

- 升级现有的 OS10 映像。
- 执行 CLI 批处理文件以配置交换机。
- 执行 ZTD 后脚本以执行其他功能。

请参阅[零接触部署](#)。

Ansible 自动交换机调配

使用 Ansible（第三方 DevOps 工具）自动执行 OS10 交换机配置。创建并执行 Ansible 行动手册以配置多个设备。有关详情，请参阅[使用 Ansible](#)。

远程访问

安装或升级 OS10 并登录后，您可以设置对 OS10 命令行接口和 Linux shell 的远程访问。使用串行端口连接交换机。串行端口设置为 115200 波特、8 数据位和无奇偶校验。

配置远程访问

1. 配置管理 IP 地址。
2. 配置管理路由。
3. 配置用户名和密码。

配置管理 IP 地址

要远程访问 OS10，请向管理端口分配 IP 地址。使用管理接口进行带外 (OOB) 交换机管理。

1. 从 CONFIGURATION 模式配置管理接口。

```
interface mgmt 1/1/1
```

2. 默认情况下，DHCP 客户端在管理接口上处于启用状态。在 INTERFACE 模式下禁用 DHCP 客户端操作。

```
no ip address dhcp
```

3. 在 INTERFACE 模式下，在管理接口上配置 IPv4 或 IPv6 地址。

```
ip address A.B.C.D/mask
```

```
ipv6 address A:B/prefix-length
```

4. 在 INTERFACE 模式下启用管理接口。

```
no shutdown
```

配置管理接口

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# no ip address dhcp
OS10(conf-if-ma-1/1/1)# ip address 10.1.1.10/24
OS10(conf-if-ma-1/1/1)# no shutdown
```

配置管理路由

要设置 OS10 的远程访问，请在将 IPv4 或 IPv6 地址分配给管理端口后配置管理路由。管理端口使用默认管理路由与其他网络进行通信。管理路由允许您将管理流量与数据流量分开。

1. (可选) 确保在 INTERFACE 模式下的管理接口上禁用了 DHCP 客户端。

```
no ip address dhcp
```

2. 在 CONFIGURATION 模式下为管理端口配置管理路由。重复命令以配置多个路由。

```
management route {ipv4-address/mask | ipv6-address/prefix-length}
{forwarding-router-address | managementethernet}
```

- *ipv4-address/mask* — 以点分隔的十进制格式 (A.B.C.D) 输入 IPv4 网络地址，然后以前缀长度格式 (/x) 输入子网掩码。
- *ipv6-address/prefix-length* — 以 x:x:x:x::x 格式输入 IPv6 地址，前缀长度为 /x 格式。前缀范围是 /0 至 /128。
- *forwarding-router-address* — 输入转发路由器的下一中继站 IPv4/IPv6 地址，用作连接到不同子网的管理网关。
- *managementethernet* — 针对配置的 IPv4/IPv6 子网在管理端口上发送流量。

 **注：**管理路由独立于 IPv4 和 IPv6 路由，前者用于通过管理端口管理交换机。

配置管理路由

```
OS10(config)# management route 10.10.20.0/24 10.1.1.1
OS10(config)# management route 172.16.0.0/16 managementethernet
```

配置用户名和密码

要设置对 OS10 的远程访问，在配置管理端口和默认路由后创建用户名和密码。用户角色是必需的条目。

以明文形式输入密码。它会转换为正在运行的配置中的 SHA-512 格式。密码必须包含至少 9 个字符，包括字母数字和特殊字符，以及以前用于同一用户名的密码中至少有五个不同的字符；例如：

```
OS10(config)# username admin password alpha404! role sysadmin
```

为了向后兼容 OS10 版本 10.3.1E 及更低版本，支持以 MD-5、SHA-256 和 SHA-512 格式输入密码。要增加所需的密码强度，请使用 `password-attributes` 命令。

- 在 CONFIGURATION 模式下创建用户名和密码。

```
username username password password role role
```

- o `username username` — 输入文本字符串。最多 32 个字母数字字符；最少 1 个字符。
- o `password password` — 输入文本字符串。最多 32 个字母数字字符；最少 9 个字符。
- o `role role` — 输入用户角色：
 - `sysadmin` — 对系统中所有命令的完全访问权限、对操作文件系统的命令的独占访问权限，以及对系统 shell 的访问权限。系统管理员可以创建用户 ID 和用户角色。默认权限级别为 15。
 - `secadmin` — 对设置安全策略和系统访问权限的配置命令的完全访问权限，如密码强度、AAA 授权和加密密钥。安全管理员可以显示安全信息，如加密密钥、登录统计信息和日志信息。默认权限级别为 15。
 - `netadmin` — 对管理流经交换机（如路由、接口和 ACL）的流量的配置命令的完全访问权限。网络管理员无法访问安全功能的配置命令或查看安全信息。默认权限级别为 15。
 - `netoperator` — EXEC 模式访问，以使用有限的显示命令集。网络操作员无法修改交换机上的任何配置设置。默认权限级别为 1。

 **注：**要更改系□管理□密□，□使用新密□重新□入管理□用□名的命令。

```
OS10(config)# username admin password beta@1 role sysadmin
```

CLI 基本信息

OS10 CLI 是用于从控制台或通过网络连接访问运行软件的设备的软件界面。CLI 是在基于 Linux 的操作系统内核上运行的 OS10 特定的命令 shell。通过利用业界标准的工具和实用程序，CLI 提供了一组强大的命令，您可以使用它们来监控和配置运行 OS10 的设备。

用户帐户

OS10 定义了两类用户帐户：

- 要登录到 CLI，请使用 `admin` 作为用户名和密码。
- 要登录到 Linux shell，请使用 `linuxadmin` 作为用户名和密码。

注：您不能删除默认的 `linuxadmin` 用户名。只有在配置了至少一个具有 `sysadmin` 角色的 OS10 用户时，才能删除默认的 `admin` 用户名。

例如，要使用 SSH 连接访问 OS10 CLI，请执行以下操作：

1. 使用设备的 IP 地址打开 SSH 会话。您也可以使用 PuTTY 或类似的工具远程访问设备。

```
ssh admin@ip-address
password: admin
```

2. 输入默认用户名和密码 (`admin`) 以登录到 OS10。您将自动置于 EXEC 模式。

```
OS10#
```

例如，要使用 SSH 连接访问 Linux shell，请输入 `linuxadmin` 作为用户名和密码：

- ```
ssh linuxadmin@management-ip-address
password: linuxadmin
```

### 关键 CLI 功能

- |                |                                                                                                                                                                 |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>一致的命令名称</b> | 提供相同功能类型的命令具有相同的名称，而不考虑其运行所在的系统部分。例如，所有 <code>show</code> 命令都将显示软件信息和统计信息，并且所有 <code>clear</code> 命令都将擦除各种类型的系统信息。                                              |
| <b>可用命令</b>    | 在 CLI 命令层次结构的每个级别上提供了有关可用命令的信息。您可以在任何级别输入问号 (?) 并查看可用命令的列表，以及每个命令的简短说明。                                                                                         |
| <b>命令完成</b>    | 命令名称（关键字）和命令选项的命令完成在层次结构的每个级别均可用。要完成部分输入的命令或选项，请单击 <b>Tab</b> 键或 <b>空格键</b> 。如果部分输入的字母是唯一标识某个命令的字符串，则将显示完整的命令名称。嘟嘟声表示您已输入不明确的命令和可能的完成显示。完成还适用于其他字符串，如接口名称和配置语句。 |

### CLI 命令模式

OS10 CLI 具有两个顶级模式：

- EXEC 模式 — 监控、故障处理、检查状态和网络连接。
- CONFIGURATION 模式 — 配置网络设备。

进入 CONFIGURATION 模式时，您将更改当前的操作配置（称为**正在运行的配置**）。默认情况下，所有配置更改都会自动保存到正在运行的配置中。

您可以通过切换到基于事务的配置模式来更改此默认行为。要切换到基于事务的配置模式，请使用 `start transaction` 命令。当您切换到基于事务的配置模式并更新候选配置时，对候选配置的更改不会添加到正在运行的配置中，直到您提交它们以激活配置。`start transaction` 命令仅适用于当前会话。将当前会话的配置模式更改为基于事务的配置模式不会影响其他 CLI 会话的配置模式。

- 在明确输入 `commit` 命令以保存对候选配置的更改后，该会话将切换回默认行为，以自动将配置更改保存到正在运行的配置。
- 当处于基于事务的配置模式下的会话终止时，并且您没有输入该 `commit` 命令时，更改将在候选配置中维护。您可以启动基于事务的新配置模式会话，并继续进行其余配置更改。
- 基于事务的配置模式下的所有会话都会更新相同的候选配置。当您在基于事务的配置模式下的任何会话上使用 `commit` 命令时，如果您在基于非事务的模式中对任何会话进行配置更改，也会在基于事务的配置模式下的所有其他会话中提交对候选配

置所做的更改。这意味着可能会对正在运行的配置应用不一致的配置更改。Dell EMC 建议一次仅在单个 CLI 会话上进行配置更改。

- 在 CLI 会话中输入 `lock` 命令时，所有其他会话上的配置更改都会被禁用，无论它们处于基于事务的配置模式还是基于非事务的配置模式。有关详情，请参阅[候选配置](#)。

### CLI 命令层次结构

CLI 命令按层次结构进行组织。执行类似功能的命令在相同级别的层次结构下分组到一起。例如，显示有关系统和系统软件的信息的所有命令都在 `show system` 命令下进行分组，并且显示有关路由表的信息的所有命令将在 `show ip route` 命令下进行分组。

要从任何子模式直接移到 EXEC 模式，请输入 `end` 命令。要向上移动一个命令模式，请输入 `exit` 命令。

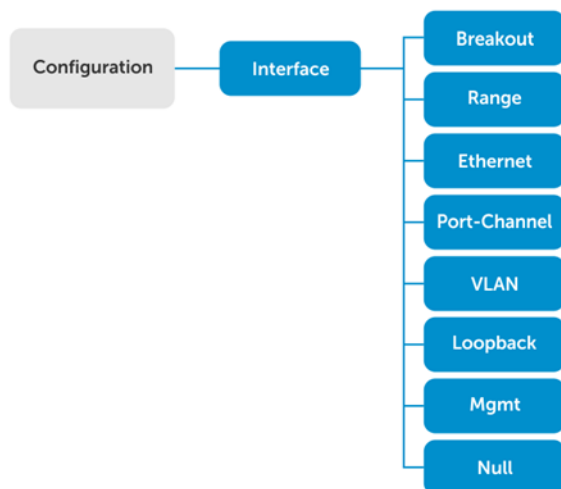
## CONFIGURATION 模式

首次登录 OS10 时，您将处于 EXEC 模式。要访问 CONFIGURATION 模式，请输入 `configure terminal` 命令。使用 CONFIGURATION 模式来管理接口、协议和功能。

```
OS10# configure terminal
OS10(config)#
```

接口模式是 CONFIGURATION 模式的子模式。在接口模式下，您可以配置第 2 层 (L2) 和第 3 层 (L3) 协议，以及接口上的 IPv4 和 IPv6 服务：

- 物理接口包括管理接口和以太网端口
- 逻辑接口包括环回、端口通道和虚拟局域网 (VLAN)



在配置模式下，您还可以使用特定协议配置模式（例如生成树协议 [STP] 或边界网关协议 [BGP]）配置 L2 和 L3 协议。

## 检查设备状态

使用 `show` 命令检查设备状态和监控活动。

- 从 EXEC 模式输入 `show ?` 以查看用于监控设备的命令列表；例如：

```
OS10# show ?
acl-table-usage Show ACL table utilization
alarms Display all current alarm situation in the system
alias Show list of aliases
bfd Show bfd session commands
boot Show boot information
candidate-configuration Current candidate configuration
class-map Show QoS class-map configuration
clock Show the system date and time
...
users Show the current list of users logged into the system
 and show the session id
version Show the software version on the system
```

|                 |                               |
|-----------------|-------------------------------|
| virtual-network | Virtual-network info          |
| vlan            | Vlan status and configuration |
| vlt             | Show VLT domain info          |
| vrrp            | VRRP group status             |
| ztd-status      | Show ztd status               |

- 进入 show command-history EXEC 模式以查看每个执行的命令的跟踪消息。

```
OS10# show command-history
 1 Thu Apr 20 19:44:38 UTC 2017 show vlan
 2 Thu Apr 20 19:47:01 UTC 2017 admin
 3 Thu Apr 20 19:47:01 UTC 2017 monitor hardware-components controllers view 0
 4 Thu Apr 20 19:47:03 UTC 2017 system general info system-version view
 5 Thu Apr 20 19:47:16 UTC 2017 admin
 6 Thu Apr 20 19:47:16 UTC 2017 terminal length 0
 7 Thu Apr 20 19:47:18 UTC 2017 terminal datadump
 8 Thu Apr 20 19:47:20 UTC 2017 %abc
 9 Thu Apr 20 19:47:22 UTC 2017 switchshow
10 Thu Apr 20 19:47:24 UTC 2017 cmsh
```

- 进入 show system EXEC 模式以查看系统状态信息；例如：

```
OS10# show system

Node Id : 1
MAC : 14:18:77:15:c3:e8
Number of MACs : 256
Up Time : 1 day 00:48:58

-- Unit 1 --
Status : up
System Identifier : 1
Down Reason : unknown
Digital Optical Monitoring : disable
System Location LED : off
Required Type : S4148F
Current Type : S4148F
Hardware Revision : X01
Software Version : 10.5.0.0
Physical Ports : 48x10GbE, 2x40GbE, 4x100GbE
BIOS : 3.33.0.0-3
System CPLD : 0.4
Master CPLD : 0.10
Slave CPLD : 0.7

-- Power Supplies --
PSU-ID Status Type AirFlow Fan Speed(rpm) Status

1 up AC NORMAL 1 13312 up
2 fail

-- Fan Status --
FanTray Status AirFlow Fan Speed(rpm) Status

1 up NORMAL 1 13195 up
2 up NORMAL 1 13151 up
3 up NORMAL 1 13239 up
4 up NORMAL 1 13239 up
```

## 命令帮助

要查看任何 CLI 模式下的有效命令列表，请输入 ?；例如：

```
OS10# ?
alarm Alarm commands
```

|                         |                                                              |
|-------------------------|--------------------------------------------------------------|
| alias                   | Set alias for a command                                      |
| batch                   | Batch Mode                                                   |
| boot                    | Tell the system where to access the software image at bootup |
| clear                   | Clear command                                                |
| clock                   | Configure the system clock                                   |
| commit                  | Commit candidate configuration                               |
| configure               | Enter configuration mode                                     |
| copy                    | Perform a file copy operation                                |
| crypto                  | Cryptography commands                                        |
| ...                     |                                                              |
| ping                    | ping -h shows help                                           |
| ping6                   | ping6 -h shows help                                          |
| reload                  | Reboot Networking Operating System                           |
| show                    | Show running system information                              |
| start                   | Activate transaction based configuration                     |
| support-assist-activity | Support Assist related activity                              |
| system                  | System command                                               |
| terminal                | Set terminal settings                                        |
| traceroute              | traceroute --help shows help                                 |
| unlock                  | Unlock candidate configuration                               |
| validate                | Validate candidate configuration                             |
| write                   | Copy from current system configuration                       |
| ztd                     | Cancel the current ZTD process.                              |

```

OS10(config)# ?
aaa Configure AAA
alias Set alias for a command
banner Configure banners
bfd Enable bfd globally
class-map Configure class map
clock Configure clock parameters
control-plane Control-plane configuration
crypto Crypto commands
dcbx DCBX commands
default Configure default attributes
dot1x Configure dot1x global information
...
uplink-state-group Create uplink state group
username Create or modify users
userrole Create custom user role
virtual-network Create a Virtual Network
vlt-domain VLT domain configurations
vrrp Configure VRRP global attributes
wred Configure WRED profile

```

## 候选配置

在基于事务的配置模式中使用 OS10 配置命令时，更改不会立即生效并存储在候选配置中。只有在使用 `commit` 命令提交更改后，配置更改才会变为活动状态。候选配置中的更改将进行验证，并应用于正在运行的配置。

候选配置使您可以避免在 OS10 配置会话期间引入错误。您可以进行更改，然后在将其提交到交换机上的活动、运行的配置之前对其进行检查。

要检查正在运行的配置与候选配置之间的差异，请使用 `show diff candidate-configuration running-configuration` 命令。

例如，在进入事务模式之前，您可以检查是否未输入任何新的配置命令。如果 `show` 命令未返回输出，则 `candidate-configuration` 和 `running-configuration` 文件是相同的。然后启动事务模式、配置新设置，并查看候选配置与正在运行的配置之间的差异。确定是否要提交对正在运行的配置的更改。要删除未提交的更改，请使用 `discard` 命令。

### 查看候选配置与正在运行的配置之间的差异

```

OS10# show diff candidate-configuration running-configuration
OS10#
OS10# start transaction
OS10# configure terminal
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# exit
OS10(config)# interface ethernet 1/1/15

```



```

OS10(config-if-eth1/1/15)# switchport mode trunk
OS10(config-if-eth1/1/15)# switchport trunk allowed vlan 100
OS10(config-if-eth1/1/15)# end

OS10# show diff candidate-configuration running-configuration
!
interface ethernet1/1/15
switchport mode trunk
switchport trunk allowed vlan 100
!
interface vlan100
no shutdown
OS10#

```

### 在事务模式下的候选配置中提交配置更改

1. 从 EXEC 模式更改为基于事务的配置模式。

```
start transaction
```

2. 输入配置命令。例如，从 INTERFACE 模式下启用接口。

```
interface ethernet 1/1/1
no shutdown
```

3. 将配置更改保存到正在运行的配置。

```
do commit
```

输入 commit 命令后，当前 OS10 会话将切换回自动提交所有配置更改的默认行为。

```

OS10# start transaction
OS10# configure terminal
OS10(config)#
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# no shutdown
OS10(config-if-eth1/1/1)# do commit

```

### 压缩的配置视图

要仅显示候选配置中的接口相关配置，请使用 show candidate-configuration compressed 和 show running-configuration compressed 命令。这些视图仅显示 VLAN 和物理接口的配置命令。

```

OS10# show candidate-configuration compressed
interface breakout 1/1/1 map 40g-1x
interface breakout 1/1/2 map 40g-1x
interface breakout 1/1/3 map 40g-1x
interface breakout 1/1/4 map 40g-1x
...
interface breakout 1/1/30 map 40g-1x
interface breakout 1/1/31 map 40g-1x
interface breakout 1/1/32 map 40g-1x
ipv6 forwarding enable
username admin password 6q9QBeYjZ$jfzxVqGhxxX3smxJSH9DDz7/3OJc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIGNs5BKH. role sysadmin
aaa authentication local
snmp-server contact http://www.dell.com/support
!
interface range ethernet 1/1/1-1/1/32
switchport access vlan 1
no shutdown
!
interface vlan 1
no shutdown
!
interface mgmt1/1/1
ip address dhcp
no shutdown
ipv6 enable
ipv6 address autoconfig
!
support-assist

```

```
!
policy-map type application policy-iscsi
!
class-map type application class-iscsi
```

```
OS10# show running-configuration compressed
interface breakout 1/1/1 map 40g-1x
interface breakout 1/1/2 map 40g-1x
interface breakout 1/1/3 map 40g-1x
interface breakout 1/1/4 map 40g-1x
...
interface breakout 1/1/30 map 40g-1x
interface breakout 1/1/31 map 40g-1x
interface breakout 1/1/32 map 40g-1x
ipv6 forwarding enable
username admin password 6q9QBeYjZ$jfxxVqGhxxX3smxJSH9DDz7/3OJc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIGNs5BKH. role sysadmin
aaa authentication local
snmp-server contact http://www.dell.com/support
!
interface range ethernet 1/1/1-1/1/32
 switchport access vlan 1
 no shutdown
!
interface vlan 1
 no shutdown
!
interface mgmt1/1/1
 ip address dhcp
 no shutdown
 ipv6 enable
 ipv6 address autoconfig
!
support-assist
!
policy-map type application policy-iscsi
!
class-map type application class-iscsi
```

## 避免配置更改

您可以使用 `lock` 命令防止在当前 CLI 会话以外的会话中对交换机进行的配置更改。要防止并允许在其他会话中进行配置更改，请在 EXEC 模式下使用 `lock` 和 `unlock` 命令。

当您输入 `lock` 命令时，其他活动 CLI 会话中的用户将无法进行配置更改。当您关闭在其中输入了 `lock` 命令的 CLI 会话时，将在所有其他会话中自动允许配置更改。

```
OS10# lock
```

```
OS10# unlock
```

## 复制正在运行的配置

正在运行的配置包含当前 OS10 系统配置，并包含一系列 OS10 命令。将正在运行的配置复制到远程服务器或本地目录作为备份或进行查看和编辑。正在运行的配置将作为一个文本文件进行复制，您可以通过文本编辑器查看和编辑该文件。

**将正在运行的配置复制到本地目录或远程服务器**

```
OS10# copy running-configuration {config://filepath | home://filepath |
ftp://userid:passwd@hostip/filepath | scp://userid:passwd@hostip/filepath |
sftp://userid:passwd@hostip/filepath | tftp://hostip/filepath}
```

```
OS10# copy running-configuration scp://root:calvin@10.11.63.120/tmp/qaz.txt
```

## 将文件复制到正在运行的配置

要将一组命令应用于当前正在运行的配置并立即执行，请从远程服务器或本地目录复制文本文件。复制的命令不会替换现有的命令。如果 `copy` 命令失败，则将保持在故障发生之前成功复制的任何命令。

```
OS10# copy {config://filepath | home://filepath |
ftp://userid:passwd@hostip/filepath | scp://userid:passwd@hostip/filepath |
sftp://userid:passwd@hostip/filepath | tftp://hostip/filepath | http://userid@hostip/
filepath}
running-configuration
```

```
OS10# copy scp://root:calvin@10.11.63.120/tmp/qaz.txt running-configuration
```

## 将正在运行的配置复制到启动配置

要显示当前 OS10 会话中配置的设置，请使用 `show running-configuration`。要在系统重新引导时保存新的配置设置，请将运行的配置复制到启动配置文件。

```
OS10# copy running-configuration startup-configuration
```

# 还原启动配置

启动配置文件 `startup.xml` 存储在 `config` 系统文件夹中。要创建备份版本，请将启动配置复制到远程服务器或本地 `config:` 或 `home:` 目录。

要还原备份配置，请将本地或远程文件复制到启动配置并重新加载交换机。下载备份配置后，输入 `reload` 命令，否则配置在重新启动后不会生效。

**注：**非默认交换机端口配置文件不会自动恢复。如果您想要还原包含非默认交换机端口配置文件的已下载配置，必须在交换机上手配置并保存配置文件，然后重新加载交换机以使配置文件生效。如果备份文件包含默认的交换机端口配置文件，您可以直接从服务器复制后配置文件，然后重新加载交换机。

## 将文件复制到启动配置

```
OS10# copy {config://filepath | home://filepath |
ftp://userid:passwd@hostip/filepath | scp://userid:passwd@hostip/filepath |
sftp://userid:passwd@hostip/filepath | tftp://hostip/filepath} config://startup.xml
```

## 备份启动文件

```
OS10# copy config://startup.xml config://backup-9-28.xml
```

## 从备份还原启动文件

```
OS10# copy config://backup-9-28.xml config://startup.xml
OS10# reload
System configuration has been modified. Save? [yes/no]:no
```

## 将启动文件备份到服务器

```
OS10# copy config://startup.xml scp://userid:password@hostip/backup-9-28.xml
```

## 从服务器还原启动文件

```
OS10# copy scp://admin:admin@hostip/backup-9-28.xml config://startup.xml
OS10# reload
System configuration has been modified. Save? [yes/no]:no
```

## 重新加载系统映像

在 EXEC 模式下，使用 `reload` 命令手动重新引导系统。系统将提示您确认操作。

```
OS10# reload

System configuration has been modified. Save? [yes/no]:yes

Saving system configuration

Proceed to reboot the system? [confirm yes/no]:yes
```

要配置在下次系统引导时加载的 OS10 映像，请在 EXEC 模式下输入 `boot system` 命令。

```
boot system {active | standby}
```

- 输入 `active` 以加载存储在 A 分区中的主 OS10 映像。
- 输入 `standby` 以加载存储在 B 分区中的次 OS10 映像。

### 设置下次引导映像

```
OS10# boot system standby
OS10# show boot
Current system image information:
=====
Type Boot Type Active Standby Next-Boot

Node-id 1 Flash Boot [A] 10.2.9999E [B] 10.2.9999E [B] standby
```

## 筛选 show 命令

您可以筛选 `show` 命令输出以查看特定信息，或者在正则表达式或短语的第一个实例上启动命令输出。

- `display-xml` — 以 XML 格式显示输出。
- `except` — 仅显示与模式不匹配的文本。
- `find` — 搜索某个模式的首次出现，并显示所有进一步的配置。
- `grep` — 仅显示与指定模式匹配的文本。正则表达式中的特殊字符，例如 `^`（与文本字符串的开头匹配）、`$`（与字符串的末尾匹配）和 `.` 支持（与字符串中的任意字符匹配）。
- `no-more` — 不对输出进行分页。
- `save` — 将输出保存到文件。

### 显示所有输出

```
OS10# show running-configuration | no-more
```

## 常见 OS10 命令

### boot

配置要在系统下次引导时使用的 OS10 映像。

|      |                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | <code>boot system [active   standby]</code>                                                                                                  |
| 参数   | <ul style="list-style-type: none"><li>• <code>active</code> — 将正在运行的分区重置为下一个引导分区。</li><li>• <code>standby</code> — 将备用分区设置为下一引导分区。</li></ul> |
| 默认   | 未配置                                                                                                                                          |
| 命令模式 | EXEC                                                                                                                                         |

|        |                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------|
| 使用情况信息 | 使用此命令可配置在引导时加载的 OS10 映像。使用 <code>show boot</code> 命令可验证下一个引导映像。 <code>boot system</code> 命令将立即应用。 |
| 示例     | <pre>OS10# boot system standby</pre>                                                              |
| 支持的版本  | 10.2.0E or later                                                                                  |

## commit

将候选配置中的更改提交至正在运行的配置。

|        |                                                                            |
|--------|----------------------------------------------------------------------------|
| 语法     | <code>commit</code>                                                        |
| 参数     | 无                                                                          |
| 默认     | 未配置                                                                        |
| 命令模式   | EXEC                                                                       |
| 使用情况信息 | 使用此命令可保存对正在运行的配置的更改。使用 <code>do commit</code> 命令可以在 CONFIGURATION 模式下保存更改。 |
| 示例     | <pre>OS10# commit</pre>                                                    |
| 示例（配置） | <pre>OS10(config)# do commit</pre>                                         |
| 支持的版本  | 10.2.0E or later                                                           |

## configure

从 EXEC 模式进入 CONFIGURATION 模式。

|        |                                                       |
|--------|-------------------------------------------------------|
| 语法     | <code>configure {terminal}</code>                     |
| 参数     | <code>terminal</code> — 从 EXEC 模式进入 CONFIGURATION 模式。 |
| 默认     | 未配置                                                   |
| 命令模式   | EXEC                                                  |
| 使用情况信息 | 输入 <code>conf t</code> 以进行自动完成。                       |
| 示例     | <pre>OS10# configure terminal OS10(config)#</pre>     |
| 支持的版本  | 10.2.0E or later                                      |

## copy

将当前运行的配置复制到启动配置，并在 OS10 交换机与远程设备之间传输文件。

|    |                                                                                                                                                                                                                                                                               |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>copy running-configuration [startup-configuration   config://filepath   coredump://filepath   ftp://filepath   home://filepath   scp://filepath   sftp://filepath   severity-profile profile-name   supportbundle://filepath   tftp://filepath   usb://filepath]</code> |
| 参数 | <ul style="list-style-type: none"> <li><code>running-configuration startup-configuration</code> — （可选）将当前运行的配置文件复制到启动配置文件。</li> <li><code>config://filepath</code> — （可选）从配置目录复制。</li> <li><code>coredump://filepath</code> — （可选）从核心转储目录复制。</li> </ul>                       |

- `ftp://userid:passwd@hostip/filepath` — (可选) 从远程 FTP 服务器复制。
- `home://username/filepath` — (可选) 从主目录复制。
- `scp://userid:passwd@hostip/filepath` — (可选) 从远程 SCP 服务器复制。
- `sftp://userid:passwd@hostip/filepath` — (可选) 从远程 SFTP 服务器复制。
- `supportbundle://filepath` — (可选) 从支持套装目录复制。
- `severity-profile://filepath` — (可选) 从严重性配置文件目录复制。
- `tftp://hostip/filepath` — (可选) 从远程 TFTP 服务器复制。
- `usb:filepath` — (可选) 从 USB 文件系统复制。

默认

未配置

命令模式

EXEC

使用情况信息

使用此命令可将正在运行的配置保存到启动配置、将核心转储文件传输到远程位置、备份启动配置、检索以前备份的配置、替换启动配置文件或传输支持套装。

 **小心:** Dell EMC Networking 建议您不要使用 `copy` 命令将 OS10 映像下载到交换机。下载的映像将占用大量的磁盘空间。使用 `image download` 命令可下载 OS10 映像。

使用 `scp` 和 `sftp` 选项时，请始终输入绝对文件路径（而不是相对于用户帐户主目录的路径）。例如：

```
copy config://startup.xml scp://dellos10:password@10.1.1.1/home/dellos10/
backup.xml
```

将 `copy` 命令与 `severity-profile` 选项配合使用可从远程位置下载或上传严重性配置文件。将严重性配置文件从远程位置复制到 OS10 交换机时，请确保严重性配置文件的名称不同于默认配置文件 (`default.xml`) 或当前活动的严重性配置文件的名称。

示例

```
OS10# dir coredump

Directory contents for folder: coredump
Date (modified) Size (bytes) Name

2017-02-15T19:05:41Z 12402278 core.netconfd-
pro.2017-02-15_19-05-09.gz

OS10# copy coredump://core.netconfd-pro.2017-02-15_19-05-09.gz scp://
os10user:os10passwd@10.11.222.1/home/os10/core.netconfd-pro.2017-02
-15_19-05-09.gz
```

示例：复制启动配置

```
OS10# dir config

Directory contents for folder: config
Date (modified) Size (bytes) Name

2017-02-15T20:38:12Z 54525 startup.xml

OS10# copy config://startup.xml scp://os10user:os10passwd@10.11.222.1/
home/os10/backup.xml
```

示例：检索备份配置

```
OS10# copy scp://os10user:os10passwd@10.11.222.1/home/os10/backup.xml
home://config.xml

OS10(conf-if-eth1/1/5)# dir home

Directory contents for folder: home
Date (modified) Size (bytes) Name

...
2017-02-15T21:19:54Z 54525 config.xml
...
```

示例：从远程位置  
下载自定义严重性  
配置文件

```
copy scp://username:password@a.b.c.d//file-path/mySevProf.xml severity-
profile://mySevProf_1.xml
```

示例：替换启动配  
置

```
OS10# home://config.xml config://startup.xml
```

支持的版本

10.2.0E or later

## delete

移除或删除文件，包括启动配置文件。

语法

```
delete [config://filepath | coredump://filepath | home://filepath |
image://filepath | startup-configuration | severity-profile profile-name |
supportbundle://filepath | usb://filepath]
```

参数

- config://filepath — (可选) 从配置目录中删除。
- coredump://filepath — (可选) 从核心转储目录中删除。
- home://filepath — (可选) 从主目录中删除。
- image://filepath — (可选) 从映像目录中删除。
- startup-configuration — (可选) 删除启动配置。
- severity-profile — (可选) 从严重性配置文件目录、严重性-配置文件://filepath 中删除。
- supportbundle://filepath — (可选) 从支持套装目录中删除。
- usb://filepath — (可选) 从 USB 文件系统中删除。

默认

未配置

命令模式

EXEC

使用情况信息

使用此命令可移除常规文件、软件映像或启动配置。移除启动配置会将系统还原到出厂默认设置。您必须使用 reload 命令重新启动交换机，以使操作生效。

**注：**

- 移除启动配置时请小心操作。
- 当配置分区的磁盘空间不足时，将显示系统日志消息：

```
SYS_STAT_LOW_DISK_SPACE: Warning! Configuration directory has 0.0%
free. Please delete unnecessary files from home directory.
```

当您看到此错误时，请从主目录中删除不需要的文件，否则可能会遇到系统性能下降。

示例

```
OS10# delete startup-configuration
```

```
OS10# delete severity-profile://mySevProf.xml
```

支持的版本

10.2.0E or later

## dir

显示存储在可用目录中的文件。

语法

```
dir {config | coredump | home | image | severity-profile | supportbundle |
usb}
```

参数

- config — (可选) 包含配置文件的文件夹。
- coredump — (可选) 包含核心转储文件的文件夹。
- home — (可选) 包含主目录中的文件的文件夹。
- image — (可选) 包含映像文件的文件夹。
- severity-profile — (可选) 包含警报严重性配置文件的文件夹。

- `supportbundle` — (可选) 包含支持套装文件的文件夹。
- `usb` — (可选) 包含 USB 驱动器上的文件的文件夹。

**默认**

未配置

**命令模式**

EXEC

**使用情况信息**

`dir` 命令至少需要一个参数。使用 `dir config` 命令可以显示配置文件。

**示例**

```
OS10# dir
config Folder containing configuration files
coredump Folder containing coredump files
home Folder containing files in user's home directory
image Folder containing image files
severity-profile Folder containing severity profiles
supportbundle Folder containing support bundle files
```

**示例 (config)**

```
OS10# dir config
Directory contents for folder: config
Date (modified) Size (bytes) Name

2017-04-26T15:23:46Z 26704 startup.xml
```

```
OS10# dir severity-profile
Date (modified) Size (bytes) Name

2019-03-27T15:24:06Z 46741 default.xml
2019-04-01T11:22:33Z 456 mySevProf.xml
```

**支持的版本**

10.2.0E or later

## discard

放弃对候选配置文件所做的更改。

**语法**

`discard`

**参数**

无

**默认**

未配置

**命令模式**

EXEC

**使用情况信息**

无

**示例**

```
OS10# discard
```

**支持的版本**

10.2.0E or later

## do

从所有 CONFIGURATION 模式下执行大多数命令，而不返回 EXEC 模式。

**语法**

`do command`

**参数**

`command` — 输入 EXEC 级命令。

**默认**

未配置

**命令模式**

INTERFACE

**使用情况信息**

无



### 示例

```
OS10(config)# interface ethernet 1/1/7
OS10(conf-if-eth1/1/7)# no shutdown
OS10(conf-if-eth1/1/7)# do show running-configuration
...
!
interface ethernet1/1/7
 no shutdown
!
...
```

**支持的版本** 10.2.0E or later

## end

从任何其他命令模式返回到 EXEC 模式。

**语法** end

**参数** 无

**默认** 未配置

**命令模式** 全部

**使用情况信息** 使用 end 命令返回到 EXEC 模式，以使用 show 命令验证当前配置的设置。

### 示例

```
OS10(config)# end
OS10#
```

**支持的版本** 10.2.0E or later

## exit

返回到下一个更高的命令模式。

**语法** exit

**参数** 无

**默认** 未配置

**命令模式** 全部

**使用情况信息** 无

### 示例

```
OS10(conf-if-eth1/1/1)# exit
OS10(config)#
```

**支持的版本** 10.2.0E or later

## hostname

设置系统主机名称。

**语法** hostname *name*

**参数** *name* — 输入交换机的主机名称，最多 64 个字符。

**默认** OS10

**命令模式** CONFIGURATION

**使用情况信息** 在 OS10 命令行提示符处使用主机名称。

MX7000 系列交换机（而不是 Dell EMC SmartFabric OS10）使用 *模块插槽* 格式自动设置默认主机名称。要计算主机名称，交换机将考虑当前插入 MX7000 机箱的模块和插入模块的机箱中的插槽。模块可以是 MX9116n 或 MX5108n。

**注：**要使交换机使用 *模块插槽* 格式自动设置默认主机名称，请在升级到版本 10.5.0 之前，删除用户定义的主机名称或使用 `no hostname` 命令设置默认主机名称。

从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从 10.5.0 开始，在 SmartFabric 服务模式下也支持。

此命令的 `no` 版本将主机名称重置为 `OS10`。

#### 示例

```
OS10(conf)# hostname R1
R1(conf)#
```

#### 支持的版本

10.3.0E or later

## license

从本地或远程位置安装许可证文件。

#### 语法

```
license install [ftp: | http: | localfs: | scp: | sftp: | tftp: | usb:]
filepath
```

#### 参数

- `ftp:` —（可选）从远程文件系统 (`ftp://userid:passwd@hostip/filepath`) 安装。
- `http[s]:` —（可选）从远程文件系统 (`http://hostip/filepath`) 安装。
- `http[s]:` —（可选）从远程服务器 (`http://hostip`) 请求。
- `localfs:` —（可选）从本地文件系统 (`localfs://filepath`) 安装。
- `scp:` —（可选）从远程文件系统 (`scp://userid:passwd@hostip/filepath`) 请求。
- `sftp:` —（可选）从远程文件系统 (`sftp://userid:passwd@hostip/filepath`) 请求。
- `tftp:` —（可选）从远程文件系统 (`tftp://hostip/filepath`) 请求。
- `usb:` —（可选）从 USB 文件系统 (`usb://filepath`) 请求。

#### 默认

未配置

#### 命令模式

EXEC

#### 使用情况信息

使用此命令安装许可证文件。有关详细信息，请参阅[安装 OS10 许可证](#)。OS10 需要永久许可证才能在 120 天试用期以外运行。许可证文件将安装在 `/mnt/license` 目录中。

#### 示例

```
OS10# license install scp://user:userpwd/10.1.1.10/CFNNX42-NOSEnterprise-
License.lic
License installation success.
```

#### 支持的版本

10.3.0E or later

## lock

锁定候选配置，并防止任何其他 CLI 会话上的任何配置更改，无论是在事务或非事务配置模式中。

#### 语法

```
lock
```

#### 参数

无

#### 默认

未配置

#### 命令模式

EXEC

#### 使用情况信息

如果候选配置中存在未提交的更改，则此 `lock` 命令将失败。

#### 示例

```
OS10# lock
```

#### 支持的版本

10.2.0E or later

## management route

配置管理端口使用的 IPv4/IPv6 静态路由。要配置多个管理路由，请重复命令。

|           |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法        | <code>management route {ipv4-address/mask   ipv6-address/prefix-length} {forwarding-router-address   managementethernet}</code>                                                                                                                                                                                                                                                                                        |
| 参数        | <ul style="list-style-type: none"><li><code>ipv4-address/mask</code> — 以点分隔的十进制格式 (A.B.C.D) 输入 IPv4 网络地址，然后以前缀长度格式 (/xx) 输入子网掩码。</li><li><code>ipv6-address/prefix-length</code> — 以 x:x:x:x::x 格式输入 IPv6 地址，前缀长度为 /xxx 格式。前缀范围是 /0 至 /128。</li><li><code>forwarding-router-address</code> — 为管理端口中的网络流量输入转发路由器（网关）的下一跳 IPv4/IPv6 地址。</li><li><code>managementethernet</code> — 将管理端口配置为路由的接口，并将该路由与管理接口相关联。</li></ul> |
| 默认        | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 命令模式      | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息    | 管理路由独立于 IP 路由，前者用于通过管理端口管理交换机。要显示当前配置的 IPv4 和 IPv6 管理路由，请使用 <code>show ip management-route</code> 和 <code>show ipv6 management-route</code> 命令。                                                                                                                                                                                                                                                                        |
| 示例 (IPv4) | <pre>OS10(config)# management route 10.10.20.0/24 10.1.1.1 OS10(config)# management route 172.16.0.0/16 managementethernet</pre>                                                                                                                                                                                                                                                                                       |
| 示例 (IPv6) | <pre>OS10(config)# management route 10::/64 10::1</pre>                                                                                                                                                                                                                                                                                                                                                                |
| 支持的版本     | 10.2.2E or later                                                                                                                                                                                                                                                                                                                                                                                                       |

## move

移动或重命名配置或主系统目录中的文件。

|          |                                                                                                                                                                                                                                                                 |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法       | <code>move [config:   home:   usb:]</code>                                                                                                                                                                                                                      |
| 参数       | <ul style="list-style-type: none"><li><code>config:</code> — 从配置目录 (<code>config://filepath</code>) 移动。</li><li><code>home:</code> — 从主目录 (<code>home://filepath</code>) 移动。</li><li><code>usb:</code> — 从 USB 文件系统 (<code>usb://filepath</code>) 移动。</li></ul> |
| 默认       | 未配置                                                                                                                                                                                                                                                             |
| 命令模式     | EXEC                                                                                                                                                                                                                                                            |
| 使用情况信息   | 使用 <code>dir config</code> 命令查看目录内容。                                                                                                                                                                                                                            |
| 示例       | <pre>OS10# move config://startup.xml config://startup-backup.xml</pre>                                                                                                                                                                                          |
| 示例 (dir) | <pre>OS10# dir config  Directory contents for folder: config Date (modified)      Size (bytes)  Name ----- 2017-04-26T15:23:46Z  26704        startup.xml</pre>                                                                                                 |
| 支持的版本    | 10.2.0E or later                                                                                                                                                                                                                                                |

## no

在 EXEC 模式下禁用或删除命令。

|    |                                                                      |
|----|----------------------------------------------------------------------|
| 语法 | <code>no [alias   debug   support-assist-activity   terminal]</code> |
|----|----------------------------------------------------------------------|

|        |                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 参数     | <ul style="list-style-type: none"> <li>alias — 移除别名定义。</li> <li>debug — 禁用调试。</li> <li>support-assist-activity — 与 SupportAssist 相关的活动。</li> <li>terminal — 重置终端设置。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                            |
| 命令模式   | EXEC                                                                                                                                                                           |
| 使用情况信息 | 在 EXEC 模式下使用此命令可禁用或移除配置。在 CONFIGURATION 模式下使用 <code>no ?</code> 可查看可用的命令。                                                                                                      |
| 示例     | <pre>OS10# no alias goint</pre>                                                                                                                                                |
| 支持的版本  | 10.2.0E or later                                                                                                                                                               |

## ping

测试到 IPv4 设备的网络连接。

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <pre>ping [vrf {management   vrf-name}] [-4] [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface] [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline] [-W timeout] [hop1 ...] destination</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 参数 | <ul style="list-style-type: none"> <li>vrf management — (可选) 对管理虚拟路由和转发 (VRF) 实例中的 IPv4 地址执行 ping 操作。</li> <li>vrf vrf-name — (可选) 对指定 VRF 实例中的 IP 地址执行 ping 操作。</li> <li>-4 — (可选) 在同时配置了 IPv4 和 IPv6 默认路由的情况下, 在 IPv6 路由上使用 IPv4 路由, 您必须在 ping 命令中使用以下选项: -4。例如, <code>OS10# ping vrf management -4 dell.com</code>。</li> <li>-a — (可选) 可听见的 ping。</li> <li>-A — (可选) 自适应 ping。数据包间间隔可适应往返时间, 以便在网络中有一个 (或多个, 如果设置预加载选项) 无应答探测器。非超级用户的最小间隔为 200 毫秒, 与往返时间较短的网络上的泛洪模式相对应。</li> <li>-b — (可选) 对广播地址执行 ping 操作。</li> <li>-B — (可选) 不允许通过 ping 更改探测器的源地址。源地址绑定到 ping 启动时使用的地址。</li> <li>-c count — (可选) 发送指定数量的 ECHO_REQUEST 数据包后停止 ping, 直至超时过期。</li> <li>-d — (可选) 在所使用的插槽上设置 SO_DEBUG 选项。</li> <li>-D — (可选) 在每一行之前打印时间戳。</li> <li>-h — (可选) 显示此命令的帮助。</li> <li>-i interval — (可选) 输入每个数据包发送之间的等待时间间隔 (以秒为单位), 默认值为 1 秒。</li> <li>-I interface-name or interface-ip-address — (可选) 输入不带空格的源接口名称或接口 IP 地址: <ul style="list-style-type: none"> <li>对于物理以太网接口, 请输入 ethernetnode/slot/port; 例如, ethernet1/1/1。</li> <li>对于 VLAN 接口, 请输入 vlanvlan-id; 例如, vlan10。</li> <li>对于环回接口, 请输入 loopbackid; 例如, loopback1。</li> <li>对于端口通道接口, 请输入 port-channelchannel-id; 例如, port-channel。</li> </ul> </li> <li>-l preload — (可选) 输入在等待回复之前通过 ping 发送的数据包数。只有超级用户可以预加载三个以上的用户。</li> <li>-L — (可选) 禁止多播目标地址的多播数据包环回。</li> <li>-m mark — (可选) 标记发送到 ping 远程设备的数据包。将此选项与策略路由配合使用。</li> <li>-M pmtudisc_option — (可选) 输入路径 MTU (PMTU) 发现策略: <ul style="list-style-type: none"> <li>do 将阻止分段, 包括本地。</li> <li>want 将在本地执行 PMTU 发现并分段大数据包。</li> <li>dont 不设置“不要分段 (DF)”标记。</li> </ul> </li> <li>-p pattern — (可选) 输入最多 16 个填充字节, 以填写发送的数据包, 从而诊断网络中与数据相关的问题。例如, -p ff 将使用全部 1's 来填充发送的数据包。</li> <li>-Q tos — (可选) 输入十进制或十六进制数据报中的最大 1500 个字节, 以设置与服务质量 (QoS) 相关的位。</li> </ul> |

- `-s packetsize` — (可选) 输入要发送的数据字节数, 从 1 到 65468, 默认值为 56。
- `-S sndbuf` — (可选) 设置 sndbuf 插槽。默认情况下, sndbuf 套接字会将一个数据包进行最大限度地缓冲。
- `-t ttl` — (可选) 输入 IPv4 的生存时间 (TTL) 值 (以秒为单位)。
- `-T timestamp_option` — (可选) 设置特殊 IP 时间戳选项。timestamp\_option 的有效值—  
tsonly (仅时间戳)、tsandaddr (时间戳和地址) 或 tsprespec host1 [host2 [host3 [host4]]] (时间戳预指定的跳)
- `-v` — (可选) Verbose 输出。
- `-V` — (可选) 显示版本并退出。
- `-w deadline` — (可选) 输入 ping 退出之前的超时值 (以秒为单位), 而不考虑发送或接收多少个数据包。
- `-W timeout` — (可选) 输入等待响应的时间 (以秒为单位)。此设置仅在没有响应时影响超时, 否则 ping 将等待两次往返时间 (RTT)。
- `hop1 ...` (可选) 为要执行的 ping 数据包输入预先指定的跳的 IPv4 地址。
- `destination` — 输入要在其上测试连接的 IP 地址。

## 默认

未配置

## 命令模式

EXEC

## 使用情况信息

此命令使用 ICMP ECHO\_REQUEST 数据报从网络主机或网关上接收 ICMP ECHO\_RESPONSE。每个 ping 数据包都有 IPv4 和 ICMP 标头, 然后是时间值和用于填充数据包的“填充”字节数。Ping 操作将数据包发送到指定的 IP 地址, 然后测量从地址或设备获取响应所需的时间。

如果目标 IP 地址处于活动状态, 则会从服务器发送回复, 包括 IP 地址、发送的字节数、生存时间 (以毫秒为单位) 和 TTL (这是从源返回到目标的跳数)。

当您使用 `-I` 选项并输入 IP 地址时, OS10 会将其视为源地址。如果您使用的是接口名称而不是 IP 地址, OS10 会将其视为出口接口。

使用 `-I` 选项时, 如果使用环回接口的 IP 地址作为源接口 ping 可访问的 IP 地址, 则 ping 操作成功。但是, 如果使用环回接口的名称作为源接口 ping 可访问的 IP 地址, 则 ping 操作失败。这是因为系统将环回接口视为出口接口。

## 示例

```
OS10# ping 20.1.1.1
PING 20.1.1.1 (20.1.1.1) 56(84) bytes of data.
64 bytes from 20.1.1.1: icmp_seq=1 ttl=64 time=0.079 ms
64 bytes from 20.1.1.1: icmp_seq=2 ttl=64 time=0.081 ms
64 bytes from 20.1.1.1: icmp_seq=3 ttl=64 time=0.133 ms
64 bytes from 20.1.1.1: icmp_seq=4 ttl=64 time=0.124 ms
^C
--- 20.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.079/0.104/0.133/0.025 ms
```

## 支持的版本

10.2.0E or later

# ping6

测试到 IPv6 设备的网络连接。

## 语法

```
ping6 [vrf {management | vrf-name}] [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface] [-l preload] [-m mark] [-M pmtudisc_option] [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline] [-W timeout] destination
```

## 参数

- `vrf management` — (可选) 对管理 VRF 实例中的 IPv6 地址执行 Ping 操作。
- `vrf vrf-name` — (可选) 对指定 VRF 实例中的 IPv6 地址执行 Ping 操作。
- `-a` — (可选) 可听见的 ping。
- `-A` — (可选) 自适应 ping。数据包间间隔可适应往返时间, 以便在网络中有一个 (或多个, 如果设置预加载选项) 无应答探测器。非超级用户的最小间隔为 200 毫秒, 与往返时间较短的网络上的泛洪模式相对应。
- `-b` — (可选) 对广播地址执行 ping 操作。
- `-B` — (可选) 不允许通过 ping 更改探测器的源地址。源地址绑定到 ping 启动时使用的地址。

- `-c count` — (可选) 发送指定数量的 ECHO\_REQUEST 数据包后停止 ping，直至超时过期。
- `-d` — (可选) 在所使用的插槽上设置 SO\_DEBUG 选项。
- `-D` — (可选) 在每一行之前打印时间戳。
- `-F flowlabel` — (可选) 在回响请求数据包上设置 20 位流标签。如果值为零，则内核将分配随机流标签。
- `-h` — (可选) 显示此命令的帮助。
- `-i interval` — (可选) 输入每个数据包发送之间的等待时间间隔 (以秒为单位)，默认值为 1 秒。
- `-I interface-name or interface-ip-address` — (可选) 输入不带空格的源接口名称或接口 IP 地址：
  - 对于物理以太网接口，请输入 `ethernetnode/slot/port`；例如，`ethernet1/1/1`。
  - 对于 VLAN 接口，请输入 `vlanvlan-id`；例如，`vlan10`。
  - 对于环回接口，请输入 `loopbackid`；例如，`loopback1`。
  - 对于端口通道接口，请输入 `port-channelchannel-id`；例如，`port-channel`。
- `-l preload` — (可选) 输入在等待回复之前通过 ping 发送的数据包数。只有超级用户可以预加载三个以上的用户。
- `-L` — (可选) 禁止多播目标地址的多播数据包环回。
- `-m mark` — (可选) 标记发送到 ping 远程设备的数据包。将此选项与策略路由配合使用。
- `-M pmtudisc_option` — (可选) 输入路径 MTU (PMTU) 发现策略：
  - `do` 将阻止分段，包括本地。
  - `want` 将在本地执行 PMTU 发现并分段大数据包。
  - `dont` 不设置“不要分段 (DF)”标记。
- `-p pattern` — (可选) 输入最多 16 个填充字节，以填写发送的数据包，从而诊断网络中与数据相关的问题。例如，`-p ff` 将使用全部 1's 来填充发送的数据包。
- `-Q tos` — (可选) 输入十进制或十六进制数据报中的最大 1500 字节，以设置与服务质量 (QoS) 相关的位。
- `-s packetsize` — (可选) 输入要发送的数据字节数，从 1 到 65468，默认值为 56。
- `-S sndbuf` — (可选) 设置 sndbuf 插槽。默认情况下，sndbuf 套接字会将一个数据包进行最大限度地缓冲。
- `-t ttl` — (可选) 输入 IPv6 的生存时间 (TTL) 值 (以秒为单位)。
- `-T timestamp_option` — (可选) 设置特殊 IP 时间戳选项。timestamp\_option 的有效值—  
`tsonly` (仅时间戳)、`tsandaddr` (时间戳和地址) 或 `tsprespec host1 [host2 [host3 [host4]]]` (时间戳预指定的跳)
- `-v` — (可选) Verbose 输出。
- `-V` — (可选) 显示版本并退出。
- `-w deadline` — (可选) 输入 ping 退出之前的超时值 (以秒为单位)，而不考虑发送或接收多少个数据包。
- `-W timeout` — (可选) 输入等待响应的的时间 (以秒为单位)。此设置仅在没有响应时影响超时，否则 ping 将等待两次往返时间 (RTT)。
- `hop1 ...` (可选) 为要执行的 ping 数据包输入预先指定的跳的 IPv6 地址。
- `destination` — 以 A:B::C:D 格式输入 IPv6 目标地址的格式以在其中测试连接。

默认

未配置

命令模式

EXEC

使用情况信息

此命令使用 ICMP ECHO\_REQUEST 数据报从网络主机或网关上接收 ICMP ECHO\_RESPONSE。每个 ping 数据包都有 IPv6 和 ICMP 标头，然后是用于填充数据包的时间值和数字“pad”字节。pingv6 操作将数据包发送到指定的 IPv6 地址，然后测量从地址或设备获取响应所需的时间。

当您使用 `-I` 选项并输入 IP 地址时，OS10 会将其视为源地址。如果您使用的是接口名称而不是 IP 地址，OS10 会将其视为出口接口。

使用 `-I` 选项时，如果使用环回接口的 IP 地址作为源接口 ping 可访问的 IP 地址，则 ping 操作成功。但是，如果使用环回接口的名称作为源接口 ping 可访问的 IP 地址，则 ping 操作失败。这是因为系统将环回接口视为出口接口。

示例

```
OS10# ping6 20::1
PING 20::1(20::1) 56 data bytes
64 bytes from 20::1: icmp_seq=1 ttl=64 time=2.07 ms
64 bytes from 20::1: icmp_seq=2 ttl=64 time=2.21 ms
```

```
64 bytes from 20::1: icmp_seq=3 ttl=64 time=2.37 ms
64 bytes from 20::1: icmp_seq=4 ttl=64 time=2.10 ms
^C
--- 20::1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.078/2.194/2.379/0.127 ms
```

**支持的版本** 10.2.0E or later

## reload

重新加载软件并重新启动已启用 ONIE 的设备。

**语法** reload

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息**  **注:** 使用此命令时请小心，因为它将重新加载 OS10 映像并重新引导设备。

**示例**

```
OS10# reload

Proceed to reboot the system? [confirm yes/no]:y
```

**支持的版本** 10.2.0E or later

## show boot

显示有关引导映像的详细信息。

**语法** show boot [detail]

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** Next-Boot 字段显示下一次重新加载使用的分区。

**示例**

```
OS10# show boot
Current system image information:
=====
Type Boot Type Active Standby Next-Boot

Node-id 1 Flash Boot [B] 10.5.0.0 [A] 10.5.0.0 [B] activ
```

**示例 (详细信息)**

```
OS10# show boot detail
Current system image information detail:
=====
Type: Node-id 1
Boot Type: Flash Boot
Active Partition: B
Active SW Version: 10.5.0.0
Active SW Build Version: 10.5.0.270
Active Kernel Version: Linux 4.9.168
Active Build Date/Time: 2019-07-29T23:35:01Z
Standby Partition: A
Standby SW Version: 10.5.0EX
Standby SW Build Version: 10.5.0EX.252
```

```
Standby Build Date/Time: 2019-07-27T17:31:55Z
Next-Boot: active[B]
```

支持的版本 10.2.0E or later

## show candidate-configuration

显示当前候选配置文件。

**语法**

```
show candidate-configuration [aaa | access-list | as-path | bgp | class-map | community-list | compressed | control-plane | dot1x | extcommunity-list | interface | ip dhcp snooping | lacp | line | lldp | logging | monitor | ospf | ospfv3 | policy-map | prefix-list | qos-map | radius-server | route-map | sflow | snmp | spanning-tree | support-assist | system-qos | trust-map | users | vlt]
```

- 参数**
- aaa — (可选) 当前候选 AAA 配置。
  - access-list — (可选) 当前候选访问列表配置。
  - as-path — (可选) 当前候选路径配置。
  - bgp — (可选) 当前候选 BGP 配置。
  - class-map — (可选) 当前候选类映射配置。
  - community-list — (可选) 当前候选社区列表配置。
  - compressed — (可选) 压缩格式的当前候选配置。
  - control-plane — (可选) 当前候选控制平面配置。
  - dot1x — (可选) 当前候选 dot1x 配置。
  - extcommunity-list — (可选) 当前候选 extcommunity 列表配置。
  - interface — (可选) 当前候选接口配置。
  - ip dhcp snooping — (可选) 当前候选 DHCP 侦听信息。
  - lacp — (可选) 当前候选 LACP 配置。
  - lldp — (可选) 当前候选 LLDP 配置。
  - logging — (可选) 当前候选日志记录配置。
  - monitor — (可选) 当前候选监控会话配置。
  - ospf — (可选) 当前候选 OSPF 配置。
  - ospfv3 — (可选) 当前候选 OSPFv3 配置。
  - policy-map — (可选) 当前候选策略-映射配置。
  - prefix-list — (可选) 当前候选前缀-列表配置。
  - qos-map — (可选) 当前候选 qos-映射配置。
  - radius-server — (可选) 当前候选 RADIUS 服务器配置。
  - route-map — (可选) 当前候选路由映射配置。
  - sflow — (可选) 当前候选 sFlow 配置。
  - snmp — (可选) 当前候选 SNMP 配置。
  - spanning-tree — (可选) 当前候选生成树配置。
  - support-assist — (可选) 当前候选支持—帮助配置。
  - system-qos — (可选) 当前候选系统-qos 配置。
  - trust-map — (可选) 当前候选信任映射配置。
  - users — (可选) 当前候选用户配置。
  - vlt — (可选) 当前候选项 VLT 域配置。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# show candidate-configuration
! Version 10.2.9999E
! Last configuration change at Apr 11 10:36:43 2017
!
username admin password
```



```
6q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/VKx8SloIhp4NoGZs0I/
UNwh8WVuxwfd9q4pWigNs5BKH.
aaa authentication local
snmp-server contact http://www.dell.com/support
snmp-server location "United States"
logging monitor disable
ip route 0.0.0.0/0 10.11.58.1
!
interface ethernet1/1/1
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/2
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/3
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/4
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/5
 switchport access vlan 1
 no shutdown
!
--more--
```

#### 示例（已压缩）

```
OS10# show candidate-configuration compressed
username admin password
6q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/VKx8SloIhp4NoGZs0I/
UNwh8WVuxwfd9q4pWigNs5BKH.
aaa authentication local
snmp-server contact http://www.dell.com/support
snmp-server location "United States"
logging monitor disable
ip route 0.0.0.0/0 10.11.58.1
!
interface range ethernet 1/1/1-1/1/32
 switchport access vlan 1
 no shutdown
!
interface vlan 1
 no shutdown
!
interface mgmt1/1/1
 ip address 10.11.58.145/8
 no shutdown
 ipv6 enable
 ipv6 address autoconfig
!
support-assist
!
policy-map type application policy-iscsi
!
class-map type application class-iscsi
```

**支持的版本** 10.2.0E or later

## show environment

显示有关环境系统组件的信息，例如温度、风扇和电压。

**语法** show environment

参数 无  
默认 未配置  
命令模式 EXEC  
使用情况信息 无  
示例

```
OS10# show environment

Unit State Temperature

1 up 43

Thermal sensors
Unit Sensor-Id Sensor-name Temperature

1 1 CPU On-Board temp sensor 32
1 2 Switch board temp sensor 28
1 3 System Inlet Ambient-1 temp sensor 27
1 4 System Inlet Ambient-2 temp sensor 25
1 5 System Inlet Ambient-3 temp sensor 26
1 6 Switch board 2 temp sensor 31
1 7 Switch board 3 temp sensor 41
1 8 NPU temp sensor 43
```

支持的版本 10.2.0E or later

show inventory

显示系统清单信息。

语法 show inventory  
参数 无  
默认 未配置  
命令模式 EXEC  
使用情况信息 无  
示例

```
OS10# show inventory
Product : S4148F-ON
Description : S4148F-ON 48x10GbE, 2x40GbE QSFP+, 4x100GbE QSFP28 Interfa
Software version : 10.5.0.0
Product Base :
Product Serial Number :
Product Part Number :

Unit Type Part Number Rev Piece Part ID Svc Tag

* 1 S4148F-ON 09H9MN X01 TW-09H9MN-28298-713-0026 9531XC2
1 S4148F-ON-PWR-1-AC 06FKHH A00 CN-06FKHH-28298-6B5-03NY
1 S4148F-ON-FANTRAY-1 0N7MH8 X01 TW-0N7MH8-28298-713-0101
1 S4148F-ON-FANTRAY-2 0N7MH8 X01 TW-0N7MH8-28298-713-0102
1 S4148F-ON-FANTRAY-3 0N7MH8 X01 TW-0N7MH8-28298-713-0103
1 S4148F-ON-FANTRAY-4 0N7MH8 X01 TW-0N7MH8-28298-713-0104
```

支持的版本 10.2.0E or later

show ip management-route

显示用于访问管理端口的 IPv4 路由。

语法 show ip management-route [all | connected | summary]

参数

- all — (可选) 显示管理端口使用的 IPv4 路由。
- connected — (可选) 仅显示直接连接到管理端口的路由。
- summary — (可选) 显示活动和非活动管理路由及其远程目标的数量。
- static — (可选) 显示非活动管理路由。

默认

未配置

命令模式

EXEC

使用情况信息

使用此命令可以查看为管理端口配置的 IPv4 静态和连接的路由。使用 management route 命令可配置 IPv4 或 IPv6 管理路由。

示例

```
OS10# show ip management-route
```

| Destination     | Gateway            | State     | Source    |
|-----------------|--------------------|-----------|-----------|
| 192.168.10.0/24 | managementethernet | Connected | Connected |

支持的版本

10.2.2E or later

## show ipv6 management-route

显示用于访问管理端口的 IPv6 路由。

| 语法            | show ipv6 management-route [all   connected   summary]                                                                                                                                                                                                                                                                      |             |         |       |       |       |       |               |                        |           |               |             |        |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------|-------|-------|-------|-------|---------------|------------------------|-----------|---------------|-------------|--------|
| 参数            | <ul style="list-style-type: none"><li>all — (可选) 显示管理端口使用的 IPv6 路由。</li><li>connected — (可选) 仅显示直接连接到管理端口的路由。</li><li>summary — (可选) 显示活动和非活动管理路由及其远程目标的数量。</li><li>static — (可选) 显示非活动管理路由。</li></ul>                                                                                                                      |             |         |       |       |       |       |               |                        |           |               |             |        |
| 默认            | 未配置                                                                                                                                                                                                                                                                                                                         |             |         |       |       |       |       |               |                        |           |               |             |        |
| 命令模式          | EXEC                                                                                                                                                                                                                                                                                                                        |             |         |       |       |       |       |               |                        |           |               |             |        |
| 使用情况信息        | 使用此命令可以查看为管理端口配置的 IPv6 静态路由和连接的路由。使用 management route 命令可配置 IPv4 或 IPv6 管理路由。                                                                                                                                                                                                                                               |             |         |       |       |       |       |               |                        |           |               |             |        |
| 示例            | <pre>OS10# show ipv6 management-route</pre> <table><tr><th>Destination</th><th>Gateway</th><th>State</th></tr><tr><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>2001:34::0/64</td><td>ManagementEthernet 1/1</td><td>Connected</td></tr><tr><td>2001:68::0/64</td><td>2001:34::16</td><td>Active</td></tr></table> | Destination | Gateway | State | ----- | ----- | ----- | 2001:34::0/64 | ManagementEthernet 1/1 | Connected | 2001:68::0/64 | 2001:34::16 | Active |
| Destination   | Gateway                                                                                                                                                                                                                                                                                                                     | State       |         |       |       |       |       |               |                        |           |               |             |        |
| -----         | -----                                                                                                                                                                                                                                                                                                                       | -----       |         |       |       |       |       |               |                        |           |               |             |        |
| 2001:34::0/64 | ManagementEthernet 1/1                                                                                                                                                                                                                                                                                                      | Connected   |         |       |       |       |       |               |                        |           |               |             |        |
| 2001:68::0/64 | 2001:34::16                                                                                                                                                                                                                                                                                                                 | Active      |         |       |       |       |       |               |                        |           |               |             |        |
| 支持的版本         | 10.2.2E or later                                                                                                                                                                                                                                                                                                            |             |         |       |       |       |       |               |                        |           |               |             |        |

## show license status

显示许可证状态信息。

|        |                                                                                |
|--------|--------------------------------------------------------------------------------|
| 语法     | <code>show license status</code>                                               |
| 参数     | 无                                                                              |
| 默认     | 未配置                                                                            |
| 命令模式   | EXEC                                                                           |
| 使用情况信息 | 使用 <code>show license status</code> 命令以验证用于正在运行的 OS10 的当前版本、其持续时间和分配给交换机的服务编号。 |
| 示例     | <pre>OS10# show license status</pre> <pre>System Information</pre>             |

```

Vendor Name : DELL EMC
Product Name : S4148F-ON
Hardware Version : X01
Platform Name : x86_64-dell_s4100_c2338-r0
PPID : TW09H9MN282987130026
Service Tag : 9531XC2
Product Base :
Product Serial Number:
Product Part Number :
License Details

Software : OS10-Enterprise
Version : 10.5.0.0
License Type : PERPETUAL
License Duration : Unlimited
License Status : Active
License location : /mnt/license/9531XC2.lic

```

**支持的版本** 10.3.0E or later

## show running-configuration

显示设备上当前运行的配置。

### 语法

```
show running-configuration [aaa | access-list | as-path | bgp | class-map |
community-list | compressed | control-plane | dot1x | extcommunity-list |
interface [virtual-network vn-id] | ip dhcp snooping | lacp | line | lldp |
logging | monitor | ospf | ospfv3 | policy-map | prefix-list | qos-map |
radius-server | route-map | sflow | snmp | spanning-tree | support-assist |
system-qos | trust-map | users | vlt]
```

### 参数

- aaa — (可选) 当前正在运行的 AAA 配置。
- access-list — (可选) 当前正在运行的访问列表配置。
- as-path — (可选) 当前正在运行的路径配置。
- bgp — (可选) 当前正在运行的 BGP 配置。
- class-map — (可选) 当前正在运行的类别映射配置。
- community-list — (可选) 当前正在运行的社区-列表配置。
- compressed — (可选) 压缩格式的当前正在运行的配置。
- control-plane — (可选) 当前正在运行的控制平面配置。
- dot1x — (可选) 当前正在运行的 dot1x 配置。
- extcommunity-list — (可选) 当前正在运行的 外部社区-列表配置。
- interface — (可选) 当前正在运行的接口配置。
  - o virtual-network *vn-id* — (可选) 当前虚拟网络配置。
- ip dhcp snooping — (可选) 当前正在运行的 DHCP 侦听信息。
- lacp — (可选) 当前正在运行的 LACP 配置。
- lldp — (可选) 当前正在运行的 LLDP 配置。
- logging — (可选) 当前正在运行的日志记录配置。
- monitor — (可选) 当前正在运行的监控会话配置。
- ospf — (可选) 当前正在运行的 OSPF 配置。
- ospfv3 — (可选) 当前正在运行的 OSPFv3 配置。
- policy-map — (可选) 当前正在运行的策略-映射配置。
- prefix-list — (可选) 当前正在运行的前缀-列表配置。
- qos-map — (可选) 当前正在运行的 qos-映射配置。
- radius-server — (可选) 当前正在运行的 radius 服务器配置。
- route-map — (可选) 当前正在运行的路由映射配置。
- sflow — (可选) 当前正在运行的 sFlow 配置。
- snmp — (可选) 当前正在运行的 SNMP 配置。
- spanning-tree — (可选) 当前正在运行的生成树配置。

- support-assist — (可选) 当前正在运行的支持-帮助配置。
- system-qos — (可选) 当前正在运行的系统-qos 配置。
- trust-map — (可选) 当前正在运行的信任映射配置。
- users — (可选) 当前正在运行的用户配置。
- vlt — (可选) 当前正在运行的 VLT 域配置。

默认

未配置

命令模式

EXEC

使用情况信息

无

示例

```
OS10# show running-configuration
! Version 10.2.9999E
! Last configuration change at Apr 11 01:25:02 2017
!
username admin password
6q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/VKx8SloIhp4NoGZs0I/
UNwh8WVuxwfd9q4pWIGNs5BKH.
aaa authentication local
snmp-server contact http://www.dell.com/support
snmp-server location "United States"
logging monitor disable
ip route 0.0.0.0/0 10.11.58.1
!
interface ethernet1/1/1
switchport access vlan 1
no shutdown
!
interface ethernet1/1/2
switchport access vlan 1
no shutdown
!
interface ethernet1/1/3
switchport access vlan 1
no shutdown
!
interface ethernet1/1/4
switchport access vlan 1
no shutdown
!
interface ethernet1/1/5
switchport access vlan 1
no shutdown
!
interface ethernet1/1/6
switchport access vlan 1
no shutdown
--more--
```

示例 (已压缩)

```
OS10# show running-configuration compressed
username admin password
6q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/VKx8SloIhp4NoGZs0I/
UNwh8WVuxwfd9q4pWIGNs5BKH.
aaa authentication local
snmp-server contact http://www.dell.com/support
snmp-server location "United States"
logging monitor disable
ip route 0.0.0.0/0 10.11.58.1
!
interface range ethernet 1/1/1-1/1/32
switchport access vlan 1
no shutdown
!
interface vlan 1
no shutdown
!
interface mgmt1/1/1
ip address 10.11.58.145/8
```

```

no shutdown
ipv6 enable
ipv6 address autoconfig

!
support-assist
!
policy-map type application policy-iscsi
!
class-map type application class-iscsi

```

**支持的版本** 10.2.0E or later

## show startup-configuration

显示启动配置文件的内容。

**语法** show startup-configuration [compressed]

**参数** compressed — (可选) 查看启动配置文件的压缩版本。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```

OS10# show startup-configuration
username admin password
6q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/VKx8SloIhp4NoGZs0I/
UNwh8WVuxwfd9q4pWigNs5BKH.
aaa authentication local
snmp-server contact http://www.dell.com/support
snmp-server location "United States"
ip route 0.0.0.0/0 10.11.58.1
!
interface ethernet1/1/1
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/2
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/3
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/4
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/5
 switchport access vlan 1
 no shutdown
!
--more--

```

**示例 (已压缩)**

```

OS10# show startup-configuration compressed
username admin password
6q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/VKx8SloIhp4NoGZs0I/
UNwh8WVuxwfd9q4pWigNs5BKH.
aaa authentication local
snmp-server contact http://www.dell.com/support
snmp-server location "United States"
ip route 0.0.0.0/0 10.11.58.1
!
interface range ethernet 1/1/1-1/1/32

```

```

switchport access vlan 1
no shutdown
!
interface vlan 1
no shutdown
!
interface mgmt1/1/1
ip address 10.11.58.145/8
no shutdown
ipv6 enable
ipv6 address autoconfig

!
support-assist
!
policy-map type application policy-iscsi
!
class-map type application class-iscsi

```

**支持的版本** 10.2.0E or later

## show system

显示系统信息。

**语法**

show system [brief | node-id]

**参数**

- brief — 查看系统信息的缩写列表。
- node-id — 查看节点 ID 号。

**默认**

未配置

**命令模式**

EXEC

**使用情况信息**

无

**示例**

```

OS10# show system

Node Id : 1
MAC : 14:18:77:15:c3:e8
Number of MACs : 256
Up Time : 1 day 00:48:58

-- Unit 1 --
Status : up
System Identifier : 1
Down Reason : unknown
Digital Optical Monitoring : disable
System Location LED : off
Required Type : S4148F
Current Type : S4148F
Hardware Revision : X01
Software Version : 10.5.0.0
Physical Ports : 48x10GbE, 2x40GbE, 4x100GbE
BIOS : 3.33.0.0-3
System CPLD : 0.4
Master CPLD : 0.10
Slave CPLD : 0.7

-- Power Supplies --
PSU-ID Status Type AirFlow Fan Speed(rpm) Status

1 up AC NORMAL 1 13312 up
2 fail

-- Fan Status --
FanTray Status AirFlow Fan Speed(rpm) Status

```

|   |    |        |   |       |    |
|---|----|--------|---|-------|----|
| 1 | up | NORMAL | 1 | 13195 | up |
| 2 | up | NORMAL | 1 | 13151 | up |
| 3 | up | NORMAL | 1 | 13239 | up |
| 4 | up | NORMAL | 1 | 13239 | up |

### 示例 (node-id)

```
OS10# show system node-id 1 fanout-configured
```

| Interface  | Breakout capable | Breakout state |
|------------|------------------|----------------|
| Eth 1/1/5  | No               | BREAKOUT_1x1   |
| Eth 1/1/6  | No               | BREAKOUT_1x1   |
| Eth 1/1/7  | No               | BREAKOUT_1x1   |
| Eth 1/1/8  | No               | BREAKOUT_1x1   |
| Eth 1/1/9  | No               | BREAKOUT_1x1   |
| Eth 1/1/10 | No               | BREAKOUT_1x1   |
| Eth 1/1/11 | No               | BREAKOUT_1x1   |
| Eth 1/1/12 | No               | BREAKOUT_1x1   |
| Eth 1/1/13 | No               | BREAKOUT_1x1   |
| Eth 1/1/14 | No               | BREAKOUT_1x1   |
| Eth 1/1/15 | No               | BREAKOUT_1x1   |
| Eth 1/1/16 | No               | BREAKOUT_1x1   |
| Eth 1/1/17 | No               | BREAKOUT_1x1   |
| Eth 1/1/18 | No               | BREAKOUT_1x1   |
| Eth 1/1/19 | No               | BREAKOUT_1x1   |
| Eth 1/1/20 | No               | BREAKOUT_1x1   |
| Eth 1/1/21 | No               | BREAKOUT_1x1   |
| Eth 1/1/22 | No               | BREAKOUT_1x1   |
| Eth 1/1/23 | No               | BREAKOUT_1x1   |
| Eth 1/1/24 | No               | BREAKOUT_1x1   |
| Eth 1/1/25 | Yes              | BREAKOUT_1x1   |

### 示例 (brief)

```
OS10# show system brief
```

Node Id : 1  
MAC : 14:18:77:15:c3:e8

-- Unit --

| Unit | Status | ReqType | CurType | Version  |
|------|--------|---------|---------|----------|
| 1    | up     | S4148F  | S4148F  | 10.5.0EX |

-- Power Supplies --

| PSU-ID | Status | Type | AirFlow | Fan | Speed(rpm) | Status |
|--------|--------|------|---------|-----|------------|--------|
| 1      | up     | AC   | NORMAL  | 1   | 13312      | up     |
| 2      | fail   |      |         |     |            |        |

-- Fan Status --

| FanTray | Status | AirFlow | Fan | Speed(rpm) | Status |
|---------|--------|---------|-----|------------|--------|
| 1       | up     | NORMAL  | 1   | 13195      | up     |
| 2       | up     | NORMAL  | 1   | 13151      | up     |
| 3       | up     | NORMAL  | 1   | 13239      | up     |
| 4       | up     | NORMAL  | 1   | 13239      | up     |

### 支持的版本

10.2.0E or later



## show version

显示软件版本信息。

|        |              |
|--------|--------------|
| 语法     | show version |
| 参数     | 无            |
| 默认     | 未配置          |
| 命令模式   | EXEC         |
| 使用情况信息 | 无            |
| 示例     |              |

```
OS10# show version
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2019 by Dell Inc. All Rights Reserved.
OS Version: 10.5.0.0
Build Version: 10.5.0.270
Build Time: 2019-07-29T23:35:01+0000
System Type: S4148F-ON
Architecture: x86_64
Up Time: 1 day 00:54:13
```

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|

## start

为活动会话激活基于事务的配置模式。

|        |                                           |
|--------|-------------------------------------------|
| 语法     | start transaction                         |
| 参数     | transaction — 启用基于事务的配置。                  |
| 默认     | 未配置                                       |
| 命令模式   | EXEC                                      |
| 使用情况信息 | 在对正在运行的配置应用配置更改之前，使用 start 命令可保存对候选配置的更改。 |

 **注：**在开始事务之前，必须在 EXEC 模式下使用 lock 命令锁定会话。否则，将提交其他会话中的配置更改。

|    |                         |
|----|-------------------------|
| 示例 | OS10# start transaction |
|----|-------------------------|

|       |                  |
|-------|------------------|
| 支持的版本 | 10.3.1E or later |
|-------|------------------|

## 系统

从 OS10 中执行 Linux 命令。

|        |                                                                                             |
|--------|---------------------------------------------------------------------------------------------|
| 语法     | system command                                                                              |
| 参数     | command — 输入要执行的 Linux 命令。                                                                  |
| 默认     | 未配置                                                                                         |
| 命令模式   | EXEC                                                                                        |
| 使用情况信息 | 从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。 |

|    |                                                               |
|----|---------------------------------------------------------------|
| 示例 | OS10# system bash<br>admin@OS10:~\$ pwd<br>/config/home/admin |
|----|---------------------------------------------------------------|

```
admin@OS10:~$ exit
OS10#
```

**支持的版本** 10.2.0E or later

## system-cli disable

禁用 `system` 命令。

**语法** `system-cli disable`

**参数** 无

**默认** 已启用

**命令模式** CONFIGURATION

**使用情况信息** 从版本 10.4.3.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。

此命令的 `no` 版本将启用 OS10 `system` 命令。

**示例**

```
OS10# configure terminal
OS10(config)# system-cli disable
```

**支持的版本** 10.4.3.0 or later

## system-user linuxadmin disable

禁用 `linuxadmin` 帐户。

**语法** `system-user linuxadmin disable`

**参数** 无

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** `linuxadmin` 帐户允许您访问 Linux shell。使用 `system-user linuxadmin disable` 命令可禁用 Linux shell 访问权限。您仍可以使用 `system` 命令从 OS10 命令行接口运行 Linux 命令。要禁用 `system` 命令以阻止执行 Linux 命令，请使用 `system-cli disable` 命令。

**示例**

```
OS10(config)# system-user linuxadmin disable
```

**支持的版本** 10.4.3.0 or later

## system identifier

在非堆栈配置中设置非默认单元 ID。

**语法** `system identifier system-id`

**参数** `system-id` — 输入系统 ID，从 1 到 9。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 系统 ID 显示在交换机前面板上的堆栈 LED 中。

从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。

## 示例

```
OS10(config)# system identifier 1
```

## 支持的版本

10.3.0E or later

# terminal

设置要在终端上显示的线路数，并启用日志记录。

**语法** `terminal {length lines | monitor}`

- 参数**
- `length lines` — 输入要在终端上显示的线路数，从 0 到 512；默认值为 24。
  - `monitor` — 启用终端上的日志记录。

**默认** 24 个终端线路

**命令模式** EXEC

**使用情况信息** 输入零 (0) 以便终端显示而不暂停。

## 示例

```
OS10# terminal monitor
```

## 支持的版本

10.2.0E or later

# traceroute

显示数据包传输到 IP 地址所用的路由。

**语法** `traceroute [vrf {management | vrf-name}] host [-46dFITnreAUDV] [-f first_ttl] [-g gate,...] [-i device] [-m max_ttl] [-N squeries] [-p port] [-t tos] [-l flow_label] [-w waittime] [-q nqueries] [-s src_addr] [-z sendwait] [--fwmark=num] host [packetlen]`

- 参数**
- `vrf management` — (可选) 将路由跟踪到管理 VRF 实例中的 IP 地址。
  - `vrf vrf-name` — (可选) 将路由跟踪到指定 VRF 实例中的 IP 地址。
  - `host` — 输入用于跟踪数据包的主机。
  - `-i interface` — (可选) 输入用于跟踪路由发送数据包的接口的 IP 地址。默认情况下，根据路由表选择接口。
  - `-m max_ttl` — (可选) 输入跟踪路由探测的最大生存时间值的最大跳数。默认值为 30。
  - `-p port` — (可选) 输入目标端口：
    - 对于 UDP 跟踪，请输入跟踪路由使用的目标端口基座。每个探测都会增加目标端口号。
    - 对于 ICMP 跟踪，请输入初始 ICMP 顺序值，每次探测进行增量。
    - 对于 TCP 跟踪，输入要连接的常数目端口。
    - `-P protocol` — (可选) 使用指定协议的原始数据包进行跟踪路由。默认协议为 253 (RFC 3692)。
    - `-s source_address` — (可选) 输入其中一个接口的备用源地址。默认情况下，使用传出接口的地址。
    - `-q nqueries` — (可选) 输入每跳的探测数据包数。默认值为 3。
    - `-N squeries` — (可选) 输入同时发送出去以加速跟踪路由的探测数据包数量。默认值为 16。
    - `-t tos` — (可选) 对于 IPv4，输入要使用的服务类型 (ToS) 和优先级值。16 可设置低延迟；8 可设置高吞吐量。
    - `-UL` — (可选) 将 UDPLITE 用于跟踪路由。默认端口是 53。
    - `-w waittime` — (可选) 输入等待探测响应的的时间 (以秒为单位)。默认值为 5 秒。
    - `-z sendwait` — (可选) 输入两次探测之间等待的最短时间间隔。默认值为 0。大于 10 的值指定的值以毫秒为单位，否则指定的值以秒为单位。当路由器速率限制 ICMP 消息时，此选项非常有用。
    - `--mtu` — (可选) 从正在跟踪的路径中查找最大传输单元 (MTU)。
    - `--back` — (可选) 根据转发方向，打印反向跳转的数量。
  - `host` — (必填) 输入目标设备的名称或 IP 地址。
  - `packet_len` — (可选) 输入探测数据包的总大小。对于 IPv4，默认值为 60 字节，IPv6 为 80。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 示例     | <pre>OS10# traceroute www.dell.com traceroute to www.dell.com (23.73.112.54), 30 hops max, 60 byte packets  1  10.11.97.254 (10.11.97.254)  4.298 ms  4.417 ms  4.398 ms  2  10.11.3.254 (10.11.3.254)  2.121 ms  2.326 ms  2.550 ms  3  10.11.27.254 (10.11.27.254)  2.233 ms  2.207 ms  2.391 ms  4  Host65.hbms.com (63.80.56.65)  3.583 ms  3.776 ms  3.757 ms  5  host33.30.198.65 (65.198.30.33)  3.758 ms  4.286 ms  4.221 ms  6  3.GigabitEthernet3-3.GW3.SCL2.ALTER.NET (152.179.99.173)  4.428 ms    2.593 ms  3.243 ms  7  0.xe-7-0-1.XL3.SJC7.ALTER.NET (152.63.48.254)  3.915 ms  3.603 ms    3.790 ms  8  TenGigE0-4-0-5.GW6.SJC7.ALTER.NET (152.63.49.254)  11.781 ms  10.600 ms  9.402 ms  9  23.73.112.54 (23.73.112.54)  3.606 ms  3.542 ms  3.773 ms</pre> |

|           |                                                                                                                                             |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 (IPv6) | <pre>OS10# traceroute 20::1 traceroute to 20::1 (20::1), 30 hops max, 80 byte packets  1  20::1 (20::1)  2.622 ms  2.649 ms  2.964 ms</pre> |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------|

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|

## unlock

解锁先前锁定的候选配置文件。

|        |                         |
|--------|-------------------------|
| 语法     | <code>unlock</code>     |
| 参数     | 无                       |
| 默认     | 未配置                     |
| 命令模式   | EXEC                    |
| 使用情况信息 | 无                       |
| 示例     | <pre>OS10# unlock</pre> |
| 支持的版本  | 10.2.0E or later        |

## username password role

根据用户名和密码创建身份验证条目，并将角色分配给用户。

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>username <i>username</i> password <i>password</i> role <i>role</i> [<i>priv-lvl</i> <i>privilege-level</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 参数 | <ul style="list-style-type: none"> <li><code>username <i>username</i></code>— 输入文本字符串。最多 32 个字母数字字符；至少一个字符。</li> <li><code>password <i>password</i></code>— 输入文本字符串。最多 32 个字母数字字符；最少 9 个字符。密码前缀 <code>\$1\$</code>、<code>\$5\$</code> 和 <code>\$6\$</code> 不支持明文密码。</li> <li><code>role <i>role</i></code>— 输入用户角色： <ul style="list-style-type: none"> <li><code>sysadmin</code> — 对系统中所有命令的完全访问权限、对操作文件系统的命令的独占访问权限，以及对系统 shell 的访问权限。系统管理员可以创建用户 ID 和用户角色。</li> <li><code>secadmin</code> — 对设置安全策略和系统访问权限的配置命令的完全访问权限，如密码强度、AAA 授权和加密密钥。安全管理员可以显示安全信息，如加密密钥、登录统计信息和日志信息。</li> <li><code>netadmin</code> — 对管理流经交换机（如路由、接口和 ACL）的流量的配置命令的完全访问权限。网络管理员无法访问安全功能的配置命令或查看安全信息。</li> <li><code>netoperator</code> — 访问 EXEC 模式以查看当前配置。网络操作员无法修改交换机上的任何配置设置。</li> </ul> </li> </ul> |

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <ul style="list-style-type: none"> <li>• <code>priv-lvl privilege-level</code> — 输入权限级别，从 0 到 15。如果未指定 <code>priv-lvl</code> 选项，系统将为 <code>netoperator</code> 角色分配权限级别 1，为 <code>sysadmin</code>、<code>secadmin</code> 和 <code>netadmin</code> 角色分配权限级别 15。</li> </ul>                                                                                                                                                                                                                                                                                                   |
| 默认     | <ul style="list-style-type: none"> <li>• 用户名和密码条目以明文形式输入。</li> <li>• 没有默认用户角色。</li> <li>• 对于 <code>netoperator</code>，默认的权限级别为 1，对于 <code>sysadmin</code>、<code>secadmin</code> 和 <code>netadmin</code> 为级别 15。</li> </ul>                                                                                                                                                                                                                                                                                                                                               |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 使用情况信息 | <p>默认情况下，密码必须至少包含 9 个字母数字字符。仅支持以下特殊字符：</p> <pre>! # % &amp; ' ( ) ; &lt; = &gt; [ ] * + - . / : ^ _</pre> <p>以明文形式输入密码。它会转换为正在运行的配置中的 SHA-512 格式。为了向后兼容 OS10 版本 10.3.1E 及更低版本，支持以 MD-5、SHA-256 和 SHA-512 格式输入密码。</p> <p>对于 <code>sysadmin</code>、<code>secadmin</code> 和 <code>netadmin</code> 角色，您不能将高于权限级别 1 的权限级别分配给具有 <code>netoperator</code> 角色且权限级别高于 2 的用户。</p> <p>要增加所需的密码强度，请使用 <code>password-attributes</code> 命令。此命令的 <code>no</code> 版本将删除用户身份验证。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p> |
| 示例     | <pre>OS10(config)# username user05 password newpwd404 role sysadmin priv-lvl 10</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## write

将当前运行的配置复制到启动配置文件。

|        |                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>write {memory}</code>                                                                                                                     |
| 参数     | <code>memory</code> — 将当前运行的配置复制到启动配置。                                                                                                          |
| 默认     | 未配置                                                                                                                                             |
| 命令模式   | EXEC                                                                                                                                            |
| 使用情况信息 | 此命令与 <code>copy running-configuration startup-configuration</code> 命令的效果相同。正在运行的配置不会保存到除启动配置以外的本地配置文件。使用 <code>copy</code> 命令将正在运行的配置更改保存到本地文件。 |
| 示例     | <pre>OS10# write memory</pre>                                                                                                                   |
| 支持的版本  | 10.2.0E or later                                                                                                                                |

## 高级 CLI 任务

- 命令别名** 提供有关创建常用命令的快捷方式的信息，请参阅[命令别名](#)。
- 批处理模式** 提供信息以运行批处理文件以执行多个命令，请参阅[批处理模式](#)。
- Linux shell 命令** 提供有关从 Linux shell 运行命令的信息，请参阅[Linux shell 命令](#)。
- OS9 命令** 提供使用 OS9 命令语法输入配置命令的信息，请参阅[使用 OS9 命令](#)。

### 命令别名

要创建常用命令或长命令的快捷方式，请使用 `alias` 命令。命令别名可执行长命令和参数。

- 要创建在其他 OS10 会话中可用的永久命令别名，请在 CONFIGURATION 模式下创建别名。
- 要创建仅在当前 OS10 会话中使用的不永久命令别名，请在 EXEC 模式下创建别名。关闭会话后，该别名将从交换机中移除。
- 在 EXEC 或 CONFIGURATION 模式下创建命令别名。

```
alias alias-name alias-value
```

- `alias-name` 区分大小写，最多包含 20 个字符。它不支持现有的关键字、参数和短格式的关键字。
- `alias-value` 是通过别名执行的 CLI 命令。要输入命令参数，请输入 `$n`，其中 `n` 是 1 到 9 的数字或星号 (\*)。输入 `$*` 以输入带有别名的最多 9 个参数。
- 您不能为 `alias` 命令创建快捷方式。
- 要删除别名，请使用 `no alias alias-name` 命令。
- 要查看当前配置的别名，请使用 `show alias [brief | detail]` 命令。

#### 创建别名

```
OS10# alias showint "show interface $*"
OS10(config)# alias goint "interface ethernet $1"
```

#### 查看以下命令的别名输出 `showint`

```
OS10# showint status
```

| Port       | Description | Status | Speed | Duplex | Mode | Vlan | Tagged-Vlans |
|------------|-------------|--------|-------|--------|------|------|--------------|
| Eth 1/1/1  |             | up     | 40G   |        | A    | 1    | -            |
| Eth 1/1/2  |             | up     | 40G   |        | A    | 1    | -            |
| Eth 1/1/3  |             | up     | 40G   |        | A    | 1    | -            |
| Eth 1/1/4  |             | up     | 40G   |        | A    | 1    | -            |
| Eth 1/1/5  |             | up     | 40G   |        | A    | 1    | -            |
| Eth 1/1/6  |             | up     | 40G   |        | A    | 1    | -            |
| Eth 1/1/7  |             | up     | 40G   |        | A    | 1    | -            |
| Eth 1/1/8  |             | up     | 40G   |        | A    | 1    | -            |
| Eth 1/1/9  |             | up     | 40G   |        | A    | 1    | -            |
| Eth 1/1/10 |             | up     | 40G   |        | A    | 1    | -            |
| ...        |             |        |       |        |      |      |              |

#### 查看以下命令的别名输出 `goint`

```
OS10(config)# goint 1/1/1
OS10(conf-if-eth1/1/1)#
```

## 查看别名信息

```
OS10# show alias
Name Type
---- -
govlt Config
goimt Config
shconfig Local
showint Local
shver Local

Number of config aliases : 2
Number of local aliases : 3
```

## 查看别名信息简述。显示别名值的前 10 个字符。

```
OS10# show alias brief
Name Type Value
---- -
govlt Config "vlt-domain..."
goimt Config "interface ..."
shconfig Local "show runni..."
showint Local "show inter..."
shver Local "show versi..."

Number of config aliases : 2
Number of local aliases : 3
```

## 查看别名详细信息。显示整个别名值。

```
OS10# show alias detail
Name Type Value
---- -
govlt Config "vlt-domain $1"
goimt Config "interface ethernet $1"
shconfig Local "show running-configuration"
showint Local "show interface $"
shver Local "show version"

Number of config aliases : 2
Number of local aliases : 3
```

# 多行别名

您可以创建多行别名，在其中将一系列多个命令保存到别名中。只有配置模式支持多行别名。

您不能使用退出 CLI 关键字作为别名名称。别名区分大小写，最多可以包含 20 个字符。

- 在 CONFIGURATION 模式下创建多行别名。交换机将进入 ALIAS 模式。

```
alias alias-name
```

- 在 ALIAS 模式下，输入命令以执行以 `line n` 命令为前缀执行。使用双引号输入命令，然后使用 `$n` 输入输入参数。您可以从 1 到 9 或星号 (\*) 等数字替换 `$n`，并在使用别名执行命令时输入参数。当使用星号 (\*) 时，您可以使用所有输入参数。输入参数的最大数量为 9。

```
line nn command
```

- (可选) 您可以在 ALIAS 模式下输入要用于定义为 `$n` 参数的默认值。

```
default n input-value
```

- (可选) 在 ALIAS 模式下输入多行别名的说明。

```
description string
```

- 在 CONFIGURATION 模式下使用命令的 `no` 格式删除别名。

```
no alias alias-name
```

您可以通过进入相应的 ALIAS 模式来修改现有的多行别名。

### 创建多行别名

```
OS10(config)# alias mTest
OS10(config-alias-mTest)# line 1 "interface $1 $2"
OS10(config-alias-mTest)# line 2 "no shutdown"
OS10(config-alias-mTest)# line 3 "show configuration"
OS10(config-alias-mTest)# default 1 "ethernet"
OS10(config-alias-mTest)# default 2 "1/1/1"
OS10(config-alias-mTest)# description InterfaceDetails
```

### 查看 mTest 的别名输出和默认值

```
OS10(config)# mTest
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
 no shutdown
 switchport access vlan 1
```

### 查看 mTest 的别名输出和不同的值

```
OS10(config)# mTest ethernet 1/1/10
OS10(config)# interface ethernet 1/1/10
OS10(conf-if-eth1/1/10)# no shutdown
OS10(conf-if-eth1/1/10)# show configuration
!
interface ethernet1/1/10
 no shutdown
 switchport access vlan 1
```

### 修改现有的多行别名

```
OS10(config)# alias mTest
OS10(config-alias-mTest)# line 4 "exit"
```

### 查看保存在多行别名中的命令

```
OS10(config-alias-mTest)# show configuration
!
alias mTest
 description InterfaceDetails
 default 1 ethernet
 default 2 1/1/1
 line 1 "interface $1 $2"
 line 2 "no shutdown"
 line 3 "show configuration"
 line 4 exit
```

### 查看别名信息

```
OS10# show alias
Name Type
---- -
mTest Config

Number of config aliases : 1
Number of local aliases : 0
```



查看别名信息简述。显示每个别名行的前 10 个字符。

```
OS10# show alias brief
Name Type Value
---- -
mTest Config line 1 "interface ..."
 line 2 "no shutdow..."
 line 3 "show confi..."
 default 1 "ethernet"
 default 2 "1/1/1"

Number of config aliases : 1
Number of local aliases : 0
```

查看别名详细信息。显示整个别名值。

```
OS10# show alias detail
Name Type Value
---- -
mTest Config line 1 "interface $1 $2"
 line 2 "no shutdown"
 line 3 "show configuration"
 default 1 "ethernet"
 default 2 "1/1/1"

Number of config aliases : 1
Number of local aliases : 0
```

删除别名

```
OS10(config)# no alias mTest
```

## 别名

创建命令别名。

|        |                                                                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>alias alias-name alias-value</code>                                                                                                                                                               |
| 参数     | <ul style="list-style-type: none"><li><code>alias-name</code> — 输入别名的名称。最多 20 个字符。</li><li><code>alias-value</code> — 输入要在双引号中执行的命令，\$ 后面是从 1 到 9 的数字或星号 (*)，包含要在命令中执行的参数。使用星号 (*) 表示任意数量的参数。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                     |
| 命令模式   | EXEC<br>CONFIGURATION                                                                                                                                                                                   |
| 使用情况信息 | 使用此命令可创建长命令和参数的快捷方式。使用数字 1 至 9 以及 \$ 以提供输入参数。此命令的 no 版本会删除别名。                                                                                                                                           |
| 示例     | 在此示例中，当您输入 <code>showint status</code> 时，请注意，CLI 上的文本将更改为 <code>show interface status</code> 。别名将更改为别名定义中指定的命令。                                                                                         |

```
OS10# alias showint "show interface $*"
OS10# showint status

Port Description Status Speed Duplex Mode Vlan Tagged-Vlans

Eth 1/1/1 up 40G A 1 -
Eth 1/1/2 up 40G A 1 -
Eth 1/1/3 up 40G A 1 -
Eth 1/1/4 up 40G A 1 -
Eth 1/1/5 up 40G A 1 -
Eth 1/1/6 up 40G A 1 -
Eth 1/1/7 up 40G A 1 -
Eth 1/1/8 up 40G A 1 -
```

|            |    |     |   |   |   |
|------------|----|-----|---|---|---|
| Eth 1/1/9  | up | 40G | A | 1 | - |
| Eth 1/1/10 | up | 40G | A | 1 | - |
| Eth 1/1/11 | up | 40G | A | 1 | - |
| Eth 1/1/12 | up | 40G | A | 1 | - |
| Eth 1/1/13 | up | 40G | A | 1 | - |
| Eth 1/1/14 | up | 40G | A | 1 | - |
| Eth 1/1/15 | up | 40G | A | 1 | - |
| Eth 1/1/16 | up | 40G | A | 1 | - |
| Eth 1/1/17 | up | 40G | A | 1 | - |
| Eth 1/1/18 | up | 40G | A | 1 | - |
| Eth 1/1/19 | up | 40G | A | 1 | - |
| Eth 1/1/20 | up | 40G | A | 1 | - |
| Eth 1/1/21 | up | 40G | A | 1 | - |
| Eth 1/1/22 | up | 40G | A | 1 | - |
| Eth 1/1/23 | up | 40G | A | 1 | - |
| Eth 1/1/24 | up | 40G | A | 1 | - |
| Eth 1/1/25 | up | 40G | A | 1 | - |
| Eth 1/1/26 | up | 40G | A | 1 | - |
| Eth 1/1/27 | up | 40G | A | 1 | - |
| Eth 1/1/28 | up | 40G | A | 1 | - |
| Eth 1/1/29 | up | 40G | A | 1 | - |
| Eth 1/1/30 | up | 40G | A | 1 | - |
| Eth 1/1/31 | up | 40G | A | 1 | - |
| Eth 1/1/32 | up | 40G | A | 1 | - |

在此示例中，当您输入 `goint 1/1/1` 时，请注意，CLI 上的文本将更改为 `interface ethernet 1/1/1`。

```

OS10(config)# alias goint "interface ethernet $1"
OS10(config)# goint 1/1/1
OS10(conf-if-eth1/1/1)#

```

**支持的版本** 10.3.0E or later

## 别名（多行）

创建多行命令别名。

|        |                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------|
| 语法     | <code>alias <i>alias-name</i></code>                                                                            |
| 参数     | <i>alias-name</i> — 输入多行别名的名称。最多 20 个字符。                                                                        |
| 默认     | 未配置                                                                                                             |
| 命令模式   | CONFIGURATION                                                                                                   |
| 使用情况信息 | 使用此命令可在别名中保存一系列多个命令。当您创建别名时，交换机将进入 ALIAS 模式。您可以使用 <code>line</code> 命令输入要执行的一系列命令。此命令的 <code>no</code> 版本会删除别名。 |

**示例**

```

OS10(config)# alias mTest
OS10(config-alias-mTest)# line 1 "interface $1 $2"
OS10(config-alias-mTest)# line 2 "no shutdown"
OS10(config-alias-mTest)# line 3 "show configuration"

```

**支持的版本** 10.4.0E(R1) or later

## 默认值（别名）

使用多行别名配置输入参数的默认值。

|    |                                                                                                                 |
|----|-----------------------------------------------------------------------------------------------------------------|
| 语法 | <code>default <i>n value</i></code>                                                                             |
| 参数 | <ul style="list-style-type: none"> <li><i>n</i> — 输入参数的编号，从 1 到 9。</li> <li><i>value</i> — 输入输入参数的值。</li> </ul> |

|        |                                                                                           |
|--------|-------------------------------------------------------------------------------------------|
| 默认     | 未配置                                                                                       |
| 命令模式   | ALIAS                                                                                     |
| 使用情况信息 | 要在输入参数值中使用特殊字符，请用双引号 (") 将字符串括起来。此命令的 <code>no</code> 版本将移除默认值。                           |
| 示例     | <pre>OS10(config)# alias mTest OS10(config-alias-mTest)# default 1 "ethernet 1/1/1"</pre> |
| 支持的版本  | 10.4.0E(R1) or later                                                                      |

## 说明（别名）

为多行别名配置文本说明。

|        |                                                                                                                                                                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>description string</code>                                                                                                                                                                                                                                                        |
| 参数     | <code>string</code> — 输入多行别名说明的文本字符串。                                                                                                                                                                                                                                                  |
| 默认     | 未配置                                                                                                                                                                                                                                                                                    |
| 命令模式   | ALIAS                                                                                                                                                                                                                                                                                  |
| 使用情况信息 | <ul style="list-style-type: none"> <li>要将特殊字符用作说明字符串的一部分，请用双引号 (") 将字符串括起来。</li> <li>输入此命令后，将不会保留字符之间的空格，除非用引号将整个说明括起来（例如，<code>"text description."</code>）。</li> <li>要覆盖配置为说明的任何以前的文本字符串，请在 <code>description</code> 命令后输入一个文本字符串。</li> <li>此命令的 <code>no</code> 版本将移除该说明。</li> </ul> |
| 示例     | <pre>OS10(config)# alias mTest OS10(config-alias-mTest)# description "This alias configures interfaces"</pre>                                                                                                                                                                          |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                                                                                                                   |

## 行（别名）

配置要在多行别名中执行的命令。

|        |                                                                                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>line nn command</code>                                                                                                                                                                   |
| 参数     | <ul style="list-style-type: none"> <li><code>nn</code> — 输入行号，从 1 到 99。命令将按行号的顺序执行。</li> <li><code>command</code> — 输入要用双引号 (") 括起的命令。</li> </ul>                                              |
| 默认     | 未配置                                                                                                                                                                                            |
| 命令模式   | ALIAS                                                                                                                                                                                          |
| 使用情况信息 | 此命令的 <code>no</code> 版本将从多行别名中删除行号和相应的命令。                                                                                                                                                      |
| 示例     | <pre>OS10(config)# alias mTest OS10(config-alias-mTest)# line 1 "interface \$1 \$2" OS10(config-alias-mTest)# line 2 "no shutdown" OS10(config-alias-mTest)# line 3 "show configuration"</pre> |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                           |

## show alias

显示在持久和非持久模式下均可用的已配置别名命令。

|    |                                                                                   |
|----|-----------------------------------------------------------------------------------|
| 语法 | <code>show alias [brief   detail]</code>                                          |
| 参数 | <ul style="list-style-type: none"> <li><code>brief</code> — 显示别名的简要信息。</li> </ul> |

|        |                                                                       |
|--------|-----------------------------------------------------------------------|
|        | <ul style="list-style-type: none"><li>• detail — 显示别名的详细信息。</li></ul> |
| 默认     | 无                                                                     |
| 命令模式   | EXEC                                                                  |
| 使用情况信息 | 无                                                                     |

示例

```
OS10# show alias
Name Type
---- -
govlt Config
goint Config
mTest Config
shconfig Local
showint Local
shver Local
Number of config aliases : 3
Number of local aliases : 3
```

示例（简要 — 显示别名值的前 10 个字符）

```
OS10# show alias brief
Name Type Value
---- -
govlt Config "vlt-domain..."
goint Config "interface ..."
mTest Config line 1 "interface ..."
 line 2 "no shutdown..."
 line 3 "show confi..."
 default 1 "ethernet"
 default 2 "1/1/1"
shconfig Local "show runni..."
showint Local "show inter..."
shver Local "show versi..."

Number of config aliases : 3
Number of local aliases : 3
```

示例（详情 — 显示整个别名值）

```
OS10# show alias detail
Name Type Value
---- -
govlt Config "vlt-domain $1"
goint Config "interface ethernet $1"
mTest Config line 1 "interface $1 $2"
 line 2 "no shutdown"
 line 3 "show configuration"
 default 1 "ethernet"
 default 2 "1/1/1"
shconfig Local "show running-configuration"
showint Local "show interface $"
shver Local "show version"

Number of config aliases : 3
Number of local aliases : 3
```

支持的版本 10.3.0E or later

## 批处理模式

要执行多个命令的序列，请创建并运行一个批处理文件。批处理文件是一个未格式化的文本文件，其中包含两个或更多命令。将批处理文件存储在主目录中。

使用 vi 编辑器或任何其他编辑器来创建批处理文件，然后使用 batch 命令运行该文件。要以批处理模式（非交互式处理）运行一系列命令，请使用 batch 命令。OS10 自动提交批处理文件中的所有命令 — 您无需输入 commit 命令。

如果批处理文件中的命令失败，批处理操作将在该命令处停止。不执行剩余的命令。

- 创建批处理文件 — 例如 `b.cmd` — 通过在远程设备上输入一系列命令。

```
interface ethernet 1/1/1
no shutdown
no switchport
ip address 172.17.4.1/24
```

- 将命令文件复制到交换机上的主目录。

```
OS10# copy scp://os10user:os10passwd@10.11.222.1/home/os10/b.cmd home://b.cmd

OS10# dir home

Directory contents for folder: home
Date (modified) Size (bytes) Name

2017-02-15T19:25:35Z 77
b.cmd
...
```

- 在 EXEC 模式下使用 `batch /home/username/filename` 命令执行批处理文件。

```
OS10# batch /home/admin/b.cmd
Jun 26 18:29:12 OS10 dn_l3_core_services[723]: Node.1-Unit.1:PRI:notice [os10:trap],
%Dell EMC (OS10) %log-notice:IP_ADDRESS_ADD: IP Address add is successful.
IP 172.17.4.1/24 in VRF:default added successfully
```

- (可选) 验证正在运行的配置中的新命令。

```
OS10# show running-configuration interface ethernet 1/1/1
!
interface ethernet1/1/1
no shutdown
no switchport
ip address 172.17.4.1/24
```

## batch

使用非交互式处理在批处理文件中执行一系列命令。

|        |                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>batch /home/username/filename</code>                                                                                                                                                      |
| 参数     | <ul style="list-style-type: none"> <li>• <code>username</code> — 输入用于复制命令文件的用户名。</li> <li>• <code>filename</code> — 输入批处理命令文件的名称。</li> </ul>                                                    |
| 默认     | 未配置                                                                                                                                                                                             |
| 命令模式   | EXEC                                                                                                                                                                                            |
| 使用情况信息 | 使用此命令可在远程计算机上创建批处理命令文件。将命令文件复制到您的交换机上的主目录。此命令在批处理模式下执行命令。OS10 自动提交批处理文件中的所有命令；您无需输入 <code>commit</code> 命令。要显示存储在主目录中的文件，请输入 <code>dir home</code> 。要查看存储在主目录中的文件，请使用 <code>dir home</code> 命令。 |

### 示例

```
batch /home/admin/b.cmd
Jun 26 18:29:12 OS10 dn_l3_core_services[723]: Node.1-Unit.1:PRI:notice
[os10:trap],
%Dell EMC (OS10) %log-notice:IP_ADDRESS_ADD: IP Address add is
successful.
IP 172.17.4.1/24 in VRF:default added successfully
```

支持的版本 10.2.0E or later

## Linux shell 命令

在 Linux shell 中，您可以在批处理文件中运行单个命令或一系列命令。

## Linux 命令示例

- 使用 -c 选项可运行单个命令。

```
admin@OS10:/opt/dell/os10/bin$ clish -c "show version"

New user admin logged in at session 10
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2019 by Dell Inc. All Rights Reserved.
OS Version: 10.5.0.0
Build Version: 10.5.0.270
Build Time: 2019-07-29T23:35:01+0000
System Type: S4148F-ON
Architecture: x86_64
Up Time: 1 day 00:54:13

User admin logged out at session 10
admin@OS10:/opt/dell/os10/bin$
```

- 使用 -B 选项可运行包含一系列命令的批处理文件。
  - 创建批处理文件（例如，batch\_cfg.txt），其中包含一系列可执行命令。

```
configure terminal
router bgp 100
neighbor 100.1.1.1
remote-as 104
no shutdown
```

- 执行批处理文件：

```
admin@OS10:/opt/dell/os10/bin$ clish -B ~/batch_cfg.txt

New user admin logged in at session 15
```

- 验证批处理文件配置的 BGP 设置。

```
admin@OS10:/opt/dell/os10/bin$ clish -c "show running-configuration bgp"

New user admin logged in at session 16
!
router bgp 100
!
neighbor 100.1.1.1
remote-as 104
no shutdown
admin@OS10:/opt/dell/os10/bin$

User admin logged out at session 16
```

- 使用 ifconfig -a 命令可显示接口配置。此时将显示与前面板端口、端口通道和 VLAN 接口对应的 Linux 内核端口号。端口通道接口采用 boporthchannel-number 格式。VLAN 接口采用 brvlan-id 格式。在此示例中，e101-001-0 可标识端口 1/1/1。

```
admin@OS10:~# ifconfig -a
e101-001-0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet6 fe80::20c:29ff:feed:9ea9 prefixlen 64 scopeid 0x20<link>
 ether 00:0c:29:ed:9e:a9 txqueuelen 1000 (Ethernet)
 RX packets 266262 bytes 18763391 (17.8 MiB)
 RX errors 0 dropped 8293 overruns 0 frame 0
 TX packets 18754 bytes 3963136 (3.7 MiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

bo1: flags=5123<UP,BROADCAST,MASTER,MULTICAST> mtu 1500 >>> port-channel
 inet6 fe80::20c:29ff:feed:9f11 prefixlen 64 scopeid 0x20<link>
 ether 00:0c:29:ed:9f:11 txqueuelen 1000 (Ethernet)
 RX packets 0 bytes 0 (0.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 0 bytes 0 (0.0 B)
 TX errors 0 dropped 1 overruns 0 carrier 0 collisions 0
```

```
br1: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500 >>> vlan1
 inet6 fe80::20c:29ff:feed:9f12 prefixlen 64 scopeid 0x20<link>
 ether 00:0c:29:ed:9f:12 txqueuelen 1000 (Ethernet)
 RX packets 257964 bytes 12155776 (11.5 MiB)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 10287 bytes 900262 (879.1 KiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- 使用 `tcpdump -i kernel-port-number` 命令可捕获指定端口接口上接收到的所有数据包。按 **Ctrl+C** 以停止显示数据包输出。例如，要捕获在以太网 1/1/1 接口上收到的数据包，请输入：

```
admin@OS10:~# tcpdump -i e101-001-0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on e101-001-0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:35:07.538133 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id
8001.00:0c:29:74:3b:7e.8204, length 43
11:35:07.538467 STP 802.1w, Rapid STP, Flags [Learn, Forward, Agreement], bridge-id
8001.00:0c:29:74:3b:7e.8204, length 43
11:35:08.416291 LLDP, length 343: OS10
11:35:09.067621 IP6 fe80::20c:29ff:feed:9f12 > ff02::1:ffed:9ea9: ICMP6, neighbor
solicitation, who has fe80::20c:29ff:feed:9ea9, length 32
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
1 packet dropped by interface
root@OS10:~#
```

- 使用 SSH 会话远程运行 `show` 命令。仅支持 `show` 命令。

输入 `$ ssh admin@ip-address "show-command"` 命令，其中 `ip-address` 是交换机的 IP 地址。

```
$ ssh admin@10.11.98.39 "show version"
admin@10.11.98.39's password:
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2019 by Dell Inc. All Rights Reserved.
OS Version: 10.5.0.0
Build Version: 10.5.0.270
Build Time: 2019-07-29T23:35:01+0000
System Type: S4148F-ON
Architecture: x86_64
Up Time: 1 day 00:54:13
```

## 使用 OS9 命令

要使用 OS 9 命令语法输入配置命令，请在 CONFIGURATION 模式下使用 `feature config-os9-style` 命令并注销会话。如果不注销 OS10 会话，则使用 OS9 命令语法进行的配置更改将不会生效。再次登录后，您可以输入 OS9 命令，但只能在新会话中输入。

例如，要使用 OS9 命令配置以太网端口 1/1/15 上的 VLAN 11：

```
OS10(config)# feature config-os9-style
OS10(config)# interface vlan 11
OS10(conf-if-vl-11)# tagged ethernet 1/1/15

OS10(conf-if-vl-11)# show configuration
!
interface vlan11
 no shutdown
 tagged ethernet 1/1/15
```

要禁用 OS9 配置样式模式，请使用 `no feature config-os9-style` 命令。

# feature config-os9-style

启用命令行接口以接受 OS9 命令语法。

|        |                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------|
| 语法     | feature config-os9-style                                                                                                      |
| 参数     | 无                                                                                                                             |
| 默认     | 未配置                                                                                                                           |
| 命令模式   | CONFIGURATION                                                                                                                 |
| 使用情况信息 | 输入 feature config-os9-style 命令后，注销会话并重新登录。在下一个会话中，您可以在 OS9 语法中输入配置命令。命令的 no 版本将禁用此功能。                                         |
| 示例     | <pre>OS10(config)# feature config-os9-style OS10(config)# interface vlan 11 OS10(conf-if-vl-11)# tagged ethernet 1/1/15</pre> |
| 支持的版本  | 10.3.0E or later                                                                                                              |



## 零接触部署

通过零接触部署 (ZTD)，OS10 用户可以自动执行交换机部署：

- 升级现有的 OS10 映像。
- 执行 CLI 批处理文件以配置交换机。
- 执行 ZTD 后脚本以执行其他功能。

当您第一次使用出厂安装的 OS10 或从 ONIE 引导菜单执行 `ONIE: OS Install` 时，ZTD 默认已启用。当 OS10 在 ZTD 模式下启动交换机时，将在所有接口上启动 DHCP 客户端 — 管理和前面板端口。ZTD 将为未标记的 VLAN 流量配置所有接口。交换机从网络上运行的 DHCP 服务器获取 IP 地址和 ZTD 调配脚本 URL，以及下载并执行 ZTD 脚本。

**注：**零接触部署是指 OS10 功能，而不是 ONIE 自动调配。

- ZTD 仅在 IPv4 网络中受支持。DHCPv6 不支持 ZTD。
- 如果 PowerEdge MX 以太网交换机在 SmartFabric 模式下运行，则不支持 ZTD。
- 如果交换机使用前面板端口访问 DHCP 服务器，则端口接口必须处于非分解模式。
- 连接到运行 DHCP 服务器的网络的前面板端口中至少有一个必须处于非分解模式。
- 在 ZTD 模式中引导后，如果交换机不会在五分钟内收到带有选项 240 的 DHCP 服务器响应，它会自动退出 ZTD 模式。在这段时间内，您可以通过输入 `ztd cancel` 命令来中止 ZTD。命令可解锁交换机配置，以便您可以输入 OS10 CLI 命令。
- 启用 ZTD 后，系统将锁定命令行接口，因此您无法输入 OS10 配置命令。只有 `show` 命令可用。

根据调配脚本的内容，ZTD 将按以下顺序执行这些任务。虽然步骤 2、3 和 4 是可选的，但您必须为至少一个 `IMG_FILE`、`CLI_CONFIG_FILE` 和 `POST_SCRIPT_FILE` 变量中的至少一个输入有效的 URL 路径。例如，如果您只想配置交换机，请仅输入 `CLI_CONFIG_FILE` URL 值。在这种情况下，ZTD 不会升级 OS10 映像，并且不会执行 ZTD 后脚本。

1. ZTD 将下载 ZTD 调配脚本中指定的文件 — OS10 映像、CLI 配置批处理文件和 ZTD 后脚本。
  - 在调配脚本中，输入 `IMG_FILE`、`CLI_CONFIG_FILE` 和 `POST_SCRIPT_FILE` 变量的文件名，如 [ZTD 调配脚本](#) 中所示。
  - 如果未指定文件名，OS10 会立即退出 ZTD 并返回 CLI 配置模式。
  - 如果任何指定文件的下载失败，ZTD 将停止。OS10 将退出 ZTD 并解锁 CLI 配置模式。
2. 如果为 `IMG_FILE` 指定了 OS10 映像，ZTD 会将软件映像安装到待机分区中。如果未针对 `CLI_CONFIG_FILE` 指定配置文件，则 ZTD 将使用新的 OS10 映像重新加载交换机。
3. 如果您使用 `CLI_CONFIG_FILE` 的配置命令指定 OS10 CLI 批处理文件，则 ZTD 将执行 `PRE-CONFIG` 和 `POST-CONFIG` 部分中的命令。执行 `PRE-CONFIG` 命令后，交换机将重新加载新的 OS10 映像，然后执行 `POST-CONFIG` 命令。有关详细信息，请参阅 [ZTD CLI 批处理文件](#)。
4. 如果为 `POST_SCRIPT_FILE` 指定 ZTD 后脚本文件，则 ZTD 将执行脚本。有关详情，请参阅 [ZTD 后脚本](#)。

**注：**ZTD 进程将执行单个交换机重新引导。只有在安装了新的 OS10 映像或执行了 CLI 批处理文件的 `PRE-CONFIG` 部分的配置命令时，交换机才会重新引导。

### ZTD 前提条件

- 将 ZTD 调配脚本存储在支持 HTTP 连接的服务器上。
- 将 OS10 映像、CLI 批处理文件和 ZTD 后脚本存储在支持 HTTP、FTP、SFTP 或 TFTP 连接的文件服务器上。
- 配置 DHCP 服务器提供选项 240，以返回 ZTD 调配脚本的 URL。
- 在 ZTD 调配脚本中，输入 OS10 映像、CLI 批处理文件和/或 ZTD 后脚本的 URL 位置。至少输入一个 URL，否则 ZTD 会失败并退出 CLI 配置模式。

### ZTD 准则

- 您可以在同一台服务器上存储 ZTD 调配脚本、OS10 映像、CLI 批处理文件和 ZTD 后脚本，包括 DHCP 服务器。
- 在 `bash` 中写入 ZTD 调配脚本。
- 在 `bash` 或 `Python` 中写入 ZTD 后脚本。在脚本第一行输入 `#!/bin/bash` 或 `#!/usr/bin/python`。OS10 中的默认 `python` 解释器为 2.7。

仅使用常见的 Linux 命令（如 `curl`）和常见的 Python 语言构造。OS10 仅提供一组有限的 Linux 软件包和 Python 库。

- 默认情况下，ZTD 在自动调配的交换机结构（如 Isilon 后端、PowerEdge MX 和 VxRail）上处于禁用状态。

### 正在取消 ZTD

要退出 ZTD 模式并通过输入 CLI 命令手动配置交换机，请通过输入 `ztd cancel` 命令来停止 ZTD 过程。当 ZTD 处于等待状态时您只能输入 `ztd cancel`；即，在从 DHCP 服务器接收应答之前。否则，该命令将返回错误消息；例如：

```
OS10# ztd cancel
% Error: ZTD cancel failed. ZTD process already started and cannot be cancelled at this stage.
```

### 禁用 ZTD

要禁用 ZTD，请输入 `reload` 命令。交换机在 ZTD 禁用模式下重新引导。

### 重新启用 ZTD

要自动升级 OS10 和/或激活新的配置设置，请使用 `reload ztd` 命令重新引导交换机，以重新启用 ZTD。系统将提示您确认删除启动配置。

 **注：**要在不丢失启动配置的情况下升级 OS10，请在 ZTD 运行调配脚本之前备份启动配置。然后，使用备份启动配置来恢复先前的系统配置。

```
OS10# reload ztd
This action will remove startup-config [confirm yes/no]:
```

### 查看 ZTD 状态

```
OS10# show ztd-status

ZTD Status : disabled
ZTD State : completed
Protocol State : idle
Reason : ZTD process completed successfully at Mon Jul 16 19:31:57 2018

```

### ZTD 日志

ZTD 将生成有关其当前状态的日志消息。

```
[os10:notify], %Dell EMC (OS10) %ZTD-IN-PROGRESS: Zero Touch Deployment
applying post configurations.
```

ZTD 还会生成失败消息。

```
[os10:notify], %Dell EMC (OS10) %ZTD-FAILED: Zero Touch Deployment failed to
download the image.
```

### 配置锁定故障处理

当启用 ZTD 时，CLI 配置会被锁定。如果您输入 CLI 命令，将显示错误消息 `configuration is locked`。要配置交换机，请通过输入 `ztd cancel` 命令来禁用 ZTD。

```
OS10# configure terminal
% Error: ZTD is in progress(configuration is locked).
OS10# ztd cancel
```

## ZTD DHCP 服务器配置

对于 ZTD 操作，通过添加所需的 ZTD 选项，在网络中配置 DHCP 服务器；例如：

```
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;
option ztd-provision-url code 240 = text;

default-lease-time 600;
max-lease-time 7200;

subnet 50.0.0.0 netmask 255.255.0.0 {
 range 50.0.0.10 50.0.0.254;
```

```
option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
}

host ztd-leaf1 {
hardware ethernet 90:b1:1c:f4:a9:b1;
fixed-address 50.0.0.8;
option ztd-provision-url "http://50.0.0.1/ztd.sh";
}
```

## ZTD 调配脚本

创建 ZTD 脚本文件，将其存储在 HTTP 服务器上。在 DHCP 服务器上使用 DHCP 选项 240 (ztd-provision-url) 配置脚本的 URL。

ZTD 将下载并运行脚本来升级 OS10 映像、配置交换机并运行 ZTD 后脚本来执行其他功能。

- 在 bash 中写入 ZTD 调配脚本。输入 `#!/bin/bash` 作为脚本中的第一行。您可以将本部分中的示例脚本用作基础。
- 对于 `IMG_FILE`，输入要下载和升级交换机的 OS10 映像的 URL 路径。映像将写入到备用分区。
- 对于 `CLI_CONFIG_FILE`，输入要下载和运行的 CLI 批处理文件的 URL 路径。
- 对于 `POST_SCRIPT_FILE`，输入要运行的脚本的 URL 路径。
- ZTD 要求将所有 ZTD 脚本（调配、CLI 批处理文件和 ZTD 后的脚本）设置为 Unix 样式行格式。
- 在以下情况下，ZTD 会失败并退出到 CLI 配置模式：
  - 您不能为 `IMG_FILE`、`CLI_CONFIG_FILE` 和 `POST_SCRIPT_FILE` 变量至少指定一个有效的 URL。
  - `IMG_FILE`、`CLI_CONFIG_FILE` 和 `POST_SCRIPT_FILE` 条目均无效，如果指定，则无法下载文件。

对于 `IMG_FILE`、`CLI_CONFIG_FILE` 和 `POST_SCRIPT_FILE` 文件，您可以指定 HTTP、SCP、SFTP 或 TFTP URL。例如：

```
scp://userid:passwd@hostip/filepath
sftp://userid:passwd@hostip/filepath
```

### 示例

```
#!/bin/bash

#####
#
#
Example OS10 ZTD Provisioning Script
#
#
#####

UPDATE THE BELOW CONFIG VARIABLES ACCORDINGLY
ATLEAST ONE OF THEM SHOULD BE FILLED

IMG_FILE="http://50.0.0.1/OS10.bin"
CLI_CONFIG_FILE="http://50.0.0.1/cli_config"
POST_SCRIPT_FILE="http://50.0.0.1/no_post_script.py"

DO NOT MODIFY THE LINES BELOW

sudo os10_ztd_start.sh "$IMG_FILE" "$CLI_CONFIG_FILE" "$POST_SCRIPT_FILE"

END
```

## ZTD CLI 批处理文件

创建 CLI 批处理文件，以便 ZTD 下载并执行以配置交换机。ZTD CLI 批处理文件包含两个部分：PRE-CONFIG 和 POST-CONFIG。

输入 PRE-CONFIG 和 POST-CONFIG 行时，必须先输入哈希标签 (#)，后跟空格以及文本 PRE-CONFIG 或 POST-CONFIG。如果 PRE-CONFIG 部分没有命令，请不要在和 # PRE-CONFIG 和 # POST-CONFIG 之间留空线；例如：

```
PRE-CONFIG
POST-CONFIG
Hostname VxRail-fabric-LEAF-1
!
lldp enable
!
spanning-tree mode rstp
spanning-tree rstp priority 0
...
```

ZTD 将执行 PRE-CONFIG 命令，首先使用当前运行的 OS10 映像执行命令，而不是在调配脚本中指定的 OS10 映像。ZTD 将 PRE-CONFIG 设置保存到启动配置。

如果 PRE-CONFIG 命令存在，则在执行 POST-CONFIG 部分中的命令之前，ZTD 将重新加载交换机。在 PRE-CONFIG 部分中输入需要交换机重新加载的 OS10 配置命令，例如 switch-port-profile。如果 ZTD 安装新的 OS10 映像 (IMG\_FILE)，则会在重新加载后激活新映像。

ZTD 随后执行 POST-CONFIG 命令并将新设置保存在启动配置中。不执行其他交换机重新加载。使用在 show running-configuration 输出中显示的确切语法输入 POST\_CONFIG 命令。

### 示例

```
PRE-CONFIG
switch-port-profile 1/1 profile-2

POST-CONFIG
snmp-server community public ro
snmp-server contact NOC@dell.com
snmp-server location delltechworld
!
clock timezone GMT 0 0
!
hostname LEAF-1
!
ip domain-list networks.dell.com
ip name-server 8.8.8.8 1.1.1.1
!
ntp server 132.163.96.5 key 1 prefer
ntp server 129.6.15.32
!
!
logging server 10.22.0.99
```

## ZTD 后脚本

一般原则是，使用 ZTD 后脚本执行配置和操作交换机所需的任何其他功能。在 ZTD 调配脚本中，为 POST\_SCRIPT\_FILE 变量指定 ZTD 后脚本路径。您可以使用脚本来通知编排服务器 ZTD 配置已完成。然后，服务器可以在交换机上配置附加设置。

例如，在 ZTD 阶段，您只能配置管理一个 VLAN 和 IP 地址，然后允许 Ansible 编排服务器执行完整的交换机配置。下面是 ZTD 后脚本中包含的用于联系 Ansible 服务器的示例 curl 脚本：

```
/usr/bin/curl -H "Content-Type:application/json" -k -X POST
--data '{"host_config_key":"'7d07e79ebdc8f7c292e495daac0fe16b'"}'
-u admin:admin https://10.16.134.116/api/v2/job_templates/9/callback/
```

# ZTD 命令

## reload ztd

重新引导交换机并在重新加载后启用 ZTD。

|        |                                                                  |
|--------|------------------------------------------------------------------|
| 语法     | reload ztd                                                       |
| 参数     | 无                                                                |
| 默认     | ZTD 已启用。                                                         |
| 命令模式   | EXEC                                                             |
| 使用情况信息 | 使用 reload ztd 命令自动升级 OS10 和/或激活新的配置设置。重新加载 ZTD 时，系统会提示您确认删除启动配置。 |

示例

```
OS10# reload ztd
```

支持的版本 10.4.1.0 or later

## show ztd-status

显示当前的 ZTD 状态：已启用、已禁用或已取消。

|        |                                                                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show ztd-status                                                                                                                                                                                                               |
| 参数     | 无                                                                                                                                                                                                                             |
| 默认     | 无                                                                                                                                                                                                                             |
| 命令模式   | EXEC                                                                                                                                                                                                                          |
| 使用情况信息 | 无                                                                                                                                                                                                                             |
| 示例     | <pre>OS10# show ztd-status  ----- ZTD Status      : disabled ZTD State       : completed Protocol State  : idle Reason         : ZTD process completed successfully at Mon Jul 16                   19:31:57 2018 -----</pre> |

```
OS10# show ztd-status

ZTD Status : disabled
ZTD State : failed
Protocol State : idle
Reason : ZTD process failed to download post script file

```

- ZTD Status — 当前操作状态：已启用或已禁用。
- ZTD State — 当前 ZTD 状态：已初始化、正在进行、已成功完成、失败或已取消。
- Protocol State — 当前的 ZTD 协议状态：已初始化、处于空闲状态、等待启用或完成 ZTD 进程、等待 DHCP 后端回调、下载文件、安装映像、执行预配置或配置后的 CLI 命令，或者执行 ZTD 后脚本文件。
- Reason — ZTD 过程成功或失败的说明。

支持的版本 10.4.1.0 or later

## ztd cancel

正在进行时停止 ZTD。取消 ZTD 后，您可以输入 CLI 命令来配置交换机。

|               |                                                                                                                                                                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ztd cancel</code>                                                                                                                                               |
| <b>参数</b>     | 无                                                                                                                                                                     |
| <b>默认</b>     | ZTD 已启用。                                                                                                                                                              |
| <b>命令模式</b>   | EXEC                                                                                                                                                                  |
| <b>使用情况信息</b> | 启用 ZTD 时，命令行接口被锁定。您不能输入 OS10 配置命令。使用 <code>ztd cancel</code> 命令以取消 ZTD 过程并返回到 CLI 配置模式。当 ZTD 处于等待状态时您只能输入 <code>ztd cancel</code> ；即，在从 DHCP 服务器接收应答之前。否则，该命令将返回错误消息。 |
| <b>示例</b>     | <pre>OS10# ztd cancel</pre>                                                                                                                                           |
| <b>支持的版本</b>  | 10.4.1.0 or later                                                                                                                                                     |

# OS10 调配

OS10 支持自动交换机调配 — 配置和监视 — 使用：

- RESTCONF API — REST 类似的协议，使用 HTTPS 连接。使用 OS10 RESTCONF API 在 OS10 交换机上使用 JavaScript Object Notation (JSON) 结构化消息来设置配置参数。您可以使用任何编程语言来创建和发送 JSON 消息；请参阅 [RESTCONF API](#)。
- SmartFabric 服务结构自动化 — 在 Isilon 后端、PowerEdge MX 和 VxRail 全包式解决方案中自动配置 OS10 交换机；请参阅 [Dell EMC PowerEdge MX SmartFabric Services Configuration and Troubleshooting Guide](#) (Dell EMC PowerEdge MX SmartFabric 服务配置和故障处理指南)。
- Linux DevOps 生态系统 — OS10 提供对未经修改的 Linux (Debian) 操作系统的访问，使您可以从 Linux DevOps 生态系统获益。程序员可以在 Python 或 C/C++ 中写入应用程序，以在 OS10 交换机上执行。
- Ansible — 第三方 DevOps 工具。Ansible 是一种功能强大的开放源代码 IT 自动化引擎，提供了一种自动化应用程序软件和 IT 基础架构的简单方式。Ansible 允许您从这些环境中删除复杂性，并加速 DevOps 计划；请参阅[使用 Ansible](#) 和[示例：使用 Ansible 配置 OS10 交换机](#)。

## 使用 Ansible

Ansible 的工作原理是使用 SSH 连接到您的节点，并将小程序（称为 *Ansible 模块*）连接到他们。Ansible 包括数百个网络模块，以支持各种网络设备供应商。Ansible 使用一种简单、强大且无代理的自动化框架。有关详细信息，请转至[通过 Ansible 实现网络自动化](#)。

### Dell EMC Networking Ansible 解决方案

Dell EMC Networking Ansible 解决方案基于开放生态系统，使组织能够从行业标准网络应用程序、网络操作系统和网络硬件进行选择。使用 Ansible 调配和管理 Dell EMC 交换机，以实现快速的新设备部署和网络配置更改。通过 Ansible，您还可以根据 Dell EMC 和第三方操作系统的已知基准来跟踪正在运行的网络设备配置。

适用于 Dell EMC Networking 解决方案的 Ansible 模块允许组织通过提供以下优势来减少设计、调配和管理网络所需的时间和工作：

- 无代理 — 不需要新软件即可在交换机上安装。
- 功能强大 — 使用 Dell EMC Open Automation 框架的裸机交换机的端到端自动化配置。
- 易于使用 — Dell EMC Networking 模块随 Ansible 版本提供。无需安装任何内容。
- 妥善做法 — 使用 CLI 用户身份验证来集中和监视会话管理。

### Dell EMC Networking Ansible 模块

Ansible 附带大量可直接在远程主机上执行或通过行动手册执行的模块。模块的收集称为 *模块库*。模块是在命令行或行动手册任务中使用的离散代码单元。您还可以编写自己的模块。

从 Ansible 2.2 开始，Ansible 核心支持 Dell EMC Networking 模块。使用这些模块可管理并自动化运行 OS6、OS 9 和 OS10 的 Dell EMC 交换机。Dell EMC Networking 模块使用 CLI 和 SSH 传输在本地连接模式下执行。Ansible 核心集成了以下 OS10 模块：

- `dello10_command`：通过 Ansible 运行 `show` 命令或 EXEC 模式命令。例如，`show version` 命令输出显示交换机上运行的当前操作系统版本。
- `dello10_config`：通过 Ansible 运行 OS10 配置命令。
- `dello10_facts`：从 OS10 交换机检索正在运行的配置。

### Dell EMC Networking Ansible 角色

Ansible 角色允许您根据已知文件结构自动加载变量文件 (`vars_files`) 和任务。按角色对内容进行分组可使角色轻松与其他用户共享。这些角色针对 OS6、OS 9 和 OS10 进行了提取。从 <https://galaxy.ansible.com/> 下载 Dell EMC Ansible Networking 角色。

有关如何使用 Ansible 角色的信息和示例，请参阅 [Dell EMC Networking 存储库](#)。

### Ansible 清单文件

清单文件包含要运行命令的主机的列表。Ansible 可以同时多个主机上运行任务。

Ansible 行动手册将 `/etc/ansible/hosts` 用作默认的清单文件。要指定不同的清单文件，请在运行 Ansible 行动手册时使用 `-i filepath` 命令作为选项。



## Ansible 行动手册文件

使用行动手册，Ansible 可以配置多个设备。行动手册是以 YAML 格式表示的人工可读脚本。Ansible 行动手册将清单和行动手册文件作为参数进行操作，并将清单文件中的主机组映射到行动手册文件中列出的任务。

## Ansible 变量

在 Ansible 中，变量定义交换机配置。许多 Dell EMC 交换机都具有通用配置。通用配置变量存储在 `vars/main.yaml` 文件中；例如，`dns_server` 和 `ntp_server`。所有特定于主机的配置均存储在 `host_vars/host_name.yaml` 配置文件中；例如，交换机的主机名称。变量还用作行动手册定义、命令行参数和清单定义的一部分。

# 示例：使用 Ansible 配置 OS10 交换机

OS10 支持 Ansible 集成，以自动执行交换机配置。有关如何使用 Ansible 脚本和创建 Ansible 行动手册的详细信息，请转至：

- [Dell EMC Ansible 文档](#)
- [Dell EMC Networking 指南](#)并搜索 Ansible

您可以从 [Dell EMC Fabric Design Center](#) 为您提供的网络设计下载自动生成的 Ansible 配置文件。

## 准备工作

在使用 Ansible 配置 OS10 交换机之前，请在您的交换机上配置基本网络设置，例如为管理接口分配 IP 地址和默认网关：

1. 使用串行线缆将终端仿真程序连接到交换机上的控制台串行端口。串行端口设置为 115200、8 数据位和无奇偶校验。
2. 配置管理接口；例如：

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# no ip address dhcp
OS10(conf-if-ma-1/1/1)# ip address 10.1.1.10/24
OS10(conf-if-ma-1/1/1)# no shutdown
OS10(conf-if-ma-1/1/1)# exit
OS10(config)# management route 10.10.20.0/24 10.1.1.1
OS10(config)# end
```

## Ansible 配置示例

在此示例中，配置使用 Ansible 角色从 Ansible 控制器节点配置 OS10 交换机，并使用：

- 用户名和密码
- NTP 服务器
- 系统日志服务器

1. 在控制器节点上安装 Ansible。您可以在 [Ansible 安装指南](#) 页面找到最新版本的 Ansible。

您可以从安装了 Python 2（版本 2.7）或 Python 3（版本 3.5 或更高版本）的任何设备运行 Ansible，包括 Red Hat、Debian、Ubuntu、CentOS、OS X、任何 BSD 等。

在此示例中，Ansible 2.7.12 安装在 Ubuntu 16.04 虚拟机上。要在控制器节点上配置个人软件包归档 (PPA) 存储库并安装 Ansible，请运行以下命令：

```
sudo apt-get update
sudo apt-get install software-properties-common
sudo apt-add-repository --yes --update ppa:ansible/ansible
sudo apt-get install ansible
```

安装 Ansible 后，通过输入以下命令验证版本：

```
$ ansible --version
```

2. 从 [Ansible Galaxy](#) 网页下载并安装 Dell EMC Networking Ansible 角色；例如：

```
$ ansible-galaxy install dell-networking.dellos-users
$ ansible-galaxy install dell-networking.dellos-logging
$ ansible-galaxy install dell-networking.dellos-ntp
```

3. 创建用于存储清单和行动手册文件的目录；例如：

```
$ mkdir AnsibleOS10
```



4. 导航到目录并创建一个清单文件。

```
$ cd AnsibleOS10/
$ vim inventory.yaml
```

5. 为 inventory.yaml 文件中的每个交换机添加 IP 地址和操作系统。在一个命令行上输入每个交换机的命令。

```
OS10switch-1 ansible_host=192.168.1.203 ansible_network_os=dellos10
OS10switch-2 ansible_host=192.168.1.204 ansible_network_os=dellos10
```

6. 创建用于特定于交换机的变量文件的 host\_vars 目录。

```
$ mkdir host_vars
```

7. 创建主机变量文件；例如，host\_vars/OS10switch-1.yaml。然后定义主机名称和登录凭据：

```
$ vim host_vars/OS10switch-1.yaml
```

```
hostname: OS10switch-1

dellos_cfg_generate: True
build_dir: /home/user/config
ansible_ssh_user: admin
ansible_ssh_pass: admin

dellos_logging:
 logging:
 - ip: 1.1.1.1
 state: present

dellos_users:
 - username: u1
 password: test@2468
 role: sysadmin
 privilege: 0
 state: present

dellos_ntp:
 server:
 - ip: 3.3.3.3
```

```
$ vim host_vars/OS10switch-2.yaml
```

```
hostname: OS10switch-2

dellos_cfg_generate: True
build_dir: /home/user/config
ansible_ssh_user: admin
ansible_ssh_pass: admin

dellos_logging:
 logging:
 - ip: 1.1.1.1
 state: present

dellos_users:
 - username: u1
 password: Test@1347
 role: sysadmin
 privilege: 0
 state: present

dellos_ntp:
 server:
 - ip: 3.3.3.3
```

参数 dellos\_cfg\_generate 将创建应用到 Ansible 控制器节点上的远程交换机的配置命令的本地副本，并将命令保存在 build\_dir 路径中定义的目录中。

## 8. 创建行动手册文件。

```
$ vim playbook.yaml

- hosts: OS10switch-1 OS10switch-2
 connection: network_cli
 roles:
 - dell-networking.dellos-logging
 - dell-networking.dellos-users
 - dell-networking.dellos-ntp
```

要查看行动手册的语法，请将 `ansible-playbook` 命令与 `--syntax-check` 标记配合使用。此命令通过分析器运行行动手册文件，以确保其包含的文件、角色和其他参数不存在语法问题。

## 9. 运行行动手册文件。在 `ansible-playbook` 命令中，库存和行动手册文件是必填条目。播放回顾将显示调配会话的结果；例如：

```
$ ansible-playbook -i inventory.yaml playbook.yaml
...
...
...
PLAY RECAP

OS10switch-1: ok=7 changed=6 unreachable=0 failed=0
OS10switch-2: ok=7 changed=6 unreachable=0 failed=0
```

## SmartFabric 服务

SmartFabric 服务 (SFS) 是一种应用程序套件，可提供网络结构自动化和基于 API 的可编程性。网络连接结构包含物理资源，例如服务器、交换机、逻辑资源-网络、模板和上行链路。SFS 是一项 OS10 功能，具有不同的个性化设置，可在多个体系结构和环境中使用。

在 OS10 中，SFS 提供：

- 网络结构基础架构自动化包括查找交换机和服务器等设备，以及结构中所有交换机上的配置自动化。
- 使用 Api 的服务器、存储设备或超融合设备的工作负载自动化。
- 用于监控结构的单个界面。
- 使用 API 升级和更换交换机。

## SmartFabric 服务特性

Dell EMC 支持：

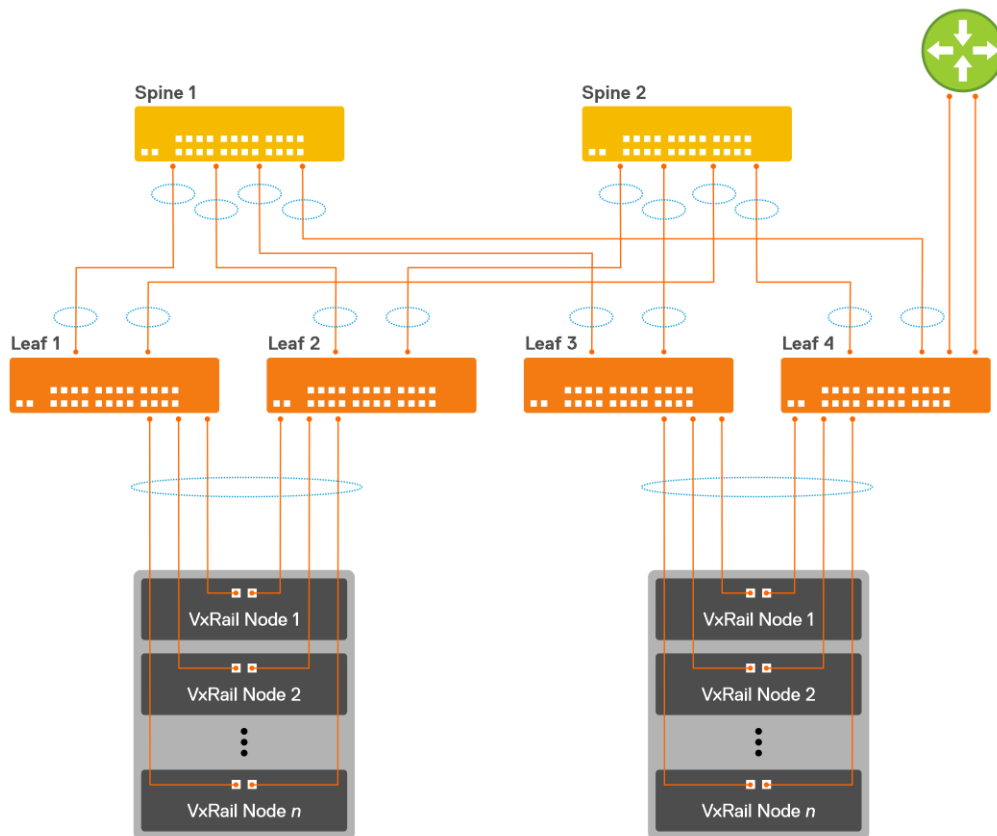
- [适用于分支和主干的 SmartFabric 服务](#)
- [适用于 PowerEdge MX 的 SmartFabric 服务](#)

## 适用于分支和主干的 SmartFabric 服务

在分支和主干体系结构中，SFS 可实现在第 3 层 (L3) 结构拓扑中连接的网络设备的查找、自动化和调配。

在分支和主干拓扑中，SFS：

- 为分支和主干配置分配所有必要的内部 IP 地址。
- 为所有相关的分支和主干交换机自动配置必要的 BGP。
- 启用基础和叠加的分支和主干。
- 提供以下 API 以用于工作负载编排：
  - 第 2 层 (L2) VLAN、L3 VLAN、L3 路由和 IP VXLAN 网络
  - 使用来自 L2 VLAN、L3 VLAN、L3 路由和 IP VXLAN 网络的网络的结构上行链路
  - 用于外部连接的 BGP 策略
  - 静态路由的路由策略
  - 静态和动态服务器模板绑定服务器查找到来自 L2 VLAN、L3 VLAN、L3 路由和 IP VXLAN 网络的网络。有关详细信息，请参阅[静态加入](#)和[动态加入](#)。

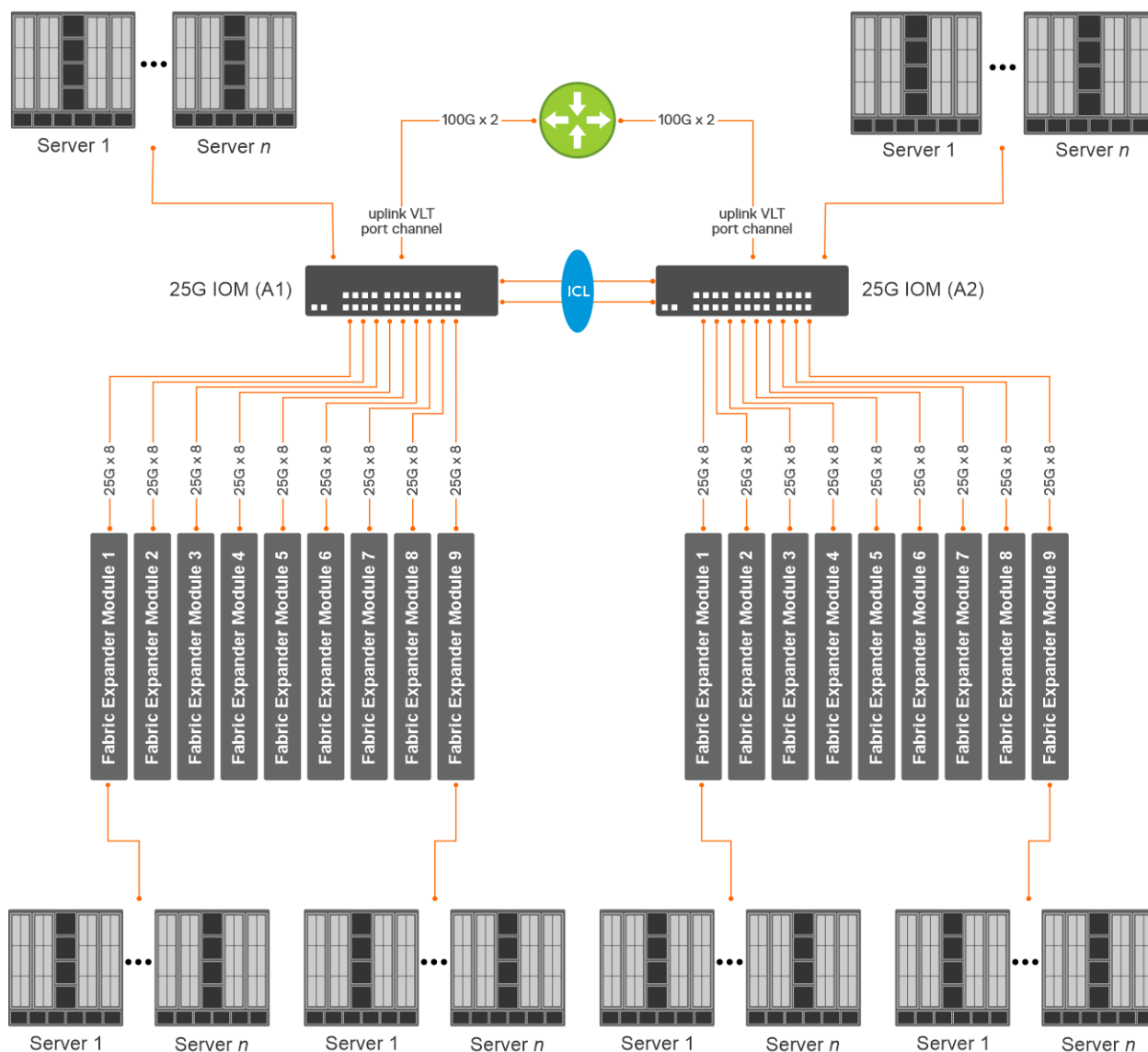


在分支和主干网络中使用的 SFS 在结构和超融合域基础架构（如 VxRail）之间创建完全集成的解决方案。

## 适用于 PowerEdge MX 的 SmartFabric 服务

SFS 是在以太网交换机 (IOM) 上运行的 Dell EMC Networking OS10 Enterprise Edition 的一项功能，专为 PowerEdge MX 7000 平台而设计。在 SFS 模式中，IOM 将作为简单的第二层输入输出聚合设备运行，从而实现与网络设备供应商的完全互操作性。

SFS 可发现在机箱中部署的 IOM，并向机箱中的管理模块提供 API，以监控 IOM 的状态。



在 MX 平台中，SFS 可提供：

- 用于监控和管理 IOM 上的生命周期操作的单一控制台。
- 用于管理 VLT 结构、数据上行链路、存储上行链路和整个结构的服务器模板的 API。

在 Dell EMC PowerEdge MX7000 基础架构中，MX9116n 结构引擎和 MX5108n 以太网交换机都支持 SFS。

有关适用于 PowerEdge MX 平台的 SmartFabric 的详细信息，请参阅 [POWEREDGE MX 以太网 I/O 模块](#)。

## 适用于分支和主干的 SmartFabric 服务

SFS 将查找并自动执行 OS10 交换机，以构建第 2 层或第 3 层网络结构。SFS 组成的 OS10 交换机群集属于域。域是可访问所有 OS10 节点的 LAN 段。所有 OS10 交换机必须位于同一域中，群集才能形成。SFS 提供 API，包括管理结构、节点清单、结构操作、服务器和加入存储设备。SFS 提供用于收集查找到的服务器和存储设备资源的 API。

### 前提条件

#### 支持的平台

- S4112F-ON、S4112T-ON
- S4128F-ON、S4128T-ON
- S4148F-ON、S4148FE-ON、S4148T-ON、S4148U-ON

- S4248FB-ON、S4248FBL-ON
- S5232F-ON、S5248F-ON、S5296F-ON
- S5212F-ON、S5224F-ON
- Z9100-ON
- Z9264F-ON

### OS10 支持的版本

OS10 10.5.0.0 版提供适用于分支和主干的 SFS。

### 适用于交换机的带外管理网络

带外 (OOB) 管理网络是一种隔离的网络，用于使用相应的管理接口远程管理服务器、交换机和存储设备。每个机架中安装的 S3048-ON 提供与管理网络之间的 1GE 连接。每个主干和分支交换机上的 OOB 管理端口均连接到 S3048-ON 交换机。

对于 S3048-ON 管理交换机，所有端口都在第 2 层和默认 VLAN 中。

## SmartFabric 服务组件

SFS 组件是网络连接结构、VLT 结构或机架、交换机和链路。

### 支持的网络拓扑

- 两个分支交换机和 VLT 对，无任何主干交换机
- 两个分支交换机和单一/多个主干交换机
- 多个分支交换机或 VLT 对和单一/多个主干交换机
- 分支（不带 VLT 互连 [VLTi]）和单个或多个主干交换机

### 网络结构

网络结构是包含群集中连接的交换机的结构。该结构包括分支交换机和主干交换机。启用 SFS 会自动在分支和主干网络中创建网络连接结构。网络结构为自动分配，具有结构 ID、名称和说明。

### VLT 结构

VLT 结构是为 VLT 对创建的结构。VLT 结构包括两个分支交换机，并且 SFS 在分支和主干环境中自动创建 VLT 结构。VLT 结构使用通用唯一标识符 (UUID) 结构 ID 进行自动分配。

 **注：**在 SFS 中，当创建了 VLT 结构时，会自动使用 VLT 对等节点的管理 IP 地址来设置 VLT 备份链路。如果在创建结构后更改了对等节点的管理 IP 地址，则会自动更新 VLT 备份链路。

### 交换机角色

交换机角色定义了分支和主干拓扑中部署的交换机的角色。在任何 Clos 拓扑中，主干和分支都是行业标准术语。角色包括：

#### 分支：

- 机架中连接到主干交换机的交换机。通过分支交换机连接到结构的服务器或终端设备。
- 交换机还可以使用 L3 路由、L3 VLAN、VXLAN 或通用网络连接到外部网络。

#### 主干：

- 连接多个分支交换机的交换机。
- 主干交换机可以通过 L3 路由或 L3 VLAN 网络连接到外部网络。

## 结构链路

结构链路在网络结构中的交换机之间建立连接。类型包括：

- 交换机间链路 (ISL)：分支与主干之间的链路。  
具有相同连接的所有并行链路都会分为一组以形成 LAG 接口。此链路称为 ISL。
- 群集间链路 (ICL) 或 VLTi：同一机架中的两个分支交换机之间的链路。

## 用于构建结构的内部网络

从 4000 到 4094 范围内将 VLAN 保留用于 SFS 内部使用。

- **群集控制 VLAN:** VLAN 4000 用于内部群集用途。当 SFS 检测到 ISL 时，它会将 ISL 分配给此 VLAN 的已标记成员。此 VLAN 将启用 PVST 并在其中一个主干交换机上强制执行根桥。
- **IP-对等 VLAN:** VLAN 范围是从 4001 到 4079，并用于 IP 对等。当 SFS 检测到分支或主干交换机上的 ISL 连接时，它会将 ISL 分配给此 VLAN 的未标记成员。此 VLAN 使用保留范围内的 IP 地址。为此 IP 启动了 eBGP 会话。
- **未全局标记的 VXLAN VLAN:** VLAN 4080。VXLAN 要求为未标记的端口限定 VLAN（端口、VLAN）对在全局范围内分配一个 VLAN。
- **内部 BGP (iBGP) ICL VLAN:** VLAN 4090。此 VLAN 在 ICL 上创建。此 VLAN 使用保留范围内的 IP 地址。为此 IP 启动了 iBGP 会话。

## SmartFabric 服务逻辑实体

为 SmartFabric 服务定义了三种类型的逻辑实体：网络、上行链路和服务器配置文件。

### 网络

网络是已填充一次的 SmartFabric 服务模板，随后可以与服务器、上行链路或接口相关联。

在 SmartFabric 服务环境中，您可以定义以下四种类型的网络：

- 一般用途网络
- VXLAN 网络
- L3 VLAN 网络。
- L3 路由网络

#### 一般用途网络

一般用途的网络是 VxRail 中的 L2 VXLAN 网络和 L3 结构中的 L2 VLAN 网络。

对于 L3 结构，SmartFabric 服务会自动创建与网络对应的虚拟网络。该虚拟网络与网络之间具有一对一的映射，这意味着对于每个 VLAN，存在具有与 VLAN ID 相同的 VNI 的虚拟网络。

#### VXLAN 网络

VXLAN 网络通基础 L3 连接的网络扩展了 L2 连接。

VXLAN 网络到接口的关联会创建绑定并将此接口关联到 VXLAN 桥。

您需要创建虚拟网络模板和网络模板，并将虚拟网络模板与网络模板相关联。

- 虚拟网络模板可定义 VNET ID。
- 网络模板可定义 VLAN ID。

除了 L2 VXLAN 网络中指定的任何内容，对于 L3 VXLAN，请指定：

- IP 地址列表。每个分支的一个 IP 地址。
- ANY-CAST IP 地址

L3 VXLAN 网络支持非对称 IRB。

#### L3 VLAN 网络

L3 VLAN 网络用于 L3 VLAN 基础。

指定：

- VLAN ID
- 要分配给 VLT 对的 IP 地址对。
- VIP 的 VRRP 网关 IP 地址

#### L3 路由网络

L3 路由网络用于在单个接口上分配 IP 地址。指定 IP 地址。

将此网络连接到具有单一接口的任何上行链路。此网络只能连接到单个实体。

## 上行链路

上行链路是一组连接到客户网络的端口。

此上行链路实体包含一组严格的网络特性。

### 分支节点的第 2 层上行链路

第 2 层上行链路是属于应用第 2 层网络的相同 VLT 对等节点的一组用户选择的端口。SFS 将为这些连接的端口创建 VLT LAG。如果端口来自单个设备，则 VLT LAG 是单臂 VLT LAG。如果这些端口存在于多个节点上，则会在这些端口上形成 VLT 或多机箱 LAG。此 LAG 可作为 VXLAN 第二层网络的接入点进行。

### 第 3 层上行链路

第 3 层上行链路可在分支或主干节点上配置。

#### 使用第 3 层 VLAN 网络

第 3 层 VLAN 网络包含 IP 地址和网关 IP 地址的列表。此外，还可以指定 DHCP 中继地址。第 3 层 VLAN 网络可以通过分支或主干节点进行配置。第 3 层 VLAN 网络可连接到上行链路。每个 VLTi 上行链路接口都包含从第 3 层 VLAN 网络上配置的 IP 地址列表分配的 IP 地址。

#### 使用第 3 层路由网络

第 3 层路由网络包含 IP 地址和网关 IP 地址的列表。此外，还可以指定 DHCP 中继地址。可在分支或主干节点上配置第 3 层路由网络。第 3 层路由网络可以连接到上行链路。每个上行链路接口都包含从第 3 层路由网络上配置的 IP 地址列表分配的 IP 地址。LACP 端口通道不能作为这些上行链路的远程端。如果指定了网关 IP，则 VRRP 已启用，并且交换机将此 IP 地址配置为网关 IP 地址。

#### 使用第 3 层 VXLAN 网络

第 3 层 VXLAN 网络是 VXLAN 类型的网络，其中包含 IP 地址列表和任意广播 IP 地址。此外，还可以指定 DHCP 中继地址。第 3 层 VXLAN 网络可以通过分支节点进行配置。第 3 层 VXLAN 网络可以连接到上行链路。每个 VLTi 上行链路接口都包含从第 3 层 VXLAN 网络上配置的 IP 地址列表分配的 IP 地址。

#### 静态路由策略

静态路由是包含网络前缀和下一跳 IP 地址的路由策略模板。此策略可连接到结构中的一个或多个节点。当此策略连接到节点时，将在节点中配置具有指定前缀和下一跳 IP 地址的静态路由。

#### eBGP 对等策略

EBGP 对等策略是包含 BGP 远程地址和远程 AS 编号的路由策略模板。远程地址可以是接口地址或环回地址。此策略可连接到连接结构中的一个或多个节点。当此策略连接到节点时，BGP 会话将与交换机关联。

## 上行链路绑定选项

以下是可用于实现上行链路绑定的选项：

- LACP
- 静态绑定
- 未配置绑定类型
- 生成树注意事项

#### LACP

在 LACP 上行链路绑定中，SmartFabric 服务等待来自远程设备的 LACP PDU，以配置上行链路的 LACP LAG。连接到上行链路的网络与创建的 LACP LAG 相关联。

#### 静态绑定

在静态绑定中，SmartFabric 服务配置上行链路的静态 LAG，并且上行链路上连接的网络与创建的 LAG 相关联。

#### 未配置绑定类型

如果未配置绑定类型，网络将连接到上行链路物理接口。此配置由第 3 层路由上行链路专用。

## 生成树注意事项

对于 VXLAN 网络，网络必须是回路。SFS 不允许在多个上行链路上配置相同的网络，以确保不会意外创建任何循环。

对于第 3 层 VLAN 的网络，默认情况下，RPVST+ 在上行链路接口上处于启用状态。建议不要更改生成树类型或将其禁用。

## 集成设备的动态加入

SFS 将根据 LLDP PDU 中通过连接的端口发送的特定自定义发起程序 TLV，查找和加入以下供应商终端主机设备。



- iDRAC
- Isilon
- VxRail
- Trident
- VxFlex

当在连接的端口中检测到新的服务器接口时，将应用新的配置。

## 静态加入的服务器

- 在连接的端口上禁用了 STP。
- 绑定可以是自动或 LACP。
- 所有类型的网络均可连接到这些端口。

## 非集成设备的静态加入

SmartFabric 服务支持在分配的端口上启用服务器，而不是基于 LLDP 的查找机制。SFS 使您可以提供启用接口的服务器配置文件和服务器接口配置文件的扩展。

- 静态启用服务器支持所有现有的绑定模式。
- 在可能的情况下，在这些端口上启用 STP。由于 VXLAN 不支持访问端口上的 STP，因此这不适用于 L3 结构。在第 3 层 VLAN 网络上 RPVST+ 已启用。对于 VXLAN 类型的网络，无法配置 STP；网络拓扑必须保持环路可用。
- 所有现有网络类型都允许在静态加入的服务器上启用。
- 由于加入是静态的，因此在移动服务器时，不支持将配置与服务器一起移动。
- 静态加入的服务器的端口角色为 EndHost 或 GenericEndHost。
- 服务器配置文件或服务器接口配置文件已删除时，所有受影响的接口都将进入默认配置。

## 在交换机上启用 SmartFabric 服务

要在分支和主干拓扑中创建 L3 网络结构，请在所有交换机中启用 SFS。启用 SFS 后，将使用默认结构设置自动创建网络连接结构。

要启用 SFS：

- 指定交换机的角色：分支或主干
- 为分支交换机配置 VLT 接口。

要从 OS10 CLI 启用交换机中的 SmartFabric 服务，请使用 `smartfabric l3fabric enable` 命令。有关详细信息，请参阅 [smartfabric l3fabric enable](#)。在交换机上启用 SFS 并设置角色后，系统会提示确认在 SFS 模式下重新加载和引导。要应用更改，请在 SFS 模式下键入 `yes` 并重新加载交换机以进行确认。

**主干：**

```
OS10(config)# smartfabric l3fabric enable role SPINE
Reboot to change the personality? [yes/no]: yes
```

**分支：**

```
OS10(config)# smartfabric l3fabric enable role LEAF vlti
ethernet 1/1/4-1/1/5
Reboot to change the personality? [yes/no]: yes
```

`no smartfabric l3fabric` 命令将禁用 L3 结构特性。在交换机中禁用 L3 结构后，系统会提示确认。

```
OS10(config)# no smartfabric l3fabric
Reboot to change the personality? [yes/no]: yes
```

您还可以通过 SFS 图形用户界面 (GUI) 启用 SFS。要使用 GUI 启用 SmartFabric 服务，请参阅[使用 GUI 启用 SmartFabric 服务](#)。

## 使用 GUI 启用 SmartFabric 服务

您可以使用 GUI 启用 SFS。要实现这一点，请：

1. 使用 OS10 CLI 在交换机上启用 RESTCONF API。

要启用 RESTCONF API，请在 CONFIGURATION 模式下使用 `rest api restconf` 命令。有关详细信息，请参阅[配置 RESTCONF API](#)。

2. 使用页面右上方显示的**编辑**选项在交换机上启用 SFS。
3. 输入交换机的角色，然后单击**确定**以启用 SFS。

 **注：**在交换机中启用 SFS 后，系统 will 重新添加端口配置。

## SmartFabric 服务图形用户界面

OS10 支持 SmartFabric 服务 GUI 以在 L3 分支和主干拓扑中设置初始 SFS 配置。SFS GUI 重点关注归零部署操作和第 3 层结构中的交换机管理。使用 SAN GUI，您可以：

1. 在交换机中启用 SFS。有关详细信息，请参阅[使用 GUI 启用 SFS](#)。
2. 使用向导在 SFS 模式下设置初始部署配置：
  - 重命名网络结构、VLT 结构或机架以及交换机。
  - 分解端口
  - 创建 L2 或 L3 上行链路。
  - 服务器板载
  - 创建跳转主机。

有关详细信息，请参阅[配置 SFS 初始设置](#)。

## 支持的平台

以下平台支持 SFS GUI：

- S4112F-ON、S4112T-ON
- S4128F-ON、S4128T-ON
- S4148F-ON、S4148FE-ON、S4148T-ON、S4148U-ON
- S5212F-ON、S5224F-ON
- S5232F-ON、S5248F-ON、S5296F-ON
- Z9264F-ON

## 启动 SmartFabric 服务 GUI

您可以使用最新版本的浏览器访问 SFS GUI，例如：

- Google Chrome
- Mozilla Firefox
- Microsoft Edge

从 SmartFabric 主交换机启动 SFS GUI，以完成 SFS 初始设置。您可以使用分支-主干拓扑中部署的主交换机的 IP 地址来访问 HTTPS 中的 SFS GUI。

## 识别 SmartFabric 主交换机

当您在所有分支交换机的分支-主干拓扑中创建第 3 层结构时，将选择一个叶交换机作为 SmartFabric 主机，而剩余的分支交换机为非主交换机。

要获取第 3 层结构中主交换机的 IP 地址，请使用 `show smartfabric cluster` 命令。有关详细信息，请参阅[显示 SmartFabric 群集](#)。

**注：**您还可以使用 `show smartfabric cluster member` 命令从任何非主设备获取主 IP 地址。有关详细信息，请参阅[显示 SmartFabric 群集成员](#)。

## 登录 SmartFabric 服务 GUI

登录页面会提示输入用户名和密码。要登录到 GUI，请使用从控制台或网络连接中创建的用于访问 OS10 交换机的凭据。登录到交换机控制台的默认用户名和密码是 `admin`。您也可以使用任何用户配置的帐户作为凭据。

**注：**OS10 使用 OS10 RESTCONF API 中的基于标记的身份验证来验证用户名和密码。

令牌时间到期后，会话将自动注销。系统将显示以下消息： `You have been logged out as the configured token validity time got expired. Please login again.`

**注：**默认令牌超时值为 120 分钟。

要注销，请单击 **Home** 右上角的 **Logout**。

**注：**您还可以通过 GUI 获取主交换机 IP 的详细信息。使用配置的 IP 地址从任何非主交换机启动 GUI。此页面显示交换机的结构模式和主节点的 IP 地址。单击主 IP 地址旁边的链接图标以启动 SFS GUI。

## 配置 SmartFabric 服务初始设置

登录到 SFS GUI 后，将显示 **Home** 页面。

主页提供以下选项：

- 更新默认结构、交换机名称和说明
  - 为外部网络连接创建上行链路
  - 分解交换机端口
  - 配置跳转主机
  - 更新网络配置
  - 将服务器板载到结构
  - 编辑默认结构设置
- 分支和主干拓扑视图 — 显示启用 SFS 之后创建的 L3 结构设计。

拓扑视图显示带有主机名称的交换机图标，以及每个节点下的服务编号信息和交换机之间的链路连接。将鼠标悬停在连接结构上可查看有关分支和主干交换机和链路连接的详细信息。

## 更新默认结构、交换机名称和描述向导

SFS 会自动为网络连接结构、机架和交换机分配唯一名称。但是，这些名称并不便于理解。使用此向导，您可以更改网络结构、机架和交换机的名称和说明。要实现这一点，请：

- 启动 **Update Default Fabric, Switch Names and Descriptions** 向导。
- 更改网络结构的名称和说明，然后单击 **NEXT**。
- 更改机架或 VLT 结构的名称和说明，然后单击 **NEXT**。
- 更改交换机的名称和说明，然后单击 **FINISH**。

## 为外部网络连接向导创建上行链路

上行链路允许网络连接结构与外部网络进行通信。SFS 支持第 2 层和第 3 层上行链路。使用此向导，您可以执行以下操作：

- 创建第 2 层或第 3 层上行链路。
- 将端口分配给上行链路。
- 将网络或路由配置文件与所创建的上行链路相关联。

**注：**在创建上行链路之前，确保外部网络配置了 L2 或 L3 配置。

从 SFS GUI **Uplinks** 选项卡中，您可以查看结构中所有上行链路的列表。此页面显示已配置的上行链路的名称、说明、介质类型、上行链路和 LAG 信息。您还可以从此选项卡中删除上行链路。要删除上行链路配置，请从列表中选择一行，然后单击 **DELETE**。

**注：**删除上行链路时，与上行链路关联的网口和路由配置文件不会被删除。

**注：**Uplinks 页面不显示与上行链路关联的网口和路由配置文件。要查看网口信息，请使用交换机中的 `show smartfabric uplinks` 命令。

## 配置第二层上行链路

要连接到另一个 L2 网络，请创建 L2 上行链路并将网络与上行链路关联。要实现这一点，请：

1. 启动 **Create Uplink for External Network Connectivity** 向导。
2. 选择 **Uplink Connectivity** 作为 **Layer 2**。
  - 注：**仅在分支交换机上创建 L2 上行链路。
3. 通过提供名称和说明，然后单击 **NEXT**，创建 L2 上行链路。
4. 从分支交换机中选择一个机架和一个或多个接口，以关联到上行链路。
  - 注：**该列表仅显示可用接口，包括分解接口。
5. 根据外部网络中的配置设置选择静态或动态 LAG，然后单击 **NEXT**。
  - 注：**要在分支交换机上形成 LAG，请选择速度相同的一个或多个接口。
6. 将网络与所选接口关联：
  - 添加多个标记的网络或单个未标记的网络，或两者。
  - 从显示的列表中添加网络，或使用 **ADD NETWORK** 创建通用网络。
7. 选择 **Yes** 或 **No** 以在此上行链路上集成通过 vCenter 在结构中自动创建的网络。
8. 单击 **FINISH**。

从 SFS GUI **Network Profiles** 选项卡中，您可以查看在 SFS 中配置的所有网络和虚拟网络的列表。此页面包含 **NETWORKS** 和 **VIRTUAL NETWORKS** 选项卡，显示相应网络配置文件的详细信息，包括网络名称、说明、网络类型。您还可以从此选项卡中删除网络配置文件。要删除网络配置文件，请从列表中选择网络配置文件，然后单击 **DELETE**。

## 配置第 3 层 VLAN 上行链路

对于 L3 VLAN 基础连接，创建 L3 VLAN 上行链路，并将网络和路由策略与上行链路关联。要实现这一点，请：

1. 启动 **Create Uplink for External Network Connectivity** 向导。
  2. 选择 **Uplink Connectivity** 作为 **Layer 3**。
  3. 选择 **Network type** 为 **L3 VLAN**。
  4. 通过提供名称和说明，然后单击 **NEXT**，创建 L3 VLAN 上行链路。
    - 注：**可以在分支和主干交换机上创建 L3 上行链路。
  5. 将主干或分支交换机的接口与 L3 上行链路关联。
    - **主干** — 选择要与上行链路关联的一个主干交换机和一个接口或多个主干交换机的接口。
    - **分支** — 从机架中选择分支交换机，以及要与上行链路关联的分支交换机的接口或多个接口。
  6. 根据外部网络中的配置设置选择静态或动态 LAG，然后单击 **Next**。
  7. 通过提供名称、说明和 VLAN ID 并将其与所选接口关联来创建 L3 VLAN 网络。
  8. 选择网络是已标记还是未标记的网络。
  9. 输入网络的 IP 地址。您可以使用 + 符号添加更多 IP 地址。
  10. 根据外部网络连接设置定义要与上行链路关联的路由策略。
    - **静态路由** — 包含网络前缀和下一跳 IP 地址的路由策略模板。
    - **eBGP** — 包含 BGP 对等 IP 地址和远程 AS 编号的路由策略模板。
- 注：**只有在将网口与上行链路或服务器配置文件关联后，网口配置才会反映在交换机中。

从 SFS GUI **Routing Profiles** 选项卡中，您可以查看在 SFS 中配置的所有路由配置文件的列表。该页面具有两个选项卡：

- **ROUTE PROFILE** — 显示详细的路由配置文件信息。

- **PROFILE SWITCH MAPPING** — 显示映射到交换机的配置文件的列表。

您还可以从相应的选项卡中删除路由配置文件和配置文件交换机映射。从选项卡中选择一个配置文件，然后单击 **DELETE**。

## 配置第 3 层路由上行链路

您可以创建 L3 路由上行链路并将网络与上行链路关联。要实现这一点，请：

1. 启动 **Create Uplink for External Network Connectivity** 向导。
2. 选择 **Uplink Ports Type** 作为 **Layer 3**。
3. 选择 **Network Type** 作为 **L3 Routed**。
4. 通过提供名称和说明，然后单击 **NEXT**，创建 L3 路由上行链路。
5. 将一个接口从主干或分支交换机与 L3 路由上行链路关联。
  - **主干** — 从主干选择一个主干交换机和一个接口，以与上行链路关联。
  - **分支** — 从机架选择分支交换机，并从分支交换机选择一个接口以与上行链路关联。

**注：**您仅可从主干或分支交换机中为 L3 路由上行链路选择一个接口。

6. 通过提供名称、说明、接口 IP 地址和前缀长度，创建要关联的 L3 路由网络。
7. 根据外部网络连接设置定义要与上行链路关联的路由策略。
  - **静态路由** — 包含网络前缀和下一跳 IP 地址的路由策略模板。
  - **eBGP** — 包含 BGP 对等 IP 地址和远程 AS 编号的路由策略模板。

**注：**您不能将 L3 路由网与多个上行口或服务器配置文件相关。

您可以从**路由配置文件**选项卡中查看和删除路由配置文件。

## 分解交换机端口向导

分解交换机的物理以太网端口或端口组的速度，以连接到外部设备或跳线主机。

此向导允许您分解以太网端口。要实现这一点，请：

1. 启动**分解交换机端口**向导。
2. 从列表中选择机架。
3. 在机架中选择分支交换机。
4. 选择要分解的分支交换机的端口组或物理以太网端口。
5. 从列表中选择相应的分解选项，然后单击**确定**。

**注：**在主干中支持分解自配置。

## 配置跳转主机向导

跳转主机是外部设备（例如笔记本电脑）可以连接到的指定端口。您只能将分支交换机中的一个端口配置为跳转端口，以便外部设备连接到 L3 结构。您可以选择不属于上行链路和 ICL 的任何可用端口，以及在 SmartFabric 部署中连接到服务器的端口。

此向导允许您配置跳转主机。要实现这一点，请：

1. 启动**配置跳转主机**向导。
2. 为跳转主机分配易于识别的名称和说明。
3. 从机架中选择分支交换机。
4. 选择分支交换机的接口作为跳转主机。
5. 将未标记的网络与跳转主机关联，然后单击**确定**。

您可以在 SFS GUI **上行链路**选项卡中查看已配置的跳转主机。您还可以从此选项卡中删除任何创建的跳转主机。从列表中选择跳转主机，然后单击**删除**。

## 更新网络配置向导

在使用 **Update Network Configuration** 向导完成初始连接结构设置后，您可以编辑在结构中的上行链路和服务器配置文件上应用的网络配置。要实现这一点，请：

1. 启动 **Update Network Configuration** 向导。
2. 选择要编辑的 VLAN 或虚拟网络。
3. 更新接口、网关和 DHCP 帮助程序 IP 地址的相关详细信息，然后单击 **OK**。

## 将服务器板载连接到结构向导

要板载连接服务器，请选择服务器配置文件，关联一个接口以板载连接服务器，并关联一个或多个网络。要实现这一点，请：

1. 启动 **Onboard a Server onto the Fabric** 向导。
2. 从列表中选择服务器配置文件，或使用 **ADD SERVER PROFILE** 为接口创建配置文件。  
**ADD SERVER PROFILE** — 通过提供服务器配置文件类型、名称和绑定技术来创建服务器配置文件。
3. 如果已查找到服务器接口，请从列表选择一个接口 ID，或者输入一个 ID，然后单击 **NEXT**。
4. 将分支交换机的接口与服务器上的板载接口关联：
  - a. 选择 NIC 绑定。
  - b. 选择是否为静态加入。如果是静态的，则分配分支交换机的接口，然后单击 **NEXT**。
5. 从列表中将网络与服务器接口配置文件关联，或根据网络连接创建网络或虚拟网络。
  - **ADD NETWORK** — 用于创建通用、I3 VLAN、VXLAN 和 L3 路由网络的模板。
  - **ADD VIRTUAL NETWORK** — 用于创建 VXLAN 网络的模板。

从 SFS GUI **Server Profiles** 选项卡中，您可以查看在 SFS 中配置的所有服务器配置文件的列表。此页面显示服务器配置文件的详细信息，例如绑定技术、服务器发现和加入状态等。您还可以从此选项卡中删除服务器配置文件。从列表选择一个服务器配置文件，然后单击 **DELETE**。

从 SFS GUI **Network Profiles** 选项卡中，您可以查看在 SFS 中配置的所有网络的列表。此页面显示网络的详细信息，例如名称、说明、QoS 优先级和网络类型。您还可以从此选项卡中删除网络。从列表选择一个网络，然后单击 **DELETE**。

## 编辑默认结构设置向导

您可以编辑在启用 SFS 时自动生成的默认结构设置。

1. 启动 **Edit Default Fabric Settings** 向导。
  2. 根据要求更改以下设置的值：
    - 分支 ASN
    - 主干 ASN
    - 专用子网前缀
    - 专用前缀长度
    - 全局子网前缀
    - 全局子网长度
    - 客户端控制 VLAN
    - 客户端管理 VLAN
  3. 单击 **OK** (确定)。
-  **注：**单击 **OK** 后，将重新加载网络结构中的所有交换机以应用结构设置更改。

## 结构操作和生命周期管理

Dell EMC Open Manage Network Integration (OMNI) 是基于高效 REST API 的插件，已与 VMware vCenter 集成。通过此插件，vCenter 可以在 VxRail HCI 堆栈上轻松部署和管理虚拟机和物理基础的大型虚拟网络。使用 OMNI，您可以执行一次超融合结构的两项操作和管理。

您可以使用 OMNI 执行常见生命周期操作。

- 升级网络结构中的 OS10 软件
- 更换结构中的交换机

有关 OMNI 的详细信息，请参阅 *VMware Integration for VxRail Fabric Automation SmartFabric User Guide*。



# SmartFabric 命令

您可以从 OS10 CLI `show` 输入 SmartFabric 服务命令以查看 SmartFabric 配置信息，包括：

- SmartFabric 群集角色（主或备份）和群集成员信息
- SmartFabric 个人设置
- SmartFabric 状态、节点和网络配置文件
- SmartFabric 上行链路

## smartfabric l3fabric enable

在交换机上启用 SmartFabric 服务，并在基于 Clos 的主干和分支体系结构中创建网络结构。

|            |                                                                                                                                                                                                                                                                 |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法         | <code>smartfabric l3fabric enable role {LEAF [vlti ethernet node/slot/port]   SPINE}</code>                                                                                                                                                                     |
| 参数         | <p><code>role</code> — 在第 3 层结构中输入交换机的角色：</p> <ul style="list-style-type: none"><li>• <code>LEAF</code> — 对于架顶式交换机指定角色作为 <code>LEAF</code>，并指定互连分支交换机的 VLTi 端口。</li><li>• <code>SPINE</code> — 为连接分支交换机的交换机指定 <code>SPINE</code> 角色。</li></ul>                  |
| 默认         | 无                                                                                                                                                                                                                                                               |
| 命令模式       | CONFIGURATION                                                                                                                                                                                                                                                   |
| 使用情况信息     | <p>启用 L3 结构并设置角色后，将使用默认结构设置来自动创建网络结构。执行该命令后，系统会提示您确认并使用更改的个性化设置重新引导。如果键入 <code>Yes</code>，交换机将重新加载配置的 SmartFabric 特性。有关支持的平台，请参阅<a href="#">适用于分支和主干的 SmartFabric 服务</a>。</p> <p><code>no smartfabric l3fabric</code> 命令将禁用 L3 结构特性。在交换机中禁用 L3 结构后，系统会提示确认。</p> |
| 示例（主干）     | <pre>OS10(config)# smartfabric l3fabric enable role SPINE  Reboot to change the personality? [yes/no]: yes</pre>                                                                                                                                                |
| 示例（分支）     | <pre>OS10(config)# smartfabric l3fabric enable role LEAF vlti ethernet 1/1/4-1/1/5  Reboot to change the personality? [yes/no]: yes</pre>                                                                                                                       |
| 示例（禁用 SFS） | <pre>OS10(config)# no smartfabric l3fabric  Reboot to change the personality? [yes/no]: yes</pre>                                                                                                                                                               |
| 支持的版本      | 10.5.0.3 or later                                                                                                                                                                                                                                               |

## show smartfabric cluster

显示在其中执行命令的交换机或 IOM 的基本群集信息。

|        |                                                                                  |
|--------|----------------------------------------------------------------------------------|
| 语法     | <code>show smartfabric cluster</code>                                            |
| 参数     | 无                                                                                |
| 默认     | 无                                                                                |
| 命令模式   | EXEC                                                                             |
| 使用情况信息 | 全交换和 SmartFabric 模式均支持此命令。有关支持的平台，请参阅 <a href="#">适用于分支和主干的 SmartFabric 服务</a> 。 |

从版本 10.5.0.1 开始，在 MX9116n 和 MX5108n 交换机上受支持。此外，从版本 10.5.0.3 开始，还在 SFS 支持的 OS10 交换机上可用。

示例

```
OS10# show smartfabric cluster

CLUSTER DOMAIN ID : 119
VIP : fde1:53ba:e9a0:de14:0:5eff:fe00:1119
ROLE : BACKUP
SERVICE-TAG : 3GB1XC2
MASTER-IPV4 : 10.11.105.15

```

支持的版本 10.5.0.1 or later

show smartfabric cluster member

显示群集成员信息，如服务编号、IP 地址、状态、角色、每个交换机的类型或 IOM 和机箱型号以及交换机所属的机箱的服务编号。

|        |                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show smartfabric cluster member                                                                                                                  |
| 参数     | 无                                                                                                                                                |
| 默认     | 无                                                                                                                                                |
| 命令模式   | EXEC                                                                                                                                             |
| 使用情况信息 | 内容显示会有所不同，具体取决于交换机角色。例如，如果您在主交换机上运行此命令，则会显示备份和主交换机信息，因为它们都是群集的成员。如果在备份节点上运行此命令，则仅显示主节点的信息。有关支持的平台，请参阅 <a href="#">适用于分支和主干的 SmartFabric 服务</a> 。 |

全交换和 SmartFabric 模式均支持此命令。

从版本 10.5.0.1 开始，在 MX9116n 和 MX5108n 交换机上受支持。此外，从版本 10.5.0.3 开始，还在 SFS 支持的 OS10 交换机上可用。

示例

```
OS10# show smartfabric cluster member
Service-tag IP Address
 Status Role Type Chassis-Service-Tag Chassis-
Slot

9A2HEM3 fde1:53ba:e9a0:de14:2204:fff:fe01:eb90
 ONLINE BACKUP
9GB1XC3 fde1:53ba:e9a0:de14:e6f0:4ff:fe3e:45dd
 ONLINE MASTER
3GB1XC2 fde1:53ba:e9a0:de14:e6f0:4ff:fe3e:3ce4
 ONLINE BACKUP
```

支持的版本 10.5.0.1 or later

show smartfabric details

显示所有结构信息，如名称、说明、ID、属于结构的节点、与结构关联的设计类型，以及结构的状态详细信息。

|        |                          |
|--------|--------------------------|
| 语法     | show smartfabric details |
| 参数     | 无                        |
| 默认     | 无                        |
| 命令模式   | EXEC                     |
| 使用情况信息 | 使用此命令可以查看已配置结构的详细列表。     |



全交换和 SmartFabric 模式均支持此命令。有关支持的平台，请参阅[适用于分支和主干的 SmartFabric 服务](#)。

从版本 10.5.0.1 开始，在 MX9116n 和 MX5108n 交换机上受支持。此外，从版本 10.5.0.3 开始，还在 SFS 支持的 OS10 交换机上可用。

示例

```
OS10# show smartfabric details

Name : AutoFab-08ee685b-d6d6-5d0c-99d2-ae78f800d4b7
Description : Auto-Fabric Generator
ID : 08ee685b-d6d6-5d0c-99d2-ae78f800d4b7
DesignType : AutoFabricDesign--1
Validation Status: VALID
VLTi Status : VALID
Placement Status: VALID
Nodes : CAC00N2, AZY1234

Name : AutoFab-100
Description : Auto-Fabric Generator
ID : 100
DesignType :
Validation Status: VALID
VLTi Status : VALID
Placement Status: VALID
Nodes : AZY1234, CAC00N2, 9GTWNK2, FHTWNK2

```

支持的版本 10.5.0.1 or later

show smartfabric networks

显示所有网络配置文件信息，例如 ID、QoS 优先级类型和 VLAN。

语法 show smartfabric networks

参数 无

默认 无

命令模式 EXEC

使用情况信息 使用此命令可以查看已配置网络配置文件的详细说明。

全交换和 SmartFabric 模式均支持此命令。有关支持的平台，请参阅[适用于分支和主干的 SmartFabric 服务](#)。

从版本 10.5.0.1 开始，在 MX9116n 和 MX5108n 交换机上受支持。此外，从版本 10.5.0.3 开始，在 SFS 支持的 PowerSwitch 平台上也可用。

示例

```
OS10# show smartfabric networks
Name Type QosPriority Vlan

v5 GENERAL PURPOSE BRONZE
8f018a8c-c355-4d81-9bee-85cfedcf8d2a 5
network100-105 GENERAL PURPOSE BRONZE
deb0886c-4a9b-47f2-8220-55afcb1f1756 100-105
Network VXLAN PLATINUM
d1de8f16-ebd0-4b1a-9689-a802d23b2b26 777
VLAN 1 GENERAL PURPOSE SILVER
4bb446a3-702c-4a0f-abdd-07dd0c14775a 1
v1 GENERAL PURPOSE BRONZE
9f2bed94-9148-46d8-9df6-3b606c83a472 500
```

支持的版本 10.5.0.1 or later

## show smartfabric nodes

显示所有节点信息，如服务编号、类型、状态、模式、与节点关联的结构 ID、机箱服务编号和机箱插槽。

|        |                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show smartfabric nodes                                                                                                                                                                                                  |
| 参数     | 无                                                                                                                                                                                                                       |
| 默认     | 无                                                                                                                                                                                                                       |
| 命令模式   | EXEC                                                                                                                                                                                                                    |
| 使用情况信息 | <p>使用此命令可查看有关所有节点的详细清单信息。</p> <p>全交换和 SmartFabric 模式均支持此命令。有关支持的平台，请参阅<a href="#">适用于分支和主干的 SmartFabric 服务</a>。</p> <p>从版本 10.5.0.1 开始，在 MX9116n 和 MX5108n 交换机上受支持。此外，从版本 10.5.0.3 开始，在 SFS 支持的 PowerSwitch 平台上也可用。</p> |

|    |                                                                                                                                                                                                                                                     |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show smartfabric nodes Service -Tag      Type      Status Mode      Chassis-Service-Tag Chassis-Slot FabricId ----- 3GB1XC2   S5232F-ON  ONLINE FABRIC 9GB1XC3   S5232F-ON  ONLINE FULL- SWITCH 9A2HEM3   S4148F-ON  ONLINE FABRIC</pre> |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|       |                   |
|-------|-------------------|
| 支持的版本 | 10.5.0.1 or later |
|-------|-------------------|

## show smartfabric personality

显示节点的个性化。

|        |                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show smartfabric personality                                                                                                                                                                                  |
| 参数     | 无                                                                                                                                                                                                             |
| 默认     | 无                                                                                                                                                                                                             |
| 命令模式   | EXEC                                                                                                                                                                                                          |
| 使用情况信息 | <p>输出因交换机的角色而异。</p> <p>全交换和 SmartFabric 模式均支持此命令。有关支持的平台，请参阅<a href="#">适用于分支和主干的 SmartFabric 服务</a>。</p> <p>从版本 10.5.0.1 开始，在 MX9116n 和 MX5108n 交换机上受支持。此外，从版本 10.5.0.3 开始，在 SFS 支持的 PowerSwitch 平台上也可用。</p> |

|    |                                                                                                                                                                                                                                                                                               |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show smartfabric personality  Personality      :None Role             : ICL              :  OS10# show smartfabric personality  Personality      :L3 Fabric Role             :LEAF ICL              :ethernet1/1/5, ethernet1/1/6 Leaf1#  OS10# show smartfabric personality</pre> |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```

Personality :L3 Fabric
Role :SPINE
ICL :

```

**支持的版本** 10.5.0.1 or later

## show smartfabric uplinks

显示所有上行链路信息，如名称、说明、ID、介质类型、本机 VLAN、配置的接口以及与上行链路关联的网络配置文件。

**语法** show smartfabric uplinks

**参数** 无

**默认** 无

**命令模式** EXEC

**使用情况信息** 使用命令查看所有已配置的上行链路信息。

全交换和 SmartFabric 模式均支持此命令。有关支持的平台，请参阅[适用于分支和主干的 SmartFabric 服务](#)。

从版本 10.5.0.1 开始，在 MX9116n 和 MX5108n 交换机上受支持。此外，从版本 10.5.0.3 开始，在 SFS 支持的 PowerSwitch 平台上也可用。

**示例**

```

OS10# show smartfabric uplinks

Name : uplink to b1
Description :
ID : 2725707d-886a-41c6-9d0d-38c4115788ff
Media Type : ETHERNET
Native Vlan : 1
Untagged-network :
Networks : deb0886c-4a9b-47f2-8220-55afcb1f1756,
 9f2bed94-9148-46d8-9df6-3b606c83a472
Configured-Interfaces : 9A2HEM3:ethernet1/1/42, 3GB1XC2:ethernet1/1/42

Name : u1
Description :
ID : e1c8169e-00dd-4a72-9e42-54485c049591
Media Type : FC
Native Vlan : 0
Untagged-network :
Networks : d1de8f16-ebd0-4b1a-9689-a802d23b2b26
Configured-Interfaces : 3GB1XC2:fibrechannel1/1/44:1

```

**支持的版本** 10.5.0.1 or later

## show smartfabric validation-error

显示所有拓扑验证错误信息，例如类别、子类别、说明、建议的操作、严重性、时间戳、EEMI、问题，以及针对每个发现的错误的建议链接。

**语法** show smartfabric validation-error

**参数** 无

**默认** 无

**命令模式** EXEC

**使用情况信息** 使用命令查看拓扑验证错误的列表以及每个错误的详细说明。

全交换和 SmartFabric 模式均支持此命令。有关支持的平台，请参阅[适用于分支和主干的 SmartFabric 服务](#)。

从版本 10.5.0.1 开始，在 MX9116n 和 MX5108n 交换机上受支持。此外，从版本 10.5.0.3 开始，在 SFS 支持的 PowerSwitch 平台上也可用。

## 示例

```
MX9116N-A1# show smartfabric validation-error
Category : FabricError
Subcategory : ISLError
Description : Unable to validate the fabric because the design
link
ICL-4_REVERSE not connected as per design
2xMX9116n_Fabric_Switching_Engines_in_same_chassis.
RecommendedAction : Make sure that the links are connected as per
design.
EEMI : NFAB0012
Severity : Severity1
ErrorK : 66d6eafe-f3f6-4567-bc1d-6dfc49284d67-ISL-
[ICL-4_REVERSE]-NotFound-Issue
Timestamp : 1549486364
RecommenedLink
 SourceNode : 1G86XC2
 SourceInterface : 1G86XC2:ethernet1/1/37
 DestinationNode : 2J86XC2
 DestinationInterface: 2J86XC2:ethernet1/1/37
ProblemLink
 SourceNode : 1G86XC2
 SourceInterface : 1G86XC2:ethernet1/1/33:4
 DestinationNode : 7D86XC2
 DestinationInterface: 7D86XC2:ethernet1/1/25:4
```

## 支持的版本

10.5.0.1 or later

# SmartFabric Director

SmartFabric Director 将管理数据中心内有或没有任何虚拟基础架构的交换机。SmartFabric Director 提供对物理和虚拟网络的操作、管理和故障处理的单一视图。

## SmartFabric Director 功能

- 定义、构建和维护第 2 层和第 3 层分支-主干数据中心（基础）。
- 基于用途模板的调配基础
- 目的和交换配置与状态的授权存储库
- 结构运行状况管理和监控，包括事件、日志、警报、状态和指标（计数器）
- 操作员驱动的补救措施
- 对交换机的完整生命周期管理，包括交换机分组和作业计划
- 使用 Openconfig 对交换机进行调配和流式遥测

有关 SmartFabric Director 的详细信息，请参阅 *Dell EMC SmartFabric Director User Guide*（Dell EMC SmartFabric Director 用户指南）。

## 在交换机上启用 SmartFabric Director 模式

要在交换机中启用 SmartFabric Director 模式，请使用 `switch-operating-mode` 命令。有关详细信息，请参阅 [switch-operating-mode](#)。

## 支持 SmartFabric Director

SmartFabric Director 使用 gRPC 网络管理接口代理 (gNMI) 代理和生命周期管理来调配交换机的遥测数据并对其进行流式传输。

OS10 支持：

- 使遥测代理能够将预配置的传感器组数据传输到 SmartFabric Director 的 gNMI 代理。有关 gNMI 代理的详细信息，请参阅 [gNMI 代理](#)。
- Google Network 操作接口 (gNOI) API，以使用 SmartFabric Director 启用生命周期管理。有关详情，请参阅[生命周期管理](#)。

## gRPC 网络管理接口代理

gNMI 代理可与 OS10 版本 10.5.0.1 及更高版本配合使用，提供配置 OS10 设备的新接口。它使用 gNMI 协议和 Openconfig Yang 模型来支持创建、读取、更新和删除 (CRUD) 操作、生命周期管理（通过 gNOI）和配置流式遥测。

gNMI 代理侦听 SmartFabric Director 以接收远程配置更改请求或升级和降级说明。在这些远程配置更改的过程中，gNMI 代理使遥测代理能够将预配置的传感器组数据以 OpenConfig 格式传输到 SmartFabric Director。有关预配置的传感器组的详细信息，请参阅[配置遥测](#)。

## 将安全配置文件设置为 gNMI 代理

在 SmartFabric Director 中建立与 gNMI 客户端之间的连接之前，请为 gNMI 代理设置有效的特定于应用程序的安全配置文件。此外，配置 FQDN 或 IP 地址以输入 SmartFabric Director 服务器；分配客户端和 CA 证书。使用具有超级管理员权限的

SmartFabric Director 中的用户角色可访问代理。分配给 gNMI 代理的安全配置文件必须在交换机上预配置。使用 `crypto security-profile` 命令可配置安全配置文件。

要为 gNMI 代理设置安全配置文件，请在 CONFIGURATION 模式下输入以下命令：

- `OS10(config)#gnmi-security-profile profile-name`

## 激活 gNMI 代理

要激活 gNMI 代理，请将交换机操作模式设置为 SmartFabric Director 模式。

**注：**更改交换机模式仅在您重新加载设备后才会生效。

要设置 SmartFabric Director 模式，请在 CONFIGURATION 模式下输入以下命令：

```
OS10# configure terminal
OS10(config)# switch-operating-mode sfd
```

运行命令后，系统将显示：

```
Manual reboot required for this command to take effect. Continue(yes/no)? :yes
OS10(config)# exit
OS10# write memory
OS10# reload

Proceed to reboot the system?
[confirm yes/no]:yes
```

当 gNMI 代理处于活动状态时，SmartFabric Director 将使用 TLS 验证和基于用户名密码的身份验证与代理建立连接。成功进行身份验证后，SmartFabric Director 将获得对 gNMI 代理的访问权限。SmartFabric Director 中的 gNMI 客户端会将一组请求发送到 gNMI 代理。

GNMI 代理将遥测代理参数配置为以 OpenConfig 格式传输遥测数据。

**注：**只有具有超级管理员权限的 SmartFabric Director 用户角色可以连接到 gNMI 代理。拒绝所有其他用户角色。因此，成功传递身份验证的用户角色可完全访问系统。

## 查看交换机模式

要确定交换机是否在 SmartFabric Director 模式下运行，您可以查看交换机运行的当前模式。

要查看交换机的操作模式，请输入以下命令：

- `OS10# show switch-operating-mode.`

```
OS10# show switch-operating-mode

Switch-Operating-Mode : SmartFabric director Mode
```

## OpenConfig 支持的遥测数据

GNMI 代理配置遥测代理程序，以将预配置的传感器配置文件映射到 OpenConfig 格式。

下表列出了受支持的 OpenConfig 型号：

表. 6: Openconfig 设备

| 传感器组名称    | YANG 容器                                                                                                                                                                                       |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| oc-device | <ul style="list-style-type: none"><li>• <code>openconfig-platform/components/component</code></li><li>• <code>openconfig-network-instance/network-instances/network-instance</code></li></ul> |

表. 7: Openconfig 系统

| 传感器组名称    | YANG 容器                                                                                                                                        |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------|
| oc-system | <ul style="list-style-type: none"> <li>openconfig-system/system/processes/process</li> <li>openconfig-platform/components/component</li> </ul> |

表. 8: Openconfig 环境

| 传感器组名称         | YANG 容器                                  |
|----------------|------------------------------------------|
| oc-environment | openconfig-platform/components/component |

表. 9: Openconfig 接口

| 传感器组名称       | YANG 容器                                    |
|--------------|--------------------------------------------|
| oc-interface | openconfig-interfaces/interfaces/interface |

表. 10: Openconfig 缓冲区统计信息

| 传感器组名称    | YANG 容器                                 |
|-----------|-----------------------------------------|
| oc-buffer | openconfig-qos/qos/interfaces/interface |

表. 11: Openconfig LAG 分发

| 传感器组名称 | YANG 容器                                    |
|--------|--------------------------------------------|
| oc-lag | openconfig-interfaces/interfaces/interface |

表. 12: Openconfig BGP 统计信息

| 传感器组名称 | YANG 容器                               |
|--------|---------------------------------------|
| oc-bgp | openconfig-bgp/bgp/neighbors/neighbor |

## 使用 SmartFabric Director 的生命周期管理

使用 SmartFabric Director 的生命周期管理可与 OS10 版本 10.5.0.1 及更高版本配合使用。GNMI 代理还会处理来自 SmartFabric Director 服务器的映像升级或降级请求。SmartFabric Director 可以使用 Google Network 操作接口 (gNOI) API 调用将这些请求发送到 gNMI 代理。

下表介绍了支持的 gNOI API:

表. 13: download\_and\_install API

| API 名称               | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| download_and_install | <p>从指定的映像-url 路径位置下载 OS10 二进制映像。支持以下映像-url 路径格式:</p> <ul style="list-style-type: none"> <li>远程 FTP 服务器</li> <li>远程 HTTP 或 HTTPS 服务器</li> <li>远程 TFTP 文件系统</li> </ul> <p>下载 OS10 二进制文件后, gNMI 代理将根据映像类型在指定位置安装该映像。例如, 如果映像类型为 OS10 NOS, 则代理将在闪存驱动器的备用分区上安装映像。如果映像下载或安装操作失败, 则系统将发送相应的错误消息。由于不需要重新引导, 因此此远程映像安装过程不会影响当前的服务。</p> <p> <b>注:</b> 仅 OS10 二进制映像支持此远程升级或降级功能。不支持固件升级, 包括 ONIE、CLPD 和 FPGA。</p> |

表. 14: 激活 API

| API 名称   | 说明                                                                                                                                     |
|----------|----------------------------------------------------------------------------------------------------------------------------------------|
| activate | <p>激活新安装的 OS10 映像。</p> <p>激活是两个阶段的进程。在第一个阶段中，引导分区在后续引导周期中设置为待机。在第二个阶段，将发出系统重新加载，以从待机分区引导新安装的 OS10 映像。激活映像操作要求重新加载系统。因此，当前的服务会受到影响。</p> |

表. 15: cancel\_upgrade API

| API 名称         | 说明                                                                                                                                           |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| cancel_upgrade | <p>取消活动的 OS10 映像下载过程。</p> <p>cancel_upgrade 进程采用一种尽力操作机制，可尝试取消活动图像文件下载。此操作将取消图像文件传输，并终止升级操作。映像文件传输完成后，映像安装过程将立即启动。因此，取消升级操作无法停止已在进行中的安装。</p> |

表. 16: get\_upgrade\_status API

| API 名称             | 说明                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| get_upgrade_status | <p>监控映像文件传输和安装操作的状态。</p> <p>此操作将向 SmartFabric Director 服务器返回以下详细信息：</p> <ul style="list-style-type: none"> <li>• 文件传输状态</li> <li>• 传输进度百分比</li> <li>• 映像安装状态</li> <li>• 文件传输进度</li> <li>• 文件大小</li> <li>• 文件传输字节</li> <li>• 文件传输速率</li> <li>• 传输任务结束时间</li> <li>• 传输任务开始时间</li> <li>• 传输任务状态下载</li> <li>• 传输任务详细信息</li> <li>• 安装全局状态</li> <li>• 安装任务结束时间</li> <li>• 安装任务开始时间</li> <li>• 安装任务状态</li> <li>• 安装任务状态详细信息</li> </ul> |

## SmartFabric Director 命令

### switch-operating mode

将交换机的操作模式设置为 SmartFabric Director 模式。

|        |                                                                                |
|--------|--------------------------------------------------------------------------------|
| 语法     | switch-operating-mode <i>Full-Switch</i>                                       |
| 参数     | <ul style="list-style-type: none"> <li>• Full-Switch — 将操作模式设置为全交换。</li> </ul> |
| 默认     | 未配置                                                                            |
| 命令模式   | CONFIGURATION 模式                                                               |
| 使用情况信息 | 无。                                                                             |
| 示例     |                                                                                |

```
OS10(config)# switch-operating-mode Full-Switch
```



支持的版本 10.4.3.0 or later

## gnmi-security-profile

设置 gNMI 代理的安全配置文件。

|        |                                                                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | gnmi-security-profile <i>profile-name</i>                                                                                                                                                          |
| 参数     | <i>profile-name</i> — 输入要与 gNMI 代理关联的安全配置文件的名称。                                                                                                                                                    |
| 默认     | 未配置                                                                                                                                                                                                |
| 命令模式   | CONFIGURATION                                                                                                                                                                                      |
| 使用情况信息 | 建立与 gNMI 代理之间的连接之前，请为 gNMI 代理设置有效的特定于应用程序的安全配置文件。此外，还可以配置 FQDN 或 IP 地址以供 SmartFabric Director 服务器输入、分配客户端和 CA 证书，并将系统管理员权限分配给用于访问代理的用户角色。在交换机上使用 <code>crypto security-profile</code> 命令配置了安全配置文件。 |

示例

```
os10(config)# gnmi-security-profile gnmi_sec_profile
```

支持的版本 10.5.0.1 or later

## show switch-operating-mode

查看交换机的操作模式。

|        |                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show switch-operating-mode                                                                                                                   |
| 参数     | 无                                                                                                                                            |
| 默认     | 未配置                                                                                                                                          |
| 命令模式   | EXEC                                                                                                                                         |
| 使用情况信息 | 某些 OS10 交换机在全交换和 SmartFabric 模式下运行。对于 PowerEdge MX 以太网 I/O 模块，请参阅 <a href="#">操作模式</a> 。此命令将更新，以在版本 10.5.0.1 中显示 SmartFabric Director 的运行模式。 |

示例

```
OS10# show switch-operating-mode
Switch-Operating-Mode : SmartFabric Director Mode
```

支持的版本 10.4.0E(R3S) or later

## show sfd status

显示与 SmartFabric Director 对应的状态。

|        |                                           |
|--------|-------------------------------------------|
| 语法     | show sfd status                           |
| 默认     | 显示控制器的 IP 地址和 SmartFabric Director 的端口状态。 |
| 命令模式   | EXEC                                      |
| 使用情况信息 | 无。                                        |

示例

```
OS10# show sfd status
Controller IP Port Status

10.14.8.102 8443 active
OS10#
```

支持的版本 10.5.0.3 or later

# 系统管理

|                   |                                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>系统横标</b>       | 提供信息以配置系统登录和当天消息 (MOTD) 文本横标, 请参阅 <a href="#">系统横标</a> 。                                                                  |
| <b>用户会话管理</b>     | 提供信息以管理活动用户会话, 请参阅 <a href="#">用户会话管理</a> 。                                                                               |
| <b>Telnet 服务器</b> | 提供信息以设置交换机上的 Telnet TCP/IP 连接, 请参阅 <a href="#">Telnet 服务器</a> 。要设置保护, 加密到交换机的安全外壳 (SSH) 连接, 请参阅 <a href="#">SSH 服务器</a> 。 |
| <b>简单网络管理协议</b>   | 提供简单网络管理协议 (SNMP) 管理器与代理之间进行通信的消息格式。SNMP 为网络监控和设备管理提供标准化框架和常用语言, 请参阅 <a href="#">简单网络管理协议</a> 。                           |
| <b>系统时钟</b>       | 提供信息以设置系统时间, 请参阅 <a href="#">系统时钟</a> 。                                                                                   |
| <b>网络时间协议</b>     | 提供信息以在服务器与客户端之间同步计时, 请参阅 <a href="#">网络时间协议</a> 。                                                                         |
| <b>动态主机配置协议</b>   | 提供信息以根据策略动态地为网络主机分配 IP 地址和其他配置参数, 请参阅 <a href="#">动态主机配置协议</a> 。                                                          |

有关如何设置与生产网络独立的管理网络的信息, 请参阅[管理 Dell EMC Networking 的网络](#)。

## 系统横标

您可以配置系统登录和当天消息 (MOTD) 文本横标。在您登录之前将显示系统登录横标。成功登录后, 将立即显示 MOTD 横标。您还可以将横标文本重置为 Dell EMC 默认横标或禁用横标显示。

## 登录横标

配置在使用交互模式登录之前显示的系统登录横标。不需要起始和结束双引号。输入单个分隔符字符或组合键 **^C** 以指定文本横标的开始和结束。

1. 输入带有单个分隔符字符的 `banner login` 命令, 然后按 **Enter** 键。
  2. 输入每行文本, 然后按 **Enter** 键。请输入最多 4096 个字符。对行数没有限制。
  3. 通过输入仅包含分隔符字符的行来填写横标配置。
- 在 CONFIGURATION 模式下启用登录横标。将分隔符和横标文本用双引号引起来。

```
banner login delimiter <Enter>
banner-text <Enter>
banner-text <Enter>
... <Enter>
delimiter
```

### 配置登录横标

```
OS10(config)# banner login %
DellEMC S4148U-ON login
Enter your username and password
%
```

要删除登录横标并将其重置为 Dell EMC 默认横标, 请使用 `no banner login` 命令。要在登录之前禁用横标显示, 请使用 `banner login disable` 命令。

## MOTD 横标

配置登录后显示的一条消息横标。输入最多 4096 个字符。要开始和结束 MOTD 横标, 请输入单个分隔符或组合键 **^C**。您可以输入任何字符作为分隔符。

要输入 MOTD 横标文本，请使用交互模式。输入带有分隔符字符的命令，然后按 **Enter** 键。然后输入每一行，然后按 **Enter** 键。通过输入仅包含分隔符字符的行来填写横标配置。不需要起始和结束双引号。

### 配置 MOTD 横标

```
OS10(config)# banner motd %
DellEMC S4148U-ON
Today's tip: Press tab or spacebar for command completion.
Have a nice day!
%
```

要删除 MOTD 横标并将其重置为 Dell EMC 默认 MOTD 横标，请使用 `no banner motd` 命令。要在登录后禁用 MOTD 横标显示，请使用 `banner motd disable` 命令。

## 系统横标命令

### banner login

配置登录到系统之前显示的登录横标。

#### 语法

```
banner login delimiter <Enter>
banner-text <Enter>
banner-text <Enter>
... <Enter>
delimiter
```

#### 参数

- *delimiter* — 输入单个分隔符字符或组合键 **^C** 以指定文本横标的开始和结束。
- *banner-text* — 输入最多 4096 个字符。对行数没有限制。

#### 默认

在您登录之前，将显示 Dell EMC 默认横标。

#### 命令模式

CONFIGURATION

#### 使用情况信息

- 要输入多行横标文本，请使用交互模式。输入带有分隔符字符的命令，然后按 **Enter** 键。然后输入每一行，然后按 **Enter** 键。通过输入仅包含分隔符字符的行来填写横标配置。不需要起始和结束双引号。
- 要删除登录横标并将其重置为 Dell EMC 默认横标，请使用 `no banner login` 命令。要在登录之前禁用横标显示，请使用 `banner login disable` 命令。

#### 示例

```
OS10(config)# banner login %
Welcome to DellEMC Z9100-ON
Enter your username and password
%
```

#### 支持的版本

10.4.1.0 or later

### banner motd

配置登录后显示的一天多行消息。

#### 语法

```
banner motd delimiter <Enter>
banner-text <Enter>
banner-text <Enter>
... <Enter>
delimiter
```

#### 参数

- *delimiter* — 输入单个分隔符字符或组合键 **^C** 以指定文本横标的开始和结束。
- *banner-text* — 输入最多 4096 个字符。行数没有限制。

#### 默认

登录后，将显示 Dell EMC 默认 MOTD 横标。

#### 命令模式

CONFIGURATION

- 使用情况信息
- 要输入 MOTD 横标文本，请使用交互模式。输入带有分隔符字符的命令，然后按 **Enter** 键。然后输入每一行，然后按 **Enter** 键。通过输入仅包含分隔符字符的行来填写横标配置。不需要起始和结束双引号。
  - 要删除登录横标并将其重置为 Dell EMC 默认横标，请使用 `no banner motd` 命令。要在登录之前禁用横标显示，请使用 `banner motd disable` 命令。

示例

```
OS10(config)# banner motd %
DellEMC S4148U-ON
Today's tip: Press tab or spacebar for command completion.
Have a nice day!
%
```

支持的版本

10.4.1.0 or later

# 用户会话管理

您可以使用以下命令管理活动用户会话：

- 在 CONFIGURATION 模式下使用 `exec-timeout timeout-value` 命令配置所有活动用户会话的超时。
- 在 EXEC 模式下使用 `kill-session session-ID` 命令清除任何用户会话。
- 在 EXEC 模式下使用 `show sessions` 命令查看活动用户会话。

## 为用户会话配置超时

```
OS10(config)# exec-timeout 300
OS10(config)#
```

## 清除用户会话

```
OS10# kill-session 3
```

## 查看活动用户会话

```
OS10# show sessions

Current session's operation mode: Non-transaction

Session-ID User In-rpcs In-bad-rpcs Out-rpc-err Out-notify Login-time
Lock

--
 3 snmp_user 114 0 0 0 2017-07-10T23:58:39Z
 4 snmp_user 57 0 0 0 2017-07-10T23:58:40Z
 6 admin 17 0 0 4 2017-07-12T03:55:18Z
*7 admin 10 0 0 0 2017-07-12T04:42:55Z
OS10#
```

Session-ID 列中的星号 (\*) 表示当前 OS10 会话。

# 用户会话管理命令

## exec-timeout

为所有用户会话配置超时值。

语法

`exec-timeout timeout-value`

参数

`timeout-value` — 输入超时值（以秒为单位），从 0 到 3600。

默认

未配置

命令模式

CONFIGURATION

|        |                                                         |
|--------|---------------------------------------------------------|
| 使用情况信息 | 此命令的 no 版本将禁用超时。                                        |
| 示例     | <pre>OS10(config)# exec-timeout 300 OS10(config)#</pre> |
| 支持的版本  | 10.3.1E or later                                        |

## kill-session

终止用户会话。

|        |                                      |
|--------|--------------------------------------|
| 语法     | <code>kill-session session-ID</code> |
| 参数     | <code>session-ID</code> — 输入用户会话 ID。 |
| 默认     | 未配置                                  |
| 命令模式   | EXEC                                 |
| 使用情况信息 | 无                                    |
| 示例     | <pre>OS10# kill-session 3</pre>      |
| 支持的版本  | 10.3.1E or later                     |

## show sessions

显示活动管理会话。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show sessions</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | 使用此命令可查看有关活动用户管理会话的信息。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 示例     | <pre>OS10# show sessions  Current session's operation mode: Non-transaction  Session-ID User      In-rpcs In-bad-rpcs Out-rpc-err Out-notify Login-time      Lock ----- 3          snmp_user 114      0           0           0           2017-07-10T23:58:39Z 4          snmp_user 57       0           0           0           2017-07-10T23:58:40Z 6          admin    17       0           0           4           2017-07-12T03:55:18Z *7         admin    10       0           0           0           2017-07-12T04:42:55Z OS10#</pre> |
| 支持的版本  | 10.3.1E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

# Telnet 服务器

要允许 Telnet TCP/IP 到 OS10 交换机的连接，请启用 Telnet 服务器。OS10 Telnet 服务器使用 Debian telnetd 软件包。默认情况下，Telnet 服务器处于禁用状态。

启用 Telnet 服务器时，使用在管理或任何前面板端口上配置的 IP 地址连接到交换机。Telnet 服务器配置是永久的，并在您重新加载交换机后保持不变。要验证 Telnet 服务器配置，请输入 `show running-configuration` 命令。

 **注：** Dell EMC Networking 建议不使用 SSH 以连接到交换机的安全加密连接。SSH 默认已启用。要配置 SSH 连接，请参考 [SSH 服务器](#)。

启用 Telnet 服务器

```
OS10(config)# ip telnet server enable
```

禁用 Telnet 服务器

```
OS10(config)# no ip telnet server enable
```

默认情况下，在默认虚拟路由和转发 (VRF) 上禁用 Telnet 服务器。要将 Telnet 服务器配置为可在管理 VRF 上访问，请使用 `ip telnet server vrf management` 命令。

在管理 VRF 上配置 Telnet 服务器

```
OS10(config)# ip telnet server vrf management
```

Telnet 命令

ip telnet server enable

启用到 OS10 交换机的 Telnet TCP/IP 连接。

|        |                                                                                                                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | ip telnet server enable                                                                                                                                                                                                                                                           |
| 参数     | 无                                                                                                                                                                                                                                                                                 |
| 默认     | 已禁用                                                                                                                                                                                                                                                                               |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                     |
| 使用情况信息 | <p>默认情况下，Telnet 服务器处于禁用状态。启用 Telnet 服务器时，使用在管理端口或任何前面板端口上配置的 IP 地址来连接到 OS10 交换机。重新加载交换机后，将维护 Telnet 服务器配置。要验证 Telnet 服务器配置，请使用 <code>show running-configuration</code> 命令。</p> <p>从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。</p> |
| 示例     | <pre>OS10(config)# ip telnet server enable</pre>                                                                                                                                                                                                                                  |
| 示例（禁用） | <pre>OS10(config)# no ip telnet server enable</pre>                                                                                                                                                                                                                               |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                                                                                                              |

ip telnet server vrf

为管理或非默认 VRF 实例配置 Telnet 服务器。

|        |                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | ip telnet server vrf {management   vrf vrf-name}                                                                                                                  |
| 参数     | <ul style="list-style-type: none"><li>management — 配置用于访问 Telnet 服务器的管理 VRF。</li><li>vrf vrf-name — 输入关键字 vrf，后跟 VRF 的名称，以配置用于访问 Telnet 服务器的非默认 VRF 实例。</li></ul> |
| 默认     | Telnet 服务器在默认 VRF 上可访问。                                                                                                                                           |
| 命令模式   | CONFIGURATION                                                                                                                                                     |
| 使用情况信息 | 默认情况下，Telnet 服务器处于禁用状态。要启用 Telnet 服务器，请使用 <code>telnet enable</code> 命令。                                                                                          |
| 示例     | <pre>OS10(config)# ip telnet server vrf management OS10(config)# ip telnet server vrf vrf-blue</pre>                                                              |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                              |

# 简单网络管理协议

网络管理站使用简单网络管理协议 (SNMP) 检索和修改网络设备中代理上的托管对象的软件配置。受管对象是一个管理信息的基础。

受管设备中的 SNMP 代理将维护管理信息库 (MIB) 中的受管对象的数据。受管对象通过其对象标识符 (OID) 进行标识。远程 SNMP 代理对本地交换机上的 MIB 中存储的 OID 执行 SNMP，以查看和检索信息。

OS10 支持标准和私有 SNMP MIB，包括所有 get 请求。MIB 以分层方式组织，并使用对象标识符访问受管对象。有关在交换机上运行的 OS10 版本中支持的 MIB 列表，请参阅该版本的 OS10 发行说明。

OS10 在 SNMP 管理者和代理之间的 SNMP 通信中支持不同的安全模式和级别。每种安全模式均指 SNMP 消息中使用的 SNMP 版本。SNMP 版本提供不同级别的安全性，如用户身份验证和消息加密。

## SNMP 安全模式和级别

OS10 支持 SNMP 安全型号 v1、v2c 和 v3。受支持的安全级别无身份验证、身份验证和隐私。

您可以在配置 SNMP 组和用户时指定 SNMP 安全模式和级别。每个安全模式都对应一个提供不同安全级别的 SNMP 版本：

- SNMPv1 不提供用户身份验证或隐私保护（加密）。SNMP 消息以纯文本形式发送。
- SNMPv2c 不提供用户身份验证或加密。SNMP 消息以纯文本形式发送。
- SNMPv3 为用户配置安全级别，提供用户身份验证和 SNMP 消息加密：
  - 无用户密码或邮件加密
  - 仅限用户身份验证
  - 用户身份验证和消息加密

## MIB

OS10 支持以下标准和 Dell EMC 企业版 MIB。

MIB 存储在 /opt/dell/os10/snmp/mibs/ 目录中。

表. 17: 标准 MIB

| 模块                 | 标准            |
|--------------------|---------------|
| BRIDGE-MIB         | IEEE 802.1D   |
| ENTITY-MIB         | RFC 6933      |
| EtherLike-MIB      | RFC 3635      |
| HOST-RESOURCES-MIB | RFC 2790      |
| IEEE8021-PFC-MIB   | IEEE 802.1Qbb |
| IEEE8023-LAG-MIB   | IEEE 802.3ad  |
| IF-MIB             | RFC 2863      |
| IP-FORWARD-MIB     | RFC 4292      |
| IP-MIB             | RFC 4293      |
| LLDP-EXT-DOT1-MIB  | IEEE 802.1AB  |
| LLDP-EXT-DOT3-MIB  | IEEE 802.1AB  |
| LLDP-MIB           | IEEE 802.1AB  |
| OSPF-MIB           | RFC 4750      |
| OSPFV3-MIB         | RFC 5643      |
| Q-BRIDGE-MIB       | IEEE 802.1Q   |
| RFC1213-MIB        | RFC 1213      |

表. 17: 标准 MIB (续)

| 模块                      | 标准       |
|-------------------------|----------|
| SFLOW-MIB               | RFC 3176 |
| SNMP-FRAMEWORK-MIB      | RFC 3411 |
| SNMP-MPD-MIB            | RFC 3412 |
| SNMP-NOTIFICATION-MIB   | RFC 3413 |
| SNMP-TARGET-MIB         | RFC 3413 |
| SNMP-USER-BASED-SM-MIB  | RFC 3414 |
| SNMP-VIEW-BASED-ACM-MIB | RFC 3415 |
| SNMPv2-MIB              | RFC 3418 |
| TCP-MIB                 | RFC 4022 |
| UDP-MIB                 | RFC 4113 |

表. 18: Dell EMC 企业版 MIB

| 模块                        | 说明            |
|---------------------------|---------------|
| DELLEMC-OS10-BGP4V2-MIB   | OS10 BGPv2 实施 |
| DELLEMC-OS10-CHASSIS-MIB  | OS10 机箱实施     |
| DELLEMC-OS10-PRODUCTS-MIB | OS10 平台产品定义   |
| DELLEMC-OS10-SMI-MIB      | OS10 SMI 实施   |
| DELLEMC-OS10-TC-MIB       | OS10 网络设备文本约定 |

**注:** 对于 BGP，OS10 支持 Dell EMC 的 MIB DELLEMC-OS10-BGP4V2-MIB.mib。当您使用 BGP4-MIB 和 OID 1.3.6.1.2.1.15 时，OS10 将会返回一条 No such object 消息。将 OID 1.3.6.1.4.1.674.11000.5000.200.1.1 用于 BGP 相关的 MIB 对象。

## SNMPv3

SNMP 版本 3 (SNMPv3) 为用户身份验证和 SNMP 消息加密提供了增强的安全模式。用户身份验证要求 SNMP 数据包来自授权来源。消息加密可确保未经授权的源无法查看数据包内容。

要配置 SNMPv3 特定的安全设置-用户身份验证和消息加密 — 使用 `snmp-server user` 命令。您可以为身份验证和隐私（加密）密码生成本地化的密钥和增强的安全性。

## SNMP 引擎 ID

引擎 ID 标识用作交换机上的本地代理的 SNMP 实体。引擎 ID 是八位冒号分隔的数字；例如，00:00:17:8B:02:00:00:01。

配置 SNMPv3 用户时，您可以指定生成本地化的身份验证和/或私钥。本地化密码密钥是使用交换机的引擎 ID 生成的。本地化的密钥更复杂，并且提供了更高的隐私保护能力。

用于生成密码密钥的引擎 ID 对于交换机是唯一的。因此，您不能在另一个交换机上复制和使用本地化的 SNMP 安全密码。

## SNMP 组和用户

访问本地 SNMP 代理的 SNMP 组的成员称为 *SNMP 用户*。远程设备上的 SNMP 用户可通过 IP 地址以及用户访问本地代理的 UDP 端口进行标识。

在 OS10 中，将根据用户所属的组分配 SNMP 访问权限。您可以配置每个组以访问 SNMP MIB 树视图。



## SNMP 视图

在 OS10 中，您可以为 SNMP 用户组中的每个安全模式和级别配置视图。每种类型的视图均在视图开始时的 MIB 树层次结构中指定对象 ID (OID)。您还可以指定是否在视图中包含或排除 MIB 树结构的其余部分。

- 读取视图提供对指定 OID 树的只读访问权限。
- 写入视图提供对指定 OID 树的读写访问权限。
- 通知视图允许将指定的 OID 树中的 SNMP 通知（陷阱和通知）发送至组的其他成员。

## 配置 SNMP

要在网络中设置与 SNMP 代理之间的通信，请执行以下操作：

- 为 SNMP 组配置只读、读写和通知访问权限。
- 为指定 SNMP 版本配置具有 SNMP 视图的组（安全模式）。
- 将用户分配到组并配置 SNMPv3 特定的身份验证和加密设置，并可选择本地化安全密钥和基于 ACL 的访问。

配置 SNMP 包含按照任意顺序执行以下任务：

- 配置 SNMP 引擎 ID
- 配置 SNMP 视图
- 配置 SNMP 组
- 配置 SNMP 用户

## 配置 SNMP 引擎 ID

引擎 ID 标识交换机上的 SNMP 本地代理。引擎 ID 是八位冒号分隔的数字；例如，80:00:02:b8:04:61:62:63。

本地引擎 ID 用于创建本地化的身份验证和/或私钥，以在 SNMPv3 消息中实现更高的安全性。在配置 SNMPv3 用户时，将生成本地化的身份验证和/或私钥。

配置远程设备及其引擎 ID，以允许远程用户查询本地 SNMP 代理。远程引擎 ID 包含在查询中，用于生成身份验证和私钥以访问本地代理。如果未配置远程引擎 ID，远程用户尝试访问本地代理将失败。

**注：**在使用 `snmp-server engineID snmp-server user` 命令配置引擎 ID 之前，使用命令 `snmp-server engineID` 建立一个引擎 ID。如果 `snmp-server engineID` 更改了已配置的引擎 ID，则必须重新配置与引擎 ID 相关的所有引擎 ID 的身份 ID 和密钥。

```
snmp-server engineID [local engineID] [remote ip-address {[udp-port port-number] remote-engineID}]
```

要在 SNMPv3 用户配置中显示本地化的身份验证和隐私密钥，请使用 `show snmp engineID local` 命令。

### 配置 SNMP 引擎 ID

```
OS10(config)# snmp-server engineID local 80:00:02:b8:04:61:62:63
```

### 显示 SNMP 引擎 ID

```
OS10# show snmp engineID local
Local default SNMP engineID: 0x800002a2036c2b59fbd8a0
```

## 配置 SNMP 视图

在交换机上的 SNMP 代理中配置 MIB 树结构的只读、读写或通知视图。

`oid-tree` 值指定视图开始时 MIB 树层次结构中的 OID。在视图中输入 `included` 或 `excluded` 以包括或排除 MIB 子树内容的剩余部分。如有必要，请重新输入命令以排除包含的内容中的树条目。

```
snmp-server view view-name oid-tree [included | excluded]
```

### 配置只读视图

```
OS10(config)# snmp-server view readonly 1.3.6.1.2.1.31.1.1.1.6 included
```

## 配置读写视图

```
OS10(config)# snmp-server view rwView 1.3.6.1.2.1.31.1.1.1.6 included
OS10(config)# snmp-server view rwView 1.3.6.1.2.1.31.0.0.0.0 excluded
```

## 显示 SNMP 视图

```
OS10# show snmp view
view name : readview
OID : 1.3.6.5
excluded : True
```

## 配置 SNMP 组

使用允许用于组成员的视图配置 SNMP 组。指定对 SNMP 代理的只读、读/写和/或通知访问权限。

安全模式对应于用户用于发送和接收 SNMP 消息的 SNMP 版本。安全级别配置 SNMPv3 用户身份验证和隐私设置：

- **auth** — 在 SNMP 消息中对用户进行身份验证。
- **noauth** — 不对用户进行身份验证或加密 SNMP 消息；以纯文本形式发送邮件。
- **priv** — 对用户进行身份验证，并对 SNMP 消息进行加密/解密。

输入 ACL 以限制用户访问权限，以便仅从交换机上的 SNMP 代理接收和发送来自允许 ACL 的用户的消息。

```
snmp-server group group-name {v1 | v2c | v3 security-level} [access acl-name]
[read view-name] [write view-name] [notify view-name]
```

要在 SNMP 代理上配置 MIB 树的视图，请使用 `snmp-server view` 命令。

要配置 SNMPv3 用户的身份验证和隐私设置，请使用 `snmp-server user` 命令。

要显示配置的 SNMP 组，请使用 `show snmp group` 命令。

### 配置 SNMPv1 或 v2c 组

```
OS10(config)# snmp-server group v2group 2c read readview notify GetsSets
```

### 配置 SNMPv3 组

```
OS10(config)# snmp-server group v3group 3 priv read readview write writeview notify
alltraps
```

## 显示 SNMP 组

```
OS10# show snmp group
groupname : v2group
version : 2c
notifyview : GetsSets
readview : readview

groupname : v3group
version : 3
security level : priv
notifyview : alltraps
readview : readview
writeview : writeview
```

## 配置 SNMP 用户

使用组成员身份配置对交换机上的 SNMP 代理的用户访问权限。将每个用户分配到组并配置 SNMPv3 特定的身份验证和加密设置，并可选择本地化安全密钥和基于 ACL 的访问。多次重新输入命令，以配置所有用户 SNMP 安全设置。

```
snmp-server user user-name group-name security-model [[noauth | auth {md5 | sha} auth-
password]
[priv {des | aes}]] [localized] [access acl-name] [remote ip-address udp-port port-
number]
```

用户分配到的组决定了用户的访问权限。要配置组的访问权限（读取、写入和通知），请使用 `snmp-server group` 命令。SNMPv3 的安全模式通过用户身份验证和数据包加密提供强大的安全性。

SNMPv3 身份验证以及隐私算法和密码不存在默认值。如果您忘记了密码，则无法恢复，您必须重新配置用户。您可以指定纯文本密码或加密的文本密码。在任一情况下，密码都将以加密形式存储在配置中，并在 `show running-config snmp` 输出中显示为已加密。

本地化的身份验证或隐私密钥更复杂，并提供了更高的隐私保护能力。本地化密钥是使用交换机的引擎 ID 生成的。因此，您不能在另一个交换机上的配置文件中使用的本地化的 SNMP 安全密码。有关详细信息，请参阅[配置 SNMP 引擎 ID](#)。要在 SNMPv3 用户配置中显示本地化的身份验证和隐私密钥，请使用 `show running-configuration snmp` 命令。

要限制用户访问交换机上的 SNMP 代理，请输入一个 `access acl-name` 值。在 IPv6 ACL 中，SNMP 仅支持 IPv6 和 UDP 类型。不支持 TCP、ICMP 和端口规则。

要显示已配置的 SNMP 用户，请使用 `show snmp user` 命令。

### 配置 SNMPv1 或 v2c 用户

```
OS10(config)# snmp-server user admin1 netadmingroup 2c acl acl_AdminOnly
```

### 配置 SNMPv3 用户

```
OS10(config)# snmp-server user privuser v3group 3 encrypted auth
md59fc53d9d908118b2804fe80e3ba8763d priv des56 d0452401a8c3ce42804fe80e3ba8763d
```

```
OS10(config)# snmp-server user n3user ngroup remote 172.31.1.3 udp-port 5009 3 auth md5
authpasswd
```

### 显示 SNMP 用户

```
OS10# show snmp user
User name : privuser
Group : v3group
Version : 3
Authentication Protocol : MD5
Privacy Protocol : AES
```

## 生成 SNMPv3 本地化密钥

SNMP v3 中基于用户的安全模型使用以下算法提供强身份验证和加密：

- 身份验证算法 — MD5 和 SHA
- 加密算法 — DES 和 AES-128

在配置 SNMP 用户而不是使用明文密码的情况下，您可以使用通过身份验证和加密算法进行加密的本地化密钥。要生成本地化密钥，请使用 Linux 中的 `Snmpkey` 实用程序。确保在 Linux 服务器中安装了以下软件包，以生成本地化密钥：

- `libnet-snmp-perl`
- `libcrypt-des-perl`
- `libdigest-hmac-perl`
- `libcrypt-rijndael-perl`

使用以下命令以生成可在配置用户时使用的本地化密钥：

```
snmpkey {md5 | sha} authpassword engineID [des | 3des | aes] privpassword
```

其中，`authpassword` 是您为身份验证协议指定的密码，`engineID` 是本地引擎 ID，`privpassword` 是为隐私协议指定的密码。

使用 `show snmp engineID local` 命令以查看本地引擎 ID。

```
OS10# show snmp engineID local

Local default SNMP engineID: 0x800002a2036c2b59fbd8a0
```

在安装了 Snmpkey 实用程序的 Linux 服务器上输入以下命令：

```
snmpkey md5 testauthpasswd 0x800002a2036c2b59fbd8a0 des testprivpasswd
authKey: 0xaa5bb0eb6e6a9f036dc548e4ad9405f8
privKey: 0xaa5bb0eb6e6a9f036dc548e4ad9405f8
```

系统将生成身份验证和隐私密钥。

在配置 SNMP 用户时使用本地化密钥。

```
OS10(config)# snmp-server user user3 Group3 3 localized auth md5
0xaa5bb0eb6e6a9f036dc548e4ad9405f8 priv des 0xaa5bb0eb6e6a9f036dc548e4ad9405f8
```

## 配置 SNMP 陷阱

SNMP 代理使用称为 SNMP 陷阱的未经请求的 SNMP 消息将事件通知发送到管理站。SNMP 陷阱可优化网络资源的使用。

SNMP 版本 1 和版本 2C 陷阱可与版本 3 陷阱共存。SNMP 版本 1 和 2C 使用陷阱类别进行访问控制。SNMP 版本 3 陷阱与具有给定身份验证级别的 SNMP 用户关联。

在 OS10 交换机上配置 SNMP 陷阱，以将通知发送到管理站。

```
snmp-server host {ipv4-address | ipv6-address} {informs version version-number | traps
version version-number | version version-number} [snmpv3-security-level] [community-name]
[udp-port port-number] [dom | entity | envmon | lldp | snmp]
```

### 配置 SNMP v1 或 v2C 陷阱

```
OS10(config)# snmp-server host 10.11.73.110 traps version 2c comm2c lldp snmp
```

### 配置 SNMP v3 陷阱

```
OS10(config)# snmp-server group Group3 3 priv notify NOTIFY
OS10(config)# snmp-server user User3 Group3 3 auth md5 testpasswd priv aes testprivpasswd
OS10(config)# snmp-server host 10.11.56.46 version 3 priv User3
```

## 配置 SNMP 通知

SNMP 代理会将事件通知发送到并接收来自网络管理站 (NMS) 的确认，也称为远程 SNMP 服务器。收到来自 NMS 的 SNMP 响应的此类通知称为“通知”。通知比陷阱更可靠。如果 SNMP 代理不会收到确认，则会重发通知，最多重试三次。

配置远程 SNMP 服务器的引擎 ID 以接收确认。

```
snmp-server host {ipv4-address | ipv6-address} {informs version version-number | traps
version version-number | version version-number} [snmpv3-security-level] [community-name]
[udp-port port-number] [dom | entity | envmon | lldp | snmp]
```

### 配置 SNMP v3 通知

```
OS10(config)# snmp-server group Group3 3 priv notify NOTIFY
OS10(config)# snmp-server engineID remote 10.1.1.1 0x80000232334abc34d
OS10(config)# snmp-server user rem-user Group3 remote 10.1.1.1 udp-port 162 3 auth md5
testpasswd priv des testprivpasswd
OS10(config)# snmp-server host 10.11.5.1 informs version 3 priv rem-user
```

## SNMP 命令

### show snmp community

显示交换机上配置的 SNMP 社区。

语法 show snmp community

参数 无

|        |                                                        |
|--------|--------------------------------------------------------|
| 默认     | 无                                                      |
| 命令模式   | EXEC                                                   |
| 使用情况信息 | 要配置 SNMP 社区, 使用 <code>snmp-server community</code> 命令。 |
| 示例     |                                                        |

```
OS10# show snmp community
Community : public
Access : read-only

Community : dellOS10
Access : read-write
ACL : dellacl
```

|       |                   |
|-------|-------------------|
| 支持的版本 | 10.4.2.0 or later |
|-------|-------------------|

## show snmp engineID

显示交换机上或在交换机上访问 SNMP 代理的远程设备上的 SNMP 引擎 ID。

|        |                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show snmp engineID {local   remote}</code>                                                                                         |
| 参数     | <ul style="list-style-type: none"><li><code>local</code> — 显示本地引擎 ID。</li><li><code>remote</code> — 显示交换机上配置的远程设备的 SNMP 引擎 ID。</li></ul> |
| 默认     | 无                                                                                                                                        |
| 命令模式   | EXEC                                                                                                                                     |
| 使用情况信息 | 要为远程设备配置本地引擎 ID 或引擎 ID, 请使用 <code>snmp-server engineID</code> 命令。                                                                        |
| 示例     |                                                                                                                                          |

```
OS10# show snmp engineID remote
Remote Engine ID IP-addr Port
0x0712 1.1.1.1 23

OS10# show snmp engineID local
Local default SNMP engineID: 0x80001f880390b11cf4abe7
```

|       |                   |
|-------|-------------------|
| 支持的版本 | 10.4.2.0 or later |
|-------|-------------------|

## show snmp group

显示交换机上配置的 SNMP 组, 包括 SNMP 视图和安全模型。

|        |                                                   |
|--------|---------------------------------------------------|
| 语法     | <code>show snmp group</code>                      |
| 参数     | 无                                                 |
| 默认     | 无                                                 |
| 命令模式   | EXEC                                              |
| 使用情况信息 | 要配置 SNMP 组, 使用 <code>snmp-server group</code> 命令。 |
| 示例     |                                                   |

```
OS10# show snmp group
groupname : v2group
version : 2c
notifyview : GetsSets
readview : readview

groupname : v3group
version : 3
security level : priv
notifyview : alltraps
readview : readview
writeview : writeview
```

**支持的版本** 10.4.2.0 or later

## show snmp user

显示配置为访问交换机上的 SNMP 代理的用户，包括 SNMP 组和安全模型。

|               |                                     |
|---------------|-------------------------------------|
| <b>语法</b>     | show snmp user                      |
| <b>参数</b>     | 无                                   |
| <b>默认</b>     | 无                                   |
| <b>命令模式</b>   | EXEC                                |
| <b>使用情况信息</b> | 要配置 SNMP 用户，使用 snmp-server user 命令。 |
| <b>示例</b>     |                                     |

```
OS10# show snmp user
User name : privuser
Group : v3group
Version : 3
Authentication Protocol : MD5
Privacy Protocol : AES
```

**支持的版本** 10.4.2.0 or later

## show snmp view

显示交换机上配置的 SNMP 视图，包括视图开始的 SNMP 对象 ID。

|               |                                                                                     |
|---------------|-------------------------------------------------------------------------------------|
| <b>语法</b>     | show snmp view                                                                      |
| <b>参数</b>     | 无                                                                                   |
| <b>默认</b>     | 无                                                                                   |
| <b>命令模式</b>   | EXEC                                                                                |
| <b>使用情况信息</b> | 使用 show snmp view 命令可验证 MIB 树中 SNMP 视图的 OID 起始点。要配置 SNMP 视图，使用 snmp-server view 命令。 |
| <b>示例</b>     |                                                                                     |

```
OS10# show snmp view
view name : readview
OID : 1.3.6.5
excluded : True
```

**支持的版本** 10.4.2.0 or later

## snmp-server community

配置 SNMP 用户社区。

|               |                                                                                                                                                                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | snmp-server community name {ro   rw} [acl acl-name]                                                                                                                                                                                               |
| <b>参数</b>     | <ul style="list-style-type: none"><li>community name — 设置社区名称字符串以用作 SNMPv1 和 SNMPv2c 访问的密码。最多 20 个字母数字字符。</li><li>ro — 为 SNMP 社区设置只读访问权限。</li><li>rw — 为 SNMP 社区设置读写访问权限。</li><li>acl acl-name — 输入现有的 IPv4 ACL 名称以限制 SNMP 社区中 SNMP 访问。</li></ul> |
| <b>默认</b>     | SNMP 社区具有只读访问权限。                                                                                                                                                                                                                                  |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                                                                                                                                     |
| <b>使用情况信息</b> | SNMPv1 和 SNMPv2c 安全模式使用基于社区的安全形式。使用此命令可为 SNMP 社区名称配置只读或读写访问权限。配置的社区文本字符串用于 SNMPv1 和 SNMPv2c 用户身份验证。                                                                                                                                               |

要显示交换机上的 SNMP 社区，请使用 `show snmp community` 命令。

从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

命令的 `no` 版本将移除配置的社区文本字符串。

示例

```
OS10(config)# snmp-server community admin rw
OS10(config)# snmp-server community public ro acl snmp-read-only-acl
```

支持的版本 10.2.0E or later

snmp-server contact

配置用于对本地 SNMP 交换机进行故障处理的联系信息。

语法 snmp-server contact text

参数 text — 输入字母数字文本字符串。最多 55 个字符。

默认 SNMP 服务器的联系人为 support。

命令模式 CONFIGURATION

使用情况信息从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 no 版本会将 SNMP 服务器联系人重置为默认值。

示例

```
OS10(config)# snmp-server contact administrator
```

支持的版本 10.2.0E or later

snmp-server enable traps

在交换机上启用 SNMP 陷阱。

语法 snmp-server enable traps [notification-type] [notification-option]

参数

- notification-type notification-option — 输入 SNMP 通知类型，以及（可选）该类型的通知选项。

表. 19: 通知类型和选项

| 通知类型                     | 通知选项                                                                                                                                                                                                                                    |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| entity — 启用实体更改陷阱。       | 无                                                                                                                                                                                                                                       |
| envmon — 启用 SNMP 环境监控陷阱。 | <ul style="list-style-type: none"><li>fan — 启用风扇陷阱。</li><li>power-supply — 启用电源设备陷阱。</li><li>temperature — 启用温度陷阱。</li></ul>                                                                                                            |
| lldp — 启用 LLDP 状态更改陷阱。   | <ul style="list-style-type: none"><li>rem-tables-change — 启用 lldpRemTablesChange 陷阱。</li></ul>                                                                                                                                          |
| snmp — 启用 SNMP 陷阱。       | <ul style="list-style-type: none"><li>authentication — 启用身份验证陷阱。</li><li>coldstart — 在打开交换机和 SNMP 代理初始化时启用冷启动陷阱。</li><li>linkdown — 启用链路关闭陷阱。</li><li>linkup — 启用链路运行陷阱。</li><li>warmstart — 当交换机重新加载且 SNMP 代理重新初始化时，启用热启动陷阱。</li></ul> |

默认 未配置

## 命令模式

CONFIGURATION

## 使用情况信息

如果不使用命令输入 `notification-type` 或 `notification-option` 参数，将启用所有陷阱。如果只输入 `notification-type`，与该类型关联的所有 `notification-option` 陷阱将启用。

要启用特定 SNMP 陷阱类型，请使用不同的通知类型和选项多次重新输入命令。

要配置主机以接收 SNMP 通知，请使用 `snmp-server host` 命令。

从版本 10.4.1.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

命令的 `no` 版本将在交换机上禁用 SNMP 陷阱。

## 示例

```
OS10(config)# snmp-server enable traps envmon fan
OS10(config)# snmp-server enable traps envmon power-supply
OS10(config)# snmp-server enable traps snmp

OS10(config)# no snmp-server enable traps snmp
```

## 支持的版本

10.4.1.0 or later

# snmp-server engineID

配置本地和远程 SNMP 引擎 ID。

## 语法

```
snmp-server engineID [local engineID] [remote ip-address {udp-port port-number} remote-engineID]
```

## 参数

- `local engineID` — 输入将交换机上的本地 SNMP 代理识别为八字节冒号分隔数字的引擎 ID。最多 27 个字符。
- `remote ip-address` — 输入访问本地 SNMP 代理的远程 SNMP 设备的 IPv4 或 IPv6 地址。
- `udp-port port-number` — 输入远程设备上的 UDP 端口号，从 0 到 65535。
- `remote-engineID` — 输入在远程设备上标识 SNMP 代理的引擎 ID，0x 加十六进制字符串。

## 默认

本地引擎 ID 使用管理以太网接口的 MAC 地址生成。

## 命令模式

CONFIGURATION

## 使用情况信息

本地引擎 ID 会为身份验证和权限密码生成本地化密钥。这些密码对 SNMP 用户进行身份验证，并对 SNMP 消息进行加密。如果重新配置本地引擎 ID，则本地化的密钥也会更改。现有值不再有效，并且将显示一条警告消息。因此，您必须使用新的本地化密码密钥重新配置 SNMP 用户。

此外，如果您更改了远程设备的已配置引擎 ID，则必须重新配置远程用户的身份验证和隐私密码。

要显示当前的本地引擎 ID，请使用 `show snmp engineID local` 命令。

从版本 10.4.2.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 `no` 版本将重置默认引擎 ID 值。

## 示例

```
OS10(config)# snmp-server engineID local 80:00:02:b8:04:61:62:63

OS10(config)# snmp-server engineID local 80:00:02:b8:04:61:62:63
% Warning: Localized passwords need to be regenerated for local user.

OS10(config)# snmp-server engineID remote 1.1.1.1 0xaaffcc

OS10(config)# snmp-server engineID remote 1.1.1.2 udp-port 432 0xabeecc
```

## 支持的版本

10.4.2.0 or later



## snmp-server group

配置 SNMP 组中的用户所允许的视图。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>snmp-server group group-name {v1   v2c   v3 security-level} [access acl-name] [read view-name] [write view-name] [notify view-name]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"><li><code>group-name</code> — 输入组的名称。最多 32 个字母数字字符。</li><li><code>v1</code> — SNMPv1 不提供用户身份验证或隐私保护。SNMP 消息以纯文本形式发送。</li><li><code>v2c</code> — SNMPv2c 不提供用户身份验证或隐私保护。SNMP 消息以纯文本形式发送。</li><li><code>v3 security-level</code> — SNMPv3 为使用 <code>snmp-server user</code> 命令配置的 SNMP 消息提供可选的用户身份验证和加密。</li><li><code>security-level</code> — (仅限 SNMPv3) 配置 SNMPv3 用户的安全级别：<ul style="list-style-type: none"><li><code>auth</code> — 在 SNMP 消息中对用户进行身份验证。</li><li><code>noauth</code> — 不对用户进行身份验证或加密 SNMP 消息；以纯文本形式发送邮件。</li><li><code>priv</code> — 对用户进行身份验证，并对 SNMP 消息进行加密/解密。</li></ul></li><li><code>access acl-name</code> — (可选) 输入 IPv4 或 IPv6 访问列表的名称，以筛选在交换机上收到的 SNMP 请求。最多 16 个字符。</li><li><code>read view-name</code> — (可选) 输入只读视图的名称。最多 32 个字符。</li><li><code>write view-name</code> — (可选) 输入读写视图的名称。最多 32 个字符。</li><li><code>notify view-name</code> — (可选) 输入通知视图的名称。最多 32 个字符。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 使用情况信息 | <p>使用此命令可设置一组 SNMP 用户的访问权限。配置接收 SNMP 消息的安全级别。指定对 SNMP 代理的只读、读/写和/或通知访问权限。要配置 SNMPv3 用户的身份验证和隐私设置，请使用 <code>snmp-server user</code> 命令。</p> <p>输入 <code>access acl-name</code> 值，以将对 SNMP 代理的访问权限限制为仅 ACL 允许的用户。</p> <p>读取视图提供对 SNMP 代理的只读访问权限。读写视图允许读写访问权限。通知视图允许将 SNMP 通知发送至组成员。</p> <p>从版本 10.4.2.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p> <p>命令的 <code>no</code> 版本将删除 SNMP 组。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 示例     | <pre>OS10(config)# snmp-server group os10admin p3 priv read readonlyview</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 支持的版本  | 10.4.2.0 or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## snmp-server host

配置主机以接收 SNMP 通知。

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>snmp-server host {ipv4-address   ipv6-address} {informs version version-number   traps version version-number   version version-number} [snmpv3-security-level] [community-name] [udp-port port-number] [dom   entity   envmon   lldp   snmp]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 参数 | <ul style="list-style-type: none"><li><code>ipv4-address   ipv6-address</code> — 输入 SNMP 主机的 IPv4 或 IPv6 地址。</li><li><code>informs</code> — 将通知消息发送至 SNMP 主机。</li><li><code>traps</code> — 将陷阱消息发送至 SNMP 主机。</li><li><code>version version-number</code> — 输入用于将陷阱或通知发送至 SNMP 主机的 SNMP 安全模式：1、2c 或 3。所有安全模式均支持陷阱；只有 2c 和 3 支持通知。要仅发送 SNMP 通知，请仅输入 <code>version-number</code>；请勿输入 <code>informs</code> 或 <code>traps</code>。对于 SNMPv3 陷阱和通知，请输入安全级别：<ul style="list-style-type: none"><li><code>noauth</code> — (仅限 SNMPv3) 在不通过用户身份验证和隐私加密的情况下发送 SNMPv3 陷阱。</li><li><code>auth</code> — (仅限 SNMPv3) 包括发送至主机的 SNMPv3 消息的用户身份验证密钥：<ul style="list-style-type: none"><li><code>md5</code> — 使用消息摘要算法 (MD5) 算法生成身份验证密钥。</li></ul></li></ul></li></ul> |

- `sha` — 使用安全哈希算法 (SHA) 算法生成身份验证密钥。
- `auth-password` — 输入用于生成标识用户身份验证密钥的文本字符串。最多 32 个字母数字字符。对于加密密码，请输入加密的字符串，而不是纯文本。
- `priv` — (仅限 SNMPv3) 为发送到主机的 SNMPv3 消息配置加密：
  - `aes` — 使用 AES 128 位算法加密邮件。
  - `des` — 使用 DES 56 位算法加密邮件。
  - `priv-password` — 输入用于生成在加密消息中使用的私钥的文本字符串。最多 32 个字母数字字符。对于加密的密码，您可以输入加密的字符串而不是纯文本。
- `community-name` — (可选) 输入 SNMPv1 或 SNMPv2c 社区字符串名称或 SNMPv3 用户名。
- `udp-port port-number` — (可选) 输入 SNMP 主机上的 UDP 端口号 (0 至 65535)。
- `dom | entity | envmon | lldp | snmp` — 输入要发送到 SNMP 主机的一种或多种陷阱和通知 (数字光学监控器、实体更改、环境监控或 LLDP 状态更改陷阱或 SNMP 类型通知)。

默认

未配置

命令模式

CONFIGURATION

使用情况信息

本地 SNMP 代理将 SNMP 通知、陷阱和通告发送至配置为主机接收器的 SNMP 管理员。您可以配置多个主机接收器。

SNMP 主机不会确认陷阱消息和从 SNMP 代理收到的通知。在接收通知时，SNMP 主机会发送确认消息。

从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

命令的 `no` 版本禁止本地代理向主机接收器发送 SNMP 陷阱、通告或通知。

**示例 — 将 SNMP 通告发送至主机**

```
OS10(config)# snmp-server host 1.1.1.1 traps version 3 priv user01 udp-port 32 entity lldp
```

**示例 — 发送 SNMP 通知主机**

```
OS10(config)# snmp-server host 1.1.1.1 informs version 2c public envmon snmp
```

**示例 — 将 SNMP 通知发送至主机**

```
OS10(config)# snmp-server host 1.1.1.1 version 3 noauth u1 snmp lldp
```

支持的版本

10.2.0E or later

## snmp-server location

配置 SNMP 服务器的位置。

语法

`snmp-server location text`

参数

`text` — 输入字母数字字符串。最多 55 个字符。

默认

无

命令模式

CONFIGURATION

使用情况信息

从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 `no` 版本将移除 SNMP 位置。

示例

```
OS10(config)# snmp-server location datacenter10
```

支持的版本

10.2.0E or later

## snmp-server user

授权用户访问 SNMP 代理并接收 SNMP 消息。

**语法** `snmp-server user user-name group-name security-model [[noauth | auth {md5 | sha} auth-password] [priv {des | aes} priv-password]] [localized] [access acl-name] [remote ip-address udp-port port-number]]`

- 参数**
- `user-name` — 输入用户的名称。最多 32 个字母数字字符。
  - `group-name` — 输入用户所属的组的名称。最多 32 个字母数字字符。
  - `security-model` — 输入为 SNMP 消息设置安全级别的 SNMP 版本：
    - 1 — SNMPv1 不提供用户身份验证或隐私保护。SNMP 消息以纯文本形式发送。
    - 2c — SNMPv2c 不提供用户身份验证或隐私保护。SNMP 消息以纯文本形式发送。
    - 3 — SNMPv3 为 SNMP 消息提供了可选的用户身份验证和加密。
  - `noauth` — (仅限 SNMPv3) 将 SNMPv3 消息配置为在没有用户身份验证和隐私加密的情况下发送。
  - `auth` — (仅限 SNMPv3) 为发送给用户的 SNMPv3 消息包含用户身份验证密钥：
    - `md5` — 使用 MD5 算法生成身份验证密钥。
    - `sha` — 使用 SHA 算法生成身份验证密钥。
    - `auth-password` — 输入用于生成标识用户的身份验证密钥的文本字符串；最多 32 个字母数字字符。对于加密的密码，您可以输入加密的字符串而不是纯文本。
  - `priv` — (仅限 SNMPv3) 为发送给用户的 SNMPv3 消息配置加密：
    - `aes` — 使用 AES 128 位算法来加密邮件。
    - `des` — 使用 DES 56 位算法来加密邮件。
    - `priv-password` — 输入用于生成在加密消息中使用的私钥的文本字符串。最多 32 个字母数字字符。对于加密密码，请输入加密的字符串，而不是纯文本。
  - `localized` — (仅限 SNMPv3) 以本地化密钥格式生成 SNMPv3 身份验证和/或私钥。
  - `access acl-name` — (可选) 输入 IPv4 或 IPv6 访问列表的名称，以筛选交换机上 SNMP 请求。最多 16 个字符。
  - `remote ip-address/prefix-length udp-port port-number` — (可选) 输入用户远程设备的 IPv4 或 IPv6 地址，以及用于连接到交换机上的 SNMP 代理的 UDP 端口号，从 0 到 65535。默认为 162。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 使用 `snmp-server user` 命令可设置 SNMP 访问所需的安全级别。对于 SNMPv3 用户，请配置用户授权和消息加密。多次重新输入此命令，以配置所有用户 SNMP 安全设置。

用户分配到的组决定了用户的 SNMP 访问权限。要配置组的 SNMP 对交换机的访问权限（读取、写入和通知），请使用 `snmp-server user` 命令。

SNMPv3 身份验证以及隐私算法和密码不存在默认值。如果您忘记了密码，则无法恢复，您必须重新配置用户。您可以指定纯文本密码或加密的文本密码。在任一情况下，密码都将以加密形式存储在配置中，并在 `show running-config snmp` 输出中显示为已加密。

本地化的身份验证或隐私密钥更复杂，并提供了更高的隐私保护能力。要在 SNMPv3 用户配置中显示本地化的身份验证和隐私密钥，请使用 `show running-configuration snmp` 命令。

要限制用户访问交换机上的 SNMP 代理，请输入一个 `access acl-name` 值。在 IPv6 ACL 中，SNMP 仅支持 IPv6 和 UDP 类型。不支持 TCP、ICMP 和端口规则。

从版本 10.4.2.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 `no` 版本将从 SNMP 组移除用户。

### 示例（加密的密码）

```
OS10(config)# snmp-server user privuser v3group v3 auth md5
9fc53d9d908118b2804fe80e3ba8763d priv des
d0452401a8c3ce42804fe80e3ba8763d
```

### 示例（纯文本密码）

```
OS10(config)# snmp-server user authuser v3group v3 auth md5 authpasswd
```

### 示例（远程用户）

```
OS10(config)# snmp-server user n3user ngroup remote 172.31.1.3 udp-port
5009 3
auth md5 authpasswd
```

### 支持的版本

10.4.2.0 or later

## snmp-server view

配置 SNMPv3 视图。

### 语法

```
snmp-server view view-name oid-tree [included | excluded]
```

### 参数

- *view-name* — 输入只读、读写或通知视图的名称。最多 32 个字符。
- *oid-tree* — 输入以 12 位点分十进制格式开头的视图的 SNMP 对象 ID。
- *included* — （可选）在视图中包含 MIB 系列。
- *excluded* — （可选）从视图中排除 MIB 系列。

### 默认

未配置

### 命令模式

CONFIGURATION

### 使用情况信息

*oid-tree* 值指定视图开始时 MIB 树层次结构中的 OID。在 *included* 或 *excluded* 视图中输入或排除 MIB 子树内容的剩余部分。

从版本 10.4.2.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 *no* 版本将移除 SNMPv3 视图。

### 示例

```
OS10(config)# snmp-server view readview 1.3.6.5 excluded
```

### 支持的版本

10.4.2.0 or later

## snmp-server vrf

配置 SNMP 代理以接收管理 VRF 实例的 SNMP 陷阱。

### 语法

```
snmp-server vrf management
```

### 参数

无

### 默认

未配置

### 命令模式

CONFIGURATION

### 使用情况信息

此命令的 *no* 版本将禁止 SNMP 代理接收 SNMP 陷阱。

### 示例

```
OS10(config)# snmp-server vrf management
```

### 支持的版本

10.4.1.0 or later

## 示例：配置 SNMP

本示例显示如何配置交换机上的 SNMP，包括 SNMP 引擎 ID、视图、组和用户。

```
OS10(config)# snmp-server contact "Contact Support"
OS10(config)# snmp-server engineID remote 192.168.1.2 udp-port 502 0xdefa
OS10(config)# snmp-server engineID local test
OS10(config)# snmp-server group sngroup 2c notify notofy_view
OS10(config)# snmp-server group snv3group 3 noauth read read_view
OS10(config)# snmp-server user snuser sngroup 3 auth sha a2FubmFuX3Rlc3Q=
OS10(config)# snmp-server view readview 1.3.6.1.2.1.2.2 included
OS10(config)# snmp-server view snview .1 excluded
```

```

OS10(config)# do show snmp engineID local
Local default SNMP engineID: 0x800002a20474657374

OS10(config)# do show snmp engineID remote
Remote Engine ID IP-addr Port
0xdefa 192.168.1.2 502
OS10(config)# do show snmp group
groupname : sngroup
version : 2c
notifyview : notofy_view

groupname : snv3group
version : 3
security level : noauth
readview : read_view

OS10(config)# do show snmp user
User name : snuser
Group : sngroup
Version : 3
Authentication Protocol : SHA

OS10(config)# do show snmp view
view name : readview
OID : 1.3.6.1.2.1.2.2
included : True

view name : snview
OID : .1
excluded : True

```

## 系统时钟

OS10 使用网络时间协议 (NTP) 将系统时钟与时间服务主机同步。当您启用 NTP 时，它会覆盖系统时间。

如果不使用 NTP，请在禁用 NTP 后设置系统时间和时区。使用 `clock set` 命令可设置当前系统时间和日期。基于硬件的实时时钟时间 (RTC) 可重置新的系统时间。

世界各地的某些地理位置可在夏季时间内观察夏令时 (DST)。要配置 DST，使用 `clock timezone {standard-timezone standard-timezone-name | {timezone-string Hours Minutes}}` 命令。OS10 仅支持标准时区的 DST 功能。

OS10 仅提供用户定义的时区配置以实现向后兼容性。如果您选择配置用户定义的时区，则必须配置 UTC 的小时和分钟偏差。用户定义的时区不支持 DST。

 **注：** Dell EMC 建⋯配置在 Linux 中支持的⋯准⋯区。使用 ? 字符完成命令，以⋯看支持的⋯准⋯区的列表。

## 配置说明

如果您配置了 DST 适用的时区，并且您想要将 OS10 降级到不支持 DST 更改的较低版本，请执行以下操作之一：

- 在降级之前，请禁用 DST 配置或使用 `clock timezone` 命令更新设置，以仅指定本地时区。
- 降级完成后，忽略 CLI 错误并使用 `clock timezone` 命令重新配置设置，以仅指定本地时区。

## 配置系统时间和日期

- 以 EXEC 模式输入时间和日期。

```
clock set time year-month-day
```

- `time` — 以 `hour:minute:second` 格式输入时间，其中 `hour` 为 1 到 24；`minute` 为 1 到 60；`second` 为 1 到 60。例如，将 5:15 PM 输入为 17:15:00。
- `year-month-day` — 以 `YYYY-MM-DD` 格式输入日期，其中 `YYYY` 是四位数年份，例如 2016；`MM` 是从 1-12 的月份；`DD` 是从 1-31 的日期。

- 在 CONFIGURATION 模式下输入时区。

```
clock timezone {standard-timezone standard-timezone-name | {timezone-string Hours Minutes}}
```

- `standard-timezone-name` — 输入在 Linux 中支持的标准时区名称。要查看支持的标准时区名称列表，请参阅[时区和 UTC 偏差参考](#)部分。
- `timezone-string` — 输入时区的名称。
- `hours` — 输入 UTC 的小时偏差，范围从 -23 到 23。
- `minutes` — 输入 UTC 的分钟偏差，范围从 0 到 59。

设置时间和日期

```
OS10# clock set 13:00:00 2018-08-30
```

查看系统时间和日期

```
OS10# show clock
2018-08-30T13:01:01.45+00:00
```

设置时区

```
OS10(config)# clock timezone standard-timezone Brazil/West
```

查看配置的时区

```
OS10# show clock timezone
Brazil/West (-04, -0400)
```

在此示例中，-04:00 为巴西/西 UTC 的负偏差。

## 时区和 UTC 偏离参考

此部分列出了不同的时区和相应的 UTC 偏离。

表. 20: 时区和 UTC 偏离量

| 大陆/国家/地区 | 城市     | UTC 偏离 |
|----------|--------|--------|
| 非洲       | 阿比让    | +00:00 |
|          | 阿克拉    | +00:00 |
|          | 亚的斯亚贝巴 | +03:00 |
|          | 阿尔及尔   | +01:00 |
|          | 阿斯马拉   | +03:00 |
|          | 巴马科    | +00:00 |
|          | 班基     | +01:00 |
|          | 班珠尔    | +00:00 |
|          | 比绍     | +00:00 |
|          | 布兰太尔   | +02:00 |
|          | 布拉柴维尔  | +01:00 |
|          | 布琼布拉   | +02:00 |
|          | 开罗     | +02:00 |
|          | 卡萨布兰卡  | +01:00 |
|          | 休达     | +01:00 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市     | UTC 偏离 |
|----------|--------|--------|
|          | 科纳克里   | +00:00 |
|          | 达喀尔    | +00:00 |
|          | 达累斯萨拉姆 | +03:00 |
|          | 吉布提    | +03:00 |
|          | 杜阿拉    | +01:00 |
|          | 阿尤恩    | +00:00 |
|          | 弗里敦    | +00:00 |
|          | 哈博罗内   | +02:00 |
|          | 哈拉雷    | +02:00 |
|          | 约翰尼斯堡  | +02:00 |
|          | 朱巴     | +03:00 |
|          | 坎帕拉    | +03:00 |
|          | 喀土穆    | +02:00 |
|          | 基加利    | +02:00 |
|          | 金沙萨    | +01:00 |
|          | 克斯     | +01:00 |
|          | 利伯维尔   | +01:00 |
|          | 洛美     | +00:00 |
|          | 罗安达    | +01:00 |
|          | 卢本巴希   | +02:00 |
|          | 卢萨卡    | +02:00 |
|          | 马拉博    | +01:00 |
|          | 马普托    | +02:00 |
|          | 马塞鲁    | +02:00 |
|          | 姆巴巴纳   | +02:00 |
|          | 摩加迪休   | +03:00 |
|          | 蒙罗维亚   | +00:00 |
|          | 内罗比    | +03:00 |
|          | 恩贾梅纳   | +01:00 |
|          | 尼亚美    | +01:00 |
|          | 努瓦克肖特  | +00:00 |
|          | 瓦加杜古   | +00:00 |
|          | 波多诺伏   | +01:00 |
|          | 圣多美    | +00:00 |
|          | 廷巴克图   | +00:00 |
|          | 的黎波里   | +02:00 |
|          | 突尼斯    | +01:00 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市          | UTC 偏离 |
|----------|-------------|--------|
| 美国       | 温特和克        | +02:00 |
|          | 阿达克         | -10:00 |
|          | 安克拉治        | -09:00 |
|          | 安圭拉         | -04:00 |
|          | 安提瓜岛        | -04:00 |
|          | 阿拉瓜伊纳       | -03:00 |
|          | 阿根廷/布宜诺斯艾利斯 | -03:00 |
|          | 阿根廷/卡塔马卡    | -03:00 |
|          | 阿根廷/科摩里瓦达维亚 | -03:00 |
|          | 阿根廷/科尔多瓦    | -03:00 |
|          | 阿根廷/胡胡伊     | -03:00 |
|          | 阿根廷/拉里奥哈    | -03:00 |
|          | 阿根廷/门多萨     | -03:00 |
|          | 阿根廷/里奥加耶戈斯  | -03:00 |
|          | 阿根廷/萨尔塔     | -03:00 |
|          | 阿根廷/圣胡安     | -03:00 |
|          | 阿根廷/圣路易斯    | -03:00 |
|          | 阿根廷/图库曼     | -03:00 |
|          | 阿根廷/乌斯怀亚    | -03:00 |
|          | 阿鲁巴         | -04:00 |
|          | 亚松森         | -04:00 |
|          | 阿蒂科肯        | -05:00 |
|          | 阿特卡         | -10:00 |
|          | 巴伊亚         | -03:00 |
|          | 巴伊亚班德拉斯     | -06:00 |
|          | 巴巴多斯        | -04:00 |
|          | 贝伦          | -03:00 |
|          | 伯利兹         | -06:00 |
|          | 布朗萨布隆       | -04:00 |
|          | 博阿维斯塔       | -04:00 |
|          | 波哥大         | -05:00 |
|          | 博伊西         | -07:00 |
|          | 布宜诺斯艾利斯     | -03:00 |
|          | 剑桥湾         | -07:00 |
|          | 大坎普         | -04:00 |
|          | 坎昆          | -05:00 |
|          | 加拉加斯        | -04:00 |



表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市            | UTC 偏离 |
|----------|---------------|--------|
|          | 卡塔马卡          | -03:00 |
|          | 卡宴            | -03:00 |
|          | 开曼            | -05:00 |
|          | 芝加哥           | -06:00 |
|          | 奇瓦瓦           | -07:00 |
|          | 科勒尔港          | -05:00 |
|          | 科尔多瓦          | -03:00 |
|          | 哥斯达黎加         | -06:00 |
|          | 克雷斯頓          | -07:00 |
|          | 库亚巴           | -04:00 |
|          | 库拉索           | -04:00 |
|          | 丹马沙           | +00:00 |
|          | 道森            | -08:00 |
|          | 道森克里克         | -07:00 |
|          | 丹佛            | -07:00 |
|          | 底特律           | -05:00 |
|          | 多米尼加          | -04:00 |
|          | 埃德蒙頓          | -07:00 |
|          | 埃鲁内佩          | -05:00 |
|          | 萨尔瓦多          | -06:00 |
|          | 恩塞纳达港         | -08:00 |
|          | 纳尔逊堡          | -07:00 |
|          | 韦恩堡           | -05:00 |
|          | 堡垒            | -03:00 |
|          | 格莱斯湾          | -04:00 |
|          | 戈特霍布          | -03:00 |
|          | 古斯贝           | -04:00 |
|          | 大特克           | -05:00 |
|          | 格林纳达          | -04:00 |
|          | 瓜德罗普          | -04:00 |
|          | 危地马拉          | -06:00 |
|          | 瓜亚基尔          | -05:00 |
|          | 圭亚那           | -04:00 |
|          | 哈里法克斯         | -04:00 |
|          | 哈瓦那           | -05:00 |
|          | 埃莫西约          | -07:00 |
|          | 印地安那州/印第安纳波利斯 | -05:00 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市         | UTC 偏离 |
|----------|------------|--------|
|          | 印地安那州/诺克斯  | -06:00 |
|          | 印地安那州/马伦戈  | -05:00 |
|          | 印地安那州/圣彼得堡 | -05:00 |
|          | 印地安那州/特尔城  | -06:00 |
|          | 印地安那州/韦威   | -05:00 |
|          | 印地安那州/文森   | -05:00 |
|          | 印地安那州/威纳马克 | -05:00 |
|          | 印第安纳波利斯    | -05:00 |
|          | 因纽维克       | -07:00 |
|          | 伊魁特        | -05:00 |
|          | 牙买加        | -05:00 |
|          | 胡胡伊        | -03:00 |
|          | 朱诺         | -09:00 |
|          | 肯塔基/路易斯维尔  | -05:00 |
|          | 肯塔基/蒙蒂塞洛   | -05:00 |
|          | 诺克斯印第安那    | -06:00 |
|          | 克拉伦代克      | -04:00 |
|          | 拉巴斯        | -04:00 |
|          | 菲莱         | -05:00 |
|          | 洛杉矶        | -08:00 |
|          | 路易斯维尔      | -05:00 |
|          | 下普林赛斯      | -04:00 |
|          | 马塞约        | -03:00 |
|          | 马那瓜        | -06:00 |
|          | 玛瑙斯        | -04:00 |
|          | 马里戈特       | -04:00 |
|          | 马提尼克       | -04:00 |
|          | 马塔莫罗斯      | -06:00 |
|          | 马萨特兰       | -07:00 |
|          | 门多萨        | -03:00 |
|          | 梅诺米尼       | -06:00 |
|          | 梅里达        | -06:00 |
|          | 梅特拉卡特拉     | -09:00 |
|          | 墨西哥城       | -06:00 |
|          | 密克隆        | -03:00 |
|          | 蒙克顿        | -04:00 |
|          | 蒙特雷        | -06:00 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市           | UTC 偏离 |
|----------|--------------|--------|
|          | 蒙得维的亚        | -03:00 |
|          | 蒙特利尔         | -05:00 |
|          | 蒙特塞拉特        | -04:00 |
|          | 拿索           | -05:00 |
|          | 纽约           | -05:00 |
|          | 尼皮贡          | -05:00 |
|          | 诺姆           | -09:00 |
|          | 诺罗尼亚         | -02:00 |
|          | 美国北达科他州/比乌拉  | -06:00 |
|          | 美国北达科他州/森特   | -06:00 |
|          | 美国北达科他州/新塞勒姆 | -06:00 |
|          | 奥希纳加         | -07:00 |
|          | 巴拿马          | -05:00 |
|          | 旁纳唐          | -05:00 |
|          | 帕拉马里博        | -03:00 |
|          | 菲尼克斯         | -07:00 |
|          | 西班牙港         | -04:00 |
|          | 太子港          | -05:00 |
|          | 阿克雷港         | -05:00 |
|          | 波多韦柳         | -04:00 |
|          | 波多黎各         | -04:00 |
|          | 彭塔阿雷纳斯       | -03:00 |
|          | 雷尼河          | -06:00 |
|          | 兰金因雷特        | -06:00 |
|          | 堡礁           | -03:00 |
|          | 里贾纳          | -06:00 |
|          | 雷索卢特         | -06:00 |
|          | 里约布兰科        | -05:00 |
|          | 罗萨里奥         | -03:00 |
|          | 圣伊萨贝尔        | -08:00 |
|          | 圣塔伦          | -03:00 |
|          | 圣地亚哥         | -04:00 |
|          | 圣多明哥         | -04:00 |
|          | 圣保罗          | -03:00 |
|          | 斯科斯比湾        | -01:00 |
|          | 希普罗克         | -07:00 |
|          | 锡特卡          | -09:00 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市      | UTC 偏离 |
|----------|---------|--------|
|          | 圣巴特米    | -04:00 |
|          | 圣约翰斯    | -03:30 |
|          | 圣基茨     | -04:00 |
|          | 圣卢西亚    | -04:00 |
|          | 圣托马斯    | -04:00 |
|          | 圣文森特    | -04:00 |
|          | 斯威夫特卡伦特 | -06:00 |
|          | 特古西加尔巴  | -06:00 |
|          | 图勒      | -04:00 |
|          | 桑德贝     | -05:00 |
|          | 蒂华纳     | -08:00 |
|          | 多伦多     | -05:00 |
|          | 托托拉岛    | -04:00 |
|          | 温哥华     | -08:00 |
|          | 维尔京     | -04:00 |
|          | 怀特霍斯    | -08:00 |
|          | 温尼伯     | -06:00 |
|          | 亚库塔特    | -09:00 |
|          | 耶洛奈夫    | -07:00 |
| 南极洲      | 卡西      | +11:00 |
|          | 戴维斯     | +07:00 |
|          | 杜蒙迪维尔   | +10:00 |
|          | 麦格里     | +11:00 |
|          | 莫森      | +05:00 |
|          | 麦克默多    | +12:00 |
|          | 帕尔默     | -03:00 |
|          | 罗瑟雷     | -03:00 |
|          | 南极      | +12:00 |
|          | 昭和      | +03:00 |
|          | 特罗尔     | +00:00 |
|          | 沃斯托克    | +06:00 |
| 北极       | 朗伊尔     | +01:00 |
| 亚洲       | 亚丁      | +03:00 |
|          | 阿拉木图    | +06:00 |
|          | 安曼      | +02:00 |
|          | 阿纳德尔    | +12:00 |
|          | 阿克套     | +05:00 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市        | UTC 偏离 |
|----------|-----------|--------|
|          | 阿克托拜      | +05:00 |
|          | 阿什哈巴德     | +05:00 |
|          | 阿什喀巴德     | +05:00 |
|          | 阿特劳       | +05:00 |
|          | 巴格达       | +03:00 |
|          | 巴林        | +03:00 |
|          | 巴库        | +04:00 |
|          | 曼谷        | +07:00 |
|          | 巴尔瑙尔      | +07:00 |
|          | 贝鲁特       | +02:00 |
|          | 比什凯克      | +06:00 |
|          | 文莱        | +08:00 |
|          | 加尔各答      | +05:30 |
|          | 赤塔        | +09:00 |
|          | 乔巴山       | +08:00 |
|          | 重庆        | +08:00 |
|          | 重庆        | +08:00 |
|          | 科伦坡       | +05:30 |
|          | 达卡        | +06:00 |
|          | 大马士革      | +02:00 |
|          | 达卡        | +06:00 |
|          | 帝力        | +09:00 |
|          | 迪拜        | +04:00 |
|          | 杜尚别       | +05:00 |
|          | 法马古斯塔     | +02:00 |
|          | 加沙        | +02:00 |
|          | 哈尔滨       | +08:00 |
|          | 希伯伦       | +02:00 |
|          | 胡志明       | +07:00 |
|          | (中国) 香港地区 | +08:00 |
|          | 科布多       | +07:00 |
|          | 伊尔库茨克     | +08:00 |
|          | 伊斯坦布尔     | +03:00 |
|          | 雅加达       | +07:00 |
|          | 查亚普拉      | +09:00 |
|          | 耶路撒冷      | +02:00 |
|          | 喀布尔       | +04:30 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市           | UTC 偏离 |
|----------|--------------|--------|
|          | 勘察           | +12:00 |
|          | 卡拉奇          | +05:00 |
|          | 喀什格尔         | +06:00 |
|          | 加德满都         | +05:45 |
|          | 加德满都         | +05:45 |
|          | 维申斯克         | +09:00 |
|          | 加尔各答         | +05:30 |
|          | 克拉斯诺雅茨克      | +07:00 |
|          | 吉隆坡          | +08:00 |
|          | 古晋           | +08:00 |
|          | 科威特          | +03:00 |
|          | (中国) 澳门特别行政区 | +08:00 |
|          | (中国) 澳门特别行政区 | +08:00 |
|          | 马加丹          | +11:00 |
|          | 孟加锡          | +08:00 |
|          | 马尼拉          | +08:00 |
|          | 马斯喀特         | +04:00 |
|          | 新库兹涅茨克       | +07:00 |
|          | 西伯利亚         | +07:00 |
|          | 鄂木斯克         | +06:00 |
|          | 奥拉尔          | +05:00 |
|          | 金边           | +07:00 |
|          | 坤甸           | +07:00 |
|          | 平壤           | +09:00 |
|          | 卡塔尔          | +03:00 |
|          | 克孜洛尔达        | +05:00 |
|          | 仰光           | +06:30 |
|          | 利雅得          | +03:00 |
|          | 西贡           | +07:00 |
|          | 库页岛          | +11:00 |
|          | 撒马尔罕         | +05:00 |
|          | 首尔           | +09:00 |
|          | 上海           | +08:00 |
|          | 新加坡          | +08:00 |
|          | 中科雷姆斯克       | +11:00 |
|          | 台北           | +08:00 |
|          | 塔什干          | +05:00 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市    | UTC 偏离 |
|----------|-------|--------|
|          | 第比利斯  | +04:00 |
|          | 德黑兰   | +03:30 |
|          | 特拉维夫  | +02:00 |
|          | 廷布    | +06:00 |
|          | 廷布    | +06:00 |
|          | 东京    | +09:00 |
|          | 托木斯克  | +07:00 |
|          | 乌戎潘当  | +08:00 |
|          | 乌兰巴托  | +08:00 |
|          | 乌兰巴托  | +08:00 |
|          | 乌鲁木齐  | +06:00 |
|          | 乌斯季涅拉 | +10:00 |
|          | 万象    | +07:00 |
|          | 海参崴   | +10:00 |
|          | 雅库茨克  | +09:00 |
|          | 仰光    | +06:30 |
|          | 叶卡捷琳堡 | +05:00 |
|          | 耶烈万   | +04:00 |
| 大西洋      | 亚速尔群岛 | -01:00 |
|          | 百慕大   | -04:00 |
|          | 卡纳里   | +00:00 |
|          | 佛得角   | -01:00 |
|          | 法罗    | +00:00 |
|          | 法罗    | +00:00 |
|          | 扬马延   | +01:00 |
|          | 马德拉   | +00:00 |
|          | 雷克雅未克 | +00:00 |
|          | 南乔治亚  | -02:00 |
|          | 圣赫勒拿  | +00:00 |
|          | 斯坦利   | -03:00 |
| 澳大利亚     | ACT   | +10:00 |
|          | 阿德莱德  | +09:30 |
|          | 布里斯班  | +10:00 |
|          | 布罗肯希尔 | +09:30 |
|          | 堪培拉   | +10:00 |
|          | 柯里    | +10:00 |
|          | 达尔文   | +09:30 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市      | UTC 偏离 |
|----------|---------|--------|
|          | 尤克拉     | +08:45 |
|          | 霍巴特     | +10:00 |
|          | LHI     | +10:30 |
|          | 林德曼     | +10:00 |
|          | 豪勋爵     | +10:30 |
|          | 墨尔本     | +10:00 |
|          | 诺斯      | +09:30 |
|          | 新南威尔士   | +10:00 |
|          | 珀斯      | +08:00 |
|          | 昆士兰     | +10:00 |
|          | 南部区     | +09:30 |
|          | 悉尼      | +10:00 |
|          | 塔斯马尼亚   | +10:00 |
|          | 维多利亚    | +10:00 |
|          | 东部      | +08:00 |
|          | 洋科维那    | +09:30 |
| 巴西       | 阿卡      | -05:00 |
|          | 迪诺罗尼亚   | -02:00 |
|          | 东部      | -03:00 |
|          | 东部      | -04:00 |
| 加拿大      | 大西洋     | -04:00 |
|          | Central | -06:00 |
|          | 伊斯坦堡    | -05:00 |
|          | 芒廷      | -07:00 |
|          | 纽芬兰     | -03:30 |
|          | 太平洋     | -08:00 |
|          | 萨斯喀彻温省  | -06:00 |
|          | 育空      | -08:00 |
| CET      |         | +01:00 |
| 智利       | 大陆      | -04:00 |
|          | 复活节岛    | -06:00 |
| CST6CDT  |         | -05:00 |
| 古巴       |         | -06:00 |
| EET      |         | -05:00 |
| 埃及       |         | +02:00 |
| 爱尔兰      |         | +02:00 |
| EST      |         | +00:00 |



表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区      | 城市    | UTC 偏离 |
|---------------|-------|--------|
| EST5EDT       |       | -05:00 |
| Etc/GMT       |       | -05:00 |
| Etc/GMT + 0   |       | +00:00 |
| Etc/GMT + +1  |       | +00:00 |
| Etc/GMT + +10 |       | -01:00 |
| Etc/GMT + +11 |       | -10:00 |
| Etc/GMT + +12 |       | -11:00 |
| Etc/GMT + +2  |       | -12:00 |
| Etc/GMT + +3  |       | -02:00 |
| Etc/GMT + +4  |       | -03:00 |
| Etc/GMT + +5  |       | -04:00 |
| Etc/GMT + +6  |       | -05:00 |
| Etc/GMT + +7  |       | -06:00 |
| Etc/GMT + +8  |       | -07:00 |
| Etc/GMT + +9  |       | -08:00 |
| Etc/GMT0      |       | -09:00 |
| Etc/GMT-0     |       | +00:00 |
| Etc/GMT-1     |       | +00:00 |
| Etc/GMT-10    |       | +01:00 |
| Etc/GMT-11    |       | +10:00 |
| Etc/GMT-12    |       | +11:00 |
| Etc/GMT-13    |       | +12:00 |
| Etc/GMT-14    |       | +13:00 |
| Etc/GMT-2     |       | +14:00 |
| Etc/GMT-3     |       | +02:00 |
| Etc/GMT-4     |       | +03:00 |
| Etc/GMT-5     |       | +04:00 |
| Etc/GMT-6     |       | +05:00 |
| Etc/GMT-7     |       | +06:00 |
| Etc/GMT-8     |       | +07:00 |
| Etc/GMT-9     |       | +08:00 |
| Etc/格林威治      |       | +09:00 |
| Etc/UCT       |       | +00:00 |
| Etc/通用        |       | +00:00 |
| Etc/UTC       |       | +00:00 |
| Etc/祖鲁        |       | +00:00 |
| 欧洲            | 阿姆斯特丹 | +00:00 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市     | UTC 偏离 |
|----------|--------|--------|
|          | 安道尔    | +01:00 |
|          | 阿斯特拉罕  | +01:00 |
|          | 雅典     | +04:00 |
|          | 贝尔法斯特  | +02:00 |
|          | 贝尔格莱德  | +00:00 |
|          | 柏林     | +01:00 |
|          | 伯拉第斯拉瓦 | +01:00 |
|          | 布鲁塞尔   | +01:00 |
|          | 布加勒斯特  | +01:00 |
|          | 布达佩斯   | +02:00 |
|          | 布辛根    | +01:00 |
|          | 基希讷乌   | +01:00 |
|          | 哥本哈根   | +02:00 |
|          | 都柏林    | +01:00 |
|          | 直布罗陀   | +00:00 |
|          | 根西岛    | +01:00 |
|          | 赫尔辛基   | +00:00 |
|          | 地曼岛    | +02:00 |
|          | 伊斯坦布尔  | +00:00 |
|          | 泽西     | +03:00 |
|          | 加里宁格勒  | +00:00 |
|          | 基辅     | +02:00 |
|          | 基洛夫    | +02:00 |
|          | 里斯本    | +03:00 |
|          | 卢布尔雅那  | +00:00 |
|          | 伦敦     | +01:00 |
|          | 卢森堡    | +00:00 |
|          | 马德里    | +01:00 |
|          | 马耳他    | +01:00 |
|          | 玛丽港    | +01:00 |
|          | 明斯克    | +02:00 |
|          | 摩纳哥    | +03:00 |
|          | 莫斯科    | +01:00 |
|          | 尼科西亚   | +03:00 |
|          | 奥斯陆    | +02:00 |
|          | 巴黎     | +01:00 |
|          | 波德戈里察  | +01:00 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区     | 城市      | UTC 偏离 |
|--------------|---------|--------|
|              | 布拉格     | +01:00 |
|              | 里加      | +02:00 |
|              | 罗马      | +01:00 |
|              | 萨马拉     | +04:00 |
|              | 圣马力诺    | +01:00 |
|              | 萨拉热窝    | +01:00 |
|              | 萨拉托夫    | +04:00 |
|              | 辛菲罗波尔   | +03:00 |
|              | 斯科普里    | +01:00 |
|              | 索非亚     | +02:00 |
|              | 斯德哥尔摩   | +01:00 |
|              | 塔林      | +02:00 |
|              | 地拉那     | +01:00 |
|              | 蒂拉斯波尔   | +02:00 |
|              | 乌里扬诺夫斯克 | +04:00 |
|              | 乌日哥罗德   | +02:00 |
|              | 瓦杜兹     | +01:00 |
|              | 梵蒂冈城国   | +01:00 |
|              | 维也纳     | +01:00 |
|              | 维尔纽斯    | +02:00 |
|              | 格勒      | +04:00 |
|              | 华沙      | +01:00 |
|              | 萨格勒布    | +01:00 |
|              | 扎波罗热    | +02:00 |
|              | 苏黎世     | +01:00 |
| GB           |         | +00:00 |
| 英国-爱尔兰       |         | +00:00 |
| GMT          |         | +00:00 |
| GMT+0        |         | +00:00 |
| GMT0         |         | +00:00 |
| GMT-0        |         | +00:00 |
| 格林威治时间       |         | +00:00 |
| (中国) 香港特别行政区 |         | +08:00 |
| HST          |         | -10:00 |
| 冰岛           |         | +00:00 |
| 印度           | 塔那那利佛   | +03:00 |
|              | 查戈斯     | +06:00 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市    | UTC 偏离 |
|----------|-------|--------|
|          | 圣诞    | +07:00 |
|          | 科科斯   | +06:30 |
|          | 科摩罗   | +03:00 |
|          | 凯尔盖朗  | +05:00 |
|          | 马埃    | +04:00 |
|          | 马尔代夫  | +05:00 |
|          | 毛里求斯  | +04:00 |
|          | 马约特   | +03:00 |
|          | 留尼旺岛  | +04:00 |
| 伊朗       |       | +03:30 |
| 以色列      |       | +02:00 |
| 牙买加      |       | -05:00 |
| 日本       |       | +09:00 |
| 夸贾林环礁    |       | +12:00 |
| 利比亚      |       | +02:00 |
| MET      |       | +01:00 |
| 墨西哥      | 巴哈诺特  | -08:00 |
|          | 包姚苏尔  | -07:00 |
|          | 总则    | -06:00 |
| MST      |       | -07:00 |
| MST7MDT  |       | -07:00 |
| 纳瓦霍      |       | -07:00 |
| NZ       |       | +12:00 |
| NZ-CHAT  |       | +12:45 |
| 太平洋      | 阿皮亚   | +13:00 |
|          | 奥克兰   | +12:00 |
|          | 布甘维尔  | +11:00 |
|          | 查塔姆   | +12:45 |
|          | 楚克    | +10:00 |
|          | 复活节   | -06:00 |
|          | 埃法特   | +11:00 |
|          | 恩德伯里  | +13:00 |
|          | 法考福   | +13:00 |
|          | 斐济    | +12:00 |
|          | 富那富提  | +12:00 |
|          | 加拉帕戈斯 | -06:00 |
|          | 冈比耶   | -09:00 |

表. 20: 时区和 UTC 偏离量 (续)

| 大陆/国家/地区 | 城市     | UTC 偏离 |
|----------|--------|--------|
|          | 瓜达康纳尔岛 | +11:00 |
|          | 关岛     | +10:00 |
|          | 火奴鲁鲁   | -10:00 |
|          | 约翰斯顿   | -10:00 |
|          | 基里巴斯   | +14:00 |
|          | 科斯雷    | +11:00 |
|          | 夸贾林环礁  | +12:00 |
|          | 马朱罗    | +12:00 |
|          | 玛贵斯    | -09:30 |
|          | 中途岛    | -11:00 |
|          | 瑙鲁     | +12:00 |
|          | 纽埃岛    | -11:00 |
|          | 诺福克    | +11:00 |
|          | 努美阿    | +11:00 |
|          | 帕果-帕果  | -11:00 |
|          | 帕劳     | +09:00 |
|          | 皮特凯恩群岛 | -08:00 |
|          | 波纳佩    | +11:00 |
|          | 波纳佩    | +11:00 |
|          | 摩尔斯比港  | +10:00 |
|          | 拉罗汤加   | -10:00 |
|          | 塞班岛    | +10:00 |
|          | 萨摩亚    | -11:00 |
|          | 塔希提    | -10:00 |
|          | 塔拉瓦    | +12:00 |
|          | 汤加塔布   | +13:00 |
|          | 特鲁克    | +10:00 |
|          | 韦克     | +12:00 |
|          | 瓦利斯    | +12:00 |
|          | 雅蒲岛    | +10:00 |
| 波兰       |        | +01:00 |
| 葡萄牙      |        | +00:00 |
| PRC      |        | +08:00 |
| PST8PDT  |        | -08:00 |
| ROC      |        | +08:00 |
| ROK      |        | +09:00 |
| 新加坡      |        | +08:00 |

表. 20: 时区和 UTC 偏离量 （续）

| 大陆/国家/地区 | 城市       | UTC 偏离 |
|----------|----------|--------|
| 土耳其      |          | +03:00 |
| UCT      |          | +00:00 |
| 通用       |          | +00:00 |
| US       | 阿拉斯加     | -09:00 |
|          | 阿留申      | -10:00 |
|          | 亚利桑那     | -07:00 |
|          | Central  | -06:00 |
|          | 伊斯坦堡     | -05:00 |
|          | 东-印地安州   | -05:00 |
|          | 夏威夷      | -10:00 |
|          | 印地安那-斯塔克 | -06:00 |
|          | 密歇根      | -05:00 |
|          | 芒廷       | -07:00 |
|          | 太平洋      | -08:00 |
|          | 太平洋-新    | -08:00 |
|          | 萨摩亚      | -11:00 |
| UTC      |          | +00:00 |
| WET      |          | +00:00 |
| W-SU     |          | +03:00 |
| 祖鲁       |          | +00:00 |

## 系统时钟命令

### clock set

设置系统时间。

|        |                                                                                               |                                                                                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>clock set time year-month-day</code>                                                    |                                                                                                                                                                          |
| 参数     | <b>时间</b>                                                                                     | 以 <code>hour:minute:second</code> 格式输入 <code>time</code> ，其中 <code>hour</code> 是 1-24； <code>minute</code> 是 1-60； <code>second</code> 是 1-60。例如，将 5:15 PM 输入为 17:15:00。 |
|        | <b>year-month-day</b>                                                                         | 以 <code>YYYY-MM-DD</code> 格式输入 <code>year-month-day</code> ，其中 <code>YYYY</code> 是四位数字的年份，例如 2016； <code>MM</code> 是从 1-12 的月份； <code>DD</code> 是从 1-31 的日期。             |
| 默认     | 未配置                                                                                           |                                                                                                                                                                          |
| 命令模式   | EXEC                                                                                          |                                                                                                                                                                          |
| 使用情况信息 | 如果系统时钟与 NTP 时间不同步，请使用此命令重置系统时间。基于硬件的实时时钟时间 (RTC) 将重置为新时间。新的系统时钟设置将立即生效。                       |                                                                                                                                                                          |
|        | 从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。 |                                                                                                                                                                          |
| 示例     | <pre>OS10# clock set 18:30:10 2017-01-25</pre>                                                |                                                                                                                                                                          |

支持的版本 10.2.1E or later

clock timezone

配置 OS10 应用于系统时钟顶部的标准或用户定义的时区。

|        |                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>clock timezone {standard-timezone standard-timezone-name   {timezone-string hours minutes}}</code>                                                                                                                                                                                                                                                                                         |
| 参数     | <ul style="list-style-type: none"><li><code>standard-timezone-name</code> — 输入 Linux 中支持的标准时区名称。要查看支持的标准时区名称列表，请参阅<a href="#">时区和 UTC 偏差参考</a>部分。</li><li><code>timezone-string</code> — 输入时区的名称。</li><li><code>hours</code> — 输入 UTC 的小时偏差，范围从 -23 到 23。</li><li><code>minutes</code> — 输入 UTC 的分钟偏差，范围从 0 到 59。</li></ul>                                                                      |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                              |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                    |
| 使用情况信息 | <p>标准时区选项应用所选标准时区的预定义偏差，包括适用于本地时间的 DST 更改。配置此命令后，OS10 会在所有日志和时间戳中使用更新后的本地时间。您可以使用 <code>?</code> 字符或按 <code>tab</code> 键以完成命令，并查看支持的时区列表。要查看支持的时区名称列表，请参阅<a href="#">时区和 UTC 偏差参考</a>部分。在字符串末尾定义“/”区域名称。“/”字符指示时区字符串后跟区域名称。例如，“Asia/Calcutta”。命令的 <code>no</code> 形式将 UTC 的本地时间重置为 UTC。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p> |

示例

```
OS10(config)# clock timezone standard-timezone Brazil/West
```

支持的版本 10.3.0E 或更高版本

show clock

显示当前的系统时钟设置。

|        |                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show clock</code>                                                                                                                               |
| 参数     | 无                                                                                                                                                     |
| 默认     | 未配置                                                                                                                                                   |
| 命令模式   | EXEC                                                                                                                                                  |
| 使用情况信息 | <p>协调通用时间 (UTC) 值是您的时区晚或早于 UTC/格林尼治平均时间的小时数。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p> |

示例

```
OS10# show clock
2017-01-25T11:00:31.68-08:00
```

支持的版本 10.2.1E or later

show clock timezone

显示系统中配置的时区。

|    |                                  |
|----|----------------------------------|
| 语法 | <code>show clock timezone</code> |
| 参数 | 无                                |
| 默认 | Etc/UTC                          |

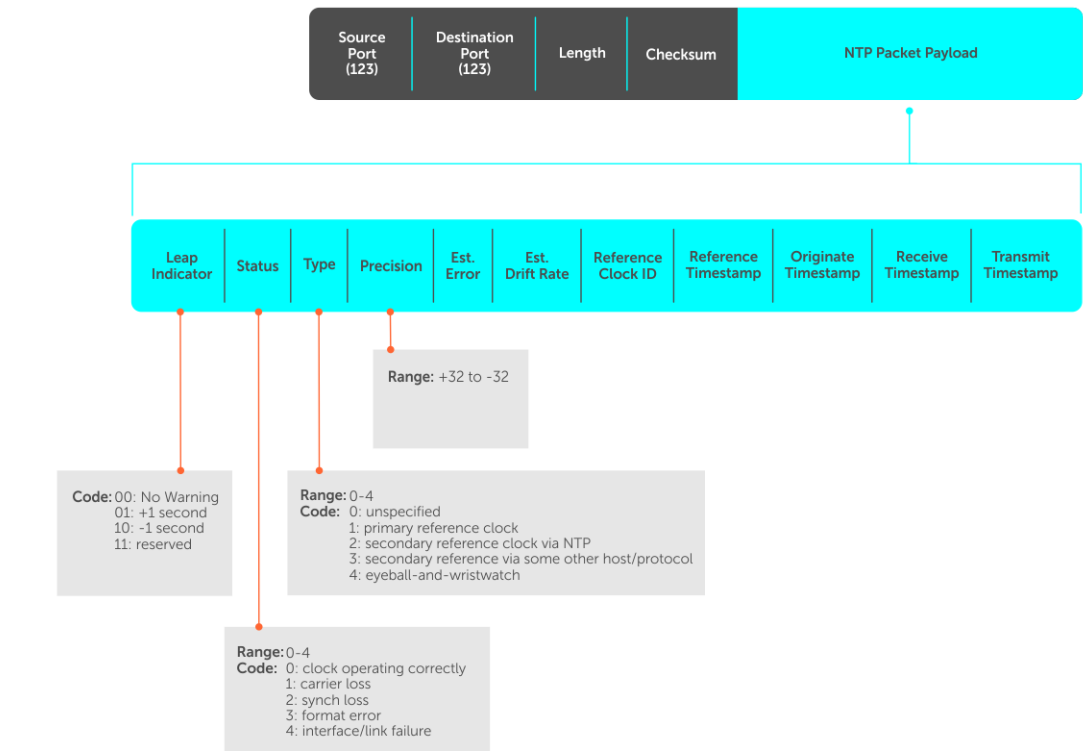
|        |                                                                                           |
|--------|-------------------------------------------------------------------------------------------|
| 命令模式   | EXEC                                                                                      |
| 使用情况信息 | 从版本 10.5.0.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。 |
| 示例     | <pre>OS10# show clock timezone Brazil/West (-04, -0400)</pre>                             |
| 支持的版本  | 10.5.0 or later                                                                           |

## 网络时间协议

网络时间协议 (NTP) 在一组分布式时间服务器和客户端之间同步计时。该协议可以协调大型的多样化网络中的时间分布。NTP 客户端与提供准确时间测量的 NTP 服务器进行同步。NTP 客户端从几个 NTP 服务器中进行选择，以确定哪个可提供最佳的可用时间源和可靠的信息传输。

为获得正确的时间，OS10 将与时间服务主机同步。对于当前时间，您可以将系统设置为轮询特定 NTP 时间服务主机。在这些时间提供服务的主机上，系统将选择一个 NTP 主机与之同步，并充当 NTP 主机的客户端。建立主机客户端关系后，网络设备将在其本地网络中传播时间信息。

NTP 客户端将消息发送到一个或多个服务器，并根据收到的方式处理答复。NTP 消息中包含的信息将允许每个客户端/服务器对等方确定其他对等方的计时特征，包括其时钟的预期精度。使用此信息，每个对等方从几个其他时钟中选择最佳时间、更新本地时钟，并估计其准确性。



**注:** OS10 同时支持 NTP 服务器和客户端角色。

## 启用 NTP

默认情况下，NTP 处于禁用状态。要启用 NTP，请配置系统同步的 NTP 服务器。要配置多个服务器，请多次输入命令。多个服务器可能会影响 CPU 资源。



- 在 CONFIGURATION 模式下输入系统同步的 NTP 服务器的 IP 地址。

```
ntp server ip-address
```

### 查看系统时钟状态

```
OS10(config)# do show ntp status
system peer: 0.0.0.0
system peer mode: unspec
leap indicator: 11
stratum: 16
precision: -22
root distance: 0.00000 s
root dispersion: 1.28647 s
reference ID: [73.78.73.84]
reference time: 00000000.00000000 Mon, Jan 1 1900 0:00:00.000
system flags: monitor ntp kernel stats
jitter: 0.000000 s
stability: 0.000 ppm
broadcastdelay: 0.000000 s
authdelay: 0.000000 s
```

### 查看计算的 NTP 同步变量

```
OS10(config)# do show ntp associations
=====
remote local st poll reach delay offset disp
=====
10.16.150.185 10.16.151.123 16 1024 0 0.00000 0.000000 3.99217
OS10# show ntp associations
=====
remote local st poll reach delay offset disp
=====
10.16.150.185 10.16.151.123 16 1024 0 0.00000 0.000000 3.99217
```

## 转播

接收时间信息的广播，并在系统中设置接口，以通过广播接收 NTP 信息。默认情况下，在所有活动接口上启用 NTP。如果禁用某个接口上的 NTP，系统会丢弃发送到该接口的任何 NTP 数据包。

- 设置接口以接收处于 INTERFACE 模式的 NTP 数据包。

```
ntp broadcast client
```

- 在 INTERFACE 模式下禁用接口上的 NTP。

```
ntp disable
```

### 配置 NTP 广播

```
OS10(config)# interface ethernet 1/1/10
OS10(conf-if-eth1/1/10)# ntp broadcast client
```

### 禁用 NTP 广播

```
OS10(config)# interface ethernet 1/1/10
OS10(conf-if-eth1/1/10)# ntp disable
```

## 源 IP 地址

配置要包含在所有 NTP 数据包中的一个接口 IP 地址。NTP 数据包的源地址是系统在默认情况下用于访问网络的接口 IP 地址。

- 在 CONFIGURATION 模式下配置 NTP 数据包的源 IP 地址。

```
ntp source interface
```

- o ethernet node/slot/port[:subport] — 输入以太网接口信息。

- o `port-channel channel-id` — 输入端口通道 ID, 从 1 到 128。
- o `vlan vlan-id` — 输入 VLAN ID 号, 从 1 到 4093。
- o `loopback id` — 输入环回接口 ID 号, 从 0 到 16383。
- o `mgmt node/slot/port` — 输入管理接口的物理端口接口。默认值为 1/1/1。

## 配置源 IP 地址

```
OS10(config)# ntp source ethernet 1/1/10
```

## 查看源 IP 配置

```
OS10(config)# do show running-configuration | grep source
ntp source ethernet1/1/1
```

# 身份验证

NTP 身份验证和相应的受信任密钥可为具有受信任时间源的 NTP 数据包提供可靠的交换。NTP 身份验证首先在密钥配置后创建第一个 NTP 数据包。NTP 身份验证使用消息摘要 5 (MD5) 算法。密钥嵌入在发送到 NTP 时间源的同步数据包中。

1. 在 CONFIGURATION 模式下启用 NTP 身份验证。

```
ntp authenticate
```

2. 在 CONFIGURATION 模式下设置身份验证密钥编号和密钥, 从 1 到 4294967295。

```
ntp authentication-key number md5 key
```

- 必须匹配 `ntp trusted-key` 命令中的数字。
- `key` 是加密的字符串。

3. 在 CONFIGURATION 模式下定义受信任密钥, 从 1 到 4294967295。此 `number` 必须与 `ntp trusted-key` 命令中的编号匹配。

```
ntp trusted-key number
```

4. 在 CONFIGURATION 模式下配置 NTP 服务器。

```
ntp server {hostname | ipv4-address | ipv6-address} [key keyid] [prefer]
```

- `hostname` — 输入关键字以查看远程设备的 IP 地址或主机名称。
- `ipv4-address` — 采用 A.B.C.D 格式输入 IPv4 地址。
- `ipv6-address` — 采用 `nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn` 格式输入 IPv6 地址。支持零省音。
- `key keyid` — 输入文本字符串作为 NTP 服务器与客户端之间交换的密钥。
- `prefer` — 输入关键字以将此 NTP 服务器设置为首选服务器。

5. 在 CONFIGURATION 模式下, 配置 NTP 的主节点并输入标识 NTP 服务器层次结构的层次编号, 从 2 到 10。默认值为 8。

```
ntp master {2-10}
```

## 配置 NTP

```
OS10(config)# ntp authenticate
OS10(config)# ntp trusted-key 345
OS10(config)# ntp authentication-key 345 md5 0 5A60910FED211F02
OS10(config)# ntp server 1.1.1.1 key 345
OS10(config)# ntp master 7
```

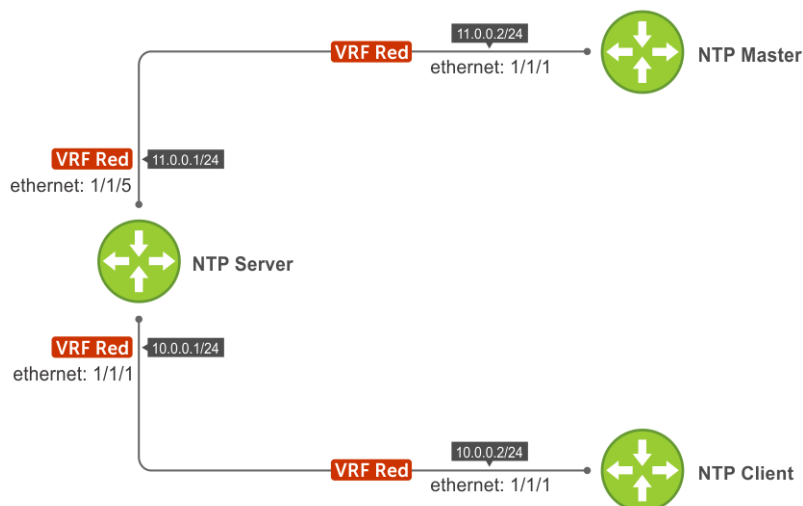
## 查看 NTP 配置

```
OS10(config)# do show running-configuration
!
ntp authenticate
ntp authentication-key 345 md5 0 5A60910FED211F02
ntp server 1.1.1.1 key 345
ntp trusted-key 345
```

```
ntp master 7
...
```

## 示例 NTP 配置

以下示例显示了通过非默认 VRF 实例 (VRF Red) 连接的 NTP 主节点 r (11.0.0.2)、服务器 (10.0.0.1) 和客户端 (10.0.0.2)。OS10 用作 NTP 服务器，以使其时钟与非默认 VRF 实例中的可用 NTP 主节点保持同步，并为 NTP 中的客户端提供时间。



要创建此示例 NTP 配置，请执行以下操作：

### 1. 配置 NTP 服务器：

#### a. 创建非默认 VRF 实例并为 VRF 分配接口。

```
OS10(config-vrf)# exit
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# no switchport
OS10(config-if-eth1/1/1)# ip vrf forwarding red
OS10(config-if-eth1/1/1)# ip address 10.0.0.1/24
OS10(config-if-eth1/1/1)# exit
OS10(config)# interface ethernet 1/1/5
OS10(config-if-eth1/1/5)# no switchport
OS10(config-if-eth1/1/5)# ip vrf forwarding red
OS10(config-if-eth1/1/5)# ip address 11.0.0.1/24
OS10(config-if-eth1/1/5)# exit
OS10(config)#
```

#### b. 在 NTP 服务器上配置 NTP 主节点 IP 地址。（在此示例中，NTP 主节点 11.0.0.2 只能通过 VRF Red 访问。）

```
OS10(config)# ntp server 11.0.0.2
OS10(config)# do show running-configuration ntp
ntp server 11.0.0.2
OS10(config)#
```

#### c. 在 VRF Red 实例中配置 NTP。

```
OS10(config)# ntp enable vrf red

"% Warning: NTP server/client will be disabled in default VRF and enabled on a red VRF"
Do you wish to continue? (y/n): y

OS10(config)#
OS10(config)# do show running-configuration ntp
ntp server 11.0.0.2
ntp enable vrf red
OS10(config)#
```

## 2. 配置 NTP 客户端:

### a. 创建非默认 VRF 实例并为 VRF 分配接口。

```
OS10(config)# ip vrf red
OS10(conf-vrf)# exit
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# ip vrf forwarding red
OS10(conf-if-eth1/1/1)# ip address 10.0.0.2/24
OS10(conf-if-eth1/1/1)# exit
OS10(config)#
```

### b. 在 NTP 客户端上配置 NTP 服务器 IP 地址。

```
OS10(config)# ntp server 10.0.0.1
OS10(config)# do show running-configuration ntp
ntp server 10.0.0.1
OS10(config)#
```

### c. 在 VRF Red 实例中配置 NTP。

```
OS10(config)# ntp enable vrf red

"% Warning: NTP server/client will be disabled in default VRF and enabled on a red
VRF"
Do you wish to continue? (y/n): y

OS10(config)# do show running-configuration ntp
ntp server 10.0.0.1
ntp enable vrf red
OS10(config)#
```

## 3. 配置 NTP 主节点:

### a. 创建非默认 VRF 实例并为 VRF 分配接口。

```
OS10(config)# ip vrf red
OS10(conf-vrf)# exit
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# ip vrf forwarding red
OS10(conf-if-eth1/1/1)# ip address 11.0.0.2/24
OS10(conf-if-eth1/1/1)# exit
OS10(config)#
```

### b. 将 NTP 配置为主节点。

```
OS10(config)# ntp master
OS10(config)# do show running-configuration ntp
ntp master 8
OS10(config)#
```

### c. 在 VRF Red 实例中配置 NTP。

```
OS10(config)# ntp enable vrf red

"% Warning: NTP server/client will be disabled in default VRF and enabled on a red
VRF"
Do you wish to continue? (y/n): y

OS10(config)# do show running-configuration ntp
ntp master 8
ntp enable vrf red
OS10(config)#
```

## 4. 验证 NTP 客户端 (10.0.0.2) 是否连接到在 VRF Red 中运行的 NTP 服务器 (10.0.0.1)。

```
OS10# show ntp associations vrf red

 remote refid st t when poll reach delay offset jitter
=====
```

```
*10.0.0.1 11.0.0.2 10 u 2 64 1 0.578 -1.060 0.008

OS10# show ntp status vrf red
associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
system peer: 10.0.0.1:123
system peer mode: client
leap indicator: 00
stratum: 11
log2 precision: -24
root delay: 0.991
root dispersion: 1015.099
reference ID: 10.0.0.1
reference time: dbc7b087.5d47aaa6 Sat, Nov 5 2016 1:12:39.364
system jitter: 0.000000
clock jitter: 0.462
clock wander: 0.003
broadcast delay: -50.000
symm. auth. delay: 0.000
OS10#
```

## 5. 验证 NTP 服务器 (10.0.0.1) 是否连接到正在 VRF Red 中运行的 NTP 主节点 (11.0.0.2)。

```
OS10(config)# do show ntp associations vrf red

 remote refid st t when poll reach delay offset jitter
=====
LOCAL(0) .LOCL. 8 1 111 64 2 0.000 0.000 0.000
*11.0.0.2 LOCAL(0) 9 u 43 64 3 0.441 0.026 0.047

OS10(config)# do show ntp status vrf red
associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
system peer: 11.0.0.2:123
system peer mode: client
leap indicator: 00
stratum: 10
log2 precision: -24
root delay: 0.441
root dispersion: 950.580
reference ID: 11.0.0.2
reference time: dbc7b03e.733f51d7 Sat, Nov 5 2016 1:11:26.450
system jitter: 0.000000
clock jitter: 0.009
clock wander: 0.000
broadcast delay: -50.000
symm. auth. delay: 0.000
OS10(config)#
```

# NTP 命令

## ntp authenticate

允许对设备与 NTP 时间服务主机的之间的 NTP 流量进行身份验证。

**语法** ntp authenticate

**参数** 无

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 您还必须使用 ntp authentication-key 命令为 NTP 流量配置身份验证密钥。

从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 no 版本将禁用 NTP 身份验证。

|       |                                |
|-------|--------------------------------|
| 示例    | OS10(config)# ntp authenticate |
| 支持的版本 | 10.2.0E or later               |

## ntp authenticate-key

为受信任的时间源配置身份验证密钥。

|        |                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | ntp authenticate-key <i>number</i> md5 [ <i>0</i>   <i>7</i> ] <i>key</i>                                                                                                                                   |
| 参数     | <ul style="list-style-type: none"> <li><i>number</i> — 输入身份验证密钥编号，从 1 到 4294967295。</li> <li>md5 — 设置为 MD5 加密。</li> <li>0 — 设置为未加密格式（默认值）。</li> <li>7 — 设置为隐藏加密。</li> <li><i>key</i> — 输入身份验证密钥。</li> </ul> |
| 默认     | 0                                                                                                                                                                                                           |
| 命令模式   | CONFIGURATION                                                                                                                                                                                               |
| 使用情况信息 | <p>身份验证数字必须与 ntp trusted-key 命令中配置的 <i>number</i> 参数相同。使用 ntp authenticate 命令启用 NTP 身份验证。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p>          |

|       |                                                      |
|-------|------------------------------------------------------|
| 示例    | OS10(config)# ntp authentication-key 1200 md5 0 dell |
| 支持的版本 | 10.2.0E or later                                     |

## ntp broadcast client

配置接口以便从 NTP 服务器接收 NTP 广播。

|        |                                              |
|--------|----------------------------------------------|
| 语法     | ntp broadcast client                         |
| 参数     | 无                                            |
| 默认     | 未配置                                          |
| 命令模式   | INTERFACE                                    |
| 使用情况信息 | 此命令的 no 版本将禁用广播。                             |
| 示例     | OS10(conf-if-eth1/1/1)# ntp broadcast client |
| 支持的版本  | 10.2.0E or later                             |

## ntp disable

默认情况下，在所有接口上已启用 NTP。禁用 NTP 可阻止接口接收 NTP 数据包。

|        |                                                                  |
|--------|------------------------------------------------------------------|
| 语法     | ntp disable                                                      |
| 参数     | 无                                                                |
| 默认     | 已启用                                                              |
| 命令模式   | INTERFACE                                                        |
| 使用情况信息 | 使用此命令可将 OS10 配置为不侦听特定服务器并阻止接口接收 NTP 数据包。此命令的 no 版本将在接口上重新启用 NTP。 |

|       |                                       |
|-------|---------------------------------------|
| 示例    | OS10(config-if-eth1/1/7)# ntp disable |
| 支持的版本 | 10.2.0E or later                      |

## ntp enable vrf

为管理或非默认 VRF 实例启用 NTP。

|        |                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | ntp enable vrf {management   vrf vrf-name}                                                                                                         |
| 参数     | <ul style="list-style-type: none"> <li>management — 输入关键字以启用管理 VRF 实例的 NTP。</li> <li>vrf vrf-name — 输入关键字和 VRF 的名称，以对该非默认 VRF 实例启用 NTP。</li> </ul> |
| 默认     | 已禁用                                                                                                                                                |
| 命令模式   | CONFIGURATION                                                                                                                                      |
| 使用情况信息 | 此命令的 no 版本将禁用管理 VRF 实例的 NTP。                                                                                                                       |
| 示例     | <pre>OS10(config)# ntp enable vrf management OS10(config)# ntp enable vrf vrf-blue</pre>                                                           |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                               |

## ntp master

配置 NTP 主服务器。

|        |                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------|
| 语法     | ntp master stratum                                                                                                               |
| 参数     | stratum — 输入层次编号以标识 NTP 服务器的层次结构，从 2 到 10。                                                                                       |
| 默认     | 8                                                                                                                                |
| 命令模式   | CONFIGURATION                                                                                                                    |
| 使用情况信息 | <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持</p> <p>此命令的 no 版本会将该值重置为默认值。</p> |
| 示例     | <pre>OS10(config)# ntp master 6</pre>                                                                                            |
| 支持的版本  | 10.2.0E or later                                                                                                                 |

## ntp server

配置 NTP 时间服务主机。

|      |                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | ntp server {hostname   ipv4-address   ipv6-address} [key keyid] [prefer]                                                                                                                                                                                                |
| 参数   | <ul style="list-style-type: none"> <li>hostname — 输入服务器的主机名称。</li> <li>ipv4-address   ipv6-address — 以 A.B.C.D 格式输入 IPv4 地址，以 A::B 格式输入 NTP 服务器的 IPv6 地址。</li> <li>key keyid — （可选）输入 NTP 对等密钥 ID，从 1 到 4294967295。</li> <li>prefer — （可选）将此对等节点配置为优先于其他服务器。</li> </ul> |
| 默认   | 未配置                                                                                                                                                                                                                                                                     |
| 命令模式 | CONFIGURATION                                                                                                                                                                                                                                                           |

|               |                                                                                                                                                                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>使用情况信息</b> | <p>您可以配置多个时间服务主机。在这些时间服务主机上，系统将选择一个 NTP 主机进行同步。要确定要选择的服务器，请使用 <code>show ntp associations</code> 命令。Dell EMC 建议限制您配置的主机的数量，因为许多轮询至 NTP 主机可能会影响网络性能。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持</p> |
| <b>示例</b>     | <pre>OS10(config)# ntp server eureka.com</pre>                                                                                                                                                                                                              |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                                                                                                                                            |

## ntp source

配置要包括在 NTP 数据包中的接口 IP 地址。

|               |                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ntp source interface</code>                                                                                                                                                                                                                                                                                                                                                                             |
| <b>参数</b>     | <p><code>interface</code> — 设置接口类型：</p> <ul style="list-style-type: none"> <li><code>ethernet node/slot/port[:subport]</code> — 输入以太网接口信息。</li> <li><code>port-channel id-number</code> — 输入端口通道号，从 1 到 128。</li> <li><code>vlan vlan-id</code> — 输入 VLAN 号，从 1 到 4093。</li> <li><code>loopback loopback-id</code> — 输入环回接口编号，从 0 到 16383。</li> <li><code>mgmt node/slot/port</code> — 输入管理端口接口信息。</li> </ul> |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本将移除配置。                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>示例</b>     | <pre>OS10(config)# ntp source ethernet 1/1/24</pre>                                                                                                                                                                                                                                                                                                                                                           |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                              |

## ntp trusted-key

设置密钥以验证 NTP 与之同步的系统。

|               |                                                                                                                                                                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ntp trusted-key number</code>                                                                                                                                                                                                                                                                    |
| <b>参数</b>     | <code>number</code> — 输入受信任的密钥 ID，从 1 到 4294967295。                                                                                                                                                                                                                                                    |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                    |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                                                                                                                                                                                          |
| <b>使用情况信息</b> | <p><code>number</code> 参数中的数值必须与 <code>ntp authentication-key</code> 命令中的 <code>number</code> 参数相同。如果更改 <code>ntp authentication-key</code> 命令，则还必须更改此命令。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持</p> <p>此命令的 <code>no</code> 版本将移除密钥。</p> |
| <b>示例</b>     | <pre>OS10(config)# ntp trusted-key 234567</pre>                                                                                                                                                                                                                                                        |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                                                                                                                                                                                       |

## show ntp associations

显示 NTP 主节点和对等节点。

|           |                                                                      |
|-----------|----------------------------------------------------------------------|
| <b>语法</b> | <code>show ntp associations [vrf {management   vrf vrf-name}]</code> |
|-----------|----------------------------------------------------------------------|



**参数**

- `management` — 输入关键字以显示与管理 VRF 实例对应的 NTP 信息。
- `vrf vrf-name` — 输入关键字，然后是 VRF 的名称，以显示与该非默认 VRF 实例对应的 NTP 信息。

**默认** 未配置

**命令模式** EXEC

**使用情况信息**

- `(none)` — 以下一个或多个符号显示：
  - `*` — 同步到此对等节点。
  - `#` — 几乎已同步到此对等节点。
  - `+` — 已为可能的同步选择对等节点。
  - `-` — 对等节点是选择的候选项。
  - `~` — 对等节点已进行静态配置。
- `remote` — NTP 对等节点的远程 IP 地址。
- `ref clock` — 远程对等参考时钟的 IP 地址。
- `st` — 对等层，即离开外部时间源的跳数。16 表示 NTP 对等节点无法访问时间源。
- `when` — 上次设备收到 NTP 数据包的时间。
- `poll` — 轮询间隔（以秒为单位）。
- `reach` — 可访问八进制比特流中的对等节点。
- `delay` — 数据包完成往返到 NTP 时间源的时间间隔或延迟（以毫秒为单位）。
- `offset` — NTP 对等节点的时钟到网络设备时钟的相对时间（以毫秒为单位）。
- `disp` — 分散。

从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持

**示例**

```
OS10# show ntp associations
remote ref clock st when poll reach delay offset disp
=====
 10.10.120.5 0.0.0.0 16 - 256 0 0.00 0.000 16000.0
*172.16.1.33 127.127.1.0 11 6 16 377 -0.08 -1499.9 104.16
 172.31.1.33 0.0.0.0 16 - 256 0 0.00 0.000 16000.0
 192.200.0.2 0.0.0.0 16 - 256 0 0.00 0.000 16000.0
```

```
OS10# show ntp associations vrf management
remote local st poll reach delay offset disp
=====
*1.1.1.2 1.1.1.1 3 64 1 0.00027 0.000056 0.43309
```

**支持的版本** 10.2.0E or later

show ntp status

显示 NTP 配置信息。

**语法** `show ntp status [vrf {management | vrf vrf-name}]`

**参数**

- `status` — (可选) 查看 NTP 状态。
- `vrf management` — (可选) 输入关键字，以显示与管理 VRF 对应的 NTP 信息。
- `vrf vrf-name` — (可选) 输入关键字，然后输入 VRF 的名称，以显示与该非默认 VRF 对应的 NTP 信息。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持

**示例 (状态)**

```
OS10# show ntp status
system peer: 0.0.0.0
system peer mode: unspec
```

```

leap indicator: 11
stratum: 16
precision: -22
root distance: 0.00000 s
root dispersion: 1.28647 s
reference ID: [73.78.73.84]
reference time: 00000000.00000000 Mon, Jan 1 1900 0:00:00.000
system flags: monitor ntp kernel stats
jitter: 0.000000 s
stability: 0.000 ppm
broadcastdelay: 0.000000 s
authdelay: 0.000000 s

```

```

OS10# show ntp status vrf management
system peer: 1.1.1.2
system peer mode: client
leap indicator: 00
stratum: 4
precision: -23
root distance: 0.00027 s
root dispersion: 0.94948 s
reference ID: [1.1.1.2]
reference time: ddc78084.f17ea38b Tue, Nov 28 2017 6:28:20.943
system flags: ntp kernel stats
jitter: 0.000000 s
stability: 0.000 ppm
broadcastdelay: 0.000000 s
authdelay: 0.000000 s
OS10#

```

```

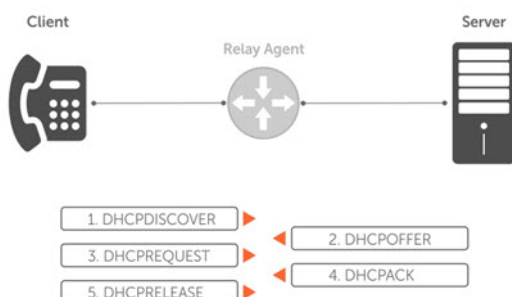
OS10# show ntp status vrf red
associd=0 status=0618 leap_none, sync_ntp, 1 event, no_sys_peer,
system peer: 11.0.0.2:123
system peer mode: client
leap indicator: 00
stratum: 10
log2 precision: -24
root delay: 0.338
root dispersion: 1136.790
reference ID: 11.0.0.2
reference time: dbc7a951.f7978096 Sat, Nov 5 2016 0:41:53.967
system jitter: 0.000000
clock jitter: 0.003
clock wander: 0.001
broadcast delay: -50.000
symm. auth. delay: 0.000

```

**支持的版本** 10.2.0E or later

## 动态主机配置协议

动态主机配置协议 (DHCP) 是一种应用程序层协议，可基于配置策略网络管理员的决定，动态地将 IP 地址和其他配置参数分配到网络终端站（也称为主机）。



|          |                                              |
|----------|----------------------------------------------|
| DHCP 服务器 | 网络设备为客户端提供配置参数。                              |
| DHCP 客户端 | 从服务器请求配置参数的网络设备。                             |
| 中继代理     | 当服务器与主机不在同一子网中时，在客户端和服务器之间传递 DHCP 消息的中间网络设备。 |

## 数据包格式和选项

DHCP 服务器将侦听端口 67 并传输到端口 68。DHCP 客户端将侦听端口 68 并传输到端口 67。

在 DHCP 数据包格式中，配置参数是 DHCP 数据包中的选项，格式为类型、长度、值 (TLV)。要限制服务器提供的参数数量，主机将输入其所需的参数，并且服务器仅发送这些参数。DHCP 使用用户数据报协议 (UDP) 作为其传输协议。



以下选项通常在 DHCP 数据包中使用。

| DHCP 选项          | 说明                                                                                                                                                                                                                                 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 子网掩码             | 1 — 客户端的子网掩码                                                                                                                                                                                                                       |
| 路由器              | 3 — 用作客户端的默认网关的路由器 IP 地址                                                                                                                                                                                                           |
| 域名服务器            | 6 — 客户端可用的域名服务器 (DNS)                                                                                                                                                                                                              |
| Domain name (域名) | 15 — 客户端用于通过 DNS 解析主机名称的域名                                                                                                                                                                                                         |
| IP 地址租用时间        | 51 — 客户端使用分配的 IP 地址的时间量                                                                                                                                                                                                            |
| DHCP 消息类型        | 53: <ul style="list-style-type: none"><li>1 — DHCPDISCOVER</li><li>2 — DHCPOFFER</li><li>3 — DHCPREQUEST</li><li>4 — DHCPDECLINE</li><li>5 — DHCPACK</li><li>6 — DHCPNACK</li><li>7 — DHCPRELEASE</li><li>8 — DHCPINFORM</li></ul> |
| 参数请求列表           | 55 — 服务器请求 DHCP 客户端的参数。这是一系列八位字节，其中每个八位组是 DHCP 选项代码                                                                                                                                                                                |
| 续订时间             | 58 — 授予 IP 地址后，客户端将尝试使用原始服务器续订其租赁的时间量                                                                                                                                                                                              |
| 重新绑定时间           | 59 — 授予 IP 地址后，客户端尝试使用任何服务器续订其租赁的时间量（如果原始服务器不响应）                                                                                                                                                                                   |
| 供应商类标识符          | 60 — 用户定义的字符串，中继代理用于将 DHCP 客户端数据包转发到特定 DHCP 服务器                                                                                                                                                                                    |
| DHCP 中继代理信息选项    | 82 — 帮助保护通过 DHCP 中继代理进行的 DHCP 流量，并确保 DHCP 中继代理与 DHCP 服务器之间的通信不会受到影响。                                                                                                                                                               |
| 用户端口堆叠           | 230 — 设置 DHCP 服务时提供 DHCP 服务器堆栈端口详细信息的堆栈选项变量                                                                                                                                                                                        |
| End              | 255 — DHCP 数据包中最后一个选项的信号                                                                                                                                                                                                           |

## DHCP 服务器

动态主机配置协议 (DHCP) 服务器根据请求向 DHCP 客户端提供网络配置参数。DHCP 服务器会动态地将四个必要的 IP 参数分配给虚拟局域网 (VLAN) 上的每台计算机 — IP 地址、网络掩码、默认网关和名称服务器地址。DHCP IP 地址分配可在服务器为客户端/服务器模型分配地址池中的 IP 信息的客户端/服务器模式下工作。

DHCP 自动执行到网络设备的网络参数分配。即使在小型网络中，DHCP 也可以更轻松地将新设备添加到网络。DHCP 访问服务提供基于服务器的集中式设置，以将客户端添加到网络。此设置意味着您无需手动创建和维护客户端的 IP 地址分配。

使用 DHCP 管理主机之间的池或 IP 地址时，您可以减少所需的 IP 地址数量。DHCP 管理 IP 地址池，方法是在有限的时段将 IP 地址租用给主机，使 DHCP 服务器可以共享有限数量的 IP 地址。DHCP 还提供连接到网络的设备的中央数据库，并消除重复的资源分配。

## 自动地址分配

自动地址分配是一种地址分配方法，可供 DHCP 服务器从可用地址池中为客户端租用 IP 地址。您不能在 DHCP 池配置下配置空 DHCP 池。为成功提交，您必须具有网络声明或主机/硬件地址（手动绑定）配置。IP 地址池是 DHCP 服务器分配的地址范围。子网编号将为地址池创建索引。

1. 在 DHCP <POOL> 模式下的接口上启用 DHCP 服务器分配的动态地址。

```
ip dhcp server
```

2. 在 DHCP 模式下创建 IP 地址池并提供名称。

```
pool name
```

3. 在 DHCP <POOL> 模式下，输入 DHCP 服务器可将地址分配到的子网。network 选项指定子网地址。prefix-length 选项指定地址的网络部分使用的位数，从 18 到 31。

```
network network/prefix-length
```

4. 在 DHCP <POOL> 模式下，输入上面指定的子网中的 IP 地址范围，DHCP 服务器使用该地址分配地址。

```
range {ip-address1 [ip-address2]}
```

 **注：**配置至少一个接口以匹配配置的网络池之一。当某个接口的 IP 地址包含在为网络池定义子网中时，它将匹配该网络池。例如，IP 地址为 10.1.1.1/24 的接口与配置有网络 10.1.1.0/24 的池相匹配。

### DHCP 服务器自动地址分配

```
OS10(config)# ip dhcp server
OS10(config-dhcp)# pool Dell
OS10(config-dhcp-Dell)# default-router 20.1.1.1
OS10(config-dhcp-Dell)# network 20.1.1.0/24
OS10(config-dhcp-Dell)# range 20.1.1.2 20.1.1.8
```

### 显示正在运行的配置

```
OS10(conf-dhcp-Dell)# do show running-configuration
...
!
ip dhcp server
!
pool Dell
network 20.1.1.0/24
default-router 20.1.1.1
range 20.1.1.2 20.1.1.8
```

## 地址租用时间

使用 `lease {days [hours] [minutes] | infinite}` 命令配置地址租用时间。默认值为 24 小时。

```
OS10(config)# ip dhcp server
OS10(config-dhcp)# pool Dell
OS10(config-dhcp-Dell)# lease 36
```

## 默认网关

确保默认路由器的 IP 地址与客户端位于同一子网中。

1. 在 CONFIGURATION 模式下启用接口上 DHCP 服务器分配的动态地址。

```
ip dhcp server
```

2. 在 DHCP 模式下创建 IP 地址池并提供名称。

```
pool name
```

3. 在 DHCP <POOL> 模式下按优先级顺序输入子网上客户端的默认网关。

```
default-router address
```

### 更改默认网关名称

```
OS10(config)# ip dhcp server
OS10(config-dhcp)# pool Dell
OS10(config-dhcp-Dell)# default-router 20.1.1.1
```

## 启用 DHCP 服务器

在 CONFIGURATION 模式下使用 `ip dhcp server` 命令在接口上启用 DHCP 服务器分配的动态地址。DHCP 服务器在默认设置下已禁用。

```
OS10(config)# ip dhcp server
OS10(config-dhcp)# no disable
```

## 主机名称解析

您有两种方法可用于主机名称解析 — 域名服务器 (DNS) 或 NetBIOS Windows 互联网命名服务 (WINS)。DHCP 和 WINS 客户端都会查询 IP 服务器，以将主机名称与 IP 地址进行比较。

1. 在 DHCP <POOL> 模式下的接口上启用 DHCP 服务器分配的动态地址。

```
ip dhcp server
```

2. 在 DHCP 模式下创建 IP 地址池并输入名称。

```
pool name
```

3. 在 DHCP <POOL> 模式下创建一个域并输入域名。

```
domain-name name
```

4. 在 DHCP <POOL> 模式下按照 DHCP 客户端可用的优先级顺序输入 DNS 服务器。

```
dns-server address
```

## DNS 地址解析

```
OS10(config)# ip dhcp server
OS10(conf-dhcp)# pool Dell
OS10(conf-dhcp-Dell)# domain-name dell.com
OS10(conf-dhcp-Dell)# dns-server 192.168.1.1
```

## NetBIOS WINS 地址解析

DHCP 客户端可以是四种类型的 NetBIOS 节点之一 — 广播、对等、组合或混合。Dell EMC 建议将混合用作 NetBIOS 节点类型。

1. 在 DHCP <POOL> 模式下的接口上启用 DHCP 服务器分配的动态地址。

```
ip dhcp server
```

2. 在 DHCP 模式下创建 IP 地址池并输入池名称。

```
pool name
```

3. 在 DHCP <POOL> 模式下按照 DHCP 客户端可用的优先级顺序输入 NetBIOS WINS 名称服务器。

```
netbios-name-server ip-address
```

4. 在 DHCP <POOL> 模式下输入关键字 Hybrid 作为 NetBIOS 节点类型。

```
netbios-node-type type
```

### 配置 NetBIOS WINS 地址解析

```
OS10(config)# ip dhcp server
OS10(conf-dhcp)# pool Dell
OS10(conf-dhcp-Dell)# netbios-name-server 192.168.10.5
OS10(conf-dhcp-Dell)# netbios-node-type Hybrid
```

## 手动绑定条目

地址绑定是客户端的 IP 地址与介质访问控制 (MAC) 地址之间的映射。DHCP 服务器会自动为客户端分配可用的 IP 地址，然后在绑定表中创建一个条目。您还可以手动为客户端创建一个条目。手动绑定有助于保证特定网络设备接收特定 IP 地址。

将手动绑定视为单个主机地址池。手动绑定数没有限制，但您只能为每个主机配置一个手动绑定。手动绑定条目不会显示在 show ip dhcp binding 输出中。

1. 在 DHCP 模式下创建地址池。

```
pool name
```

2. 在 DHCP <POOL> 模式下输入客户端 IP 地址。

```
host address
```

3. 在 DHCP <POOL> 模式下输入客户端硬件地址。

```
hardware-address hardware-address
```

### 配置手动绑定

```
OS10(config)# ip dhcp server
OS10(conf-dhcp)# pool static
OS10(conf-dhcp-static)# host 20.1.1.2
OS10(conf-dhcp-static)# hardware-address 00:01:e8:8c:4d:0a
```

### 查看 DHCP 绑定表

```
OS10# show ip dhcp binding
IP Address Hardware address Lease expiration Hostname
```

```
+-----+
11.1.1.254 00:00:12:12:12:12 Jan 27 2016 06:23:45

Total Number of Entries in the Table = 1
```

使用固定主机配置（也称为手动绑定），您必须配置具有匹配子网的网络池。静态主机到 MAC 地址映射池通过子网配置从网络池中继承网络掩码，包括主机的地址范围。

在下面的示例中，池 `host1` 是固定主机映射池，将从池 `hostnetwork` 中继承子网和其他属性，这是 DHCP 客户端 IP 地址池。`host2` 没有匹配的网络池。因此，具有 MAC 地址 `00:0c:29:aa:22:f4` 的 DHCP 客户端无法获得正确的参数。

```
OS10# show running-configuration interface ethernet 1/1/2
!
interface ethernet1/1/2
no shutdown
no switchport
ip address 100.1.1.1/24
flowcontrol receive off

OS10# show running-configuration ip dhcp
!
ip dhcp server
no disable
!
pool host1
host 100.1.1.34
hardware-address 00:0c:29:ee:4c:f4
!
pool hostnetwork
lease infinite
network 100.1.1.0/24
!
pool host2
host 20.1.1.34
hardware-address 00:0c:29:aa:22:f4
```

## DHCP 中继代理

即使客户端和服务端位于不同的 IP 网络上，DHCP 中继代理也会在远程 DHCP 服务器上转发 DHCP 消息。您可以配置远程 DHCP 服务器的 IP 地址。

您可以将设备配置为 DHCP 服务器或 DHCP 中继代理程序，但不能同时配置。

如果在 VRF 之间没有泄漏路由，DHCP 中继代理支持多虚拟路由和转发 (VRF) 实例。面向客户端和面向服务器的接口必须在同一 VRF 中。

DHCPv6 中继代理执行与 DHCP 中继代理相同的角色，但与 IPv6 网络中的相同。DHCP 中继代理会将 DHCPv4/DHCPv6 消息从配置的接口作为单播消息转发到 DHCPv6 服务器。DHCP 中继代理随后会将服务器的响应转发到客户端。

在接口上配置 DHCPv6 中继时，您必须：

- 在接口上配置 IPv6 地址。
- 确保 DHCPv6 服务器可访问。

## 用于安全保护的选项 82

DHCP（由 RFC 2131 定义）不提供身份验证或安全机制。为提供安全保护，DHCP 中继代理支持选项 82（具有线路 ID 子选项），即接收客户端请求的接口的可打印名称。

此选项可保护通过 DHCP 中继代理进行的所有 DHCP 流量，并确保 DHCP 中继代理与 DHCP 服务器之间的通信不会受到影响。

DHCP 中继代理在将 DHCP 数据包转发到 DHCP 服务器之前插入选项 82。DHCP 服务器包含选项 82，并返回到中继代理的响应。中继代理使用此信息将答复转发到接收请求的接口，而不是使其在整个 VLAN 泛洪。但是，在将响应转发给客户端之前，中继代理会从其 DHCP 响应中删除选项 82。

 **注：** 选项 82 受支持，但不可配置。

## 查看 DHCP 信息

使用 `show ip dhcp binding` 命令可查看 DHCP 绑定表条目。

```
OS10# show ip dhcp binding
 IP Address Hardware address Lease expiration Hostname
+-----+-----+-----+-----+
11.1.1.254 00:00:12:12:12:12 Jan 27 2016 06:23:45
Total Number of Entries in the Table = 1
```

## 系统域名和列表

如果您输入了部分域，则系统会搜索不同的域以完成或完全限定该部分域。完全限定的域名 (FQDN) 是以句点或句号结束的任何名称。

OS10 首先将搜索主机表以解析部分域。主机表同时包含静态配置和动态学习的主机和 IP 地址。如果 OS10 无法解析域，则会尝试为本地系统分配的域名。如果这不能解析部分域，系统会搜索配置的域列表。

您最多可以配置 `ip domain-list` 命令五次，以输入可能的域名列表。系统将按配置的顺序搜索域名，直至找到匹配项或列表耗尽。

1. 在 CONFIGURATION 模式下输入域名，最多 64 个字母数字字符。

```
ip domain-name name
```

2. 添加名称以在 CONFIGURATION 模式下完成非限定主机名称。

```
ip domain-list name
```

您可以配置与非默认 VRF 实例对应的域名和列表。

1. 在 CONFIGURATION 模式下输入与非默认 VRF 实例对应的域名。

```
ip domain-name vrf vrf-name server-name
```

2. 添加名称以完成与非默认 VRF 实例对应的非限定主机名称。

```
ip domain-list vrf vrf-name name
```

### 配置本地系统域名和列表

```
OS10(config)# ip domain-name ntengg.com
OS10(config)# ip domain-list dns1
OS10(config)# ip domain-list dns2
OS10(config)# ip domain-list dns3
OS10(config)# ip domain-list dns4
OS10(config)# ip domain-list dns5
```

```
OS10(config)# ip domain-name vrf vrf-blue ntengg.com
OS10(config)# ip domain-list vrf vrf-blue dns1
OS10(config)# ip domain-list vrf vrf-blue dns2
OS10(config)# ip domain-list vrf-vrfblue dns3
OS10(config)# ip domain-list vrf vrf-blue dns4
OS10(config)# ip domain-list vrf vrf-blue dns5
```

### 查看本地系统域名信息

```
OS10# show running-configuration

! Version 10.2.9999E
! Last configuration change at Feb 20 04:50:33 2017
!
username admin password 6q9QBeYjZ$jfxzVqGhxxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWlIgNs5BKH.
aaa authentication system:local
```



```
ip domain-name dell.com
ip domain-list fl0.com
ip name-server 1.1.1.1 2::2
ip host dell-fl0.com 10.10.10.10
snmp-server community public read-only
snmp-server contact http://www.dell.com/support/
snmp-server location United States
debug radius false
```

## DHCP 侦听

DHCP 侦听是一种第 2 层安全功能，可帮助网络设备监控 DHCP 消息并阻止不受信任的或流氓 DHCP 服务器。

在交换机上启用 DHCP 侦听后，交换机将开始监控可信 DHCP 服务器和 DHCP 客户端之间的所有事务，并使用该信息构建 DHCP 侦听绑定表。您可以配置连接到 DHCP 服务器的接口以作为可信接口。默认情况下，所有其他接口都不受信任。

DHCP 侦听绑定表包含以下信息：

- 客户端 IP 地址
- 客户端 MAC 地址
- 面向客户端的接口
- 客户端 VLAN
- 租赁时间
- DHCP 绑定类型 — 静态或动态

交换机将连接到交换机上的可信接口的 DHCP 服务器视为合法服务器。当交换机在不受信任的接口上收到 DHCP 服务器启动的数据包（UDP 目标端口 67）时，它会丢弃数据包。

当交换机收到 DHCP 续订、释放或拒绝来自客户端的消息时，它将检查 DHCP 侦听绑定表是否匹配。如果 DHCP 消息中的信息与表格匹配，交换机会将消息转发至 DHCP 服务器。如果信息不匹配，交换机会将客户端解释为未经授权的客户端，并丢弃数据包。

当出现以下情况之一时，DHCP 侦听交换机将移除动态了解的 DHCP 侦听绑定条目：

- 租赁到期
- 从客户端收到 DHCP RELEASE 数据包
- 从客户端收到 DHCP DECLINE 数据包
- 用户操作，例如 DHCP 清除或禁用 DHCP 侦听

您可以使用 CLI 添加静态 DHCP 侦听绑定条目。如果为客户端添加静态条目，则同一客户端存在的任何动态条目都将被覆盖。如果交换机收到 DHCP RELEASE 或 DHCP DECLINE 数据包，则交换机不会移除静态条目。

默认情况下，在 VLAN 上全局禁用并启用 DHCP 侦听。要使 DHCP 侦听功能正常工作，请在全局范围内启用该功能。

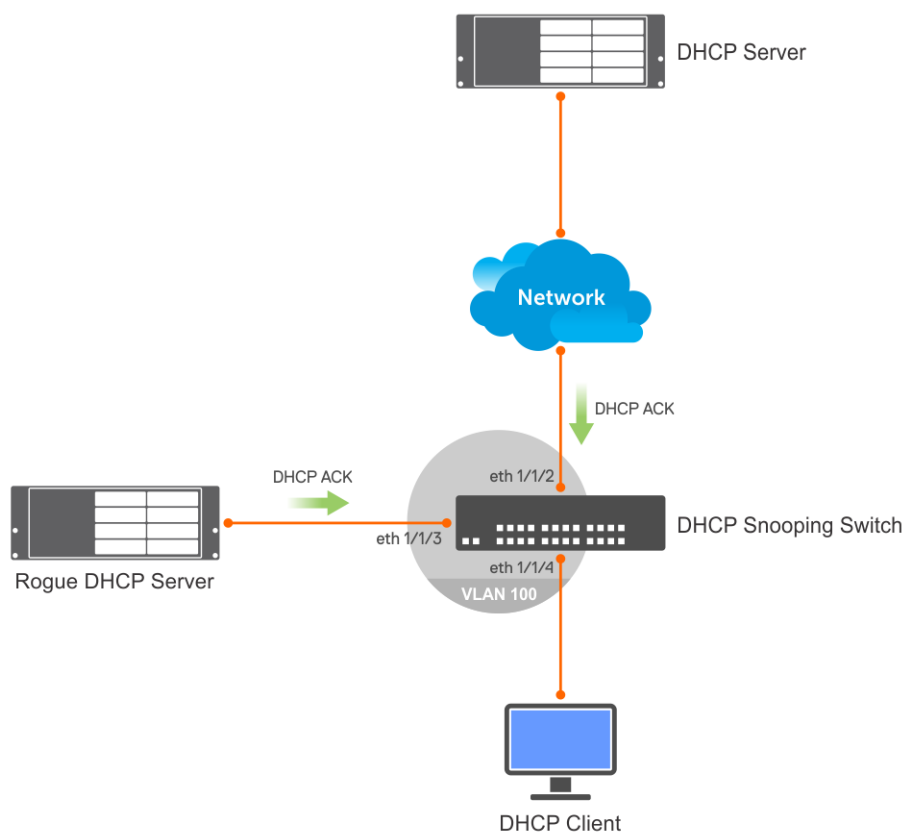
 **注：**如果将 DHCP 客户端从不受信任的接口移至 VLAN 中的另一个不受信任的接口，DHCP 侦听绑定数据不会更新。交换机将丢弃来自客户端的后续数据包。但是，如果您将 DHCP 客户端从不受信任的接口移到受信任的接口，不会来自客户端的流量。

### 对 DHCP 侦听的限制

- 管理 VLAN 不支持 DHCP 侦听。
- VxLAN 桥不支持 DHCP 侦听。
- 受支持的 DHCP 侦听绑定条目的最大数量为 4000。
- OS10 不支持多跳 DHCP 侦听。
- 要使 DHCP 侦听功能正常工作，请确保 DHCP 服务器支持选项 82 (RFC 3046)。
- 启用 DHCP 服务器上的选项 82 (RFC 3046)，以使 DHCP 侦听功能正常工作。

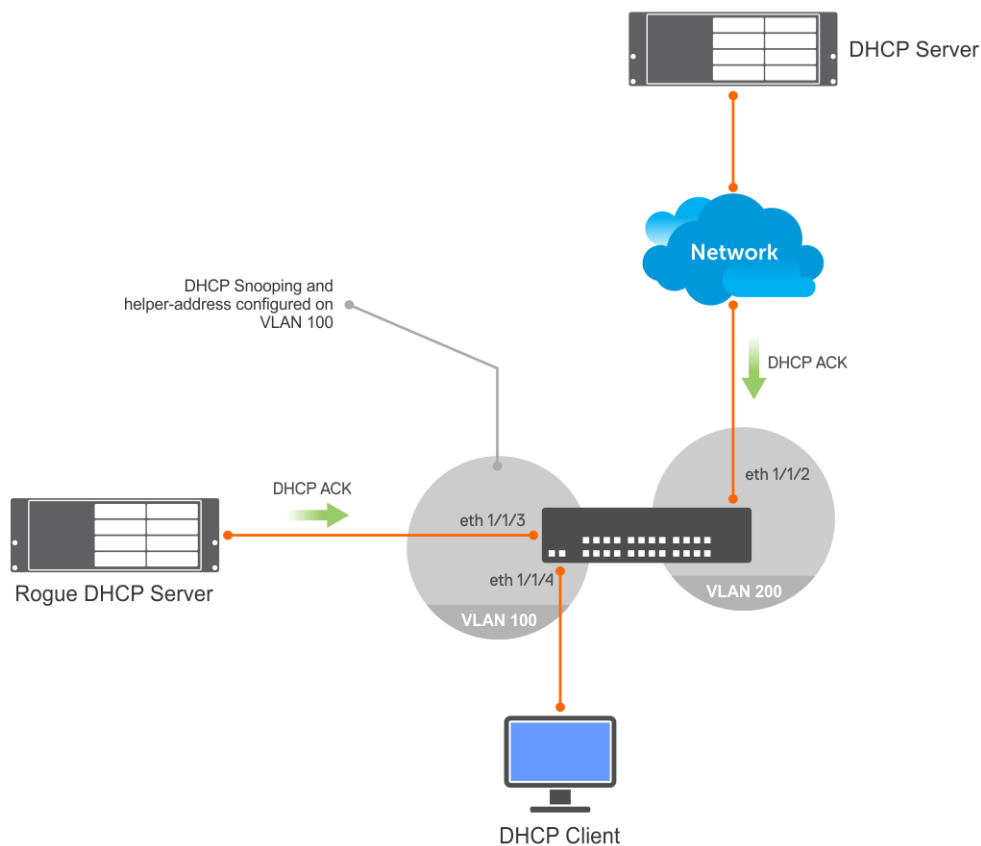
### 流氓 DHCP 服务器检测

在下面的拓扑中，受信任的 DHCP 服务器、DHCP 客户端和流氓 DHCP 服务器将连接到 DHCP 侦听交换机。DHCP 客户端和 DHCP 服务器位于同一 VLAN 上。物理接口 eth 1/1/2 是受信任的接口。当流氓 DHCP 服务器向客户端发送 DHCP 数据包时，交换机会分析该数据包。由于流氓服务器连接到交换机至不受信任的 eth 1/1/3 接口，交换机将服务器视为流氓 DHCP 服务器，并丢弃数据包。



### DHCP 侦听和 DHCP 中继

在下面的拓扑中，DHCP 侦听交换机是 VLAN 100 上 DHCP 客户端的 DHCP 中继代理。通过 eth 1/1/2 可从 VLAN 200 访问 DHCP 服务器。交换机将客户端 DHCP 消息转发到受信任的 DHCP 服务器。在将 DHCP 数据包转发到 DHCP 客户端之前，交换机会从 DHCP 服务器中处理 DHCP 数据包。当流氓服务器连接到不受信任的 eth 1/1/3 接口时，交换机将丢弃来自该接口的 DHCP 数据包。



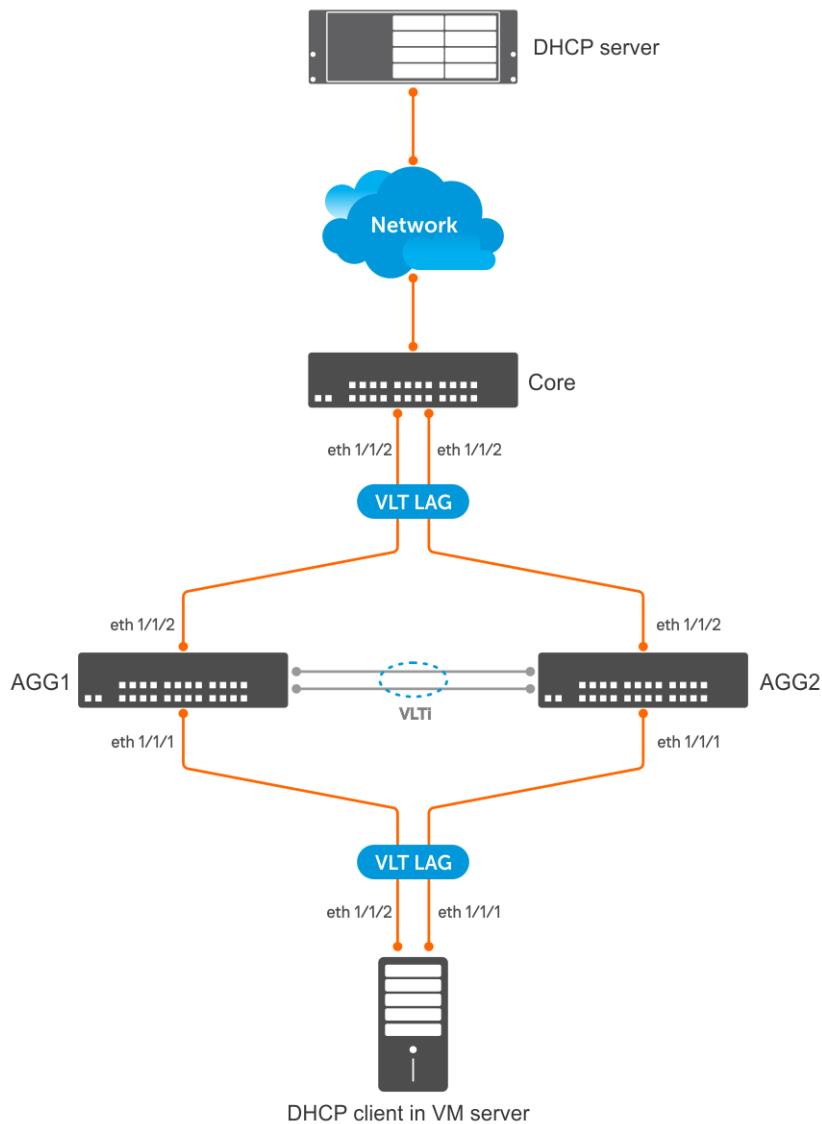
## VLT 环境中的 DHCP 侦听

OS10 在 VLT 环境中支持 DHCP 侦听。VLT 拓扑中的 DHCP 侦听交换机将在交换机之间同步 DHCP 侦听绑定信息。系统将 VLT 对等节点之间的 VLT<sub>i</sub> 链路解释为受信任的接口。要在 VLT 环境中配置 DHCP 侦听，请执行以下操作：

- 在两个 VLT 对等节点上启用 DHCP 侦听。
- 将面向 DHCP 服务器的 VLT 端口通道接口配置为受信任接口。

在下面的 VLT 拓扑中，AGG1 和 AGG2 是 VLT 对等节点，并且将 VLT 端口通道接口连接到虚拟机服务器和 CORE 交换机。通过 CORE 交换机可以访问 DHCP 服务器。下文介绍了 VLT 环境中 DHCP 侦听的功能：

- 其中一个 VLT 对等节点会通过 VLT 端口通道接口从 VM 服务器上的 DHCP 客户端接收 DHCP 客户端数据包。交换机将处理此数据包。
- VLT 对等节点通过 VLT 端口通道接口将 DHCP 客户端数据包转发到 CORE 交换机。
- CORE 交换机将 DHCP 回复数据包从 DHCP 服务器转发到其中一个 VLT 对等节点，以处理数据包。
- 如果 DHCP 回复数据包来自受信任的 DHCP 服务器，则 VLT 对等节点会将回复数据包转发到虚拟机服务器上的 DHCP 客户端。
- VLT 对等节点将同步 DHCP 侦听绑定表。



## 全局启用和配置 DHCP 侦听

1. 在 CONFIGURATION 模式下，全局启用 DHCP 侦听。

```
ip dhcp snooping
```

2. 在 INTERFACE 模式下，将连接到 DHCP 服务器的物理或端口通道接口指定为受信任。

```
ip dhcp snooping trust
```

## 在绑定表中添加静态 DHCP 侦听条目

- 在 CONFIGURATION 模式下，在绑定表中添加静态 DHCP 侦听条目。

```
ip dhcp snooping binding mac mac-address vlan vlan-id ip ip-address interface
[ethernet slot/port/sub-port | port-channel port-channel-id | VLTi]
```

## 添加静态 DHCP 侦听条目的示例

```
OS10(config)# ip dhcp snooping binding mac 00:04:96:70:8a:12 vlan 100 ip 100.1.1.2
interface ethernet 1/1/4
```

## 从绑定表中移除静态 DHCP 侦听条目

- 在 CONFIGURATION 模式下从绑定表中移除静态 DHCP 侦听条目。

```
no ip dhcp snooping binding mac mac-address vlan vlan-id interface [ethernet slot/
port/sub-port | port-channel port-channel-id]
```

在绑定表中移除静态 DHCP 侦听条目的示例

```
OS10(config)# no ip dhcp snooping binding mac 00:04:96:70:8a:12 vlan 100 ip 100.1.1.2
interface ethernet 1/1/4
```

从 DHCP 侦听绑定表中清除动态了解的条目

- 在 EXEC 模式下使用以下命令：

```
clear ip dhcp snooping binding [mac mac-address] [vlan vlan-id] [interface {ethernet
slot/port/sub-port | port-channel port-channel-id}]
```

 **小心:** 使用 `clear ip dhcp snooping binding` 命令清除 DHCP 侦听绑定表还会清除系统上的源地址验证 (SAV) 和动态 ARP 检查 (DAI) 条目。这会影响连接到已启用 DHCP 侦听的 VLAN 的客户端的流量。

从 DHCP 侦听绑定表中清除动态了解的条目的示例

以下示例将清除与 MAC 地址 04:56:79:86:73:fe 关联的所有动态 DHCP 侦听绑定条目

```
OS10# clear ip dhcp snooping binding mac 04:56:79:86:73:fe
```

以下示例将清除与 VLAN 100 关联的所有动态 DHCP 侦听绑定条目：

```
OS10# clear ip dhcp snooping binding vlan 100
```

以下示例将清除与端口通道 10 上带 MAC 地址 04:56:79:86:73:fe 的 VLAN 100 关联的所有动态 DHCP 侦听绑定条目：

```
OS10# clear ip dhcp snooping binding mac 04:56:79:86:73:fe vlan 100 port-channel 10
```

查看 DHCP 绑定表的内容

- 在 EXEC 模式下使用以下命令：

```
show ip dhcp snooping binding [vlan vlan-name]
```

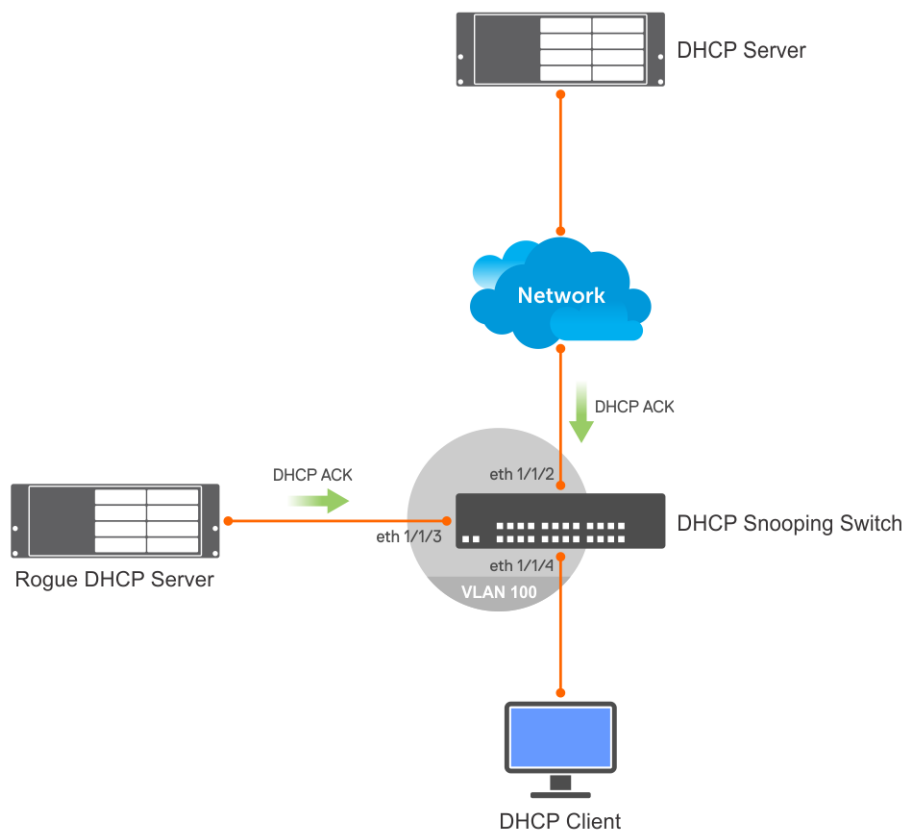
查看 DHCP 绑定表内容的示例

```
OS10# show ip dhcp snooping binding
Codes : S - Static D - Dynamic
IPv4 Address MAC Address Expires(Sec) Type VLAN Interface
=====
10.1.1.22 11:22:11:22:11:22 120331 S 100 ethernet1/1/4
33.1.1.44 11:22:11:22:11:23 120331 S 200 port-channel100
103.1.1.5 11:22:11:22:11:24 120331 D 300 ethernet1/1/5:4
```

DHCP 侦听示例

简单第二层网络中的 DHCP 侦听

本示例使用一种简单的拓扑，其中包含 DHCP 侦听交换机和 DHCP 服务器。DHCP 客户端连接到侦听交换机，并且流氓 DHCP 服务器尝试伪装成合法 DHCP 服务器。通过类似以下内容的配置，DHCP 侦听交换机会丢弃来自连接到未受信任接口的流氓 DHCP 服务器的数据包。



## DHCP 服务器

```
OS10(config)# interface ethernet 1/1/1
S10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# ip address 10.1.1.1/24
OS10(conf-if-eth1/1/1)# exit
OS10(config)# ip dhcp server
OS10(config-dhcp)# no disable
OS10(config-dhcp)# pool dell_server1
OS10(config-dhcp-dell_server1)# lease 0 1 0
OS10(config-dhcp-dell_server1)# network 10.1.1.0/24
OS10(config-dhcp-dell_server1)# range 10.1.1.2 10.1.1.100
```

## DHCP 侦听交换机

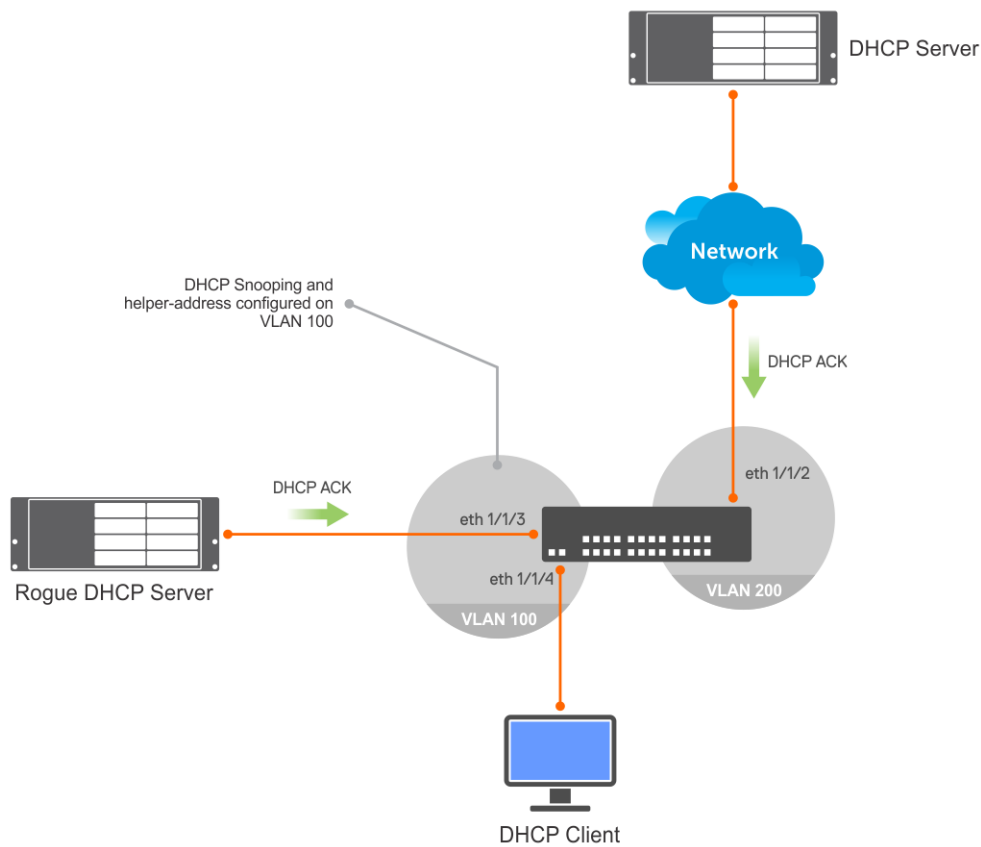
```
OS10# configure terminal
OS10(config)# ip dhcp snooping
OS10(config)# interface vlan 100
OS10(config-if-vl-100)# exit
OS10(config)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# switchport access vlan 100
OS10(conf-if-eth1/1/2)# ip dhcp snooping trust
OS10(conf-if-eth1/1/2)# interface ethernet 1/1/3
OS10(conf-if-eth1/1/3)# switchport access vlan 100
OS10(conf-if-eth1/1/3)# interface ethernet 1/1/4
OS10(conf-if-eth1/1/4)# switchport access vlan 100
```

## DHCP 客户端

```
OS10(config)# interface ethernet 1/1/4
OS10(conf-if-eth1/1/4)# no switchport
OS10(conf-if-eth1/1/4)# no ip address
OS10(conf-if-eth1/1/4)# ip address dhcp
OS10(conf-if-eth1/1/4)# end
```

## DHCP 侦听交换机作为中继代理

本示例使用一种简单的拓扑，将 DHCP 侦听交换机配置为 DHCP 中继代理。通过不同的 VLAN 将 DHCP 服务器和 DHCP 客户端连接到侦听交换机。流氓 DHCP 服务器尝试伪装成合法 DHCP 服务器。通过类似以下内容的配置，DHCP 侦听交换机会丢弃来自连接到未受信任接口的流氓 DHCP 服务器的数据包。



### DHCP 侦听交换机

```
OS10# configure terminal
OS10(config)# ip dhcp snooping
OS10(config)# end
OS10# configure terminal
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# no shutdown
OS10(conf-if-vl-100)# ip address 10.1.1.1/24
OS10(conf-if-vl-100)# ip helper-address 10.2.1.2
OS10(conf-if-vl-100)# exit
OS10(config)# interface vlan 200
OS10(conf-if-vl-200)# no shutdown
OS10(conf-if-vl-200)# ip address 10.2.1.1/24
OS10(conf-if-vl-200)# exit
OS10(config)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# switchport access vlan 200
OS10(conf-if-eth1/1/2)# ip dhcp snooping trust
OS10(conf-if-eth1/1/2)# exit
OS10(config)# interface ethernet 1/1/4
OS10(conf-if-eth1/1/4)# no shutdown
OS10(conf-if-eth1/1/4)# switchport access vlan 100
OS10(conf-if-eth1/1/4)# exit
OS10(config)# interface ethernet 1/1/3
OS10(conf-if-eth1/1/3)# no shutdown
OS10(conf-if-eth1/1/3)# switchport access vlan 100
OS10(conf-if-eth1/1/3)# end
```

## DHCP 服务器

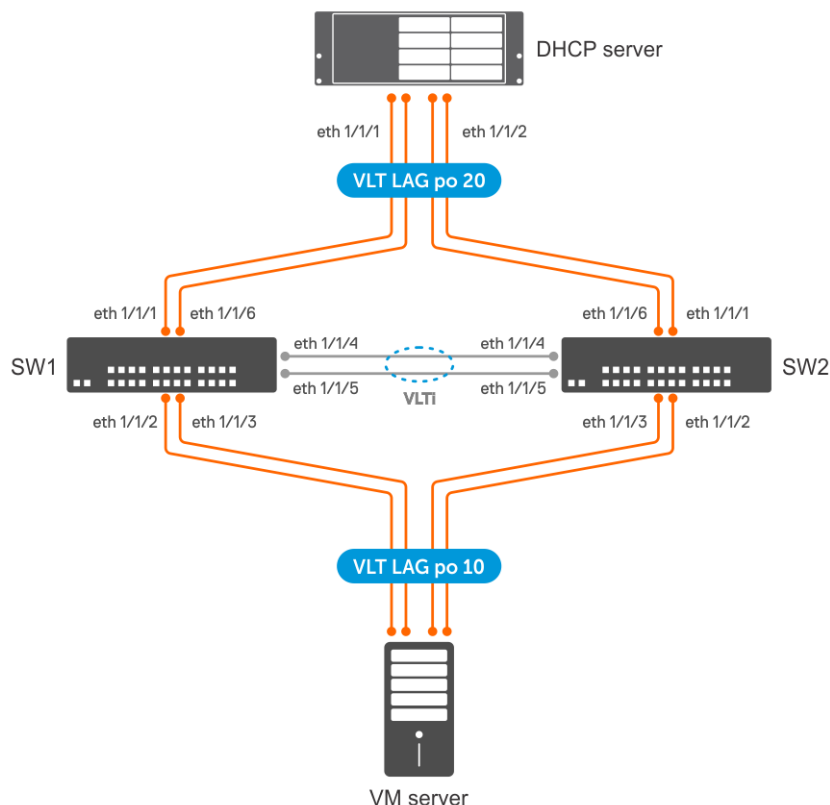
```
OS10# configure terminal
OS10(config)# ip dhcp server
OS10(config-dhcp)# no disable
OS10(config-dhcp)# pool dell_1
OS10(config-dhcp-dell_1)# network 10.1.1.0/24
OS10(config-dhcp-dell_1)# range 10.1.1.2 10.1.1.250
OS10(config-dhcp-dell_1)# exit
OS10(config-dhcp)# pool dell_2
OS10(config-dhcp-dell_2)# network 10.2.1.0/24
OS10(config-dhcp-dell_2)# exit
OS10(config-dhcp)# exit
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# ip address 10.2.1.2/24
```

## DHCP 客户端

```
OS10(config)# interface ethernet 1/1/4
OS10(config-if-eth1/1/4)# no switchport
OS10(config-if-eth1/1/4)# no ip address
OS10(config-if-eth1/1/4)# ip address dhcp
OS10(config-if-eth1/1/4)# end
```

## 第二层 VLT 设置中的 DHCP 侦听

在此第 2 层 VLT 设置中，虚拟机上的 DHCP 客户端将连接到 SW1 和 SW2，并从 DHCP 服务器获取 IP 地址。



## SW 1

## DHCP 侦听配置

- 全局启用 DHCP 侦听。

```
OS10(config)# ip dhcp snooping
```



## VLAN 配置

- 创建 VLAN。

```
OS10# configure terminal
OS10(config)# interface vlan 100
OS10(config-if-vl-100)# no shutdown
```

## VLT 配置

1. 创建 VLT 域并配置 VLTi。

```
OS10(config)# interface range ethernet 1/1/4-1/1/5
OS10(config-range-eth1/1/4-1/1/5)# no switchport
OS10(config-range-eth1/1/4-1/1/5)# exit
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# discovery-interface ethernet 1/1/4-1/1/5
```

2. 配置 VLT MAC 地址。

```
OS10(config-vlt-1)# vlt-mac 12:5e:23:2d:76:3e
```

3. 指定 VLT 对等节点的管理 IP 地址作为备份链路。

```
OS10(config-vlt-1)# backup destination 10.10.10.2
```

4. 配置 VLT 端口通道。

### VLT 端口通道到虚拟机

```
OS10(config)# interface port-channel 10
OS10(config-if-po-10)# description SW1ToVM
OS10(config-if-po-10)# vlt-port-channel 10
OS10(config-if-po-10)# switchport mode access
OS10(config-if-po-10)# switchport access vlan 100
OS10(config-if-po-10)# exit
OS10(config)# interface ethernet 1/1/2-1/1/3
OS10(config-if-eth1/1/2-1/1/3)# no shutdown
OS10(config-if-eth1/1/2-1/1/3)# channel-group 10
```

### VLT 端口通道到 DHCP 服务器

```
OS10(config)# interface port-channel 20
OS10(config-if-po-20)# description SW1ToDHCP-Server
OS10(config-if-po-20)# vlt-port-channel 20
OS10(config-if-po-20)# switchport mode access
OS10(config-if-po-20)# switchport access vlan 100
OS10(config-if-po-20)# ip dhcp snooping trust
OS10(config-if-po-20)# exit
OS10(config)# interface ethernet 1/1/1,1/1/6
OS10(config-if-eth1/1/1,1/1/6)# no shutdown
OS10(config-if-eth1/1/1,1/1/6)# channel-group 20
```

## SW 2

### DHCP 侦听配置

- 全局启用 DHCP 侦听。

```
OS10(config)# ip dhcp snooping
```

## VLAN 配置

- 创建 VLAN。

```
OS10# configure terminal
OS10(config)# interface vlan 100
OS10(config-if-vl-100)# no shutdown
```

## VLT 配置

## 1. 创建 VLT 域并配置 VLTi。

```
OS10(config)# interface range ethernet 1/1/4-1/1/5
OS10(config-range-eth1/1/4-1/1/5)# no switchport
OS10(config-range-eth1/1/4-1/1/5)# exit
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# discovery-interface ethernet 1/1/4-1/1/5
```

## 2. 配置 VLT MAC 地址。

```
OS10(config-vlt-1)# vlt-mac 12:5e:23:f4:23:54
```

## 3. 指定 VLT 对等节点的管理 IP 地址作为备份链路。

```
OS10(config-vlt-1)# backup destination 10.10.10.1
```

## 4. 配置 VLT 端口通道。

### VLT 端口通道到虚拟机

```
OS10(config)# interface port-channel 10
OS10(config-if-po-10)# description SW2ToVM
OS10(config-if-po-10)# vlt-port-channel 10
OS10(config-if-po-10)# switchport mode access
OS10(config-if-po-10)# switchport access vlan 100
OS10(config-if-po-10)# exit
OS10(config)# interface ethernet 1/1/2-1/1/3
OS10(config-if-eth1/1/2-1/1/3)# no shutdown
OS10(config-if-eth1/1/2-1/1/3)# channel-group 10
```

### VLT 端口通道到 DHCP 服务器

```
OS10(config)# interface port-channel 20
OS10(config-if-po-20)# description SW2ToDHCP-Server
OS10(config-if-po-20)# vlt-port-channel 20
OS10(config-if-po-20)# switchport mode access
OS10(config-if-po-20)# switchport access vlan 100
OS10(config-if-po-20)# ip dhcp snooping trust
OS10(config-if-po-20)# exit
OS10(config)# interface ethernet 1/1/1,1/1/6
OS10(config-if-eth1/1/1,1/1/6)# no shutdown
OS10(config-if-eth1/1/1,1/1/6)# channel-group 20
```

## DHCP 服务器

### DHCP 服务器配置

```
OS10(config)# interface vlan 100
OS10(config-if-vl-100)# ip address 10.1.1.1/24
OS10(config-if-vl-100)# exit
OS10(config)# ip dhcp server
OS10(config-dhcp)# no disable
OS10(config-dhcp)# pool dell_server1
OS10(config-dhcp-dell_server1)# lease 0 1 0
OS10(config-dhcp-dell_server1)# network 10.1.1.0/24
OS10(config-dhcp-dell_server1)# range 10.1.1.2 10.1.1.100
```

## 验证两个 VLT 对等节点上的 DHCP 侦听

以下输出显示 DHCP 侦听交换机（VLT 对等节点）侦听的 DHCP 消息。接口列显示本地 VLT 端口通道号。

```
OS10# show ip dhcp snooping binding
```

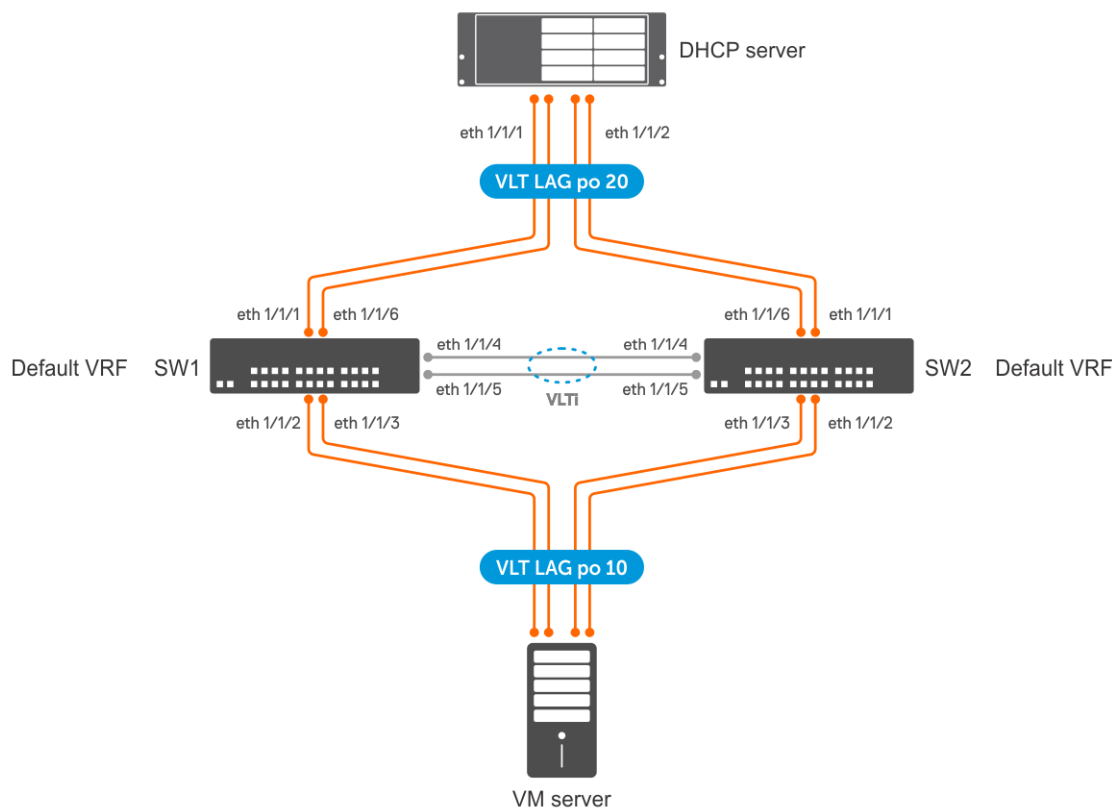
```
Number of entries : 1
```

```
Codes : S - Static D - Dynamic
```

| IPv4 Address | MAC Address       | Expires (Sec) | Type | Interface      | VLAN    |
|--------------|-------------------|---------------|------|----------------|---------|
| 10.1.1.2     | 14:18:77:0d:05:e9 | 3600          | D    | port-channel10 | vlan100 |

## VLT 设置中的 DHCP 侦听和 DHCP 中继代理

在此 VLT 设置中，虚拟机上的 DHCP 客户端将连接到 SW1 和 SW2，并从 DHCP 服务器获取 IP 地址。客户端和 DHCP 服务器的 VLAN 在 SW 1 和 SW 2 上均处于的默认 VRF 状态。



### SW 1

#### DHCP 侦听配置

- 全局启用 DHCP 侦听。

```
OS10(config)# ip dhcp snooping
```

#### VLAN 配置

- 创建 VLAN 并为其分配用作虚拟机网关的 IP 地址。

```
OS10# configure terminal
OS10(config)# interface vlan 100
OS10(config-if-vl-100)# no shutdown
OS10(config-if-vl-100)# ip address 10.1.1.1/24
OS10(config-if-vl-100)# exit
```

- 创建另一个 VLAN 并为其分配可与 DHCP 服务器通信的 IP 地址。

```
OS10# configure terminal
OS10(config)# interface vlan 200
OS10(config-if-vl-200)# no shutdown
OS10(config-if-vl-200)# ip address 10.2.1.1/24
OS10(config-if-vl-200)# exit
```

- 将 SW 1 配置为 VM 中的客户端的 DHCP 中继代理。您在此处指定的 IP 地址是 DHCP 服务器的 IP 地址

```
OS10# configure terminal
OS10(config)# interface vlan 100
OS10(config-if-vl-100)# ip helper-address 10.2.1.2
```

#### VLT 配置

## 1. 创建 VLT 域并配置 VLTi。

```
OS10(config)# interface range ethernet 1/1/4-1/1/5
OS10(config-range-eth1/1/4-1/1/5)# no switchport
OS10(config-range-eth1/1/4-1/1/5)# exit
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# discovery-interface ethernet 1/1/4-1/1/5
```

## 2. 配置 VLT MAC 地址。

```
OS10(config-vlt-1)# vlt-mac 12:5e:23:2d:76:3e
```

## 3. 指定 VLT 对等节点的管理 IP 地址作为备份链路。

```
OS10(config-vlt-1)# backup destination 10.10.10.2
```

## 4. 配置 VLT 端口通道。

### SW1 到 VM VLT 端口通道配置

```
OS10(config)# interface port-channel 10
OS10(config-if-po-10)# description SW1ToVM
OS10(config-if-po-10)# vlt-port-channel 10
OS10(config-if-po-10)# switchport mode access
OS10(config-if-po-10)# switchport access vlan 100
OS10(config-if-po-10)# exit
OS10(config)# interface ethernet 1/1/2-1/1/3
OS10(config-if-eth1/1/2-1/1/3)# no shutdown
OS10(config-if-eth1/1/2-1/1/3)# channel-group 10
```

## SW 1 到 DHCP 服务器配置

```
OS10(config)# interface port-channel 20
OS10(config-if-po-20)# description SW1ToDHCP-Server
OS10(config-if-po-20)# vlt-port-channel 20
OS10(config-if-po-20)# switchport mode trunk
OS10(config-if-po-20)# switchport trunk allowed vlan 100,200
OS10(config-if-po-20)# ip dhcp snooping trust
OS10(config-if-po-20)# exit
OS10(config)# interface ethernet 1/1/1,1/1/6
OS10(config-if-eth1/1/1,1/1/6)# no shutdown
OS10(config-if-eth1/1/1,1/1/6)# channel-group 20
```

### (可选) 对等节点路由配置

- 配置对等节点路由。

```
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# peer-routing
```

## SW 2

### DHCP 侦听配置

- 全局启用 DHCP 侦听。

```
OS10(config)# ip dhcp snooping
```

### VLAN 配置

- 创建 VLAN 并为其分配用作虚拟机网关的 IP 地址。

```
OS10# configure terminal
OS10(config)# interface vlan 100
OS10(config-if-vl-100)# no shutdown
OS10(config-if-vl-100)# ip address
OS10(config-if-vl-100)# ip address 10.1.1.2/24
OS10(config-if-vl-100)# exit
```

- 创建另一个 VLAN 并为其分配可与 DHCP 服务器通信的 IP 地址。

```
OS10# configure terminal
OS10(config)# interface vlan 200
OS10(config-if-vl-200)# no shutdown
OS10(config-if-vl-200)# ip address
OS10(config-if-vl-200)# ip address 10.2.1.3/24
OS10(config-if-vl-200)# exit
```

- 将 SW 1 配置为 VM 中的客户端的 DHCP 中继代理。您在此处指定的 IP 地址是 DHCP 服务器的 IP 地址

```
OS10# configure terminal
OS10(config)# interface vlan 100
OS10(config-if-vl-100)# ip helper-address 10.2.1.2
```

## VLT 配置

1. 创建 VLT 域并配置 VLTi。

```
OS10(config)# interface range ethernet 1/1/4-1/1/5
OS10(config-range-eth1/1/4-1/1/5)# no switchport
OS10(config-range-eth1/1/4-1/1/5)# exit
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# discovery-interface ethernet 1/1/4-1/1/5
```

2. 配置 VLT MAC 地址。

```
OS10(config-vlt-1)# vlt-mac 12:5e:23:f4:23:54
```

3. 指定 VLT 对等节点的管理 IP 地址作为备份链路。

```
OS10(config-vlt-1)# backup destination 10.10.10.1
```

4. 配置 VLT 端口通道。

### SW2 到 VM VLT 端口通道配置

```
OS10(config)# interface port-channel 10
OS10(config-if-po-10)# description SW2ToVM
OS10(config-if-po-10)# vlt-port-channel 10
OS10(config-if-po-10)# switchport mode access
OS10(config-if-po-10)# switchport access vlan 100
OS10(config-if-po-10)# exit
OS10(config)# interface ethernet 1/1/2-1/1/3
OS10(config-if-eth1/1/2-1/1/3)# no shutdown
OS10(config-if-eth1/1/2-1/1/3)# channel-group 10
```

## SW 2 到 DHCP 服务器配置

```
OS10(config)# interface port-channel 20
OS10(config-if-po-20)# description SW2ToDHCP-Server
OS10(config-if-po-20)# vlt-port-channel 20
OS10(config-if-po-20)# switchport mode trunk
OS10(config-if-po-20)# switchport trunk allowed vlan 100,200
OS10(config-if-po-20)# ip dhcp snooping trust
OS10(config-if-po-20)# exit
OS10(config)# interface ethernet 1/1/1,1/1/6
OS10(config-if-eth1/1/1,1/1/6)# no shutdown
OS10(config-if-eth1/1/1,1/1/6)# channel-group 20
```

### (可选) 对等节点路由配置

- 配置对等节点路由。

```
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# peer-routing
```

## DHCP 服务器

## VLAN 配置

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# exit
OS10(config)# interface vlan 200
OS10(conf-if-vl-200)# ip address 10.2.1.2/24
OS10(conf-if-vl-200)# exit
OS10(config)# interface port-channel 20
OS10(conf-if-po-20)# switchport mode trunk
OS10(conf-if-po-20)# switchport trunk allowed vlan 100,200
```

## DHCP 服务器配置

```
OS10(config)# ip dhcp server
OS10(config-dhcp)# no disable
OS10(config-dhcp)# pool dell_server1
OS10(config-dhcp-dell_server1)# network 10.1.1.0/24
OS10(config-dhcp-dell_server1)# range 10.1.1.3 10.1.1.250
OS10(config-dhcp-dell_server1)# lease 0 1 0
OS10(config-dhcp-dell_server1)# default-router 10.1.1.1
OS10(config-dhcp)# pool dell_2
OS10(config-dhcp-dell_2)# network 10.2.1.0/24
OS10(config-dhcp-dell_2)# range 10.2.1.4 10.2.1.100
OS10(config-dhcp-dell_2)# lease 0 1 0
```

## 到达 VLAN 100 的路由

```
OS10(config)#ip route 10.1.1.0/24 10.2.1.1
```

## 验证两个 VLT 对等节点上的 DHCP 侦听

以下输出显示 DHCP 侦听交换机（VLT 对等节点）侦听的 DHCP 消息。

```
OS10# show ip dhcp snooping binding
```

Number of entries : 1

Codes : S - Static D - Dynamic

| IPv4 Address | MAC Address       | Expires(Sec) | Type | Interface      | VLAN |
|--------------|-------------------|--------------|------|----------------|------|
| 10.1.1.3     | 14:18:77:0d:05:e9 | 3600         | D    | port-channel10 | 100  |

## 动态 ARP 检查

动态地址解析协议 (ARP) 检查 (DAI) 是一项安全功能，可防止局域网遭受中间人 ARP 哄骗攻击。

启用 DAI 时，交换机会拦截已启用 DAI 的 VLAN 上的 ARP 数据包。交换机随后会将源 IP 和源 MAC 地址、VLAN 以及接收的数据包的接口（物理或端口通道）与 DHCP 侦听绑定表进行比较。如果数据包中的信息与 DHCP 侦听绑定表中的任何条目都不匹配，交换机将丢弃数据包。

 **注：** Dell EMC Networking 建议在系口上启用 DHCP 侦听之前启用 DAI。

### DAI 违规日志记录

您可以配置系统以记录与 ARP 数据包对应的 DAI 验证失败。如果已启用，则会在控制台中记录 DAI 违规。默认情况下，DAI 违规日志记录已禁用。

如果您将接口配置为可信，则交换机会将从主机进入接口的 ARP 数据包作为合法数据包进行解释。默认情况下，DAI 中的所有接口处于不可信状态。

要使 DAI 正常工作，请在交换机上启用 DHCP 侦听功能。默认情况下，DAI 已禁用。

### DAI 统计信息

系统将维护包含以下详细信息的 DAI 统计信息：

- 有效的 ARP 请求
- 无效的 ARP 请求
- 有效的 ARP 回复

- 无效的 ARP 回复

您可以使用 `clear ip arp inspection statistics` 命令清除 DAI 统计信息。

### DAI 可信接口

默认情况下，所有端口都不可信，并且所有数据包都会在所有启用 DAI 的 VLAN 上进行 DAI 验证过程。您可以通过将接口配置为可信来配置接口，以绕过 ARP 检查。

 **注：**在 VLAN 启用 DAI 时，Dell EMC Networking 建议在 DHCP 监听可信接口上配置 `arp inspection-trust` 命令。

### 动态 ARP 检查的限制

- 不支持使用 VxLAN 桥进行动态 ARP 检查。
- 建议的动态 ARP 检查条目的最大数量为 2000。

### 启用动态 ARP 检查

- 启用 DHCP 侦听。有关配置 DHCP 侦听的详细信息，请参阅 [DHCP 侦听](#)。
- 在处于 INTERFACE VLAN 模式的 VLAN 上启用动态 ARP 检查。

```
arp inspection
```

### 启用动态 ARP 检查违规日志记录

- 在 CONFIGURATION 模式下使用以下命令：

```
arp inspection violation logging
```

### 绕过接口上的动态 ARP 检查

- 在 INTERFACE 模式下使用以下命令：

```
arp inspection-trust
```

### 清除 DAI 统计信息

- 在 EXEC 模式下清除 DAI 统计信息。

```
clear ip arp inspection statistics [vlan vlan-name]
```

### 查看 DAI 数据库

- 在 EXEC 模式下查看 DAI 数据库

```
show ip arp inspection database [vlan vlan-name]
```

使用 `vlan` 选项查看特定 VLAN 的 DAI 数据库。

### 查看 DAI 数据库的示例

```
OS10# show ip arp inspection database
Number of entries : 828
```

| Address   | Hardware Address  | Interface       | VLAN     |
|-----------|-------------------|-----------------|----------|
| 10.2.1.1  | 00:40:50:00:00:00 | port-channel100 | vlan3001 |
| 10.1.1.13 | 00:2a:10:01:00:00 | port-channel100 | vlan3001 |
| 10.1.1.62 | 00:2a:10:01:00:01 | port-channel100 | vlan3001 |

### 查看 DAI 统计信息

您可以查看交换机收到的有效和无效的 ARP 请求以及交换机已发送的回复。

- 在 EXEC 模式下使用以下命令：

```
show ip arp inspection statistics vlan vlan-name
```

## 查看 DAI 统计信息的示例

```
OS10# show ip arp inspection statistics
Dynamic ARP Inspection (DAI) Statistics

Valid ARP Requests : 0
Valid ARP Replies : 1000
Invalid ARP Requests : 1000
Invalid ARP Replies : 0
```

### • 查看 DAI 违规信息

```
show ip arp inspection logging
```

## 查看 DAI 违规信息的示例

```
OS10# show ip arp inspection logging
Total Number of Clients : 1
New Clients learnt in current Interval : 0
Invalid ARP packets in current interval :
0
Address Hw-Address Port VLAN First-detected-time Packet-
count

10.1.1.1 12:d3:43:a1:2e:23 ethernet1/1/1 10 00:23:14 2
```

## 源地址验证

源地址验证 (SAV) 是一项安全功能，它指示交换机仅允许来自 DHCP 侦听绑定表中的客户端的 IP 流量。

启用 SAV 后，交换机会将数据包中的源 IP 和 MAC 地址与 DHCP 侦听绑定表进行比较。如果匹配，设备将转发数据包。如果不匹配，则会丢弃数据包。

默认情况下，SAV 处于禁用状态。

 **注：** Dell EMC Networking 建议在系上启用 DHCP 侦听之前启用 SAV。

OS10 支持三种类型的源地址验证：

1. 源 IP 地址验证
2. 源 IP 和 MAC 地址验证
3. DHCP 源 MAC 地址验证

### 源 IP 地址验证

此功能将根据源 IP 地址筛选 IP 流量，并仅允许来自 DHCP 侦听绑定表中的客户端的流量。交换机将数据包中的以下内容与 DHCP 侦听绑定表进行比较：

- 源 IP 地址
- 客户端连接的 VLAN
- 客户端连接到的接口（物理或端口通道）

如果匹配，交换机将转发数据包。

### 源 IP 和 MAC 地址验证

此功能会基于源 IP 和源 MAC 地址筛选 IP 流量，并仅允许来自 DHCP 侦听绑定表中的客户端的流量。交换机将数据包中的以下内容与 DHCP 侦听绑定表进行比较：

- 源 MAC 地址
- 源 IP 地址
- 客户端连接的 VLAN
- 客户端连接到的接口（物理或端口通道）

如果匹配，交换机将转发数据包。

### DHCP 源 MAC 地址验证

交换机将 DHCP 数据包的源 MAC 地址与 DHCP 数据包中的客户端硬件地址 (CHADDR) 字段进行比较，并在存在不匹配时丢弃 DHCP 数据包。



## 对源地址验证的限制

- 由于 SAV 功能与用户 ACL 共享 TCAM 内存，因此系统可以支持的 SAV 规则的最大数量取决于分配给用户 ACL 的 TCAM 内存量。

## 启用源 IP 地址验证

- 在 INTERFACE 模式下启用源 IP 地址验证。

```
ip dhcp snooping source-address-validation ip [vlan vlan-name]
```

使用 `vlan` 选项可选择为一个或多个 VLAN 指定 SAV。范围是从 1 到 4093。如果未指定 `vlan` 选项，则会在接口的所有 VLAN 上启用 SAV。

## 启用源 IP 和 MAC 地址验证

- 在 INTERFACE 模式下启用源 IP 和 MAC 地址验证。

```
ip dhcp snooping source-address-validation ipmac [vlan vlan-name]
```

使用 `VLAN` 选项可选择为一个或多个 VLAN 指定 SAV。范围是从 1 到 4093。如果未指定 `vlan` 选项，则会在接口的所有 VLAN 上启用 SAV。

## 启用 DHCP 源 MAC 地址验证

- 在 CONFIGURATION 模式下启用 DHCP 源 MAC 地址验证。

```
ip dhcp snooping verify mac-address
```

# DHCP 命令

## default-router address

根据 IP 地址池为客户端分配默认网关。

|        |                                                                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>default-router address [address2...address8]</code>                                                                                                                                               |
| 参数     | <ul style="list-style-type: none"><li>• <code>address</code> — 输入一个 IPv4 或 IPv6 地址，用作子网中的客户端的默认网关（采用 A.B.C.D 或 A::B 格式）。</li><li>• <code>address2...address8</code> — （可选）按优先级顺序输入最多八个 IP 地址。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                     |
| 命令模式   | DHCP-POOL                                                                                                                                                                                               |
| 使用情况信息 | 按优先级顺序配置最多八个 IP 地址。使用此命令的 <code>no</code> 版本可以移除配置。                                                                                                                                                     |
| 示例     | <pre>OS10(conf-dhcp-20.1.1.1)# default-router 20.1.1.100</pre>                                                                                                                                          |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                        |

## disable

禁用 DHCP 服务器。

|        |                                      |
|--------|--------------------------------------|
| 语法     | <code>disable</code>                 |
| 参数     | 无                                    |
| 默认     | 已禁用                                  |
| 命令模式   | DHCP                                 |
| 使用情况信息 | 此命令的 <code>no</code> 版本将启用 DHCP 服务器。 |

|              |                                        |
|--------------|----------------------------------------|
| <b>示例</b>    | <pre>OS10(conf-dhcp)# no disable</pre> |
| <b>支持的版本</b> | 10.2.0E or later                       |

## dns-server address

根据地址池将 DNS 服务器分配给客户端。

|               |                                                                                                                                                                                                    |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>dns-server address [address2...address8]</code>                                                                                                                                              |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>address</code> — 输入用来服务于子网上的客户端的 DNS 服务器 IP 地址，格式为 A.B.C.D 或 A::B。</li> <li><code>address2...address8</code> — （可选）按优先级顺序输入最多八个 DNS 服务器地址。</li> </ul> |
| <b>默认</b>     | 未配置                                                                                                                                                                                                |
| <b>命令模式</b>   | DHCP-POOL                                                                                                                                                                                          |
| <b>使用情况信息</b> | 无                                                                                                                                                                                                  |
| <b>示例</b>     | <pre>OS10(conf-dhcp-Dell)# dns-server 192.168.1.1</pre>                                                                                                                                            |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                                                                                   |

## domain-name

配置设备所在域的名称。

|               |                                                       |
|---------------|-------------------------------------------------------|
| <b>语法</b>     | <code>domain-name domain-name</code>                  |
| <b>参数</b>     | <code>domain-name</code> — 输入最多包含 32 个字符的域的名称。        |
| <b>默认</b>     | 未配置                                                   |
| <b>命令模式</b>   | DHCP-POOL                                             |
| <b>使用情况信息</b> | 这是附加到未完全限定的主机名称的默认域名。此命令的 <code>no</code> 版本将移除配置。    |
| <b>示例</b>     | <pre>OS10(conf-dhcp-Dell)# domain-name dell.com</pre> |
| <b>支持的版本</b>  | 10.2.0E or later                                      |

## hardware-address

配置手动配置的客户端硬件地址。

|               |                                                                       |
|---------------|-----------------------------------------------------------------------|
| <b>语法</b>     | <code>hardware-address nn:nn:nn:nn:nn:nn</code>                       |
| <b>参数</b>     | <code>nn:nn:nn:nn:nn:nn</code> — 输入 48 位硬件地址。                         |
| <b>默认</b>     | 未配置                                                                   |
| <b>命令模式</b>   | DHCP-POOL                                                             |
| <b>使用情况信息</b> | 客户端硬件地址是用于手动地址绑定的客户端计算机的 MAC 地址。                                      |
| <b>示例</b>     | <pre>OS10(conf-dhcp-static)# hardware-address 00:01:e8:8c:4d:0a</pre> |
| <b>支持的版本</b>  | 10.2.0E or later                                                      |

## host

将主机分配给单个 IPv4 或 IPv6 地址池以进行手动配置。

|        |                                                              |
|--------|--------------------------------------------------------------|
| 语法     | <code>host A.B.C.D/A::B</code>                               |
| 参数     | <code>A.B.C.D/A::B</code> — 输入主机 IP 地址，采用 A.B.C.D 或 A::B 格式。 |
| 默认     | 未配置                                                          |
| 命令模式   | DHCP-POOL                                                    |
| 使用情况信息 | 主机地址是客户端计算机用于 DHCP 的 IP 地址。                                  |
| 示例     | <pre>OS10(conf-dhcp-Dell)# host 20.1.1.100</pre>             |
| 支持的版本  | 10.2.0E or later                                             |

## ip dhcp server

进入 DHCP 配置模式。

|        |                                                                       |
|--------|-----------------------------------------------------------------------|
| 语法     | <code>ip dhcp server</code>                                           |
| 参数     | 无                                                                     |
| 默认     | 未配置                                                                   |
| 命令模式   | CONFIGURATION                                                         |
| 使用情况信息 | 使用 <code>ip dhcp server</code> 命令输入在接口上启用 DHCP 服务器分配的动态地址所需的 DHCP 模式。 |
| 示例     | <pre>OS10(config)# ip dhcp server OS10(conf-dhcp)#</pre>              |
| 支持的版本  | 10.2.0E or later                                                      |

## ip helper-address

配置 DHCP 服务器地址。

|           |                                                                                                                                                                                                         |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法        | <code>ip helper-address address [vrf vrf-name]</code>                                                                                                                                                   |
| 参数        | <ul style="list-style-type: none"><li><code>address</code> — 输入将 UDP 广播转发至 DHCP 服务器的 IPv4 地址（格式为 A.B.C.D）。</li><li><code>vrf vrf-name</code> — （可选）输入 <code>vrf</code>，然后输入用于访问主机地址的 VRF 的名称。</li></ul> |
| 默认        | 已禁用                                                                                                                                                                                                     |
| 命令模式      | INTERFACE                                                                                                                                                                                               |
| 使用情况信息    | 只有 L3 接口支持 DHCP 服务器。配置 IP 帮助程序地址之后，地址将 UDP 广播转发至 DHCP 服务器。您可以通过对每个 DHCP 服务器地址重复相同的命令，在接口上配置多个帮助程序地址。此命令的 <code>no</code> 版本将值恢复为默认值。面向客户端和面向服务器的接口必须在同一 VRF 中。                                          |
| 示例 (IPv4) | <pre>OS10(config)# interface eth 1/1/22 OS10(conf-if-eth1/1/22)# ip helper-address 20.1.1.1 vrf blue</pre>                                                                                              |
| 支持的版本     | 10.2.0E or later                                                                                                                                                                                        |

## ipv6 helper-address

配置 DHCPv6 服务器地址。

|    |                                                              |
|----|--------------------------------------------------------------|
| 语法 | <code>ipv6 helper-address ipv6-address [vrf vrf-name]</code> |
|----|--------------------------------------------------------------|

|        |                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 参数     | <ul style="list-style-type: none"> <li><code>vrf vrf-name</code> — (可选) 输入关键字 <code>vrf</code>，然后输入可以访问主机地址的 VRF 的名称。</li> <li><code>ipv6-address</code> — 以 A::B 格式指定 DHCPv6 服务器地址。</li> </ul> |
| 默认     | 已禁用                                                                                                                                                                                             |
| 命令模式   | INTERFACE                                                                                                                                                                                       |
| 使用情况信息 | 在 DHCPv6 客户端连接的接口上使用此命令，以在 IPv6 客户端和 DHCPv6 服务器之间转发数据包。配置 IPv6 帮助程序地址之后，地址会将 UDP 广播从 IPv6 客户端转发至 DHCPv6 服务器。您可以通过对每个 DHCPv6 服务器地址重复相同的命令，在接口上配置多个帮助程序地址。此命令的 <code>no</code> 版本将删除 IPv6 帮助程序地址。 |
| 示例     | <pre>OS10(config)# interface ethernet 1/1/22 OS10(conf-if-eth1/1/22)# ipv6 helper-address 2001:db8:0:1:1:1:1:1 vrf blue</pre>                                                                   |
| 支持的版本  | 10.4.1.0 or later                                                                                                                                                                               |

lease

为池中的 IP 地址配置租赁时间。

|         |                                                                                                                                                                                                                                            |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法      | <code>lease {infinite   days [hours] [minutes]}</code>                                                                                                                                                                                     |
| 参数      | <ul style="list-style-type: none"> <li><code>infinite</code> — 输入关键字以配置永不过期的租用。</li> <li><code>days</code> — 输入租赁天数，从 0 到 31。</li> <li><code>hours</code> — 输入租用小时数，从 0 到 23。</li> <li><code>minutes</code> — 输入租赁分钟数，从 0 到 59。</li> </ul> |
| 默认      | 24 小时                                                                                                                                                                                                                                      |
| 命令模式    | DHCP-POOL                                                                                                                                                                                                                                  |
| 使用情况信息  | 此命令的 <code>no</code> 版本将移除租用配置。                                                                                                                                                                                                            |
| 示例      | <pre>OS10(conf-dhcp-Dell)# lease 2 5 10</pre>                                                                                                                                                                                              |
| 示例（无限大） | <pre>OS10(conf-dhcp-Dell)# lease infinite</pre>                                                                                                                                                                                            |
| 支持的版本   | 10.2.0E or later                                                                                                                                                                                                                           |

netbios-name-server address

配置可供 DHCP 客户端使用的 NetBIOS WINS 服务器。

|        |                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>netbios-name-server ip-address [address2...address8]</code>                                                  |
| 参数     | <p><code>ip-address</code> — 输入 NetBIOS WINS 服务器的地址。</p> <p><code>address2...address8</code> — (可选) 输入其他服务器地址。</p> |
| 默认     | 未配置                                                                                                                |
| 命令模式   | DHCP-POOL                                                                                                          |
| 使用情况信息 | 配置最多八个可供 Microsoft DHCP 客户端使用的 NetBIOS WINS 服务器，按优先级顺序。此命令的 <code>no</code> 版本将值恢复为默认值。                            |
| 示例     | <pre>OS10(conf-dhcp-Dell)# netbios-name-server 192.168.10.5</pre>                                                  |
| 支持的版本  | 10.2.0E or later                                                                                                   |

## netbios-node-type

为 DHCP 客户端配置 NetBIOS 节点类型。

|        |                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>netbios-node-type type</code>                                                                                                                                                                          |
| 参数     | <code>type</code> — 输入 NetBIOS 节点类型： <ul style="list-style-type: none"><li>• Broadcast — 输入 b-node。</li><li>• Hybrid — 输入 h-node。</li><li>• Mixed — 输入 m-node。</li><li>• Peer-to-peer — 输入 p-node。</li></ul> |
| 默认     | 混合                                                                                                                                                                                                           |
| 命令模式   | DHCP-POOL                                                                                                                                                                                                    |
| 使用情况信息 | 此命令的 <code>no</code> 版本会将该值重置为默认值。                                                                                                                                                                           |
| 示例     | <pre>OS10(conf-dhcp-Dell)# netbios-node-type h-node</pre>                                                                                                                                                    |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                             |

## network

配置地址池中的一系列 IPv4 或 IPv6 地址。

|        |                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------|
| 语法     | <code>network address/mask</code>                                                                   |
| 参数     | <code>address/mask</code> — 以 <code>.c/x</code> 或 <code>: : b/x</code> 格式输入 IP 地址和子网掩码范围。           |
| 默认     | 未配置                                                                                                 |
| 命令模式   | DHCP-POOL                                                                                           |
| 使用情况信息 | 使用 <code>network</code> 命令以配置 DHCP 服务器可以分配地址的 IPv4 或 IPv6 子网地址。 <code>mask</code> 的前缀长度为 18 到 31 位。 |
| 示例     | <pre>OS10(config-dhcp-Dell)# network 20.1.1.1/24</pre>                                              |
| 支持的版本  | 10.2.0E or later                                                                                    |

## pool

配置 IP 地址池名称。

|        |                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>pool pool-name</code>                                                                                                                        |
| 参数     | <code>pool-name</code> — 输入 DHCP 服务器池名称。                                                                                                           |
| 默认     | 未配置                                                                                                                                                |
| 命令模式   | CONFIGURATION                                                                                                                                      |
| 使用情况信息 | 使用 <code>pool</code> 命令命名可用 IP 地址的池，由 DHCP 服务器用于将 IP 地址分配给客户端并进入 DHCP POOL 模式。在此模式下，使用 <code>network</code> 命令可配置由 DHCP 服务器为其分配地址的 IPv4 或 IPv6 子网。 |
| 示例     | <pre>OS10(conf-dhcp)# pool Dell OS10(conf-dhcp-Dell)#</pre>                                                                                        |
| 支持的版本  | 10.2.0E or later                                                                                                                                   |

## range

配置 IP 地址的范围。

|        |                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>range {ip-address1 [ip-address2]}</code>                                                                                                                                                |
| 参数     | <ul style="list-style-type: none"><li><code>ip-address1</code> — IP 地址范围的第一个 IP 地址。</li><li><code>ip-address2</code> — IP 地址范围的最后一个 IP 地址。</li></ul>                                          |
| 默认     | 未配置                                                                                                                                                                                           |
| 命令模式   | DHCP-POOL                                                                                                                                                                                     |
| 使用情况信息 | 使用 <code>range</code> 命令配置 OS10 交换机（作为 DHCP 服务器）可以分配给 DHCP 客户端的 IP 地址范围。此命令的 <code>no</code> 版本仅要求第一个 IP 地址来删除范围配置。                                                                           |
| 示例     | <pre>OS10(config)# OS10(config)# ip dhcp server OS10(config-dhcp)# pool pool1 OS10(config-dhcp-pool1)# network 192.168.10.0/24 OS10(config-dhcp-pool1)# range 192.168.10.2 192.168.10.8</pre> |
| 支持的版本  | 10.4.1 或更高版本                                                                                                                                                                                  |

## show ip dhcp binding

显示包含 IPv4 地址的 DHCP 绑定表。

|        |                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show ip dhcp binding</code>                                                                                                                                                                                          |
| 参数     | 无                                                                                                                                                                                                                          |
| 默认     | 未配置                                                                                                                                                                                                                        |
| 命令模式   | EXEC                                                                                                                                                                                                                       |
| 使用情况信息 | 在 DHCP POOL 模式下使用 <code>host</code> 和 <code>hardware-address</code> 命令配置静态 IP 到 MAC 地址映射后，使用此命令在 DHCP 绑定表中验证主机的单个手动绑定。                                                                                                     |
| 示例     | <pre>OS10# show ip dhcp binding   IP Address  Hardware address  Lease expiration  Hostname +-----+-----+-----+-----+ 11.1.1.254    00:00:12:12:12:12  Jan 27 2016 06:23:45  Total Number of Entries in the Table = 1</pre> |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                           |

## DHCP 侦听命令

### arp inspection

在 VLAN 上启用动态 ARP 检查 (DAI)。

|        |                                            |
|--------|--------------------------------------------|
| 语法     | <code>arp inspection</code>                |
| 参数     | 无                                          |
| 默认     | 已禁用                                        |
| 命令模式   | INTERFACE VLAN                             |
| 使用情况信息 | Dell EMC Networking 建议在启用 DHCP 侦听之前启用 DAI。 |

|       |                                      |
|-------|--------------------------------------|
| 示例    | OS10(conf-if-vl-230)# arp inspection |
| 支持的版本 | 10.5.0 or later                      |

## arp inspection-trust

将端口配置为信任，因此不会针对 DAI 数据库验证 ARP 帧。

|        |                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | arp inspection-trust                                                                                                                                                                  |
| 参数     | 无                                                                                                                                                                                     |
| 默认     | 所有接口都不受信任                                                                                                                                                                             |
| 命令模式   | INTERFACE                                                                                                                                                                             |
| 使用情况信息 | <div> <div> <i>i</i> </div> <div> <b>注:</b> 为 VLAN 启用 DAI 时，Dell EMC Networking 建议在 DHCP 侦听可信接口上配置 arp inspection-trust 命令。 </div> </div> <p>具有 sysadmin 和 secadmin 角色的用户可以访问此命令。</p> |

|       |                                               |
|-------|-----------------------------------------------|
| 示例    | OS10(conf-if-eth1/1/33)# arp inspection-trust |
| 支持的版本 | 10.5.0 or later                               |

## arp inspection violation logging

在 VLAN 上启用动态 ARP 检查 (DAI)。

|        |                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------|
| 语法     | arp inspection violation logging                                                                           |
| 参数     | <ul style="list-style-type: none"> <li>violation logging — 输入 violation logging 以启用 DAI 冲突日志记录。</li> </ul> |
| 默认     | 已禁用                                                                                                        |
| 命令模式   | CONFIGURATION                                                                                              |
| 使用情况信息 | 启用此 violation logging 选项时，将记录每个违反的 ARP 请求，其中包含源 IP 地址、源 MAC 地址和接口详细信息。                                     |

|       |                                              |
|-------|----------------------------------------------|
| 示例    | OS10(conf)# arp inspection violation logging |
| 支持的版本 | 10.5.0 or later                              |

## clear ip arp inspection statistics

清除动态 ARP 检查统计信息。

|        |                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------|
| 语法     | clear ip arp inspection statistics [vlan <b>vlan-id</b> ]                                         |
| 参数     | <ul style="list-style-type: none"> <li>vlan <b>vlan-id</b> — 输入 VLAN ID。范围是从 1 到 4093。</li> </ul> |
| 默认     | 无                                                                                                 |
| 命令模式   | EXEC                                                                                              |
| 使用情况信息 | 具有 sysadmin 和 secadmin 角色的用户可以访问此命令。                                                              |

|        |                                      |
|--------|--------------------------------------|
| 示例（全局） | OS10# clear ip dhcp snooping binding |
| 支持的版本  | 10.5.0 or later 或更高版本                |

## clear ip dhcp snooping binding

清除 DHCP 侦听绑定表中的动态条目。

|          |                                                                                                                                                                                                                                                                       |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法       | <code>clear ip dhcp snooping binding [mac <b>mac-address</b>] [vlan <b>vlan-id</b>] [interface {ethernet <b>slot/port/sub-port</b>&gt;   port-channel <b>port-channel-id</b>}]</code>                                                                                 |
| 参数       | <ul style="list-style-type: none"><li>• <code>mac <b>mac-address</b></code>— 输入服务器为其租用 IP 地址的主机的 MAC 地址。</li><li>• <code>vlan <b>vlan-id</b></code>— 输入 VLAN ID。范围是从 1 到 4093。</li><li>• <code>interface <b>type</b></code>— 输入接口类型信息。您可以输入物理、VLAN 或端口通道接口。</li></ul> |
| 默认       | 无                                                                                                                                                                                                                                                                     |
| 命令模式     | EXEC                                                                                                                                                                                                                                                                  |
| 使用情况信息   | <p>此命令将清除 DHCP 侦听绑定表中的动态条目。</p> <p> <b>小心:</b> 使用 <code>clear ip dhcp snooping binding</code> 命令清除 DHCP 侦听绑定表，也会清除系统上的 SAV 和 DAI 条目。这会影响连接到已启用 DHCP 侦听的 VLAN 的客户端的流量。</p>            |
| 示例（全局）   | <pre>OS10# clear ip dhcp snooping binding</pre>                                                                                                                                                                                                                       |
| 示例（MAC）  | <pre>OS10# clear ip dhcp snooping binding mac 04:56:79:86:73:fe</pre>                                                                                                                                                                                                 |
| 示例（端口通道） | <pre>OS10# clear ip dhcp snooping binding mac 04:56:79:86:73:fe vlan 100 port-channel 10</pre>                                                                                                                                                                        |
| 支持的版本    | 10.5.0 or later 或更高版本                                                                                                                                                                                                                                                 |

## ip dhcp snooping（全局）

启用全局 DHCP 侦听。

|        |                                                                                                                                                                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip dhcp snooping</code>                                                                                                                                                                                                                            |
| 参数     | 无                                                                                                                                                                                                                                                        |
| 默认     | 已禁用                                                                                                                                                                                                                                                      |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                            |
| 使用情况信息 | <p>启用此功能后，交换机将开始监控 DHCP 服务器和 DHCP 客户端之间的所有事务，并使用该信息构建 DHCP 侦听绑定表。</p> <p>如果禁用 DHCP 侦听，系统将移除 DHCP 侦听绑定表。源地址验证和动态 ARP 检查条目也将移除。</p> <p>具有 <code>sysadmin</code> 和 <code>secadmin</code> 角色的用户可以访问此命令。</p> <p>此命令的 <code>no</code> 版本将在全局范围内禁用 DHCP 侦听。</p> |
| 示例     | <pre>OS10(config)# ip dhcp snooping</pre>                                                                                                                                                                                                                |
| 支持的版本  | 10.5.0 or later 或更高版本                                                                                                                                                                                                                                    |

## ip dhcp snooping（接口）

在 VLAN 上启用 DHCP 侦听。

|    |                               |
|----|-------------------------------|
| 语法 | <code>ip dhcp snooping</code> |
| 参数 | 无                             |
| 默认 | 已启用（如果全局启用）                   |



|               |                                                                                                                                                                                                                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>命令模式</b>   | INTERFACE VLAN                                                                                                                                                                                                                                                                                                                         |
| <b>使用情况信息</b> | <p>启用此功能后，交换机将开始监控 DHCP 服务器和 DHCP 客户端之间的所有事务，并使用该信息构建 DHCP 侦听绑定表。</p> <p>系统将监听已启用 DHCP 侦听的 VLAN 上来自 DHCP 客户端的数据包，并将数据包转发到 VLAN 的所有物理和端口通道接口。</p> <p>系统将处理通过受信任的物理接口和端口通道接口接收的 DHCP 服务器数据包，并将数据包转发到所有 VLAN 成员接口。</p> <p>您可以在全局范围内启用 DHCP 侦听，并在接口上禁用它。</p> <p>具有 sysadmin 和 secadmin 角色的用户可以访问此命令。</p> <p>此命令的 no 版本会禁用接口上的 DHCP 侦听。</p> |
| <b>示例</b>     | <pre>OS10(config-if-vl-4)# ip dhcp snooping</pre>                                                                                                                                                                                                                                                                                      |
| <b>支持的版本</b>  | 10.5.0 or later 或更高版本                                                                                                                                                                                                                                                                                                                  |

## ip dhcp snooping binding

在 DHCP 绑定表中创建静态 DHCP 侦听绑定条目。

|               |                                                                                                                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ip dhcp snooping binding mac address vlan vlan-id ip ip-address interface [ethernet slot/port/sub-port   port-channel port-channel-id   VLTi]</code>                                                                                                                                   |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>mac address</code>— 输入服务器为其租用 IP 地址的主机的 MAC 地址。</li> <li><code>vlan vlan-id</code>— 输入主机所属 VLAN 的 VLAN ID。范围是从 1 到 4093。</li> <li><code>ip ip-address</code>— 输入主机的 IP 地址。</li> <li><code>interface interface-type</code>— 输入接口类型信息。</li> </ul> |
| <b>默认</b>     | 无                                                                                                                                                                                                                                                                                            |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                                                                                                                                                                                |
| <b>使用情况信息</b> | <p>当您创建静态 DHCP 侦听条目时，它不会超时。</p> <p>为 VLAN 创建静态条目之前，请先创建 VLAN。如果在创建静态条目之前未创建 VLAN，系统会显示一条错误消息。</p> <p>在删除端口通道或 VLAN 之前，请移除所有关联的 DHCP 侦听条目。</p> <p>具有 sysadmin 和 secadmin 角色的用户可以访问此命令。</p> <p>此命令的 no 版本会从 DHCP 侦听绑定表中删除静态条目。</p>                                                             |
| <b>示例</b>     | <pre>OS10(config)# ip dhcp snooping binding mac 00:04:96:70:8a:12 vlan 100 ip 100.1.1.2 interface ethernet 1/1/4</pre>                                                                                                                                                                       |
| <b>支持的版本</b>  | 10.5.0 or later                                                                                                                                                                                                                                                                              |

## ip dhcp snooping trust

在已启用 DHCP 侦听的 VLAN 中将接口配置为受信任。

|               |                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ip dhcp snooping trust</code>                                                                         |
| <b>参数</b>     | 无                                                                                                           |
| <b>默认</b>     | 不受信任                                                                                                        |
| <b>命令模式</b>   | INTERFACE                                                                                                   |
| <b>使用情况信息</b> | <p>此命令将物理或端口通道接口配置为受信任。默认情况下，已启用 DHCP 侦听的 VLAN 中的所有物理和端口通道接口都不受信任。您可以将面向 DHCP 服务器的物理或端口通道接口配置为受信任。仅当系统通</p> |

过受信任接口进入入口时，系统才允许 DHCP 服务器数据包。如果系统在不受信任的接口上接收 DHCP 数据包，则会将连接到不受信任接口的设备解释为流氓 DHCP 服务器并丢弃数据包。

此命令的 `no` 版本将接口重置为不受信任。

示例

```
OS10(conf-if-eth1/1/33)# ip dhcp snooping trust
```

支持的版本 10.5.0 or later

ip dhcp snooping verify mac-address

启用 DHCPv4 源 MAC 地址验证

语法 ip dhcp snooping verify mac-address

参数 无

默认 已禁用

命令模式 CONFIGURATION

使用情况信息 此命令可启用 DHCPv4 源 MAC 地址验证，以验证 DHCP 数据包的源硬件地址与 DHCP 有效负载中的客户端硬件地址字段 (CHADDR)。

示例

```
OS10(config)# ip dhcp snooping verify mac-address
```

支持的版本 10.5.0 or later

show ip arp inspection database

显示 DAI 数据表的内容。

语法 show ip arp inspection database

参数 无

默认 无

命令模式 EXEC

使用情况信息 此命令将显示从中处理 ARP 数据包的已侦听主机的列表。

示例

```
OS10# show ip arp inspection database
Number of entries : 3

Address Hardware Address Interface VLAN

55.2.1.1 00:40:50:00:00:00 port-channel100 vlan3001
200.1.1.134 00:2a:10:01:00:00 port-channel100 vlan3001
200.1.1.62 00:2a:10:01:00:01 port-channel100 vlan3001
```

支持的版本 10.5.0 or later

show ip arp inspection statistics

显示有效和无效的 ARP 请求和回复统计信息。

语法 show ip arp inspection statistics [vlan **vlan-id**]

参数 • vlan **vlan-id**— 输入 VLAN ID。范围是从 1 到 4093。

默认 无

命令模式

EXEC

使用情况信息

此命令将显示处理的有效和无效的 ARP 请求和响应数量。

示例

```
OS10# show ip arp inspection statistics
Dynamic ARP Inspection (DAI) Statistics

Valid ARP Requests : 1118
Valid ARP Replies : 18649
Invalid ARP Requests : 577
Invalid ARP Replies : 470
```

支持的版本

10.5.0 or later

## show ip arp inspection logging

显示有关启用了 DAI 的 VLAN 的 ARP 数据包信息。

语法

show ip arp inspection logging

默认

无

命令模式

EXEC

示例

```
OS10# show ip arp inspection logging
Total Number of Clients : 1
New Clients learnt in current Interval : 0
Invalid ARP packets in current interval :
0
Address Hw-Address Port VLAN First-detected-time Packet-
count

10.1.1.1 12:d3:43:a1:2e:23 ethernet1/1/1 10 00:23:14 2
```

支持的版本

10.5.0 or later

## show ip dhcp snooping binding

显示 DHCP 侦听绑定表的内容。

语法

show ip dhcp snooping binding [vlan **vlan-id**]

参数

- vlan **vlan-id**— 输入 VLAN ID。范围是从 1 到 4093。

默认

无

命令模式

EXEC

使用情况信息

动态学习的条目显示为 D，静态配置的条目显示为 S。

示例

```
OS10# show ip dhcp snooping binding

Codes : S - Static D - Dynamic

IPv4 Address MAC Address Expires(Sec) Type Interface VLAN
=====
10.1.1.22 11:22:11:22:11:22 120331 S ethernet1/1/4 100
10.1.1.44 11:22:11:22:11:23 120331 S port-channel100
200
10.1.1.5 11:22:11:22:11:24 120331 D ethernet1/1/5:4
300
```

支持的版本

10.5.0 or later

# DNS 命令

OS10 支持 DNS 主机和域参数的配置。

## ip domain-list

将域名添加到 DNS 列表。

|        |                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip domain-list [vrf vrf-name] [server-name] name</code>                                                                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"><li><code>vrf vrf-name</code> — (可选) 输入 <code>vrf</code> 和 VRF 的名称, 以将域名添加到与该 VRF 对应的 DNS 列表中。</li><li><code>server-name</code> — (可选) 输入服务器名称以将域名添加到 DNS 列表。</li><li><code>name</code> — 输入要附加到 DNS 列表中的域的名称。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                        |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                              |
| 使用情况信息 | 在 DNS 列表中最多有六个域名。使用 <code>ip domain-list</code> 命令可配置域名以完成非限定主机名称。域名在 DNS 请求中附加了不完整的主机名称。此命令的 <code>no</code> 版本将从 DNS 列表移除域名。                                                                                                                             |
| 示例     | <pre>OS10(config)# ip domain-list jay dell.com</pre>                                                                                                                                                                                                       |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                           |

## ip domain-name

配置默认域并附加到不完整的 DNS 请求。

|        |                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip domain-name [vrf vrf-name] server-name</code>                                                                                                                                |
| 参数     | <ul style="list-style-type: none"><li><code>vrf vrf-name</code> — (可选) 输入 <code>vrf</code> VRF 的名称, 然后配置与该 VRF 对应的域。</li><li><code>server-name</code> — (可选) 输入默认域使用的服务器名称。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                   |
| 命令模式   | CONFIGURATION                                                                                                                                                                         |
| 使用情况信息 | 此域将附加到不完整的 DNS 请求。此命令的 <code>no</code> 版本将值恢复为默认值。                                                                                                                                    |
| 示例     | <pre>OS10(config)# ip domain-name jay dell.com</pre>                                                                                                                                  |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                      |

## ip host

配置主机名称服务器与 IP 地址之间的映射。

|        |                                                                                                                                                                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip host [vrf vrf-name] [host-name] address</code>                                                                                                                                                                                                                |
| 参数     | <ul style="list-style-type: none"><li><code>vrf vrf-name</code> — (可选) 输入 <code>vrf</code> 和 VRF 的名称, 然后将名称服务器配置为该 VRF 的 IP 地址映射。</li><li><code>host-name</code> — (可选) 输入主机的名称。</li><li><code>address</code> — 输入名称服务器的 IPv4 或 IPv6 地址, 格式为 A.B.C.D 或 A::B。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                    |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                          |
| 使用情况信息 | 名称到 IP 地址表使用此映射信息解析主机名称。此命令的 <code>no</code> 版本将禁用映射。                                                                                                                                                                                                                  |

## 示例

```
OS10(config)# ip host dell 1.1.1.1
```

## 支持的版本

10.2.0E or later

## ip name-server

配置最多三个用于网络名称服务器的 IPv4 或 IPv6 地址。

### 语法

```
ip name-server ip-address [ip-address2 ip-address3]
```

### 参数

- *ip-address* — 输入要用于完成不合格名称的域名服务器的 IPv4 或 IPv6 地址，例如无法解析的不完整域名。
- *ip-address2 ip-address3* — （可选）输入两个附加 IPv4 或 IPv6 名称服务器，用空格分隔。

### 默认

未配置

### 命令模式

CONFIGURATION

### 使用情况信息

OS10 不支持通过 VLAN 发送 DNS 查询。DNS 查询在所有其他接口（包括管理端口）上发送出去。您可以单独配置 IPv4 和 IPv6 域名服务器。在双堆栈设置中，即使仅配置了此命令，系统也会将（请求 IPv4）和 AAAA（请求 IPv6）记录请求发送到 DNS 服务器。此命令的 `no` 版本将移除 IP 名称-服务器配置。

## 示例

```
OS10(config)# ip name-server 10.1.1.5
```

## 支持的版本

10.2.0E or later

## show hosts

显示主机表和 DNS 配置。

### 语法

```
show hosts [vrf vrf-name]
```

### 参数

*vrf vrf-name* — 输入 *vrf* 和 VRF 的名称，以显示与该 VRF 对应的 DNS 主机信息。

### 默认

未配置

### 命令模式

EXEC

### 使用情况信息

无

## 示例

```
OS10# show hosts
Default Domain Name : dell.com
Domain List : abc.com
Name Servers : 1.1.1.1 20::2
=====
 Static Host to IP mapping Table
=====
Host IP-Address

dell-pc1 20.1.1.1
```

## 支持的版本

10.2.0E or later

## IPv4 DHCP 限制

本部分列出了 DHCP 限制。

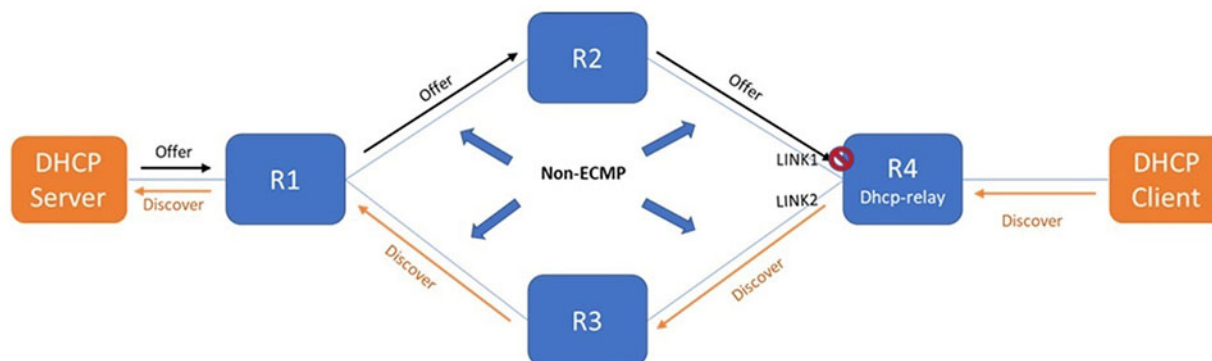
## IPv4 DHCP 非对称路由

OS10 不支持 IPv4 非对称路由的 DHCP 中继。OS10 支持 IPv6 非对称路由的 DHCP 中继。

DHCP 中继代理将侦听最佳 DHCP 服务器路径。如果通过 DHCP 中继代理程序未侦听的路径发送 DHCP OFFER 数据包，则 DHCP OFFER 数据包将丢弃。在这种情况下，已启用 DHCP 客户端的接口将不会接收 IPv4 地址。

例如，在下面的拓扑中，DHCP DISCOVER 数据包由链路 2 上的中继代理 (R4) 发送。中继代理路由表仅指向链路 2 以访问 DHCP 服务器。但是，DHCP 服务器会将 DHCP OFFER 数据包发送到不同路径上的中继代理 (R4)，并且将丢弃 DHCP OFFER 数据包。

发生此问题的原因是中继代理仅侦听可访问的 DHCP 服务器的最佳路径上行链路接口。



## 接口

您可以在第 2 层 (L2) 或第 3 层 (L3) 模式下配置和监控物理接口（以太网）、端口通道和虚拟局域网 (VLAN)。

**表. 21: 接口类型**

| 接口类型      | 支持    | 默认模式 | 需要创建      | 默认状态  |
|-----------|-------|------|-----------|-------|
| 以太网 (PHY) | L2、L3 | 未设置  | 否         | 未启用关闭 |
| 管理        | 不适用   | 不适用  | 否         | 未启用关闭 |
| 环回        | L3    | L3   | 是         | 未启用关闭 |
| 端口通道      | L2、L3 | 未设置  | 是         | 未启用关闭 |
| VLAN      | L2、L3 | L3   | 是，默认情况下除外 | 未启用关闭 |

## 以太网接口

默认情况下，以太网端口接口处于启用状态。要禁用以太网接口，请使用 `shutdown` 命令。使用 `show interface status` 命令可查看接口的状况。

要重新启用已禁用的接口，请使用 `no shutdown` 命令。

1. 在 Global CONFIGURATION 模式下配置以太网端口接口。

```
interface ethernet node/slot/port[:subport]
```

2. 在 INTERFACE 模式下禁用并重新启用以太网端口接口。

```
shutdown
```

```
no shutdown
```

## 禁用以太网端口接口

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# shutdown
```

## 启用以太网端口接口

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
```

## 统一端口组

在 OS10 统一端口组中，所有端口都在以太网或光纤通道 (FC) 模式下运行。您不能混用相同统一端口组中的端口模式。要激活以太网接口，请将端口组配置为在以太网模式下运行并指定端口速度。要激活光纤通道接口，请参阅[光纤通道接口](#)。

## S4148U-ON

在 S4148U-ON 交换机上，端口组中可用的以太网和光纤通道接口取决于当前配置的端口配置文件。有关详细信息，请参阅[S4148U-ON 端口配置文件](#)。

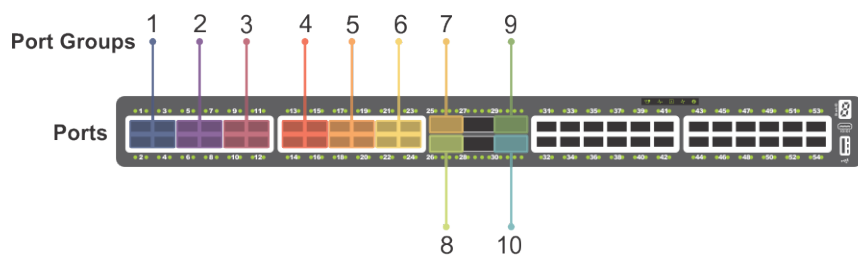


图 1: S4148U-ON 统一端口组

## MX9116n 结构交换引擎

在 MX9116n 结构交换引擎模块上：

- QSFP28-DD 端口组 1 至 12 仅在以太网模式下运行。有关详情，请参阅 [双密度 QSFP28 接口](#) 页面上的 275。
- 默认情况下，QSFP28 端口组 13 和 14 在以太网 1x100GE 模式下运行。
- 统一端口组 15 和 16 默认在以太网 1x100GE 模式下运行，并且支持光纤通道和其他以太网模式。在以太网模式下，统一端口组 15 和 16 包含的分解选项与 QSFP28-DD 和 QSFP28 端口组 1 至 14 不同。
- 如果 MX9116n 模块处于 SmartFabric 模式，则使用 OpenManage Enterprise-Modular 接口可为统一端口组配置分解接口和速度。

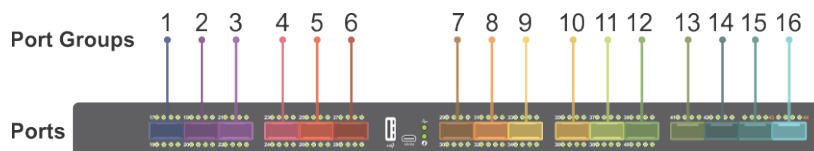


图 2: MX9116n 结构交换引擎统一端口组

要在统一端口组中启用以太网接口，请执行以下操作：

1. 在 CONFIGURATION 模式下配置统一端口组。为 *node/slot* 输入 1/1。端口组范围取决于交换机。

```
port-group node/slot/port-group
```

2. 在 PORT-GROUP 模式下为以太网操作激活统一端口组。要在光纤通道模式下激活统一端口组，请参阅[光纤通道接口](#)。可用的选项取决于交换机。

```
mode Eth {100g-1x | 50g-2x | 40g-1x | 25g-4x | 10g-4x}
```

- 100g-1x — 将端口组重置为 100GE 模式。
- 50g-2x — 将端口组拆分为两个 50GE 接口。
- 40g-1x — 将端口组设置为 40GE 模式，以便与 QSFP+ 40GE 收发器配合使用。
- 25g-4x — 将端口组拆分为四个 25GE 接口。
- 10g-4x — 将端口组拆分为四个 10GE 接口。

3. 返回 CONFIGURATION 模式。

```
exit
```

4. 进入以太网接口模式以配置其他设置。输入单个接口、连字符分隔的范围或用逗号分隔的多个接口。

```
interface ethernet node/slot/port[:subport]
```

## 配置以太网统一端口接口

```
OS10(config)# port-group 1/1/13
OS10(conf-pg-1/1/13)# mode Eth 25g-4x
OS10(conf-pg-1/1/13)# exit
OS10(config)# interface ethernet 1/1/41:1
OS10(conf-if-eth1/1/41:1)#
```



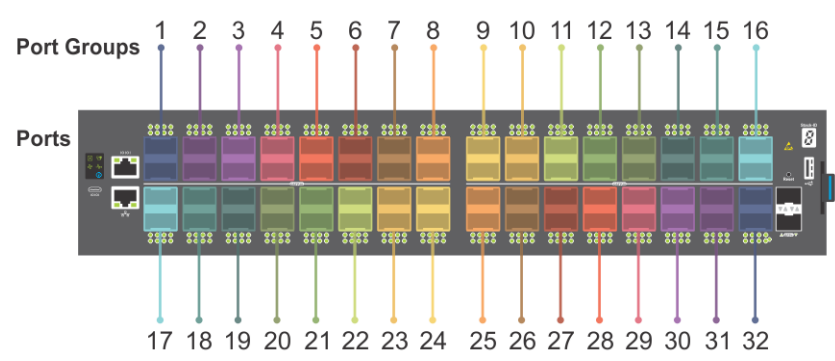
查看以太网统一端口接口

```
OS10(config)# interface ethernet 1/1/41
OS10(conf-if-eth1/1/41:1)# show configuration
!
interface ethernet1/1/41:1
no shutdown
```

Z9264F-ON port-group profiles

在 Z9264F-ON 交换机上，端口组配置文件将确定可用的前面板以太网端口和受支持的分解接口。QSFP28 端口只能在以太网模式下运行。使用端口组配置文件可配置分解接口并指定端口速度。

**注：**在 Z9264F-ON 端口上可启用以太网接口的配置步骤与 S4100-ON 系列不同。按照本中介介的步骤在 Z9264F-ON 交换机上配置分解接口。



每对奇数和偶数编号的端口均配置为端口组。例如：

| hybrid-group     | profile      | Ports  | Mode         |
|------------------|--------------|--------|--------------|
| port-group1/1/1  | restricted   | 1/1/1  | Eth 10g-4x   |
|                  |              | 1/1/2  | Eth Disabled |
| port-group1/1/2  | restricted   | 1/1/3  | Eth 10g-4x   |
|                  |              | 1/1/4  | Eth Disabled |
| port-group1/1/3  | restricted   | 1/1/5  | Eth 10g-4x   |
|                  |              | 1/1/6  | Eth Disabled |
| .                |              |        |              |
| .                |              |        |              |
| port-group1/1/31 | unrestricted | 1/1/61 | Eth 100g-1x  |
|                  |              | 1/1/62 | Eth 100g-1x  |
| port-group1/1/32 | unrestricted | 1/1/63 | Eth 100g-1x  |
|                  |              | 1/1/64 | Eth 100g-1x  |

在 Z9264F-ON 交换机上，端口组中的可用以太网接口取决于当前配置的端口组配置文件。有关端口组配置文件中支持的分解模式的详细信息，请参阅配置文件中 CLI 命令。

要启用以太网接口：

1. 在 CONFIGURATION 模式下配置 Z9264F-ON 端口组。为 node/slot 输入 1/1。端口组的范围从 1 到 32。

```
port-group node/slot/port-group
```

2. 在 PORT-GROUP 模式下配置受限配置文件。此命令仅适用于端口组中的奇数端口，并且将禁用端口组中的偶数编号端口。

```
profile restricted
```

3. 为端口组内的奇数端口配置端口模式。

```
port node/slot/port mode Eth port-mode
```

- 100g-1x — 将端口重置为 100GE 模式。
- 40g-1x — 将端口设置为 40GE 模式，以便与 QSFP+40GE 收发器配合使用。

- 25g-4x — 将一个端口拆分为四个 25GE 接口。
- 10g-4x — 将一个端口拆分为四个 10GE 接口。

4. 返回 CONFIGURATION 模式。

```
exit
```

5. 进入以太网接口模式以配置其他设置。输入单个接口、连字符分隔的范围或用逗号分隔的多个接口。

```
interface ethernet node/slot/port[:subport]
```

配置受限端口组配置文件

```
OS10(config)# port-group 1/1/2
OS10(conf-pg-1/1/2)# profile restricted
OS10(conf-pg-1/1/2)# port 1/1/3 mode Eth 25g-4x
OS10(conf-pg-1/1/2)# exit
OS10(config)# interface ethernet 1/1/3:2
OS10(conf-if-eth1/1/3:2)#
```

查看接口

```
OS10(config)# interface ethernet 1/1/3:2
OS10(conf-if-eth1/1/3:2)# show configuration
!
interface ethernet1/1/3:2
no shutdown
```

# S5200F-ON 交换机上的端口组

在 S5200F-ON 系列交换机上，端口组确定可用的前面板以太网端口和受支持的分解接口。

当您将其某个端口转换为特定模式时，属于该端口组的所有端口也会在相同的模式下运行。例如，如果您将以太网 1/1/1 接口转换为 10g-4x，则属于端口组 1/1/1（即 1/1/2、1/1/3 和 1/1/4）的所有其他接口也会以 10g-4x 的模式运行。

下图显示了 S5212F-ON 交换机上支持的端口组和分解模式：

```
OS10# show port-group

Port-group Mode Ports FEM
port-group1/1/1 Eth 10g-4x 1 2 3 4 -
port-group1/1/2 Eth 10g-4x 5 6 7 8 -
port-group1/1/3 Eth 10g-4x 9 10 11 12 -
port-group1/1/4 Eth 100g-1x 13 -
port-group1/1/5 Eth 100g-1x 14 -
port-group1/1/6 Eth 100g-1x 15 -
```

表. 22: S5212F-ON 交换机上的端口组和分解模式

| 端口组             | 端口         | 支持的分解模式                                                                                                                       |
|-----------------|------------|-------------------------------------------------------------------------------------------------------------------------------|
| Port-group1/1/1 | 1、2、3、4    | <ul style="list-style-type: none"><li>• 25g-4x</li><li>• 10g-4x</li></ul>                                                     |
| Port-group1/1/2 | 5、6、7、8    | <ul style="list-style-type: none"><li>• 25g-4x</li><li>• 10g-4x</li></ul>                                                     |
| Port-group1/1/3 | 9、10、11、12 | <ul style="list-style-type: none"><li>• 25g-4x</li><li>• 10g-4x</li></ul>                                                     |
| Port-group1/1/4 | 13         | <ul style="list-style-type: none"><li>• 100g-1x</li><li>• 50g-2x</li><li>• 40g-1x</li><li>• 25g-4x</li><li>• 10g-4x</li></ul> |

表. 22: S5212F-ON 交换机上的端口组和解模模式 (续)

| 端口组              | 端口 | 支持的解模模式                                                                                                                             |
|------------------|----|-------------------------------------------------------------------------------------------------------------------------------------|
| Port-group1/1/14 | 14 | <ul style="list-style-type: none"> <li>• 100g-1x</li> <li>• 50g-2x</li> <li>• 40g-1x</li> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul> |
| Port-group1/1/6  | 15 | <ul style="list-style-type: none"> <li>• 100g-1x</li> <li>• 50g-2x</li> <li>• 40g-1x</li> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul> |

下图显示了 S5224F-ON 交换机上支持的端口组和解模模式：

```
OS10# show port-group
Port-group Mode Ports FEM
port-group1/1/1 Eth 10g-4x 1 2 3 4 -
port-group1/1/2 Eth 10g-4x 5 6 7 8 -
port-group1/1/3 Eth 10g-4x 9 10 11 12 -
port-group1/1/4 Eth 10g-4x 13 14 15 16 -
port-group1/1/5 Eth 10g-4x 17 18 19 20 -
port-group1/1/6 Eth 10g-4x 21 22 23 24 -
port-group1/1/7 Eth 100g-1x 25 -
port-group1/1/8 Eth 100g-1x 26 -
port-group1/1/9 Eth 100g-1x 27 -
port-group1/1/10 Eth 100g-1x 28 -
```

表. 23: S5224F-ON 交换机上的端口组和解模模式

| 端口组             | 端口          | 支持的解模模式                                                                                                                             |
|-----------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Port-group1/1/1 | 1、2、3、4     | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/2 | 5、6、7、8     | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/3 | 9、10、11、12  | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/4 | 13、14、15、16 | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/5 | 17、18、19、20 | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/6 | 21、22、23、24 | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/7 | 25          | <ul style="list-style-type: none"> <li>• 100g-1x</li> <li>• 50g-2x</li> <li>• 40g-1x</li> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul> |
| Port-group1/1/8 | 26          | <ul style="list-style-type: none"> <li>• 100g-1x</li> <li>• 50g-2x</li> <li>• 40g-1x</li> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul> |

表. 23: S5224F-ON 交换机上的端口组和解析模式 （续）

| 端口组              | 端口 | 支持的解析模式                                                                                                                       |
|------------------|----|-------------------------------------------------------------------------------------------------------------------------------|
| Port-group1/1/9  | 27 | <ul style="list-style-type: none"><li>• 100g-1x</li><li>• 50g-2x</li><li>• 40g-1x</li><li>• 25g-4x</li><li>• 10g-4x</li></ul> |
| Port-group1/1/10 | 28 | <ul style="list-style-type: none"><li>• 100g-1x</li><li>• 50g-2x</li><li>• 40g-1x</li><li>• 25g-4x</li><li>• 10g-4x</li></ul> |

下图显示了 S5248F-ON 交换机上支持的端口组和解析模式：

```
OS10# show port-group
Port-group Mode Ports FEM
port-group1/1/1 Eth 25g-4x 1 2 3 4 -
port-group1/1/2 Eth 25g-4x 5 6 7 8 -
port-group1/1/3 Eth 25g-4x 9 10 11 12 -
port-group1/1/4 Eth 25g-4x 13 14 15 16 -
port-group1/1/5 Eth 25g-4x 17 18 19 20 -
port-group1/1/6 Eth 25g-4x 21 22 23 24 -
port-group1/1/7 Eth 25g-4x 25 26 27 28 -
port-group1/1/8 Eth 25g-4x 29 30 31 32 -
port-group1/1/9 Eth 25g-4x 33 34 35 36 -
port-group1/1/10 Eth 25g-4x 37 38 39 40 -
port-group1/1/11 Eth 25g-4x 41 42 43 44 -
port-group1/1/12 Eth 25g-4x 45 46 47 48 -
port-group1/1/13 Eth 100g-2x 49 50 -
port-group1/1/14 Eth 100g-2x 51 52 -
port-group1/1/15 Eth 100g-1x 53 -
port-group1/1/16 Eth 100g-1x 54 -
port-group1/1/17 Eth 100g-1x 55 -
port-group1/1/18 Eth 100g-1x 56 -
```

表. 24: S5248F-ON 交换机上的端口组和解析模式

| 端口组             | 端口          | 支持的解析模式                                                                   |
|-----------------|-------------|---------------------------------------------------------------------------|
| Port-group1/1/1 | 1、2、3、4     | <ul style="list-style-type: none"><li>• 25g-4x</li><li>• 10g-4x</li></ul> |
| Port-group1/1/2 | 5、6、7、8     | <ul style="list-style-type: none"><li>• 25g-4x</li><li>• 10g-4x</li></ul> |
| Port-group1/1/3 | 9、10、11、12  | <ul style="list-style-type: none"><li>• 25g-4x</li><li>• 10g-4x</li></ul> |
| Port-group1/1/4 | 13、14、15、16 | <ul style="list-style-type: none"><li>• 25g-4x</li><li>• 10g-4x</li></ul> |
| Port-group1/1/5 | 17、18、19、20 | <ul style="list-style-type: none"><li>• 25g-4x</li><li>• 10g-4x</li></ul> |
| Port-group1/1/6 | 21、22、23、24 | <ul style="list-style-type: none"><li>• 25g-4x</li><li>• 10g-4x</li></ul> |
| Port-group1/1/7 | 25、26、27、28 | <ul style="list-style-type: none"><li>• 25g-4x</li><li>• 10g-4x</li></ul> |
| Port-group1/1/8 | 29、30、31、32 | <ul style="list-style-type: none"><li>• 25g-4x</li><li>• 10g-4x</li></ul> |
| Port-group1/1/9 | 33、34、35、36 | <ul style="list-style-type: none"><li>• 25g-4x</li></ul>                  |

表. 24: S5248F-ON 交换机上的端口组和解析模式 (续)

| 端口组              | 端口          | 支持的解析模式                                                                                                                   |
|------------------|-------------|---------------------------------------------------------------------------------------------------------------------------|
|                  |             | <ul style="list-style-type: none"> <li>10g-4x</li> </ul>                                                                  |
| Port-group1/1/10 | 37、38、39、40 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul>                                                  |
| Port-group1/1/11 | 41、42、43、44 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul>                                                  |
| Port-group1/1/12 | 45、46、47、48 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul>                                                  |
| Port-group1/1/13 | 49、50       | <ul style="list-style-type: none"> <li>100g-2x</li> <li>50g-4x</li> <li>40g-2x</li> <li>25g-8x</li> <li>10g-8x</li> </ul> |
| Port-group1/1/14 | 51、52       | <ul style="list-style-type: none"> <li>100g-2x</li> <li>50g-4x</li> <li>40g-2x</li> <li>25g-8x</li> <li>10g-8x</li> </ul> |
| Port-group1/1/15 | 53          | <ul style="list-style-type: none"> <li>100g-1x</li> <li>50g-2x</li> <li>40g-1x</li> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/16 | 54          | <ul style="list-style-type: none"> <li>100g-1x</li> <li>50g-2x</li> <li>40g-1x</li> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/17 | 55          | <ul style="list-style-type: none"> <li>100g-1x</li> <li>50g-2x</li> <li>40g-1x</li> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/18 | 56          | <ul style="list-style-type: none"> <li>100g-1x</li> <li>50g-2x</li> <li>40g-1x</li> <li>25g-4x</li> <li>10g-4x</li> </ul> |

下图显示了 S5296F-ON 交换机上支持的端口组和解析模式：

```
OS10# show port-group
```

| Port-group       | Mode       | Ports       | FEM |
|------------------|------------|-------------|-----|
| port-group1/1/1  | Eth 25g-4x | 1 2 3 4     | -   |
| port-group1/1/2  | Eth 25g-4x | 5 6 7 8     | -   |
| port-group1/1/3  | Eth 25g-4x | 9 10 11 12  | -   |
| port-group1/1/4  | Eth 25g-4x | 13 14 15 16 | -   |
| port-group1/1/5  | Eth 25g-4x | 17 18 19 20 | -   |
| port-group1/1/6  | Eth 25g-4x | 21 22 23 24 | -   |
| port-group1/1/7  | Eth 25g-4x | 25 26 27 28 | -   |
| port-group1/1/8  | Eth 25g-4x | 29 30 31 32 | -   |
| port-group1/1/9  | Eth 25g-4x | 33 34 35 36 | -   |
| port-group1/1/10 | Eth 25g-4x | 37 38 39 40 | -   |

|                  |             |     |    |    |    |   |   |
|------------------|-------------|-----|----|----|----|---|---|
| port-group1/1/11 | Eth 10g-4x  | 41  | 42 | 43 | 44 | - |   |
| port-group1/1/12 | Eth 25g-4x  | 45  | 46 | 47 | 48 | - |   |
| port-group1/1/13 | Eth 25g-4x  | 49  | 50 | 51 | 52 | - |   |
| port-group1/1/14 | Eth 25g-4x  | 53  | 54 | 55 | 56 | - |   |
| port-group1/1/15 | Eth 25g-4x  | 57  | 58 | 59 | 60 | - |   |
| port-group1/1/16 | Eth 25g-4x  | 61  | 62 | 63 | 64 | - |   |
| port-group1/1/17 | Eth 25g-4x  | 65  | 66 | 67 | 68 | - |   |
| port-group1/1/18 | Eth 25g-4x  | 69  | 70 | 71 | 72 | - |   |
| port-group1/1/19 | Eth 25g-4x  | 73  | 74 | 75 | 76 | - |   |
| port-group1/1/20 | Eth 25g-4x  | 77  | 78 | 79 | 80 | - |   |
| port-group1/1/21 | Eth 25g-4x  | 81  | 82 | 83 | 84 | - |   |
| port-group1/1/22 | Eth 25g-4x  | 85  | 86 | 87 | 88 | - |   |
| port-group1/1/23 | Eth 25g-4x  | 89  | 90 | 91 | 92 | - |   |
| port-group1/1/24 | Eth 25g-4x  | 93  | 94 | 95 | 96 | - |   |
| port-group1/1/25 | Eth 100g-1x | 97  |    |    |    |   | - |
| port-group1/1/26 | Eth 100g-1x | 98  |    |    |    |   | - |
| port-group1/1/27 | Eth 100g-1x | 99  |    |    |    |   | - |
| port-group1/1/28 | Eth 100g-1x | 100 |    |    |    |   | - |
| port-group1/1/29 | Eth 100g-1x | 101 |    |    |    |   | - |
| port-group1/1/30 | Eth 100g-1x | 102 |    |    |    |   | - |
| port-group1/1/31 | Eth 100g-1x | 103 |    |    |    |   | - |
| port-group1/1/32 | Eth 100g-1x | 104 |    |    |    |   | - |

**表. 25: S5296F-ON 交换机上的端口组和解模模式**

| 端口组              | 端口          | 支持的分解模式                                                                  |
|------------------|-------------|--------------------------------------------------------------------------|
| Port-group1/1/1  | 1、2、3、4     | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/2  | 5、6、7、8     | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/3  | 9、10、11、12  | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/4  | 13、14、15、16 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/5  | 17、18、19、20 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/6  | 21、22、23、24 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/7  | 25、26、27、28 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/8  | 29、30、31、32 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/9  | 33、34、35、36 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/10 | 37、38、39、40 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/11 | 41、42、43、44 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/12 | 45、46、47、48 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/13 | 49、50、51、52 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/14 | 53、54、55、56 | <ul style="list-style-type: none"> <li>25g-4x</li> <li>10g-4x</li> </ul> |
| Port-group1/1/15 | 57、58、59、60 | <ul style="list-style-type: none"> <li>25g-4x</li> </ul>                 |

表. 25: S5296F-ON 交换机上的端口组和分解模式 (续)

| 端口组              | 端口          | 支持的分解模式                                                                                                                             |
|------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------|
|                  |             | <ul style="list-style-type: none"> <li>• 10g-4x</li> </ul>                                                                          |
| Port-group1/1/16 | 61、62、63、64 | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/17 | 65、66、67、68 | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/18 | 69、70、71、72 | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/19 | 73、74、75、76 | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/20 | 77、78、79、80 | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/21 | 81、82、83、84 | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/22 | 85、86、87、88 | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/23 | 89、90、91、92 | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/24 | 93、94、95、96 | <ul style="list-style-type: none"> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul>                                                        |
| Port-group1/1/25 | 97          | <ul style="list-style-type: none"> <li>• 100g-1x</li> <li>• 50g-2x</li> <li>• 40g-1x</li> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul> |
| Port-group1/1/26 | 98          | <ul style="list-style-type: none"> <li>• 100g-1x</li> <li>• 50g-2x</li> <li>• 40g-1x</li> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul> |
| Port-group1/1/27 | 99          | <ul style="list-style-type: none"> <li>• 100g-1x</li> <li>• 50g-2x</li> <li>• 40g-1x</li> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul> |
| Port-group1/1/28 | 100         | <ul style="list-style-type: none"> <li>• 100g-1x</li> <li>• 50g-2x</li> <li>• 40g-1x</li> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul> |
| Port-group1/1/29 | 101         | <ul style="list-style-type: none"> <li>• 100g-1x</li> <li>• 50g-2x</li> <li>• 40g-1x</li> <li>• 25g-4x</li> <li>• 10g-4x</li> </ul> |
| Port-group1/1/30 | 102         | <ul style="list-style-type: none"> <li>• 100g-1x</li> <li>• 50g-2x</li> </ul>                                                       |

表. 25: S5296F-ON 交换机上的端口组和分解模式 （续）

| 端口组              | 端口  | 支持的分解模式                                                                                                                       |
|------------------|-----|-------------------------------------------------------------------------------------------------------------------------------|
|                  |     | <ul style="list-style-type: none"><li>• 40g-1x</li><li>• 25g-4x</li><li>• 10g-4x</li></ul>                                    |
| Port-group1/1/31 | 103 | <ul style="list-style-type: none"><li>• 100g-1x</li><li>• 50g-2x</li><li>• 40g-1x</li><li>• 25g-4x</li><li>• 10g-4x</li></ul> |
| Port-group1/1/32 | 104 | <ul style="list-style-type: none"><li>• 100g-1x</li><li>• 50g-2x</li><li>• 40g-1x</li><li>• 25g-4x</li><li>• 10g-4x</li></ul> |

要配置分解模式，请执行以下操作：

1. 在 CONFIGURATION 模式下配置端口组。为 *node/slot* 和端口组编号输入 1/1。

```
port-group node/slot/port-group
```

2. 在 PORT-GROUP 模式下配置分解模式。

```
mode Eth breakout-mode
```

- 100g-2x — 将端口组拆分为两个 100GE 接口。
  - 100g-1x — 将端口组设置为 100GE 模式。
  - 50g-4x — 将端口组拆分为四个 50GE 接口。
  - 50g-2x — 将端口组拆分为两个 50GE 接口。
  - 40g-2x — 将端口组拆分为两个 40GE 接口，以便与 QSFP+ 40GE 收发器配合使用。
  - 40g-1x — 将端口组设置为 40GE 模式，以便与 QSFP+ 40GE 收发器配合使用。
  - 25g-8x — 将端口组拆分为八个 25GE 接口。
  - 25g-4x — 将端口组拆分为四个 25GE 接口。
  - 10g-8x — 将端口组拆分为八个 10GE 接口。
  - 10g-4x — 将端口组拆分为四个 10GE 接口。
3. 返回 CONFIGURATION 模式。

```
exit
```

4. 输入接口分解模式以配置其他设置，例如速度。

```
interface ethernet node/slot/port[:subport]
```

下面显示了将端口组从 25g-4x 模式转换为 10g-4x 模式：

```
OS10# configure terminal
OS10(config)# port-group 1/1/1
OS10(conf-pg-1/1/1)# mode Eth 10g-4x
OS10(conf-pg-1/1/1)# exit
OS10(config)# interface ethernet 1/1/1:1
OS10(conf-if-eth1/1/1:1)# speed
1000 Set speed to 1000 Mbps
10000 Set speed to 10000 Mbps
auto Automatic Settings (default)
OS10(conf-if-eth1/1/1:1)# speed 1000
```



## L2 模式配置

每个物理以太网接口使用唯一的 MAC 地址。端口通道和 VLAN 使用单个 MAC 地址。默认情况下，所有接口在 L2 模式下运行。在 L2 模式下，您可以在接口上配置交换和 L2 协议，例如 VLAN 和生成树协议 (STP)。

在访问或中继模式下启用端口接口上的 L2 交换。默认情况下，在访问模式下配置接口。访问模式允许 L2 交换单个 VLAN 上的未标记流量（VLAN 1 为默认值）。中继模式允许 L2 交换访问 VLAN 上的未标记流量，并在一个或多个 VLAN 上标记流量。

默认情况下，端口的本机 VLAN 是交换机的默认 VLAN ID。您可以使用 `switchport access vlan vlan-id` 命令更改本机 VLAN。

中继接口具有使用 802.1q 封装标记的 VLAN 流量。如果访问接口接收的数据包中的 802.1q 标记与访问 VLAN ID 不同，则会丢弃数据包。

默认情况下，中继接口仅将未标记的流量传送到访问 VLAN 上。必须手动配置标记的流量的其他 VLAN。

### 1. 选择两个可用选项之一：

- 在 INTERFACE 模式下配置 L2 中继以及端口可以传输的已标记 VLAN 流量。默认情况下，中继端口不会添加到任何已标记的 VLAN。您必须先创建 VLAN，然后才能为其分配接口。

```
switchport mode trunk
switchport trunk allowed vlan vlan-id-list
```

- 在 INTERFACE 模式下重新配置分配给 L2 访问或中继端口的访问 VLAN。

```
switchport access vlan vlan-id
```

### 2. 在 INTERFACE 模式下启用用于 L2 流量传输的接口。

```
no shutdown
```

### L2 接口配置

```
OS10(config)# interface ethernet 1/1/7
OS10(conf-if-eth1/1/7)# switchport mode trunk
OS10(conf-if-eth1/1/7)# switchport trunk allowed vlan 5,10
OS10(conf-if-eth1/1/7)# no shutdown
```

## L3 模式配置

默认情况下，以太网和端口通道接口处于 L2 访问模式。禁用 L2 模式，然后将 IP 地址分配给以太网端口接口时，您将该端口置于 L3 模式下。

在 L3 模式下配置一个主 IP 地址。您可以在一个接口上配置最多 255 个次要 IP 地址。系统中至少有一个接口必须处于 L3 模式，然后才能配置或输入 L3 协议模式，如 OSPF。

### 1. 从 INTERFACE 模式下的 L2 交换中移除端口。

```
no switchport
```

### 2. 在 INTERFACE 模式下配置 L3 路由。添加 secondary 以配置备份 IP 地址。

```
ip address address [secondary]
```

### 3. 在 INTERFACE 模式下启用用于 L3 流量传输的接口。

```
no shutdown
```

### L3 接口配置

```
OS10(config)# interface ethernet 1/1/9
OS10(conf-if-eth1/1/9)# no switchport
OS10(conf-if-eth1/1/9)# ip address 10.10.1.92/24
OS10(conf-if-eth1/1/9)# no shutdown
```

查看 L3 配置错误

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip address 1.1.1.1/24
% Error: remove Layer 2 configuration before assigning an IP
```

光纤通道接口

OS10 统一端口组支持 FC 接口。统一端口组在光纤通道或以太网模式下运行。要激活 FC 接口，请将端口组配置为在光纤通道模式下运行并指定端口速度。默认情况下，FC 接口已禁用。

S4148U-ON

在 S4148U-ON 交换机上，FC 接口在所有端口组中可用。激活的 FC 接口取决于当前配置的端口配置文件。有关详细信息，请参阅 [S4148U-ON 端口配置文件](#)。

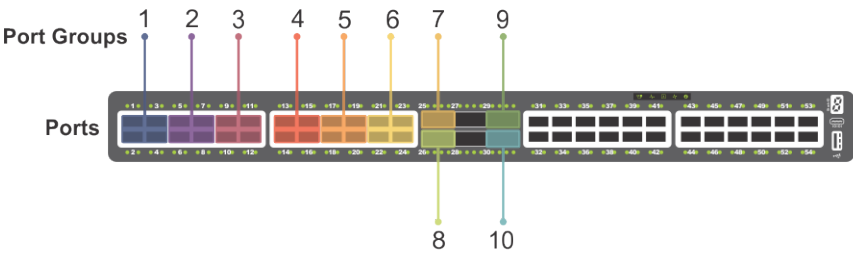


图 3: S4148U-ON 统一端口组

MX9116n 结构交换引擎

在 MX9116n 结构交换引擎模块上，FC 接口仅在统一端口组 15 和 16（端口 43 和 44）中可用。

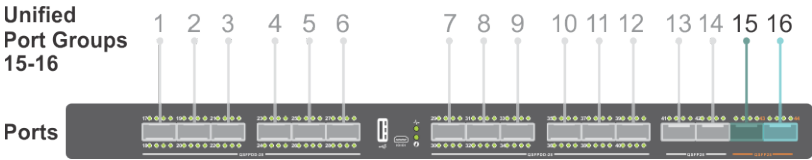


图 4: MX9116n 结构交换引擎 — 统一端口组

- 1. 在 CONFIGURATION 模式下配置统一端口组。为 *node/slot* 输入 1/1。端口组范围取决于交换机。

```
port-group node/slot/port-group
```

- 2. 在 PORT-GROUP 模式下为 FC 操作激活统一端口组。可用的 FC 模式取决于交换机。

```
mode fc {32g-4x | 32g-2x | 32g-1x | 16g-4x}
```

- 16g-4x — 将统一端口组拆分为四个 16 GFC 接口。
- 32g-1x — 将统一端口组拆分为一个 32 GFC 接口。1x-32G 接口的速率限制为 28G。
- 32g-2x — 将统一端口组拆分为两个 32 GFC 接口。
- 32g-4x — 将统一端口组拆分为四个 32 GFC 接口。每个 4x-32GE 分解接口的速率限制为 25G。

- 3. 返回 CONFIGURATION 模式。

```
exit
```

- 4. 进入 FC 接口模式以启用数据传输。输入单个接口、连字符分隔的范围或用逗号分隔的多个接口。

```
interface fibrechannel node/slot/port[:subport]
```

5. (可选) 在 INTERFACE 模式下重新配置接口速度。

```
speed {8 | 16 | 32 | auto}
```

6. 在接口上应用 vfabric 配置。有关 vfabric 配置的详细信息, 请参阅[虚拟连接结构](#)。

```
vfabric fabric-ID
```

7. 在 INTERFACE 模式下启用 FC 接口。

```
no shutdown
```

## 配置 FC 接口

```
OS10(config)# port-group 1/1/15
OS10(conf-pg-1/1/15)# mode FC 16g-4x
OS10(conf-pg-1/1/15)# exit
OS10(config)# interface fibrechannel 1/1/43:1
OS10(conf-if-fc-1/1/43:1)# speed 32
OS10(conf-if-fc-1/1/43:1)# no shutdown
```

## 查看 FC 接口

```
OS10(config)# interface fibrechannel 1/1/43:1
OS10(conf-if-fc-1/1/43:1)# show configuration
!
interface fibrechannel1/1/43:1
 no shutdown
 speed 32
 vfabric 100
```

```
OS10# show interface fibrechannel 1/1/43:1
Fibrechannel 1/1/43:1 is up, FC link is up
Address is 14:18:77:20:8d:fc, Current address is 14:18:77:20:8d:fc
Pluggable media present, QSFP+ type is QSFP+ 4x(16GBASE FC SW)
 Wavelength is 850
 Receive power reading is 0.0
FC MTU 2188 bytes
LineSpeed 8G
Port type is F, Max BB credit is 1
WWN is 20:78:14:18:77:20:8d:cf
Last clearing of "show interface" counters: 00:02:32
Input statistics:
 33 frames, 3508 bytes
 0 class 2 good frames, 33 class 3 good frames
 0 frame too long, 0 frame truncated, 0 CRC
 1 link fail, 0 sync loss
 0 primitive seq err, 0 LIP count
 0 BB credit 0, 0 BB credit 0 packet drops
Output statistics:
 33 frames, 2344 bytes
 0 class 2 frames, 33 class 3 frames
 0 BB credit 0, 0 oversize frames
6356027325 total errors
Rate Info:
 Input 116 bytes/sec, 1 frames/sec, 0% of line rate
 Output 78 bytes/sec, 1 frames/sec, 0% of line rate
Time since last interface status change: 00:00:24
```

## 配置波长

您可以为 SPF+ 光学器件配置光纤传输波长值。此配置使您能够将激光波长和频率调整为最多两个小数位数（以纳米级为单位）。

当 SPF+ 光学器件插入接口时, 要配置和查看光纤传输波长, 请执行以下操作:

1. 在接口配置模式下，输入以下命令：

```
wavelength wavelength-value
```

**注：**支持的波长范围为 1528.38 nm 至 1568.77 nm。

```
OS10(config-if-eth1/1/14)# wavelength 1530.00
```

2. 使用以下命令查看您配置的光纤传输值：

```
show interface phy-eth interface transceiver | grep "Tunable wavelength"
```

```
OS10# show interface phy-eth 1/1/14 transceiver | grep "Tunable wavelength"
SFP1/1/14 Tunable wavelength= 1530.000nm
```

**注：**要指定波长值，必须确切输入六位数字 — 在小数点前面四位，在小数点后面两位。值必须符合以下格式：ABCD.EF，例如，1545.23。任何不符合此格式的数字都会被拒绝，包括完整的数字，如 1568。但是，接受以下类型的值：1568.00。

## 管理接口

管理接口提供对网络设备的 OOB 管理访问权限。您可以配置管理接口，但此接口上的配置选项会受到限制。如果网关地址和 IP 地址出现在主路由表中，则无法配置它们。此接口不支持代理 ARP。

1. 在 CONFIGURATION 模式下配置管理接口。

```
interface mgmt 1/1/1
```

2. 默认情况下，DHCP 客户端在管理接口上处于启用状态。在 INTERFACE 模式下禁用 DHCP 客户端操作。

```
no ip address dhcp
```

3. 在 INTERFACE 模式下配置管理接口上的 IP 地址和掩码。

```
ip address A.B.C.D/prefix-length
```

4. 在 INTERFACE 模式下启用管理接口。

```
no shutdown
```

### 配置管理接口

```
OS10(config)# interface mgmt 1/1/1
OS10(config-if-ma-1/1/1)# no ip address dhcp
OS10(config-if-ma-1/1/1)# ip address 10.1.1.10/24
OS10(config-if-ma-1/1/1)# no shutdown
```

## 管理接口

对于管理连接，请使用管理 VLAN。VLAN 4020 是默认的管理 VLAN，默认情况下处于启用状态。Mgmt1/1/1 端口是 VLAN 4020 的一部分。

您不能在管理接口上配置网关地址、IP 地址和代理 ARP。

## VLAN 接口

VLAN 是逻辑接口，默认情况下，在 L2 模式下。物理接口和端口通道可以是 VLAN 的成员。

OS10 支持 VLAN 间的路由。您可以将 IP 地址添加到 VLAN，并以物理接口的使用方式在路由协议中使用。

在路由协议中使用 VLAN 时，您必须配置 `no shutdown` 命令以启用 VLAN 路由流量。在 VLAN 中，`shutdown` 命令可防止 L3 流量通过该接口。L2 流量不受此命令的影响。

- 在 INTERFACE 模式下的接口上以 A.B.C.D/x 格式配置 IP 地址。次要 IP 地址是接口的备份 IP 地址。

```
ip address ip-address/mask [secondary]
```

## 配置 VLAN

```
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)# ip address 1.1.1.2/24
```

您不能同时在同一 VLAN 上使用出口速率塑型和入口速率监察。

# 用户配置的默认 VLAN

默认情况下，VLAN1 用作默认 VLAN，用于在中继或访问模式下切换 OS10 端口上未标记的 L2 流量。默认 VLAN 用于在交换机之间发送和接收未标记的协议流量，例如 STP。如果您将 VLAN1 用于数据流量以满足特定于网络的需求，请重新配置默认 VLAN 的 VLAN ID。

- 在 CONFIGURATION 模式下为默认 VLAN 分配新的 VLAN ID，从 1 到 4093。

```
default vlan-id vlan-id
```

在 `show vlan` 输出中，星号 (\*) 表示默认 VLAN。

## 重新配置默认 VLAN

```
OS10# show vlan
Q: A - Access (Untagged), T - Tagged
 NUM Status Description Q Ports
* 1 up
Eth1/1/1-1/1/25,1/1/29,1/1/31-1/1/54

OS10(config)# interface vlan 10
Sep 19 17:28:10 OS10 dn_ifm[932]: Node.1-Unit.1:PRI:notice [os10:notify],
%Dell EMC (OS10) %IFM_ASTATE_UP: Interface admin state up :vlan10
OS10(conf-if-vl-10)# exit

OS10(config)# default vlan-id 10
Sep 19 17:28:15 OS10 dn_ifm[932]: Node.1-Unit.1:PRI:notice [os10:trap], %Dell EMC (OS10)
%IFM_OSTATE_DN: Interface operational state is down :vlan1
Sep 19 17:28:16 OS10 dn_ifm[932]: Node.1-Unit.1:PRI:notice [os10:trap], %Dell EMC (OS10)
%IFM_OSTATE_UP: Interface operational state is up :vlan10

OS10(config)# do show vlan
Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring VLANs
Q: A - Access (Untagged), T - Tagged
 NUM Status Description Q Ports
* 1 down
* 10 up
Eth1/1/1-1/1/25,1/1/29,1/1/31-1/1/54
```

# VLAN 扩展配置文件

在交换机上扩展 VLAN 数量时，使用 VLAN 扩展配置文件。VLAN 扩展配置文件占用的内存较少。在交换机上配置 VLAN 之前，请先启用扩展配置文件。扩展配置文件在您创建的所有 VLAN 上全局应用 L2 模式，并禁用 L3 传输。要启用 VLAN 上的 L3 路由流量，请使用 `mode L3` 命令。

**注：**使用 VLAN 扩展配置文件配置时，第 3 个 VLAN、已启用 IGMP 侦听的 VLAN 和 FCoE VLAN 需要 `mode L3` 配置。

- 在 CONFIGURATION 模式下配置 L2 VLAN 扩展配置文件。

```
scale-profile vlan
```

2. (可选) 在 INTERFACE VLAN 模式下在 VLAN 上启用 L3 路由。

```
mode L3
```

在使用已配置的 VLAN 从较低版本升级 OS10 之后, 如果配置 VLAN 扩展配置文件并在 VLAN 上启用 L3 路由, 请保存配置并使用 reload 命令应用扩展配置文件设置。

### 应用 VLAN 扩展配置文件

```
OS10(config)# scale-profile vlan
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)# mode L3
```

在配置扩展配置文件 VLAN 时, Dell EMC 建议以下顺序:

1. 使用 scale-profile vlan 命令可启用扩展配置文件 VLAN。
2. 禁用 IGMP 和 MLDP。

有关禁用 IGMP 和 MLD 的详细信息, 请参阅[互联网组管理协议](#)和[多播侦听器查找协议](#)。

3. 将生成树模式配置为 RSTP。
4. 配置 VLAN。
5. 进入以太网接口模式并将 VLAN 添加到接口。

 **注:** 请勿使用 interface range 命令进入以太网接口模式。

## 环回接口

环回接口是软件模拟接口的虚拟接口。由于环回接口与物理硬件实体无关, 因此环回接口状态不受硬件状态更改的影响。

路由至本地到 OS10 设备的环回接口进程的数据包。由于此接口不是物理接口, 因此为提供协议稳定性, 您可以在此接口上配置路由协议。您可以将环回接口置于默认的 L3 模式下。

- 在 CONFIGURATION 模式下输入环回接口编号, 从 0 到 16383。

```
interface loopback number
```

- 在 EXEC 模式下输入环回接口编号以查看配置。

```
show interface loopback number
```

- 在 CONFIGURATION 模式下输入要删除的环回接口的环回接口编号。

```
no interface loopback number
```

### 查看环回接口

```
OS10# show interface loopback 4
Loopback 4 is up, line protocol is up
Hardware is unknown.
Interface index is 102863300
Internet address is 120.120.120.120/24
Mode of IPv4 Address Assignment : MANUAL
MTU 1532 bytes
Flowcontrol rx false tx false
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters : 00:00:11
Queuing strategy : fifo
 Input 0 packets, 0 bytes, 0 multicast
 Received 0 errors, 0 discarded
 Output 0 packets, 0 bytes, 0 multicast
 Output 0 errors, Output 0 invalid protocol
Time since last interface status change : 00:00:11
```

# 端口通道接口

默认情况下未配置端口通道。链路聚合 (LA) 是一种将多个物理接口分组到单个逻辑接口 — 链路聚合组 (LAG) 或端口通道的方法。端口通道将聚合成员链路的带宽、提供冗余和负载均衡流量。如果某个成员端口出现故障，OS10 设备会将流量重定向到其他端口。

一个物理接口一次只能属于一个端口通道。端口通道必须包含相同接口类型和速度的接口。OS10 最多支持 128 个端口通道，每个通道最多支持 32 个端口。

要配置端口通道，请使用与以太网端口接口相同的配置命令。端口通道对于网络配置是透明的，并作为单一接口进行管理。例如，为组配置一个 IP 地址，并使用端口通道上所有路由流量的 IP 地址。

通过配置端口通道，您可以通过聚合一组较低的链路来创建更大容量的接口。例如，您可以通过将四个 10G 以太网接口一起聚合来构建一个 40G 接口。如果这四个接口中的一个发生故障，流量将在其余三个接口间重新分布。

**静态** 端口通道以静态方式配置。

**动态** 端口通道使用链路聚合控制协议 (LACP) 进行动态配置。

LAG 的成员端口将根据端口 ID 添加并编程到硬件中，而不是端口启动的顺序。负载均衡可在重置和重新加载期间生成可预测的结果。

## 创建端口通道

最多可以创建 128 个端口通道，每个组最多 32 个端口成员。将端口通道配置为与物理接口相似，启用或配置协议或 ACL 至端口通道。启用端口通道后，将其置于 L2 或 L3 模式下。

要将端口通道置于 L2 模式或配置 IP 地址以将端口通道置于 L3 模式，请使用 `switchport` 命令。

- 在 CONFIGURATION 模式下创建端口通道。

```
interface port-channel id-number
```

### 创建端口通道

```
OS10(config)# interface port-channel 10
```

## 添加端口成员

当您接口添加到端口通道时：

- 管理状态将应用到端口信道。
- 端口通道配置将应用到成员接口。
- 端口通道在 L2（默认）或 L3 模式下运行。要将端口通道置于 L2 模式，请使用 `switchport mode` 命令。要在配置 IP 地址之前将端口通道置于 L3 模式并移除 L2 配置，请使用 `no switchport` 命令。
- 所有接口的速度必须相同。
- 接口不能包含非默认的 L2/L3 配置设置。仅支持 `description` 和 `shutdown` 或 `no shutdown` 命令。您不能将 IP 地址或静态 MAC 地址添加到成员接口。
- 您不能在端口通道接口上启用流控制。端口通道成员的物理接口上支持流控制。
- 端口通道支持 802.3ad LACP。LACP 标识了同样配置的链路，并将端口动态分组到逻辑通道中。LACP 将激活交换机在端口通道中支持的最大兼容端口数。
- 如果全局禁用生成树操作，则已启用 LACP 的端口通道成员的 L2 接口可能会因数据包回路而摆动。

### 添加端口成员 — 静态 LAG

静态端口通道 LAG 包含您使用 `channel-group mode on` 命令手动分配的成员接口。

```
OS10(config)# interface port-channel 10
Aug 24 4:5:38: %Node.1-Unit.1:PRI:OS10 %dn_ifm
%log-notice:IFM_ASTATE_UP: Interface admin state up.:port-channel10
Aug 24 4:5:38: %Node.1-Unit.1:PRI:OS10 %dn_ifm
%log-notice:IFM_OSTATE_DN: Interface operational state is down.:port-channel10
OS10(conf-if-po-10)# exit

OS10(config)# interface ethernet 1/1/2
```

```
OS10(config-if-eth1/1/2)# channel-group 10 mode on
Aug 24 4:5:56: %Node.1-Unit.1:PRI:OS10 %dn ifm
%log-notice:IFM_OSTATE_UP: Interface operational state is up.:port-channel10
```

### 添加端口成员 — 动态 LACP

LACP 使端口可动态捆绑为端口通道的成员。要配置 LACP 操作的端口，请使用 `channel-group mode {active|passive}` 命令。主动和被动模式允许 LACP 在端口之间进行协商，以确定是否可以根据配置设置来形成端口通道。

```
OS10(config)# interface port-channel 100
OS10(config-if-po-100)# exit

OS10(config)# interface ethernet 1/1/2
OS10(config-if-eth1/1/2)# channel-group 100 mode active
```

## 最小链路数

在必须处于 *oper up* 状态的端口通道 LAG 中配置最小链路，以考虑将处于 *oper up* 状态的端口通道。

### 注:

如果您已配置的最低链路条件未满足，则仅在您配置了最小链路的设备中（而不是在端口通道另一端的设备上）端口通道停止运行。

当不满足最小链接条件时，为使端口通道在两侧停止运行，您必须在端口通道的两端配置最小链路。

在 PORT-CHANNEL 模式下，输入必须处于 *oper up* 状态的 LAG 中的链路数量，从 1 到 32，默认值为 1。

```
minimum-links number
```

### 配置最小的正常运行链路

```
OS10(config)# interface port-channel 1
OS10(config-if-po-1)# minimum-links 5
```

## 分配端口通道 IP 地址

您可以将 IP 地址分配给端口通道并使用 L3 路由协议中的端口通道。

- 在 INTERFACE PORT-CHANNEL 模式下配置接口上的 IP 地址和掩码。
  - `ip address ip-address/mask [secondary-ip-address]`
    - `ip-address/mask` — 以点分隔的十进制格式和掩码指定 IP 地址。
    - `secondary-ip-address` — 以点分隔的十进制格式（即，充当接口的备份 IP 地址）指定辅助 IP 地址。

### 分配端口通道 IP 地址

```
OS10# configure terminal
OS10(config)# interface port-channel 1
OS10(config-if-po-1)# ip address 1.1.1.1/24
OS10(config-if-po-1)#
```

## 卸下或禁用端口通道

您可以删除或禁用端口通道。

- 在 CONFIGURATION 模式下删除端口通道。

```
no interface port-channel channel-number
```



2. 在 CONFIGURATION 模式下禁用端口通道以将端口通道内的所有接口置于停止运行状态。

```
shutdown
```

### 删除端口通道

```
OS10(config)# interface port-channel 10
OS10(conf-if-po-10)# no interface port-channel 10
```

## 负载均衡流量

使用哈希来平衡端口通道的成员接口之间的流量。负载均衡使用源和目标数据包信息在将数据传输到目标时通过多个接口分发流量。

对于没有 L3 标头的数据包，默认情况下，OS10 会自动对哈希算法使用 `load-balancing mac-selection destination-mac` 命令。

同时配置 IP 和 MAC 哈希方案时，MAC 哈希方案优先于 IP 哈希方案。

- 选择一种或多种负载均衡方法，并在 CONFIGURATION 模式下通过端口通道替换默认的 IP 4 元组方法来平衡流量。

```
OS10(config)# load-balancing
 ingress-port Ingress port configurations
 tcp-udp-selection TCP-UDP port for load-balancing configurations
 ip-selection IPV4 load-balancing configurations
 ipv6-selection IPV6 load-balancing configurations
 mac-selection MAC load-balancing configurations
```

- `ingress-port [enable]` — 启用入口端口配置。
- `tcp-udp-selection [l4-destination-port | l4-source-port]` — 使用哈希计算中的第 4 层目标端口或第 4 层源端口。
- `ip-selection [destination-ip | source-ip | protocol | vlan-id | l4-destination-port | l4-source-port]` — 使用目标 IP 地址、源 IP 地址、协议、VLAN ID、第 4 层目标端口或哈希计算中的第 4 层源端口。
- `ipv6-selection [destination-ip | source-ip | protocol | vlan-id | l4-destination-port | l4-source-port]` — 使用目标 IPv6 地址、源 IPv6 地址、协议、VLAN ID、第 4 层端口或哈希计算中的第 4 层源端口。
- `mac-selection [destination-mac | source-mac] [ethertype | vlan-id]` — 在哈希计算中使用目标 MAC 地址或源 MAC 地址和 ethertype 或 VLAN ID。

### 配置负载均衡

```
OS10(config)# load-balancing ip-selection destination-ip source-ip
```

## 更改哈希算法

`load-balancing` 命令可选择应用于端口通道上的流量负载均衡的哈希条件。如果您没有获得流量分配，请使用 `hash-algorithm` 命令选择 LAG 的哈希方案。旋转或偏移 L2 LAG 哈希，直至达到所需的流量分布。

- 在 CONFIGURATION 模式下将默认值 (0) 更改为另一种算法，并将其应用于 LAG 哈希。

```
hash-algorithm lag {crc | xor | random}
```

### 更改哈希算法

```
OS10(config)# hash-algorithm lag crc
```

## 配置接口范围

通过批量接口配置，您可以将相同的配置应用到多个物理或逻辑接口，或者显示其当前配置。接口范围是指将同一命令应用于的一组接口。

您可以使用接口范围进行以下操作：

- 以太网物理接口
- 端口通道
- VLAN 接口

批量配置包括配置中接口范围内的任何非现有接口。

只有在配置的接口范围仅包含 VLAN 端口时，才能配置默认 VLAN。当其中一个 VLAN 端口发生故障时，接口范围内的所有 VLAN 端口都会受到影响。

创建接口范围，允许使用 `interface range` 命令将其他命令应用到该接口范围。

### 配置以太网地址的范围并启用它们

```
OS10(config)# interface range ethernet 1/1/1-1/1/5
OS10(conf-range-eth1/1/1-1/1/5)# no shutdown
```

### 查看配置

```
OS10(conf-range-eth1/1/1-1/1/5)# show configuration
!
interface ethernet1/1/1
 no shutdown
 switchport access vlan 1
!
interface ethernet1/1/2
 no shutdown
 switchport access vlan 1
!
interface ethernet1/1/3
 no shutdown
 switchport access vlan 1
!
interface ethernet1/1/4
 no shutdown
 switchport access vlan 1
!
interface ethernet1/1/5
 no shutdown
 switchport access vlan 1
```

### 配置 VLAN 的范围

```
OS10(config)# interface range vlan 1-100
OS10(conf-range-vl-1-100)#
```

### 配置端口通道的范围

```
OS10(config)# interface range port-channel 1-25
OS10(conf-range-po-1-25)#
```

## 交换机端口配置文件

端口配置文件用于确定以太网和统一端口上已启用的前面板端口和受支持的分解模式。更改交换机上的端口配置文件以自定义上行链路和统一端口操作，以及前面板数据端口的可用性。

要在下一次重新引导时更改端口配置文件，请使用 `switch-port-profile` 命令和所需的配置文件，将其保存到启动配置中，然后使用 `reload` 命令应用更改。

1. 在 CONFIGURATION 模式下配置特定于平台的端口配置文件。对于独立交换机，请为 `node/unit` 输入 1/1。

```
switch-port-profile node/unit profile
```

2. 在 EXEC 模式下将端口配置文件更改保存到启动配置。

```
write memory
```

### 3. 在 EXEC 模式下重新加载交换机。

```
reload
```

交换机将使用新的端口配置重新启动，并重置系统默认设置，除了交换机端口配置文件和以下配置的设置：

- 管理接口 1/1/1 配置
- 管理 IPv4/IPv6 静态路由
- 系统主机名称
- 统一转发表 (UFT) 模式
- ECMP 最大路径

您必须在应用新的端口配置文件并重新加载交换机后手动重新配置交换机上的其他设置。

**注：**更改交换机端口配置文件后，不要立即备份和恢复启动文件，而无需使用 `write memory` 命令，以及使用 `reload` 命令重新加载交换机。否则，新配置文件将不会生效。

#### 配置端口配置文件

```
OS10(config)# switch-port-profile 1/1 profile-6
OS10(config)# exit
OS10# write memory
OS10# reload
```

#### 验证端口配置文件

```
OS10(config)# show switch-port-profile 1/1
```

| Node/Unit | Current   | Next-boot | Default   |
|-----------|-----------|-----------|-----------|
| 1/1       | profile-2 | profile-2 | profile-1 |

Supported Profiles:

```
profile-1
profile-2
profile-3
profile-4
profile-5
profile-6
```

## S4148-ON 系列端口配置文件

在 S4148-ON 系列交换机上，端口配置文件将确定可用的前面板以太网端口和上行链路端口上支持的分解接口。在端口配置文件中，蓝色框表示支持的端口和分解接口。空格表示不可用的端口和速度。

- 10GE 模式是 SFP+ 10GE 端口，或者 QSFP+/QSFP28 端口的 4x10G 分解。
- 25GE 是 QSFP28 端口的 4x25G 分解。
- 40GE 模式是支持 QSFP+ 40GE 收发器的 QSFP+ 端口或 QSFP28 端口。
- 50GE 是 QSFP28 端口的 2x50G 分解。
- 100GE 模式是 QSFP28 端口。

**注：**对于具有 SFP 和以太网端口的 S4148U-ON 端口配置文件，请参考 [S4148U-ON 端口配置文件](#)。S4148U-ON SFP 端口支持光通道和以太网模式。

例如，`profile-1` 可在 48 个端口（1-24 和 31-54）上启用 10G 速度，并且在 QSFP28 端口 25-26 和 29-30 上启用 4x10G 分解；QSFP+ 端口 27 和 28 已停用。`profile-3` 可在四十个端口上启用 10G 速度，以及所有 QSFP28 端口和 QSFP+ 端口上的 4x10G 分解。同样，`profile-1` 可在端口 25-30 上禁用 40G 速度；`profile-3` 可在这些端口上启用 40G。有关详细信息，请参阅[交换机端口配置文件](#)。

|                        |            | SFP+ |   |   |   | SFP+ |   |   |   | SFP+ |    |    |    | SFP+ |    |    |    | SFP+ |    |    |    | QSFP28 |    |    |    | QSFP28 |  |  |  | QSFP+ |  |  |  | QSFP+ |  |  |  | QSFP28 |  |  |  | QSFP28 |  |  |  | SFP+ |  |  |  | SFP+ |    |    |    | SFP+ |    |    |    | SFP+ |    |    |    | SFP+ |    |    |    | SFP+ |    |    |    |    |    |    |    |
|------------------------|------------|------|---|---|---|------|---|---|---|------|----|----|----|------|----|----|----|------|----|----|----|--------|----|----|----|--------|--|--|--|-------|--|--|--|-------|--|--|--|--------|--|--|--|--------|--|--|--|------|--|--|--|------|----|----|----|------|----|----|----|------|----|----|----|------|----|----|----|------|----|----|----|----|----|----|----|
| Port Number→           |            | 1    | 2 | 3 | 4 | 5    | 6 | 7 | 8 | 9    | 10 | 11 | 12 | 13   | 14 | 15 | 16 | 17   | 18 | 19 | 20 | 21     | 22 | 23 | 24 | 25     |  |  |  | 26    |  |  |  | 27    |  |  |  | 28     |  |  |  | 29     |  |  |  | 30   |  |  |  | 31   | 32 | 33 | 34 | 35   | 36 | 37 | 38 | 39   | 40 | 41 | 42 | 43   | 44 | 45 | 46 | 47   | 48 | 49 | 50 | 51 | 52 | 53 | 54 |
| Profile                | Port Modes |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
| Profile-1<br>(default) | 1GE/10GE   |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 25GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 40GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 50GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 100GE      |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
| Profile-2              | 1GE/10GE   |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 25GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 40GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 50GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 100GE      |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
| Profile-3              | 1GE/10GE   |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 25GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 40GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 50GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 100GE      |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
| Profile-4              | 1GE/10GE   |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 25GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 40GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 50GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 100GE      |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
| Profile-5              | 1GE/10GE   |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 25GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 40GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 50GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 100GE      |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
| Profile-6              | 1GE/10GE   |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 25GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 40GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 50GE       |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |
|                        | 100GE      |      |   |   |   |      |   |   |   |      |    |    |    |      |    |    |    |      |    |    |    |        |    |    |    |        |  |  |  |       |  |  |  |       |  |  |  |        |  |  |  |        |  |  |  |      |  |  |  |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |      |    |    |    |    |    |    |    |

**1GE 模式：** 仅在 SFP+ 端口上支持 1GE；在 QSFP+ 和 QSFP28 端口 25-26 上不支持 1GE。

**分解接口：** 在 CONFIGURATION 模式下使用 `interface breakout` 命令可配置 4x10G、4x25G 和 2x50G 分解接口。

要查看属于每个端口组的端口，请使用 `show port-group` 命令。

## S4148U-ON 端口配置文件

S4148U-ON 端口配置文件确定可用的前面板统一端口和以太网端口以及支持的分解接口。在端口配置文件图中，蓝色框表示支持的以太网端口模式和分解接口。褐色框表示支持的光纤通道端口模式和分解接口。空格表示不可用的端口和速度。统一端口组的编号为 1 到 10。

S4148U-ON 统一端口模式 — SFP+ 端口 1-24 以及 QSFP28 端口 25-26 和 29-30：

- 在以太网模式下，10GE 是的 SFP+ 端口，或 QSFP+/QSFP28 端口的 4x10G 分解。
- 25GE 是 QSFP28 以太网端口的 4x25G 分解。
- 40GE 是使用 QSFP+ 40GE 收发器的 QSFP+ 或 QSFP28 以太网端口。
- 50GE 是 QSFP28 以太网端口的 2x50G 分解。
- 100GE 是 QSFP28 以太网端口。
- 4x8GFC 是 SFP+ 或 QSFP28 FC 端口组中的分解接口。
- 2x16GFC 是 SFP+ 或 QSFP28 FC 端口组中的分解接口（子端口 1 和 3）。
- 4x16GFC 是 QSFP28 FC 端口组中的分解接口。
- 1x32GFC（子端口 1）是 QSFP28 FC 端口组中的分解接口。

S4148U-ON 以太网模式 — QSFP+ 端口 27-28 和 SFP+ 端口 31-54：

- 10GE 模式是 SFP+ 10GE 端口或 QSFP+ 端口的 4x10G 分解。
- 40GE 模式是 QSFP+ 端口。

例如，所有 S4148U-ON 在统一端口 1-24 和以太网端口 31-54 上激活支持 10G 速度，但仅 profile-1 和 profile-2 在具有 4x10G 分解的 40GE 模式下激活 QSFP+ 端口 27-28。同样，所有 S4148U-ON 配置文件都在统一端口 1-24 上激活 8GFC 速度，但仅 profile-1、profile-2 和 profile-3 激活端口组 1-6 中的 2x16GFC。在 QSFP28 端口组中，profile-1 和 profile-2 支持 1x32GFC；profile-3 和 profile-4 支持 4x16GFC。

|                         |           | SFP+ |   | SFP+ |   | SFP+ |   | SFP+ |   | SFP+ |    | QSFP28 |    | QSFP28 |    | QSFP+ |    | QSFP+ |    | QSFP28 |    | QSFP28 |    | SFP+ |    | SFP+ |    | SFP+ |    | SFP+ |    | SFP+ |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|-------------------------|-----------|------|---|------|---|------|---|------|---|------|----|--------|----|--------|----|-------|----|-------|----|--------|----|--------|----|------|----|------|----|------|----|------|----|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--|--|--|--|--|--|--|--|--|--|--|--|
| Unified Port Group →    |           | 1    |   | 2    |   | 3    |   | 4    |   | 5    |    | 6      |    | 7      |    | 8     |    |       |    |        |    | 9      |    | 10   |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
| Port Number →           |           | 1    | 2 | 3    | 4 | 5    | 6 | 7    | 8 | 9    | 10 | 11     | 12 | 13     | 14 | 15    | 16 | 17    | 18 | 19     | 20 | 21     | 22 | 23   | 24 | 25   | 26 | 27   | 28 | 29   | 30 | 31   | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 |  |  |  |  |  |  |  |  |  |  |  |  |
| Uplink Port Breakouts → |           |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    | 1    | 2  | 3    | 4  | 1    | 2  | 3    | 4  | 1  | 2  | 3  | 4  | 1  | 2  | 3  | 4  | 1  | 2  | 3  | 4  | 1  | 2  | 3  | 4  |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
| Profile-1<br>(default)  | 1GE/10GE  |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 25GE      |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 40GE      |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 50GE      |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 100GE     |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
| Profile-2*              | 4x8GFC**  |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 2x16GFC** |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 4x16GFC** |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 1x32GFC   |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 2x32GFC   |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
| Profile-3               | 1GE/10GE  |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 25GE      |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 40GE      |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 50GE      |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 100GE     |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
| Profile-4               | 4x8GFC**  |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 2x16GFC** |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 4x16GFC** |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 1x32GFC   |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |
|                         | 2x32GFC   |      |   |      |   |      |   |      |   |      |    |        |    |        |    |       |    |       |    |        |    |        |    |      |    |      |    |      |    |      |    |      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |  |  |  |  |  |  |  |  |

\*profile-1 和 profile-2 激活统一和以太网端口上的相同端口模式功能。不同之处在于，在 profile-1 中，默认情况下 SFP+ 统一端口 1-24 显示在光纤通道模式下，并且每个端口组具有 2x16GFC 分解。在 profile-2 中，默认情况下 SFP+ 统一端口 1-24 显示在以太网 10GE 模式下。profile-1 允许您连接 FC 设备进行即插即用；profile-2 专为基于以太网的标准数据网络而设计。

**\*\*超额订阅：**配置超额订阅以支持光纤通道接口上的突发存储流量。超额订阅使端口可以更快地运行，但可能会导致流量丢失。要支持超额订阅，请在接口配置模式下使用 `speed` 命令。此命令在以太网接口上不受支持。在 S4148U-ON 端口配置文件中：

- 4x8GFC 模式下的 SFP+ 和 QSFP28 端口组支持成员接口上的 16GFC 超额订阅。
- 2x16GFC 模式下的 QSFP28 端口支持 32GFC 超额订阅。2x16GFC 模式下的 SFP+ 端口组不支持 32GFC 超额订阅。2x16GFC 模式可激活子端口 1 和 3。
- 4x16GFC 模式下的 QSFP28 端口支持 32GFC 超额订阅。

### 分解接口：

- 要在统一端口上配置分解接口，请在端口组配置模式下使用 `mode {FC | Eth}` 命令。`mode {FC | Eth}` 命令将统一端口配置为以行速率运行，并确保无流量损失。
- 要在 QSFP+ 以太网端口上配置分解接口，请在全局配置模式下使用 `interface breakout` 命令。

**1GE 模式：**仅 SFP+ 端口支持 1GE；QSFP+ 和 QSFP28 端口 25-30 不支持 1GE。

要查看属于每个端口组的端口，请使用 `show port-group` 命令。

## 在接口上配置协商模式

在 OS10 上，默认情况下，auto 协商模式处于启用状态。

要强制协商，请使用以下命令：

negotiation on

要禁用协商，请使用以下命令：

```
negotiation off
```

要将协商模式重置为您使用的介质的默认设置，请使用以下命令之一：

negotiation auto

no negotiation

以下示例显示了将非默认配置添加到正在运行的配置:

```
OS10(conf-if-eth1/1/50)# negotiation off
OS10(conf-if-eth1/1/50)# show configuration
```

```

!
interface ethernet1/1/50
 no shutdown
 switchport access vlan 1
 negotiation off
 flowcontrol receive on
OS10(conf-if-eth1/1/50)# negotiation on
OS10(conf-if-eth1/1/50)# show configuration
!
interface ethernet1/1/50
 no shutdown
 switchport access vlan 1
 negotiation on
 flowcontrol receive on

```

以下示例显示了未将默认配置添加到正在运行的配置中：

```

OS10(conf-if-eth1/1/50)# negotiation auto
OS10(conf-if-eth1/1/50)# show configuration
!
interface ethernet1/1/50
 no shutdown
 switchport access vlan 1
 flowcontrol receive on

```

以下示例显示了 `no negotiation` 命令将接口重置为使用的介质的默认设置。

```

OS10(conf-if-eth1/1/50)# no negotiation
OS10(conf-if-eth1/1/50)# show configuration
!
interface ethernet1/1/50
 no shutdown
 switchport access vlan 1
 flowcontrol receive on
OS10(conf-if-eth1/1/50)# do show interface ethernet 1/1/50
Ethernet 1/1/50 is up, line protocol is up
Hardware is Eth, address is e4:f0:04:3e:2d:86
 Current address is e4:f0:04:3e:2d:86
Pluggable media present, QSFP28 type is QSFP28 100GBASE-CR4-2.0M
 Wavelength is 64
 Receive power reading is not available

Interface index is 112
Internet address is not set
Mode of IPv4 Address Assignment: not set
Interface IPv6 oper status: Disabled
MTU 1532 bytes, IP MTU 1500 bytes
LineSpeed 100G, Auto-Negotiation on

```

## 配置分解模式

使用受支持的分解线缆，您可以将 40GE QSFP+ 或 100GE QSFP28 端口以太网端口拆分为单独的分解接口。所有分解接口的速度都相同。您可以使用 QSFP+ 收发器将 QSFP28 端口设置为在 40GE 模式下运行。

```

interface breakout node/slot/port map {10g-4x | 25g-4x | 40g-1x | 50g-2x |
100g-1x}

```

- *node/slot/port* — 输入物理端口信息。
- 10g-4x — 将 QSFP28 端口或 QSFP+ 端口拆分为四个 10G 接口。
- 25g-4x — 将 QSFP28 端口拆分为四个 25G 接口。
- 40g-1x — 设置要与 QSFP+ 40G 收发器一起使用的 QSFP28 端口。
- 50g-2x — 将 QSFP28 端口拆分为两个 50G 接口。
- 100g-1x — 将 QSFP28 端口重置为 100G 速度。

要配置以太网分解接口，请在 CONFIGURATION 模式下使用 `interface ethernet node/slot/port:subport` 命令。

每个分解接口以配置的速度运行。使用 `interface breakout` 命令的 `no` 版本将端口重置为其默认速度：40G 或 100G。

要在统一端口上配置分解接口，请在端口组配置模式下使用 `mode {Eth | FC}` 命令。

**注：**您不能将 40G 端口 13、14、15、16、29、30、31 和 32 配置在 S6010 平台上拆分的四个 10G 接口。

配置接口分解

```
OS10(config)# interface breakout 1/1/7 map 10g-4x
```

显示接口分解

```
OS10# show interface status
```

| Port        | Description | Status | Speed | Duplex | Mode | Vlan | Tagged-Vlans |
|-------------|-------------|--------|-------|--------|------|------|--------------|
| Eth 1/1/1   |             | down   | 0     | auto   | -    |      |              |
| Eth 1/1/2   |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/7:1 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/7:2 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/7:3 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/7:4 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/25  |             | down   | 0     | auto   | A    | 1    | -            |

分解自动配置

您可以全局启用前面板以太网端口，以在 QSFP+ 或 QSFP28 端口中自动检测 SFP 可插拔介质。端口将自动配置分解接口的介质类型和速度。例如，如果您将具有 4x10G 远端收发器的 40G 直连线缆 (DAC) 插入 QSFP28 端口，则端口将在 10g-4x 接口分解模式下自动配置。

RJ-45 端口和作为端口组成员的端口不支持分解自动配置。默认情况下，分解自动配置处于禁用状态。

启用分解自动配置

```
OS10(config)# feature auto-breakout
```

显示分解自动配置

将线缆插入以太网端口 1/1/25 之前，请执行以下操作：

```
OS10# show interface status
```

| Port       | Description | Status | Speed | Duplex | Mode | Vlan | Tagged-Vlans |
|------------|-------------|--------|-------|--------|------|------|--------------|
| Eth 1/1/1  |             | down   | 0     | auto   | -    |      |              |
| Eth 1/1/2  |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/25 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/29 |             | down   | 0     | auto   | A    | 1    | -            |

在以太网端口 1/1/25 中输入 `feature auto-breakout` 并插入分解线缆后：

```
OS10# show interface status
```

| Port         | Description | Status | Speed | Duplex | Mode | Vlan | Tagged-Vlans |
|--------------|-------------|--------|-------|--------|------|------|--------------|
| Eth 1/1/1    |             | down   | 0     | auto   | -    |      |              |
| Eth 1/1/2    |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/25:1 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/25:2 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/25:3 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/25:4 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/29   |             | down   | 0     | auto   | A    | 1    | -            |

# 重置默认配置

您可以清除以太网或光纤通道接口上所有已配置的设置，并将接口重置为其默认设置。默认情况下：

- 以太网接口都使用 `no shutdown` 命令启用，并分配给默认 VLAN。
- 使用 `shutdown` 命令可禁用光纤通道接口。

## 限制

`default interface` 命令将移除端口接口上的所有软件设置和所有 L3、VLAN 和端口通道配置。但是，该命令不会从其他软件功能中移除接口的配置，如 VLT。如果不移除这些已配置的设置，命令将不会执行。例如，如果您将以太网接口配置为 VLT 域中的查找接口，并且不删除此设置，则将接口重置为其默认配置失败：

```
OS10(config)# vlt-domain 10
OS10(conf-vlt-10)# discovery-interface ethernet 1/1/1
OS10(conf-vlt-10)# exit
OS10(config)# default interface ethernet 1/1/1
Proceed to cleanup the interface config? [confirm yes/no]:y
% Error: Discovery Interface mode must not be in switchport mode
```

## 配置

1. 在 CONFIGURATION 模式下，进入 INTERFACE 模式并查看当前配置的设置。

```
interface {ethernet | fibrechannel} node/slot/port[:subport]
show config
```

2. 返回 CONFIGURATION 模式。

```
exit
```

3. 在 CONFIGURATION 模式下将接口重置为其默认配置。使用 `default interface range` 命令可以逗号分隔的字符串或端口范围输入多个接口。

```
default interface {ethernet | fibrechannel} node/slot/port[:subport]
```

4. 进入 INTERFACE 模式并验证出厂默认配置。

```
interface {ethernet | fibrechannel} node/slot/port[:subport]
show config
```

## 重置默认以太网配置

```
OS10(conf-if-eth1/1/2)# show configuration
!
interface ethernet 1/1/2
no shutdown
no switchport
negotiation on
ip address 1.2.3.4/24
ip address 2.2.2.2/24 secondary
ip address 3.3.3.3/24 secondary
ipv6 address 10::1/64
ip access-group test in
lldp med network-policy add 10
ip ospf priority 10
flowcontrol transmit on

OS10(conf-if-eth1/1/2)# exit
S10(config)# default interface ethernet 1/1/2
Proceed to cleanup the interface config? [confirm yes/no]:y
Sep 9 01:06:28 OS10 dn_13_core_services[968]: Node.1-Unit.1:PRI:notice [os10:trap],
%Dell EMC (OS10) %IP_ADDRESS_DEL: IP Address delete is successful. IP 2.2.2.2/24 deleted
successfully
Sep 9 01:06:28 OS10 dn_13_core_services[968]: Node.1-Unit.1:PRI:notice [os10:trap],
%Dell EMC (OS10) %IP_ADDRESS_DEL: IP Address delete is successful. IP 3.3.3.3/24 deleted
successfully
Sep 9 01:06:28 OS10 dn_13_core_services[968]: Node.1-Unit.1:PRI:notice [os10:trap],
%Dell EMC (OS10) %IP_ADDRESS_DEL: IP Address delete is successful. IP 1.2.3.4/24 deleted
successfully
Sep 9 01:06:28 OS10 dn_13_core_services[968]: Node.1-Unit.1:PRI:notice [os10:trap],
```



```
%Dell EMC (OS10) %IP_ADDRESS_DEL: IP Address delete is successful. IP 10::1/64 deleted successfully

OS10(config)# do show running-configuration interface ethernet 1/1/2
!
interface ethernet1/1/2
no shutdown
switchport access vlan 1
```

## 重置默认光纤通道配置

```
OS10# show running-configuration interface fibrechannel 1/1/1
!
interface fibrechannel1/1/1
no shutdown
description fc-port

OS10(conf-if-fc1/1/1)# exit
OS10(config)# default interface fc1/1/1
Proceed to cleanup the interface config? [confirm yes/no]:y
!
OS10(config)# do show running-configuration interface fibrechannel 1/1/1
interface fibrechannel1/1/1
shutdown
```

# 转发纠错

转发纠错 (FEC) 可增强数据可靠性。

## OS10 支持的 FEC 模式：

- CL74-FC — 支持 25G 和 50G
- CL91-RS — 支持 100G
- CL108-RS — 支持 25G 和 50G
- 关闭 — 禁用 FEC

 **注：**OS10 不支持 10G 和 40G 上的 FEC。

## 配置 FEC

```
OS10(config)# interface ethernet 1/1/41
OS10(conf-if-eth1/1/41)# fec CL91-RS
```

## 查看 FEC 配置

```
OS10# show interface ethernet 1/1/41
Ethernet 1/1/41 is up, line protocol is up
Hardware is Dell EMC Eth, address is e4:f0:04:3e:1a:06
 Current address is e4:f0:04:3e:1a:06
Pluggable media present, QSFP28 type is QSFP28_100GBASE_CR4_2M
 Wavelength is 64
 Receive power reading is
Interface index is 17306108
Internet address is not set
Mode of IPv4 Address Assignment: not set
Interface IPv6 oper status: Disabled
MTU 1532 bytes, IP MTU 1500 bytes
LineSpeed 100G, Auto-Negotiation on
FEC is cl91-rs, Current FEC is cl91-rs
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 60
Last clearing of "show interface" counters: 00:00:17
Queuing strategy: fifo
Input statistics:
 7 packets, 818 octets
 2 64-byte pkts, 0 over 64-byte pkts, 5 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
 7 Multicasts, 0 Broadcasts, 0 Unicasts
 0 runts, 0 giants, 0 throttles
```

```

0 CRC, 0 overrun, 0 discarded
Output statistics:
15 packets, 1330 octets
10 64-byte pkts, 0 over 64-byte pkts, 5 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
15 Multicasts, 0 Broadcasts, 0 Unicasts
0 throttles, 0 discarded, 0 Collisions, 0 wred drops
Rate Info(interval 30 seconds):
Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
Output 0 Mbits/sec, 0 packets/sec, 0% of line rate
Time since last interface status change: 00:00:13
--more--

```

## 节能以太网

节能以太网 (EEE) 在闲置期间可减少物理层设备 (PHY) 的能耗。EEE 允许 Dell EMC Networking 的设备符合环保计算标准。

当链路处于空闲状态时，以太网链路会消耗电力。EEE 允许以太网链路仅在数据传输过程中使用常规电源模式。在支持低功耗空闲 (LPI) 模式的设备上启用了 EEE。此类设备可在没有数据传输期间进入 LPI 模式来节省电力。

在 LPI 模式下，链路两端的系统通过关闭某些服务来节省电力。EEE 以透明方式从 LPI 模式转换为高层协议和应用程序。

EEE 在自动协商阶段通告。自动协商会检测到链接另一端的设备支持的能力，确定通用能力，并配置联合操作。

自动协商可在开机时执行，在检测到 PHY 错误时或在以太网线缆重新连接后从 LAN 控制器中对命令执行。在链路建立进程中，两个链路伙伴均指示其 EEE 能力。如果协商的 PHY 类型的两个链路伙伴均支持 EEE，则 EEE 将在任一方向独立工作。

更改 EEE 配置将重置接口，因为设备会重新启动第 1 层自动协商。您可能想要为需要更长时间唤醒的设备启用链路层查找协议 (LLDP)，以便能够在其接收路径上接受数据。这样使设备能够与发送链路伙伴协商延长的系统唤醒时间。

 **注：**EEE 功能不适用于 Base-T 交换机。

## 启用节能以太网

默认情况下，EEE 处于禁用状态。要降低功耗，请启用 EEE。

1. 在 CONFIGURATION 模式下输入物理以太网接口信息。

```
interface ethernet node/slot/port[:subport]
```

2. 在 INTERFACE 模式下启用 EEE。

```
eee
```

### 启用 EEE

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# eee
```

### 禁用 EEE

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no eee
```

## 清除 EEE 计数器

您可以清除全局或每个接口上的物理以太网接口上的 EEE 计数器。

### 清除所有 EEE 计数器

```
OS10# clear counters interface eee
Clear all eee counters [confirm yes/no]:yes
```

清除特定接口的计数器

```
OS10# clear counters interface 1/1/48 eee
Clear eee counters on ethernet1/1/48 [confirm yes/no]:yes
```

查看 EEE 状态/统计信息

您可以使用 show 命令查看指定接口或所有接口的 EEE 状态或统计信息。

查看指定接口的 EEE 状态

```
OS10# show interface ethernet 1/1/48 eee

Port EEE Status Speed Duplex

Eth 1/1/48 on up 1000M
```

查看所有接口上的 EEE 状态

```
OS10# show interface eee

Port EEE Status Speed Duplex

Eth 1/1/1 off up 1000M
...
Eth 1/1/47 on up 1000M
Eth 1/1/48 on up 1000M
Eth 1/1/49 n/a
Eth 1/1/50 n/a
Eth 1/1/51 n/a
Eth 1/1/52 n/a
```

查看指定接口的 EEE 统计信息

```
OS10# show interface ethernet 1/1/48 eee statistics
Eth 1/1/48
 EEE : on
 TxIdleTime(us) : 2560
 TxWakeTime(us) : 5
 Last Clearing : 18:45:53
 TxEventCount : 0
 TxDuration(us) : 0
 RxEventCount : 0
 RxDuration(us) : 0
```

查看所有接口上的 EEE 统计信息

```
OS10# show interface eee statistics

Port EEE TxEventCount TxDuration(us) RxEventCount RxDuration(us)

Eth 1/1/1 off 0 0 0 0
...
Eth 1/1/47 on 0 0 0 0
Eth 1/1/48 on 0 0 0 0
Eth 1/1/49 n/a
...
Eth 1/1/52 n/a
```

## EEE 命令

### clear counters interface eee

清除所有 EEE 计数器。

**语法** clear counters interface eee

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# clear counters interface eee
Clear all eee counters [confirm yes/no]:yes
```

**支持的版本** 10.3.0E or later

### clear counters interface ethernet eee

清除指定以太网接口上的 EEE 计数器。

**语法** clear counters interface ethernet *node/slot/port[:subport]* eee

**参数** *node/slot/port[:subport]* — 输入接口信息。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# clear counters interface 1/1/48 eee
Clear eee counters on ethernet1/1/48 [confirm yes/no]:yes
```

**支持的版本** 10.3.0E or later

## eee

在物理端口上启用或禁用节能以太网(EEE)。

**语法** eee

**参数** 无

**默认** 在 Base-T 设备上启用并且在 S3048-ON 和 S4048T-ON 交换机上禁用。

**命令模式** 接口

**使用情况信息** 要禁用 EEE，请使用此命令的 no 版本。

**示例（启用 EEE）**

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# eee
```

**示例（禁用 EEE）**

```
OS10(config)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# no eee
```

**支持的版本** 10.3.0E or later

show interface eee

显示所有接口的 EEE 状态。

- 语法 show interface eee
- 参数 无
- 默认 未配置
- 命令模式 EXEC
- 示例

```
OS10# show interface eee

Port EEE Status Speed Duplex

Eth 1/1/1 off up 1000M
...
Eth 1/1/47 on up 1000M
Eth 1/1/48 on up 1000M
Eth 1/1/49 n/a
Eth 1/1/50 n/a
Eth 1/1/51 n/a
Eth 1/1/52 n/a
```

支持的版本 10.3.0E or later

show interface eee statistics

显示所有接口的 EEE 统计信息。

- 语法 show interface eee statistics
- 参数 无
- 默认 未配置
- 命令模式 EXEC
- 示例

```
OS10# show interface eee statistics

Port EEE TxEventCount TxDuration(us) RxEventCount RxDuration(us)

Eth 1/1/1 off 0 0 0 0
...
Eth 1/1/47 on 0 0 0 0
Eth 1/1/48 on 0 0 0 0
Eth 1/1/49 n/a
...
Eth 1/1/52 n/a
```

支持的版本 10.3.0E or later

show interface ethernet eee

显示指定接口的 EEE 状态。

- 语法 show interface ethernet node/slot/port[:subport] eee
- 参数 node/slot/port[:subport] — 输入接口信息。
- 默认 未配置
- 命令模式 EXEC

## 示例

```
OS10# show interface ethernet 1/1/48 eee

Port EEE Status Speed Duplex

Eth 1/1/48 on up 1000M
```

## 支持的版本

10.3.0E or later

# show interface ethernet eee statistics

显示指定接口的 EEE 统计信息。

**语法** `show interface ethernet node/slot/port[:subport] eee statistics`

**参数** `node/slot/port[:subport]`— 输入接口信息。

**默认** 未配置

**命令模式** EXEC

## 示例

```
OS10# show interface ethernet 1/1/48 eee statistics
Eth 1/1/48
 EEE : on
 TxIdleTime(us) : 2560
 TxWakeTime(us) : 5
 Last Clearing : 18:45:53
 TxEventCount : 0
 TxDuration(us) : 0
 RxEventCount : 0
 RxDuration(us) : 0
```

## 支持的版本

10.3.0E or later

# 查看接口配置

要查看基本接口信息，请使用 `show interface`、`show running-configuration` 和 `show interface status` 命令。通过输入 CTRL+C 停止从 `show` 命令滚动输出。以 EXEC 模式显示有关物理或虚拟接口的信息，包括运行/停止状态、MAC 和 IP 地址以及输入/输出流量计数器。

```
show interface [type]
```

- `phy-eth node/slot/port[:subport]` — 显示有关连接到接口的物理介质的信息。
- `status` — 显示接口状态。
- `ethernet node/slot/port[:subport]` — 显示以太网接口信息。
- `loopback id` — 显示环回接口信息，从 0 到 16383。
- `mgmt node/slot/port` — 显示管理接口信息。
- `port-channel id-number` — 显示端口通道接口信息，从 1 到 128。
- `vlan vlan-id` — 显示 VLAN 接口信息，从 1 到 4093。

## 查看接口信息

```
OS10# show interface
Ethernet 1/1/1 is up, line protocol is down
Hardware is Eth, address is 00:0c:29:66:6b:90
 Current address is 00:0c:29:66:6b:90
Pluggable media present, QSFP+ type is QSFP+ 40GBASE CR4
 Wavelength is 64
 Receive power reading is 0.000000 dBm
Interface index is 15
Internet address is not set
Mode of IPv4 Address Assignment: not set
Interface IPv6 oper status: Enabled
MTU 1532 bytes, IP MTU 1500 bytes
```

```

LineSpeed 0, Auto-Negotiation on
Configured FEC is off, Negotiated FEC is off
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 60
Last clearing of "show interface" counters: 02:46:35
Queuing strategy: fifo
Input statistics:
 0 packets, 0 octets
 0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
 0 Multicasts, 0 Broadcasts, 0 Unicasts
 0 runts, 0 giants, 0 throttles
 0 CRC, 0 overrun, 0 discarded
Output statistics:
 0 packets, 0 octets
 0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
 0 Multicasts, 0 Broadcasts, 0 Unicasts
 0 throttles, 0 discarded, 0 Collisions, 0 wred drops
Rate Info(interval 30 seconds):
 Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
 Output 0 Mbits/sec, 0 packets/sec, 0% of line rate
Time since last interface status change: 02:46:36

```

```

Ethernet 1/1/2 is up, line protocol is up
Hardware is Eth, address is 00:0c:29:66:6b:94
 Current address is 00:0c:29:66:6b:94
Pluggable media present, QSFP+ type is QSFP+ 40GBASE CR4
 Wavelength is 64
 Receive power reading is 0.000000 dBm
Interface index is 17
Internet address is not set
Mode of IPv4 Address Assignment: not set
Interface IPv6 oper status: Enabled
Link local IPv6 address: fe80::20c:29ff:fe66:6b94/64
MTU 1532 bytes, IP MTU 1500 bytes
LineSpeed 40G, Auto-Negotiation on
Configured FEC is off, Negotiated FEC is off
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 60
Last clearing of "show interface" counters: 02:46:35
Queuing strategy: fifo
Input statistics:
 0 packets, 0 octets
 0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
 0 Multicasts, 0 Broadcasts, 0 Unicasts
 0 runts, 0 giants, 0 throttles
 0 CRC, 0 overrun, 0 discarded
Output statistics:
 0 packets, 0 octets
 0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
 0 Multicasts, 0 Broadcasts, 0 Unicasts
 0 throttles, 0 discarded, 0 Collisions, 0 wred drops
Rate Info(interval 30 seconds):
 Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
 Output 0 Mbits/sec, 0 packets/sec, 0% of line rate
Time since last interface status change: 02:46:35
--more--

```

## 查看特定接口信息

```

OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
 ip address 1.1.1.1/24
 no switchport
 no shutdown

```

查看候选配置

```
OS10(conf-if-eth1/1/1)# show configuration candidate
!
interface ethernet1/1/1
 ip address 1.1.1.1/24
 no switchport
 no shutdown
```

查看正在运行的配置

```
OS10# show running-configuration
Current Configuration ...
!
interface ethernet1/1/1
 no ip address
 shutdown
!
interface ethernet1/1/2
 no ip address
 shutdown
!
interface ethernet1/1/3
 no ip address
 shutdown
!
interface ethernet1/1/4
 no ip address
 shutdown
...
```

查看 L3 接口

```
OS10# show ip interface brief
```

| Interface Name   | IP-Address       | OK  | Method | Status | Protocol |
|------------------|------------------|-----|--------|--------|----------|
| Ethernet 1/1/1   | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/2   | unassigned       | YES | unset  | up     | up       |
| Ethernet 1/1/3   | 3.1.1.1/24       | YES | manual | up     | up       |
| Ethernet 1/1/4   | 4.1.1.1/24       | YES | manual | up     | up       |
| Ethernet 1/1/5   | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/6   | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/7   | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/8   | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/9   | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/10  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/11  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/12  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/13  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/14  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/15  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/16  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/17  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/18  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/19  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/20  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/21  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/22  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/23  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/24  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/25  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/26  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/27  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/28  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/29  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/30  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/31  | unassigned       | NO  | unset  | up     | down     |
| Ethernet 1/1/32  | unassigned       | NO  | unset  | up     | down     |
| Management 1/1/1 | 10.16.153.226/24 | YES | manual | up     | up       |
| Vlan 1           | unassigned       | NO  | unset  | up     | down     |
| Vlan 10          | unassigned       | NO  | unset  | up     | down     |



|         |            |    |       |    |      |
|---------|------------|----|-------|----|------|
| Vlan 20 | unassigned | NO | unset | up | down |
| Vlan 30 | unassigned | NO | unset | up | down |

## 查看 VLAN 配置

```
OS10# show vlan
Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring VLANs,
 @ - Attached to Virtual Network
Q: A - Access (Untagged), T - Tagged
 NUM Status Description Q Ports
 1 Inactive
 10 Inactive
 20 Inactive
 22 Inactive
 23 Active A Eth1/1/1,1/1/6-1/1/32
 24 Inactive
 25 Inactive
 26 Inactive
 27 Inactive
 28 Inactive
 29 Inactive
 30 Inactive
 A Eth1/1/2
```

## 数字光学监控

数字光学监控 (DOM) 功能可监控数字光学介质的温度、电压、偏向、传输功率 (Tx) 和接收功率 (Rx)。当达到配置的阈值时，此功能还会为任何波动生成事件日志、警报和陷阱。

每个 DOM 类别有四个阈值级别 — 温度、电压、偏向、传输功率和接收功率，如下表中所述：

- 高
- 高警告
- 低
- 低警告

OS10 DOM 子系统会定期监控光学收发器的温度、电压、偏离、传输功率和接收功率更改，并在其各自的值与预定义的阈值相交时生成事件日志、警报和陷阱。

**表. 26: DOM 警报**

| 警报类别      | 警报名称   | 是否生成陷阱? | 严重性级别 |
|-----------|--------|---------|-------|
| 温度        | 温度高    | Y       | 主要    |
|           | 温度高警告  | N       | 次要    |
|           | 温度低    | Y       | 主要    |
|           | 温度低警告  | N       | 次要    |
| 电压        | 电压高    | Y       | 主要    |
|           | 电压高警告  | N       | 次要    |
|           | 电压低    | Y       | 主要    |
|           | 电压低警告  | N       | 次要    |
| 偏离        | 偏离高    | Y       | 主要    |
|           | 偏离高警告  | N       | 次要    |
|           | 偏离低    | Y       | 主要    |
|           | 偏离低警告  | N       | 次要    |
| 传输功率 (Tx) | Tx 高   | Y       | 主要    |
|           | Tx 高警告 | N       | 次要    |
|           | Tx 低   | Y       | 主要    |

表. 26: DOM 警报 (续)

| 警报类别      | 警报名称   | 是否生成陷阱? | 严重性级别 |
|-----------|--------|---------|-------|
| 接收功率 (Rx) | Tx 低警告 | N       | 次要    |
|           | Rx 高   | Y       | 主要    |
|           | Rx 高警告 | N       | 次要    |
|           | Rx 低   | Y       | 主要    |
|           | Rx 低警告 | N       | 次要    |

您可以启用或禁用 DOM 功能、配置陷阱并查看 DOM 状态。

## 启用 DOM 和 DOM 陷阱

要生成 DOM 警报，请执行以下操作。

1. 启用 DOM。

```
OS10(config)# dom enable
```

2. 启用 DOM 陷阱。

```
OS10(config)# snmp-server enable traps dom
```

您可以在 EXEC 模式下运行 `show alarms` 命令，以查看生成的任何警报。

### 查看 DOM 警报

```
OS10# show alarms
```

| Index | Severity | Name                | Raise-time              | Source        |
|-------|----------|---------------------|-------------------------|---------------|
| ----- | -----    | -----               | -----                   | -----         |
| 0     | major    | EQM_MEDIA_TEMP_HIGH | Tue 06-04-2019 12:32:07 | Node.1-Unit.1 |

### 查看 DOM 事件日志消息

以下是事件日志的示例：

- 高温警告：

```
Aug 03 06:35:47 OS10 dn_eqm[9135]: [os10:alarm], %Dell EMC (OS10)
%EQM_MEDIA_TEMP_HIGH: Media high temperature threshold crossed major warning
SET media 1/1/21 high threshold crossed, 82.00:78.00 Aug 03 06:35:47 OS10
dn_eqm[9135]: [os10:alarm], %Dell EMC (OS10) %EQM_MEDIA_VOLTAGE_HIGH: Media high
voltage threshold crossed major warning SET media 1/1/21 high threshold crossed,
6.00:3.63
```

在此示例中，高温的阈值为 78.00，但当前的温度为 82.00。

- 高接收功率警告：

```
Aug 03 06:35:47 OS10 dn_eqm[9135]: [os10:alarm], %Dell EMC (OS10)
%EQM_MEDIA_RX_POWER_HIGH: Media high rx_power threshold crossed major warning
SET media 1/1/21 high threshold crossed, 7.00:3.30 Aug 03 06:35:47 OS10
dn_eqm[9135]: [os10:alarm], %Dell EMC (OS10) %EQM_MEDIA_BIAS_HIGH: Media high
bias threshold crossed major warning SET media 1/1/21 high threshold crossed,
120.00:105.00
```

在此示例中，高接收功率的阈值为 3.30，但当前的接收功率为 7.00。

### 查看 DOM 陷阱

下面是 DOM 陷阱的示例。

```
2018-08-21 17:38:18 <UNKNOWN> [UDP: [10.11.56.49]:51635->[10.11.86.108]:162]:
iso.3.6.1.2.1.1.3.0 = Timeticks: (0) 0:00:00.00 iso.3.6.1.6.3.1.1.4.1.0 = OID:
iso.3.6.1.4.1.674.11000.5000.100.4.1.3.1.15 iso.3.6.1.4.1.674.11000.5000.100.4.1.3.2.4 = INTEGER: 1
```

```
iso.3.6.1.4.1.674.11000.5000.100.4.1.3.2.5 = INTEGER: 21 iso.3.6.1.4.1.674.11000.5000.100.4.1.3.2.1 =
INTEGER: 1081393 iso.3.6.1.4.1.674.11000.5000.100.4.1.3.2.3 = INTEGER: 1
iso.3.6.1.4.1.674.11000.5000.100.4.1.3.2.2 = STRING: "SET media 1/1/21 high threshold crossed, 82.00:78.00"
```

```
2018-08-21 17:38:18 <UNKNOWN> [UDP: [10.11.56.49]:48521->[10.11.86.108]:162]:
iso.3.6.1.2.1.1.3.0 = Timeticks: (1) 0:00:00.01 iso.3.6.1.6.3.1.1.4.1.0 = OID:
iso.3.6.1.4.1.674.11000.5000.100.4.1.3.1.19
iso.3.6.1.4.1.674.11000.5000.100.4.1.3.2.3 = INTEGER: 1
iso.3.6.1.4.1.674.11000.5000.100.4.1.3.2.1 = INTEGER: 1081397
iso.3.6.1.4.1.674.11000.5000.100.4.1.3.2.4 = INTEGER: 1
iso.3.6.1.4.1.674.11000.5000.100.4.1.3.2.2 = STRING: "SET media 1/1/21 high threshold
crossed, 6.00:3.63" iso.3.6.1.4.1.674.11000.5000.100.4.1.3.2.5 = INTEGER: 21
```

## 接口命令

### channel-group

为端口通道组分配接口。

**语法** `channel-group channel-number mode {active | on | passive}`

- 参数**
- `channel-number` — 输入端口通道号，从 1 到 128。
  - `mode` — 设置 LACP 本端模式。
  - `active` — 将通道模式设置为活动。
  - `on` — 将通道模式设置为静态。
  - `passive` — 将通道模式设置为被动。

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息** 此命令的 `no` 版本会将值重置为默认值，并从端口通道组取消分配接口。

**示例**

```
OS10(config)# interface ethernet 1/1/2:1
OS10(conf-if-eth1/1/2:1)# channel-group 20 mode active
```

**支持的版本** 10.3.0E or later

### default interface

将以太网或光纤通道接口重置为其默认设置。

**语法** `default interface interface-type`

- 参数** `interface-type` — 输入接口类型：
- `ethernet node/slot/port[:subport]` — 将以太网接口重置为其默认设置。
  - `fibrechannel node/slot/port[:subport]` — 将光纤通道接口重置为其默认设置。
  - `range ethernet node/slot/port[:subport]-node/slot/port[:subport]` — 将一系列以太网接口重置为其默认设置。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 要从以太网或光纤通道接口移除配置并将接口重置为其默认设置，请使用 `default interface` 命令。默认情况下：

- 使用 `no shutdown` 命令可启用以太网接口；使用 `shutdown` 命令可禁用光纤通道接口。
  - 以太网接口将分配给默认 VLAN。
- `default interface` 命令将移除物理接口上的所有软件设置和所有 L3、VLAN 和端口通道配置。您必须从其他软件功能中手动移除配置的接口链路；例如，如果您将以太网接口配置为 VLT 域中的查找接口。使用 `default interface range` 命令可以逗号分隔的字符串或端口范围输入多个接口。

此命令不能撤消。命令的 no 版本不起作用。

#### 示例 (以太网)

```
OS10# show running-configuration interface ethernet 1/1/15
!
interface ethernet1/1/15
no shutdown
no switchport
ip address 101.1.2.2/30
ipv6 address 2101:100:2:1::2/64
ipv6 ospf 65535 area 0.0.0.0
ipv6 ospf cost 10
ip ospf 65535 area 0.0.0.0
ip ospf cost 10

OS10# configure terminal

OS10(config)# default interface ethernet 1/1/15
Proceed to cleanup the interface config? [confirm yes/no]:yes
Mar 5 22:00:48 OS10 dn_l3_core_services[590]: Node.1-Unit.1:PRI:notice
[os10:trap], %Dell EMC (OS10) %log-notice:IP_ADDRESS_DEL: IP Address
delete is successful. IP 101.1.2.2/30 deleted successfully
Mar 5 22:00:48 OS10 dn_l3_core_services[590]: Node.1-Unit.1:PRI:notice
[os10:trap], %Dell EMC (OS10) %log-notice:IP_ADDRESS_DEL: IP Address
delete is successful. IP 2101:100:2:1::2/64 deleted successfully

OS10(config)# end

OS10# show running-configuration interface ethernet 1/1/15
!
interface ethernet1/1/15
no shutdown
switchport access vlan 1
```

#### 示例 (光纤通道)

```
OS10# show running-configuration interface fibrechannel 1/1/1
!
interface fibrechannel1/1/1
no shutdown
description fc-port

OS10(config)# default interface fibrechannel 1/1/1
Proceed to cleanup the interface config? [confirm yes/no]:y
!
OS10 # show running-configuration interface fibrechannel 1/1/1
interface fibrechannel1/1/1
shutdown
```

#### 示例 (接口范围)

```
OS10(config)# interface range ethernet 1/1/1-1/1/4
OS10(conf-range-eth1/1/1-1/1/4)# show configuration
!
interface ethernet1/1/1
no shutdown
no switchport
ip address 192.21.43.1/31
ipv6 address 2000:21:43::21:43:1/127
!
interface ethernet1/1/2
no shutdown
no switchport
!
interface ethernet1/1/3
no shutdown
no switchport
ip address 192.28.43.1/31
ipv6 address 2000:28:43::28:43:1/127
!
interface ethernet1/1/4
no shutdown
no switchport
```

```

ip address 192.41.43.1/31
ipv6 address 2000:41:43::41:43:1/127

OS10(conf-range-eth1/1/1-1/1/4)# exit

OS10(config)# default interface range ethernet 1/1/1,1/1/2-1/1/4

Proceed to cleanup interface range config? [confirm yes/no]:yes
Mar 5 22:21:12 OS10 dn_l3_core_services[590]: Node.1-Unit.1:PRI:notice
[os10:trap], %Dell EMC (OS10) %log-notice:IP_ADDRESS_DEL: IP Address
delete is successful. IP 192.21.43.1/31 deleted successfully
Mar 5 22:21:12 OS10 dn_l3_core_services[590]: Node.1-Unit.1:PRI:notice
[os10:trap], %Dell EMC (OS10) %log-notice:IP_ADDRESS_DEL: IP Address
delete is successful. IP 2000:21:43::21:43:1/127 deleted successfully
Mar 5 22:21:12 OS10 dn_l3_core_services[590]: Node.1-Unit.1:PRI:notice
[os10:trap], %Dell EMC (OS10) %log-notice:IP_ADDRESS_DEL: IP Address
delete is successful. IP 192.28.43.1/31 deleted successfully
Mar 5 22:21:12 OS10 dn_l3_core_services[590]: Node.1-Unit.1:PRI:notice
[os10:trap], %Dell EMC (OS10) %log-notice:IP_ADDRESS_DEL: IP Address
delete is successful. IP 2000:28:43::28:43:1/127 deleted successfully
Mar 5 22:21:12 OS10 dn_l3_core_services[590]: Node.1-Unit.1:PRI:notice
[os10:trap], %Dell EMC (OS10) %log-notice:IP_ADDRESS_DEL: IP Address
delete is successful. IP 192.41.43.1/31 deleted successfully
Mar 5 22:21:12 OS10 dn_l3_core_services[590]: Node.1-Unit.1:PRI:notice
[os10:trap], %Dell EMC (OS10) %log-notice:IP_ADDRESS_DEL: IP Address
delete is successful. IP 2000:41:43::41:43:1/127 deleted successfully
Mar 5 22:21:12 OS10 dn_ifm[602]: Node.1-Unit.1:PRI:notice [os10:trap],
%Dell EMC (OS10) %log-notice:IFM_OSTATE_UP: Interface operational state
is up :vlan1

OS10(config)# interface range ethernet 1/1/1-1/1/4
OS10(conf-range-eth1/1/1-1/1/4)# show configuration
!
interface ethernet1/1/1
no shutdown
switchport access vlan 1
!
interface ethernet1/1/2
no shutdown
switchport access vlan 1
!
interface ethernet1/1/3
no shutdown
switchport access vlan 1
!
interface ethernet1/1/4
no shutdown
switchport access vlan 1

OS10(conf-range-eth1/1/1-1/1/4)#

```

**支持的版本** 10.4.0E(R1) or later

## default vlan-id

重新配置默认 VLAN 的 VLAN ID。

**语法** `default vlan-id vlan-id`

**参数** *vlan-id* — 输入默认 VLAN ID 号，从 1 到 4093。

**默认** VLAN1

**命令模式** CONFIGURATION

**使用情况信息** 默认情况下，VLAN1 用作默认 VLAN，用于在中继或访问模式下切换 OS10 端口上未标记的 L2 流量。如果将 VLAN1 用于网络特定的数据流量，请重新配置默认 VLAN 的 VLAN ID。命令会重新配置交换机访问模式中所有端口的访问 VLAN ID（默认 VLAN）。在将 VLAN ID 配置为默认 VLAN 之前，请确保其存在。

## 示例

```
OS10(config)# default vlan-id 10

OS10(config)# do show running-configuration
...
!
interface vlan1
no shutdown
!
interface vlan10
no shutdown
!
interface ethernet1/1/1
no shutdown
switchport access vlan 10
!
interface ethernet1/1/2
no shutdown
switchport access vlan 10
!
interface ethernet1/1/3
no shutdown
switchport access vlan 10
!
interface ethernet1/1/4
no shutdown
switchport access vlan 10
```

## 支持的版本

10.4.0E(R1) or later

# description (Interface)

配置接口的文本说明。

**语法** `description string`

**参数** `string` — 输入接口说明的文本字符串。最多 240 个字符。

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息**

- 要使用特殊字符作为说明字符串的一部分，请用双引号将字符串括起来。
- 输入此命令后，将不会保留字符之间的空格，除非用引号将整个说明括起来；例如，`"text description"`。
- 在 `description` 命令后输入文本字符串，以覆盖之前配置的任何文本字符串。
- 使用 `show running-configuration interface` 命令查看为每个接口配置的说明。
- 此命令的 `no` 版本将删除说明。

## 示例

```
OS10(conf-if-eth1/1/7)# description eth1/1/7
```

## 支持的版本

10.2.0E or later

# duplex

在管理端口上配置双工模式。

**语法** `duplex {full | half | auto}`

**参数**

- `full` — 将物理接口设置为双向传输。
- `half` — 将物理接口设置为仅单向传输。
- `auto` — 将端口设置为与连接的设备自动协商速度。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 您只能在管理端口上使用此命令。此命令的 `no` 版本将从管理端口中移除双工模式配置。

**示例**

```
OS10(config-if-ma-1/1/1)# duplex auto
```

**支持的版本** 10.3.0E or later

## enable dom

启用或禁用 DOM 功能。

**语法** dom enable

**参数** 无

**默认** 已禁用

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本将禁用数字光学监控。

**示例**

```
OS10# configure terminal
OS10(config)# dom enable
```

```
OS10# configure terminal
OS10(config)# no dom enable
```

**支持的版本** 10.4.3.0 or later

## enable dom traps

如果指定的参数超过三次所定义的阈值，则启用 DOM 陷阱。

**语法** snmp-server enable traps dom {temperature | voltage | rx-power | tx-power | bias}

**参数** temperature | voltage | rx-power | tx-power | bias — 输入关键字以针对指定类别启用 DOM 陷阱。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本将禁用 DOM 陷阱。

**示例**

```
OS10# configure terminal
OS10(config)# snmp-server enable traps dom temperature
```

```
OS10# configure terminal
OS10(config)# no snmp-server enable traps dom temperature
```

**支持的版本** 10.4.3.0 or later

## feature auto-breakout

支持前面板以太网端口自动检测 SFP 介质和自动配置分解接口。

**语法** feature auto-breakout

**参数** 无

**默认** 未配置

|        |                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 命令模式   | CONFIGURATION                                                                                                                                                                                              |
| 使用情况信息 | <p>输入 <code>feature auto-breakout</code> 命令并将受支持的分解线缆插入 QSFP+ 或 QSFP28 端口后，端口根据介质类型和速度自动配置分解接口。</p> <p>使用 <code>interface breakout</code> 命令手动配置分解接口。插入端口的介质类型不再自动获知。此命令的 <code>no</code> 版本将禁用自动分解功能。</p> |
| 示例     | <pre>OS10(config)# feature auto-breakout</pre>                                                                                                                                                             |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                                       |

## fec

在 25G、50G 和 100G 接口上配置转发纠错。

|        |                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>fec {CL74-FC   CL91-RS   CL108-RS   off}</code>                                                                                                      |
| 参数     | <ul style="list-style-type: none"> <li>CL74-FC — 支持 25G 和 50G</li> <li>CL91-RS — 支持 100G</li> <li>CL108-RS — 支持 25G 和 50G</li> <li>off — 禁用 FEC</li> </ul> |
| 默认     | <ul style="list-style-type: none"> <li>对于 25G 和 50G 接口: off</li> <li>对于 100G 接口: CL91-RS</li> </ul>                                                        |
| 命令模式   | CONFIGURATION                                                                                                                                              |
| 使用情况信息 | 此命令的 <code>no</code> 版本会将该值重置为默认值。                                                                                                                         |
| 示例     | <pre>OS10(config)# interface ethernet 1/1/41 OS10(config-if-eth1/1/41)# fec CL91-RS</pre>                                                                  |
| 支持的版本  | 10.3.0E or later                                                                                                                                           |

## interface breakout

将前面板以太网端口拆分为多个分解接口。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>interface breakout node/slot/port map {100g-1x   50g-2x   40g-1x   25g-4x   10g-4x   25g-4x}</code>                                                                                                                                                                                                                                                                                                        |
| 参数     | <ul style="list-style-type: none"> <li><code>node/slot/port</code> — 输入物理端口信息。</li> <li><code>100g-1x</code> — 将 QSFP28 端口重置为 100G 速度。</li> <li><code>50g-2x</code> — 将 QSFP28 端口拆分为两个 50GE 接口。</li> <li><code>40g-1x</code> — 设置要与 QSFP+ 40GE 收发器一起使用的 QSFP28 端口。</li> <li><code>25g-4x</code> — 将 QSFP28 端口拆分为四个 25GE 接口。</li> <li><code>10g-4x</code> — 将 QSFP28 端口或 QSFP+ 端口拆分为四个 10GE 接口。</li> </ul>        |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                              |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                    |
| 使用情况信息 | <ul style="list-style-type: none"> <li>每个分解接口将以配置的速度运行；例如，10G、25G 或 50G。</li> <li><code>no interface breakout node/slot/port</code> 命令将端口重置为其默认速度：40G 或 100G。</li> <li>要在统一端口上配置分解接口，请在端口组配置模式下使用 <code>mode {Eth   FC}</code> 命令。</li> <li>在 MX9116n 结构引擎和 MX5108n 以太网交换机上，面向背板服务器的端口不支持 <code>interface breakout</code> 命令。在 <code>show inventory media</code> 输出中，背板端口的状态类别显示为 <code>FIXED</code>。</li> </ul> |
| 示例     | <pre>OS10(config)# interface breakout 1/1/41 map 10g-4x</pre>                                                                                                                                                                                                                                                                                                                                                    |



**支持的版本** 10.2.2E or later

## interface ethernet

配置物理以太网接口。

**语法** `interface ethernet node/slot/port:subport`

**参数** `node/slot/port:subport` — 输入以太网接口信息。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本将删除接口。

**示例**

```
OS10(config)# interface ethernet 1/1/10:1
OS10(conf-if-eth1/1/10:1)#
```

**支持的版本** 10.2.0E or later

## interface loopback

配置环回接口。

**语法** `interface loopback id`

**参数** `id` — 输入环回接口 ID 号，从 0 到 16383。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本将删除环回接口。

**示例**

```
OS10(config)# interface loopback 100
OS10(conf-if-lo-100)#
```

**支持的版本** 10.2.0E or later

## interface mgmt

配置管理端口。

**语法** `interface mgmt node/slot/port`

**参数** `node/slot/port` — 输入管理接口的物理端口接口信息。

**默认** 已启用

**命令模式** CONFIGURATION

**使用情况信息** 您不能删除管理端口。要向管理端口分配 IP 地址，请使用 `ip address` 命令。

**示例**

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)#
```

**支持的版本** 10.2.0E or later

## interface null

在交换机上配置空接口。

|               |                                                               |
|---------------|---------------------------------------------------------------|
| <b>语法</b>     | <code>interface null number</code>                            |
| <b>参数</b>     | <i>number</i> — 输入要设置为空 (0) 的接口编号。                            |
| <b>默认</b>     | 0                                                             |
| <b>命令模式</b>   | CONFIGURATION                                                 |
| <b>使用情况信息</b> | 无法删除空接口。空接口中的唯一可用配置命令为 <code>ip unreachable</code> 。          |
| <b>示例</b>     | <pre>OS10(config)# interface null 0 OS10(conf-if-nu-0)#</pre> |
| <b>支持的版本</b>  | 10.3.0E or later                                              |

## interface port-channel

创建端口通道接口。

|               |                                                                         |
|---------------|-------------------------------------------------------------------------|
| <b>语法</b>     | <code>interface port-channel channel-id</code>                          |
| <b>参数</b>     | <i>channel-id</i> — 输入端口通道 ID 号，从 1 到 128。                              |
| <b>默认</b>     | 未配置                                                                     |
| <b>命令模式</b>   | CONFIGURATION                                                           |
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本将删除接口。                                           |
| <b>示例</b>     | <pre>OS10(config)# interface port-channel 10 OS10(conf-if-po-10)#</pre> |
| <b>支持的版本</b>  | 10.2.0E or later                                                        |

## interface range

配置用于批量配置的以太网、端口通道或 VLAN 接口的范围。

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>interface range {ethernet node/slot/port[:subport]-node/slot/port[:subport],[...]}   {port-channel IDnumber-IDnumber,[...]}   vlan vlanID-vlanID,[...]}</code>                                                                                                                                                                                                                                                                                         |
| <b>参数</b>     | <ul style="list-style-type: none"><li><code>node/slot/port[:subport]-node/slot/port[:subport]</code> — 输入一系列以太网接口。</li><li><code>IDnumber-IDnumber</code> — 输入端口通道号范围，从 1 到 128。</li><li><code>vlanID-vlanID</code> — 输入 VLAN ID 编号范围，从 1 到 4093。</li></ul>                                                                                                                                                                                                  |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>使用情况信息</b> | <p>输入最多六个逗号分隔接口范围，逗号之间不带空格。在创建接口范围时，不会对接口进行排序，并且按输入的顺序显示。您不能混用带有 VLAN 的以太网端口等接口配置。</p> <ul style="list-style-type: none"><li>如果至少一个接口有效，则创建 <code>Abulk</code> 配置。</li><li>非现有接口将从批量配置中排除，并显示一条警告消息。</li><li>此命令有多个端口范围，提示将排除较小的端口范围。</li><li>如果您输入重叠的端口范围，端口范围将扩展到最小端口和最大端端口。</li><li>您只能使用 <code>interface vlan</code> 和 <code>interface port-channel</code> 命令创建的 VLAN 和端口通道接口。</li><li>您不能使用 <code>interface range</code> 命令创建虚拟 VLAN 或端口通道接口。</li></ul> |

- 此命令的 `no` 版本将删除接口范围。

#### 示例

```
OS10(config)# interface range ethernet 1/1/7-1/1/24
OS10(conf-range-eth1/1/7-1/1/24)#
```

#### 支持的版本

10.2.0E or later

## interface vlan

创建 VLAN 接口。

#### 语法

`interface vlan vlan-id`

#### 参数

`vlan-id` — 输入 VLAN ID 号，从 1 到 4093。

#### 默认

VLAN 1

#### 命令模式

CONFIGURATION

#### 使用情况信息

不支持 FTP、TFTP、MAC ACL 和 SNMP 操作。IP ACL 仅在 VLAN 上受支持。此命令的 `no` 版本将删除接口。

 **注：**在 SmartFabric 服务模式下，创建 VLAN 处于禁用状态。

#### 示例

```
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)#
```

#### 支持的版本

10.2.0E or later

## link-bundle-utilization

配置链路套装利用率。

#### 语法

`link-bundle-utilization trigger-threshold value`

#### 参数

`value` — 输入在端口通道成员上触发流量监控的端口通道带宽百分比，从 0 到 100。

#### 默认

已禁用

#### 命令模式

CONFIGURATION

#### 使用情况信息

无

#### 示例

```
OS10(config)# link-bundle-utilization trigger-threshold 10
```

#### 支持的版本

10.2.0E or later

## mode

将前面板统一端口组配置为在光纤通道或以太网模式下运行，或者将 QSFP28-DD 或 QSFP28 端口组配置为在以太网模式下激活的接口上以指定速度运行。

#### 语法

`mode {Eth {100g-2x | 100g-1x | 50g-2x | 40g-2x | 40g-1x | 25g-8x [fabric-expander-mode] | 25g-4x | 10g-8x | 10g-4x} | FC {32g-4x | 32g-2x | 32g-1x | 16g-4x}}`

#### 参数

- `mode Eth` — 在以太网模式下配置端口组并将速度设置为：
  - `100g-2x` — 将 QSFP28-DD 端口拆分为两个 100GE 接口。
  - `100g-1x` — 将 QSFP28 端口组重置为 100GE 模式。
  - `50g-2x` — 将 QSFP28 端口拆分为两个 50GE 接口。
  - `40g-2x` — 将端口组拆分为两个 40GE 接口。

- 40g-1x — 将端口组设置为 40G 模式，以便与 QSFP+ 40GE 收发器配合使用。
- 25g-8x fabric-expander-mode — 将 QSFP28-DD 端口拆分为八个 25GE 接口，以连接到结构扩展器。
- 25g-8x — 将端口组拆分为八个 25GE 接口。
- 25g-4x — 将端口组拆分为四个 25GE 接口。
- 10g-8x — 将端口组拆分为八个 10GE 接口。
- 10g-4x — 将端口组拆分为四个 10GE 接口。
- mode FC — 将端口组配置为在光纤通道模式下运行并将速度设置为：
  - 32g-4x — 将端口组拆分为四个 32GFC 接口。
  - 32g-2x — 将端口组拆分为两个 32GFC 接口，子端口 1 和 3。
  - 32g-1x — 将端口组拆分为一个 32GFC 接口，子端口 1。
  - 16g-4x — 将端口组拆分为四个 16GFC 接口；支持 4x32GFC 超额订阅。

**默认** S4148U-ON：取决于激活的端口配置文件。

MX9116n 结构交换引擎：

- QSFP28-DD 端口组 1 到 9 在 8x25GE 结构扩展器模式 (FEM) 下运行。
- QSFP28-DD 端口组 10 到 12 在 2x100GE 模式下运行。
- QSFP28 端口组 13 和 14 在 1x100GE 模式下运行。
- 统一端口组 15 和 16 在以太网 1x100GE 模式下运行。

## 命令模式

## 使用情况信息

PORT-GROUP

- mode {FC | Eth} 命令将端口组配置为以线路速率运行，并保证不会丢失流量。
- 要在 FC 接口上配置超额订阅，请使用 speed 命令。
- 要查看当前活动的端口和子端口，请使用 show interfaces status 命令。
- 命令的 no 版本将端口组接口重置为默认的以太网端口模式/速度。在接口上重置模式之前，请使用 no mode 命令。

## 示例

```
OS10(config-pg-1/1/2)# mode FC 16g-4x
OS10(config-pg-1/1/8)# mode Eth 10g-4x
```

## 示例：重置模式

```
OS10(config-pg-1/1/2)# mode FC 16g-4x
OS10(config-pg-1/1/2)# no mode
OS10(config-pg-1/1/2)# mode Eth 10g-4x
```

**支持的版本** 10.3.1E or later

# mode l3

在配置 VLAN 扩展配置文件后在 VLAN 上启用 L3 路由。

**语法** mode l3

**参数** 无

**默认** 未配置

**命令模式** INTERFACE VLAN

**使用情况信息** 要配置 VLAN 扩展配置文件，请使用 scale-profile vlan 命令。扩展配置文件在您创建的所有 VLAN 上全局应用 L2 模式，并禁用 L3 传输。要启用 VLAN 上的 L3 路由流量，请使用 mode L3 命令。

## 示例

```
OS10(config)# interface vlan 10
OS10(config-if-vl-10)# mode L3
```

**支持的版本** 10.4.0E(X2) or later

# mtu

设置以太网 L2 或 L3 接口的链路最大传输单位 (MTU) 帧大小。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | mtu value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 参数     | value — 输入最大帧大小（以字节为单位），从 1280 到 65535。S3000-ON 的最大帧大小是 12000，而 S4000-ON 是 9216。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 默认     | 1532 字节                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 命令模式   | INTERFACE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | <p>要返回默认 MTU 值，请使用 <code>no mtu</code> 命令。如果 IP 数据包包含 L2 标头，则 IP MTU 必须至少是小于 L2 MTU 的 32 字节。</p> <ul style="list-style-type: none"><li>Port-channels<ul style="list-style-type: none"><li>所有成员都必须具有相同的链路 MTU 值和相同的 IP MTU 值。</li><li>端口通道链路 MTU 和 IP MTU 必须小于或等于在通道成员上配置的链路 MTU 和 IP MTU 值。例如，如果成员具有 2100 MTU 的链路和 IP MTU 2000，则端口通道的 MTU 值不能高于 2100（对于 IP MTU）或 2000 字节（对于 IP MTU）。</li></ul></li><li>VLAN<ul style="list-style-type: none"><li> <b>注：</b>首先必须在 VLAN 成员上配置 MTU，然后再配置 VLAN MTU。</li><li>VLAN 的所有成员必须具有相同的 MTU 值。</li><li>标记的成员必须具有一个比未标记成员高 4 个字节的链路 MTU，以对数据包标签进行帐户。</li><li>确保 VLAN 成员的 MTU 大于或等于 VLAN MTU。如果您在配置 VLAN MTU 后在 VLAN 成员上配置 MTU，则 VLAN MTU 可能不会更新。OS10 选择 VLAN 或 VLAN 成员上的最低 MTU 值配置为 VLAN MTU。</li></ul></li></ul> <p>例如，VLAN 包含链路 MTU 为 1522 和 IP MTU 为 1500 的标记成员，以及链路 MTU 为 1518 和 IP MTU 为 1500 的未标记成员。VLAN 的链路 MTU 不能超过 1518 字节，并且其 IP MTU 不能超过 1500 字节。</p> |

|    |                                             |
|----|---------------------------------------------|
| 示例 | <pre>OS10(conf-if-eth1/1/7)# mtu 3000</pre> |
|----|---------------------------------------------|

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|

# negotiation

在接口上配置协商模式。

|        |                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | negotiation {auto   on   off}                                                                                                                                                 |
| 参数     | <p>auto — 将协商模式设置为默认设置。默认设置取决于您使用的介质。</p> <p>on — 强制实施接口协商。</p> <p>off — 禁用接口协商。</p>                                                                                          |
| 默认     | 自动                                                                                                                                                                            |
| 命令模式   | INTERFACE CONFIGURATION                                                                                                                                                       |
| 使用情况信息 | <p>使用 <code>show interfaces</code> 命令查看接口协商状态。</p> <p>该链路的两端必须已启用或禁用自动协商，链路才会启动。</p> <p>使用 <code>negotiation auto</code> 命令或 <code>no negotiation</code> 命令将协商模式重置为其默认设置。</p> |

|    |                                                                                                                                        |
|----|----------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10(conf-if-eth1/1/50)# negotiation off OS10(conf-if-eth1/1/50)# show configuration ! interface ethernet1/1/50 no shutdown</pre> |
|----|----------------------------------------------------------------------------------------------------------------------------------------|

```

switchport access vlan 1
negotiation off
flowcontrol receive on
OS10(conf-if-eth1/1/50)# negotiation on
OS10(conf-if-eth1/1/50)# show configuration
!
interface ethernet1/1/50
no shutdown
switchport access vlan 1
negotiation on
flowcontrol receive on
OS10(conf-if-eth1/1/50)# negotiation auto
OS10(conf-if-eth1/1/50)# show configuration
!
interface ethernet1/1/50
no shutdown
switchport access vlan 1
flowcontrol receive on
OS10(conf-if-eth1/1/50)#
OS10(conf-if-eth1/1/50)# negotiation on
OS10(conf-if-eth1/1/50)# show configuration
!
interface ethernet1/1/50
no shutdown
switchport access vlan 1
negotiation on
flowcontrol receive on
OS10(conf-if-eth1/1/50)# no negotiation
OS10(conf-if-eth1/1/50)# show configuration
!
interface ethernet1/1/50
no shutdown
switchport access vlan 1
flowcontrol receive on
OS10(conf-if-eth1/1/50)# do show interface ethernet 1/1/50
Ethernet 1/1/50 is up, line protocol is up
Hardware is Eth, address is e4:f0:04:3e:2d:86
Current address is e4:f0:04:3e:2d:86
Pluggable media present, QSFP28 type is QSFP28 100GBASE-CR4-2.0M
Wavelength is 64
Receive power reading is not available

Interface index is 112
Internet address is not set
Mode of IPv4 Address Assignment: not set
Interface IPv6 oper status: Disabled
MTU 1532 bytes, IP MTU 1500 bytes
LineSpeed 100G, Auto-Negotiation on

```

**支持的版本** 10.2.0E 或更高版本

## port mode Eth

将 Z9264F-ON QSFP28 端口组配置为在以太网模式下运行，并在激活的接口上使用指定的速度。

### 语法

```
port node/slot/port mode Eth port-mode
```

### 参数

- *node/slot/port* — 输入接口类型详情。
- *mode Eth* — 在以太网模式下配置端口组并将速度设置为：
  - 100g-1x — 将端口重置为 100GE 模式。
  - 50g-2x — 将一个端口拆分为两个 50GE 接口。
  - 40g-1x — 将端口设置为 40GE 模式，以便与 QSFP+40GE 收发器配合使用。
  - 25g-4x — 将一个端口拆分为四个 25GE 接口。
  - 10g-4x — 将一个端口拆分为四个 10GE 接口。

### 默认

100g-1x

|               |                                                                                                                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>命令模式</b>   | PORT-GROUP                                                                                                                                                                                                                       |
| <b>使用情况信息</b> | 要查看当前活动的端口和子端口，请使用 <code>show port-group</code> 命令。命令的 <code>no</code> 版本将端口组接口重置为默认的以太网端口模式/速度。                                                                                                                                 |
| <b>示例</b>     | <pre> OS10(config)# port-group 1/1/2 OS10(conf-pg-1/1/2)# profile restricted OS10(conf-pg-1/1/2)# port 1/1/3 mode Eth 25g-4x OS10(conf-pg-1/1/2)# exit OS10(config)# interface ethernet 1/1/3:2 OS10(conf-if-eth1/1/3:2)# </pre> |
| <b>支持的版本</b>  | 10.4.3.0 or later                                                                                                                                                                                                                |

## port-group

配置一组前面板统一端口或双密度 QSFP28 (QSFP28-DD) 或单密度 QSFP28 端口组。

|               |                                                                                                                                                                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>port-group node/slot/port-group</code>                                                                                                                                                                                                                |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>node/slot</code> — 在配置端口组时，为 <code>node/slot</code> 输入 1/1。</li> <li><code>port-group</code> — 输入端口组编号，从 1 到 16。可用端口组范围取决于交换机。</li> </ul>                                                                      |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                         |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                                                                                                                                               |
| <b>使用情况信息</b> | 输入 PORT-GROUP 以： <ul style="list-style-type: none"> <li>在光纤通道或以太网模式下配置统一端口，并使用指定的速度中断接口。</li> <li>使用指定的速度将 MX9116n QSFP28-DD 或 QSFP28 端口组分成多个接口。</li> <li>使用指定的速度将 Z9264F-ON QSFP28 端口组划分为多个接口。</li> </ul> 要查看属于端口组的端口，请使用 <code>show port-group</code> 命令。 |

**示例**

```

OS10(config)# port-group 1/1/8
OS10(conf-pg-1/1/8)#

```

**支持的版本** 10.3.1E or later

## profile

在 Z9264F-ON 交换机上配置分解接口。

|               |                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>profile {restricted   unrestricted}</code>                                                                                                                                                                                                                                                                                                                                                                           |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>restricted</code> — 仅适用于端口组中的奇数编号端口。端口组中的偶数编号端口处于禁用状态。支持的速度包括：               <ul style="list-style-type: none"> <li>100g-1x</li> <li>40g-1x</li> <li>25g-4x</li> <li>10g-4x</li> </ul> </li> <li><code>unrestricted</code> — 适用于端口组中的奇数编号和偶数编号端口。支持的速度包括：               <ul style="list-style-type: none"> <li>100g-1x</li> <li>50g-2x</li> <li>40g-1x</li> </ul> </li> </ul> |
| <b>默认</b>     | 不受限                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>命令模式</b>   | PORT-GROUP                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>使用情况信息</b> | 输入 <code>profile</code> 命令以配置分解接口。使用 <code>port</code> 命令以指定速度。Z9264F-ON 交换机共有 64 个物理端口，最多可支持 128 个逻辑端口。要查看属于端口组的端口，请使用 <code>show port-group</code> 命令。                                                                                                                                                                                                                                                                   |

|       |                                                                                   |
|-------|-----------------------------------------------------------------------------------|
| 示例    | <pre>OS10(config)# port-group 1/1/2 OS10(conf-pg-1/1/2)# profile restricted</pre> |
| 支持的版本 | 10.4.3.0 or later                                                                 |

## scale-profile vlan

在交换机上配置 L2 VLAN 扩展配置文件。

|        |                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | scale-profile vlan                                                                                                                                                                |
| 参数     | 无                                                                                                                                                                                 |
| 默认     | 未配置                                                                                                                                                                               |
| 命令模式   | CONFIGURATION                                                                                                                                                                     |
| 使用情况信息 | <p>当您扩展 VLAN 的数量时，使用 VLAN 扩展配置文件，以使交换机占用的内存更少。在交换机上配置 VLAN 之前，请先启用扩展配置文件。扩展配置文件在您创建的所有 VLAN 上全局应用 L2 模式，并禁用 L3 传输。命令的 no 版本将禁用 L2 VLAN 扩展。要启用 VLAN 上的 L3 路由流量，请使用 mode L3 命令。</p> |
| 示例     | <pre>OS10(config)# scale-profile vlan</pre>                                                                                                                                       |
| 支持的版本  | 10.4.0E(X2) or later                                                                                                                                                              |

## show discovered-expanders

显示连接到 MX9116n 结构交换引擎的结构扩充器。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show discovered-expanders                                                                                                                                                                                                                                                                                                                                                                                       |
| 语法     | show discovered-expanders                                                                                                                                                                                                                                                                                                                                                                                       |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                                                                               |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                            |
| 使用情况信息 | <p>使用 show discovered-expanders 命令验证自动查找到的结构扩充器。</p> <p>如果结构交换引擎处于 SmartFabric 模式，则它会自动查找并配置连接的结构扩充器：</p> <ul style="list-style-type: none"> <li>结构扩充器和虚拟插槽 ID 的虚拟端口将创建并映射到结构引擎上 FEM 模式下的 8x25GE 分解接口。</li> <li>系统会自动发现设备 ID。</li> <li>服务器流量通过结构扩充器上的 QSFP28-DD 上行链路传输到结构引擎。</li> </ul> <p>如果结构交换引擎处于完全切换模式，请使用 CLI 配置交换机。您必须手动配置结构扩展器的设备 ID，有关详情，请参阅<a href="#">虚拟端口</a>。设备 ID 也称为<a href="#">虚拟插槽 ID</a>。</p> |
| 示例     | <pre>OS10# show discovered-expanders Service-  Model          Type  Chassis-   Chassis-slot  Port-group Virtual- tag              service-tag              Slot- Id ----- 403RPK2  MX7116n Fabric  1    SKY003Q    A2             1/1/2       71                                Expander Module</pre>                                                                                                           |
| 支持的版本  | 10.4.0E(R3S) or later                                                                                                                                                                                                                                                                                                                                                                                           |



## show interface

显示接口信息。

### 语法

show interface [type]

### 参数

interface type — 输入接口类型:

- phy-eth node/slot/port[:subport] — 显示有关连接到接口的物理端口的信息。
- status — 显示接口状态。
- ethernet node/slot/port[:subport] — 显示以太网接口信息。
- loopback id — 显示环回 ID, 从 0 到 16383。
- mgmt node/slot/port — 显示管理接口信息。
- null — 显示控接口信息。
- port-channel id-number — 显示端口通道接口 ID, 从 1 到 128。
- vlan vlan-id — 显示 VLAN 接口编号, 从 1 到 4093。

### 默认

未配置

### 命令模式

EXEC

### 使用情况信息

使用 do show interface 命令从其他命令模式查看接口信息。

### 示例

```
OS10# show interface
Ethernet 1/1/2 is up, line protocol is up
Hardware is Dell EMC Eth, address is 00:0c:29:54:c8:57
Current address is 00:0c:29:54:c8:57
Pluggable media present, QSFP+ type is QSFP+ 40GBASE CR 1.0M
Wavelength is 64
Receive power reading is 0.0
Interface index is 17305094
Internet address is not set
Mode of IPv4 Address Assignment: not set
Interface IPv6 oper status: Enabled
Link local IPv6 address: fe80::20c:29ff:fe54:c857/64
Global IPv6 address: 2::1/64
MTU 1532 bytes, IP MTU 1500 bytes
LineSpeed 40G, Auto-Negotiation on
FEC is auto, Current FEC is off
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 60
Last clearing of "show interface" counters: 00:40:14
Queuing strategy: fifo
Input statistics:
 0 packets, 0 octets
 0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
 0 Multicasts, 0 Broadcasts, 0 Unicasts
 0 runts, 0 giants, 0 throttles
 0 CRC, 0 overrun, 0 discarded
Output statistics:
 0 packets, 0 octets
 0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
 0 Multicasts, 0 Broadcasts, 0 Unicasts
 0 throttles, 0 discarded, 0 Collisions, 0 wredrops
Rate Info(interval 299 seconds):
 Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
 Output 0 Mbits/sec, 0 packets/sec, 0% of line rate
Time since last interface status change: 3 weeks 1 day 20:30:38

--more--
```

### 示例 (端口通道)

```
OS10# show interface port-channel 1
Port-channel 1 is up, line protocol is down
Address is 90:b1:1c:f4:a5:8c, Current address is 90:b1:1c:f4:a5:8c
Interface index is 85886081
Internet address is not set
Mode of IPv4 Address Assignment: not set
```

```
MTU 1532 bytes
LineSpeed 0
Minimum number of links to bring Port-channel up is 1
Maximum active members that are allowed in the portchannel is 5
Members in this channel:
ARP type: ARPA, ARP Timeout: 60
```

```
OS10# show interface port-channel summary
LAG Mode Status Uptime Ports
22 L2 up 20:38:08 Eth 1/1/10 (Up)
 Eth 1/1/11 (Down)
 Eth 1/1/12 (Inact)
23 L2 up 20:34:32 Eth 1/1/20 (Up)
 Eth 1/1/21 (Up)
 Eth 1/1/22 (Up)
```

## 示例 (VLAN)

```
OS10# show interface vlan 20
Vlan 20 is up, line protocol is down
vlan name: vlanname20
Address is 0c:9b:1d:68:89:6a, Current address is 0c:9b:1d:68:89:6a
Interface index is 60
Internet address is not set
Mode of IPv4 Address Assignment: not set
Interface IPv6 oper status: Enabled
MTU 1532 bytes, IP MTU 1500 bytes
LineSpeed 0
ARP type: ARPA, ARP Timeout: 60
Last clearing of "show interface" counters: 00:05:14
Queuing strategy: fifo
Input statistics:
 0 packets, 0 octets
Output statistics:
 0 packets, 0 octets
Time since last interface status change: 00:05:15
```

**支持的版本** 10.2.0E or later

## show interface transceiver “Tunable wavelength”

显示光纤接口的已配置波长值。

**语法** `show interface phy-eth interface transceiver | grep “Tunable wavelength”`

**参数** `interface` — 指定您想要查看其视觉波长详细信息的接口。

**默认** 无。

**命令模式** EXEC PRIVILEGE

**使用情况信息** 无。

**示例**

```
OS10# show interface phy-eth 1/1/14 transceiver | grep "Tunable wavelength"

SFP1/1/14 Tunable wavelength= 1530.000nm
```

**支持的版本** 10.4.2E 或更高版本

## show inventory media

显示在交换机端口中安装的介质。

**语法** `show inventory media`

**参数** 无

命令模式

使用情况信息

EXEC

使用 `show inventory media` 命令验证插入端口的介质类型。

在 MX9116n 结构交换引擎和 MX5108n 以太网交换机上，面向服务器的接口位于背板上，并在默认情况下处于启用状态。要查看到服务器的背板端口连接，请使用 `show inventory media` 命令。在输出中，FIXED 端口不使用外部收发器，并且始终显示为 Dell EMC Qualified。

示例

```
OS10# show inventory media

System Inventory Media

Node/Slot/Port Category Media Serial Number Dell EMC
Qualified

1/1/1 Not Present
1/1/2 SFP+ SFP+ 10GBASE SR AM70843 true
1/1/3 Not Present
1/1/4 SFP+ SFP+ 10GBASE SR AKN0LC7 false
1/1/5 SFP+ SFP+ 10GBASE SR AM718GQ true
1/1/6 SFP+ SFP+ 10GBASE SR AM708XM true
1/1/7 SFP+ SFP+ 10GBASE SR AQ2237K true
1/1/8 SFP+ SFP+ 10GBASE SR AGT047N true
1/1/9 Not Present
1/1/10 Not Present
1/1/11 Not Present
1/1/12 Not Present
1/1/13 Not Present
1/1/14 Not Present
1/1/15 SFP+ SFP+ 10GBASE SR AK60QJN false
1/1/16 SFP+ SFP+ 10GBASE SR AL30KWM true
1/1/17 SFP+ SFP+ 10GBASE SR AQ22DMB true
1/1/18 SFP+ SFP+ 10GBASE SR AQM146U true
...
```

示例：MX9116n 结构引擎

```
OS10# show inventory media

System Inventory Media

Node/Slot/Port Category Media Serial Number Dell EMC
Qualified

1/1/1 FIXED INTERNAL true
1/1/2 FIXED INTERNAL true
1/1/3 FIXED INTERNAL true
1/1/4 FIXED INTERNAL true
1/1/5 FIXED INTERNAL true
1/1/6 FIXED INTERNAL true
1/1/7 FIXED INTERNAL true
1/1/8 FIXED INTERNAL true
1/1/9 FIXED INTERNAL true
1/1/10 FIXED INTERNAL true
1/1/11 FIXED INTERNAL true
1/1/12 FIXED INTERNAL true
1/1/13 FIXED INTERNAL true
1/1/14 FIXED INTERNAL true
1/1/15 FIXED INTERNAL true
1/1/16 FIXED INTERNAL true
```

示例：MX5108n 以太网交换机

```
OS10# show inventory media

System Inventory Media

Node/Slot/Port Category Media Serial Number Dell EMC
Qualified

1/1/1 FIXED INTERNAL true
1/1/2 FIXED INTERNAL true
```

|       |       |          |      |
|-------|-------|----------|------|
| 1/1/3 | FIXED | INTERNAL | true |
| 1/1/4 | FIXED | INTERNAL | true |
| 1/1/5 | FIXED | INTERNAL | true |
| 1/1/6 | FIXED | INTERNAL | true |
| 1/1/7 | FIXED | INTERNAL | true |
| 1/1/8 | FIXED | INTERNAL | true |
| ...   |       |          |      |

**支持的版本** 10.2.0E or later

## show link-bundle-utilization

显示有关链路套装利用率的信息。

**语法** show link-bundle-utilization

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# show link-bundle-utilization

Link-bundle trigger threshold - 60
```

**支持的版本** 10.2.0E or later

## show port-channel summary

显示端口通道摘要信息。

**语法** show port-channel summary

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10(conf-if-eth1/1/4)# do show port-channel summary
Flags: D - Down I - member up but inactive P - member up and active
U - Up (port-channel)

Group Port-Channel Type Protocol Member Ports

22 port-channel22 (U) Eth STATIC 1/1/2(D) 1/1/3(P)
23 port-channel23 (D) Eth DYNAMIC 1/1/4(I)
```

**示例（接口）**

```
OS10(conf-range-eth1/1/10-1/1/11,1/1/13,1/1/14)# do show port-channel
summary
Flags: D - Down U - member up but inactive P - member up and active
U - Up (port-channel)

Group Port-Channel Type Protocol Member Ports

22 port-channel22 (U) Eth STATIC 1/1/10(P) 1/1/11(P) 1/1/12(P) 1/1/13(P)
1/1/14(P) 1/1/15(P) 1/1/16(P) 1/1/17(P) 1/1/18(P) 1/1/19(P)
23 port-channel23 (D) Eth STATIC
OS10(config)# interface range e1/1/12-1/1/13,1/1/15,1/1/17-1/1/18
OS10(conf-range-eth1/1/12-1/1/13,1/1/15,1/1/17-1/1/18)# no channel-group
```

```
OS10(conf-range-eth1/1/12-1/1/13,1/1/15,1/1/17-1/1/18)# do show port-channel summary
Flags: D - Down U - member up but inactive P - member up and active
U - Up (port-channel)

Group Port-Channel Type Protocol Member Ports

22 port-channel22 (U) Eth STATIC 1/1/10(P) 1/1/11(P) 1/1/14(P) 1/1/16(P)
1/1/19(P)
23 port-channel23 (D) Eth STATIC
```

支持的版本 10.2.0E or later

show port-group

显示交换机上的当前端口组配置。

- 语法 show port-group
- 参数 无
- 默认 无
- 命令模式 EXEC
- 使用情况信息 要查看属于每个端口组的端口，请使用 show port-group 命令。要配置端口组，请使用 port-group 命令。

示例：S4148U-ON

```
OS10(config)# show port-group
port-group mode ports
1/1/1 Eth 10g-4x 1 2 3 4
1/1/2 FC 16g-2x 5 6 7 8
1/1/3 FC 16g-2x 9 10 11 12
1/1/4 FC 16g-2x 13 14 15 16
1/1/5 FC 16g-2x 17 18 19 20
1/1/6 FC 16g-2x 21 22 23 24
1/1/7 Eth 100g-1x 25
1/1/8 Eth 40g-1x 26
1/1/9 Eth 100g-1x 29
1/1/10 Eth 40g-1x 30
```

示例：MX9116n结构引擎

```
OS10(config)# show port-group
Port-group Mode Ports FEM
port-group1/1/1 Eth 25g-8x 17 18 FEM
port-group1/1/2 Eth 25g-8x 19 20 FEM
port-group1/1/3 Eth 25g-8x 21 22 FEM
port-group1/1/4 Eth 25g-8x 23 24 FEM
port-group1/1/5 Eth 25g-8x 25 26 FEM
port-group1/1/6 Eth 25g-8x 27 28 FEM
port-group1/1/7 Eth 25g-8x 29 30 FEM
port-group1/1/8 Eth 25g-8x 31 32 FEM
port-group1/1/9 Eth 25g-8x 33 34 FEM
port-group1/1/10 Eth 100g-2x 35 36 -
port-group1/1/11 Eth 100g-2x 37 38 -
port-group1/1/12 Eth 100g-2x 39 40 -
port-group1/1/13 Eth 100g-1x 41 -
port-group1/1/14 Eth 100g-1x 42 -
port-group1/1/15 Eth 100g-1x 43 -
port-group1/1/16 Eth 100g-1x 44 -
```

示例：Z9264F-ON

```
OS10(config)# show port-group
hybrid-group profile Ports Mode
port-group1/1/1 restricted 1/1/1 Eth 10g-4x
1/1/2 Eth Disabled
port-group1/1/2 restricted 1/1/3 Eth 10g-4x
1/1/4 Eth Disabled
```

|                 |            |        |              |
|-----------------|------------|--------|--------------|
| port-group1/1/3 | restricted | 1/1/5  | Eth 10g-4x   |
|                 |            | 1/1/6  | Eth Disabled |
| port-group1/1/4 | restricted | 1/1/7  | Eth 10g-4x   |
|                 |            | 1/1/8  | Eth Disabled |
| port-group1/1/5 | restricted | 1/1/9  | Eth 10g-4x   |
|                 |            | 1/1/10 | Eth Disabled |
| port-group1/1/6 | restricted | 1/1/11 | Eth 10g-4x   |
|                 |            | 1/1/12 | Eth Disabled |
| port-group1/1/7 | restricted | 1/1/13 | Eth 10g-4x   |
|                 |            | 1/1/14 | Eth Disabled |
| port-group1/1/8 | restricted | 1/1/15 | Eth 10g-4x   |

- 支持的版本**
- 10.3.1E or later
  - 10.4.3.0 or later — 已添加 Z9264F-ON 平台支持

## show switch-port-profile

显示交换机上的当前和默认端口配置文件。

- 语法** `show switch-port-profile node/slot`
- 参数**
- `node/slot` — 输入交换机信息。对于独立交换机，输入 1/1。
- 默认** `profile-1`
- 命令模式** EXEC
- 使用情况信息** 交换机端口配置文件用于确定可用的前面板端口以及以太网和统一端口上的分解模式。要显示当前端口配置文件，请使用 `show switch-port-profile` 命令。要将交换机重置为默认端口配置文件，请使用 `no switch-port-profile node/slot` 命令。

**示例**

```
OS10(config)# show switch-port-profile 1/1
```

| Node/Unit | Current   | Next-boot | Default   |
|-----------|-----------|-----------|-----------|
| 1/1       | profile-2 | profile-2 | profile-1 |

Supported Profiles:

```
profile-1
profile-2
profile-3
profile-4
profile-5
profile-6
```

- 支持的版本** 10.3.1E or later

## show system

显示 DOM 功能的状态（无论是已启用还是已禁用）。

- 语法** `show system`
- 参数** 无
- 默认** DOM 已禁用
- 命令模式** EXEC
- 使用情况信息** 无

**示例**

```
OS10# show system
Node Id : 1
MAC : 14:18:77:15:c3:e8
Number of MACs : 256
Up Time : 1 day 00:48:58
```

```
-- Unit 1 --
Status : up
System Identifier : 1
Down Reason : unknown
Digital Optical Monitoring : disable
System Location LED : off
Required Type : S4148F
Current Type : S4148F
Hardware Revision : X01
Software Version : 10.5.0.0
Physical Ports : 48x10GbE, 2x40GbE, 4x100GbE
BIOS : 3.33.0.0-3
System CPLD : 0.4
Master CPLD : 0.10
Slave CPLD : 0.7
```

**支持的版本** 10.4.3.0 or later

## show unit-provision

显示连接到结构交换引擎的结构扩展器的设备 ID 和服务编号。

**语法** show unit-provision

**语法** show unit-provision

**参数** 无

**命令模式** EXEC

**使用情况信息** 如果结构交换引擎处于完全切换模式，则必须手动配置已连接结构扩展器的设备 ID。有关详情，请参阅[虚拟端口](#)。使用 show unit-provision 命令显示已分配和未分配的单元 ID 以及服务编号调配名称值。使用 unit-provision 命令配置具有未分配设备 ID 和调配名称的结构扩展器。

**示例**

```
OS10# show unit-provision
```

| Node ID | Unit ID | Provision Name | Discovered Name | State |
|---------|---------|----------------|-----------------|-------|
| 1       | 71      |                |                 |       |
| 1       | 72      |                |                 |       |
| 1       | 73      |                |                 |       |
| 1       | 74      |                |                 |       |
| 1       | 75      |                |                 |       |
| 1       | 76      |                |                 |       |
| 1       | 77      |                |                 |       |
| 1       | 78      | 403RPK2        | 403RPK2         | up    |
| 1       | 79      |                |                 |       |
| 1       | 80      |                |                 |       |
| 1       | 81      |                |                 |       |
| 1       | 82      |                |                 |       |

**支持的版本** 10.4.0E(R3S) or later

## show vlan

显示当前的 VLAN 配置。

**语法** show vlan [vlan-id]

**参数** vlan-id — (可选) 输入 VLAN ID，从 1 到 4093。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

|           |                                                                                                                                                                                       |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>示例</b> | <pre> OS10# show vlan Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring VLANs Q: A - Access (Untagged), T - Tagged NUM Status Description Q Ports 1 down </pre> |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**支持的版本** 10.2.0E or later

## shutdown

禁用接口。

|               |                                                                                                                                                                                                                     |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | shutdown                                                                                                                                                                                                            |
| <b>参数</b>     | 无                                                                                                                                                                                                                   |
| <b>默认</b>     | 已禁用                                                                                                                                                                                                                 |
| <b>命令模式</b>   | INTERFACE                                                                                                                                                                                                           |
| <b>使用情况信息</b> | <p>此命令将物理接口标记为对于流量不可用。禁用 VLAN 或端口通道会导致不同的行为。禁用 VLAN 后，该 VLAN 内的 L3 功能将被禁用，并且 L2 流量将继续流动。在端口通道上使用 shutdown 命令，以禁用端口通道上的所有流量和单个接口。使用 no shutdown 命令可启用接口上的端口通道。shutdown 和 description 命令是您可以在作为端口通道成员的接口上配置的唯一命令。</p> |

|           |                                                                                         |
|-----------|-----------------------------------------------------------------------------------------|
| <b>示例</b> | <pre> OS10(config)# interface ethernet 1/1/7 OS10(conf-if-eth1/1/7)# no shutdown </pre> |
|-----------|-----------------------------------------------------------------------------------------|

**支持的版本** 10.2.0E or later

## speed（光纤通道）

配置光纤通道接口的传输速率。

|               |                                                                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | speed {8   16   32   auto}                                                                                                                                                                                                                |
| <b>参数</b>     | <p>将光纤通道接口的速度设置为：</p> <ul style="list-style-type: none"> <li>8 — 8 GFC</li> <li>16 — 16 GFC</li> <li>32 — 32 GFC</li> <li>auto — 将端口速度设置为已安装介质的速度。</li> </ul>                                                                             |
| <b>默认</b>     | 自动                                                                                                                                                                                                                                        |
| <b>命令模式</b>   | INTERFACE                                                                                                                                                                                                                                 |
| <b>使用情况信息</b> | <p>speed 命令仅在管理和光纤通道接口上受支持。此命令在以太网接口上不受支持。</p> <ul style="list-style-type: none"> <li>要配置 FC 接口上突发存储流量的超额订阅，请使用 speed 命令。超额订阅使端口可以更快地运行，但可能会导致流量丢失。4x16GFC 模式下的 QSFP28 分解接口支持 32GFC 超额订阅。</li> <li>此命令的 no 版本将端口速度重置为默认值 auto。</li> </ul> |

|           |                                               |
|-----------|-----------------------------------------------|
| <b>示例</b> | <pre> OS10(conf-if-fc-1/1/2)# speed 16 </pre> |
|-----------|-----------------------------------------------|

**支持的版本** 10.3.1E or later



## speed (管理)

配置管理接口的传输速度。

|        |                                                                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>speed {10   100   1000   auto}</code>                                                                                                                                                                                   |
| 参数     | <p>将管理端口速度设置为：</p> <ul style="list-style-type: none"><li>• 10 — 10M</li><li>• 100 — 100M</li><li>• 1000 — 1000M</li><li>• auto — 将端口设置为与连接的设备自动协商速度。</li></ul>                                                                |
| 默认     | 自动                                                                                                                                                                                                                            |
| 命令模式   | INTERFACE                                                                                                                                                                                                                     |
| 使用情况信息 | <p><code>speed</code> 命令仅在管理和光纤通道接口上受支持。此命令在以太网接口上不受支持。</p> <ul style="list-style-type: none"><li>• 手动配置管理端口速度时，匹配远程设备的速度。Dell EMC 强烈建议使用管理端口的自动协商。</li><li>• 此命令的 <code>no</code> 版本将端口速度重置为默认值 <code>auto</code>。</li></ul> |
| 示例     | <pre>OS10(config-if-ma-1/1/1)# speed auto</pre>                                                                                                                                                                               |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                              |

## switch-port-profile

在交换机上配置端口配置文件。端口配置文件确定可用的前面板端口和分解模式。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>switch-port-profile node/unit profile</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 参数     | <ul style="list-style-type: none"><li>• <code>node/unit</code> — 输入交换机信息。对于独立交换机，输入 1/1。</li><li>• <code>profile</code> — 输入特定于平台的配置文件的名称。</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 默认     | <code>profile-1</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 使用情况信息 | <ul style="list-style-type: none"><li>• S4148-ON 系列端口配置文件：<ul style="list-style-type: none"><li>◦ <code>profile-1</code> — SFP+ 10G 端口 (1-24 和 31-54) 和 QSFP28 100G 端口 (25-26 和 29-30) 已启用。<br/>QSFP28 端口支持 100GE 和 4x10G、4x25G 和 2x50G 分解。</li><li>◦ <code>profile-2</code> — 在 40G 模式下 SFP+ 10G 端口 (1-24 和 31-50)、QSFP+ 40G 端口 (27-28) 和 QSFP28 端口 (25-26 和 29-30) 已启用。<br/>QSFP+ 和 QSFP28 端口支持 40GE 和 4x10G 分解。</li><li>◦ <code>profile-3</code> — SFP+ 10G 端口 (5-24 和 31-50)、QSFP+ 40G 端口 (27-28) 和具有 40G 和 100G 功能的 QSFP28 端口 (25-26 和 29-30) 已启用。<br/>QSFP+ 端口支持 40GE 和 4x10G 分解。QSFP28 端口通过 QSFP28 接收器支持 100GE 和 4x25G 分解，并且通过 QSFP+ 接收器支持 40GE 和 4x10G 分解。</li><li>◦ <code>profile-4</code> — SFP+ 10G 端口 (5-24 和 31-50)、QSFP+ 40G 端口 (27-28) 和具有 40G 和 100G 功能的 QSFP28 端口 (25-26 和 29-30) 已启用。<br/>QSFP+ 端口支持 40GE 和 4x10G 分解。QSFP28 端口通过 QSFP28 接收器支持 100GE 和 2x50G 分解，并且通过 QSFP+ 接收器支持 40GE 和 4x10G 分解。</li><li>◦ <code>profile-5</code> — SFP+ 10G 端口 (1-24 和 31-54)、QSFP+ 40G 端口 (27-28)、具有 40G 功能的 QSFP28 端口 (26 和 30)，以及具有 40G 和 100G 功能的 QSFP28 端口 (25 和 29) 已启用。<br/>QSFP+ 端口支持 40GE 和 4x10G 分解。QSFP28 端口 26 和 30 通过 QSFP+ 收发器支持 40GE 和 4x10G 分解。QSFP28 端口 25 和 29 通过 QSFP28 接收器支持 100GE 和 4x25G 分解，并且通过 QSFP+ 接收器支持 40GE 和 4x10G 分解。</li></ul></li></ul> |

- profile-6 — SFP+ 10G 端口 (1-24 和 31-54)、QSFP+ 40G 端口 (27-28)、具有 40G 功能的 QSFP28 端口 (26 和 30)，以及具有 40G 和 100G 功能的 QSFP28 端口 (25 和 29) 已启用。  
QSFP+ 端口支持 40GE 和 4x10G 分解。QSFP28 端口 26 和 30 通过 QSFP+ 收发器支持 40GE 和 4x10G 分解。QSFP28 端口 25 和 29 通过 QSFP28 接收器支持 100GE 和 2x50G 分解，并且通过 QSFP+ 接收器支持 40GE 和 4x10G 分解。
- S4148U-ON 端口配置文件：
  - profile-1 — SFP+ 统一端口 (1-24)、QSFP28 统一端口 (25-26 和 29-30)、QSFP+ 以太网端口 (27-28) 和 SFP+ 以太网端口 (31-54) 已启用。
    - 默认情况下，SFP+ 统一端口组在 FC 模式和 2x16GFC 分解 (端口 1 和 3) 下运行，并且支持 4x8GFC。SFP+ 统一端口支持以太网 10GE 模式。
    - 默认情况下，QSFP28 统一端口 25 和 29 在以太网 100GE 模式下运行，并且支持 40GE 以及 QSFP+ 收发器和 4x10G 分解。QSFP28 端口 25 和 29 在 FC 模式下支持 1x32GFC、2x16GFC 和 4x8GFC。
    - 默认情况下，QSFP28 统一端口 26 和 30 在以太网 40GE 模式下运行并且支持 4x10G 分解。QSFP28 端口 26 和 30 在 FC 模式下支持 1x32GFC、2x16GFC 和 4x8GFC。
    - 默认情况下，QSFP+ 以太网端口以 40GE 运行，并且支持 4x10G 分解。
    - SFP+ 以太网端口以 10GE 运行。
  - profile-2 — SFP+ 统一端口 (1-24)、QSFP28 统一端口 (25-26 和 29-30)、QSFP+ 以太网端口 (27-28) 和 SFP+ 以太网端口 (31-54) 已启用。
    - 默认情况下，SFP+ 统一端口在以太网 10GE 模式下运行。SFP+ 统一端口组在 FC 模式下支持 4x8GFC 和 2x16GFC 分解 (端口 1 和 3)。
    - 默认情况下，QSFP28 统一端口 25 和 29 在以太网 100GE 模式下运行，并且支持 40GE 以及 QSFP+ 收发器和 4x10G 分解。QSFP28 端口 25 和 29 在 FC 模式下支持 1x32GFC、2x16GFC 和 4x8GFC。
    - 默认情况下，QSFP28 统一端口 26 和 30 在以太网 40GE 模式下运行并且支持 4x10G 分解。QSFP28 端口 26 和 30 在 FC 模式下支持 1x32GFC、2x16GFC 和 4x8GFC。
    - 默认情况下，QSFP+ 以太网端口以 40GE 运行，并且支持 4x10G 分解。
    - SFP+ 以太网端口以 10GE 运行。
  - profile-3 — SFP+ 统一端口 (1-24)、QSFP28 端口统一端口 (25-26 和 29-30) 以及 SFP+ 以太网端口 (31-54) 已启用。QSFP+ 以太网端口 (27-28) 不可用。
    - 默认情况下，SFP+ 统一端口在以太网 10GE 模式下运行。SFP+ 统一端口组在 FC 模式下支持 4x8GFC 和 2x16GFC 分解 (端口 1 和 3)。
    - 默认情况下，QSFP28 统一端口在以太网 100GE 模式下运行并且支持 4x25G 和 4x10G 分解。QSFP28 端口在 FC 模式下支持 2x16GFC 和 4x16GFC 分解。
    - SFP+ 以太网端口以 10GE 运行。
  - profile-4 — SFP+ 统一端口 (1-24)、QSFP28 端口统一端口 (25-26 和 29-30) 以及 SFP+ 以太网端口 (31-54) 已启用。QSFP+ 以太网端口 (27-28) 不可用。
    - 默认情况下，SFP+ 统一端口在以太网 10GE 模式下运行。SFP+ 统一端口在 FC 模式下支持 4x8FC。
    - 默认情况下，QSFP28 统一端口在以太网 100GE 模式下运行并且支持 2x50G、4x25G 和 4x10G 分解。QSFP28 端口在 FC 模式下支持 4x16GFC 分解。
    - SFP+ 以太网端口以 10GE 运行。

## 使用情况信息

- 在 2x16GFC 模式下设置端口组将激活奇数接口 1 和 3。在 1x32GFC 模式下的端口组仅激活接口 1。
- 要显示交换机上的当前端口配置文件，请使用 `show switch-port-profile` 命令。
- 要更改交换机上的端口配置文件，请将 `switch-port-profile` 命令与所需的配置文件一起使用，并将其保存到启动配置中，然后使用 `reload` 命令应用更改。交换机将重新启动并显示新的端口配置。该命令的 `no` 版本将重置为默认配置文件。当交换机重新加载新的端口配置文件时，除了交换机端口配置文件和以下配置的设置，启动配置将重置为系统默认值：
  - 管理接口 1/1/1 配置
  - 管理 IPv4/IPv6 静态路由
  - 系统主机名称
  - 统一转发表 (UFT) 模式
  - ECMP 最大路径

您必须在应用新的端口配置文件后在交换机上手动重新配置其他设置并使用 `reload` 命令应用更改。

## 示例

```
OS10(config)# switch-port-profile 1/1 profile-1
Warning: Switch port profile will be applied only after a save and
reload. All management port
```

```
configurations will be retained but all other configurations will be
wiped out after the reload.
OS10(config)# do write memory
OS10(config)# do reload
```

**支持的版本** 10.3.0E or later

## switchport access vlan

在 L2 访问或中继模式中为端口分配访问 VLAN 成员身份。

**语法** `switchport access vlan vlan-id`

**参数** `vlan vlan-id` — 输入 VLAN ID 号，从 1 到 4093。

**默认** VLAN 1

**命令模式** INTERFACE

**使用情况信息** 此命令可为未标记流量启用 L2 切换，并将端口接口分配给默认 VLAN1。使用此命令可更改用于传送未标记流量的访问 VLAN 的分配。您必须先创建 VLAN，然后才能为其分配访问接口。此命令的 `no` 版本会将 L2 访问或中继端口上的访问 VLAN 成员身份重置为 VLAN 1。

**示例**

```
OS10(conf-if-eth1/1/3)# switchport mode access
OS10(conf-if-eth1/1/3)# switchport access vlan 100
```

**支持的版本** 10.2.0E or later

## switchport mode

将接口置于 L2 访问或中继模式。

**语法** `switchport mode {access | trunk}`

**参数**

- `access` — 启用单个 VLAN 上的未标记帧的 L2 交换。
- `trunk` — 通过 `switchport trunk allowed vlan` 命令启用访问 VLAN 上未标记帧以及指定的 VLAN 上的标记框架的 L2 交换。

**默认** `access`

**命令模式** INTERFACE

**使用情况信息**

- 如果为某个接口分配 IP 地址，则不能使用此命令启用 L2 交换 — 必须先移除该 IP 地址。
- `access` 参数会自动将接口添加到默认 VLAN1 以传输未标记的流量。使用 `switchport access vlan` 命令可更改 VLAN 分配的访问权限。
- `trunk` 参数可配置接口以传输标记的 VLAN 流量。您必须使用 `switchport trunk allowed vlan` 命令手动配置中继端口 VLAN 成员身份。
- 在配置 L3 模式接口时，使用 `no switchport` 命令移除所有 L2 配置。
- 使用 `no switchport mode` 命令可将接口上的中继端口恢复为 VLAN1 上的 L2 访问模式。

**示例**

```
OS10(conf-if-eth1/1/7)# switchport mode access
```

**支持的版本** 10.2.0E or later

## switchport trunk allowed vlan

配置 L2 中继接口可以携带的已标记 VLAN 流量。L2 中继端口没有已标记 VLAN 的成员身份，并且不会传输已标记流量。

**语法** `switchport trunk allowed vlan vlan-id-list`

**参数** `vlan-id-list` — 输入 L2 中继端口可以携带已标记流量的 VLAN 编号。支持逗号分隔和连字符 VLAN 数字范围。

|        |                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | 无                                                                                                                                                  |
| 命令模式   | INTERFACE                                                                                                                                          |
| 使用情况信息 | 使用此命令的 <code>no</code> 版本可以移除配置。                                                                                                                   |
| 示例     | <pre>OS10(config-if-eth1/1/2)# switchport trunk allowed vlan 1000</pre> <pre>OS10(config-if-eth1/1/2)# no switchport trunk allowed vlan 1000</pre> |
| 支持的版本  | 10.2.0E or later                                                                                                                                   |

## unit-provision

调配在全交换模式下连接到 MX9116n 接口交换引擎的结构扩展器的设备 ID。

|        |                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>unit-provision node/unit-id provision_name</code>                                                                                                                                                                                                                                                                                          |
| 语法     | <code>unit-provision node/unit-id provision_name</code>                                                                                                                                                                                                                                                                                          |
| 参数     | <ul style="list-style-type: none"> <li><code>node/unit-id</code> — 为 <code>node</code> 输入 1 以及 <code>show unit-provision</code> 输出中显示的未分配设备 ID。</li> <li><code>provision_name</code> — 输入在 <code>show discovered-expanders</code> 输出中显示的结构扩展器的服务编号。</li> </ul>                                                                                   |
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                    |
| 使用情况信息 | <ul style="list-style-type: none"> <li>要验证在结构引擎上当前配置的模式，请使用 <code>show operating mode</code> 命令。如果结构引擎处于全交换模式，则必须使用 <code>unit-provision</code> 命令手动调配结构扩展器。此命令可为服务编号或调配名称分配设备 ID。要传输服务器流量，您必须使用 <code>interface ethernet node/virtual-slot/port</code> 命令将设备 ID 输入为虚拟插槽编号，以配置结构扩展器上的虚拟端口。</li> <li>命令的 <code>no</code> 版本将移除结构扩展器调配。</li> </ul> |
| 示例     | <pre>OS10(config)# unit-provision 1/78 403RPK2</pre>                                                                                                                                                                                                                                                                                             |
| 支持的版本  | 10.4.0E(R3S) or later                                                                                                                                                                                                                                                                                                                            |

## wavelength

为可调的 10 GB SFP+ 光学收发器配置波长。

|        |                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>wavelength wavelength-value</code>                                                                                  |
| 参数     | <code>wavelength-value</code> — 输入一个值以为 SPF+ 光学器件设置波长。范围从 1528.38 到 1568.77。                                              |
| 默认     | 无。                                                                                                                        |
| 命令模式   | INTERFACE CONFIGURATION                                                                                                   |
| 使用情况信息 | 要指定波长值，必须确切输入六位数字 — 在小数点前面四位，在小数点后面两位。值必须符合以下格式：ABCD.EF，例如，1545.23。任何不符合此格式的数字都会被拒绝，包括完整的数字，如 1568。但是，接受以下类型的值：1568.00。   |
| 示例     | <pre>OS10# configure terminal OS10(config)# interface ethernet 1/1/14 OS10(config-if-eth1/1/14)# wavelength 1530.00</pre> |
| 支持的版本  | 10.4.2E 或更高版本                                                                                                             |

# PowerEdge MX 以太网 I/O 模块

Dell EMC PowerEdge MX7000 支持以下以太网模块：MX9116n 结构交换引擎、MX7116n 结构扩展模块和 MX5108n 以太网交换机。有关详情，请参阅 Dell EMC PowerEdge MX7000 文档。

- MX9116n 结构交换引擎是一种可扩展的 L2/L3 交换机，旨在提供高带宽、低延迟 25GE 网络；例如，在私有云和软件定义的存储 (SDS) 网络中。此高端交换机提供：
  - 十六个 25 GE 面向服务器的端口
  - 12 个双密度 QSFP (QSFP28-DD) 端口，用于连接到结构扩展器或划分为：8x10GE、8x25GE 或 4x50GE 端口，用于连接到架顶式交换机或其他以太网设备；或者 2x40 GE/2x100 GE 端口，用于上行链路，连接到 SAN 存储以及交换机互连。
  - 在 1x100GE、2x50GE、1x40GE、4x25GE 或 4x10GE 模式下运行的两个单密度 QSFP28 端口。
  - 两个 QSFP28 统一端口，在以太网或光纤通道 1x100 GE、1x40 GE、4x25 GE、4x10 GE、2x50 GE 或 4x32GFC、2x32GFC、1x32GFC 或 4x16GFC 模式下运行
- MX7116n 结构扩展器模块作为非受管以太网中继器运行，可使用 QSFP28-DD 连接将服务器连接到结构交换引擎。扩展器模块提供：
  - 十六个 25 GE 面向服务器的端口
  - 两个 QSFP28-DD 端口，用于连接到结构交换引擎
- MX5108n 以太网交换机是基础的以太网交换机，旨在为单个 MX7000 机箱安装提供高性能、低延迟网络。它可以提供 FCoE 传输，但没有本地光纤通道功能，并且提供：
  - 八个 25 GE 面向服务器的端口
  - 两个 100GE QSFP28 上行链路端口
  - 一个 40GE QSFP+ 上行链路端口
  - 四个 10GBASE-T 上行链路端口

有关详情，请参阅：

- [统一端口组](#) 页面上的 211 — 以太网和光纤通道接口
- [双密度 QSFP28 接口](#) 页面上的 275
- [单密度 QSFP28 接口](#)
- [面向服务器的接口](#)
- [虚拟端口](#)

## 运行模式

MX9116n 结构交换引擎和 MX5108n 以太网交换机在全交换和 SmartFabric 模式下运行。SmartFabric 交换机将自动置于 SmartFabric 模式。不属于 SmartFabric 的交换机将自动置于全交换模式。要验证当前配置的模式，请使用 `show switch-operating-mode` 命令。

```
OS10# show switch-operating-mode
Switch-Operating-Mode : Smart Fabric Mode
```

要更改模式，请使用 OpenManage Enterprise-Modular (OME-Modular) 用户界面。您不能使用 OS10 CLI 更改模式。有关详情，请参阅 *Dell EMC OpenManage Enterprise - Modular User's Guide — Ethernet IO Modules chapter* (Dell EMC OpenManage Enterprise - Modular 用户指南 — 以太网 IO 模组一章)。

### 全交换模式

默认情况下，PowerEdge MX 以太网交换机在全交换模式下运行。在全交换模式下，所有受支持的 OS10 CLI 命令和硬件支持的功能均可用。

您还可以使用 OpenManage Enterprise-Modular 界面执行某些任务，包括：

- 配置主机名称和 IP 管理协议，例如 SNMP 和 NTP。
- 将端口状态设置为启动或停止。
- 监控系统日志、警报和事件。
- 更新和管理固件。
- 查看物理拓扑。
- 使用电源控制。

SmartFabric 模式

在 SmartFabric 模式下，PowerEdge MX 交换机作为第二层 I/O 聚合设备运行。OpenManage Enterprise - Modular 界面支持大多数交换机配置设置。使用 SmartFabric 模式配置您的交换机。

SmartFabric 模式支持所有 OS10 show 命令和以下 CLI 配置命令子集：其他 CLI 配置命令不可用。

- clock — 配置时钟参数。
- end — 退出到 EXEC 模式。
- exit — 退出当前模式
- help — 显示可用命令。
- hostname — 设置系统主机名称。
- interface — 配置管理接口、VLAN 接口或一系列接口。
- ip name-server — 配置名称服务器的 IP 地址；最多支持三个名称服务器。
- logging — 配置系统日志记录。
- management route — 配置 IPv4 或 IPv6 管理路由。
- no — 在配置模式下删除或禁用命令。
- ntp — 配置网络时间协议。
- snmp-server — 配置 SNMP 服务器。
- spanning-tree
  - disable — 全局禁用生成树。
  - mac-flush-timer — 设置用于刷新 MAC 地址条目的时间。
  - mode — 启用生成树模式，如 RSTP 或 MST。
  - mst — 配置多个生成树 (MST) 模式。
  - rstp — 配置快速生成树协议 (RSTP) 模式。
  - vlan — 在 VLAN 范围上配置生成树。
- username — 创建或修改用户凭据。
- SupportAssist — 配置 SupportAssist 相关设置。
- Security — 配置与网络安全对应的功能。
- Fibre Channel — 配置与光纤通道接口对应的功能。

表. 27: 操作模式之间的差异

| 全交换模式                                                               | SmartFabric 模式                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 您保存的所有配置更改都将在您重新加载交换机后保留。                                           | 只有使用这些 OS10 管理命令（在两种模式中支持）进行的配置更改才会保存和保留。所有其他 CLI 配置命令均已禁用。 <div>clock<br/>hostname<br/>ip name-server<br/>logging<br/>management route<br/>ntp<br/>snmp-server<br/>spanning-tree<br/>username</div> OpenManage Enterprise - Modular 控制台可以管理数据平面配置。 |
| 默认情况下，所有交换机接口都分配给 VLAN 1，并且位于同一 L2 桥域中。                             | 尽管前面板端口接口默认情况下在 L2 模式下运行，但 L2 桥接处于禁用状态。                                                                                                                                                                                                             |
| 默认情况下，所有配置更改都保存在正在运行的配置中。要显示当前配置，请使用 show running-configuration 命令。 | 使用功能特定的 show 命令（如 show interface 和 show vlan），而不是 show running-configuration，来验证配置更改。                                                                                                                                                               |

更改操作模式

要在全交换和 SmartFabric 模式之间切换 MX9116n 结构交换引擎或 MX5108n 以太网交换机，请使用 OpenManage Enterprise-Modular 接口创建新结构。

全交换到 SmartFabric 模式

除受支持的配置命令子集以外，所有已删除的全交换 CLI 配置更改都将被删除，但您也可以输入并保存在 SmartFabric 模式下（请参阅[操作模式](#)）。

SmartFabric 到全交换模式

当您更改为全交换模式时，将仅保留您使用所保存的两种模式中支持的配置命令子集进行的配置更改。

此外，您对端口接口所作的更改将被删除，但管理状态（关机/无关机）、MTU、速度和自动协商模式除外。当 IOM 移至全交换模式时，将重新应用这些更改。

限制

- VLAN 4001 至 4020 将保留用于内部交换机通信，不能分配给接口。
- 在 SmartFabric 模式下，虽然您可以使用 CLI 创建 VLAN 1 至 4000 和 4021 至 4094，但不能为其分配接口。因此，请勿使用 CLI 在 SmartFabric 模式下创建 VLAN。
- 在 MX7116n 结构扩展器上，两个 QSFP28-DD 上行链路接口仅在以太网模式下运行。使用结构扩展器上最左侧的 QSFP28-DD 端口 1 连接到具有双端口网络接口卡 (NIC) 的服务器。请勿使用最右侧的 QSFP28-DD 端口 2；保留以供将来用于连接到具有四端口 NIC 的服务器。

I/O 模块上的端口组

端口组是一个逻辑端口，包含单个或多个硬件端口，并提供单个线缆接口。在 PowerEdge MX IO 模块上，只有 MX9116n 结构交换引擎支持端口组：

- [统一端口组](#)
- [双密度 QSFP 接口](#)
- [单密度 QSFP 接口](#)

MX7116n 结构扩展器模块和 MX5108n 以太网交换机不支持端口组。

双密度 QSFP28 接口

在 MX9116n 结构交换引擎模块上，在 PORT-GROUP 模式下配置双密度 QSFP28 端口（QSFP28 端口-DD）端口。QSFP28-DD 端口组包含两个以太网 100G 端口。这些端口不能用作单个 200GE 端口。使用 QSFP28-DD 端口：

- 连接到结构扩展器以扩展结构。
- 连接到以太网机架式服务器或存储设备。
- 连接到另一个交换机或路由器。

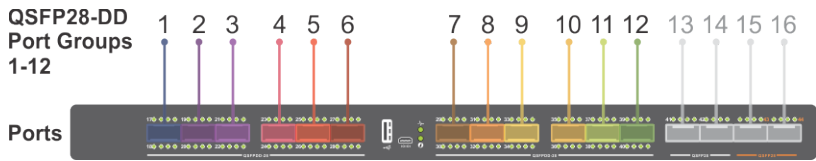


图 5: MX9116n 结构交换引擎 — QSFP28-DD 端口组

QSFP28-DD 端口组为 1 到 12，并且包含物理端口 1/1/17 到 1/1/40。面向服务器的端口是 1/1/1 到 1/1/16。

QSFP28-DD 以太网接口支持结构扩展器模式 (FEM) 和本机以太网模式。

- 在 FEM 模式下，8x25GE 接口仅使用受支持的线缆连接到连接的结构扩展器。
- 在本机以太网模式下，接口连接到上游交换机、机架式服务器或其他以太网设备。

默认情况下，QSFP28-DD 端口组 1 到 9 在启用了 8x25GE 分解接口的 FEM 模式下配置。QSFP28-DD 端口组 10 到 12 在启用了 2x100GE 分解接口的本地模式下配置。

- 有关如何配置单密度 QSFP28 以太网端口组 13 和 14 的信息，请参阅[单密度 QSFP28 接口](#)。
- 有关如何配置统一端口组 15 和 16 以在以太网或光纤通道模式下运行的信息，请参阅[统一端口组](#) 页面上的 211。
- 如果 MX9116n 模块处于 SmartFabric 模式，则使用 OpenManage Enterprise - Modular 接口在 QSFP28-DD 端口上配置分解接口和速度。



1. 要配置 QSFP28-DD 端口接口，请从 CONFIGURATION 模式进入 PORT-GROUP 模式。为 *node/slot* 输入 1/1。QSFP28-DD 端口组范围为 1 到 12。

```
port-group node/slot/port-group
```

2. (可选) 要验证当前的 QSFP28-DD 端口组配置，请输入 `show port-group` 命令。

```
OS10# show port-group
Port-group Mode Ports FEM
port-group1/1/1 Eth 25g-8x 17 18 FEM
port-group1/1/2 Eth 25g-8x 19 20 FEM
port-group1/1/3 Eth 25g-8x 21 22 FEM
port-group1/1/4 Eth 25g-8x 23 24 FEM
port-group1/1/5 Eth 25g-8x 25 26 FEM
port-group1/1/6 Eth 25g-8x 27 28 FEM
port-group1/1/7 Eth 25g-8x 29 30 FEM
port-group1/1/8 Eth 25g-8x 31 32 FEM
port-group1/1/9 Eth 25g-8x 33 34 FEM
port-group1/1/10 Eth 100g-2x 35 36 -
port-group1/1/11 Eth 100g-2x 37 38 -
port-group1/1/12 Eth 100g-2x 39 40 -
...
```

要将 QSFP28-DD 端口组重置为其默认设置，请在 PORT-GROUP 模式下输入 `no mode` 命令。此命令可将 QSFP-DD 端口组 1 到 9 设置为 8x25GE FEM 模式，并将 QSFP DD 端口组 10 到 12 设置为 2x100GE 模式。

```
no mode
```

3. 要激活 QSFP28-DD 接口进行以太网操作，请在 PORT-GROUP 模式下输入 `mode Eth` 命令。

```
mode Eth {100g-2x | 50g-4x | 40g-2x | 25g-8x fabric-expander-mode | 25g-8x | 10g-8x}
```

- 100g-2x — 将 QSFP28-DD 端口拆分为两个 100GE 接口。
- 50g-4x — 将 QSFP28-DD 端口拆分为四个 50GE 接口。
- 40g-2x — 将 QSFP28-DD 端口拆分为两个 40GE 接口。
- 25g-8x fabric-expander-mode — 将 QSFP28-DD 端口拆分为八个 25GE 接口，以仅连接到 MX7116n 结构扩展器。
- 25g-8x — 将 QSFP28-DD 端口拆分为八个 25GE 接口。
- 10g-8x — 将 QSFP28-DD 端口拆分为八个 10GE 接口。

4. 返回 CONFIGURATION 模式。

```
exit
```

5. 进入以太网接口模式以配置其他设置。输入单个接口、连字符分隔的范围或用逗号分隔的多个接口。

```
interface ethernet node/slot/port[:subport]
```

要显示 QSFP28-DD 端口组中的以太网 100GE 端口配置，请输入 `show port-group` 命令。要显示以太网 25GE 子端口配置，请输入 `show interfaces status` 命令。

## 配置 QSFP28-DD 接口

```
OS10(config)# port-group 1/1/7
OS10(conf-pg-1/1/7)# mode Eth 25g-8x
OS10(conf-pg-1/1/7)# exit
OS10(config)# interface ethernet 1/1/29:4
OS10(conf-if-eth-1/1/29:4)#
```

## 查看 QSFP28-DD 接口

```
OS10(config)# interface ethernet 1/1/29:4
OS10(conf-if-eth1/1/29:4)# show configuration
!
interface ethernet1/1/29:4
no shutdown
```



查看 QSFP28-DD 端口组和默认模式

```
OS10# show port-group
Port-group Mode Ports FEM
port-group1/1/1 Eth 25g-8x 17 18 FEM
port-group1/1/2 Eth 25g-8x 19 20 FEM
port-group1/1/3 Eth 25g-8x 21 22 FEM
port-group1/1/4 Eth 25g-8x 23 24 FEM
port-group1/1/5 Eth 25g-8x 25 26 FEM
port-group1/1/6 Eth 25g-8x 27 28 FEM
port-group1/1/7 Eth 25g-8x 29 30 FEM
port-group1/1/8 Eth 25g-8x 31 32 FEM
port-group1/1/9 Eth 25g-8x 33 34 FEM
port-group1/1/10 Eth 100g-2x 35 36 -
port-group1/1/11 Eth 100g-2x 37 38 -
port-group1/1/12 Eth 100g-2x 39 40 -
...
```

查看 QSFP28-DD 默认 8x25G 分解接口

```
OS10# show interface status

Port Description Status Speed Duplex Mode Vlan Tagged-Vlans

...
Eth 1/1/17:1 down 0 auto A 1 -
Eth 1/1/17:2 down 0 auto A 1 -
Eth 1/1/17:3 down 0 auto A 1 -
Eth 1/1/17:4 down 0 auto A 1 -
Eth 1/1/18:1 down 0 auto A 1 -
Eth 1/1/18:2 down 0 auto A 1 -
Eth 1/1/18:3 down 0 auto A 1 -
Eth 1/1/18:4 down 0 auto A 1 -
Eth 1/1/19:1 down 0 auto A 1 -
Eth 1/1/19:2 down 0 auto A 1 -
Eth 1/1/19:3 down 0 auto A 1 -
Eth 1/1/19:4 down 0 auto A 1 -
Eth 1/1/20:1 down 0 auto A 1 -
Eth 1/1/20:2 down 0 auto A 1 -
Eth 1/1/20:3 down 0 auto A 1 -
Eth 1/1/20:4 down 0 auto A 1 -
Eth 1/1/21:1 down 0 auto A 1 -
Eth 1/1/21:2 down 0 auto A 1 -
Eth 1/1/21:3 down 0 auto A 1 -
Eth 1/1/21:4 down 0 auto A 1 -
Eth 1/1/22:1 down 0 auto A 1 -
Eth 1/1/22:2 down 0 auto A 1 -
Eth 1/1/22:3 down 0 auto A 1 -
Eth 1/1/22:4 down 0 auto A 1 -
...
```

# 虚拟端口

虚拟端口是连接到下游服务器且不具有交换机上物理硬件位置的逻辑 OS10 端口。当 MX9116n 结构交换引擎板载 MX7116n 结构扩展模块时，将创建虚拟端口。板载过程包含查找和配置。

结构扩展器查找

结构扩展器充当具有十六个面向服务器的 25GE 端口和两个 QSFP28-DD 上行链路端口的非托管以太网中继器。当符合以下条件时，在全交换模式下连接的结构交换引擎会自动发现结构扩展器：

- 结构扩展器通过在每个设备上的 QSFP28-DD 端口之间连接线缆，连接到结构引擎。
- 在结构引擎上，连接到结构扩展器的 QSFP28-DD 端口组处于 25g-8x fabric-expander-mode 模式下。
- 在包含结构扩展器的 MX7000 机箱中至少安装了一个计算底座。

**注：**如果通过结构扩展器连接到引擎上的其他 QSFP28-DD 端口来移除结构扩展器，将保持虚拟端口上的所有配置。映射到虚拟端口的 QSFP28-DD 分解接口会更改。

**注:** 如果 MX7000 机箱中的服务器具有双端口 NIC，则将结构引擎连接到结构扩展器上的 QSFP28-DD 端口 1。请勿连接到 QSFP28-DD 端口 2。

要验证自动查找到的结构扩展器，请输入 `show discovered-expanders` 命令。

```
OS10# show discovered-expanders
Service-tag Model Type Chassis-service-tag Chassis-slot Port-group Virtual-Slot-
Id

403RPK2 MX7116n Fabric 1 SKY003Q A2 port-
group1/1/2
Expander Module
```

结构扩展器虚拟插槽配置

如果结构交换引擎处于 SmartFabric 模式，则会自动配置连接的结构扩展器：

- 结构扩充器和虚拟插槽 ID 的虚拟端口将创建并映射到结构引擎上 FEM 模式下的 8x25GE 分解接口。
- 系统会自动发现设备 ID。
- 服务器流量通过结构扩充器上的 QSFP28-DD 上行链路传输到结构引擎。

如果结构交换引擎处于全交换模式，您可以使用图形用户界面通过 CLI 以 SmartFabric 模式执行相同的交换机配置，但必须手动配置结构扩展器的设备 ID。设备 ID 也称为虚拟插槽 ID。

1. 找到 `show discovered-expanders` 输出中结构扩展器的服务编号。
2. 显示在 EXEC 模式下为结构扩展器保留的未分配设备 ID。调配的结构扩展器的服务编号显示在 `show unit-provision` 输出的 Provision Name 列中。

```
OS10# show unit-provision

Node ID | Unit ID | Provision Name | Discovered Name | State |
-----+-----+-----+-----+-----+
1 | 71 | | | |
1 | 72 | | | |
1 | 73 | | | |
1 | 74 | | | |
1 | 75 | | | |
1 | 76 | | | |
1 | 77 | | | |
1 | 78 | SP0012 | SP0012 | up |
1 | 79 | | | |
1 | 80 | | | |
1 | 81 | | | |
1 | 82 | | | |
```

3. 在 CONFIGURATION 模式下配置结构扩展器的服务编号（调配名称）的设备 ID。

```
OS10(config)# unit-provision node/unit-id provision_name
```

- `node/unit-id` — 为 `node` 输入 1 以及 `show unit-provision` 输出中的未分配设备 ID。
- `provision_name` — 从 `show discovered-expanders` 输出中的 Chassis-service-tag 字段输入结构扩展器的服务编号。

4. 在 EXEC 模式下验证发现的结构扩展器及其虚拟插槽 ID。

```
OS10# show discovered-expanders

Service-tag Model Type Chassis-service-tag Chassis-slot Port-group Virtual-
Slot-Id

403RPK2 MX7116n Fabric 1 SKY003Q A2 port-group1/1/2
71
Expander Module
```

当结构交换引擎查找结构扩展器时，它将通过将端口组 1 到 9 中的每个 8x25GE FEM 分解接口映射到结构扩展器虚拟端口来创建虚拟端口。

表. 28: 示例: 结构扩展器虚拟端口映射

| 结构扩展器服务编号 | 结构引擎 QSFP28-DD 端口组 | 结构引擎 QSFP28-DD 8x25GE 接口 | 结构扩展器分配的单元 ID (虚拟插槽) | 结构扩展器虚拟端口 |
|-----------|--------------------|--------------------------|----------------------|-----------|
| SKY003Q   | 1/1/1              | 1/1/17:1                 | 71                   | 1/71/1    |
|           |                    | 1/1/17:2                 |                      | 1/71/2    |
|           |                    | 1/1/17:3                 |                      | 1/71/3    |
|           |                    | 1/1/17:4                 |                      | 1/71/4    |
|           |                    | 1/1/18:1                 |                      | 1/71/5    |
|           |                    | 1/1/18:2                 |                      | 1/71/6    |
|           |                    | 1/1/18:3                 |                      | 1/71/7    |
|           |                    | 1/1/18:4                 |                      | 1/71/8    |



注: 在 `show interface status` 输出中, 映射到结构扩展器虚拟端口的结构交换引擎 8x25GE 接口显示为 dormant。

```
OS10# show interface status

Port Description Status Speed Duplex Mode Vlan Tagged-Vlans

...
Eth 1/1/17:1 dormant
Eth 1/1/17:2 dormant
Eth 1/1/17:3 dormant
Eth 1/1/17:4 dormant
Eth 1/1/18:1 dormant
Eth 1/1/18:2 dormant
Eth 1/1/18:3 dormant
Eth 1/1/18:4 dormant
...
```

您还可以使用 `show interface` 命令显示结构引擎物理端口到结构扩展器虚拟端口映射, 以及行的运行状态。

```
OS10# show interface ethernet 1/1/30:3
Ethernet 1/1/30:3 is up, line protocol is dormant
Interface is mapped to ethernet1/77/7
```

5. 验证连接到服务器且处于 CONFIGURATION 模式的结构扩展器上的虚拟端口。在结构扩展器上, 设备 ID 71 至 82 用作虚拟插槽编号 1/71 至 1/82。

```
OS10# show interface status
```

6. 在 CONFIGURATION 模式下配置结构扩展器虚拟端口以传输服务器流量。

```
OS10# interface ethernet node/virtual-slot/port
```

- `node 1` 适用于结构扩展器。
- `virtual-slot` 是分配给结构扩展器的设备 ID 编号, 从 71 到 82。
- `port` 是虚拟端口号 1 至 8。

查看结构扩展器虚拟端口

```
OS10# show interface status
```

| Port       | Description | Status | Speed | Duplex | Mode | Vlan | Tagged-Vlans |
|------------|-------------|--------|-------|--------|------|------|--------------|
| ...        |             |        |       |        |      |      |              |
| Eth 1/71/1 |             | up     | 25G   | auto   | A    | 1    | -            |
| Eth 1/71/2 |             | up     | 25G   | auto   | A    | 1    | -            |
| Eth 1/71/3 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/71/4 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/71/5 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/71/6 |             | up     | 25G   | auto   | A    | 1    | -            |

|            |      |     |      |   |   |   |
|------------|------|-----|------|---|---|---|
| Eth 1/71/7 | down | 0   | auto | A | 1 | - |
| Eth 1/71/8 | down | 0   | auto | A | 1 | - |
| Eth 1/72/1 | up   | 25G | auto | A | 1 | - |
| Eth 1/72/2 | up   | 25G | auto | A | 1 | - |
| Eth 1/72/3 | down | 0   | auto | A | 1 | - |
| Eth 1/72/4 | down | 0   | auto | A | 1 | - |
| Eth 1/72/5 | down | 0   | auto | A | 1 | - |
| Eth 1/72/6 | down | 0   | auto | A | 1 | - |
| Eth 1/72/7 | down | 0   | auto | A | 1 | - |
| Eth 1/72/8 | down | 0   | auto | A | 1 | - |
| Eth 1/73/1 | down | 0   | auto | A | 1 | - |
| Eth 1/73/2 | down | 0   | auto | A | 1 | - |
| Eth 1/73/3 | down | 0   | auto | A | 1 | - |
| Eth 1/73/4 | down | 0   | auto | A | 1 | - |
| Eth 1/73/5 | down | 0   | auto | A | 1 | - |
| Eth 1/73/6 | down | 0   | auto | A | 1 | - |
| Eth 1/73/7 | down | 0   | auto | A | 1 | - |
| Eth 1/73/8 | down | 0   | auto | A | 1 | - |
| ...        |      |     |      |   |   |   |
| Eth 1/81/1 | down | 0   | auto | A | 1 | - |
| Eth 1/81/2 | down | 0   | auto | A | 1 | - |
| Eth 1/81/3 | down | 0   | auto | A | 1 | - |
| Eth 1/81/4 | down | 0   | auto | A | 1 | - |
| Eth 1/81/5 | down | 0   | auto | A | 1 | - |
| Eth 1/81/6 | down | 0   | auto | A | 1 | - |
| Eth 1/81/7 | down | 0   | auto | A | 1 | - |
| Eth 1/81/8 | down | 0   | auto | A | 1 | - |
| Eth 1/82/1 | down | 0   | auto | A | 1 | - |
| Eth 1/82/2 | down | 0   | auto | A | 1 | - |
| Eth 1/82/3 | down | 0   | auto | A | 1 | - |
| Eth 1/82/4 | down | 0   | auto | A | 1 | - |
| Eth 1/82/5 | down | 0   | auto | A | 1 | - |
| Eth 1/82/6 | down | 0   | auto | A | 1 | - |
| Eth 1/82/7 | down | 0   | auto | A | 1 | - |
| Eth 1/82/8 | down | 0   | auto | A | 1 | - |

## 单密度 QSFP28 接口

在 MX9116n 结构交换引擎模块上，QSFP28 端口组包含一个以太网 100G 端口。默认情况下，QSFP28 端口组 13 和 14（物理端口 41 和 42）在 1x100GE 模式下运行。

有关如何将 QSFP28-DD 端口组 1 至 12 配置为在以太网模式下运行的信息，请参阅[双密度 QSFP28 接口](#)。

有关如何将统一端口组 15 和 16 配置为在以太网或光纤通道模式下运行的信息，请参阅[统一端口组](#)。

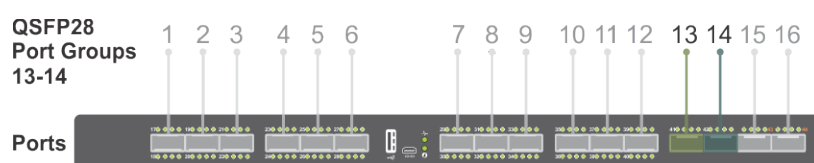


图 6: MX9116n 结构交换引擎 — QSFP28 端口组

- 要配置 QSFP28 端口组接口，请从配置模式输入端口组模式。为 *node/slot* 输入 1/1。QSFP28 端口组范围为 13 至 14。

```
port-group node/slot/port-group
```

- 在 PORT-GROUP 模式下为以太网操作激活 QSFP28 端口组接口。

```
mode Eth {100g-1x | 50g-2x | 40g-1x | 25g-4x | 10g-4x}
```

- 100g-1x — 将端口组重置为 100GE 模式。
- 50g-2x — 将 QSFP28 端口拆分为两个 50GE 接口。
- 40g-1x — 将 QSFP28 端口拆分为一个 40GE 接口。
- 25g-4x — 将 QSFP28 端口拆分为四个 25GE 接口。
- 10g-4x — 将 QSFP28D 端口拆分为四个 10GE 接口。

3. 返回 CONFIGURATION 模式。

```
exit
```

4. 进入以太网接口模式以配置其他设置。输入单个接口、连字符分隔的范围或用逗号分隔的多个接口。

```
interface ethernet node/slot/port[:subport]
```

要显示 QSFP28 端口组中的以太网端口，请输入 show port-group 命令。要显示以太网 25GE 子端口，请输入 show interfaces status 命令。

配置 QSFP28 端口组接口

```
OS10(config)# port-group 1/1/13
OS10(conf-pg-1/1/13)# mode Eth 25g-4x
OS10(conf-pg-1/1/13)# exit
OS10(config)# interface ethernet 1/1/41:4
OS10(conf-if-eth-1/1/41:4)#
```

查看 QSFP28 端口组接口

```
OS10(config)# interface ethernet 1/1/41:4
OS10(conf-if-eth1/1/41:4)# show configuration
!
interface ethernet1/1/41:4
no shutdown
```

查看 QSFP28 端口组和默认模式

```
OS10# show port-group
Port-group Mode Ports FEM
...
port-group1/1/13 Eth 100g-1x 41 -
port-group1/1/14 Eth 100g-1x 42 -
...
```

查看 QSFP28 分解接口

```
OS10# show interface status
```

| Port         | Description | Status | Speed | Duplex | Mode | Vlan | Tagged-Vlans |
|--------------|-------------|--------|-------|--------|------|------|--------------|
| ...          |             |        |       |        |      |      |              |
| Eth 1/1/41:1 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/41:2 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/41:3 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/41:4 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/42:1 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/42:2 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/42:3 |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/42:4 |             | down   | 0     | auto   | A    | 1    | -            |
| ...          |             |        |       |        |      |      |              |

# 面向服务器的接口

在 MX9116n 结构交换引擎和 MX5108n 以太网交换机上，面向服务器的接口位于内部，并在默认情况下处于启用状态。要查看服务器的内部端口连接，请使用 show inventory media 命令。

在输出中，面向服务器的接口将 INTERNAL 显示为其介质。FIXED 端口不使用外部收发器，并且始终显示为 Dell EMC Qualified true。要查看面向服务器的背板端口状态，请使用 show interface status 命令。

 **注：**在 MX9116n 结构交换引擎上，具有双端口 NIC 的服务器可连接到奇数内部以太网接口；例如，1/1/1、1/1/3、1/1/5 等。

查看内部以太网端口服务器连接 — MX9116n 结构交换引擎

```
OS10# show inventory media

```

| System Inventory Media |          |          |               |                    |
|------------------------|----------|----------|---------------|--------------------|
| Node/Slot/Port         | Category | Media    | Serial Number | Dell EMC Qualified |
| 1/1/1                  | FIXED    | INTERNAL |               | true               |
| 1/1/2                  | FIXED    | INTERNAL |               | true               |
| 1/1/3                  | FIXED    | INTERNAL |               | true               |
| 1/1/4                  | FIXED    | INTERNAL |               | true               |
| 1/1/5                  | FIXED    | INTERNAL |               | true               |
| 1/1/6                  | FIXED    | INTERNAL |               | true               |
| 1/1/7                  | FIXED    | INTERNAL |               | true               |
| 1/1/8                  | FIXED    | INTERNAL |               | true               |
| 1/1/9                  | FIXED    | INTERNAL |               | true               |
| 1/1/10                 | FIXED    | INTERNAL |               | true               |
| 1/1/11                 | FIXED    | INTERNAL |               | true               |
| 1/1/12                 | FIXED    | INTERNAL |               | true               |
| 1/1/13                 | FIXED    | INTERNAL |               | true               |
| 1/1/14                 | FIXED    | INTERNAL |               | true               |
| 1/1/15                 | FIXED    | INTERNAL |               | true               |
| 1/1/16                 | FIXED    | INTERNAL |               | true               |
| ...                    |          |          |               |                    |

查看内部以太网端口服务器连接 — MX5108n 以太网交换机

| OS10# show inventory media |          |          |               |                    |
|----------------------------|----------|----------|---------------|--------------------|
| System Inventory Media     |          |          |               |                    |
| Node/Slot/Port             | Category | Media    | Serial Number | Dell EMC Qualified |
| 1/1/1                      | FIXED    | INTERNAL |               | true               |
| 1/1/2                      | FIXED    | INTERNAL |               | true               |
| 1/1/3                      | FIXED    | INTERNAL |               | true               |
| 1/1/4                      | FIXED    | INTERNAL |               | true               |
| 1/1/5                      | FIXED    | INTERNAL |               | true               |
| 1/1/6                      | FIXED    | INTERNAL |               | true               |
| 1/1/7                      | FIXED    | INTERNAL |               | true               |
| 1/1/8                      | FIXED    | INTERNAL |               | true               |
| ...                        |          |          |               |                    |

查看内部以太网端口状态

| OS10# show interface status |             |        |       |        |      |      |              |
|-----------------------------|-------------|--------|-------|--------|------|------|--------------|
| Port                        | Description | Status | Speed | Duplex | Mode | Vlan | Tagged-Vlans |
| Eth 1/1/1                   |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/2                   |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/3                   |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/4                   |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/5                   |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/6                   |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/7                   |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/8                   |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/9                   |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/10                  |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/11                  |             | up     | 25G   |        | A    | 1    | -            |
| Eth 1/1/12                  |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/13                  |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/14                  |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/15                  |             | down   | 0     | auto   | A    | 1    | -            |
| Eth 1/1/16                  |             | down   | 0     | auto   | A    | 1    | -            |
| ...                         |             |        |       |        |      |      |              |

# 更换 SmartFabric 中的 MX 以太网 IO 模块

OS10 使您能够在发生错误时更换属于 SmartFabric 的以太网 I/O 模块 (IOM)。更换机制可用于以下 IOM：

- MX9116n 结构交换引擎 (FSE)
- MX5108n 以太网交换机

有关 MX 模块和结构的信息，请参阅 Dell EMC PowerEdge MX7000 说明文件。有关操作模式和机箱的详细信息，请参阅 Dell EMC OpenManage Enterprise - Modular 说明文件。这些文档位于 Dell EMC Networking 网站，网址：[www.dell.com/support](http://www.dell.com/support)。

## 部署说明

Dell EMC 建议：

- 更换 IOM 必须是机箱部署中的新设备。
  - 注：**新设备意味着之前未在 OME-Modular 多机箱组中部署的 IOM。
- SmartFabric 中的其他 IOM 必须处于正常运行状态。
- 新 IOM 的型号必须与故障 IOM 相同。例如：如果故障 IOM 型号是 MX9116n FSE，您必须使用新的 MX9116n FSE 作为替换 IOM。
- 新 IOM 的 OS10 版本必须与故障 IOM 相同。您可以通过登录 OME 模块化图形用户界面 (GUI) 来检查 OS10 版本。
  - 注：**OS10 出厂安装在 MX9116n FSE 或 MX5108n 以太网交换机中。如果出现故障的 IOM 具有 OS10 升级的版本，则必须将新 IOM 升级到相同版本。要升级 OS10 映像，请参阅[下载 OS10 映像进行升级](#)。

## 更换 SmartFabric 中的 IOM

要更换属于 SmartFabric 的 IOM，请执行以下操作：

1. 以物理方式卸下故障 IOM 并插入新 IOM，请参阅[卸下并更换 IOM](#)。
2. 验证固件版本并配置 IOM 设置，请参阅[验证和配置 IOM 设置](#)。
3. 识别 PowerEdge MX 机箱中连接的主 IOM，请参阅[识别主 IOM](#)。
4. 使用模块替换命令从主 IOM 启动替换工作流，请参阅[启动模块更换工作流](#)。模块更换命令是必须从 Linux shell 执行的 Linux 命令。
5. 将线缆连接至新的 IOM，请参阅[将线缆连接到新的 IOM](#)。

**主和成员 IOM：**单个 MX 机箱支持四个以太网 IOM，其中一个 IOM 是主节点，其余三个是成员。在多机箱环境中，在所有连接到可扩展结构的 IOM 中，一个 IOM 是主节点，剩余的是成员。

## 卸下并更换出现故障的 IOM

1. 识别发生故障的 IOM 以进行更换。
2. 在断开线缆的连接之前，使用端口号标记每根线缆。
3. 卸下出现故障的 IOM。
4. 将新 IOM 插入空插槽。
  - 注：**请勿重新连接线缆。
5. 确认 OME 模块化可识别新 IOM。
  - 注：**要确认新 IOM 在正确的机箱和插槽中列出，请登录 OME 模块化 GUI。

## 验证和配置 IOM 设置

- 验证新 IOM 上的固件版本。您可能需要升级新 IOM 上的固件。要查看挂起的固件升级，请使用 `show image firmware` 命令。有关详细信息，请参阅[安装固件升级](#)。
- 在新的 IOM 上配置主机名称和 IP 管理协议，例如 SNMP 和 NTP。有关详细信息，请参阅[系统管理](#)。
  - 注：**特定于故障 IOM 的 OME-Modular GUI 配置适用于新的 IOM。移除故障 IOM 时，CLI 配置将丢失。使用 OS10 CLI 重新应用新 IOM 中的配置。SmartFabric 服务模式支持所有 OS10 `show` 命令和 CLI 配置命令的子集。有关支持的命令的详细信息，请参阅[操作模式](#)。

# 识别主 IOM

要启动模块更换过程，请确定连接到 SmartFabric 的主 IOM。

要识别 SmartFabric 中的主 IOM，请使用 `show smartfabric cluster member` 命令。有关详细信息，请参阅[显示 SmartFabric 群集成员](#)。从 SmartFabric 中连接的任何 IOM 运行命令。显示的内容会有所不同，具体取决于交换机角色。

如果命令在成员上运行，则系统仅显示主 IOM 的详细信息。系统将显示服务编号和主服务器的 IPv6 地址等信息。如果在主节点中运行命令，系统将显示机箱部署中所有 IOM 的详细信息。使用模块替换命令之前，请使用显示的 IPv6 地址登录主 IOM。有关如何从成员登录到主 IOM 的更多信息，请参阅[从成员登录到主 IOM](#)。

此外，您还可以使用 `show smartfabric cluster` 命令查看主 IOM 的 IPv4 地址。有关详细信息，请参阅[显示 SmartFabric 群集](#)。

要标识主 IOM，请执行以下操作：

- 在 EXEC 模式下使用 `show smartfabric cluster member` 命令查看主 IOM 的详细信息。

```
MX9116N-A1# show smartfabric cluster member
```

如果在主 IOM 上使用 `show smartfabric cluster member` 命令，系统将显示以下输出：

```
MX9116N-A1# show smartfabric cluster member
```

| Service-tag | IP Address                            | Status | Role   | Type    | Chassis-Service-Tag | Chassis-Slot |
|-------------|---------------------------------------|--------|--------|---------|---------------------|--------------|
| HRA0024     | fde1:53ba:e9a0:de14:2204:fff:fe13:143 | ONLINE | MASTER | MX9116n | ARH0006             | B2           |

如果在成员 IOM 上使用 `show smartfabric cluster member` 命令，则系统将显示以下输出：

```
MX9116N-B2# show smartfabric cluster member
```

| Service-tag | IP Address                             | Status | Role   | Type    | Chassis-Service-Tag | Chassis-Slot |
|-------------|----------------------------------------|--------|--------|---------|---------------------|--------------|
| -           |                                        |        |        |         |                     |              |
| HRA0015 B1  | fde1:53ba:e9a0:de14:2204:fff:fe0c:d637 | ONLINE | BACKUP | MX9116n | ARH0004             |              |
| HRA0039 B1  | fde1:53ba:e9a0:de14:2204:fff:fe20:5249 | ONLINE | BACKUP | MX9116n | ARH0010             |              |
| HRA0016 B2  | fde1:53ba:e9a0:de14:2204:fff:fe0c:e637 | ONLINE | BACKUP | MX9116n | ARH0004             |              |
| HRA0035 B1  | fde1:53ba:e9a0:de14:2204:fff:fe21:7fc9 | ONLINE | BACKUP | MX9116n | ARH0009             |              |
| HRA0008 B2  | fde1:53ba:e9a0:de14:2204:fff:fe20:7f49 | ONLINE | BACKUP | MX9116n | ARH0002             |              |
| HRA0023 B1  | fde1:53ba:e9a0:de14:2204:fff:fe0c:f1b7 | ONLINE | BACKUP | MX9116n | ARH0006             |              |
| HRA0031 B1  | fde1:53ba:e9a0:de14:2204:fff:fe16:d553 | ONLINE | BACKUP | MX9116n | ARH0008             |              |
| HRA0036 B2  | fde1:53ba:e9a0:de14:2204:fff:fe20:56c9 | ONLINE | BACKUP | MX9116n | ARH0009             |              |
| HRA0019 B1  | fde1:53ba:e9a0:de14:2204:fff:fe21:1c9  | ONLINE | BACKUP | MX9116n | ARH0005             |              |
| HRA0017 A1  | fde1:53ba:e9a0:de14:2204:fff:fe21:9f49 | ONLINE | BACKUP | MX9116n | ARH0005             |              |
| HRA0032 B2  | fde1:53ba:e9a0:de14:2204:fff:fe17:3bd3 | ONLINE | BACKUP | MX9116n | ARH0008             |              |
| HRA0024     | fde1:53ba:e9a0:de14:2204:fff:fe13:143  | ONLINE | MASTER | MX9116n | ARH0006             | B2           |
| ...         |                                        |        |        |         |                     |              |

## 从成员登录到主 IOM

要使用模块替换命令，请从成员访问主 IOM。

使用主 IOM 的 IPv6 地址登录到主 IOM。登录主 IOM 后，使用模块替换命令启动替换 workflow。



1. 在已连接的 IOM 中从 EXEC 模式登录 Linux shell。

```
OS10# system bash
admin@MX9116N-A2:~$
```

2. 使用 IOM 中显示的 IPv6 地址登录到主 IOM。

```
admin@MX9116N-A1:~$ ssh admin@<ipv6-address>
```

当您从成员 IOM 登录主 IOM 时的输出示例：

```
admin@OS10:~$ ssh admin@fdel:53ba:e9a0:cccc:3417:ebff:fe2c:ca84
Debian GNU/Linux 9

Dell EMC Networking Operating System (OS10)
admin@fdel:53ba:e9a0:cccc:3417:ebff:fe2c:ca84's password:
Linux OS10 4.9.110 #1 SMP Debian 4.9.110-3+deb9u4 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

-* Dell EMC Network Operating System (OS10) *-
-* *-
-* Copyright (c) 1999-2019 by Dell Inc. All Rights Reserved. *-
-* *-

This product is protected by U.S. and international copyright and
intellectual property laws. Dell EMC and the Dell EMC logo are
trademarks of Dell Inc. in the United States and/or other
jurisdictions. All other marks and names mentioned herein may be
trademarks of their respective companies.

%Warning : Default password for admin account should be changed to secure the system
WARNING: Cluster manager is still using default credentials
```

## 启动模块更换工作流

要启动模块更换工作流，请使用主 IOM 中的模块更换 `sfs_node_replace.py` 命令。在模块更换命令中输入服务编号信息作为参数。您可以在 IOM 上的快速服务编号中找到服务编号信息。要查看信息，请拉出系统前面的信息编号。

启动工作流之前，系统会提示输入 admin 凭据。

- 从 Linux 提示符处运行模块更换命令。要显示 MX 以太网输入/输出模块的服务编号，请在 SmartFabric 或全交换模式下使用 `show smartfabric cluster member` 命令。

```
admin@MX9116N-A2:~$ sfs_node_replace.py NewServiceTag oldServiceTag
```

- `NewServiceTag` — 新 IOM 的服务编号
- `OldServiceTag` — 故障 IOM 的服务编号

如果 IOM 不是 SmartFabric 的一部分，则系统会显示以下错误：

```
Enter the Username for the Admin: admin

Password:

No Fabric found for specified nodes. Please recheck and issue this command again.
```

使用主 IOM 中的模块更换命令时的输出示例：

```
admin@MX9116N-A2:~$ sfs_node_replace.py JDB1XC2 68RRNK2

Enter the Username for the Admin: admin

Password:

% Total % Received % Xferd Average Speed Time Time Time Current
 100 142 100 89 100 53 646 384 --:--:-- --:--:-- --:--:-- 649

Node replacement work-flow is initiated, the node JDB1XC2 will reboot into Fabric mode.
```

成功进行身份验证后，系统将启动模块更换工作流，而新 IOM 将重新启动并置于 SmartFabric 服务模式。

## 连接新的 IOM

交换机重新引导至 SmartFabric 服务模式后，请连接所有最初连接至故障 IOM 的线缆。

## 光纤通道

带有光纤通道 (FC) 端口的 OS10 交换机采用以下模式之一运行：直接连接 (F\_Port)、NPIV 代理网关 (NPG) 或 FIP 侦听桥 (FSB)。在 FSB 模式下，您不能使用 FC 端口。

### F\_Port

光纤通道结构端口 (F\_Port) 是将 FC 结构连接到节点的交换机端口。S4148U-ON、MX9116n 和 MX7116n 交换机支持 F\_Port。在 CONFIGURATION 模式下，使用 `feature fc domain-ID domain-ID` 命令可全局启用光纤通道 F\_Port 模式。

```
OS10(config)# feature fc domain-id 100
```

### NPIV 代理网关

节点端口 (N\_Port) 是网络节点上充当主机或存储设备的端口，用于 FC 点对点或 FC 交换结构拓扑。

N\_Port ID 虚拟化 (NPIV) 允许多个 N\_Port ID 共享单个物理 N\_Port。

NPIV 代理网关 (NPG) 提供以太网光纤通道 (FCoE) 到光纤通道 (FC) 桥接，反之亦然。从 OS 10.4.1 开始，NPG 还支持 FC 到 FC 交换。

S4148U-ON 在 NPG 模式下支持 CNA 和 HBA。

MX9116n 和 MX7116n 交换机支持 NPG 模式。

在 CONFIGURATION 模式下使用 `feature fc npg` 命令可全局启用 NPG 模式。

要将端口模式从默认 N\_Port 进行更改，请在 FC 接口上使用 `fc port-mode F` 命令。

**注：**在 NPG 或 F 端口模式下配置的交换机中，OS10 不支持扩展配置文件 VLAN 配置。要在 NPG 或 F 端口模式下使用扩展配置文件配置，请使用 `mode L3` 命令在 vfabric VLAN 上启用基于 CPU 的 VLAN 泛洪。

### FIP 侦听桥

FCoE 在以太网网络上封装 FC 帧。FCoE 初始化协议 (FIP) 可建立与以太网端口的 FC 连接。FSB 实施安全特性以在以太网网络中采用有效的 FCoE 流量。FIP 和 FCoE 提供了以太网上 FC 仿真链路。OS10 交换机的以太网端口在 FSB 下运行。

MX9116n 和 MX5108n 交换机在全交换和 SmartFabric 模式下运行。当交换机处于 SmartFabric 模式时，对于已启用 FCoE 的接口，Dell EMC 建议将未标记的 VLAN 用作 1。

```
OS10(config)# feature fip-snooping
```

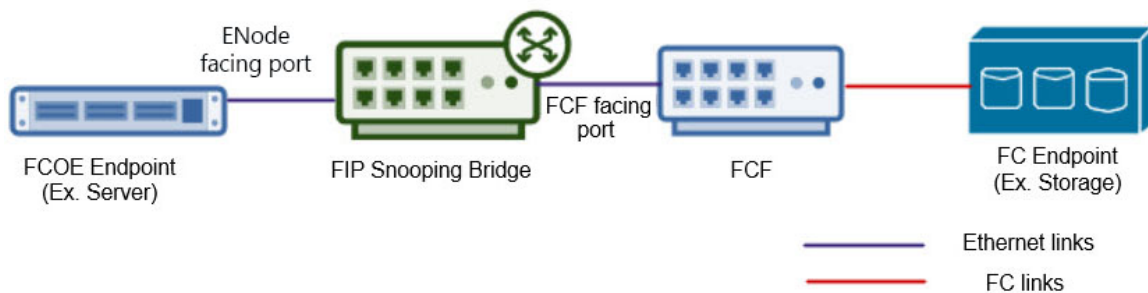
在 FSB 模式下运行的以太网交换机将在已启用 FIP 的 VLAN 上侦听数据包，并发现以下信息：

- 终端节点 (ENodes)
- 光纤通道转发器 (FCF)
- ENodes 与 FCF 之间的连接
- ENodes 与 FCF 之间的会话

**注：**OS10 在 F\_Port 模式下支持多个 ENode。

**注：**在更改 IOM 操作模式之前，从启动配置中移除所有 NPIV 代理网关 (NPG)、F 端口和 vfabric 相关的配置。

通过使用已查找到的信息，交换机可安装提供安全保护和点对点链路模拟的 ACL 条目。



## 以太网光纤通道

以太网光纤通道 (FCoE) 将封装以太网网络上的光纤通道帧。

FCoE 初始化协议 (FIP) 可建立与以太网端口之间的光纤通道连接。

FIP 侦听桥 (FSB) 可实施安全特性，以在以太网网络中采用有效的 FCoE 流量。

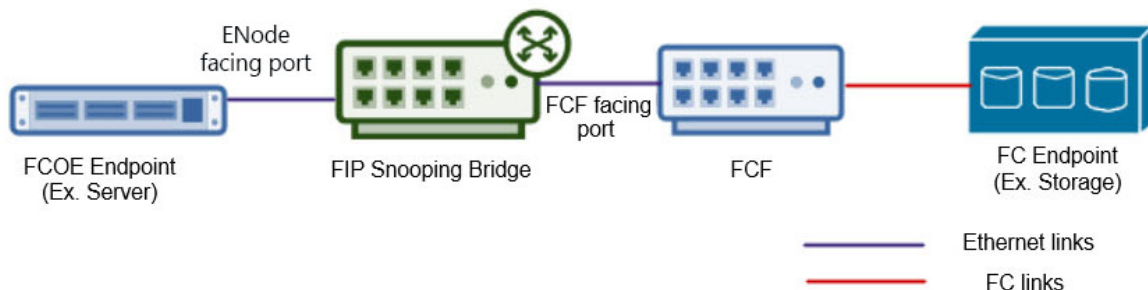
FIP 和 FCoE 提供基于以太网的 FC 仿真链路。

配置为在 FSB 模式下运行的以太网交换机将侦听已启用 FCoE 的 VLAN 上的 FIP 数据包，并发现以下信息：

- 终端节点 (ENodes)
- 光纤通道转发器 (FCF)
- ENodes 与 FCF 之间的连接
- ENodes 与 FCF 之间的会话

**注：** OS10 在 F\_Port 模式下支持多个 ENode。

通过使用已查找到的信息，交换机可安装提供安全保护和点对点链路模拟的 ACL 条目。



## 配置 FIP 侦听

1. 在 CONFIGURATION 模式下使用 `feature fip-snooping` 命令在全局范围内启用 FIP 侦听。
2. 对 VLAN 应用 FIP 侦听之前，请确保 VLAN 已包含使用 FCF 端口模式启用的以太网或 LAG 成员。在 INTERFACE 模式下使用 `fip-snooping port-mode fcf` 命令在以太网或端口通道上启用 FCF 模式。
3. 在 VLAN INTERFACE 模式下使用 `fip-snooping enable` 命令在 VLAN 上启用 FIP 侦听。您可以在最多 12 个 VLAN 上应用 FIP 侦听。
4. 使用 `fip-snooping fc-map fc-map` 命令可将 FC 映射添加到 VLAN。
5. 在 CONFIGURATION 模式下使用 `fcoe max-sessions-per-enodemac max-session-number` 命令可配置允许的最大 ENode 会话数（从 1 到 64）。

**注：** OS10 交换机不支持多跳 FIP 侦听（多跳 FSB）功能；不支持直接到已启用 FIP 侦听的接口（接口路由）上的其他 FIP 侦听接口。

### 配置 FIP 侦听桥

```
OS10(config)# feature fip-snooping
OS10(config)# interface ethernet 1/1/32
```

```

OS10(conf-if-eth1/1/32)# fip-snooping port-mode fcf
OS10(conf-if-eth1/1/32)# exit
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# fip-snooping enable
OS10(conf-if-vl-100)# fip-snooping fc-map 0xEFC64
OS10(conf-if-vl-100)# exit
OS10(config)# fcoe max-sessions-per-enodemac 64

```

## 查看 FIP 侦听配置详细信息

```

OS10# show fcoe statistics interface vlan 100
Number of Vlan Requests :0
Number of Vlan Notifications :0
Number of Multicast Discovery Solicits :2
Number of Unicast Discovery Solicits :0
Number of FLOGI :2
Number of FDISC :16
Number of FLOGO :0
Number of Enode Keep Alive :9021
Number of VN Port Keep Alive :3349
Number of Multicast Discovery Advertisement :4437
Number of Unicast Discovery Advertisement :2
Number of FLOGI Accepts :2
Number of FLOGI Rejects :0
Number of FDISC Accepts :16
Number of FDISC Rejects :0
Number of FLOGO Accepts :0
Number of FLOGO Rejects :0
Number of CVL :0
Number of FCF Discovery Timeouts :0
Number of VN Port Session Timeouts :0
Number of Session failures due to Hardware Config :0

```

```

OS10# show fcoe vlan
* = Default VLAN
VLAN FC-MAP FCFs Enodes Sessions

*1 - - - - -
100 0X0EFC00 1 2 17

```

```

OS10# show fcoe system
Mode: FIP Snooping Bridge
FCOE VLAN List (Operational) : 1, 100
FCFs : 1
Enodes : 2
Sessions : 17

```

```

OS10# show fcoe sessions
Enode MAC Enode Interface FCF MAC FCF interface VLAN FCoE
MAC FC-ID PORT WWPNN PORT WNNN
aa:bb:cc:00:00:00 ethernet1/1/54 aa:bb:cd:00:00:00 port-channel5 100
0e:fc:00:01:00:01 01:00:01 31:00:0e:fc:00:00:00:00 21:00:0e:fc:00:00:00:00
aa:bb:cc:00:00:00 ethernet1/1/54 aa:bb:cd:00:00:00 port-channel5 100
0e:fc:00:01:00:02 01:00:02 31:00:0e:fc:00:00:00:00 21:00:0e:fc:00:00:00:00

```

```

OS10# show fcoe fcf
FCF MAC FCF Interface VLAN FC-MAP FKA_ADV_PERIOD No. of Enodes

54:7f:ee:37:34:40 port-channel5 100 0e:fc:00 4000 2

```

```

OS10# show fcoe enode
Enode MAC Enode Interface VLAN FCFs Sessions

d4:ae:52:1b:e3:cd ethernet1/1/54 100 1 5

```

# 术语

|                 |                                             |
|-----------------|---------------------------------------------|
| <b>ENode</b>    | 终端节点或 FCoE 节点                               |
| <b>FC</b>       | 光纤通道                                        |
| <b>FC ID</b>    | 由 FC 用于识别端点的 3 字节地址                         |
| <b>FC 映射</b>    | 每 VLAN 配置的 3 字节前缀，用于帧 FCoE MAC 地址           |
| <b>FCF</b>      | 光纤通道转发器                                     |
| <b>FCoE</b>     | 以太网光纤通道                                     |
| <b>FCoE MAC</b> | 用于标识 FCoE 会话的唯一 MAC 地址。这是 FC ID 和 FC 映射的组合。 |
| <b>FIP</b>      | FCoE 初始化协议                                  |
| <b>NPG</b>      | NPIV 代理网关                                   |
| <b>NPIV</b>     | N_Port ID 虚拟化                               |

## 虚拟结构

虚拟结构 (vfabric) 将物理结构划分为逻辑结构。每个 vfabric 单独进行管理。结构 ID 可标识每个 vfabric。您只可以在 F\_Port 模式下配置一个 vfabric 并且在 NPG 模式下配置多个 vfabrics。F\_Port 和 NPG 模式相互排斥。

如果您已在 F\_Port 模式下配置了 vfabric，则在 NPG 模式下配置 vfabrics 时，禁用 F\_Port 模式。禁用 F\_Port 模式时，现有的 vfabric 将移除，并且您必须在 NPG 模式下配置新的 vfabric。如果要从 NPG 模式移至 F\_Port 模式，请禁用 NPG 模式，并在 F\_Port 模式下创建新 vfabric。

分区允许您通过将连接到 vfabric 的设备分区为子集来提高网络安全性。分区将限制 vfabric 成员之间的不必要交互。有关详情，请参阅 [光纤通道分区](#) 页面上的 292。

配置 vfabric ID 后，您可以创建一个名称，关联 VLAN 将流量传输到 vfabric，配置 FCoE 参数，配置默认分区并激活分区集。

 **注：** 勿关已用作 vfabric VLAN 的 VLAN。

要在 F\_Port 模式下配置 vfabric：

1. 在 CONFIGURATION 模式下使用 `vfabric fabric-ID` 命令配置 vfabric。交换机将进入 vfabric CONFIGURATION 模式
2. 使用 `vlan vlan-ID` 命令将 VLAN ID 与 vfabric 关联。
3. 使用 `fcoe fcmap fc-map` 命令添加 FC 映射。
4. 使用 `zoneset activate zoneset-name` 命令激活分区集。
5. 当使用 `zone default-zone permit` 命令时，允许在缺少活动分区集配置的情况下访问所有已登录的成员。已登录成员是成功登录到 FC 结构的 FC 节点，由 vfabric 标识。
6. （可选）使用 `name vfabric-name` 命令将名称添加到 vfabric。
7. 在 FC INTERFACE 模式下使用 `vfabric fabric-ID` 命令将 vfabric 应用到 FC 接口。

### F\_Port 模式下 vfabric 配置的示例

```
OS10(config)# vfabric 100
OS10(conf-vfabric-100)# name 100
OS10(conf-vfabric-100)# vlan 1023
OS10(conf-vfabric-100)# fcoe fcmap 0xEFC64
OS10(conf-vfabric-100)# zoneset activate set
OS10(conf-vfabric-100)# zone default-zone permit
OS10(conf-vfabric-100)# exit
OS10(config)# interface fibrechannel 1/1/1
OS10(conf-if-fc1/1/1)# vfabric 100
```

### 查看 vfabric 配置

```
OS10(conf-vfabric-100)# show configuration
!
vfabric 100
 name 100
 vlan 1023
```

```
fcoe fcmap 0xEFC64
zoneset activate set
zone default-zone permit
```

```
OS10# show vfabric
Fabric Name 100
Fabric Type FPORT
Fabric Id 100
Vlan Id 1023
FC-MAP 0xEFC64
Config-State ACTIVE
Oper-State UP
=====
Switch Config Parameters
=====
Domain ID 100
=====
Switch Zoning Parameters
=====
Default Zone Mode: Allow
Active ZoneSet: set
=====
Members
fibrechannell1/1/1
fibrechannell1/1/2
fibrechannell1/1/3
fibrechannell1/1/4
fibrechannell1/1/5
fibrechannell1/1/6
fibrechannell1/1/7
fibrechannell1/1/8
fibrechannell1/1/9
fibrechannell1/1/10
fibrechannell1/1/11
fibrechannell1/1/12
fibrechannell1/1/15
fibrechannell1/1/17
fibrechannell1/1/18
fibrechannell1/1/19
fibrechannell1/1/20
fibrechannell1/1/21
fibrechannell1/1/22
fibrechannell1/1/23
fibrechannell1/1/24
fibrechannell1/1/25:1
fibrechannell1/1/29:1
fibrechannell1/1/30:1
fibrechannell1/1/30:3
=====
```

要在 NPG 模式下配置 vfabric:

1. 在 CONFIGURATION 模式下使用 `vfabric fabric-ID` 命令配置 vfabric。交换机将进入 vfabric CONFIGURATION 模式。
2. 使用 `vlan vlan-ID` 命令将 VLAN ID 与 vfabric 关联。
3. 使用 `fcoe {fcmap fc-map | fcf-priority fcf-priority-value | fka-adv-period adv-period | vlan-priority vlan-priority-value | keep-alive}` 命令添加 FCoE 参数。
4. (可选) 使用 `name vfabric-name` 命令将名称添加到 vfabric。
5. 在 INTERFACE 模式下使用 `vfabric fabric-ID` 命令将 vfabric 应用到接口。

#### 在 NPG 模式下配置 vfabric

```
OS10(config)# vfabric 10
OS10(conf-vfabric-10)# name 10
OS10(conf-vfabric-10)# vlan 100
OS10(conf-vfabric-10)# fcoe fcmap 0x0efc01
OS10(conf-vfabric-10)# fcoe fcf-priority 128
OS10(conf-vfabric-10)# fcoe fka-adv-period 8
OS10(conf-vfabric-10)# fcoe vlan-priority 3
OS10(conf-vfabric-10)# exit
```

```
OS10(config)# interface ethernet 1/1/31
OS10(conf-if-eth1/1/31)# vfabric 10
```

## 查看 vfabric 配置

```
OS10(conf-vfabric-10)# show configuration
!
vfabric 10
 name 10
 vlan 100
 fcoe fcmap 0xEFC01
 fcoe fcf-priority 128
 fcoe fka-adv-period 8
 fcoe vlan-priority 3
```

```
OS10# show vfabric
Fabric Name 10
Fabric Type NPG
Fabric Id 10
Vlan Id 100
FC-MAP 0xEFC01
Vlan priority 3
FCF Priority 128
FKA-Adv-Period Enabled, 8
Config-State ACTIVE
Oper-State DOWN
=====
Members
=====
```

```
OS10# show running-configuration vfabric
!
vfabric 10
 name 10
 vlan 100
 fcoe fcmap 0xEFC01
 fcoe fcf-priority 128
 fcoe fka-adv-period 8
 fcoe vlan-priority 3
```

# 光纤通道分区

光纤通道 (FC) 分区将 FC 结构分区成多个子集，以限制不必要的交互、提高安全性并更有效地管理结构。创建分区并将成员添加到分区中。通过 FC 别名、全球通用名称 (WWN) 或 FC ID 来标识成员。一个分区最多可以有 255 个唯一成员。创建分区集并将分区添加到分区集。一个交换机可以有多个分区集，但一次只能在结构中激活一个分区集。

1. (可选) 在 CONFIGURATION 模式下使用 `fc alias alias-name` 命令创建 FC 别名。交换机进入 Alias CONFIGURATION 模式。
2. 在 Alias CONFIGURATION 模式下使用 `member {wwn wwn-ID | fc-id fc-id}` 命令将成员添加到别名。最多可以添加 255 个唯一成员。
3. 在 CONFIGURATION 模式下使用 `fc zone zone-name` 命令创建一个分区。交换机将进入分区 CONFIGURATION 模式。
4. 在分区 CONFIGURATION 模式下适用 `member {alias-name alias-name | wwn wwn-ID | fc-id fc-id}` 命令将成员添加到分区。
5. 在 CONFIGURATION 模式下使用 `fc zoneset zoneset-name` 命令创建分区集。交换机将进入分区集 CONFIGURATION 模式。
6. 在分区集 CONFIGURATION 模式下使用 `member zone-name` 命令将现有分区添加到分区集。
7. 在 vfabric CONFIGURATION 模式下使用 `zoneset activate zoneset-name` 命令激活分区集。分区集中的成员将变为活动状态。
8. 在 vfabric CONFIGURATION 模式下允许使用 `zone default-zone permit` 命令在缺少活动分区集配置的情况下访问所有已登录的 FC 节点。默认区域在注册状态更改通知 (RSCN) 消息中通告最多 255 个成员。

 **注：**当活动分区集不可用时，默认区域允许或拒绝对 FC 节点的访问。当默认区域操作设置为 `permit` 时，交换机允许在所有可能的 FC 节点对之间进行通信。未配置默认分区操作时，交换机将拒绝 FC 节点之间的任何通信。

要在 FC 接口上配置 vfabric，请将 VLAN ID 关联到 vfabric 并添加 FC 映射。有关详情，请参阅 [虚拟结构](#) 页面上的 290。



配置 FC 分区

```
OS10(config)# fc zone hba1
OS10(config-fc-zone-hba1)# member wwn 10:00:00:90:fa:b8:22:19
OS10(config-fc-zone-hba1)# member wwn 21:00:00:24:ff:7b:f5:c8
OS10(config-fc-zone-hba1)# exit

OS10(config)# fc zoneset set
OS10(conf-fc-zoneset-set)# member hba1
OS10(conf-fc-zoneset-set)# exit

OS10(config)# vfabric 100
OS10(conf-vfabric-100)# zoneset activate set
OS10(conf-vfabric-100)# zone default-zone permit
```

查看 FC 分区配置

```
OS10(config-fc-zone-hba1)# show configuration
!
fc zone hba1
 member wwn 21:00:00:24:ff:7b:f5:c8
 member wwn 10:00:00:90:fa:b8:22:19
```

```
OS10# show fc zone

 Zone Name Zone Member
=====
hba1 21:00:00:24:ff:7b:f5:c8
 10:00:00:90:fa:b8:22:19

hba2 20:01:00:0e:1e:e8:e4:99
 50:00:d3:10:00:ec:f9:1b
 50:00:d3:10:00:ec:f9:05
 50:00:d3:10:00:ec:f9:1f
 20:35:78:2b:cb:6f:65:57
```

查看 FC 分区集配置

```
OS10(conf-fc-zoneset-set)# show configuration
!
fc zoneset set
 member hba1
 member hba2
```

```
OS10# show fc zoneset active

vFabric id: 100
Active Zoneset: set
ZoneName ZoneMember
=====
hba2 *20:01:00:0e:1e:e8:e4:99
 20:35:78:2b:cb:6f:65:57
 50:00:d3:10:00:ec:f9:05
 50:00:d3:10:00:ec:f9:1b
 50:00:d3:10:00:ec:f9:1f

hba1 *10:00:00:90:fa:b8:22:19
 *21:00:00:24:ff:7b:f5:c8
```

```
OS10# show fc zoneset set
ZoneSetName ZoneName ZoneMember
=====
set hba1 21:00:00:24:ff:7b:f5:c8
 10:00:00:90:fa:b8:22:19
 21:00:00:24:ff:7f:ce:ee
 21:00:00:24:ff:7f:ce:ef

 hba2 20:01:00:0e:1e:e8:e4:99
 50:00:d3:10:00:ec:f9:1b
```

```
50:00:d3:10:00:ec:f9:05
50:00:d3:10:00:ec:f9:1f
20:35:78:2b:cb:6f:65:57
```

## 以太网上的 F\_Port

OS10 支持在连接到聚合网络适配器 (CNA) 的以太网端口上配置 F\_Port 模式。启用 F\_Port 模式后，配置 vfabric 并将 vfabric 应用到连接到 CNA 的以太网端口。您只能在 F\_Port 模式中配置一个 vfabric。

您可以将已配置的 vfabric 应用到多个以太网接口。您还可以将以太网接口添加到端口通道，并将 vfabric 应用到端口通道。

### 配置示例

```
OS10(config)# feature fc domain-id 100
OS10(config)# vfabric 100
OS10(conf-vfabric-100)# name 100
OS10(conf-vfabric-100)# vlan 1023
OS10(conf-vfabric-100)# fcoe fcmap 0xEFC64
OS10(conf-vfabric-100)# zoneset activate set
OS10(conf-vfabric-100)# zone default-zone permit
OS10(conf-vfabric-100)# exit
OS10(config)# interface ethernet 1/1/30
OS10(conf-if-eth1/1/30)# vfabric 100
```

## 将 FCoE 流量固定到端口通道的特定端口

您可以通过在 FCoE LAG 上配置固定端口来隔离 FIP 和 FCoE 流量。

FCoE LAG 是端口通道，用于在服务器与存储设备之间的中间交换机中的 FIP 和 FCoE 流量。

通过将多个路径中的流量转发至多个上游设备，VLT 提供了聚合链路上的主动/主动 LAN 连接，而无需 STP 阻止任何上行链路。这可用于以太网流量，但 FCoE 需要针对每个 SAN 结构的专用链路。VLT 上发送的 FCoE 流量将中断 SAN 结构隔离。

FC 会话在 FC 节点之间形成，而 FCoE 会话在以太网节点之间发生。

要形成 FC 或 FCoE 会话，结构登录请求和回复必须通过相同的端口遍历交换机。通过交换机从服务器启动的结构登录请求达到了 SAN 结构。登录接受响应将哈希输出到端口通道中的任何端口。如果服务器收到的响应与发送请求的端口不同，服务器将继续重试此请求。由于此操作，基于登录接受响应学习的 FC 或 FCoE 会话将更改为不稳定状态。会话将保持变化，直到请求和响应在同一端口中聚合。为避免这种情况，请在端口通道中固定其中一个端口。

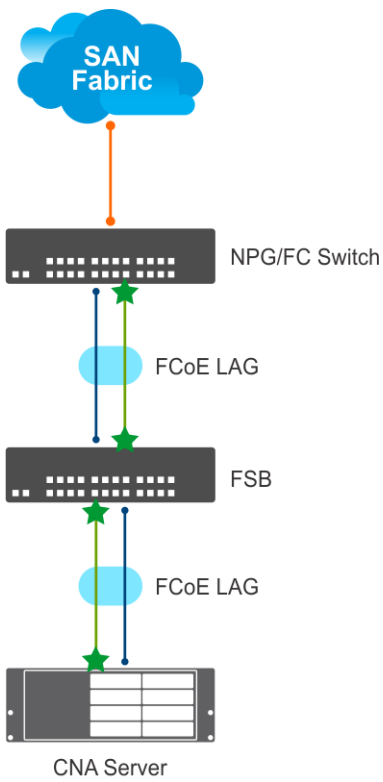
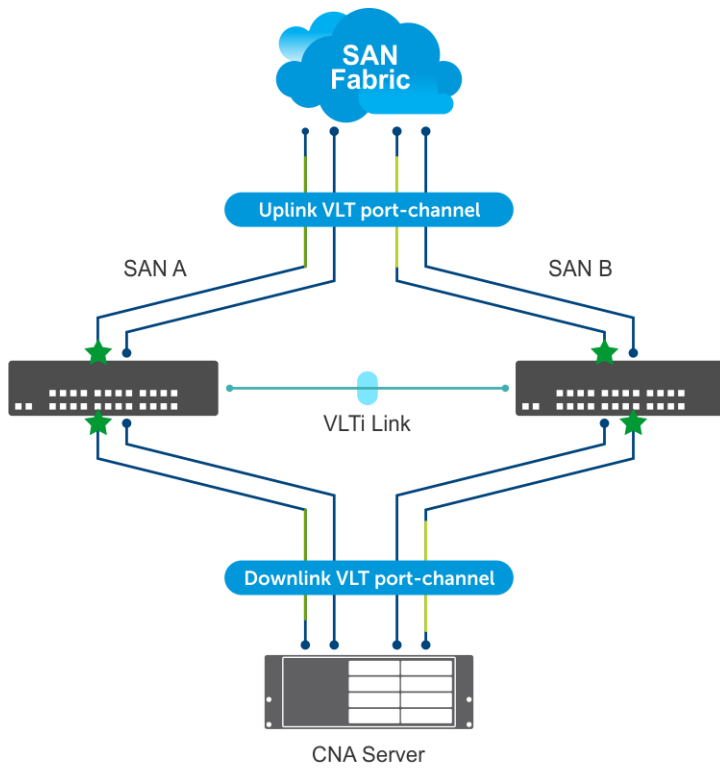
要在多层 VLT 网络上支持 FCoE，请在 FCoE LAG 中使用端口固定。端口固定是一种静态配置，用于将 FIP 和 FCoE 流量限制为覆盖硬件 LAG 哈希的端口通道中的一个端口。系统会根据 ACL 配置，对在端口 FCoE 会话期间交换的数据包进行分类和重定向。剩余的以太网流量基于 LAG 哈希流经端口通道中的固定端口和其他端口。如果 FCoE LAG 中有多个端口，Dell EMC 建议使用固定端口。在 VLT 网络中，服务器有两个与 SAN 连接的唯一 FCoE 会话，以及基于固定端口配置的流量流。如果端口通道中只有一个端口，则无需固定端口。

**注：**固定端口配置在 FSB、NPG 的以太网下行链路端口通道和 F\_Port 模式下受支持。

### 限制：

- 系统使用适用于 ENode MAC 的 ACL 表，其中包含与 FCF 类似的重定向端口选项。这将限制 FC 或 FCoE 会话的数量。
- 当固定端口停机时，您必须手动将端口通道中的另一个活动端口重新配置为固定端口。您只能在中间交换机（而不是服务器）中执行此重新配置。
- 如果配置中存在不匹配的情况，或者驻留的端口发生故障，则即使服务器和存储设备的路径有效，系统也不会使用端口通道中的其他端口。
- 当 FCoE 会话处于活动状态时添加或删除已驻留的端口时，系统将根据配置清除并重新启动 FCoE 会话。在配置过程中，系统会显示警告消息。

下图显示了 FCoE 流量流过固定端口的 VLT 和非 VLT 网络。



## VLT 网络上的 FSB 配置示例

1. 全局启用 FIP 侦听功能。

```
OS10(config)# feature fip-snooping
```

2. 创建 FCoE VLAN。

```
OS10(config)#interface vlan 1001
OS10(conf-if-vl-1001)# fip-snooping enable
```

3. 配置 VLTi 接口。

```
OS10(config)# interface ethernet 1/1/27
OS10(conf-if-eth1/1/27)# no shutdown
OS10(conf-if-eth1/1/27)# no switchport
```

4. 配置 VLT。

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.151.110 <<Enter the management IP address
of the VLT peer>>
OS10(conf-vlt-1)# discovery-interface ethernet1/1/27
```

5. 启用 DCBX。

```
OS10(config)# dcbx enable
```

6. 启用接口上的 PFC 参数。

```
OS10(config)# class-map type network-qos fcoematch
OS10(config-cmap-nqos)# match qos-group 3
OS10(config-cmap-nqos)# exit
OS10(config)# policy-map type network-qos PFC
OS10(config-pmap-network-qos)# class fcoematch
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 3
```

7. 创建上行链路和下行链路端口通道，并配置 FCF 饰面端口。

```
OS10(config)# interface port-channel 10
OS10(conf-if-po-10)# description uplink_VLT_LAG
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode trunk
OS10(conf-if-po-10)# switchport access vlan 1
OS10(conf-if-po-10)# switchport trunk allowed vlan 1001,10
OS10(conf-if-po-10)# vlt-port-channel 1
OS10(conf-if-po-10)# fip-snooping port-mode fcf
```

```
OS10(config)# interface port-channel 20
OS10(conf-if-po-20)# description downlink_VLT_LAG
OS10(conf-if-po-20)# no shutdown
OS10(conf-if-po-20)# switchport mode trunk
OS10(conf-if-po-20)# switchport access vlan 1
OS10(conf-if-po-20)# switchport trunk allowed vlan 1001,10
OS10(conf-if-po-20)# vlt-port-channel 2
```

8. 在下行链路和上行链路接口上应用 PFC 配置。此外，还包括端口通道的接口，并将其中一个接口配置为固定端口。

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# description uplink_port_channel_member1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# channel-group 10 mode active
OS10(conf-if-eth1/1/1)# fcoe-pinned-port
OS10(conf-if-eth1/1/1)# no switchport
```

```
OS10(config-if-eth1/1/1)# service-policy input type network-qos PFC
OS10(config-if-eth1/1/1)# priority-flow-control mode on
```

```
OS10(config)# interface ethernet 1/1/2
OS10(config-if-eth1/1/2)# description uplink_port_channel_member2
OS10(config-if-eth1/1/2)# no shutdown
OS10(config-if-eth1/1/2)# channel-group 10 mode active
OS10(config-if-eth1/1/2)# no switchport
OS10(config-if-eth1/1/2)# service-policy input type network-qos PFC
OS10(config-if-eth1/1/2)# priority-flow-control mode on
```

```
OS10(config)# interface ethernet 1/1/3
OS10(config-if-eth1/1/3)# description downlink_port_channel_member1
OS10(config-if-eth1/1/3)# no shutdown
OS10(config-if-eth1/1/3)# channel-group 20 mode active
OS10(config-if-eth1/1/3)# fcoe-pinned-port
OS10(config-if-eth1/1/3)# no switchport
OS10(config-if-eth1/1/3)# service-policy input type network-qos PFC
OS10(config-if-eth1/1/3)# priority-flow-control mode on
```

```
OS10(config)# interface ethernet 1/1/4
OS10(config-if-eth1/1/4)# description downlink_port_channel_member2
OS10(config-if-eth1/1/4)# no shutdown
OS10(config-if-eth1/1/4)# channel-group 20 mode active
OS10(config-if-eth1/1/4)# no switchport
OS10(config-if-eth1/1/4)# service-policy input type network-qos PFC
OS10(config-if-eth1/1/4)# priority-flow-control mode on
```

## 查看配置

VLT 详细信息:

```
OS10# show vlt 1
Domain ID : 1
Unit ID : 2
Role : primary
Version : 2.0
Local System MAC address : 50:9a:4c:d3:cf:70
Primary priority : 32768
VLT MAC address : 50:9a:4c:d3:cf:70
IP address : fda5:74c8:b79e:1::2
Delay-Restore timer : 90 seconds
Peer-Routing : Disabled
Peer-Routing-Timeout timer : 0 seconds
VLTi Link Status
 port-channel1000 : up
```

| VLT | Peer | Unit ID | System MAC Address | Status | IP Address          | Version |
|-----|------|---------|--------------------|--------|---------------------|---------|
| 1   |      |         | 50:9a:4c:d3:e2:f0  | up     | fda5:74c8:b79e:1::1 | 2.0     |

```
OS10# show vlt 1 vlt-port-detail
vlt-port-channel ID : 1
```

| VLT | Unit ID | Port-Channel   | Status | Configured ports | Active ports |
|-----|---------|----------------|--------|------------------|--------------|
| 1   |         | port-channel10 | up     | 2                | 2            |
| * 2 |         | port-channel10 | up     | 2                | 2            |

```
vlt-port-channel ID : 2
```

| VLT | Unit ID | Port-Channel   | Status | Configured ports | Active ports |
|-----|---------|----------------|--------|------------------|--------------|
| 1   |         | port-channel20 | up     | 2                | 2            |
| * 2 |         | port-channel20 | up     | 2                | 2            |

查找到的 ENode:

```
OS10# show fcoe enode
Enode MAC Enode Interface VLAN FCFs Sessions

f4:e9:d4:a4:7d:c3 Po 20(Eth 1/1/3) 1001 1 1
```

查找到的 FCF:

| FCF MAC           | FCF Interface     | VLAN | FC-MAP   | FKA_ADV_PERIOD | No. of Enodes |
|-------------------|-------------------|------|----------|----------------|---------------|
| 14:18:77:20:78:e0 | Po 10 (Eth 1/1/1) | 1001 | 0e:fc:00 | 8000           | 1             |

FCoE 会话:

| Enode MAC<br>MAC          | Enode Interface<br>FC-ID<br>PORT WWPN          | FCF MAC                                      | FCF interface<br>PORT WNNN                   | VLAN | FCoE |
|---------------------------|------------------------------------------------|----------------------------------------------|----------------------------------------------|------|------|
| f4:e9:d4:a4:7d:c3<br>1001 | Po20 (Eth 1/1/3)<br>01:34:02 0e:fc:00:01:00:00 | 14:18:77:20:78:e0<br>20:01:f4:e9:d4:a4:7d:c3 | Po 10 (Eth 1/1/1)<br>20:00:f4:e9:d4:a4:7d:c3 |      |      |

固定端口状态:

| Interface | pinned-port | FCoE Status |
|-----------|-------------|-------------|
| Po 10     | Eth 1/1/1   | Up          |
| Po 20     | Eth 1/1/3   | Up          |

## VLT 网络上的 FC 交换机配置示例

1. 启用 F\_PORT 模式。

```
OS10(config)# feature fc domain-id 1
```

2. 创建 FC 分区。

```
OS10(config)# fc zone zoneA
OS10(config-fc-zone-zoneA)# member wwn 10:00:00:90:fa:b8:22:19 <<Enter the WWN of Initiator CNA>>
OS10(config-fc-zone-zoneA)# member wwn 21:00:00:24:ff:7b:f5:c8 <<Enter the WWN of Target>>
```

3. 创建 FC 分区集。

```
OS10(config)# fc zoneset zonesetA
OS10(conf-fc-zoneset-zonesetA)# member zoneA
```

4. 创建 vfabric VLAN。

```
OS10(config)# interface vlan 1001
```

5. 创建 vfabric 并激活 FC 分区集。

```
OS10(config)# vfabric 1
OS10(conf-vfabric-1)# vlan 1001
OS10(conf-vfabric-1)# fcoe fcmap 0xEFC00
OS10(conf-vfabric-1)# zoneset activate zonesetA
```

6. 配置 VLTi 接口。

```
OS10(config)# interface ethernet 1/1/27
OS10(conf-if-eth1/1/27)# no shutdown
OS10(conf-if-eth1/1/27)# no switchport
```

7. 配置 VLT。

```
OS10(config)# vlt-domain 10
OS10(conf-vlt-10)# backup destination 10.16.151.110
OS10(conf-vlt-10)# discovery-interface ethernet1/1/27
```

## 8. 启用 DCBX。

```
OS10(config)# dcbx enable
```

## 9. 在接口上应用 vfabric。

```
OS10(config)# interface port-channel 10
OS10(conf-if-po-10)# description downlink_VLT_LAG_to_FSB
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode trunk
OS10(conf-if-po-10)# switchport access vlan 1
OS10(conf-if-po-10)# switchport trunk allowed vlan 10
OS10(conf-if-po-10)# vlt-port-channel 1
OS10(conf-if-po-10)# vfabric 1
```

```
OS10(config)# interface fibrechannel 1/1/26
OS10(conf-if-fc1/1/26)# description target_connected_port
OS10(conf-if-fc1/1/26)# no shutdown
OS10(conf-if-fc1/1/26)# vfabric 1
```

## 10. 在下行链路接口上应用 PFC 配置。将接口包括到端口通道并将其中一个接口配置为固定端口。

```
OS10(config)# interface ethernet 1/1/9
OS10(conf-if-eth1/1/9)# description downlink_port_channel_member1
OS10(conf-if-eth1/1/9)# no shutdown
OS10(conf-if-eth1/1/9)# channel-group 10 mode active
OS10(conf-if-eth1/1/9)# fcoe-pinned-por
OS10(conf-if-eth1/1/9)# no switchport
OS10(conf-if-eth1/1/9)# service-policy input type network-qos PFC
OS10(conf-if-eth1/1/9)# priority-flow-control mode on
```

```
OS10(config)# interface ethernet 1/1/10
OS10(conf-if-eth1/1/10)# description downlink_port_channel_member2
OS10(conf-if-eth1/1/10)# no shutdown
OS10(conf-if-eth1/1/10)# channel-group 10 mode active
OS10(conf-if-eth1/1/10)# no switchport
OS10(conf-if-eth1/1/10)# service-policy input type network-qos PFC
OS10(conf-if-eth1/1/10)# priority-flow-control mode on
```

## 查看配置

命名服务器条目：

```
OS10# show fc ns switch brief
Total number of devices = 2
Intf# Domain FC-ID Enode-WWPN Enode-WWNN
port-channel10(Eth 1/1/9) 1 01:00:00 20:01:f4:e9:d4:a4:7d:c3
20:00:f4:e9:d4:a4:7d:c3
fibrechannel1/1/26 1 01:68:00 21:00:00:24:ff:7c:ae:0e
21:00:00:24:ff:7c:ae:0e
```

分区集详细信息：

```
vFabric id: 1
Active Zoneset: zonesetA
ZoneName ZoneMember
=====
zoneA *20:01:f4:e9:d4:a4:7d:c3
 *21:00:00:24:ff:7c:ae:0e
```

固定端口状态：

```
OS10# show fcoe pinned-port
Interface pinned-port FCoE Status

Po 10 Eth 1/1/9 Up
```

## 非 VLT 网络上的 FSB 配置示例

以下示例说明了非 VLT 网络中的中间交换机配置，以与服务器通信。

### 1. 全局启用 FIP 侦听功能。

```
OS10(config)# feature fip-snooping
```

### 2. 创建 FCoE VLAN。

```
OS10(config)#interface vlan 1001
OS10(conf-if-vl-1001)# fip-snooping enable
```

### 3. 启用 DCBX。

```
OS10(config)# dcbx enable
```

### 4. 启用接口上的 PFC 参数。

```
OS10(config)# class-map type network-qos fcoematch
OS10(config-cmap-nqos)# match qos-group 3
OS10(config-cmap-nqos)# exit
OS10(config)# policy-map type network-qos PFC
OS10(config-pmap-network-qos)# class fcoematch
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 3
```

### 5. 创建上行链路和下行链路端口通道，并配置 FCF 饰面端口。

```
OS10(config)# interface port-channel 10
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode trunk
OS10(conf-if-po-10)# switchport access vlan 1
OS10(conf-if-po-10)# switchport trunk allowed vlan 1001,10
OS10(conf-if-po-10)# fip-snooping port-mode fcf
```

```
OS10(config)# interface port-channel 20
OS10(conf-if-po-20)# no shutdown
OS10(conf-if-po-20)# switchport mode trunk
OS10(conf-if-po-20)# switchport access vlan 1
OS10(conf-if-po-20)# switchport trunk allowed vlan 1001,10
```

### 6. 在下行链路和上行链路接口上应用 PFC 配置。此外，还包括端口通道的接口，并将其中一个接口配置为固定端口。

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# channel-group 10 mode active
OS10(conf-if-eth1/1/1)# fcoe-pinned-port
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# service-policy input type network-qos PFC
OS10(conf-if-eth1/1/1)# priority-flow-control mode on
```

```
OS10(config)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# channel-group 10 mode active
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# service-policy input type network-qos PFC
OS10(conf-if-eth1/1/2)# priority-flow-control mode on
```

```
OS10(config)# interface ethernet 1/1/3
OS10(conf-if-eth1/1/3)# no shutdown
OS10(conf-if-eth1/1/3)# channel-group 20 mode active
OS10(conf-if-eth1/1/3)# fcoe-pinned-port
OS10(conf-if-eth1/1/3)# no switchport
```



```
OS10(config-if-eth1/1/3)# service-policy input type network-qos PFC
OS10(config-if-eth1/1/3)# priority-flow-control mode on
```

```
OS10(config)# interface ethernet 1/1/4
OS10(config-if-eth1/1/4)# no shutdown
OS10(config-if-eth1/1/4)# channel-group 20 mode active
OS10(config-if-eth1/1/4)# no switchport
OS10(config-if-eth1/1/4)# service-policy input type network-qos PFC
OS10(config-if-eth1/1/4)# priority-flow-control mode on
```

## 查看配置

查找到的 ENode:

```
OS10# show fcoe enode
Enode MAC Enode Interface VLAN FCFs Sessions

f4:e9:d4:a4:7d:c3 Po 20(Eth 1/1/3) 1001 1 1
```

查找到的 FCF:

```
OS10# show fcoe fcf
FCF MAC FCF Interface VLAN FC-MAP FKA_ADV_PERIOD No. of Enodes

14:18:77:20:78:e0 Po 10(Eth 1/1/1) 1001 0e:fc:00 8000 1
```

FCoE 会话:

```
Enode MAC Enode Interface FCF MAC FCF interface VLAN FCoE
MAC FC-ID PORT WWPN PORT WNNN

f4:e9:d4:a4:7d:c3 Po20(Eth 1/1/3) 14:18:77:20:78:e0 Po 10(Eth 1/1/1)
1001 0e:fc:00:01:00:00 01:34:02 20:01:f4:e9:d4:a4:7d:c3 20:00:f4:e9:d4:a4:7d:c3
```

固定端口状态:

```
OS10# show fcoe pinned-port
Interface pinned-port FCoE Status

Po 10 Eth 1/1/1 Up
Po 20 Eth 1/1/3 Up
```

## 非 VLT 网络上的 FC 交换机配置示例

1. 启用 F\_PORT 模式。

```
OS10(config)# feature fc domain-id 1
```

2. 创建 FC 分区。

```
OS10(config)# fc zone zoneA
OS10(config-fc-zone-zoneA)# member wwn 10:00:00:90:fa:b8:22:19 <<Enter the WWN of Initiator CNA>>
OS10(config-fc-zone-zoneA)# member wwn 21:00:00:24:ff:7b:f5:c8 <<Enter the WWN of Target>>
```

3. 创建 FC 分区集。

```
OS10(config)# fc zoneset zonesetA
OS10(config-fc-zoneset-zonesetA)# member zoneA
```

4. 创建 vfabric VLAN。

```
OS10(config)# interface vlan 1001
```

5. 创建 vfabric 并激活 FC 分区集。

```
OS10(config)# vfabric 1
OS10(conf-vfabric-1)# vlan 1001
OS10(conf-vfabric-1)# fcoe fcmap 0xEFC00
OS10(conf-vfabric-1)# zoneset activate zonesetA
```

6. 启用 DCBX。

```
OS10(config)# dcbx enable
```

7. 在接口上应用 vfabric。

```
OS10(config)# interface port-channel 10
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode trunk
OS10(conf-if-po-10)# switchport access vlan 1
OS10(conf-if-po-10)# switchport trunk allowed vlan 10
OS10(conf-if-po-10)# vfabric 1
```

```
OS10(config)# interface fibrechannel 1/1/26
OS10(conf-if-fc1/1/26)# description target_connected_port
OS10(conf-if-fc1/1/26)# no shutdown
OS10(conf-if-fc1/1/26)# vfabric 1
```

8. 在下行链路接口上应用 PFC 配置。将接口包括到端口通道并将其中一个接口配置为固定端口。

```
OS10(config)# interface ethernet 1/1/9
OS10(conf-if-eth1/1/9)# no shutdown
OS10(conf-if-eth1/1/9)# channel-group 10 mode active
OS10(conf-if-eth1/1/9)# fcoe-pinned-por
OS10(conf-if-eth1/1/9)# no switchport
OS10(conf-if-eth1/1/9)# service-policy input type network-qos PFC
OS10(conf-if-eth1/1/9)# priority-flow-control mode on
```

```
OS10(config)# interface ethernet 1/1/10
OS10(conf-if-eth1/1/10)# no shutdown
OS10(conf-if-eth1/1/10)# channel-group 10 mode active
OS10(conf-if-eth1/1/10)# no switchport
OS10(conf-if-eth1/1/10)# service-policy input type network-qos PFC
OS10(conf-if-eth1/1/10)# priority-flow-control mode on
```

查看配置

命名服务器条目：

```
OS10# show fc ns switch brief
Total number of devices = 2
Intf# Domain FC-ID Enode-WWPN Enode-WWNN
port-channel10(Eth 1/1/9) 1 01:00:00 20:01:f4:e9:d4:a4:7d:c3
20:00:f4:e9:d4:a4:7d:c3
fibrechannel1/1/26 1 01:68:00 21:00:00:24:ff:7c:ae:0e
21:00:00:24:ff:7c:ae:0e
```

分区集详细信息：

```
vFabric id: 1
Active Zoneset: zonesetA
ZoneName ZoneMember
=====
zoneA *20:01:f4:e9:d4:a4:7d:c3
 *21:00:00:24:ff:7c:ae:0e
```

固定端口状态：

```
OS10# show fcoe pinned-port
Interface pinned-port FCoE Status

Po 10 Eth 1/1/9 Up
```

# 多跳 FIP 侦听桥

在典型部署中，ENode 连接的交换机不直接连接到核心 FC 交换机。交换机之间连接了多个中间交换机。要建立点对点连接和 ENode 与 FCF 之间的安全传输，所有中间交换机都必须支持 FSB 以传递 FIP 和 FCoE 流量。

OS10 交换机支持多跳 FIP 侦听桥。您可以将多个 FSB 互连以与上游 FC 交换机进行通信。

- 访问 FSB — 这是直接连接 ENode 的节点。在下面的示例中，FSB1 是访问 FSB。
- 核心 FSB — 这是直接连接 FCF 的节点。在下面的示例中，FSB2 是核心 FSB。

默认端口模式是 ENode。您必须使用 `fip-snooping port-mode` 命令明确配置其他模式。支持以下端口模式：

- ENode — 每个接口只能获知一个 ENode MAC 地址。在连接到 ENode 的端口上配置此模式。
- FCF — 如果您将 FSB 配置为 FCF 端口模式，则在 ENode 和 FCF 之间发送的所有 FIP 数据包都将侦听，会话和 ENodes 将获知。在连接到面向 FCF 端的访问 FSB 端口上配置 FCF 模式。
- ENode 传输 — 此模式在 ENodes 连接到的中间 FSB 或第 2 层 (L2) DCBX 交换机上配置。
- FCF 传输 — 只侦听 FCF 通告和 VLAN 响应以获知 FCF。FCF 传输不会获知 ENodes 和会话信息。在核心 FSB 交换机的面向 FCF 端配置 FCF 传输模式。

FCF 可处于 NPG 或 F 端口模式。访问 FSB 交换机会验证这些帧并根据 FCF 安装 ACL，以仅允许跨 FCF 的 FCoE 和 FIP 流量。

 **注：** 连接到 FCF 模式的 FSB 交换机的 ENode 不支持端口固定。您不能使用 `show` 命令查看 ENode 或会话信息。

## 清除虚拟链路帧

当 FSB 因某种原因清除 FCoE 会话时，网络中的其他设备（如 ENode、FCF 和传输交换机）不会收到通知，并且认为该会话完好无损。FSB 将丢弃与清除的会话对应的 FCoE 数据。ENode 需要很长时间来识别问题并从中恢复。有时，接口摆动将发生，并且可能需要手动干预才能恢复。要自动恢复，FSB 会将清除虚拟链路 (CVL) 帧从 FCF 发送到 ENode。

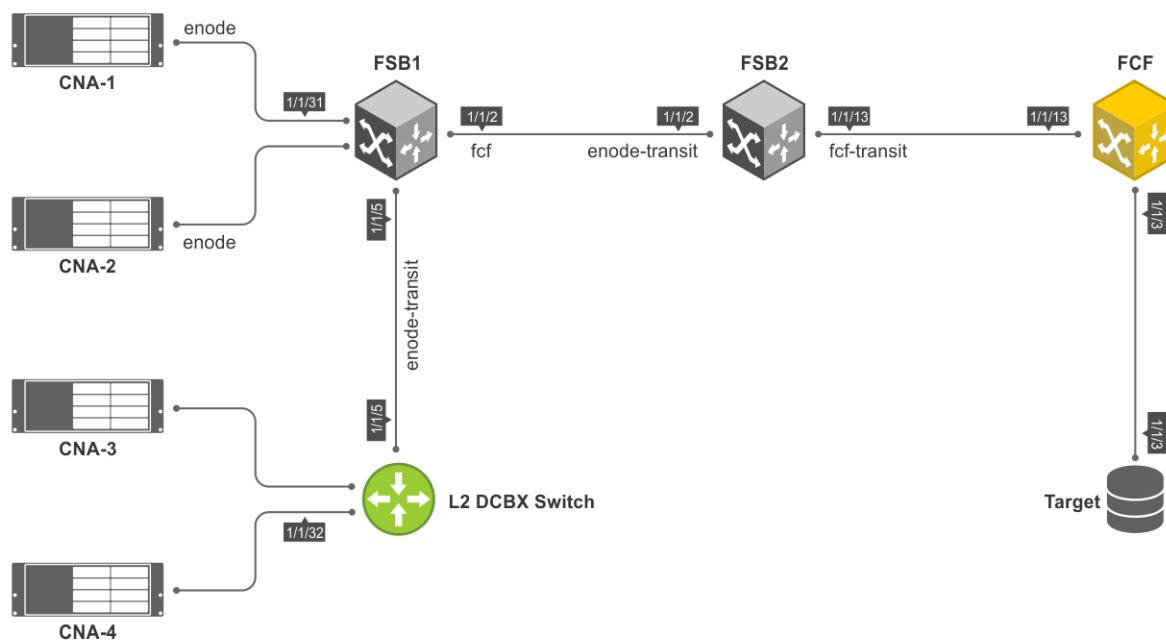
## 配置说明

- 如果配置其端口固定在上行链路或下行链路端的 FSB，则必须将面向 FCF 的接口配置为 FCF 端口模式。
- OS10 目前不支持将单端口必须配置为 ENode 和 FCF 相关的端口模式的拓扑。
- 如果您在 FSB 上配置了 FCF 转换端口模式，Dell EMC 建议不要直接连接其上的 ENode。

## 配置多跳 FSB

以下示例显示了一个简单的多跳 FSB 设置。此拓扑中显示的 CNA-2 和 CNA-3 仅用于说明目的。以下示例不包括 CNA-2 和 CNA-3 配置。

确保访问和核心 FSB 交换机以 FSB 模式运行。



要配置多跳 FSB，请执行以下操作：

1. 配置 L2 交换机。

- a. 在连接到 CNA-4 和 FSB1 的接口上禁用流控制。

```
L2switch(config)# interface ethernet 1/1/32
L2switch(config-if-eth1/1/32)# no flowcontrol receive
L2switch(config-if-eth1/1/32)# no flowcontrol transmit

L2switch(config)# interface ethernet 1/1/5
L2switch(config-if-eth1/1/5)# no flowcontrol receive
L2switch(config-if-eth1/1/5)# no flowcontrol transmit
```

- b. 启用 DCBX。

```
L2switch(config)# dcbx enable
```

- c. 为要通过的 FCoE 流量创建 VLAN。

```
L2switch(config)# interface vlan 777
```

- d. 创建类别映射。

```
L2switch(config)# class-map type network-qos c3
L2switch(config-cmap-nqos)# match qos-group 3
```

```
L2switch(config)# class-map type queuing q0
L2switch(config-cmap-queuing)# match queue 0
L2switch(config-cmap-queuing)# exit
L2switch(config)# class-map type queuing q3
L2switch(config-cmap-queuing)# match queue 3
L2switch(config-cmap-queuing)# exit
```

- e. 创建策略映射。

```
L2switch# configure terminal
L2switch(config)# policy-map type network-qos nqpolicy
L2switch(config-pmap-network-qos)# class c3
L2switch(config-pmap-c-nqos)# pause
L2switch(config-pmap-c-nqos)# pfc-cos 3
```

```
L2switch(config)# policy-map type queuing ets_policy
L2switch(config-pmap-queuing)# class q0
L2switch(config-pmap-c-que)# bandwidth percent 30
```

```
L2switch(config-pmap-c-que)# class q3
L2switch(config-pmap-c-que)# bandwidth percent 70
```

f. 创建 qos 映射。

```
L2switch(config)# qos-map traffic-class tc-q-map1
L2switch(config-qos-map)# queue 3 qos-group 3
L2switch(config-qos-map)# queue 0 qos-group 0-2,4-7
```

g. 在 CNA-4 和 FSB1 连接的接口上应用 QoS 配置。

```
L2switch(config)# interface ethernet 1/1/32
L2switch(config-if-eth1/1/32)# priority-flow-control mode on
L2switch(config-if-eth1/1/32)# ets mode on
L2switch(config-if-eth1/1/32)# trust-map dot1p default
L2switch(config-if-eth1/1/32)# qos-map traffic-class tc-q-map1
L2switch(config-if-eth1/1/32)# service-policy input type network-qos nqpolicy
L2switch(config-if-eth1/1/32)# service-policy output type queuing ets_policy

L2switch(config)# interface ethernet 1/1/5
L2switch(config-if-eth1/1/5)# priority-flow-control mode on
L2switch(config-if-eth1/1/5)# ets mode on
L2switch(config-if-eth1/1/5)# trust-map dot1p default
L2switch(config-if-eth1/1/5)# qos-map traffic-class tc-q-map1
L2switch(config-if-eth1/1/5)# service-policy input type network-qos nqpolicy
L2switch(config-if-eth1/1/5)# service-policy output type queuing ets_policy
```

h. 在 CNA-4 和 FSB1 连接的接口上配置 VLAN。

```
L2switch(config)# interface ethernet 1/1/32
L2switch(config-if-eth1/1/32)# switchport mode trunk
L2switch(config-if-eth1/1/32)# switchport trunk allowed vlan 777

L2switch(config)# interface ethernet 1/1/5
L2switch(config-if-eth1/1/5)# switchport mode trunk
L2switch(config-if-eth1/1/5)# switchport trunk allowed vlan 777
```

2. 配置访问 FSB、FSB1。本示例介绍了

a. 在连接到 CNA1、L2 交换机和 FSB2 的接口上禁用流控制。

```
FSB1(config)# interface ethernet 1/1/31
FSB1(config-if-eth1/1/31)# no flowcontrol receive
FSB1(config-if-eth1/1/31)# no flowcontrol transmit

FSB1(config)# interface ethernet 1/1/5
FSB1(config-if-eth1/1/5)# no flowcontrol receive
FSB1(config-if-eth1/1/5)# no flowcontrol transmit

FSB1(config)# interface ethernet 1/1/2
FSB1(config-if-eth1/1/2)# no flowcontrol receive
FSB1(config-if-eth1/1/2)# no flowcontrol transmit
```

b. 通过 cvl 选项启用 FIP 侦听。

```
FSB1(config)# feature fip-snooping with-cvl
```

c. 启用 DCBX。

```
FSB1(config)# dcbx enable
```

d. 创建 FCoE VLAN，并在 FCoE VLAN 上配置 FIP 侦听。

```
FSB1(config)# interface vlan 777
FSB1(config-if-vl-777)# fip-snooping enable
```

e. 创建类别映射。

```
FSB1(config)# class-map type network-qos c3
FSB1(config-cmap-nqos)# match qos-group 3
```

```
FSB1(config)# class-map type queuing q0
FSB1(config-cmap-queuing)# match queue 0
FSB1(config-cmap-queuing)# exit
FSB1(config)# class-map type queuing q3
FSB1(config-cmap-queuing)# match queue 3
FSB1(config-cmap-queuing)# exit
```

f. 创建策略映射。

```
FSB1(config)# policy-map type network-qos nqpolicy
FSB1(config-pmap-network-qos)# class c3
FSB1(config-pmap-c-nqos)# pause
FSB1(config-pmap-c-nqos)# pfc-cos 3
```

```
FSB1(config)# policy-map type queuing ets_policy
FSB1(config-pmap-queuing)# class q0
FSB1(config-pmap-c-que)# bandwidth percent 30
FSB1(config-pmap-c-que)# class q3
FSB1(config-pmap-c-que)# bandwidth percent 70
```

g. 创建 qos 映射。

```
FSB1(config)# qos-map traffic-class tc-q-map1
FSB1(config-qos-map)# queue 3 qos-group 3
FSB1(config-qos-map)# queue 0 qos-group 0-2,4-7
```

h. 在 CNA1、L2 交换机和 FSB2 连接的接口上应用 QoS 配置。

```
FSB1(config)# interface ethernet 1/1/31
FSB1(conf-if-eth1/1/31)# priority-flow-control mode on
FSB1(conf-if-eth1/1/31)# ets mode on
FSB1(conf-if-eth1/1/31)# trust-map dot1p default
FSB1(conf-if-eth1/1/31)# qos-map traffic-class tc-q-map1
FSB1(conf-if-eth1/1/31)# service-policy input type network-qos nqpolicy
FSB1(conf-if-eth1/1/31)# service-policy output type queuing ets_policy

FSB1(config)# interface ethernet 1/1/5
FSB1(conf-if-eth1/1/5)# priority-flow-control mode on
FSB1(conf-if-eth1/1/5)# ets mode on
FSB1(conf-if-eth1/1/5)# trust-map dot1p default
FSB1(conf-if-eth1/1/5)# qos-map traffic-class tc-q-map1
FSB1(conf-if-eth1/1/5)# service-policy input type network-qos nqpolicy
FSB1(conf-if-eth1/1/5)# service-policy output type queuing ets_policy

FSB1(config)# interface ethernet 1/1/2
FSB1(conf-if-eth1/1/2)# priority-flow-control mode on
FSB1(conf-if-eth1/1/2)# ets mode on
FSB1(conf-if-eth1/1/2)# trust-map dot1p default
FSB1(conf-if-eth1/1/2)# qos-map traffic-class tc-q-map1
FSB1(conf-if-eth1/1/2)# service-policy input type network-qos nqpolicy
FSB1(conf-if-eth1/1/2)# service-policy output type queuing ets_policy
```

i. 在 CNA1、L2 交换机和 FSB2 连接的接口上配置 VLAN。

```
FSB1(config)# interface ethernet 1/1/31
FSB1(conf-if-eth1/1/31)# switchport mode trunk
FSB1(conf-if-eth1/1/31)# switchport trunk allowed vlan 777

FSB1(config)# interface ethernet 1/1/5
FSB1(conf-if-eth1/1/5)# switchport mode trunk
FSB1(conf-if-eth1/1/5)# switchport trunk allowed vlan 777

FSB1(config)# interface ethernet 1/1/2
FSB1(conf-if-eth1/1/2)# switchport mode trunk
FSB1(conf-if-eth1/1/2)# switchport trunk allowed vlan 777
```

- j. 在 L2 DCBX 交换机连接的接口和 FSB2 连接的接口上配置 FIP 侦听端口模式。默认端口模式为 ENode。因此，CNA1 连接的接口不需要其他配置。

在 L2 DCBX 交换机连接的接口上：

```
FSB1(config)# interface ethernet 1/1/5
FSB1(conf-if-eth1/1/5)# fip-snooping port-mode enode-transit
```

在 FSB 连接的接口上：

```
FSB1(config)# interface ethernet 1/1/2
FSB1(conf-if-eth1/1/2)# fip-snooping port-mode fcf
```

### 3. 配置核心 FSB、FSB2。

- a. 在连接到 FSB1 和 FCF 的接口上禁用流控制。

```
FSB2(config)# interface ethernet 1/1/2
FSB2(conf-if-eth1/1/2)# no flowcontrol receive
FSB2(conf-if-eth1/1/2)# no flowcontrol transmit

FSB2(config)# interface ethernet 1/1/13
FSB2(conf-if-eth1/1/13)# no flowcontrol receive
FSB2(conf-if-eth1/1/13)# no flowcontrol transmit
```

- b. 通过 cvl 选项启用 FIP 侦听。

```
FSB2(config)# feature fip-snooping with-cvl
```

- c. 启用 DCBX。

```
FSB2(config)# dcbx enable
```

- d. 创建 FCoE VLAN，并在 FCoE VLAN 上配置 FIP 侦听。

```
FSB2(config)# interface vlan 777
FSB2(conf-if-vl-777)# fip-snooping enable
```

- e. 创建类别映射。

```
FSB2(config)# class-map type network-qos c3
FSB2(config-cmap-nqos)# match qos-group 3
```

```
FSB2(config)# class-map type queuing q0
FSB2(config-cmap-queuing)# match queue 0
FSB2(config-cmap-queuing)# exit
FSB2(config)# class-map type queuing q3
FSB2(config-cmap-queuing)# match queue 3
FSB2(config-cmap-queuing)# exit
```

- f. 创建策略映射。

```
FSB2(config)# policy-map type network-qos nqpolicy
FSB2(config-pmap-network-qos)# class c3
FSB2(config-pmap-c-nqos)# pause
FSB2(config-pmap-c-nqos)# pfc-cos 3
```

```
FSB2(config)# policy-map type queuing ets_policy
FSB2(config-pmap-queuing)# class q0
FSB2(config-pmap-c-que)# bandwidth percent 30
FSB2(config-pmap-c-que)# class q3
FSB2(config-pmap-c-que)# bandwidth percent 70
```

- g. 创建 qos 映射。

```
FSB2(config)# qos-map traffic-class tc-q-map1
FSB2(config-qos-map)# queue 3 qos-group 3
FSB2(config-qos-map)# queue 0 qos-group 0-2,4-7
```

- h. 在 FSB1 和 FCF 连接的接口上应用 QoS 配置。

```
FSB2(config)# interface ethernet 1/1/2
FSB2(conf-if-eth1/1/2)# priority-flow-control mode on
FSB2(conf-if-eth1/1/2)# ets mode on
FSB2(conf-if-eth1/1/2)# trust-map dot1p default
FSB2(conf-if-eth1/1/2)# qos-map traffic-class tc-q-map1
FSB2(conf-if-eth1/1/2)# service-policy input type network-qos nqpolicy
FSB2(conf-if-eth1/1/2)# service-policy output type queuing ets_policy

FSB2(config)# interface ethernet 1/1/13
FSB2(conf-if-eth1/1/13)# priority-flow-control mode on
FSB2(conf-if-eth1/1/13)# ets mode on
FSB2(conf-if-eth1/1/13)# trust-map dot1p default
FSB2(conf-if-eth1/1/13)# qos-map traffic-class tc-q-map1
FSB2(conf-if-eth1/1/13)# service-policy input type network-qos nqpolicy
FSB2(conf-if-eth1/1/13)# service-policy output type queuing ets_policy
```

- i. 在 FSB1 和 FCF 连接的接口上配置 VLAN。

```
FSB2(config)# interface ethernet 1/1/2
FSB2(conf-if-eth1/1/2)# switchport mode trunk
FSB2(conf-if-eth1/1/2)# switchport trunk allowed vlan 777

FSB2(config)# interface ethernet 1/1/13
FSB2(conf-if-eth1/1/13)# switchport mode trunk
FSB2(conf-if-eth1/1/13)# switchport trunk allowed vlan 777
```

- j. 在 FSB1 和 FCF 连接的接口上配置 FIP 侦听端口模式。

在 FSB1 连接的接口上：

```
FSB2(config)# interface ethernet 1/1/2
FSB2(conf-if-eth1/1/2)# fip-snooping port-mode enode-transit
```

在 FCF 连接的接口上：

```
FSB2(config)# interface ethernet 1/1/13
FSB2(conf-if-eth1/1/13)# fip-snooping port-mode fcf-transit
```

#### 4. 配置 FCF。以下配置假定 FCF 处于 F 端口模式。

- a. 在连接到 FSB2 的接口上禁用流控制。

```
FCF(config)# interface ethernet 1/1/13
FCF(conf-if-eth1/1/13)# no flowcontrol receive
FCF(conf-if-eth1/1/13)# no flowcontrol transmit
```

- b. 在全局范围内启用光纤通道 F 端口模式。

```
FCF(config)# feature fc domain-id 2
```

- c. 创建分区。

```
FCF(config)# fc zone zoneA
FCF(config-fc-zone-zoneA)# member wwn 20:01:f4:e9:d4:a4:7d:c3
FCF(config-fc-zone-zoneA)# member wwn 21:00:00:24:ff:7c:ae:0e
```

- d. 创建分区集。

```
FCF(config)# fc zoneset zonesetA
FCF(conf-fc-zoneset-set)# member zoneA
```

- e. 创建 vfabric VLAN。

```
FCF(config)# interface vlan 777
```

- f. 创建 vfabric 并激活分区集。

```
FCF(config)# vfabric 2
FCF(conf-vfabric-2)# vlan 777
```



```
FCF(config-vfabric-2)# fcoe fcmap 0xEFC00
FCF(config-vfabric-2)# zoneset activate zonesetA
```

g. 启用 DCBX。

```
FCF(config)# dcbx enable
```

h. 创建类别映射和策略映射。

```
FCF(config)# class-map type network-qos c3
FCF(config-cmap-nqos)# match qos-group 3
```

```
FCF(config)# class-map type queuing q0
FCF(config-cmap-queuing)# match queue 0
FCF(config-cmap-queuing)# exit
FCF(config)# class-map type queuing q3
FCF(config-cmap-queuing)# match queue 3
FCF(config-cmap-queuing)# exit
```

```
FCF(config)# policy-map type network-qos nqpolicy
FCF(config-pmap-network-qos)# class c3
FCF(config-pmap-c-nqos)# pause
FCF(config-pmap-c-nqos)# pfc-cos 3
```

```
FCF(config)# policy-map type queuing ets_policy
FCF(config-pmap-queuing)# class q0
FCF(config-pmap-c-que)# bandwidth percent 30
FCF(config-pmap-c-que)# class q3
FCF(config-pmap-c-que)# bandwidth percent 70
```

i. 创建 qos 映射。

```
FCF(config)# qos-map traffic-class tc-q-map1
FCF(config-qos-map)# queue 3 qos-group 3
FCF(config-qos-map)# queue 0 qos-group 0-2,4-7
```

j. 在 FSB2 和目标连接的接口上应用 vfabric。

```
FCF(config)# interface ethernet 1/1/13
FCF(config-if-eth1/1/13)# no shutdown
FCF(config-if-eth1/1/13)# switchport access vlan 1
FCF(config-if-eth1/1/13)# vfabric 2
```

```
FCF(config)# interface fibrechannel 1/1/3
FCF(config-if-fc1/1/3)# description target_connected_port
FCF(config-if-fc1/1/3)# no shutdown
FCF(config-if-fc1/1/3)# vfabric 2
```

k. 在连接到 FSB2 的接口上应用 QoS 配置。

```
FCF(config)# interface ethernet 1/1/13
FCF(config-if-eth1/1/13)# priority-flow-control mode on
FCF(config-if-eth1/1/13)# ets mode on
FCF(config-if-eth1/1/13)# trust-map dot1p default
FCF(config-if-eth1/1/13)# qos-map traffic-class tc-q-map1
FCF(config-if-eth1/1/13)# service-policy input type network-qos nqpolicy
FCF(config-if-eth1/1/13)# service-policy output type queuing ets_policy
```

## 验证多跳 FSB 配置

通过运行以下 show 命令验证配置：

- 要验证 FSB 模式和 CVL 状态，请使用 show fcoe system 命令。

```
FSB1# show fcoe system
Mode : FSB
CVL Status : Enabled
```

```

FCOE VLAN List (Operational) : 777
FCFs : 1
Enodes : 2
Sessions : 2

```

- 要验证已查找到的 ENode，请使用 `show fcoe enode` 命令。

```

FSB1# show fcoe enode
Enode MAC Enode Interface VLAN FCFs Sessions

32:03:cf:45:00:00 Eth 1/1/31 777 1 1
f4:e9:d4:f9:fc:40 Eth 1/1/5 777 1 1

```

- 要验证已查找到的 FCF，请使用 `show fcoe fcf` 命令。

```

FSB1# show fcoe fcf
FCF MAC FCF Interface VLAN FC-MAP FKA_ADV_PERIOD No.
of Enodes FCF Mode

14:18:77:20:86:ce Eth 1/1/2 777 0e:fc:00 8000
2 F

```

```

FSB2# show fcoe fcf
FCF MAC FCF Interface VLAN FC-MAP FKA_ADV_PERIOD No.
of Enodes FCF Mode

14:18:77:20:86:ce Eth 1/1/13 777 0e:fc:00 8000
0 FT

```

- 要验证 FCoE 会话的列表，请使用 `show fcoe sessions` 命令。

```

FSB1# show fcoe sessions
Enode MAC Enode Interface FCF MAC FCF interface VLAN FCoE
MAC FC-ID PORT WWPNN
PORT WNNN

32:03:cf:45:00:00 Eth 1/1/31 14:18:77:20:86:ce Eth 1/1/2 777
0e:fc:00:05:00:05 05:00:05 33:00:55:2c:cf:55:00:00
23:00:55:2c:cf:55:00:00
f4:e9:d4:f9:fc:40 Eth 1/1/5 14:18:77:20:86:ce Eth 1/1/2 777
0e:fc:00:02:01:00 02:01:00 20:01:f4:e9:d4:a4:7d:c3
20:00:f4:e9:d4:a4:7d:c3

```

- 要验证 FCF 上的名称服务器条目，请使用 `show fc ns switch brief` 命令。

```

FCF# show fc ns switch brief
Total number of devices = 3

Intf# Domain FC-ID Enode-WWPN Enode-WWNN

fibrechannel1/1/3 2 02:00:00 21:00:00:24:ff:7c:ae:0e
20:04:00:11:0d:64:67:00
ethernet1/1/13 2 02:01:00 20:01:f4:e9:d4:a4:7d:c3
23:00:55:2c:cf:55:00:00

```

- 要验证 FCF 上的活动分区集，请使用 `show fc zoneset active` 命令。

```

FCF# show fc zoneset active

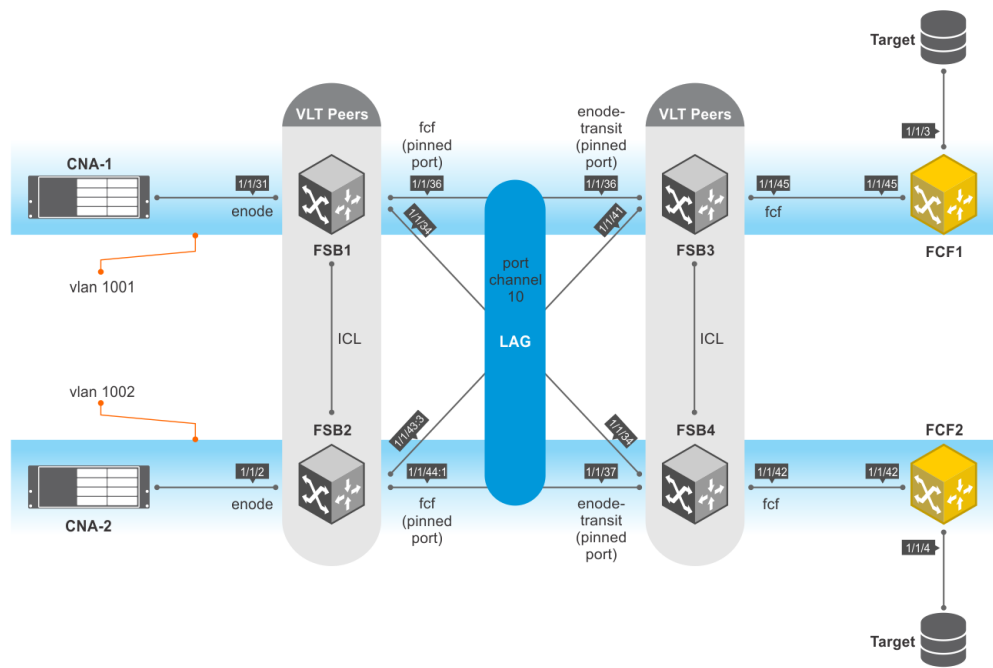
vFabric id: 2
Active Zoneset: zonesetA
ZoneName ZoneMember
=====
zoneA
20:01:f4:e9:d4:a4:7d:c3

21:00:00:24:ff:7c:ae:0e

```

多跳 FSB 配置示例

以下是多跳 FSB 拓扑示例。



在此拓扑中：

- FSB1 和 FSB2 — 访问 FSB。
- FSB3 和 FSB4 — 核心 FSB。
- 在 FSB1 和 FSB2 之间配置 VLT，并且在访问 FSB 与核心 FSB 之间配置的 VLT 端口通道需要端口固定。端口模式如下：
  - 直接连接的 CNA 端口 — ENode
  - 连接到 FSB3 和 FSB4 的端口 — FCF
- 在 FSB3 和 FSB4 之间配置 VLT，并且在访问 FSB 与核心 FSB 之间配置的 VLT 端口通道需要端口固定。端口模式如下：
  - 连接到 FSB1 和 FSB2 的端口 — ENode 传输
  - 连接到 FCF 的端口，用于固定以在 ENode 端口上工作 — FCF

下表列出了 FSB1、FSB3 和 FCF1 上的高级别配置。这些配置分别适用于 FSB2、FSB4 和 FCF2。

表. 29: FSB1、FSB3 和 FCF1 上的高级配置

| FSB1/FSB2                                                                                                                                                                                                                                                                                                                                                                               | FSB3/FSB4                                                                                                                                                                                                                                                                                                                                                                                  | FCF1/FCF2                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>1. 启用 FIP 侦听。</div> <div>2. 启用 DCBX。</div> <div>3. 创建 FCoE VLAN 并配置 FIP 侦听。</div> <div>4. 创建类别映射。</div> <div>5. 创建策略映射。</div> <div>6. 创建 qos 映射。</div> <div>7. 配置端口通道。</div> <div>8. 配置 VLTi 接口成员链路。</div> <div>9. 配置 VLT 域。</div> <div>10. 配置 VLAN。</div> <div>11. 在上行链路 (FSB3/FSB4) 和下行链路接口 (CNA-1/CNA-2) 上应用 QoS 配置。将上行链路接口配置为固定端口。</div> <div>12. 在上行链路接口上配置 FIP 侦听端口模式。</div> | <div>1. 启用 FIP 侦听。</div> <div>2. 启用 DCBX。</div> <div>3. 创建 FCoE VLAN 并配置 FIP 侦听。</div> <div>4. 创建类别映射。</div> <div>5. 创建策略映射。</div> <div>6. 创建 qos 映射。</div> <div>7. 配置端口通道。</div> <div>8. 配置 VLTi 接口成员链路。</div> <div>9. 配置 VLT 域。</div> <div>10. 配置 VLAN。</div> <div>11. 在上行链路 (FCF1/FCF2) 和下行链路接口 (FSB1/FSB2) 上应用 QoS 配置。将下行链路接口配置为固定端口。</div> <div>12. 在上行链路接口和端口通道上配置 FIP 侦听端口模式。</div> | <div>1. 在全局范围内启用光纤通道 F 端口模式。</div> <div>2. 创建分区。</div> <div>3. 创建分区集。</div> <div>4. 创建 vfabric VLAN。</div> <div>5. 创建 vfabric 并激活分区集。</div> <div>6. 启用 DCBX。</div> <div>7. 创建类别映射。</div> <div>8. 创建策略映射。</div> <div>9. 创建 qos 映射。</div> <div>10. 在下行链路接口上应用 QoS 配置 (FSB3/FSB4)。</div> <div>11. 在下行链路和上行链路 (目标连接) 接口上应用 vfabric。</div> |

## FSB1 配置

### 1. 启用 FIP 侦听。

```
FSB1(config)# feature fip-snooping with-cvl
```

### 2. 启用 DCBX。

```
FSB1(config)# dcbx enable
```

### 3. 创建 FCoE VLAN 并配置 FIP 侦听。

```
FSB1(config)#interface vlan1001
FSB1(config-if-vl-1001)# fip-snooping enable
FSB1(config-if-vl-1001)# no shutdown
```

```
FSB1(config)#interface vlan1002
FSB1(config-if-vl-1002)# fip-snooping enable
FSB1(config-if-vl-1002)# no shutdown
```

### 4. 创建类别映射。

```
FSB1(config)# class-map type network-qos c3
FSB1(config-cmap-nqos)# match qos-group 3
```

```
FSB1(config)# class-map type queuing q0
FSB1(config-cmap-queuing)# match queue 0
FSB1(config-cmap-queuing)# exit
FSB1(config)# class-map type queuing q3
FSB1(config-cmap-queuing)# match queue 3
FSB1(config-cmap-queuing)# exit
```

### 5. 创建策略映射。

```
FSB1(config)# policy-map type network-qos nqpolicy
FSB1(config-pmap-network-qos)# class c3
FSB1(config-pmap-c-nqos)# pause
FSB1(config-pmap-c-nqos)# pfc-cos 3
```

```
FSB1(config)# policy-map type queuing ets_policy
FSB1(config-pmap-queuing)# class q0
FSB1(config-pmap-c-que)# bandwidth percent 30
FSB1(config-pmap-c-que)# class q3
FSB1(config-pmap-c-que)# bandwidth percent 70
```

### 6. 创建 qos 映射。

```
FSB1(config)# qos-map traffic-class tc-q-map1
FSB1(config-qos-map)# queue 3 qos-group 3
FSB1(config-qos-map)# queue 0 qos-group 0-2,4-7
```

### 7. 配置端口通道。

```
FSB1(config)# interface port-channel 10
FSB1(config-if-po-10)# no shutdown
FSB1(config-if-po-10)# vlt-port-channel 1
```

## 8. 配置 VLTi 接口成员链路。

```
FSB1(config)# interface ethernet1/1/32
FSB1(conf-if-eth1/1/32)# no shutdown
FSB1(conf-if-eth1/1/32)# no switchport
```

```
FSB1(config)# interface ethernet1/1/33
FSB1(conf-if-eth1/1/33)# no shutdown
FSB1(conf-if-eth1/1/33)# no switchport
```

```
FSB1(config)# interface ethernet1/1/34
FSB1(conf-if-eth1/1/34)# no shutdown
FSB1(conf-if-eth1/1/34)# no switchport
FSB1(conf-if-eth1/1/34)# channel-group 10
```

```
FSB1(config)# interface ethernet 1/1/36
FSB1(conf-if-eth1/1/36)# no shutdown
FSB1(conf-if-eth1/1/36)# no switchport
FSB1(conf-if-eth1/1/36)# channel-group 10
```

## 9. 配置 VLT 域。

```
FSB1(config)# vlt-domain 2
FSB1(conf-vlt-2)# discovery-interface ethernet1/1/32-1/1/33
FSB1(conf-vlt-2)# vlt-mac 1a:2b:3c:0a:0b:0c
```

## 10. 在 FSB1 上配置 VLAN。

```
FSB1(config)# interface ethernet 1/1/31
FSB1(conf-if-eth1/1/31)# no shutdown
FSB1(conf-if-eth1/1/31)# switchport mode trunk
FSB1(conf-if-eth1/1/31)# switchport access vlan 1
FSB1(conf-if-eth1/1/31)# switchport trunk allowed vlan 1001
```

```
FSB1(config)# interface port-channel 10
FSB1(conf-if-po-10)# switchport mode trunk
FSB1(conf-if-po-10)# switchport access vlan 1
FSB1(conf-if-po-10)# switchport trunk allowed vlan 1001-1002
```

## 11. 在连接到 FSB2 和 CNA-1 的接口上应用 QoS 配置。将连接到 FSB2 的接口配置为固定端口。

```
FSB1(config)# interface ethernet 1/1/36
FSB1(conf-if-eth1/1/36)# flowcontrol receive off
FSB1(conf-if-eth1/1/36)# priority-flow-control mode on
FSB1(conf-if-eth1/1/36)# ets mode on
FSB1(conf-if-eth1/1/36)# trust-map dot1p default
FSB1(conf-if-eth1/1/36)# qos-map traffic-class tc-q-map1
FSB1(conf-if-eth1/1/36)# service-policy input type network-qos nqpolicy
FSB1(conf-if-eth1/1/36)# service-policy output type queuing ets_policy
FSB1(conf-if-eth1/1/36)# fcqe-pinned-port
```

```
FSB1(config)# interface ethernet 1/1/31
FSB1(conf-if-eth1/1/31)# flowcontrol receive off
FSB1(conf-if-eth1/1/31)# priority-flow-control mode on
FSB1(conf-if-eth1/1/31)# ets mode on
FSB1(conf-if-eth1/1/31)# trust-map dot1p default
FSB1(conf-if-eth1/1/31)# qos-map traffic-class tc-q-map1
FSB1(conf-if-eth1/1/31)# service-policy input type network-qos nqpolicy
FSB1(conf-if-eth1/1/31)# service-policy output type queuing ets_policy
```

## 12. 在端口通道接口上配置 FIP 侦听端口模式。默认端口模式为 ENode。因此，连接到 CNA-1 的接口不需要其他配置。

```
FSB1(config)# interface port-channel 10
FSB1(conf-if-po-10)# fip-snooping port-mode fcf
```

## FSB2 配置

### 1. 启用 FIP 侦听。

```
FSB2(config)# feature fip-snooping with-cvl
```

### 2. 启用 DCBX。

```
FSB2(config)# dcbx enable
```

### 3. 创建 FCoE VLAN 并配置 FIP 侦听。

```
FSB2(config)#interface vlan1001
FSB2(conf-if-vl-1001)# fip-snooping enable
FSB2(conf-if-vl-1001)# no shutdown
```

```
FSB2(config)#interface vlan1002
FSB2(conf-if-vl-1002)# fip-snooping enable
FSB2(conf-if-vl-1002)# no shutdown
```

### 4. 创建类别映射。

```
FSB2(config)# class-map type network-qos c3
FSB2(config-cmap-nqos)# match qos-group 3
```

```
FSB2(config)# class-map type queuing q0
FSB2(config-cmap-queuing)# match queue 0
FSB2(config-cmap-queuing)# exit
FSB2(config)# class-map type queuing q3
FSB2(config-cmap-queuing)# match queue 3
FSB2(config-cmap-queuing)# exit
```

### 5. 创建策略映射。

```
FSB2(config)# policy-map type network-qos nqpolicy
FSB2(config-pmap-network-qos)# class c3
FSB2(config-pmap-c-nqos)# pause
FSB2(config-pmap-c-nqos)# pfc-cos 3
```

```
FSB2(config)# policy-map type queuing ets_policy
FSB2(config-pmap-queuing)# class q0
FSB2(config-pmap-c-que)# bandwidth percent 30
FSB2(config-pmap-c-que)# class q3
FSB2(config-pmap-c-que)# bandwidth percent 70
```

### 6. 创建 qos 映射。

```
FSB2(config)# qos-map traffic-class tc-q-map1
FSB2(config-qos-map)# queue 3 qos-group 3
FSB2(config-qos-map)# queue 0 qos-group 0-2,4-7
```

### 7. 配置端口通道。

```
FSB2(config)# interface port-channel 10
FSB2(conf-if-po-10)# no shutdown
FSB2(conf-if-po-10)# vlt-port-channel 1
```

## 8. 配置 VLTi 接口成员链路。

```
FSB2(config)# interface ethernet1/1/43:1
FSB2(config-if-eth1/1/43:1)# no shutdown
FSB2(config-if-eth1/1/43:1)# no switchport
```

```
FSB2(config)# interface ethernet1/1/43:2
FSB2(config-if-eth1/1/43:2)# no shutdown
FSB2(config-if-eth1/1/43:2)# no switchport
```

```
FSB2(config)# interface ethernet 1/1/43:3
FSB2(config-if-eth1/1/43:3)# no shutdown
FSB2(config-if-eth1/1/43:3)# no switchport
FSB2(config-if-eth1/1/43:3)# channel-group 10
```

```
FSB2(config)# interface ethernet1/1/44:1
FSB2(config-if-eth1/1/44:1)# no shutdown
FSB2(config-if-eth1/1/44:1)# no switchport
FSB2(config-if-eth1/1/44:1)# channel-group 10
```

## 9. 配置 VLT 域。

```
FSB2(config)# vlt-domain 2
FSB2(config-vlt-2)# discovery-interface ethernet1/1/43:1-1/1/43:2
FSB2(config-vlt-2)# vlt-mac 1a:2b:3c:0a:0b:0c
```

## 10. 在 FSB2 上配置 VLAN。

```
FSB2(config)# interface ethernet 1/1/2
FSB2(config-if-eth1/1/2)# no shutdown
FSB2(config-if-eth1/1/2)# switchport mode trunk
FSB2(config-if-eth1/1/2)# switchport access vlan 1
FSB2(config-if-eth1/1/2)# switchport trunk allowed vlan 1002
```

```
FSB2(config)# interface port-channel 10
FSB2(config-if-po-10)# switchport mode trunk
FSB2(config-if-po-10)# switchport access vlan 1
FSB2(config-if-po-10)# switchport trunk allowed vlan 1001-1002
```

## 11. 在连接到 FSB4 和 CNA-2 的接口上应用 QoS 配置。将连接到 FSB4 的接口配置为固定端口。

```
FSB2(config)# interface ethernet 1/1/44:1
FSB2(config-if-eth1/1/44:1)# flowcontrol receive off
FSB2(config-if-eth1/1/44:1)# priority-flow-control mode on
FSB2(config-if-eth1/1/44:1)# ets mode on
FSB2(config-if-eth1/1/44:1)# trust-map dot1p default
FSB2(config-if-eth1/1/44:1)# qos-map traffic-class tc-q-map1
FSB2(config-if-eth1/1/44:1)# service-policy input type network-qos nqpolicy
FSB2(config-if-eth1/1/44:1)# service-policy output type queuing ets_policy
FSB2(config-if-eth1/1/44:1)# fcoe-pinned-port
```

```
FSB2(config)# interface ethernet 1/1/2
FSB2(config-if-eth1/1/2)# flowcontrol receive off
FSB2(config-if-eth1/1/2)# priority-flow-control mode on
FSB2(config-if-eth1/1/2)# ets mode on
FSB2(config-if-eth1/1/2)# trust-map dot1p default
FSB2(config-if-eth1/1/2)# qos-map traffic-class tc-q-map1
FSB2(config-if-eth1/1/2)# service-policy input type network-qos nqpolicy
FSB2(config-if-eth1/1/2)# service-policy output type queuing ets_policy
```

## 12. 在端口通道接口上配置 FIP 侦听端口模式。默认端口模式为 ENode。因此，连接到 CNA-2 的接口不需要其他配置。

```
FSB2(config)# interface port-channel 10
FSB2(config-if-po-10)# fip-snooping port-mode fcf
```

## FSB3 配置

### 1. 启用 FIP 侦听。

```
FSB3(config)# feature fip-snooping with-cvl
```

### 2. 启用 DCBX。

```
FSB3(config)# dcbx enable
```

### 3. 创建 FCoE VLAN 并配置 FIP 侦听。

```
FSB3(config)#interface vlan1001
FSB3(conf-if-vl-1001)# fip-snooping enable
FSB3(conf-if-vl-1001)# no shutdown
```

```
FSB3(config)#interface vlan1002
FSB3(conf-if-vl-1002)# fip-snooping enable
FSB3(conf-if-vl-1002)# no shutdown
```

### 4. 创建类别映射。

```
FSB3(config)# class-map type network-qos c3
FSB3(config-cmap-nqos)# match qos-group 3
```

```
FSB3(config)# class-map type queuing q0
FSB3(config-cmap-queuing)# match queue 0
FSB3(config-cmap-queuing)# exit
FSB3(config)# class-map type queuing q3
FSB3(config-cmap-queuing)# match queue 3
FSB3(config-cmap-queuing)# exit
```

### 5. 创建策略映射。

```
FSB3(config)# policy-map type network-qos nqpolicy
FSB3(config-pmap-network-qos)# class c3
FSB3(config-pmap-c-nqos)# pause
FSB3(config-pmap-c-nqos)# pfc-cos 3
```

```
FSB3(config)# policy-map type queuing ets_policy
FSB3(config-pmap-queuing)# class q0
FSB3(config-pmap-c-que)# bandwidth percent 30
FSB3(config-pmap-c-que)# class q3
FSB3(config-pmap-c-que)# bandwidth percent 70
```

### 6. 创建 qos 映射。

```
FSB3(config)# qos-map traffic-class tc-q-map1
FSB3(config-qos-map)# queue 3 qos-group 3
FSB3(config-qos-map)# queue 0 qos-group 0-2,4-7
```

### 7. 配置端口通道。

```
FSB3(config)# interface port-channel 10
FSB3(conf-if-po-10)# no shutdown
FSB3(conf-if-po-10)# vlt-port-channel 1
```



## 8. 配置 VLTi 接口成员链路。

```
FSB3(config)# interface ethernet1/1/39
FSB3(config-if-eth1/1/39)# no shutdown
FSB3(config-if-eth1/1/39)# no switchport
```

```
FSB3(config)# interface ethernet1/1/40
FSB3(config-if-eth1/1/40)# no shutdown
FSB3(config-if-eth1/1/40)# no switchport
```

```
FSB3(config)# interface ethernet1/1/41
FSB3(config-if-eth1/1/41)# no shutdown
FSB3(config-if-eth1/1/41)# no switchport
FSB3(config-if-eth1/1/41)# channel-group 10
```

```
FSB3(config)# interface ethernet 1/1/36
FSB3(config-if-eth1/1/36)# no shutdown
FSB3(config-if-eth1/1/36)# no switchport
FSB3(config-if-eth1/1/36)# channel-group 10
```

## 9. 配置 VLT 域。

```
FSB3(config)# vlt-domain 3
FSB3(config-vlt-3)# discovery-interface ethernet1/1/39-1/1/40
FSB3(config-vlt-3)# vlt-mac 1a:2b:3c:2a:1b:1c
```

## 10. 在 FSB3 上配置 VLAN。

```
FSB3(config)# interface ethernet 1/1/45
FSB3(config-if-eth1/1/45)# no shutdown
FSB3(config-if-eth1/1/45)# switchport mode trunk
FSB3(config-if-eth1/1/45)# switchport access vlan 1
FSB3(config-if-eth1/1/45)# switchport trunk allowed vlan 1001
```

```
FSB3(config)# interface port-channel 10
FSB3(config-if-po-10)# switchport mode trunk
FSB3(config-if-po-10)# switchport access vlan 1
FSB3(config-if-po-10)# switchport trunk allowed vlan 1001-1002
```

## 11. 在连接到 FCF1 和 FSB1 的接口上应用 QoS 配置。将连接到 FSB1 的接口配置为固定端口。

```
FSB3(config)# interface ethernet 1/1/45
FSB3(config-if-eth1/1/45)# flowcontrol receive off
FSB3(config-if-eth1/1/45)# priority-flow-control mode on
FSB3(config-if-eth1/1/45)# ets mode on
FSB3(config-if-eth1/1/45)# trust-map dot1p default
FSB3(config-if-eth1/1/45)# qos-map traffic-class tc-q-map1
FSB3(config-if-eth1/1/45)# service-policy input type network-qos nqpolicy
FSB3(config-if-eth1/1/45)# service-policy output type queuing ets_policy
```

```
FSB3(config)# interface ethernet 1/1/36
FSB3(config-if-eth1/1/36)# flowcontrol receive off
FSB3(config-if-eth1/1/36)# priority-flow-control mode on
FSB3(config-if-eth1/1/36)# ets mode on
FSB3(config-if-eth1/1/36)# trust-map dot1p default
FSB3(config-if-eth1/1/36)# qos-map traffic-class tc-q-map1
FSB3(config-if-eth1/1/36)# service-policy input type network-qos nqpolicy
FSB3(config-if-eth1/1/36)# service-policy output type queuing ets_policy
FSB3(config-if-eth1/1/36)# fcoe-pinned-port
```

## 12. 在端口通道和连接到 FCF1 的接口上配置 FIP 侦听端口模式。

```
FSB3(config)# interface port-channel 10
FSB3(config-if-po-10)# fip-snooping port-mode enode-transit
```

```
FSB3(config)# interface ethernet 1/1/45
FSB3(config-if-eth1/1/45)# fip-snooping port-mode fcf
```

## FSB4 配置

### 1. 启用 FIP 侦听。

```
FSB4(config)# feature fip-snooping with-cvl
```

### 2. 启用 DCBX。

```
FSB4(config)# dcbx enable
```

### 3. 创建 FCoE VLAN 并配置 FIP 侦听。

```
FSB4(config)#interface vlan1001
FSB4(config-if-vl-1001)# fip-snooping enable
FSB4(config-if-vl-1001)# no shutdown
```

```
FSB4(config)#interface vlan1002
FSB4(config-if-vl-1002)# fip-snooping enable
FSB4(config-if-vl-1002)# no shutdown
```

### 4. 创建类别映射。

```
FSB4(config)# class-map type network-qos c3
FSB4(config-cmap-nqos)# match qos-group 3
```

```
FSB4(config)# class-map type queuing q0
FSB4(config-cmap-queuing)# match queue 0
FSB4(config-cmap-queuing)# exit
FSB4(config)# class-map type queuing q3
FSB4(config-cmap-queuing)# match queue 3
FSB4(config-cmap-queuing)# exit
```

### 5. 创建策略映射。

```
FSB4(config)# policy-map type network-qos nqpolicy
FSB4(config-pmap-network-qos)# class c3
FSB4(config-pmap-c-nqos)# pause
FSB4(config-pmap-c-nqos)# pfc-cos 3
```

```
FSB4(config)# policy-map type queuing ets_policy
FSB4(config-pmap-queuing)# class q0
FSB4(config-pmap-c-que)# bandwidth percent 30
FSB4(config-pmap-c-que)# class q3
FSB4(config-pmap-c-que)# bandwidth percent 70
```

### 6. 创建 qos 映射。

```
FSB4(config)# qos-map traffic-class tc-q-map1
FSB4(config-qos-map)# queue 3 qos-group 3
FSB4(config-qos-map)# queue 0 qos-group 0-2,4-7
```

### 7. 配置端口通道。

```
FSB4(config)# interface port-channel 10
FSB4(config-if-po-10)# no shutdown
FSB4(config-if-po-10)# vlt-port-channel 1
```

### 8. 配置 VLTi 接口成员链路。

```
FSB4(config)# interface ethernet1/1/34
FSB4(config-if-eth1/1/34)# no shutdown
FSB4(config-if-eth1/1/34)# no switchport
FSB4(config-if-eth1/1/34)# channel-group 10
```

```
FSB4(config)# interface ethernet1/1/37
FSB4(config-if-eth1/1/37)# no shutdown
```

```
FSB4(config-if-eth1/1/37)# no switchport
FSB4(config-if-eth1/1/37)# channel-group 10
```

## 9. 配置 VLT 域。

```
FSB4(config)# vlt-domain 3
FSB4(config-vlt-2)# discovery-interface ethernet1/1/40
FSB4(config-vlt-2)# vlt-mac 1a:2b:3c:2a:1b:1c
```

## 10. 在 FSB4 上配置 VLAN。

```
FSB4(config)# interface ethernet 1/1/42
FSB4(config-if-eth1/1/42)# no shutdown
FSB4(config-if-eth1/1/42)# switchport mode trunk
FSB4(config-if-eth1/1/42)# switchport access vlan 1
FSB4(config-if-eth1/1/42)# switchport trunk allowed vlan 1002
```

```
FSB4(config)# interface port-channel 10
FSB4(config-if-po-10)# switchport mode trunk
FSB4(config-if-po-10)# switchport access vlan 1
FSB4(config-if-po-10)# switchport trunk allowed vlan 1001-1002
```

## 11. 在连接到 FCF2 的接口上应用 QoS 配置。

```
FSB4(config)# interface ethernet 1/1/42
FSB4(config-if-eth1/1/42)# flowcontrol receive off
FSB4(config-if-eth1/1/42)# priority-flow-control mode on
FSB4(config-if-eth1/1/42)# ets mode on
FSB4(config-if-eth1/1/42)# trust-map dot1p default
FSB4(config-if-eth1/1/42)# qos-map traffic-class tc-q-map1
FSB4(config-if-eth1/1/42)# service-policy input type network-qos nqpolicy
FSB4(config-if-eth1/1/42)# service-policy output type queuing ets_policy
```

## 12. 在端口通道和连接到 FCF2 的接口上配置 FIP 侦听端口模式。将连接到 FSB2 的接口配置为固定端口。

```
FSB4(config)# interface port-channel 10
FSB4(config-if-po-10)# fip-snooping port-mode enode-transit
```

```
FSB4(config)# interface ethernet 1/1/42
FSB4(config-if-eth1/1/42)# fip-snooping port-mode fcf
```

```
FSB4(config)# interface ethernet 1/1/37
FSB4(config-if-eth1/1/37)# fcoe-pinned-port
```

## FCF1 配置

### 1. 在全局范围内启用光纤通道 F 端口模式。

```
FCF1(config)# feature fc domain-id 2
```

### 2. 创建分区。

```
FCF1(config)# fc zone zoneA
FCF1(config-fc-zone-zoneA)# member wwn 23:05:22:11:0d:64:67:11
FCF1(config-fc-zone-zoneA)# member wwn 50:00:d3:10:00:ec:f9:00
```

### 3. 创建分区集。

```
FCF1(config)# fc zoneset zonesetA
FCF1(config-fc-zoneset-setA)# member zoneA
```

### 4. 创建 vfabric VLAN。

```
FCF1(config)# interface vlan 1001
```

## 5. 创建 vfabric 并激活分区集。

```
FCF1(config)# vfabric 1
FCF1(conf-vfabric-1)# vlan 1001
FCF1(conf-vfabric-1)# fcoe fcmap 0xEFC00
FCF1(conf-vfabric-1)# zoneset activate zonesetA
```

## 6. 启用 DCBX。

```
FCF1(config)# dcbx enable
```

## 7. 创建类别映射。

```
FCF1(config)# class-map type network-qos c3
FCF1(config-cmap-nqos)# match qos-group 3
```

```
FCF1(config)# class-map type queuing q0
FCF1(config-cmap-queuing)# match queue 0
FCF1(config-cmap-queuing)# exit
FCF1(config)# class-map type queuing q3
FCF1(config-cmap-queuing)# match queue 3
FCF1(config-cmap-queuing)# exit
```

## 8. 创建策略映射。

```
FCF1(config)# policy-map type network-qos nqpolicy
FCF1(config-pmap-network-qos)# class c3
FCF1(config-pmap-c-nqos)# pause
FCF1(config-pmap-c-nqos)# pfc-cos 3
```

```
FCF1(config)# policy-map type queuing ets_policy
FCF1(config-pmap-queuing)# class q0
FCF1(config-pmap-c-que)# bandwidth percent 30
FCF1(config-pmap-c-que)# class q3
FCF1(config-pmap-c-que)# bandwidth percent 70
```

## 9. 创建 qos 映射。

```
FCF1(config)# qos-map traffic-class tc-q-map1
FCF1(config-qos-map)# queue 3 qos-group 3
FCF1(config-qos-map)# queue 0 qos-group 0-2,4-7
```

## 10. 在连接到 FSB3 的接口上应用 QoS 配置。

```
FCF1(config)# interface ethernet 1/1/45
FCF1(conf-if-eth1/1/45)# no shutdown
FCF1(conf-if-eth1/1/45)# flowcontrol receive off
FCF1(conf-if-eth1/1/45)# priority-flow-control mode on
FCF1(conf-if-eth1/1/45)# ets mode on
FCF1(conf-if-eth1/1/45)# trust-map dot1p default
FCF1(conf-if-eth1/1/45)# qos-map traffic-class tc-q-map1
FCF1(conf-if-eth1/1/45)# service-policy input type network-qos nqpolicy
FCF1(conf-if-eth1/1/45)# service-policy output type queuing ets_policy
```

## 11. 在连接到 FSB3 的接口和目标上应用 vfabric。

```
FCF1(config)# interface ethernet 1/1/45
FCF1(conf-if-eth1/1/45)# switchport access vlan 1
FCF1(conf-if-eth1/1/45)# vfabric 1
```

```
FCF1(config)# interface fibrechannel 1/1/3
FCF1(conf-if-fc1/1/3)# description target_connected_port
FCF1(conf-if-fc1/1/3)# no shutdown
FCF1(conf-if-fc1/1/3)# vfabric 1
```

## FCF2 配置

1. 在全局范围内启用光纤通道 F 端口模式。

```
FCF2(config)# feature fc domain-id 3
```

2. 创建分区。

```
FCF2(config)# fc zone zoneB
FCF2(config-fc-zone-zoneB)# member wwn 20:01:00:0e:1e:f1:f1:84
FCF2(config-fc-zone-zoneB)# member wwn 53:00:a3:10:00:ec:f9:01
```

3. 创建分区集。

```
FCF2(config)# fc zoneset zonesetB
FCF2(config-fc-zoneset-setB)# member zoneB
```

4. 创建 vfabric VLAN。

```
FCF2(config)# interface vlan 1002
```

5. 创建 vfabric 并激活分区集。

```
FCF2(config)# vfabric 2
FCF2(config-vfabric-2)# vlan 1002
FCF2(config-vfabric-2)# fcoe fcmap 0xEFC00
FCF2(config-vfabric-2)# zoneset activate zonesetB
```

6. 启用 DCBX。

```
FCF2(config)# dcbx enable
```

7. 创建类别映射。

```
FCF2(config)# class-map type network-qos c3
FCF2(config-cmap-nqos)# match qos-group 3
```

```
FCF2(config)# class-map type queuing q0
FCF2(config-cmap-queuing)# match queue 0
FCF2(config-cmap-queuing)# exit
FCF2(config)# class-map type queuing q3
FCF2(config-cmap-queuing)# match queue 3
FCF2(config-cmap-queuing)# exit
```

8. 创建策略映射。

```
FCF2(config)# policy-map type network-qos nqpolicy
FCF2(config-pmap-network-qos)# class c3
FCF2(config-pmap-c-nqos)# pause
FCF2(config-pmap-c-nqos)# pfc-cos 3
```

```
FCF2(config)# policy-map type queuing ets_policy
FCF2(config-pmap-queuing)# class q0
FCF2(config-pmap-c-que)# bandwidth percent 30
FCF2(config-pmap-c-que)# class q3
FCF2(config-pmap-c-que)# bandwidth percent 70
```

9. 创建 qos 映射。

```
FCF2(config)# qos-map traffic-class tc-q-map1
FCF2(config-qos-map)# queue 3 qos-group 3
FCF2(config-qos-map)# queue 0 qos-group 0-2,4-7
```

10. 在连接到 FSB4 的接口上应用 QoS 配置。

```
FCF2(config)# interface ethernet 1/1/42
FCF2(config-if-eth1/1/42)# no shutdown
FCF2(config-if-eth1/1/42)# flowcontrol receive off
FCF2(config-if-eth1/1/42)# priority-flow-control mode on
```

```
FCF2(config-if-eth1/1/42)# ets mode on
FCF2(config-if-eth1/1/42)# trust-map dot1p default
FCF2(config-if-eth1/1/42)# qos-map traffic-class tc-q-map1
FCF2(config-if-eth1/1/42)# service-policy input type network-qos nqpolicy
FCF2(config-if-eth1/1/42)# service-policy output type queuing ets_policy
```

## 11. 在连接到 FSB4 的接口和目标上应用 vfabric。

```
FCF2(config)# interface ethernet 1/1/42
FCF2(config-if-eth1/1/42)# switchport access vlan 1
FCF2(config-if-eth1/1/42)# vfabric 1
```

```
FCF2(config)# interface fibrechannel 1/1/4
FCF2(config-if-fc1/1/4)# description target_connected_port
FCF2(config-if-fc1/1/4)# no shutdown
FCF2(config-if-fc1/1/4)# vfabric 2
```

## 验证配置

您可以使用以下 show 命令验证配置：

### FSB1

```
FSB1# show fcoe sessions
Enode MAC Enode Interface FCF MAC FCF interface VLAN FCoE
MAC FC-ID PORT WWPN
PORT WWNN

f4:e9:d4:f9:fc:42 Eth 1/1/31 14:18:77:20:86:ce Po 10(Eth 1/1/36) 1001
0e:fc:00:02:02:00 02:02:00 23:05:22:11:0d:64:67:11 22:04:22:13:0d:64:67:00
```

```
FSB1# show fcoe fcf
FCF MAC FCF Interface VLAN FC-MAP FKA_ADV_PERIOD No. of
Enodes FCF Mode

14:18:77:20:86:ce Po 10(Eth 1/1/36) 1001 0e:fc:00 8000
1 F
```

```
FSB1# show fcoe system
Mode : FSB
CVL Status : Enabled
FCOE VLAN List (Operational) : 1001,1002
FCFs : 1
Enodes : 1
Sessions : 1
```

### FSB2

```
FSB2# show fcoe sessions
Enode MAC Enode Interface FCF MAC FCF interface VLAN FCoE
MAC FC-ID PORT WWPN PORT WWNN

00:0e:1e:f1:f1:84 Eth 1/1/1 14:18:77:20:80:ce Po 10(Eth 1/1/44:1)1002
0e:fc:00:02:01:00 02:01:00 20:01:00:0e:1e:f1:f1:84 20:00:00:0e:1e:f1:f1:84
```

```
FSB2# show fcoe fcf
FCF MAC FCF Interface VLAN FC-MAP FKA_ADV_PERIOD No. of
Enodes FCF Mode

```

```
14:18:77:20:80:ce Po 10(Eth 1/1/44:1) 1002 0e:fc:00 8000
1 F
```

```
FSB2# show fcoe system
Mode : FSB
CVL Status : Enabled
FCOE VLAN List (Operational) : 1001,1002
FCFs : 1
Enodes : 1
Sessions : 1
```

### FSB3

```
FSB3# show fcoe sessions
Enode MAC Enode Interface FCF MAC FCF interface VLAN FCoE
MAC FC-ID PORT WWPN
PORT WNNN

f4:e9:d4:f9:fc:42 Po 10(Eth 1/1/36) 14:18:77:20:86:ce Eth 1/1/45 1001
0e:fc:00:02:02:00 02:02:00 23:05:22:11:0d:64:67:11 22:04:22:13:0d:64:67:00
```

```
FSB3# show fcoe fcf
FCF MAC FCF Interface VLAN FC-MAP FKA_ADV_PERIOD No. of
Enodes FCF Mode

14:18:77:20:86:ce Eth 1/1/45 1001 0e:fc:00 8000
1 F
```

```
FSB3# show fcoe system
Mode : FSB
CVL Status : Enabled
FCOE VLAN List (Operational) : 1001,1002
FCFs : 1
Enodes : 1
Sessions : 1
```

### FSB4

```
FSB4# show fcoe sessions
Enode MAC Enode Interface FCF MAC FCF interface VLAN
FCoE MAC FC-ID PORT WWPN PORT WNNN

00:0e:1e:f1:f1:84 Po 10(Eth 1/1/37) 14:18:77:20:80:ce Eth 1/1/42 1002
0e:fc:00:02:01:00 02:01:00 20:01:00:0e:1e:f1:f1:84 20:00:00:0e:1e:f1:f1:84
```

```
FSB4# show fcoe fcf
FCF MAC FCF Interface VLAN FC-MAP FKA_ADV_PERIOD No. of
Enodes FCF Mode

14:18:77:20:80:ce Eth 1/1/42 1002 0e:fc:00 8000
1 F
```

```
FSB4# show fcoe system
Mode : FSB
CVL Status : Enabled
FCOE VLAN List (Operational) : 1001,1002
FCFs : 1
Enodes : 1
Sessions : 1
```

FCF1

```
FCF1# show fcoe sessions
Enode MAC Enode Interface FCF MAC FCF interface VLAN FCoE
MAC FC-ID PORT WWPN PORT WWNN

f4:e9:d4:f9:fc:42 Eth 1/1/45 14:18:77:20:86:ce ~ 1001 0e:fc:00:02:02:00
02:02:00 23:05:22:11:0d:64:67:11 22:04:22:13:0d:64:67:00

FCF1# show fc ns switch brief
Total number of devices = 2

Intf# Domain FC-ID Enode-WWPN Enode-WWNN

fibrechannel1/1/3 2 02:00:00 50:00:d3:10:00:ec:f9:00
51:00:d3:10:00:ec:f9:01
ethernet1/1/45 2 02:02:00 23:05:22:11:0d:64:67:11
22:04:22:13:0d:64:67:00
```

FCF2

```
FCF2# show fcoe sessions
Enode MAC Enode Interface FCF MAC FCF interface VLAN FCoE
MAC FC-ID PORT WWPN PORT WWNN

00:0e:1e:f1:f1:84 Eth 1/1/42 14:18:77:20:80:ce ~ 1002 0e:fc:00:02:01:00
02:00:01 20:01:00:0e:1e:f1:f1:84 20:00:00:0e:1e:f1:f1:84

FCF2# show fc ns switch brief
Total number of devices = 2

Intf# Domain FC-ID Enode-WWPN Enode-WWNN

fibrechannel1/1/4 3 02:01:00 53:00:a3:10:00:ec:f9:01
52:00:a3:10:00:ec:f9:00
ethernet1/1/42 3 02:00:01 20:01:00:0e:1e:f1:f1:84
20:00:00:0e:1e:f1:f1:84
```

配置指导准则

配置不同的模式时，例如，F\_Port、NPG 或 FSB，请考虑以下事项：

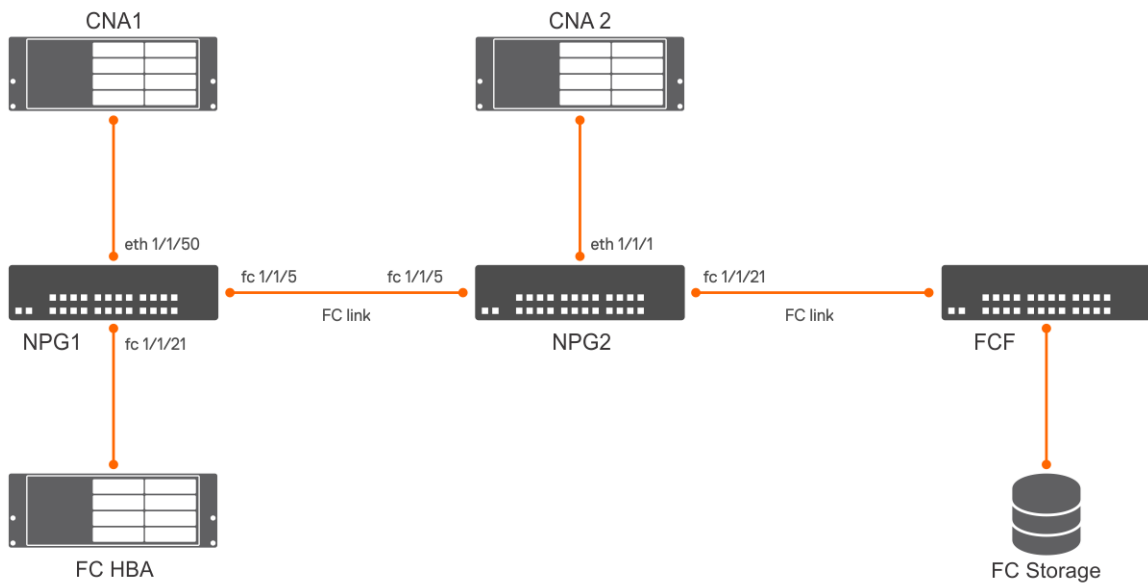
- F\_Port、NPG 和 FSB 模式相互排斥。一次只能启用一种模式。
- 您仅可在启用特定功能后启用模式特定的命令。
- 在禁用 F\_Port 和 NPG 功能之前，请删除模式特定的配置。禁用 FSB 后，系统将自动移除配置。

NPIV 代理网关级联

OS10 支持在聚合网络适配器 (CNA) 或光纤通道主机总线适配器 (FC HBA) 和 FCoE 转发器 (FCF) 交换机之间将两台交换机连接 NPIV 代理网关 (NPIV)。

在下图中，NPG1 和 NPG2 相互连接，可为 CNA1 和 FC HBA1 和 FCF1 交换机提供 FCoE 和 FC 服务。





## NPG1 交换机配置

1. 启用 NPG 功能。

```
OS10(config)# feature fc npg
```

2. 配置 vFabric。

```
OS10(config)# vfabric 2
OS10(conf-vfabric-2)# vlan 1000
OS10(conf-vfabric-2)# name fcoe_fabric
OS10(conf-vfabric-2)# fcoe fcmap 0efc02
```

3. 在连接到 FC HBA 的接口上应用 vFabric 配置并将端口模式更改为 F\_Port。

```
OS10(config)# interface fibrechannel 1/1/21
OS10(conf-if-fc1/1/21)# vfabric 2
```

4. 在连接到 CNA 1 的接口上应用 vFabric 配置。

```
OS10(config)# interface ethernet 1/1/50
OS10(conf-if-eth1/1/50)# vfabric 2
```

5. 全局启用 DCBX。

```
OS10(config)# dcbx enable
```

6. 创建类别映射和策略映射。

```
OS10(config)# class-map type network-qos cmap1
OS10(config-cmap-nqos)# match qos-group 3
OS10(config)# policy-map type network-qos pmap1
OS10(config-pmap-network-qos)# class cmap1
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 3
```

7. 禁用连接到 CNA 1 的接口上的 LLFC。

```
OS10(config)# interface ethernet 1/1/50
OS10(conf-if-eth1/1/50)# no flowcontrol receive
```

8. 在连接到 CNA 1 的接口上启用 PFC 模式。

```
OS10(config)# interface ethernet 1/1/50
OS10(config-if-eth1/1/50)# priority-flow-control mode on
```

9. 在连接到 CNA 1 的接口上应用服务策略。

```
OS10(config)# interface ethernet 1/1/50
OS10(config-if-eth1/1/50)# service-policy input type network-qos pmap1
```

10. 配置连接到 NPG2 的接口。

```
OS10(config)# interface fibrechannel 1/1/5
OS10(config-if-fc1/1/5)# vfabric 2
```

## NPG2 交换机配置

1. 启用 NPG 功能。

```
OS10(config)# feature fc npg
```

2. 配置 vFabric。

```
OS10(config)# vfabric 2
OS10(config-vfabric-2)# vlan 1000
OS10(config-vfabric-2)# name fcoe_fabric
OS10(config-vfabric-2)# fcoe fcmap 0efc02
```

3. 在连接到 NPG1 交换机的接口上应用 vFabric 配置。将端口模式更改为 F\_Port。

```
OS10(config)# interface fibrechannel 1/1/5
OS10(config-if-fc1/1/21)# vfabric 2
OS10(config-if-fc1/1/21)# fc port-mode f
```

4. 在连接到 CNA 2 的接口上应用 vFabric 配置。

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# vfabric 2
```

5. 全局启用 DCBX。

```
OS10(config)# dcbx enable
```

6. 创建类别映射和策略映射。

```
OS10(config)# class-map type network-qos cmap1
OS10(config-cmap-nqos)# match qos-group 3
OS10(config)# policy-map type network-qos pmap1
OS10(config-pmap-network-qos)# class cmap1
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 3
```

7. 禁用连接到 CNA 2 的接口上的 LLFC。

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# no flowcontrol receive
```

8. 在连接到 CNA 2 的接口上启用 PFC 模式。

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# priority-flow-control mode on
```

9. 在连接到 CNA 2 的接口上应用服务策略。

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# service-policy input type network-qos pmap1
```

10. 配置连接到 FCF 的接口。

```
OS10(config)# interface fibrechannel 1/1/21
OS10(config-if-fc1/1/21)# vfabric 2
```

## 在 FCoE 中支持未标记的 VLAN

在 SmartFabric 模式下，OS10 为 FCoE 的以太网上行链路和以太网服务器端口（这是 FCoE VLAN 的一部分）提供 VLAN 支持。

FCoE 上行链路标识交换机上的 FIP 侦听桥 (FSB) 模式。您必须在 FCoE 上行链路和服务端口上配置相同的未标记 VLAN，以便 FCoE 会话启动。

在 SmartFabric 模式下，您可以将任何未标记的 VLAN 分配给属于具有一个或多个 FC 网关上行链路的 FCoE VLAN 的以太网服务器端口。FC 网关上行链路标识交换机上的 N 端口代理网关 (NPG) 模式。此外，您还可以将任何未标记的 VLAN 分配给属于具有一个或多个 FC Direct 连接上行链路的 FCoE VLAN 的以太网服务器端口。FC Direct 连接上行链路标识交换机上的 F 端口模式。

### 限制

- SmartFabric 模式不支持来自同一 IOM 的多个 FCoE 上行链路。
- 在 FCoE 模式下，服务器端口和 FCoE 上行链路上的未标记 VLAN 必须相同。这种情况可确保 L2 框架中未标记的 FIP VLAN 查找数据包，并切换到未标记的 VLAN。
- 您不能配置与不同未标记的 VLAN 对应的多个 FCoE 上行链路。

## F\_Port 命令

在 F\_Port 模式下支持以下命令：

### fc alias

创建 FC 别名。创建别名后，将成员添加到 FC 别名。FC 别名可以具有最多 255 个唯一成员。

**语法** `fc alias alias-name`

**参数** `alias-name` — 输入 FC 别名的名称。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本将删除 FC 别名。要删除 FC 别名，请首先从 FC 分区中将其删除。  
从版本 10.4.1.0 开始，在全交换模式下的 MX9116n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

### 示例

```
OS10(config)# fc alias test
OS10(config-fc-alias-test)# member wwn 21:00:00:24:ff:7b:f5:c9
OS10(config-fc-alias-test)# member wwn 20:25:78:2b:cb:6f:65:57
```

**支持的版本** 10.3.1E or later

### fc zone

创建 FC 分区并将成员添加到分区中。一个 FC 分区最多可以有 255 个唯一成员。

**语法** `fc zone zone-name`

**参数** `zone-name` — 输入分区的名称。

**默认** 未配置

|               |                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>命令模式</b>   | CONFIGURATION                                                                                                                                                     |
| <b>使用情况信息</b> | <p>此命令的 <code>no</code> 版本将删除 FC 分区。要删除 FC 分区，请首先从 FC 分区集中将其移除。</p> <p>从版本 10.4.1.0 开始，在全交换模式下的 MX9116n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p>        |
| <b>示例</b>     | <pre>OS10(config)# fc zone hba1 OS10(config-fc-zone-hba1)# member wwn 10:00:00:90:fa:b8:22:19 OS10(config-fc-zone-hba1)# member wwn 21:00:00:24:ff:7b:f5:c8</pre> |
| <b>支持的版本</b>  | 10.3.1E or later                                                                                                                                                  |

## fc zoneset

创建 FC 分区集，并将现有 FC 分区添加到分区集。

|               |                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>fc zoneset zoneset-name</code>                                                                                             |
| <b>参数</b>     | <code>zoneset-name</code> — 输入 FC 分区集的名称。名称必须以字母开头，并且可以包含以下字符：A-Z、a-z、0-9、\$、_、-、^                                               |
| <b>默认</b>     | 未配置                                                                                                                              |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                    |
| <b>使用情况信息</b> | <p>此命令的 <code>no</code> 版本将移除 FC 分区集。</p> <p>从版本 10.4.1.0 开始，在全交换模式下的 MX9116n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p> |
| <b>示例</b>     | <pre>OS10(config)# fc zoneset set OS10(config-fc-zoneset-set)# member hba1</pre>                                                 |
| <b>支持的版本</b>  | 10.3.1E or later                                                                                                                 |

## feature fc

全局启用 F\_Port。

|               |                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>feature fc domain-id domain-id</code>                                                                                                |
| <b>参数</b>     | <code>domain-id</code> — 输入 F_Port 的域 ID，从 1 到 239。                                                                                        |
| <b>默认</b>     | 已禁用                                                                                                                                        |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                              |
| <b>使用情况信息</b> | <p>此命令的 <code>no</code> 版本会禁用 F_Port。仅当 vfabric 和分区配置不可用时，您才能禁用 F_Port。在禁用 F_Port 之前，请移除 vfabric 和分区配置。您一次只能启用以下选项之一：F_Port、NPG 或 FSB。</p> |
| <b>示例</b>     | <pre>OS10(config)# feature fc domain-id 100</pre>                                                                                          |
| <b>支持的版本</b>  | 10.3.1E or later                                                                                                                           |

## member (别名)

将成员添加到现有 FC 别名。通过 FC 别名、全球通用名称 (WWN) 或 FC ID 来识别成员。

|           |                                                                                    |
|-----------|------------------------------------------------------------------------------------|
| <b>语法</b> | <code>member {wwn wwn-ID   fc-id fc-id}</code>                                     |
| <b>参数</b> | <ul style="list-style-type: none"> <li><code>wwn-ID</code> — 输入 WWN 名称。</li> </ul> |

|        |                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <ul style="list-style-type: none"> <li>• <i>fc-id</i> — 输入 FC ID 名称。</li> </ul>                                                                                      |
| 默认     | 未配置                                                                                                                                                                  |
| 命令模式   | 别名配置                                                                                                                                                                 |
| 使用情况信息 | <p>从版本 10.4.0E(R3S) 开始在全交换模式下的 MX9116n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持</p> <p>此命令的 <i>no</i> 版本将从 FC 别名移除成员。</p>                                       |
| 示例     | <pre>OS10(config)# fc alias test OS10(config-fc-alias-test)# member wwn 21:00:00:24:ff:7b:f5:c9 OS10(config-fc-alias-test)# member wwn 20:25:78:2b:cb:6f:65:57</pre> |
| 支持的版本  | 10.3.1E or later                                                                                                                                                     |

## member (zone)

将成员添加到现有分区。通过 FC 别名、全球通用名称 (WWN) 或 FC ID 来识别成员。

|        |                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>member {alias-name <i>alias-name</i>   wwn <i>wwn-ID</i>   fc-id <i>fc-id</i>}</code>                                                                       |
| 参数     | <ul style="list-style-type: none"> <li>• <i>alias-name</i> — 输入 FC 别名名称。</li> <li>• <i>wwn-ID</i> — 输入 WWN 名称。</li> <li>• <i>fc-id</i> — 输入 FC ID 名称。</li> </ul>  |
| 默认     | 未配置                                                                                                                                                               |
| 命令模式   | 分区配置                                                                                                                                                              |
| 使用情况信息 | <p>从版本 10.4.0E(R3S) 开始在全交换模式下的 MX9116n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持</p> <p>此命令的 <i>no</i> 版本将从区域中移除成员。</p>                                       |
| 示例     | <pre>OS10(config)# fc zone hba1 OS10(config-fc-zone-hba1)# member wwn 10:00:00:90:fa:b8:22:19 OS10(config-fc-zone-hba1)# member wwn 21:00:00:24:ff:7b:f5:c8</pre> |
| 支持的版本  | 10.3.1E or later                                                                                                                                                  |

## 成员（分区集）

将分区添加到现有分区集。

|        |                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>member <i>zone-name</i></code>                                                                                        |
| 参数     | <i>zone-name</i> — 输入现有的分区名称。                                                                                               |
| 默认     | 未配置                                                                                                                         |
| 命令模式   | 分区集 CONFIGURATION                                                                                                           |
| 使用情况信息 | <p>从版本 10.4.0E(R3S) 开始在全交换模式下的 MX9116n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持</p> <p>此命令的 <i>no</i> 版本将从分区集移除分区。</p> |
| 示例     | <pre>OS10(config)# fc zoneset set OS10(conf-fc-zoneset-set)# member hba1</pre>                                              |
| 支持的版本  | 10.3.1E or later                                                                                                            |

## show fc alias

显示 FC 别名及其成员的详细信息。

|        |                                                                                   |
|--------|-----------------------------------------------------------------------------------|
| 语法     | show fc alias [ <i>alias-name</i> ]                                               |
| 参数     | <i>alias-name</i> — (可选) 输入 FC 别名名称。                                              |
| 默认     | 未配置                                                                               |
| 命令模式   | EXEC                                                                              |
| 使用情况信息 | 从版本 10.4.0E(R3S) 开始在全交换模式下的 MX9116n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持 |

|    |                                                                                                                                                                                          |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show fc alias  Alias Name                Alias Member ===== test                      21:00:00:24:ff:7b:f5:c9                            20:25:78:2b:cb:6f:65:57  OS10#</pre> |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|       |                  |
|-------|------------------|
| 支持的版本 | 10.3.1E or later |
|-------|------------------|

## show fc interface-area-id mapping

显示 FC ID 到接口映射的详细信息。

|        |                                   |
|--------|-----------------------------------|
| 语法     | show fc interface-area-id mapping |
| 参数     | 无                                 |
| 默认     | 未配置                               |
| 命令模式   | EXEC                              |
| 使用情况信息 | 无                                 |

|    |                                                                                                                                                                     |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show fc interface-area-id mapping  Intf Name                FC-ID                Status ===== ethernet1/1/40           0a:02:00             Active</pre> |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|       |                   |
|-------|-------------------|
| 支持的版本 | 10.4.1.0 or later |
|-------|-------------------|

## show fc ns switch

显示 FC NS 交换机参数的详细信息。

|        |                           |
|--------|---------------------------|
| 语法     | show fc ns switch [brief] |
| 参数     | 无                         |
| 默认     | 未配置                       |
| 命令模式   | EXEC                      |
| 使用情况信息 | 无                         |

|    |                                                                                                                    |
|----|--------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show fc ns switch  Total number of devices = 1 Switch Name                10:00:14:18:77:13:38:28</pre> |
|----|--------------------------------------------------------------------------------------------------------------------|

```

Domain Id 4
Switch Port port-channel10 (Eth 1/1/9)
FC-Id 04:00:00
Port Name 50:00:d3:10:00:ec:f9:05
Node Name 50:00:d3:10:00:ec:f9:00
Class of Service 8
Symbolic Port Name Compellent Port QLGC FC 8Gbps; Slot=06
Port=01 in Controller: SN 60665 of Storage Center: DEVTEST 60665
Symbolic Node Name Compellent Storage Center: DEVTEST 60665
Port Type N_PORT
Registered with NameServer Yes
Registered for SCN No

```

#### 示例 (brief)

```

OS10# show fc ns switch brief
Total number of devices = 1
Intf# Domain FC-ID Enode-WWPN
Enode-WWNN
port-channel10 (Eth 1/1/9) 4 04:00:00 10:00:00:90:fa:b8:22:18
20:00:00:90:fa:b8:22:18

```

#### 支持的版本

10.3.1E or later

## show fc zone

显示 FC 分区和分区成员。

|               |                                       |
|---------------|---------------------------------------|
| <b>语法</b>     | <code>show fc zone [zone-name]</code> |
| <b>参数</b>     | <code>zone-name</code> — 输入 FC 分区名称。  |
| <b>默认</b>     | 未配置                                   |
| <b>命令模式</b>   | EXEC                                  |
| <b>使用情况信息</b> | 无                                     |
| <b>示例</b>     |                                       |

```

OS10# show fc zone

Zone Name Zone Member
=====
hba1 21:00:00:24:ff:7b:f5:c8
 10:00:00:90:fa:b8:22:19
 21:00:00:24:ff:7f:ce:ee
 21:00:00:24:ff:7f:ce:ef
hba2 20:01:00:0e:1e:e8:e4:99
 50:00:d3:10:00:ec:f9:1b
 50:00:d3:10:00:ec:f9:05
 50:00:d3:10:00:ec:f9:1f
 20:35:78:2b:cb:6f:65:57

```

#### 示例 (包含分区名称)

```

OS10# show fc zone hba1

Zone Name Zone Member
=====
hba1 21:00:00:24:ff:7b:f5:c8
 10:00:00:90:fa:b8:22:19
 21:00:00:24:ff:7f:ce:ee
 21:00:00:24:ff:7f:ce:ef

```

#### 支持的版本

10.3.1E or later

# show fc zoneset

显示 FC 分区集、分区集中的区域和区域成员。

|        |                                         |
|--------|-----------------------------------------|
| 语法     | show fc zoneset [active   zoneset-name] |
| 参数     | zoneset-name — 输入 FC 分区集名称。             |
| 默认     | 未配置                                     |
| 命令模式   | EXEC                                    |
| 使用情况信息 | 无                                       |
| 示例     |                                         |

```
OS10# show fc zoneset
ZoneSetName ZoneName ZoneMember
=====
set hba1 21:00:00:24:ff:7b:f5:c8
 10:00:00:90:fa:b8:22:19
 21:00:00:24:ff:7f:ce:ee
 21:00:00:24:ff:7f:ce:ef

 hba2 20:01:00:0e:1e:e8:e4:99
 50:00:d3:10:00:ec:f9:1b
 50:00:d3:10:00:ec:f9:05
 50:00:d3:10:00:ec:f9:1f
 20:35:78:2b:cb:6f:65:57

vFabric id: 100
Active Zoneset: set
ZoneName ZoneMember
=====
hba2 20:01:00:0e:1e:e8:e4:99
 20:35:78:2b:cb:6f:65:57
 50:00:d3:10:00:ec:f9:05
 50:00:d3:10:00:ec:f9:1b
 50:00:d3:10:00:ec:f9:1f

hba1 *10:00:00:90:fa:b8:22:19
 *21:00:00:24:ff:7b:f5:c8
 21:00:00:24:ff:7f:ce:ee
 21:00:00:24:ff:7f:ce:ef
```

## 示例（活动分区集）

```
OS10# show fc zoneset active

vFabric id: 100
Active Zoneset: set
ZoneName ZoneMember
=====
hba2 20:01:00:0e:1e:e8:e4:99
 20:35:78:2b:cb:6f:65:57
 50:00:d3:10:00:ec:f9:05
 50:00:d3:10:00:ec:f9:1b
 50:00:d3:10:00:ec:f9:1f

hba1 *10:00:00:90:fa:b8:22:19
 *21:00:00:24:ff:7b:f5:c8
 21:00:00:24:ff:7f:ce:ee
 21:00:00:24:ff:7f:ce:ef
```

## 示例（包含分区集名称）

```
OS10# show fc zoneset set
ZoneSetName ZoneName ZoneMember
=====
set hba1 21:00:00:24:ff:7b:f5:c8
 10:00:00:90:fa:b8:22:19
 21:00:00:24:ff:7f:ce:ee
 21:00:00:24:ff:7f:ce:ef
```



|      |                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------------------------------|
| hba2 | 20:01:00:0e:1e:e8:e4:99<br>50:00:d3:10:00:ec:f9:1b<br>50:00:d3:10:00:ec:f9:05<br>50:00:d3:10:00:ec:f9:1f<br>20:35:78:2b:cb:6f:65:57 |
|------|-------------------------------------------------------------------------------------------------------------------------------------|

**支持的版本** 10.3.1E or later

## zone default-zone permit

在没有活动分区集配置的情况下启用 vfabric 的所有已登录 FC 节点之间的访问。

|               |                                                                            |
|---------------|----------------------------------------------------------------------------|
| <b>语法</b>     | zone default-zone permit                                                   |
| <b>参数</b>     | 无                                                                          |
| <b>默认</b>     | 未配置                                                                        |
| <b>命令模式</b>   | Vfabric CONFIGURATION                                                      |
| <b>使用情况信息</b> | 默认区域在注册状态更改通知 (RSCN) 消息中通告最多 255 个成员。此命令的 no 版本将在没有活动分区集的情况下禁用 FC 节点之间的访问。 |

|           |                                                                                       |
|-----------|---------------------------------------------------------------------------------------|
| <b>示例</b> | <pre>OS10(config)# vfabric 100 OS10(conf-vfabric-100)# zone default-zone permit</pre> |
|-----------|---------------------------------------------------------------------------------------|

**支持的版本** 10.3.1E or later

## zoneset activate

激活现有分区集。您只能在 vfabric 中激活一个分区集。

|               |                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | zoneset activate zoneset-name                                                                         |
| <b>参数</b>     | zoneset-name — 输入现有分区集名称。                                                                             |
| <b>默认</b>     | 未配置                                                                                                   |
| <b>命令模式</b>   | vfabric CONFIGURATION                                                                                 |
| <b>使用情况信息</b> | 禁用活动分区集后，zone default-zone permit 命令配置会生效。基于此配置，默认分区允许或拒绝 vfabric 的所有已登录 FC 节点之间的访问。此命令的 no 版本将停用分区集。 |

从版本 10.4.1.0 开始，在全交换模式下的 MX9116n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

|           |                                                                                   |
|-----------|-----------------------------------------------------------------------------------|
| <b>示例</b> | <pre>OS10(config)# vfabric 100 OS10(conf-vfabric-100)# zoneset activate set</pre> |
|-----------|-----------------------------------------------------------------------------------|

**支持的版本** 10.3.1E or later

## NPG 命令

在 NPG 模式下支持以下命令：

### fc port-mode F

在光纤通道接口上配置端口模式。

|           |                |
|-----------|----------------|
| <b>语法</b> | fc port-mode F |
|-----------|----------------|

|        |                                                                                             |
|--------|---------------------------------------------------------------------------------------------|
| 参数     | 无                                                                                           |
| 默认     | N_Port                                                                                      |
| 命令模式   | Fibre Channel INTERFACE                                                                     |
| 使用情况信息 | 当端口处于关闭模式且启用了 NPG 模式时，配置端口模式。此命令的 no 版本将端口模式恢复为默认值。                                         |
| 示例     | <pre>OS10(config)# interface fibrechannel 1/1/1 OS10(conf-if-fc1/1/1)# fc port-mode F</pre> |
| 支持的版本  | 10.4.1.0 or later                                                                           |

## feature fc npg

全局启用 NPG 模式。

|        |                                                      |
|--------|------------------------------------------------------|
| 语法     | feature fc npg                                       |
| 参数     | 无                                                    |
| 默认     | 已禁用                                                  |
| 命令模式   | CONFIGURATION                                        |
| 使用情况信息 | 您一次只能启用以下选项之一：F_Port、NPG 或 FSB。此命令的 no 版本将禁用 NPG 模式。 |
| 示例     | <pre>OS10(config)# feature fc npg</pre>              |
| 支持的版本  | 10.4.0E(R1) or later                                 |

## show npg devices

显示连接到交换机的 NPG 设备。

|            |                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法         | show npg devices [brief]                                                                                                                                                                                                                                                                                                                                                                                 |
| 参数         | 无                                                                                                                                                                                                                                                                                                                                                                                                        |
| 默认         | 未配置                                                                                                                                                                                                                                                                                                                                                                                                      |
| 命令模式       | EXEC                                                                                                                                                                                                                                                                                                                                                                                                     |
| 使用情况信息     | 使用 brief 选项可显示最少详细信息。                                                                                                                                                                                                                                                                                                                                                                                    |
| 示例         | <pre>OS10# show npg devices ENode[0]: ENode MAC :d4:ae:52:1a:ee:54 ENode Interface: port-channel10(Eth 1/1/9) FCF MAC :14:18:77:20:7c:e3 Fabric Interface :Fc 1/1/25 FCoE Vlan :1001 Vfabric Id :10 ENode WWPN :20:01:d4:ae:52:1a:ee:54 ENode WWNN :20:00:d4:ae:52:1a:ee:54 FCoE MAC :0e:fc:00:01:04:02 FC-ID :01:04:02 Login Method :FLOGI Time since discovered(in Secs) :6253 Status :LOGGED_IN</pre> |
| 示例 (brief) | <pre>Total NPG Devices = 1 ENode-Interface  ENode-WWPN                FCoE-Vlan  Fabric-Intf  Vfabric-Id  Log</pre>                                                                                                                                                                                                                                                                                      |

```
Po 10 (Eth 1/1/9) 20:01:d4:ae:52:1a:ee:54 1001 Fc 1/1/25 10 FLO
LOGGED_IN
```

支持的版本 10.4.0E(R1) or later

## F\_Port 和 NPG 命令

F\_Port 和 NPG 模式均支持以下命令：

### clear fc statistics

清除指定 vfabric 或光纤通道接口的 FC 统计信息。

**语法** `clear fc statistics [vfabric vfabric-ID | interface fibrechannel]`

**参数**

- *vfabric-ID* — 输入 vfabric ID。
- *fibrechannel* — 输入光纤通道接口名称。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# clear fc statistics vfabric 100
OS10# clear fc statistics interface fibrechannel1/1/25
```

支持的版本 10.4.1.0 or later

### fcoe

将 FCoE 参数添加到 vfabric。

**语法** `fcoe {fcmmap fc-map | fcf-priority fcf-priority-value | fka-adv-period adv-period | vlan-priority vlan-priority-value | keep-alive}`

**参数**

- *fc-map* — 输入 FC 映射 ID, 从 0xefc00 到 0xefc0ff。
- *fcf-priority-value* — 输入 FCF 优先级值, 从 1 到 255。
- *adv-period* — 输入 FCF 持续时间通告, 从 8 秒到 90 秒。
- *vlan-priority-value* — 输入 VLAN 优先级值, 从 0 到 7。

**默认**

- *fcmmap* — 0x0EFC00
- *fcf-priority* — 128
- *fka-adv-period* — 8
- *vlan-priority* — 3
- *keep-alive* — True

**命令模式** Vfabric CONFIGURATION

**使用情况信息** 此命令的 no 版本将禁用 FCoE parameters。

**示例**

```
OS10(config)# vfabric 10
OS10(conf-vfabric-10)# name 10
OS10(conf-vfabric-10)# fcoe fcmmap 0x0efc01
OS10(conf-vfabric-10)# fcoe fcf-priority 128
OS10(conf-vfabric-10)# fcoe fka-adv-period 8
OS10(conf-vfabric-10)# fcoe vlan-priority 3
```

支持的版本 10.3.1E or later

# name

配置 vfabric 名称。

|        |                                             |
|--------|---------------------------------------------|
| 语法     | <code>name vfabric-name</code>              |
| 参数     | <code>vfabric-name</code> — 输入 vfabric 的名称。 |
| 默认     | 未配置                                         |
| 命令模式   | Vfabric CONFIGURATION                       |
| 使用情况信息 | 此命令的 <code>no</code> 版本将移除 vfabric 名称。      |

示例

```
OS10(config)# vfabric 100
OS10(conf-vfabric-100)# name test_vfab
```

支持的版本 10.3.1E or later

# show fc statistics

显示 FC 统计信息。

|        |                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show fc statistics {vfabric vfabric-ID   interface fibrechannel}</code>                                                            |
| 参数     | <ul style="list-style-type: none"><li><code>vfabric-ID</code> — 输入 vfabric ID。</li><li><code>fibrechannel</code> — 输入光纤通道接口名称。</li></ul> |
| 默认     | 未配置                                                                                                                                      |
| 命令模式   | EXEC                                                                                                                                     |
| 使用情况信息 | 无                                                                                                                                        |

示例 (vfabric)

```
OS10# show fc statistics vfabric 100
Number of FLOGI : 43
Number of FDISC : 6
Number of FLOGO : 0
Number of FLOGI Accepts : 43
Number of FLOGI Rejects : 0
Number of FDISC Accepts : 6
Number of FDISC Rejects : 0
Number of FLOGO Accepts : 0
Number of FLOGO Rejects : 0
```

示例 (接口)

```
OS10# show fc statistics interface fibrechannel1/1/25:1
Number of FLOGI : 1
Number of FDISC : 0
Number of FLOGO : 0
Number of FLOGI Accepts : 1
Number of FLOGI Rejects : 0
Number of FDISC Accepts : 0
Number of FDISC Rejects : 0
Number of FLOGO Accepts : 0
Number of FLOGO Rejects : 0
```

支持的版本 10.3.1E or later

# show fc switch

显示 FC 交换机参数。

|    |                             |
|----|-----------------------------|
| 语法 | <code>show fc switch</code> |
|----|-----------------------------|

|        |                                                                                            |
|--------|--------------------------------------------------------------------------------------------|
| 参数     | 无                                                                                          |
| 默认     | 未配置                                                                                        |
| 命令模式   | EXEC                                                                                       |
| 使用情况信息 | 无                                                                                          |
| 示例     | <pre>OS10# show fc switch Switch Mode : FPORT Switch WWN   : 10:00:14:18:77:20:8d:cf</pre> |
| 支持的版本  | 10.3.1E or later                                                                           |

## show running-config vfabric

显示 vfabric 的正在运行配置。

|        |                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show running-config vfabric                                                                                                               |
| 参数     | 无                                                                                                                                         |
| 默认     | 未配置                                                                                                                                       |
| 命令模式   | EXEC                                                                                                                                      |
| 使用情况信息 | 无                                                                                                                                         |
| 示例     | <pre>OS10# show running-configuration vfabric ! vfabric 10 vlan 100 fcoe fcmap 0xEFC00 fcoe fcf-priority 140 fcoe fka-adv-period 13</pre> |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                      |

## show vfabric

显示 vfabric 详细信息。

|        |                                                                                                                                                                                                                                                                                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show vfabric                                                                                                                                                                                                                                                                                                   |
| 参数     | 无                                                                                                                                                                                                                                                                                                              |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                            |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                           |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                              |
| 示例     | <pre>OS10# show vfabric Fabric Name          SAN_FABRIC Fabric Type          FPORT Fabric Id             10 VlanId                1001 FC-MAP                0EFC00 Config-State         ACTIVE Oper-State            UP ===== Switch Config Parameters ===== Domain ID 4 ===== Switch Zoning Parameters</pre> |

```

=====
Default Zone Mode: Deny
Active ZoneSet: zoneset5
=====
Members
 fibrechannel1/1/25
 port-channel10 (Eth 1/1/9)

```

**支持的版本** 10.3.1E or later

## vfabric

配置 vfabric。

**语法** `vfabric fabric-ID`

**参数** *fabric-ID* — 输入结构 ID，从 1 到 255。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 在配置 vfabric 之前启用 F\_Port 或 NPG 功能。您只能在 F\_Port 模式中配置一个 vfabric。仅当您使用有效的 VLAN 和 FC 映射来配置 vfabric 时，vfabric 才会变为活动状态。请勿将跨区 VLAN 用作 vfabric VLAN。

此命令的 no 版本将移除 vfabric。仅当未在任何接口上应用 vfabric 时，您才可以移除它。

从版本 10.4.1.0 开始，在全交换模式下的 MX9116n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

**示例**

```

OS10(config)# vfabric 100

```

**支持的版本** 10.3.1E or later

## vfabric (interface)

将现有 vfabric 应用到以太网或 FC 接口。

**语法** `vfabric fabric-ID`

**参数** *fabric-ID* — 输入结构 ID，从 1 到 255。

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息** 此命令的 no 版本将从接口移除 vfabric。

**示例**

```

OS10(config)# interface fibrechannel 1/1/1
OS10(config-if-fc1/1/1)# vfabric 100

```

```

OS10(config)# interface ethernet 1/1/10
OS10(config-if-eth1/1/10)# vfabric 200

```

**支持的版本** 10.3.1E or later

## vlan

将现有 VLAN ID 关联到 vfabric 以传输流量。

**语法** `vlan vlan-ID`

|        |                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------|
| 参数     | <i>vlan-ID</i> — 输入现有的 VLAN ID。                                                                                                      |
| 默认     | 未配置                                                                                                                                  |
| 命令模式   | Vfabric CONFIGURATION                                                                                                                |
| 使用情况信息 | 在将 VLAN ID 关联到 vfabric 之前，先创建它。请勿将跨区 VLAN 用作 vfabric VLAN。此命令的 no 版本会从 vfabric 中删除 VLAN ID。                                          |
| 示例     | <pre>OS10(config)# interface vlan 1023 OS10(conf-if-vl-1023)# exit OS10(config)# vfabric 100 OS10(conf-vfabric-100)# vlan 1023</pre> |
| 支持的版本  | 10.3.1E or later                                                                                                                     |

## FIP 侦听命令

在 FIP 侦听模式下支持以下命令：

### feature fip-snooping

全局启用 FIP 侦听功能。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>feature fip-snooping [with-cvl]</code>                                                                                                                                                                                                                                                                                                                                                                                           |
| 参数     | <i>with-cvl</i> — 启用 CVL。                                                                                                                                                                                                                                                                                                                                                                                                              |
| 默认     | 已禁用                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | <p>您一次只能启用以下选项之一：F_Port、NPG 或 FSB。</p> <p>您可以包括 <i>with-cvl</i> 选项以将清除虚拟链路 (CVL) 帧从 FCF 发送到 ENode。当 FCoE 会话中断时，此选项可帮助系统自动恢复。如果已启用 FIP 侦听，您可以输入 <code>feature fip-snooping with-cvl</code> 命令来启用 CVL。您不必明确禁用 FIP 侦听来启用 CVL。但是，要禁用 CVL，您必须禁用 FIP 侦听，然后在不使用 <i>with-cvl</i> 选项的情况下重新启用。</p> <p>此命令的 no 版本将禁用 FIP 侦听。禁用 FIP 侦听后，系统将自动删除所有 FIP 侦听 VLAN 和端口模式配置。如果系统中存在任何与 FIP 侦听相关的配置，OS10 将返回错误消息。从系统中删除所有与 FIP 侦听相关的配置后，您只能禁用 FIP 侦听。</p> |
| 示例     | <pre>OS10(config)# feature fip-snooping  OS10(config)# feature fip-snooping with-cvl</pre>                                                                                                                                                                                                                                                                                                                                             |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                                                                                                                                                                                                                                                                   |

### fip-snooping enable

在指定 VLAN 上启用 FIP 侦听。

|      |                                  |
|------|----------------------------------|
| 语法   | <code>fip-snooping enable</code> |
| 参数   | 无                                |
| 默认   | 已禁用                              |
| 命令模式 | VLAN INTERFACE                   |

**使用情况信息** 仅在使用 `feature fip-snooping` 命令全局启用 FIP 侦听功能后，才能在 VLAN 上启用 FIP 侦听。OS10 支持最多 12 个 VLAN FIP 侦听。此命令的 `no` 版本将禁用 VLAN 上的 FIP 侦听。

**示例**

```
OS10(config)# interface vlan 3
OS10(conf-if-vl-3)# fip-snooping enable
```

**支持的版本** 10.4.0E(R1) or later

## fip-snooping fc-map

配置特定 VLAN 的 FC 映射值。

**语法** `fip-snooping fc-map fc-map`  
**参数** `fc-map` — 输入 FC 映射 ID，从 0xefc00 到 0xefcff。  
**默认** 未配置  
**命令模式** VLAN INTERFACE  
**使用情况信息** 此命令的 `no` 版本将禁用 FC 映射配置。

**示例**

```
OS10(config)# interface vlan 3
OS10(conf-if-vl-3)# fip-snooping fc-map 0xEFC64
```

**支持的版本** 10.4.0E(R1) or later

## fip-snooping port-mode

为接口设置 FIP 侦听端口模式。

**语法** `fip-snooping port-mode {enode | enode-transit | fcf | fcf-transit}`  
**参数** `enode | enode-transit | fcf | fcf-transit` — 输入关键字以设置 FIP 侦听端口模式。  
**默认** ENode 端口模式  
**命令模式** INTERFACE  
**使用情况信息** OS10 仅在运行 FSB 模式的交换机以及以太网和端口通道接口上支持此配置。您不能在端口通道成员上配置 FIP 侦听端口模式。  
使用此命令可更改端口模式。默认情况下，接口的端口模式设置为 ENode。仅在您启用 FIP 侦听后配置端口模式。在禁用 FIP 侦听之前，请将端口模式重置为其默认值 ENode。  
当端口模式设置为非默认值（`enode-transit`、`fcf` 或 `fcf-transit`）时，您不能禁用 FIP 侦听。  
如果您想要将端口模式从一个值更改为另一个值，则可以直接使用 `fip-snooping port mode` 命令。您不必明确使用命令的 `no` 形式。  
此命令的 `no` 版本将端口模式重置为 ENode。

**示例**

```
OS10(config)# interface ethernet 1/1/32
OS10(conf-if-eth1/1/32)# fip-snooping port-mode fcf
```

**支持的版本** 10.4.0E(R1) or later10.4.3.0 or later — 添加了 `enode-transit` 和 `fcf-transit` 端口模式支持。

## FCoE 命令

所有三种模式均支持以下命令：F\_Port、NPG 和 FSB。



## clear fcoe database

清除指定 VLAN 的 FCoE 数据库。

**语法** `clear fcoe database vlan vlan-id {enode enode-mac-address | fcf fcf-mac-address | session fcoe-mac-address}`

**参数**

- *vlan-id* — 输入 VLAN ID。
- *enode-mac-address* — 输入 ENode 的 MAC 地址。
- *fcf-mac-address* — 输入 FCF 的 MAC 地址。
- *fcoe-mac-address* — 输入 FCoE 会话的 MAC 地址。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# clear fcoe database vlan 100 enode aa:bb:cc:00:00:00
```

**支持的版本** 10.4.0E(R1) or later

## clear fcoe statistics

清除指定接口的 FCoE 统计信息。

**语法** `clear fcoe statistics [interface interface-type]`

**参数** *interface-type* — (可选) 输入接口类型。接口可以是以太网、VLAN 或端口通道。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 如果未指定 *interface interface-type* 信息，则命令将清除所有接口和 VLAN 的统计信息。

**示例**

```
OS10# clear fcoe statistics interface ethernet 1/1/1
OS10# clear fcoe statistics interface port-channel 5
```

**支持的版本** 10.4.0E(R1) or later

## fcoe-pinned-port

将端口标记为端口通道中的固定端口。FSB、NPG 中的以太网 LAG 和 F\_Port 模式时支持此配置。VLTi LAG 不支持此功能。

**语法** `fcoe-pinned-port`

**参数** *node/slot/port[:subport]* — 输入接口类型的详细信息。

**默认** 已禁用

**命令模式** Port-channel INTERFACE

**使用情况信息** 您只能为每个端口通道配置单端口。如果端口配置不正确，或者驻留的端口发生故障，则不会使用端口通道中的其他端口，即使端口具有到服务器的有效路径也是如此。此命令的 *no* 版本将移除固定的端口配置。

**示例**

```
OS10(conf-if-eth-1/1/9)# channel-member 10
OS10(conf-if-eth-1/1/9)# fcoe-pinned-port
Warning: Any existing FCoE session in port-channel will get cleared. Do
you want to continue(yes/no)?yes
```

**支持的版本** 10.4.2.0 or later

## fcoe max-sessions-per-enodemac

配置 ENode 允许的最大会话数。

**语法** `fcoe max-sessions-per-enodemac max-session-number`

**参数** `max-session-number` — 输入允许的最大会话数，从 1 到 64。

**默认** 32

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本会将会话数重置为默认值。

 **注:** 在 MX9116N-ON 结构模式下，此命令不可用。因此，在 MX9116N-ON 中，FCoE 会话数始终为 32。如果设备处于全切换模式，您可以使用 `fcoe max-sessions-per-enodemac 64` 命令，将每个 ENode 的最大会话 FCoE 数设置为 64。

**示例**

```
OS10(config)# fcoe max-sessions-per-enodemac 64
```

**支持的版本** 10.4.0E(R1) or later

## fcoe priority-bits

为 FCoE 应用程序 TLV 配置优先级位。

**语法** `fcoe priority-bits priority-value`

**参数** `priority-value` — 输入 FCoE 应用程序 TLV 中通告的 PFC 优先级值。您可以输入以下值之一：0x01, 0x02, 0x04, 0x08, 0x10, 0x20, 0x40, or 0x80。

**默认** 0x08

**命令模式** CONFIGURATION

**使用情况信息** 您一次只能配置一个 PFC 优先级。此命令的 `no` 版本将配置恢复为默认值。

**示例**

```
OS10(config)# fcoe priority-bits 0x08
```

**支持的版本** 10.4.0E(R3) or later

## lldp tlv-select dcbxp-appln fcoe

为接口启用 FCoE 应用程序 TLV。

**语法** `lldp tlv-select dcbxp-appln fcoe`

**参数** 无

**默认** 已启用

**命令模式** INTERFACE

**使用情况信息** FCoE 应用程序 TLV 中通告的默认优先级值为 3。如果接口中的 PFC 配置与 3 匹配，则 FCoE 应用程序 TLV 将通告为 3。否则，不会通告 FCoE 应用程序 TLV。

当使用 `fcoe priority-bits` 命令配置应用程序优先级时，所配置的值将在 TLV 中通告，而不依赖 PFC 配置。

此命令的 `no` 版本将禁用 FCoE 应用程序 TLV。

**示例**

```
OS10(conf-if-eth1/1/1)# lldp tlv-select dcbx-appln fcoe
```

**支持的版本** 10.4.0E(R3) or later

## show fcoe enode

显示连接到交换机的 ENode 的详细信息。

|        |                                                                           |
|--------|---------------------------------------------------------------------------|
| 语法     | show fcoe enode [ <i>enode-mac-address</i> ]                              |
| 参数     | <i>enode-mac-address</i> — (可选) 输入 ENode 的 MAC 地址。此选项显示与指定 ENode 相关的详细信息。 |
| 默认     | 未配置                                                                       |
| 命令模式   | EXEC                                                                      |
| 使用情况信息 | 无                                                                         |
| 示例     |                                                                           |

```
OS10# show fcoe enode
Enode MAC Enode Interface VLAN FCFs Sessions

d4:ae:52:1b:e3:cd Po 20 (Eth 1/1/3) 1001 1 1
```

支持的版本 10.4.0E(R1) or later

## show fcoe fcf

显示连接到交换机的 FCF 的详细信息。

|        |                                                                  |
|--------|------------------------------------------------------------------|
| 语法     | show fcoe [ <i>fcf-mac-address</i> ]                             |
| 参数     | <i>fcf-mac-address</i> — (可选) 输入 FCF 的 MAC 地址。此选项显示指定 FCF 的详细信息。 |
| 默认     | 未配置                                                              |
| 命令模式   | EXEC                                                             |
| 使用情况信息 | 无                                                                |
| 示例     |                                                                  |

```
OS10# show fcoe fcf
FCF MAC FCF Interface VLAN FC-MAP FKA_ADV_PERIOD No.
of Enodes FCF Mode

00:0c:84:a8:00:00 Eth 1/1/36 777 0e:fc:00 8000
0 F
00:0d:84:a8:01:02 Eth 1/1/37 778 0e:fc:01 8000
0 FT
```

支持的版本 10.4.0E(R1) or later

## show fcoe pinned-port

显示端口通道、相应的固定端口配置和端口状态（如果 FCoE 会话已形成）。

|        |                                                               |
|--------|---------------------------------------------------------------|
| 语法     | show fcoe pinned-port [ <i>port-channel port-channel-id</i> ] |
| 参数     | <i>port-channel-id</i> — 输入端口通道 ID 以显示相应的配置。                  |
| 默认     | 未配置                                                           |
| 命令模式   | EXEC                                                          |
| 使用情况信息 | 无                                                             |
| 示例     |                                                               |

```
OS10# show fcoe pinned-port
Interface pinned-port FCoE Status
```

```

Po 10 Eth 1/1/1 Up
Po 20 Eth 1/1/3 Up
Po 30 Eth 1/1/7 Down

```

**支持的版本** 10.4.2.0 or later

## show fcoe sessions

显示已建立的 FCoE 会话的详细信息。

- 语法** `show fcoe sessions [interface vlan vlan-id]`
- 参数** `vlan-id` — (可选) 输入 VLAN ID。此选项显示在指定 VLAN 上建立的会话。
- 默认** 未配置
- 命令模式** EXEC
- 使用情况信息** 无
- 示例**

```

Enode MAC Enode Interface FCF MAC FCF interface
VLAN FCoE MAC FC-ID PORT WWPN
aa:bb:cc:00:00:00 Po 20(Eth 1/1/3) aa:bb:cd:00:00:00 Po 10(Eth 1/1/1)
100 0e:fc:00:01:00:01 01:00:01 31:00:0e:fc:00:00:00:00
21:00:0e:fc:00:00:00:00
aa:bb:cc:00:00:00 Po 20(Eth 1/1/3) aa:bb:cd:00:00:00 Po 10(Eth 1/1/1)
100 0e:fc:00:01:00:02 01:00:02 31:00:0e:fc:00:00:00:00
21:00:0e:fc:00:00:00:00

```

**支持的版本** 10.4.0E(R1) or later

## show fcoe statistics

显示 FCoE 控制平面的统计信息。

- 语法** `show fcoe statistics [interface interface-type]`
- 参数** `interface-type` — (可选) 输入接口类型。此选项显示指定接口的统计信息。
- 默认** 未配置
- 命令模式** EXEC
- 使用情况信息** 无
- 示例**

```

OS10# show fcoe statistics interface port-channel10
Number of Vlan Requests :0
Number of Vlan Notifications :0
Number of Multicast Discovery Solicits :2
Number of Unicast Discovery Solicits :0
Number of FLOGI :2
Number of FDISC :16
Number of FLOGO :0
Number of Enode Keep Alive :9021
Number of VN Port Keep Alive :3349
Number of Multicast Discovery Advertisement :4437
Number of Unicast Discovery Advertisement :2
Number of FLOGI Accepts :2
Number of FLOGI Rejects :0

```

```

Number of FDISC Accepts :16
Number of FDISC Rejects :0
Number of FLOGO Accepts :0
Number of FLOGO Rejects :0
Number of CVL :0
Number of FCF Discovery Timeouts :0
Number of VN Port Session Timeouts :0
Number of Session failures due to Hardware Config :0

```

**支持的版本** 10.4.0E(R1) or later

## show fcoe system

显示与 FCoE 有关的系统信息。

**语法** show fcoe system

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```

OS10# show fcoe system
Mode: FIP Snooping Bridge
CVL Status: Enabled
FCOE VLAN List (Operational) : 1, 100
FCFs : 1
Enodes : 2
Sessions : 17

```

**支持的版本** 10.4.0E(R1) or later

## show fcoe vlan

显示 FIP 侦听 VLAN 的详细信息。

**语法** show fcoe vlan

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```

OS10# show fcoe vlan
* = Default VLAN
VLAN FC-MAP FCFs Enodes Sessions

*1 - - - -
100 0X0EFC00 1 2 17

```

**支持的版本** 10.4.0E(R1) or later

第 2 层

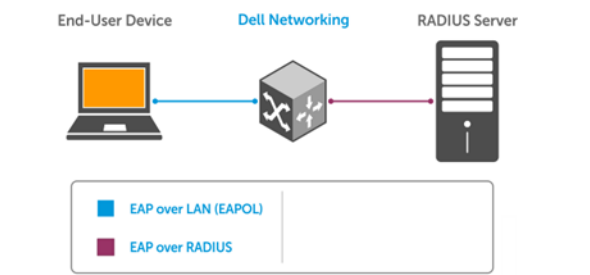
|                                            |                                                                                         |
|--------------------------------------------|-----------------------------------------------------------------------------------------|
| 802.1X                                     | 在使用可扩展身份验证协议 (EAP) 发送或接收数据包之前验证设备凭据，请参阅 <a href="#">802.1X 命令</a> 。                     |
| 链路聚合控制协议 (LACP)                            | 在两个系统之间交换信息并自动在系统之间建立链路聚合组 (LAG)，请参阅 <a href="#">LACP 命令</a> 。                          |
| 链路层发现协议 (LLDP)                             | 使局域网 (LAN) 设备通告其配置，并从相邻的已启用 LLDP 的基础架构设备接收配置信息，请参阅 <a href="#">LLDP 命令</a> 。            |
| 介质访问控制 (MAC)                               | 使用表格配置网络上设备的限制、冗余、平衡和故障检测设置，请参阅 <a href="#">MAC 命令</a> 。                                |
| 多个生成树 (MST)                                | 映射 MST 实例并将多个虚拟局域网 (VLAN) 映射到单个生成树实例，从而减少所需实例的数量，请参阅 <a href="#">MST 命令</a> 。           |
| Rapid Per-VLAN Spanning-Tree Plus (RPVST+) | 快速生成树和增强的按 VLAN 生成树的组合，以实现更快的聚合和互操作性，请参阅 <a href="#">RPVST+ 命令</a> 。                    |
| 快速生成树协议 (RSTP)                             | 通过使用生成树和多个生成树协议 (STP 和 MSTP) 配置的设备实现更快的聚合和互操作性，请参阅 <a href="#">RSTP 命令</a> 。            |
| 虚拟 LAN (VLAN)                              | 提高了安全性以将用户组与不同的 VLAN 隔离，并且能够跨多个设备创建单个 VLAN，请参阅 <a href="#">VLAN 命令</a> 。                |
| 端口监控 (本地/远程)                               | 在指定端口上监控入口或出口流量，或同时监控入口和出口流量。监控方法包括端口镜像、远程端口监控和封装的远程端口监控（请参阅 <a href="#">本地/远程命令</a> ）。 |

802.1X

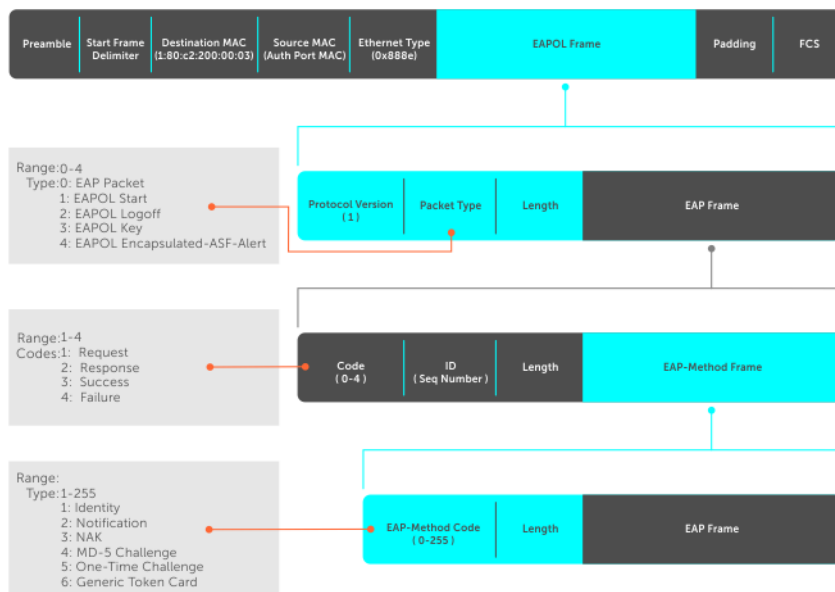
IEEE 802.1X 标准定义了基于客户端和服务器的访问控制，可防止未经授权的客户端通过可公开访问的端口连接到 LAN。仅在入站流量的 OS10 中需要身份验证。无论身份验证状态如何，出站流量都会传输。

802.1X 采用可扩展身份验证协议 (EAP)，通过使用中间网络访问设备，为身份验证服务器（通常为远程身份验证拨入服务 [RADIUS]）提供设备凭据。网络接入设备可调节终端用户设备与身份验证服务器之间的所有通信，以便网络保持安全。

网络接入设备使用以太网 EAP（也称为 EAPOL — EAP over LAN）与终端用户设备通信，并使用 EAP-over-RADIUS 与服务器通信。



**注：**OS10 不支持将 RADIUS 作为后端身份服务器。



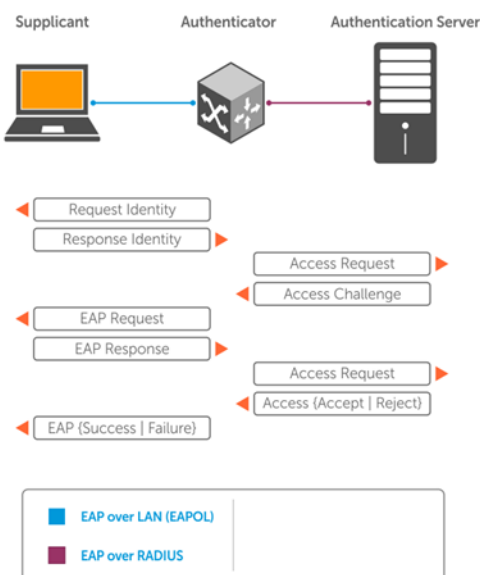
身份验证过程涉及三个设备：

- **请求者** — 尝试接入网络的设备将执行请求者的角色。在与设备关联的端口获得授权之前，此设备的定期流量不会到达网络。在此之前，请求者只能将 802.1x 消息（EAPOL 帧）与授权码进行交换。
- **验证者** — 验证者是网络的入口管理员、转换和转发身份验证服务器与请求者之间的请求和响应。验证者还会根据身份验证进程的结果更改端口状态。在 Dell EMC 设备上执行身份验证。
- **身份验证服务器** — 身份验证服务器选择身份验证方法，验证请求者提供的信息，并授予网络访问权限。

## 端口身份验证

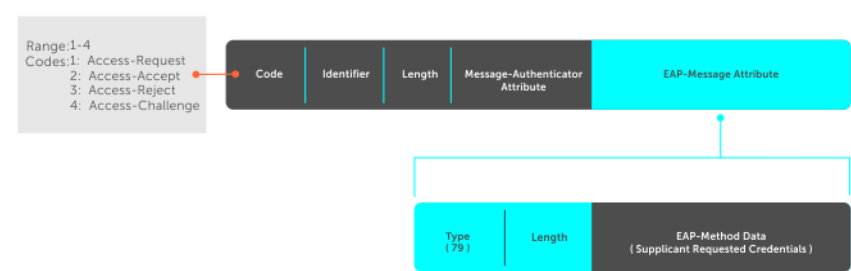
当身份验证程序感知链路状态从向下更改为向上时，将开始以下进程：

1. 认证器请求请求者使用 EAP 请求身份框架来识别自己。
2. 请求者在 EAP 响应识别框架中响应其身份。
3. 认证器解包 EAPOL 框架中的 EAP 响应，将其封装在 RADIUS 访问请求框架中，然后将该框架转发到身份验证服务器。
4. 身份验证服务器会回复访问质询框架，请求请求者使用 EAP 方法验证其身份。认证器将转换质询并转发给请求者。
5. 请求者协商身份验证方法，并在 EAP 响应中提供 EAP 请求信息。另一个访问请求框架会转换并将响应转发到身份验证服务器。
6. 如果请求者提供的身份信息有效，则身份验证服务器将发送一个指定网络权限的访问接受框架。认证器将端口状态更改为授权并转发 EAP 成功框架。如果标识信息无效，则服务器发送访问拒绝框架。如果端口状态仍然为未授权，则身份验证器将转发 EAP 故障框架。



# EAP over RADIUS

802.1x 使用 RADIUS 在授权码和身份验证服务器之间传输 EAP 数据包。EAP 消息以类型、长度、值 (TLV) 格式的属性能形式封装在 RADIUS 数据包中 — EAP 消息的类型值是 79。

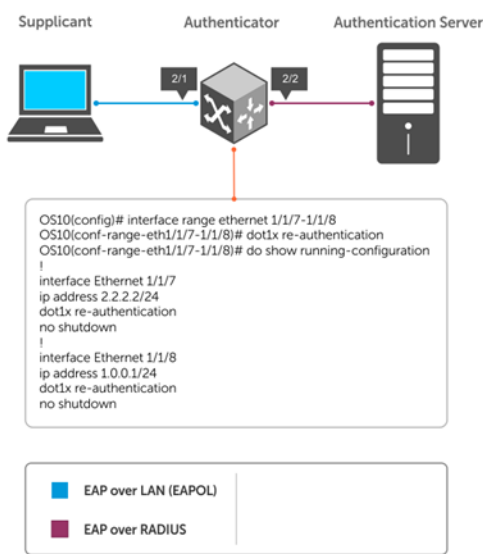


## 配置 802.1X

您可以在单个进程中的一个端口上配置和启用 802.1X。OS10 支持 802.1X 以及 EAP-MD5。所有平台均支持将 RADIUS 为身份验证服务器。

如果主 RADIUS 服务器变得无响应，则授权码将使用辅助 RADIUS 服务器（如果已配置）开始。

**注：** 端口通道或端口通道成员不支持 802.1X。



## 启用 802.1X

- 在 CONFIGURATION 模式下全局启用 802.1X。

```
dot1x system-auth-control
```

- 在 INTERFACE 模式下输入接口或接口范围。

```
interface range
```



### 3. 仅在 INTERFACE 模式下启用请求者接口上的 802.1X。

```
dot1x port-control auto
```

#### 配置和验证 802.1X 配置

```
OS10(config)# dot1x system-auth-control
OS10(config)# interface range 1/1/7-1/1/8
OS10(config-range-eth1/1/7-1/1/8)# dot1x port-control auto
OS10(config-range-eth1/1/7-1/1/8)# dot1x re-authentication
OS10(config-range-eth1/1/7-1/1/8)# do show dot1x interface ethernet 1/1/7
```

```
802.1x information on ethernet1/1/7

Dot1x Status: Enable
Port Control: AUTO
Port Auth Status: UNAUTHORIZED
Re-Authentication: Enable
Tx Period: 60 seconds
Quiet Period: 60 seconds
Supplicant Timeout: 30 seconds
Server Timeout: 30 seconds
Re-Auth Interval: 3600 seconds
Max-EAP-Req: 2
Host Mode: MULTI_HOST
Auth PAE State: Initialize
Backend State: Idle
```

## 身份重新传输

如果身份验证者发送请求标识帧，但请求者没有响应，则授权码将等待 30 秒，然后重新传输该帧。有多种原因会导致请求者无法响应 — 在请求到达时请求者可能正在引导，并且可能存在物理层问题等。

1. 在 INTERFACE 模式下配置身份验证程序在重新传输 EAP 请求标识帧之前等待的时间，从 1 到 65535 – 1 年，默认值为 60。

```
dot1x timeout tx-period seconds
```

2. 配置在 INTERFACE 模式下身份验证程序重新传输请求标识帧的最大次数，从 1 到 10；默认值为 2。

```
dot1x max-req retry-count
```

#### 配置和验证重新传输时间

```
OS10(config)# dot1x system-auth-control
OS10(config)# interface range 1/1/7-1/1/8
OS10(config-range-eth1/1/7-1/1/8)# dot1x timeout tx-period 120
OS10(config-range-eth1/1/7-1/1/8)# dot1x max-req 5
OS10(config-range-eth1/1/7-1/1/8)# do show dot1x interface ethernet 1/1/7
```

```
802.1x information on ethernet1/1/7

Dot1x Status: Enable
Port Control: AUTO
Port Auth Status: UNAUTHORIZED
Re-Authentication: Enable
Tx Period: 120 seconds
Quiet Period: 60 seconds
Supplicant Timeout: 30 seconds
Server Timeout: 30 seconds
Re-Auth Interval: 3600 seconds
Max-EAP-Req: 5
Host Mode: MULTI_HOST
Auth PAE State: Initialize
Backend State: Idle
```

## 查看接口运行的配置

```
OS10(conf-range-eth1/1/7-1/1/8)# do show running-configuration interface
...
!
interface ethernet1/1/7
 no shutdown
 dot1x max-req 5
 dot1x port-control auto
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout tx-period 120
!
interface ethernet1/1/8
 no shutdown
 dot1x max-req 5
 dot1x port-control auto
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout tx-period 120
...
```

## 故障静默期

如果请求者未通过身份验证进程，则在默认情况下，授权码将在 30 秒后发送另一个请求标识帧。静默期是身份验证失败后的传输间隔时间。

请求身份重新传输间隔适用于无响应的请求者。对于无响应的请求者，您可以配置最多 10 次的时间间隔。

1. 在 INTERFACE 模式下配置身份验证程序重新传输 *Request Identity* 帧的最大次数，从 1 到 65535；默认值为 60 秒。

```
dot1x timeout quiet-period seconds
```

## 配置和验证端口身份验证

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout quiet-period 120
OS10(conf-range-eth1/1/7-1/1/8)# do show dot1x interface ethernet 1/1/7
802.1x information on ethernet1/1/7

Dot1x Status: Enable
Port Control: AUTO
Port Auth Status: UNAUTHORIZED
Re-Authentication: Enable
Tx Period: 120 seconds
Quiet Period: 120 seconds
Supplicant Timeout: 30 seconds
Server Timeout: 30 seconds
Re-Auth Interval: 3600 seconds
Max-EAP-Req: 5
Host Mode: MULTI_HOST
Auth PAE State: Initialize
Backend State: Idle
```

## 查看接口运行的配置

```
OS10(conf-range-eth1/1/7-1/1/8)# do show running-configuration interface
...
!
interface ethernet1/1/7
 no shutdown
 dot1x max-req 5
 dot1x port-control auto
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout tx-period 120
!
interface ethernet1/1/8
 no shutdown
 dot1x max-req 5
```

```
dot1x port-control auto
dot1x re-authentication
dot1x timeout quiet-period 120
dot1x timeout tx-period 120
...
```

## 端口控制模式

802.1X 要求端口处于三种状态之一：强制授权、强制不授权或自动。

**强制授权（默认）** 这是一种授权状态。连接到此端口的设备不使用身份验证进程，但可在网络上通信。将端口置于此状态与在端口上禁用 802.1X 相同。force-authorized 为默认模式。

**强制不授权** 这是一种不授权的状态。连接到此端口的设备不使用身份验证进程，但不允许在网络上通信。将端口置于此状态与关闭端口相同。请求者发起身份验证的任何尝试都将被忽略。

**auto** 默认情况下，此状态为不授权。连接到此端口的设备受身份验证过程的约束。如果过程成功，该端口将获得授权，并且已连接的设备将在网络上通信。

- 在 INTERFACE 模式下将端口置于自动、强制授权（默认）或强制不授权状态。

```
dot1x port-control {auto | force-authorized | force-unauthorized}
```

### 配置并验证强制授权状态

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x port-control force-authorized
OS10(conf-range-eth1/1/7-1/1/8)# do show dot1x interface ethernet 1/1/7
```

```
802.1x information on ethernet1/1/7

Dot1x Status: Enable
Port Control: AUTHORIZED
Port Auth Status: UNAUTHORIZED
Re-Authentication: Enable
Tx Period: 120 seconds
Quiet Period: 120 seconds
Supplicant Timeout: 30 seconds
Server Timeout: 30 seconds
Re-Auth Interval: 3600 seconds
Max-EAP-Req: 5
Host Mode: MULTI_HOST
Auth PAE State: Initialize
Backend State: Initialize
```

### 查看接口运行的配置

```
OS10(conf-range-eth1/1/7-1/1/8)# do show running-configuration interface
...
!
interface ethernet1/1/7
no shutdown
dot1x max-req 5
dot1x re-authentication
dot1x timeout quiet-period 120
dot1x timeout tx-period 120
!
interface ethernet1/1/8
no shutdown
dot1x max-req 5
dot1x re-authentication
dot1x timeout quiet-period 120
dot1x timeout tx-period 120
...
```

## 重新验证端口

配置重新进行身份验证的时间段。在对请求者进行身份验证并且端口获得授权后，配置身份验证者以对请求者进行身份验证。如果启用重新进行身份验证，请求者将每 3600 秒重新进行一次身份验证。

- 在 INTERFACE 模式下重新验证请求者，从 1 到 65535，默认值为 3600。

```
dot1x timeout re-authperiod seconds
```

### 配置并验证重新验证的时间段

```
OS10(config)# interface range ethernet 1/1/7-1/1/8
OS10(conf-range-eth1/1/7-1/1/8)# dot1x re-authentication
OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout re-authperiod 3600
OS10(conf-range-eth1/1/7-1/1/8)# show dot1x interface ethernet 1/1/7
```

```
802.1x information on ethernet1/1/7

Dot1x Status: Enable
Port Control: AUTHORIZED
Port Auth Status: UNAUTHORIZED
Re-Authentication: Enable
Tx Period: 120 seconds
Quiet Period: 120 seconds
Supplicant Timeout: 30 seconds
Server Timeout: 30 seconds
Re-Auth Interval: 3600 seconds
Max-EAP-Req: 5
Host Mode: MULTI_HOST
Auth PAE State: Initialize
Backend State: Initialize
```

### 查看接口运行的配置

```
OS10(conf-range-eth1/1/7-1/1/8)# do show running-configuration interface
...
!
interface ethernet1/1/7
no shutdown
dot1x max-req 5
dot1x re-authentication
dot1x timeout quiet-period 120
dot1x timeout re-authperiod 3600
dot1x timeout tx-period 120
!
interface ethernet1/1/8
no shutdown
dot1x max-req 5
dot1x re-authentication
dot1x timeout quiet-period 120
dot1x timeout re-authperiod 3600
dot1x timeout tx-period 120
...
```

## 配置超时

如果请求者或身份验证服务器无响应，则在默认情况下，授权码将在 30 秒后终止身份验证进程。配置验证者在终止之前等待响应的时间量。

- 在 INTERFACE 模式下因无响应的请求者而终止身份验证过程，从 1 到 65535，默认值为 30。

```
dot1x timeout supp-timeout seconds
```

- 在 INTERFACE 模式下因无响应的身份验证服务器而终止身份验证过程，从 1 到 65535，默认值为 30。

```
dot1x timeout server-timeout seconds
```

## 配置和验证服务器超时

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout supp-timeout 45
OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout server-timeout 60
OS10(conf-range-eth1/1/7-1/1/8)# do show dot1x interface ethernet 1/1/7

802.1x information on ethernet1/1/7

Dot1x Status: Enable
Port Control: AUTHORIZED
Port Auth Status: UNAUTHORIZED
Re-Authentication: Enable
Tx Period: 120 seconds
Quiet Period: 120 seconds
Supplicant Timeout: 45 seconds
Server Timeout: 60 seconds
Re-Auth Interval: 3600 seconds
Max-EAP-Req: 5
Host Mode: MULTI_HOST
Auth PAE State: Initialize
Backend State: Initialize
```

## 查看接口运行的配置

```
OS10(conf-range-eth1/1/7-1/1/8)# do show running-configuration interface
...
!
interface ethernet1/1/7
 no shutdown
 dot1x max-req 5
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout re-authperiod 3600
 dot1x timeout server-timeout 60
 dot1x timeout supp-timeout 45
 dot1x timeout tx-period 120
!
interface ethernet1/1/8
 no shutdown
 dot1x max-req 5
 dot1x re-authentication
 dot1x timeout quiet-period 120
 dot1x timeout re-authperiod 3600
 dot1x timeout server-timeout 60
 dot1x timeout supp-timeout 45
 dot1x timeout tx-period 120
...

```

# 802.1X 命令

## dot1x host-mode

允许对一个或多个请求者在接口上进行 802.1X 身份验证。

**语法** dot1x host-mode {multi-host}

**参数**

- multi-host — 允许将多个主机连接到单个支持 802.1X 的端口。您只能为所有客户端授权其中一个连接的客户端来授予网络访问权限。如果该端口未经授权（重新身份验证失败或收到 EAPOL 注销），该设备将拒绝所有连接的客户端的网络访问。

**默认** 多主机

**命令模式** INTERFACE

**使用情况信息** 此命令的 no 版本会将该值重置为默认值。

**示例**

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x host-mode multi-host
```

**支持的版本** 10.2.0E or later

## dot1x max-req

更改设备在重新启动 802.1X 身份验证之前发送到请求者的最大请求数。

**语法** dot1x max-req *retry-count*

**参数** max-req *retry-count* — 输入发送给请求者的请求的重试次数，然后重启 802.1X 重新身份验证，从 1 到 10。

**默认** 2

**命令模式** INTERFACE

**使用情况信息** 此命令的 no 版本会将该值重置为默认值。

**示例**

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x max-req 4
```

**支持的版本** 10.2.0E or later

## dot1x port-control

控制对接口执行的 802.1X 身份验证。

**语法** dot1x port-control {force-authorized | force-unauthorized | auto}

**参数**

- force-authorized — 禁用接口上的 802.1X 身份验证，并允许接口上的所有流量，无需进行身份验证。
- force-unauthorized — 使端口处于未授权状态，忽略客户端对身份验证进行的所有尝试。
- auto — 启用接口上的 802.1X 身份验证。

**默认** 强制授权

**命令模式** INTERFACE

**使用情况信息** 此命令的 no 版本会将该值重置为默认值。

**示例**

```
OS10(config)# interface range ethernet 1/1/7-1/1/8
OS10(conf-range-eth1/1/7-1/1/8)# dot1x port-control auto
```

**支持的版本** 10.2.0E or later

## dot1x re-authentication

启用 802.1X 请求方的定期重新验证。

**语法** dot1x re-authentication

**参数** 无

**默认** 已禁用

**命令模式** INTERFACE

**使用情况信息** 此命令的 no 版本将禁用 802.1X 请求方的定期重新身份验证。

**示例**

```
OS10(conf-range-eth1/1/7-1/1/8)# dot1x re-authentication
```

**支持的版本** 10.2.0E or later

## dot1x timeout quiet-period

设置在与请求者进行身份验证交换失败后设备保持安静状态的秒数。

|               |                                                                            |
|---------------|----------------------------------------------------------------------------|
| <b>语法</b>     | <code>dot1x timeout quiet-period seconds</code>                            |
| <b>参数</b>     | <code>quiet period seconds</code> — 输入 802.1X 安静期限超时的描述，从 1 到 65535。       |
| <b>默认</b>     | 60 秒                                                                       |
| <b>命令模式</b>   | INTERFACE                                                                  |
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本会将该值重置为默认值。                                         |
| <b>示例</b>     | <pre>OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout quiet-period 120</pre> |
| <b>支持的版本</b>  | 10.2.0E or later                                                           |

## dot1x timeout re-authperiod

设置重新身份验证尝试之间的秒数。

|               |                                                                              |
|---------------|------------------------------------------------------------------------------|
| <b>语法</b>     | <code>dot1x timeout re-authperiod seconds</code>                             |
| <b>参数</b>     | <code>re-authperiod seconds</code> — 输入 802.1X 重新身份验证超时的秒数，从 1 到 65535。      |
| <b>默认</b>     | 3600 秒                                                                       |
| <b>命令模式</b>   | INTERFACE                                                                    |
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本会将该值重置为默认值。                                           |
| <b>示例</b>     | <pre>OS10(conf-range-eth1/1/7-1/1/8)# dot1x timeout re-authperiod 7200</pre> |
| <b>支持的版本</b>  | 10.2.0E or later                                                             |

## dot1x timeout server-timeout

设置设备在将数据包重新传输到身份验证服务器之前等待的秒数。

|               |                                                                       |
|---------------|-----------------------------------------------------------------------|
| <b>语法</b>     | <code>dot1x timeout server-timeout seconds</code>                     |
| <b>参数</b>     | <code>server-timeout seconds</code> — 输入 802.1X 服务器超时的秒数，从 1 到 65535。 |
| <b>默认</b>     | 30 秒                                                                  |
| <b>命令模式</b>   | INTERFACE                                                             |
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本会将该值重置为默认值。                                    |
| <b>示例</b>     | <pre>OS10(conf-range-eth1/1/7-1/1/8)# dot1x server-timeout 60</pre>   |
| <b>支持的版本</b>  | 10.2.0E or later                                                      |

## dot1x timeout supp-timeout

设置在设备重新传输帧之前，设备等待请求者响应 EAP 请求帧的秒数。

|             |                                                                     |
|-------------|---------------------------------------------------------------------|
| <b>语法</b>   | <code>dot1x timeout supp-timeout seconds</code>                     |
| <b>参数</b>   | <code>supp-timeout seconds</code> — 输入 802.1X 请求者超时的秒数，从 1 到 65535。 |
| <b>默认</b>   | 30 秒                                                                |
| <b>命令模式</b> | INTERFACE                                                           |

|        |                                                                             |
|--------|-----------------------------------------------------------------------------|
| 使用情况信息 | 此命令的 <code>no</code> 版本会将该值重置为默认值。                                          |
| 示例     | <pre>OS10 (conf-range-eth1/1/7-1/1/8) # dot1x timeout supp-timeout 45</pre> |
| 支持的版本  | 10.2.0E or later                                                            |

## dot1x timeout tx-period

设置在您重置请求之前，设备等待来自请求者响应 EAP 请求/身份框架的秒数。

|        |                                                                           |
|--------|---------------------------------------------------------------------------|
| 语法     | <code>dot1x timeout tx-period seconds</code>                              |
| 参数     | <code>tx-period seconds</code> — 输入 802.1X 传输超时的秒数，从 1 到 65535。           |
| 默认     | 60 秒                                                                      |
| 命令模式   | INTERFACE                                                                 |
| 使用情况信息 | 此命令的 <code>no</code> 版本会将该值重置为默认值。                                        |
| 示例     | <pre>OS10 (conf-range-eth1/1/7-1/1/8) # dot1x timeout tx-period 120</pre> |
| 支持的版本  | 10.2.0E or later                                                          |

## show dot1x

显示全局 802.1X 配置信息。

|        |                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show dot1x</code>                                                                                                                            |
| 参数     | 无                                                                                                                                                  |
| 默认     | 未配置                                                                                                                                                |
| 命令模式   | EXEC                                                                                                                                               |
| 使用情况信息 | 无                                                                                                                                                  |
| 示例     | <pre>OS10# show dot1x PAE Capability:      Authenticator only Protocol Version:    2 System Auth Control: Enable Auth Server:         Radius</pre> |
| 支持的版本  | 10.2.0E or later                                                                                                                                   |

## show dot1x interface

显示 802.1X 配置信息。

|        |                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show dot1x interface ethernet node/slot/port[:subport]</code>                                                                                             |
| 参数     | <code>ethernet node/slot/port[:subport]</code> — 输入以太网接口信息。                                                                                                     |
| 命令模式   | EXEC                                                                                                                                                            |
| 使用情况信息 | 使用此命令可查看特定接口的 dot1x 接口配置。                                                                                                                                       |
| 示例     | <pre>OS10# show dot1x interface 802.1x information on ethernet1/1/1 ----- Dot1x Status:                  Enable 802.1x information on ethernet1/1/2 -----</pre> |



```

Dot1x Status: Enable
802.1x information on ethernet1/1/3

Dot1x Status: Enable
802.1x information on ethernet1/1/4

Dot1x Status: Enable
802.1x information on ethernet1/1/5

Dot1x Status: Enable
802.1x information on ethernet1/1/6

Dot1x Status: Enable
802.1x information on ethernet1/1/7

Dot1x Status: Enable
Port Control: AUTO
Port Auth Status: UNAUTHORIZED
--more--

```

### 示例（未全局启用 dot1x 时）

```

OS10# show dot1x interface
802.1x not enabled in the system
OS10#

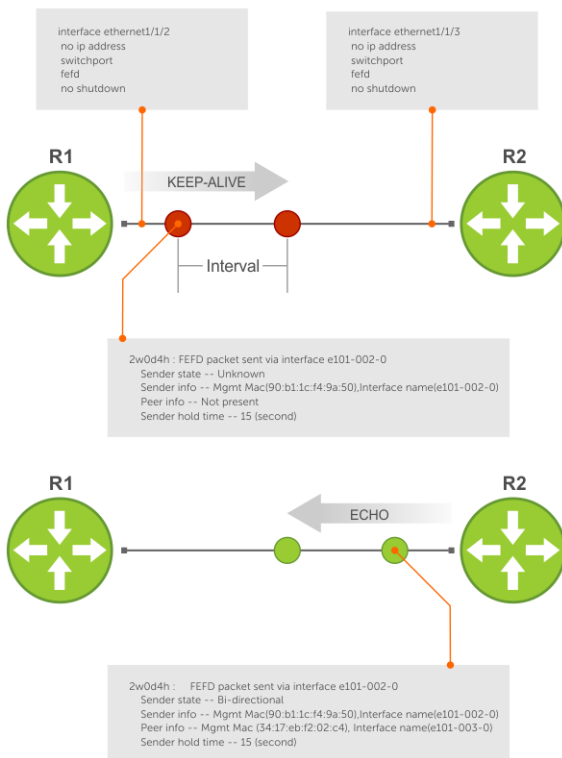
```

支持的版本 10.2.0E or later

## 远端故障检测

远端故障检测（FEFD）是一种在网络中检测远程数据链路错误的协议。

FEFD 使用链路层回声协议来检测和传输以太网和光纤链路路上的远端故障。启用 FEFD 后，交换机会定期交换 FEFD 回声帧以识别链路故障。如果本地交换机不会对等方收到针对配置的 FEFD 消息间隔三倍的时间间隔，则本地交换机假定对等链路已关闭。FEFD 消息间隔的默认间隔时间为 15 秒。例如，在默认配置下，如果本地交换机不会对等端收到 45 秒的回显消息，则会将对等链路关闭。



当发生以下问题时，FEFD 可帮助检测远端故障：

- 尽管链路的物理层 (L1) 在两端均处于连接状态，但只有一侧接收数据包。
- 收发器未连接至正确的端口。

FEFD 状态

FEFD 包含以下四种状态：

- Idle — FEFD 已禁用。
- Unknown — 当 FEFD 启用并且在与对等方成功握手后更改为 bi-directional。此外，如果对等方在 normal 模式下停机也会显示。
- bi-directional — 接口已启动、已连接并正在接收其邻居的回声。
- err-disabled — 仅当 FEFD 模式是 aggressive 且接口未收到其邻居的三个回声时才会找到。要在此状态下重置接口，请使用 fefd reset 命令。

FEFD 模式

FEFD 以两种模式运行 — 正常模式和攻击模式。

- 正常模式 — 在接口上启用正常模式并且检测到远端故障时，无需进行任何干预即可重置接口，使其恢复 FEFD 的运行状态。
- 攻击模式 — 在处于相同状态的接口上启用攻击模式时，您必须手动重置该接口。

以下事件说明了如何进行 FEFD 状态转换：

- 当您在接口上启用 FEFD 时，链路会从空闲状态转换为未知状态。
- 在未知状态下，接口会以固定的时间间隔开始发送链路状态信息。当对等方完成握手后，接口状态将更改为双向。
- 当某个接口处于双向状态时，如果它不会从对等主机接收到配置的 FEFD 消息间隔三倍的时间间隔，则在正常模式下，接口状态将更改为未知。在攻击模式下，接口状态将更改为 err-disabled。

如果接口状态更改为 err-disabled，请使用 fefd reset [interface] 全局命令重置这些接口。未知或 err-disabled 状态使线路协议关闭，因此它上面的协议可以检测到对等链路已关闭。

表. 30: FEFD 状态更改

| 本地事件<br>(用户干预)           | 配置的 FEFD<br>模式 | 本地状态<br>(显示显示屏)<br>(结果) | 本地管理员<br>状态<br>(结果) | 本地线路协议<br>状态<br>(结果) | 远程状态<br>(显示显示屏)<br>(结果) | 远程管理员状<br>态 | 远程线路协议<br>状态 |
|--------------------------|----------------|-------------------------|---------------------|----------------------|-------------------------|-------------|--------------|
| 关机 (用户配置)                | 正常             | 管理员关闭                   | 关闭                  | 关闭                   | 线路协议关闭。                 | 上移          | 关闭           |
| 关机 (用户配置)                | 攻击             | 管理员关闭                   | 关闭                  | 关闭                   | 线路协议关闭。                 | 上移          | 关闭           |
| FEFD + FEFD<br>禁用 (用户配置) | 正常             | 本地已禁用                   | 上移                  | 上移                   | 未知                      | 上移          | 关闭           |
| FEFD + FEFD<br>禁用 (用户配置) | 攻击             | 本地已禁用                   | 上移                  | 关闭                   | Err-disabled            | 上移          | 关闭           |
| 链路故障 (卸下<br>线缆或收发器)      | 正常             | 未知                      | 上移                  | 关闭                   | 未知                      | 上移          | 关闭           |
| 链路故障 (卸下<br>线缆或收发器)      | 攻击             | 未知                      | 上移                  | 关闭                   | 未知                      | 上移          | 关闭           |
| FEFD 启用<br>(用户配置)        | 正常             | 双向                      | 上移                  | 上移                   | 双向                      | 上移          | 上移           |

表. 30: FEFD 状态更改 (续)

| 本地事件<br>(用户干预)    | 配置的 FEFD<br>模式 | 本地状态<br>(显示显示屏)<br>(结果) | 本地管理员<br>状态<br>(结果) | 本地线路协议<br>状态<br>(结果) | 远程状态<br>(显示显示屏)<br>(结果) | 远程管理员状态 | 远程线路协议<br>状态 |
|-------------------|----------------|-------------------------|---------------------|----------------------|-------------------------|---------|--------------|
| FEFD 启用<br>(用户配置) | 攻击             | 双向                      | 上移                  | 上移                   | 双向                      | 上移      | 上移           |

限制

- 您可以全局启用 FEFD 或在接口上启用。如果全局启用 FEFD，则 FEFD 接口配置会覆盖全局 FEFD 配置。
- OS10 仅在物理接口上支持 FEFD。在任何其他接口上不支持 FEFD。但是，您可以对属于某个端口通道的单个物理接口启用 FEFD。

全局启用 FEFD

要全局配置 FEFD：

1. 请执行以下某项操作：

- 在 CONFIGURATION 模式下使用 `fehd-global` 命令在全局范围内配置 FEFD 正常模式。

```
OS10(Config)# fehd-global
```

- 在 CONFIGURATION 模式下使用 `fehd-global mode normal` 命令在全局范围内配置 FEFD 正常模式。

```
OS10(Config)# fehd-global mode normal
```

- 在 CONFIGURATION 模式下使用 `fehd-global mode aggressive` 命令在全局范围内配置 FEFD 攻击模式。

```
OS10(Config)# fehd-global mode aggressive
```

2. (可选) 在 CONFIGURATION 模式下使用 `fehd-global interval` 命令配置 FEFD 间隔并输入间隔（以秒为单位）。范围为 3 到 255 秒。

```
OS10(Config)# fehd-global interval 20
```

3. (可选) 如果需要，请在 INTERFACE 模式下使用 `fehd disable` 命令来禁用特定接口上的 FEFD。

```
OS10(Config-if-eth1/1/1)# no fehd interval 20
```

启用接口上的 FEFD

要在接口上配置 FEFD，请执行以下操作：

1. 请执行以下某项操作：

- 在 INTERFACE 模式下使用 `fehd` 命令在接口上配置 FEFD 正常模式。

```
OS10(Config-if-eth1/1/1)# fehd
```

- 在 INTERFACE 模式下使用 `fehd mode normal` 命令在接口上配置 FEFD 正常模式。

```
OS10(Config-if-eth1/1/1)# fehd mode normal
```

- 在 INTERFACE 模式下使用 `fehd mode aggressive` 命令在接口上配置 FEFD 攻击模式。

```
OS10(Config-if-eth1/1/1)# fehd mode aggressive
```

2. (可选) 在 INTERFACE 模式下使用 `fefd interval` 命令配置 FEFD 间隔并输入间隔 (以秒为单位)。范围为 3 到 255 秒。

```
OS10(Config-if-eth1/1/1)# fefd interval 20
```

## Reset FEFD err-disabled interface

当系统在 FEFD 攻击模式下检测到远端故障时，该接口会移动到 `err-disabled` 状态。要使接口返回 FEFD 运行状态，请执行以下操作：

- 在 EXEC 模式下输入 `fefd reset` 命令。

```
OS10# fefd reset ethernet 1/1/1
```

## 显示 FEFD 信息

要查看 FEFD 信息，请执行以下操作：

- 要全局查看 FEFD 信息，请在 EXEC 模式下使用 `show fefd` 命令。
- 要查看某个接口的 FEFD 信息，请在 EXEC 模式下使用 `show fefd interface` 命令。

以下是 FEFD 全局信息的输出示例：

```
OS10# show fefd
FEFD is globally 'ON', interval is 15 seconds, mode is Normal.
INTERFACE MODE INTERVAL STATE
=====
eth1/1/1 NA NA Idle (Not running)
eth1/1/2 NA NA Idle (Not running)
eth1/1/3 NA NA Idle (Not running)
eth1/1/4 NA NA Idle (Not running)
eth1/1/5 NA NA Idle (Not running)
eth1/1/6 NA NA Idle (Not running)
eth1/1/7 NA NA Idle (Not running)
```

以下是接口的 FEFD 信息的输出示例：

```
rt-maa-s4248FBL-3# show fefd ethernet 1/1/1
FEFD is globally 'ON', interval is 15 seconds, mode is Normal.
INTERFACE MODE INTERVAL STATE
=====
eth1/1/1 NA NA Idle (Not running)
```

## FEFD 命令

### debug fefd

启用 FEFD 调试。

|      |                                                                                                                                                                                                                                                                |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | <code>debug fefd {all   events   packets} [interface]</code>                                                                                                                                                                                                   |
| 参数   | <ul style="list-style-type: none"><li><code>all</code> — 输入关键字以查看所有 FEFD 调试信息。</li><li><code>events</code> — 输入关键字以查看有关 FEFD 状态更改的调试信息。</li><li><code>packets</code> — 输入关键字以查看有关发送和接收的 FEFD 数据包的调试信息。</li><li>(可选) <code>interface</code> — 输入接口信息。</li></ul> |
| 默认   | 未配置                                                                                                                                                                                                                                                            |
| 命令模式 | EXEC 特权                                                                                                                                                                                                                                                        |

|       |                             |
|-------|-----------------------------|
| 示例    | <pre>OS10# debug fefd</pre> |
| 支持的版本 | 10.4.3.0 or later           |

## fefd

在接口上配置 FEFD。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>fefd [mode {normal   aggressive}   interval <b>seconds</b>   disable]</code>                                                                                                                                                                                                                                                                                                                                                                  |
| 参数     | <ul style="list-style-type: none"><li>（可选）<code>mode</code> — 输入关键字并输入 <code>normal</code> 以启用正常模式或 <code>aggressive</code> 以启用攻击模式。</li><li><code>interval</code> — 输入关键字并输入 FEFD 间隔（以秒为单位），以配置接口上 FEFD 控制数据包之间的间隔。范围是从 3 到 255。默认值为 15 秒。</li><li><code>disable</code> — 在全局配置 FEFD 时，输入关键字以禁用特定接口上的 FEFD。</li></ul>                                                                                                                              |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 命令模式   | INTERFACE                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 使用情况信息 | <p>不带任何参数的 <code>fefd</code> 命令将启用正常模式，默认 FEFD 间隔为 15 秒。</p> <p>如果您使用 <code>no fefd</code> 命令，则系统不会禁用 FEFD（如果 <code>fefd mode</code> 命令已存在于配置中）。同样，如果使用 <code>no fefd mode</code> 命令，则系统不会禁用 FEFD（如果 <code>fefd</code> 命令已存在于配置中）。</p> <p>要在 FEFD 全局启用的情况下禁用接口上的 FEFD，请在接口上使用 <code>fefd disable</code> 命令。</p> <p>要取消配置接口上的 FEFD，请使用 <code>no fefd</code> 命令或 <code>no fefd mode</code> 命令。要返回默认 FEFD 间隔，请使用 <code>no fefd interval</code> 命令。</p> |

|    |                                                          |
|----|----------------------------------------------------------|
| 示例 | <pre>OS10(conf-if-eth1/1/9)# fefd</pre>                  |
|    | <pre>OS10(conf-if-eth1/1/9)# fefd mode aggressive</pre>  |
|    | <pre>OS10(conf-if-eth1/1/9)# fefd mode interval 10</pre> |

|       |                   |
|-------|-------------------|
| 支持的版本 | 10.4.3.0 or later |
|-------|-------------------|

## fefd-global

全局配置 FEFD。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>fefd-global [mode {normal   aggressive}   interval <b>seconds</b>]</code>                                                                                                                                                                                                                                                                                                                                                    |
| 参数     | <ul style="list-style-type: none"><li>（可选）<code>mode</code> — 输入关键字并输入 <code>normal</code> 以启用正常模式或 <code>aggressive</code> 以启用攻击模式。</li><li>（可选）<code>interval</code> — 输入关键字并输入 FEFD 间隔（以秒为单位），以配置全局 FEFD 控制数据包之间的间隔。范围是从 3 到 255。默认值为 15 秒。</li></ul>                                                                                                                                                                           |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 使用情况信息 | <p>不带参数的 <code>fefd-global</code> 命令将启用正常模式，默认 FEFD 间隔为 15 秒。</p> <p>如果您使用 <code>no fefd-global</code> 命令，则系统不会禁用 FEFD（如果 <code>fefd-global mode</code> 命令已存在于配置中）。同样，如果使用 <code>no fefd-global mode</code> 命令，则系统不会禁用 FEFD（如果 <code>fefd-global</code> 命令已存在于配置中）。</p> <p>要在全局范围内取消配置 FEFD，请使用 <code>no fefd-global</code> 命令或 <code>no fefd-global mode</code> 命令。要返回默认 FEFD 间隔，请使用 <code>no fefd-global interval</code> 命令。</p> |

|       |                                           |
|-------|-------------------------------------------|
| 示例    | OS10(config)# fefd-global                 |
|       | OS10(config)# fefd-global mode aggressive |
|       | OS10(config)# fefd mode interval 10       |
| 支持的版本 | 10.4.3.0 or later                         |

fefd reset

重置处于禁用错误状态的接口，因为 FEFD 被设置为攻击模式。

|        |                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------|
| 语法     | fefd reset [ <i>interface</i> ]                                                                             |
| 参数     | <ul style="list-style-type: none"> <li>(可选) <i>interface</i> — 输入接口名称以重置接口的禁用状态，因为 FEFD 设置为攻击模式。</li> </ul> |
| 默认     | 未配置                                                                                                         |
| 命令模式   | EXEC                                                                                                        |
| 使用情况信息 | 如果不输入接口名称，此命令将重置所有接口的错误禁用状态，因为 FEFD 设置为攻击模式。                                                                |
| 示例     | OS10# fefd reset                                                                                            |
|        | OS10# fefd reset ethernet 1/1/2                                                                             |
| 支持的版本  | 10.4.3.0 or later                                                                                           |

show fefd

全局或为特定接口显示 FEFD 信息。

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法              | show fefd [ <i>interface</i> ]                                                                                                                                                                                                                                                                                                                                                                                            |
| 参数              | <ul style="list-style-type: none"> <li>(可选) <i>interface</i> — 输入接口信息。</li> </ul>                                                                                                                                                                                                                                                                                                                                         |
| 默认              | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 命令模式            | EXEC 和 EXEC 权限                                                                                                                                                                                                                                                                                                                                                                                                            |
| 使用情况信息          | 下表介绍了 show fefd 命令输出中的字段：                                                                                                                                                                                                                                                                                                                                                                                                 |
| 字段              | 说明                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 接口              | 显示接口名称                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 模式              | 当接口在其配置中包含 fefd reset 时，显示模式 — 攻击、正常或不适用。                                                                                                                                                                                                                                                                                                                                                                                 |
| Interval (间隔时间) | 显示 FEFD 数据包之间的间隔。                                                                                                                                                                                                                                                                                                                                                                                                         |
| 状态              | 显示接口的状态，可以是以下项之一： <ul style="list-style-type: none"> <li>双向 — 接口已启动、已连接，并且正在接收其邻居的回显。</li> <li>Err-disabled — 仅当 FEFD 模式是 Aggressive 且接口未收到其邻居的三个回声时才会找到。要在此状态下重置接口，请使用 fefd reset 命令。</li> <li>Unknown — 当 FEFD 启用并且在与对等方成功握手后更改为 bi-directional。此外，如果对等方在 normal 模式下停机也会显示。</li> <li>本地禁用 — 接口的配置中包含 fefd reset 命令。</li> <li>管理员关闭 — 使用 Shutdown 命令禁用接口。</li> <li>线路协议关闭 — 在使用 shutdown 命令禁用本地设备接口时远程设备上的状态。</li> </ul> |

示例

```
OS10# show fefd
FEFD is globally 'ON', interval is 22 seconds,mode is NORMAL.
INTERFACE MODE INTERVAL STATE
=====
eth1/1/1 Normal 22 Unknown
eth1/1/2 Normal 22 Unknown
eth1/1/3 Normal 22 Unknown
eth1/1/4 Normal 22 Unknown
eth1/1/5 Normal 22 Unknown
eth1/1/6 Normal 22 Unknown
eth1/1/7 Normal 22 Unknown
eth1/1/8 Normal 22 Unknown
eth1/1/9 Aggressive 22 Err-disabled
eth1/1/10 Normal 22 Unknown
```

支持的版本 10.4.3.0 or later

链路聚合控制协议

分组以太网接口以形成单个链路层接口，名为 LAG 或端口通道。在物理接口之间聚合多个链路可创建单个逻辑 LAG，这将平衡聚合的以太网套装中的成员链路上的流量，并增加上行链路带宽。如果一个成员链路失败，LAG 将继续通过剩余链路传输流量。有关 LAG 负载均衡和哈希的信息，请参阅[负载均衡](#)。

您可以使用 LACP 在两个系统（也称为伙伴系统）之间创建动态滞后的交换信息，并自动在系统之间建立 LAG。LACP 允许在链路上交换消息，请执行以下操作：

- 同意该链路所属 LAG 的身份。
- 将链接移动到该 LAG。
- 启用传输和接收功能。

LACP 通过跨 LAN 以太网链路持续交换自定义 MAC PDU 来运行。该协议仅在配置为支持 LACP 的端口之间交换数据包。

模式

LAG 包括三种配置模式 — 打开、活动和非活动。

- 开启** 将通道模式设置为静态。接口充当静态 LAG 的成员。
- 活动** 将接口设置为活动协商状态。LACP 在此模式下配置的任何链路上运行。主动模式下的端口会通过使用 LACP 数据包自动发起与其他端口的协商。主动模式下的端口可在主动模式或被动模式下使用另一个端口设置端口通道。
- 被动** 将接口设置为非活动的协商状态，但 LACP 在链路上运行。被动模式下的端口还会响应协商请求（在活动模式的端口中）。被动模式下的端口响应 LACP 数据包。被动模式下的端口无法在被动模式下使用另一个端口设置 LAG。

- 静态和动态 LAG 中更没有双重成员关系：
  - 如果物理接口是静态 LAG 的一部分，该 `channel-group id mode active` 命令将在该接口上被拒绝。
  - 如果物理接口是动态 LAG 的一部分，该 `channel-group id` 命令将在该接口上被拒绝。
- 您不能将静态和动态成员添加到相同的 LAG。
- `shutdown` 和 `no interface port-channel` 命令之间存在差异：
  - LAG 上的 `shutdownxyz` 命令将禁用 LAG，并保留用户命令。
  - `no interface port-channel channel-number` 命令将删除指定的 LAG，包括动态创建的 LAG。接口恢复并准备好进行配置。
- 每个通道最多允许 128 个端口通道，每个通道最多 16 个成员。

配置

默认情况下，LACP 处于全局启用状态。您可以配置具有兼容的活动和被动 LACP 模式的聚合端口，以自动链接它们。

1. 在 CONFIGURATION 模式下配置系统优先级（1 到 65535；数字越高，优先级越低；默认值为 32768）。

```
lacp system-priority priority-value
```

2. 在 INTERFACE 模式下配置 LACP 端口优先级（1 到 65535；数字越高，优先级越低；默认值为 32768）。

```
lacp port-priority priority-value
```

3. 在 INTERFACE 模式下配置 LACP 率（默认正常）。

```
lacp rate [fast | normal]
```

## 配置 LACP

```
OS10(config)# lacp system-priority 65535
OS10(config)# interface range ethernet 1/1/7-1/1/8
OS10(conf-range-eth1/1/7-1/1/8)# lacp port-priority 4096
OS10(conf-range-eth1/1/7-1/1/8)# lacp rate fast
```

## 验证 LACP 配置

```
OS10(conf-range-eth1/1/7-1/1/8)# do show running-configuration
...
!
interface ethernet1/1/7
 lacp port-priority 4096
 lacp rate fast
 no shutdown
!
interface ethernet1/1/8
 lacp port-priority 4096
 lacp rate fast
 no shutdown
!
...
```

# 接口

创建 LAG 并添加 LAG 成员接口。默认情况下，所有接口都处于 no shutdown 和 switchport 模式。

1. 在 CONFIGURATION 模式下创建 LAG。

```
interface port-channel port-channel number
```

2. 进入 INTERFACE 模式。

```
interface ethernet node/slot/port[:subport]
```

3. 在 INTERFACE 模式下将通道组模式设置为有效。

```
channel-group number mode active
```

## 配置动态 LAG 接口

```
OS10(config)# interface port-channel 10
OS10(conf-if-po-10)# exit
OS10(config)# interface ethernet 1/1/10
OS10(conf-if-eth1/1/10)# no switchport
OS10(conf-if-eth1/1/10)# channel-group 10 mode active
OS10(conf-if-eth1/1/10)# exit
OS10(config)# interface ethernet 1/1/11
OS10(conf-if-eth1/1/11)# no switchport
OS10(conf-if-eth1/1/11)# channel-group 10 mode active
```



## 速率

协议数据单元 (PDU) 在端口通道 (LAG) 接口之间交换以保持 LACP 会话。PDU 以较慢或较快的传输速率进行传输，具体取决于 LACP 超时值。超时值是 LAG 接口在 LACP 会话停止之前等待来自远程系统 PDU 的时间量。

默认情况下，LACP 速率为 **normal**（长超时）。如果配置 **fast** LACP 速率，将会设置短的超时。

- 设置 CONFIGURATION 模式下的 LACP 速率。

```
lacp rate [fast | normal]
```

### 配置 LACP 超时

```
OS10(conf-if-eth1/1/29)# lacp rate fast
```

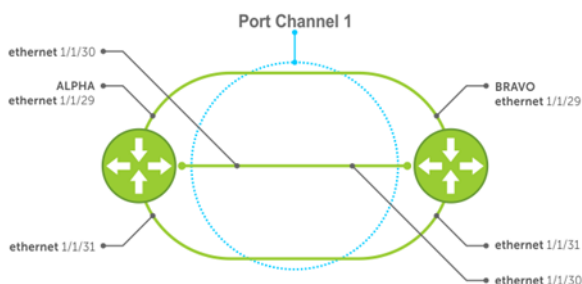
### 查看端口状态

```
OS10# show lacp port-channel
```

```
Port-channel 20 admin up, oper up, mode lacp
Actor System ID: Priority 32768, Address f8:b1:56:00:02:33
Partner System ID: Priority 4096, Address 10:11:22:22:33:33
Actor Admin Key 20, Oper Key 20, Partner Oper Key 10
LAG ID 20 is an aggregatable link
A - Active LACP, B - Passive LACP, C - Short Timeout, D - Long Timeout
E - Aggregatable Link, F - Individual Link, G - IN_SYNC, H - OUT_OF_SYNC,
I - Collection enabled, J - Collection disabled, K - Distribution enabled,
L - Distribution disabled, M - Partner Defaulted, N - Partner Non-defaulted,
O - Receiver is in expired state, P - Receiver is not in expired state
Port ethernet1/1/14 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State BCFHJKNO Key 20 Priority 32768
Oper: State BDEGIKNO Key 20 Priority 32768
Partner Admin: State BCEGIKNP Key 0 Priority 0
Oper: State BDEGIKNO Key 10 Priority 32768
Port ethernet1/1/16 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State BCFHJKNO Key 20 Priority 32768
Oper: State BDEGIKNO Key 20 Priority 32768
Partner Admin: State BCEGIKNP Key 0 Priority 0
Oper: State BDEGIKNO Key 10 Priority 32768
```

## 配置示例

此示例拓扑基于两个路由器 — Alpha 和 Bravo。



### Alpha LAG 配置摘要

```
OS10(config)# interface port-channel 1
OS10(conf-if-po-1)# exit
OS10(config)# interface ethernet 1/1/29
OS10(conf-if-eth1/1/29)# no switchport
OS10(conf-if-eth1/1/29)# channel-group 1 mode active
OS10(conf-if-eth1/1/29)# interface ethernet 1/1/30
OS10(conf-if-eth1/1/30)# no switchport
OS10(conf-if-eth1/1/30)# channel-group 1 mode active
```

```
OS10(config-if-eth1/1/30)# interface ethernet 1/1/31
OS10(config-if-eth1/1/31)# no switchport
OS10(config-if-eth1/1/31)# channel-group 1 mode active
```

## Bravo LAG 配置摘要

```
OS10(config)# interface port-channel 1
OS10(config-if-po-1)# exit
OS10(config)# interface ethernet 1/1/29
OS10(config-if-eth1/1/29)# no switchport
OS10(config-if-eth1/1/29)# channel-group 1 mode active
OS10(config-if-eth1/1/29)# interface ethernet 1/1/30
OS10(config-if-eth1/1/30)# no switchport
OS10(config-if-eth1/1/30)# channel-group 1 mode active
OS10(config-if-eth1/1/30)# interface ethernet 1/1/31
OS10(config-if-eth1/1/31)# no switchport
OS10(config-if-eth1/1/31)# channel-group 1 mode active
```

## Alpha 验证 LAG 端口配置

```
OS10# show lacp port-channel
```

```
Port-channel 1 admin up, oper up, mode lacp
Actor System ID: Priority 32768, Address 34:17:eb:f2:c7:c4
Partner System ID: Priority 32768, Address 34:17:eb:f2:9b:c4
Actor Admin Key 1, Oper Key 1, Partner Oper Key 1
LACP LAG ID 1 is an aggregatable link
A - Active LACP, B - Passive LACP, C - Short Timeout, D - Long Timeout
E - Aggregatable Link, F - Individual Link, G - IN_SYNC, H - OUT_OF_SYNC,
I - Collection enabled, J - Collection disabled, K - Distribution enabled,
L - Distribution disabled, M - Partner Defaulted, N - Partner Non-defaulted,
O - Receiver is in expired state, P - Receiver is not in expired state
Port ethernet1/1/29 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State BCFHJKNO Key 1 Priority 32768
Oper: State BDEGIKNO Key 1 Priority 32768
Partner Admin: State BCEGIKNP Key 0 Priority 0
Oper: State BDEGIKNO Key 1 Priority 32768
Port ethernet1/1/30 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State BCFHJKNO Key 1 Priority 32768
Oper: State BDEGIKNO Key 1 Priority 32768
Partner Admin: State BCEGIKNP Key 0 Priority 0
Oper: State BDEGIKNO Key 1 Priority 32768
Port ethernet1/1/31 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State BCFHJKNO Key 1 Priority 32768
Oper: State BDEGIKNO Key 1 Priority 32768
Partner Admin: State BCEGIKNP Key 0 Priority 0
Oper: State BDEGIKNO Key 1 Priority 32768
```

## Bravo 验证 LAG 端口配置

```
bravo# show interface ethernet 1/1/29
```

```
Ethernet 1/1/29 is up, line protocol is up
Port is part of Port-channel
Hardware is Dell EMC Eth, address is 90:b1:1c:f4:9b:a2
Current address is 90:b1:1c:f4:9b:a2
Pluggable media present, QSFP+ type is QSFP+ 40GBASE CR 1.0M
Wavelength is 25
SFP receive power reading is 0.0
Interface index is 16866812
Internet address is not set
Mode of IPv4 Address Assignment : not set
MTU 1532 bytes, IP MTU bytes
LineSpeed auto
Flowcontrol rx tx
ARP type: ARPA, ARP Timeout: 240
Last clearing of show "interface" counters :
Queuing strategy : fifo
Input statistics:
 466 packets, 45298 octets
 224 64-byte pkts, 1 over 64-byte pkts, 241 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
```

```

 466 Multicasts, 0 Broadcasts
 0 runts, 0 giants, 0 throttles
 0 CRC, 0 overrun, 465 discarded
Output statistics:
 7840 packets, 938965 octets
 0 64-byte pkts,1396 over 64-byte pkts, 6444 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
 7840 Multicasts, 0 Broadcasts,0 Unicasts
 0 throttles, 0 discarded, 0 Collisions, 0 wredrops
Rate Info(interval 299 seconds):
 Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
 Output 0 Mbits/sec, 1 packets/sec, 0% of line rate
Time since last interface status change : 01:25:29

```

## 验证 LAG 1

```

OS10# show interface port-channel 1

Port-channel 1 is up,line protocol is up
Hardware address is Current address is
Interface index is 85886081
Minimum number of links to bring Port-channel up is 1
Internet address is not set
Mode of IPv4 Address Assignment : not set
Lag MTU is 1500 ,IP MTU bytes
Linespeed AUTO
Members in this channel ethernet1/1/29 ethernet1/1/30 ethernet1/1/31
ARP type: ARPA Arp timeout: 240
Last clearing of "show interface" counters :
Queuing strategy :fifo
Input statistics:
1388 packets, 135026 octets
666 64-byte pkts,1 over 64-byte pkts, 721 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
1388 Multicasts, 0 Broadcasts
0 runts, 0 giants, 0 throttles
0 CRC, 0 overrun, 1387 discarded
Output statistics:
2121444503 packets, 135773749275 octets
2121421152 64-byte pkts,4182 over 64-byte pkts, 19169 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
23351 Multicasts, 0 Broadcasts,2121421152 Unicasts
0 throttles, 143426 discarded, 0 Collisions, 0 wredrops
Rate Info(interval 299 seconds):
Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
Output 0 Mbits/sec, 3 packets/sec, 0% of line rate
Time since last interface status change : 01:24:43

```

## 验证 LAG 状态

```

OS10# show lacp port-channel

Port-channel 1 admin up, oper up, mode lacp
Actor System ID: Priority 32768, Address 90:b1:1c:f4:9b:8a
Partner System ID: Priority 32768, Address 00:01:e8:8a:fd:9e
Actor Admin Key 1, Oper Key 1, Partner Oper Key 1
LACP LAG ID 1 is an aggregatable link

A - Active LACP, B - Passive LACP, C - Short Timeout, D - Long Timeout
E - Aggregatable Link, F - Individual Link, G - IN_SYNC, H - OUT_OF_SYNC,
I - Collection enabled, J - Collection disabled, K - Distribution enabled,
L - Distribution disabled, M - Partner Defaulted, N - Partner Non-defaulted,
O - Receiver is in expired state, P - Receiver is not in expired state

Port ethernet1/1/29 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State Key 1 Priority 32768
Oper: State Key 1 Priority 32768
Partner Admin: State Key 0 Priority 0
Oper: State Key 1 Priority 32768
Port ethernet1/1/30 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State Key 1 Priority 32768
Oper: State Key 1 Priority 32768

```

```
Partner Admin: State Key 0 Priority 0
Oper: State Key 1 Priority 32768
Port ethernet1/1/31 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State Key 1 Priority 32768
Oper: State Key 1 Priority 32768
Partner Admin: State Key 0 Priority 0
Oper: State Key 1 Priority 32768
```

## 验证 LAG 成员资格

```
OS10# show lacp interface ethernet 1/1/29

Interface ethernet1/1/29 is up
Channel group is 1 port channel is po1
PDUS sent: 17
PDUS rcvd: 11
Marker sent: 0
Marker rcvd: 0
Marker response sent: 0
Marker response rcvd: 0
Unknown packetse rcvd: 0
Illegal packetse rcvd: 0
Local Port: MAC Address=74:e6:e2:f5:b5:80
System Identifier=32768,32768
Port Identifier=32768,32768
Operational key=1
LACP_Activity=passive
LACP_Timeout=Long Timeout(30s)
Synchronization=IN_SYNC
Collecting=true
Distributing=true
Partner information refresh timeout=Long Timeout(90s)
Actor Admin State=BCFHJKNO
Actor Oper State=BDEGIKNO
Neighbor: 276
MAC Address=00:00:00:00:00:00
System Identifier=,00:00:00:00:00:00
Port Identifier=0,14:18:77:7a:2d:00
Operational key=1
LACP_Activity=passive
LACP_Timeout=Long Timeout(30s)
Synchronization=IN_SYNC
Collecting=true
Distributing=true
Partner Admin State=BCEGIKNP
Partner Oper State=BDEGIKNO
```

## LACP 回退

LACP 回退允许下游设备（例如连接到配置为 LACP 的交换机端口的服务器）在系统无法完成 LACP 握手时建立链接。

例如，当服务器以 PXE 模式启动时，服务器无法交换 LACP PDU，并且交换机不会启用这些端口。

每当 PXE 服务器重新引导时，端口通道和端口都会停止运行。在重新引导时，端口将启动，而不是端口通道。LACP 回退使端口通道能够正常运行，并将数据包发送至 PXE 服务器。

启用 LACP 回退后，交换机将启动计时器。如果计时器在 LACP 完成之前过期，则交换机将选择端口组的一个端口并使其正常运行。

您可以使用 `lacp fallback timeout timer-value` 命令来设置计时器。

如果在特定时间段内没有从对等节点接收 LACP PDU，LACP 回滚功能会将成员端口添加到 LACP 端口通道。

服务器使用回退端口来完成 PXE 引导过程。当服务器从操作系统启动时，该进程将完成 LACP 握手，而回退端口重新组合其他成员。成员端口将变为活动状态，并将数据包发送到 PXE 服务器。

当交换机开始接收 LACP PDU 时，OS10 将静态添加的成员端口与 LACP 端口通道取消组合，并使用正常 LACP 功能继续。

当您启用 LACP 回退时，将根据以下条件选择显示的端口：

- LACP 端口优先级配置允许确定端口分配。当端口通道处于 LACP 回滚模式时，优先级最低的端口将处于活动状态。

- 如果端口通道中的所有端口具有相同的端口优先级，交换机将在内部通过基本名称、模块号、端口号来比较接口名称，然后选择要激活的最低值。例如，以太网 1 小于以太网 2，因此以太网 1 变为活动状态。
- 在 VLT 网络中，如果两个 VLT 对等节点上的接口名称相同，则具有较低系统 MAC 地址的交换机中的端口将变为活动状态。

- 限制**
- OS10 交换机不能是 PXE 客户端，无论其是作为 VLT 对等节点还是 ToR 交换机。
  - 如果要在 VLT 域中配置 LACP 回退，请在两个 VLT 对等节点中配置 `lacp fallback` 命令。
  - 如果您未在其中一个 VLT 对等节点中启用 LACP 回退，或者在对等节点中配置不同的超时值，则交换机的行为可能会有所不同。
  - 只有当交换机未收到来自对等节点的 LACP PDU 时，LACP 回退功能才会向端口通道添加或分组成员端口，以使连接到 PXE 客户端设备的链路正常运行。当 PXE 客户端处理未标记的 DHCP 请求时，您需要在未标记的 VLAN 上配置 LACP 回退，以访问 DHCP/PXE 服务器。
  - 在 LACP 回退选择之后，如果优先级端口较低的端口配置为属于相同的端口通道，则会触发再选。

## 配置 LACP 回退

1. 在端口通道 INTERFACE 模式下，使用 `lacp fallback enable` 命令启用 LACP 回退。
2. 在端口通道 INTERFACE 模式下，使用 `lacp fallback timeout timer-value` 设置接收 LACP PDU 的计时器。
3. （可选）在端口通道 INTERFACE 模式下，使用 `lacp fallback preemption {enable | disable}` 启用或禁用 LACP 回退端口抢占。

**配置示例**

```
OS10# configure terminal
OS10(config)# interface port-channel 1
OS10(conf-if-po-1)# lacp fallback enable
OS10(conf-if-po-1)# lacp fallback timeout 20
OS10(conf-if-po-1)# lacp fallback preemption enable
```

**查看 LACP 回退配置**

```
OS10# show port-channel summary

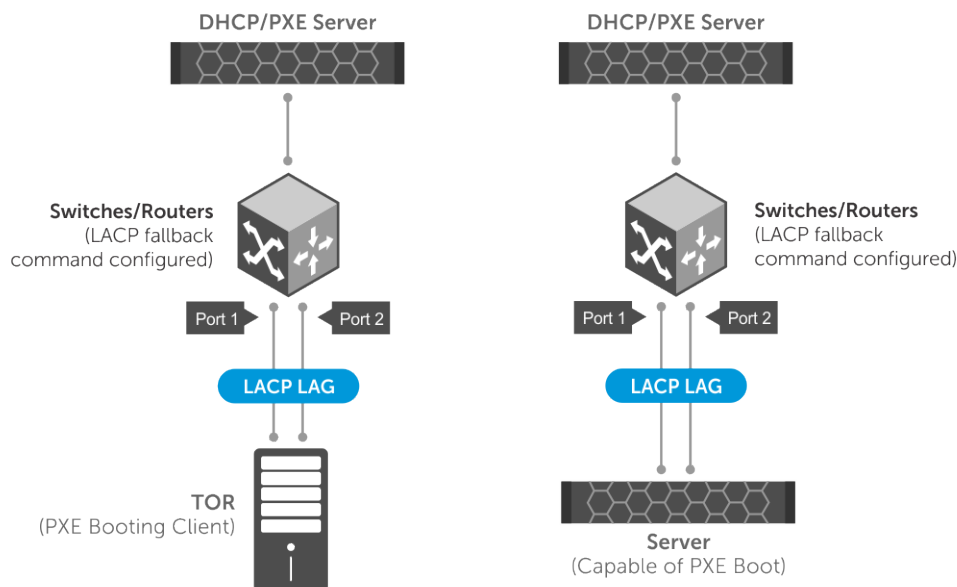
Flags: D - Down I - member up but inactive P - member up and active
 U - Up (port-channel) F - Fallback enabled

Group Port-Channel Type Protocol Member Ports

1 port-channel11 (UF) Eth DYNAMIC 1/1/10 (P) 1/1/11 (I)
```

## 在非 VLT 网络中的 LACP 回退

在非 VLT 网络中，LACP 回退允许通过正常 LACP 重新启动连接到交换机的 ToR 或服务器。交换机的另一端连接到 DHCP/PXE 服务器，如下图所示：

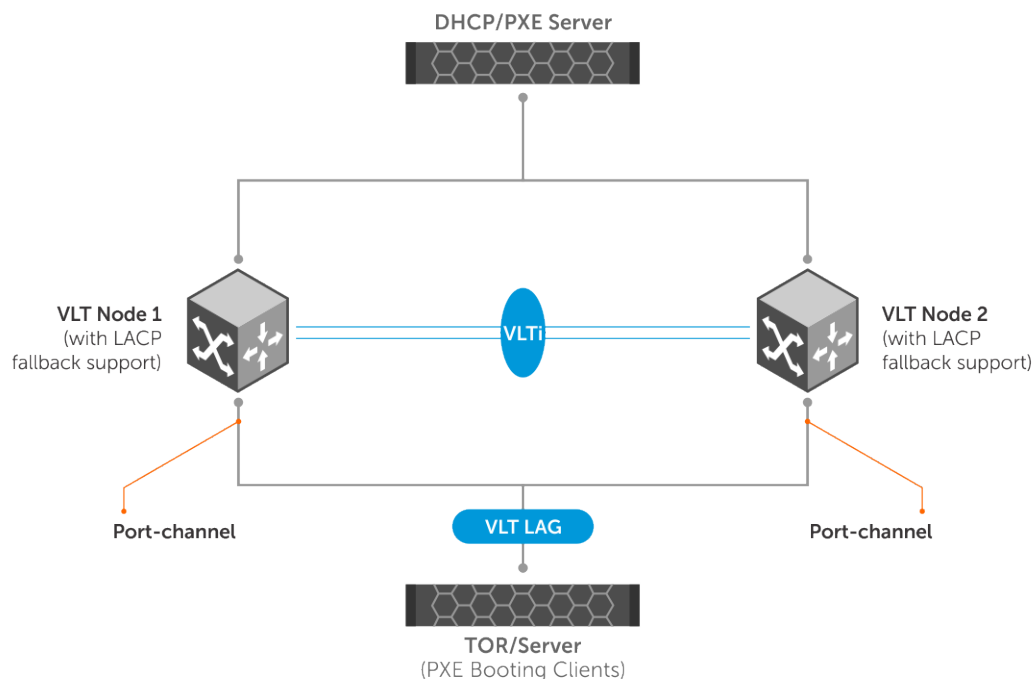


在上述情况下，LACP 回退的工作方式如下所示：

1. ToR/服务器引导
2. 交换机会检测到已启动的链路，并检查已启用回退的状态。如果启用了回退，设备将等待任何 LACP BPDU 的超时时间。如果在该时间段内未收到 LACP BPDU，则 LAG 进入回退模式，并将第一个正在运行的 UP 端口添加到端口通道，而不是将其置于非活动状态。
3. 现在 ToR/服务器将启动一个端口并处于活动状态。活动端口将数据包发送到 DHCP/PXE 服务器。
4. 从 DHCP 服务器接收响应后，ToR/服务器从 TFTP/NFS 服务器引导。
5. 当 ToR/服务器使用引导映像和配置完全加载时，服务器将开始发送 LACP PDU。
6. 当交换机从 ToR/服务器接收 LACP PDU 时，设备将从回退模式退出，并通过正常的 LACP 进程激活 LAG。

## VLT 域中的 LACP 回退

在 VLT 域中，LACP 回退允许通过 VLT 端口通道重新引导连接至 VLT 节点的 ToR 或服务器。VLT 节点的另一端连接到 DHCP/PXE 服务器，如下图所示：



在上述情况下，LACP 回退的工作方式如下所示：

1. ToR/服务器引导
2. 其中一个 VLT 对等节点负责控制 LACP 回退模式。所有事件都将发送到控制 VLT 对等节点，以确定应启动的端口，然后决定将传递给对等设备。
3. 控制 VLT 对等节点可以决定在本地端口通道或对等 VLT 端口通道中打开其中一个端口。
4. 其中一个端口、本地或对等节点，将根据控制 VLT 对等方的决定变为活动状态。
5. 现在 ToR/服务器将启动一个端口并处于活动状态。活动端口将数据包发送到 DHCP/PXE 服务器。
6. 从 DHCP 服务器接收响应后，ToR/服务器从 TFTP/NFS 服务器引导。
7. 当 ToR/服务器使用引导映像和配置完全加载时，服务器将开始发送 LACP PDU。
8. 当交换机从 ToR/服务器接收 LACP PDU 时，控制 VLT 对等节点将使 LACP 端口进入回退模式并恢复正常功能。

## LACP 命令

### channel-group

为端口通道组分配和配置物理接口。

|           |                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b> | <code>channel-group number mode {active   on   passive}</code>                                                                                                                                                                                                                                                                                                                                  |
| <b>参数</b> | <ul style="list-style-type: none"> <li>• <i>number</i> — 输入端口通道组编号（1 至 128）。最大端口通道数为 128。支持最大物理端口/最大 NPU。</li> <li>• <i>mode</i> — 输入接口端口通道模式。</li> <li>• <i>active</i> — 输入以启用 LACP 接口。当端口通过发送 LACP 数据包与其他端口开始协商时，接口处于活动协商状态。</li> <li>• <i>on</i> — 输入以便该接口不属于动态 LAG 的一部分，但充当静态 LAG 成员。</li> <li>• <i>passive</i> — 仅当检测到设备时才能启用 LACP。当端口响应 LACP 数据包接收但不启动写上直到检测到设备之前，接口将处于被动协商状态。</li> </ul> |

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息** 从端口通道中删除最后一个物理接口时，端口通道仍然存在。在单个成员端口上配置这些属性。如果配置具有不兼容属性的成员端口，OS10 会在端口通道中挂起该端口。端口通道中的成员端口必须具有相同的链路速度功能和双工功能设置。此命令的 `no` 版本将从端口通道移除接口。

## 示例

```
OS10(config)# interface ethernet 1/1/10
OS10(conf-if-eth1/1/10)# channel-group 10 mode active
OS10(conf-if-eth1/1/10)# exit
OS10(config)# interface ethernet 1/1/11
OS10(conf-if-eth1/1/11)# channel-group 10 mode active
```

## 支持的版本

10.2.0E or later

## clear lacp counters

清除 LACP 组的所有接口的统计信息。

### 语法

```
clear lacp counters [interface port-channel channel-number]
```

### 参数

- *interface port channel* — (可选) 输入接口端口通道编号。
- *channel-number* — (可选) 输入 LACP 端口通道编号 (1 到 128) 。

### 默认

未配置

### 命令模式

EXEC

### 使用情况信息

如果在未启用聚合协议的情况下对静态端口通道组使用此命令，则设备将忽略该命令。如果不输入端口通道编号，则所有 LACP 端口组的 LACP 计数器都将清除。

## 示例

```
OS10# clear lacp counters
```

## 示例（端口通道）

```
OS10# clear lacp counters interface port-channel 20
```

## 支持的版本

10.2.0E or later

## lacp fallback enable

启用 LACP 回退模式。

### 语法

```
lacp fallback enable
```

### 参数

无

### 默认

已禁用

### 命令模式

Port-channel INTERFACE

### 使用情况信息

此命令的 *no* 版本将禁用 LACP 回退模式。

## 示例

```
OS10# configure terminal
OS10(config)# interface port-channel 1
OS10(conf-if-po-1)# lacp fallback enable
```

## 支持的版本

10.3.2E(R3) or later

## lacp fallback preemption

启用或禁用 LACP 回退端口抢占。

### 语法

```
lacp fallback preemption {enable | disable}
```

### 参数

- *enable* — 启用端口通道上的抢占。
- *disable* — 禁用端口通道上的抢占。

### 默认

已启用

### 命令模式

Port-channel INTERFACE



## 使用情况信息

启用抢占时，回退端口选择将抢占已选择的回退端口，并选择新的回退端口。

将根据以下事件选择新端口：

- 当非回退端口配置为低优先级时。
- 当低优先级端口在运行时变为开启状态时。
- 当具有最少编号的端口在运行时变为开启状态时。
- 如果在禁用了抢占的情况下在端口上配置了非默认 LACP 端口优先级，则选择具有最低优先级的端口作为回退端口。
- `lacp fallback preemption disable` 命令不适用于已配置或触发的端口优先级事件。

## 示例

```
OS10# configure terminal
OS10(config)# interface port-channel 1
OS10(config-if-po-1)# lacp fallback preemption enable
```

```
OS10# configure terminal
OS10(config)# interface port-channel 1
OS10(config-if-po-1)# lacp fallback preemption disable
```

## 支持的版本

10.4.1.0 or later

## lacp fallback timeout

配置 LACP 回退超时期限。

### 语法

`lacp fallback timeout timer-value`

### 参数

*timer-value*— 输入定时器值（以秒为单位），从 0 到 100 秒。

### 默认

15 秒

### 命令模式

Port-channel INTERFACE

### 使用情况信息

此命令的 `no` 版本将计时器返回到默认值。

### 示例

```
OS10# configure terminal
OS10(config)# interface port-channel 1
OS10(config-if-po-1)# lacp fallback timeout 20
```

## 支持的版本

10.3.2E(R3) or later

## lacp max-bundle

配置端口通道中允许的最大活动成员数。

### 语法

`lacp max-bundle max-bundle-number`

### 参数

*max-bundle-number* — 输入最大套装大小（1 到 32）。

### 默认

32

### 命令模式

INTERFACE

### 使用情况信息

此命令的 `no` 版本将最大套装大小重置为默认值。

### 示例

```
OS10(config-if-po-10)# lacp max-bundle 10
```

## 支持的版本

10.2.0E or later

## Lacp port-priority

设置 LACP 的物理接口的优先级。

|               |                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>lacp port-priority priority</code>                                                                                                             |
| <b>参数</b>     | <i>priority</i> — 输入物理接口的优先级（0 到 65535）。                                                                                                             |
| <b>默认</b>     | 32768                                                                                                                                                |
| <b>命令模式</b>   | INTERFACE                                                                                                                                            |
| <b>使用情况信息</b> | LACP 将端口优先级与端口号结合使用，以创建端口标识符。端口优先级决定了存在硬件限制（以防止所有兼容的端口进行聚合）时或者当您为通道组配置了八个以上的端口时，将哪些端口置于待机模式。设置优先级时，较大的数字表示优先级较低。此命令的 <code>no</code> 版本将端口优先级恢复为默认值。 |
| <b>示例</b>     | <pre>OS10(config-range-eth1/1/7-1/1/8)# lacp port-priority 32768</pre>                                                                               |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                                     |

## lacp rate

设置 LACP 发送控制数据包的速率。

|               |                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>lacp rate {fast   normal}</code>                                                                                     |
| <b>参数</b>     | <ul style="list-style-type: none"><li><code>fast</code> — 输入 1 秒快速速率。</li><li><code>normal</code> — 输入 30 秒默认速率。</li></ul> |
| <b>默认</b>     | 30 秒                                                                                                                       |
| <b>命令模式</b>   | INTERFACE                                                                                                                  |
| <b>使用情况信息</b> | 更改 LACP 定时器率，以修改 LACP 超时的持续时间。此命令的 <code>no</code> 版本将速率重置为默认值。                                                            |
| <b>示例</b>     | <pre>OS10(config-range-eth1/1/7-1/1/8)# lacp rate fast</pre>                                                               |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                           |

## lacp system-priority

设置 LACP 设备的系统优先级。

|               |                                                                                                                                         |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>参数</b>     | <i>priority</i> — 输入物理接口的优先级值（0 到 65535）。                                                                                               |
| <b>默认</b>     | 32768                                                                                                                                   |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                           |
| <b>使用情况信息</b> | 运行 LACP 的每个设备都具有 LACP 系统优先级值。LACP 将系统优先级与 MAC 地址结合使用，以形成系统 ID，并且在与其他系统协商过程中也是如此。系统 ID 对于每个设备都是唯一的。此命令的 <code>no</code> 版本会将系统优先级重置为默认值。 |
| <b>示例</b>     | <pre>OS10(config)# lacp system-priority 32768</pre>                                                                                     |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                        |

## show lacp counter

显示有关 LACP 统计信息的信息。

|           |                                                                        |
|-----------|------------------------------------------------------------------------|
| <b>语法</b> | <code>show lacp counter [interface port-channel channel-number]</code> |
|-----------|------------------------------------------------------------------------|

参数

- interface port channel — (可选) 输入接口端口通道。
- channel-number — (可选) 输入 LACP 通道组编号 (1 到 128) 。

默认未配置

命令模式EXEC

使用情况信息如果不输入 channel-number 参数, 将显示所有通道组。

示例

```
OS10# show lacp counter interface port-channel 1
```

| LACPDU's Port | Marker Sent | Marker Recv | Marker Sent | Response Recv | Response Sent | LACPDU's Recv | Pkts | Err |
|---------------|-------------|-------------|-------------|---------------|---------------|---------------|------|-----|
| -----         |             |             |             |               |               |               |      |     |
| port-channel1 |             |             |             |               |               |               |      |     |
| Ethernet1/1   | 554         | 536         | 0           | 0             | 0             | 0             | 0    |     |
| Ethernet1/2   | 527         | 514         | 0           | 0             | 0             | 0             | 0    |     |
| Ethernet1/3   | 535         | 520         | 0           | 0             | 0             | 0             | 0    |     |
| Ethernet1/4   | 515         | 502         | 0           | 0             | 0             | 0             | 0    |     |
| Ethernet1/5   | 518         | 505         | 0           | 0             | 0             | 0             | 0    |     |
| Ethernet1/6   | 540         | 529         | 0           | 0             | 0             | 0             | 0    |     |
| Ethernet1/7   | 541         | 530         | 0           | 0             | 0             | 0             | 0    |     |
| Ethernet1/8   | 547         | 532         | 0           | 0             | 0             | 0             | 0    |     |
| Ethernet1/9   | 544         | 532         | 0           | 0             | 0             | 0             | 0    |     |
| Ethernet1/10  | 513         | 501         | 0           | 0             | 0             | 0             | 0    |     |
| Ethernet1/11  | 497         | 485         | 0           | 0             | 0             | 0             | 0    |     |
| Ethernet1/12  | 493         | 486         | 0           | 0             | 0             | 0             | 0    |     |
| Ethernet1/13  | 492         | 485         | 0           | 0             | 0             | 0             | 0    |     |
| --more--      |             |             |             |               |               |               |      |     |

支持的版本10.2.0E or later

## show lacp interface

显示有关特定 LACP 接口的信息。

语法

```
show lacp interface ethernet node/slot/port
```

参数

```
node/slot/port
```

 — 输入接口信息。

默认未配置

命令模式EXEC

使用情况信息如果您在主动或被动端口通道模式下配置链路, 则会显示 LACP\_activity 字段。Port Identifier 字段显示作为信息一部分的端口优先级, 包括端口号。例如, Port Identifier=0x8000,0x101 的端口优先级值为 0x8000, 而端口号值为 0x101。

示例

```
OS10# show lacp interface ethernet 1/1/129
Invalid Port id, Max. Port Id is: 32
OS10# show lacp interface ethernet 1/1/29

Interface ethernet1/1/29 is up
 Channel group is 1 port-channel is po1
 PDUS sent: 365
 PDUS rcvd: 17
 Marker sent: 0
 Marker rcvd: 0
 Marker response sent: 0
 Marker response rcvd: 0
 Unknown packetse rcvd: 0
 Illegal packetse rcvd: 0
Local Port: ethernet1/1/29 MAC Address=90:b1:1c:f4:9b:8a
System Identifier=32768,32768
Port Identifier=32768,32768
Operational key=1
LACP_Activity=passive
LACP_Timeout=Long Timeout(30s)
Synchronization=IN_SYNC
```

```

Collecting=true
Distributing=true
Partner information refresh timeout=Long Timeout(90s)
Actor Admin State=BCFHJKNO
Actor Oper State=BDEGIKNO
Neighbor: 178
MAC Address=00:00:00:00:00:00
System Identifier=,00:00:00:00:00:00
Port Identifier=0,00:01:e8:8a:fd:9e
Operational key=1
LACP_Activity=passive
LACP_Timeout=Long Timeout(30s)
Synchronization=IN_SYNC
Collecting=true
Distributing=true
Partner Admin State=BCEGIKNP
Partner Oper State=BDEGIKMO

```

**支持的版本** 10.2.0E or later

## show lacp neighbor

显示有关 LACP 邻居的信息。

**语法** `show lacp neighbor [interface port-channel channel-number]`

- 参数**
- `interface port channel` — (可选) 输入接口端口通道。
  - `channel-number` — (可选) 输入 LACP 邻居的端口通道号 (1 至 128) 。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 如果不输入 `channel-number` 参数, 将显示所有通道组。

**示例**

```

OS10# show lacp neighbor interface port-channel 1

Flags:S-Device is sending Slow LACPDUs F-Device is sending Fast LACPdus
 A-Device is in Active mode P-Device is in Passive mode
Port-channel port-channell neighbors
Port: ethernet1/1/29
Partner System Priority: 32768
Partner System ID: 00:01:e8:8a:fd:9e
Partner Port: 178
Partner Port Priority: 32768
Partner Oper Key: 1
Partner Oper State:aggregation synchronization collecting distributing
defaulted expired

```

**支持的版本** 10.2.0E or later

## show lacp port channel

显示有关 LACP 端口通道的信息。

**语法** `show lacp port-channel [interface port-channel channel-number]`

- 参数**
- `interface port channel` — (可选) 输入接口端口通道。
  - `channel-number` — (可选) 输入 LACP 邻居的端口通道号 (1 至 128) 。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 如果不输入 `channel-number` 参数, 则会显示所有通道组。

## 示例

```
OS10# show lacp port-channel 1

Port-channel 1 admin up, oper up, mode lacp
Actor System ID: Priority 32768, Address 90:b1:1c:f4:9b:8a
Partner System ID: Priority 32768, Address 00:01:e8:8a:fd:9e
Actor Admin Key 1, Oper Key 1, Partner Oper Key 1
LACP LAG ID 1 is an aggregatable link
A-Active LACP, B-Passive LACP, C-Short Timeout, D-Long Timeout
E-Aggregatable Link, F-Individual Link, G-IN_SYNC, H-OUT_OF_SYNC,
I-Collection enabled, J-Collection disabled, K-Distribution enabled,
L-Distribution disabled, M-Partner Defaulted, N-Partner Non-defaulted,
O-Receiver is in expired state, P-Receiver is not in expired state
Port ethernet1/1/29 is Enabled, LACP is enabled and mode is lacp
Actor Admin: State BCFHJKNO Key 1 Priority 32768
Oper: State BDEGIKNO Key 1 Priority 32768
Partner Admin: State BCEGIKNP Key 0 Priority 0
Oper: State BDEGIKMO Key 1 Priority 32768
```

**支持的版本** 10.2.0E or later

## show lacp system-identifier

显示设备的 LACP 系统标识符。

**语法** show lacp system-identifier

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** LACP 系统 ID 是可配置 LACP 系统优先级值和 MAC 地址的组合。运行 LACP 的每个系统都具有 LACP 的系统优先级值。配置介于 1 和 65535 之间的值。默认值为 32768。LACP 使用系统优先级和 MAC 地址来形成系统 ID，并在与其他设备协商期间使用系统优先级。较高的系统优先级值意味着优先级较低。每个设备的系统 ID 不同。

## 示例

```
OS10# show lacp system-identifier

Actor System ID: Priority 32768, Address 90:b1:1c:f4:9b:8a
```

**支持的版本** 10.2.0E or later

# 链路层发现协议

链路层发现协议 (LLDP) 允许局域网 (LAN) 上的网络设备将通告其身份和功能，并学习相邻 LAN 设备中的功能。

- 默认情况下，在接口上已启用 LLDP。
- 已启用 LLDP 的接口最多支持八个邻居。OS10 交换机在每个系统上最多支持 250 个邻居。
- OS10 交换机将接收并定期传输链路层查找协议数据单元 (LLDPDU)。默认传输间隔为 30 秒。
- 从邻居接收到的 LLDPDU 信息将在特定时间段（称为生存时间 [TTL]）过期。默认的 TTL 值是 120 秒。
- 生成树阻止的端口将允许 LLDPDU。
- 802.1x 控制端口不允许 LLDPDU，直至连接的设备进行了身份验证。
- 链路层发现协议 — 默认情况下，在所有接口上启用介质端点查找 (LLDP-MED)。

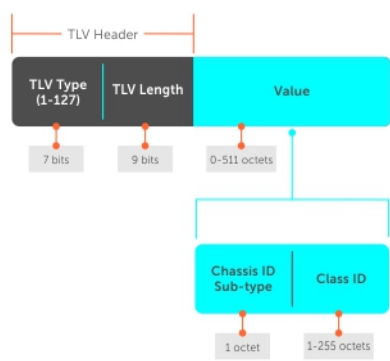
## 协议数据单元

LLDP 设备以 LLDPDU 形式通告功能，LLDPDU 是类型、长度和值 (TLV) 的序列。

**类型** 包含 TLV 类型。

**长度** 值字段的大小（以字节为单位）。

值 包含要通告的设备功能信息。



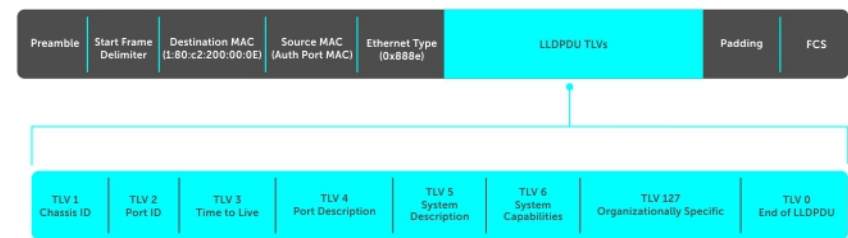
LAN 设备将 LLDPDU（一系列 TLV）传输到相邻 LAN 设备。LLDP 是一种单向协议，LAN 设备可发送和/或接收通告，但它们不能请求和响应通告。

每个 LLDP 框架均从三个强制 TLV 开始，后跟零个或更多的可选 TLV 以及 LLDPDU TLV 的末尾。三个必需的 TLV 必须在 LLDPDU 的开头，顺序如下：

- 机箱 ID TLV
- 端口 ID TLV
- 生存时间 TLV

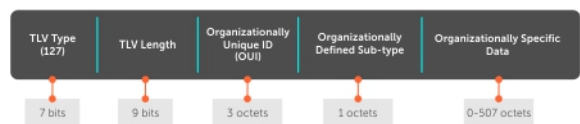
表. 31: 必需的 TLV

| 必需的 TLV        | 类型 | 说明                        |
|----------------|----|---------------------------|
| 机箱 ID          | 1  | 标识机箱。                     |
| Port ID（端口 ID） | 2  | 标识 LAN 设备用于传输 LLDPDU 的端口。 |
| 生存时间           | 3  | 此 LLDPDU 中接收的信息有效的秒数。     |
| LLDPDU 结束      | 0  | 标记 LLDPDU 结束。             |



可选的 TLV

OS10 支持基本 TLV、管理 TLV、IEEE 802.1 和 IEEE 802.3 组织特定的 TLV，以及 LLDP 介质端点查找 (MED) TLV。



**注：**传输端支持的 LLDPDU 最大大小为 1500 字节。如果在添加特定类型的可选 TLV 时传输的 TLV 大小超过 1500 字节，则将删除该类型的所有可选 TLV。仅允许符合支持的最大大小的可选 TLV。

## 基本 TLV

表. 32: 基本 TLV

| TLV                     | 类型 | 说明                                                                                                                     |
|-------------------------|----|------------------------------------------------------------------------------------------------------------------------|
| Port description (端口说明) | 4  | 用于描述端口的用户定义的字母数字字符串 (端口 ID 或接口说明)。                                                                                     |
| 系统名称                    | 5  | 标识系统的用户定义的字母数字字符串。                                                                                                     |
| 系统说明                    | 6  | 包括以下信息： <ul style="list-style-type: none"><li>• 主机描述</li><li>• 戴尔操作系统版本</li><li>• 戴尔应用程序软件版本</li><li>• 构建时间戳</li></ul> |
| 系统功能                    | 7  | 确定系统的功能。                                                                                                               |
| 管理地址                    | 8  | 管理接口的网络地址。                                                                                                             |

## 组织特定的 TLV

表. 33: 802.1x 组织特定的 TLV (类型 - 127, OUI - 00-80-C2)

| TLV        | 子类型 | 说明                                    |
|------------|-----|---------------------------------------|
| 链路聚合       | 7   | 指示是否聚合与传输 LLDPDU 的端口关联的链路。还提供聚合端口标识符。 |
| 端口 VLAN ID | 1   | 端口所属的未标记的 VLAN。                       |
| 协议标识       | 4   | 不支持。                                  |

表. 34: 802.3 组织特定的 TLV (类型 - 127, OUI - 00-12-0F)

| TLV           | 子类型 | 说明                                                   |
|---------------|-----|------------------------------------------------------|
| MAC/PHY 配置/状态 | 1   | 指示双工和位速率功能，以及发送设备的当前双工和位速率设置。还指示当前设置是由自动协商还是手动配置引起的。 |
| 通过 MDI 供电     | 2   | 不支持。                                                 |
| 最大框架大小        | 4   | MAC 和 PHY 的最大框架大小功能。                                 |

表. 35: iDRAC 组织特定的 TLV；在 iDRAC 自定义的 TLV 中使用的子类型 (类型 - 127, OUI - 0xF8-0xB1-0x56)

| TLV     | 子类型 | 说明                                                                                                                            |
|---------|-----|-------------------------------------------------------------------------------------------------------------------------------|
| 始发者     | 1   | 指示用作始发者的 iDRAC 字符串。此字符串使外部交换机可以标识 iDRAC LLDP PDU。                                                                             |
| 端口类型    | 2   | 下面是适用的端口类型： <ol style="list-style-type: none"><li>1. iDRAC 端口 (专用)</li><li>2. NIC 端口</li><li>3. iDRAC 和 NIC 端口 (共享)</li></ol> |
| 端口 FQDD | 3   | 唯一标识服务器中的 NIC 端口的端口号。                                                                                                         |
| 服务器服务编号 | 4   | 服务器的服务编号 ID。                                                                                                                  |

**表. 35: iDRAC 组织特定的 TLV；在 iDRAC 自定义的 TLV 中使用的子类型（类型 - 127, OUI – 0xF8-0xB1-0x56）（续）**

| TLV      | 子类型 | 说明                                       |
|----------|-----|------------------------------------------|
| 服务器型号名称  | 5   | 服务器的型号名称。例如，PowerEdge FC640。             |
| 服务器插槽编号  | 6   | 服务器的插槽编号。例如，1、2、3、1a 和 1b。               |
| 机箱服务编号   | 7   | 机箱的服务编号 ID。（仅适用于刀片服务器。）                  |
| 机箱型号     | 8   | 机箱的型号名称。（仅适用于刀片服务器。）                     |
| IOM 服务编号 | 9   | IOM 设备的服务编号 ID。（仅适用于刀片服务器。）              |
| IOM 型号名称 | 10  | IOM 设备的型号名称。（仅适用于刀片服务器。）                 |
| IOM 插槽标签 | 11  | IOM 设备的插槽标签。例如，A1、B1、A2 和 B2（仅适用于刀片服务器）。 |
| IOM 端口号  | 12  | NIC 的端口号。例如，1、2 和 3。                     |

**表. 36: Isilon 相关的 TLV（类型 - 127, OUI – 0xF8-0xB1-0x56）**

| TLV                                                             | 子类型 | 说明                                                                                      |
|-----------------------------------------------------------------|-----|-----------------------------------------------------------------------------------------|
| <b>在 LLDP 自定义的 TLV（由 Isilon 节点进行事务处理）中使用的子类型</b>                |     |                                                                                         |
| 始发者                                                             | 1   | 指示用作始发者的 Isilon 字符串。此字符串使 OS10 交换机可以标识 LLDP PDU 发起的 Isilon。                             |
| RA 前缀                                                           | 2   | 指示 SLAAC 的 IPV6 地址前缀。Isilon 节点使用此前缀与主实例和 OS10 交换机进行通信，以计算特定结构实例的虚拟 IP 地址。每个结构的 RA 前缀不同。 |
| 结构 ID                                                           | 3   | 指示 LLDP PDU 源自的结构的 ID。                                                                  |
| <b>Isilon 相关的 TLV - LLDP 自定义的 TLV 中使用的子类型（由 OS10 交换机进行事务处理）</b> |     |                                                                                         |
| 始发者                                                             | 1   | 指示用作始发者的 OS10 字符串。该字符串使 OS10 交换机可以标识 LLDP PDU。                                          |
| Role（角色）                                                        | 2   | 适用的角色如下：<br>1. 分支<br>2. 主干<br>3. 未知                                                     |
| IP 地址                                                           | 3   | 指示始发者的 IPv6 地址。                                                                         |
| 结构的虚拟 IP 地址                                                     | 4   | 主节点的虚拟 IP 地址。Isilon 节点还可以在需要时使用此 IPv6 地址。                                               |
| 物理接口的 MAC 地址                                                    | 5   | 适用于 ND 的 OS10 交换机使用的 MAC 地址。                                                            |

**表. 37: 服务编号 TLV（类型 - 127, OUI – 0xF8-0xB1-0x56）**

| TLV  | 子类型 | 说明            |
|------|-----|---------------|
| 服务编号 | 21  | 指示与设备关联的服务编号。 |



表. 38: ID TLV 解决方案 (类型 - 127, OUI - 0xF8-0xB1-0x56)

| TLV    | 子类型 | 说明        |
|--------|-----|-----------|
| 产品基座   | 22  | 指示产品基座。   |
| 产品序列号  | 23  | 指示产品序列号。  |
| 产品部件编号 | 24  | 指示产品部件编号。 |

## 介质端点查找

LLDP-MED 提供了特定于组织的 TLV，以允许端点设备和网络连接设备通告其特性和配置信息。

LLDP-MED IEEE 802 LAN 网络边缘的设备使用 LLDP-MED 框架（如 IP 手机和会议室）加入 IP 通信服务。LLDP-MED 网络连接设备提供对 LLDP-MED 端点设备（如 IP 手机）的基于 IEEE 802 的 LAN 基础架构的访问权限。OS10 设备用作 LLDP-MED 网络连接设备。

LLDP-MED 提供网络连接设备：

- 管理库存。
- 管理以太网供电 (PoE)。
- 识别物理位置。
- 识别网络策略。

**注：**仅支持 Rx 功能来管理 PoE 和标识物理位置。LLDP-MED 设计为但不限于 VoIP 端点。

## 网络连接设备

OS10 用作 LLDP-MED 网络连接设备（类型 4）。网络连接设备将 LLDP-MED 功能 TLV 传输到端点设备并存储端点设备通告的信息。

- 127/1 — LLDP-MED 功能

- 如果传输设备支持 LLDP-MED
  - 支持哪些 LLDP-MED TLV
  - LLDP 设备类
- 127/2 — 网络策略

应用程序类型、VLAN ID、L2 优先级和 DSCP 值。
- 127/3 — 本地识别

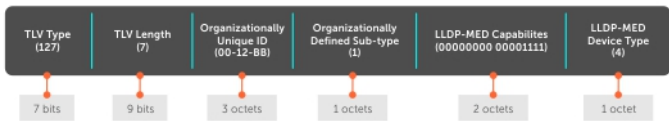
设备的物理位置，以三种格式之一表示：
  - 基于坐标的 LCI
  - 市政地址 LCI
  - 紧急电话服务 ELIN
- 127/4 — 通过 MDI 扩展电源

电源要求、优先级和电源状态。

## LLDP-MED 功能 TLV

LLDP-MED 功能 TLV 可传达端点设备和网络连接设备支持的 TLV 类型。TLV 中的 LLDP-MED 功能字段的值是 2 个八字节位图。每个位代表一个 LLDP-MED 功能。

默认情况下，LLDP-MED 在接口上处于启用状态。如果禁用 LLDP-MED，请使用 `lldp med enable` 命令在接口上启用它。仅当设备从对等节点收到 TLV 时，才会传输 MED 的 PDU。即使您在接口上启用了 MED，设备也不会发送 PDU。



# LLDP-MED 功能

|        |               |
|--------|---------------|
| 位 0    | LLDP-MED 功能   |
| 位 1    | 网络策略          |
| 位 2    | 位置 ID         |
| 位 3    | MDI-PSE 的扩展功率 |
| 位 4    | MDI-PD 的扩展功率  |
| 位 5    | 资源清册          |
| 位 6-15 | 保留            |

# LLDP-MED 设备类型

|       |        |
|-------|--------|
| 0     | 未定义类型  |
| 1     | 端点类别 1 |
| 2     | 端点类别 2 |
| 3     | 端点类别 3 |
| 4     | 网络连接   |
| 5-255 | 保留     |

# 网络策略 TLV

LLDP-MED 上下文中的网络策略是设备及关联的 L2 和 L3 配置的 VLAN 配置。

LLDP-MED 网络策略 TLV 包括：

- VLAN ID
- VLAN 已标记或未标记状态
- L2 优先级
- DSCP 值

一个整数表示应用程序类型 Type integer，表示定义了唯一网络策略的设备功能。TLV 为与 OS10 命令一起使用的每个应用程序类型生成单独 LLDP-MED 网络策略，请参阅[通告 LLDP-MED TLV](#)。

**注：**信号是在端点设备和网络连接设备之间交换以建立和维护连接的一系列控制数据包。这些信号数据包可能需要与建立连接的介质数据包不同的网络策略。在这种情况下，请配置信号应用程序。

|            |                                                                              |
|------------|------------------------------------------------------------------------------|
| 0 — 保留     | —                                                                            |
| 1 — 语音     | 用于支持交互式语音服务的专用 IP 电话话机和其他设备。                                                 |
| 2 — 语音信号   | 仅在语音控件数据包使用与语音数据不同的网络策略时使用。                                                  |
| 3 — 来宾语音   | 仅适用于具有自己的 IP 电话机的来宾用户和支持交互式语音服务的其他设备的单独受限语音服务。                               |
| 4 — 来宾语音信号 | 仅在来宾语音控制数据包使用与语音数据不同的网络策略时使用。                                                |
| 5 — 软件电话语音 | 用于设备上的软件电话应用程序，例如个人计算机或笔记本电脑。此类不支持多个 VLAN；如果需要，将使用未标记的 VLAN 或单个标记特定数据的 VLAN。 |
| 6 — 视频会议   | 仅用于支持实时交互式视频的专用视频会议和类似设备。                                                    |
| 7 — 流视频    | 用于基于广播或多播的视频内容分发和类似的应用程序，支持流视频服务（需要特定的网络策略处理）。                               |
| 8 — 视频信号   | 仅在视频控制数据包使用与视频数据不同的网络策略时使用。                                                  |
| 9-255 — 保留 | —                                                                            |



## 定义网络策略

您可以手动定义 LLDP-MED 网络策略。在 CONFIGURATION 模式下配置的 LLDP 命令是全局的，并且影响所有接口。在 INTERFACE 模式下配置 LLDP 命令仅影响特定接口。

创建最多 32 个网络策略，并将 LLDP-MED 的网络策略连接到一个端口。

- 在 CONFIGURATION 模式下定义 LLDP-MED 网络策略。

```
lldp-med network-policy number app {voice | voice-signaling | guest-voice |
guestvoice-signaling | softphone-voice | streaming-video | video-conferencing | video-
signaling}{vlan vlan-id vlan-type {tag | untag} priority priority dscp dscp value}
```

### 为语音应用程序配置 LLDP-MED 网络策略

```
OS10(config)# lldp med network-policy 10
OS10(config)# lldp med network-policy 10 app
OS10(config)# lldp med network-policy 10 app voice
OS10(config)# lldp med network-policy 1 app voice vlan 10 vlan-type tag
OS10(config)# lldp med network-policy 1 app voice-signaling vlan 10 vlan-type tag
priority 2 dscp 1
```

## 数据包计时器值

LLDPDU 将定期传输。您可以为 LLDPDU 传输配置 LLDP 数据包计时器值。

- 在 CONFIGURATION 模式下配置 LLDP 数据包计时器值。

```
lldp timer
```

- 在 CONFIGURATION 模式下输入保留时间的乘数值。

```
lldp holdtime-multiplier
```

- 在 CONFIGURATION 模式下输入任何接口上 LLDP 初始化的延迟（以秒为单位）。

```
lldp reinit
```

### 配置 LLDPDU 计时器

```
OS10(config)# lldp timer 60
OS10(config)# do show lldp timers
LLDP Timers:
Holdtime in seconds: 120
Reinit-time in seconds: 2
Transmit interval in seconds: 60
```

### 配置 LLDPDU 间隔

```
OS10(config)# lldp holdtime-multiplier 2
OS10(config)# do show lldp timers
LLDP Timers:
Holdtime in seconds: 60
Reinit-time in seconds: 2
Transmit interval in seconds: 30
```

## 禁用和启用 LLDP

默认情况下，为每个接口和全局启用 LLDP。您可以在接口上或全局禁用 LLDP。如果您全局禁用 LLDP，则 LLDP 在所有接口上处于禁用状态，不论某个接口上之前已启用还是已禁用 LLDP。当您全局启用 LLDP 时，接口模式下的 LLDP 配置优先于全局 LLDP 配置。

1. 在 INTERFACE 模式下禁用 LLDPDU 传输或接收。

```
no lldp transmit
no lldp receive
```

2. 在 CONFIGURATION 模式下禁用 LLDP 存留时间乘数值。

```
no lldp holdtime-multiplier
```

3. 在 CONFIGURATION 模式下禁用 LLDP 初始化。

```
no lldp reinit
```

4. 在 CONFIGURATION 或 INTERFACE 模式下禁用 LLDP MED。

```
no lldp med
```

5. 在 INTERFACE 模式下禁用 LLDP TLV。

```
no lldp tlv-select
```

6. 在 CONFIGURATION 模式下全局禁用 LLDP。

```
no lldp enable
```

### 禁用 LLDP

```
OS10(config)# no lldp timer 100
OS10(config)# no lldp holdtime-multiplier 10
OS10(config)# no lldp reinit 8
```

### 禁用 LLDP 接口

```
OS10(config)# interface ethernet 1/1/4
OS10(conf-if-eth1/1/4)# no lldp med
OS10(conf-if-eth1/1/4)# no lldp tlv-select
OS10(conf-if-eth1/1/4)# no lldp transmit
OS10(conf-if-eth1/1/4)# no lldp receive
```

### 启用 LLDP

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# lldp transmit
OS10(conf-if-eth1/1/1)# lldp receive
```

### 全局禁用 LLDP

```
OS10(config)# no lldp enable
```

## 在管理端口上禁用和启用 LLDP

默认情况下，在管理端口上已启用 LLDP。您可以在管理端口上禁用或启用以下 LLDP 配置。

1. 在 INTERFACE 模式下禁用 LLDPDU 传输和接收。

```
no lldp transmit
no lldp receive
```

## 2. 在 INTERFACE 模式下禁用 LLDP TLV。

```
no lldp tlv-select basic-tlv {port-description | system-name | system-description |
system-capabilities | management-address}
no lldp tlv-select dot1tlv port-vlan-id
```

### 禁用 LLDP 传输或接收

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# no lldp transmit
OS10(conf-if-ma-1/1/1)# no lldp receive
```

### 启用 LLDP 传输或接收

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# lldp transmit
OS10(conf-if-ma-1/1/1)# lldp receive
```

### 禁用 LLDP TLV

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# no lldp tlv-select basic-tlv system-name system-description
OS10(conf-if-ma-1/1/1)# no lldp tlv-select dot1tlv port-vlan-id
```

### 启用 LLDP TLV

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# lldp tlv-select basic-tlv system-name system-description
OS10(conf-if-ma-1/1/1)# lldp tlv-select dot1tlv port-vlan-id
```

## 通告 TLV

将系统配置为从所有接口或特定接口通告 TLV。如果配置接口，则只有接口使用指定的 TLV 发送 LLDPDU。

### 1. 在 INTERFACE 模式下启用基本 TLV 属性以传输和接收 LLDP 数据包。

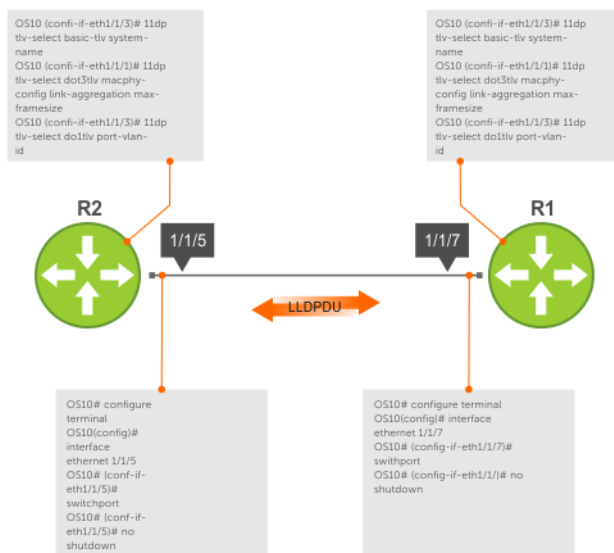
```
lldp tlv-select basic-tlv {port-description | system-name | system-description |
system-capabilities | management-address}
```

### 2. 在 INTERFACE 模式下启用 dot3 TLV 以传输和接收 LLDP 数据包。

```
lldp tlv-select dot3tlv {macphy-config | max-framesize}
```

### 3. 在 INTERFACE 模式下启用 dot1 TLV 以传输和接收 LLDP 数据包。

```
lldp tlv-select dot1tlv { port-vlan-id | link-aggregation | vlan-name}
```



## 配置通告 TLV

```
OS10 (conf-if-eth1/1/3)# lldp tlv-select basic-tlv system-name
OS10 (conf-if-eth1/1/1)# lldp tlv-select dot3tlv macphy-config max-framesize
OS10 (conf-if-eth1/1/3)# lldp tlv-select dot1tlv link-aggregation
```

## 通告 VLAN 名称 TLV

您可以将系统配置为通告 LLDP PDU 中的 VLAN 名称。将系统配置通告 VLAN 名称之前，请配置 VLAN 名称。

默认情况下，此功能被禁用。启用此功能后，系统将开始使用配置的默认 VLAN 名称 LLDP PDU 发送。如果默认的 VLAN 没有配置的名称，系统将不会使用 VLAN 名称发送 LLDP PDU。

### 传输默认 VLAN 的 VLAN 名称

1. 从 CONFIGURATION 模式进入 INTERFACE 模式。

```
OS10(config)# interface ethernet 1/1/1
```

2. 在 INTERFACE 模式下启用 vlan-name 选项。

```
OS10 (conf-if-eth1/1/1)# lldp tlv-select dot1-tlv vlan-name
```

3. 在 INTERFACE 模式下进入 INTERFACE VLAN 模式。

```
OS10 (config)# interface vlan 1
```

4. 在 INTERFACE VLAN 模式下指定 VLAN 1 的名称。

```
OS10 (conf-if-vl-1)# vlan-name vlan1
```

### 传输特定 VLAN 集的 VLAN 名称

一个接口最多可以传输八个 VLAN 名称。如果指定 10 个 VLAN，并且默认 VLAN 具有配置的名称，则该接口将使用默认 VLAN 的 VLAN 名称以及配置有名称的前七个已配置的 VLAN 来传输 LLDPDU。如果默认 VLAN 未配置名称，则接口将传输配置有名称的前八个 VLAN 的 VLAN 名称，并排除默认 VLAN。

为多个 VLAN 指定一个名称，并配置一个接口，以便在 PDU 中最多发送八个 VLAN 名称，其中包含默认 VLAN（如果具有名称）。

1. 在 CONFIGURATION 模式下创建 VLAN。

```
interface range vlan range
```

2. 在 INTERFACE 模式下指定所需 VLAN 的名称。

```
vlan-name vlan-name
```

3. 在 INTERFACE 模式下将端口模式配置为中继。

```
switchport mode trunk
```

4. OS10(config-if-eth1/1/1)#lldp tlv-select dot1-tlv vlan-name

5. 在 INTERFACE 模式下将接口配置为创建的 VLAN 的未标记成员。

```
switchport trunk allowed vlan vlan-range
```

6. 在 INTERFACE 模式下配置接口以发送 PDU 中特定 VLAN 的名称。

```
lldp vlan-name-tlv allowed vlan vlan-IDs
```

### 将系统配置为在 TLV 中传输 VLAN 名称的示例

从 1 到 10 为 VLAN 指定名称并且将 ethernet 1/1/1 接口配置为传输九个 VLAN 的名称。未明确配置接口来传输默认 VLAN 的名称 VLAN 1。

```
OS10# configure terminal
OS10(config)# interface range vlan 2-10
OS10(config)# interface vlan 1
OS10(config-if-vl-1)#vlan-name vlan1
OS10(config)# interface vlan 2
OS10(config-if-vl-2)#vlan-name vlan2
OS10(config)# interface vlan 3
OS10(config-if-vl-3)#vlan-name vlan4
OS10(config)# interface vlan 4
OS10(config-if-vl-4)#vlan-name vlan4
OS10(config)# interface vlan 5
OS10(config-if-vl-5)#vlan-name vlan5
OS10(config)# interface vlan 6
OS10(config-if-vl-6)#vlan-name vlan6
OS10(config)# interface vlan 7
OS10(config-if-vl-7)#vlan-name vlan7
OS10(config)# interface vlan 8
OS10(config-if-vl-8)#vlan-name vlan8
OS10(config)# interface vlan 9
OS10(config-if-vl-9)#vlan-name vlan9
OS10(config)# interface vlan 10
OS10(config-if-vl-10)#vlan-name vlan10
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# switchport mode trunk
OS10(config-if-eth1/1/1)# switchport trunk allowed vlan 2-10
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)#lldp vlan-name-tlv allowed vlan 2,3,4,5,6,7,8,9,10
```

接口将传输默认 VLAN 的名称，即使未明确配置 VLAN 名称也是如此。接口将传输前八个 VLAN 名称，并排除 VLAN 9 和 VLAN 10 的名称。下面显示接口将传输 VLAN 1 到 8 的名称：

```
OS10# show lldp interface ethernet 1/1/1 local-device
Device ID: 34:17:eb:f2:05:c4
Port ID: ethernet1/1/1
System Name: OS10
Capabilities: Router, Bridge, Repeater
System description:
 Dell EMC Networking OS10 Enterprise.
 Copyright (c) 1999-2019 by Dell Inc. All Rights Reserved.
 System Description: OS10 Enterprise.
 OS Version: 10.4.9999EX.
 System Type: S4048-ON
Port description: ethernet1/1/1
Time To Live: 120
Maximum size of LLDP PDU: 1500
Current LLDP PDU Size: 387
LLDP PDU Truncated(Too many TLV's): false
VLAN Name(s):
```

| VLAN | NAME  |
|------|-------|
| 1    | vlan1 |
| 2    | vlan2 |
| 3    | vlan3 |
| 4    | vlan4 |
| 5    | vlan5 |
| 6    | vlan6 |
| 7    | vlan7 |
| 8    | vlan8 |

Maximum size of LLDP PDU: 1500  
 Current LLDP PDU Size: 386  
 LLDP PDU Truncated(Too many TLV's): false  
 LLDP MED Capabilities:  
   Supported:  
     LLDP-MED Capabilities,  
     Network Policy,  
     Inventory Management  
   Current:  
     LLDP-MED Capabilities,  
     Network Policy  
 LLDP MED Device Type: Network connectivity

以下示例显示 VLAN 3 名称已删除:

```
OS10(conf-if-eth1/1/1)#no lldp vlan-name-tlv allowed vlan 3
```

以下输出显示接口删除 VLAN 3 并开始发送 VLAN 9 的名称:

```

OS10# show lldp interface ethernet 1/1/1 local-device
Device ID: 34:17:eb:f2:05:c4
Port ID: ethernet1/1/1
System Name: OS10
Capabilities: Router, Bridge, Repeater
System description:
 Dell EMC Networking OS10 Enterprise.
 Copyright (c) 1999-2019 by Dell Inc. All Rights Reserved.
 System Description: OS10 Enterprise.
 OS Version: 10.4.9999EX.
 System Type: S4048-ON
Port description: ethernet1/1/1
Time To Live: 120
Maximum size of LLDP PDU: 1500
Current LLDP PDU Size: 387
LLDP PDU Truncated(Too many TLV's): false
VLAN Name(s):
 VLAN NAME
 ---- -
 1 vlan1
 2 vlan2
 4 vlan4
 5 vlan5
 6 vlan6
 7 vlan7
 8 vlan8
 9 vlan9
Maximum size of LLDP PDU: 1500
Current LLDP PDU Size: 386
LLDP PDU Truncated(Too many TLV's): false
LLDP MED Capabilities:
 Supported:
 LLDP-MED Capabilities,
 Network Policy,
 Inventory Management
 Current:
 LLDP-MED Capabilities,
 Network Policy
LLDP MED Device Type: Network connectivity

```



## 网络策略通告

默认情况下，在所有接口上已启用 LLDP-MED。配置 OS10 以从配置的接口通告 LLDP-MED TLV。在将策略应用到接口之前，定义 LLDP-MED 网络策略。每个接口仅连接一个网络策略。

- 在 INTERFACE 模式下定义 LLDP-MED 网络策略。

```
lldp-med network-policy {add | remove} number
```

- add — 将网络策略连接到接口。
- remove — 从接口移除网络策略。
- number — 输入网络策略索引号，从 1 到 32。

### 配置通告 LLDP-MED 网络策略

```
OS10(config-if-eth1/1/5)# lldp-med network-policy add 1
```

## 快速启动重复计数

快速启动重复计数使网络连接设备能够在有限的时间内以更快的速度进行通告。快速启动计时器在网络连接设备从新检测到的端点接收到第一个 LLDP 帧时启动。

新检测到 LLDP-MED 端点或将其连接到网络时，该 `lldp-med fast-start-repeat-count` 使网络可以快速检测端点。LLDP-MED 快速启动重复计数指定在 LLDP-MED 快速启动期间发送的 LLDP 数据包数。默认情况下，该设备每个间隔发送三个数据包。在激活期间从 1 到 10 发送的数据包数量。

快速可用性对于紧急呼叫服务位置 (E911) 等应用程序至关重要。

- 在 CONFIGURATION 模式下启用快速启动重复计数，这是激活期间发送的数据包数，从 1 到 10，默认值为 3。

```
lldp-med fast-start-repeat-count number
```

### 配置快速启动重复计数

```
OS10(config)# lldp med fast-start-repeat-count 5
```

## 查看 LLDP 配置

- 在 EXEC 模式下查看 LLDP 配置。

```
show running-configuration
```

- 在 EXEC 模式下查看 LLDP 错误消息。

```
show lldp errors
```

- 以 EXEC 模式下查看 LLDP 计时器。

```
show lldp timers
```

- 以 EXEC 模式下查看 LLDP 流量。

```
show lldp traffic
```

### 查看正在运行的配置

```
OS10# show running-configuration
```

### 查看 LLDP 错误

```
OS10# show lldp errors
Total Memory Allocation Failures : 0
```

```
Total Input Queue Overflows : 0
Total Table Overflows : 0
```

### 查看 LLDP 计时器

```
OS10# show lldp timers
LLDP Timers:
Holdtime in seconds: 120
Reinit-time in seconds: 2
Transmit interval in seconds: 30
```

### 查看 LLDP 全局流量

```
OS10# show lldp traffic
LLDP traffic statistics:
Total Frames Out : 0
Total Entries Aged : 0
Total Frames In : 0
Total Frames Received In Error : 0
Total Frames Discarded : 0
Total TLVS Unrecognized : 0
Total TLVS Discarded : 0
```

### 查看 LLDP 接口流量

```
OS10# show lldp traffic interface ethernet 1/1/1
LLDP Traffic Statistics:
Total Frames Out : 0
Total Entries Aged : 0
Total Frames In : 0
Total Frames Received In Error : 0
Total Frames Discarded : 0
Total TLVS Unrecognized : 0
Total TLVS Discarded : 0

LLDP MED Traffic Statistics:
Total Med Frames Out : 0
Total Med Frames In : 0
Total Med Frames Discarded : 0
Total Med TLVS Discarded : 0
Total Med Capability TLVS Discarded: 0
Total Med Policy TLVS Discarded : 0
Total Med Inventory TLVS Discarded : 0
```

## 相邻代理通告

- 在 EXEC 模式下查看有关相邻设备的简要信息。

```
show lldp neighbors
```

- 在 EXEC 模式下查看邻居通告的所有信息。

```
show lldp neighbors detail
```

- 在 EXEC 模式下查看邻居通告的所有接口特定信息。

```
show lldp neighbors interface ethernetnode/slot/port[:subport]
```

### 查看 LLDP 邻居

```
OS10# show lldp neighbors
Loc PortID Rem Host Name Rem Port Id Rem Chassis Id

ethernet1/1/2 Not Advertised fortyGigE 0/56 00:01:e8:8a:fd:35
ethernet1/1/20:1 Not Advertised GigabitEthernet 1/0 00:01:e8:05:db:05
```

查看 LLDP 邻居详细信息

```
OS10# show lldp neighbors interface ethernet 1/1/1 detail

Remote Chassis ID Subtype: Mac address (4)
Remote Chassis ID: 00:13:21:57:ca:40
Remote Port Subtype: Interface name (5)
Remote Port ID: ethernet1/1/10
Remote Port Description: Ethernet port 1
Local Port ID: ethernet1/1/1
Locally assigned remote Neighbor Index: 3
Remote TTL: 120
Information valid for next 105 seconds
Time since last information change of this neighbor: 00:00:15
Remote System Name: LLDP-pkt-gen
Remote Management Address (IPv4): 10.1.1.1
Remote System Desc: LLDP packet generator using scapy
Existing System Capabilities: Repeater, Bridge, Router
Enabled System Capabilities: Repeater, Bridge, Router
Remote Max Frame Size: 0
Remote Aggregation Status: false
MAC PHY Configuration:
 Auto-neg supported: 1
 Auto-neg enabled: 1
 Auto-neg advertised capabilities:
 10BASE-T half duplex mode,
 10BASE-T full duplex mode,
 100BASE-TX half duplex mode,
 100BASE-TX full duplex mode
MED Capabilities:
 Supported:
 LLDP-MED Capabilities,
 Network Policy,
 Location Identification,
 Extended Power via MDI - PSE,
 Extended Power via MDI - PD,
 Inventory Management
 Current:
 LLDP-MED Capabilities,
 Network Policy,
 Location Identification,
 Extended Power via MDI - PD,
 Inventory Management
 Device Class: Endpoint Class 3
Network Policy:
 Application: voice, Tag: Tagged, Vlan: 50, L2 Priority: 6, DSCP Value: 46
Inventory Management:
 H/W Revision : 12.1.1
 F/W Revision : 10.1.9750B
 S/W Revision : 10.1.9750B
 Serial Number : B11G152
 Manufacturer : Dell
 Model : S6010-ON
 Asset ID : E1001
Power-via-MDI:
 Power Type: PD Device
 Power Source: Local and PSE
 Power Priority: Low
 Power required: 6.5
Location Identification:
 Civic-based:
 2C:02:49:4E:01:02:54:4E:03:07:43:68:65:6E:6E:61:69:04:06:47:75:69:
 6E:64:79:05:0B:53:49:44:43:4F:49:6E:64:45:73:74:17:05:4F:54:50:2D:
 31
 ECS-ELIN:
 39:39:36:32:30:33:35:38:32:34
```

查看 LLDP 邻居接口

|                                                    |               |             |                |
|----------------------------------------------------|---------------|-------------|----------------|
| OS10# show lldp neighbors interface ethernet 1/1/1 |               |             |                |
| Loc PortID                                         | Rem Host Name | Rem Port Id | Rem Chassis Id |

```

ethernet1/1/1 OS10 ethernet1/1/2 4:17:eb:f7:06:c4
```

## 生存时间

从邻居接收到的信息将在特定时间后过期（以秒为单位），称为 TTL。TTL 是 LLDPDU 传输间隔（问候），并且一个整数称为乘数。例如，LLDPDU 发送间隔 (30) 乘以乘数 (4)，(30 x 4 = 120)。默认乘数为 4，默认 TTL 为 120 秒。

1. 在 CONFIGURATION 模式下调整 TTL 值。

```
lldp holdtime-multiplier
```

2. 在 CONFIGURATION 模式下返回默认乘数值。

```
no lldp holdtime-multiplier
```

### 配置 TTL

```
OS10(config)# lldp holdtime-multiplier 2
```

### 返回乘数值

```
OS10(config)# no lldp holdtime-multiplier
```

## VLT 域中的通告管理地址 TLV

管理地址 TLV 将管理接口的 IP 地址通告至相邻 LAN 设备。系统将在所有物理端口的管理地址 TLV 中通告此信息。在 VLT 域中，对等节点 VLT 设备会在管理地址 TLV 中传输其本地管理接口的 IP 地址。

要与 Cisco 应用程序为中心的基础架构 (ACI) 等解决方案集成，VLT 对等节点的 OS10 交换机必须在 LLDPDU 的管理地址 TLV 通告一个通用 IP 地址。此通用 IP 地址也称为虚拟 IP 地址，因此 VLT 对等节点显示为 Cisco ACI 的单个交换机。

配置属于 VLT 对的 OS10 交换机，以选择单个 IPv4 或 IPv6 地址作为虚拟 IP 地址。启用此功能后，OS10 会选择管理接口上配置的每个子网的最低 IP 地址，或将管理 VLAN 作为虚拟 IP 地址。LLDP 在管理地址 TLV 中通告此虚拟 IP 地址。

 **注：**此功能仅适用于 VLT 域中的设备。

## 在管理地址 TLV 中通告虚拟管理 IP 地址

您可以启用系统，以在 VLT 对中选择单个 IP 地址，在全局或特定接口上使用 `lldp management-addr-tlv {ipv4 | ipv6} virtual-ip` 命令。LLDP 在管理地址 TLV 中通告此选举的虚拟 IP 地址。

启用发送管理地址 TLV 中的虚拟管理 IP 地址的服务：

- 允许服务在 CONFIGURATION 模式下使用 `lldp management-addr-tlv ipv4 virtual-ip` 发送管理地址 TLV 中的虚拟 IP 地址。  
在 CONFIGURATION 模式下启用时，配置将全局应用，并且系统将在管理地址 TLV 中通告选择的 IP 地址。
- 允许服务在 INTERFACE 模式下使用 `lldp management-addr-tlv ipv4 virtual-ip` 发送管理地址 TLV 中的虚拟 IP 地址。  
在 INTERFACE 模式下启用时，配置将应用于特定接口，并且系统将在管理地址 TLV 中通告选举的 IP 地址。

```
MX9116-B1(config)#lldp management-addr-tlv ipv4 virtual-ip
MX9116-B1(config-if-eth1/1/6)#lldp management-addr-tlv ipv4 virtual-ip
```

## LLDP 命令

### clear lldp counters

从所有物理接口清除 LLDP 和 LLDP-MED 传输、发送、接收和丢弃统计信息。

**语法** `clear lldp counters`

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 所有物理接口的计数器默认值将重设为零。

**示例**

```
OS10# clear lldp counters
```

**支持的版本** 10.2.0E or later

### clear lldp table

清除所有接口的 LLDP 相邻节点信息。

**语法** `clear lldp table`

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 在所有接口上清除邻居信息。

**示例**

```
OS10# clear lldp table
```

**支持的版本** 10.2.0E or later

### lldp enable

全局启用或禁用 LLDP。

**语法** `lldp enable`

**参数** 无

**默认** 已启用

**命令模式** CONFIGURATION

**使用情况信息** 此命令对所有以太网 PHY 接口启用全局 LLDP，但在您手动禁用 LLDP 的接口上除外。此命令的 `no` 版本将全局禁用 LLDP，不论是否手动禁用接口上的 LLDP。

**示例**

```
OS10(config)# lldp enable
```

**支持的版本** 10.3.1E or later

### lldp holdtime-multiplier

为保留时间配置乘数值（以秒为单位）。

**语法** `lldp holdtime-multiplier integer`

|        |                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------|
| 参数     | <i>integer</i> — 输入保留时间乘数值（以秒为单位），从 2 到 10。                                                       |
| 默认     | 4 秒                                                                                               |
| 命令模式   | CONFIGURATION                                                                                     |
| 使用情况信息 | 保留时间是接收系统在丢弃它之前等待保存信息的时间量（以秒为单位）。公式：保留时间 = （更新的频率间隔）x （保留时间乘数）。此命令的 <code>no</code> 版本会将该值重置为默认值。 |
| 示例     | <pre>OS10(config)# lldp holdtime-multiplier 2</pre>                                               |
| 支持的版本  | 10.2.0E or later                                                                                  |

## lldp med fast-start-repeat-count

配置在快速启动机制激活期间发送的数据包数。

|        |                                                             |
|--------|-------------------------------------------------------------|
| 语法     | <code>lldp-med fast-start-repeat-count <i>number</i></code> |
| 参数     | <i>number</i> — 输入激活快速启动机制期间发送的数据包数，从 1 到 10。               |
| 默认     | 3                                                           |
| 命令模式   | CONFIGURATION                                               |
| 使用情况信息 | 无                                                           |
| 示例     | <pre>OS10(config)# lldp med fast-start-repeat-count 5</pre> |
| 支持的版本  | 10.2.0E or later                                            |

## lldp med

启用或禁用接口上的 LLDP-MED。

|        |                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>lldp med {enable   disable}</code>                                                                                                  |
| 参数     | <ul style="list-style-type: none"> <li><code>enable</code> — 启用接口上的 LLDP-MED。</li> <li><code>disable</code> — 禁用接口上的 LLDP-MED。</li> </ul> |
| 默认     | 通过网络策略 TLV 启用                                                                                                                             |
| 命令模式   | INTERFACE                                                                                                                                 |
| 使用情况信息 | LLDP-MED 会传达端点设备和网络连接设备支持的 TLV 类型。使用 <code>no lldp med</code> 或 <code>lldp med disable</code> 命令可禁用特定接口上的 LLDP-MED。                       |
| 示例     | <pre>OS10(conf-if-eth1/1/1)# lldp med disable</pre>                                                                                       |
| 支持的版本  | 10.2.0E or later                                                                                                                          |

## lldp med network-policy

手动定义 LLDP-MED 网络策略。

|    |                                                                                                                                                                                                                                                                                                |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>lldp-med network-policy <i>number</i> app {voice   voice-signaling   guest-voice   guestvoice-signaling   softphone-voice   streaming-video   video-conferencing   video-signaling} {vlan <i>vlan-id</i> vlan-type {tag   untag} priority <i>priority</i> dscp <i>dscp value</i>}</code> |
| 参数 | <ul style="list-style-type: none"> <li><i>number</i> — 输入网络策略索引号，从 1 到 32。</li> <li><i>app</i> — 输入可用于网络策略的应用程序类型： <ul style="list-style-type: none"> <li><code>voice</code> — 语音网络策略应用程序</li> </ul> </li> </ul>                                                                               |

- o voice-signaling — 语音信号网络策略应用程序
- o guest-voice — 来宾语音网络-策略应用程序
- o guestvoice-signaling — 来宾语音信号网络策略应用程序
- o softphone-voice — SoftPhone 语音网络-策略应用程序
- o streaming-video — 流视频网络-策略应用程序
- o video-conferencing — 语音会议网络策略应用程序
- o video-signaling — 视频信号网络策略应用程序
- vlan *vlan-id* — 输入所选应用程序的 VLAN 编号，从 1 到 4093。
- vlan-type — 输入应用程序使用的 VLAN 类型。
- tag — 输入标记的 VLAN 编号。
- untag — 输入未标记的 VLAN 编号。
- priority *priority* — 输入为应用程序设置的用户优先级。
- dscp *dscp value* — 输入为应用程序设置的 DSCP 值。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 您可以创建最多 32 个网络策略并将 LLDP-MED 网络策略连接到一个端口。

**示例**

```
OS10(config)# lldp med network-policy 10 app voice vlan 10 vlan-type tag
priority 2 dscp 1
```

**支持的版本** 10.2.0E or later

## lldp med network-policy (Interface)

在接口之间附加或删除 LLDP-MED 网络策略。

**语法** lldp-med network-policy {add | remove} *number*

- 参数**
- add — 将网络策略连接到接口。
  - remove — 从接口移除网络策略。
  - *number* — 输入网络策略索引号，从 1 到 32。

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息** 针对每个接口仅连接一个网络策略。

**示例**

```
OS10(config-if-eth1/1/5)# lldp med network-policy add 1
```

**支持的版本** 10.2.0E or later

## lldp med tlv-select

将 LLDP-MED TLV 类型配置为传输或接收。

**语法** lldp med tlv-select {network-policy | inventory}

- 参数**
- network-policy — 启用或禁用端口描述 TLV。
  - inventory — 启用或禁用系统 TLV。

**默认** 已启用

**命令模式** INTERFACE

**使用情况信息** 无

**示例**

```
OS10(config-if-eth1/1/3)# lldp med tlv-select network-policy
```

**支持的版本** 10.2.0E or later

## lldp port-description-tlv advertise

指定在端口说明 TLV 中通告接口说明还是端口 ID。

**语法** `lldp port-description-tlv advertise [description | port-id]`

**参数**

- `description` — 通告接口说明。
- `port-id` — 通告端口 ID。

**默认** 接口说明已通告。

**命令模式** INTERFACE

**使用情况信息** 确定是在端口说明 TLV 中通告接口说明还是端口 ID。

**示例**

```
OS10(config-if-eth1/1/1)# lldp port-description-tlv advertise description
```

```
OS10(config-if-eth1/1/1)# lldp port-description-tlv advertise port-id
```

**支持的版本** 10.4.3.0 or later

## lldp receive

启用或禁用特定接口上的 LLDP 数据包接收。

**语法** `lldp receive`

**参数** 无

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息** 在使用 `lldp receive` 命令之前，在系统上全局启用 LLDP。此命令的 `no` 版本将禁止接收 LLDP 数据包。

**示例**

```
OS10(config-if-eth1/1/3)# lldp receive
```

**支持的版本** 10.2.0E or later

## lldp reinit

配置在任何接口上初始化 LLDP 的延迟时间（以秒为单位）。

**语法** `lldp reinit seconds`

**参数** `seconds` — 输入延迟计时器值（以秒为单位），从 1 到 10。

**默认** 2 秒

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本会将该值重置为默认值。

**示例**

```
OS10(config)# lldp reinit 5
```

**支持的版本** 10.2.0E or later

## lldp timer

配置 LLDP 数据包发送到对等主机的速率（以秒为单位）。

**语法** `lldp timer seconds`



|        |                                                  |
|--------|--------------------------------------------------|
| 参数     | <i>seconds</i> — 输入 LLDP 计时器速率（以秒为单位），从 5 到 254。 |
| 默认     | 30 秒                                             |
| 命令模式   | CONFIGURATION                                    |
| 使用情况信息 | 此命令的 <i>no</i> 版本将 LLDP 计时器设置回其默认值。              |
| 示例     | <pre>OS10(config)# lldp timer 25</pre>           |
| 支持的版本  | 10.2.0E or later                                 |

## lldp tlv-select basic-tlv

启用或禁用 TLV 属性以传输和接收 LLDP 数据包。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>lldp tlv-select basic-tlv {port-description   system-name   system-description   system-capabilities   management-address [ipv4   ipv6]}</code>                                                                                                                                                                                                                                                                                                                                     |
| 参数     | <ul style="list-style-type: none"> <li><code>port-description</code> — 启用或禁用端口描述 TLV。</li> <li><code>system-name</code> — 启用或禁用系统 TLV。</li> <li><code>system-description</code> — 启用或禁用系统描述 TLV。</li> <li><code>system-capabilities</code> — 启用或禁用系统功能 TLV。</li> <li><code>management-address</code> — 启用或禁用管理地址 TLV（IPv4 和 IPv6）。</li> <li><code>management-address ipv4</code> — 仅启用或禁用 IPv4 管理地址 TLV。</li> <li><code>management-address ipv6</code> — 仅启用或禁用 IPv6 管理地址 TLV。</li> </ul> |
| 默认     | 已启用                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 命令模式   | INTERFACE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 使用情况信息 | 命令的 <i>no</i> 形式会禁用 LLDP 数据包中 TLV 属性传输和接收。                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 示例     | <pre>OS10(conf-if-eth1/1/3)# lldp tlv-select basic-tlv system-name</pre>                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## lldp management-addr-tlv virtual-ip

使 VLT 对等节点可以在管理地址 TLV 中发送选择的虚拟 IP 地址。

|        |                                                                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>lldp management-addr-tlv {ipv4   ipv6} virtual-ip</code>                                                                                                                   |
| 参数     | <ul style="list-style-type: none"> <li><code>ipv4</code> — 为 ipv4 VLT 对等节点选择将虚拟 IPv4 地址发送到管理 TLV。</li> <li><code>ipv6</code> — 为 ipv6 VLT 对等节点选择将虚拟 IPv6 地址发送到管理 TLV。</li> </ul> |
| 默认     | 已禁用                                                                                                                                                                              |
| 命令模式   | <ul style="list-style-type: none"> <li>CONFIGURATION</li> <li>INTERFACE</li> </ul>                                                                                               |
| 使用情况信息 | <p>在 CONFIGURATION 模式下启用时，系统会在所有接口的管理地址 TLV 中通告选择的 IP 地址。</p> <p>在 INTERFACE 模式下启用时，系统会在特定接口的管理地址 TLV 中通告选择的 IP 地址。</p> <p>此命令的 <i>no</i> 版本将重置为默认值。默认情况下，系统会传输本地管理 IP 地址。</p>   |
| 示例     | <pre>MX9116N-B1(config)# lldp management-addr-tlv ipv4 virtual-ip MX9116N-B1(conf-if-eth1/1/3)# lldp management-addr-tlv ipv6 virtual-ip</pre>                                   |
| 支持的版本  | 10.5.0 or later                                                                                                                                                                  |

## lldp tlv-select dot1tlv

启用或禁用 dot.1 TLV 以在 LLDP 数据包中传输。

|             |                                                                                                                                                                               |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法          | lldp tlv-select dot1tlv { port-vlan-id   link-aggregation   vlan-name }                                                                                                       |
| 参数          | <ul style="list-style-type: none"><li>port-vlan-id — 输入端口 VLAN ID。</li><li>link-aggregation — 启用链路聚合 TLV。</li><li>vlan-name — 配置 dot1 TLV 以在 LLDP 帧中发送和接收 VLAN 的名称。</li></ul> |
| 默认          | 启用。vlan-name 已禁用。                                                                                                                                                             |
| 命令模式        | INTERFACE                                                                                                                                                                     |
| 使用情况信息      | 在 LLDPDU 中，link-aggregation 参数将链路聚合通告为 dot1 TLV。<br>vlan-name 参数通告 LLDP 帧中的 VLAN 名称。<br>此命令的 no 版本将禁用 TLV 传输。                                                                 |
| 示例（端口）      | <pre>OS10(conf-if-eth1/1/3)# lldp tlv-select dot1tlv port-vlan-id</pre>                                                                                                       |
| 示例（链路聚合）    | <pre>OS10(conf-if-eth1/1/3)# lldp tlv-select dot1tlv link-aggregation</pre>                                                                                                   |
| 示例（VLAN 名称） | <pre>OS10(conf-if-eth1/1/3)# lldp tlv-select dot1tlv vlan-name</pre>                                                                                                          |
| 支持的版本       | 10.2.0E or later                                                                                                                                                              |

## lldp tlv-select dot3tlv

启用或禁用 dot3 TLV 在 LLDP 数据包中传输。

|        |                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------|
| 语法     | lldp tlv-select dot3tlv { macphy-config   max-framesize }                                                              |
| 参数     | <ul style="list-style-type: none"><li>macphy-config — 启用端口 VLAN ID TLV。</li><li>max-framesize — 启用最大帧大小 TLV。</li></ul> |
| 默认     | 已启用                                                                                                                    |
| 命令模式   | INTERFACE                                                                                                              |
| 使用情况信息 | 此命令的 no 版本将禁用 TLV 传输。                                                                                                  |
| 示例     | <pre>OS10(conf-if-eth1/1/3)# lldp tlv-select dot3tlv macphy-config</pre>                                               |
| 支持的版本  | 10.2.0E or later                                                                                                       |

## lldp transmit

支持在特定接口上传输 LLDP 数据包。

|        |                                                  |
|--------|--------------------------------------------------|
| 语法     | lldp transmit                                    |
| 参数     | 无                                                |
| 默认     | 未配置                                              |
| 命令模式   | INTERFACE                                        |
| 使用情况信息 | 此命令的 no 版本禁用在特定接口上传输 LLDP 数据包。                   |
| 示例     | <pre>OS10(conf-if-eth1/1/9)# lldp transmit</pre> |

支持的版本 10.2.0E or later

lldp vlan-name-tlv allowed vlan

指定要在 LLDP PDU 中传输的单个或多个 VLAN 的名称。

|        |                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | lldp vlan-name-tlv allowed vlan <b>vlan-id</b>                                                                                                                                                                                                                                                                                                                        |
| 参数     | <b>vlan-id</b> — 指定单个 VLAN 或多个 VLAN。                                                                                                                                                                                                                                                                                                                                  |
| 默认     | 已禁用                                                                                                                                                                                                                                                                                                                                                                   |
| 命令模式   | INTERFACE                                                                                                                                                                                                                                                                                                                                                             |
| 使用情况信息 | <p>此命令指定要在 LLDP PDU 中传输的 VLAN 名称以及配置的默认 VLAN。如果不使用此命令，接口将发送默认 VLAN 的名称（如果配置了名称）。</p> <p>如果您使用此命令来传输多个 VLAN 名称，则不会排除任何没有名称配置的 VLAN。</p> <p>一个接口最多可以传输八个 VLAN 名称。如果指定 10 个 VLAN，并且默认 VLAN 已配置名称，则该接口将使用默认 VLAN 的 VLAN 名称以及已配置名称的前七个 VLAN 来传输 LLDPDU。如果默认 VLAN 未配置名称，则接口将传输配置有名称的前八个 VLAN 的 VLAN 名称，并排除默认 VLAN。</p> <p>具有 sysadmin、secadmin 和 netadmin 角色的用户可以访问此命令。</p> |

|    |                                                                                                                                                                     |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10(config-if-eth1/1/1)# lldp vlan-name-tlv allowed vlan vlan2</pre> <pre>OS10(config-if-eth1/1/1)# lldp vlan-name-tlv allowed vlan 2-10,12,14-16,20,24</pre> |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|

支持的版本 10.5.0 or later

show lldp interface

显示从特定接口通告的 LLDP 信息。

|        |                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show lldp interface ethernet <i>node/slot/port[:subport]</i> [ <i>local-device</i>   <i>med</i> ]                                                                                                                                                                                                                    |
| 参数     | <ul style="list-style-type: none"><li>• ethernet <i>node/slot/port[:subport]</i> — 输入以太网接口信息。</li><li>• local-device — 输入用于查看本地设备信息的接口。</li><li>• med — 输入用于查看 MED 信息的接口。</li></ul>                                                                                                                                  |
| 默认     | 无                                                                                                                                                                                                                                                                                                                    |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                 |
| 使用情况信息 | 使用 med 参数查看特定接口的 MED 信息。使用 local-device 参数查看清单详细信息。                                                                                                                                                                                                                                                                  |
| 示例     | <pre>OS10# show lldp interface ethernet 1/1/5 ethernet1/1/5 Tx State           : Enabled Rx State           : Enabled Tx SEM State       : initialize Rx SEM State       : wait-port-operational Notification Status : Disabled Notification Type   : mis-configuration DestinationMacAddr : 01:80:c2:00:00:0e</pre> |

|          |                                                                                                                                                                                                      |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例（本地设备） | <pre>OS10# show lldp interface ethernet 1/1/1 local-device  Device ID: 90:b1:1c:f4:a6:25 Port ID: ethernet1/1/2:1 System Name: 0075 Capabilities: Router, Bridge, Repeater System description:</pre> |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```

Dell EMC Networking OS10 Enterprise.
Copyright (c) 1999-2019 by Dell Inc. All Rights Reserved.
System Description: OS10 Enterprise.
OS Version: 10.4.9999EX.
System Type: S4048-ON

Port description: ethernet1/1/2:1
VLAN Name(s):
 VLAN NAME

 2 VLAN2
 3 VLAN3
Maximum size of LLDP PDU: 1500
Current LLDP PDU Size: 359
LLDP PDU Truncated(Too many TLV's): false
Time To Live: 150
LLDP MED Capabilities:
Supported:
LLDP-MED Capabilities,
Network Policy,
Inventory Management
Current:
LLDP-MED Capabilities,
Network Policy
LLDP MED Device Type: Network connectivity

```

#### 示例 (MED)

```

OS10# show lldp interface ethernet 1/1/20:1 med
Port	Capabilities	Network Policy	Location	Inventory	POE
ethernet1/1/20:1 | Yes | Yes | No | No | No
Network Polices :

```

**支持的版本** 10.2.0E or later

## show lldp errors

显示与内存分配失败、队列溢出和表溢出相关的 LLDP 错误。

**语法** show lldp errors

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```

OS10# show lldp errors
Total Memory Allocation Failures: 0
Total Input Queue Overflows: 0
Total Table Overflows: 0

```

**支持的版本** 10.2.0E or later

## show lldp med

显示所有接口的 LLDP MED 信息。

**语法** show lldp med

**参数** 无

**默认** 未配置

命令模式

使用情况信息

示例

EXEC

使用 show lldp interface 命令查看特定接口的 MED 信息。

```
OS10# show lldp med
Fast Start Repeat Count: 3
LLDP MED Device Type: Network Connectivity
Port	Capabilities	Network Policy	Location	Inventory	POE
ethernet1/1/1 | Yes | Yes | No | No | No
ethernet1/1/2 | Yes | Yes | No | No | No
ethernet1/1/3 | Yes | Yes | No | No | No
ethernet1/1/4 | Yes | Yes | No | Yes | No
ethernet1/1/5 | Yes | Yes | No | No | No
ethernet1/1/6 | Yes | Yes | No | No | No
ethernet1/1/7 | Yes | Yes | No | Yes | No
ethernet1/1/8 | Yes | Yes | No | No | No
ethernet1/1/9 | Yes | Yes | No | No | No
ethernet1/1/10 | Yes | Yes | No | No | No
ethernet1/1/11 | Yes | Yes | No | No | No
ethernet1/1/12 | Yes | Yes | No | No | No
ethernet1/1/13 | Yes | Yes | No | No | No
ethernet1/1/14 | Yes | Yes | No | No | No
ethernet1/1/15 | Yes | Yes | No | No | No
ethernet1/1/16 | Yes | Yes | No | No | No
ethernet1/1/17 | Yes | Yes | No | No | No
ethernet1/1/18 | Yes | Yes | No | No | No
ethernet1/1/19 | Yes | Yes | No | No | No
ethernet1/1/20 | Yes | Yes | No | No | No
ethernet1/1/21 | Yes | Yes | No | No | No
ethernet1/1/22 | Yes | Yes | No | No | No
ethernet1/1/23 | Yes | Yes | No | No | No
ethernet1/1/24 | Yes | Yes | No | No | No
ethernet1/1/25 | Yes | Yes | No | No | No
ethernet1/1/26 | Yes | Yes | No | No | No
ethernet1/1/27 | Yes | Yes | No | No | No
ethernet1/1/28 | Yes | Yes | No | No | No
ethernet1/1/29 | Yes | Yes | No | No | No
ethernet1/1/30 | Yes | Yes | No | No | No
ethernet1/1/31 | Yes | Yes | No | No | No
ethernet1/1/32 | Yes | Yes | No | No | No
```

支持的版本

10.2.0E or later

## show lldp neighbors

显示 LLDP 邻居系统信息的状态。

语法

参数

命令模式

使用情况信息

示例

show lldp neighbors [detail | interface ethernet node/slot/port[:subport]]

- detail — 查看 LLDP 邻居详细信息
- interface ethernet node/slot/port[:subport] — 输入以太网接口信息。

EXEC

此命令状态信息包括本地端口 ID、远程主机名称、远程端口 ID 远程 VLAN 名称、和远程节点 ID。

```
OS10# show lldp neighbors
Loc PortID Rem Host Name Rem Port Id Rem Chassis Id
-----|-----|-----|-----|
ethernet1/1/2 Not Advertised fortyGigE 0/56 00:01:e8:8a:fd:35
ethernet1/1/20:1 Not Advertised GigabitEthernet 1/0 00:01:e8:05:db:05
```

示例（详细信息）

```
OS10# show lldp neighbors interface ethernet 1/1/1 detail

Remote Chassis ID Subtype: Mac address (4)
Remote Chassis ID: 00:50:56:a6:29:54
```

```
Remote Port Subtype: Interface alias (1)
Remote Port ID: ethernet1/1/1
Remote Port Description: ethernet1/1/1
Local Port ID: ethernet1/1/1
Locally assigned remote Neighbor Index: 2
Remote TTL: 120
Information valid for next 99 seconds
Time since last information change of this neighbor: 15:51:41
Remote System Name: OS10
Remote System Desc: OS10
Existing System Capabilities: Repeater, Bridge, Router
Enabled System Capabilities: Repeater, Bridge, Router
Remote Port Vlan ID: 1
Remote VLAN Name(s):
 VLAN NAME

 2 VLAN2
 6 VLAN6
Remote Max Frame Size: 1532
Remote Aggregation Status: false
MAC PHY Configuration:
Auto-neg supported: 1
Auto-neg enabled: 1
Auto-neg advertised capabilities:
1000BASE-T half duplex mode
Dell EMC Organization Specific Detail:
Originator: Switch
Service Tag: B8D1XC2
Product Base: base1
Product Serial Number: sn1
Product Part Number: pn1
```

**示例（接口）**

```
OS10# show lldp neighbors interface ethernet 1/1/1
Loc PortID Rem Host Name Rem Port Id Rem Chassis Id

ethernet1/1/1 OS10 ethernet1/1/2 4:17:eb:f7:06:c4
```

**支持的版本** 10.2.0E or later

**show lldp timers**

显示 LLDP 的保留时间、延迟时间和更新频率间隔配置信息。

|        |                  |
|--------|------------------|
| 语法     | show lldp timers |
| 参数     | 无                |
| 默认     | 未配置              |
| 命令模式   | EXEC             |
| 使用情况信息 | 无                |
| 示例     |                  |

```
OS10# show lldp timers
LLDP Timers:
Holdtime in seconds: 120
Reinit-time in seconds: 6
Transmit interval in seconds: 30
```

**支持的版本** 10.2.0E or later

**show lldp tlv-select interface**

显示为接口启用的 TLV。

|    |                                                                         |
|----|-------------------------------------------------------------------------|
| 语法 | show lldp tlv-select interface ethernet <i>node/slot/port[:subport]</i> |
|----|-------------------------------------------------------------------------|

|        |                                                                 |
|--------|-----------------------------------------------------------------|
| 参数     | ethernet <i>node/slot/port[:subport]</i> — 输入以太网接口信息，从 1 到 253。 |
| 默认     | 未配置                                                             |
| 命令模式   | EXEC                                                            |
| 使用情况信息 | 无                                                               |
| 示例     |                                                                 |

```
OS10# show lldp tlv-select interface ethernet 1/1/1
port-description
system-capabilities
system-description
system-name
port-vlan
mac-phy-config
link-aggregation
max-frame-size
vlan-name
```

**支持的版本** 10.2.0E or later

## show lldp traffic

显示 LLDP 流量信息，包括计数器、传输和接收的数据包、丢弃的数据包和无法识别的 TLV。

|        |                                                                                 |
|--------|---------------------------------------------------------------------------------|
| 语法     | show lldp traffic [ <i>interface ethernet node/slot/port[:subport]</i> ]        |
| 参数     | <i>interface ethernet node/slot/port[:subport]</i> — (可选) 输入以太网接口信息以查看 LLDP 流量。 |
| 默认     | 未配置                                                                             |
| 命令模式   | EXEC                                                                            |
| 使用情况信息 | 无                                                                               |
| 示例     |                                                                                 |

```
OS10# show lldp traffic
LLDP Traffic Statistics:
Total Frames Out : 1504
Total Entries Aged : 2
Total Frames In : 67
Total Frames Received In Error : 0
Total Frames Discarded : 0
Total TLVS Unrecognized : 0
Total TLVS Discarded : 0
```

### 示例 (接口)

```
OS10# show lldp traffic interface ethernet 1/1/2
LLDP Traffic Statistics:
Total Frames Out : 45
Total Entries Aged : 1
Total Frames In : 33
Total Frames Received In Error : 0
Total Frames Discarded : 0
Total TLVS Unrecognized : 0
Total TLVS Discarded : 0

LLDP MED Traffic Statistics:
Total Med Frames Out : 2
Total Med Frames In : 1
Total Med Frames Discarded : 0
Total Med TLVS Discarded : 0
Total Med Capability TLVS Discarded: 0
Total Med Policy TLVS Discarded : 0
Total Med Inventory TLVS Discarded : 0
```

**支持的版本** 10.2.0E or later

## show network-policy profile

显示网络策略配置文件。

|        |                                                           |
|--------|-----------------------------------------------------------|
| 语法     | <code>show network-policy profile [profile number]</code> |
| 参数     | <i>profile number</i> — (可选) 输入网络策略配置文件编号, 从 1 到 32。      |
| 默认     | 未配置                                                       |
| 命令模式   | EXEC                                                      |
| 使用情况信息 | 如果不输入网络配置文件 ID, 则会显示所有已配置的网络策略配置文件。                       |
| 示例     |                                                           |

```
OS10# show network-policy profile 10
Network Policy Profile 10
 voice vlan 17 cos 4
 Interface:
 none
Network Policy Profile 30
 voice vlan 30 cos 5
 Interface:
 none
Network Policy Profile 36
 voice vlan 4 cos 3
 Interface:
 ethernet 1/1/1, ethernet 1/1/3-5
```

支持的版本 10.2.0E or later

## 介质访问控制

所有以太网交换端口都维护介质访问控制 (MAC) 地址表。网络中的每个物理设备均包含 MAC 地址。OS10 设备会在 MAC 地址表中自动输入 MAC 作为动态条目的地址。

了解 MAC 的地址条目可能会过时。将帐龄计时器设置为零 (0) 以禁用 MAC 老化。对于任何动态输入, 如果在具有 MAC 地址的设备上没有数据包到达计时器期限内的源或目标地址, 则会从表移除该地址。

- 在 CONFIGURATION 模式下输入帐龄时间 (以秒为单位), 从 0 到 1000000, 默认值为 1800。

```
mac address-table aging-time seconds
```

### 配置老化时间

```
OS10(config)# mac address-table aging-time 900
```

### 禁用老化时间

```
OS10(config)# mac address-table aging-time 0
```

## 静态 MAC 地址

手动配置静态 MAC 地址条目。静态条目不受老化的约束。

- 在 CONFIGURATION 模式下的 MAC 地址表中创建静态 MAC 地址条目。

```
mac-address-table static nn:nn:nn:nn:nn vlan vlan-id interface [ethernet node/slot/
port[:subport] | port-channel channel-number]
```

 **注:** 在使用 `mac-address-table static` 命令之前, 请创建所需的 VLAN。如果在配置静态 MAC 地址条目之前未创建 VLAN, 系统会显示一条错误消息。



## 设置静态 MAC 地址

```
OS10(config)# interface vlan 10
OS10(conf-if-vl-11)# exit
OS10(config)# mac address-table static 34:17:eb:f2:ab:c6 vlan 10 interface ethernet 1/1/5
```

## MAC 地址表

OS10 维护 MAC 地址表条目的列表。

- 在 EXEC 模式下查看 MAC 地址表的内容。

```
show mac address-table {dynamic | static} [address mac-address | vlan vlan-id |
interface {ethernet node/slot/port[:subport] | port-channel number}] [count [vlan
vlan-id] [interface {type node/slot/port[:subport] | port-channel number}]
```

- dynamic — (可选) 显示动态 MAC 地址表条目信息。
- static — (可选) 显示静态 MAC 地址表条目信息。
- address mac-address — (可选) 显示 MAC 地址信息。
- interface ethernet node/slot/port[:subport] — (可选) 显示动态和静态 MAC 地址条目的列表。
- interface port-channel number — (可选) 显示端口通道信息, 从 1 到 128。
- count — (可选) 显示动态和静态 MAC 地址条目的数量。
- vlan vlan-id — (可选) 仅显示指定 VLAN 的信息, 从 1 到 4093。

### 查看 MAC 的地址表条目

```
OS10# show mac address-table
VlanId Mac Address Type Interface
1 00:00:15:c6:ca:49 dynamic ethernet1/1/21
1 00:00:20:2a:25:55 dynamic ethernet1/1/21
1 90:b1:1c:f4:aa:ce dynamic ethernet1/1/21
1 90:b1:1c:f4:aa:c6 dynamic ethernet1/1/21
10 34:17:eb:02:8c:33 static ethernet1/1/1
```

### 查看 MAC 地址表计数

```
OS10# show mac address-table count
MAC Entries for all vlans :
Dynamic Address Count : 4
Static Address (User-defined) Count : 1
Total MAC Addresses in Use: 5
```

## 清除 MAC 地址表

您可以清除 MAC 地址表中维护的动态地址条目。

- 在 EXEC 模式下清除动态条目的 MAC 地址表。

```
clear mac address-table dynamic [[all] [address mac_addr] [vlan vlan-id] [interface
{ethernet type node/slot/port[:subport] | port-channel number}]
```

- all — (可选) 清除所有动态条目。
- address mac\_address — (可选) 清除 MAC 地址条目。
- vlan vlan-id — (可选) 从 VLAN 编号中清除 MAC 地址表条目, 从 1 到 4093。
- ethernet node/slot/port[:subport] — (可选) 清除以太网接口条目。
- port-channel number — (可选) 清除端口通道号, 从 1 到 128。

### 清除 MAC 地址表

```
OS10# clear mac address-table dynamic vlan 20 interface ethernet 1/2/20
```

## MAC 命令

### clear mac address-table dynamic

从 MAC 地址表中清除 L2 动态地址条目。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>clear mac address-table dynamic {all   address <i>mac_addr</i>   vlan <i>vlan-id</i>   interface {ethernet <i>node/slot/port[:subport]</i>   port-channel <i>number</i>}</code>                                                                                                                                                                                                                                                                                                                                                                          |
| 参数     | <ul style="list-style-type: none"><li>• <code>all</code> — (可选) 删除所有 MAC 地址表条目。</li><li>• <code>address <i>mac_addr</i></code> — (可选) 从地址表中删除已配置的 MAC 地址, 格式为 <code>nn:nn:nn:nn:nn:nn</code>。</li><li>• <code>vlan <i>vlan-id</i></code> — (可选) 从地址表中删除所有基于 VLAN 编号的条目, 从 1 到 4093。</li><li>• <code>interface</code> — (可选) 清除接口类型:<ul style="list-style-type: none"><li>◦ <code>ethernet <i>node/slot/port[:subport]</i></code> — 从地址表中删除以太网接口配置。</li><li>◦ <code>port-channel <i>channel-number</i></code> — 从地址表中删除端口通道接口配置, 从 1 到 128。</li></ul></li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 使用情况信息 | 使用 <code>all</code> 参数可从地址表中删除所有动态条目。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 示例     | <pre>OS10# clear mac address-table dynamic all</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

#### 示例 (VLAN)

```
OS10# clear mac address-table dynamic vlan 20
```

支持的版本 10.2.0E or later

### mac address-table aging-time

为 L2 地址表中的条目配置帐龄时间。

|        |                                                                       |
|--------|-----------------------------------------------------------------------|
| 语法     | <code>mac address-table aging-time <i>seconds</i></code>              |
| 参数     | <code><i>seconds</i></code> — 输入 MAC 表条目的帐龄时间 (以秒为单位), 从 0 到 1000000。 |
| 默认     | 1800 秒                                                                |
| 命令模式   | CONFIGURATION                                                         |
| 使用情况信息 | 将帐龄计时器设置为零 (0), 以禁用所有动态条目的 MAC 地址老化。上次设备检测到 MAC 地址的帐龄时间。              |
| 示例     | <pre>OS10(config)# mac address-table aging-time 3600</pre>            |
| 支持的版本  | 10.2.0E or later                                                      |

### mac address-table static

为 L2 MAC 地址表配置静态条目。

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>mac address-table static <i>mac-address</i> vlan <i>vlan-id</i> interface {ethernet <i>node/slot/port[:subport]</i>   port-channel <i>number</i>}</code>                                                                                                                                                                                                                                                                                                    |
| 参数 | <ul style="list-style-type: none"><li>• <code>mac-address</code> — 以 <code>nn:nn:nn:nn:nn:nn</code> 格式输入要添加到表的 MAC 地址。</li><li>• <code>vlan <i>vlan-id</i></code> — 输入要将静态 MAC 地址应用到的 VLAN, 从 1 到 4093。</li><li>• <code>interface</code> — 输入接口类型:<ul style="list-style-type: none"><li>◦ <code>ethernet <i>node/slot/port[:subport]</i></code> — 输入以太网信息。</li><li>◦ <code>port-channel <i>channel-number</i></code> — 输入端口通道接口编号, 从 1 到 128。</li></ul></li></ul> |
| 默认 | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|           |                                                                                                      |
|-----------|------------------------------------------------------------------------------------------------------|
| 命令模式      | CONFIGURATION                                                                                        |
| 使用情况信息    | 此命令的 no 版本会将该值重置为默认值。                                                                                |
| 示例 (VLAN) | <pre>OS10(config)# mac address-table static 34:17:eb:f2:ab:c6 vlan 1 interface ethernet 1/1/30</pre> |
| 示例 (端口通道) | <pre>OS10(config)# mac address-table static 34:17:eb:02:8c:33 vlan 10 interface port-channel 1</pre> |
| 支持的版本     | 10.2.0E or later                                                                                     |

show mac address-table

显示有关 MAC 地址表的信息。

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法        | <pre>show mac address-table [address mac-address   aging-time   [count [vlan vlan-id]   dynamic   interface {ethernet node/slot/port[:subport]   port- channel number}]   static [address mac-address]   vlan vlan-id</pre>                                                                                                                                                                                                                                                                                                               |
| 参数        | <ul style="list-style-type: none"><li>• address mac-address — (可选) 显示 MAC 地址表信息。</li><li>• aging-time — (可选) 显示 MAC 地址表老化时间信息。</li><li>• count — (可选) 显示动态和静态 MAC 地址条目的数量。</li><li>• dynamic — (可选) 仅显示动态 MAC 地址表条目。</li><li>• interface — 设置接口类型:<ul style="list-style-type: none"><li>◦ ethernet node/slot/port[:subport] — 显示物理接口 MAC 地址表信息。</li><li>◦ port-channel channel-number — 显示端口通道接口的 MAC 地址表信息，从 1 到 128。</li></ul></li><li>• static — (可选) 仅显示静态 MAC 地址表条目。</li><li>• vlan vlan-id — (可选) 仅显示 VLAN 信息，从 1 到 4093。</li></ul> |
| 默认        | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 命令模式      | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 使用情况信息    | 网络设备维护在启动配置文件中保存的静态 MAC 地址条目，并重新引导和删除动态条目。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 示例 (地址)   | <pre>OS10# show mac address-table address 90:b1:1c:f4:a6:8f VlanId  Mac Address      Type      Interface 1       90:b1:1c:f4:a6:8f      dynamic   ethernet1/1/3</pre>                                                                                                                                                                                                                                                                                                                                                                     |
| 示例 (老化时间) | <pre>OS10# show mac address-table aging-time Global Mac-address-table aging time : 1800</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 示例 (计数)   | <pre>OS10# show mac address-table count MAC Entries for all vlans : Dynamic Address Count : 5 Static Address (User-defined) Count : 0 Total MAC Addresses in Use: 5</pre>                                                                                                                                                                                                                                                                                                                                                                 |
| 示例 (动态)   | <pre>OS10# show mac address-table dynamic VlanId  Mac Address      Type      Interface 1       90:b1:1c:f4:a6:8f      dynamic   ethernet1/1/3</pre>                                                                                                                                                                                                                                                                                                                                                                                       |
| 示例 (以太网)  | <pre>OS10# show mac address-table interface ethernet 1/1/3 VlanId  Mac Address      Type      Interface 1       66:38:3a:62:31:3a      dynamic   ethernet1/1/3</pre>                                                                                                                                                                                                                                                                                                                                                                      |
| 支持的版本     | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

# 生成树协议

生成树协议是一种禁止在网络拓扑中循环的第二层网络协议。当存在多个网络路径且网络中的设备与这些路径争用或共享时，生成树非常有用。

## EdgePort

Edgeport 允许接口在跳过阻塞和学习状态大约 30 秒内向前转发流量。

 **小心:** 仅在连接到终端站的链路上配置 Edgeport。如果您在连接到网络的接口上启用，Edgeport 可能会导致回路。Edge 端口不会接收 BPDU。

- 在 INTERFACE 模式下的接口上启用 Edgeport。

```
spanning-tree port type edge
```

### 配置 Edgeport

```
OS10(conf-if-eth1/1/4)# spanning-tree port type edge
```

### 查看接口状态

```
OS10# show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of MSTI 0 is designated Forwarding
Edge port:yes port guard :none (default)
Link type is point-to-point (auto)
Boundary: YES bpduguard :disable bpduguard shutdown-on-violation :disable RootGuard: disable LoopGuard disable
Bpdus (MRecords) sent 610, received 5
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated PortID

ethernet1/1/4 128.272 128 500 FWD 0 32768 90b1.1cf4.a911 128.272
=====
```

## 生成树扩展

STP 扩展提供了一种通过安全地强制实施活动网络拓扑来确保高效的网络融合的方法。OS10 支持 BPDU 筛选、BPDU 防护、根防护和环路防护 STP 扩展。

在 BPDU 违规后，系统会丢弃常规数据流量。

- BPDU 筛选

防止网络从故障设备中意外使 BPDU 泛洪。在接口上启用 BPDU 筛选会导致系统发送或接收 BPDU。
- BPDU 防护

阻止 L2 桥接端口和连接到终端主机和服务器的 LAG 端口接收任何 BPDU。启用 BPDU 防护时，如果端口收到任何 BPDU 帧，则将桥或 LAG 端口置于 Error\_Disable 或阻止状态。在 LAG 的情况下，所有成员端口都会置于阻止状态。数据流量被丢弃，但端口继续将 BPDU 转发到后来丢弃的 CPU。为防止进一步接收 BPDU，请将端口配置为使用 violation action 命令关闭。有关 STP 命令的详细信息，请参阅 STP 命令。
- 根防护

避免桥接环路并在网络过渡期间保留根桥位置。STP 选择具有最低优先级值的根桥。在网络过渡期间，另一个具有较低优先级的桥可能会尝试成为根桥并会导致无法预测的网络行为。为避免此类尝试并保留根桥位置，请配置 spanning-tree guard root 命令。在属于指定端口的端口上启用根防护。根防护配置适用于端口上配置的所有 VLAN。
- 环路防护

防止线缆或接口硬件故障导致 L2 转发环路。当发生硬件故障时，参与的生成树链路将成为单向的，并且端口停止接收 BPDU。当阻止的端口停止接收 BPDU 时，它会转换为转发状态，从而导致网络中的生成树循环。在转换为环路不一致状态的端口上启用环路防护，直至使用 spanning-tree guard loop 命令接收 BPDU。接收到 BPDU 后，该端口将移出环路不一致或阻止状态，并转换为由 STP 确定的相应状态。对每个端口启用环路防护可在端口上配置的所有 VLAN 上启用该功能。如果在某个端口上禁用环路防护，它将进入侦听状态。

 **注:**  
1. 根防护和环路防护相互排斥。

2. 从活动配置中配置一种防护会覆盖另一种防护。

1. 在 INTERFACE 模式下启用生成树 BPDU 筛选器。

```
spanning-tree bpdupfilter enable
```

2. 在 INTERFACE 模式下启用 STP BPDU 防护。

```
spanning-tree bpduguard enable
```

BPDU 防护违规会导致系统执行以下操作：

- 关闭端口通道接口，并且所有成员端口在硬件中处于禁用状态。
- 将物理端口添加到已处于 Error\_Disable 状态的端口通道；此外，硬件中的新成员端口处于禁用状态。
- 从 Error Disabled 状态的端口通道中移除物理端口。从端口通道中移除物理端口后，系统将在物理端口上清除 Error\_Disabled 状态，并在硬件中启用。

要清除 Error Disabled 状态，请执行以下操作：

- 在接口上使用 shutdown 命令。
- 使用 spanning-tree bpduguard disable 命令禁用接口上的 BPDU 防护。
- 使用 spanning-tree disable 命令禁用接口上的 STP。

3. 设置防护类型以在 INTERFACE 模式下避免环路。

```
spanning-tree guard {loop | root | none}
```

- loop — 将防护类型设置为环路。
- root — 将防护类型设置为根。
- none — 将防护类型设置为无。

#### 在环路防护条件下端口已启用

- 在 RPVST+ 模式下，任何已启用 STP 的端口或端口通道接口都支持环路防护。
- 您不能在 STP 端口上同时启用根防护和环路防护。环路防护配置会覆盖现有的根防护配置，反之亦然。
- 在端口上同时启用 BPDU 防护和环路防护会导致端口仍处于阻止状态，并阻止流量流过它。例如，当您同时配置 Portfast BPDU 防护和环路防护时：
  - 如果从远程设备接收到 BPDU，BPDU 防护会将该端口置于 Err-Disabled 阻止状态，并且该端口上没有流量转发。
  - 如果没有从发送 BPDU 的远程设备接收到 BPDU，则环路防护会将该端口置于环路不一致的阻止状态，并且该端口上没有流量转发。
- 在 PVST+ 网络中使用，STP 环路防护将按每个端口或端口通道在 VLAN 级别执行。如果未在端口通道接口上接收到 BPDU，则端口或端口通道将仅转换为该 VLAN 的环路不一致或阻止状态。

#### BPDU 筛选器

```
OS10(conf-if-eth1/1/4)# spanning-tree bpdupfilter enable
OS10(conf-if-eth1/1/4)# do show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of vlan1 is designated Blocking
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary: NO bpdup filter : Enable bpdup guard : bpduguard shutdown-on-
violation :disable RootGuard: enable LoopGuard disable
Bpdus (MRecords) sent 134, received 138
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated

ethernet1/1/4 128.272 128 500 BLK 500 32769 90b1.1cf4.a911 128.272
```

#### BPDU 防护

```
OS10(config)# interface ethernet 1/1/4
OS10(conf-if-eth1/1/4)# spanning-tree bpduguard enable
OS10(conf-if-eth1/1/4)# do show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of vlan1 is designated Blocking
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary: NO bpdup filter : Enable bpdup guard : bpduguard shutdown-on-
violation :enable RootGuard: enable LoopGuard disable
Bpdus (MRecords) sent 134, received 138
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated

ethernet1/1/4 128.272 128 500 BLK 500 32769 90b1.1cf4.a911 128.272
```

```

ethernet1/1/4 128.272 128 500 BLK 500 32769 90b1.1cf4.a911 128.272
```

## 环路防护

```
OS10(config)# interface ethernet 1/1/4
OS10(conf-if-eth1/1/4)# spanning-tree guard loop
OS10(conf-if-eth1/1/4)# do show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of vlan1 is root Forwarding
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary: NO bpduguard filter : bpduguard shutdown-on-
violation :disable RootGuard: disable LoopGuard enable
Bpdus (MRecords) sent 7, received 20
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated PortID

ethernet1/1/4 128.272 128 500 FWD 0 32769 90b1.1cf4.9d3b 128.272
```

## 根防护

```
OS10(conf-if-eth1/1/4)# spanning-tree guard root
OS10(conf-if-eth1/1/4)# do show spanning-tree interface ethernet 1/1/4
ethernet1/1/4 of vlan1 is root Forwarding
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary: NO bpduguard filter : bpduguard shutdown-on-
violation :disable RootGuard: enable LoopGuard disable
Bpdus (MRecords) sent 7, received 33
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated PortID

ethernet1/1/4 128.272 128 500 BLK 500 32769 90b1.1cf4.a911 128.272
```

# 从 BPDU 防护违规中恢复

1. 当某个端口上存在 BPDU 防护违规时，OS10 将关闭该端口或将其移至 BLOCKED 状态。在 CONFIGURATION 模式下使用以下命令关闭端口。命令的 no 版本将端口移至 BLOCKED 状态。

```
errdisable detect cause bpduguard
```

2. 在 CONFIGURATION 模式下，使用以下命令来恢复端口，使其因检测到 BPDU 防护违规而关闭。当恢复选项启用时，该端口将在恢复计时器到期后启动。默认恢复计时器值为 60 秒。当恢复选项处于禁用状态时，该端口将保持无限期关闭。您必须使用 no shutdown 命令手动启动端口。

```
errdisable recovery cause bpduguard
```

命令的 no 版本将禁用恢复选项。

3. 要更改恢复计时器值，请在 CONFIGURATION 模式下使用以下命令。

```
errdisable recovery interval interval-value
```

## 配置示例

```
OS10(config)# errdisable detect cause bpduguard
OS10(config)# errdisable recovery interval 45
OS10(config)# errdisable recovery cause bpduguard
```

## 查看检测和恢复详细信息

```
OS10# show errdisable detect
```

| Error-Disable Cause | Detect Status |
|---------------------|---------------|
|---------------------|---------------|

```

bpduguard Enabled

OS10# show errdisable recovery

Error-Disable Recovery Timer Interval: 300 seconds

Error-Disable Reason Recovery Status

bpduguard Enabled

Interface Errdisable Cause Recovery Time left

ethernet 1/1/1:1 bpduguard 273
ethernet 1/1/2 bpduguard 4
port-channel 12 bpduguard 45
```

## MAC 刷新优化

OS10 提供了 MAC 地址识别技术，可优化生成树协议 (STP) 模块发送的 MAC 刷新调用数。

如果发送到硬件的调用次数过高，则会丢弃流量或影响系统性能。为防止流量丢弃和泛洪，您可以使用 MAC 刷新优化功能。

此功能可精细调整与 MAC 刷新相关的参数，例如 MAC 刷新阈值和 MAC 刷新计时器，以减少发送到硬件的调用次数。发送清除请求以清除 MAC 地址表条目称为刷新指示。发送的调用次数在显示生成树命令中显示为刷新调用。

您可以通过将 MAC 刷新计时器设置为非零值来启用 MAC 刷新优化功能。默认情况下，此功能已启用，默认计时器值为 200 毫秒。

要禁用 MAC 刷新优化，请将 MAC 刷新计时器值配置为 0。

将 MAC 刷新计时器配置为非零值且阈值为零时，系统将调用一次基于实例的刷新，并启动计时器。当计时器过期时，系统将再次调用基于实例的刷新。

show spanning-tree {brief | details | active} 命令可显示以下信息：

```
Flush Interval 200 centi-sec, Flush Invocations 32
Flush Indication threshold 2
```

默认情况下，RSTP、RPVST 和 MSTP 已启用此功能。此功能在具有 MSTP & RPVST（多实例）的可扩展拓扑中非常有用，其中多个 MAC 刷新调用将被调用。

### RSTP

RSTP 允许基于每个端口进行刷新，直至发送的调用数等于已配置的 MAC 刷新阈值。

当发送的调用数达到配置的阈值时，RSTP 将忽略基于端口的其他刷新，并启动 MAC 刷新计时器。当计时器过期时，RSTP 将调用整个表刷新，其中将针对所有端口请求一个刷新。

RSTP 是单个实例，因此不需要 MAC 刷新优化。但是，要启用此功能，请将 MAC 刷新计时器配置为非零值。此配置将全局应用，并且适用于 RSTP、MSTP 和 RPVST。更改 STP 模式后，将保留此配置。

对于 RSTP，阈值将设置为更大的值 (65,535)，因为 RSTP 不需要此优化。即使已启用此功能，仅在刷新次数达到 65,535 后才会调用全局刷新。

### MSTP

MSTP 允许基于（VLAN 列表，端口）进行刷新，直至发送的调用数等于已配置的 MAC 刷新阈值。

当调用数超过配置的阈值时，MSTP 将忽略基于其他（VLAN 列表，端口）的刷新，并启动 MAC 刷新计时器。计时器启动时，系统会阻止所有其他刷新指示。当该特定实例的计时器过期时，系统会触发基于实例的刷新。

MSTP 的默认 MAC 刷新阈值为 5。

### RPVST

RPVST 允许基于（VLAN，端口）进行刷新，直至发送的调用数等于已配置的 MAC 刷新阈值。

当发送的调用数超过配置的阈值时，RPVST 将忽略基于其他（VLAN，端口）的刷新，并启动 MAC 刷新计时器。计时器启动时，系统会阻止其他刷新。当该特定实例的计时器过期时，系统会触发基于 VLAN 的刷新。

默认情况下，MAC 刷新阈值设置为 5。但是，Dell EMC 建议根据参与 STP 拓扑的端口数来配置此值。



## 调试配置

使用 `debug spanning-tree bpdu` 命令可监控并验证 MST 配置是否按配置进行通信。要确保所有必要的参数匹配-区域名称、地区版本和 VLAN 到实例映射，请检查您的各个设备。使用 `show spanning-tree mst` 命令可查看 MST 配置，或者使用 `show running-configuration` 命令查看总体 MST 配置。

**从同一个区域接收的用于通信的 MST 标记** MST 路由器位于同一地区。如果调试日志指示数据包来自不同的区域，则其中一个密钥参数不匹配。

**MST 地区名称和版本** 配置的名称和版本在所有设备中必须相同。如果区域名称为空，则在一个设备上配置了一个名称，但在另一个设备上未配置或配置了不同的名称 — 包括拼写和大写不同。

**MST 实例** 使用 `show` 命令可验证 VLAN 到 MST 的实例映射。如果在发送或接收的日志中看到额外的 MST 实例，则在一个路由器上配置了一个额外的 MST 实例，但其他路由器不适用。

- 以 EXEC 模式查看 BPDU。

```
debug spanning-tree bpdu
```

- 在 EXEC 模式下查看 MST 触发的拓扑更改消息。

```
debug spanning-tree events
```

### 查看 MST 配置

```
OS10# show spanning-tree mst configuration
Region Name: force10
Revision: 100
MSTI VID
0 1,31-4093
1 2-10
2 11-20
3 21-30
```

## 为快速状态转移设置生成树链接类型

如 IEEE 802.1w 中的规定，OS10 假设以全双工模式运行的端口是点对点链路。点对点链路可更快地转换为转发状态。默认情况下，OS10 从双工模式派生端口的链路类型。您可以使用 `spanning-tree link-type` 命令来覆盖双工模式。

OS10 假定在半双工模式下运行的端口是共享链路，其快速转换功能不适用。此外，如果您将某个端口明确指定为共享链路，则不能使用快速转换功能，而不考虑双工设置。

要加快生成树的状态转换，您可以将链路类型设置为点对点。要将链路类型设置为点对点，请执行以下操作：

- 在 INTERFACE 模式下使用以下命令。

```
spanning-tree link-type point-to-point
```

## 常见的 STP 命令

### clear spanning-tree counters

清除 STP 的计数器。

**语法** `clear spanning-tree counters [interface {ethernet node/slot/port[:subport] | port-channel number}]`

**参数**

- `interface` — 输入接口类型：
  - `ethernet node/slot/port[:subport]` — 从物理端口删除生成树计数器。
  - `port-channel number` — 删除端口通道接口的生成树计数器，从 1 到 128。

**默认** 未配置



|        |                                                                         |
|--------|-------------------------------------------------------------------------|
| 命令模式   | EXEC                                                                    |
| 使用情况信息 | 清除设备上每个以太网接口或端口通道的所有 STP 的计数器。                                          |
| 示例     | <pre>OS10# clear spanning-tree counters interface port-channel 10</pre> |
| 支持的版本  | 10.2.0E or later                                                        |

## debug spanning-tree

使 STP 可以调试和显示协议信息。

|        |                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | debug spanning-tree {all   bpdu [tx   rx]   events}                                                                                          |
| 参数     | <ul style="list-style-type: none"> <li>all — 调试所有生成树操作。</li> <li>bpdu — 输入传输 (tx) 或接收 (rx) 以启用调试方向。</li> <li>events — 调试 PVST 事件。</li> </ul> |
| 默认     | 未配置                                                                                                                                          |
| 命令模式   | EXEC                                                                                                                                         |
| 使用情况信息 | 无                                                                                                                                            |
| 示例     | <pre>OS10# debug spanning-tree bpdu rx</pre>                                                                                                 |
| 支持的版本  | 10.2.0E or later                                                                                                                             |

## errdisable detect cause bpduguard

在检测 BPDU 防护违规时，将端口配置为关闭，或将端口移至受阻状态。

|        |                                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | errdisable detect cause bpduguard                                                                                                                                                                                            |
| 参数     | 无                                                                                                                                                                                                                            |
| 默认     | 已启用                                                                                                                                                                                                                          |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                |
| 使用情况信息 | <p>此命令仅适用于已启用 STP 的端口。只有在端口上配置 BPDU 防护时，命令才会生效。</p> <p>当检测原因选项启用时，每当发生 BPDU 防护冲突时，端口都将关闭。</p> <p>禁用该选项时，该端口将不会关闭，但会在发生 BPDU 防护违规时移至阻止状态。在这种情况下，端口将在生成树模式下停止运行，并且当恢复计时器过期时，端口将正常运行，而不考虑恢复原因配置。</p> <p>命令的 no 版本将禁用检测原因选项。</p> |
| 示例     | <pre>OS10(config)# errdisable detect cause bpduguard</pre>                                                                                                                                                                   |
| 支持的版本  | 10.4.2.0 or later                                                                                                                                                                                                            |

## errdisable recovery cause bpduguard

由于 BPDU 防护违规，启用以恢复端口。

|      |                                     |
|------|-------------------------------------|
| 语法   | errdisable recovery cause bpduguard |
| 参数   | 无                                   |
| 默认   | 已禁用                                 |
| 命令模式 | CONFIGURATION                       |

#### 使用情况信息

此命令仅适用于已启用 STP 的端口。仅当在端口上配置了 BPDU 防护并且在端口上已启用 `errdisable detect cause bpduguard` 时，命令才会生效。

当恢复选项启用时，该端口将在恢复计时器到期后启动。

当恢复选项已禁用时，该端口将无限期关闭。您必须使用 `shutdown` 和 `no shutdown` 命令手动启动端口。

命令的 `no` 版本将禁用恢复选项。

#### 示例

```
OS10(config)# errdisable recovery cause bpduguard
```

#### 支持的版本

10.4.2.0 or later

## errdisable recovery interval

将恢复时间间隔计时器配置为在 BPDU 防护违规时延迟端口恢复。

#### 语法

```
errdisable recovery interval interval-value
```

#### 参数

*interval-value*— 以秒为单位输入时间间隔。范围从 30 到 65535。

#### 默认

300 秒

#### 命令模式

CONFIGURATION

#### 使用情况信息

此命令仅适用于已启用 STP 的端口。只有在端口上配置 BPDU 防护时，命令才会生效。

只要存在 BPDU 防护违规，就会开始恢复计时器。

命令的 `no` 版本会将计时器重置为默认值。

#### 示例

```
OS10(config)# errdisable recovery interval 45
```

#### 支持的版本

10.4.2.0 or later

## clear spanning-tree detected-protocol

强制 MST 端口与邻居重新协商。

#### 语法

```
clear spanning-tree detected-protocol [interface {ethernet node/slot/port[:subport] | port-channel number}]
```

#### 参数

- *interface* — 输入接口类型：
  - *ethernet node/slot/port[:subport]* — 输入以太网接口信息，从 1 到 48。
  - *port-channel number* — 输入端口通道号，从 1 到 128。

#### 默认

未配置

#### 命令模式

EXEC

#### 使用情况信息

使用此命令可强制 RPVST+ 端口与邻居重新协商。如果在没有参数的情况下使用此命令，则此命令将应用于每个设备端口。

#### 示例

```
OS10# clear spanning-tree detected-protocol interface ethernet 1/1/1
```

#### 支持的版本

10.2.0E or later

## spanning-tree bpduguard

启用或禁用接口上的 BPDU 筛选。

#### 语法

```
spanning-tree bpduguard {enable | disable}
```

**参数**

- enable — 启用接口上的 BPDU 筛选器。
- disable — 禁用接口上的 BPDU 筛选器。

**默认** 已禁用

**命令模式** INTERFACE

**使用情况信息** 使用 enable 参数可启用 BPDU 筛选。

**示例**

```
OS10(config-if-eth1/1/4)# spanning-tree bpdufilter enable
```

**支持的版本** 10.2.0E or later

## spanning-tree bpduguard

启用或禁用接口上的 BPDU 防护。

**语法** spanning-tree bpduguard {enable | disable}

**参数**

- enable — 启用接口上的 BPDU 防护筛选器。
- disable — 禁用接口上的 BPDU 防护筛选器。

**默认** 已禁用

**命令模式** INTERFACE

**使用情况信息** BPDU 防护可防止端口接收 BPDU。如果端口接收到 BPDU，则将其置于错误禁用状态。

**示例**

```
OS10(config-if-eth1/1/4)# spanning-tree bpduguard enable
```

**支持的版本** 10.2.0E or later

## spanning-tree disable

在交换机或指定接口上使用 spanning-tree mode 命令全局禁用配置的生成树模式。

**语法** spanning-tree disable

**参数** 无

**默认** 未配置。

**使用情况信息** 此命令的 no 版本将重新启用 STP，并应用当前配置的生成树设置。

**命令模式** CONFIGURATION

INTERFACE

**示例**

```
OS10(config)# interface ethernet 1/1/4
OS10(config-if-eth1/1/4)# spanning-tree disable
```

**支持的版本** 10.3.0E or later

## spanning-tree guard

启用或禁用接口上的环路防护或根防护。

**语法** spanning-tree guard {loop | root | none}

**参数**

- loop — 启用接口上的环路防护。
- root — 启用接口上的根防护。
- none — 将防护模式设置为无。

**默认** 未配置

|               |                                                               |
|---------------|---------------------------------------------------------------|
| <b>使用情况信息</b> | 环路防护和根防护配置相互排斥。从活动配置中配置一种防护会覆盖另一种防护。                          |
| <b>命令模式</b>   | INTERFACE                                                     |
| <b>示例</b>     | <pre>OS10(config-if-eth1/1/4)# spanning-tree guard root</pre> |
| <b>支持的版本</b>  | 10.2.0E or later                                              |

## spanning-tree link-type

设置生成树的链接类型，以实现更快的融合。

|               |                                                                                                                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>spanning-tree link-type {auto   point-to-point   shared}</code>                                                                                                                                                           |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>auto</code> — 根据接口的双工设置输入关键字来设置链路类型。</li> <li><code>point-to-point</code> — 指定接口是点对点还是全双工链路。</li> <li><code>shared</code> — 指定接口为半双工介质。</li> </ul>                                 |
| <b>默认</b>     | 自动                                                                                                                                                                                                                              |
| <b>命令模式</b>   | INTERFACE                                                                                                                                                                                                                       |
| <b>使用情况信息</b> | <p>如 IEEE 802.1w 中的规定，OS10 假设以全双工模式运行的端口是点对点链路。点对点链路可更快地转换为转发状态。默认情况下，OS10 从双工模式派生端口的链路类型。您可以使用 <code>spanning-tree link-type</code> 命令来覆盖双工模式。</p> <p>由于半双工模式被视为共享链路，因此快速中转功能不适用于共享链接。如果将某个端口指定为共享链路，则不能使用快速中转功能，而不考虑双工设置。</p> |
| <b>示例</b>     | <pre>OS10(config)# spanning-tree link-type point-to-point</pre>                                                                                                                                                                 |
| <b>支持的版本</b>  | OS10 原有命令。                                                                                                                                                                                                                      |

## spanning-tree mac-flush-timer

启用或禁用 MAC 刷新优化。

|               |                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>spanning-tree mac-flush-timer timer-interval</code>                                                                                      |
| <b>参数</b>     | <code>timer-interval</code> — 以毫秒为单位输入计时器间隔，从 0 到 500。默认值为 200 毫秒。                                                                             |
| <b>默认</b>     | 已启用                                                                                                                                            |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                                  |
| <b>使用情况信息</b> | <p>此命令将配置刷新间隔时间（以毫秒为单位），并控制从生成树模块调用的调用数。如果计时器设置为 0，将进行基于端口和间隔的刷新。如果计时器设置为非零值，基于实例的刷新将根据 MAC 的刷新阈值进行。此命令的 <code>no</code> 版本将刷新间隔计时器重置为默认值。</p> |
| <b>示例</b>     | <pre>OS10(config)# spanning-tree mac-flush-timer 500</pre> <pre>OS10(config)# no spanning-tree mac-flush-timer</pre>                           |
| <b>支持的版本</b>  | 10.4.3.0 or later                                                                                                                              |

## spanning-tree mode

启用 STP 类型：RSTP、快速 PVST+ 或 MST。

|           |                                                                                          |
|-----------|------------------------------------------------------------------------------------------|
| <b>语法</b> | <code>spanning-tree mode {rstp   mst   rapid-pvst}</code>                                |
| <b>参数</b> | <ul style="list-style-type: none"> <li><code>rstp</code> — 将 STP 模式设置为“RSTP”。</li> </ul> |

|           |                                                                                                                     |
|-----------|---------------------------------------------------------------------------------------------------------------------|
|           | <ul style="list-style-type: none"><li>• mst — 将 STP 模式设置为 MST。</li><li>• rapid-pvst — 将 STP 模式设置为 RPVST+。</li></ul> |
| 默认        | RPVST+                                                                                                              |
| 命令模式      | CONFIGURATION                                                                                                       |
| 使用情况信息    | 所有 STP 实例在之前的 STP 模式下都停止，并在新模式下重新启动。您还可以将更改为 RSTP/MST 模式。                                                           |
| 示例 (RSTP) | <pre>OS10(config)# spanning-tree mode rstp</pre>                                                                    |
| 示例 (MST)  | <pre>OS10(config)# spanning-tree mode mst</pre>                                                                     |
| 支持的版本     | 10.2.0E or later                                                                                                    |

## spanning-tree port

将端口类型设置为 Edgeport。

|        |                                                                      |
|--------|----------------------------------------------------------------------|
| 语法     | spanning-tree port type edge                                         |
| 参数     | 无                                                                    |
| 默认     | 未配置                                                                  |
| 命令模式   | INTERFACE                                                            |
| 使用情况信息 | 在运行 STP 的设备上配置 Edgeport 时，该端口将立即转换为转发状态。只有连接到终端主机的已配置端口将充当 EdgePort。 |
| 示例     | <pre>OS10(config)# spanning-tree port type edge</pre>                |
| 支持的版本  | 10.2.0E or later                                                     |

## show errdisable

显示有关 errdisable 配置和端口恢复状态的信息。

|        |                                                                                                                                                                                                                                                                                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show errdisable [detect   recovery]                                                                                                                                                                                                                                                                            |
| 参数     | <ul style="list-style-type: none"><li>• detect — 显示是否为问题启用了错误禁用检测。</li><li>• recovery — 显示错误禁用端口的恢复原因、恢复间隔和恢复状态的详细信息。</li></ul>                                                                                                                                                                                |
| 默认     | 无                                                                                                                                                                                                                                                                                                              |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                           |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                              |
| 示例     | <pre>OS10# show errdisable detect  Error-Disable Cause          Detect Status ----- bpduguard                    Enabled  OS10# show errdisable recovery  Error-Disable Recovery Timer Interval: 300 seconds  Error-Disable Reason          Recovery Status ----- bpduguard                      Enabled</pre> |

| Interface        | Errdisable Cause | Recovery Time left (seconds) |
|------------------|------------------|------------------------------|
| ethernet 1/1/1:1 | bpduguard        | 273                          |
| ethernet 1/1/2   | bpduguard        | 4                            |
| port-channel 12  | bpduguard        | 45                           |

**支持的版本** 10.4.2.0 or later

## show spanning-tree interface

显示以太网和端口通道的生成树接口信息。

**语法** `show spanning-tree interface {ethernet node/slot/port [:subport] | port-channel port-id} [detail]`

- 参数**
- `ethernet node/slot/port[:subport]` — 显示物理接口的生成树信息。
  - `port-channel port-id` — 显示端口通道编号的生成树信息，从 1 到 128。
  - `detail` — (可选) 显示有关接口的详细信息。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# show spanning-tree interface ethernet 1/1/6:2 detail
Port 281 (ethernet1/1/6:2) of RSTP 1 is root Forwarding
Port path cost 2000, Port priority 128, Port Identifier 281.128
Designated root has priority 32768, address 34:17:44:55:66:7f
Designated bridge has priority 32768, address 34:17:44:55:66:7f
Designated port id is 151.128, designated path cost
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state 1
Link type is point-to-point by default, auto
PVST Simulation is enabled by default
BPDU sent 3, received 7
```

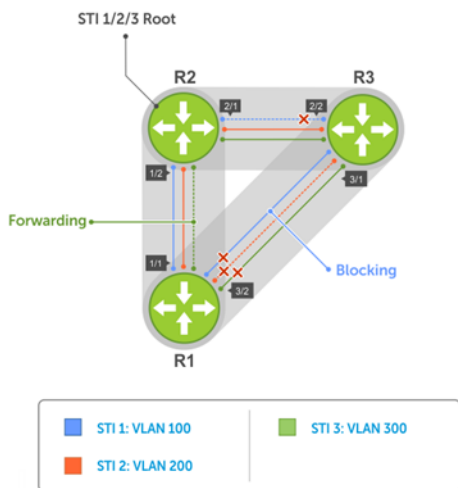
**支持的版本** 10.2.0E or later

## Rapid per-VLAN spanning-tree plus

Rapid per-VLAN spanning-tree plus (RPVST+) 用于按 VLAN 创建单个拓扑。默认情况下，RPVST+ 处于启用状态；它可提供比 STP 更快的融合，并在默认 VLAN (VLAN 1) 上运行。

配置快速 PVST+ 是一个四步流程：

1. 确保接口处于 L2 模式。
2. 将接口置于 VLAN 中。默认情况下，交换机端口接口是默认 (VLAN1) 的成员。
3. 启用快速 PVST+。只有 STP 的其他变体存在时才需要此步骤。
4. (可选) 为 VLAN 选择非默认桥优先级，以实现负载均衡。

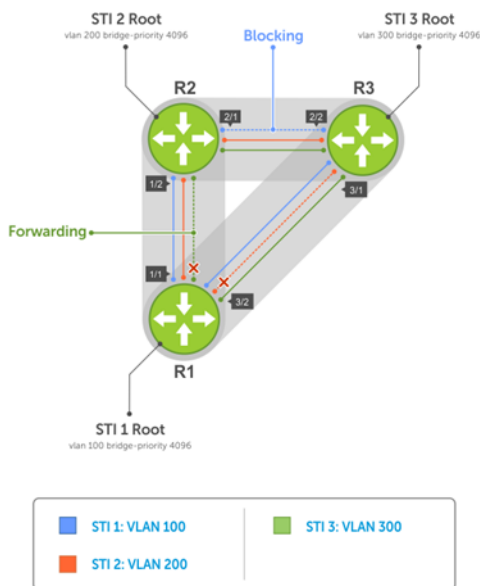


每个 VLAN 都分配有增量默认桥优先级。例如，如果为 VLAN 1 分配了桥优先级值 32769，则 VLAN 2（如果已创建）分配有桥优先级值 32770；同样，为 VLAN 10（如果已创建）分配了桥优先级值 32778，依此类推。所有三个实例都具有相同的转发拓扑。

**注：** Mt.Echo 支持 64 个实例，其中 1 个实例 VLT 控制 VLAN 保留，1 个用于 L3 VLAN，1 个用于默认的 STP 实例。当您运行快速 pvst 命令时，每个 VLAN 都会分配一个实例，直至 VLAN 数达到 61，然后映射默认实例。

## 负载均衡和根选择

默认情况下，所有 VLAN 使用相同的转发拓扑 — R2 将选择为根，并且所有 10G 以太网端口都具有相同的成本。可以修改每个 VLAN 的桥优先级以启用不同的转发拓扑。



要实现 RPVST+ 负载均衡，请在每个桥上分配不同的优先级。

## 启用 RPVST+

默认情况下，RPVST+ 已启用，并且仅在您将第一个成员端口添加到 VLAN 之后创建实例。要加入 RPVST+，端口通道或物理接口必须是 VLAN 的成员。将所有物理和端口通道接口添加到默认 VLAN (VLAN1)。

- 在 CONFIGURATION 模式下启用快速 PVST+ 模式。

```
spanning-tree mode rapid-pvst
```

配置 RPVST+

```
OS10(config)# spanning-tree mode rapid-pvst
```

查看 RPVST+ 配置

```
OS10# show spanning-tree active
Spanning tree enabled protocol rapid-pvst with force-version rstp
VLAN 1
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 3417.4455.667f
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32769, Address 90b1.1cf4.a523
Configured hello time 2, max age 20, forward delay 15
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated PortID

ethernet1/1/5 128.276 128 500 FWD 0 32768 3417.4455.667f 128.146
ethernet1/1/6 128.280 128 500 BLK 0 32768 3417.4455.667f 128.150
Interface
Name Role PortID Prio Cost Sts Cost Link-type Edge

ethernet1/1/5 Root 128.276 128 500 FWD 0 AUTO No
ethernet1/1/6 Altr 128.280 128 500 BLK 0 AUTO No
```

选择根桥

RPVST+ 根据 VLAN 桥优先级确定根桥。为一个桥分配较低优先级会增加其成为根桥的可能性。命令 `show spanning-tree brief` 将显示所有端口的相关信息，而不考虑操作状态。

- 将数字分配为桥优先级，或将其指定为 CONFIGURATION 模式下的根，从 0 到 61440。

```
spanning-tree {vlan vlan-id priority priority-value}
```

- `vlan-id` — 输入介于 1 到 4093 之间的值。
- `priority priority-value` — 以 4096 为增量输入优先级值，默认值为 32768。分配的数字越小，桥成为根桥的可能性更大。有效的桥优先级值包括：0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344 或 61440。所有其他值都将被拒绝。

配置根桥

```
OS10(config)# spanning-tree vlan 1 priority 4096
```

查看活动配置

```
OS10(config)# do show spanning-tree active
Spanning tree enabled protocol rapid-pvst with force-version rstp
VLAN 1
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 4097, Address 90b1.1cf4.a523
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 4097, Address 90b1.1cf4.a523
We are the root of VLAN 1
Configured hello time 2, max age 20, forward delay 15
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated PortID

ethernet1/1/5 128.276 128 500 FWD 0 4097 90b1.1cf4.a523 128.276
ethernet1/1/6 128.280 128 500 FWD 0 4097 90b1.1cf4.a523 128.280
Interface
Name Role PortID Prio Cost Sts Cost Link-type Edge

ethernet1/1/5 Desg 128.276 128 500 FWD 0 AUTO No
ethernet1/1/6 Desg 128.280 128 500 FWD 0 AUTO No
```



## 查看简要配置

```
OS10# show spanning-tree brief
Spanning tree enabled protocol rapid-pvst with force-version rstp
VLAN 1
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 4097, Address 90b1.1cf4.a523
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 4097, Address 90b1.1cf4.a523
We are the root of VLAN 1
Configured hello time 2, max age 20, forward delay 15
```

| Interface Name | PortID  | Prio | Cost       | Sts | Cost | Bridge ID | Designated ID  | PortID  |
|----------------|---------|------|------------|-----|------|-----------|----------------|---------|
| ethernet1/1/1  | 128.260 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.260 |
| ethernet1/1/2  | 128.264 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.264 |
| ethernet1/1/3  | 128.268 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.268 |
| ethernet1/1/4  | 128.272 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.272 |
| ethernet1/1/5  | 128.276 | 128  | 500        | FWD | 0    | 4097      | 90b1.1cf4.a523 | 128.276 |
| ethernet1/1/6  | 128.280 | 128  | 500        | FWD | 0    | 4097      | 90b1.1cf4.a523 | 128.280 |
| ethernet1/1/7  | 128.284 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.284 |
| ethernet1/1/8  | 128.288 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.288 |
| ethernet1/1/9  | 128.292 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.292 |
| ethernet1/1/10 | 128.296 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.296 |
| ethernet1/1/11 | 128.300 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.300 |
| ethernet1/1/12 | 128.304 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.304 |
| ethernet1/1/13 | 128.308 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.308 |
| ethernet1/1/14 | 128.312 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.312 |
| ethernet1/1/15 | 128.316 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.316 |
| ethernet1/1/16 | 128.320 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.320 |
| ethernet1/1/17 | 128.324 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.324 |
| ethernet1/1/18 | 128.328 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.328 |
| ethernet1/1/19 | 128.332 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.332 |
| ethernet1/1/20 | 128.336 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.336 |
| ethernet1/1/21 | 128.340 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.340 |
| ethernet1/1/22 | 128.344 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.344 |
| ethernet1/1/23 | 128.348 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.348 |
| ethernet1/1/24 | 128.352 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.352 |
| ethernet1/1/25 | 128.356 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.356 |
| ethernet1/1/26 | 128.360 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.360 |
| ethernet1/1/27 | 128.364 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.364 |
| ethernet1/1/28 | 128.368 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.368 |
| ethernet1/1/29 | 128.372 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.372 |
| ethernet1/1/30 | 128.376 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.376 |
| ethernet1/1/31 | 128.380 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.380 |
| ethernet1/1/32 | 128.384 | 128  | 2000000000 | FWD | 0    | 32769     | 0000.0000.0000 | 128.384 |

```
Interface
Name Role PortID Prio Cost Sts Cost Link-type Edge

ethernet1/1/1 Disb 128.260 128 2000000000 FWD 0 AUTO No
ethernet1/1/2 Disb 128.264 128 2000000000 FWD 0 AUTO No
ethernet1/1/3 Disb 128.268 128 2000000000 FWD 0 AUTO No
ethernet1/1/4 Disb 128.272 128 2000000000 FWD 0 AUTO No
ethernet1/1/5 Desg 128.276 128 500 FWD 0 AUTO No
ethernet1/1/6 Desg 128.280 128 500 FWD 0 AUTO No
ethernet1/1/7 Disb 128.284 128 2000000000 FWD 0 AUTO No
ethernet1/1/8 Disb 128.288 128 2000000000 FWD 0 AUTO No
ethernet1/1/9 Disb 128.292 128 2000000000 FWD 0 AUTO No
ethernet1/1/10 Disb 128.296 128 2000000000 FWD 0 AUTO No
ethernet1/1/11 Disb 128.300 128 2000000000 FWD 0 AUTO No
```

## 根分配

RPVST+ 根据最小桥 ID 分配根桥。将一个桥指定为根桥，将另一个桥指定为辅助根桥。

- 在 CONFIGURATION 模式下将设备配置为根或辅助根。

```
spanning-tree vlan vlan-id root {primary | secondary}
```

- `o vlan-id` — 输入 VLAN ID 号，从 1 到 4093。

- o primary — 输入桥作为主桥或根桥。主要桥值为 24576。
- o secondary — 将桥输入为辅助根桥。第二桥值为 28672。

## 将根桥配置为主桥

```
OS10(config)# spanning-tree vlan 1 root primary
```

## 验证根桥信息

```
OS10# show spanning-tree active
```

```
Spanning tree enabled protocol rapid-pvst with force-version rstp
```

```
VLAN 1
```

```
Executing IEEE compatible Spanning Tree Protocol
```

```
Root ID Priority 24577, Address 90b1.1cf4.a523
```

```
Root Bridge hello time 2, max age 20, forward delay 15
```

```
Bridge ID Priority 24577, Address 90b1.1cf4.a523
```

```
We are the root of VLAN 1
```

```
Configured hello time 2, max age 20, forward delay 15
```

| Interface Name | PortID  | Prio | Cost | Sts | Cost | Bridge ID            | Designated PortID |
|----------------|---------|------|------|-----|------|----------------------|-------------------|
| ethernet1/1/5  | 128.276 | 128  | 500  | FWD | 0    | 24577 90b1.1cf4.a523 | 128.276           |
| ethernet1/1/6  | 128.280 | 128  | 500  | LRN | 0    | 24577 90b1.1cf4.a523 | 128.280           |

| Interface Name | Role | PortID  | Prio | Cost | Sts | Cost | Link-type | Edge |
|----------------|------|---------|------|------|-----|------|-----------|------|
| ethernet1/1/5  | Desg | 128.276 | 128  | 500  | FWD | 0    | AUTO      | No   |
| ethernet1/1/6  | Desg | 128.280 | 128  | 500  | LRN | 0    | AUTO      | No   |

## 全局参数

所有非根桥都接受根桥上的计时器值。

- 转发时间** 接口从丢弃状态转换为获知状态或从获知状态转换为转发状态所需的时间量。
- 问候时间** 桥发送 BPDU 的时间间隔。
- 最大期限** 在桥通过重新计算 RPVST+ 拓扑来刷新信息之前保持配置信息的时间长度。

- 在 CONFIGURATION 模式下修改转发时间（以秒为单位），从 4 到 30，默认值为 15。

```
spanning-tree vlan vlan-id forward-time seconds
```

- 在 CONFIGURATION 模式下修改问候时间，从 1 到 10，默认值为 2。由于大型配置涉及更多数量的端口，Dell EMC 建议增加问候时间。

```
spanning-tree vlan vlan-id hello-time seconds
```

- 在 CONFIGURATION 模式下更改最大期限（以秒为单位），从 6 到 40，默认值为 20。

```
spanning-tree vlan vlan-id max-age seconds
```

## 查看 RPVST+ 全局参数

```
OS10# show spanning-tree active
```

```
Spanning tree enabled protocol rapid-pvst with force-version rstp
```

```
VLAN 1
```

```
Executing IEEE compatible Spanning Tree Protocol
```

```
Root ID Priority 32769, Address 90b1.1cf4.a523
```

```
Root Bridge hello time 2, max age 20, forward delay 15
```

```
Bridge ID Priority 32769, Address 90b1.1cf4.a523
```

```
We are the root of VLAN 1
```

```
Configured hello time 2, max age 20, forward delay 15
```

# RPVST+ 命令

## show spanning-tree vlan

按 VLAN ID 显示 RPVST+ 状态和配置信息。

|        |                                                 |
|--------|-------------------------------------------------|
| 语法     | show spanning-tree vlan <i>vlan-id</i>          |
| 参数     | <i>vlan vlan-id</i> — 输入 VLAN ID 号, 从 1 到 4093。 |
| 默认     | 未配置                                             |
| 命令模式   | EXEC                                            |
| 使用情况信息 | 无                                               |
| 示例     |                                                 |

```
OS10# show spanning-tree
Spanning tree enabled protocol rapid-pvst
VLAN 1
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32769, Address 74e6.e2f5.bb80
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32769, Address 74e6.e2f5.bb80
We are the root of VLAN 1
Configured hello time 2, max age 20, forward delay 15
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated

ethernet1/1/1 128.260 128 2000000000 FWD 0 32769 0000.0000.0000 128.260
ethernet1/1/2 128.264 128 2000000000 FWD 0 32769 0000.0000.0000 128.264
ethernet1/1/3 128.268 128 2000000000 FWD 0 32769 0000.0000.0000 128.268
ethernet1/1/4 128.272 128 2000000000 FWD 0 32769 0000.0000.0000 128.272
ethernet1/1/5 128.276 128 2000000000 FWD 0 32769 0000.0000.0000 128.276
ethernet1/1/6 128.280 128 2000000000 FWD 0 32769 0000.0000.0000 128.280
ethernet1/1/7 128.284 128 2000000000 FWD 0 32769 0000.0000.0000 128.284
ethernet1/1/8 128.288 128 2000000000 FWD 0 32769 0000.0000.0000 128.288
ethernet1/1/9 128.292 128 2000000000 FWD 0 32769 0000.0000.0000 128.292
ethernet1/1/10 128.296 128 2000000000 FWD 0 32769 0000.0000.0000 128.296
ethernet1/1/11 128.300 128 2000000000 FWD 0 32769 0000.0000.0000 128.300
ethernet1/1/12 128.304 128 2000000000 FWD 0 32769 0000.0000.0000 128.304
```

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|

## spanning-tree vlan cost

设置每个 VLAN 的接口的路径成本以进行 PVST 计算。

|        |                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | spanning-tree vlan <i>vlan-id</i> cost { <i>value</i> }                                                                                                                                                                                                                                                                                                                          |
| 参数     | <i>value</i> — 输入端口成本值以设置 PVST 计算的接口的路径成本, 从 1 到 200000000。                                                                                                                                                                                                                                                                                                                      |
| 默认     | <ul style="list-style-type: none"><li>• 100 Mb/s 以太网接口 = 200000</li><li>• 1 Gb 以太网接口 = 20000</li><li>• 10 Gb 以太网接口 = 2000</li><li>• 带有一个 100 Mb/s 以太网的端口通道接口 = 200000</li><li>• 带有一个 1 Gb 以太网的端口通道接口 = 20000</li><li>• 带有一个 10 Gb 以太网的端口通道接口 = 2000</li><li>• 带有两个 1 Gb 以太网的端口通道 = 18000</li><li>• 带有两个 10 Gb 以太网的端口通道 = 1800</li><li>• 带有两个 100 Mbps 以太网端口通道 = 180000</li></ul> |
| 命令模式   | INTERFACE                                                                                                                                                                                                                                                                                                                                                                        |
| 使用情况信息 | LAN 接口的介质速度决定了 STP 端口路径成本默认值。                                                                                                                                                                                                                                                                                                                                                    |

|       |                                                                      |
|-------|----------------------------------------------------------------------|
| 示例    | <pre>OS10(config-if-eth1/1/4)# spanning-tree vlan 10 cost 1000</pre> |
| 支持的版本 | 10.2.0E or later                                                     |

## spanning-tree vlan disable

禁用指定 VLAN 上的生成树。

|        |                                                         |
|--------|---------------------------------------------------------|
| 语法     | <code>spanning-tree vlan <i>vlan-id</i> disable</code>  |
| 参数     | <i>vlan-id</i> — 输入 VLAN ID 号, 从 1 到 4093。              |
| 默认     | 已启用                                                     |
| 命令模式   | CONFIGURATION                                           |
| 使用情况信息 | 此命令的 <code>no</code> 版本在指定 VLAN 上启用生成树。                 |
| 示例     | <pre>OS10(config)# spanning-tree vlan 100 disable</pre> |
| 支持的版本  | 10.4.0E(R1) or later                                    |

## spanning-tree vlan forward-time

在移动到转发状态之前, 为接口配置时间间隔以在阻止状态或学习状态等待。

|        |                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>spanning-tree vlan <i>vlan-id</i> forward-time <i>seconds</i></code>                                                                         |
| 参数     | <ul style="list-style-type: none"> <li><i>vlan-id</i> — 输入 VLAN ID 号, 从 1 到 4093。</li> <li><i>seconds</i> — 输入转发延迟时间 (以秒为单位), 从 4 到 30。</li> </ul> |
| 默认     | 15 秒                                                                                                                                               |
| 命令模式   | CONFIGURATION                                                                                                                                      |
| 使用情况信息 | 无                                                                                                                                                  |
| 示例     | <pre>OS10(config)# spanning-tree vlan 10 forward-time 16</pre>                                                                                     |
| 支持的版本  | 10.2.0E or later                                                                                                                                   |

## spanning-tree vlan force-version

将生成树的强制版本配置为传输 BPDU。

|        |                                                                                               |
|--------|-----------------------------------------------------------------------------------------------|
| 语法     | <code>spanning-tree vlan <i>vlan-id</i> force-version <i>rstp</i></code>                      |
| 参数     | <ul style="list-style-type: none"> <li><i>rstp</i> — 强制 RPVST+ 传输到 RSTP 的 BPDU 的版本</li> </ul> |
| 默认     | 未配置                                                                                           |
| 命令模式   | CONFIGURATION                                                                                 |
| 使用情况信息 | 强制实施支持 RPVST+ 的桥以在 STP 兼容模式下操作。                                                               |
| 示例     | <pre>OS10(config)# spanning-tree mst force-version</pre>                                      |
| 支持的版本  | 10.2.0E or later                                                                              |

## spanning-tree vlan hello-time

设置 RPVST BPDU 的生成和传输之间的时间间隔。

|        |                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>spanning-tree vlan <i>vlan-id</i> hello-time <i>seconds</i></code>                                                                         |
| 参数     | <ul style="list-style-type: none"><li><i>vlan-id</i> — 输入 VLAN ID 号, 从 1 到 4093。</li><li><i>seconds</i> — 输入问候时间间隔值 (以秒为单位), 从 1 到 10。</li></ul> |
| 默认     | 2 秒                                                                                                                                              |
| 命令模式   | CONFIGURATION                                                                                                                                    |
| 使用情况信息 | Dell EMC 建议增加针对大型配置 (特别是具有多个端口的配置) 的问候时间。                                                                                                        |
| 示例     | <pre>OS10(config)# spanning-tree vlan 10 hello-time 5</pre>                                                                                      |
| 支持的版本  | 10.2.0E or later                                                                                                                                 |

## spanning-tree vlan mac-flush-threshold

为指定 VLAN 配置 MAC-清洗阈值。

|        |                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>spanning-tree vlan <i>vlan-id</i> mac-flush-threshold <i>threshold-value</i></code>                                                                                               |
| 参数     | <ul style="list-style-type: none"><li><i>vlan-id</i> — 输入生成树 VLAN ID 号, 从 1 到 4093。</li><li><i>threshold-value</i> — 输入刷新次数的阈值, 从 0 到 65535。默认值为 5。</li></ul>                           |
| 默认     | 未配置                                                                                                                                                                                     |
| 命令模式   | CONFIGURATION                                                                                                                                                                           |
| 使用情况信息 | 阈值指示在开始刷新优化之前允许调用基于端口的刷新请求数。当刷新间隔值为非零时, 将触发基于端口和实例的刷新, 直至达到阈值为止。达到阈值后, MAC 刷新计时器即会启动。在计时器到期时, 系统会触发基于 VLAN 的刷新。当计时器正在运行时, 将抑制任何基于端口和 VLAN 的刷新。命令的 <code>no</code> 形式将特定实例的刷新指示阈值重置为默认值。 |
| 示例     | <pre>OS10(config)# spanning-tree vlan 100 mac-flush-threshold 255</pre>                                                                                                                 |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                    |

## spanning-tree vlan max-age

配置在通过重新计算 RPVST 刷新信息之前桥维护配置信息的时间段。

|        |                                                                       |
|--------|-----------------------------------------------------------------------|
| 语法     | <code>spanning-tree vlan <i>vlan-id</i> max-age <i>seconds</i></code> |
| 参数     | <code>max-age <i>seconds</i></code> — 输入最长期限值 (以秒为单位), 从 6 到 40。      |
| 默认     | 20 秒                                                                  |
| 命令模式   | CONFIGURATION                                                         |
| 使用情况信息 | 无                                                                     |
| 示例     | <pre>OS10(config)# spanning-tree vlan 10 max-age 10</pre>             |
| 支持的版本  | 10.2.0E or later                                                      |

## spanning-tree vlan priority

设置 RPVST+ 的优先级值。

|    |                                                                               |
|----|-------------------------------------------------------------------------------|
| 语法 | <code>spanning-tree vlan <i>vlan-id</i> priority <i>priority value</i></code> |
|----|-------------------------------------------------------------------------------|

|        |                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 参数     | <code>priority priority value</code> — 输入桥优先级值（以 4096 为增量），从 0 到 61440。有效的优先级值包括：0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344 和 61440。所有其他值都将被拒绝。 |
| 默认     | 未配置                                                                                                                                                                                      |
| 命令模式   | CONFIGURATION                                                                                                                                                                            |
| 使用情况信息 | RPVST+ 协议可确定根桥。为一个桥分配较低优先级，以提高其成为根桥的概率。 <code>priority value</code> 较低的值会增加该桥成为根桥的概率。                                                                                                    |
| 示例     | <pre>OS10(config)# spanning-tree vlan 10 priority 0</pre>                                                                                                                                |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                         |

## spanning-tree vlan priority (接口)

当两个桥争用根桥的位置时，设置接口优先级。

|        |                                                                        |
|--------|------------------------------------------------------------------------|
| 语法     | <code>spanning-tree vlan vlan-id priority value</code>                 |
| 参数     | <code>value</code> — 以 16 为增量输入优先级值，从 0 到 240。                         |
| 默认     | 128                                                                    |
| 命令模式   | INTERFACE                                                              |
| 使用情况信息 | 打破两个桥之间的绑定，这会争用根桥。                                                     |
| 示例     | <pre>OS10(config-if-eth1/1/4)# spanning-tree vlan 10 priority 16</pre> |
| 支持的版本  | 10.2.0E or later                                                       |

## spanning-tree vlan root

将设备指定为主或辅助根桥。

|        |                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>spanning-tree vlan vlan-id root {primary   secondary}</code>                                                                                                                                                                      |
| 参数     | <ul style="list-style-type: none"> <li><code>vlan-id</code> — 输入 VLAN ID 号，从 1 到 4093。</li> <li><code>root</code> — 将桥指定为主根或辅助根。</li> <li><code>primary</code> — 将桥指定为主桥或根桥。</li> <li><code>secondary</code> — 将桥指定为辅助或辅助根桥。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                     |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                           |
| 使用情况信息 | 无                                                                                                                                                                                                                                       |
| 示例     | <pre>OS10(config)# spanning-tree vlan 1 root primary</pre>                                                                                                                                                                              |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                        |

## 快速生成树协议

快速生成树协议 (RSTP) 与 STP 类似，但配置了 STP 和 MSTP 的设备可提供更快的融合和互操作性。默认情况下，RSTP 处于禁用状态。L2 模式下所有已启用的接口都会自动添加到 RSTP 拓扑。

配置 RSTP 流程包含两个步骤：

1. 确保接口处于 L2 模式。
2. 全局启用 RSTP。

**注：**只要某个端口成环指定的端口，就会在设备（环口 + 1/2 \* 环口）后点名延迟的设备；如果将环口置0秒，则在设备0秒延迟。如果3秒内未收到BPDU，端口将声明阻塞操作，并移至阻塞状态。

## 全局启用

RSTP 可在处于 L2 模式的所有物理和端口通道接口上启用 STP，以自动将接口包括在 RSTP 拓扑中。只有一个从一个桥到任何其他桥的路径已启用。桥通过禁用某个链路端口来阻止冗余路径。

- 在 CONFIGURATION 模式下将生成树模式配置为 RSTP。

```
spanning-tree mode rstp
```

- 在 CONFIGURATION 模式下禁用所有 L2 接口的全局 RSTP。

```
spanning-tree disable
```

- 在 INTERFACE 模式下从 RSTP 拓扑中移除接口。

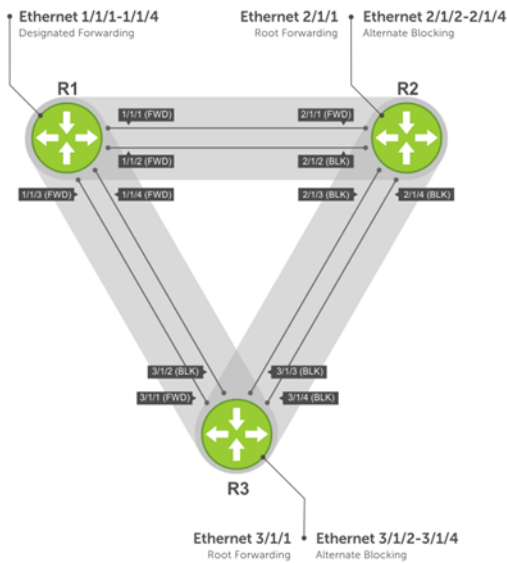
```
spanning-tree disable
```

- 在 INTERFACE 模式下重新启用接口。

```
no spanning-tree disable
```

- 在 CONFIGURATION 模式下为所有 L2 接口全局重新启用 RSTP。

```
no spanning-tree disable
```



## 查看参与 RSTP 的所有端口

```
OS10# show spanning-tree
Spanning tree enabled protocol rstp with force-version rstp
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 3417.4455.667f
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 90b1.1cf4.a523
Configured hello time 2, max age 20, forward delay 15
Interface
```

| Name            | PortID  | Prio | Cost      | Sts | Cost | Bridge ID | Designated     | PortID |
|-----------------|---------|------|-----------|-----|------|-----------|----------------|--------|
| ethernet1/1/1   | 128.260 | 128  | 200000000 | BLK | 0    | 0         | 0000.0000.0000 | 0.0    |
| ethernet1/1/2   | 128.264 | 128  | 200000000 | BLK | 0    | 0         | 0000.0000.0000 | 0.0    |
| ethernet1/1/3   | 128.268 | 128  | 200000000 | BLK | 0    | 0         | 0000.0000.0000 | 0.0    |
| ethernet1/1/4   | 128.272 | 128  | 200000000 | BLK | 0    | 0         | 0000.0000.0000 | 0.0    |
| ethernet1/1/5:1 | 128.276 | 128  | 200000000 | BLK | 0    | 0         | 0000.0000.0000 | 0.0    |
| ethernet1/1/5:2 | 128.277 | 128  | 200000000 | BLK | 0    | 0         | 0000.0000.0000 | 0.0    |

| ethernet1/1/5:3 | 128.278 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
|-----------------|---------|---------|-----------|-----------|-----|-------|----------------|---------|
| ethernet1/1/5:4 | 128.279 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/6:1 | 128.280 | 128     | 2000      | FWD       | 0   | 32768 | 3417.4455.667f | 128.150 |
| ethernet1/1/6:2 | 128.281 | 128     | 2000      | FWD       | 0   | 32768 | 3417.4455.667f | 128.151 |
| ethernet1/1/6:3 | 128.282 | 128     | 2000      | FWD       | 0   | 32768 | 3417.4455.667f | 128.152 |
| ethernet1/1/6:4 | 128.283 | 128     | 2000      | BLK       | 0   | 32768 | 3417.4455.667f | 128.153 |
| ethernet1/1/7   | 128.284 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/8   | 128.288 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/9   | 128.292 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/10  | 128.296 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/11  | 128.300 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/12  | 128.304 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/13  | 128.308 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/14  | 128.312 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/15  | 128.316 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/16  | 128.320 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/17  | 128.324 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/18  | 128.328 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/19  | 128.332 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/20  | 128.336 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/21  | 128.340 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/22  | 128.344 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/23  | 128.348 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/24  | 128.352 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/25  | 128.356 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/26  | 128.360 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/27  | 128.364 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/28  | 128.368 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/29  | 128.372 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/30  | 128.376 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/31  | 128.380 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| ethernet1/1/32  | 128.384 | 128     | 200000000 | BLK       | 0   | 0     | 0000.0000.0000 | 0.0     |
| Interface       |         |         |           |           |     |       |                |         |
| Name            | Role    | PortID  | Prio      | Cost      | Sts | Cost  | Link-type      | Edge    |
| -----           |         |         |           |           |     |       |                |         |
| ethernet1/1/1   | Disb    | 128.260 | 128       | 200000000 | BLK | 0     | AUTO           | No      |
| ethernet1/1/2   | Disb    | 128.264 | 128       | 200000000 | BLK | 0     | AUTO           | No      |
| ethernet1/1/3   | Disb    | 128.268 | 128       | 200000000 | BLK | 0     | AUTO           | No      |
| ethernet1/1/4   | Disb    | 128.272 | 128       | 200000000 | BLK | 0     | AUTO           | No      |
| ethernet1/1/5:1 | Disb    | 128.276 | 128       | 200000000 | BLK | 0     | AUTO           | No      |

## 全局参数

根桥将设置转发时间、问候时间和最长期限的值，并覆盖加入 RSTP 组的其他桥上设置的值。

**注：** Dell EMC 建议仅有经验的网络管理员更改 RSTP 组参数。对 RSTP 参数的不当规划修改可能会对网络性能造成负面影响。

- 转发时间

15 秒 — 在将接口转换为转发状态之前，其在侦听状态和学习状态下等待的时间量。
- 问候时间

2 秒 — 桥发送 RSTP BPDU 的时间间隔。
- 最大期限

20 秒 — 在通过重新计算 RSTP 拓扑来刷新信息之前桥保持配置信息的时间长度。
- 端口成本

要设置接口路径成本的端口成本值，请执行以下操作：
  - 100 Mb/s 以太网接口 — 200000
  - 1 Gb 以太网接口 — 20000
  - 10 Gb 以太网接口 — 2000
  - 40 Gb 以太网接口 — 500
  - 端口通道，带有 100 Mb/s 以太网接口 — 200000
  - 端口通道，带有 1 Gb 以太网接口 — 20000
  - 端口通道，带有 10 Gb 以太网接口 — 2000
  - 端口通道，带有 1x40 Gb 以太网接口 — 500
  - 端口通道，带有 2x40 Gb 以太网接口 — 250
- 在 CONFIGURATION 模式下将转发时间从 4 更改为 30，默认值为 15。

```
spanning-tree rstp forward-time seconds
```



- 在 CONFIGURATION 模式下更改问候时间，从 1 到 10，默认值为 2。对于大型配置，尤其是涉及更多数量的端口，Dell EMC 建议增加问候时间。

```
spanning-tree rstp hello-time seconds
```

- 在 CONFIGURATION 模式下更改问候时间，从 6 到 40，默认值为 20。

```
spanning-tree rstp max-age seconds
```

查看当前接口参数

```
OS10# show spanning-tree active

Spanning tree enabled protocol rstp with force-version rstp
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 90b1.1cf4.9b8a
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 90b1.1cf4.9b8a
We are the root
Configured hello time 2, max age 20, forward delay 15
Interface Designated
Name PortID Prio Cost Sts Cost Bridge ID PortID

ethernet1/1/1 244.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.244
ethernet1/1/2 248.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.248
ethernet1/1/3 252.128 128 500 FWD 0 32768 90b1.1cf4.9b8a 128.252
ethernet1/1/4 256.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.256
Interface
Name Role PortID Prio Cost Sts Cost Link-type Edge

ethernet1/1/1 Altr 128.244 128 500 BLK 0 AUTO No
ethernet1/1/2 Altr 128.248 128 500 BLK 0 AUTO No
ethernet1/1/3 Root 128.252 128 500 FWD 0 AUTO No
ethernet1/1/4 Altr 128.256 128 500 BLK 0 AUTO No
```

接口参数

在 L2 模式下设置接口的端口成本和端口优先级值。

- 端口成本** 基于接口类型的值。上表列出了默认值。端口成本越高，端口被选为转发端口的可能性就越小。
- 端口优先级** 在多个端口具有相同的端口成本的情况下，影响将端口选为转发端口的可能性。

- 在 INTERFACE 模式下将接口的端口成本从 1 更改为 200000000。

```
spanning-tree rstp cost cost
```

- 在 INTERFACE 模式下更改接口的端口优先级，从 0 到 240，默认值为 128。

```
spanning-tree rstp priority priority-value
```

查看当前全局参数值

```
OS10# show spanning-tree active

Spanning tree enabled protocol rstp with force-version rstp
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 90b1.1cf4.9b8a
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 90b1.1cf4.9b8a
We are the root
Configured hello time 2, max age 20, forward delay 15
Interface Designated
Name PortID Prio Cost Sts Cost Bridge ID PortID

ethernet1/1/1 244.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.244
ethernet1/1/2 248.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.248
ethernet1/1/3 252.128 128 500 FWD 0 32768 90b1.1cf4.9b8a 128.252
ethernet1/1/4 256.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.256
```

| Interface Name | Role | PortID  | Prio | Cost | Sts | Cost | Link-type | Edge |
|----------------|------|---------|------|------|-----|------|-----------|------|
| ethernet1/1/1  | Altr | 128.244 | 128  | 500  | BLK | 0    | AUTO      | No   |
| ethernet1/1/2  | Altr | 128.248 | 128  | 500  | BLK | 0    | AUTO      | No   |
| ethernet1/1/3  | Root | 128.252 | 128  | 500  | FWD | 0    | AUTO      | No   |
| ethernet1/1/4  | Altr | 128.256 | 128  | 500  | BLK | 0    | AUTO      | No   |

## 根桥选择

RSTP 将确定根桥。为一个桥分配较低优先级会增加选择其成为根桥的可能性。

- 分配一个数字作为桥优先级，或将其指定为 CONFIGURATION 模式下的主要或辅助根桥。配置优先级值范围，从 0 到 65535（4096 的倍数），默认值为 32768。分配的数字越小，桥成为根桥的可能性就越大。

```
spanning-tree rstp priority priority-value
```

### 查看桥优先级和根桥分配

```
OS10# show spanning-tree active
Spanning tree enabled protocol rstp with force-version rstp
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 3417.4455.667f
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 36864, Address 90b1.1cf4.a523
Configured hello time 2, max age 20, forward delay 15
```

| Interface Name  | PortID  | Prio | Cost | Sts | Cost | Bridge ID            | Designated PortID |
|-----------------|---------|------|------|-----|------|----------------------|-------------------|
| ethernet1/1/6:3 | 128.282 | 128  | 2000 | FWD | 0    | 32768 3417.4455.667f | 128.152           |
| ethernet1/1/6:4 | 128.283 | 128  | 2000 | BLK | 0    | 32768 3417.4455.667f | 128.153           |

```
Interface
Name Role PortID Prio Cost Sts Cost Link-type Edge

ethernet1/1/6:3 Root 128.282 128 2000 FWD 0 AUTO No
ethernet1/1/6:4 Altr 128.283 128 2000 BLK 0 AUTO No
```

## 为快速状态转移设置生成树链接类型

如 IEEE 802.1w 中的规定，OS10 假设以全双工模式运行的端口是点对点链路。点对点链路可更快地转换为转发状态。默认情况下，OS10 从双工模式派生端口的链路类型。您可以使用 `spanning-tree link-type` 命令来覆盖双工模式。

OS10 假定在半双工模式下运行的端口是共享链路，其快速转换功能不适用。此外，如果您将某个端口明确指定为共享链路，则不能使用快速转换功能，而不考虑双工设置。

要加快生成树的状态转换，您可以将链路类型设置为点对点。要将链路类型设置为点对点，请执行以下操作：

- 在 INTERFACE 模式下使用以下命令。

```
spanning-tree link-type point-to-point
```

## RSTP 命令

### show spanning-tree active

显示 RSTP 活动接口的 RSTP 配置和信息。

|      |                           |
|------|---------------------------|
| 语法   | show spanning-tree active |
| 参数   | 无                         |
| 默认   | 未配置                       |
| 命令模式 | EXEC                      |

使用情况信息

无

示例

```
OS10# show spanning-tree active

Spanning tree enabled protocol rstp with force-version rstp
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 90b1.1cf4.9b8a
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 90b1.1cf4.9b8a
We are the root
Configured hello time 2, max age 20, forward delay 15
Interface Designated
Name PortID Prio Cost Sts Cost Bridge ID PortID

ethernet1/1/1 244.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.244
ethernet1/1/2 248.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.248
ethernet1/1/3 252.128 128 500 FWD 0 32768 90b1.1cf4.9b8a 128.252
ethernet1/1/4 256.128 128 500 BLK 0 32768 90b1.1cf4.9b8a 128.256
Interface
Name Role PortID Prio Cost Sts Cost Link-type Edge

ethernet1/1/1 Altr 128.244 128 500 BLK 0 AUTO No
ethernet1/1/2 Altr 128.248 128 500 BLK 0 AUTO No
ethernet1/1/3 Root 128.252 128 500 FWD 0 AUTO No
ethernet1/1/4 Altr 128.256 128 500 BLK 0 AUTO No
```

支持的版本

10.2.0E or later

### spanning-tree mode

启用 STP 类型：RSTP、快速 PVST+ 或 MST。

语法

spanning-tree mode {rstp | mst | rapid-pvst}

参数

- rstp — 将 STP 模式设置为“RSTP”。
- mst — 将 STP 模式设置为 MST。
- rapid-pvst — 将 STP 模式设置为 RPVST+。

默认

RPVST+

命令模式

CONFIGURATION

使用情况信息

所有 STP 实例在之前的 STP 模式下都停止，并在新模式下重新启动。您还可以将更改为 RSTP/MST 模式。

示例 (RSTP)

```
OS10(config)# spanning-tree mode rstp
```

示例 (MST)

```
OS10(config)# spanning-tree mode mst
```

支持的版本

10.2.0E or later

### spanning-tree rstp force-version

配置生成树的强制版本以传输 BPDU。

语法

spanning-tree rstp force-version stp

参数

stp — 强制 RSTP 传输的 BPDU 的版本。

默认

未配置

命令模式

CONFIGURATION

使用情况信息

强制支持 RSTP 或 MST 的桥以使用 STP 兼容的方式操作，以避免框架在敏感的已知 LAN 协议中进行错误排序和复制。

## 示例

```
OS10(config)# spanning-tree rstp force-version stp
```

## 支持的版本

10.2.0E or later

## spanning-tree rstp forward-time

在移动到转发状态之前，为接口配置时间间隔以在阻止状态或学习状态等待。

## 语法

```
spanning-tree rstp forward-time seconds
```

## 参数

*seconds* — 输入在移动到转发状态之前，接口在阻止状态或学习状态下等待的秒数（4 至 30）。

## 默认

15 秒

## 命令模式

CONFIGURATION

## 使用情况信息

无

## 示例

```
OS10(config)# spanning-tree rstp forward-time 16
```

## 支持的版本

10.2.0E or later

## spanning-tree rstp hello-time

设置 RSTP BPDU 的生成和传输之间的时间间隔。

## 语法

```
spanning-tree rstp hello-time seconds
```

## 参数

*seconds* — 输入问候时间间隔值（以秒为单位），从 1 到 10。

## 默认

2 秒

## 命令模式

CONFIGURATION

## 使用情况信息

Dell EMC 建议增加针对大型配置（特别是具有多个端口的配置）的问候时间。

## 示例

```
OS10(config)# spanning-tree rstp hello-time 5
```

## 支持的版本

10.2.0E or later

## spanning-tree rstp mac-flush-threshold

设置 RSTP 实例上的刷新指示阈值。

## 语法

```
spanning-tree rstp mac-flush-threshold threshold-value
```

## 参数

*threshold-value* — 输入刷新次数的阈值，从 0 到 65535。默认值是 65535。

## 默认

未配置

## 命令模式

CONFIGURATION

## 使用情况信息

阈值指示在触发刷新间隔计时器之前要执行的刷新指示的数量。当刷新指示阈值设置为默认值并且刷新间隔设置为非默认值时，在第一次刷新指示触发器期间将发生刷新。当刷新指示阈值为非默认值 (n) 且刷新间隔值为非默认值时，将触发基于端口的刷新，直至达到阈值 (n)。达到阈值后，MAC 刷新计时器即会启动。在计时器到期时，系统会触发基于实例的清洗。当计时器正在运行时，将抑制所有基于端口和实例的刷新。命令的 `no` 形式会将刷新指示阈值设置为默认值。

## 示例

```
OS10(config)# spanning-tree rstp mac-flush-threshold 255
```

## 支持的版本

10.4.0E(R1) or later

## spanning-tree rstp max-age

配置在通过重新计算 RSTP 拓扑刷新信息之前桥维护配置信息的时间段。

|        |                                                        |
|--------|--------------------------------------------------------|
| 语法     | <code>max-age seconds</code>                           |
| 参数     | <code>seconds</code> — 输入最长期限值（以秒为单位），从 6 到 40。        |
| 默认     | 20 秒                                                   |
| 命令模式   | CONFIGURATION                                          |
| 使用情况信息 | 无                                                      |
| 示例     | <pre>OS10(config)# spanning-tree rstp max-age 10</pre> |

支持的版本 10.2.0E or later

## spanning-tree rstp priority

设置 RSTP 的优先级值。

|        |                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>spanning-tree rspt priority priority value</code>                                                                                                                                  |
| 参数     | <code>priority priority value</code> — 输入桥优先级值（以 4096 为增量），从 0 到 61440。有效的优先级值包括：0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344 和 61440。所有其他值都将被拒绝。 |
| 默认     | 未配置                                                                                                                                                                                      |
| 命令模式   | CONFIGURATION                                                                                                                                                                            |
| 使用情况信息 | RSTP 将确定根桥，但您可以为一个桥分配较低优先级，以提高其成为根桥的可能性。 <code>priority value</code> 较低的值会增加该桥成为根桥的概率。                                                                                                   |
| 示例     | <pre>OS10(config)# spanning-tree rstp priority 5002</pre>                                                                                                                                |

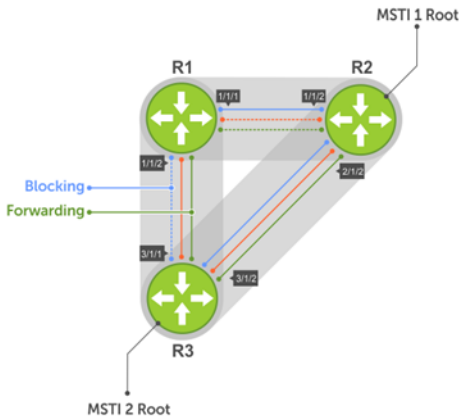
支持的版本 10.2.0E or later

## 多个生成树

MSTP 是快速生成树协议的一种变化，可减少 RPVST+ 的一些难题。RPVST+ 允许适用于每个 VLAN 的生成树实例。如果您有多个 VLAN，则此 1:1 方法不适合 — 每个生成树实例都会占用带宽和处理资源。您可以配置多个生成树实例 (MSTI)，并将多个 VLAN 映射到一个生成树实例以减少实例总数。有关 RPVST+ 的详细信息，请参阅 [RPVST+](#)。

启用 MST 时，第 2 层 (L2) 模式中的所有端口都参与 MST。OS10 仅支持一个 MST 区域。

您可以使用 MST 协议 (MSTP) 实现负载均衡。例如，如下图所示，当您将三个 VLAN 映射到两个生成树实例 (MSTI) 时，VLAN 100 流量采用与 VLAN 200 和 300 流量不同的路径。



配置 MST 流程包含四个步骤：

1. 如果当前运行的生成树协议 (STP) 版本并非 MST，请启用 MST。
2. (可选) 将 VLAN 映射到不同的实例，以使流量的负载均衡良好，并且链路利用率很高。
3. 确保在运行 MST 的所有桥中配置相同的地区名称。
4. (可选) 配置版本号。所有桥上的版本号都相同。

## 配置 MSTP

在全局启用 MST 时，所有交换机端口、端口通道和 VLAN 接口都会自动分配给 MSTI 零 (0)。在 MSTI 中，仅为转发启用了一条路径。

- 在 CONFIGURATION 模式下启用 MST。

```
spanning-tree mode mst
```

### 配置和验证 MSTP

```
OS10(config)# spanning-tree mode mst
OS10(config)# do show spanning-tree
show spanning-tree mst configuration
Region Name: abc
Revision: 0
MSTI VID
0 1,7-4093
1 2
2 3
3 4
4 5
5 6
```

## 添加或移除接口

默认情况下，在 L2 交换机端口模式下启用所有接口，并且所有 L2 接口都是生成树的一部分。

- 在 INTERFACE 模式下禁用接口上的生成树。

```
spanning-tree disable
```

- 在 INTERFACE 模式下启用接口上的 MST。

```
no spanning-tree disable
```

## 创建实例

您可以创建多个 MSTP 实例并映射 VLAN。要充分利用 MSTP，请创建多个 MSTI 并将 VLAN 映射到它们。

1. 在 CONFIGURATION 模式下输入实例编号。

```
spanning tree mst configuration
```

2. 在 MULTIPLE-SPANNING-TREE 模式下输入 MST 实例编号，从 0 到 63。对于 Mt.Echo 平台，MULTIPLE-SPANNING-TREE 模式为 0 到 61。

 **注：** Mt. Echo 平台总共支持 64 个实例，其中 1 个为 VLT 控制 VLAN，1 个用于 L3 VLAN，1 个用于默认的 STP 实例。运行快速 pvst 风格时，将为每个 VLAN 分配一个实例，直至 VLAN 数达到 61。61 之后的 VLAN 映射到默认实例。

```
instance instance-number
```

3. 输入要在 MULTIPLE-SPANNING-TREE 模式下参与 MST 实例的 VLAN 和 ID，从 1 到 4096。

```
instance vlan-id
```

## 创建 MST 实例

```
OS10(config)# spanning-tree mst configuration
OS10(conf-mst)# name Dell
OS10(conf-mst)# revision 100
OS10(conf-mst)# instance 1 vlan 2-10
OS10(conf-mst)# instance 2 vlan 11-20
OS10(conf-mst)# instance 3 vlan 21-30
```

## 查看 VLAN 实例映射

```
OS10# show spanning-tree mst configuration
Region Name: Dell
Revision: 100
MSTI VID
0 1,31-4093
1 2-10
2 11-20
3 21-30
```

## 查看端口转发/丢弃状态

```
OS10# show spanning-tree msti 0 brief
Spanning tree enabled protocol msti with force-version mst
MSTI 0 VLANs mapped 1,31-4093
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 3417.4455.667f
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID Priority 32768, Address 90b1.1cf4.a523
Configured hello time 2, max age 20, forward delay 15, max hops 20
CIST regional root ID Priority 32768, Address 90b1.1cf4.a523
CIST external path cost 500
```

| Interface Name | PortID  | Prio | Cost       | Sts | Cost | Designated Bridge ID | PortID  |
|----------------|---------|------|------------|-----|------|----------------------|---------|
| ethernet1/1/1  | 128.260 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.260 |
| ethernet1/1/2  | 128.264 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.264 |
| ethernet1/1/3  | 128.268 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.268 |
| ethernet1/1/4  | 128.272 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.272 |
| ethernet1/1/5  | 128.276 | 128  | 500        | FWD | 0    | 32768 3417.4455.667f | 128.146 |
| ethernet1/1/6  | 128.280 | 128  | 500        | BLK | 0    | 32768 3417.4455.667f | 128.150 |
| ethernet1/1/7  | 128.284 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.284 |
| ethernet1/1/8  | 128.288 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.288 |
| ethernet1/1/9  | 128.292 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.292 |
| ethernet1/1/10 | 128.296 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.296 |
| ethernet1/1/11 | 128.300 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.300 |
| ethernet1/1/12 | 128.304 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.304 |
| ethernet1/1/13 | 128.308 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.308 |
| ethernet1/1/14 | 128.312 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.312 |
| ethernet1/1/15 | 128.316 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.316 |
| ethernet1/1/16 | 128.320 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.320 |
| ethernet1/1/17 | 128.324 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.324 |
| ethernet1/1/18 | 128.328 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.328 |
| ethernet1/1/19 | 128.332 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.332 |
| ethernet1/1/20 | 128.336 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.336 |
| ethernet1/1/21 | 128.340 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.340 |
| ethernet1/1/22 | 128.344 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.344 |
| ethernet1/1/23 | 128.348 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.348 |
| ethernet1/1/24 | 128.352 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.352 |
| ethernet1/1/25 | 128.356 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.356 |
| ethernet1/1/26 | 128.360 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.360 |
| ethernet1/1/27 | 128.364 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.364 |
| ethernet1/1/28 | 128.368 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.368 |
| ethernet1/1/29 | 128.372 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.372 |
| ethernet1/1/30 | 128.376 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.376 |
| ethernet1/1/31 | 128.380 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.380 |
| ethernet1/1/32 | 128.384 | 128  | 2000000000 | BLK | 0    | 32768 90b1.1cf4.a523 | 128.384 |

```
Interface
Name Role PortID Prio Cost Sts Cost Link-type Edge

ethernet1/1/1 Disb 128.260 128 2000000000 BLK 0 AUTO No
ethernet1/1/2 Disb 128.264 128 2000000000 BLK 0 AUTO No
```

|                |      |         |     |           |     |   |      |    |
|----------------|------|---------|-----|-----------|-----|---|------|----|
| ethernet1/1/3  | Disb | 128.268 | 128 | 200000000 | BLK | 0 | AUTO | No |
| ethernet1/1/4  | Disb | 128.272 | 128 | 200000000 | BLK | 0 | AUTO | No |
| ethernet1/1/5  | Root | 128.276 | 128 | 500       | FWD | 0 | AUTO | No |
| ethernet1/1/6  | Altr | 128.280 | 128 | 500       | BLK | 0 | AUTO | No |
| ethernet1/1/7  | Disb | 128.284 | 128 | 200000000 | BLK | 0 | AUTO | No |
| ethernet1/1/8  | Disb | 128.288 | 128 | 200000000 | BLK | 0 | AUTO | No |
| ethernet1/1/9  | Disb | 128.292 | 128 | 200000000 | BLK | 0 | AUTO | No |
| ethernet1/1/10 | Disb | 128.296 | 128 | 200000000 | BLK |   |      |    |

## 根选择

MSTP 根据最小桥 ID 确定根桥。要增加桥被选为根桥的可能性，请为该桥分配较低的桥优先级数值。

您可以设置优先级值 0 以强制交换机成为根交换机。值 0 为最高优先级。

- 在 CONFIGURATION 模式下为特定实例分配桥优先级编号，从 0 到 61440，增量为 4096，默认值为 32768。

```
spanning-tree mst instance-number priority priority
```

### 分配根桥优先级

```
OS10(config)# spanning-tree mst 0 priority 32768
```

### 验证根桥优先级

```

OS10# show spanning-tree active
Spanning tree enabled protocol msti with force-version mst
MSTI 0 VLANs mapped 1,31-4093
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 3417.4455.667f
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID Priority 32768, Address 90b1.1cf4.a523
Configured hello time 2, max age 20, forward delay 15, max hops 20
CIST regional root ID Priority 32768, Address 90b1.1cf4.a523
CIST external path cost 500
Interface
Name PortID Prio Cost Sts Cost Bridge ID PortID

ethernet1/1/5 128.276 128 500 FWD 0 32768 3417.4455.667f 128.146
ethernet1/1/6 128.280 128 500 BLK 0 32768 3417.4455.667f 128.150
Interface
Name Role PortID Prio Cost Sts Cost Link-type Edge

ethernet1/1/5 Root 128.276 128 500 FWD 0 AUTO No
ethernet1/1/6 Altr 128.280 128 500 BLK 0 AUTO No

```

## 非 Dell EMC 硬件

OS10 仅支持一个 MST 区域。要使桥位于另一个桥的相同 MST 区域中，以下属性必须与唯一名称、版本和 VLAN 映射匹配。名称和版本号的默认值与所有 Dell EMC 硬件匹配。如果您使用的是非 Dell EMC 硬件，请确保这些值在所有设备上匹配。

区域是三个唯一属性的组合：

- 名称 — 分配给区域的助记字符串。默认值是系统 MAC 地址。
- 版本 — 一个 2 字节数字。默认值为 0。
- VLAN 到实例映射 — 在 MSTI 中放置 VLAN。

## 区域名称或版本

您可以更改 MSTP 区域名称或版本。

- 在 MULTIPLE-SPANNING-TREE 模式下更改区域名称。最多 32 个字符。

```
name name
```



- 在 MULTIPLE-SPANNING-TREE 模式下更改区域版本号，范围为 0 到 65535，默认值为 0。

```
revision number
```

配置和验证区域名称

```
OS10(config-mstp)# name my-mstp-region
OS10(config-mstp)# do show spanning-tree mst config
MST region name: my-mstp-region
Revision: 0
MSTI VID
 1 100
 2 200-300
```

修改参数

根桥可设置转发延迟、问候时间、最长期限和最大跳的值，并覆盖在其他 MST 桥上设置的值。

- 转发时间** 在将某个接口转换为转发状态之前其处于正在丢弃状态和正在学习状态的等待时间。
- 问候时间** 桥发送 MST BPDU 的时间间隔。
- 最长期限** 在桥通过重新计算 MST 拓扑来刷新信息之前保持配置信息的时间长度。
- 最大跳数** 在接收设备丢弃 BPDU 之前传输的最大跳数。

 **注:** Dell EMC 建议仅有经验的网络管理员更改 MST 参数。MST 参数计划编制不当可能会对网络性能造成负面影响。

- 在 CONFIGURATION 模式下将转发时间参数从 4 更改为 30，默认值为 15。

```
spanning-tree mst forward-time seconds
```

- 在 CONFIGURATION 模式下更改最长期限参数，从 1 到 10，默认值为 2。Dell EMC 建议增加针对大型配置（特别是具有更多端口的配置）的问候时间。

```
spanning-tree mst hello-time seconds
```

- 在 CONFIGURATION 模式下更改问候时间参数，从 6 到 40，默认值为 20。

```
spanning-tree mst max-age seconds
```

- 在 CONFIGURATION 模式下更改最大跳参数，从 1 到 40，默认值为 20。

```
spanning-tree mst max-hops number
```

MST 配置

```
OS10(config)# spanning-tree mst
OS10(config)# spanning-tree mst forward-time 16
OS10(config)# spanning-tree mst hello-time 5
OS10(config)# spanning-tree mst max-age 10
OS10(config)# spanning-tree mst max-hops 30
```

查看 MSTP 参数值

```
OS10# show spanning-tree active
Spanning tree enabled protocol msti with force-version mst
MSTI 0 VLANs mapped 1,31-4093
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 3417.4455.667f
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID Priority 32768, Address 90b1.1cf4.a523
Configured hello time 10, max age 40, forward delay 30, max hops 40
CIST regional root ID Priority 32768, Address 90b1.1cf4.a523
CIST external path cost 500
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated


```

|               |         |         |      |      |     |       |                |         |
|---------------|---------|---------|------|------|-----|-------|----------------|---------|
| ethernet1/1/5 | 128.276 | 128     | 500  | FWD  | 0   | 32768 | 3417.4455.667f | 128.146 |
| ethernet1/1/6 | 128.280 | 128     | 500  | BLK  | 0   | 32768 | 3417.4455.667f | 128.150 |
| Interface     |         |         |      |      |     |       |                |         |
| Name          | Role    | PortID  | Prio | Cost | Sts | Cost  | Link-type      | Edge    |
| -----         |         |         |      |      |     |       |                |         |
| ethernet1/1/5 | Root    | 128.276 | 128  | 500  | FWD | 0     | AUTO           | No      |
| ethernet1/1/6 | Altr    | 128.280 | 128  | 500  | BLK | 0     | AUTO           | No      |

## 接口参数

调整两个接口参数，以提高或降低端口成为转发端口的可能性。

- 端口成本**
接口类型值。端口成本越高，端口为转发端口的可能性就越小。
- 端口优先级**
在多个端口具有相同的端口成本的情况下，影响将端口选为转发端口的可能性。

按接口的端口成本默认值：

- 100 Mb/s 以太网接口 — 200000
  - 1 Gb 以太网接口 — 20000
  - 10 Gb 以太网接口 — 2000
  - 端口通道，带有 100 Mb/s 以太网接口 — 180000
  - 端口通道，带有 1 Gb 以太网接口 — 18000
  - 端口通道，带有 10 Gb 以太网接口 — 1800
1. 在 INTERFACE 模式下将接口的端口成本从 1 更改为 200000000。

```
spanning-tree msti number cost 1
```

2. 在 INTERFACE 模式下将接口的端口成本从 0 更改为 240，以 16 为增量，默认值为 128。

```
spanning-tree msti number priority 32
```

### 查看 MSTi 接口配置

```

OS10(conf-if-eth1/1/7)# do show spanning-tree msti 0 interface ethernet 1/1/7
ethernet1/1/7 of MSTI 0 is Designated Forwarding
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: Yes, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 69, Received: 0

```

|               |        |      |      |     |      |            |                |        |  |
|---------------|--------|------|------|-----|------|------------|----------------|--------|--|
| Interface     |        |      |      |     |      | Designated |                |        |  |
| Name          | PortID | Prio | Cost | Sts | Cost | Bridge ID  |                | PortID |  |
| -----         |        |      |      |     |      |            |                |        |  |
| ethernet1/1/7 | 0.284  | 0    | 1    | FWD | 0    | 32768      | 90b1.1cf4.9b8a | 0.284  |  |

## MST 命令

### instance

配置 MST 实例和一个或多个映射到 MST 实例的 VLAN。

- 语法**

```
instance instance-number {vlan vlan-range}
```
- 参数**
  - *instance* — 输入 MST 实例值，从 0 到 63。对于 Mt.Echo 平台，请输入一个从 0 到 61 的 MST 实例值。
  - *vlan range* — 输入 VLAN 范围值，从 1 到 4093。
- 默认**
未配置
- 命令模式**
MULTIPLE-SPANNING-TREE
- 使用情况信息**
默认情况下，所有 VLAN 映射到 MST 实例零 (0)，除非您使用 *vlan range* 命令将 VLAN 映射到非零实例。此命令的 *no* 版本将移除与实例相关的配置。

## 示例

```
OS10(conf-mst)# instance 1 vlan 2-10
OS10(conf-mst)# instance 2 vlan 11-20
OS10(conf-mst)# instance 3 vlan 21-30
```

## 支持的版本

10.2.0E or later

## name

为 MST 区域分配名称。

### 语法

name **region-name**

### 参数

**region-name** — 输入 MST 区域的名称。最多 32 个字符。

### 默认

系统 MAC 地址

### 命令模式

MULTIPLE-SPANNING-TREE

### 使用情况信息

默认情况下，MST 协议将系统 MAC 地址分配为区域名称。同一区域内的两个 MST 设备必须共享相同的地区名称，包括匹配大小写。

## 示例

```
OS10(conf-mst)# name my-mst-region
```

## 支持的版本

10.2.0E or later

## revision

配置 MSTP 配置的版本号。

### 语法

revision *number*

### 参数

*number* — 输入 MSTP 配置的版本号，从 0 到 65535。

### 默认

0

### 命令模式

MULTIPLE-SPANNING-TREE

### 使用情况信息

要使相同 MST 区域中的一个桥与另一个桥保持一致，必须在所有 Dell EMC 硬件设备上匹配版本号的默认值。如果存在非 Dell EMC 设备，请确保所有设备上的版本号值匹配。有关详细信息，请参阅[非戴尔硬件](#)。

## 示例

```
OS10(conf-mst)# revision 10
```

## 支持的版本

10.2.0E or later

## spanning-tree mst

配置 MST 实例并确定根和桥优先级。

### 语法

spanning-tree mst *instance number* priority | root {primary | secondary}

### 参数

- *instance number* — 输入 MST 实例号（从 0 至 63）。对于 Mt.Echo 平台，请输入一个从 0 到 61 的 MST 实例值。
- *priority priority value* — 设置桥优先级值，增量为 4096，从 0 至 61440。有效的优先级值包括：0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344 和 61440。所有其他值都将被拒绝。
- *root* — 输入主要或次要根。
- *primary* — 将设备输入为主根目录。
- *secondary* — 将设备输入为次要根。

### 默认

未配置

### 命令模式

CONFIGURATION

|               |                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------|
| <b>使用情况信息</b> | MSTP 将确定根桥，但您可以为一个桥分配较低优先级，以提高其成为根桥的可能性。 <i>priority-value</i> 较低的值会增加该桥成为根桥的概率。此命令的 <code>no</code> 版本会将该值重置为默认值。 |
| <b>示例</b>     | <pre> OS10(config)# spanning-tree mst 0 priority 0 OS10(config)# spanning-tree mst 2 root primary </pre>           |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                   |

## spanning-tree msti

配置接口的 MSTI、成本和优先级值。

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>spanning-tree msti instance {cost cost   priority value}</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>msti instance</code> — 输入 MST 实例号，从 0 到 63。对于 Mt.Echo 平台，请输入一个从 0 到 61 的 MST 实例值。</li> <li><code>cost cost</code> — (可选) 输入端口成本值 (从 1 到 200000000)。默认值： <ul style="list-style-type: none"> <li>100 Mb/s 以太网接口 = 200000</li> <li>1 Gb 以太网接口 = 20000</li> <li>10 Gb 以太网接口 = 2000</li> <li>带有一个 100 Mb/s 以太网的端口通道接口 = 200000</li> <li>带有一个 1 Gb 以太网的端口通道接口 = 20000</li> <li>带有一个 10 Gb 以太网的端口通道接口 = 2000</li> <li>带有两个 1 Gb 以太网的端口通道 = 18000</li> <li>带有两个 10 Gb 以太网的端口通道 = 1800</li> <li>带有两个 100 Mbps 以太网端口通道 = 180000</li> </ul> </li> <li><code>priority value</code> — 以 16 为增量输入一个值，其优先级为 0 到 240，默认值为 128。</li> </ul> |
| <b>默认</b>     | 优先级值为 128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>命令模式</b>   | INTERFACE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>使用情况信息</b> | 此 <code>cost</code> 值基于接口类型。 <code>cost</code> 值越大，选择端口来转发端口的可能越小。如果多个端口具有相同的成本值，则 <code>priority</code> 会影响将端口选为转发端口的可能性。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>示例</b>     | <pre> OS10(config-if-eth1/1/1)# spanning-tree msti 1 priority 0 OS10(config-if-eth1/1/1)# spanning-tree msti 1 cost 3 </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## spanning-tree mst configuration

进入 MST 模式以从配置模式配置 MSTP。

|               |                                                                              |
|---------------|------------------------------------------------------------------------------|
| <b>语法</b>     | <code>spanning-tree mst configuration</code>                                 |
| <b>参数</b>     | 无                                                                            |
| <b>默认</b>     | 已禁用                                                                          |
| <b>命令模式</b>   | CONFIGURATION                                                                |
| <b>使用情况信息</b> | 使用此命令可进入 STP MST 配置模式。                                                       |
| <b>示例</b>     | <pre> OS10(config)# spanning-tree mst configuration OS10(config-mst)# </pre> |
| <b>支持的版本</b>  | 10.2.0E or later                                                             |

## spanning-tree mst disable

禁用指定 MST 实例上的生成树。

|        |                                                                                 |
|--------|---------------------------------------------------------------------------------|
| 语法     | <code>spanning-tree mst instance-number disable</code>                          |
| 参数     | <i>instance-number</i> — 输入实例编号，从 0 到 63。对于 Mt.Echo 平台，请输入一个从 0 到 61 的 MST 实例值。 |
| 默认     | 已启用                                                                             |
| 命令模式   | CONFIGURATION                                                                   |
| 使用情况信息 | 此命令的 <code>no</code> 版本将在指定的 MST 实例上启用生成树。                                      |
| 示例     | <pre>OS10(config)# spanning-tree mst 10 disable</pre>                           |
| 支持的版本  | 10.4.0E(R1) or later                                                            |

## spanning-tree mst force-version

配置 STP 的强制版本以传输 BPDU。

|        |                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>spanning-tree mst force-version {stp   rstp}</code>                                                                                             |
| 参数     | <ul style="list-style-type: none"><li><code>stp</code> — 强制将 MST 传输的 BPDU 版本变为 STP。</li><li><code>rstp</code> — 强制将 MST 传输的 BPDU 版本变为 RSTP。</li></ul> |
| 默认     | 未配置                                                                                                                                                   |
| 命令模式   | CONFIGURATION                                                                                                                                         |
| 使用情况信息 | 强制实施支持 MST 的桥以在 STP 兼容模式下操作。                                                                                                                          |
| 示例     | <pre>OS10(config)# spanning-tree mst force-version</pre>                                                                                              |
| 支持的版本  | 10.2.0E or later                                                                                                                                      |

## spanning-tree mst forward-time

在移动到转发状态之前，为接口配置时间间隔以在阻止状态或学习状态等待。

|        |                                                            |
|--------|------------------------------------------------------------|
| 语法     | <code>spanning-tree mst forward-time seconds</code>        |
| 参数     | <i>seconds</i> — 输入在移动到转发状态之前，接口在阻止状态或学习状态下等待的秒数（4 至 30）。  |
| 默认     | 15 秒                                                       |
| 命令模式   | CONFIGURATION                                              |
| 使用情况信息 | 此命令的 <code>no</code> 版本会将该值重置为默认值。                         |
| 示例     | <pre>OS10(config)# spanning-tree mst forward-time 16</pre> |
| 支持的版本  | 10.2.0E or later                                           |

## spanning-tree mst hello-time

设置 MSTP BPDU 的生成和传输之间的时间间隔。

|    |                                                   |
|----|---------------------------------------------------|
| 语法 | <code>spanning-tree mst hello-time seconds</code> |
| 参数 | <i>seconds</i> — 输入问候时间间隔值（以秒为单位），从 1 到 10。       |
| 默认 | 2 秒                                               |

|        |                                                                           |
|--------|---------------------------------------------------------------------------|
| 命令模式   | CONFIGURATION                                                             |
| 使用情况信息 | Dell EMC 建议增加针对大型配置（特别是具有多个端口的配置）的问候时间。此命令的 <code>no</code> 版本会将该值重置为默认值。 |
| 示例     | <pre>OS10(config)# spanning-tree mst hello-time 5</pre>                   |
| 支持的版本  | 10.2.0E or later                                                          |

## spanning-tree mst mac-flush-threshold

配置特定实例的 mac 刷新阈值。

|        |                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>spanning-tree mst instance-number mac-flush-threshold threshold-value</code>                                                                                           |
| 参数     | <ul style="list-style-type: none"> <li><code>instance-number</code>— 输入实例编号，从 0 到 4094。</li> <li><code>threshold-value</code>— 输入刷新次数的阈值，从 0 到 65535。默认值为 5。</li> </ul>      |
| 默认     | 未配置                                                                                                                                                                          |
| 命令模式   | CONFIGURATION                                                                                                                                                                |
| 使用情况信息 | 此阈值指示在开始刷新优化之前允许调用的基于端口的刷新请求数。当刷新间隔值为非零时，将触发基于端口和实例的刷新，直至达到阈值为止。达到阈值后，MAC 刷新计时器即会启动。在计时器到期时，系统会触发基于实例的清洗。当计时器正在运行时，将抑制所有基于端口和实例的刷新。命令的 <code>no</code> 形式将特定实例的刷新指示阈值设置为默认值。 |
| 示例     | <pre>OS10(config)# spanning-tree mst 10 mac-flush-threshold 255</pre>                                                                                                        |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                         |

## spanning-tree mst max-age

配置在通过重新计算 MST 拓扑刷新信息之前桥维护配置信息的时间段。

|        |                                                       |
|--------|-------------------------------------------------------|
| 语法     | <code>max-age seconds</code>                          |
| 参数     | <code>seconds</code> — 输入最长期限值（以秒为单位），从 6 到 40。       |
| 默认     | 20 秒                                                  |
| 命令模式   | CONFIGURATION                                         |
| 使用情况信息 | 此命令的 <code>no</code> 版本会将该值重置为默认值。                    |
| 示例     | <pre>OS10(config)# spanning-tree mst max-age 10</pre> |
| 支持的版本  | 10.2.0E or later                                      |

## spanning-tree mst max-hops

将 BPDU 的最大跳数配置为在被丢弃之前传输。

|        |                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>spanning-tree mst max-hops number</code>                                                                                                                                  |
| 参数     | <code>number</code> — 输入从 6 到 40 的最大跳值。                                                                                                                                         |
| 默认     | 20                                                                                                                                                                              |
| 命令模式   | CONFIGURATION                                                                                                                                                                   |
| 使用情况信息 | 接收 BPDU 的设备将等待，直到 <code>max-hops</code> 值到期，然后才丢弃该设备。当设备收到 BPDU 时，它将递减剩余跳的接收值，并使用结果值作为 BPDU 中的剩余跳。如果剩余的 MSTP 1333 跳达到零，设备将丢弃 BPDU 并使其拥有的端口信息过期。命令配置适用于 MST 区域中的所有通用 IST (CIST)。 |

|       |                                             |
|-------|---------------------------------------------|
| 示例    | OS10(config)# spanning-tree mst max-hops 30 |
| 支持的版本 | 10.2.0E or later                            |

show spanning-tree mst

显示 MST 配置信息。

|        |                                      |
|--------|--------------------------------------|
| 语法     | show spanning-tree mst configuration |
| 参数     | 无                                    |
| 默认     | 未配置                                  |
| 命令模式   | EXEC                                 |
| 使用情况信息 | 请先启用 MSTI，然后再使用此命令。                  |
| 示例     |                                      |

```
OS10# show spanning-tree mst configuration
Region Name: asia
Revision: 0
MSTI VID
0 1,7-4093
1 2
2 3
3 4
4 5
5 6
```

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|

show spanning-tree msti

显示 MST 实例信息。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show spanning-tree msti [ <i>instance-number</i> [ <i>brief</i>   <i>guard</i>   <i>virtual-interface</i>   <i>interface interface</i> ]]                                                                                                                                                                                                                                                                                                                                                                                                    |
| 参数     | <ul style="list-style-type: none"> <li><i>instance-number</i> — (可选) 显示 MST 实例信息，从 0 到 63。对于 Mt.Echo 平台，请输入一个从 0 到 61 的 MST 实例值。</li> <li><i>brief</i> — (可选) 显示 MST 实例摘要信息。</li> <li><i>guard</i> — (可选) 显示已启用的防护和当前的端口状态。</li> <li><i>virtual-interface</i> — (可选) 显示特定于 VLT 的 MST 信息。</li> <li><i>interface interface</i>— (可选) 显示接口类型信息：               <ul style="list-style-type: none"> <li><i>ethernet node/slot/port[:subport]</i> — 输入以太网端口信息，从 1 到 48。</li> <li><i>port-channel</i> — 输入端口通道接口信息，从 1 到 128。</li> </ul> </li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | 查看特定 MST 实例编号的 MST 实例信息、详细信息或简要，或查看物理以太网端口或端口通道信息。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 示例（简要） |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

```
OS10# show spanning-tree msti 0 brief
Spanning tree enabled protocol msti with force-version mst
MSTI 0 VLANs mapped 1-99,101-199,301-4093
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 90b1.1cf4.9b8a
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID Priority 32768, Address 90b1.1cf4.9b8a
We are the root of MSTI 0
Configured hello time 2, max age 20, forward delay 15, max hops 20
Interface Designated
Name PortID Prio Cost Sts Cost Bridge ID PortID


```

```

ethernet1/1/1 132.128 128 2000000000 BLK 0 32768 90b1.1cf4.9b8a 128.132
ethernet1/1/2 136.128 128 2000000000 BLK 0 32768 90b1.1cf4.9b8a 128.136
ethernet1/1/3 140.128 128 2000000000 BLK 0 32768 90b1.1cf4.9b8a 128.140
ethernet1/1/4 144.128 128 2000000000 BLK 0 32768 90b1.1cf4.9b8a 128.144
ethernet1/1/5 148.128 128 2000000000 BLK 0 32768 90b1.1cf4.9b8a 128.148
ethernet1/1/6 152.128 128 2000000000 BLK 0 32768 90b1.1cf4.9b8a 128.152
ethernet1/1/7 156.128 128 2000000000 BLK 0 32768 90b1.1cf4.9b8a 128.156
...
Interface
Name Role PortID Prio Cost Sts Cost Link-type Edge

ethernet1/1/1 Disb 128.132 128 2000000000 BLK 0 SHARED No
ethernet1/1/2 Disb 128.136 128 2000000000 BLK 0 SHARED No
ethernet1/1/3 Disb 128.140 128 2000000000 BLK 0 SHARED No
ethernet1/1/4 Disb 128.144 128 2000000000 BLK 0 SHARED No
ethernet1/1/5 Disb 128.148 128 2000000000 BLK 0 SHARED No
ethernet1/1/6 Disb 128.152 128 2000000000 BLK 0 SHARED No
ethernet1/1/7 Disb 128.156 128 2000000000 BLK 0 SHARED No
ethernet1/1/8 Disb 128.160 128 2000000000 BLK 0 SHARED No
ethernet1/1/9 Disb 128.164 128 2000000000 BLK 0 SHARED No

```

示例（接口）

```

OS10# show spanning-tree msti 1 interface ethernet 1/1/1
ethernet1/1/1 of vlan1 is root Forwarding
Edge port:no (default) port guard :none (default)
Link type is point-to-point (auto)
Boundary :internal bpdu filter : bpdu guard : bpduguard shutdown-on-
violation :disable RootGuard: disable LoopGuard disable
Bpdus (MRecords) sent 3779, received 7
Interface Designated
Name PortID Prio Cost Sts Cost Bridge ID PortID

ethernet1/1/1 128.132 128 20000 FWD 0 32768 74e6.e2f5.dd80 128.132

```

示例（防护）

```

OS10# show spanning-tree msti 1 guard
Interface
Name Instance Sts Guard Type

ethernet1/1/1 MSTI 1 FWD root
ethernet1/1/2 MSTI 1 FWD loop
ethernet1/1/3 MSTI 1 BLK none
ethernet1/1/4 MSTI 1 FWD none
ethernet1/1/5 MSTI 1 BLK none
ethernet1/1/6 MSTI 1 BLK none
ethernet1/1/7 MSTI 1 BLK none
ethernet1/1/8 MSTI 1 BLK none
...

```

示例（虚拟接口）

```

agg-6146 # show spanning-tree msti 0 virtual-interface
VFP(VirtualFabricPort) of MSTI 0 is Designated Forwarding
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: No, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 250, Received: 240
Interface Designated
Name PortID Prio Cost Sts Cost Bridge ID PortID

VFP(VirtualFabricPort) 0.1 0 1 FWD 0 32768 3417.ebf2.a8c4 0.1

```

命令历史记录 10.2.0E or later

# 虚拟 LAN

VLAN 将单个平面 L2 广播域分段至多个逻辑 L2 网络。每个 VLAN 均由以太网框架中包含 12 位的 VLAN ID 或标签唯一标识。VLAN ID 的范围为 1 到 4093，并且总共提供 4093 个逻辑网络。

您可以将单个物理设备上的端口分配到一个或多个 VLAN，以便在单个物理设备上创建多个逻辑实例。跨不同物理设备的虚拟逻辑交换机将模拟单个物理网络上的多个逻辑分段的 L2 网络。



每个 VLAN 都有自己的广播域。来自属于 VLAN 的端口的单播、多播和广播网络流量仅转发或泛洪至同一 VLAN 中的端口。从一个 VLAN 到另一个的 VLAN 路由之间的流量。您还可以为每个 VLAN 分配一个 IP 地址，以将所有端口分组到单个 IP 子网内。

在 SmartFabric 服务模式下，您最多可以配置 256 个上行链路 VLAN，包括默认 VLAN（在硬件容量有限的情况下）。对于每个上行链路 VLAN 接口，系统都会创建一个 ACL 条目以对流量进行分类。此 ACL 条目可将流量从 VLAN 映射到相应的流量类别 (TC) 队列。如果创建超过 256 个 VLAN，则在光纤通道网关或光纤通道直连模式下创建上行链路时，ACL 表创建将失败。

在 SmartFabric 模式下，虽然您可以使用 CLI 创建 VLAN 1 至 4000 和 4021 至 4094，但不能为其分配接口。因此，请勿使用 CLI 在 SmartFabric 模式下创建 VLAN。

使用 VLAN 对 L2 网络进行分段以执行以下操作：

- 最大限度减少 L2 网络中的广播和多播流量
- 通过将端口隔离到不同的 VLAN 提高安全性
- 轻松网络管理

## 默认 VLAN

所有接口端口在 L2 模式下都进行正常管理，并且自动置于默认 VLAN 中作为未标记接口。

当您在中继模式下将某个端口分配到非默认 VLAN 时，该接口仍将保留默认 VLAN 的未标记成员和新 VLAN 的标记成员。在访问模式下为非默认 VLAN 分配端口时，它将从默认 VLAN 中移除，并将其分配给新 VLAN 作为新 VLAN 的未标记成员。

- VLAN 1 是默认 VLAN。
- 您无法删除默认 VLAN。但是，您可以使用 `default vlan-id` 命令更改默认 VLAN ID 号。

使用 `show vlan` 命令可验证接口是否属于默认 VLAN (VLAN 1)。

### 更新 VLAN 配置

```
OS10# show vlan

Codes: * - Default VLAN, G-GVRP VLANs, R-Remote Port Mirroring VLANs, P-Primary, C-Community, I-Isolated
Q: A-Access (Untagged), T-Tagged
 x-Dot1x untagged, X-Dot1x tagged
 G-GVRP tagged, M-Vlan-stack, H-VSN tagged
 i-Internal untagged, I-Internal tagged, v-VLT untagged, V-VLT tagged
 NUM Status Description Q Ports
* 1 up A Eth1/1/1-1/1/54
```

## 创建或移除 VLAN

您可以创建 VLAN 并将物理接口或端口通道 LAG 接口添加到 VLAN 作为已标记或未标记的成员。您可以将以太网接口添加为中继端口或访问端口，但不能同时添加。

### 在访问和中继模式下具有物理和端口通道端口的多个非默认 VLAN

```
OS10# show vlan

Codes: * - Default VLAN, G-GVRP VLANs, R-Remote Port Mirroring VLANs, P-Primary, C-Community, I-Isolated
Q: A-Access (Untagged), T-Tagged
 x-Dot1x untagged, X-Dot1x tagged
 G-GVRP tagged, M-Vlan-stack, H-VSN tagged
 i-Internal untagged, I-Internal tagged, v-VLT untagged, V-VLT tagged
 NUM Status Description Q Ports
* 1 up A Eth1/1/2 1/1/3:2 1/1/3:3 1/1/3:4
1/1/4
1/1/5 1/1/6 1/1/7 1/1/8 1/1/9 1/1/10 1/1/11 1/1/12 1/1/13 1/1/14 1/1/15 1/1/16 1/1/17
1/1/18
1/1/19 1/1/20 1/1/21 1/1/22 1/1/23 1/1/24 1/1/25:1 1/1/25:2 1/1/25:3 1/1/25:4 1/1/26
1/1/27
1/1/28 1/1/30 1/1/32
 A Po40
 T Eth1/1/3:2
 T Po40
 A Eth1/1/31
 200 up A Po40
 T Eth1/1/3:2
 T Po40
 A Eth1/1/31
```

```

320 up T Eth1/1/25:4 1/1/32
 T Po40
 A Eth1/1/3:1
49 1/1/50 1/1/51 1/1/52 1/1/53 1/1/54

```

shutdown 命令将停止 L3 级路由流量。L2 流量将继续通过 VLAN。如果 VLAN 不是使用 IP 地址配置的路由 VLAN，则此 shutdown 命令对 VLAN 流量没有影响。

使用 no interface vlan *vlan-id* 命令删除 VLAN 时，分配给该 VLAN 的任何接口都将分配给默认 VLAN 作为未标记接口。

要配置基于端口的 VLAN，请针对与 VLAN 相关的配置任务进入 INTERFACE-VLAN 模式并创建 VLAN。要启用 VLAN，请在 L2 模式下分配成员接口。

1. 创建 VLAN 并在 INTERFACE 模式下输入 VLAN 编号，从 1 到 4093。

```
interface vlan vlan-id
```

2. 在 CONFIGURATION 模式下删除 VLAN。

```
no interface vlan vlan-id
```

## 创建 VLAN

```
OS10(config)# interface vlan 108
```

## 删除 VLAN

```
OS10(config)# no interface vlan 108
```

## 查看配置的 VLAN

```

OS10(config)# do show interface vlan

Vlan 1 is up, line protocol is up
Address is , Current address is
Interface index is 69208865
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:

Vlan 200 is up, line protocol is up
Address is , Current address is
Interface index is 69209064
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:

Vlan 320 is up, line protocol is up
Address is , Current address is
Interface index is 69209184
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:

```

## 访问模式

访问端口是唯一一个 VLAN 的未标记成员。在访问模式中配置端口，然后配置哪些 VLAN 将传输该接口的流量。如果未在访问模式或访问端口中配置某个端口的 VLAN，该接口将为 VLAN 1（默认 VLAN）传输流量。

通过指定新 VLAN，更改 VLAN 中的访问端口成员资格。您必须先创建 VLAN，然后才能在访问模式下将端口分配给该 VLAN。使用 `no switchport access vlan` 命令重置为默认 VLAN。

1. 在 INTERFACE 模式下配置端口。

```
interface ethernet node/slot/port[:subport]
```

2. 在 INTERFACE 模式下访问时将接口设置为交换机端口模式。

```
switchport mode access
```

3. 在 INTERFACE 模式下输入未标记端口的 VLAN 编号。

```
switchport access vlan vlan-id
```

### 在访问模式下配置端口

```
OS10(config)# interface ethernet 1/1/9
OS10(config-if-eth1/1/9)# switchport mode access
OS10(config-if-eth1/1/9)# switchport access vlan 604
```

### 显示正在运行的配置

```
OS10# show running-configuration
...
!
interface ethernet1/1/5
...
switchport access vlan 604
no shutdown
!
interface vlan1
no shutdown
...
```

## 中继模式

中继端口可以是在接口上设置的多个 VLAN 的成员。中继端口为所有 VLAN 传输流量。要在具有多个 VLAN 的中继端口上传输流量，OS10 使用标记或 802.1q 封装方法。

1. 在 INTERFACE 模式下配置端口。

```
interface ethernet node/slot/port[:subport]
```

2. 在 INTERFACE 模式下将交换机模式更改为中继模式。

```
switchport mode trunk
```

3. 在 INTERFACE 模式下在中继端口上输入允许的 VLAN。

```
switchport trunk allowed vlan vlan-id
```

### 在中继模式下配置端口

```
OS10(config)# interface ethernet 1/1/6
OS10(conf-if-eth1/1/6)# switchport mode trunk
OS10(conf-if-eth1/1/6)# switchport trunk allowed vlan 108
```

### 查看正在运行的配置

```
OS10# show running-configuration
...
```

```
!
interface ethernet1/1/8
 switchport mode trunk
 switchport trunk allowed vlan 108
 no shutdown
!
interface vlan1
 no shutdown
!
...
```

## 分配 IP 地址

您可以为每个 VLAN 分配 IP 地址，使其成为 L3 VLAN。该 VLAN 中的所有端口都属于该特定的 IP 子网。

不同 VLAN 路由中的端口之间的流量使用 IP 地址。使用 `shutdown` 和 `no shutdown` 命令配置 L3 VLAN 接口，使其保持管理正常运行或关闭。此调配仅影响 VLAN 的各个成员的 L3 流量，不会影响 L2 流量。

您不得将 IP 地址分配给默认 VLAN (VLAN 1)。

**注：**但是，零接触部署 (ZTD) 应用程序需要此功能。当 ZTD 正在进行中时，系统会将 IP 地址分配给默认 VLAN 以建立连接。完成 ZTD 后，系统将移除分配给默认 VLAN 的 IP 地址。

您可以将 VLAN 和其他逻辑接口置于 L3 模式，以接收和发送路由流量。

1. 在 CONFIGURATION 模式下创建 VLAN，从 1 到 4093。

```
interface vlan vlan-id
```

2. 在 VLAN 模式下为 VLAN 分配 IP 地址和掩码。

```
ip address ip-address/prefix-length [secondary]
```

- *ip-address/prefix-length* — 输入以点分隔的十进制 A.B.C.D/x 格式输入 IP 地址。
- *secondary* — 输入接口备份 IP 地址。

### 向 VLAN 分配 IP 地址

```
OS10(config)# interface vlan 200
OS10(conf-if-vl-200)# ip address 10.1.15.1/8
```

### 查看 VLAN 配置

```
OS10(conf-if-vl-200)# do show interface vlan

Vlan 1 is up, line protocol is up
Address is , Current address is
Interface index is 69208865
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:

Vlan 200 is up, line protocol is up
Address is , Current address is
Interface index is 69209064
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:

Vlan 320 is up, line protocol is up
```

```
Address is , Current address is
Interface index is 69209184
Internet address is 20.2.11.1/24
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:
```

## 查看 VLAN 配置

您可以使用 `show` 命令查看与 VLAN 有关的配置信息。

- 在 EXEC 模式下查看 VLAN 状态和配置信息。

```
show vlan
```

- 在 EXEC 模式下查看 VLAN 接口配置。

```
show interfaces vlan
```

- 在 EXEC 模式下查看特定 VLAN ID 的 VLAN 接口配置。

```
show interfaces vlan vlan-id
```

### 查看 VLAN 配置

```
OS10# show vlan

Codes: * - Default VLAN, G-GVRP VLANs, R-Remote Port Mirroring VLANs, P-Primary, C-
Community, I-Isolated
Q: A-Access (Untagged), T-Tagged
 x-Dot1x untagged, X-Dot1x tagged
 G-GVRP tagged, M-Vlan-stack, H-VSN tagged
 i-Internal untagged, I-Internal tagged, v-VLT untagged, V-VLT tagged
 NUM Status Description Q Ports
* 1 up A Eth1/1/1-1/1/32
 200 up T Eth1/1/3:2
 320 up T Po40
 A Eth1/1/31
 T Eth1/1/25:4 1/1/32
 T Po40
 A Eth1/1/3:1
```

### 查看接口 VLAN 配置

```
OS10# show interface vlan
Vlan 1 is up, line protocol is up
Address is , Current address is
Interface index is 69208865
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:

Vlan 200 is up, line protocol is up
Address is , Current address is
Interface index is 69209064
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
```

```
interface status change:

Vlan 320 is up, line protocol is up
Address is , Current address is
Interface index is 69209184
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:
```

## 查看特定 VLAN 的接口配置

```
OS10# show interface vlan 320
Vlan 320 is up, line protocol is up
Address is , Current address is
Interface index is 69209184
Internet address is not set
MTU 1532 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 240
Last clearing of "show interface" counters Queueing strategy: fifo Time since last
interface status change:
```

## VLAN 命令

### 说明 (VLAN)

添加所选 VLAN 的说明。

|               |                                                    |
|---------------|----------------------------------------------------|
| <b>语法</b>     | <code>description <i>description</i></code>        |
| <b>参数</b>     | <i>description</i> — 输入用于标识 VLAN 的文本字符串。最多 80 个字符。 |
| <b>默认</b>     | 未配置                                                |
| <b>命令模式</b>   | INTERFACE-VLAN                                     |
| <b>使用情况信息</b> | 无                                                  |
| <b>示例</b>     | <pre>OS10(conf-if-vlan)# description vlan3</pre>   |
| <b>支持的版本</b>  | 10.2.0E or later                                   |

## interface vlan

创建 VLAN 接口。

|               |                                                                                                                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>interface vlan <i>vlan-id</i></code>                                                                                                                                                                             |
| <b>参数</b>     | <i>vlan-id</i> — 输入 VLAN ID 号, 从 1 到 4093。                                                                                                                                                                             |
| <b>默认</b>     | VLAN 1                                                                                                                                                                                                                 |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                                                                                                          |
| <b>使用情况信息</b> | 不支持 FTP、TFTP、MAC ACL 和 SNMP 操作。IP ACL 仅在 VLAN 上受支持。此命令的 <code>no</code> 版本将删除接口。<br> <b>注:</b> 在 SmartFabric 服务模式下, 创建 VLAN 处于禁用状态。 |

示例

```
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)#
```

支持的版本 10.2.0E or later

show vlan

显示 VLAN 配置。

- 语法 show vlan *vlan-id*
- 参数 *vlan-id* — (可选) 输入 VLAN ID 号, 从 1 到 4093。
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 使用此命令可以查看特定 VLAN ID 的 VLAN 配置信息。

示例

```
OS10(config)# do show vlan
Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring
VLANs
Q: A - Access (Untagged), T - Tagged
 NUM Status Description Q Ports
* 1 Active A Eth1/1/15
 2101 Active A Po100
 2102 Active T Eth1/1/1,1/1/3
 2102 Active T Po100
 2102 Active T Eth1/1/1,1/1/3
```

支持的版本 10.2.0E or later

端口监控

端口监控可以监控一个端口的入口或出口流量并与另一个端口比较以进行分析。监控端口 (MG) 或目标端口是用于接收分析的受监控流量的端口。受监控端口 (MD) 或源端口是监控进行流量分析的源接口。

 注: 此功能在 Z9332F-ON 平台上不受支持。

端口监控有以下不同类型:

- 本地端口监控 — 端口监控是在同一交换机中完成的。交换机将传入和传出流量的副本从一个端口转发到另一个端口, 以进行进一步分析。
- 远程端口监控 (RPM) — 端口监控是在同一网络中通过远程设备运行的流量上完成的。L2 网络携带受监控流量。
- 封装的远程端口监控 (ERPM) — 在 L3 网络上进行端口监控。源端口的流量封装并转发到另一个交换机中的目标端口。

本地端口监控

对于本地端口监控, 受监控的源端口和监控目标端口位于同一设备上。

配置本地监控会话

- 验证预期监控端口没有 no shutdown 和 no switchport 以外的配置。

```
show running-configuration
```

- 在 CONFIGURATION 模式下创建监控会话。

```
monitor session session-id [local]
```

3. 在 MONITOR-SESSION 模式下输入监控流量的源和方向。

```
source interface interface-type {both | rx | tx}
```

4. 在 MONITOR-SESSION 模式下输入流量的目标。

```
destination interface interface-type
```

创建监控会话

```
OS10(config)# monitor session 1
OS10(conf-mon-local-1)#
```

配置源和目标端口以及流量方向

```
OS10(conf-mon-local-1)# source interface ethernet 1/1/7-1/1/8 rx
OS10(conf-mon-local-1)# destination interface ethernet1/1/1
OS10(conf-mon-local-1)# no shut
```

查看已配置的监控会话

在“State”字段中，true 指示端口已启用。在“Reason”字段中，Is UP 指示硬件资源已分配。

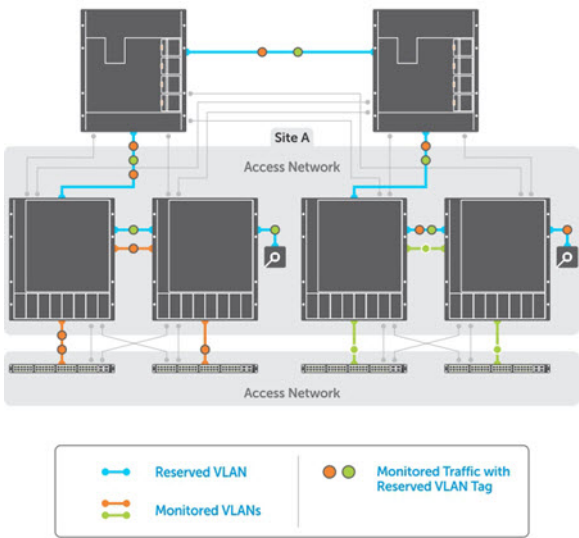
```
OS10# show monitor session all
S.Id Source Destination Dir SrcIP DstIP DSCP TTL State Reason

1 ethernet1/1/7 ethernet1/1/1 rx N/A N/A N/A N/A true Is UP
```

远程端口监控

远程端口监控可监控多个设备的多个源端口上的入口和/或出口流量，并将受监控流量转发到不同远程设备上的多个目标端口。远程端口监控可帮助网络管理员监控和分析流量，以对网络问题进行故障处理。

在远程端口监控会话中，监控的流量使用 VLAN ID 进行标记，并在用户定义的不可路由的 L2 VLAN 上切换。VLAN 保留为仅承载受监控的流量，在 VLAN 的所有出口端口上转发。您必须配置每个用于与保留的 L2 VLAN 传输受监控流量的中间交换机。远程端口监控支持监控在多个网络设备间分布多个源和目标端口的会话。



会话和 VLAN 要求

RPM 需要以下各项：

- 源会话，如在不同源设备上的受监控端口。
- 保留标记的 VLAN 用于传输源、中间和目标设备上配置的受监控流量。
- 目标会话，其中目标端口连接到目标设备上的分析器。



使用源和目标端口配置任何网络设备。使网络设备在用于多个远程端口监控会话的保留 VLAN 的中间传输会话中正常工作。您可以启用和禁用单个监控会话。

在配置 RPM 会话时，请考虑以下事项：

- 远程端口监控会话通过为保留的 VLAN 标记前缀添加为受监控的数据包，以使用保留 VLAN 进行传输来反映受监控的流量。
- 镜像数据包的源地址、目标地址和原始 VLAN ID 以将标记的 VLAN 标头添加为前缀。未标记的源数据包使用保留的 VLAN ID 进行标记。
- 保留 VLAN 的成员端口必须具有 MTU 和 IPMTU 值  $MAX+4$  以保存 VLAN 标签参数。
- 要与源会话关联，保留的 VLAN 最多可以有四个成员端口。
- 要与目标会话关联，保留的 VLAN 可以有多个成员端口。
- 保留的 VLAN 不能有未标记的端口。

## 保留的 L2 VLAN

- 保留的 VLAN 中的 MAC 地址学习会自动禁用。
- 用于保留的远程监视 VLAN 的 VLAN ID 没有限制。有效的 VLAN ID 从 2 到 4093。默认的 VLAN ID 不受支持。
- 在受监控的流量中，如果设备配置了 L3 VLAN，则在保留的 VLAN 用于传输镜像流量的路径中，具有与中间或目标设备相同的目标 MAC 地址的数据包将被接收流量的设备丢弃。

## 源会话

- 在远程端口监控中将物理端口和端口通道配置为源，并在同一源会话中使用它们。您可以同时使用通过 `switchport` 命令配置的 L2 和 L3 端口作为源端口。（可选）配置一个或多个源 VLAN 以配置要在源端口上监控的 VLAN 流量。
- 使用默认的 VLAN 和本机 VLAN 作为源 VLAN。
- 您不能配置用于将镜像流量传输为源 VLAN 的专用 VLAN。

## 限制

- 当使用源 VLAN 时，请使用 `flow-based enable` 命令启用基于流的监控。
- 在源 VLAN 中，仅监控接收的 (rx) 流量。
- 如果端口通道或 VLAN 在远程端口监控会话中将成员端口配置为目标端口，则无法在源会话中配置源端口通道或源 VLAN。
- 您不能将用于远程端口监控的目标端口用作源端口，包括作为端口运行的会话。
- 用于传输镜像流量的保留 VLAN 必须是 L2 VLAN。不支持 L3 VLAN。

## 配置远程端口监控

远程端口监控需要源接口、不同源网络设备上的受监控端口和保留的已标记 VLAN，以用于传输在源、中间和目标设备上配置的镜像流量。

1. 在 CONFIGURATION 模式下创建远程监控会话。

```
monitor session session-id type rpm-source
```

2. 在 MONITOR-SESSION 模式下输入要进行监控流量的源。

```
source interface interface-range direction
```

3. 在 MONITOR-SESSION 模式下输入要发送流量的目标。

```
destination remote-vlan vlan-id
```

4. 在 MONITOR-SESSION 模式下启用监控接口。

```
no shut
```

### 创建远程监控会话

```
OS10(config)# monitor session 10 type rpm-source
OS10(conf-mon-rpm-source-10) #
```

## 配置源和目标端口以及流量方向

```
OS10(conf-mon-rpm-source-10)# source interface vlan 10 rx
OS10(conf-mon-rpm-source-10)# destination remote-vlan 100
OS10(conf-mon-rpm-source-10)# no shut
```

## 查看监控会话

```
OS10(conf-mon-rpm-source-10)# do show monitor session all
S.Id Source Destination Dir SrcIP DstIP DSCP TTL State Reason

1 vlan10 vlan 100 rx N/A N/A N/A N/A true Is UP
```

## 封装的远程端口监控

您还可以将受监控流量通过 L3 网络传输到远程分析器。封装的远程端口监控 (ERPM) 会话将镜像来自源端口、LAG 或源 VLAN 的流量，并使用可路由的 GRE 封装的数据包将流量转发到会话中指定的目标 IP 地址。

在配置 ERPM 会话时，请考虑以下事项：

- OS10 仅支持 ERPM 源会话。在远程分析器的目标 IP 地址处终止封装的数据包。
- 源 IP 地址必须是会话的有效本地 IP 地址。
- 目标 IP 地址必须在支持标准 GRE 解封装的远程 L3 节点上。
- 如果无法访问目标 IP 地址，会话将会停止。
- OS10 不支持目标交换机上的 ERPM 目标会话和解封 ERPM 数据包。
- 在每个会话中最多可配置四个 ERPM 会话，最多为 128 个源端口。您可以采用以下一种方法配置这四个 ERPM 会话：
  - 单向有四个入口或四个出口会话。
  - 双向有两个入口和两个出口会话。
- 仅可通过基于流的监控来监控源 VLAN。基于流的源 VLAN 监控中仅支持入口。
- 您不能将具有 ERPM 流量的接口配置为 ERPM 会话的源。
- 您不能以源的形式监控 RPM VLAN。
- 您不能为两个会话配置相同的目标 IP 地址。
- 您不能将用作 GRE 隧道的出口的接口配置为源接口。
- ERPM 仅支持 IPv4 GRE 隧道。
- ERPM 不支持同等成本多路径 (ECMP)。
- 您只能将第三方设备用作隧道传输设备。
- OS10 不支持监控 VLAN 子接口和 CPU 生成的数据包。

## 配置封装的远程端口监控

封装的远程端口监控要求有效的源和目标 IP 地址。确保源 IP 地址为本地，并且目标 IP 地址为远程。您还可以配置生存时间 (TTL) 和区分服务代码点 (DSCP) 值。

1. 在 CONFIGURATION 模式下创建监控会话。

```
monitor session session-id type erpm-source
```

2. 在 MONITOR-SESSION 模式下配置源端口。

```
source interface interface-type {both | rx | tx}
```

3. 在 MONITOR-SESSION 模式下配置源和目标 IP 地址以及协议类型。

```
source-ip source ip-address destination-ip destination ip-address [gre-protocol protocol-value]
```

4. 在 MONITOR-SESSION 模式下配置 TTL 和 DSCP 值。

```
ip {ttl ttnumber | dscp dscp-number}
```

5. 在 MONITOR-SESSION 模式下启用监控接口。

```
no shut
```

### 创建监控会话

```
OS10(config)# monitor session 10 type erpm-source
OS10(conf-mon-erpm-source-10)#
```

### 配置源端口、源和目标 IP 地址以及协议类型

```
OS10(conf-mon-erpm-source-10)# source interface ethernet 1/1/2
OS10(conf-mon-erpm-source-10)# source-ip 1.1.1.1 destination-ip 3.3.3.3 gre-protocol
35006
OS10(conf-mon-erpm-source-10)# ip ttl 16
OS10(conf-mon-erpm-source-10)# ip dscp 63
OS10(conf-mon-erpm-source-10)# no shut
```

### 查看已配置的 ERPM 会话

```
OS10(conf-mon-erpm-source-6)# do show monitor session all

S.Id Source Destination Dir Mode Source IP Dest IP DSCP TTL Gre-Protocol
State Reason

6 ethernet1/1/2 remote-ip both port 1.1.1.1 3.3.3.3 63 16 35006
true Is UP
```

### 查看正在运行的监控会话配置

```
OS10# show running-configuration monitor
!
monitor session 10 type erpm-source
source-ip 1.1.1.1 destination-ip 3.3.3.3
source interface ethernet1/1/2
no shut
```

## 基于流的监控

基于流的监控通过仅检查指定的流量而不是所有接口流量来节省带宽。使用基于流的监控，您只能监控在入口访问列表 (ACL) 中与条件相匹配的源端口接收的流量。IPv4 ACL、IPv6 ACL 和 MAC ACL 支持基于流的监控。

1. 在 MONITOR-SESSION 模式下启用监控会话的基于流的监控。

```
flow-based enable
```

2. 返回 CONFIGURATION 模式。

```
exit
```

3. 在 CONFIGURATION 模式下创建访问列表。

```
ip access-list access-list-name
```

4. 在 CONFIG-ACL 模式中使用 seq、permit 和 deny 语句定义访问列表规则。ACL 规则描述了要监控的流量。

```
seq sequence-number {deny | permit} {source [mask] | any | host ip-address} [count
[byte]] [fragments] [threshold-in-msgs count] [capture session session-id]
```

5. 返回 CONFIGURATION 模式。

```
exit
```

6. 在 CONFIGURATION 模式下将基于流的监控 ACL 应用到受监控的源端口。访问列表名称的最大长度为 140 个字符。

```
ip access-group access-list-name {in | out}
```

启用基于流的监控

```
OS10(config)# monitor session 1
OS10(conf-mon-local-1)# flow-based enable
OS10(conf-mon-local-1)# exit
OS10(config)# ip access-list ipacl1
OS10(conf-ipv4-acl)# deny ip host 1.1.1.23 any capture session 1 count
OS10(conf-ipv4-acl)# exit
OS10(config)# mac access-list mac1
OS10(conf-mac-acl)# deny any any capture session 1
OS10(conf-mac-acl)# exit
OS10(config)# interface ethernet 1/1/9
OS10(conf-if-eth1/1/9)# mac access-group mac1 in
OS10(conf-if-eth1/1/9)# end
OS10# show mac access-lists in
Ingress MAC access-list mac1
Active on interfaces :
 ethernet1/1/9
seq 10 deny any any capture session 1 count (0 packets)
```

VLT 上的远程端口监控

在网络中，使用对等 VLT 节点配置的设备被视为单个设备。您可以在网络中的 VLT 设备上应用远程端口监控 (RPM)。在故障切换情况下，受监控流量通过 VLT 互连链路到达连接到架顶式交换机 (ToR) 的数据包分析器。

- 注:

- 在配置了 RPM 的 VLT 设备中，当 VLT 链路关闭时，受监控的数据包可能会丢弃一段时间。这段时间等同于 VLT 故障切换恢复时间，这是延迟还原。
  - ERPM 在 VLT 设备上不起作用。

VLT 上的 RPM 情景

请考虑一个简单的 VLT 设置，其中两个 VLT 设备使用 VLTi 连接，而架顶式交换机使用环形拓扑中的 VLT LAG 连接到两个 VLT 对等节点。在此设置中，下表介绍了在使用 RPM 镜像流量时可能出现的情况。

- 注:

□ 接到 VLT 域但不属于 VLT LAG 的端口称□孤立端口。

表. 39: VLT 上的 RPM 情景

| 情况说明                                                      | 建议                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 将孤立端口或 VLT LAG 或 VLTi 成员端口镜像到 VLT LAG。将数据包分析器连接到 ToR 交换机。 | <div>对等 VLT 设备上的建议配置：</div> <div>1. 创建 RPM VLAN</div> <div><pre>! interface vlan 100 no shutdown remote-span !</pre></div> <div>2. 为 RPM VLAN - RPM 会话创建 L2 ACL，然后将其连接到 VLTi LAG 接口。</div> <div><pre>! mac access-list rpm seq 10 permit any any capture session 10 vlan 100 !  interface ethernet 1/1/1 no shutdown switchport access vlan 1 mac access-group rpm in !</pre></div> |

表. 39: VLT 上的 RPM 情景 (续)

| 情况说明                                                                                           | 建议                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                | <p>3. 在对等 VLT 设备上创建基于流的 RPM 会话，以监控作为源的 VLTi LAG 接口。</p> <pre> ! monitor session 10 type rpm-source destination remote-vlan 100 flow-based enable source interface ethernet1/1/1 (ICL lag member) ! </pre>                                                                                                                                                                                                                                             |
| <p>将具有 VLTi LAG 的 VLAN 镜像为同一 VLT 设备上的任何孤立端口的成员。数据包分析器通过孤立端口连接到本地 VLT 设备。</p>                   | <p>VLT 设备上的建议配置：</p> <p>1. 为本地会话创建 L2 ACL，然后将其连接到 VLTi LAG 接口。</p> <pre> ! mac access-list local seq 10 permit any any capture session 10 !  interface ethernet 1/1/1 no shutdown switchport access vlan 1 mac access-group local in ! </pre> <p>2. 在 VLT 设备上创建基于流的本地会话，以监控作为源的 VLTi LAG 接口成员（以太网 1/1/1）。</p> <pre> ! monitor session 10 type destination interface ethernet 1/1/10 flow-based enable source interface ethernet1/1/1 no shut ! </pre> |
| <p>将具有 VLTi LAG 的 VLAN 作为成员镜像到同一 VLT 设备上的 VLT LAG。将数据包分析器连接到 ToR 交换机。</p>                      | —                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <p>将 ToR 的 VLT LAG 或 ToR 中的任意端口镜像到 VLT 设备中的任何孤立端口。将 VLT 节点配置为中间设备。将数据包分析器连接到 ToR 交换机。</p>      | —                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <p>将 VLT LAG 镜像至同一 VLT 设备上的任何孤立端口。数据包分析器通过孤立端口连接到本地 VLT 设备。</p>                                | <p>如果数据包分析器直接连接到配置了源会话的 VLT 对等节点，请使用本地端口监控而不是 RPM。</p>                                                                                                                                                                                                                                                                                                                                                                                                |
| <p>通过 VLTi，将主要 VLT 设备中的孤立端口镜像到辅助 VLT 设备上的任何孤立端口。数据包分析器通过孤立端口连接到辅助 VLT 设备。在这种情况下，镜像数据包是重复的。</p> | —                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <p>通过 VLTi 将主 VLT 设备的 VLT LAG 镜像到辅助 VLT 设备上的任何孤立端口。数据包分析器通过孤立端口连接到辅助 VLT 设备。</p>               | —                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <p>将 VLTi LAG 或 VLT LAG 的成员端口镜像到同一设备中的任何孤立端口。数据包分析器通过孤立端口连接到本地 VLT 设备。</p>                     | <p>如果数据包分析器直接连接到配置了源会话的 VLT 对等主机，则使用本地端口监控而不是 RPM。</p>                                                                                                                                                                                                                                                                                                                                                                                                |
| <p>将 VLTi LAG 上的成员端口镜像到同一 VLT 设备上的 VLT LAG。将数据包分析器连接到 ToR 交换机。</p>                             | —                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <p>将 VLT LAG 或 VLT 成员端口作为源 VLAN 和目标 VLAN 的一部分进行镜像。将数据包分析器连接到 ToR 交换机。</p>                      | —                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

# 端口监控命令

## description

配置端口监控会话的说明。监控会话可以是：本地、RPM 或 ERPM。

|        |                                       |
|--------|---------------------------------------|
| 语法     | <code>description string</code>       |
| 参数     | <i>string</i> — 输入监控会话的说明。最多 255 个字符。 |
| 默认     | 未配置                                   |
| 命令模式   | MONITOR-SESSION                       |
| 使用情况信息 | 此命令的 <code>no</code> 版本将移除说明文本。       |
| 示例     |                                       |

```
OS10(conf-mon-local-1)# description remote
```

```
OS10(conf-mon-rpm-source-5)# description "RPM Sesssion"
```

```
OS10(conf-mon-erpm-source-10)# description "ERPM Session"
```

支持的版本 10.2.0E or later

## destination

设置将监控流量发送到的目标。监控会话可以是本地或 RPM。

|        |                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>destination {interface interface-type   remote-vlan vlan-id}</code>                                                                                                                                                                                                                                                                                        |
| 参数     | <i>interface-type</i> — 输入本地监控会话的接口类型。 <ul style="list-style-type: none"><li><code>ethernet node/slot/port[:subport]</code> — 输入以太网接口信息作为目标。</li><li><code>port-channel id-number</code> — 输入一个端口通道号，从 1 到 128。</li><li><code>vlan vlan-id</code> — 输入一个 VLAN ID 作为目标，从 1 到 4093。</li></ul> <i>remote-vlan vlan-id</i> — 输入远程 VLAN ID 作为 RPM 监控会话的目标，从 1 到 4093。 |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                              |
| 命令模式   | MONITOR-SESSION                                                                                                                                                                                                                                                                                                                                                  |
| 使用情况信息 | 此命令的 <code>no</code> 版本会将该值重置为默认值。                                                                                                                                                                                                                                                                                                                               |
| 示例     |                                                                                                                                                                                                                                                                                                                                                                  |

```
OS10(conf-mon-local-10)# destination interface port-channel 10
```

```
OS10(conf-mon-rpm-source-3)# destination remote-vlan 20
```

支持的版本 10.2.0E or later

## flow-based

启用基于流的监控。监控会话可以是：本地、RPM 或 ERPM。

|        |                                   |
|--------|-----------------------------------|
| 语法     | <code>flow-based enable</code>    |
| 参数     | 无                                 |
| 默认     | 已禁用                               |
| 命令模式   | MONITOR-SESSION                   |
| 使用情况信息 | 此命令的 <code>no</code> 版本将禁用基于流的监控。 |

|       |                                                            |
|-------|------------------------------------------------------------|
| 示例    | <pre>OS10(conf-mon-local-1)# flow-based enable</pre>       |
|       | <pre>OS10(conf-mon-rpm-source-2)# flow-based enable</pre>  |
|       | <pre>OS10(conf-mon-erpm-source-3)# flow-based enable</pre> |
| 支持的版本 | 10.2.0E or later                                           |

## ip

配置 ERPM 流量的 IP 生存时间 (TTL) 值和差分服务代码点 (DSCP) 值。

|        |                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <pre>ip {ttl ttl-number   dscp dscp-number}</pre>                                                                                             |
| 参数     | <ul style="list-style-type: none"> <li><i>ttl-number</i> — 输入 TTL 值, 从 1 到 255。</li> <li><i>dscp-number</i> — 输入 DSCP 值, 从 0 到 63。</li> </ul> |
| 默认     | <ul style="list-style-type: none"> <li>TTL: 255</li> <li>DSCP: 0</li> </ul>                                                                   |
| 命令模式   | MONITOR-SESSION (ERPM)                                                                                                                        |
| 使用情况信息 | 此命令的 <code>no</code> 版本将移除已配置的 TTL 和 DSCP 值。                                                                                                  |
| 示例     | <pre>OS10(conf-mon-erpm-source-10)# ip ttl 16 OS10(conf-mon-erpm-source-10)# ip DSCP 63</pre>                                                 |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                          |

## monitor session

创建用于通过端口监控来监控流量的会话。

|           |                                                                                                                                                                                                                               |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法        | <pre>monitor session session-id type [local   rpm-source   erpm-source]</pre>                                                                                                                                                 |
| 参数        | <ul style="list-style-type: none"> <li><i>session-id</i> — 输入监控会话 ID, 从 1 到 18。</li> <li><i>local</i> — (可选) 输入本地监控会话。</li> <li><i>rpm-source</i> — (可选) 输入远程监控会话。</li> <li><i>erpm-source</i> — (可选) 输入封装的远程监控会话。</li> </ul> |
| 默认        | 本地                                                                                                                                                                                                                            |
| 命令模式      | CONFIGURATION                                                                                                                                                                                                                 |
| 使用情况信息    | 此命令的 <code>no</code> 版本将删除监控会话。                                                                                                                                                                                               |
| 示例        | <pre>OS10(config)# monitor session 1 OS10(conf-mon-local-1)#</pre>                                                                                                                                                            |
| 示例 (RPM)  | <pre>OS10(config)# monitor session 5 type rpm-source OS10(conf-mon-rpm-source-5)#</pre>                                                                                                                                       |
| 示例 (ERPM) | <pre>OS10(config)# monitor session 10 type erpm-source OS10(conf-mon-erpm-source-10)#</pre>                                                                                                                                   |
| 支持的版本     | 10.2.0E or later                                                                                                                                                                                                              |

show monitor session

显示有关监控会话的信息。

- 语法

show monitor session {session-id | all}
- 参数

- session-id — 输入会话 ID 号，从 1 到 18。
  - all — 查看所有监控会话。
- 默认

全部
- 命令模式

EXEC
- 使用情况信息

在“State”字段中，true 指示端口已启用。在“Reason”字段中，Is UP 指示硬件资源已分配。
- 示例（特定会话）

```
OS10# show monitor session 1
S.Id Source Destination Dir Mode Source IP Dest IP DSCP TTL Gre-P

1 ethernet1/1/1 remote-ip both port 11.11.11.1 11.11.11.11 0 255 35006
```

示例（所有会话）

```
OS10# show monitor session all
S.Id Source Destination Dir Mode Source IP Dest IP DSCP TTL Gr

1 ethernet1/1/1 remote-ip both port 11.11.11.1 11.11.11.11 0 255 35
9 ethernet1/1/9 both port N/A N/A N/A N/A
7 ethernet1/1/9 vlan40 both port N/A N/A N/A N/A
4 ethernet1/1/1 both port N/A N/A 0 255 35
Destination is not resolved
6 ethernet1/1/2 remote-ip both port 11.11.11.1 2.2.2.1 0 255 35
session does not exist
```

支持的版本

10.2.0E or later

shut

禁用监控会话。监控会话可以是：本地、RPM 或 ERPM。

- 语法

shut
- 参数

无
- 默认

已禁用
- 命令模式

MONITOR-SESSION
- 使用情况信息

此命令的 no 版本将启用监控会话。
- 示例

```
OS10(config)# monitor session 1
OS10(conf-mon-local-1)# no shut
```

```
OS10(config)# monitor session 5 type rpm-source
OS10(conf-mon-rpm-source-5)# no shut
```

```
OS10(config)# monitor session 10 type erpm-source
OS10(conf-mon-erpm-source-10)# no shut
```

支持的版本

10.2.0E or later

源

配置用于端口监控的源。监控会话可以是：本地、RPM 或 ERPM。

- 语法

source interface interface-type {both | rx | tx}



- 参数**
- *interface-type* — 输入接口类型：
    - *ethernet node/slot/port[:subport]* — 输入作为受监控源的以太网接口信息。
    - *port-channel id-number* — 输入端口通道接口编号作为受监控源，从 1 到 128。
    - *vlan vlan-id* — 输入 VLAN 标识符作为受监控源，从 1 到 4093。
  - *both* — 监控接收和传输数据包。VLAN 接口上不支持此选项。
  - *rx* — 仅监控接收的数据包。
  - *tx* — 仅监控传输的数据包。VLAN 接口上不支持此选项。

**默认** 未配置

**命令模式** MONITOR-SESSION

**使用情况信息**

**示例**

```
OS10(config)# monitor session 1
OS10(conf-mon-local-1)# source interface ethernet 1/1/7 rx
```

```
OS10(config)# monitor session 5 type rpm-source
OS10(conf-mon-rpm-source-5)# source interface ethernet 1/1/10 rx
```

```
OS10(config)# monitor session 10 type erpm-source
OS10(conf-mon-erpm-source-10)# source interface ethernet 1/1/5 rx
```

**支持的版本** 10.2.0E or later

## source-ip

配置 ERPM 监控会话的受监控端口的源、目标和协议类型。

**语法** *source-ip source ip-address destination-ip destination ip-address [gre-protocol protocol-value]*

- 参数**
- *source ip-address* — 输入源 IP 地址。
  - *destination ip-address* — 输入目标 IP 地址。
  - *protocol-value* — 输入 GRE 协议值，从 1 到 65535，默认值：35006。

**默认** 未配置

**命令模式** MONITOR-SESSION

**使用情况信息**

**示例**

```
OS10(config)# monitor session 10
OS10(conf-mon-erpm-source-10)# source-ip 10.16.132.181 destination-ip
172.16.10.11 gre-protocol 35006
```

**支持的版本** 10.4.0E(R1) or later

## 第 3 层

|                         |                                                                                                                                                                    |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>双向转发检测 (BFD)</b>     | 在具有相邻路由器的链路中提供快速故障检测（请参阅 <a href="#">BFD 命令</a> ）。                                                                                                                 |
| <b>边界网关协议 (BGP)</b>     | 提供外部网关协议，用于在自治系统内部及之间传输域间路由信息（请参阅 <a href="#">BGP 命令</a> ）。                                                                                                        |
| <b>同等成本多路径 (ECMP)</b>   | 在多个最佳路径上提供到单个目标的下一跳数据包转发（请参阅 <a href="#">ECMP 命令</a> ）。                                                                                                            |
| <b>IPv4 路由</b>          | 根据路由表，将数据包转发到目标 IP 地址。此路由表可定义数据包的路由方式（动态、直接广播到、使用代理 ARP）以及数据包中包含的信息类型（请参阅 <a href="#">IPv4 路由命令</a> ）。                                                             |
| <b>IPv6 路由</b>          | 为 IPv6 地址空间、无状态自动配置、标头格简化来提供路由，并改进了对选项和扩展的支持（请参阅 <a href="#">IPv6 路由命令</a> ）。                                                                                      |
| <b>首先打开最短路径 (OSPF)</b>  | 提供链路状态路由协议，该协议与使用链路状态通告 (LSA) 的同一自治系统区域中的所有其他设备进行通信。OS10 支持最多 10,000 个 OSPF 路由用于 OSPFv2，以将最多 8,000 个路由指定为外部，并将最多 2000 个路由指定为区域内/间路由（请参阅 <a href="#">OSPF 命令</a> ）。 |
| <b>虚拟路由器冗余协议 (VRRP)</b> | 提供一种机制，以消除静态路由网络中的单点故障（请参阅 <a href="#">VRRP 命令</a> ）。                                                                                                              |
| <b>虚拟路由和转发 (VRF)</b>    | 提供一种机制，用于将物理路由器分区为多个虚拟路由器（请参阅 <a href="#">VRF 命令</a> ）。                                                                                                            |

## 虚拟路由和转发

VRF 将物理路由器分区成多个虚拟路由器 (VR)。控制平面和数据平面在每个 VR 中隔离；流量不流经 VR。VRF 允许路由表的多个实例同时共存于同一路由器中。

OS10 支持管理 VRF 实例、默认 VRF 实例和最多 512 个非默认 VRF 实例。使用默认和非默认的 VRF 实例来配置路由。

您可以将管理接口从默认状态移至管理 VRF 实例。默认情况下，您不需要创建管理 VRF 实例，因为它已存在于系统中。

默认情况下，OS10 最初将所有物理接口和所有逻辑接口分配给默认 VRF 实例。

## 配置管理 VRF

您只可以向管理 VRF 实例添加管理接口。

在将管理接口分配给管理 VRF 实例之前，请在管理接口上删除所有已配置的设置（包括 IP 地址）。

1. 在 CONFIGURATION 模式下输入 `ip vrf management` 命令。仅使用基于非事务配置的模式。请勿使用基于事务的模式。
2. 在 VRF CONFIGURATION 模式下，使用 `interface management` 命令添加管理接口。

### 配置管理 VRF

```
OS10(config)# ip vrf management
OS10(conf-vrf)# interface management
```

您可以在管理或默认 VRF 实例中启用各种服务。管理和默认 VRF 实例中支持的服务如下：

**表. 40: 支持的服务**

| 应用程序 | 管理 VRF | 默认 VRF | 非默认 VRF |
|------|--------|--------|---------|
| BGP  | 否      | 是      | 是       |

表. 40: 支持的服务 (续)

| 应用程序          | 管理 VRF | 默认 VRF | 非默认 VRF |
|---------------|--------|--------|---------|
| COPP ACL      | 是      | 是      | 否       |
| DHCP 客户端      | 是      | 是      | 是       |
| DHCP 中继       | 否      | 是      | 是       |
| DHCP 服务器      | 否      | 是      | 否       |
| DNS 客户端       | 是      | 是      | 是       |
| FTP 客户端       | 是      | 是      | 是       |
| HTTP 客户端      | 是      | 是      | 是       |
| ICMP/Ping     | 是      | 是      | 是       |
| NTP 客户端       | 是      | 是      | 是       |
| NTP 服务器       | 是      | 是      | 是       |
| OSPFV2/OSPFV3 | 否      | 是      | 是       |
| RADIUS 服务器    | 是      | 是      | 是       |
| SCP 客户端       | 是      | 是      | 是       |
| sFlow         | 是      | 是      | 是       |
| SFTP          | 是      | 是      | 是       |
| SNMP 陷阱       | 是      | 是      | 否       |
| SSH 服务器       | 是      | 是      | 是       |
| 系统日志          | 是      | 是      | 是       |
| TACACS+ 服务器   | 是      | 是      | 是       |
| Telnet 服务器    | 是      | 是      | 是       |
| TFTP 客户端      | 是      | 是      | 是       |
| 跟踪路由          | 是      | 是      | 是       |
| VLT 备份链路      | 是      | 是      | 否       |
| VRRP          | 是      | 是      | 是       |

## 为管理 VRF 实例配置静态路由

配置将流量定向到管理接口的静态路由：

```
management route ip-address mask managementethernet
```

或

```
management route ipv6-address prefix-length managementethernet
```

您还可以将管理路由配置为将流量定向到物理接口。例如：

```
management route 10.1.1.0/24 managementethernet
```

或

```
management route 2::/64 managementethernet
```

## 配置非默认 VRF 实例

除了管理 VRF 实例和默认 VRF，OS10 还支持非默认 VRF 实例。最多可以创建 512 个非默认的 VRF 实例。

虽然可以将管理接口仅分配给管理 VRF 实例，但您可以将任何物理或逻辑接口（VLAN、端口通道或环回）分配到非默认 VRF 实例。

创建新的非默认 VRF 实例时，OS10 不会为其分配任何接口。您可以将新的 VRF 实例分配给任何现有的物理或逻辑接口，前提是它们尚未分配给另一个非默认 VRF。

 **注：**创建新逻辑接口时，OS10 会将其自动分配给默认 VRF 实例。此外，OS10 最初将所有物理第 3 层接口分配给默认的 VRF 实例。

您可以将分配给非默认 VRF 实例的任何接口重新分配回默认 VRF 实例。

- 要创建非默认 VRF 实例，请在 CONFIGURATION 模式下指定名称并输入 VRF 配置模式：

```
CONFIGURATION
```

```
ip vrf vrf-name
```

## 为非默认 VRF 实例分配接口

创建非默认 VRF 实例之后，您可以将接口关联到您创建的 VRF 实例。

要为非默认 VRF 分配接口，请执行以下步骤：

1. 输入要分配给非默认 VRF 实例的接口。

```
CONFIGURATION
```

```
interface ethernet 1/1/1
```

2. 从 L2 交换中移除接口。

```
INTERFACE
```

```
no switchport
```

3. 为非默认 VRF 分配接口。

```
INTERFACE CONFIGURATION
```

```
ip vrf forwarding vrf-test
```

在为 VRF 实例分配接口之前，请确保未在接口上配置 IP 地址。

4. 将一个 IPv4 地址分配给接口。

```
INTERFACE CONFIGURATION
```

```
ip address 10.1.1.1/24
```

5. 将一个 IPv6 地址分配给接口。

```
INTERFACE CONFIGURATION
```

```
ipv6 address 1::1/64
```

您也可以使用 `ipv6 address autoconfig` 命令自动配置 IPv6 地址。

 **注：**在 VRF 实例中配置任何路由协议之前，您必须先将 IP 地址分配给要在其上配置路由协议的 VRF 实例的至少一个接口。

## 为非默认 VRF 实例分配环回接口

创建非默认 VRF 实例之后，您可以将环回接口与您创建的 VRF 实例关联。

要为非默认 VRF 分配环回接口，请执行以下步骤：

1. 输入要分配给非默认 VRF 实例的环回接口。

CONFIGURATION

```
interface loopback 5
```

2. 为非默认 VRF 分配接口。

INTERFACE CONFIGURATION

```
ip vrf forwarding vrf-test
```

在将 n 接口分配给 VRF 实例之前，请确保未在接口上配置 IP 地址。

3. 将一个 IPv4 地址分配给接口。

INTERFACE CONFIGURATION

```
ip address 10.1.1.1/24
```

4. 将一个 IPv6 地址分配给接口。

INTERFACE CONFIGURATION

```
ipv6 address 1::1/64
```

您也可以使用 `ipv6 address autoconfig` 命令自动配置 IPv6 地址。

## 将接口分配回默认 VRF 实例

表. 41: 要删除的配置

| CONFIGURATION                        | MODE                    | 命令                                                                                                |
|--------------------------------------|-------------------------|---------------------------------------------------------------------------------------------------|
| IP 地址 — 在接口配置模式中，撤销 IP 地址配置。         | INTERFACE CONFIGURATION | OS10(conf-if-eth1/1/10:1)#no ip address <i>ipv4-address</i> 或 no ipv6 address <i>ipv6-address</i> |
| 端口 — 在接口配置模式中，删除与要删除的 VRF 实例对应的接口关联。 | INTERFACE CONFIGURATION | OS10(conf-if-eth1/1/10:1)#no ip vrf forwarding                                                    |

要将某个接口分配回默认 VRF，请执行以下步骤：

1. 输入要分配回默认 VRF 实例的接口。

CONFIGURATION

```
interface ethernet 1/1/1
```

2. 移除与该接口关联的 IPv4 地址。

INTERFACE CONFIGURATION

```
no ip address
```

3. 移除与该接口关联的 IPv6 地址。

INTERFACE CONFIGURATION

```
no ipv6 address
```

4. 将接口分配回默认的 VRF 实例。

INTERFACE CONFIGURATION

```
no ip vrf forwarding
```

## 将管理接口重新分配给默认 VRF 实例

要将管理接口分配回默认 VRF，请执行以下步骤：

1. 输入管理 VRF 实例。

CONFIGURATION

```
ip vrf management
```

2. 移除与该接口关联的 IPv4 地址。

INTERFACE CONFIGURATION

```
no ip address
```

3. 移除与该接口关联的 IPv6 地址。

```
INTERFACE CONFIGURATION
```

```
no ipv6 address
```

4. 将管理接口分配回默认的 VRF 实例。

```
CONFIGURATION VRF
```

```
no interface management
```

## 删除非默认 VRF 实例

删除非默认 VRF 实例之前，请确保首先删除或禁用与该 VRF 实例对应的所有依赖项和关联。以下过程介绍了如何删除非默认 VRF 实例：

删除所有依赖项后，您可以删除您已创建的非默认 VRF 实例。

- 使用以下命令删除非默认 VRF 实例：

```
CONFIGURATION
```

```
no ip vrf vrf-name
```

 **注：** 您不能删除默认的 VRF 实例。

## 为非默认 VRF 实例配置静态路由

- 在非默认 VRF 实例中配置静态路由。静态路由由包含可通过非默认 VRF 访问的下一跳邻居的 IP 地址。这些 IP 地址也可能属于非默认 VRF 实例的接口。

```
CONFIGURATION
```

```
ip route vrf vrf-name ip-address mask next-hop-ip-address 或 ipv6 route vrf vrf-name ipv6-address prefix-length next-hp[=ipv6-address
```

例如：ip route vrf red 10.1.1.0/24 20.1.1.6 或 ipv6 route vrf red 2::/64 3::1

- 配置在非默认 VRF 实例的情况下将流量定向到前面板端口的路由。

```
CONFIGURATION
```

```
ip route ip-address-mask ethernet interface-type 或 ipv6 route ipv6-address-mask ethernet interface-type
```

例如：ip route 10.1.1.0/24 ethernet 1/1/1 或 ipv6 route 2::/64 ethernet 1/1/1。其中，以太网 1/1/1 是非默认 VRF 的一部分。

## 在 IPv6 邻居中配置静态条目

- 在 IPv6 邻居查找中配置静态条目。

```
CONFIGURATION
```

```
ipv6 neighbor vrf vrf-test 1::1 ethernet 1/1/1 xx:xx:xx:xx:xx:xx
```

## VRF 配置

以下配置说明了典型的 VRF 设置：

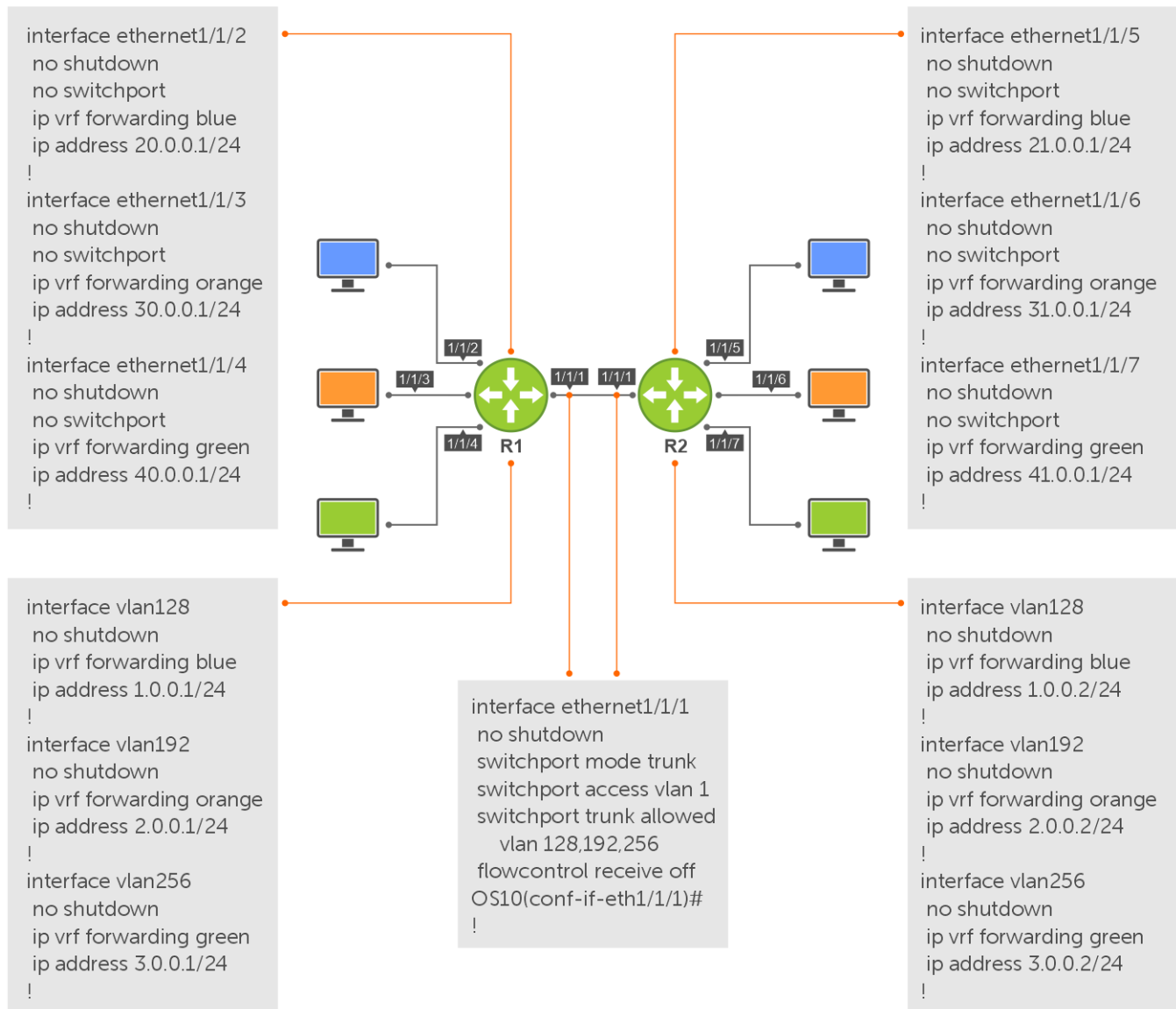


图 7: 设置 VRF 接口

## 路由器 1

```
ip vrf blue
!
ip vrf orange
!
ip vrf green
!
interface ethernet 1/1/1
 no ip address
 no switchport
 no shutdown
!
interface ethernet1/1/2
 no shutdown
 no switchport
 ip vrf forwarding blue
 ip address 20.0.0.1/24
!
interface ethernet1/1/3
 no shutdown
 no switchport
 ip vrf forwarding orange
```

```

ip address 30.0.0.1/24
!
interface ethernet1/1/4
no shutdown
no switchport
ip vrf forwarding green
ip address 40.0.0.1/24
!
interface vlan128
mode L3
no shutdown
ip vrf forwarding blue
ip address 1.0.0.1/24
!
interface vlan192
mode L3
no shutdown
ip vrf forwarding orange
ip address 2.0.0.1/24
!
!
interface vlan256
mode L3
no shutdown
ip vrf forwarding green
ip address 3.0.0.1/24
!
ip route vrf green 31.0.0.0/24 3.0.0.1

```

## 路由器 2

```

ip vrf blue
!
ip vrf orange
!
ip vrf green
!
interface ethernet 1/1/1
no ip address
no switchport
no shutdown
!
interface ethernet1/1/5
no shutdown
no switchport
ip vrf forwarding blue
ip address 21.0.0.1/24
!
interface ethernet1/1/6
no shutdown
no switchport
ip vrf forwarding orange
ip address 31.0.0.1/24
!
interface ethernet1/1/7
no shutdown
no switchport
ip vrf forwarding green
ip address 41.0.0.1/24
!
interface vlan128
mode L3
no shutdown
ip vrf forwarding blue
ip address 1.0.0.2/24
!
interface vlan192
mode L3
no shutdown
ip vrf forwarding orange
ip address 2.0.0.2/24
!
interface vlan256

```



```

mode L3
no shutdown
ip vrf forwarding green
ip address 3.0.0.2/24
!
ip route vrf green 30.0.0.0/24 3.0.0.2

```

## 路由器 1 显示命令输出

```

OS10# show ip vrf
VRF-Name Interfaces
blue Eth1/1/2
 Vlan128

default Mgmt1/1/1
 Vlan1,24-25,200

green Eth1/1/4
 Vlan256

orange Eth1/1/3
 Vlan192

OS10# show ip route vrf blue
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, * - candidate default,
 + - summary route, > - non-active route
Gateway of last resort is not set

```

| Destination   | Gateway                    | Dist/Metric | Last Change |
|---------------|----------------------------|-------------|-------------|
| C 20.0.0.0/24 | via 20.0.0.1 ethernet1/1/2 | 0/0         | 01:46:41    |

```

OS10# show ip route vrf orange
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, * - candidate default,
 + - summary route, > - non-active route
Gateway of last resort is not set

```

| Destination   | Gateway                    | Dist/Metric | Last Change |
|---------------|----------------------------|-------------|-------------|
| C 30.0.0.0/24 | via 30.0.0.1 ethernet1/1/3 | 0/0         | 01:55:00    |

```

OS10# show ip route vrf green
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, * - candidate default,
 + - summary route, > - non-active route
Gateway of last resort is not set

```

| Destination   | Gateway                    | Dist/Metric | Last Change |
|---------------|----------------------------|-------------|-------------|
| C 40.0.0.0/24 | via 40.0.0.1 ethernet1/1/4 | 0/0         | 02:01:15    |

## 路由器 2 显示命令输出

```

OS10# show ip vrf
VRF-Name Interfaces
blue Eth1/1/5
 Vlan128

default Mgmt1/1/1
 Vlan1,24-25,200

```

```

green Eth1/1/7
 Vlan256

orange Eth1/1/6
 Vlan192

OS10# show ip route vrf blue
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, * - candidate default,
 + - summary route, > - non-active route
Gateway of last resort is not set

```

| Destination   | Gateway                    | Dist/Metric | Last Change |
|---------------|----------------------------|-------------|-------------|
| C 21.0.0.0/24 | via 21.0.0.1 ethernet1/1/5 | 0/0         | 02:05:00    |

```

OS10# show ip route vrf orange
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, * - candidate default,
 + - summary route, > - non-active route
Gateway of last resort is not set

```

| Destination   | Gateway                    | Dist/Metric | Last Change |
|---------------|----------------------------|-------------|-------------|
| C 31.0.0.0/24 | via 31.0.0.1 ethernet1/1/6 | 0/0         | 02:09:19    |

```

OS10# show ip route vrf green
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, * - candidate default,
 + - summary route, > - non-active route
Gateway of last resort is not set

```

| Destination   | Gateway                    | Dist/Metric | Last Change |
|---------------|----------------------------|-------------|-------------|
| C 41.0.0.0/24 | via 41.0.0.1 ethernet1/1/7 | 0/0         | 02:45:16    |

## 查看 VRF 实例信息

要显示有关 VRF 配置的信息，请使用 `show ip vrf` 命令。要显示有关所有 VRF 实例（包括默认 VRF 0）的信息，请勿输入 `vrf-name` 的值。

- 显示 VRF 实例接口。

```
EXEC
```

```
show ip vrf [vrf-name]
```

## 静态路由泄漏

路由泄漏使在默认或非默认 VRF 实例中配置的路由可供另一个 VRF 实例使用。您可以将路由从源 VRF 实例泄露到目标 VRF 实例。

需要在源和目标 VRF 中泄漏路由，以实现端到端流量流。

如果在同一子网中存在任何连接的路由，则会优先处理连接的路由。

在静态路由泄漏的情况下，DHCP 功能对重叠子网不起作用。例如，如果不同 VRF 上的两个接口位于同一子网中，并且配置了相同的 DHCP 服务器，则只有其中一个接口获取 IP 地址。另一个接口不会获得 IP 地址，因为来自两个接口的客户端请求具有相同的 MAC 和子网地址。服务器没有任何唯一的参数来区分请求来自两个不同的客户端。

## 限制

- 在 VLT 条件下，在 VLT 对等节点之间未同步泄漏的路由的已解析 ARP 条目。当泄漏的路由配置处于活动状态时，在源 VRF 中解析的 ARP 条目将编程为泄漏的 VRF。
- 从 10.4.2 降级的过程中，将会恢复泄漏的路由配置。但是，路由在目标 VRF 实例中保持非活动状态。
- 从 10.4.2 降级时，不会恢复 `update-source-if` 命令。

## 配置静态路由泄漏

要配置静态路由泄漏，请执行以下操作：

1. 在源 VRF 实例中输入包含要泄漏的静态路由的接口。

```
interface interface-name
CONFIGURATION 模式
```

2. 在 INTERFACE CONFIGURATION 模式中，将接口分配给源 VRF 实例。

```
ip vrf forwarding vrf1
INTERFACE CONFIGURATION 模式
```

3. 将一个 IP 地址分配给接口。

```
ip address ip-address
VRF CONFIGURATION 模式
```

4. 输入要将静态路由泄露到的 VRF 实例的接口。

```
interface interface-name
CONFIGURATION 模式
```

5. 在 INTERFACE CONFIGURATION 模式中，将接口分配给目标 VRF 实例。

```
ip vrf forwarding vrf2
INTERFACE CONFIGURATION 模式
```

6. 配置要在目标 VRF 实例上泄漏的静态路由。

```
ip route vrf dest-vrf-name route nexthop-interface
```

7. 配置先前在源 VRF 实例中配置的静态路由，以便在目标 VRF 实例中可用。

```
ip route vrf src-vrf-name route nexthop-interface
```

```
OS10(config)#interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip vrf forwarding VRF1
OS10(conf-if-eth1/1/1)# ip address 120.0.0.1/24
OS10(config)#interface ethernet 1/1/2
OS10(conf-if-eth1/1/1)# ip vrf forwarding VRF2
OS10(conf-if-eth1/1/1)# ip address 140.0.0.1/24
OS10(config)#ip route vrf VRF1 140.0.0.0/24 interface ethernet 1/1/2
OS10(config)#ip route vrf VRF2 120.0.0.0/24 interface ethernet 1/1/1
```

The following example shows the show output:

```
OS10(config)# do show ip route vrf VRF1
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, * - candidate default,
 + - summary route, > - non-active route
Gateway of last resort is not set
Destination Gateway Dist/Metric Last Change

```

```
C 120.0.0.0/24 via 120.0.0.1 ethernet1/1/1 0/0 00:00:57
S 140.0.0.0/24 Direct,VRF2 ethernet1/1/2 1/0 00:00:04
```

```
OS10(config)# do show ip route vrf VRF2
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
```

```
O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
E2 - OSPF external type 2, * - candidate default,
+ - summary route, > - non-active route
Gateway of last resort is not set
Destination Gateway Dist/Metric Last Change

S 120.0.0.0/24 Direct,VRF1 ethernet1/1/1 1/0 00:00:05
C 140.0.0.0/24 via 140.0.0.1 ethernet1/1/2 0/0 00:01:54
```

## 为泄漏的路由配置源 IP 地址

如果没有为任何自发起数据包（例如，ping 或路由跟踪）明确地提及源 IP，则会基于其源选择算法 VRF 来选择源。

**注：**对于要流过的端到端流量，您必须为自发起数据包指定源，并将其泄露到目标 VRF 中。

要缓解此问题并控制泄漏的路由的源 IP 地址，您可以创建环回接口并将其与泄漏的 VRF 相关联。

要明确地提及泄漏的 VRF 的源接口，请执行以下操作：

输入以下命令：

```
update-source-if
```

VRF CONFIGURATION 模式

在泄漏的 VRF 中配置源 IP 地址后，如果在没有 -I 选项的情况下启动 ping，则源 IP 地址将为环回接口的地址。

## 使用路由目标的路由泄漏

您可以使用路由目标将一个 VRF 实例中的路由泄露到另一个实例。

**注：**您可以仅使用默认和非默认 VRF 实例上的路由目标泄露路由。您不能使用管理 VRF 实例上的路由目标来泄漏路由。

要使用路由目标在一个 VRF 实例中泄漏路由，请执行以下操作：

1. 输入要使用路由目标泄露路由的 VRF。

```
CONFIGURATION
```

```
ip vrf source-vrf-name
```

2. 导出属于一个 VRF 实例的路由。

```
VRF CONFIGURATION
```

```
ip route-export 1::1
```

3. 输入您想要将路由泄露到的非默认 VRF 实例。

```
CONFIGURATION
```

```
ip vrf destination-vrf-name
```

```
ip route-import 1::1
```

源 VRF 实例中现在可以使用从源 VRF 实例导出的路由。

**注：**当您配置正在泄漏的静态路由时，只有一个 ECMP 的路由（最佳 ECMP 路由）将泄露到另一个 VRF 实例。其他 ECMP 静态路由不会泄漏到其他 VRF 实例。

## 使用路由映射的路由泄漏

您可以使用路由映射将一个 VRF 实例中的路由泄露到另一个 VRF 实例。

要使用路由映射在一个 VRF 实例中泄漏路由，请执行以下操作：

1. 输入要使用路由目标泄露路由的 VRF。

```
CONFIGURATION
```

```
ip vrf source-vrf-name
```

```
ip vrf VRF-A
```

## 2. 配置 IP 前缀。

CONFIGURATION

```
ip prefix-list prefix-list-name {permit | deny} ip-address
```

```
ip prefix-list abc permit 20.0.0.0/24
or
ip prefix-list abc deny 20.0.0.0/24
```

## 3. 配置路由映射。

CONFIGURATION

```
route-map route-map-name
```

```
route-map xyz
```

## 4. 将前缀列表与路由映射关联。

CONFIGURATION

```
route-map route-map-name {permit | deny} rule
```

```
match ip address prefix-list prefix-list-name
```

```
route-map xyz permit 10
match ip address prefix-list abc
or
route-map xyz deny 10
match ip address prefix-list abc
```

## 5. 使用路由映射从 VRF 实例导出路由。

VRF CONFIGURATION

```
ip route-export route-target route-map-name route-map-name
```

```
ip route-export 1:1 route-map xyz
```

## 6. 输入要使用路由映射来泄漏路由的目标 VRF 实例。

CONFIGURATION

```
ip vrf destination-vrf-name
```

```
ip vrf VRF-B
```

## 7. 将这些泄漏的路由导入另一个 VRF 实例。

VRF CONFIGURATION

```
ip route-import route-target
```

```
ip route-import 1:1
```

```
OS10(config)#interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip vrf forwarding VRF1
OS10(conf-if-eth1/1/1)# ip address 120.0.0.1/24

OS10(config)#interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# ip vrf forwarding VRF2
OS10(conf-if-eth1/1/2)# ip address 140.0.0.1/24
OS10(config)#ip route vrf VRF1 160.0.0.0/24 120.0.0.2
OS10(config)# ip vrf VRF1
OS10(conf-vrf)# ip route-export 1:1
OS10(config)# ip vrf VRF2
OS10(conf-vrf)# ip route-import 1:1
```

## VRF 命令

### interface management

向管理 VRF 实例添加管理接口。

|        |                                            |
|--------|--------------------------------------------|
| 语法     | <code>interface management</code>          |
| 参数     | 无                                          |
| 默认     | 未配置                                        |
| 命令模式   | VRF CONFIGURATION                          |
| 使用情况信息 | 此命令的 <code>no</code> 版本从管理 VRF 实例中将移除管理接口。 |
| 示例     |                                            |

```
OS10(config)# ip vrf management
OS10(conf-vrf)# interface management
```

支持的版本 10.4.0E(R1) or later

### ip domain-list vrf

为管理 VRF 实例或您创建的任何非默认 VRF 实例配置域列表。

|        |                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip domain-list vrf {management   vrf-name} domain-names</code>                                                                                                                                                                             |
| 参数     | <ul style="list-style-type: none"><li>• <code>management</code> — 输入关键字 <code>management</code> 以配置管理 VRF 实例的域列表。</li><li>• <code>vrf-name</code> — 输入非默认 VRF 实例的名称，以配置该非默认 VRF 实例的域列表。</li><li>• <code>domain-names</code> — 输入域名的列表。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                              |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                    |
| 使用情况信息 | 此命令的 <code>no</code> 版本会从管理或非默认 VRF 实例中移除域列表配置。                                                                                                                                                                                                  |
| 示例     |                                                                                                                                                                                                                                                  |

```
OS10(config)# ip domain-list vrf management dns1 dell.com
or
OS10(config)# ip domain-list vrf blue dns1 dell.com
```

支持的版本 10.4.0E(R1) or later

### ip domain-name vrf

配置管理 VRF 实例或您创建的任何非默认 VRF 实例的域名。

|        |                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip domain-name vrf {management   vrf-name} domain-name</code>                                                                                                                                                                     |
| 参数     | <ul style="list-style-type: none"><li>• <code>management</code> — 输入关键字 <code>management</code> 以配置管理 VRF 实例的域名。</li><li>• <code>vrf-name</code> — 输入非默认 VRF 实例的名称，以配置该 VRF 实例的域名。</li><li>• <code>domain-name</code> — 输入域名。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                     |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                           |
| 使用情况信息 | 此命令的 <code>no</code> 版本将从管理或非默认 VRF 实例中移除域名。                                                                                                                                                                                            |
| 示例     |                                                                                                                                                                                                                                         |

```
OS10(config)# ip domain-name vrf management dell.com
or
OS10(config)# ip domain-name vrf blue dell.com
```

支持的版本 10.4.0E(R1) or later

## ip vrf

创建非默认 VRF 实例。

|        |                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip vrf vrf-name</code>                                                                                                             |
| 参数     | <ul style="list-style-type: none"><li><code>vrf-name</code>— 输入要创建的非默认 VRF 的名称。输入长度不超过 32 个字符的 VRF 名称。</li></ul>                         |
| 默认     | 未配置                                                                                                                                      |
| 命令模式   | CONFIGURATION                                                                                                                            |
| 使用情况信息 | 仅在基于非事务配置模式下输入 <code>ip vrf vrf-name</code> 命令。请勿使用基于事务的模式。最多可以创建 128 个非默认的 VRF 实例。 <code>no ip vrf vrf-name</code> 命令将移除您指定的非默认 VRF 实例。 |
| 示例     | <pre>OS10(config)# ip vrf vrf-test OS10(conf-vrf-test)#</pre>                                                                            |
| 支持的版本  | 10.4.1.0 or later                                                                                                                        |

## ip ftp vrf

为管理或非默认 VRF 实例配置 FTP 客户端。

|        |                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip ftp vrf {management   vrf vrf-name}</code>                                                                                                                                      |
| 参数     | <ul style="list-style-type: none"><li><code>management</code> — 输入关键字以在管理 VRF 实例上配置 FTP 客户端。</li><li><code>vrf vrf-name</code> — 输入关键字，然后输入 VRF 的名称，以便在该非默认 VRF 实例上配置 FTP 客户端。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                      |
| 命令模式   | CONFIGURATION                                                                                                                                                                            |
| 使用情况信息 | 此命令的 <code>no</code> 版本将从 FTP 客户移除管理 VRF 实例配置。                                                                                                                                           |
| 示例     | <pre>OS10(config)# ip ftp vrf management OS10(config)# ip ftp vrf vrf-blue</pre>                                                                                                         |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                     |

## ip host vrf

为管理 VRF 实例或非默认 VRF 实例配置主机名称，并将主机名称映射到 IPv4 或 IPv6 地址。

|        |                                                                                                                                                                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip host vrf {management   vrf-name} hostname {IP-address   Ipv6-address}</code>                                                                                                                                                                                                                   |
| 参数     | <ul style="list-style-type: none"><li><code>management</code> — 输入关键字 <code>management</code> 以配置管理 VRF 实例的主机名称。</li><li><code>vrf-name</code>— 输入要为该 VRF 实例配置主机名称的非默认 VRF 实例的名称。</li><li><code>hostname</code>— 输入主机名称。</li><li><code>IP-address   Ipv6-address</code>— 输入主机 IPv4 或 IPv6 地址。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                     |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                           |
| 使用情况信息 | 此命令的 <code>no</code> 版本会从管理或非默认 VRF 实例中移除主机名称。                                                                                                                                                                                                                                                          |
| 示例     | <pre>OS10(config)# ip host vrf management dell 10.1.1.1 or OS10(config)# ip host vrf blue dell 10.1.1.1</pre>                                                                                                                                                                                           |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                                                                                                                                    |

## ip http vrf

为管理或非默认 VRF 实例配置 HTTP 客户端。

|        |                                                                                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip http vrf {management   vrf vrf-name}</code>                                                                                                                                           |
| 参数     | <ul style="list-style-type: none"><li>• <code>management</code> — 输入关键字以配置用于管理 VRF 实例的 HTTP 客户端。</li><li>• <code>vrf vrf-name</code> — 输入关键字，然后输入 VRF 的名称，以便为该非默认 VRF 实例配置 HTTP 客户端。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                            |
| 命令模式   | CONFIGURATION                                                                                                                                                                                  |
| 使用情况信息 | 此命令的 <code>no</code> 版本将从 HTTP 客户端中移除管理 VRF 实例配置。                                                                                                                                              |
| 示例     | <pre>OS10(config)# ip http vrf management OS10(config)# ip http vrf vrf-blue</pre>                                                                                                             |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                           |

## ip name-server vrf

为管理 VRF 实例或非默认 VRF 实例配置 DNS 名称服务器。

|        |                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip name-server vrf {management   vrf-name}</code>                                                                                                                                                      |
| 参数     | <ul style="list-style-type: none"><li>• <code>management</code> — 输入关键字 <code>management</code> 以配置管理 VRF 实例的 DNS 名称服务器。</li><li>• <code>vrf-name</code> — 输入非默认 VRF 实例的名称，以配置该 VRF 实例的 DNS 名称服务器。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                          |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                |
| 使用情况信息 | 此命令的 <code>no</code> 版本将从管理或非默认 VRF 实例移除名称服务器。                                                                                                                                                               |
| 示例     | <pre>OS10(config)# ip name-server vrf management or OS10(config)# ip name-server vrf blue</pre>                                                                                                              |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                                         |

## ip route-import

从另一个 VRF 实例将 IPv4 静态路由导入到 VRF 实例中。

|        |                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>[no] ip route-import route-target</code>                                                                                     |
| 参数     | <ul style="list-style-type: none"><li>• <code>route-target</code> — 输入非默认 VRF 实例的 <code>route-target</code>，从 1 到 65535。</li></ul> |
| 默认     | 未配置                                                                                                                                |
| 命令模式   | VRF CONFIG                                                                                                                         |
| 使用情况信息 | <p>您可以仅导入相对于非默认或默认 VRF 实例的路由。您不能将属于管理 VRF 实例的路由导入另一个 VRF 实例。</p> <p>使用此命令的 <code>no</code> 形式以移除导入的路由。</p>                         |
| 示例     | <pre>OS10(conf-vrf)# ip route-import 1:1 ==&gt; No route-map attached</pre>                                                        |
| 支持的版本  | 10.4.3.0 或更高版本                                                                                                                     |



## ip route-export

将 IPv4 静态路由从一个 VRF 实例导出到另一个实例。

|        |                                                                                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>[no] ip route-export route-target [route-map route-map-name]</code>                                                                                                                   |
| 参数     | <ul style="list-style-type: none"><li>• <code>route-target</code> — 输入 VRF 实例的 <code>route-target</code>。</li><li>• <code>route-map route-map-name</code> — (可选) 输入路由映射名称以指定路由映射。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                         |
| 命令模式   | VRF CONFIG                                                                                                                                                                                  |
| 使用情况信息 | 您可以仅导出与非默认或默认 VRF 实例对应的路由。您不能导出属于管理 VRF 实例的路由。<br>使用此命令的 <code>no</code> 形式撤销配置。                                                                                                            |

### 示例

```
OS10(conf-vrf)# ip route-export 1:1 ==> No route-map attached
OS10(conf-vrf)# ip route-export 1:1 route-map abc ==> Route-map abc
attached to filter export routes
```

支持的版本 10.4.3.0 或更高版本

## ipv6 route-import

从另一个 VRF 实例将 IPv6 静态路由导入到 VRF 实例中。

|        |                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>[no] ipv6 route-import route-target</code>                                                                    |
| 参数     | <ul style="list-style-type: none"><li>• <code>route-target</code> — 输入 VRF 实例的 <code>route-target</code>。</li></ul> |
| 默认     | 未配置                                                                                                                 |
| 命令模式   | VRF CONFIG                                                                                                          |
| 使用情况信息 | 您可以仅导入与非默认或默认 VRF 实例对应的 IPv6 路由。您不能将属于管理 VRF 实例的 IPv6 路由导入到另一个 VRF 实例。<br>使用此命令的 <code>no</code> 形式以移除导入的路由。        |

### 示例

```
OS10(conf-vrf)# ipv6 route-import 1:1 ==> No route-map attached
```

支持的版本 10.4.3.0 或更高版本

## ipv6 route-export

将 IPv6 静态路由从 VRF 实例导出至另一个 VRF 实例。

|        |                                                                                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>[no] ipv6 route-export route-target [route-map route-map-name]</code>                                                                                                                 |
| 参数     | <ul style="list-style-type: none"><li>• <code>route-target</code> — 输入 VRF 实例的 <code>route-target</code>。</li><li>• <code>route-map route-map-name</code> — (可选) 输入路由映射名称以指定路由映射。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                         |
| 命令模式   | VRF CONFIG                                                                                                                                                                                  |
| 使用情况信息 | 您可以仅导出与非默认或默认 VRF 实例对应的 IPv6 路由。您不能将属于管理 VRF 实例的 IPv6 路由导出到另一个 VRF 实例。<br>使用此命令的 <code>no</code> 形式撤销配置。                                                                                    |

### 示例

```
OS10(conf-vrf)# ipv6 route-export 1:1 ==> No route-map attached
OS10(conf-vrf)# ipv6 route-export 1:1 route-map abc ==> Route-map abc
attached to filter export routes
```

**支持的版本** 10.4.3.0 或更高版本

## ip scp vrf

为管理或非默认 VRF 实例配置 SCP 连接。

**语法** `ip scp vrf {management | vrf vrf-name}`

- 参数**
- `management` — 输入关键字以配置管理 VRF 实例的 SCP 连接。
  - `vrf vrf-name` — 输入关键字，然后是 VRF 的名称，以配置该 VRF 实例的 SCP 连接。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本从 SCP 客户端中删除管理 VRF 实例配置。

**示例**

```
OS10(config)# ip scp vrf management
OS10(config)# ip scp vrf vrf-blue
```

**支持的版本** 10.4.0E(R1) or later

## ip sftp vrf

为管理或非默认 VRF 实例配置 SFTP 客户端。

**语法** `ip sftp vrf {management | vrf vrf-name}`

- 参数**
- `management` — 输入关键字以配置用于管理 VRF 实例的 SFTP 客户端。
  - `vrf vrf-name` — 输入关键字，然后输入 VRF 的名称，以便为该非默认 VRF 实例配置 SFTP 客户端。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本从 SFTP 客户端中删除管理 VRF 实例配置。

**示例**

```
OS10(config)# ip sftp vrf management
OS10(config)# ip sftp vrf vrf-blue
```

**支持的版本** 10.4.0E(R1) or later

## ip tftp vrf

为管理或非默认 VRF 实例配置 TFTP 客户端。

**语法** `ip tftp vrf {management | vrf vrf-name}`

- 参数**
- `management` — 输入关键字以配置用于管理 VRF 实例的 TFTP 客户端。
  - `vrf vrf-name` — 输入关键字，然后输入 VRF 的名称，以便为该非默认 VRF 实例配置 TFTP 客户端。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本将从 TFTP 客户端移除管理 VRF 实例配置。

**示例**

```
OS10(config)# ip tftp vrf management
OS10(config)# ip tftp vrf vrf-blue
```

**支持的版本** 10.4.0E(R1) or later

## ip vrf management

配置管理 VRF 实例。

|        |                                                                           |
|--------|---------------------------------------------------------------------------|
| 语法     | ip vrf management                                                         |
| 参数     | 无                                                                         |
| 默认     | 未配置                                                                       |
| 命令模式   | CONFIGURATION                                                             |
| 使用情况信息 | 仅在基于非事务配置模式下输入 ip vrf management 命令。请勿使用基于事务的模式。此命令的 no 版本将移除管理 VRF 实例配置。 |
| 示例     | <pre>OS10(config)# ip vrf management OS10(conf-vrf)#</pre>                |
| 支持的版本  | 10.4.0E(R1) or later                                                      |

## show hosts vrf

显示管理或非默认 VRF 实例中的主机表。

|        |                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show hosts vrf {management   vrf-name}                                                                                                                                                                                                                                                                                                                           |
| 参数     | <ul style="list-style-type: none"><li>management — 输入关键字管理以显示管理 VRF 实例中的主机表。</li><li>vrf-name— 输入要在该 VRF 实例中显示主机表的非默认 VRF 实例的名称。</li></ul>                                                                                                                                                                                                                       |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                              |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                             |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                                                                                |
| 示例     | <pre>OS10# show hosts vrf management Default Domain Name : dell.com Domain List : abc.com xyz.net Name Servers : 10.16.126.1 =====           Static Host to IP mapping Table ===== Host                                     IP-Address ----- google.com                             172.217.160.142 yahoo.com                               98.139.180.180</pre> |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                                                                                                                                                                                             |

## show ip vrf

显示 VRF 实例信息。

|        |                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show ip vrf [management   vrf-name]                                                                                                                    |
| 参数     | <ul style="list-style-type: none"><li>management — 输入关键字 management 以显示与管理 VRF 实例对应的信息。</li><li>vrf-name— 输入要显示与该 VRF 实例对应的信息的非默认 VRF 实例的名称。</li></ul> |
| 默认     | 未配置                                                                                                                                                    |
| 命令模式   | EXEC                                                                                                                                                   |
| 使用情况信息 | 无                                                                                                                                                      |
| 示例     | <pre>OS10# show ip vrf VRF-Name          Interfaces</pre>                                                                                              |

```

default Mgmt1/1/1
 Eth1/1/1-1/1/2
 Vlan1

management

OS10# show ip vrf management
VRF-Name Interfaces
management

```

**支持的版本** 10.4.0E(R1) or later

## update-source-ip

为 VRF 实例中的任何泄露路由配置源 IP 接口。

**语法** `update-source-ip interface interface-id`  
要撤销此配置，请使用 `no update-source-ip` 命令。

**参数** `interface interface-id` — 输入环回接口标识符。范围从 0 到 16383。

**默认** 未配置

**命令模式** VRF CONFIGURATION

**示例**

```
OS10(conf-vrf) # update-source-ip loopback 1
```

**支持的版本** 10.4.2E 或更高版本。

## 双向转发检测

双向转发检测 (BFD) 协议用于快速检测两个相邻路由器之间的通信故障。BFD 将替代现有路由协议中的链路状态检测机制。它还提供了没有路由协议的链路的故障检测解决方案。

BFD 以毫秒而不是秒提供转发路径故障检测。由于 BFD 与路由协议无关，因此它提供了一致的网络故障检测。BFD 消除了多种与协议相关的计时器和方法。网络融合速度更快，因为 BFD 会更快、更一致地触发路由协议中的链路状态变化。

BFD 是一种简单的问候机制。运行 BFD 的两个邻接路由器使用三向握手建立会话。建立会话后，路由器以秒为间隔交换定期控制数据包。如果路由器在指定时间内未收到问候数据包，将会通知路由协议转发路径已关闭。

此外，当会话参数中存在状态更改或更改时，BFD 会发送控制包。这些控制数据包的发送方式与路由协议中的传输和接收间隔无关。

BFD 是一种独立的通用协议，可以使用任何封装来支持所有介质、拓扑和路由协议。OS10 在第 3 层 (L3) 和用户数据报协议 (UDP) 封装实施 BFD。BFD 在静态和动态路由协议（例如 VRRP、OSPF、OSPFv3、IS-IS 和 BGP）上受支持。

系统将显示 BFD 状态更改通知。

 **注：** BFD 不支持边界网关协议 (BGP)。

## BFD 会话状态

要在两个路由器之间建立 BFD 会话，请在该链路的两端启用 BFD。BFD 路由器可以在主动和被动角色中运行。

- 活动路由器将启动 BFD 会话。两个路由器可以在同一个会话中处于活动状态。
- 被动路由器不会启动会话。它只响应来自活动路由器的会话初始化请求。

BFD 会话可以在异步和要求模式下进行。但是，OS10 BFD 仅支持异步模式。

- 在异步模式下，两个系统都以指定的时间间隔发送定期控制消息，以指示其会话状态为 Up。
- 在按需模式下，如果一台路由器请求模式，则其他路由器停止发送定期控制数据包；它只会从需求模式启动器发送对状态查询的响应。两个对等路由器（但不能同时）都可以随时请求模式。

BFD 会话可以有四种状态：Administratively Down、DownInit 和 Up。默认 BFD 会话状态为 Down。

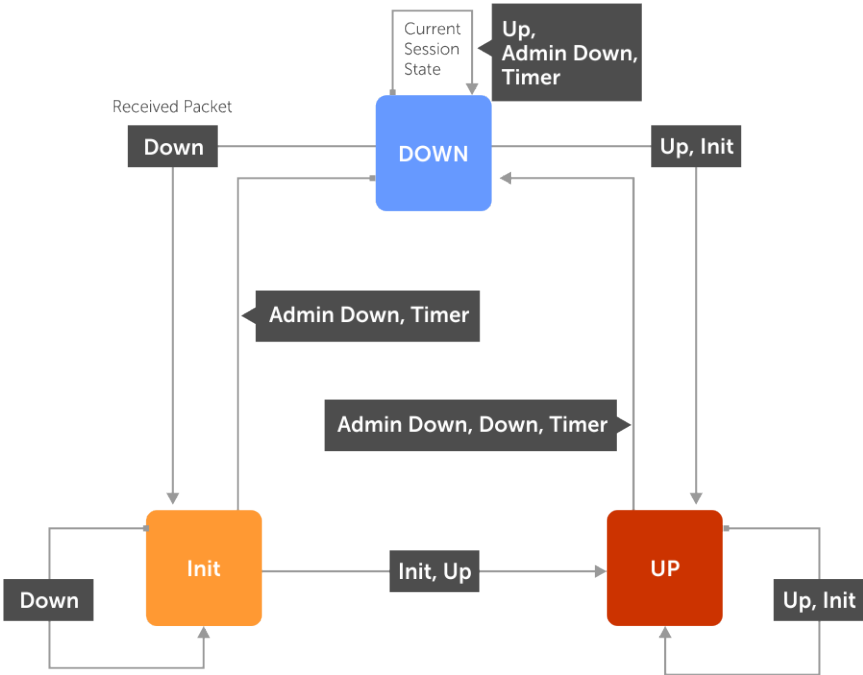
- Administratively Down — 本地 BFD 路由器不参与会话。
- Down — 远程 BFD 路由器未发送控制数据包或不会在会话的检测时间内发送。
- Init — 本地 BFD 外部正在与会话中的远程路由器通信。
- Up — 两个 BFD 路由器都在发送控制数据包。

在以下情况中，BFD 会话的状态更改为 Down：

- 在检测时间内未收到控制数据包。
- 要求模式处于活动状态，并且不会收到控制数据包以响应轮询数据包。

**BFD 会话状态更改示例**

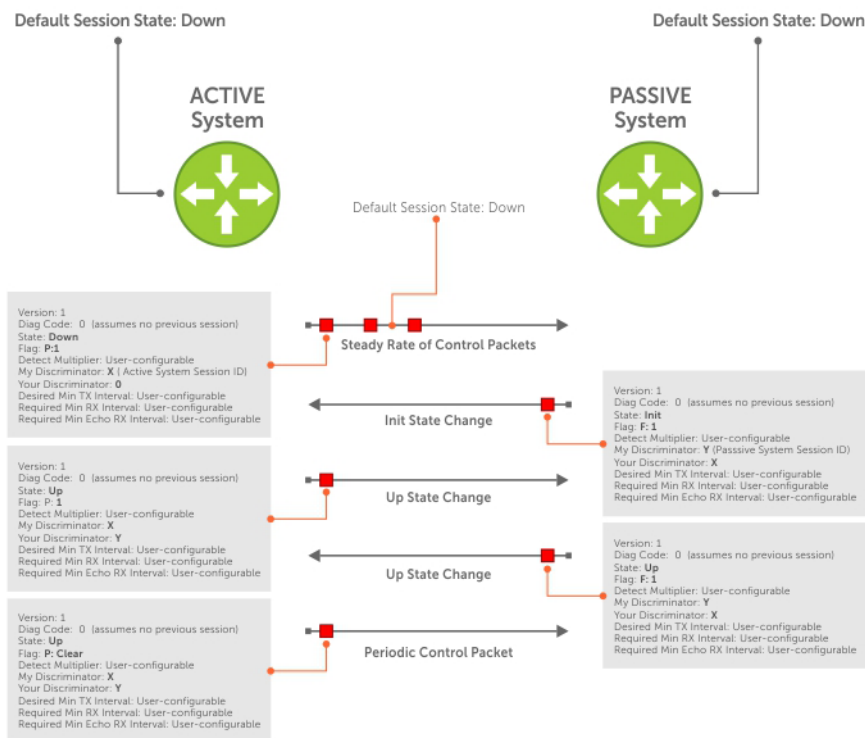
路由器上的会话状态根据其从对等路由器收到的状态通知而更改。例如，如果当前会话状态为 Down，并且路由器收到来自远程路由器的 Down 状态通知，则本地路由器上的会话状态将更改为 Init。



**BFD 三向握手**

BFD 会话需要在相邻路由器之间建立三向握手。在下面的示例中，握手假定：

- 一个路由器处于活动状态，另一个路由器处于被动状态。
  - 这是在此链路上建立的第一个会话。
  - 两个端口上的默认会话状态为 Down。
1. 活动系统将发送控制数据包的稳定流，表明其会话状态为 Down 直至被动系统响应。这些数据包将以活动系统所需的传输间隔发送。此 Your Discriminator 字段设置为零。
  2. 当被动系统收到控制数据包时，它会将其会话状态更改为 Init，并发送响应以指示其状态更改。响应将在 My Discriminator 字段中包含其会话 ID，在 Your Discriminator 字段中包括远程系统的会话 ID。
  3. 活动系统会接收来自被动系统的响应并将其会话状态更改为 Up。然后，它会发送控制数据包，指示此状态更改。鉴别器值将交换并传输间隔协商。
  4. 被动系统接收控制数据包并将其状态更改为 Up。两个系统都同意会话已建立。但是，由于两个成员都必须发送一个控制数据包（需要响应），因此只要会话参数中发生更改或状态更改，则被动系统将发送最终响应，指示状态更改。在此之后，定期控制数据包将交换。



## BFD 配置

在为路由协议配置 BFD 之前，请在链路上的两个路由器上全局启用 BFD。默认情况下，BFD 处于禁用状态。

- OS10 支持：
  - 64 个 BFD 会话，最小 100 次传输和接收间隔，乘数为 4
  - 100 个 BFD 会话，最小 200 次传输和接收间隔，乘数为 3
- OS10 不支持请求模式、身份验证和回显功能。
- OS10 不支持多跳和虚拟链路上的 BFD。
- OS10 仅支持路由协议的协议活动。
- OS10 BFD 仅支持 BGP 路由协议。对于 IPv4 和 IPv6 BGP，OS10 仅支持默认虚拟路由和转发 (VRF)。

## 全局配置 BFD

在为静态路由或路由协议配置 BFD 之前，请在每个路由器上全局配置 BFD，包括全局 BFD 会话设置。默认情况下，BFD 处于禁用状态。

- 在 CONFIGURATION 模式下配置全局 BFD 会话参数。

```
bfd interval milliseconds min_rx milliseconds multiplier number role {active | passive}
```

- `interval milliseconds` — 输入将控制数据包发送到 BFD 对等方的时间间隔，从 100 到 1000。默认值为 200。Dell EMC 建议使用超过 100 毫秒的时间。
- `min_rx milliseconds` — 输入从 BFD 对等方的接收控制数据包的最长等待时间，从 100 到 1000。默认值为 200。Dell EMC 建议使用超过 100 毫秒的时间。
- `multiplier number` — 输入在将会话状态更改为 Down 之前不能从 BFD 对等方收到的连续数据包数，从 3 到 50。默认值为 3。
- `role {active | passive}` — 如果路由器启动 BFD 会话，则输入 active。两个 BFD 对等方可以同时处于活动状态。如果路由器未启动 BFD 会话，并且仅响应来自活动 BFD 的请求以初始化会话，则输入 passive。默认值为 active。

2. 在 CONFIGURATION 模式下，全局启用 BFD。

```
bfd enable
```

要验证 BFD 是否处于全局启用状态，请使用 show running-config bfd 命令。

BFD 全局配置

```
OS10(config)# bfd interval 250 min_rx 300 multiplier 4 role passive
OS10(config)# bfd enable
OS10(config)# do show running-config bfd
!
bfd enable
bfd interval 250 min_rx 300 multiplier 4 role passive
```

查看有关活动 BFD 邻居的信息

```
OS10#show bfd neighbors active
* - Active session role

--
LocalAddr RemoteAddr Interface State RxInt TxInt Mult VRF
Clients

--
* 100.100.1.1 100.100.1.2 ethernet1/1/26:1 up 200 200 3 red ospfv2
* 100.100.3.1 100.100.3.2 ethernet1/1/26:3 up 200 200 3 default ospfv2
* 200.1.1.2 200.1.1.1 vlan102 up 200 200 3 black bgp
* 200.1.5.2 200.1.5.1 vlan105 up 200 200 3 default ospfv2
* 200.1.11.2 200.1.11.1 vlan111 up 200 200 3 green rtmv4
* 200.1.12.2 200.1.12.1 vlan112 up 200 200 3 default rtmv4
* 201.1.1.2 201.1.1.1 vlan101 up 200 200 3 green ospfv2
```

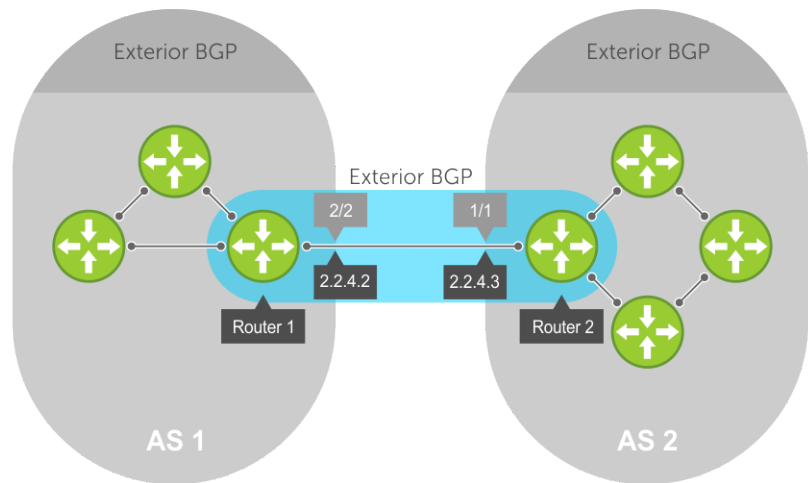
BFD for BGP

在 BGP 核心网络中，BFD 将启用更快的网络重新聚合。BFD 快速检测内部 BGP (iBGP) 与外部 BGP (eBGP) 对等主机之间的 BGP 快速转发路径中的通信故障。BFD for BGP 在物理、端口通道和 VLAN 接口上受支持。BFD for BGP 不支持 BGP 多跳功能。

在配置 BFD for BGP 之前，请先在互连路由器上配置 BGP。有关详细信息，请参阅[边界网关协议](#)。

BFD for BGP 示例

在此 BFD for BGP 配置示例中，路由器 1 和路由器 2 使用传输网络中的 eBGP 以互连 AS1 和 AS2。EBGP 路由器彼此交换信息，并使用 iBGP 路由器来维护每个自治系统中的连接性和可访问性。



当您使用 BGP 邻居配置 BFD 会话时，您可以执行以下操作：

- 使用 `neighbor ip-address` 和 `bfd` 命令与指定的 BGP 邻居建立 BFD 会话。
- 使用 `bfd all-neighbors` 命令与通过 BGP 查找到的所有邻居建立 BFD 会话。

例如：

#### 路由器 1

```
OS10(conf)# bfd enable
OS10(conf)# router bgp 1
OS10(config-router-bgp-1)# neighbor 2.2.4.3
OS10(config-router-neighbor)# bfd
OS10(config-router-neighbor)# no shutdown
OR
OS10(conf)# bfd enable
OS10(conf)# router bgp 1
OS10(config-router-bgp-1)# bfd all-neighbors interval 200 min_rx 200 multiplier 6 role active
```

#### 路由器 2

```
OS10(conf)# bfd enable
OS10(conf)# router bgp 2
OS10(config-router-bgp-2)# neighbor 2.2.4.2
OS10(config-router-neighbor)# bfd
OS10(config-router-neighbor)# no shutdown
OR
OS10(conf)# bfd enable
OS10(conf)# router bgp 2
OS10(config-router-bgp-2)# bfd all-neighbors interval 200 min_rx 200 multiplier 6 role active
```

来自路由器的 BFD 数据包将分配给最高优先级的出口队列，以最大限度减少传输延迟。从 BGP 邻居接收的传入 BFD 控制数据包将分配给控制平面监察 (CoPP) 框架内的最高优先级队列，以避免因队列拥塞而丢弃 BFD 数据包。

BFD 会通知 BGP 其在链路上检测到的任何故障情况。BGP 将启动恢复操作。

BFD for BGP 仅在直接连接的 BGP 邻居上以及 BGP IPv4 和 IPv6 网络中受支持。最多支持 100 个并发 BFD 会话。

如果每个 BFD for BGP 邻居在配置的 BFD 间隔内收到 BFD 控制数据包以进行故障检测，则 BFD 会话将保持正常运行，并且 BGP 会保持其邻接。如果 BFD for BGP 邻居在检测间隔内未收到控制数据包，则路由器会通知 BFD 会话的任何客户端以及有关故障的其他路由协议。然后，它会依赖于使用 BGP 链路的路由协议来确定对故障情况的相应响应。正常响应是通过绕过出现故障的邻居路由器来终止路由协议和重新聚合的对等会话。只要 BFD 检测到故障条件，就会生成一条日志消息。

## 配置 BFD for BGP

OS10 使用默认 VRF 支持 IPv4 或 IPv6 BGP 邻居的 BFD 会话。配置 BFD for BGP 时，您可以使用 BGP 查找到的所有 BGP 邻居或指定的邻居启用 BFD 会话。

1. 在 CONFIGURATION 模式下，配置 BFD 会话参数并在所有接口上全局启用 BFD（如在[全局配置 BFD](#)中所述）。

```
bfd interval milliseconds min_rx milliseconds multiplier number role {active | passive}
bfd enable
```

2. 在 CONFIGURATION 模式下输入远程 BFD 对等节点的 AS 编号，从 1 到 65535 适用于 2 字节 AS 编号，从 1 到 4294967295 适用于 4 字节 AS 编号。每个系统仅支持一个 AS 编号。如果输入一个 4 字节 AS 数字，则 4 字节 AS 支持自动启用。

```
router bgp as-number
```

3. 在 ROUTER-BGP 模式下输入 BFD 对等节点的 IP 地址。在 ROUTER-NEIGHBOR 模式下启用 BFD 会话和 BGP 链路。使用在步骤 1 中配置的全局 BFD 会话参数。

```
neighbor ip-address
 bfd
 no shutdown
```

或



在 ROUTER-BGP 模式下使用 BGP 发现的所有邻居配置 BFD 会话。您配置的 BFD 会话参数将覆盖在步骤 1 中配置的全局会话参数。

```
bfd all-neighbors [interval milliseconds min_rx milliseconds multiplier number role
{active | passive}]
```

- *interval milliseconds* — 输入将控制数据包发送到 BFD 对等方的时间间隔，从 100 到 1000；默认值为 200。Dell EMC 建议使用超过 100 毫秒的时间。
- *min\_rx milliseconds* — 输入从 BFD 对等方接收控制数据包的最长等待时间，从 100 到 1000；默认值为 200。Dell EMC 建议使用超过 100 毫秒的时间。
- *multiplier number* — 输入在将会话状态更改为 Down 之前不能从 BFD 对等方收到的最大连续数据包数；从 3 到 50；默认值为 3。
- *role {active | passive}* — 如果路由器启动 BFD 会话，则输入 active。两个 BFD 对等方可以同时处于活动状态。如果路由器未启动 BFD 会话，并且仅响应来自活动 BFD 的请求以初始化会话，则输入 passive。默认值为 active。

要忽略为指定邻居配置的 `bfd all-neighbors` 设置，请在 ROUTER-NEIGHBOR 模式下输入 `bfd disable` 命令。

或

在 ROUTER-BGP 模式下输入带有邻居名称的 BGP 模板。在 ROUTER-TEMPLATE 模式下使用继承模板的所有邻居配置 BFD 会话。有关如何使用 BGP 模板的详细信息，请参阅[对等模板](#)。使用在步骤 1 中配置的全局 BFD 会话参数。

```
template template-name
 bfd
 no shutdown
```

#### 4. 在 EXEC 模式下验证 BFD for BGP 配置。

```
show bfd neighbors [detail]
```

#### BFD for BGP 所有邻居配置

```
OS10(conf)# bfd interval 200 min_rx 200 multiplier 6 role active
OS10(conf)# bfd enable
OS10(conf)# router bgp 4
OS10(config-router-bgp-4)# bfd all-neighbors interval 200 min_rx 200 multiplier 6 role
active
```

#### BFD for BGP 单邻居配置

```
OS10(conf)# bfd interval 200 min_rx 200 multiplier 6 role active
OS10(conf)# bfd enable
OS10(conf)# router bgp 1
OS10(config-router-bgp-1)# neighbor 150.150.1.1
OS10(config-router-neighbor)# bfd
OS10(config-router-neighbor)# no shutdown
```

#### BFD for BGP 模板配置

```
OS10(config)# router bgp 300
OS10(config-router-bgp-300)# template ebgppg
OS10(config-router-template)# bfd
OS10(config-router-template)# exit
OS10(config-router-bgp-300)# neighbor 3.1.1.1
OS10(config-router-neighbor)# inherit template ebgppg
OS10(config-router-neighbor)# no shutdown
```

#### 显示 BFD 操作

```
OS10# show bfd neighbors
* - Active session role

LocalAddr RemoteAddr Interface State Rx-int Tx-int Mult VRF Clients
```

```

* 150.150.1.2 150.150.1.1 vlan10 up 1000 1000 5 default bgp
```

```
OS10# show bfd neighbors detail
Session Discriminator: 1
Neighbor Discriminator: 2
Local Addr: 150.150.1.2
Local MAC Addr: 90:b1:1c:f4:ab:fd
Remote Addr: 150.150.1.1
Remote MAC Addr: 90:b1:1c:f4:a4:d4
Interface: vlan10
State: up
Configured parameters:
TX: 1000ms, RX: 1000ms, Multiplier: 5
Actual parameters:
TX: 1000ms, RX: 1000ms, Multiplier: 5
Neighbor parameters:
TX: 200ms, RX: 200ms, Multiplier: 49
Role: active
VRF: default
Client Registered: bgp
Uptime: 01:58:09
Statistics:
 Number of packets received from neighbor: 7138
 Number of packets sent to neighbor: 7138
```

## 验证 BFD for BGP

```
OS10(config-router-bgp-101)# show ip bgp summary
BGP router identifier 30.1.1.2 local AS number 101
Global BFD is enabled
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx
20.1.1.1 101 781 777 11:16:13 0
30.1.1.1 101 787 779 11:15:35 0
```

```
OS10(config-router-bgp-101)# show ip bgp neighbors
BGP neighbor is 20.1.1.1, remote AS 101, local AS 101 internal link
```

```
BGP version 4, remote router ID 30.1.1.1
BGP state ESTABLISHED, in this state for 11:19:01
Last read 00:24:31 seconds
Hold time is 180, keepalive interval is 60 seconds
Configured hold time is 180, keepalive interval is 60 seconds
Fall-over disabled
```

### Neighbor is using Global level BFD Configuration

```
Received 784 messages
 1 opens, 0 notifications, 0 updates
 783 keepalives, 0 route refresh requests
Sent 780 messages
 2 opens, 0 notifications, 0 updates
 778 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
Minimum time before advertisements start is 0 seconds
Capabilities received from neighbor for IPv4 Unicast:
 MULTIPROTO_EXT(1)
 ROUTE_REFRESH(2)
 CISCO_ROUTE_REFRESH(128)
 4_OCTET_AS(65)
Capabilities advertised to neighbor for IPv4 Unicast:
 MULTIPROTO_EXT(1)
 ROUTE_REFRESH(2)
 CISCO_ROUTE_REFRESH(128)
 4_OCTET_AS(65)
Prefixes accepted 0, Prefixes advertised 0
Connections established 1; dropped 0
Last reset never
For address family: IPv4 Unicast
 Allow local AS number 0 times in AS-PATH attribute
Prefixes ignored due to:
```

```
Martian address 0, Our own AS in AS-PATH 0
Invalid Nexthop 0, Invalid AS-PATH length 0
Wellknown community 0, Locally originated 0
```

```
Local host: 20.1.1.2, Local port: 179
Foreign host: 20.1.1.1, Foreign port: 58248
```

## BFD for OSPF

您可以将 BFD 配置为监控并通知 OSPF 邻居之间的可访问状态。当您将 BFD 与 OSPF 结合使用时，会在所有参与 OSPF 完全状态的邻接接口之间建立 BFD 会话。如果某个邻接接口出现故障，BFD 会通知 OSPF 协议发生了链路状态变化。

要配置 BFD for OSPF：

1. 全局启用 BFD。
2. 在互连路由器上配置 OSPF。有关详细信息，请参阅[首先打开最短路径（OSPFv2 和 OSPFv3）](#)。

### 全局启用 BFD

要全局启用 BFD：

全局启用 BFD。

```
bfd enable
```

CONFIGURATION 模式

### 与 OSPFv2 邻居建立 BFD 会话

您可以在一个位置与所有 OSPF 邻居建立 BFD 会话。此外，您还可以使用与单个 OSPF 接口相对应的 OSPF 邻居建立 BFD 会话。

要与 OSPFv2 邻居建立 BFD 会话，请执行以下操作：

1. 全局启用 BFD

```
bfd enable
```

CONFIGURATION 模式
2. 进入 ROUTER-OSPF 模式

```
router ospf ospf-instance
```

CONFIGURATION 模式
3. 与所有 OSPFv2 邻居建立会话。

```
bfd all-neighbors
```

ROUTER-OSPF 模式
4. 进入 INTERFACE CONFIGURATION 模式。

```
interface interface-name
```

CONFIGURATION 模式
5. 与单个 OSPF 接口相对应的 OSPFv2 邻居建立 BFD 会话。

```
ip ospf bfd all-neighbors
```

INTERFACE CONFIGURATION 模式

### 在非默认 VRF 实例中与 OSPFv2 邻居建立 BFD 会话

要在非默认 VRF 实例中与 OSPFv2 邻居建立 BFD 会话：

1. 全局启用 BFD

```
bfd enable
```

CONFIGURATION 模式

2. 进入 INTERFACE CONFIGURATION 模式。

```
interface interface-name
CONFIGURATION 模式
```

3. 将非默认 VRF 与所输入的接口相关联。

```
ip vrf forwarding vrf1
INTERFACE CONFIGURATION 模式
```

4. 将一个 IP 地址分配给 VRF。

```
ip address ip-address
VRF CONFIGURATION 模式
```

5. 将接口连接到 OSPF 区域。

```
ip ospf ospf-instance area area-address
VRF CONFIGURATION 模式
```

6. 在非默认 VRF 实例中的单个 OSPF 接口中与 OSPFv2 邻居建立 BFD 会话。

```
ip ospf bfd all-neighbors
VRF CONFIGURATION 模式
```

7. 在非默认 VRF 实例中进入 ROUTER-OSPF 模式。

```
router ospf ospf-instance vrf vrf-name
```

8. 与非默认 VRF 中的所有 OSPFv2 实例建立 BFD 会话。

```
bfd all-neighbors
```

```
OS10# show running-configuration ospf
!
interface vlan200
 no shutdown
 ip vrf forwarding red
 ip address 20.1.1.1/24
 ip ospf 200 area 0.0.0.0
 ip ospf bfd all-neighbors disable
!
interface vlan300
 no shutdown
 ip vrf forwarding red
 ip address 30.1.1.1/24
 ip ospf 200 area 0.0.0.0
!
router ospf 200 vrf red
 bfd all-neighbors
 log-adjacency-changes
 router-id 2.3.3.1
!
```

在此示例中，OSPF 在非默认 VRF 红色中已启用。BFD 在路由器 OSPF 级别已全局启用，并且与此 VRF OSPF 实例关联的所有接口将继承全局 BFD 配置。但是，此全局 BFD 配置不适用于已存在接口级别 BFD 配置的接口。此外，VLAN 200 采用接口级别 BFD 配置，因为接口级别 BFD 配置优先于全局 OSPF 级别 BFD 配置。

## 更改 OSPFv2 BFD 会话参数

使用默认间隔和默认角色来配置 BFD 会话。

可配置的参数包括：所需的传输间隔、要求的最短 rx 间隔、检测倍数和系统角色。为所有 OSPF 会话或特定接口上的所有 OSPF 会话配置这些参数。如果全局更改参数，则更改将影响所有 OSPF 邻居会话。如果在接口级别更改参数，则更改将影响该接口上的所有 OSPF 会话。

 **注：**默认情况下，OSPF 对其邻居使用以下 BFD 参数：min\_tx = 200 msec、min\_rx = 200 msec、multiplier = 3、role = active。如果在接口上下文中配置了 BFD，将获得高优先级。

要更改单个接口上所有 OSPFv2 会话或 OSPF 会话的参数，请使用以下命令：

1. 更改 OSPF 会话的参数。

```
bfd all-neighbors interval milliseconds min_rx milliseconds multiplier value role [active
| passive]
```

ROUTER-OSPF 模式

2. 更改接口上所有 OSPF 会话的参数。

```
ip ospf bfd all-neighbors interval milliseconds min_rx milliseconds multiplier value role
[active | passive]
```

INTERFACE CONFIGURATION 模式

## 禁用 BFD for OSPFv2

如果您在全局范围内禁用 BFD，所有会话都会断开，并且远程系统上的会话将处于“关闭”状态。如果禁用某个接口上的 BFD，该接口上的会话将断开，远程系统上的会话将处于“关闭”状态。禁用 BFD 不会触发 BFD 客户端更改；在会话终止之前将发送最终的 Admin Down 数据包。

要禁用 BFD 会话，请使用以下命令：

1. 禁用所有 OSPF 邻居的 BFD 会话。

```
no bfd all-neighbors
```

ROUTER-OSPF 模式

2. 使用以下命令在接口级别禁用 OSPFv2：

```
ip ospf bfd all-neighbors disable
```

INTERFACE CONFIGURATION 模式

要重新启用 BFD，请使用以下命令单独禁用接口：

- no ip ospf bfd all-neighbors command
- ip ospf bfd all-neighbors

## 配置 BFD for OSPFv3

BFD for OSPFv3 提供对 IPv6 的支持：

1. 全局启用 BFD。
2. 与 OSPFv3 邻居建立会话。

### 与 OSPFv3 邻居建立 BFD 会话

要与 OSPFv3 邻居建立 BFD 会话，请执行以下操作：

1. 全局启用 BFD

```
bfd enable
```

CONFIGURATION 模式

2. 进入 ROUTER-OSPF 模式

```
router ospfv3 ospfv3-instance
```

CONFIGURATION

3. 与所有 OSPFv3 邻居建立会话。

```
bfd all-neighbors
```

ROUTER-OSPFv3 模式

4. 进入 INTERFACE CONFIGURATION 模式。

```
interface interface-name
```

CONFIGURATION 模式

5. 与单个 OSPF 接口相对应的 OSPFv3 邻居建立 BFD 会话。

```
ipv6 ospf bfd all-neighbors
```

INTERFACE CONFIGURATION 模式

## 在非默认 VRF 实例中与 OSPFv3 邻居建立 BFD 会话

要在非默认 VRF 实例中与 OSPFv3 邻居建立 BFD 会话：

1. 全局启用 BFD  
`bfd enable`  
CONFIGURATION 模式
2. 进入 INTERFACE CONFIGURATION 模式。  
`interface interface-name`  
CONFIGURATION 模式
3. 将非默认 VRF 与所输入的接口相关联。  
`ip vrf forwarding vrf1`  
INTERFACE CONFIGURATION 模式
4. 将一个 IP 地址分配给 VRF。  
`ip address ip-address`  
VRF CONFIGURATION 模式
5. 将接口连接到 OSPF 区域。  
`ipv6 ospf ospf-instance area area-address`  
VRF CONFIGURATION 模式
6. 在非默认 VRF 实例中的单个 OSPF 接口中建立与 OSPFv3 邻居的 BFD 会话。  
`ipv6 ospf bfd all-neighbors`  
VRF CONFIGURATION 模式
7. 在非默认 VRF 实例中进入 ROUTER-OSPF 模式。  
`router ospf ospf-instance vrf vrf-name`  
CONFIGURATION 模式
8. 与非默认 VRF 中的所有 OSPFv2 实例建立 BFD 会话。  
`bfd all-neighbors`

## 更改 OSPFv3 会话参数

使用默认间隔和默认角色来配置 BFD 会话。

可配置的参数包括：所需的传输间隔、要求的最短 rx 间隔、检测倍数和系统角色。为所有 OSPFv3 会话或特定接口上的所有 OSPFv3 会话配置这些参数。如果全局更改参数，则更改将影响所有 OSPFv3 邻居会话。如果在接口级别更改参数，则更改将影响该接口上的所有 OSPF 会话。

**注：**默认情况下，OSPF 对其邻居使用以下 BFD 参数：min\_tx = 200 msec、min\_rx = 200 msec、multiplier = 3、role = active。如果在接口上下文中配置了 BFD，将获得高优先级。

要更改单个接口上所有 OSPFv3 会话或 OSPF 会话的参数，请使用以下命令：

1. 更改 OSPF 会话的参数。  
`bfd all-neighbors interval milliseconds min_rx milliseconds multiplier value role [active | passive]`  
ROUTER-OSPFv3 模式
2. 更改接口上所有 OSPF 会话的参数。  
`ipv6 ospf bfd all-neighbors interval milliseconds min_rx milliseconds multiplier value role [active | passive]`  
INTERFACE CONFIGURATION 模式

## 禁用 BFD for OSPFv3

如果您在全局范围内禁用 BFD，所有会话都会断开，并且远程系统上的会话将处于“关闭”状态。如果禁用某个接口上的 BFD，该接口上的会话将断开，远程系统上的会话将处于“关闭”状态。禁用 BFD 不会触发 BFD 客户端更改；在会话终止之前将发送最终的 Admin Down 数据包。

要禁用 BFD 会话，请使用以下命令：

1. 禁用所有 OSPF 邻居的 BFD 会话。

```
no bfd all-neighbors
```

ROUTER-OSPFv3 模式

2. 在接口上禁用所有 OSPF 邻居的 BFD 会话。

```
ipv6 ospf bfd all-neighbors disable
```

INTERFACE CONFIGURATION 模式

要重新启用 BFD，请使用以下命令单独禁用接口：

- no ipv6 ospf bfd all-neighbors command
- ipv6 ospf bfd all-neighbors

## 适用于静态路由的 BFD

静态路由 BFD 功能支持将静态路由与 BFD 会话关联，以监控静态路由可访问性。根据 BFD 会话的状态，静态路由将添加到路由信息库 (RIB) 或从中删除。配置 BFD 时，下一跳可访问性取决于与指定的下一跳对应的 BFD 会话的 BFD 状态。如果配置的下一跳的 BFD 会话关闭，则 RIB 中不会安装静态路由。

对于静态路由，BFD 会话必须处于正常运行。您必须在两个对等节点上配置 BFD，并将其作为下一跳。静态路由和 BFD 配置的配置顺序没有依赖关系。您可以为所有静态路由或不为任何静态路由配置 BFD。对于 IPv4 和 IPv6 静态路由，OS10 均支持 BFD。

 **注：**您可以为所有静态路由配置 BFD。这意味着，没有某些静态路由配置 BFD 的配置。

## 为所有静态路由启用 BFD

为静态路由配置 BFD 是一个三步过程：

1. 全局启用 BFD。
2. 在系统上的两个路由器上配置静态路由（本地或远程）。以下一跳接口相互指向的方式配置静态路由。
3. 使用 `ip route bfd` 命令为静态路由配置 BFD。

## 为 IPv4 静态路由建立 BFD 会话

为静态路由的下一跳建立会话。

要终止 BFD 会话，请使用以下命令。

为处于静态路由的下一跳的所有邻居建立 BFD 会话。

```
ip route bfd [interval interval min_rx min_rx multiplier value role {active | passive}]
```

CONFIGURATION 模式

输入发送和接收 BFD 控制数据包的时间间隔；从 100 到 1000。

## 为非默认 VRF 实例中的 IPv4 静态路由建立 BFD 会话

要在非默认 VRF 实例中为 IPv4 静态路由建立 BFD 会话，请使用以下命令。

为处于静态路由的下一跳的所有邻居建立 BFD 会话。

```
ip route bfd [vrf vrf-name] [interval interval min_rx min_rx multiplier value role {active | passive}]
```

CONFIGURATION 模式

输入发送和接收 BFD 控制数据包的时间间隔；从 100 到 1000。

## 更改 IPv4 静态路由会话参数

使用默认间隔和默认角色来配置 BFD 会话。

为所有静态路由配置以下各项：

- 所需的 TX 间隔
- 所需的最小 RX 间隔
- 检测乘数
- 系统角色

为所有静态路由配置这些参数。如果您更改参数，更改将影响静态路由的所有会话。要更改静态路由会话的参数，请使用以下命令。

- 在 CONFIGURATION 模式下更改所有静态路由会话的参数。

```
ip route bfd interval milliseconds min_rx milliseconds multiplier value role [active | passive]
```

输入发送和接收 BFD 控制数据包的时间间隔；从 100 到 1000。

 **注：**默认情况下，OSPF 对其邻居使用以下 BFD 参数：min\_tx = 200 msec、min\_rx = 200 msec、multiplier = 3、role = active。

## 禁用适用于 IPv4 静态路由的 BFD

如果禁用 BFD，所有静态路由 BFD 会话都会被分解。

最终的 Admin Down 数据包将发送至远程系统上的所有邻居，并且这些邻居将变为关闭状态。要禁用适用于 IPv4 静态路由的 BFD，请使用以下命令。

禁用适用于静态路由的 BFD。

```
no ip route bfd
```

CONFIGURATION 模式

## 为 IPv6 静态路由建立 BFD 会话

要为 IPv6 静态路由建立 BFD 会话，请使用以下命令。

为处于静态路由的下一跳的所有邻居建立 BFD 会话。

```
ipv6 route bfd [interval interval min_rx min_rx multiplier value role {active | passive}]
```

CONFIGURATION 模式

输入发送和接收 BFD 控制数据包的时间间隔；从 100 到 1000。

 **注：**默认情况下，OSPF 对其邻居使用以下 BFD 参数：min\_tx = 200 msec、min\_rx = 200 msec、multiplier = 3、role = active。这些值以毫秒为单位进行配置

## 为非默认 VRF 实例中的 IPv6 静态路由建立 BFD 会话

要为非默认 VRF 实例中的 IPv6 静态路由建立 BFD 会话，请使用以下命令。

为处于静态路由的下一跳的所有邻居建立 BFD 会话。

```
ipv6 route bfd [vrf vrf-name] [interval interval min_rx min_rx multiplier value role {active | passive}]
```

CONFIGURATION 模式

输入发送和接收 BFD 控制数据包的时间间隔；从 100 到 1000。

 **注：**默认情况下，OSPF 对其邻居使用以下 BFD 参数：min\_tx = 200 msec、min\_rx = 200 msec、multiplier = 3、role = active。这些值以毫秒为单位进行配置



# 更改 IPv6 静态路由会话参数

要更改 IPv6 静态路由会话的参数，请执行以下操作：

- 在 CONFIGURATION 模式下更改所有静态路由会话的参数。  
`ipv6 route bfd interval milliseconds min_rx milliseconds multiplier value role [active | passive]`  
输入发送和接收 BFD 控制数据包的时间间隔；从 100 到 1000。

 **注：**默认情况下，OSPF 对其邻居使用以下 BFD 参数：min\_tx = 200 msec、min\_rx = 200 msec、multiplier = 3、role = active。

# 禁用适用于 IPv6 静态路由的 BFD

要禁用适用于 IPv6 静态路由的 BFD，请使用以下命令。

禁用适用于静态路由的 BFD。

```
no ipv6 route bfd
CONFIGURATION 模式
```

# BFD 命令

## bfd

启用具有指定邻居的 BFD 会话。

|      |                                    |
|------|------------------------------------|
| 语法   | bfd                                |
| 参数   | 无                                  |
| 默认   | 未配置                                |
| 命令模式 | ROUTER-NEIGHBOR<br>ROUTER-TEMPLATE |

- 使用情况信息**
- 使用 bfd 命令可配置 BFD 会话，其中包含指定的邻居或继承 BGP 模板的邻居。在 ROUTER-BGP 模式下使用 `neighbor {ip-address | ipv6-address}` BGP 命令指定邻居。在 ROUTER-BGP 模式下使用 `template template-name` 命令指定 BGP 模板。在 ROUTER-NEIGHBOR 模式下使用 `no bfd` 命令禁用邻居的 BGP 会话。
  - 使用 `bfd all-neighbors` 命令为查找到的邻居之间的所有 BFD 会话配置 L3 协议特定的 BFD 参数。您配置的 BFD 参数将覆盖使用 `bfd interval` 命令配置的全局会话参数。

## 示例

```
OS10(conf)# router bgp 1
OS10(config-router-bgp-1)# neighbor 10.1.1.1
OS10(config-router-neighbor)# bfd
OS10(config-router-neighbor)# no shutdown

OS10(config)# router bgp 300
OS10(config-router-bgp-300)# template ebgpbg
OS10(config-router-template)# bfd
OS10(config-router-template)# exit
OS10(config-router-bgp-300)# neighbor 3.1.1.1
OS10(config-router-neighbor)# inherit template ebgpbg
OS10(config-router-neighbor)# no shutdown
```

**支持的版本** 10.4.1.0 or later

## bfd all-neighbors

配置由 L3 协议查找到的邻居之间建立的所有 BFD 会话参数。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>bfd all-neighbors [milliseconds min_rx milliseconds multiplier number role {active   passive}]</code>                                                                                                                                                                                                                                                                                                                                                                                                          |
| 参数     | <ul style="list-style-type: none"><li><code>interval milliseconds</code> — 输入将控制数据包发送到 BFD 对等节点的时间间隔，从 100 到 1000。Dell EMC 建议使用超过 100 毫秒的时间。</li><li><code>min_rx milliseconds</code> — 输入从 BFD 对等方的接收控制数据包的最长等待时间，从 100 到 1000。Dell EMC 建议使用超过 100 毫秒的时间。</li><li><code>multiplier number</code> — 输入在将会话状态更改为 Down 之前不能从 BFD 对等方收到的最大连续数据包数，从 3 到 50。</li><li><code>role {active   passive}</code> — 如果路由器启动 BFD 会话，则输入 active。两个 BFD 对等方可以同时处于活动状态。如果路由器未启动 BFD 会话，并且仅响应来自活动 BFD 的请求以初始化会话，则输入 passive。</li></ul> |
| 默认     | 将控制数据包发送到 BFD 对等方的时间间隔为 200 毫秒。<br>接收来自 BFD 对等方的控制数据包的最长等待时间为 200 毫秒。<br>必须从 BFD 对等方收到的连续数据包数为 3。<br>BFD 角色为 active                                                                                                                                                                                                                                                                                                                                                                                                  |
| 命令模式   | ROUTER-OSPF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | <ul style="list-style-type: none"><li>使用 <code>bfd all-neighbors</code> 命令可配置查找到的邻居之间的 BFD 会话。您配置的 BFD 会话参数将覆盖使用 <code>bfd interval</code> 命令配置的全局会话参数。要禁用 BFD 并忽略为指定邻居配置的 <code>bfd all-neighbors</code> 设置，请在 ROUTER-NEIGHBOR 模式下输入 <code>bfd disable</code> 命令。</li><li>要移除所有 BGP 邻居已配置的全邻居设置，请输入该命令的 <code>no</code> 版本。要返回默认值，请输入 <code>bfd all-neighbors</code> 命令。</li></ul>                                                                                                                                  |
| 示例     | <pre>OS10(conf-ospf-bgp)# bfd all-neighbors interval 250 min_rx 300 multiplier 4 role passive</pre>                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 支持的版本  | 10.4.1.0 or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## bfd disable

忽略为指定的邻居配置的 `bfd all-neighbors` 设置并禁用 BFD。

|        |                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>bfd disable</code>                                                                                                   |
| 参数     | 无                                                                                                                          |
| 默认     | 未配置                                                                                                                        |
| 命令模式   | ROUTER-NEIGHBOR                                                                                                            |
| 使用情况信息 | 在 ROUTER-BGP 模式下使用 <code>neighbor ip-address BGP</code> 命令指定邻居。使用 <code>bfd disable</code> 命令禁用与邻居的 BFD 会话。                |
| 示例     | <pre>OS10(conf)# router bgp 1 OS10(config-router-bgp-1)# neighbor 10.1.1.1 OS10(config-router-neighbor)# bfd disable</pre> |
| 支持的版本  | 10.4.1.0 or later                                                                                                          |

## bfd enable

在交换机上的所有接口上启用 BFD。

|    |                         |
|----|-------------------------|
| 语法 | <code>bfd enable</code> |
|----|-------------------------|

|        |                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------|
| 参数     | 无                                                                                                 |
| 默认     | BFD 已禁用。                                                                                          |
| 命令模式   | CONFIGURATION                                                                                     |
| 使用情况信息 | 在为静态路由或路由协议配置 BFD 之前，请在 BFD 会话中的每个路由器上全局启用 BFD。要全局禁用所有接口上的 BFD，请输入 <code>no bfd enable</code> 命令。 |
| 示例     | <pre>OS10(config)# bfd enable</pre>                                                               |
| 支持的版本  | 10.4.1.0 or later                                                                                 |

## bfd interval

为交换机上的所有 BFD 会话配置参数。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>bfd interval milliseconds min_rx milliseconds multiplier number role {active   passive}</code>                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 参数     | <ul style="list-style-type: none"> <li><code>interval milliseconds</code> — 输入将控制数据包发送到 BFD 对等方的时间间隔，从 100 到 1000。Dell EMC 建议使用超过 100 毫秒的时间。</li> <li><code>min_rx milliseconds</code> — 输入从 BFD 对等方的接收控制数据包的最长等待时间，从 100 到 1000。Dell EMC 建议使用超过 100 毫秒的时间。</li> <li><code>multiplier number</code> — 输入在将会话状态更改为 Down 之前可能从 BFD 对等方丢失的连续数据包数，从 3 到 50。</li> <li><code>role {active   passive}</code> — 如果路由器启动 BFD 会话，则输入 <code>active</code>。两个 BFD 对等方可以同时处于活动状态。如果路由器未启动 BFD 会话，并且仅响应来自活动 BFD 的请求以初始化会话，则输入 <code>passive</code>。</li> </ul> |
| 默认     | <p>将控制数据包发送到 BFD 对等方的时间间隔为 200 毫秒。</p> <p>接收来自 BFD 对等方的控制数据包的最长等待时间为 200 毫秒。</p> <p>必须从 BFD 对等方收到的连续数据包数为 3。</p> <p>BFD 角色为 <code>active</code>。</p>                                                                                                                                                                                                                                                                                                                                                                                             |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 使用情况信息 | 使用此命令可配置全局 BFD 会话设置。要配置在使用由 L3 协议查找到的邻居中建立的会话中使用的 BFD 参数，请使用 <code>bfd all-neighbors</code> 命令。此命令的任何版本都不会删除已配置的全局设备并返回默认值。                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 示例     | <pre>OS10(config)# bfd interval 250 min_rx 300 multiplier 4 role passive</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 支持的版本  | 10.4.1.0 or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## ip ospf bfd all-neighbors

为此接口中的所有 OSPFv2 邻居启用和配置默认 BFD 参数。

|    |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>ip ospf bfd all-neighbors [disable][interval millisec min_rx min_rx multiplier role {active   passive}]</code>                                                                                                                                                                                                                                                                                                 |
| 参数 | <ul style="list-style-type: none"> <li><code>disable</code> — 只禁用接口上的 BFD 会话。</li> <li><code>interval milliseconds</code> — 输入将控制数据包发送到 BFD 对等方的时间间隔，从 100 到 1000。Dell EMC 建议使用超过 100 毫秒的时间。</li> <li><code>min_rx milliseconds</code> — 输入从 BFD 对等方的接收控制数据包的最长等待时间，从 100 到 1000。Dell EMC 建议使用超过 100 毫秒的时间。</li> <li><code>multiplier number</code> — 输入在将会话状态更改为 Down 之前不能从 BFD 对等方收到的最大连续数据包数，从 3 到 50。</li> </ul> |

- `role {active | passive}` — 如果路由器启动 BFD 会话，则输入 `active`。两个 BFD 对等方可以同时处于活动状态。如果路由器未启动 BFD 会话，并且仅响应来自活动 BFD 的请求以初始化会话，则输入 `passive`。

#### 默认

将控制数据包发送到 BFD 对等方的时间间隔为 200 毫秒。

接收来自 BFD 对等方的控制数据包的最长等待时间为 200 毫秒。

必须从 BFD 对等方收到的连续数据包数为 3。

BFD 角色为 `active`

#### 命令模式

CONFIG-INTERFACE

#### 使用情况信息

- 此命令可用于为与 OSPFv2 关联的接口启用或禁用 BFD。接口级别 BFD 配置优先于 OSPF 全局级别 BFD 配置。如果接口级别全局 OSPF 不存在 BFD 配置，则将继承 BFD 配置。

#### 示例

```
(conf-if-eth1/1/1)#ip ospf bfd all-neighbors
```

#### 支持的版本

10.4.2E 或更高版本

## ipv6 ospf bfd all-neighbors

为此接口中的所有 OSPFv3 邻居启用和配置默认 BFD 参数。

#### 语法

```
ipv6 ospf bfd all-neighbors [disable][interval millisec min_rx min_rx
multiplier role {active | passive}]
```

使用 `no ipv6 ospf bfd all-neighbors` 为所有 OSPFv3 邻居禁用默认 BFD 参数。

#### 参数

- `disable` — 只禁用接口上的 BFD 会话。
- `interval milliseconds` — 输入将控制数据包发送到 BFD 对等方的时间间隔，从 100 到 1000。您不能配置小于 100 毫秒的值。
- `min_rx milliseconds` — 输入从 BFD 对等方的接收控制数据包的最长等待时间，从 100 到 1000。Dell EMC 建议使用超过 100 毫秒的时间。
- `multiplier number` — 输入在将会话状态更改为 Down 之前不能从 BFD 对等方收到的最大连续数据包数，从 3 到 50。
- `role {active | passive}` — 如果路由器启动 BFD 会话，则输入 `active`。两个 BFD 对等方可以同时处于活动状态。如果路由器未启动 BFD 会话，并且仅响应来自活动 BFD 的请求以初始化会话，则输入 `passive`。

#### 默认

将控制数据包发送到 BFD 对等方的时间间隔为 200 毫秒。

接收来自 BFD 对等方的控制数据包的最长等待时间为 200 毫秒。

必须从 BFD 对等方收到的连续数据包数为 3。

BFD 角色为 `active`

#### 命令模式

CONFIG-INTERFACE

#### 使用情况信息

- 此命令可用于为与 OSPFv3 关联的接口启用或禁用 BFD。接口级别 BFD 配置优先于 OSPF 全局级别 BFD 配置。如果接口级别全局 OSPF 不存在 BFD 配置，则将继承 BFD 配置。支持所有类型的接口。

#### 示例

```
(conf-if-eth1/1/1)#ipv6 ospf bfd all-neighbors
```

#### 支持的版本

10.4.2E 或更高版本

## ip route bfd

启用或禁用静态路由上的 BFD。

#### 语法

```
ip route bfd [vrf vrf-name] [interval interval min_rx wait-time multiplier
number role {active | passive}]
```

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 参数     | <ul style="list-style-type: none"> <li><code>vrf vrf-name</code> — 输入 <code>vrf</code> 和 VRF 的名称, 以在该 VRF 中配置静态路由。</li> <li><code>interval milliseconds</code> — 输入将控制数据包发送到 BFD 对等方的时间间隔, 从 100 到 1000。Dell EMC 建议使用超过 100 毫秒的时间。</li> <li><code>min_rx milliseconds</code> — 输入从 BFD 对等方的接收控制数据包的最短等待时间, 从 100 到 1000。Dell EMC 建议使用超过 100 毫秒的时间。</li> <li><code>multiplier number</code> — 输入在将会话状态更改为 Down 之前不能从 BFD 对等方收到的最大连续数据包数; 从 3 到 50。</li> <li><code>role {active   passive}</code> — 如果路由器启动 BFD 会话, 则输入 <code>active</code>。两个 BFD 对等方可以同时处于活动状态。如果路由器未启动 BFD 会话, 并且仅响应来自活动 BFD 的请求以初始化会话, 则输入 <code>passive</code>。</li> </ul> |
| 默认     | <p>将控制数据包发送到 BFD 对等方的时间间隔为 200 毫秒。</p> <p>接收来自 BFD 对等方的控制数据包的最长等待时间为 200 毫秒。</p> <p>必须从 BFD 对等方收到的连续数据包数为 3。</p> <p>BFD 角色为 <code>active</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 命令模式   | CONFIG                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 使用情况信息 | <p>使用此命令可以为指定的 VRF 的所有已配置 IPv4 静态路由启用或禁用 BFD。如果未指定 VRF 名称, 则该命令适用于默认 VRF。</p> <p>此命令的版本可以禁用静态路由上的 BFD。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 示例     | <pre>OS10(config)# ip route bfd interval 250 min_rx 250 multiplier 4 role active</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 支持的版本  | 10.4.2E 或更高版本                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## ipv6 route bfd

启用或禁用 IPv6 静态路由上的 BFD。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ipv6 route bfd [vrf vrf-name] [interval millisec min_rx min_rx multiplier role {active   passive}]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"> <li><code>vrf vrf-name</code> — 输入关键字 VRF, 然后键入 VRF 名称, 以在该 VRF 中配置静态路由。</li> <li><code>interval milliseconds</code> — 输入将控制数据包发送到 BFD 对等方的时间间隔, 从 100 到 1000。</li> <li><code>min_rx milliseconds</code> — 输入从 BFD 对等方的接收控制数据包的最长等待时间, 从 100 到 1000。Dell EMC 建议使用超过 100 毫秒的时间。</li> <li><code>multiplier number</code> — 输入在将会话状态更改为 Down 之前不能从 BFD 对等方收到的最大连续数据包数, 从 3 到 50。</li> <li><code>role {active   passive}</code> — 如果路由器启动 BFD 会话, 则输入 <code>active</code>。两个 BFD 对等方可以同时处于活动状态。如果路由器未启动 BFD 会话, 并且仅响应来自活动 BFD 的请求以初始化会话, 则输入 <code>passive</code>。</li> </ul> |
| 默认     | <p>将控制数据包发送到 BFD 对等方的时间间隔为 200 毫秒。</p> <p>接收来自 BFD 对等方的控制数据包的最长等待时间为 200 毫秒。</p> <p>必须从 BFD 对等方收到的连续数据包数为 3。</p> <p>BFD 角色为 <code>active</code>。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 命令模式   | CONFIG                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 使用情况信息 | <ul style="list-style-type: none"> <li>使用此命令可以为指定的 VRF 的所有已配置 IPv6 静态路由启用或禁用 BFD。如果未指定 VRF 名称, 则该命令适用于默认 VRF。</li> </ul> <p>此命令的版本可以禁用 IPv6 静态路由上的 BFD。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 示例     | <pre>OS10(config)# ipv6 route bfd interval 250 min_rx 250 multiplier 4 role active</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

支持的版本10.4.2E 或更高版本

show bfd neighbors

显示有关使用默认 VRF 的所有接口的 BFD 邻居的信息。

- 语法
- show bfd neighbors [detail | interface]
- 参数
- detail — (可选) 查看有关 BFD 邻居的详细信息。
  - active — (可选) 查看有关其状态为“正常运行”的活动 BFD 邻居的信息。
  - interface interface-type — (可选) 输入以下接口类型之一：
    - ethernet node/slot/port[:subport] — 显示以太网接口信息。
    - port-channel id-number — 显示端口通道接口 ID, 从 1 到 128。
    - vlan vlan-id — 显示 VLAN 接口编号, 从 1 到 4093。

默认未配置

命令模式EXEC

使用情况信息使用此命令验证相邻的 BFD 会话是否使用默认的 VRF 实例。使用 detail 参数可查看 BFD 会话参数。

示例

```
OS10# show bfd neighbors
* - Active session role
```

| LocalAddr     | RemoteAddr  | Interface        | State | RxInt | TxInt | Mult | VRF |
|---------------|-------------|------------------|-------|-------|-------|------|-----|
| * 100.100.1.1 | 100.100.1.2 | ethernet1/1/26:1 | up    | 200   | 200   | 3    | re  |
| * 100.100.3.1 | 100.100.3.2 | ethernet1/1/26:3 | up    | 200   | 200   | 3    | de  |
| * 200.1.1.2   | 200.1.1.1   | vlan102          | up    | 200   | 200   | 3    | bl  |
| * 200.1.5.2   | 200.1.5.1   | vlan105          | up    | 200   | 200   | 3    | de  |
| * 200.1.11.2  | 200.1.11.1  | vlan111          | up    | 200   | 200   | 3    | gr  |
| * 200.1.12.2  | 200.1.12.1  | vlan112          | up    | 200   | 200   | 3    | de  |
| * 201.1.1.2   | 201.1.1.1   | vlan101          | up    | 200   | 200   | 3    | gr  |
| * 201.1.1.2   | 201.1.1.1   | vlan301          | down  | 1000  | 1000  | 3    | de  |
| * 201.1.2.2   | 201.1.2.1   | vlan302          | down  | 1000  | 1000  | 3    | de  |
| * 201.1.3.2   | 201.1.3.1   | vlan303          | down  | 1000  | 1000  | 3    | de  |
| * 201.1.4.2   | 201.1.4.1   | vlan304          | down  | 1000  | 1000  | 3    | de  |
| * 201.1.5.2   | 201.1.5.1   | vlan305          | down  | 1000  | 1000  | 3    | de  |
| * 201.1.6.2   | 201.1.6.1   | vlan306          | down  | 1000  | 1000  | 3    | de  |

```
OS10# show bfd neighbors detail
Session Discriminator: 1
Neighbor Discriminator: 2
Local Addr: 150.150.1.2
Local MAC Addr: 90:b1:1c:f4:ab:fd
Remote Addr: 150.150.1.1
Remote MAC Addr: 90:b1:1c:f4:a4:d4
Interface: vlan10
State: up
Configured parameters:
TX: 1000ms, RX: 1000ms, Multiplier: 5
Actual parameters:
TX: 1000ms, RX: 1000ms, Multiplier: 5
Neighbor parameters:
TX: 200ms, RX: 200ms, Multiplier: 49
Role: active
VRF: default
Client Registered: bgp
Uptime: 01:58:09
Statistics:
 Number of packets received from neighbor: 7138
 Number of packets sent to neighbor: 7138
```

支持的版本10.4.1.0 or later



# 边界网关协议

边界网关协议 (BGP) 是一种自治系统路由协议，用于在自治系统 (AS) 之间传输非域间路由信息。BGP 与其他 BGP 系统交换网络可访问性信息。BGP 通过使用从一个路由器到另一个路由器的多个路径，增加了网络连接的可靠性。与大多数路由协议不同，BGP 使用 TCP 作为其传输协议。

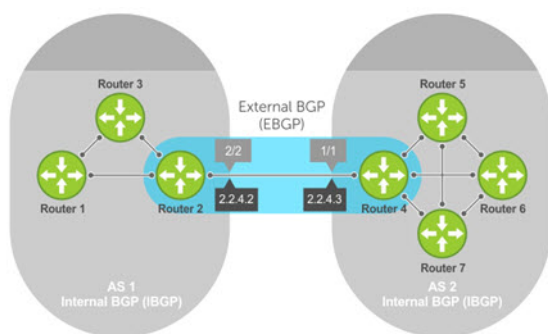
## 自治系统

BGP 自治系统是使用共享网络路由策略的单一管理下的节点集合。每个 AS 都有一个编号 (互联网机构分配) — 您不会分配 BGP 编号。

互联网分配的编号机构 (IANA) 将每个网络标识为唯一的编号 (ASN)。AS 编号 64512 至 65534 将保留用于私有。在实时环境中不能使用数字 0 和 65535。IANA 分配介于 1 和 64511 范围内的 AS 编号。

- 多主机 AS** 维护到多个 AS 的连接。一个连接发生完整故障时，此组允许 AS 保持到互联网的连接。这种类型的 AS 不允许流量从一个 AS 传递到另一个 AS。
- 存根 AS** 仅连接一个 AS。
- 运输 AS** 为单独的网络提供连接。例如，路由器 1 使用路由器 2 (传输 AS) 以连接到路由器 4。互联网服务提供商 (ISP) 始终是传输 AS，因为它们提供从一个网络到另一个网络的连接。ISP 使用传输 AS 来向客户网络销售传输服务。

当 BGP 在 AS - AS1 或 AS2 内运行时，它充当内部边界网关协议 (IBGP)。BGP 在 AS 端点 AS1 和 AS2 之间运行时，它充当外部边界网关协议 (EBGP)。IBGP 提供的路由器与路径相同，以到达 AS 外部的路由器。EBGP 路由器与其他 EBGP 路由器和 IBGP 路由器交换信息，以维持连接性和可访问性。



## 无类别域间路由

BGPv4 支持使用无类别域间路由 (CIDR) 以及聚合路由和 AS 路径。CIDR 使用包含 IP 地址和掩码的前缀来定义网络，从而有效地利用 IPv4 地址空间。使用聚合路由可减少路由表的大小。

## 路径向量路由

BGP 使用路径向量协议来维护动态更新的路径信息。检测并丢弃返回到原始节点的路径信息更新。BGP 不使用传统内部网关协议 (IGP) 值表，但会根据路径、网络策略和/或规则集做出路由决策。

## 全网格拓扑

在 AS 中，对于从内部 BGP 对等节点接收的路由，BGP 网络必须位于 full mesh 中，以发送到另一个 IBGP 对等节点。每个 BGP 路由器都与会话中的所有其他 BGP 路由器进行交流。例如，在具有四个 BGP 路由器的 AS 中，每个路由器拥有三个对等主机；在具有六个路由器的 AS 中，每个路由器有五个对等节点。

# 会话和对等

BGP 会话从两个使用 BGP 进行通信的路由器开始。会话的两个端点称为对等。对等也称为邻居。事件和计时器确定对等方之间的信息交换。BGP 重点关注流量路由策略。

## 会话

在与其他 BGP 对等的操作中，BGP 进程使用简单有限状态机制，其中包含六个状态 — Idle、Connect、Active、OpenSent、OpenConfirm 和 Established。对于每个对等会话，BGP 实施会跟踪会话的状态。BGP 定义了每个对等交换将会话从一种状态更改为另一种状态的消息。

- 空闲** BGP 将初始化所有资源、拒绝所有入站 BGP 连接尝试，并开始 TCP 与对等的连接。

|             |                                                                                              |
|-------------|----------------------------------------------------------------------------------------------|
| 连接          | 路由器将等待 TCP 连接完成，并在成功时转换为 OpenSent 状态。如果此转换不成功，BGP 将重置 ConnectRetry 计时器并在计时器到期时转换为 Active 状态。 |
| 活动          | 路由器将 ConnectRetry 计时器重设为零，并返回到 Connect 状态。                                                   |
| OpenSent    | 在成功的 OpenSent 转换后，路由器发送一条 Open 消息并等待一个返回。                                                    |
| OpenConfirm | 当对等方之间同意打开的消息参数后，邻居关系将建立并处于 OpenConfirm 状态。路由器随后会收到并检查打开消息参数上的协议以建立会话。                       |
| 已创建         | Keepalive 消息将进行交换，并且在成功接收后，路由器处于 Established 状态。Keepalive 消息将继续定期发送。Keepalive 计时器将建立状态以验证连接。 |

建立连接后，路由器将向其对等方发送和接收信息、更新和通知消息。

对等模板

对等模板允许 BGP 邻居继承相同的出站策略。您可以使用适用于各个对等的共享策略创建对等组，而不是手动配置每个具有相同策略的邻居。对等模板通过简化的配置提供高效的更新计算。

对等模板还有助于汇聚速度。当 BGP 进程向多个对等方发送相同的信息时，可以设置长的输出队列来发布信息。对于作为对等模板成员的对等，该信息将发送到一个位置，然后传递到模板中的对等。

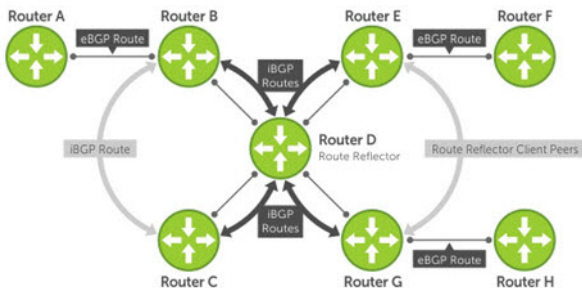
路由反射器

路由反射器 (RR) 将 IBGP 核心重组为一个层次结构，并允许路由通告规则。路由反射将 IBGP 对等体分成两个组 — 客户对等体和非客户对等体。

- 如果从非客户对等体收到路由，它将反映所有客户端对等体的路由
- 如果从客户端对等体收到路由，则会反映到所有非工作区和客户端对等体的路由

RR 及其客户端对等形成路由反射群集。BGP 扬声器仅通知给定前缀的最佳路由。RR 规则会在路由器做出最佳路径决定后应用。

**注：** 勿在路径中使用 RR — 平面 RR 的次 RR 可能生成回路。



路由器 B、C、D、E 和 G 是相同 AS—AS100 的成员。这些路由器也在相同的路由反射群集中，其中路由器 D 是路由反射器。路由器 E 和 G 是路由器 D 的客户端对等体，以及路由器 D 的路由器 B 和 C 和非客户端对等体。

1. 路由器 B 通过 EBGP 接收来自路由器 A 的通告。由于通过 EBGP 学习了路由，因此路由器 B 向所有 IBGP 对等体（路由器 C 和 D）通告。
2. 路由器 C 接收通告，但不会将其通告给任何对等体，因为只有其他对等体是路由器 D（IBGP 对等体），并且路由器 D 已从路由器 B 通过 IBGP 了解它。
3. 由于路由器 C 是非客户端对等体，因此路由器 D 不会将路由通告到路由器 C。路由通告来自路由器 B，也就是一种非客户端对等体。
4. 路由器 D 向路由器 E 和 G 反映了通告，因为它们是路由器 D 的客户端对等体。
5. 路由器 E 和 G 向其 EBGP 对等体通告此 IBGP 了解的路由 — 路由器 F 和 H。

多协议 BGP

多协议 BGP (MBGP) 是支持多个地址系列的 BGP 的扩展 — IPv4 和 IPv6。MBGP 会携带多组单播和多播路由，具体取决于地址系列。

您可以按每个路由器、按模板和/或按对等方式启用 MBGP 功能。默认值是 IPv4 单播路由。



BGP 会话支持多个地址系列接口 (AFI) 和子地址系列接口 (SAFI) 组合，BGP 使用开放消息将此信息传递给对等方。因此，IPv6 路由信息通过 IPv4 对等节点进行交换，反之亦然。

支持 IPv6 的 BGP 路由器可以使用 IPv6 对等节点设置 BGP 会话。如果现有 BGP-v4 会话能够交换 ipv6 前缀，则将使用这两者来传送 ipv4 以及 ipv6 前缀。如果 BGP-v4 邻居停机，还会影响 IPv6 路由交换。如果 BGP-v6 会话存在，它将继续独立于 BGP-v4 进行操作。

多协议 BGPv6 支持许多与 BGPv4 相同的特性和功能。MBGP 的 IPv6 增强功能包括支持 IPv6 地址系列和网络层可访问性信息 (NLRI) 以及使用 IPv6 地址的下一跳属性。

## 属性

使用 BGP 获得的路由具有关联的属性，用于确定当特定目标存在多个路径时到目标的最佳路由。这些属性被称为 *BGP 属性*，这会影响路由选择以设计可靠的网络。对于支持的 BGP 属性数没有硬编码限制。

路由选择的 BGP 属性：

- 权重
- 本地首选项
- 复合鉴别器
- 来源
- AS 路径
- 下一跳

## 社区

BGP 社区是具有一个或多个通用属性的路由集。社区同时为多个路由分配通用属性。不会拒绝重复的社区。

## 选择条件

BGP 属性的最佳路径选择条件：

1. 首选具有最大权重属性的路径，并首选具有最大 LOCAL\_PREF 属性的路径。
2. 使用 `network` 命令、`redistribute` 命令或 `aggregate-address` 命令，首选本地起源的路径。使用 `network` 或 `redistribute` 命令发起的路由优于源自 `aggregate-address` 命令的路由。
3. (可选) 如果配置 `bgp bestpath as-path ignore` 命令，请跳过此步骤，因为不会考虑 AS\_PATH。首选具有最短 AS\_PATH 的路径：
  - AS\_SET 的路径长度为 1，而不论集中有多少
  - 未配置 AS\_PATH 的路径的路径长度为 0
  - AS\_PATH 长度中不包括 AS\_CONFED\_SET
  - 无论 AS\_CONFED\_SEQUENCE 中有多少个 AS，AS\_CONFED\_SEQUENCE 路径长度为 1
4. 首选原始类型的路径 — IGP 低于 EGP，EGP 低于 INCOMPLETE。
5. 首选具有最低的多鉴别器 (MED) 属性的路径：
  - 只有当第一个邻接 AS 与两个路径相同时，才会执行此比较。仅当 AS\_SEQUENCE 中第一个 AS 对于两个路径都相同时，才会比较 MED。
  - 配置 `bgp always-compare-med` 命令以比较 MED 的所有路径。
  - 不带 MED 的路径被视为“最坏”，并分配有 4294967295 的 MED。
6. 首选外部 (EBGP) 到内部 (IBGP) 路径或联合 EBGP 路径，并首选具有最低 IGP 指标的路径到 BGP 下一跳。
7. 系统认为路径相等，并且仅当不满足条件时才执行以下步骤：
  - 使用 `maximum-path` 命令配置 IBGP 多路径或 EBGP 多路径。
  - 所比较的路径与 AS 路径中的值相同，但具有不同的下一跳。
  - 这些路径分别从 IBGP 或 EBGP 邻居接收。
8. 如果启用 `bgp bestpath router-id ignore` 命令，则执行以下操作：
  - 如果路由器 ID 对于多个路径是相同的，因为路由是从同一个路由接收的 — 跳过此步骤。
  - 如果多个路径的路由器 ID 不相同，请首选首先作为最佳路径接收的路径。路径选择算法将返回，而不执行任何详细的检查。
9. 首选从具有最低路由器 ID 的 BGP 路由器发起外部路径。如果两个路径都是外部的，请首选最早的路径。对于包含 RR 属性的路径，始发者 ID 替换为路由器 ID。如果两个路径具有相同的路由器 ID，请首选具有最低群集 ID 长度的路径。没有群集 ID 长度的路径被设置为 0 群集 ID 长度。

10. 首选路径来自具有最低地址的邻居。邻居地址在 BGP 邻居配置中使用，并与与本地路由器的 TCP 连接中使用的远程对等控制器相对应。

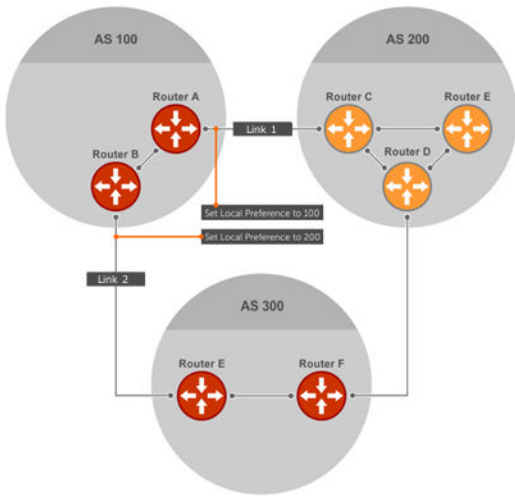
在非确定性模式下，此 `bgp non-deterministic-med` 命令适用。路径将按照它们到达的顺序进行比较。此方法会导致系统选择一组路径中的不同最佳路径。根据从邻居收到的顺序，MED 可能会在相邻路径之间进行比较。在确定模式下，系统将比较 MED。由于 AS 组中的所有路径都来自相同 AS，在 AS 组中相邻路径之间比较 MED。

## 权重和本地首选项

权重属性对于路由器是本地的，不向邻近的路由器通告。如果路由器了解多个到同一目标的路由，将首选具有最高权重的路由。具有最高权重的路由安装在 IP 路由表中。

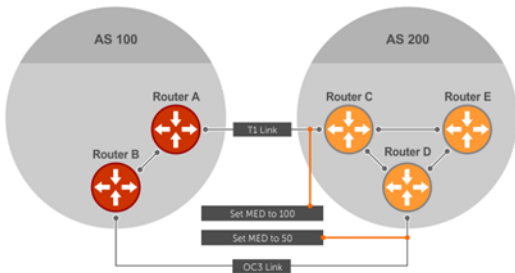
本地首选项 — LOCAL\_PREF 表示整个 AS 中的优先级别。数字越高，路由的首选项就越高。

LOCAL\_PREF 是确定最佳路径的条件之一 — 其他条件可能会影响选择，请参阅[最佳路径选择](#)。假设 LOCAL\_PREF 是应用的唯一属性，并且 AS 100 有两个可能的路径连接到 200。虽然穿过路由器 A 的路径较短，但 LOCAL\_PREF 设置具有穿过路由器 B 和 300 的首选路径。这会通告到 AS 100 中的所有路由器，从而使所有 BGP 扬声器更喜欢穿过路由器 B 的路径。



## 复合鉴别器

如果两个自治系统连接到多个位置，请使用复合鉴别器 (MED) 将首选项分配给首选路径。MED 是用于确定最佳路径的条件之一 — 其他条件可能也会影响选择。



将 AS 分配给 MED 值。其他 AS 使用该值来确定首选路径。假设 MED 是唯一应用的属性，并且在 100 和 200 之间有两个连接。每个连接都是一个 BGP 会话。AS 200 将链路 1 退出点的 MED 设置为 100，并将链路 2 退出点的 MED 设置为 50。这会通过链路 2 设置路径首选项。MED 通告为 AS 100 路由器，因此它们知道是首选路径。

MED 是不可传递的属性。如果 AS 100 将 MED 发送到 AS 200，则 AS 200 不会将其作为 AS 300 或作为 AS 400 传递。MED 是两个参与的 AS (AS 100 和 AS 200) 的本地相关的属性。MED 在两个链路之间通告 — 如果链路停止，则 AS 100 可连接到 AS 300 和 AS 400。

## 来源

原始位置指示前缀如何引入 BGP。有三个原始代码 — IGP、EGP 和 INCOMPLETE。

|                   |                                   |
|-------------------|-----------------------------------|
| <b>IGP</b>        | 前缀源自通过 IGP 获知的信息。                 |
| <b>EGP</b>        | 前缀来源于从 EGP（由下一代协议 (NGP) 替换）获知的信息。 |
| <b>INCOMPLETE</b> | 前缀来源于未知源。                         |

IGP 的指示灯表示路由衍生自原始 AS。EGP 意味着从外部网关协议获知路由。将路由安装到 BGP 中的聚合、重新分发或其他间接方式导致了 INCOMPLETE 来源代码。

问号 (?) 指示原始代码为 INCOMPLETE，而小写字母 (i) 指示 IGP 的原始代码。

## 原始配置

```
OS10# show ip bgp
BGP local RIB : Routes to be Added , Replaced , Withdrawn
BGP local router ID is 30.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
n - network S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network Next Hop Metric LocPrf Weight Path
*>I 1.1.1.0/24 17.1.1.2 0 0 0 i
*>I 2.2.2.0/24 17.1.1.2 0 0 0 ?
*>I 3.3.3.0/24 17.1.1.2 0 0 0 e
```

## AS 路径和下一跳

AS 路径是在更新中列出的所有前缀都已通过的列表。当向 EBGp 邻居通告时，BGP 扬声器会添加本地 AS 编号。包含 AS 路径编号 0 的任何更新均有效。

下一跳是用于达到通告路由器的 IP 地址：

- 对于 EBGp 邻居，下一跳地址是邻居之间连接的 IP 地址。
- 对于 IBGP 邻居，EBGP 下一跳地址将传送到本地 AS。当 BGP 扬声器向本地外部的另一个 BGP 扬声器通告自身时，以及在 AS 中通告路由时，下一跳属性将设置。

对于 EBGp 邻居，如果下一跳地址与邻居 IP 地址不同，则 BGP 路由对应的下一跳地址将不会解析。下一跳属性还可作为将流量定向到另一个 BGP 扬声器的方法，而不是等待扬声器通告。当下一跳 BGP 邻居不可访问时，与该 BGP 邻居之间的连接将在按住计时器到期后停止。

当您启用 `fast-external-fallover` 并且路由器已从 BGP 邻居了解路由时，如果下一跳无法访问，则 BGP 会话将立即终止，而无需等待暂停时间。

## 最佳路径选择

最佳路径选择会从每个目标可用的所有路径中选择最佳路由，并在 IP 路由表中记录每个选定的路由以进行流量转发。仅将有效的路由用于最佳路径选择。BGP 将以路径到达的顺序来比较所有路径，并选择最佳路径。活动路由的路径按其相邻外部数字的升序顺序进行分组。

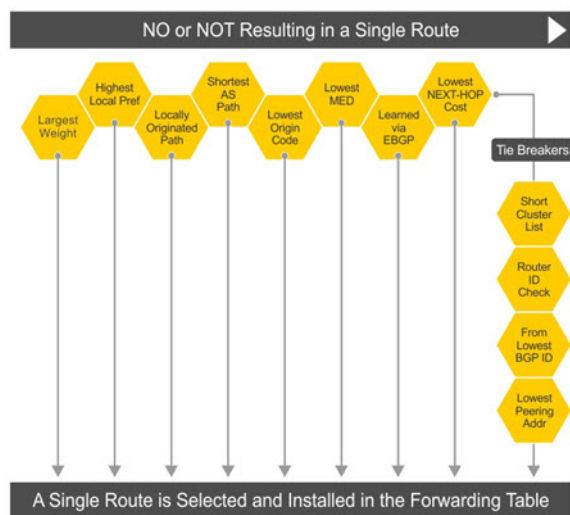
OS10 遵循 **确定性的** MED 从一组路径中选择不同的最佳路径。这可能取决于从邻居接收不同最佳路径的顺序 — MED 可能会在相邻路径之间进行比较。BGP 最佳路径选择默认为确定性。

根据特定条件选择每个组中的最佳路径 — 一次只选择一个最佳路径。如果 BGP 收到多个最佳路径，它将移至下一个有效路径列表，并继续，直至到达列表末尾。

配置 `non-deterministic-med` 命令时，路径将按照它们到达的顺序进行比较。OS10 遵循此方法以从一组路径中选择不同的最佳路径，具体取决于从邻居收到的顺序 — MED 可能会在相邻路径之间进行比较。

默认情况下，`bestpath as-path multipath-relax` 命令将禁用。这可防止 BGP 在两个或更多 EBGp 对等节点上对已学习的路由进行负载均衡。要在不同的 EBGp 对等节点上启用负载均衡，请输入 `bestpath as-path multipath-relax` 命令。

如果同时配置 `bgp bestpath as-path ignore` 命令和 `bestpath as-path multipath-relax` 命令，则会显示一条错误消息 — 一次只启用一个命令。



## 更多路径支持

更多路径（添加路径）通过针对同一地址前缀向其对等体通告多个路径（而不使用新的路径替换现有路径），从而减少了融合时间。默认情况下，BGP 扬声器仅针对给定地址前缀向其对等体通告最佳路径。

如果最佳路径变得不可用，则 BGP 扬声器从其本地路由器信息库信息基础 (RIB) 提取其路径，并重新计算新的最佳路径。这种情况需要 IGP 和 BGP 融合，并且是一个漫长的过程。如果当前最佳路径不可用，BGP 添加路径还有助于切换到下一个新的最佳路径。

添加路径功能仅在 IBGP 对等体上支持通告更多路径，在 EGP 对等主机或 BGP 对等组上不受支持。

### 忽略路由器 ID 计算

避免在特定条件下的外部路径之间不必要的 BGP 最佳路径转移。`bestpath router-id ignore` 命令可减少由路由和转发平面更改导致的网络中断，并允许更快的融合。

## 通告成本

作为重新分发的路由的默认流程，OS10 支持 IGP 成本 MED。默认情况下，自动汇总和同步均处于禁用状态。

### BGPv4 和 BGPv6 支持

- 确定性 MED，默认
- 缺少 MED 的路径被视为最差路径并分配有 0xffffffff MED 值。
- 系统引导时的延迟配置 — OS10 在发送消息之前读取整个配置文件以启动 BGP 对等体会话。

## 4 字节 AS 编号

默认情况下，OS10 支持 4 字节 AS 编号配置。4 字节支持在 OPEN 消息中作为新的 BGP 功能 4-BYTE-AS 进行通告。一种 BGP 扬声器，可向对等方通告 4 字节 AS 功能，并且从对等方那里获得相同的数据必须在所有消息中将 AS 编号编码为 4 字节的实体。

如果对等方的 AS 编号不同，则 4 字节扬声器将使用保留的 2 字节 ASN（名为 AS\_TRANS23456）启动邻居会话。AS\_TRANS 用于在 2 字节和 4 字节之间互操作。

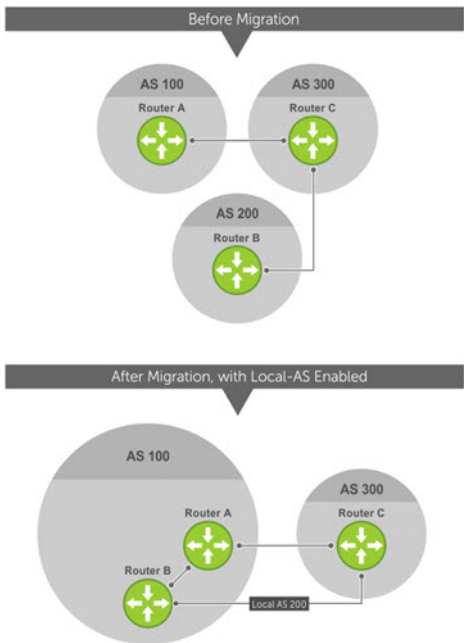
其中，2 字节格式为 1 到 65535，4 字节格式为 1 到 4294967295。您也可以使用点分十进制格式输入数字。例如，您可以输入 0.123。

## AS 编号迁移

您可以透明地更改整个 BGP 网络的 AS 编号。更改 AS 编号可确保在迁移过程中路由在整个网络中传播。当将一个 AS 迁移到另一个 AS 并将多个 AS 合并时，如果 AS 编号发生变化，则 EGP 网络可能会失去其到 IBGP 的路由。

当必须迁移网络的所有 IBGP 和 EBGP 对等体都必须更新以维持网络可访问性，迁移会非常困难。本地 AS 允许 BGP 扬声器像虚拟 AS 网络运行（物理 AS 网络除外）。

迁移后禁用 local-as 命令。在迁移后禁用 local-as 命令失败会导致 local-as 命令替换系统的原始值。使用新的 AS 编号将重新配置系统。



路由器 A、路由器 B 和路由器 C 分别属于 AS 100、200 和 300。路由器 A 获得的路由器 B — 路由器 B 具有路由器 C 作为其客户端。当路由器 B 迁移到路由器 A 时，它必须维护与路由器 C 的连接，而不会立即更新路由器 C 的配置。本地 AS 允许显示路由器 B，就好像它仍属于路由器 B 的旧网络 AS 200，以便与路由器 C 通信。

在使用 no prepend 命令时，本地 AS 不会在从 EBGP 对等方收到 AS 编号的情况下预置更新。如果未选择 no prepend，则默认情况下，本地设置将作为路径中的第一个 AS 分段添加。如果您使用入站路由映射将 AS-PATH 从对等方预置到更新，则会线添加本地 AS。

如果路由器 B 在路由器 C 上应用入站路由映射以将 65001 65002 预置到 AS-PATH，则这些事件会在路由器 B 上进行：

- 接收并验证更新。
- 将 local-as 预置为 200 AS-PATH。
- 将 65001 65002 预置为 AS-PATH。

本地 AS 将预置，然后路由映射呈现穿过 AS 200 中的路由器的更新，然后再达到路由器 B。

## 正常重新启动

OS10 仅在帮助程序模式中为 BGP 提供正常重新启动功能。

邻居正在重新启动的 BGP 路由器称为帮助程序。

如果在重启的路由器上启用正常重新启动，则在重新启动过程中，帮助程序会保持其从其邻居中获知的路由。

切换后，正常重新启动操作便会开始。两个路由器都重新建立其邻居关系，并再次交换其 BGP 路由。帮助程序将继续转发指向重新启动对等节点的前缀，并且重新启动路由器继续将流量转发到其对等节点，即使这些邻居关系正在重新启动。当重新启动路由器从所有支持正常重启的 BGP 对等节点接收所有路由更新时，正常重新启动即完成。BGP 会话将再次进入正常运行状态。

## 配置边界网关协议

默认情况下，BGP 已禁用。要启用 BGP 进程并开始交换信息，请分配 AS 编号并在 ROUTER-BGP 模式下使用命令以配置 BGP 邻居。

**BGP 邻居邻接更改** 记录所有 BGP 邻居更改

**快速外部故障切换** 已启用

|          |                                                                                                                                      |
|----------|--------------------------------------------------------------------------------------------------------------------------------------|
| 正常重新启动   | 已禁用                                                                                                                                  |
| 本地首选项    | 100                                                                                                                                  |
| 4 字节 AS  | 已启用                                                                                                                                  |
| MED      | 0                                                                                                                                    |
| 路由摆动抑制参数 | <ul style="list-style-type: none"> <li>• 半寿命 = 15 分钟</li> <li>• 最大抑制时间 = 60 分钟</li> <li>• 重复使用 = 750</li> <li>• 抑制 = 2000</li> </ul> |
| 计时器      | <ul style="list-style-type: none"> <li>• 保持连接 = 60 秒</li> <li>• 维持时间 = 180 秒</li> </ul>                                              |
| 添加路径     | 已禁用                                                                                                                                  |

## 启用 BGP

启用 BGP 之前，使用以下命令将 BGP 路由器 ID 分配给交换机：

- 在 ROUTER BGP 模式下，输入 `router-id ip-address` 命令。其中，`ip-address` 是与已配置的 L3 接口（物理、环回或 LAG）对应的 IP 地址。

默认情况下，BGP 已禁用。系统支持一个 AS 编号 — 您必须为您的设备分配 AS 编号。要建立 BGP 会话和路由流量，请至少配置一个 BGP 邻居或对等。在 BGP 中，具有已建立 TCP 连接的路由器称为 *邻居* 或 *对等*。建立连接后，相邻的完整 BGP 路由表将在随后的增量更新中进行交换。邻居还交换了 KEEPALIVE 消息以保持连接。

您可以将 BGP 邻居路由器或对等节点归类为内部或外部。直接连接 EBG 对等体，除非您启用 EBG 多跳 — IBGP 对等体用户无需直接连接。EBGP 邻居的 IP 地址通常是直接连接到路由器的接口的 IP 地址。BGP 进程首先确定所有内部 BGP 对等体是否均可访问，这会确定可访问的外部主机。

1. 分配 AS 编号，然后从 CONFIGURATION 模式中进入 ROUTER-BGP 模式，从 1 到 65535 适用于 2 字节，从 1 到 4294967295 适用于 4 字节。每个系统仅支持一个 AS 编号。如果输入一个 4 字节 AS 数字，则 4 字节 AS 支持自动启用。

```
router bgp as-number
```

2. 在 ROUTER-BGP 模式下输入邻居。

```
neighbor ip-address
```

3. 在 ROUTER-NEIGHBOR 模式下添加远程 AS，从 1 到 65535 适用于 2 字节，或从 1 到 4294967295 适用于 4 字节。

```
remote-as as-number
```

4. 在 ROUTER-NEIGHBOR 模式下启用 BGP 邻居。

```
no shutdown
```

5. （可选）在 ROUTER-NEIGHBOR 模式下为模板添加文本说明。

```
description text
```

要在更改 BGP 邻居的配置时重置配置，请使用 `clear ip bgp *` 命令。要查看 BGP 状态，请使用 `show ip bgp summary` 命令。

### 配置 BGP

```
OS10# configure terminal
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 5.1.1.1
OS10(config-router-neighbor)# remote-as 1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# description n1_abcd
OS10(config-router-neighbor)# exit
```



```
OS10(config-router-bgp-100)# template t1
OS10(config-router-template)# description peer_template_1_abcd
```

### 查看具有 2 字节 AS 编号的 BGP 摘要

```
OS10# show ip bgp summary

BGP router identifier 202.236.164.86 local AS number 64901
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx
120.10.1.1 64701 664 662 04:47:52 established 12000
```

### 查看具有 4 字节 AS 编号的 BGP 摘要

```
OS10# show ip bgp summary
BGP router identifier 11.1.1.1, local AS number 4294967295
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
1 neighbor(s) using 8192 bytes of memory

Neighbor AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/Pfx
5.1.1.2 4294967295 0 0 0 0 0 00:00:00 Active
```

对于路由器 ID，系统选择第一个配置的 IP 地址或随机数。要查看 BGP 邻居的状态，请使用 `show ip bgp neighbors` 命令。对于 BGP 邻居配置信息，请使用 `show running-config bgp` 命令。

此示例显示了两个相邻节点，一个是外部 BGP 邻居；另一个是内部 BGP 邻居。每个邻居输出的第一行显示 AS 编号，并且状态为外部或内部。

`show ip bgp neighbors` 输出的第三行包含 BGP 状态。如果显示除 *established* 以外的其他内容，则邻居不会交换信息和路由。有关详细信息，请参阅 [IPv6 命令](#)。

### 查看 BGP 邻居

```
OS10# show ip bgp neighbors
BGP neighbor is 5.1.1.1, remote AS 1, internal link
BGP version 4, remote router ID 6.1.1.1
BGP state established, in this state for 00:03:11
Last read 01:08:40 seconds, hold time is 180, keepalive interval is 60 seconds
Received 11 messages
3 opens, 1 notifications, 3 updates
4 keepalives, 0 route refresh requests
Sent 14 messages
3 opens, 1 notifications, 0 updates
10 keepalives, 0 route refresh requests

Minimum time between advertisement runs is 0 seconds
Description: nl_abcd
Capabilities received from neighbor for IPv4 Unicast:
MULTIPROTO_EXT(1)ROUTE_REFRESH(2)CISCO_ROUTE_REFRESH(128)
Capabilities advertised to neighbor for IPv4 Unicast:
MULTIPROTO_EXT(1)ROUTE_REFRESH(2)CISCO_ROUTE_REFRESH(128)

Prefixes accepted 3, Prefixes advertised 0

Connections established 3; dropped 2
Closed by neighbor sent 00:03:26 ago

Local host: 5.1.1.2, Local port: 43115
Foreign host: 5.1.1.1, Foreign port: 179
```

### 查看 BGP 运行的配置

```
OS10# show running-configuration bgp
!
router bgp 100
!
neighbor 5.1.1.1
description nl_abcd
```

## 在非默认 VRF 实例中配置 BGP

在非默认 VRF 实例中配置 BGP。

1. 分配 AS 编号，然后从 CONFIGURATION 模式中进入 ROUTER-BGP 模式，从 1 到 65535 适用于 2 字节，从 1 到 4294967295 适用于 4 字节。每个系统仅支持一个 AS 编号。如果输入一个 4 字节 AS 数字，则 4 字节 AS 支持自动启用。

```
router bgp as-number
```

2. 在非默认 VRF 实例中进入 ROUTER-BGP-VRF 模式。

```
vrf vrf-name
```

3. 在 CONFIG-ROUTER-VRF 模式下进入邻居。

```
neighbor ip-address
```

4. 在 ROUTER-NEIGHBOR 模式下添加远程 AS，从 1 到 65535 适用于 2 字节，或从 1 到 4294967295 适用于 4 字节。

```
remote-as as-number
```

5. 在 ROUTER-NEIGHBOR 模式下启用 BGP 邻居。

```
no shutdown
```

6. (可选) 在 ROUTER-NEIGHBOR 模式下为模板添加文本说明。

```
description text
```

要在更改 BGP 邻居的配置时重置配置，请使用 `clear ip bgp *` 命令。要查看 BGP 状态，请使用 `show ip bgp summary` 命令。

### 配置 BGP

```
OS10# configure terminal
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# vrf blue
OS10(config-router-vrf)# neighbor 5.1.1.1
OS10(config-router-neighbor)# remote-as 1
OS10(config-router-neighbor)# description n1_abcd
OS10(config-router-neighbor)# exit
OS10(config-router-vrf)# template t1
OS10(config-router-template)# description peer_template_1_abcd
```

## 禁用 ASN 值的通知

修改接收的路由的 AS\_PATH 属性。

- 在 CONFIG-ROUTER-NEIGHBOR 模式下禁用预置本地 AS 编号。

```
local-as as-number no-prepend
```

- 在 CONFIG-ROUTER-NEIGHBOR 模式中禁用预置全局配置的 AS 编号。

```
local-as as-number no-prepend replace-as
```

## 配置双堆栈

对于 BGPv4 和 BGPv6，OS10 支持双堆栈。双堆栈 BGP 允许通过不同 IPv4 和 IPv6 对等节点同时交换同一 IPv4 或 IPv6 前缀。您可以在相应的地址系列模式下使用 `activate` 命令来启用双堆栈。默认情况下，为所有邻居的 IPv4 地址系列启用 `activate` 命令。

如果 BGP v4 邻居想要传输 ipv6 前缀信息，将激活 IPv6 地址系列。对于执行 ipv4 前缀的 BGP-v6 邻居，它将激活 IPv4 地址系列。



1. 在 CONFIG-ROUTER-BGP 模式下启用对 IPv6 单播系列的支持。

```
address family ipv6 unicast
```

2. 在 CONFIG-ROUTER-BGP-AF 模式下，在 BGP 邻居/模板上启用 IPv6 单播支持。

```
activate
```

## 配置管理距离

路由器使用管理距离确定两个或更多路由之间的最佳路径以到达同一目标。管理距离表示路由的可靠性；管理距离越低，路由就越可靠。如果路由表管理器 (RTM) 从一个或多个路由协议接收单个目标的路由更新，则会根据管理距离选择最佳路由。

您可以使用 `distance bgp` 命令为以下 BGP 路由分配管理距离：

- 外部 BGP (eBGP) 路由
- 内部 BGP (iBGP) 路由
- 本地路由

如果未配置 BGP 路由的管理距离，将使用以下默认值：

- eBGP — 20
- iBGP — 200
- 本地路由 — 200

要更改 BGP 的管理距离，请使用以下命令：

```
distance bgp external-distance internal-distance local-distance
```

### 配置管理距离

1. 在 CONFIGURATION 模式下启用 BGP 并指定 AS 编号，从 0.1 到 65535.65535 或从 1 到 4294967295。

```
OS10# configure terminal
OS10(config)# router bgp 100
```

2. 使用以下命令之一从 ROUTER-BGP 模式进入相应的 ADDRESS-FAMILY 模式：

IPv4:

```
address-family ipv4 unicast
```

IPv6:

```
address-family ipv6 unicast
```

3. 从相应的 ADDRESS-FAMILY 模式更改 BGP 的管理距离。

IPv4:

```
distance bgp 21 200 200
```

IPv6:

```
distance bgp 21 201 250
```

以下示例提供了非默认 VRF 的配置：

```
OS10# configure terminal OS10(config)# router bgp 100
```

```
OS10(config-router-bgp-100)# vrf blue
OS10(config-router-bgp-100-vrf)# address-family ipv4 unicast
OS10(configure-router-bgp-v4-vrf-af)# distance bgp 21 200 200
OS10(config-router-bgp-100-vrf)# address-family ipv6 unicast
OS10(configure-router-bgp-v6-vrf-af)# distance bgp 21 201 250
```

## 对等模板

要一次配置多个 BGP 邻居，请创建并填充 BGP 对等模板。配置对等模板的优点是对等模板的成员将继承模板的配置属性并共享更新策略。在将成员添加到对等模板之前，请始终创建对等模板并为其分配名称。在为模板配置任何路由策略之前，请创建对等模板。

1. 启用 BGP，并在 CONFIGURATION 模式下将 AS 编号分配给本地 BGP 扬声器，从 1 到 65535 适用于 2 字节，从 1 到 4294967295 | 0.1 到 65535.65535 适用于 4 字节，或从 0.1 到 65535.65535（以点分隔格式）。

```
router bgp as-number
```

2. 通过在 ROUTER-BGP 模式中为其分配邻居名称来创建对等模板。

```
template template-name
```

3. （可选）在 ROUTER-TEMPLATE 模式下为模板添加文本说明。

```
description text
```

4. 在 ROUTER-NEIGHBOR 模式下输入地址系列模式。

```
address-family {[ipv4 | ipv6] [unicast]}
```

5. 筛选路由由更新中的网络、创建路由映射，并在 ROUTER-BGP-NEIGHBOR-AF 模式下分配筛选条件。

```
distribute-list prefix-list-name {in | out}
```

```
route-map map-name {in | out}
```

6. 在 ROUTER-TEMPLATE 模式下将邻居添加为远程 AS，从 1 到 65535 适用于 2 字节，从 1 到 4294967295 | 0.1 到 65535.65535 适用于 4 字节，或从 0.1 到 65535.65535（以点分隔格式）。

```
neighbor ip-address
```

7. （可选）添加远程邻居，然后在 ROUTER-TEMPLATE 模式中输入 AS 编号。

```
remote-as as-number
```

- 要添加 EBGP 邻居，请使用与 `router bgp as-number` 命令中配置的 BGP 不同的数字配置 `as-number` 参数。
- 要添加 IBGP 邻居，请使用与 `router bgp as-number` 命令中配置的 BGP 相同的数字配置 `as-number` 参数。

8. 在 ROUTER-NEIGHBOR 模式下为对等模板分配要继承到邻居的对等组名称。

```
inherit template template-name
```

9. 在 ROUTER-BGP 模式下启用邻居。

```
no shutdown
```

当您将对等体添加到对等组时，它会继承所有对等组配置的参数。禁用对等组后，对等模板内处于已建立状态的所有对等体将移至闲置状态。如果邻居配置了以下任何命令，则不能成为对等组的一部分：

- advertisement-interval
- next-hop-self
- route-map out
- route-reflector-client
- send-community

如果邻居配置比对等组更具体，并且邻居配置不影响传出更新，则邻居可能会将其配置添加到对等组。

要显示分配给 BGP 邻居的对等组配置，请使用 `show ip bgp peer-group peer-group-name` 命令。`show ip bgp neighbor` 命令输出不会显示对等组配置。

以下示例显示了配置示例：

### 配置对等模板

```
OS10# configure terminal
OS10(config)# router bgp 64601
OS10(config-router-bgp-64601)# template leaf_v4_ebgp
```

```

OS10(config-router-template)# description peer_template_1_abcd
OS10(config-router-template)# address-family ipv4 unicast
OS10(config-router-bgp-template-af)# distribute-list leaf_v4_in in
OS10(config-router-bgp-template-af)# distribute-list leaf_v4_out out
OS10(config-router-bgp-template-af)# route-map set_aspath_prepend in
OS10(config-router-bgp-template-af)# exit
OS10(config-router-template)# exit
OS10(config-router-bgp-64601)# neighbor 100.5.1.1
OS10(config-router-neighbor)# inherit template leaf_v4
OS10(config-router-neighbor)# remote-as 64802
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-64601)# neighbor 100.6.1.1
OS10(config-router-neighbor)# inherit template leaf_v4
OS10(config-router-neighbor)# remote-as 64802
OS10(config-router-neighbor)# no shutdown

```

## 查看对等组状态

```

OS10# show ip bgp peer-group leaf_v4
Peer-group leaf_v4, remote AS 0
 BGP version 4
 Minimum time between advertisement runs is 30 seconds
 Description: peer_template_1_abcd
 For address family: Unicast
 BGP neighbor is leaf_v4, peer-group external
 Update packing has 4_OCTET_AS support enabled

Number of peers in this group 2
Peer-group members:
 100.5.1.1
 100.6.1.1

```

```

OS10# show ip bgp peer-group leaf_v4 summary
BGP router identifier 100.0.0.8 local AS number 64601

```

| Neighbor  | AS    | MsgRcvd | MsgSent | Up/Down  | State/Pfx |
|-----------|-------|---------|---------|----------|-----------|
| 100.5.1.1 | 64802 | 376     | 325     | 04:28:25 | 1251      |
| 100.6.1.1 | 64802 | 376     | 327     | 04:26:17 | 1251      |

## 查看正在运行的配置

```

OS10# show running-configuration bgp
!
router bgp 64601
 bestpath as-path multipath-relax
 bestpath med missing-as-worst
 non-deterministic-med
 router-id 100.0.0.8
 !
 template leaf_v4
 description peer_template_1_abcd !
 address-family ipv4 unicast
 distribute-list leaf_v4_in in
 distribute-list leaf_v4_out out
 route-map set_aspath_prepend in
 !
 neighbor 100.5.1.1
 description leaf_connected_ebgp_neighbor
 bfd
 inherit template leaf_v4
 remote-as 64802
 no shutdown
 !
 neighbor 100.6.1.1
 description leaf_connected_ebgp_neighbor
 bfd
 inherit template leaf_v4
 remote-as 64802
 no shutdown
 !

```

## 非默认 VRF 实例的对等模板

您可以创建对等模板，以便一次将多个邻居添加到您创建的非默认 VRF 实例。

1. 启用 BGP，并在 CONFIGURATION 模式下将 AS 编号分配给本地 BGP 扬声器，从 1 到 65535 适用于 2 字节，从 1 到 4294967295 | 0.1 到 65535.65535 适用于 4 字节，或从 0.1 到 65535.65535（以点分隔格式）。

```
router bgp as-number
```

2. 进入 CONFIG-ROUTER-VRF 模式，以创建适用于您创建的非默认 VRF 实例的对等模板。

```
vrf vrf-name
```

3. 在 CONFIG-ROUTER-VRF 模式下通过为其分配邻居名称来创建对等模板。

```
template template-name
```

4. 在 ROUTER-TEMPLATE 模式下将邻居添加为远程 AS，从 1 到 65535 适用于 2 字节，从 1 到 4294967295 | 0.1 到 65535.65535 适用于 4 字节，或从 0.1 到 65535.65535（以点分隔格式）。

```
neighbor ip-address
```

5. 添加远程邻居，然后在 ROUTER-TEMPLATE 模式中输入 AS 编号。

```
remote-as as-number
```

- 要添加 EBGP 邻居，请使用与 `router bgp as-number` 命令中配置的 BGP 不同的数字配置 `as-number` 参数。
  - 要添加 IBGP 邻居，请使用与 `router bgp as-number` 命令中配置的 BGP 相同的数字配置 `as-number` 参数。
6. （可选）在 ROUTER-TEMPLATE 模式下为模板添加文本说明。

```
description text
```

7. 在 ROUTER-NEIGHBOR 模式下为对等模板分配要继承到邻居的对等组名称。

```
inherit template template-name
```

8. 在 ROUTER-BGP 模式下启用邻居。

```
neighbor ip-address
```

9. 在 ROUTER-NEIGHBOR 模式下启用对等组。

```
no shutdown
```

当您将对等体添加到对等组时，它会继承所有对等组配置的参数。禁用对等组后，对等模板内处于已建立状态的所有对等体将移至闲置状态。如果邻居配置了以下任何命令，则不能成为对等组的一部分：

- advertisement-interval
- next-hop-self
- route-map out
- route-reflector-client
- send-community

如果邻居配置比对等组更具体，并且邻居配置不影响传出更新，则邻居可能会将其配置添加到对等组。

要显示分配给 BGP 邻居的对等组配置，请使用 `show ip bgp peer-group peer-group-name` 命令。`show ip bgp neighbor` 命令输出不会显示对等组配置。

### 配置对等模板

```
OS10(config)# router bgp 300
OS10(config-router-bgp-300) vrf blue
OS10(config-router-vrf)# template ebpgpg
OS10(config-router-template)# remote-as 100
OS10(config-router-template)# description peer_template_1_abcd
OS10(config-router-template)# exit
OS10(config-router-vrf)# neighbor 3.1.1.1
OS10(config-router-neighbor)# inherit template ebpgpg
OS10(config-router-neighbor)# no shutdown
```

## 邻居故障切换

BGP 邻居故障切换功能可在保持稳定的同时减少融合时间。启用故障切换时，BGP 会跟踪对等远程地址和对等本地地址的 IP 可访问性。

当远程或对等本地地址无法访问时，BGP 会将会话与对等控制器断开。例如，如果对等 IPv6 目标/本地地址的路由表中不存在活动路由，BGP 将使会话停止。

默认情况下，保留时间将监管 BGP 会话。按每个邻居或对等组配置 BGP 快速故障切换。BGP 路由器通常会携带大型路由表，因为不需要频繁的会话重置。如果启用故障切换，则在添加的主机路由达到内部对等节点失败时与内部 BGP 对等节点的连接将立即重置。

1. 在 ROUTER-BGP 模式下输入邻居 IP 地址。

```
neighbor ip-address
```

2. 在 ROUTER-NEIGHBOR 模式下禁用快速故障切换。

```
no fall-over
```

3. 在 ROUTER-BGP 模式下输入邻居 IP 地址。

```
neighbor ip-address
```

4. 在 ROUTER-NEIGHBOR 模式下启用 BGP 快速故障切换。

```
fall-over
```

### 配置邻居故障切换

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 3.1.1.1
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# fall-over
OS10(config-router-neighbor)# no shutdown
```

### 验证邻居上的邻居故障切换

```
OS10(config-router-neighbor)# do show ip bgp neighbors 3.1.1.1
BGP neighbor is 3.1.1.1, remote AS 100, local AS 100 internal link

BGP version 4, remote router ID 3.3.3.33
BGP state ESTABLISHED, in this state for 00:17:17
Last read 00:27:54 seconds
Hold time is 180, keepalive interval is 60 seconds
Configured hold time is 180, keepalive interval is 60 seconds
Fall-over enabled

Received 23 messages
 1 opens, 0 notifications, 1 updates
 21 keepalives, 0 route refresh requests
Sent 21 messages
 1 opens, 0 notifications, 0 updates
 20 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
Minimum time before advertisements start is 0 seconds
Capabilities received from neighbor for IPv4 Unicast:
 MULTIPROTO_EXT(1)
 ROUTE_REFRESH(2)
 CISCO_ROUTE_REFRESH(128)
 4_OCTET_AS(65)
Capabilities advertised to neighbor for IPv4 Unicast:
 MULTIPROTO_EXT(1)
 ROUTE_REFRESH(2)
 CISCO_ROUTE_REFRESH(128)
 4_OCTET_AS(65)
Prefixes accepted 3, Prefixes advertised 0
Connections established 1; dropped 0
Last reset never
For address family: IPv4 Unicast
 Allow local AS number 0 times in AS-PATH attribute
```

```
Prefixes ignored due to:
Martian address 0, Our own AS in AS-PATH 0
Invalid Nexthop 0, Invalid AS-PATH length 0
Wellknown community 0, Locally originated 0

For address family: IPv6 Unicast
Allow local AS number 0 times in AS-PATH attribute
Local host: 3.1.1.3, Local port: 58633
Foreign host: 3.1.1.1, Foreign port: 179
```

## 验证对等组上的邻居故障切换

```
OS10# show running-configuration

!
router bgp 102
!
address-family ipv4 unicast
aggregate-address 6.1.0.0/16
!
neighbor 40.1.1.2
inherit template bgppg
no shutdown
!
neighbor 60.1.1.2
inherit template bgppg
no shutdown
!
neighbor 32.1.1.2
remote-as 100
no shutdown
!
template bgppg
fall-over
remote-as 102
!
```

## 配置密码

您可以启用消息摘要 5 (MD5) 身份验证，并在两个 BGP 邻居之间的 TCP 连接上输入密码。

在两个 BGP 对等体上配置相同的密码。在两个 BGP 对等体之间配置 MD5 身份验证时，将会验证 TCP 连接的每个分段，并在 TCP 连接上发送的每个分段中检查 MD5 摘要。为邻居配置密码可以建立新连接。

 **注：**您可以使用 MD5 身份验证来保护 VTEP 邻居通信。

### 配置密码

- 在 ROUTER-NEIGHBOR CONFIGURATION 或 ROUTER-TEMPLATE CONFIGURATION 模式下配置 BGP 对等体中的密码。在 ROUTER-NEIGHBOR 模式下提供的密码优先于在 ROUTER-TEMPLATE 模式下的密码。以纯文本形式或采用加密格式输入密码。
  - password {9 encrypted password-string|password-string}

### 查看密码配置

- show configuration

### ROUTER-NEIGHBOR 模式下的对等体 1

```
OS10# configure terminal
OS10(config)# interface ethernet 1/1/5
OS10(config-if-eth1/1/5)# no switchport
OS10(config-if-eth1/1/5)# ip address 11.1.1.1/24
OS10(config-if-eth1/1/5)# router bgp 10
OS10(config-router-bgp-10)# neighbor 11.1.1.2
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# remote-as 10
OS10(config-router-neighbor)# password abcdell
```

## ROUTER-TEMPLATE 模式下的对等体 1

```
OS10# configure terminal
OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# no switchport
OS10(conf-if-eth1/1/5)# ip address 11.1.1.1/24
OS10(conf-if-eth1/1/5)# router bgp 10
OS10(config-router-bgp-10)# template pass
OS10(config-router-template)# password 9
f785498c228f365898c0efdc2f476b4b27c47d972c3cd8cd9b91f518c14ee42d
OS10(config-router-template)# exit
OS10(config-router-bgp-10)# neighbor 11.1.1.2
OS10(config-router-neighbor)# inherit template pass
```

### 查看对等体 1 中的密码配置

```
OS10(config-router-neighbor)# show configuration
!
neighbor 11.1.1.2
password 9 0fbelad397712f74f4df903b4ff4b7b6e22cc377180432d7523a70d403d41565
remote-as 10
no shutdown

OS10(config-router-neighbor)# do show running-configuration bgp
!
router bgp 10
!
template pass
password 9 f785498c228f365898c0efdc2f476b4b27c47d972c3cd8cd9b91f518c14ee42d
!
neighbor 11.1.1.2
inherit template pass
password 9 01320afb39f49134882b0a9814fe6e8e228f616f60a35958844775314c00f0e5
remote-as 10
no shutdown
```

## ROUTER-NEIGHBOR 模式下的对等体 2

```
OS10# configure terminal
OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# no switchport
ip OS10(conf-if-eth1/1/5)# ip address 11.1.1.2/24
OS10(conf-if-eth1/1/5)# router bgp 20
OS10(config-router-bgp-20)# neighbor 11.1.1.1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# remote-as 20
OS10(config-router-neighbor)# password abcdell
```

## ROUTER-TEMPLATE 模式下的对等体 2

```
OS10# configure terminal
OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# no switchport
OS10(conf-if-eth1/1/5)# ip address 11.1.1.2/24
OS10(conf-if-eth1/1/5)# router bgp 20
OS10(config-router-bgp-20)# template pass
OS10(config-router-template)# password 9
f785498c228f365898c0efdc2f476b4b27c47d972c3cd8cd9b91f518c14ee42d
OS10(config-router-template)# exit
OS10(config-router-bgp-20)# neighbor 11.1.1.1
OS10(config-router-neighbor)# inherit template pass
```

### 查看对等体 2 中的密码配置

```
OS10(config-router-neighbor)# show configuration
!
neighbor 11.1.1.1
password 9 0fbelad397712f74f4df903b4ff4b7b6e22cc377180432d7523a70d403d41565
```

```
remote-as 20
no shutdown
```

```
OS10(config-router-neighbor)# do show running-configuration bgp
!
router bgp 20
 neighbor 11.1.1.2
 password 9 f785498c228f365898c0efdc2f476b4b27c47d972c3cd8cd9b91f518c14ee42d
 remote-as 20
 no shutdown
```

## 快速外部故障切换

快速外部故障切换会终止任何直接相邻对等节点的 EBGP 会话（如果用于到达对等主机的链路关闭）。BGP 不会等待保留计时器过期。

默认情况下，快速外部故障切换处于启用状态。要禁用或重新启用它，请使用 `[no] fast-external-fallover` 命令。要使 `fast-external-fallover` 命令对已建立的 BGP 会话生效，您必须使用 `clear ip bgp {* | peer-ipv4-address | peer-ipv6-address}` 命令重置会话。

### 查看快速外部故障切换配置

```
OS10(config)# do show running-configuration bgp
!
router bgp 300
!
 neighbor 3.1.1.1
 remote-as 100
 no shutdown
!
 neighbor 3::1
 remote-as 100
 no shutdown
!
 address-family ipv6 unicast
 activate
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
 ip address 3.1.1.3/24
 no switchport
 no shutdown
 ipv6 address 3::3/64
OS10(conf-if-eth1/1/1)# shutdown
OS10(conf-if-eth1/1/1)# do show ip bgp summary
BGP router identifier 11.11.11.11 local AS number 300
Neighbor AS MsgRcvd MsgSent Up/
Down State/Pfx
3.1.1.1 100 6 6
00:00:15 Active
3::1 100 8 11
00:00:15 Active
OS10(conf-if-eth1/1/1)#
```

### 查看快速外部故障切换取消配置

```
OS10(config-router-bgp-300)# do show running-configuration bgp
!
router bgp 300
 no fast-external-fallover
!
 neighbor 3.1.1.1
 remote-as 100
 no shutdown
!
 neighbor 3::1
 remote-as 100
 no shutdown
```



```

!
 address-family ipv6 unicast
 activate
OS10(config-router-bgp-300)#
OS10(conf-if-eth1/1/1)# do clear ip bgp *
OS10# show ip bgp summary
BGP router identifier 11.11.11.11 local AS number 300
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx

3.1.1.1 100 7 4 00:00:08 3
3::1 100 9 5 00:00:08 4
OS10#
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# shutdown
OS10(conf-if-eth1/1/1)# do show ip bgp summary
BGP router identifier 11.11.11.11 local AS number 300
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx

3.1.1.1 100 7 4 00:00:29 3
3::1 100 9 5 00:00:29 4
OS10(conf-if-eth1/1/1)#
OS10(config-router-bgp-neighbor-af)# Apr 27 01:39:03 OS10 dn_sm[2065]: Node.1-
Unit.1:PRI:alert [os10:event],
%Dell EMC (OS10) %BGP_NBR_BKWD_STATE_CHG: Backward state change occurred Hold Time
expired for Nbr:3.1.1.3 VRF:default
Apr 27 01:39:03 OS10 dn_sm[2065]: Node.1-Unit.1:PRI:alert [os10:event], %Dell EMC
(OS10) %BGP_NBR_BKWD_STATE_CHG: Backward
state change occurred Hold Time expired for Nbr:3::3 VRF:default

```

## 被动对等

启用对等模板时，系统将发送打开的消息以启动 TCP 连接。如果为对等模板启用被动对等，则系统不会发送打开的消息，但会响应打开的消息。

当与身份验证的 BGP 邻居连接拒绝被动对等模板时，系统会阻止同一子网上的其他被动对等模板与 BGP 邻居进行连接。要解决此限制，请更改 BGP 配置或更改对等模板配置的顺序。

您可以使用 `limit` 命令限制邻居接受的被动会话的数量。

1. 在 CONFIGURATION 模式下启用 BGP 并为本地 BGP 扬声器分配 AS 编号（1 到 65535 适用于 2 字节，1 到 4294967295 适用于 4 字节）。

```
router bgp as-number
```

2. 在 ROUTER-BGP 模式下配置不会启动与其他对等节点的 TCP 连接的模板。最多 16 个字符。

```
template template-name
```

3. 在 ROUTER-BGP-TEMPLATE 模式下为远程邻居创建和输入编号（从 1 到 4294967295）。

```
remote-as as-number
```

4. 在 ROUTER-BGP-TEMPLATE 模式下启用对等侦听并输入最大动态对等计数（1 到 4294967295）。

```
listen neighbor ip-address limit
```

只有当对等模板对在子网上发送的 OPEN 消息进行响应时，才会将其 BGP 的状态更改为 ESTABLISHED。建立对等模板后，对等模板与其他任何对等模板相同，请参阅[对等模板](#)。

如果未在对等收听模式下配置 BGP 设备，则会出现一个与动态对等的会话。在 BGPv4/v6 动态对等上不支持密码。

### 配置被动对等

```

OS10(config)# router bgp 10
OS10(config-router-bgp-10)# template bgppg
OS10(config-router-template)# remote-as 100
OS10(config-router-template)# listen 32.1.0.0/8 limit 10

```

## 本地 AS

在 BGP 网络迁移过程中，您可以保持现有的 AS 编号。在迁移后，使用要禁用的新信息重新配置您的路由器。被动对等模板不支持网络迁移。您必须先配置[对等模板](#)，然后才能将其指定为 AS。

1. 在 ROUTER-BGP 模式下，输入邻居 IP 地址，即 A.B.C.D。

```
neighbor ip-address
```

2. 输入对等节点的本地 AS 编号，该 AS 值未预置未在 ROUTER-NEIGHBOR 模式下来自邻居的通告（从 1 到 4294967295）。

```
local-as as number [no prepend]
```

3. 返回到 ROUTER-BGP 模式。

```
exit
```

4. 在 ROUTER-BGP 模式下输入为对等组分配的模板名称。最多 16 个字符。

```
template template-name
```

5. 在 ROUTER-TEMPLATE 模式下输入对等主机的本地 AS 编号。

```
local-as as number [no prepend]
```

6. 在 ROUTER-TEMPLATE 模式下添加远程 AS(从 1 到 65535 适用于 2 字节，或从 1 到 4294967295 适用于 4 字节)。

```
remote-as as-number
```

### 允许来自邻居的外部路由

```
OS10(config)# router bgp 10
OS10(conf-router-bgp-10)# neighbor 32.1.1.2
OS10(conf-router-neighbor)# local-as 50
OS10(conf-router-neighbor)# exit
OS10(conf-router-bgp-10)# template bgppg1
OS10(conf-router-template)# fall-over
OS10(conf-router-template)# local-as 400
OS10(conf-router-template)# remote-as 102
```

### 本地 AS 编号已禁用

```
OS10(config)# router bgp 102
OS10(conf-router-bgp-102)# neighbor 32.1.1.2
OS10(conf-router-neighbor)# no local-as 100
```

## AS 编号限制

设置 AS 路径中 AS 编号出现的次数。allow-as 参数将许可 BGP 扬声器允许在从对等方收到的更新中配置的次数的 AS 编号。如果本地 AS 编号显示的次数超过命令中的次数，则会检测到 AS-PATH 循环。

1. 在 ROUTER-BGP 模式下输入要使用 AS 路径的邻居 IP 地址。

```
neighbor ip address
```

2. 在 ROUTER-NEIGHBOR 模式下输入地址系列模式。

```
address-family {{ipv4 | ipv6} unicast | l2vpn evpn}
```

3. 允许邻居 IP 地址以在 ROUTER-BGP-NEIGHBOR-AF 模式中使用 AS 路径的指定次数（1 到 10）。

```
allowas-in number
```

## 配置 AS 数字外观

```
OS10(config)# router bgp 10
OS10(conf-router-bgp-10)# neighbor 1.1.1.2
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# allowas-in 5
```

## 查看 AS 路径中的 AS 编号

```
OS10# show running-configuration bgp
!
router bgp 101
 no fast-external-fallover
 !
 address-family ipv4 unicast
 dampening
 !
 neighbor 17.1.1.2
 remote-as 102
 no shutdown
 !
 address-family ipv4 unicast
 allowas-in 4
```

## 显示 IP BGP

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172:16:1::2
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv6 unicast
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# end
OS10# show running-configuration bgp
!
router bgp 100
 !
 neighbor 172:16:1::2
 remote-as 100
 no shutdown
 !
 address-family ipv6 unicast
 activate
 allowas-in 1
OS10# show ip bgp
BGP local RIB : Routes to be Added , Replaced , Withdrawn
BGP local router ID is 100.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed/network, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

```

|     | Network       | Next Hop    | Metric | LocPrf | Weight | Path            |
|-----|---------------|-------------|--------|--------|--------|-----------------|
| *>I | 55::/64       | 172:16:1::2 | 0      | 0      | 0      | 100 200 300 400 |
| i   |               |             |        |        |        |                 |
| *>I | 55:0:0:1::/64 | 172:16:1::2 | 0      | 0      | 0      | 100 200 300 400 |
| i   |               |             |        |        |        |                 |
| *>I | 55:0:0:2::/64 | 172:16:1::2 | 0      | 0      | 0      | 100 200 300 400 |
| i   |               |             |        |        |        |                 |

## 重新分发路由

添加从其他路由实例或协议到 BGP 进程的路由。您可以使用 `redistribute` 命令在 BGP 进程中包含 OSPF、静态或直接连接的路由。

- 在 ROUTER-BGP-AF 模式下包括直接连接或用户配置的（静态）路由。

```
redistribute {connected | static}
```

- 在 ROUTER-BGP-AF 模式下包括 IS-IS 中的特定 OSPF 路由（1 到 65535）。

```
redistribute ospf process-id
```

### 禁用重新分发的路由

```
OS10(conf-router-bgp-af)# no redistribute ospf route-map ospf-to-bgp
```

### 重新分发路由 — 重新分发路由

```
OS10(config)# router bgp 102
OS10(config-router-bgp-102)# address-family ipv4 unicast OS10
(configure-router-bgpv4-af)# redistribute ospf 12
```

## 其他路径

默认情况下，add-path 命令已禁用。

1. 在 CONFIGURATION 模式下分配 AS 编号。

```
router bgp as-number
```

2. 在 ROUTER-BGP 模式下输入邻居和 IP 地址 (A.B.C.D)。

```
neighbor ip-address
```

3. 在 ROUTER-NEIGHBOR 模式下输入地址系列模式。

```
address-family {[ipv4 | ipv6] [unicast]}
```

4. 允许指定的邻居在 ROUTER-BGP 模式下发送或接收多个路径通告。count 参数可以控制已通告的路径数量，而不是收到的路径数。

```
add-path [both | received | send] count
```

### 启用其他路径

```
OS10(config)# router bgp 102
OS10(conf-router-bgp-102)# neighbor 32.1.1.2
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# add-path both 3
```

## MED 属性

与相同的 EBGp 路径进行比较时，OS10 使用 MULTI\_EXIT\_DISC 或 MED 属性。不会采用与数字不同的相邻路径执行 MED 比较。

1. 从与在 ROUTER-BGP 模式下不同的邻居，在路径中启用 MED 比较。

```
always-compare-med
```

2. 在 ROUTER-BGP 模式下更改 MED 选择的最佳路径。

```
bestpath med {confed | missing-as-best}
```

- confed — 选择最佳路径 MED，与从 BGP 联盟获得的路径比较。
- missing-as-best — 将缺少 MED 的路径视为最首选的路径。
- missing-as-worst — 将缺少 MED 的路径视为最低优先级。

### 修改 MED 属性

```
OS10(config)# router bgp 100
OS10(conf-router-bgp-100)# always-compare-med
OS10(conf-router-bgp-100)# bestpath med confed
```

## 本地首选项属性

您可以更改路由器接收的所有路由的 LOCAL\_PREFERENCE 属性值。要在 ROUTER-BGP 模式下将 LOCAL\_PREF 值从 0 更改为 4294967295（默认值 100），请使用 `default local preference value` 命令。

要查看 BGP 配置，请使用 `show running-configuration` 命令。操作 LOCAL\_PREF 属性值的更灵活的方法是使用路由映射。

1. 在 CONFIGURATION 模式下为路由映射分配名称。

```
route-map map-name {permit | deny | sequence-number}
```

2. 在 ROUTE-MAP 模式下，更改满足此路由映射条件的路由的 LOCAL\_PREF 值，然后返回到 CONFIGURATION 模式。

```
set local-preference value
exit
```

3. 进入 ROUTER-BGP 模式。

```
router bgp as-number
```

4. 输入邻居以在 ROUTER-BGP 模式下应用路由映射配置。

```
neighbor {ip-address}
```

5. 在 ROUTER-BGP-NEIGHBOR-AF 模式下将路由映射应用到邻居的传入或传出路由。

```
route-map map-name {in | out}
```

6. 在 ROUTER-BGP 模式下输入对等组以在应用路由映射配置。

```
template template-name
```

7. 在 CONFIG-ROUTER-TEMPLATE-AF 模式下将路由映射应用到对等组的传入或传出路由。

```
route-map map-name {in | out}
```

### 配置和查看本地首选项属性

```
OS10(config)# route-map bgproutemap 1
OS10(conf-route-map)# set local-preference 500
OS10(conf-route-map)# exit
OS10(config)# router bgp 10
OS10(conf-router-bgp-10)# neighbor 10.1.1.4
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# route-map bgproutemap in
```

```
OS10 configure terminal
OS10(config)# route-map bgproutemap 1
OS10(conf-route-map)# set local-preference 500
OS10(conf-route-map)# exit
OS10(config)# router bgp 64601
OS10(conf-router-bgp-64601)# template bgppg
OS10(conf-router-template)# address-family ipv4 unicast
OS10(conf-router-bgp-template-af)# route-map bgproutemap in
```

### 查看路由映射

```
OS10(conf-route-map)# do show route-map
route-map bgproutemap, permit, sequence 1
Match clauses:
Set clauses:
 local-preference 500
 metric 400
 origin incomplete
```

## 权重属性

您可以根据权重值影响 BGP 路由。当存在多个到同一目标的路由时，具有较高权重值的路由具有优先权。

1. 在 ROUTER-BGP 模式下为邻居连接分配权重。

```
neighbor {ip-address}
```

2. 在 ROUTER-NEIGHBOR 模式下设置路由的权重值（1 到 4294967295，默认值为 0）。

```
weight weight
```

3. 返回到 ROUTER-BGP 模式。

```
exit
```

4. 在 ROUTER-BGP 模式下为对等组分配权重值。

```
template template name
```

5. 在 ROUTER-BGP 模式下设置路由的权重值。

```
weight weight
```

### 修改权重属性

```
OS10(config)# router bgp 10
OS10(config-router-bgp-10)# neighbor 10.1.1.4
OS10(config-router-neighbor)# weight 400
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-10)# template zanzibar
OS10(config-router-template)# weight 200
```

## 启用多路径

默认情况下您可以具有一个到目标的路径，并且可以启用多路径以允许到目标的最多 64 个并行路径。show ip bgp network 命令包括该网络的多路径信息。

- 在 ROUTER-BGP 模式下启用多个并行路径。

```
maximum-paths {ebgp | ibgp} number
```

### 启用多路径

```
OS10(config)# router bgp 10
OS10(config-router-bgp-10)# maximum-paths ebgp 10
```

## 路由映射筛选器

筛选路由允许您实施 BGP 策略。使用路由映射来控制 BGP 邻居或对等组接受和通告的路由。

1. 输入要在 ROUTER-BGP 模式下筛选路由的邻居 IP 地址。

```
neighbor ipv4-address
```

2. 在 ROUTER-NEIGHBOR 模式下输入地址系列模式。

```
address-family {[ipv4 | ipv6] [unicast]}
```

3. 在 ROUTER-BGP-NEIGHBOR-AF 模式下创建路由映射并分配筛选条件，然后返回到 CONFIG-ROUTER-BGP 模式。

```
route-map map-name {in | out}
exit
```

- in — 输入用于传入路由更新的筛选器。
- out — 输入用于传出路由更新的筛选器。

4. 在 ROUTER-BGP 模式下输入对等模板名称。

```
template template-name
```

5. 输入地址系列模式。

```
address-family {[ipv4 | ipv6] [unicast]}
```

6. 创建路由映射，并在 ROUTER-BGP-TEMPLATE-AF 模式下指定筛选条件。

```
route-map map-name {in | out}
```

## 筛选 BGP 路由

```
OS10(config)# router bgp 102
OS10(conf-router-bgp-102)# neighbor 40.1.1.2
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# route-map metro in
OS10(conf-router-bgp-neighbor-af)# exit
OS10(conf-router-bgp-102)# template ebgp
OS10(conf-router-template)# address-family ipv4 unicast
OS10(conf-router-bgp-template-af)# route-map metro in
```

## 路由反射器群集

BGP 路由反射器面向具有大型网络的 AS。它们减少了 BGP 控制流量的数量。在正确配置路由反射的情况下，IBGP 路由器并非在群集内完全网格化，而是接收所有路由信息。

配置路由器的群集，其中一个路由器是集中式路由器，而其他路由器是从集中式路由器接收更新的客户端。

1. 为 ROUTER-BGP 模式中的路由器反射器群集分配 ID。您可以在 AS 中有多个群集。

```
cluster-id cluster-id
```

2. 在 ROUTER-BGP 模式下将邻居分配给路由器反射器群集。

```
neighbor {ip-address}
```

3. 在 ROUTER-NEIGHBOR 模式下将邻居配置为路由反射器客户端，然后返回到 ROUTER-BGP 模式。

```
route-reflector-client
exit
```

4. 在 ROUTER-BGP 模式下，将对等组模板分配为路由反射器群集的一部分。

```
template template-name
```

5. 在 ROUTER-TEMPLATE 模式下将模板配置为路由反射器客户端。

```
route-reflector-client
```

启用路由反射器时，系统会自动为所有客户端启用路由反射。要禁用此反射器中所有客户端之间的路由反射，请在 ROUTER-BGP 模式下使用 `no bgp client-to-client reflection` 命令。在禁用路由反射之前，您必须完全网格化所有客户端。

## 配置 BGP 路由反射器

```
OS10(config)# router bgp 102
OS10(conf-router-bgp-102)# cluster-id 4294967295
OS10(conf-router-bgp-102)# neighbor 32.1.1.2
OS10(conf-router-neighbor)# route-reflector-client
OS10(conf-router-neighbor)# exit
OS10(conf-router-bgp-102)# template zanzibar
OS10(conf-router-template)# route-reflector-client
```

## 聚合路由

OS10 提供多种方法来聚合 BGP 路由表中的路由。必须在路由表中至少有一个聚合路由，以使配置的聚合路由变为活动状态。AS\_SET 包括聚合路由中包含的路由 AS\_PATH 和社区信息。

1. 在 CONFIGURATION 模式下分配 AS 编号。

```
router bgp as-number
```

2. 在 ROUTER-BGP 模式下输入地址系列模式。

```
address-family {[ipv4 | ipv6] [unicast]}
```

3. 在 ROUTER-BGPv4-AF 模式下聚合地址。

```
aggregate-address ip-address/mask
```

### 配置聚合路由

```
OS10(config)# router bgp 105
OS10(conf-router-bgp-105)# address-family ipv4 unicast
OS10(conf-router-bgpv4-af)# aggregate-address 3.3.0.0/16
```

### 查看正在运行的配置

```
OS10(conf-router-bgpv4-af)# do show running-configuration bgp
! Version
! Last configuration change at Jul 27 06:51:17 2016
!
!
router bgp 105
!
address-family ipv4 unicast
aggregate-address 3.3.0.0/16
!

neighbor 32.1.1.2
remote-as 104
no shutdown
!
address-family ipv4 unicast
```

## 联盟

在 AS 中组织路由器的另一种方式并且减少 IBGP 对等的网格是配置 BGP 联盟。与路由映射器一样，Dell EMC 建议仅将 BGP 联盟用于涉及每个路由器的许多 IBGP 对等会。

配置 BGP 联盟时，会将 AS 转换为较小的子 AS。对于网络外部设备，联盟显示为一个 AS。在联盟子 AS 中，IBGP 邻居是完全网状的并且 MED、NEXT\_HOP 和 LOCAL\_PREF 属性在联盟之间保持。

1. 在 ROUTER-BGP 模式下输入联盟 ID AS 编号（1 到 65535 适用于 2 字节，1 到 4294967295 适用于 4 字节）。

```
confederation identifier as-number
```

2. 在 ROUTER-BGP 模式下输入作为对等的联盟子 AS，从 1 到 65535 适用于 2 字节，1 到 4294967295 适用于 4 字节。所有联盟路由器必须为 4 字节或 2 字节。您不能混用路由器 ASN 支持。

```
confederation peers as-number [... as-number]
```

### 配置 BGP 联盟

```
OS10(config)# router bgp 65501
OS10(conf-router-bgp-65501)# confederation identifier 100
OS10(conf-router-bgp-65501)# confederation peers 65502 65503 65504
OS10(conf-router-bgp-65501)# neighbor 1.1.1.2
OS10(conf-router-neighbor)# remote-as 65502
OS10(conf-router-neighbor)# no shutdown
```



```

OS10(conf-router-neighbor)# exit
OS10(conf-router-bgp-65501)# neighbor 2.1.1.2
OS10(conf-router-neighbor)# remote-as 65503
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# exit
OS10(conf-router-bgp-65501)# neighbor 3.1.1.2
OS10(conf-router-neighbor)# remote-as 65504
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# exit
OS10(conf-router-bgp-65501)# end
OS10# show running-configuration bgp
!
router bgp 65501
 confederation identifier 100
 confederation peers 65502 65503 65504
 !
 neighbor 1.1.1.2
 remote-as 65502
 no shutdown
 !
 neighbor 2.1.1.2
 remote-as 65503
 no shutdown
 !
 neighbor 3.1.1.2
 remote-as 65504
 no shutdown

```

## 路由抑制

当 EBGp 路由变得不可用时，它们会“摆动”，并且路由器会发出“撤销”和“更新”通知。当路由撤销、撤销后重新通告或属性更改时，会发生摆动。

路由器对“撤销”和“更新”通知的持续反应会导致 BGP 进程不稳定。为了最大限度地减少这种不稳定性，请为摆动路由配置惩罚值（一个数值）。当该惩罚值达到配置的限制时，将不会通告路由，即使路由已打开，处罚值也是 1024。

随着时间的推移，路由仍未摆动，罚值将递减或衰退。如果路由再次摆动，则会为其分配另一个处罚。处罚值是累积的，添加了正在撤回、重新通告或属性更改。

当抑制应用到路由时，将通过以下方法描述其路径：

|               |                    |
|---------------|--------------------|
| <b>历史记录条目</b> | 存储有关发生停机的路由的信息的条目。 |
| <b>抑制路径</b>   | 不再通告的路径。           |
| <b>惩罚路径</b>   | 为其分配了惩罚的路径。        |

1. 在 ROUTER-BGP 模式下启用路由抑制。

```
dampening [half-life | reuse | max-suppress-time]
```

- *half-life* — 惩罚值降低之后的分钟数（1 到 45，默认为 15）。在路由器将 1024 的惩罚分配给某个路由后，该惩罚将在半生存期到期后减半。
- *reuse* — 数字与摆动路由的惩罚值进行比较。如果惩罚值小于重复使用值，则摆动路由再次通告或不再抑制（1 到 20000，默认为 750）。从历史记录状态中删除了提取的路由。
- *suppress* — 数字与摆动路由的惩罚值进行比较。如果惩罚值大于抑制值，则摆动路由将不再通告并被抑制（1 到 20000，默认为 2000）。
- *max-suppress-time* — 抑制路由的最大分钟数（1 到 255，默认值为半生存期的值或 60 分钟的四倍）。

2. 查看所有摆动统计信息或在 EXEC 模式下满足条件的特定路由。

```
show ip bgp flap-statistics [ip-address [mask]]
```

- *ip-address [mask]* — 输入 IP 地址和掩码。
- *filter-list as-path-name* — 输入 AS-PATH ACL 的名称。
- *regex regular-expression* — 输入要匹配的正则表达式。

更改最佳路径选择方法时，现有路径的路径选择将保持不变，除非您在 EXEC 模式下使用 `clear ip bgp` 命令对其进行重置。

## 配置值以重复使用或重新启动路由

```
OS10(config)# router bgp 102
OS10(config-router-bgp-102)# address-family ipv4 unicast
OS10(config-router-bgpv4-af)# dampening 2 2000 3000 10
```

## 查看抑制（非活动）路由

```
OS10# show ip bgp flap-statistics

BGP local router ID is 13.176.123.28
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network
From Reuse Path
Total number of prefixes: 0
```

## 查看抑制路径

```
OS10# show ip bgp dampened-paths

BGP local router ID is 80.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network From Reuse Path
d* 3.1.2.0/24 80.1.1.2 00:00:12 800 9 8 i
d* 3.1.3.0/24 80.1.1.2 00:00:12 800 9 8 i
d* 3.1.4.0/24 80.1.1.2 00:00:12 800 9 8 i
d* 3.1.5.0/24 80.1.1.2 00:00:12 800 9 8 i
d* 3.1.6.0/24 80.1.1.2 00:00:12 800 9 8 i
Total number of prefixes: 5
```

# 计时器

要调整所有邻居的路由计时器，请使用 `timers` 命令配置计时器值。如果两个对等节点均与不同的存活和保留时间值进行协商并保留时间值，则最终的保留时间值为接收到的最低值。新的存活时间值是接受的保留时间值的三分之一。

- 在 ROUTER-NEIGHBOR 模式下为所有邻居配置计时器值。

```
timers keepalive holdtime
```

- `keepalive` — 发送至邻居路由器的存活消息之间的时间间隔（以秒为单位）（1 到 65535，默认值为 60）。
- `holdtime` — 最后的存活消息与生命路由器死亡之间的时间间隔（以秒为单位）（3 到 65535，默认值为 180）。

## 更改计时器示例

```
OS10(config)# router bgp 102
OS10(config-router-bgp-102)# neighbor 10.5.2.3
OS10(config-router-neighbor)# timers 120 200
```

## 查看非默认值

```
OS10# show running-configuration
...
neighbor 32.1.1.2
remote-as 103
timers 120 200
no shutdown
```

# 邻居软重新配置

BGP 软重新配置允许快速路径更改。更改路由策略需要重置 BGP 会话或 TCP 连接，以使策略生效。

由于 BGP 高速缓存的硬重置以及重建会话所需的时间，重置导致流量不必要的中断。BGP 软重新配置允许将策略应用于会话而不清除 BGP 会话。您可以通过每个邻居执行软重新配置（入站或出站）。BGP 软重新配置会清除策略而不重置 TCP 连接。配置软重新配置后，使用 `clear ip bgp` 命令使邻居使用软重新配置。

为邻居启用软重新配置并运行 `clear ip bgp soft in` 命令时，存储在路由器重现和更新中的更新数据库将会重新评估。使用此命令时，仅当路由刷新请求未与对等控制器协商时，重现和更新过程才会触发。如果请求在使用 `clear ip bgp soft in` 命令之后协商，BGP 会将路由刷新请求发送到邻居，并接收对等方的所有更新。

要使用软重新配置或软重置而不进行预配置，两个 BGP 对等节点必须支持软路由刷新。在对等节点建立 TCP 会话的情况下，软路由将在 OPEN 消息中刷新通告。要确定 BGP 路由器是否支持此功能，请使用 `show ip bgp neighbors` 命令。如果路由器支持路由刷新功能，将显示 `Received route refresh capability from peer` 消息。

1. 为 ROUTER-BGP 模式下的 BGP 邻居和 BGP 模板启用软重新配置。BGP 存储邻居接收但不会重置对等会话的所有更新。使用此命令将启动更新的存储，这是入站软重新配置所必需的。

```
neighbor {ip-address} soft-reconfiguration inbound
```

2. 在 ROUTER-NEIGHBOR 模式下输入地址系列模式。

```
address-family {[ipv4 | ipv6] [unicast]}
```

3. 为属于模板的邻居配置软配置。

```
soft-reconfiguration inbound
```

4. 在 EXEC 模式下清除所有信息或仅特定的详细信息。

```
clear ip bgp {neighbor-address | *} [soft in]
```

- \* — 清除所有对等。
- neighbor-address — 使用此 IP 地址清除邻居。

## 对 IPv4 邻居进行软重新配置

```
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# soft-reconfiguration inbound
OS10(conf-router-bgp-neighbor-af)# end
OS10# clear ip bgp 10.2.1.2
```

## 对 IPv6 邻居进行软重新配置

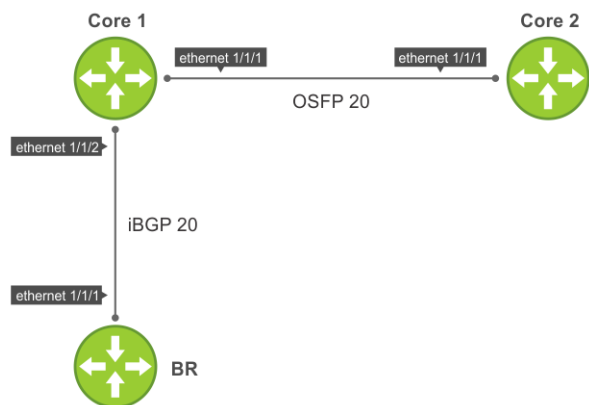
```
OS10(conf-router-neighbor)# address-family ipv6 unicast
OS10(conf-router-bgp-neighbor-af)# soft-reconfiguration inbound
OS10(conf-router-bgp-neighbor-af)# end
OS10# clear ip bgp 2001:0000:3221:DFE8:63::FEAB
```

# 重新分发 iBGP 路由到 OSPF

当您配置系统将 BGP 路由重新分发至 OSPF 时，默认情况下，系统仅重新分发 eBGP 路由。要将 iBGP 路由重新分发至 OSPF，请配置路由映射并将其应用到 OSPF 配置下的 `redistribute` 命令。

## 配置示例

以下示例拓扑具有两个交换机 Core 1 和 Core 2，它们分别相互连接，并使用 OSPF 共享路由。边界路由器 BR 连接到 Core 1，并使用内部 BGP 进行共享。Core 1 将由 iBGP 学习的路由重新分配至 Core 2 OSPF。



### BR 上的配置

BR 配置了 BGP，这将形成 BGP 邻居与 Core 1 的邻接关系。

```

interface Loopback0
 ip address 192.168.100.1/24
!
interface ethernet1/1/1
 no shutdown
 no switchport
 ip address 10.10.9.1
!
router bgp 20
 network 192.168.100.0
 neighbor 10.10.9.2 remote-as 20
 address-family ipv4 unicast

```

### Core 1 上的配置

Core 1 同时配置了 OSPF 和 BGP。Core 1 具有与 Core 2 的 OSPF 邻居邻接，并且 BGP 与 BR 邻居邻接。iBGPtoOSPF 前缀列表已配置并应用于路由映射。match ip address prefix-list iBGPtoOSPF 命令将处理 iBGP 学习的路由。

```

ip prefix-list iBGPtoOSPF seq 15 permit 192.168.100.0/24
route-map iBGPtoOSPF permit 20
 match ip address prefix-list iBGPtoOSPF
!
interface ethernet1/1/1
 no shutdown
 no switchport
 ip address 10.10.30.2/24
 ip router ospf 10 area 0.0.0.0
!
interface ethernet1/1/2
 no shutdown
 no switchport
 ip address 10.10.9.2/24
!
router ospf 10
 router-id 2.2.2.2
 redistribute bgp 20 route-map iBGPtoOSPF
!
router bgp 20
 neighbor 10.10.9.1
 remote-as 20
 address-family ipv4 unicast
 allowas-in 1

```

### Core 2 上的配置

Core 2 已配置 OSPF，其与 Core 1 形成邻居邻接。

```

interface ethernet1/1/1
 no shutdown
 no switchport
 ip address 10.10.30.3/24

```

```

ip router ospf 10 area 0.0.0.0
no shutdown
!
!
router ospf 10
router-id 3.3.3.3

```

### 示例 IPv6 配置

以下示例拓扑具有两个交换机 Core 1 和 Core 2，它们分别相互连接，并使用 OSPF 共享路由。边界路由器 BR 连接到 Core 1 并使用 BGP 共享路由。Core 1 将通过 iBGP 学习的路由重新分配到 OSPF 并与其他路由器共享。此网络使用 IPv6 寻址。

### BR 上的配置

BR 配置了 BGP，这将形成 BGP 邻居与 Core 1 的邻接关系。

```

interface Loopback0
 ipv6 address 2020::1/64
!
interface ethernet1/1/1
 no switchport
 ip address 2030::1/64
!
!
address-family ipv6 unicast
router bgp 20
 neighbor 2030::2 remote-as 20

```

### Core 1 上的配置

Core 1 同时配置了 OSPF 和 BGP。Core 1 具有与 Core 2 的 OSPF 邻居邻接，并且 BGP 与 BR 邻居邻接。iBGPtoOSPF 前缀列表已配置并应用于路由映射。match ip address prefix-list iBGPtoOSPF 命令将处理 iBGP 学习的路由。

```

ip prefix-list iBGPtoOSPF seq 15 permit 2020::1/64
route-map iBGPtoOSPF permit 20
 match ip address prefix-list iBGPtoOSPF
!
!
interface ethernet1/1/1
 no switchport
 ipv6 address 2035::1/64
 ipv6 ospf 10 area 0.0.0.0
 no shutdown
!
interface Ethernet1/1/2
 no switchport
 ipv6 address 2030::2/64
 no shutdown
!
router ospfv3 10
 router-id 2.2.2.2
 redistribute bgp 10 route-map iBGPtoOSPF
!
router bgp 20
 neighbor 2030::1
 remote-as 20
 address-family ipv6 unicast
 activate
 allowas-in 1

```

### Core 2 上的配置

Core 2 已配置 OSPF，其与 Core 1 形成邻居邻接。

```

interface Ethernet 1/1/1
 no switchport
 ipv6 address 2035::2/64
 ipv6 ospf 10 area 0.0.0.0
 no shutdown
!
router ospfv3 10
 router-id 3.3.3.3

```

# 调试 BGP

使用以下过程调试 BGP。

- 要调试 BGP：

```
debug ip bgp
```

## BGP 命令

### activate

使邻居或对等组成为当前的地址系列标识符 (AFI)。

|        |                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | activate                                                                                                                                 |
| 参数     | 无                                                                                                                                        |
| 默认     | 未配置                                                                                                                                      |
| 命令模式   | ROUTER-BGP-NEIGHBOR-AF                                                                                                                   |
| 使用情况信息 | 此命令与 IPv4 或 IPv6 邻居交换 IPv4 或 IPv6 地址系列信息。默认情况下，IPv4 单播地址系列已启用。要激活 IPv6 邻居的 IPv6 地址系列，请使用 activate 命令。要为 IPv6 邻居停用 IPv4 地址系列，请使用 no 激活命令。 |
| 示例     | <pre>OS10(conf-router-neighbor)# address-family ipv4 unicast OS10(conf-router-bgp-neighbor-af)# activate</pre>                           |
| 支持的版本  | 10.2.0E or later                                                                                                                         |

### add-path

允许系统通告同一目标的多条路径，而不会将以前的路径替换为新路径。

|           |                                                                                                                                                                                           |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法        | add-path {both path count   receive   send path count}                                                                                                                                    |
| 参数        | <ul style="list-style-type: none"><li>• both path count — 输入要向对等节点通告的路径数量，从 2 到 64。</li><li>• receive — 从对等节点接收多条路径。</li><li>• send path count — 输入将多个路径发送至对等的多个路径的数量，从 2 到 64。</li></ul> |
| 默认        | 未配置                                                                                                                                                                                       |
| 命令模式      | ROUTER-BGP-NEIGHBOR-AF                                                                                                                                                                    |
| 使用情况信息    | 在不使用新路径替换现有路径的情况下，为相同地址前缀通告对等节点的多条路径将缩短聚合时间。此命令的 no 版本将禁用同一目标的多个路径通告。                                                                                                                     |
| 示例 (IPv4) | <pre>OS10(conf-router-bgp-af)# add-path both 64</pre>                                                                                                                                     |
| 示例 (IPv6) | <pre>OS10(conf-router-bgpv6-af)# add-path both 64</pre>                                                                                                                                   |
| 示例 (接收)   | <pre>OS10(conf-router-bgpv6-af)# add-path receive</pre>                                                                                                                                   |
| 支持的版本     | 10.2.0E or later                                                                                                                                                                          |

## address-family

进入 IP 地址系列的全局地址系列配置模式。

|              |                                                                                                                                                 |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法           | <code>address-family {[ipv4   ipv6] unicast}</code>                                                                                             |
| 参数           | <ul style="list-style-type: none"><li><code>ipv4 unicast</code> — 输入 IPv4 单播地址系列。</li><li><code>ipv6 unicast</code> — 输入 IPv6 单播地址系列。</li></ul> |
| 默认           | 无                                                                                                                                               |
| 命令模式         | ROUTER-BGP                                                                                                                                      |
| 使用情况信息       | 此命令仅适用于属于模板或邻居的所有 IPv4 或 IPv6 对等方。此命令的 <code>no</code> 版本将删除后续的地址系列配置。                                                                          |
| 示例 (IPv4 单播) | <pre>OS10(config)# router bgp 3 OS10(conf-router-bgp-3)# address-family ipv4 unicast OS10(conf-router-bgpv4-af)#</pre>                          |
| 示例 (IPv6 单播) | <pre>OS10(config)# router bgp 4 OS10(conf-router-bgp-4)# address-family ipv6 unicast OS10(conf-router-bgpv6-af)#</pre>                          |
| 支持的版本        | 10.3.0E or later                                                                                                                                |

## advertisement-interval

设置 BGP 邻居之间或 BGP 对等组内的通告的最短时间间隔。

|        |                                                                            |
|--------|----------------------------------------------------------------------------|
| 语法     | <code>advertisement-interval seconds</code>                                |
| 参数     | <code>seconds</code> — 以秒为单位输入 BGP 通告之间的时间间隔值，从 1 到 600。                   |
| 默认     | EBGP 30 秒，IBGP 5 秒                                                         |
| 命令模式   | ROUTER-NEIGHBOR                                                            |
| 使用情况信息 | 时间间隔适用于 ROUTER-TEMPLATE 模式下模板的所有对等组成员。此命令的 <code>no</code> 版本将通告间隔值重置为默认值。 |
| 示例     | <pre>OS10(conf-router-neighbor)# advertisement-interval 50</pre>           |
| 支持的版本  | 10.3.0E or later                                                           |

## advertisement-start

延迟在指定时间启动 OPEN 消息。

|        |                                                                           |
|--------|---------------------------------------------------------------------------|
| 语法     | <code>advertisement-start seconds</code>                                  |
| 参数     | <code>seconds</code> — 输入在开始发送 BGP OPEN 消息之前的时间间隔值（以秒为单位），从 0 到 240。      |
| 默认     | 未配置                                                                       |
| 命令模式   | ROUTER-NEIGHBOR                                                           |
| 使用情况信息 | 时间间隔适用于 ROUTER-TEMPLATE 模式下模板的所有对等组成员。此命令的 <code>no</code> 版本将禁用通告开始时间间隔。 |
| 示例     | <pre>OS10(conf-router-neighbor)# advertisement-start 30</pre>             |
| 支持的版本  | 10.3.0E or later                                                          |

## aggregate-address

汇总了一系列前缀，以更大限度减少路由表中的条目数。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>aggregate-address address/mask [as-set] [summary-only] [advertise-map map-name] [attribute-map route-map-name] [suppress-map route-map-name]</code>                                                                                                                                                                                                                                                                               |
| 参数     | <ul style="list-style-type: none"><li>• <code>address/mask</code> — 输入 IP 地址和掩码。</li><li>• <code>as-set</code> — (可选) 生成 AS 设置路径信息。</li><li>• <code>summary-only</code> — (可选) 从更新中筛选更具体的路由。</li><li>• <code>advertise-map map-name</code> — (可选) 输入要通告的映射名称。</li><li>• <code>attribute-map route-map-name</code> — (可选) 输入路由映射名称以设置聚合属性。</li><li>• <code>suppress-map route-map-name</code> — (可选) 输入路由映射名称以有条件地筛选来自更新的特定路由。</li></ul> |
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 命令模式   | ROUTER-BGPv4-AF                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | 必须在 BGP 路由表中包括聚合地址中的至少一个路由，以使配置的聚合变为活动状态。如果聚合内的路由持续更改，请勿将 <code>as-set</code> 参数添加到聚合中，因为聚合变动会跟踪 AS_PATH 中的更改。此命令的 <code>no</code> 版本将禁用聚合地址配置。                                                                                                                                                                                                                                                                                         |
| 示例     | <pre>OS10(config-router-bgpv4-af)# aggregate-address 6.1.0.0/16 summary-only</pre>                                                                                                                                                                                                                                                                                                                                                      |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                        |

## allowas-in

配置在交换机拒绝路由之前，本地 AS 编号在 BGP AS\_PATH 路径属性中可以出现的次数。

|           |                                                                                                                        |
|-----------|------------------------------------------------------------------------------------------------------------------------|
| 语法        | <code>allowas-in as-number</code>                                                                                      |
| 参数        | <code>as-number</code> — 输入局部变量的次数，从 1 到 10。                                                                           |
| 默认        | 已禁用                                                                                                                    |
| 命令模式      | ROUTER-BPG-NEIGHBOR-AF                                                                                                 |
| 使用情况信息    | 使用此命令可启用 BGP 扬声器，以接受更新中对对等体收到的指定次数的本地 AS 数字。此命令的 <code>no</code> 版本会将该值重置为默认值。                                         |
| 示例 (IPv4) | <pre>OS10(config-router-neighbor)# address-family ipv4 unicast OS10(config-router-bgp-neighbor-af)# allowas-in 5</pre> |
| 示例 (IPv6) | <pre>OS10(config-router-template)# address-family ipv6 unicast OS10(config-router-bgp-template-af)# allowas-in 5</pre> |
| 支持的版本     | 10.3.0E or later                                                                                                       |

## always-compare-med

比较从不同邻居接收的路径中 MULTI\_EXIT\_DISC (MED) 属性。

|        |                                                                                     |
|--------|-------------------------------------------------------------------------------------|
| 语法     | <code>always-compare-med</code>                                                     |
| 参数     | 无                                                                                   |
| 默认     | 已禁用                                                                                 |
| 命令模式   | ROUTER-BGP                                                                          |
| 使用情况信息 | 使用此命令后，使用 <code>clear ip bgp *</code> 命令重新计算最佳路径。此命令的 <code>no</code> 版本会将该值重置为默认值。 |



- 注:** 要为非默认 VRF 实例配置这些设置, 先使用以下命令进入 ROUTER-CONFIG-VRF 子模式:
1. 使用 `router bgp as-number` 命令进入 ROUTER BGP 模式。
  2. 在 ROUTER BGP 模式下, 使用 `vrf vrf-name` 命令进入 ROUTER BGP VRF 模式。

#### 示例

```
OS10(conf-router-bgp-10)# always-compare-med
```

#### 支持的版本

10.2.0E or later

## as-notation

更改 AS 数字表示法的格式, 并且需要 four-octet-assupport。

**语法** `as-format {asdot | asdot+ | asplain}`

- 参数**
- `asdot` — 指定为 `asdot` 格式的 AS 数字表示法。
  - `asdot+` — 指定为 `asdot+` 格式的 AS 数字表示法。
  - `asplain` — 指定为 `asplain` 格式的 AS 数字表示法。

**默认** `asplain`

**命令模式** ROUTER-BGP

- 使用情况信息**
- 注:** 要为非默认 VRF 实例配置这些设置, 请先使用以下命令进入 ROUTER-CONFIG-VRF 子模式:
1. 使用 `router bgp as-number` 命令进入 ROUTER BGP 模式。
  2. 在 ROUTER BGP 模式下, 使用 `vrf vrf-name` 命令进入 ROUTER BGP VRF 模式。

#### 示例

```
OS10(conf-router-bgp-2)# as-notation asdot
OS10(conf-router-bgp-2)# as-notation asdot+
OS10(conf-router-bgp-2)# as-notation asplain
```

#### 支持的版本

10.1.0E or later

## bestpath as-path

为最佳路径计算配置 AS 路径选择条件。

**语法** `bestpath as-path {ignore | multipath-relax}`

- 参数**
- `ignore` — 输入以在 BGP 最佳路径计算中忽略 AS 路径。
  - `multipath-relax` — 输入以在多路径计算期间包含从不同 AS 路径接收的前缀。

**默认** 已启用

**命令模式** ROUTER-BGP

**使用情况信息** 要在不同的 EBGP 对等节点上启用负载均衡, 请配置 `multipath-relax` 选项。如果同时配置 `ignore` 或 `multipath-relax` 选项, 则会显示系统生成的错误消息。此命令的 `no` 版本将禁用配置。

- 注:** 要为非默认 VRF 实例配置这些设置, 先使用以下命令进入 ROUTER-CONFIG-VRF 子模式:
1. 使用 `router bgp as-number` 命令进入 ROUTER BGP 模式。
  2. 在 ROUTER BGP 模式下, 使用 `vrf vrf-name` 命令进入 ROUTER BGP VRF 模式。

#### 示例

```
OS10(conf-router-bgp-10)# bestpath as-path multipath-relax
```

#### 支持的版本

10.3.0E or later

## bestpath med

更改针对路径选择比较 MED 的过程中的最佳路径 MED 属性。

|        |                                                                                                                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>bestpath med {confed   missing-as-worst}</code>                                                                                                                                                                                                                                                                                                      |
| 参数     | <ul style="list-style-type: none"><li><code>confed</code> — 比较 BGP 联合路径中的 MED。</li><li><code>missing-as-worst</code> — 将缺失的 MED 视为最不首选的路径。</li></ul>                                                                                                                                                                                                       |
| 默认     | 已禁用                                                                                                                                                                                                                                                                                                                                                        |
| 命令模式   | ROUTER-BGP                                                                                                                                                                                                                                                                                                                                                 |
| 使用情况信息 | <p>在应用此命令之前，请使用 <code>always-compare-med</code> 命令。此命令的 <code>no</code> 版本将重置 MED 比较影响。</p> <p><b>注：</b> 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式：</p> <ol style="list-style-type: none"><li>使用 <code>router bgp as-number</code> 命令进入 ROUTER BGP 模式。</li><li>在 ROUTER BGP 模式下，使用 <code>vrf vrf-name</code> 命令进入 ROUTER BGP VRF 模式。</li></ol> |
| 示例     | <pre>OS10(conf-router-bgp-2)# bestpath med confed</pre>                                                                                                                                                                                                                                                                                                    |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                           |

## bestpath router-id

在最佳路径选择期间，忽略外部路径的路由器 id 信息比较。

|        |                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>bestpath router-id {ignore}</code>                                                                                                                                                                                                                                                                                                                           |
| 参数     | <code>ignore</code> — 输入以针对最佳路径计算忽略 AS 路径。                                                                                                                                                                                                                                                                                                                         |
| 默认     | 已启用                                                                                                                                                                                                                                                                                                                                                                |
| 命令模式   | ROUTER-BGP                                                                                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | <p>如果您未收到多个路径的相同路由器 ID，请选择您首先收到的路径。如果针对多个路径收到了相同的路由器 ID，请忽略路径信息。此命令的 <code>no</code> 版本会将该值重置为默认值。</p> <p><b>注：</b> 要为非默认 VRF 实例配置这些设置，先使用以下命令进入 ROUTER-CONFIG-VRF 子模式：</p> <ol style="list-style-type: none"><li>使用 <code>router bgp as-number</code> 命令进入 ROUTER BGP 模式。</li><li>在 ROUTER BGP 模式下，使用 <code>vrf vrf-name</code> 命令进入 ROUTER BGP VRF 模式。</li></ol> |
| 示例     | <pre>OS10(conf-router-bgp-2)# bestpath router-id ignore</pre>                                                                                                                                                                                                                                                                                                      |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                                   |

## clear ip bgp

重置 BGP IPv4 或 IPv6 邻居会话。

|      |                                                                                                                                                                                                                                                                                                                                                            |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | <code>clear ip bgp [vrf vrf-name] {ipv4-address   ipv6-address   *} [ipv4   ipv6   soft in]</code>                                                                                                                                                                                                                                                         |
| 参数   | <ul style="list-style-type: none"><li><code>vrf vrf-name</code> — (可选) 输入 vrf 和 VRF 的名称，以清除与该 VRF 对应的 IPv4 或 IPv6 BGP 邻居会话的名称。</li><li><code>IPv4-address</code> — 输入 IPv4 地址以清除 BGP 邻居配置。</li><li><code>IPv6-address</code> — 输入 IPv6 地址以清除 BGP 邻居配置。</li><li><code>*</code> — 清除所有 BGP 会话。</li><li><code>soft</code> — 配置和激活策略而不重置 BGP TCP 会话。</li></ul> |
| 默认   | 未配置                                                                                                                                                                                                                                                                                                                                                        |
| 命令模式 | EXEC                                                                                                                                                                                                                                                                                                                                                       |

**使用情况信息** 无。

**示例**

```
OS10# clear ip bgp 1.1.15.4
```

**支持的版本** 10.3.0E or later

## clear ip bgp \*

重置 BGP 会话。软参数、BGP 软重新配置、清除策略而不重置 TCP 连接。

**语法** `clear ip bgp * [soft [in | out]]`

**参数**

- `*` — 输入以清除所有 BGP 会话。
- `soft` — (可选) 输入以配置和激活策略而不重置 BGP TCP 会话 — BGP 软重新配置。
- `in` — (可选) 输入以仅激活入口 (入站) 策略。
- `out` — (可选) 输入以仅激活出口 (出站) 策略。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无。

**示例**

```
OS10# clear ip bgp *
```

**支持的版本** 10.3.0E or later

## clear ip bgp dampening

清除抑制和取消抑制前缀的路径信息。

**语法** `clear ip bgp dampening [vrf vrf-name] [ipv4-prefix | ipv6-prefix]`

**参数**

- `vrf vrf-name` — (可选) 输入 `vrf` 和 VRF 的名称以清除抑制路径信息。
- `ipv4-prefix` — (可选) 输入抑制路径的 IPv4 前缀。
- `ipv6-prefix` — (可选) 输入抑制路径的 IPv6 前缀。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# clear ip bgp dampening 1.1.15.5
```

**支持的版本** 10.3.0E or later

## clear ip bgp flap-statistics

清除前缀的所有或特定 IPv4 或 IPv6 摆动计数。

**语法** `clear ip bgp [vrf vrf-name] [ipv4-address | ipv6-address] flap-statistics [ipv4-prefix | ipv6-prefix]`

**参数**

- `vrf vrf-name` — (可选) 输入 `vrf`, 然后输入 VRF 的名称以清除摆动统计信息。
- `ipv4-address` — (可选) 输入 IPv4 地址以清除从指定对等方获知的前缀的摆动计数。
- `ipv6-address` — (可选) 输入 IPv6 地址以清除摆动计数。
- `ipv4-prefix` — (可选) 输入 IPv4 前缀以清除给定前缀的摆动计数。
- `ipv6-prefix` — (可选) 输入 IPv6 前缀以清除给定前缀的摆动计数。

**默认** 未配置

|          |                                                           |
|----------|-----------------------------------------------------------|
| 命令模式     | EXEC                                                      |
| 使用情况信息   | 无                                                         |
| 示例（所有前缀） | <pre>OS10# clear ip bgp flap-statistics</pre>             |
| 示例（IPv4） | <pre>OS10# clear ip bgp 1.1.15.4 flap-statistics</pre>    |
| 示例（给定前缀） | <pre>OS10# clear ip bgp flap-statistics 1.1.15.0/24</pre> |
| 支持的版本    | 10.3.0E or later                                          |

## connection-retry-timer

配置计时器以重试到 BGP 邻居或对等组的连接。

|        |                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>connection-retry-timer retry-timer-value</code>                                                                         |
| 参数     | <code>retry-timer-value</code> — 输入时间间隔（以秒为单位的），从 10 到 65535。                                                                 |
| 默认     | 60 秒                                                                                                                          |
| 命令模式   | CONFIG-ROUTER-NEIGHBOR<br>CONFIG-ROUTER-TEMPLATE                                                                              |
| 使用情况信息 | 此命令的 <code>no</code> 版本将计时器重置为默认值。                                                                                            |
| 示例     | <pre>OS10(config-router-neighbor)# connection-retry-timer 1000 OS10(config-router-template)# connection-retry-timer 100</pre> |
| 支持的版本  | 10.3.0E or later                                                                                                              |

## confederation

为 BGP 联盟配置标识符。

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法      | <code>confederation {identifier as-num   peers as-number}</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 参数      | <ul style="list-style-type: none"> <li><code>identifier as-num</code> — 输入 AS 编号，从 0 到 65535 适用于 2 字节，从 1 到 4294967295 适用于 4 字节，或从 0.1 到 65535.65535 适用于点分隔格式。</li> <li><code>peers as-number</code>— 为 BGP 联盟中的对等节点输入数字，从 1 到 4294967295。</li> </ul>                                                                                                                                                                                                                                                                                                                                                             |
| 默认      | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 命令模式    | ROUTER-BGP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 使用情况信息  | <p>将系统配置为接受 4 字节格式，然后输入 4 字节 AS 数字。联盟中的所有路由器必须为 4 字节或 2 字节标识的路由器。您不能混用 2 字节和 4 字节标识的路由器。在此命令中配置的自治系统编号对 EBGp 邻居可见。每个自治系统都是完全网状的，并包含一些与其他自治系统的连接。在整个联盟中保留下一跳 (MED) 和本地首选项信息。系统接受不带 LOCAL_PREF 属性的联盟 EBGp 对等节点。OS10 发送 AS_CONFED_SET 并接受 AS_CONFED_SET 和 AS_CONF_SEQ。此命令的 <code>no</code> 版本将删除联盟配置。</p> <div> <div> <i>i</i> </div> <div> <b>注：</b> 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式： <ol style="list-style-type: none"> <li>使用 <code>router bgp as-number</code> 命令进入 ROUTER BGP 模式。</li> <li>在 ROUTER BGP 模式下，使用 <code>vrf vrf-name</code> 命令进入 ROUTER BGP VRF 模式。</li> </ol> </div> </div> |
| 示例（标识符） | <pre>OS10(conf-router-bgp-2)# confederation identifier 1</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

### 示例（对等节点）

```
OS10(conf-router-bgp-2)# confederation peers 2
```

支持的版本 10.3.0E or later

## client-to-client

启用群集中客户端之间的路由反射。

**语法** `client-to-client {reflection}`

**参数** `reflection` — 输入以启用在群集中允许的路由反射。

**默认** 已启用

**命令模式** ROUTER-BGP

**使用情况信息** 配置路由反射器以启用所有客户端之间的路由反射。您必须完全啮合所有客户端，然后再禁用路由反射。此命令的 `no` 版本将禁用群集中的路由反射。

**注:** 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式：

1. 使用 `router bgp as-number` 命令进入 ROUTER BGP 模式。
2. 在 ROUTER BGP 模式下，使用 `vrf vrf-name` 命令进入 ROUTER BGP VRF 模式。

### 示例

```
OS10(conf-router-bgp-2)# client-to-client reflection
```

支持的版本 10.2.0E or later

## cluster-id

为具有多个路由反射器的 BGP 群集分配群集 ID。

**语法** `cluster-id {number | ip-address}`

- 参数**
- `number`— 以 32 位数字输入路由反射器群集 ID，从 1 到 4294967295。
  - `ip-address`— 输入 IP 地址作为路由反射器群集 ID。

**默认** 路由器 ID

**命令模式** ROUTER-BGP

**使用情况信息** 如果一个群集只包含一个路由反射器，则该群集 ID 为路由反射器的路由器 ID。为实现冗余，BGP 群集可能包含两个或更多路由反射器。如果没有群集 ID，路由反射器将无法从群集内的其他路由反射器识别路由更新。显示群集 ID 的默认格式为 A.B.C.D 格式。如果您将群集 ID 输入为整数，则将显示一个整数。此命令的 `no` 版本会将该值重置为默认值。

**注:** 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式：

1. 使用 `router bgp as-number` 命令进入 ROUTER BGP 模式。
2. 在 ROUTER BGP 模式下，使用 `vrf vrf-name` 命令进入 ROUTER BGP VRF 模式。

### 示例

```
OS10(conf-router-bgp-10)# cluster-id 3.3.3.3
```

支持的版本 10.3.0E or later

## bgp dampening

启用 BGP 路由摆动抑制并配置抑制参数。

**语法** `bgp dampening [half-life | reuse-limit | suppress-limit | max-suppress-time | route-map-name]`

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 参数     | <ul style="list-style-type: none"> <li><i>half-life</i> — (可选) 输入半寿命时间 (以分钟为单位), 在该时间段后惩罚将降低。在路由器将 1024 的惩罚分配给某个路由后, 该惩罚将在半生存期到期后减半, 从 1 到 45。</li> <li><i>reuse-limit</i> — (可选) 输入重复使用限制值, 这将与摆动路由的惩罚值进行比较。如果惩罚值小于重复使用值, 则摆动路由将再次通告, 并且不会被抑制, 从 1 到 20000。</li> <li><i>suppress-limit</i> — (可选) 输入抑制-限制值, 这将与摆动路由的惩罚值进行比较。如果惩罚值大于抑制值, 则不再通告摆动路由, 从 1 到 20000。</li> <li><i>max-suppress-time</i> — (可选) 输入抑制路由的最大分钟数, 从 1 到 255。</li> <li><i>route-map-name</i> — (可选) 输入路由映射的名称。</li> </ul> |
| 默认     | half-life 15; reuse-limit 750; suppress-limit 2000; max-suppress-time 60                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 命令模式   | ROUTER-BGP-AF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 使用情况信息 | 要降低 BGP 进程的不稳定性, 请设置路由摆动抑制参数。设置抑制参数后, 请清除有关路由抑制的信息, 并将抑制的路由返回到 Active 状态。您还可以查看有关路由摆动的统计信息, 或者将路径选择从默认确定性模式下更改为非确定性模式。此命令的 no 版本会将该值重置为默认值。                                                                                                                                                                                                                                                                                                                                                    |
| 示例     | <pre>OS10(config-router-bgpv4-af)# dampening 2 751 2001 51 map1</pre>                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## debug ip bgp

启用边界网关协议 (BGP) 调试并显示与 BGP 处理相关的消息。

|        |                                       |
|--------|---------------------------------------|
| 语法     | debug ip bgp                          |
| 参数     | 无                                     |
| 默认     | 无                                     |
| 命令模式   | EXEC                                  |
| 使用情况信息 | no debug ip bgp 命令将停止显示与 BGP 处理相关的消息。 |
| 示例     | <pre>OS10# debug ip bgp</pre>         |
| 支持的版本  | OS10 原有命令。                            |

## description

为 BGP 邻居或对等模板配置说明。

|        |                                                                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | description text                                                                                                                                                                                                                                                                                            |
| 参数     | text — 输入 BGP 邻居或对等模板的说明。                                                                                                                                                                                                                                                                                   |
| 默认     | 无                                                                                                                                                                                                                                                                                                           |
| 命令模式   | ROUTER-BGP-NEIGHBOR<br>ROUTER-BGP-TEMPLATE                                                                                                                                                                                                                                                                  |
| 使用情况信息 | 此命令的 no 版本将移除该说明。                                                                                                                                                                                                                                                                                           |
| 示例     | <pre>OS10# configure terminal OS10(config)# router bgp 100 OS10(config-router-bgp-100)# neighbor 8.8.8.8 OS10(config-router-neighbor)# description n1_abcd OS10(config-router-neighbor)# exit OS10(config-router-bgp-100)# template t1 OS10(config-router-template)# description peer_template_1_abcd</pre> |
| 支持的版本  | 10.4.1.0 or later                                                                                                                                                                                                                                                                                           |

## default-metric

将重新分配的路由的默认指标分配到本地发起的路由。

|           |                                                                                                                                                                                                                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法        | <code>default-metric number</code>                                                                                                                                                                                                                                                                     |
| 参数        | <i>number</i> — 输入要分配给来自其他协议的路由的数字，从 1 到 4294967295。                                                                                                                                                                                                                                                   |
| 默认        | 已禁用                                                                                                                                                                                                                                                                                                    |
| 命令模式      | ROUTER-BGP                                                                                                                                                                                                                                                                                             |
| 使用情况信息    | 为本地发起的路由（如重新分发的路由）分配指标。重新分发 BGP 中的路由后，使用此命令重置指标值 — 新指标不会立即生效。仅当您禁用并重新启用指定协议的路由重新分发后，新指标才会生效。要重新启用路由分配，请使用 <code>redistribute {connected [route-map map-name]   ospf process-id   static [route-map map-name]}</code> 命令，或者在重置 BGP 之后使用 <code>clear ip bgp *</code> 命令。此命令的 <code>no</code> 版本将移除默认度量值。 |
| 示例 (IPv4) | <pre>OS10(conf-router-bgpv4-af)# default-metric 60</pre>                                                                                                                                                                                                                                               |
| 示例 (IPv6) | <pre>OS10(conf-router-bgpv6-af)# default-metric 60</pre>                                                                                                                                                                                                                                               |
| 支持的版本     | 10.3.0E or later                                                                                                                                                                                                                                                                                       |

## default-originate

配置到 BGP 对等节点或邻居的默认路由。

|        |                                                                                                                                                                                     |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>default-originate [route-map route-map-name]</code>                                                                                                                           |
| 参数     | <i>route-map route-map-name</i> — （可选）输入路由映射名称。最多 140 个字符。                                                                                                                          |
| 默认     | 已启用                                                                                                                                                                                 |
| 命令模式   | ROUTER-BGP-NEIGHBOR-AF<br>ROUTER-TEMPLATE-AF                                                                                                                                        |
| 使用情况信息 | 此命令的 <code>no</code> 版本将移除默认路由。                                                                                                                                                     |
| 示例     | <pre>OS10(conf-router-bgp-10)# template lunar OS10(conf-router-bgp-template)# address-family ipv6 unicast OS10(conf-router-template-af)# default-originate route-map rmap-bgp</pre> |
| 支持的版本  | 10.4.1.0 or later                                                                                                                                                                   |

## distance bgp

设置 BGP 路由的管理距离。

|      |                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | <code>distance bgp external-distance internal-distance local-distance</code>                                                                                                                                                                                                   |
| 参数   | <ul style="list-style-type: none"><li><i>external-distance</i> — 输入要分配给从 AS 外部的邻居获知的路由的编号，从 1 到 255。</li><li><i>internal-distance</i> — 输入要分配给从 AS 中的路由器获知的路由的编号，从 1 到 255。</li><li><i>local-distance</i> — 输入要分配给从 <code>network</code> 命令中列出的网络获知的路由的编号，从 1 到 255。</li></ul> |
| 默认   | <ul style="list-style-type: none"><li><i>external-distance</i> — 20</li><li><i>internal-distance</i> — 200</li><li><i>local-distance</i> — 200</li></ul>                                                                                                                       |
| 命令模式 | <ul style="list-style-type: none"><li>CONFIG-ROUTER-BGP-ADDRESS-FAMILY</li><li>CONFIG-ROUTER-BGP-VRF-ADDRESS-FAMILY</li></ul>                                                                                                                                                  |

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 使用情况信息 | 此命令用于配置 eBGP 路由、iBGP 路由和本地 BGP 路由的管理距离。管理距离表示路由的可靠性；管理距离越低，路由就越可靠。路由表中未安装分配了 255 的管理距离的路由。来联合的路由被视为 iBGP 路由。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 示例     | <p>默认 VRF:</p> <p>IPv4</p> <pre>OS10# configure terminal OS10(config)# router bgp 100 OS10(config-router-bgp-100)# address-family ipv4 unicast OS10(configure-router-bgpv4-af)# distance bgp 10 200 210</pre> <p>IPv6</p> <pre>OS10# configure terminal OS10(config)# router bgp 100 OS10(config-router-bgp-100)# address-family ipv6 unicast OS10(configure-router-bgpv6-af)# distance bgp 10 200 210</pre> <p>非默认 VRF</p> <pre>OS10(config-router-bgp-100)# vrf blue OS10(config-router-bgp-100-vrf)# address-family ipv4 unicast OS10(configure-router-bgpv4-vrf-af)# distance bgp 21 200 200 OS10(config-router-bgp-100-vrf)# address-family ipv6 unicast OS10(configure-router-bgpv6-vrf-af)# distance bgp 21 201 250</pre> |
| 支持的版本  | 10.4.2.0 或更高版本                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

distributed-list

通过已建立的前缀列表分发 BGP 信息。

|        |                                                                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>distributed-list prefix-list-name {in   out}</code>                                                                                                                                                                                                         |
| 参数     | <ul style="list-style-type: none"><li><code>prefix-list-name</code>— 输入已建立前缀列表的名称。</li><li><code>in</code> — 输入以分发入站流量。</li><li><code>out</code> — 输入以分发出站流量。</li></ul>                                                                                           |
| 默认     | 无                                                                                                                                                                                                                                                                 |
| 命令模式   | ROUTER-BGP-NEIGHBOR-AF<br>ROUTER-TEMPLATE-AF                                                                                                                                                                                                                      |
| 使用情况信息 | 此命令的 no 版本将移除 route-map。                                                                                                                                                                                                                                          |
| 示例     | <pre>OS10(conf-router-neighbor)# address-family ipv4 unicast OS10(conf-router-bgp-neighbor-af)# distributed-list inbgg in</pre> <pre>OS10(conf-router-template)# address-family ipv4 unicast OS10(conf-router-bgp-template-af)# distributed-list outbgg out</pre> |
| 支持的版本  | 10.4.1.0 or later                                                                                                                                                                                                                                                 |

bgp 默认本地-首选项

更改在内部 BGP 对等主机之间交换的路由的默认本地首选项值。

|    |                                                                                         |
|----|-----------------------------------------------------------------------------------------|
| 语法 | <code>default local-preference number</code>                                            |
| 参数 | <code>number</code> — 输入要分配给路由的数字，作为这些路由的优先级别。当路由比较时，首选具有较高优先级或本地首选项值，从 1 到 4294967295。 |



|        |                                                                  |
|--------|------------------------------------------------------------------|
| 默认     | 100                                                              |
| 命令模式   | ROUTER-BGP                                                       |
| 使用情况信息 | 所有路由器在 AS 中应用此命令设置。此命令的 <code>no</code> 版本会删除本地首选项值。             |
| 示例     | <pre>OS10(conf-router-bgp-1)# default local-preference 200</pre> |
| 支持的版本  | 10.3.0E or later                                                 |

## ebgp-multihop

允许间接连接网络上的 eBGP 邻居。

|        |                                                                                         |
|--------|-----------------------------------------------------------------------------------------|
| 语法     | <code>ebgp-multihop hop count</code>                                                    |
| 参数     | <code>hop count</code> — 为跳数输入一个值，从 1 到 255。                                            |
| 默认     | 对于 eBGP 为 1。对于 iBGP 为 255。                                                              |
| 命令模式   | ROUTER-NEIGHBOR                                                                         |
| 使用情况信息 | 此命令可避免安装默认的多跳的对等路由，以防止循环并在对等之间创建邻居关系。间接连接的网络对于最佳路径选择无效。此命令的 <code>no</code> 版本将移除多跳的会话。 |
| 示例     | <pre>OS10(conf-router-neighbor)# ebgp-multihop 2</pre>                                  |
| 支持的版本  | 10.3.0E or later                                                                        |

## enforce-first-as

强制实施从 EBGP 对等体收到的路由的 AS 路径中的第一个 AS 与配置的远程 AS 相同。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>enforce-first-as</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 默认     | 已启用                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 命令模式   | ROUTER-BGP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 使用情况信息 | <p>要验证已拒绝路由的统计信息，请使用 <code>show ip bgp neighbors</code> 命令。如果路由被拒绝，则重置会话。在发生故障时，现有 BGP 会话会抖动。对于从 EBGP 对等体收到的更新，BGP 可确保第一个 AS 段中的第一个 AS 与对等体始终一样，否则更新将丢弃并且计数器增量。此命令的 <code>no</code> 版本将关闭默认设置。</p> <p> <b>注：</b> 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式：</p> <ol style="list-style-type: none"><li>1. 使用 <code>router bgp as-number</code> 命令进入 ROUTER BGP 模式。</li><li>2. 在 ROUTER BGP 模式下，使用 <code>vrf vrf-name</code> 命令进入 ROUTER BGP VRF 模式。</li></ol> |
| 示例     | <pre>OS10(conf-router-bgp-1)# enforce-first-as</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## fall-over

为 BGP 邻居启用或禁用 BGP 会话快速回滚。

|    |                        |
|----|------------------------|
| 语法 | <code>fall-over</code> |
| 参数 | 无                      |
| 默认 | 已禁用                    |

|        |                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 命令模式   | ROUTER-NEIGHBOR                                                                                                                                                      |
| 使用情况信息 | 按每个邻居或对等组配置 BGP 快速回滚。当您在模板上启用此命令时，它将同时启用所有继承对等组模板的对等方。启用故障切换时，BGP 会跟踪对等远程地址和对等本地地址的 IP 可访问性。当地址无法访问时 — 对等 IPv6 目标或本地地址的路由表中不存在活动路由 — BGP 将使对等方的会话停止。此命令的 no 版本将禁用回滚。 |
| 示例     | <pre>OS10(conf-router-neighbor)# fall-over</pre>                                                                                                                     |
| 支持的版本  | 10.3.0E or later                                                                                                                                                     |

## fast-external-fallover

当指向直接连接的外部对等的链路失败时，立即重置 BGP 会话。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | fast-external-fallover                                                                                                                                                                                                                                                                                                                                                                                               |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 命令模式   | ROUTER-BGP                                                                                                                                                                                                                                                                                                                                                                                                           |
| 使用情况信息 | 快速外部衰减在检测到 IP 不可转或链路故障后立即终止 EBGP 会话。这仅在您手动重置所有现有 BGP 会话后才适用。要使配置生效，请使用 <code>clear ip bgp</code> 命令。此命令的 no 版本将禁用快速外部故障切换。<br><div> <i>i</i> <b>注:</b> 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式： <ol style="list-style-type: none"> <li>1. 使用 <code>router bgp as-number</code> 命令进入 ROUTER BGP 模式。</li> <li>2. 在 ROUTER BGP 模式下，使用 <code>vrf vrf-name</code> 命令进入 ROUTER BGP VRF 模式。</li> </ol> </div> |
| 示例     | <pre>OS10(conf-router-bgp-10)# fast-external-fallover</pre>                                                                                                                                                                                                                                                                                                                                                          |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                                                                                     |

## graceful-restart

启用正常或无命中重启并为重新启动过程配置所需的参数。

|        |                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | graceful-restart role receiver-only                                                                                                                                                                                                                                                                                                                                                     |
| 参数     | <ul style="list-style-type: none"> <li>• role — 设置本地路由器的重新启动角色</li> <li>• receiver-only — 本地路由器仅支持正常重新启动作为接收器</li> </ul>                                                                                                                                                                                                                                                                |
| 默认     | 已禁用                                                                                                                                                                                                                                                                                                                                                                                     |
| 命令模式   | ROUTER BGP                                                                                                                                                                                                                                                                                                                                                                              |
| 使用情况信息 | 在节点上启用正常重启后，其 BGP 邻居将充当帮助器，而不会丢弃会话和维护路由信息，从而使流量不受干扰。此命令的 no 版本将禁用 graceful-restart helper 模式。<br><div> <i>i</i> <b>注:</b> 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式： <ol style="list-style-type: none"> <li>1. 使用 <code>router bgp as-number</code> 命令进入 ROUTER BGP 模式。</li> <li>2. 在 ROUTER BGP 模式下，使用 <code>vrf vrf-name</code> 命令进入 ROUTER BGP VRF 模式。</li> </ol> </div> |
| 示例     | <pre>OS10(conf-router-bgp-10)# graceful-restart role receiver-only</pre>                                                                                                                                                                                                                                                                                                                |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                                                        |

## inherit template

配置邻居用于继承对等组配置的对等组模板名称。

|        |                                                                                                |
|--------|------------------------------------------------------------------------------------------------|
| 语法     | <code>inherit template template-name</code>                                                    |
| 参数     | <ul style="list-style-type: none"><li><code>template-name</code> — 输入模板名称。最多 16 个字符。</li></ul> |
| 默认     | 未配置                                                                                            |
| 命令模式   | ROUTER-NEIGHBOR                                                                                |
| 使用情况信息 | 当网络邻居继承模板时，在模板上启用的所有功能在邻居上也受支持。此命令的 <code>no</code> 版本将禁用对等组模板配置。                              |
| 示例     | <pre>OS10(conf-router-neighbor)# inherit template zanzibar</pre>                               |
| 支持的版本  | 10.2.0E or later                                                                               |

## listen

启用对等侦听并设置动态对等方的前缀范围。

|        |                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>listen ip-address [limit count]</code>                                                                                                                    |
| 参数     | <ul style="list-style-type: none"><li><code>ip-address</code> — 输入 BGP 邻居 IP 地址。</li><li><code>limit count</code> — (可选) 输入最大动态对等计数，从 1 到 4294967295。</li></ul> |
| 默认     | 未配置                                                                                                                                                             |
| 命令模式   | ROUTER-TEMPLATE                                                                                                                                                 |
| 使用情况信息 | 启用用于侦听的被动对等会话。此命令的 <code>no</code> 版本将禁用被动对等会话。                                                                                                                 |
| 示例     | <pre>OS10(conf-router-template)# listen 1.1.0.0/16 limit 4</pre>                                                                                                |
| 支持的版本  | 10.2.0E or later                                                                                                                                                |

## local-as

为对等体配置本地 AS 编号。

|        |                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>local-as as-number [no-prepend]</code>                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"><li><code>as-number</code> — 输入本地 AS 编号，从 1 到 4294967295。</li><li><code>no-prepend</code> — (可选) 输入此值，以便本地 AS 值不会附加到 <code>AS_PATH</code> 属性。</li></ul> |
| 默认     | 已禁用                                                                                                                                                                                       |
| 命令模式   | ROUTER-NEIGHBOR 或 ROUTER-TEMPLATE                                                                                                                                                         |
| 使用情况信息 | 方便了 BGP 网络迁移操作，并允许您维持现有的 AS 数字。此命令的 <code>no</code> 版本会将该值重置为默认值。<br><code>no local-as</code> 命令将删除 <code>local-as</code> 配置。                                                             |

**示例（邻居）**

```
OS10(conf-router-bgp-10)# neighbor lunar
OS10(conf-router-neighbor)# local-as 20
```

**示例（模板）**

```
OS10(conf-router-bgp-10)# template solar
OS10(conf-router-template)# local-as 20
```

**示例（替换 AS）**

```
OS10(conf-router-bgp-10)# neighbor SJC
OS10(conf-router-template)# local-as 20 no-prepend replace-as
```

支持的版本 10.3.0E or later

log-neighbor-changes

为邻居状态中的更改启用日志记录。

|        |                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | log-neighbor-changes                                                                                                                                                                                                                                                                                                                                                                                        |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                                                                           |
| 默认     | 已启用                                                                                                                                                                                                                                                                                                                                                                                                         |
| 命令模式   | ROUTER-BGP                                                                                                                                                                                                                                                                                                                                                                                                  |
| 使用情况信息 | <div>OS10 可保存日志，包括邻居运行状态和重置原因。要查看日志，请使用 <code>show bgp config</code> 命令。此命令的 <code>no</code> 版本将禁用此功能。</div> <div><div>i</div><div>注: 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式:</div><div><div>1.</div><div>使用 <code>router bgp as-number</code> 命令进入 ROUTER BGP 模式。</div></div><div><div>2.</div><div>在 ROUTER BGP 模式下，使用 <code>vrf vrf-name</code> 命令进入 ROUTER BGP VRF 模式。</div></div></div> |

示例

OS10 (conf-router-bgp-10) # log-neighbor-changes

支持的版本 10.3.0E or later

maximum-paths

配置负载共享的最大等成本路径数。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | maximum-paths [ebgp number   ibgp number] maxpaths                                                                                                                                                                                                                                                                                                                                                                      |
| 参数     | <ul style="list-style-type: none"><li>ebgp — 为外部 BGP 路由启用多路径支持。</li><li>ibgp — 为内部 BGP 路由启用多路径支持。</li><li>number— 输入并行路径的数量，从 1 到 64。</li></ul>                                                                                                                                                                                                                                                                         |
| 默认     | 64 个路径                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 命令模式   | ROUTER-BGP                                                                                                                                                                                                                                                                                                                                                                                                              |
| 使用情况信息 | <div>Dell EMC 建议不要在路由反射器中同时使用多路径和添加路径。要重新计算最佳路径，请使用 <code>clear ip bgp *</code> 命令。此命令的 <code>no</code> 版本将值重置为默认值</div> <div><div>i</div><div>注: 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式:</div><div><div>1.</div><div>使用 <code>router bgp as-number</code> 命令进入 ROUTER BGP 模式。</div></div><div><div>2.</div><div>在 ROUTER BGP 模式下，使用 <code>vrf vrf-name</code> 命令进入 ROUTER BGP VRF 模式。</div></div></div> |

示例 (EBGP)

OS10 (conf-router-bgp-2) # maximum-paths ebgp 2 maxpaths

示例 (IBGP)

OS10 (conf-router-bgp-2) # maximum-paths ibgp 4 maxpaths

支持的版本 10.3.0E or later

maximum-prefix

配置对等节点允许的最大前缀数。

|    |                                                                                    |
|----|------------------------------------------------------------------------------------|
| 语法 | maximum-prefix {number [threshold] [warning]}                                      |
| 参数 | <ul style="list-style-type: none"><li>number— 输入最大前缀编号，从 1 到 4294967295。</li></ul> |

- *threshold*—（可选）输入阈值百分比，范围从 1 到 100。
- *warning-only* —（可选）在超过最大限制时，输入设置路由器发送警告日志消息。如果未设置此参数，则当最大前缀数限制超过上限时，路由器将停止对等节点。

**默认** 75% 阈值

**命令模式** ROUTER-BGP-NEIGHBOR-AF

**使用情况信息** 如果配置此命令且邻居收到的前缀超出了配置允许的数量，则邻居会停止。要查看前缀信息，请使用 `show ip bgp summary` 命令。在将 `clear ip bgp` 命令用于邻居或邻居所属的对等组之前，相邻节点保持关闭状态。此命令的 `no` 版本会将该值重置为默认值。

**示例**

```
OS10(conf-router-bgp-neighbor-af)# maximum-prefix 20 100 warning-only
```

**支持的版本** 10.3.0E or later

## neighbor

创建远程 IP 对等节点并进入邻居配置模式。

**语法** `neighbor ip-address`

- 参数**
- *ip-address* — 输入邻居的 IPv4 或 IPv6 地址。
  - *interface interface-type* — 输入连接到未编号的邻居的接口。

**默认** 未配置

**命令模式** CONFIG-ROUTER-BGP

**使用情况信息** 使用 BGP 邻居创建远程对等。请始终使用此命令输入 BGP 对等节点的 IP 地址。如果配置的对等节点地址是本地 IP 地址，则命令将不会验证。

 **注:** 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式：

1. 使用 `router bgp as-number` 命令进入 ROUTER BGP 模式。
2. 在 ROUTER BGP 模式下，使用 `vrf vrf-name` 命令进入 ROUTER BGP VRF 模式。

此命令的 `no` 版本将禁用 BGP 邻居配置。

**示例**

```
OS10(conf-router-bgp-2)# neighbor 32.1.0.0
OS10(conf-router-neighbor)#
```

**支持的版本** 10.3.0E or later

## next-hop-self

禁用邻居的下一跳计算。

**语法** `next-hop-self`

**参数** 无

**默认** 已启用

**命令模式** ROUTER-NEIGHBOR-AF

**使用情况信息** 影响 EBGp 路由到 IBGP 对等方的下一跳处理。此命令的 `no` 版本将禁用下一跳计算。

**示例**

```
OS10(conf-router-neighbor-af)# next-hop-self
```

**支持的版本** 10.3.0E or later

## non-deterministic-med

按到达的顺序比较路径。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>non-deterministic-med</code>                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 默认     | 已禁用                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 命令模式   | ROUTER-BGP                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 使用情况信息 | <p>路径将按照它们到达的顺序进行比较。OS10 使用此方法从一组路径中选择不同的最佳路径，具体取决于从邻居接收的顺序。MED 能/不能在相邻的路径之间进行比较。当您从确定性更改为不确定性时，现有路径的路径选择将保持确定性，直至您使用 <code>clear ip bgp</code> 命令清除现有路径。此命令的 <code>no</code> 版本将 BGP 最佳路径选择配置为非确定性。</p> <p><b>注：</b> 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式：</p> <ol style="list-style-type: none"><li>1. 使用 <code>router bgp as-number</code> 命令进入 ROUTER BGP 模式。</li><li>2. 在 ROUTER BGP 模式下，使用 <code>vrf vrf-name</code> 命令进入 ROUTER BGP VRF 模式。</li></ol> |
| 示例     | <pre>OS10(conf-router-bgp-10)# non-deterministic-med</pre>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## outbound-optimization

为 IBGP 对等组成员启用出站优化。

|        |                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>outbound-optimization</code>                                                                                                                                                                                                                                                                                                                                                        |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                                                         |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                       |
| 命令模式   | ROUTER-BGP                                                                                                                                                                                                                                                                                                                                                                                |
| 使用情况信息 | <p>动态启用或禁用出站优化，以重置所有邻居会话。启用出站优化时，所有对等节点都会收到相同的更新数据包。选择为邻居的可访问接口地址之一的下一跳地址对于对等也相同。此命令的 <code>no</code> 版本将禁用出站优化。</p> <p><b>注：</b> 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式：</p> <ol style="list-style-type: none"><li>1. 使用 <code>router bgp as-number</code> 命令进入 ROUTER BGP 模式。</li><li>2. 在 ROUTER BGP 模式下，使用 <code>vrf vrf-name</code> 命令进入 ROUTER BGP VRF 模式。</li></ol> |
| 示例     | <pre>OS10(conf-router-bgp-10)# outbound-optimization</pre>                                                                                                                                                                                                                                                                                                                                |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                                                          |

## password

在两个邻近的 TCP 连接上配置消息摘要 5 (MD5) 身份验证的密码。

|      |                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | <code>password {9 encrypted password-string  password-string}</code>                                                                                                        |
| 参数   | <ul style="list-style-type: none"><li>• <code>9 encrypted password-string</code>— 输入 9，然后输入加密的密码。</li><li>• <code>password-string</code>— 输入用于身份验证的密码。最多 128 个字符。</li></ul> |
| 默认   | 已禁用                                                                                                                                                                         |
| 命令模式 | ROUTER-NEIGHBOR                                                                                                                                                             |

## ROUTER-TEMPLATE

### 使用情况信息

您可以输入纯文本格式的密码。在 ROUTER-NEIGHBOR 模式下提供的密码优先于在 ROUTER-TEMPLATE 模式下的密码。此命令的 `no` 版本将禁用身份验证。

### 示例

```
OS10(conf-router-neighbor)# password abcdell
```

```
OS10(conf-router-neighbor)# password 9
f785498c228f365898c0efdc2f476b4b27c47d972c3cd8cd9b91f518c14ee42d
```

### 支持的版本

10.3.0E or later

## redistribute

在 BGP 中重新分配已连接、静态和 OSPF 路由。

### 语法

```
redistribute {connected [route-map map name] | ospf process-id | static
[route-map map name]}
```

### 参数

- `connected` — 输入以从物理连接的接口重新分发路由。
- `route-map map name` — (可选) 输入已配置的路由映射的名称。
- `ospf process-id` — 输入 OSPF 进程的编号 (1 到 65535) 。
- `static` — 输入以重新分发手动配置的路由。

### 默认

已禁用

### 命令模式

ROUTER-BGPv4-AF 或 ROUTER-BGPv6-AF

### 使用情况信息

静态路由被视为不完整的路由。当您使用 `redistribute ospf process-id` 命令而不使用其他参数时，系统会重新分发所有 OSPF 的内部路由、外部类型 1 路由和外部类型 2 路由。此命令的 `no` 版本会将该值重置为默认值。

### 示例 (已连接)

```
OS10(conf-router-bgp-102)# address-family ipv4 unicast
OS10(conf-router-bgpv4-af)# redistribute connected route-map mapbgp1
```

### 示例 (静态 — IPv4)

```
OS10(conf-router-bgp-102)# address-family ipv4 unicast
OS10(conf-router-bgpv4-af)# redistribute static route-map mapbgp2
```

### 示例 (静态 — IPv6)

```
OS10(conf-router-bgp-102)# address-family ipv6 unicast
OS10(conf-router-bgpv6-af)# redistribute static
```

### 示例 (OSPF — IPv4)

```
OS10(conf-router-bgp-102)# address-family ipv4 unicast
OS10(conf-router-bgpv4-af)# redistribute ospf 1
```

### 示例 (OSPF — IPv6)

```
OS10(conf-router-bgp-102)# address-family ipv6 unicast
OS10(conf-router-bgpv6-af)# redistribute ospf 1
```

### 支持的版本

10.2.0E or later

## remote-as

向指定的 BGP 邻居或对等组添加远程。

### 语法

```
remote-as as-number
```

### 参数

`as-number` — 指定 AS 编号，范围从 1 到 65535 适用于 2 字节，或从 1 到 4294967295 适用于 4 字节。

### 默认

无

|        |                                                  |
|--------|--------------------------------------------------|
| 命令模式   | CONFIG-ROUTER-NEIGHBOR<br>CONFIG-ROUTER-TEMPLATE |
| 使用情况信息 | 此命令的 <code>no</code> 版本将删除远程 AS。                 |

#### 示例

```
OS10(config)# router bgp 300
OS10(config-router-bgp-300)# template ebgppg
OS10(config-router-template)# remote-as 100
```

|       |                   |
|-------|-------------------|
| 支持的版本 | 10.4.1.0 or later |
|-------|-------------------|

## remove-private-as

从接收传出更新移除私有 AS 编号。

|      |                                                  |
|------|--------------------------------------------------|
| 语法   | <code>remove-private-as</code>                   |
| 参数   | 无                                                |
| 默认   | 已禁用                                              |
| 命令模式 | CONFIG-ROUTER-NEIGHBOR<br>CONFIG-ROUTER-TEMPLATE |

|        |   |
|--------|---|
| 使用情况信息 | 无 |
|--------|---|

#### 示例

```
OS10(config)# router bgp 300
OS10(config-router-bgp-300)# template ebgppg
OS10(config-router-template)# remove-private-as
```

|       |                   |
|-------|-------------------|
| 支持的版本 | 10.4.1.0 or later |
|-------|-------------------|

## route-map

将已建立的路由映射应用到 BGP 邻居或对等组的传入或出站路由。

|    |                                                                                                                                                                                   |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>route-map route-map-name {in   out}</code>                                                                                                                                  |
| 参数 | <ul style="list-style-type: none"> <li><code>route-map-name</code> — 输入已配置的路由映射的名称。</li> <li><code>in</code> — 将路由映射作为入站策略连接</li> <li><code>out</code> — 将路由映射作为出站策略连接</li> </ul> |

|    |   |
|----|---|
| 默认 | 无 |
|----|---|

|      |                        |
|------|------------------------|
| 命令模式 | ROUTER-BGP-TEMPLATE-AF |
|------|------------------------|

|        |                                                     |
|--------|-----------------------------------------------------|
| 使用情况信息 | 此命令的 <code>no</code> 版本将删除 <code>route-map</code> 。 |
|--------|-----------------------------------------------------|

#### 示例

```
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# route-map bgproutemap in
```

```
OS10(conf-router-template)# address-family ipv4 unicast
OS10(conf-router-bgp-template-af)# route-map bgproutemap in
```

|       |                   |
|-------|-------------------|
| 支持的版本 | 10.4.1.0 or later |
|-------|-------------------|



## route-reflector-client

将邻居配置为路由反射器群集的成员。

|        |                                                                                             |
|--------|---------------------------------------------------------------------------------------------|
| 语法     | <code>route-reflector-client</code>                                                         |
| 参数     | 无                                                                                           |
| 默认     | 未配置                                                                                         |
| 命令模式   | ROUTER-TEMPLATE                                                                             |
| 使用情况信息 | 该设备配置为路由反射器，并且 BGP 邻居配置为路由反射器群集中的客户端。此命令的 <code>no</code> 版本将删除路由反射器的所有客户端 — 该路由器不再用作路由反射器。 |
| 示例     | <pre>OS10(conf-router-template)# route-reflector-client</pre>                               |
| 支持的版本  | 10.3.0E or later                                                                            |

## router bgp

启用 BGP 并将 AS 编号分配给本地 BGP 扬声器。

|        |                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>router bgp as-number</code>                                                                                                         |
| 参数     | <code>as-number</code> — 输入 AS 编号范围。 <ul style="list-style-type: none"><li>1 到 65535，以 2 字节为单位</li><li>1 到 4294967295，以 4 字节为单位</li></ul> |
| 默认     | 无                                                                                                                                         |
| 命令模式   | CONFIGURATION                                                                                                                             |
| 使用情况信息 | AS 编号可以是 16 位整数。此命令的 <code>no</code> 版本会将该值重置为默认值。                                                                                        |
| 示例     | <pre>OS10(config)# router bgp 3 OS10(conf-router-bgp-3)#</pre>                                                                            |
| 支持的版本  | 10.3.0E or later                                                                                                                          |

## router-id

将用户指定的 ID 分配给 BGP 路由器。

|        |                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>router-id ip-address</code>                                                                                                                                                                                                                                                                                                                                                                           |
| 参数     | <code>ip-address</code> — 以点分隔的十进制格式输入 IP 地址。                                                                                                                                                                                                                                                                                                                                                               |
| 默认     | 第一个配置的 IP 地址或随机数                                                                                                                                                                                                                                                                                                                                                                                            |
| 命令模式   | ROUTER-BGP                                                                                                                                                                                                                                                                                                                                                                                                  |
| 使用情况信息 | 更改 BGP 路由器的路由器 ID 以重置对等会话。此命令的 <code>no</code> 版本会将该值重置为默认值。<br> <b>注:</b> 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式： <ol style="list-style-type: none"><li>使用 <code>router bgp as-number</code> 命令进入 ROUTER BGP 模式。</li><li>在 ROUTER BGP 模式下，使用 <code>vrf vrf-name</code> 命令进入 ROUTER BGP VRF 模式。</li></ol> |
| 示例     | <pre>OS10(conf-router-bgp-10)# router-id 10.10.10.40</pre>                                                                                                                                                                                                                                                                                                                                                  |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                                                                            |

## send-community

向 BGP 邻居或对等组发送社区属性。

|        |                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>send-community {extended   standard}</code>                                                                             |
| 参数     | <ul style="list-style-type: none"><li><code>extended</code> — 输入扩展社区属性。</li><li><code>standard</code> — 输入已启动的社区属性。</li></ul> |
| 默认     | 未配置                                                                                                                           |
| 命令模式   | ROUTER-NEIGHBOR                                                                                                               |
| 使用情况信息 | 社区属性指示具有相同属性的所有路由属于同一社区分组。属于该模板的所有邻居将继承为模板配置的功能。此命令的 <code>no</code> 版本将禁止向 BGP 邻居或对等组发送社区属性。                                 |
| 示例     | <pre>OS10(conf-router-neighbor)# send-community extended</pre>                                                                |
| 支持的版本  | 10.3.0E or later                                                                                                              |

## sender-side-loop-detection

为 BGP 邻居启用发送方回路检测过程。

|           |                                                                                                                                                                               |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法        | <code>sender-side-loop-detection</code>                                                                                                                                       |
| 参数        | 无                                                                                                                                                                             |
| 默认        | 已启用                                                                                                                                                                           |
| 命令模式      | ROUTER-BGP-NEIGHBOR-AF                                                                                                                                                        |
| 使用情况信息    | 在开始通告路由之前，此命令可帮助根据 AS 路径检测路由环路。要将邻居配置为接受路由，请使用 <code>neighbor allowas-in</code> 命令。此命令的 <code>no</code> 版本将禁用该邻居的发件方回路检测。                                                     |
| 示例 (IPv4) | <pre>OS10(conf-router-bgp-102)# neighbor 3.3.3.1 OS10(conf-router-neighbor)# address-family ipv4 unicast OS10(conf-router-bgp-neighbor-af)# sender-side-loop-detection</pre>  |
| 示例 (IPv6) | <pre>OS10(conf-router-bgp-102)# neighbor 32::1 OS10(conf-router-neighbor)# address-family ipv6 unicast OS10(conf-router-bgp-neighbor-af)# no sender-side-loop-detection</pre> |
| 支持的版本     | 10.3.0E or later                                                                                                                                                              |

## show ip bgp

显示 BGP 邻居交换的信息。

|        |                                                                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show ip bgp [vrf vrf-name] ip-address/mask</code>                                                                                                                                |
| 参数     | <ul style="list-style-type: none"><li><code>vrf vrf-name</code> — (可选) 输入 vrf 和 VRF 的名称，以查看与该 VRF 对应的路由信息。</li><li><code>ip-address/mask</code> — 以 A.B.C.D/x 格式输入 IP 地址和掩码。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                    |
| 命令模式   | EXEC                                                                                                                                                                                   |
| 使用情况信息 | 无                                                                                                                                                                                      |
| 示例     | <pre>OS10# show ip bgp 1.1.1.0/24 BGP routing table entry for 1.1.1.0/24 Paths: (1 available, table Default-IP-Routing-Table.)  Received from :</pre>                                  |

```

3.1.1.1(3.3.3.33) Best

AS_PATH : 100
Next-Hop : 3.1.1.1, Cost : 0

Origin INCOMPLETE, Metric 0, LocalPref 100, Weight 0, confed-external
Route-reflector origin : 0.0.0.0

```

**支持的版本** 10.3.0E or later

## show ip bgp dampened-paths

显示抑制或非活动的 BGP 路由。

**语法** `show ip bgp [vrf vrf-name] dampened-paths`

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息**

- `vrf vrf-name` — (可选) 输入 `vrf` 和 VRF 的名称，以查看与该 VRF 对应的特定社区列表影响的路由。
- `Network` — 显示抑制路由的网络 ID。
- `From` — 显示通告抑制路由的邻居的 IP 地址。
- `Reuse` — 显示 HH:MM:SS，直至抑制路由可用。
- `Path` — 将全部 AS 列为到达目标网络所通过的抑制路由。

**示例**

```

OS10# show ip bgp dampened-paths

BGP local router ID is 80.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, >
best
Origin codes: i - IGP, e - EGP, ? - incomplete

```

|    | Network    | From     | Reuse    | Path      |
|----|------------|----------|----------|-----------|
| d* | 3.1.2.0/24 | 80.1.1.2 | 00:00:12 | 800 9 8 i |
| d* | 3.1.3.0/24 | 80.1.1.2 | 00:00:12 | 800 9 8 i |
| d* | 3.1.4.0/24 | 80.1.1.2 | 00:00:12 | 800 9 8 i |
| d* | 3.1.5.0/24 | 80.1.1.2 | 00:00:12 | 800 9 8 i |
| d* | 3.1.6.0/24 | 80.1.1.2 | 00:00:12 | 800 9 8 i |

```

Total number of prefixes: 5

```

**支持的版本** 10.3.0E or later

## show ip bgp flap-statistics

显示 BGP 路由的 BGP 摆动统计信息。

**语法** `show ip bgp [vrf vrf-name] flap-statistics`

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息**

- `vrf vrf-name` — (可选) 输入 `vrf` 和 VRF 的名称，以查看与该 VRF 对应的 BGP 路由上的摆动统计信息。
- `Network` — 显示摆动路由的网络 ID。
- `From` — 显示通告摆动路由的邻居的 IP 地址。
- `Duration` — 显示路由首次摆动后的 HH:MM:SS。
- `Flaps` — 显示路由摆动的次数。
- `Reuse` — 显示 HH:MM:SS 直至摆动路由可用。
- `Path` — 列出摆动路由传递以达到目标网络的所有 AS。

示例

```
OS10# show ip bgp flap-statistics
BGP local router ID is 80.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, >
best
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network From Flaps Duration Reuse Path
*> 3.1.2.0/24 80.1.1.2 1 00:00:11 00:00:00 800 9 8 i
*> 3.1.3.0/24 80.1.1.2 1 00:00:11 00:00:00 800 9 8 i
*> 3.1.4.0/24 80.1.1.2 1 00:00:11 00:00:00 800 9 8 i
*> 3.1.5.0/24 80.1.1.2 1 00:00:11 00:00:00 800 9 8 i
*> 3.1.6.0/24 80.1.1.2 1 00:00:11 00:00:00 800 9 8 i
Total number of prefixes: 5
```

支持的版本 10.3.0E or later

show ip bgp ipv4 unicast

显示 BGP IPv4 路由的路由信息。

语法

show ip bgp [vrf vrf-name] ipv4 unicast [summary | neighbors [ip-address] [advertised-routes | dampened-paths | flap-statistics | denied-routes | routes]]]

参数

- vrf vrf-name — (可选) 输入 vrf VRF 的名称，以查看与该 VRF 对应的 IPv4 单播摘要信息。
- summary — 显示 IPv4 单播摘要信息。
- neighbors — 显示邻居的相关信息。
- ip-address — 显示有关特定邻居的信息。
- advertised-routes — 显示通告给邻居的路由。
- dampened-paths — 显示从邻居接收的抑制路由。
- flap-statistics — 显示从邻居接收的路由的摆动统计信息。
- received-routes — 显示从邻居接收的路由。
- denied-routes — 显示邻居拒绝的路由。
- routes — 显示从邻居中获知的路由。

默认

未配置

命令模式

EXEC

使用情况信息

此命令将显示使用 network 命令配置的本地通告 BGPv4 路由。这些路由将显示用于重新分发/网络的路由的 r。

示例

```
OS10# show ip bgp ipv4 unicast summary
BGP router identifier 80.1.1.1 local AS number 102
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx
80.1.1.2 800 8 4 00:01:10 5
```

支持的版本 10.3.0E or later

show ip bgp ipv6 unicast

显示 BGP IPv6 路由的路由信息。

语法

show ip bgp [vrf vrf-name] ipv6 unicast [summary | neighbors [ip-address] [advertised-routes | dampened-paths | flap-statistics | denied-routes | routes]]]

参数

- vrf vrf-name — (可选) 输入 vrf，然后输入 VRF 的名称，以查看与该 VRF 对应的 IPv6 单播信息。
- neighbors — 显示 IPv6 邻居信息。
- ip-address — 显示有关特定邻居的信息。
- summary — 显示 IPv6 单播摘要信息。
- advertised-routes — 显示通告给邻居的路由。

- dampened-paths — 显示从邻居接收的抑制路由。
- flap-statistics — 显示从邻居接收的路由的摆动统计信息。
- received-routes — 显示从邻居接收的路由。
- denied-routes — 显示邻居拒绝的路由。
- routes — 显示从邻居中获知的路由。

默认  
命令模式  
使用情况信息  
示例

未配置  
EXEC  
无

```
OS10# show ip bgp ipv6 unicast summary
BGP router identifier 80.1.1.1 local AS number 102
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx
80.1.1.2 800 8 4 00:01:10 5

OS10# show ip bgp ipv6 unicast neighbors interface ethernet 1/1/1
advertised-routes
BGP local router ID is 40.1.1.2
Status codes: s suppressed, S stale, d dampened, h history, * valid, >
best
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network Next Hop Metric
LocPrf Weight Path
*> 1000::/64 fe80::3617:ebff:feff:dc5e 0
0 0 10

OS10# show ip bgp ipv6 unicast neighbors interface ethernet 1/1/1 routes
BGP local router ID is 40.1.1.2
Status codes: s suppressed, S stale, d dampened, h history, * valid, >
best
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network Next Hop Metric
LocPrf Weight Path
*> 1000::/64 fe80::3617:ebff:feff:dc5e 0
100 0 10

OS10# show ip bgp ipv6 unicast neighbors interface ethernet 1/1/1
received-routes
BGP local router ID is 40.1.1.2
Status codes: D denied
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network Next Hop Metric
LocPrf Weight Path
*> 1001::/64 fe80::3617:ebff:feff:dc5e 0
0 0 10

OS10# show ip bgp ipv6 unicast neighbors interface ethernet 1/1/1 denied-
routes
BGP local router ID is 40.1.1.2
Status codes: D denied
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network Next Hop Metric
LocPrf Weight Path
D 1002::/64 fe80::3617:ebff:feff:dc5e 0
0 0 10
```

支持的版本 10.3.0E or later

## show ip bgp neighbors

显示 BGP 邻居交换的信息。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show ip bgp [vrf vrf-name] neighbors [ip-address] [advertised-routes   dampened-routes   flap-statistics   denied-routes   routes]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"><li>• <code>vrf vrf-name</code> — 输入 <code>vrf</code> 和 VRF 的名称，以查看与该 VRF 对应的 BGP 邻居之间交换的信息。</li><li>• <code>ip-address</code> — 输入特定邻居的 IPv6 地址/IPv4</li><li>• <code>denied-routes</code> — 显示策略拒绝的路由的列表</li><li>• <code>advertised-routes</code> — 显示通告给邻居的路由</li><li>• <code>dampened-routes</code> — 显示从邻居接收的抑制路由</li><li>• <code>flap-statistics</code> — 显示从邻居接收的路由的摆动统计信息</li><li>• <code>received-routes</code> — 显示从邻居接收的路由。</li><li>• <code>routes</code> — 显示从邻居学习的路由</li></ul>                                                                                                                                                                                                                                                                                                                                                                 |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | <ul style="list-style-type: none"><li>• <code>BGP neighbor</code> — 显示 BGP 邻居地址及其编号。该行中的最后一个短语指示 BGP 路由器及其邻居之间的链路是否为外部或内部。如果它们位于相同 AS 中，则链路为内部；否则，链路为外部。</li><li>• <code>BGP version</code> — 显示 BGP 版本（始终为版本 4）和远程路由器 ID。</li><li>• <code>BGP state</code> — 显示邻居的 BGP 状态和时间量（以小时:分钟:秒为单位）的状态。</li><li>• <code>Last read</code> — 显示上次读取的信息：<ul style="list-style-type: none"><li>◦ 上次读取是指路由器从其邻居中读取消息的时间（以小时:分钟:秒为单位）。</li><li>◦ 暂存时间是指从其邻居中的消息之间配置的秒数。</li><li>◦ 保留间隔是保留消息之间的秒数，以帮助确保 TCP 会话仍处于活动状态。</li></ul></li><li>• <code>Received messages</code> — 显示收到的 BGP 消息数、通知数或错误消息数，以及队列中等待处理的消息数。</li><li>• <code>Sent messages</code> — 显示已发送的 BGP 消息数、通知数或错误消息数，以及队列中等待处理的消息数。</li><li>• <code>Description</code> — 显示为 BGP 邻居配置的描述性名称。只有当配置说明时才会显示此字段。</li><li>• <code>Local host</code> — 显示本地路由器的对等地址和 TCP 的端口号。</li><li>• <code>Foreign host</code> — 显示邻居的对等地址和 TCP 的端口号。</li></ul> |

虽然从 BGP 邻居接收的路由的状态代码可能不会显示在 `show ip bgp neighbors ip-address received-routes` 输出中，但它们会在 `show ip bgp` 输出中正确显示。

### 示例

```
OS10# show ip bgp neighbors
BGP neighbor is 80.1.1.2, remote AS 800, local AS 102 external link

 BGP version 4, remote router ID 12.12.0.2
 BGP state ESTABLISHED, in this state for 00:02:51
 Last read 00:18:23 seconds
 Hold time is 90, keepalive interval is 30 seconds
 Configured hold time is 180, keepalive interval is 60 seconds
 Fall-over disabled

 Received 11 messages
 1 opens, 0 notifications, 3 updates
 7 keepalives, 0 route refresh requests
 Sent 8 messages
 1 opens, 0 notifications, 0 updates
 7 keepalives, 0 route refresh requests
 Minimum time between advertisement runs is 30 seconds
 Description: nl_abcd
 Capabilities received from neighbor for IPv4 Unicast:
MULTIPROTO_EXT(1)MULTIPROTO_EXT(1)MULTIPROTO_EXT(1)ROUTE_REFRESH(2)
 Capabilities advertised to neighbor for IPv4 Unicast:
MULTIPROTO_EXT(1)MULTIPROTO_EXT(1)ROUTE_REFRESH(2)CISCO_ROUTE_REFRESH
(128)4_OCTET_AS(65)
 Prefixes accepted 5, Prefixes advertised 0
 Connections established 1; dropped 1
 Closed by neighbor sent 00:02:51 ago
```

```

For address family: IPv4 Unicast
Next hop set to self
Allow local AS number 0 times in AS-PATH attribute

For address family: IPv6 Unicast
Next hop set to self
Allow local AS number 0 times in AS-PATH attribute

Local host: 80.1.1.1, Local port: 57812
Foreign host: 80.1.1.2, Foreign port: 179

```

## 通告路由示例

```

OS10# show ip bgp ipv6 unicast neighbors 192:168:1::2 advertised-routes
BGP local router ID is 100.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, >
best
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight
Path
*>55::/64 192:168:1::1 0 0 0
100i
*>55:0:0:1::/64 192:168:1::1 0 0 0
100i
*>55:0:0:2::/64 192:168:1::1 0 0 0
100i
*>55:0:0:3::/64 192:168:1::1 0 0 0
100i
*>55:0:0:4::/64 192:168:1::1 0 0 0
100i
*>55:0:0:5::/64 192:168:1::1 0 0 0
100i
*>55:0:0:6::/64 192:168:1::1 0 0 0
100i
*>55:0:0:7::/64 192:168:1::1 0 0 0
100i
*>55:0:0:8::/64 192:168:1::1 0 0 0
100i
*>55:0:0:9::/64 192:168:1::1 0 0 0
100i
*>172:16:1::/64 192:168:1::1 0 0 0
100?
Total number of prefixes: 11
OS10#

```

## 接收路由示例

```

OS10# show ip bgp ipv6 unicast neighbors 172:16:1::2 received-routes
BGP local router ID is 100.1.1.1
Status codes: D denied
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Path
D 55::/64 172:16:1::2 0 0 i
55:0:0:1::/64 172:16:1::2 0 0 i
55:0:0:2::/64 172:16:1::2 0 0 i
D 55:0:0:3::/64 172:16:1::2 0 0 i
D 55:0:0:4::/64 172:16:1::2 0 0 i
D 55:0:0:5::/64 172:16:1::2 0 0 i
D 55:0:0:6::/64 172:16:1::2 0 0 i
55:0:0:7::/64 172:16:1::2 0 0 i
D 55:0:0:8::/64 172:16:1::2 0 0 i
D 55:0:0:9::/64 172:16:1::2 0 0 i
Total number of prefixes: 10
OS10#

```

## 被拒路由示例

```

OS10# show ip bgp ipv6 unicast neighbors 172:16:1::2 denied-routes
BGP local router ID is 100.1.1.1
Status codes: D denied
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Path
D 55::/64 172:16:1::2 0 0 100 200 300 400i
D 55:0:0:1::/64 172:16:1::2 0 0 100 200 300 400i

```

```
D 55:0:0:2::/64 172:16:1::2 0 0 100 200 300 400i
Total number of prefixes: 3
OS10#
```

路由示例

```
OS10# show ip bgp ipv6 unicast neighbors 172:16:1::2 routes
BGP local router ID is 100.1.1.1
Status codes: s suppressed, S stale, d dampened, h history, * valid, >
best
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*>55::/64 172:16:1::2 44 55 0 i
*>55:0:0:1::/64 172:16:1::2 44 55 0 i
*>55:0:0:2::/64 172:16:1::2 44 55 0 i
*>55:0:0:3::/64 172:16:1::2 44 55 0 i
*>55:0:0:4::/64 172:16:1::2 44 55 0 i
*>55:0:0:5::/64 172:16:1::2 44 55 0 i
*>55:0:0:6::/64 172:16:1::2 44 55 0 i
*>55:0:0:7::/64 172:16:1::2 44 55 0 i
*>55:0:0:8::/64 172:16:1::2 44 55 0 i
*>55:0:0:9::/64 172:16:1::2 44 55 0 i
Total number of prefixes: 10
OS10#
```

支持的版本 10.3.0E or later

show ip bgp peer-group

显示有关对等组中的 BGP 对等节点的信息。

- 语法

show ip bgp [vrf vrf-name] peer-group peer-group-name
- 参数
  - vrf vrf-name — (可选) 输入 vrf 以查看与该 VRF 对应的对等组中的 BGP 对等节点的相关信息。
  - peer-group-name — (可选) 输入对等组名称，以仅查看有关对等组的信息。
- 默认

未配置
- 命令模式

EXEC
- 使用情况信息
  - Peer-group — 显示对等组名称。最短时间显示 BGP 通告之间的时间间隔。
  - Administratively shut — 如果不启用对等组，将显示对等组的状态。如果启用对等组，则不会显示此行。
  - BGP version — 显示支持的 BGP 版本。
  - Description — 显示为 BGP 对等模板配置的描述性名称。只有当配置说明时才会显示此字段。
  - For address family — 将 IPv4 单播显示为地址系列。
  - BGP neighbor — 显示 BGP 邻居的名称。
  - 对等节点数 — 显示为此对等组配置的对等节点的数量。
  - Peer-group members — 列出对等组中的对等节点的 IP 地址。如果地址为出站优化，则 IP 地址旁边会显示一个 \*。

示例

```
OS10# show ip bgp peer-group bgppg
Peer-group bgppg, remote AS 103
 BGP version 4
 Minimum time between advertisement runs is 30 seconds
 Description: peer_template_1_abcd
 For address family: Unicast
 BGP neighbor is bgppg, peer-group external
 Update packing has 4_OCTET_AS support enabled
```

示例（摘要）

```
OS10# show ip bgp peer-group ebgp summary
BGP router identifier 32.1.1.1 local AS number 6
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx
17.1.1.2 7 7 6 00:01:54 5
```



支持的版本 10.2.0E or later

show ip bgp summary

显示所有 BGP 连接的状态。

- 语法
- show ip bgp [vrf vrf-name] summary
- 参数
- vrf vrf-name — (可选) 输入 vrf VRF 的名称, 以查看与该 VRF 对应的所有 BGP 连接的状态。
- 默认
- 未配置
- 命令模式
- EXEC
- 使用情况信息
- Neighbor — 显示 BGP 邻居地址。
  - AS — 显示邻居的 AS 编号
  - MsgRcvd — 显示邻居接收的 BGP 消息的数量。
  - MsgSent — 显示邻居发送的 BGP 消息的数量。
  - Up/Down — 显示邻居在 Established 阶段中的时间量。如果邻居从未移入 Established 阶段, 则不会显示该词。输出格式为:

1 day = 00:12:23 (hours:minutes:seconds), 1 week = 1d21h (DaysHours),  
1 week + 11w2d (WeeksDays)

- State/Pfxrxd — 如果邻居处于 Established 阶段, 这是收到的网络前缀的编号。如果您使用 neighbor maximum-prefix 命令配置了最大限制, 则会在此列中显示 prfxd。如果邻居未处于 Established 阶段, 则显示当前阶段 - Idle、Connect、Active、OpenSent、OpenConfirm。当对等节点在状态之间转换并清除收到的路由时, 此列中可能会显示密码 Purging。如果邻居处于禁用状态, 则会在此列中显示密码 Admin shut。

聚合路由的抑制状态可能不会显示在命令输出中。

示例

```
OS10# show ip bgp summary
BGP router identifier 80.1.1.1 local AS number 102
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx
80.1.1.2 800 24 23 00:09:15 5
```

未计数对等节点的示例:

支持的版本 10.2.0E or later

show ip route

显示有关 IPv4 BGP 路由表条目的信息。

- 语法
- show ip route [vrf vrf-name] bgp
- 参数
- vrf vrf-name — 输入 vrf 和 VRF 的名称, 以查看与该 VRF 对应的 BGP 邻居之间交换的信息。
- 默认
- 未配置
- 命令模式
- EXEC
- 使用情况信息
- 此命令将显示有关 IPv4 BGP 路由表条目的信息。

示例

```
OS10# show ip route
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, * - candidate default,
 + - summary route, > - non-active route
Gateway of last resort is not set
 Destination Gateway Dist/Metric Last Change

```

|   |                 |              |                |       |          |
|---|-----------------|--------------|----------------|-------|----------|
| C | 10.1.1.0/24     | via 10.1.1.1 | ethernet1/1/17 | 0/0   | 01:18:34 |
| B | IN 100.1.1.0/24 | via 10.1.1.2 |                | 200/0 | 00:03:46 |
| B | IN 101.1.1.0/24 | via 10.1.1.2 |                | 200/0 | 00:03:46 |
| B | IN 102.1.1.0/24 | via 10.1.1.2 |                | 200/0 | 00:03:46 |
| B | IN 103.1.1.0/24 | via 10.1.1.2 |                | 200/0 | 00:03:46 |
| B | IN 104.1.1.0/24 | via 10.1.1.2 |                | 200/0 | 00:03:46 |

```
OS10# show ip route bgp
Codes: C - connected
S - static
B - BGP, IN - internal BGP, EX - external BGP
O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
E2 - OSPF external type 2, * - candidate default,
+ - summary route, > - non-active route
Gateway of last resort is not set
Destination Gateway Dist/Metric Last Change

B IN 1.1.1.0/24 via 169.254.0.1 vlan100 200/0 00:17:34
```

**支持的版本** 10.4.2.0 或更高版本

## show ipv6 route

显示有关 IPv6 BGP 路由表条目的信息。

|               |                                                                                                                             |
|---------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>show ipv6 route [vrf vrf-name] bgp</code>                                                                             |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>vrf vrf-name</code> — 输入 vrf 和 VRF 的名称，以查看与该 VRF 对应的 BGP 邻居之间交换的信息。</li> </ul> |
| <b>默认</b>     | 未配置                                                                                                                         |
| <b>命令模式</b>   | EXEC                                                                                                                        |
| <b>使用情况信息</b> | 此命令将显示有关 IPv6 BGP 路由表条目的信息。                                                                                                 |
| <b>示例</b>     | <pre>OS10# show ipv6 route</pre>                                                                                            |

**支持的版本** 10.4.2.0 或更高版本

## 软重新配置入站

为邻居启用软重新配置。

|               |                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>soft-reconfiguration inbound</code>                                                                                                                       |
| <b>参数</b>     | 无                                                                                                                                                               |
| <b>默认</b>     | 未配置                                                                                                                                                             |
| <b>命令模式</b>   | ROUTER-BGP-NEIGHBOR-AF                                                                                                                                          |
| <b>使用情况信息</b> | 对等组级别不支持此命令。要为对等组中的对等控制器启用软重新配置，必须在每个对等组级别启用此命令。使用软重新配置入站时，从此邻居接收的所有更新都将原样存储，而不考虑入站策略。当稍后执行入站软重新配置时，存储的信息将生成一组新的入站更新。此命令的 <code>no</code> 版本将禁用 BGP 邻居的软重新配置入站。 |

**示例 (IPv4)**

```
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# soft-reconfiguration inbound
```

**示例 (IPv6)**

```
OS10(conf-router-neighbor)# address-family ipv6 unicast
OS10(conf-router-bgp-neighbor-af)# soft-reconfiguration inbound
```

**支持的版本** 10.3.0E or later

## template

创建对等组模板，以将其分配给 BGP 邻居。

|        |                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>template template-name</code>                                                                                                                                                                                                                                                                                      |
| 参数     | <code>template-name</code> — 输入对等组模板名称。最多 16 个字符。                                                                                                                                                                                                                                                                        |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                      |
| 命令模式   | CONFIG-ROUTER-BGP                                                                                                                                                                                                                                                                                                        |
| 使用情况信息 | 对等组模板的成员会继承模板的配置属性并共享相同的更新策略。此命令的 <code>no</code> 版本将删除对等模板配置。<br><div><div><i>i</i></div><div><b>注:</b> 要为非默认 VRF 实例配置这些设置，您必须先使用以下命令进入 ROUTER-CONFIG-VRF 子模式：<br/>1. 使用 <code>router bgp as-number</code> 命令进入 ROUTER BGP 模式。<br/>2. 在 ROUTER BGP 模式下，使用 <code>vrf vrf-name</code> 命令进入 ROUTER BGP VRF 模式。</div></div> |
| 示例     | <pre>OS10(conf-router-bgp-10)# template solar OS10(conf-router-bgp-template)#</pre>                                                                                                                                                                                                                                      |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                         |

## timers

调整 BGP 存活和存留计时器。

|        |                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>timers keepalive holdtime</code>                                                                                                                                                        |
| 参数     | <ul style="list-style-type: none"><li><code>keepalive</code>— 输入发送至邻居路由器的存活消息之间的时间间隔（以秒为单位），从 1 到 65535。</li><li><code>holdtime</code>— 输入上次存活消息与声明路由器失效之间的时间间隔（以秒为单位），从 3 到 65535。</li></ul> |
| 默认     | keepalive 60 秒; holdtime 180 秒                                                                                                                                                                |
| 命令模式   | ROUTER-BGP                                                                                                                                                                                    |
| 使用情况信息 | 已配置的计时器值将在 BGP 硬重置后生效。计时器值将对等节点进行协商。此命令的 <code>no</code> 版本会将该值重置为默认值。                                                                                                                        |
| 示例     | <pre>OS10(conf-router-bgp)# timers 30 90</pre>                                                                                                                                                |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                              |

## vrf

进入 CONFIG-ROUTER-VRF 命令模式。

|        |                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>vrf vrf-name</code>                                                                                                                       |
| 参数     | 无                                                                                                                                               |
| 默认     | 无                                                                                                                                               |
| 命令模式   | ROUTER-BGP                                                                                                                                      |
| 使用情况信息 | 此模式允许您将 BGP 配置应用于非默认 VRF。                                                                                                                       |
| 示例     | <pre>OS10(config)#router bgp 100 OS10(config-router-bgp-100)# OS10(config-router-bgp-100)#vrf vrf_test1  OS10(config-router-bgp-100-vrf)#</pre> |

支持的版本 10.3.0E or later

weight

为来自邻居接口的路由分配默认权重。

|        |                                                           |
|--------|-----------------------------------------------------------|
| 语法     | <code>weight number</code>                                |
| 参数     | <code>number</code> — 输入数字作为路由的权重，从 1 到 4294967295。       |
| 默认     | 0                                                         |
| 命令模式   | ROUTER-BGP-NEIGHBOR                                       |
| 使用情况信息 | 在最佳路径选择过程中首选具有最高权重值的路径。此命令的 <code>no</code> 版本会将该值重置为默认值。 |
| 示例     | <pre>OS10(config-router-bgp-neighbor)# weight 4096</pre>  |

支持的版本 10.3.0E or later

同等成本多路径

ECMP 是一种路由技术，在这种情况下，通过多个最佳路径转发到单个目标。启用 ECMP 时，OS10 使用哈希算法确定下一跳。哈希算法基于各种数据包字段和内部值中的值进行哈希决策。

在 CONFIGURATION 模式下配置哈希算法。

```
hash-algorithm ecmp {crc | crc16cc | crc32LSB | crc32MSB | xor | xor1 | xor2 | xor4 | xor8 | random}
```

更改哈希算法

```
OS10(config)# hash-algorithm ecmp crc
```

负载均衡

为了提高带宽，需要跨成员链路平衡流量。RTAG7 是一种哈希算法，可以在采用受控模式在中继组中平衡流量负载。RTAG7 可以平衡流量，以便在流量变得更多样时更有效地将成员链路用作流量。

RTAG7 将生成包含以下两个部分的哈希：

- 第一个部分将从数据包标头生成以识别流量中的微流。默认情况下，列出的所有参数已针对负载均衡启用，入口端口除外。

```
OS10# show load-balance

Load-Balancing Configuration For LAG and ECMP:

IPV4 Load Balancing : Enabled
IPV6 Load Balancing : Enabled
MAC Load Balancing : Enabled
TCP-UDP Load Balancing : Enabled
Ingress Port Load Balancing : Disabled
IPV4 FIELDS : source-ip destination-ip protocol vlan-id l4-destination-port l4-
source-port
IPV6 FIELDS : source-ip destination-ip protocol vlan-id l4-destination-port l4-
source-port
MAC FIELDS : source-mac destination-mac ethertype vlan-id
TCP-UDP FIELDS: l4-destination-port l4-source-port
```

- 第二个端口将从静态物理配置生成，例如入口和出口端口号。

要根据任何参数生成负载均衡，请使用 `load-balance` 命令更改哈希字段。该示例显示如何启用入口端口以根据入口参数生成负载均衡。

```
OS10(config)# load-balancing ingress-port enable
OS10(config)# do show load-balance
Load-Balancing Configuration For LAG and ECMP:

IPV4 Load Balancing : Enabled
IPV6 Load Balancing : Enabled
MAC Load Balancing : Enabled
TCP-UDP Load Balancing : Enabled
Ingress Port Load Balancing : Enabled
IPV4 FIELDS : source-ip destination-ip protocol vlan-id l4-destination-port l4-source-port
IPV6 FIELDS : source-ip destination-ip protocol vlan-id l4-destination-port l4-source-port
MAC FIELDS : source-mac destination-mac ethertype vlan-id
TCP-UDP FIELDS: l4-destination-port l4-source-port
```

## 弹性哈希

要增加带宽和实现负载均衡，流量会在 ECMP 组的下一跳或端口通道的成员端口之间分布。OS10 使用哈希算法来确定哈希密钥。端口通道中的出口端口或 ECMP 组中的下一跳将根据哈希密钥进行选择，具体取决于端口通道中的端口数或 ECMP 组中的下一跳。当成员链路停机或添加新成员链路时，流量流将根据新的哈希结果进行映射。

在此部分中，“成员链路”一词是指成员物理端口（使用端口通道）或下一跳（使用 ECMP 组）。

通过弹性哈希，当成员链路停机时，现有的流不会受到影响；它们不会重新映射。弹性哈希会将流量从故障链路重新分配到另一个成员链路，而不重新映射其他现有流。但是，在添加新成员链路时，会进行最低重新映射。

端口通道和同等成本多路径组 (ECMP) 均支持弹性哈希。弹性哈希是一种全局配置。您可以为端口通道和单独的 ECMP 配置弹性哈希。

- i

注:
- S4200-ON 和 Z9332F-ON 平台上不支持弹性哈希。
  - 流映射表中的条目数始终为偶数。

要为端口通道或 ECMP 组启用弹性哈希，请在 CONFIGURATION 模式下使用以下命令：

```
OS10(config)# enhanced-hashing resilient-hashing ecmp

OS10(config)# enhanced-hashing resilient-hashing lag
```

## 支持的平台

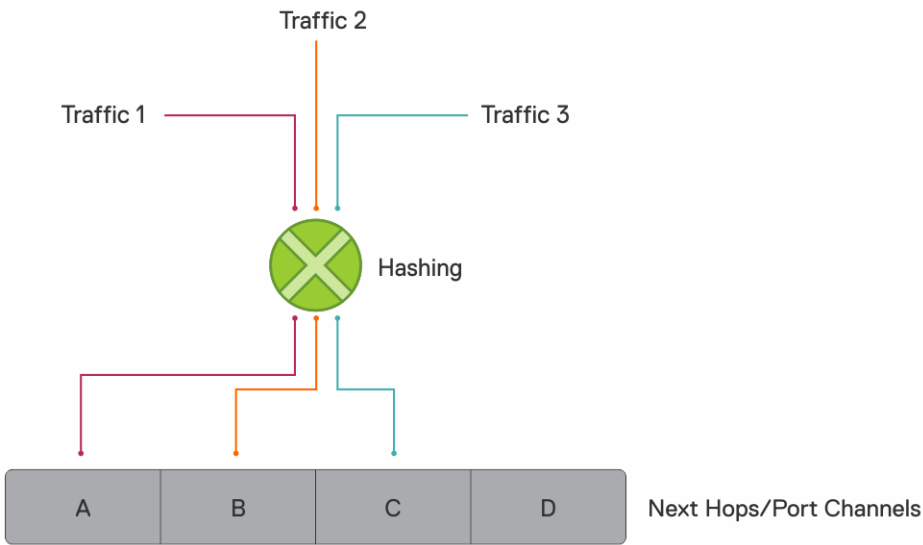
下表列出了支持弹性哈希的平台。

表. 42: 弹性哈希功能支持的平台

| 平台                                                   | ECMP 上的弹性哈希 | 端口通道上的弹性哈希 |
|------------------------------------------------------|-------------|------------|
| S6000-ON、S6010-ON、S4048T-ON、S4100-ON 系列、S5200F-ON 系列 | Y           | Y          |
| Z9100-ON 系列、Z9200-ON 系列                              | Y           | N          |
| MX 系列                                                | Y           | N          |
| S3000-ON、S4200-ON 系列                                 | N           | N          |

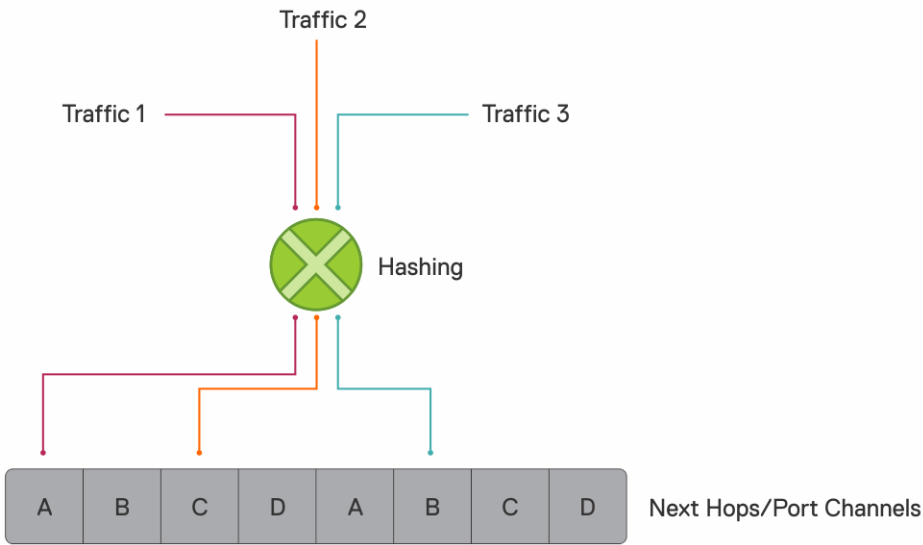
示例

正常流量流，无弹性哈希



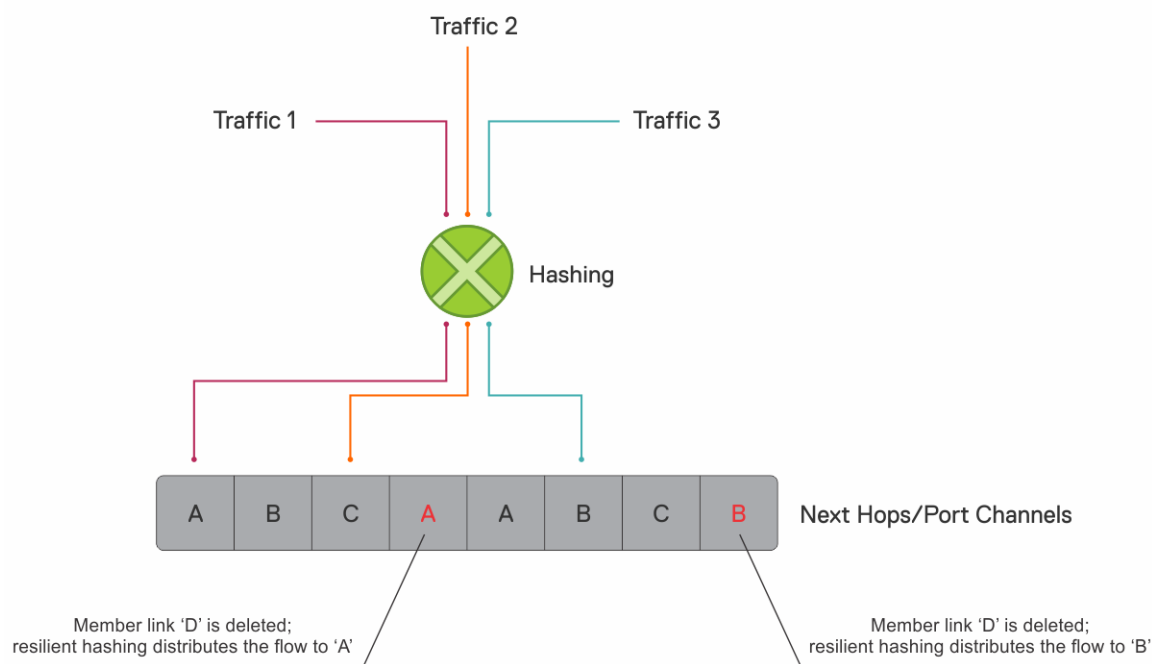
启用弹性哈希功能的流量流

为 ECMP 组启用弹性哈希时，将创建具有 64 条路径的流映射表（OS10 默认的最大 ECMP 路径数），并且流量均匀分布。在下面的示例中，流量 1 映射到下一跳“A”；流量 2 映射到下一跳“C”；流量 3 映射到下一跳“B”。



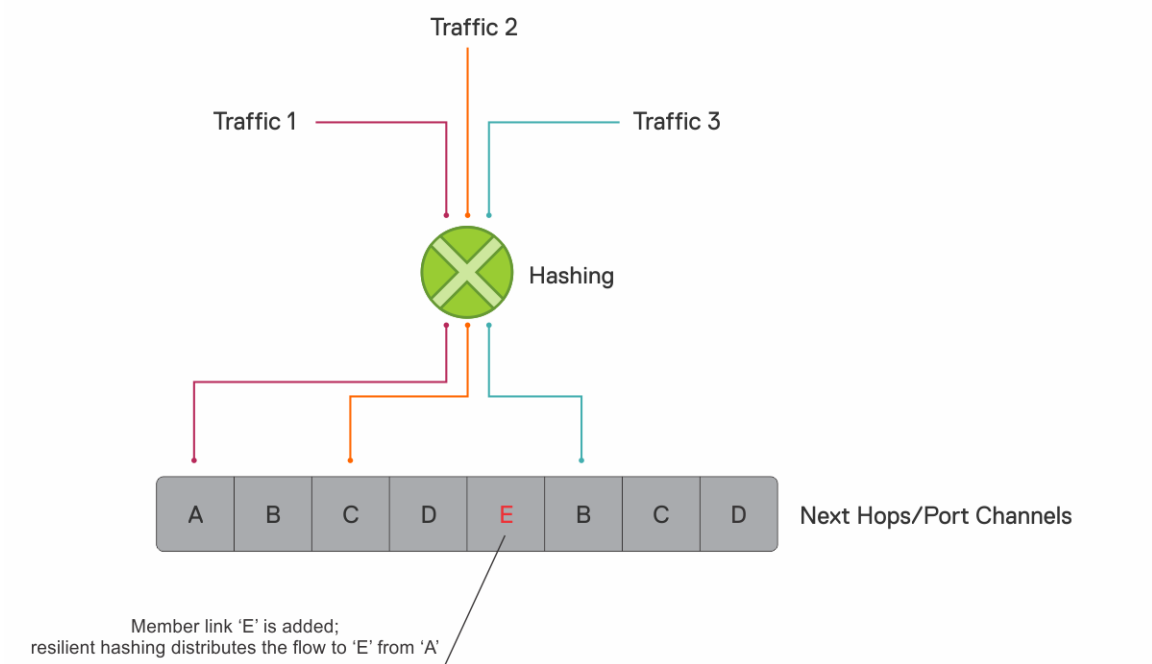
成员链路中断

在下面的示例中，如果成员链路 D 发生故障，则弹性哈希会将用于成员链路 D 的流量分配给 A 和 B。现有的 1、2 和 3 流量不会受到干扰。



### 成员链路已添加

但是，在添加新成员链路时，弹性哈希会完成最小重新映射以实现更好的负载均衡，如下所示：



### 重要事项

- 端口通道上的弹性哈希仅适用于单播流量。
- 对于 ECMP 组上的弹性哈希，ECMP 路径必须为 64 的倍数。在启用弹性哈希之前，请确保将最大 ECMP 路径设置为 64 的倍数。您可以使用 `ip ecmp-group maximum-paths` 命令配置此值。

# 最大 ECMP 组和路径

交换机上支持的 ECMP 组的最大数量取决于交换机上配置的最大 ECMP 路径。要查看 ECMP 组和路径的最大数量，请使用 `show ip ecmp-group details` 命令。

```
OS10# show ip ecmp-group details
Maximum Number of ECMP Groups : 256
Maximum ECMP Path per Group : 64
Next boot configured Maximum ECMP Path per Group : 64
```

每个组的 ECMP 路径的最大数量的默认值为 64。此值可配置，您最多可为每个组配置 128 个 ECMP 路径。

Maximum ECMP Path per Group 是硬件中配置的当前值。Next boot configured Maximum ECMP Path per Group 是配置为最大 ECMP 路径的值，并将在下次重新引导后生效。

您可以使用 `ip ecmp-group maximum-paths number` 命令来增加或减少 ECMP 组的最大数量。ECMP 组的数量与 ECMP 路径数成正比。

要配置每个 ECMP 路由的最大路径：

```
OS10# configure terminal
OS10(config)# ip ecmp-group maximum-paths 10
OS10(config)# exit
OS10# write memory
OS10# reload
```

## ECMP 命令

### enhanced-hashing

确保在成员链路停机时不重新映射现有流量流。

|        |                                                                                                                                     |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | enhanced-hashing resilient-hashing {lag   ecmp}                                                                                     |
| 参数     | <ul style="list-style-type: none"><li>resilient-hashing — 输入关键字以启用增强哈希。</li><li>{ecmp   lag} — 输入关键字以启用端口通道或 ECMP 组的弹性哈希。</li></ul> |
| 默认     | 已禁用                                                                                                                                 |
| 命令模式   | CONFIGURATION                                                                                                                       |
| 使用情况信息 | 此命令的 no 版本将禁用弹性哈希。有关支持的平台，请参阅 <a href="#">支持的平台</a> 。                                                                               |
| 示例     | <pre>OS10(config)# enhanced-hashing resilient-hashing ecmp</pre> <pre>OS10(config)# enhanced-hashing resilient-hashing lag</pre>    |
| 支持的版本  | 10.4.3.0 or later                                                                                                                   |

### hash-algorithm

更改在 ECMP 路径和链路聚合组 (LAG) 间分布流量流的哈希算法。

|    |                                                                                                                                                                                                |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | hash-algorithm {ecmp   lag   seed {seed-value}} {crc   crc16cc   crc32LSB   crc32MSB   xor   xor1   xor2   xor4   xor8   random}                                                               |
| 参数 | <ul style="list-style-type: none"><li>ecmp — 启用 ECMP 哈希配置。</li><li>lag — 仅为第二层 (L2) 启用 LAG 哈希配置。</li><li>seed — 更改哈希算法种子值以获得更好的哈希值。</li><li>seed-value — 输入哈希算法种子值，从 0 到 4294967295。</li></ul> |



- `crc` — 启用循环冗余检查 (CRC) 多项式以进行哈希计算。
- `crc16cc` — 使用 CRC16-CCITT 多项式的 16 位 CRC16
- `crc32LSB` — 计算的 CRC32 的 LSB 16 位 (默认值)
- `crc32MSB` — 计算的 CRC32 的 MSB 16 位
- `xor` — 启用计算的高 8 位 CRC 和低 8 位 XOR 值。
- `xor1` — 启用 CRC16-BISYNC 的高 8 位和低 8 位 xor1
- `xor2` — 启用 CRC16-BISYNC 的高 8 位和低 8 位 xor2
- `xor4` — 启用 CRC16-BISYNC 的高 8 位和低 8 位 xor4
- `xor8` — 启用 CRC16-BISYNC 的高 8 位和低 8 位 xor8
- `random` — 启用 ECMP 或 LAG 哈希计算的哈希算法随机种子值。

**默认** `crc`

**命令模式** CONFIGURATION

**使用情况信息** 使用此命令计算的哈希值对于整个系统是唯一的。不同的哈希算法基于端口通道成员和数据包值的数量。默认哈希算法可在各种测试方案中产生最平衡的结果，但如果默认算法不能提供流量的满意度分布，请使用此命令来指定另一种算法。

当端口通道成员离开或添加到端口通道时，哈希算法将重新计算以平衡各成员之间的流量。此命令的 `no` 版本将值恢复为默认值。

**示例**

```
OS10(config)# hash-algorithm lag crc
```

**支持的版本** 10.3.0E or later

## ip ecmp-group maximum-paths

配置每个路由的 ECMP 路径的最大数量。

**语法** `ip ecmp-group maximum-paths number`

**参数** `number` — 输入 ECMP 路径的最大数量，从 2 到 128。

**默认** 64

**命令模式** CONFIGURATION

**使用情况信息** 要保存新的 ECMP 设置，请使用 `write memory` 命令，然后重新加载系统以使新设置生效。此命令的 `no` 版本将值恢复为默认值。

**示例**

```
OS10# configure terminal
OS10(config)# ip ecmp-group maximum-paths 2
OS10(config)# exit
OS10# write memory
OS10# reload
```

**支持的版本** 10.4.3.0 or later

## link-bundle-utilization trigger-threshold

配置阈值以在 ECMP 链路套装上触发流量监控分布。

**语法** `link-bundle-utilization trigger-threshold value`

**参数** `value` — 输入链路套装触发阈值，从 0 到 100。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本将禁用配置。

示例

OS10(config)# link-bundle-utilization trigger-threshold 80

支持的版本 10.2.0E or later

load-balancing

使用哈希算法中的默认参数来分配或负载均衡传入流量。

语法

load-balancing {ingress-port enable | [tcp-udp-selection l4-destination-port | l4-source-port] | [ip-selection destination-ip | source-ip | protocol | vlan-id | l4-destination-port | l4-source-port] | [ipv6-selection destination-ip | source-ip | protocol | vlan-id | l4-destination-port | l4-source-port] | [mac-selection destination-mac | source-mac | ethertype | vlan-id]}

- 参数
- ingress-port enable — 启用入口端口上的负载均衡。
  - tcp-udp-selection — 启用用于负载均衡配置的 TCP UDP 端口。
  - ip-selection — 启用在哈希计算中使用 IPv4 密钥参数。
  - ipv6-selection — 启用在哈希计算中使用的 IPV6 密钥参数。
  - destination-ip — 启用哈希计算中的目标 IP 地址。
  - source-ip — 启用哈希计算中的源 IP 地址。
  - protocol — 启用哈希计算中的协议信息。
  - vlan-id — 启用哈希计算中 VLAN ID 信息。
  - l4-destination-port — 启用哈希计算中的第 4 层 (L4) 目标端口信息。
  - l4-source-port — 启用哈希计算中的 L4 源端口信息。
  - mac-selection — 启用 MAC 负载均衡配置。
  - destination-mac — 启用哈希计算中的目标 MAC 信息。
  - source-mac — 启用哈希计算中的源 MAC 信息。
  - ethertype — 启用哈希计算中的以太网类型信息。

- 默认
- ip-selelection-source-ip dest-ip vlan-id l4-source-port l4-dest-port ipv4 protocol
  - ipv6-selection-source-ipv6 dest-ipv6 vlan-id l4-source-port l4-dest-port ipv6 protocol
  - mac-selection-source-mac destination-mac vlan-id ethertype
  - tcp-udp-selection-l4-source-port l4-dest-port

命令模式 CONFIGURATION

- 使用情况信息
- IPv4 —选择: source-ip destination-ip protocol vlan-id l4-destination-port l4-source-port
  - IPv6 目标地址: source-ip destination-ip protocol vlan-id l4-destination-port l4-source-port
  - MAC 参数: source-mac destination-mac ethertype vlan-id
  - TCP/UDP 参数: l4-destination-port l4-source-port

此命令的 no 版本会将该值重置为默认值。

示例 (入口)

OS10(config)# load-balancing ingress-port enable

示例 (IP 选择)

OS10(config)# load-balancing ip-selection destination-ip source-ip

支持的版本 10.2.0E or later

## show enhanced-hashing resilient-hashing

显示 enhanced-hashing 命令的状态。

|        |                                                      |
|--------|------------------------------------------------------|
| 语法     | show enhanced-hashing resilient-hashing {lag   ecmp} |
| 参数     | lag   ecmp — 输入关键字以查看端口通道或 ECMP 组的增强哈希。              |
| 默认     | 已禁用                                                  |
| 命令模式   | EXEC                                                 |
| 使用情况信息 | 无                                                    |

示例

```
OS10# show enhanced-hashing resilient-hashing lag
Resilient Hashing Configuration For LAG:

LAG Resilient hashing : Disabled
```

```
OS10# show enhanced-hashing resilient-hashing ECMP
Resilient Hashing Configuration For ECMP:

ECMP Resilient hashing : Disabled
```

|       |                   |
|-------|-------------------|
| 支持的版本 | 10.4.3.0 or later |
|-------|-------------------|

## show hash-algorithm

显示哈希算法信息。

|        |                     |
|--------|---------------------|
| 语法     | show hash-algorithm |
| 参数     | 无                   |
| 默认     | 未配置                 |
| 命令模式   | EXEC                |
| 使用情况信息 | 无                   |

示例

```
OS10# show hash-algorithm
EcmpAlgo - crc LabAlgo - crc
```

|       |                  |
|-------|------------------|
| 支持的版本 | 10.3.0E or later |
|-------|------------------|

## show ip ecmp-group details

显示 ECMP 组和路径的数量。

|        |                            |
|--------|----------------------------|
| 语法     | show ip ecmp-group details |
| 参数     | 无                          |
| 默认     | 未配置                        |
| 命令模式   | EXEC                       |
| 使用情况信息 | 无                          |

示例

```
OS10# show ip ecmp-group details
Maximum Number of ECMP Groups : 256
Maximum ECMP Path per Group : 64
Next boot configured Maximum ECMP Path per Group : 64
```

|       |                   |
|-------|-------------------|
| 支持的版本 | 10.4.3.0 or later |
|-------|-------------------|

## show load-balance

显示全局流量负载均衡配置。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show load-balance                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 示例     | <pre>OS10# show load-balance  Load-Balancing Configuration For LAG &amp; ECMP: ----- IPV4 Load Balancing Enabled IPV4 FIELDS : source-ipv4 dest-ipv4 vlan protocol L4-source-port L4-dest- port  IPV6 Load Balancing Enabled IPV6 FIELDS : source-ipv6 dest-ipv6 vlan protocol L4-source-port L4-dest- port  Mac Load Balancing Enabled MAC FIELDS : source-mac dest-mac vlan ethertype  mac-in-mac header based hashing is disabled TcpUdp Load Balancing Enabled</pre> |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## IPv4 路由

OS10 支持 IPv4 寻址，包括可变长度子网掩码 (VLSM)、地址解析协议 (ARP)、静态路由和路由协议。使用 VLSM，您可以配置一个具有不同掩码的网络。您也可以使用超网，这会增加子网的数量。您可以向 IP 地址添加掩码，以分隔 IP 地址的网络和主机部分，从而添加子网。

您需要为 IP 主机配置 IPv4 路由，以便在同一网络或不同的网络中彼此通信。

## 分配接口 IP 地址

您可以将主要和辅助 IP 地址分配给物理或逻辑接口，以实现系统与连接到特定接口的主机之间的 IP 通信。将一个主要地址和辅助 IP 地址分配给每个接口。默认情况下，所有端口都在默认 VLAN 中 — VLAN 1。

1. 在 CONFIGURATION 模式下输入要分配 IP 地址的接口类型信息。

```
interface interface
```

- ethernet — 物理接口
- port-channel — 端口通道 ID 号
- vlan — VLAN ID 号
- loopback — 环回接口 ID
- mgmt — 管理接口

2. 在 INTERFACE 模式下启用接口。

```
no shutdown
```

3. 在 INTERFACE 模式下从默认 VLAN 中移除接口。

```
no switchport
```

#### 4. 在 INTERFACE 模式下配置接口上的主要 IP 地址和掩码。

```
ip address ip-address mask [secondary]
```

- *ip-address mask*— 以点分隔的十进制格式输入 IP 地址 — A.B.C.D.和掩码（以斜杠前缀长度格式 [/24]）。
- *secondary* — 输入接口的辅助备份 IP 地址。

#### 将接口 IP 地址分配给接口

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/4)# no shutdown
OS10(conf-if-eth1/1/4)# no switchport
OS10(conf-if-eth1/1/4)# ip address 10.10.1.4/8
```

#### 查看接口配置

```
OS10# show interface ethernet 1/1/1
Ethernet 1/1/1 is up, line protocol is up
Hardware is Dell EMC Eth, address is 00:0c:29:98:1b:79
Current address is 00:0c:29:98:1b:79
Pluggable media present, QSFP+ type is QSFP+ 40GBASE CR 1.0M
Wavelength is 64
SFP receive power reading is 0.0
Interface index is 16866084
Internet address is not set
Mode of IPv4 Address Assignment: not set
MTU 1532 bytes
LineSpeed 40G, Auto-Negotiation on
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout: 60
Last clearing of "show interface" counters: 3 weeks 1 day 23:12:50
Queuing strategy: fifo
Input statistics:
 0 packets, 0 octets
 0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
 0 Multicasts, 0 Broadcasts, 0 Unicasts
 0 runts, 0 giants, 0 throttles
 0 CRC, 0 overrun, 0 discarded
Output statistics:
 0 packets, 0 octets
 0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
 0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
 0 Multicasts, 0 Broadcasts, 0 Unicasts
 0 throttles, 0 discarded, 0 Collisions, 0 wredrops
Rate Info(interval 299 seconds):
 Input 0 Mbits/sec, 0 packets/sec, 0% of line rate
 Output 0 Mbits/sec, 0 packets/sec, 0% of line rate
Time since last interface status change: 3 weeks 1 day 20:54:37
```

## 配置静态路由

您可以配置开放最短路径优先 (OSPF) 的手动或静态路由。

- 在 CONFIGURATION 模式下配置静态路由。

```
ip route ip-prefix/mask {next-hop | interface interface [route-preference]}
```

- *ip-prefix*— 以点分隔的十进制格式表示 IPv4 地址。
- *mask*— 以斜杠前缀长度格式 (/X) 作为掩码。
- *next-hop*— 以点分隔的十进制格式表示下一跳 IP 地址。
- *interface*— 具有节点/插槽/端口信息的接口类型
- *route-preference*— (可选) 路由首选项范围, 从 1 到 255。

#### 配置静态路由

```
OS10(config)# ip route 200.200.200.0/24 10.1.1.2
```

## 查看配置静态路由

```
OS10# show ip route static
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
Destination Gateway Dist/Metric Last Change

S 200.200.200.0/24 via 10.1.1.2 ethernet1/1/1 0/0 00:00:03
```

如果下一跳位于直接连接的子网上，OS10 将安装静态路由。不在直接连接的子网中的下一跳将在接口配置的子网上递归解析为下一跳，也会自动配置。例如，如果 interface ethernet 1/1/5 在子网 100.0.0.0/8 上具有 IP 地址，并且 10.1.1.0/24 递归解析为 100.1.1.1，则系统将安装静态路由：

- 当接口出现故障时，OS10 将收回该路由。
- 当接口亮起时，OS10 会重新安装路由。
- 当递归解析为 *broken* 时，OS10 将收回路由。
- 当满足递归解析时，OS10 会重新安装路由。

## 地址解析协议

地址解析协议 (ARP) 通过以太网运行，可让终端站了解 IP 网络上邻居的 MAC 地址。使用 ARP，OS10 会自动更新将 MAC 地址映射到相应 IP 地址的 *ARP cache* 表。*ARP cache* 将在您配置的时间段后删除动态获知的地址。

### 配置静态 ARP 条目

您可以在 ARP 映射表中手动配置静态条目。动态 ARP 容易受到欺骗。为避免哄骗，请配置静态条目。静态条目优先于动态 ARP 条目。

**注：**在默认转发表模式下，在第 3 层端口通道上获悉的最大 ARP 条目数限制为 32000。此限制仅适用于 Z9100 和 S5200。

1. 在 INTERFACE 模式下配置接口的 IP 地址和 MAC 地址映射。

```
ip arp ip-address mac address
```

- *ip-address*— 采用点分隔十进制格式格式的 IP 地址（以 A.B.C.D 格式表示）。
- *mac address*— 采用 nnnn.nnnn.nnnn 格式的 MAC 地址

这些条目不存在，您只能手动将其移除。要移除静态 ARP 条目，请使用 `no arp ip-address` 命令。

### 配置静态 ARP 条目

```
OS10(config)# interface ethernet 1/1/6
OS10(conf-if-eth1/1/6)# ip arp 10.1.1.5 08:00:20:b7:bd:32
```

### 查看 ARP 条目

```
OS10# show ip arp interface ethernet 1/1/6
Address Hardware address Interface Egress Interface

10.1.1.5 08:00:20:b7:bd:32 ethernet1/1/6 ethernet1/1/6
```

## IPv4 路由命令

### clear ip arp

从特定接口清除动态 ARP 条目，或者（可选）从内容可寻址内存 (CAM) 中删除（无刷新）ARP 条目。

**语法** `clear ip arp [vrf vrf-name] [interface interface | ip ip-address] [no-refresh]`

- 参数**
- `vrf vrf-name` — (可选) 输入 `vrf` 和 VRF 的名称, 以清除与该 VRF 对应的 ARP 条目。
  - `interface interface` — (可选) 指定接口类型:
    - `ethernet` — 物理接口。
    - `port-channel` — 端口通道标识符。
    - `vlan` — VLAN 标识符。
    - `loopback` — 环回接口标识符。
    - `virtual-network vn-id` — 虚拟网络 ID。
  - `ip ip-address` — (可选) 指定要清除的 ARP 条目的 IP 地址。
  - `no-refresh` — (可选) 从 CAM 删除 ARP 条目。您还可以将此选项与 `interface` 或 `ip ip-address` 一起使用, 以指定要删除的动态 ARP 条目。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 当删除的 ARP 条目再次解决并在 CAM 中重新安装时, 传输流量可能无法在此期间转发。

 **注:** 使用此选项时要格外小心。

**示例**

```
OS10# clear ip arp interface ethernet 1/1/5
```

**支持的版本** 10.2.0E or later

## clear ip route

从 IP 路由表中清除指定的路由。

**语法** `clear ip route [vrf vrf-name] { * | A.B.C.D/mask }`

- 参数**
- `vrf vrf-name` — (可选) 输入关键字 `vrf`, 然后输入 VRF 的名称, 以清除与该 VRF 对应的路由。
  - `*` — 清除整个 IP 路由表。此选项将刷新路由表中的所有路由。流量流将影响交换机中的所有路由。
  - `A.B.C.D/mask` — 指定要从 IP 路由表中移除的 IP 路由。此选项将刷新路由表中的所有路由。流量流仅影响交换机中的指定路由。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 此命令不会从路由表中移除静态路由。

**示例**

```
OS10# clear ipv6 route 10.1.1.0/24
```

**支持的版本** 10.3.0E or later

## ip address

配置接口的 IP 地址。

**语法** `ip address ip-address/mask`

**参数** `ip-address/mask` — 输入 IP 地址。

**默认** 无

**命令模式** INTERFACE

**使用情况信息** 此命令的 `no` 版本将移除接口的 IP 地址集。

**示例**

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip address 10.1.1.0/24
```

**支持的版本** 10.3.0E or later

## ip address dhcp

在接口上启用 DHCP 客户端操作。

|        |                                        |
|--------|----------------------------------------|
| 语法     | <code>ip address dhcp</code>           |
| 参数     | 无                                      |
| 默认     | 无                                      |
| 命令模式   | INTERFACE                              |
| 使用情况信息 | 此命令的 <code>no</code> 版本将禁用接口上 DHCP 操作。 |
| 示例     |                                        |

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# ip address dhcp
```

|       |                  |
|-------|------------------|
| 支持的版本 | 10.3.0E or later |
|-------|------------------|

## ip arp

配置静态 ARP 并将邻居的 IP 地址映射到 MAC 地址。

|        |                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip arp mac-address</code>                                                                           |
| 参数     | <code>mac-address</code> — 输入 IP 邻居的 MAC 地址（采用 A.B.C.D 格式）。                                               |
| 默认     | 未配置                                                                                                       |
| 命令模式   | INTERFACE                                                                                                 |
| 使用情况信息 | 请勿使用 Class D（多播）或 Class E（已保留）IP 地址。零 MAC 地址 (00:00:00:00:00:00) 无效。此命令的 <code>no</code> 版本将禁用 IP ARP 配置。 |
| 示例     |                                                                                                           |

```
OS10(conf-if-eth1/1/6)# ip arp 10.1.1.5 08:00:20:b7:bd:32
```

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|

## ip arp gratuitous

允许接口接收或发送免费的 ARP 请求和更新。

|        |                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip arp gratuitous {update   request}</code>                                                                                                                |
| 参数     | <ul style="list-style-type: none"><li><code>update</code> — 指定为免费 ARP 启用或禁用 ARP 高速缓存更新。</li><li><code>request</code> — 指定以启用或禁用当检测到重复地址时发送不必要的 ARP 请求。</li></ul> |
| 默认     | 未配置                                                                                                                                                              |
| 命令模式   | CONFIG-INTERFACE                                                                                                                                                 |
| 使用情况信息 | 当收到对免费 ARP 请求的答复时，它表示网络中存在 IP 地址冲突。此命令的 <code>no</code> 版本将禁用免费 ARP 的 ARP 高速缓存更新。                                                                                |
| 示例     |                                                                                                                                                                  |

```
OS10(conf-if-eth1/1/6)# ip arp gratuitous update
OS10(conf-if-eth1/1/6)# ip arp gratuitous request
```

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|



ip route

在网络设备上分配静态路由。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip route [vrf <b>vrf-name</b>] dest-ip-prefix mask {next-hop [ interface interface-type] [route-preference]}</code>                                                                                                                                                                                                                                                                                                                                                                                                               |
| 参数     | <ul style="list-style-type: none"><li><code>vrf vrf-name</code> — (可选) 输入 <code>vrf</code> 和 VRF 的名称，以配置与该 VRF 对应的静态路由。在 <code>ip route</code> 关键字后面使用此 VRF 选项，以配置该特定 VRF 上的静态路由。</li><li><code>dest-ip-prefix</code> — 以点分隔的 A.B.C.D 十进制格式输入目标 IP 前缀。</li><li><code>mask</code> — 以斜杠前缀长度 /x 格式输入掩码。</li><li><code>next-hop</code> — 以点分隔的十进制 A.B.C.D 格式输入下一跳 IP 地址。</li><li><code>interface interface-type</code> — 输入接口类型和接口信息。支持的接口类型为：以太网、端口信道、VLAN 和空。</li><li><code>route-preference</code> — (可选) 输入介于 1 到 255 之间的范围。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 使用情况信息 | 此命令的 <code>no</code> 版本将删除静态路由配置。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 示例     | <pre>OS10(config)# ip route 200.200.200.0/24 10.1.1.2</pre> <pre>OS10(config)# ip route 200.200.200.0/24 interface null 0</pre>                                                                                                                                                                                                                                                                                                                                                                                                         |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

show ip arp

显示特定 IP 地址或 MAC 地址、静态、动态和所有 ARP 条目的摘要的 ARP 表条目。

语法

```
show ip arp [vrf vrf-name] [interface [ethernet | vlan | port-channel] | ip-address | mac-address | static | dynamic | summary]
```

参数

- `vrf vrf-name` — 输入 `vrf` 和 VRF 的名称，以显示与该 VRF 对应的 ARP 条目。
- `interface` — （可选）输入关键字和接口信息：
  - `ethernet` — 输入 node/slot/port[:subport] 信息。
  - `vlan` — 输入 VLAN ID 号，从 1 到 4093。
  - `port-channel` — 输入端口通道 ID 号，从 1 到 128。
- `ip-address` — （可选）输入 ARP 条目的 IP 地址（采用 A.B.C.D 格式）。
- `mac-address` — （可选）以 nn:nn:nn:nn:nn:nn 格式输入 MAC 地址。
- `static` — （可选）输入关键字以显示静态 ARP 条目。
- `dynamic` — （可选）输入关键字以显示动态 ARP 条目。
- `summary` — （可选）输入关键字以显示所有 ARP 条目的摘要。

默认

未配置

命令模式

EXEC

使用情况信息

此命令同时显示静态和动态 ARP 条目。

示例（IP 地址）

```
OS10# show ip arp 192.168.2.2
```

| Address     | Hardware address  | Interface        | Egress Interface |
|-------------|-------------------|------------------|------------------|
| 192.168.2.2 | 90:b1:1c:f4:a6:e6 | ethernet1/1/49:1 | ethernet1/1/49:1 |

示例（静态）

```
OS10# show ip arp summary
```

| Total Entries | Static Entries | Dynamic Entries |
|---------------|----------------|-----------------|
|---------------|----------------|-----------------|

|       |       |       |
|-------|-------|-------|
| ----- | ----- | ----- |
| 3994  | 0     | 3994  |

|                               |                   |                  |                  |
|-------------------------------|-------------------|------------------|------------------|
| OS10# show ip arp 192.168.2.2 |                   |                  |                  |
| Address                       | Hardware address  | Interface        | Egress Interface |
| -----                         | -----             | -----            | -----            |
| 192.168.2.2                   | 90:b1:1c:f4:a6:e6 | ethernet1/1/49:1 | ethernet1/1/49:1 |

|                   |                   |                  |                  |
|-------------------|-------------------|------------------|------------------|
| OS10# show ip arp |                   |                  |                  |
| Address           | Hardware address  | Interface        | Egress Interface |
| -----             | -----             | -----            | -----            |
| 192.168.2.2       | 90:b1:1c:f4:a6:e6 | ethernet1/1/49:1 | ethernet1/1/49:1 |
| 193.168.2.3       | 54:bf:64:e6:d4:c5 | vlan4000         | port-channel1000 |

**示例（动态）**

|                           |                   |                  |                  |
|---------------------------|-------------------|------------------|------------------|
| OS10# show ip arp dynamic |                   |                  |                  |
| Address                   | Hardware address  | Interface        | Egress Interface |
| -----                     | -----             | -----            | -----            |
| 192.168.2.2               | 90:b1:1c:f4:a6:e6 | ethernet1/1/49:1 | ethernet1/1/49:1 |
| 193.168.2.3               | 54:bf:64:e6:d4:c5 | vlan4000         | port-channel1000 |

**支持的版本**
10.2.0E or later

**show ip route**

显示 IP 路由信息。

**语法**

```
show ip route [vrf vrf-name] [all | bgp | connected | ospf process-id | static | ip
summary] load-balancing {ingress-port enable | [tcp-udp-selection l4-destination-po
port] | [ip-selection destination-ip | source-ip | protocol | vlan-id | l4-destinat
source-port] | [ipv6-selection destination-ip | source-ip | protocol | vlan-id | l4
l4-source-port] | [mac-selection destination-mac | source-mac | ethertype | vlan-id
}
```

- 参数**
  - vrf vrf-name —（可选）输入 vrf，然后选择 VRF 名称，以列出特定 VRF 的路由表中的路由。
  - all —（可选）显示活动和非活动 IP 路由。
  - bgp —（可选）显示 BGP 路由信息。
  - connected —（可选）仅显示直接连接的路由。
  - ospf process-id —（可选）显示 OSPF 进程的路由信息，从 1 到 65535。
  - static —（可选）显示静态路由信息。
  - ip-prefix/mask —（可选）显示目标前缀列表的路由。  

*i*
**注:** 此选项仅适用于准确的前缀和掩码长度。
  - summary —（可选）显示 IP 路由摘要。

**默认**
未配置

**命令模式**
EXEC

**使用情况信息**
无

**示例**

```
OS10# show ip route
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
 Destination Gateway Dist/Metric Last Change

 C 10.1.1.0/24 via 10.1.1.1 vlan100 0/0 01:16:56
 B EX 10.1.2.0/24 via 10.1.2.1 vlan101 20/0 01:16:56
 O 10.1.3.0/24 via 10.1.3.1 vlan102 110/2 01:16:56
 B IN 10.1.4.0/24 via 10.1.4.1 vlan103 200/0 01:16:56
```

```

OS10(config)# do show ip route vrf VRF1
Codes: C - connected
S - static
B - BGP, IN - internal BGP, EX - external BGP
O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
E2 - OSPF external type 2, * - candidate default,
+ - summary route, > - non-active route
Gateway of last resort is not set
Destination Gateway Dist/Metric Last Change

C 120.0.0.0/24 via 120.0.0.1 ethernet1/1/1 0/0 00:00:57
S 160.0.0.0/24 via 120.0.0.2 ethernet1/1/1 1/0 00:00:04
OS10(config)# do show ip route vrf VRF2
Codes: C - connected
S - static
B - BGP, IN - internal BGP, EX - external BGP
O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
E2 - OSPF external type 2, * - candidate default,
+ - summary route, > - non-active route
Gateway of last resort is not set
Destination Gateway Dist/Metric Last Change

C 140.0.0.0/24 via 140.0.0.1 ethernet1/1/2 0/0 00:01:54
B IN 160.0.0.0/24 via 120.0.0.2 200/0 00:00:02

```

#### 支持的版本

10.2.0E or later

## IPv6 路由

OS10 支持 IPv6 路由和寻址，包括邻居发现协议 (NDP)、无状态 IPv6 地址自动配置以及有状态的 IPv6 地址配置。为 IP 主机配置 IPv6 路由，以便在同一网络或不同网络中彼此通信。

 **注：** OS10 不支持下一代路由信息协议 (RIPNG)。

## 启用或禁用 IPv6

默认情况下：

- 在物理以太网接口、VLAN 和端口组上已启用 IPv6 转发。仅当您启用接口上的 IPv6 地址自动配置，并使用 `ipv6 address autoconfig` 命令将其设置为主机模式时，才会禁用 IPv6 转发。
- 在管理以太网接口上已永久禁用 IPv6 转发功能以使其保持主机模式，并且不会作为路由器运行，而不管 `ipv6 address autoconfig` 设置如何。

如有必要，您可以手动禁用接口上的 IPv6 处理，以便配置的 IPv6 地址不会生效。当您重新启用 IPv6 时，IPv6 地址会再次生效。

如果您禁用 IPv6 并在层 (L3) 模式下配置层 (L2) 接口，则不会在接口上自动重新启用 IPv6。您必须手动重新启用它。

当使用 `ipv6 enable` 命令在接口上重新启用 IPv6 时，将自动生成链路本地地址。

#### 禁用和启用 IPv6

```

OS10(config)# interface ethernet 1/1/8
OS10(conf-if-eth1/1/8)# ipv6 address 2111:dddd:0eee::22/64
OS10(conf-if-eth1/1/8)# no ipv6 address autoconfig
OS10(conf-if-eth1/1/8)# no ipv6 enable
OS10(conf-if-eth1/1/8)# ipv6 enable

```

#### 显示 IPv6 状态

```

OS10# show interface ethernet 1/1/20
Ethernet 1/1/20 is up, line protocol is up
Hardware is Dell EMC Eth, address is ec:f4:bb:fb:fa:30
Current address is ec:f4:bb:fb:fa:30
Pluggable media present, QSFP+ type is QSFP+ 40GBASE CR 1.0M

```

```

Wavelength is 850
Receive power reading is 0.0
Interface index is 17305562
Internet address is 20.20.20.1/24
Mode of IPv4 Address Assignment: MANUAL
Interface IPv6 oper status: Enabled
Link local IPv6 address: fe80::eef4:bbff:febf:fa30/64
Global IPv6 address: 2020::1/64
...

```

```

OS10# show ipv6 interface brief
Interface Name admin/protocol IPV6 Address/Link-Local Address IPv6 Oper Status
=====
Ethernet 1/1/1:1 up / up fe80::eef4:bbff:febf:f9f0/64 Enabled
 2017::1/64
Ethernet 1/1/20 up / up fe80::eef4:bbff:febf:fa30/64 Enabled
 2020::1/64
Management 1/1/1 up / up fe80::eef4:bbff:febf:f9ef/64 Enabled
Vlan 1 up / up fe80::eef4:bbff:febf:fa59/64 Enabled

```

## IPv6 地址

IPv6 地址包含 48 位全局路由前缀、可选的 16 位子网 ID 以及采用扩展通用标识符的 64 位接口标识符 (EUI) - 64 格式。

IPv6 128 位地址表示为一系列由冒号分隔的八个 16 位十六进制字段：X:X:X:X:X:X:X。

```
2001:0db8:0000:0000:0000:0000:1428:57a
```

每个字段中的前导零是可选的。您还可以使用两个冒号 (::) 表示零的连续十六进制字段，但在每个地址中只能使用一次短版本：

```
2001:db8::1428:57ab
```

在下面的示例中，所有地址均有效并且等同：

- 2001:0db8:0000:0000:0000:0000:1428:57ab
- 2001:0db8:0000:0000:0000::1428:57ab
- 2001:0db8:0:0:0:0:1428:57ab
- 2001:0db8:0:0::1428:57ab
- 2001:0db8::1428:57ab
- 2001:db8::1428:57ab

使用 CIDR 表示法可以写入 IPv6 网络。IPv6 网络或子网是连续的一组 IPv6 地址，必须为 2 的幂。网络中所有主机的初始地址位完全相同，是网络的前缀。

网络由网络中的第一个地址和小数位数（以十进制分隔，以小数点分隔）表示。由于单个主机被视为带有 128 位前缀的网络，因此主机地址可能使用以下 /128 编写。

例如，2001:0db8:1234::/48 代表网络的地址 2001:0db8:1234:0000:0000:0000:0000:0000（通过 2001:0db8:1234:ffff:ffff:ffff:ffff:ffff）。

一旦您分配了 IPv6 地址，就会在接口上启用 IPv6 数据包处理。您可以使用 `no ipv6 enable` 和 `ipv6 enable` 命令在使用 IPv6 地址配置的接口上手动禁用和重新启用 IPv6 处理。

要从某个接口移除所有 IPv6 地址，请使用 `no ipv6 address` 命令。要删除特定的 IPv6 地址，请使用 `ipv6 address ipv6-address/mask` 命令。

### 链路本地地址

当 OS10 交换机启动时，IPv6 单播链路本地地址将自动分配到使用无状态配置的接口。链路本地地址允许本地链路上的 IPv6 设备进行通信，而无需全局唯一地址。IPv6 将保留地址块 FE80::/10，用于链路本地单播寻址。

### 全局地址

要启用 IPv6 全局地址的无状态自动配置并将接口设置为主机模式，请使用 `ipv6 address autoconfig` 命令。路由器将接收 IPv6 路由器通告 (RA) 中的网络前缀。接口 ID 将附加到前缀。在主机模式下，IPv6 转发已禁用。

`no ipv6 address autoconfig` 命令将禁用 IPv6 全局地址自动配置，并将接口设置为启用 IPv6 转发的路由器模式。

### DHCP 分配的地址

作为无状态自动配置的替代方案，您可以启用网络主机，通过使用 `ipv6 address dhcp` 命令的状态自动配置来使用 DHCP 服务器获取 IPv6 地址。DHCPv6 服务器使用前缀池来配置接口上的网络地址。接口 ID 将自动生成。

**注：**在管理接口或管理 VLAN 上，使用 DHCPv6 获取 IP 地址时，将为接口分配带有 /128 前缀掩码的 IPv6 地址。但是，为了保持向后兼容性和允许访问，还提供了带有 /64 前缀的静态路由。

### 手动配置的地址

一个接口可以有多个 IPv6 地址。要配置 IPv6 地址以及链路本地地址，请使用 `ipv6 address ipv6-address/mask` 命令。输入完整的 128 位 IPv6 地址，包括网络前缀和 64 位接口 ID。

**注：**Dell EMC Networking 不建议在同一接口上同时配置静态 IPv6 地址和 DHCPv6。

您还可以通过分配以下命令来手动配置 IPv6 地址：

- 使用 `ipv6 address ipv6-prefix eui64` 命令的带 EUI-64 参数的网络前缀。64 位接口 ID 会根据 MAC 地址自动生成。
- 要使用的链路本地地址，而不是在使用 `ipv6 address link-local` 命令启用 IPv6 时自动配置的链路本地地址。

### 配置 IPv6 地址

```
OS10(config)# interface ethernet 1/1/8
OS10(conf-if-eth1/1/8)# ipv6 address 2001:dddd:0eee::4/64
```

### 配置网络前缀

```
OS10(config)# interface ethernet 1/1/8
OS10(conf-if-eth1/1/8)# ipv6 address 2001:FF21:1:1::/64 eui64
```

### 配置链路本地地址

```
OS10(config)# interface ethernet 1/1/8
OS10(conf-if-eth1/1/8)# ipv6 address FE80::1/64 link-local
```

## 无状态自动配置

当接口启动时，OS10 使用无状态自动配置来生成具有 FE80::/64 前缀的唯一链路本地 IPv6 地址，以及从 MAC 地址生成的接口 ID。要使用无状态自动配置，以使用路由器通告中接收的前缀分配全局唯一地址，请使用 `ipv6 address autoconfig` 命令。

无状态自动配置可在主机模式中设置接口，并允许连接到 IPv6 网络的接口，以自动配置 IPv6 地址并与本地链路上的其他 IPv6 设备进行通信。自动 IPv6 接口配置不需要 DHCP 服务器。本地链路上的 IPv6 设备发送路由器通告 (RA) 消息，以响应启动时收到的请求消息。

使用以下命令执行 IPv6 地址的无状态自动配置：

|               |                                                        |
|---------------|--------------------------------------------------------|
| <b>前缀通告</b>   | 路由器使用路由器通告消息通告网络前缀。主机将其接口标识符添加到 MAC 地址，以生成有效的 IPv6 地址。 |
| <b>重复地址检测</b> | IPv6 主机节点会在配置其 IPv6 地址之前，使用此机制检查是否在网络上的任何位置使用该地址。      |
| <b>前缀重新编号</b> | 当组织更改其服务提供商时，对网络中的主机进行透明重新编号。                          |

IPv6 提供了在 RA 上添加前缀以响应路由器请求 (RS) 的灵活性。默认情况下，在收到 RS 消息时，将发送 RA 响应消息。IPv6 无状态自动配置的系统操作仅支持路由器端。邻居查找 (ND) 消息通告，因此邻居可使用此信息自动配置其地址。接收的 ND 消息不用于创建 IPv6 地址。

将记录路由器之间的 RA 值不一致性。将被检查一致性的值包括：

- 当前跳限制
- M 和 O 标记
- 可访问时间
- 重新传输计时器
- MTU 选项
- 相同前缀的首选和有效生存期值

NDP 中的路由器重定向功能与 IPv4 路由器重定向消息类似。NDP 使用 ICMPv6 重定向消息 (类型 137) 来通知节点链路上存在的更好路由器。

## 邻居查找

IPv6 NDP 确定邻近 IPv6 设备是否可访问，并接收本地链路上 IPv6 设备的 IPv6 地址。使用邻居地址的链路层和全局前缀，OS10 对接口上的 IPv6 地址执行无状态自动配置。

ICMPv6 RA 消息将通告已启用 IPv6 的接口的 IPv6 地址，并允许路由器了解 IPv6 邻居中的任何地址更改。默认情况下，RA 在接口上处于禁用状态。

### 前提条件

要启用 RA 消息，交换机必须处于路由器模式且启用了 IPv6 转发，并且使用 `no ipv6 address autoconfig` 命令禁用了无状态自动配置。

### 启用路由器通告消息

1. 启用 IPv6 邻居查找并在接口模式下发送 ICMPv6 RA 消息。

```
ipv6 nd send-ra
```

2. (可选) 在接口模式下配置 IPv6 邻居查找选项。

- `ipv6 nd hop-limit hops` — (可选) 设置 RA 消息中通告的跳限制，并将其包含在由路由器发送的 IPv6 数据包中，从 0 到 255；默认值为 64。0 表示路由器未指定任何跳限制。
- `ipv6 nd managed-config-flag` — (可选) 在 RA 消息中发送，以告知主机使用状态地址自动配置（如 DHCPv6）来获取 IPv6 地址。
- `ipv6 nd max-ra-interval seconds` — (可选) 设置发送 RA 消息的最长时间间隔，从 4 到 1800 秒，默认值为 600。
- `ipv6 nd mtu number` — (可选) 设置链路上的 RA 消息中使用的最大传输单位 (MTU)，从 1280 到 65535 字节；默认值为 1500。默认情况下，RA 消息中不包含 MTU 设置。
- `ipv6 nd other-config-flag` — (可选) 通知主机使用状态自动配置来获得与非地址相关的信息。
- `ipv6 nd ra-lifetime seconds` — (可选) 设置 RA 消息中默认路由器的生存期，从 0 到 9000 毫秒；默认值为 3 乘以 `max-ra-interval` 设置。0 表示此路由器未用作默认路由器。
- `ipv6 nd reachable-time milliseconds` — (可选) 设置路由器在接收到邻居可访问性确认后看到邻居显示的通告时间，从 0 到 3600000 毫秒；默认值为 0。0 表示在 RA 消息中未发送可访问的时间。
- `ipv6 nd retrans-timer seconds` — (可选) 设置重新传输邻居请求消息之间的时间，从 100 到 4292967295 毫秒。默认情况下，未配置任何重新传输计时器。

3. 在接口模式下配置 IPv6 邻居查找所通告的 IPv6 前缀。

```
ipv6 nd prefix {ipv6-prefix | default} [no-advertise] [no-autoconfig] [no-rtr-address]
[off-link] [lifetime {valid-lifetime seconds | infinite}]
{preferred-lifetime seconds | infinite}]
```

- `ipv6-prefix` — 以 `x::y/mask` 格式输入 IPv6 前缀以包括 RA 消息中的前缀。包括在接口上配置的子网中尚未存在的前缀。
- `default` — 配置在接口上配置的所有子网中通告的前缀参数。
- `no-advertise` — (可选) 不通告指定的前缀。默认情况下，将通告已配置子网中的所有前缀。
- `no-autoconfig` — (可选) 针对 `radvd.conf` 文件中的指定前缀将 `AdvAutonomous` 设置为 `Off`。此设置会告诉主机不要使用此前缀进行地址自动配置。默认情况下，`AdvAutonomous` 为 `On`。
- `no-rtr-address` — (可选) 针对 `radvd.conf` 文件中的前缀将 `AdvRouterAddr` 设置为 `Off`。`Off` 设置告知主机不使用通告路由器地址进行链路上确定。默认情况下，`AdvRouterAddr` 为 `On`。
- `off-link` — (可选) 针对 `radvd.conf` 文件中的前缀将 `AdvOnLink` 设置为 `Off`。`Off` 设置告知主机不使用此前缀用于链路上确定。默认情况下，`AdvOnLink` 为 `On`。
- `lifetime {valid-lifetime seconds | infinite}` — (可选) 针对 `radvd.conf` 文件中的前缀设置 `AdvValidLifetime` (以秒为单位)。此前缀仅对指定生存期内的链路上确定有效。默认值为 86400 秒 (1 天)。`infinite` 设置允许前缀对无时间限制的链路上确定有效。
- `lifetime {preferred-lifetime seconds | infinite}` — (可选) 针对 `radvd.conf` 文件中的前缀设置 `AdvPreferredLifetime` (以秒为单位)。使用无状态自动配置从前缀生成的 IPv6 地址在配置的生命周期内保持首选。默认值为 14400 秒 (4 小时)。`infinite` 设置允许使用前缀进行自动配置的地址为首选地址，且无时间限制。

默认情况下，会通告在接口上的 IPv6 地址中配置的所有前缀。要修改为接口子网前缀通告的默认值，请使用 `ipv6 nd prefix default` 命令并指定新的默认设置。

链路上确定是用于将数据包 IPv6 转发到目标 IPv6 地址的进程。



## 配置邻居查找

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 nd mtu 1500
OS10(conf-if-eth1/1/1)# ipv6 nd send-ra
```

## 配置通告 IPv6 前缀

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 nd prefix default lifetime infinite infinite
OS10(conf-if-eth1/1/1)# ipv6 nd prefix 2002::/64
```

## 重复地址查找

要在将 IPv6 单播地址分配到接口之前确定其是否唯一，OS10 交换机将发送邻居请求消息。如果重复地址发现 (DAD) 的进程在网络中检测到重复地址，该地址不会在接口上配置。DAD 默认已启用。

默认情况下，当检测到重复地址时，IPv6 不会被禁用。仅重复地址未应用。其他 IPv6 地址仍在接口上处于活动状态。

要在检测到重复的链路本地地址时禁用接口上的 IPv6，请使用 `ipv6 nd dad disable-ipv6-on-failure` 命令。要在解决重复链路本地地址后重新启用 IPv6，请输入 `no ipv6 enable`，然后输入 `ipv6 enable` 命令。

- 在接口模式下禁用或重新启用 IPv6 重复地址查找。

```
ipv6 nd dad {disable | enable}
```

- 如果在接口模式中发现重复的链路本地地址，则禁用接口上的 IPv6。

```
ipv6 nd dad disable-ipv6-on-dad-failure
```

## 禁用重复地址查找

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 nd dad disable
```

## 对重复的链路本地地址禁用 IPv6

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 nd dad disable-ipv6-on-dad-failure
```

## 静态 IPv6 路由

要在两个 IPv6 网络设备之间定义显式路由，请在接口上配置静态路由。静态路由对于仅有一条路径到外部网络的小型网络非常有用，或者为大型网络中的某些流量类型提供安全性。

- 在 CONFIGURATION 模式下输入静态路由信息，包括以 `in x::x::x::x` 格式显示的 IPv6 地址和掩码。长度为 0 到 64。

```
ipv6 route ipv6-prefix/mask {next-hop | interface interface [route-preference]}
```

- `next-hop` — 以 `x::x::x::x` 格式输入下一跳 IPv6 地址。
- `interface interface` — 输入接口类型，然后输入插槽/端口或编号信息。
- `route-preference` — (可选) 输入路由首选项范围，从 1 到 255。

配置静态 IPv6 路由后，配置接口上转发路由器的地址。IPv6 邻居接口必须配置有 IPv6 地址。

## 配置 IPv6 静态路由和查看配置

```
OS10(config)# ipv6 route 2111:dddd:0eee::22/128 2001:db86:0fff::2
OS10(config)# do show ipv6 route static
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, > - non-active route
```

```

Gateway of last resort is not set
 Destination Gateway Dist/Metric Last Change

S 2111:dddd:eee::22/12via 2001:db86:fff::2 ethernet1/1/1 1/1 00:01:24

```

## IPv6 目标无法访问

默认情况下，在 IPv6 路由表中找不到 IPv6 路由的匹配条目时，数据包将丢弃，并且不会发送错误消息。您可以启用将 IPv6 destination unreachable 错误消息发送至源而不丢弃数据包的功能。

### 启用 IPv6 无法访问的目标消息传送

```

OS10(config)# interface ethernet 1/1/8
OS10(conf-if-eth1/1/8)# ipv6 unreachable

```

## IPv6 逐跳选项

IPv6 数据包中的逐跳标头扩展包含数据包路径中所有 IPv6 路由器处理的选项。默认情况下，IPv6 数据包中的逐跳标头选项不会在本地处理。要在接口上启用 IPv6 逐跳选项的本地处理，请使用 ipv6 hop-by-hop 命令。

### 启用 IPv6 逐跳选项转发

```

OS10(config)# interface ethernet 1/1/8
OS10(conf-if-eth1/1/8)# ipv6 hop-by-hop

```

## 查看 IPv6 信息

要查看 IPv6 的配置信息，请使用 show ipv6 route 命令。要查看 IPv6 地址信息，请使用 show address ipv6 命令。

### 查看 IPv6 连接的信息

```

OS10# show ipv6 route connected
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
 Destination Gateway Dist/Metric Last Change

C 2001:db86::/32 via 2001:db86:fff::1 ethernet1/1/1 0/0 00:03:24

```

### 查看 IPv6 静态信息

```

OS10# show ipv6 route static
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
 Destination Gateway Dist/Metric Last Change

S 2111:dddd:eee::22/12via 2001:db86:fff::2 ethernet1/1/1 1/1 00:01:24

```



# IPv6 命令

## clear ipv6 neighbors

删除 IPv6 邻居发现高速缓存中的所有条目或特定接口的邻居。静态条目不会移除。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>clear ipv6 neighbors [vrf vrf-name] [ipv6-address   interface   virtual-network vn-id   all]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 参数     | <ul style="list-style-type: none"><li><code>vrf vrf-name</code> — (可选) 输入 vrf 和 VRF 的名称, 以清除与该 VRF 对应的邻居。如果未指定此选项, 则默认 VRF 中的邻居将清除。</li><li><code>ipv6-address</code> — 以 <code>x:x:x:x::x</code> 格式输入邻居的 IPv6 地址, 以移除特定的 IPv6 邻居。<code>::</code> 表示法指定零的连续十六进制字段。</li><li><code>interface interface</code> — 要移除在特定接口上学习的所有邻居条目, 请输入关键字接口, 然后是接口类型和接口的插槽/端口或号码信息:<ul style="list-style-type: none"><li>对于 10 Gb 以太网接口, 输入 <code>TenGigabitEthernet</code>, 然后输入插槽/端口/子端口[/子端口]信息。</li><li>对于 40 Gb 以太网接口, 输入 <code>fortyGigE</code>, 然后输入插槽/端口信息。</li><li>对于端口通道接口, 输入 <code>port-channel</code>, 然后输入数字。</li><li>对于 VLAN 接口, 输入 <code>vlan</code>, 然后输入 1 到 4093 之间的某个数字。</li><li><code>virtual-network vn-id</code> — 对于虚拟网络, 输入 <code>virtual-network</code> 和网络的 ID。</li></ul></li></ul> |
| 默认     | 无。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | 此命令的 <code>no</code> 版本会将该值重置为默认值。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 示例     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 支持的版本  | 10.4.1.0 or later 或更高版本                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## clear ipv6 route

清除 IPv6 路由表中的路由。

|        |                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>clear ipv6 route [vrf vrf-name] {*   A::B/mask}</code>                                                                                                                                                                                                         |
| 参数     | <ul style="list-style-type: none"><li><code>vrf vrf-name</code> — (可选) 输入 vrf 和 VRF 的名称, 以清除与该 VRF 对应的 IPv6 路由。</li><li><code>*</code> — 清除所有路由并刷新 IPv6 路由表。交换机中所有路由的流量流都会受到影响。</li><li><code>A::B/mask</code> — 移除 IPv6 路由并刷新 IPv6 路由表。交换机中的流量流仅受指定路由的影响。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                  |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                 |
| 使用情况信息 | 此命令不会从路由表中移除静态路由。                                                                                                                                                                                                                                                    |
| 示例     | <pre>OS10# clear ipv6 route *</pre>                                                                                                                                                                                                                                  |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                     |

## ipv6 address

在接口上配置全局单播 IPv6 地址。

|      |                                                                                      |
|------|--------------------------------------------------------------------------------------|
| 语法   | <code>ipv6 address ipv6-address/prefix-length</code>                                 |
| 参数   | <code>ipv6-address/prefix-length</code> — 输入包含网络前缀长度的完整 128 位 IPv6 地址, 包括 64 位接口标识符。 |
| 默认   | 无                                                                                    |
| 命令模式 | INTERFACE                                                                            |

## 使用情况信息

一个接口可以有多个 IPv6 地址。要配置 IPv6 地址以及链路本地地址，请使用 `ipv6 address ipv6-address/mask` 命令并指定完整的 128 位 IPv6 地址。要通过仅输入网络前缀和长度来配置全局唯一的 IPv6 地址，请使用 `ipv6 address ipv6-prefix/prefix-length eui-64` 命令。

此命令的 `no` 版本将移除接口上的 IPv6 地址。

 **注:** Dell EMC Networking 不建议在同一接口上同时配置静态 IPv6 地址和 DHCPv6。

## 示例

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 address 2111:dddd:0eee::22/64
```

## 支持的版本

10.3.0E or later

# ipv6 address autoconfig

使用从 RA 获得的网络前缀获取全局 IPv6 地址。

## 语法

`ipv6 address autoconfig`

## 参数

无

## 默认

已禁用（在管理接口上除外）

## 命令模式

INTERFACE

## 使用情况信息

- 此命令可在主机模式下将接口设置为通过查找本地链路上的前缀来执行 IPv6 无状态自动配置，并添加基于 EUI-64 的接口标识符以生成每个 IPv6 地址。命令将禁用 IPv6 转发。地址根据 RA 消息中接收的前缀进行配置。
- 此命令的 `no` 版本将禁用 IPv6 地址自动配置，在路由器模式下重置接口，并重新启用 IPv6 转发。

## 示例

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# ipv6 address autoconfig
OS10(conf-if-eth1/1/1)#
```

## 支持的版本

10.3.0E or later

# ipv6 address dhcp

在接口上启用 DHCP 客户端操作。

## 语法

`ipv6 address dhcp`

## 参数

无

## 默认

无

## 命令模式

INTERFACE

## 使用情况信息

此命令的 `no` 版本将禁用接口上 DHCP 操作。

 **注:** Dell EMC Networking 不建议在同一接口上同时配置静态 IPv6 地址和 DHCPv6。

## 示例

```
OS10(config)# interface mgmt 1/1/1
OS10(conf-if-ma-1/1/1)# ipv6 address dhcp
```

## 支持的版本

10.3.0E or later

## ipv6 enable

启用和禁用使用 IPv6 地址配置的接口上的 IPv6 转发。

**语法** `ipv6 enable`

**参数** 无

**默认** 无

**命令模式** INTERFACE

**使用情况信息** 使用此命令可以禁用和重新启用接口上的 IPv6 转发，以确保安全或从重复地址发现 (DAD) 故障中恢复。此命令的 `no` 版本将禁用 IPv6 转发。

**示例**

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# ipv6 address 2111:dddd:0eee::22/128
OS10(config-if-eth1/1/1)# no ipv6 enable
OS10(config-if-eth1/1/1)# ipv6 enable
```

**支持的版本** 10.3.0E or later

## ipv6 address eui-64

通过仅输入网络前缀和长度来配置接口上的全局 IPv6 地址。

**语法** `ipv6 address ipv6-prefix/prefix-length eui-64`

**参数** `ipv6-prefix` — 以 `x:x::y/mask` 格式输入 IPv6 前缀。

**默认** 无

**命令模式** INTERFACE

**使用情况信息** 除了通过无状态自动配置生成的链路本地地址外，还可使用此命令来手动配置 IPv6 地址。仅指定网络前缀和长度。64 位接口 ID 会自动从 MAC 地址计算。此命令可启用对接口的 IPv6 处理。此命令的 `no` 版本将移除 IPv6 地址配置。

**示例**

```
OS10(config)# interface mgmt 1/1/1
OS10(config-if-ma-1/1/1)# ipv6 address 2111:dddd:0eee::/64 eui-64
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 address link-local

在要使用的接口上配置链路本地 IPv6 地址，而不是自动配置无状态自动配置的链路本地地址。

**语法** `ipv6 address ipv6-prefix link-local`

**参数** `ipv6-prefix` — 以 `x:x::y/mask` 格式输入 IPv6 前缀。

**默认** 无

**命令模式** INTERFACE

**使用情况信息**

- 一个接口只能有一个链路本地地址。默认情况下，当路由器启动并启用 IPv6 时，将使用基于 MAC 的 EUI-64 接口 ID 自动生成 IPv6 链路本地地址。使用此命令可手动配置链路本地地址以替换自动配置的地址。例如，要配置更易于用户识别的链路本地地址，请将 `fe80::eef4:bbff:febf:fa30/64` 替换为 `fe80::1/64`。
- 此命令的 `no` 版本将移除指定的链路本地地址。

**示例**

```
OS10(config)# interface mgmt 1/1/1
OS10(config-if-ma-1/1/1)# ipv6 address 2111:dddd:0eee::22/64 link-local
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 hop-by-hop

启用和禁用 IPv6 数据包标头中的逐跳选项。

|               |                                                                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ipv6 hop-by-hop</code>                                                                                                                                 |
| <b>参数</b>     | 无                                                                                                                                                            |
| <b>默认</b>     | IPv6 数据包中的逐跳标头选项不在接口上处理。                                                                                                                                     |
| <b>命令模式</b>   | INTERFACE                                                                                                                                                    |
| <b>使用情况信息</b> | <ul style="list-style-type: none"><li>使用此命令可以在符合 RFC 8200、IPv6 规范的前提下，使用逐跳选项启用 IPv6 数据包的本地处理。</li><li>此命令的 <code>no</code> 版本将禁用 IPv6 处理逐跳标头选项的处理。</li></ul> |

### 示例：禁用逐跳选项处理

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# no ipv6 hop-by-hop
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 nd dad

禁用或重新启用 IPv6 重复地址查找 (DAD)。

|               |                                                                                                                                                                                                                                                                                                               |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ipv6 nd dad {disable   enable   disable-ipv6-on-dad-failure}</code>                                                                                                                                                                                                                                     |
| <b>参数</b>     | <ul style="list-style-type: none"><li><code>disable</code> — 禁用接口上的重复地址发现。</li><li><code>enable</code> — 重新启用 IPv6 重复地址查找（如果已禁用）。</li><li><code>disable-ipv6-on-dad-failure</code> — 启用现有自动配置链路本地地址上的重复地址发现。</li></ul>                                                                                        |
| <b>默认</b>     | 在接口上启用重复地址发现。                                                                                                                                                                                                                                                                                                 |
| <b>命令模式</b>   | INTERFACE                                                                                                                                                                                                                                                                                                     |
| <b>使用情况信息</b> | <ul style="list-style-type: none"><li>OS10 交换机将发送邻居请求消息，以确定自动配置的 IPv6 单播链路本地地址在将其分配到接口之前是否是唯一的。如果重复地址发现 (DAD) 的进程在网络中检测到重复地址，链路本地地址将无法配置。其他 IPv6 地址仍在接口上处于活动状态。</li><li>默认情况下，如果在网络中检测到重复的链路本地地址，DAD 将不会禁用 IPv6。要在检测到重复的链路本地地址时禁用接口上的 IPv6，请使用 <code>ipv6 nd dad disable-ipv6-on-failure</code> 命令。</li></ul> |

### 示例：禁用 DAD

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 nd dad disable
```

### 示例：在链路本地地址上启用 DAD

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 nd dad disable-ipv6-on-dad-failure
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 nd hop-limit

设置在 RA 消息中通告的跳限制，并将其包含在路由器发送的 IPv6 数据包中。

|               |                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ipv6 nd hop-limit hops</code>                                                                        |
| <b>参数</b>     | <ul style="list-style-type: none"><li><code>hop-limit hops</code> — 输入允许用于 RA 消息的最大跳数，从 0 到 255。</li></ul> |
| <b>默认</b>     | 64 跳                                                                                                       |
| <b>命令模式</b>   | INTERFACE                                                                                                  |
| <b>使用情况信息</b> | 已配置的跳限制将在 RA 消息中通告，并将其包含在路由器发送的 IPv6 数据包中。0 表示路由器未指定任何跳限制。                                                 |

## 示例

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd hop-limit 100
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 nd managed-config-flag

发送 RA 消息，通知主机使用状态地址自动配置（如 DHCPv6）来获取 IPv6 地址。

**语法** `ipv6 nd managed-config-flag`

**参数** 无

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息** 此命令的 `no` 版本将禁用 RA 消息中的 `managed-config-flag` 选项。

## 示例

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd managed-config-flag
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 nd max-ra-interval

设置发送 RA 消息之间的最长时间间隔。

**语法** `ipv6 nd max-ra-interval seconds`

**参数**

- `max-ra-interval seconds` — 输入时间间隔（以秒为单位），从 4 到 1800。

**默认** 600 秒

**命令模式** INTERFACE

**使用情况信息** 此命令的 `no` 版本将恢复用于发送 RA 消息的默认时间间隔。

## 示例

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd max-ra-interval 300
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 nd mtu

设置在 RA 消息的本地链路上使用的最大传输单元 (MTU)。

**语法** `ipv6 nd mtu number`

**参数**

- `mtu number` — 输入标头大小（以字节为单位），从 1280 到 65535。

**默认** 1500 字节

**命令模式** INTERFACE

**使用情况信息** 此命令的 `no` 版本将还原 RA 消息中通告的默认 MTU 值。

## 示例

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd mtu 2500
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 nd other-config-flag

发送 RA 消息，通知主机使用状态自动配置来获取与非地址相关的信息。

|        |                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------|
| 语法     | ipv6 nd other-config-flag                                                                           |
| 参数     | 无                                                                                                   |
| 默认     | 未配置                                                                                                 |
| 命令模式   | INTERFACE                                                                                           |
| 使用情况信息 | 此命令的 no 版本将禁用 RA 消息中的 other-config-flag 选项。                                                         |
| 示例     | <pre>OS10(config)# interface ethernet 1/2/3 OS10(conf-if-eth1/2/3)# ipv6 nd other-config-flag</pre> |
| 支持的版本  | 10.4.0E(R1) or later                                                                                |

## ipv6 nd prefix

将消息中包含的 IPv6 前缀配置为邻近 IPv6 路由器。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | ipv6 nd prefix { <i>ipv6-prefix</i>   default} [no-advertise] [no autoconfig] [no-rtr-address] [off-link] [lifetime { <i>valid-lifetime seconds</i>   infinite}] [ <i>preferred-lifetime seconds</i>   infinite]]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 参数     | <ul style="list-style-type: none"><li>• <i>ipv6-prefix</i> — 以 <i>x::y/mask</i> 格式输入 IPv6 前缀以包括 RA 消息中的前缀。包括在接口上的子网中尚未存在的前缀。</li><li>• <i>default</i> — 配置在接口上配置的所有子网中通告的前缀参数。</li><li>• <i>no-advertise</i> — (可选) 不通告指定的前缀。默认情况下，将通告已配置子网中的所有前缀。</li><li>• <i>no-autoconfig</i> — (可选) 针对 <i>radvd.conf</i> 文件中的指定前缀将 <i>AdvAutonomous</i> 设置为 Off。此设置会告诉主机不要使用此前缀进行地址自动配置。默认情况下，<i>AdvAutonomous</i> 为 On。</li><li>• <i>no-rtr-address</i> — (可选) 针对 <i>radvd.conf</i> 文件中的前缀将 <i>AdvRouterAddr</i> 设置为 Off。Off 设置告知主机不使用通告路由器地址进行链路上确定。默认情况下，<i>AdvRouterAddr</i> 为 On。</li><li>• <i>off-link</i> — (可选) 针对 <i>radvd.conf</i> 文件中的前缀将 <i>AdvOnLink</i> 设置为 Off。Off 设置告知主机不使用此前缀用于链路上确定。默认情况下，<i>AdvOnLink</i> 为 On。</li><li>• <i>lifetime {valid-lifetime seconds   infinite}</i> — (可选) 针对 <i>radvd.conf</i> 文件中的前缀设置 <i>AdvValidLifetime</i> (以秒为单位)。此前缀仅对指定生存期内的链路上确定有效。默认值为 86400 秒 (1 天)。infinite 设置允许前缀对无时间限制的链路上确定有效。</li><li>• <i>lifetime {preferred-lifetime seconds   infinite}</i> — (可选) 针对 <i>radvd.conf</i> 文件中的前缀设置 <i>AdvPreferredLifetime</i> (以秒为单位)。使用无状态自动配置从前缀生成的 IPv6 地址在配置的生命周期内保持首选。默认值为 14400 秒 (4 小时)。infinite 设置允许使用前缀进行自动配置的地址为首选地址，且无时间限制。</li></ul> |
| 默认     | 将通告在接口上的 IPv6 子网中配置的所有前缀。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 命令模式   | INTERFACE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 使用情况信息 | <ul style="list-style-type: none"><li>• 默认情况下，会通告在接口上的 IPv6 地址中配置的所有前缀。要在接口上的子网前缀中通告所有默认参数，请输入 <i>default</i> 关键字。</li><li>• 如果您使用有效或首选生存期值配置前缀，则 <i>ipv6 nd prefix default no autoconfig</i> 命令不会应用默认前缀值。</li><li>• 链路上确定用于将数据包 IPv6 转发到目标 IPv6 地址。</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 示例     | <p><b>启用路由器通告</b></p> <pre>OS10(conf-if-eth1/1/1)# ipv6 address 2001:0db8:2000::1/64 OS10(conf-if-eth1/1/1)# ipv6 nd send-ra</pre> <p><b>更改接口子网前缀的默认设置</b></p> <pre>OS10(conf-if-eth1/1/1)# ipv6 nd prefix default lifetime infinite infinite</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

### 禁用通告接口子网前缀

```
OS10(config-if-eth1/1/1)# ipv6 nd prefix 2001:0db8:2000::/64 no-advertise
```

### 通告没有接口地址的前缀

```
OS10(config-if-eth1/1/1)# ipv6 nd prefix 2001:0db8:3000::/64 no-autoconfig
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 nd ra-lifetime

设置 RA 消息中默认路由器的生存期。

**语法** `ipv6 nd ra-lifetime seconds`

**参数**

- `ra-lifetime seconds` — 输入生存期的值（以毫秒为单位），从 0 毫秒到 9000 毫秒。

**默认** `max-ra-interval` 值的三倍

**命令模式** INTERFACE

**使用情况信息** 此命令的 `no` 版本将还原默认的生存期值。0 表示此路由器未用作默认路由器。

**示例**

```
OS10(config)# interface ethernet 1/2/3
OS10(config-if-eth1/2/3)# ipv6 nd max-ra-interval 300
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 nd reachable-time

设置路由器在接收到可访问性确认后将其视为已有邻居的已通告时间。

**语法** `ipv6 nd reachable-time milliseconds`

**参数**

- `reachable-time milliseconds` — 输入可访问时间（以毫秒为单位），从 0 到 3600000。

**默认** 0

**命令模式** INTERFACE

**使用情况信息** 此命令的 `no` 版本将还原默认的可访问时间。0 表示在 RA 消息中未发送可访问的时间。

**示例**

```
OS10(config)# interface ethernet 1/2/3
OS10(config-if-eth1/2/3)# ipv6 nd reachable-time 1000
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 nd retrans-timer

设置重新传输邻居请求消息之间的时间。

**语法** `ipv6 nd retrans-timer seconds`

**参数**

- `retrans-timer seconds` — 输入重新传输时间间隔（以毫秒为单位），从 100 到 4292967295。

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息** 此命令的 `no` 版本将禁用已配置的重新传输计时器。

## 示例

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd retrans-timer 1000
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 nd send-ra

启用发送 ICMPv6 RA 消息。

**语法** `ipv6 nd send-ra`

**参数** 无

**默认** RA 消息已禁用。

**命令模式** INTERFACE

**使用情况信息**

- 使用 ICMPv6 RA 消息，邻居发现协议 (NDP) 将通告已启用 IPv6 的接口的 IPv6 地址，并了解 IPv6 邻居中的任何地址更改。在启用发送 RA 消息之前，交换机必须处于路由器模式，同时 IPv6 转发已启用并且无状态自动配置已禁用 `no ipv6 address autoconfig` 命令。
- `no` 版本命令将禁用 RA 消息。

## 示例

```
OS10(config)# interface ethernet 1/2/3
OS10(conf-if-eth1/2/3)# ipv6 nd send-ra
```

**支持的版本** 10.4.0E(R1) or later

## ipv6 route

配置静态 IPv6 静态路由。

**语法** `ipv6 route [vrf vrf-name] dest-ipv6-prefix mask {next-hop | interface interface-type [route-preference]}`

**参数**

- `vrf vrf-name` — (可选) 输入 vrf，然后输入要在该 VRF 中安装 IPv6 路由的 VRF 的名称。
- `dest-ipv6-prefix` — 以 `x:x:x:x::x` 格式输入目标 IPv6 地址。
- `mask` — 以斜杠前缀长度 `/x` 格式输入掩码。
- `next-hop` — 以 `x:x:x:x::x` 格式输入下一跳 IPv6 地址。
- `interface interface-type` — 输入接口类型，然后输入插槽/端口或编号信息。支持的接口类型为：以太网、端口信道、VLAN 和空。
- `route-preference` — (可选) 输入路由首选项范围，从 1 到 255。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 当接口出现故障时，系统将收回路由。当接口恢复正常运行时，路由将重新安装。当递归解析中断时，系统将收回路由。当满足递归解析时，路由将重新安装。在创建 IPv6 静态路由接口后，如果未向对等接口分配 IP 地址，则必须手动对等主机执行 ping 操作以解析邻居信息。

此命令的 `no` 版本将移除 IPv6 路由配置。

## 示例

```
OS10(config)# ipv6 route 2111:dddd:0eee::22/128 2001:db86:0fff::2
```

```
OS10(config)# ipv6 route 2111:dddd:0eee::22/128 interface null 0
```

**支持的版本** 10.2.0E or later



ipv6 unreachableables

允许在接口上生成错误消息，以用于具有无法访问的目标的 IPv6 数据包。

|        |                                                                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | ipv6 unreachableables                                                                                                                                                                              |
| 参数     | 无                                                                                                                                                                                                  |
| 默认     | 不发送 ICMPv6 不可访问的消息。                                                                                                                                                                                |
| 命令模式   | INTERFACE                                                                                                                                                                                          |
| 使用情况信息 | <ul style="list-style-type: none"><li>默认情况下，在 IPv6 路由表中找不到 IPv6 路由的匹配条目时，数据包将丢弃，并且不会发送错误消息。使用此命令可以启用将 IPv6 destination unreachable 错误消息发送至源而不丢弃数据包的功能。</li><li>此命令的 no 版本将禁止生成不可访问的目标消息。</li></ul> |
| 示例     | <pre>OS10(config)# interface ethernet 1/2/3 OS10(conf-if-eth1/2/3)# ipv6 unreachableables</pre>                                                                                                    |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                               |

show ipv6 neighbors

显示 IPv6 查找信息。输入不带选项的命令将显示存储在控制处理器 (CP) 上的所有 IPv6 邻居地址。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show ipv6 neighbors [vrf vrf-name] [ipv6-address  interface interface]                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 参数     | <ul style="list-style-type: none"><li>vrf vrf-name — (可选) 输入 vrf 和 VRF 的名称，以显示与该 VRF 对应的邻居。如果未指定此选项，则将显示与默认 VRF 相对应的邻居。</li><li>ipv6-address — 以 x:x:x:x:x 格式输入邻居的 IPv6 地址。:: 表示法指定零的连续十六进制字段。</li><li>interface interface — 输入 interface 接口类型和插槽/端口或编号信息：<ul style="list-style-type: none"><li>对于 10 Gb 以太网接口，输入 TenGigabitEthernet，然后输入插槽/端口/子端口[/子端口]信息。</li><li>对于 40 Gb 以太网接口，输入 fortyGigE，然后输入插槽/端口信息。</li><li>对于端口通道接口，输入 port-channel，然后输入数字。</li><li>对于 VLAN 接口，输入 vlan，然后输入 1 到 4093 之间的某个数字。</li></ul></li></ul> |
| 默认     | 无。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 使用情况信息 | 此命令的 no 版本会将该值重置为默认值。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 示例     | <pre>OS10# show ipv6 neighbors IPv6 Address      Hardware Address  State  Interface      VLAN ----- 1001:db8:a1::2    00:c5:05:02:12:91 REACH  ethernet1/1/5   12 1001:db8:a1::f    00:f5:50:02:54:75 REACH  port-channel15  12 200::2            00:c5:05:02:12:91 STALE  ethernet1/1/10 400::f            00:f5:50:02:54:75 REACH  port-channel20</pre>                                                                                                                                                                   |
| 支持的版本  | 10.4.1.0 or later 或更高版本                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

show ipv6 route

显示 IPv6 路由。

|    |                                                                                                                                         |
|----|-----------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | show ipv6 route [vrf vrf-name] [all   bgp   connected   static   A::B/mask   summary]                                                   |
| 参数 | <ul style="list-style-type: none"><li>vrf vrf-name — (可选) 输入 vrf 和 VRF 的名称，以显示与该 VRF 对应的 IPv6 路由。如果不指定此选项，则将显示与默认 VRF 相对应的路由。</li></ul> |

- all — (可选) 显示包括非活动路由的所有路由。
- bgp — (可选) 显示 BGP 路由信息。
- connected — (可选) 仅显示直接连接的路由。
- static — (可选) 显示所有静态路由。
- A::B/mask — (可选) 输入 IPv6 目标地址和掩码。  
 **注:** 此选项仅适用于准确的前缀和掩码长度。
- summary — (可选) 显示 IPv6 路由摘要。

**默认** 未配置  
**命令模式** EXEC  
**使用情况信息** 无  
**示例 (所有)**

```
OS10# show ipv6 route all
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
 Destination Gateway Dist/Metric Last Change

```

**示例 (已连接)**

```
OS10# show ipv6 route connected
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, > - non-active route
Gateway of last resort is not set
 Destination Gateway Dist/Metric Last Change

C 2001:db86::/32 via 2001:db86:fff::1 ethernet1/1/1 0/0 00:03:24
```

**示例 (摘要)**

```
OS10# show ipv6 route summary
Route Source Active Routes Non-Active Routes
Ospf 0 0
Bgp 0 0
Connected 0 0
Static 0 0
Ospf Inter-area 0 0
NSSA External-1 0 0
NSSA External-2 0 0
Ospf External-1 0 0
Ospf External-2 0 0
Bgp Internal 0 0
Bgp External 0 0
Ospf Intra-area 0 0
Total 0 0
```

**支持的版本** 10.2.0E or later

**show ipv6 interface brief**

显示 IPv6 接口信息。

**语法** show ipv6 interface brief  
**参数** brief — 显示 IPv6 接口信息的简要摘要。  
**默认** 无

命令模式

EXEC

使用情况信息

使用 do show ipv6 interface brief 命令可以其他模式查看 IPv6 接口信息。

示例（简要）

```
OS10# show ipv6 interface brief
```

| Interface Name    | admin/protocol | IPv6 Address/Link-Local Address  | IPv6 Oper Status |
|-------------------|----------------|----------------------------------|------------------|
| Management Vlan 1 | 1/1/1 up/up    | fe80::20c:29ff:fe54:c852/64      | Enabled          |
| Ethernet 1/1/2    | up/up          | fe80::20c:29ff:fe54:c853/64      | Enabled          |
| Ethernet 1/1/3    | up/up          | 1001:1:1:1:20c:29ff:fe54:c853/64 | Enabled          |
| Ethernet 1/1/4    | up/up          | fe80::4/64                       | Disabled         |
|                   |                | 3000::1/64                       |                  |
|                   |                | 4000::1/64                       |                  |
|                   |                | fe80::4/64                       | Enabled          |
|                   |                | 4::1/64                          |                  |
|                   |                | 5::1/64                          |                  |

支持的版本

10.2.0E or later 或更高版本

## 首先打开最短路径

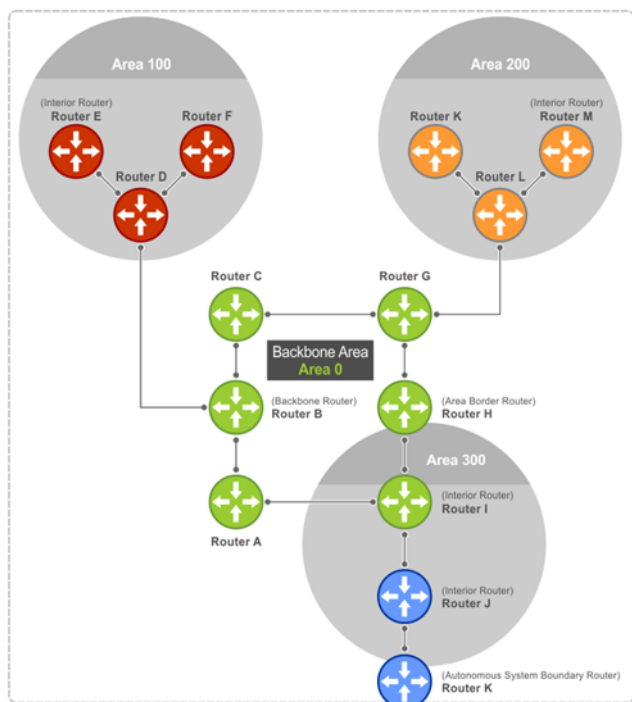
OSPF 路由是一种链路状态路由协议，允许向同一自治系统 (AS) 区域内的所有其他路由器发送链路状态通告 (LSA)。OSPF LSA 包括有关连接的接口、所使用的指标和其他属性的信息。OSPF 路由器会累积链路状态信息，并使用最短路径优先 (SPF) 算法来计算每个节点的最短路径。

## 自治系统区域

OSPF 在层次结构中运行。层级中的最大实体是自治系统 (AS)。AS 是共享通用路由策略的通用管理下的网络集合。OSPF 是一种内部网关间路由协议 (IGRP)，用于接收来自 AS 的路由并将路由发送到另一个 AS。

您可以划分为多个区域，它们是以管理方式分组的连续网络和连接主机组。具有多个接口的路由器可以加入多个区域。这些路由器称为区域边界路由器 (ABR)，为每个区域维护单独的数据库。区域是 OSPF 路由器的逻辑分组，可通过整数或点分十进制数字标识。

通过区域，您可以进一步阻止 AS 中的一个或多个区域中的路由器。区域允许子网络隐藏在 AS 中 — 最大限度地减少所有路由器上的路由表的大小。AS 中的某个区域可能无法查看另一个区域拓扑的详细信息。区域编号或路由器的 IP 地址可标识 AS 区域。



## 区域、网络和邻居

网络主干网为区域 0，也称为区域 0.0.0.0，是任何 AS 的核心。所有其他区域必须连接到区域 0。OSPF 主干在各区域之间分布路由信息。它包含所有区域边界路由器和网络，而不是全部包含在任何区域及其连接的路由器中。

主干是唯一具有默认区域编号的区域。您可以配置所有其他区域的区域 ID。如果配置两个非主干区域，则必须在 OSPF 中启用 B 位。路由器、A、B、C、G、H 和 I 是主干，请参阅[自治系统区域](#)。

- 除默认路由外，存根区域 (SA) 不会接收外部路由信息。这些区域会从区间 (IA) 路由接收信息。
- 次末端区域 (NSSA) 可以导入 AS 外部路由信息，并将其作为类型-7 LSA 发送至主干。
- 完全端化区域也称为“无摘要”区域。

将分配的存根区域内的所有路由器配置为端化，不生成不适用的 LSA。例如，类型 5 LSA 用于外部区域，端化区域路由器可能不会生成外部 LSA。虚拟链路无法遍历端化区域。

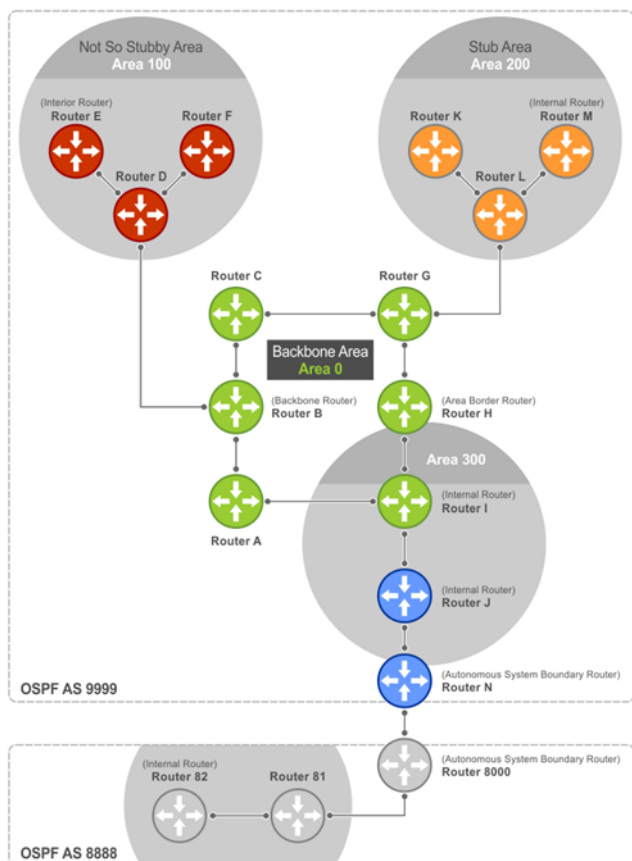
### 网络和邻居

作为一种链路状态协议，OSPF 会将路由信息发送至与其他 OSPF 路由器有关的链路的状态。这些链路的向上或向下状态非常重要。共享链接的路由器将成为该网段上的邻居。OSPF 使用该 hello 协议作为邻居查找和 keepalive 机制。两个路由器是邻居后，它们可能会继续进行交换并同步其数据库，从而形成邻接。

## 路由器类型

路由器类型是 OSPF 进程的属性 — 多个 OSPF 进程可能在一台路由器上运行。连接到多个区域的路由器（从连接到另一个的 BGP 进程接收路由）同时充当区域边界路由器和自治系统边界路由器。

每个路由器都有一个以十进制 A.B.C.D 格式写入的唯一 ID。您不必将路由器 ID 与有效的 IP 地址相关联。要更轻松地进行故障处理，请确保路由器 ID 与路由器的 IP 地址相同。



### 主干路由器

主干路由器 (BR) 是 OSPF 主干的一部分，区域 0，并且包含所有 ABR。BR 包含仅连接到主干的路由器和另一个 ABR，但仅属于区域 0 的一部分 — 如示例中的路由器 I 所示。

### 区域边界路由器

在 AS 中，区域边界路由器 (ABR) 将一个或多个区域连接到主干。ABR 会为连接到的每个区域保留链路状态数据库的副本。它可能会保留链路状态数据库的多个副本。ABR 在将信息发送到其他连接的区域之前，会从其某个连接区域中汇总获知的信息。ABR 可以连接到 AS 中的多个区域，并被视为它所连接的每个区域的成员 — 如示例中的路由器 H 所示。

### 自治系统边界路由器

自治系统边界路由器 (ASBR) 连接到多个 AS，并与其他 AS 中的路由器交换信息。ASBR 连接到一个非 IGP，例如 BGP 或使用静态路由 — 如示例中的路由器 N 所示。

### 内部路由器

内部路由器 (IR) 只具有与同一区域中的路由器的邻区 — 如示例中的路由器 E、F、I、K 和 M 所示。

## 指定和备份指定的路由器

OSPF 将会显示指定的路由器 (DR) 和备份指定的路由器 (BDR)。DR 将为整个多接入网络生成 LSA。指定的路由器将允许减少网络流量和拓扑数据库的大小。

### 指定的路由器

维护网络的完整拓扑表，并通过多播将更新发送到其他路由器。某个区域中的所有路由器均形成与灾难恢复的从属/主关系。每次路由器发送更新时，路由器都会将其发送到 DR 和 BDR。灾难恢复将更新发送到该区域中的所有其他路由器。

### 备份指定的路由器

灾难恢复失败时将接管的路由器。

每个路由器与 DR 和 BDR 交换信息。DR 和 BDR 将信息转发给其他路由器。在广播网络分段中，OSPF 数据包的数量将通过以下方式减少：DR 将 OSPF 更新发送到网络段上所有 OSPF 路由器都在侦听的多播 IP 地址。

DR 和 BDR 是可配置的。如果未定义 DR 或 BDR，OS10 将根据协议为其分配。要确定哪些路由器是 DR 和 BDR，OSPF 将查看该分段上路由器的优先级。默认路由器优先级为 1。具有最高优先级的路由器将选择灾难恢复。如果存在关联，则路由器 ID 较高的路由器优先。选择灾难恢复后，BDR 的选择方式相同。路由器优先级设置为零的路由器不能成为 DR 或 BDR。

# 链路状态通告

链路状态通告 (LSA) 会将路由器的路由拓扑传递至网络中的所有其他路由器。

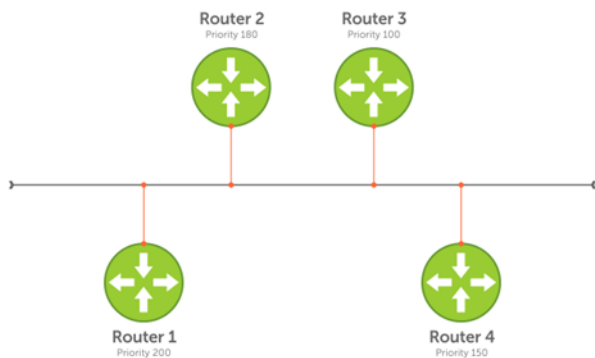
|                                                           |                                                                                                                            |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>类型 1 — 路由器 LSA</b>                                     | 路由器列出了位于同一区域中的其他路由器或网络的链路。类型 1 LSA 仅在各自的区域内泛洪。类型 1 LSA 的链路状态 ID 为原始路由器 ID。                                                 |
| <b>类型 2 — 网络 LSA</b>                                      | 某个区域中的 DR 会列出在该区域中加入的路由器。类型 2 LSA 仅在各自的区域内泛洪。类型 2 LSA 的链路状态 ID 是 DR 的 IP 接口地址。                                             |
| <b>类型 3 — 摘要 LSA (OSPFv2)、区域间前缀 LSA (OSPFv3)</b>          | ABR 将在其中一个连接的区域上获取信息并对其进行汇总，然后将其发送到它所连接的其他区域。类型 3 LSA 的链路状态 ID 是目标网络的 IP 地址。                                               |
| <b>类型 4 — AS 边界路由器摘要 LSA (OSPFv2)、区域内路由器 LSA (OSPFv3)</b> | 在某些情况下，类型 5 外部 LSA 泛洪到下一跳信息可能不可用的区域，因为可能使用不同的路由协议。ABR 会让路由器的信息泛洪，类型 5 生成的 ASBR。类型 4 LSA 的链路状态 ID 是所述的 ASBR 的路由器 ID。        |
| <b>类型 5 — AS 外部 LSA</b>                                   | LSA 包含从其他路由进程导入 OSPF 的信息。类型 5 LSA 泛洪将到达除存根区域以外的所有区域。类型 5 LSA 的链路状态 ID 为外部网络编号。                                             |
| <b>类型 7 — NSSA 外部 LSA (OSPFv2)、LSA (OSPFv3)</b>           | NSSA 中的路由器不会接收来自 ABR 的外部 LSA，但会发送外部路由信息进行重新分发。它们使用类型 7 LSA 告诉 ABR 有关这些外部路由的信息，其中 ABR 随后会转换为类型 5 外部 LSA，并正常泛洪到 OSPF 网络其余部分。 |
| <b>类型 8 — 链路 LSA (OSPFv3)</b>                             | 类型 8 LSA 将携带本地链路的 IPv6 地址信息。                                                                                               |
| <b>类型 9 — 链路本地不透明 LSA (OSPFv2)、区域内前缀 LSA (OSPFv3)</b>     | RFC2370 for OSPFv2 定义的链路本地不透明 LSA。区域内前缀 LSA 带有路由器的 IPv6 前缀和 OSPFv3 的网络链路。                                                  |
| <b>类型 11 — 正常 LSA (OSPFv3)</b>                            | 仅在 OSPFv3 路由器正常重新启动期间发送 OSPFv3 的链路本地不透明 LSA。                                                                               |

LSA 标头对于 LSA 类型是通用的。其大小为 20 个字节。LSA 标头的其中一个字段是链路状态 ID。每个路由器链接均定义为四种类型之一 — 类型 1、2、3 或 4。LSA 包括一个链路 ID 字段，该字段通过网络编号和掩码标识此链路连接到的对象。根据类型，链路 ID 具有不同的含义。

- |   |                     |
|---|---------------------|
| 1 | 到另一个路由器或相邻路由器的点对点连接 |
| 2 | 与灾难恢复的传输网络 IP 地址的连接 |
| 3 | 与存根网络 IP 网络或子网号的连接  |
| 4 | 虚拟链路邻接路由器 ID        |

# 路由器优先级

路由器优先级决定了网络指定的路由器。默认路由器优先级为 1。当两个路由器连接到网络时，都将尝试成为 DR。路由器优先级较高的路由器优先。如果存在关联，则路由器 ID 较高的路由器优先。路由器优先级设置为零的路由器不能成为 DR 或 BDR。如果未分配，系统将选择优先级最高的路由器作为 DR。优先级第二高的是 BDR。优先级等级从 0 到 255，255 为最高优先级。



Router 1 selected by the system as DR.  
Router 2 selected by the system as BDR.

If R1 fails, the BDR router becomes the DR. The new BDR election occurs according to router priority.

R4 becomes the BDR.

## OSPF 路由限制

OS10 支持最多 16000 个 OSPF 路由。在此范围内，唯一限制是针对仅可扩展至 1000 个路由的区域内的路由。其他 OSPF 路由可以扩展到最多 16 K。

## 最短路径优先限制

使用最短路径优先 (SPF) 限制在网络不稳定期间延迟 SPF 计算。在 OSPF 网络中，拓扑更改事件会在开始时间后触发 SPF 计算。当开始计时器完成时，保留时间可能会延迟另一次 SPF 计算。

当挂起计时器正在运行时：

- 每次发生拓扑更改时，SPF 计算会延迟两倍配置的保留时间，最多可达最长等待时间。
- 如果未发生任何拓扑更改，将执行 SPF 计算，并且保留计时器将重置为其配置的值。

根据 OSPF 网络拓扑的稳定性，设置启动、保留和等待计时器。输入值（以毫秒为单位）。如果未指定开始时间、保存时间或最大等待值，则将使用默认值。

OSPFv2 和 OSPFv3 实例支持 SPF 限制。默认情况下，OSPF 实例中的 SPF 计时器已禁用。输入此命令的 `no` 版本已移除配置的 SPF 计时器，并禁用 SPF 限制。

1. 从 CONFIGURATION 模式配置 OSPF 实例，从 1 到 65535。

```
router {ospf | ospfv3} instance-number
```

2. 在 OSPF INSTANCE 模式下设置 OSPF 限制计时器。

```
timers spf [start-time [hold-time [max-wait]]]
```

- `start-time` — 在拓扑更改后执行 SPF 计算之前配置初始延迟，从 1 到 600000 毫秒；默认值未 1000。
- `hold-time` — 当更改新拓扑时在执行 SPF 计算之前配置额外的延迟，从 1 到 600000 毫秒；默认值为 10000。
- `max-wait` — 配置可延迟 SPF 计算的最大保留时间，从 1 到 600000 毫秒；默认值为 10000。

### 启用 SPF 限制 (OSPFv2)

```
OS10(config)# router ospf 100
OS10(config-router-ospf-100)# timers spf 1200 2300 3400
```

### 启用 SPF 限制 (OSPFv3)

```
OS10(config)# router ospfv3 10
OS10(config-router-ospf-10)# timers spf 2000 3000 4000
```

### 查看 OSPFv2 SPF 限制

```
OS10(config-router-ospf-100)# do show ip ospf
Routing Process ospf 100 with ID 12.1.1.1
```



```
Supports only single TOS (TOS0) routes
It is Flooding according to RFC 2328
SPF schedule delay 1200 msecs, Hold time between two SPFs 2300 msecs
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
Area (0.0.0.1)
Number of interface in this area is 1
SPF algorithm executed 1 times
```

## 查看 OSPFv3 SPF 限制

```
OS10(config-router-ospfv3-100)# timers spf 1345 2324 9234

OS10(config-router-ospfv3-100)# do show ipv6 ospf
Routing Process ospfv3 100 with ID 129.240.244.107
SPF schedule delay 1345 msecs, Hold time between two SPFs 2324 msecs
Min LSA origination 5000 msec, Min LSA arrival 1000 msec
Min LSA hold time 0 msec, Max LSA wait time 0 msec
Number of area in this router is 1, normal 1 stub 0 nssa
Area (0.0.0.1)
Number of interface in this area is 1
SPF algorithm executed 2 times
```

## OSPFv2

OSPFv2 支持 IPv4 地址系列。OSPFv2 路由器最初交换 hello 消息以设置邻居路由器的邻区。此 hello 过程将在 AS 的路由器之间建立邻接。AS 区域中的每个路由器都不需要建立邻接。如果同一子网上的两个路由器在此过程中同意成为邻居，则它们会以 LSA 的形式开始交换网络拓扑信息。

在 OSPFv2 中，广播上的邻居和非广播多访问 (NBMA) 网络链路通过其接口地址进行标识，而其他类型的链路上的邻居通过路由器标识符 (RID) 来标识。

## 启用 OSPFv2

默认情况下，OSPFv2 处于禁用状态。将至少一个接口配置为物理或环回，并为接口分配 IP 地址。您可以为除区域 0 以外的任何区域分配编号 ID。OSPFv2 进程在全局配置时自动启动，您可以为一个或多个接口启用它。

1. 在 CONFIGURATION 模式下全局启用 OSPF 并配置 OSPF 实例。

```
router ospf instance-number
```

2. 输入接口信息以在 INTERFACE 模式下配置 OSPF 接口。

```
interface ethernet node/slot/port[:subport]
```

3. 在 INTERFACE 模式下启用接口。

```
no shutdown
```

4. 禁用默认的交换机端口配置，并将其从接口或 INTERFACE 模式中的 LAG 端口移除。

```
no switchport
```

5. 在 INTERFACE 模式下将一个 IP 地址分配给接口。

```
ip address ip-address/mask
```

6. 在 INTERFACE 模式下启用接口上的 OSPFv2。

```
ip ospf process-id area area-id
```

- *process-id*— 输入特定 OSPF 进程的 OSPFv2 进程 ID，从 1 到 65535。
- *area-id*— 输入 OSPFv2 区域 ID 作为 IP 地址 (A.B.C.D) 或数字 (从 1 到 65535)。



## 启用 OSPFv2 配置

```
OS10(config)# router ospf 100
OS10(conf-router-ospf-100)# exit
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# ip address 11.1.1.1/24
OS10(conf-if-eth1/1/1)# ip ospf 100 area 0.0.0.0
```

## 查看 OSPFv2 配置

```
OS10# show running-configuration ospf
!
interface ethernet1/1/1
 ip ospf 100 area 0.0.0.0
!
router ospf 100
...
```

## 在非默认 VRF 实例中启用 OSPFv2

要在非默认 VRF 实例中启用 OSPFv2，请执行以下操作：

1. 创建要在其中启用 OSPFv2 的非默认 VRF 实例：

```
ip vrf vrf-name
```

2. 启用 OSPF 并在 VRF CONFIGURATION 模式下配置 OSPF 实例。

```
router ospf instance-number vrf vrf-name
```

3. 输入接口信息以在 INTERFACE 模式下配置 OSPF 接口。

```
interface ethernet node/slot/port[:subport]
```

4. 在 INTERFACE 模式下启用接口。

```
no shutdown
```

5. 禁用默认的交换机端口配置，并将其从接口或 INTERFACE 模式中的 LAG 端口移除。

```
no switchport
```

6. 将接口与您之前创建的非默认 VRF 实例关联。

```
ip vrf forwarding vrf-name
```

7. 将一个 IP 地址分配给接口。

```
ip address ip-address/mask
```

8. 在接口上启用 OSPFv2。

```
ip ospf process-id area area-id
```

- *process-id*— 输入特定 OSPF 进程的 OSPFv2 进程 ID，从 1 到 65535。
- *area-id*— 输入 OSPFv2 区域 ID 作为 IP 地址 (A.B.C.D) 或数字 (从 1 到 65535)。

## 启用 OSPFv2 配置

```
OS10(config)# ip vrf vrf-blue
OS10(config-vrf-blue)# router ospf 100 vrf-blue
OS10(conf-router-ospf-100)# exit
OS10(config)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# ip vrf forwarding vrf-blue
```

```
OS10(config-if-eth1/1/1)# ip address 11.1.1.1/24
OS10(config-if-eth1/1/1)# ip ospf 100 area 0.0.0.0
```

#### 注:

如果您想要将与一个 VRF 实例相关联的接口移至另一个默认或非默认 VRF 实例，则必须先删除该接口上已经存在的 OSPF 或 Layer3 配置。如果将接口从一个 VRF 实例移至另一个实例，而不删除这些现有的 Layer3 或 OSPF 配置，则这些配置不会在新的 VRF 实例中生效。

请考虑在默认 VRF 实例上配置了 OSPF 实例 100 的情况，并在名为 VRF-Red 的非默认 VRF 实例上配置 OSPF 实例 200。默认 VRF 实例上的接口 eth1/1/1 连接到 OSPF 进程 100 区域 1。在这种情况下，如果您想要将 eth1/1/1 从默认 VRF 实例移至 VRF-Red，则必须先移除接口 eth1/1/1 当前连接到的 OSPF 区域配置。

## 分配路由器标识符

为了进行管理和故障处理，您可以为 OSPFv2 进程分配路由器 ID。使用路由器的 IP 地址作为路由器 ID。

- 在 ROUTER-OSPF Mode 模式下为 OSPFv2 进程分配路由器 ID

```
router-id ip-address
```

### 分配路由器 ID

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# router-id 10.10.1.5
```

### 查看 OSPFv2 状态

```
OS10# show ip ospf 10
Routing Process ospf 10 with ID 10.10.1.5
Supports only single TOS (TOS0) routes
It is an Autonomous System Boundary Router
It is Flooding according to RFC 2328
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
Area (0.0.0.0)
 Number of interface in this area is 3
 SPF algorithm executed 38 times
 Area ranges are
```

## 存根区域

类型 5 LSA 不会泛洪至存根区域。ABR 将默认路由通告到它所连接的存根区域。存根区域路由器使用默认路由到达外部目标。

1. 启用 OSPF 路由并进入 ROUTER-OSPF 模式，从 1 到 65535。

```
router ospf instance number
```

2. 在 ROUTER-OSPF 模式下将区域配置为存根区域。

```
area area-id stub [no-summary]
```

- *area-id*— 将 OSPF 区域 ID 输入为 A.B.C.D 格式或数字（从 1 到 65535）的 IP 地址。
- *no-summary* —（可选）输入以防止 ABR 将摘要 LSA 发送至存根区域。

### 配置存根区域

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# area 10.10.5.1 stub
```

## 查看存根区域配置

```
OS10# show ip ospf
Routing Process ospf 10 with ID 130.6.196.14
Supports only single TOS (TOS0) routes
It is Flooding according to RFC 2328
SPF schedule delay 1000 msecs, Hold time between two SPFs 10000 msecs
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 0 stub 1 nssa 0
 Area (10.10.5.1)
 Number of interface in this area is 0
 SPF algorithm executed 1 times
 Area ranges are
```

```
OS10# show running-configuration ospf
!
router ospf 10
 area 10.10.5.1 stub
```

## 被动接口

被动接口不发送或接收路由信息。将接口配置为被动接口可禁止接收和发送路由更新。

虽然被动接口不会发送或接收路由更新，但该接口上的网络包含在通过其他接口发送的 OSPF 更新中。

1. 在 INTERFACE 模式下输入接口类型。

```
interface ethernet node/slot/port[:subport]
```

2. 在 INTERFACE 模式下将接口配置为被动接口。

```
ip ospf passive
```

### 配置被动接口

```
OS10(config)# interface ethernet 1/1/6
OS10(conf-if-eth1/1/6)# ip ospf passive
```

### 查看被动接口

```
OS10# show running-configuration
!!!
!!
interface ethernet1/1/6
 ip address 10.10.10.1/24
 no switchport
 no shutdown
 ip ospf 100 area 0.0.0.0
 ip ospf passive
!!
!
```

您可以使用 `no ip ospf passive` 命令禁用被动接口。

## 快速聚合

快速聚合将最小源和到达 LSA 参数设置为零 (0)，从而允许快速路由计算。较高的聚合级别可能会导致 OSPF 邻接造成偶尔丢失。

聚合级别 1 符合大多数聚合的要求。数字越高，聚合的速度越快，路由计算和更新的频率越高。这会影响 CPU 利用率，并且可能会影响较大的拓扑中的邻接稳定性。

 **注：** 仅在使用 Dell EMC 技术支持进行检查后选择更高的聚合级别。

如果禁用快速聚合，则 LSA 参数会分别设置为 0 毫秒和 1000 毫秒。将聚合参数从 1 设置为 4 表示实际聚合级别。每个会合设置都将 LSA 参数调整为零，但 `convergence-level` 参数会更改集中速度。数字越高，聚合越快。

- 在 ROUTER-OSPF 模式下启用 OSPFv2 快速聚合并输入聚合级别，从 1 到 4。

```
fast-converge convergence-level
```

## 配置快速聚合

```
OS10(config)# router ospf 65535
OS10(conf-router-ospf-65535)# fast-converge 1
```

## 查看快速聚合

```
OS10(conf-router-ospf-65535)# do show ip ospf

Routing Process ospf 65535 with ID 99.99.99.99
Supports only single TOS (TOS0) routes
It is an Autonomous System Border Router
It is an Area Border Router
It is Flooding according to RFC 2328
Convergence Level 1
Min LSA origination 0 msec, Min LSA arrival 0 msec
Min LSA hold time 0 msec, Max LSA wait time 0 msec
Number of area in this router is 3, normal 1 stub 1 nssa 1
 Area BACKBONE (0)
 Number of interface in this area is 1
 SPF algorithm executed 28 times
 Area ranges are

 Area (2)
 Number of interface in this area is 1
 SPF algorithm executed 28 times
 Area ranges are

 Area (3)
 Number of interface in this area is 1
 SPF algorithm executed 28 times
 Area ranges are
```

## 禁用快速聚合

```
OS10(conf-router-ospf-65535)# no fast-converge
```

## 接口参数

为避免出现路由错误，所有接口上的接口参数值必须一致。例如，为 OSPF 网络中所有路由器上的问候数据包设置相同的时间间隔，以防止 OSPF 邻居配置错误。

- 要在 CONFIGURATION 模式下更改 OSPFv2 参数，请输入接口。

```
interface interface-name
```

- 在 INTERFACE 模式下，更改与 OSPF 流量相关联的成本，从 1 到 65535。默认值取决于接口速度。

```
ip ospf cost
```

- 更改在 INTERFACE 模式下声明邻居失效之前路由器等待的时间间隔，从 1 到 65535。默认时间间隔为 40。失效间隔必须为问候间隔的四倍，并且在 OSPF 网络中的所有路由器上必须相同。

```
ip ospf dead-interval seconds
```

- 在 INTERFACE 模式下，更改问候数据包传输之间的时间间隔，从 1 到 65535。默认时间间隔为 10。OSPF 网络中所有路由器上的问候时间间隔必须相同。

```
ip ospf hello-interval seconds
```

5. 在 INTERFACE 模式下更改接口的优先级，以确定 OSPF 广播网络的 DR，从 0 到 255。所有接口的默认优先级为 1。

```
ip ospf priority number
```

6. 在 INTERFACE 模式下，更改 LSA 之间的重新传输间隔时间（以秒为单位），从 1 到 3600。默认的重新传输间隔时间为 5。在 OSPF 网络中的所有路由器上，重新传输时间间隔必须相同。

```
ip ospf retransmit-interval seconds
```

7. 更改 INTERFACE 模式下发送到接口的链路状态更新数据包之间的等待时间，从 1 到 3600。默认等待时间为 1。OSPF 网络中的所有路由器上的传输延迟必须相同。

```
ip ospf transmit-delay seconds
```

### 更改参数和查看接口状态

```
OS10(conf-if-eth1/1/1)# ip ospf hello-interval 5
OS10(conf-if-eth1/1/1)# ip ospf dead-interval 20
OS10(conf-if-eth1/1/1)# ip ospf retransmit-interval 30
OS10(conf-if-eth1/1/1)# ip ospf transmit-delay 200
```

### 查看 OSPF 接口配置

```
OS10(conf-if-eth1/1/1)# do show ip ospf interface

ethernet1/1/1 is up, line protocol is up
Internet Address 11.1.1.1/24, Area 0.0.0.0
Process ID 65535, Router ID 99.99.99.99, Network Type broadcast, Cost: 1
Transmit Delay is 200 sec, State BDR, Priority 1
Designated Router (ID) 150.1.1.1, Interface address 11.1.1.2
Backup Designated router (ID) 99.99.99.99, Interface address 11.1.1.1
Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 30
Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 150.1.1.1(Designated Router)
```

## 重新分发路由

将其他路由实例或协议的路由添加到 OSPFv2 进程，并在 OSPFv2 进程中包含 BGP、静态或连接的路由。除非存在与 OSPFv2 重新分发关联的路由映射，否则请勿将 IBGP 路由来路由到 OSPFv2。

 **注：**在正在运行的配置中重新分发静态命令时，如果配置了静态路由（也通过 OSPF 进行了学习），即使静态路由由首选项高于 OSPF，路由表中也会安装静态路由。

- 在 ROUTER-OSPF 模式下输入将分配到 OSPFv2 进程的路由。

```
redistribute {bgp as-number| connected | static} [route-map map-name]
```

- o bgp | connected | static — 输入关键字以重新分发这些路由。
- o route-map map-name — 输入已配置的路由映射的名称。

### 配置重新分发路由

```
OS10(conf-router-ospf-10)# redistribute bgp 4 route-map aloha
OS10(conf-router-ospf-10)# redistribute connected route-map aloha
OS10(conf-router-ospf-10)# redistribute static route-map aloha
```

### 查看 OSPF 配置

```
OS10(conf-router-ospf-10)# do show running-configuration ospf
!
router ospf 10
 redistribute bgp 4 route-map aloha
 redistribute connected route-map aloha
 redistribute static route-map aloha
!
```

## 默认路由

您可以生成外部默认路由并将默认信息分发至 OSPFv2 路由域。

- 在 ROUTER-OSPF 模式下使用 `default-information originate [always]` 命令生成默认路由。

### 配置默认路由

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# default-information originate always
```

### 查看默认路由配置

```
OS10(config-router-ospf-10)# show configuration
!
router ospf 10
 default-information originate always
```

## 摘要地址

您可以为 ASBR 配置一个摘要地址，以通告作为指定地址范围涵盖的所有重新分发路由的聚合的一个外部路由。

- 在 ROUTER-OSPF 模式下配置摘要地址。  
`summary-address ip-address/mask [not-advertise | tag tag-value]`

### 配置摘要地址

```
OS10(config)# router ospf 100
OS10(config-router-ospf-100)# summary-address 10.0.0.0/8 not-advertise
```

### 查看摘要地址

```
OS10(config-router-ospf-100)# show configuration
!
router ospf 100
 summary-address 10.0.0.0/8 not-advertise
```

## 正常重新启动

当网络设备重新启动时，相邻的邻居和对等节点会检测到该情况。在正常重新启动期间，重新启动设备和邻居将继续转发数据包，而不会中断网络性能。在重新启动过程中帮助的邻居称为帮助器路由器。

启用正常重新启动后，重新启动设备将在转发表中保留 OSPF 学习的路由。要重新建立与邻居的 OSPF 邻区，重新启动 OSPF 进程会将宽限期 LSA 发送给所有邻居。在响应中，帮助器路由器进入帮助程序模式，并将确认发送回重新启动设备。

OS10 支持正常重启帮助程序模式。使用 `graceful-restart role helper-only` 命令在 ROUTER OSPF 模式下启用帮助程序模式。

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# graceful-restart role helper-only
```

使用该命令的 `no` 版本可禁用帮助程序模式。

## OSPFv2 身份验证

您可以通过明文或 MD5 启用 OSPF 身份验证。

- 在 INTERFACE 模式下，在接口上设置明文身份验证方案。  
`ip ospf authentication-key key`
- 在 INTERFACE 模式下设置 MD5 身份验证。  
`ip ospf message-digest-key keyid md5 key`

## 配置文本身份验证

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip ospf authentication-key sample
```

## 查看文本身份验证

```
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
 ip address 10.10.10.2/24
 no switchport
 no shutdown
 ip ospf 100 area 0.0.0.0
 ip ospf authentication-key sample
```

## 配置 MD5 身份验证

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip ospf message-digest-key 2 md5 sample12345
```

## 查看 MD5 身份验证

```
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
 ip address 10.10.10.2/24
 no switchport
 no shutdown
 ip ospf 100 area 0.0.0.0
 ip ospf message-digest-key 2 md5 sample12345
```

# OSPFv2 故障处理

您可以对 OSPFv2 操作进行故障处理，并查看有关中断进程的典型问题。

- OSPF 是否已全局启用？
- 在接口上是否已启用 OSPF？
- 是否正确建立了邻区？
- 是否已针对 L3 正确配置了接口？
- 路由器是否是正确的区域类型？
- OSPF 数据库中是否包括 OSPF 路由？
- 除了 OSPF 数据库外，路由表中是否还包括 OSPF 路由？
- 是否可以对相邻路由器接口的 IPv4 地址执行 ping 命令？

## 使用 show 命令对 OSPF 进行故障处理

- 查看在 EXEC 模式下已启用的所有 OSPF 进程 ID 的摘要。

```
show running-configuration ospf
```

- 以 EXEC 模式查看 IP 路由的摘要信息。

```
show ip route summary
```

- 以 EXEC 模式查看 OSPF 数据库的摘要信息。

```
show ip ospf database
```

- 以 EXEC 模式查看连接到本地路由器的 OSPF 邻居的配置。

```
show ip ospf neighbor
```

- 以 EXEC 模式查看 OSPF 计算的路由。

```
show ip ospf routes
```

### 查看 OSPF 配置

```
OS10# show running-configuration ospf
!
interface ethernet1/1/1
ip ospf 100 area 0.0.0.0
!
router ospf 100
log-adjacency-changes
```

## 调试 OSPF

使用以下流程调试 OSPFv2 和 OSPFv3。

- 要调试 OSPFv2:

```
debug ip ospfv2
```

- 要调试 OSPFv3:

```
debug ip ospfv3
```

## OSPFv2 命令

### area default-cost

设置由 ABR 生成的摘要默认路由的指标，并将其发送至存根区域。

|        |                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>area area-id default-cost cost</code>                                                                                                                                           |
| 参数     | <ul style="list-style-type: none"> <li>• <i>area-id</i> — 以点分隔的十进制 A.B.C.D 格式输入 OSPF 区域 ID，或者输入编号，从 0 到 65535。</li> <li>• <i>cost</i> — 输入存根区域的已通告外部路由指标的成本，范围从 0 到 65535。</li> </ul> |
| 默认     | 成本为 1                                                                                                                                                                                 |
| 命令模式   | ROUTER-OSPF                                                                                                                                                                           |
| 使用情况信息 | 成本也称为参考带宽或带宽。在存根区域边缘的边界路由器上使用 <code>area default-cost</code> 命令。此命令的 <code>no</code> 版本会将该值重置为默认值。                                                                                    |
| 示例     | <pre>OS10(conf-router-ospf-10)# area 10.10.1.5 default-cost 10</pre>                                                                                                                  |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                      |

### area nssa

将区域定义为 NSSA。

|      |                                                                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | <code>area area-id nssa [default-information-originate   no-redistribution   no-summary]</code>                                                                                                                                                                                                                           |
| 参数   | <ul style="list-style-type: none"> <li>• <i>area-id</i> — 将 OSPF 区域 ID 输入为 A.B.C.D 格式或数字（从 1 到 65535）的 IP 地址。</li> <li>• <i>no-redistribution</i> — （可选）阻止 <code>redistribute</code> 命令将路由分发到 NSSA。仅在 NSSA ABR 中使用 <code>no-redistribution</code> 命令。</li> <li>• <i>no-summary</i> — （可选）确保不向 NSSA 发送任何摘要 LSA。</li> </ul> |
| 默认   | 未配置                                                                                                                                                                                                                                                                                                                       |
| 命令模式 | ROUTER-OSPF                                                                                                                                                                                                                                                                                                               |



**使用情况信息** 此命令的 `no` 版本将移除 NSSA。

**示例**

```
OS10(config-router-ospf-10)# area 10.10.1.5 nssa
```

**支持的版本** 10.2.0E or later

## area range

汇总与 ABR 中某个区域上的地址/掩码匹配的路由。

**语法** `area area-id range ip-address [no-advertise]`

**参数**

- `area-id` — 将 OSPF 区域 ID 设置为 A.B.C.D 格式或数字（从 1 到 65535）的 IP 地址。
- `ip-address` — （可选）以点分十进制格式输入 IP 地址/掩码。
- `no-advertise` — （可选）将状态设置为不通知。类型 3 摘要-LSA 会取消，并且组件网络在其他区域中保持隐藏状态。

**默认** 未配置

**命令模式** ROUTER-OSPF

**使用情况信息** 此命令的 `no` 版本将禁用路由汇总。

**示例**

```
OS10(config-router-ospf-10)# area 0 range 10.1.1.4/8 no-advertise
```

**支持的版本** 10.2.0E or later

## area stub

将区域定义为 OSPF 存根区域。

**语法** `area area-id stub [no-summary]`

**参数**

- `area-id` — 将 OSPF 区域 ID 设置为 A.B.C.D 格式或数字（从 1 到 65535）的 IP 地址。
- `no-summary` — （可选）防止 ABR 将摘要发送至存根区域。

**默认** 未配置

**命令模式** ROUTER-OSPF

**使用情况信息** 此命令的 `no` 版本将删除存根区域。

**示例**

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# area 10.10.1.5 stub
```

**支持的版本** 10.2.0E or later

## auto-cost reference-bandwidth

基于配置的自动成本参考带宽值计算接口的默认指标。

**语法** `auto-cost reference-bandwidth value`

**参数**

`value` — 输入参考带宽值以计算 OSPF 接口成本（以每秒兆位数为单位），从 1 到 4294967。

**默认** 100000

**命令模式** ROUTER-OSPF

**使用情况信息** 在 INTERFACE 模式下通过 `ip ospf cost` 命令设置的值将覆盖通过 `auto-cost` 命令所产生的成本。此命令的 `no` 版本会将该值重置为默认值。

|       |                                                                                                      |
|-------|------------------------------------------------------------------------------------------------------|
| 示例    | <pre>OS10(config)# router ospf 10 OS10(conf-router-ospf-10)# auto-cost reference-bandwidth 150</pre> |
| 支持的版本 | 10.2.0E or later                                                                                     |

## clear ip ospf process

清除所有 OSPF 路由表。

|        |                                                                                                                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>clear ip ospf {instance-number} [vrf vrf-name] process</code>                                                                                                                                       |
| 参数     | <ul style="list-style-type: none"> <li><code>instance-number</code> — 输入 OSPF 实例编号，从 1 到 65535。</li> <li><code>vrf vrf-name</code> — 输入关键字 <code>vrf</code> 后跟 VRF 的名称，以重置在该 VRF 中配置的 OSPF 进程。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                       |
| 命令模式   | EXEC                                                                                                                                                                                                      |
| 使用情况信息 | 此命令将清除 OSPF 路由表中的所有条目。                                                                                                                                                                                    |
| 示例     | <pre>OS10# clear ip ospf 3 vrf vrf-test process</pre>                                                                                                                                                     |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                          |

## clear ip ospf statistics

清除 OSPF 流量统计信息。

|        |                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>clear ip ospf [instance-number] [vrf vrf-name] statistics</code>                                                                                                                                                |
| 参数     | <ul style="list-style-type: none"> <li><code>instance-number</code> — （可选）输入 OSPF 的实例编号，从 1 到 65535。</li> <li><code>vrf vrf-name</code> — （可选）输入关键字 <code>vrf</code>，后跟 VRF 的名称，以清除配置的 VRF 中的 OSPF 流量统计信息。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                   |
| 命令模式   | EXEC                                                                                                                                                                                                                  |
| 使用情况信息 | 此命令将清除指定实例或所有已配置 OSPF 实例中的 OSPF 流量统计信息，并将其重置为零。                                                                                                                                                                       |
| 示例     | <pre>OS10# clear ip ospf 10 vrf vrf-test statistics</pre>                                                                                                                                                             |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                                                  |

## debug ip ospfv2

启用开放式最短路径优先第 2 版 (OSPFv2) 调试，并显示与 OSPFv2 处理相关的消息。

|        |                                                         |
|--------|---------------------------------------------------------|
| 语法     | <code>debug ip ospfv2</code>                            |
| 参数     | 无                                                       |
| 默认     | 无                                                       |
| 命令模式   | EXEC                                                    |
| 使用情况信息 | <code>no debug ip ospfv2</code> 命令将停止显示与处理 OSPFv2 相关的消息 |
| 示例     | <pre>debug ip ospfv2</pre>                              |
| 支持的版本  | OS10 原有命令。                                              |

## default-information originate

生成默认的外部路由信息并分发给 OSPF 路由域。

**语法** `default-information originate [always]`

**参数** `always` — (可选) 始终通告默认路由。

**默认** 已禁用

**命令模式** ROUTER-OSPF

**使用情况信息** 此命令的 `no` 版本将禁用默认路由的分布。

**示例**

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# default-information originate always
```

**支持的版本** 10.3.0E or later

## default-metric

为 OSPF 进程的重新分配路由分配指标值。

**语法** `default-metric number`

**参数** `number` — 输入默认指标值, 从 1 到 16777214。

**默认** 未配置

**命令模式** ROUTER-OSPF

**使用情况信息** 此命令的 `no` 版本将禁用默认指标配置。

**示例**

```
OS10(conf-router-ospf-10)# default-metric 2000
```

**支持的版本** 10.2.0E or later

## fast-converge

将最小 LSA 源和到达时间设置为零 (0), 以允许更快的路由计算, 因此聚合所需的时间更少。

**语法** `fast-converge convergence-level`

**参数** `convergence-level` — 输入所需的聚合级别值, 从 1 到 4。

**默认** 未配置

**命令模式** ROUTER-OSPF

**使用情况信息** 融合级别 1 (最佳) 符合大多数融合的要求。

 **注:** 仅在咨询 Dell EMC 技术支持后选择更高的融合级别。

此命令的 `no` 版本将禁用快速融合配置。

**示例**

```
OS10(conf-router-ospf-10)# fast-converge 3
```

**支持的版本** 10.2.0E or later

## graceful-restart

在正常或未命中重新启动期间启用帮助程序模式。

**语法** `graceful-restart role helper-only`

**参数** 无

|        |                                   |
|--------|-----------------------------------|
| 默认     | 已禁用                               |
| 命令模式   | ROUTER-OSPF                       |
| 使用情况信息 | 此命令的 <code>no</code> 版本将禁用帮助程序模式。 |

#### 示例

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# graceful-restart role helper-only
```

|       |                  |
|-------|------------------|
| 支持的版本 | 10.3.0E or later |
|-------|------------------|

## ip ospf area

将接口连接到 OSPF 区域。

**语法** `ip ospf process-id area area-id`

- 参数**
- `process-id` — 设置特定 OSPF 进程的 OSPF 进程 ID，从 1 到 65535。
  - `area area-id` — 以点分隔的十进制 A.B.C.D 格式输入 OSPF 区域 ID，或者输入一个从 1 到 65535 的区域 ID 号。

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息** 此命令的 `no` 版本将从 OSPF 区域中移除接口。

#### 示例

```
OS10(config-if-vl-10)# ip ospf 10 area 5
```

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|

## ip ospf authentication-key

配置文本身份验证密钥以启用接口上的 OSPF 流量。

**语法** `ip ospf authentication-key key`

**参数** `key` — 输入用于身份验证密钥的八个字符的字符串。

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息** 要交换 OSPF 信息，同一网络中的所有邻接路由器都必须使用相同的身份验证密钥。此命令的 `no` 版本将删除身份验证密钥。

#### 示例

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# ip ospf authentication-key sample
```

|       |                  |
|-------|------------------|
| 支持的版本 | 10.3.0E or later |
|-------|------------------|

## ip ospf cost

更改与接口上的 OSPF 流量关联的成本。

**语法** `ip ospf cost cost`

**参数** `cost` — 输入一个值作为接口的 OSPF 成本，从 1 到 65535。

**默认** 基于带宽参考

**命令模式** INTERFACE

**使用情况信息** 如果未配置，接口开销基于 `auto-cost` 命令。此命令可配置多个供应商的 OSPF，以确保所有路由器使用相同的成本。如果手动配置成本，则基于参考带宽的计算得出的成本不适用于该接口。此命令的 `no` 版本会移除 IP OSPF 成本配置。

**示例**

```
OS10(config)# interface vlan 10
OS10(conf-if-vl-1)# ip ospf cost 10
```

**支持的版本** 10.2.0E or later

## ip ospf dead-interval

设置自从路由器收到上次问候数据包以来的时间间隔。超过该时间间隔后，相邻路由器会将路由器声明为失效。

**语法** `ip ospf dead-interval seconds`

**参数** `seconds` — 输入停顿间隔值（以秒为单位），从 1 到 65535。

**默认** 40 秒

**命令模式** INTERFACE

**使用情况信息** 默认情况下，停顿间隔为默认呼叫间隔的四倍。此命令的 `no` 版本会将该值重置为默认值。

**示例**

```
OS10(conf-if-vl-10)# ip ospf dead-interval 10
```

**支持的版本** 10.2.0E or later

## ip ospf hello-interval

设置在接口上发送的问候数据包之间的时间间隔。

**语法** `ip ospf hello-interval seconds`

**参数** `seconds` — 输入问候间隔值（以秒为单位），从 1 到 65535。

**默认** 10 秒

**命令模式** INTERFACE

**使用情况信息** 网络中的所有路由器都必须具有与问候数据包相同的问候时间间隔。此命令的 `no` 版本会将该值重置为默认值。

 **注：**为 OSPF 配置命令的时间间隔时，OSPF 失效间隔值隐式设置为大于命令的间隔值的四倍的值。

**示例**

```
OS10(conf-if-vl-10)# ip ospf hello-interval 30
```

**支持的版本** 10.2.0E or later

## ip ospf message-digest-key

启用 OSPF MD5 身份验证，并在接口上发送 OSPF 消息摘要密钥。

**语法** `ip ospf message-digest-key keyid md5 key`

**参数**

- `keyid` — 输入接口的 MD5 密钥 ID，从 1 到 255。
- `key` — 输入字符串作为密码。最多 16 个字符。

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息** 同一网络中的所有邻接路由器必须使用相同的密钥值来交换 OSPF 信息。此命令的 `no` 版本将删除身份验证密钥。

|       |                                                                                                                        |
|-------|------------------------------------------------------------------------------------------------------------------------|
| 示例    | <pre>OS10(config)# interface ethernet 1/1/1 OS10(conf-if-eth1/1/1)# ip ospf message-digest-key 2 md5 sample12345</pre> |
| 支持的版本 | 10.3.0E or later                                                                                                       |

## ip ospf mtu-ignore

允许在收到 DBD 数据包时进行 OSPF MTU 不匹配检测。

|        |                                                                                                                                     |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | ip ospf mtu-ignore                                                                                                                  |
| 参数     | 无                                                                                                                                   |
| 默认     | 未配置                                                                                                                                 |
| 命令模式   | INTERFACE                                                                                                                           |
| 使用情况信息 | 当邻居交换 DBD 数据包时，OSPF 进程将检查邻居是否在通用接口上使用相同的 MTU。如果 DBD 数据包中的接收 MTU 高于传入接口上配置的 IP MTU OSPF，则不会建立邻接。此命令的 no 版本将禁用 IP OSPF mtu-ignore 配置。 |
| 示例     | <pre>OS10(conf-if-vl-10)# ip ospf mtu-ignore</pre>                                                                                  |
| 支持的版本  | 10.2.0E or later                                                                                                                    |

## ip ospf network

设置接口的网络类型。

|        |                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------|
| 语法     | ip ospf network {point-to-point   broadcast}                                                                             |
| 参数     | <ul style="list-style-type: none"> <li>point-to-point — 将接口设置为点对点网络的一部分。</li> <li>broadcast — 将接口设置为广播网络的一部分。</li> </ul> |
| 默认     | 广播                                                                                                                       |
| 命令模式   | INTERFACE                                                                                                                |
| 使用情况信息 | 此命令的 no 版本会将该值重置为默认值。                                                                                                    |
| 示例     | <pre>OS10(conf-if-eth1/1/1)# ip ospf network broadcast</pre>                                                             |
| 支持的版本  | 10.2.0E or later                                                                                                         |

## ip ospf passive

将接口配置为被动接口，并禁止接收和发送到被动接口的路由更新。

|        |                                                                                                                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | ip ospf passive                                                                                                                                                                                                                                        |
| 参数     | 无                                                                                                                                                                                                                                                      |
| 默认     | 未配置                                                                                                                                                                                                                                                    |
| 命令模式   | INTERFACE                                                                                                                                                                                                                                              |
| 使用情况信息 | <p>必须先配置接口，然后才能将接口设置为被动模式。此命令的 no 版本将禁用被动接口配置。</p> <p> <b>注：</b>由于环回接口为隐式被动，因此不会在环回接口上影响发送和接收 OSPF 路由更新的配置。但是，与这些环回接口相对应的网络信息仍在通过 OSPF 配置的其他接口发送的 OSPF LSA 中发布。</p> |
| 示例     | <pre>OS10(conf-if-eth1/1/6)# ip ospf passive</pre>                                                                                                                                                                                                     |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                       |

## ip ospf priority

设置接口的优先级，以确定 OSPF 网络的灾难恢复。

|        |                                                                           |
|--------|---------------------------------------------------------------------------|
| 语法     | <code>ip ospf priority number</code>                                      |
| 参数     | <i>number</i> — 输入路由器优先级编号，从 0 到 255。                                     |
| 默认     | 1                                                                         |
| 命令模式   | INTERFACE                                                                 |
| 使用情况信息 | 当连接到网络的两个路由器尝试成为灾难恢复时，具有更高路由器优先级的路由器优先。此命令的 <code>no</code> 版本会将该值重置为默认值。 |
| 示例     | <pre>OS10(conf-if-eth1/1/6)# ip ospf priority 4</pre>                     |
| 支持的版本  | 10.2.0E or later                                                          |

## ip ospf retransmit-interval

设置属于接口的邻接的丢失 LSA 之间的重新传输时间。

|        |                                                                   |
|--------|-------------------------------------------------------------------|
| 语法     | <code>ip ospf retransmit-interval seconds</code>                  |
| 参数     | <i>seconds</i> — 以秒为单位输入一个值，作为重新传输之间的间隔，从 1 到 3600。               |
| 默认     | 5 秒                                                               |
| 命令模式   | INTERFACE                                                         |
| 使用情况信息 | 将时间间隔设置为足够大的值，以避免不必要的重新传输。此命令的 <code>no</code> 版本会将该值重置为默认值。      |
| 示例     | <pre>OS10(conf-if-eth1/1/6)# ip ospf retransmit-interval 20</pre> |
| 支持的版本  | 10.2.0E or later                                                  |

## ip ospf transmit-delay

设置在接口上发送链路状态更新包所需的估计时间。

|        |                                                                                            |
|--------|--------------------------------------------------------------------------------------------|
| 语法     | <code>ip ospf transmit-delay seconds</code>                                                |
| 参数     | <i>seconds</i> — 以秒为单位设置发送链路状态更新所需的时间，从 1 到 3600。                                          |
| 默认     | 1 秒                                                                                        |
| 命令模式   | INTERFACE                                                                                  |
| 使用情况信息 | 设置 <code>ip ospf transmit-delay</code> 值时，请考虑接口的传输和传播延迟。此命令的 <code>no</code> 版本会将该值重置为默认值。 |
| 示例     | <pre>OS10(conf-if-eth1/1/4)# ip ospf transmit-delay 5</pre>                                |
| 支持的版本  | 10.2.0E or later                                                                           |

## log-adjacency-changes

允许记录有关 OSPF 邻接状态变化的 syslog 消息。

|    |                                    |
|----|------------------------------------|
| 语法 | <code>log-adjacency-changes</code> |
| 参数 | 无                                  |
| 默认 | 已禁用                                |

**命令模式** ROUTER-OSPF

**使用情况信息** 此命令的 `no` 版本会将该值重置为默认值。

**示例**

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# log-adjacency-changes
```

**支持的版本** 10.2.0E or later

## max-metric router-lsa

将 OSPF 配置为在路由器上通告最大指标，使其不需要作为其他路由器的中间跳。

**语法** `max-metric router-lsa`

**参数** 无

**默认** 未配置

**命令模式** ROUTER-OSPF

**使用情况信息** 网络中的路由器在计算最短路径后，不希望其他路由器作为下一个中间跳。此命令的 `no` 版本将禁用最大指标通告配置。

**示例**

```
OS10(conf-router-ospf-10)# max-metric router-lsa
```

**支持的版本** 10.2.0E or later

## maximum-paths

允许转发多个路径上的数据包。

**语法** `maximum-paths number`

**参数** `number` — 输入 OSPF 的路径数量，从 1 到 128。

**默认** 64

**命令模式** ROUTER-OSPF

**使用情况信息** 此命令的 `no` 版本会将该值重置为默认值。

**示例**

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# maximum-paths 1
```

**支持的版本** 10.2.0E or later

## redistribute

将来自另一个路由协议或路由实例的信息重新分配到 OSPFv2 进程。

**语法** `redistribute {bgp as-number | connected | static} [route-map map-name]`

**参数**

- `as-number` — 输入自治编号以重新分发整个 OSPF 实例的 BGP 路由信息，从 1 到 4294967295。
- `connected` — 输入要重新分发的接口上来自连接的活动路由的信息。
- `static` — 输入重新分发的接口上来自静态路由的信息。
- `route-map name` — 输入已配置的路由映射的名称。

**默认** 未配置

**命令模式** ROUTER-OSPF

**使用情况信息** 重新分发 OSPF 时，不会从 BGP 配置中完全移除该进程。此命令的 `no` 版本将禁用重新分发配置。



## 示例

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# redistribute bgp 4 route-map dell1
```

## 示例（已连接）

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# redistribute connected route-map dell2
```

## 支持的版本

10.2.0E or later

## router-id

为 OSPF 进程配置固定路由器 ID。

### 语法

`router-id ip-address`

### 参数

`ip-address` — 输入路由器的 IP 地址作为路由器 ID。

### 默认

未配置

### 命令模式

ROUTER-OSPF

### 使用情况信息

为每个路由器配置 IP 地址格式的任意值。每个路由器 ID 必须是唯一的。为活动的 OSPF 路由器进程使用固定的路由器 ID。更改路由器 ID 会导致现有 OSPF 邻接。新的路由器 ID 将立即变为有效。此命令的 `no` 版本将禁用路由器 ID 配置。

## 示例

```
OS10(config)# router ospf 10
OS10(conf-router-ospf-10)# router-id 10.10.1.5
```

## 支持的版本

10.2.0E or later

## router ospf

进入路由器 OSPF 模式并配置 OSPF 实例。

### 语法

`router ospf instance-number [vrf vrf-name]`

### 参数

- `instance-number` — 输入路由器 OSPF 实例编号，从 1 到 65535。
- `vrf vrf-name` — 输入关键字 `vrf`，后跟 VRF 的名称，以便在该 VRF 中配置 OSPF 实例。

### 默认

未配置

### 命令模式

CONFIGURATION

### 使用情况信息

在使用此命令之前，为接口分配 IP 地址。此命令的 `no` 版本将删除 OSPF 实例。

## 示例

```
OS10(config)# router ospf 10 vrf vrf-test
```

## 支持的版本

10.2.0E or later

## show ip ospf

显示 OSPF 实例配置信息。

### 语法

`show ip ospf [instance-number] [vrf vrf-name]`

### 参数

- `instance-number` — 查看指定实例编号的 OSPF 信息，从 1 到 65535。
- `vrf vrf-name` — 输入关键字 `vrf`，后跟 VRF 的名称，以显示与该 VRF 对应的 OSPF 配置信息。

### 默认

未配置

### 命令模式

EXEC

### 使用情况信息

无

示例

```
OS10# show ip ospf 10
Routing Process ospf 10 with ID 111.2.1.1
Supports only single TOS (TOS0) routes
It is an Autonomous System Boundary Router
It is Flooding according to RFC 2328
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
 Area (0.0.0.0)
 Number of interface in this area is 3
 SPF algorithm executed 38 times
 Area ranges are
```

支持的版本 10.2.0E or later

show ip ospf asbr

显示 OSPF 可见的所有 ASBR。

- 语法 show ip ospf [process-id] [vrf vrf-name] asbr
- 参数
  - process-id — (可选) 根据进程 ID 显示信息。
  - vrf vrf-name — (可选) 显示在指定 VRF 中配置的 OSPF 进程可见的 ASBR 路由器。
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 您可以隔离外部路由的问题。通过将 LSA 成本添加到达 ASBR 路由器的成本来计算外部 OSPF 路由。如果外部路由不具有正确的成本，此命令将确定原始路由器的路径是否正确。将显示不在直接连接区域中的 ASBR。您可以通过标记确定 ASBR 是否位于直接连接的区域。对于直接连接区域中的 ASBR，设置了 E 标记。

示例

```
OS10# show ip ospf 10 asbr

RouterID Flags Cost Nexthop Interface Area
112.2.1.1 E/-/-/ 1 110.1.1.2 vlan3050 0.0.0.0
111.2.1.1 E/-/-/ 0 0.0.0.0 - -
```

支持的版本 10.2.0E or later

show ip ospf database

显示所有 LSA 信息。必须启用 OSPF 才能生成输出。

- 语法 show ip ospf [process-id] [vrf vrf-name] database
- 参数
  - process-id — (可选) 查看特定 OSPF 进程 ID 的 LSA 信息。如果未输入进程 ID，此命令将应用于所有已配置的 OSPF 进程。
  - vrf vrf-name — (可选) 输入关键字 vrf，后跟 VRF 的名称，以显示与该 VRF 对应的 OSPF 进程 LSA 信息。
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息
  - Link ID — 标识路由器 ID。
  - ADV Router — 标识通告路由器的 ID。
  - Age — 显示 LS 时限。
  - Seq# — 标识 LS 序列号。这标识了旧的或重复的 LSA。
  - Checksum — 显示 LSA 的完整内容的 Fletcher 校验和。
  - Link count — 显示该路由器的接口数量。

示例

```
OS10# show ip ospf 10 database
OSPF Router with ID (111.2.1.1) (Process ID 10)

Router (Area 0.0.0.0)

Link ID ADV Router Age Seq# Checksum Link
count
111.2.1.1 111.2.1.1 1281 0x8000000d 0x9bf2 3
111.111.111.1 111.111.111.1 1430 0x8000021a 0x515a 1
111.111.111.2 111.111.111.2 1430 0x8000021a 0x5552 1
112.2.1.1 112.2.1.1 1282 0x8000000b 0x0485 3
112.112.112.1 112.112.112.1 1305 0x80000250 0xbab2 1
112.112.112.2 112.112.112.2 1305 0x80000250 0xbeaa 1

Network (Area 0.0.0.0)

Link ID ADV Router Age Seq# Checksum
110.1.1.2 112.2.1.1 1287 0x80000008 0xd2b1
111.1.1.1 111.2.1.1 1458 0x80000008 0x1b8f
111.2.1.1 111.2.1.1 1458 0x80000008 0x198f
112.1.1.1 112.2.1.1 1372 0x80000008 0x287c
112.2.1.1 112.2.1.1 1372 0x80000008 0x267c

Summary Network (Area 0.0.0.0)
```

支持的版本 10.2.0E or later

show ip ospf database asbr-summary

显示有关 AS 边界 LSA 的信息。

- 语法
- show ip ospf [process-id] database asbr-summary
- 参数
- process-id — (可选) 显示指定 OSPF 进程 ID 的 AS 边界 LSA 信息。如果未输入进程 ID，则此操作仅适用于第一个 OSPF 过程。
  - vrf vrf-name — (可选) 为与指定 VRF 对应的 OSPF 进程 ID 显示 AS 边界 LSA 信息。
- 默认
- 未配置
- 命令模式
- EXEC
- 使用情况信息
- LS Age — 显示 LS 年限。
  - Options — 显示可选功能。
  - LS Type — 显示 LS 类型。
  - Link State ID — 标识路由器 ID。
  - Advertising Router — 标识通告路由器的 ID。
  - LS Seq Number — 标识 LS 序列号。这标识了旧的或重复的 LSA。
  - Checksum — 显示 LSA 的完整内容的 Fletcher 校验和。
  - Length — 显示 LSA 长度（以字节为单位）。
  - Network Mask — 标识在该区域上实施的网络掩码。
  - TOS — 显示 ToS 选项。唯一可用的选项为零。
  - Metric — 显示 LSA 指标。

示例

```
OS10# show ip ospf 10 database asbr-summary

OSPF Router with ID (1.1.1.1) (Process ID 100)

Summary Asbr (Area 0.0.0.1)

LS age: 32
Options: (No TOS-Capability, No DC)
LS type: Summary Asbr
Link State ID: 8.1.1.1
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000001
```

```
Checksum: 0xB595
Length: 28
Network Mask: /0
 TOS: 0 Metric: 0
```

**支持的版本** 10.2.0E or later

## show ip ospf database external

显示有关 AS 外部类型 5 LSA 的信息。

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>show ip ospf [process-id] [vrf vrf-name] database external</code>                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>参数</b>     | <ul style="list-style-type: none"><li>• <code>process-id</code> — (可选) 显示指定 OSPF 进程 ID 的外部类型 5 LSA 信息。如果未输入进程 ID, 则此命令仅适用于第一个 OSPF 过程。</li><li>• <code>vrf vrf-name</code> — (可选) 显示与 VRF 对应的指定 OSPF 进程 ID 的外部类型 5 LSA 信息。</li></ul>                                                                                                                                                                                                                                          |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>命令模式</b>   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>使用情况信息</b> | <ul style="list-style-type: none"><li>• LS Age — 显示 LS 时限。</li><li>• Options — 显示路由器上可用的可选功能。</li><li>• LS Type — 显示 LS 类型。</li><li>• Link State ID — 标识路由器 ID。</li><li>• Advertising Router — 标识通告路由器的 ID。</li><li>• LS Seq Number — 标识 LS 序列号。这标识了旧的或重复的 LSA。</li><li>• Checksum — 显示 LSA 的完整内容的 Fletcher 校验和。</li><li>• Length — 显示 LSA 长度 (以字节为单位)。</li><li>• Network Mask — 标识在该区域上实施的网络掩码。</li><li>• TOS — 显示 ToS 选项。唯一可用的选项为零。</li><li>• Metric — 显示 LSA 指标。</li></ul> |

### 示例

```
OS10# show ip ospf 10 database external

OSPF Router with ID (111.2.1.1) (Process ID 10)

 Type-5 AS External

LS age: 1424
Options: (No TOS-capability, No DC, E)
LS type: Type-5 AS External
Link State ID: 110.1.1.0
Advertising Router: 111.2.1.1
LS Seq Number: 0x80000009
Checksum: 0xc69a
Length: 36
Network Mask: /24
 Metric Type: 2
 TOS: 0
 Metric: 20
 Forward Address: 110.1.1.1
 External Route Tag: 0
```

**支持的版本** 10.2.0E or later

## show ip ospf database network

显示有关网络类型 2 LSA 的信息。

|           |                                                                                                                                                    |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b> | <code>show ip ospf [process-id] [vrf vrf-name] database network</code>                                                                             |
| <b>参数</b> | <ul style="list-style-type: none"><li>• <code>process-id</code> — (可选) 显示指定的 OSPF 进程 ID 的网络类型 2 LSA 的信息。如果未输入进程 ID, 则此命令仅适用于第一个 OSPF 过程。</li></ul> |

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | • <code>vrf vrf-name</code> — (可选) 显示与 VRF 对应的指定 OSPF 进程 ID 的网络类型 2 LSA 的信息。                                                                                                                                                                                                                                                                                                                                                                                                       |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 使用情况信息 | <ul style="list-style-type: none"> <li>• LS Age — 显示 LS 年限。</li> <li>• Options — 显示可选功能。</li> <li>• LS Type — 显示 LS 类型。</li> <li>• Link State ID — 标识路由器 ID。</li> <li>• Advertising Router — 标识通告路由器的 ID。</li> <li>• LS Seq Number — 标识 LS 序列号。这标识了旧的或重复的 LSA。</li> <li>• Checksum — 显示 LSA 的完整内容的 Fletcher 校验和。</li> <li>• Length — 显示 LSA 长度 (以字节为单位)。</li> <li>• Network Mask — 标识在该区域上实施的网络掩码。</li> <li>• TOS — 显示 ToS 选项。唯一可用的选项为零。</li> <li>• Metric — 显示 LSA 指标。</li> </ul> |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre> OS10# show ip ospf 10 database network OSPF Router with ID (111.2.1.1) (Process ID 10)                  Network (Area 0.0.0.0)  LS age: 1356 Options: (No TOS-capability, No DC, E) LS type: Network Link State ID: 110.1.1.2 Advertising Router: 112.2.1.1 LS Seq Number: 0x80000008 Checksum: 0xd2b1 Length: 32 Network Mask: /24     Attached Router: 111.2.1.1     Attached Router: 112.2.1.1 </pre> |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|

## show ip ospf database nssa external

显示有关 NSSA 外部类型 7 LSA 的信息。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show ip ospf [process-id] [vrf vrf-name] database nssa external</code>                                                                                                                                                                                                                                                                                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"> <li>• <code>process-id</code> — (可选) 显示指定 OSPF 进程 ID 的 NSSA 外部类型 7 LSA 信息。如果未输入进程 ID, 则此命令仅适用于第一个 OSPF 过程。</li> <li>• <code>vrf vrf-name</code> — (可选) 显示与 VRF 对应的指定 OSPF 进程 ID 的 NSSA 外部类型 7 LSA 信息。</li> </ul>                                                                                                                                                                                                                                       |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 使用情况信息 | <ul style="list-style-type: none"> <li>• LS Age — 显示 LS 时限。</li> <li>• Options — 显示路由器上可用的可选功能。</li> <li>• LS Type — 显示 LS 类型。</li> <li>• Link State ID — 标识路由器 ID。</li> <li>• Advertising Router — 标识通告路由器的 ID。</li> <li>• LS Seq Number — 标识 LS 序列号。这标识了旧的或重复的 LSA。</li> <li>• Checksum — 显示 LSA 的完整内容的 Fletcher 校验和。</li> <li>• Length — 显示 LSA 长度 (以字节为单位)。</li> <li>• Network Mask — 标识在该区域上实施的网络掩码。</li> <li>• TOS — 显示 ToS 选项。唯一可用的选项为零。</li> <li>• Metric — 显示 LSA 指标。</li> </ul> |

## 示例

```
OS10# show ip ospf database nssa external

 OSPF Router with ID (2.2.2.2) (Process ID 100)

 NSSA External (Area 0.0.0.1)

LS age: 98
Options: (No TOS-Capability, No DC, No Type 7/5 translation)
LS type: NSSA External
Link State ID: 0.0.0.0
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000001
Checksum: 0x430C
Length: 36
Network Mask: /0
 Metric Type: 1
 TOS: 0
 Metric: 16777215
 Forward Address: 0.0.0.0
 External Route Tag: 0

LS age: 70
Options: (No TOS-Capability, No DC, No Type 7/5 translation)
LS type: NSSA External
Link State ID: 0.0.0.0
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000001
Checksum: 0x2526
Length: 36
Network Mask: /0
 Metric Type: 1
 TOS: 0
 Metric: 0
 Forward Address: 0.0.0.0
 External Route Tag: 0

LS age: 65
Options: (No TOS-Capability, No DC, No Type 7/5 translation)
LS type: NSSA External
Link State ID: 12.1.1.0
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000001
Checksum: 0xBDEA
Length: 36
Network Mask: /24
 Metric Type: 2
 TOS: 0
 Metric: 20
 Forward Address: 0.0.0.0
 External Route Tag: 0

LS age: 65
Options: (No TOS-Capability, No DC, No Type 7/5 translation)
LS type: NSSA External
Link State ID: 13.1.1.0
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000001
Checksum: 0xB0F6
Length: 36
Network Mask: /24
 Metric Type: 2
 TOS: 0
 Metric: 20
 Forward Address: 0.0.0.0
 External Route Tag: 0

LS age: 65
Options: (No TOS-Capability, No DC, No Type 7/5 translation)
LS type: NSSA External
Link State ID: 14.1.1.0
Advertising Router: 2.2.2.2
```

```

LS Seq Number: 0x80000001
Checksum: 0xA303
Length: 36
Network Mask: /24
 Metric Type: 2
 TOS: 0
 Metric: 20
 Forward Address: 0.0.0.0
 External Route Tag: 0

```

**支持的版本** 10.2.0E or later

## show ip ospf database opaque-area

显示有关不透明区域类型 10 LSA 的信息。

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | show ip ospf [ <i>process-id</i> ] [ <i>vrf vrf-name</i> ] database opaque-area                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>参数</b>     | <ul style="list-style-type: none"> <li>• <i>process-id</i> — (可选) 显示 OSPF 进程 ID 的不透明区域类型 10 信息。如果未输入进程 ID, 则此命令仅适用于第一个 OSPF 过程。</li> <li>• <i>vrf vrf-name</i> — (可选) 显示与 VRF 对应的 OSPF 进程 ID 的不透明区域类型 10 信息。</li> </ul>                                                                                                                                                                                                                                                                |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>命令模式</b>   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>使用情况信息</b> | <ul style="list-style-type: none"> <li>• LS Age — 显示 LS 时限。</li> <li>• Options — 显示路由器上可用的可选功能。</li> <li>• LS Type — 显示 LS 类型。</li> <li>• Link State ID — 标识路由器 ID。</li> <li>• Advertising Router — 标识通告路由器的 ID。</li> <li>• LS Seq Number — 标识 LS 序列号。这标识了旧的或重复的 LSA。</li> <li>• Checksum — 显示 LSA 的完整内容的 Fletcher 校验和。</li> <li>• Length — 显示 LSA 长度 (以字节为单位)。</li> <li>• Opaque Type — 标识不透明类型字段, 即 LS ID 的前 8 位。</li> <li>• Opaque ID — 标识不透明的类型特定 ID, 即 LS ID 的剩余 24 位。</li> </ul> |

### 示例

```

OS10# show ip ospf database opaque-area
 OSPF Router with ID (1.1.1.1) (Process ID 100)

 Type-10 Area Local Opaque (Area 0.0.0.1)

LS age: 3600
Options: (No TOS-Capability, No DC)
LS type: Type-10 Area Local Opaque
Link State ID: 8.1.1.2
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000008
Checksum: 0x83B8
Length: 28
Opaque Type: 8
Opaque ID: 65794
!!
!

```

**支持的版本** 10.2.0E or later

## show ip ospf database opaque-as

显示有关不透明类型 11 LSA 的信息。

|           |                                              |
|-----------|----------------------------------------------|
| <b>语法</b> | show ip ospf [ <i>process-id</i> ] opaque-as |
|-----------|----------------------------------------------|

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 参数     | <i>process-id</i> — (可选) 显示指定 OSPF 进程 ID 的不透明 AS 类型 11 LSA 信息。如果未输入进程 ID, 则此命令仅适用于第一个 OSPF 过程。                                                                                                                                                                                                                                                                                                                                                                                         |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 使用情况信息 | <ul style="list-style-type: none"> <li>• LS Age — 显示 LS 时限。</li> <li>• Options — 显示路由器上可用的可选功能。</li> <li>• LS Type — 显示 LS 类型。</li> <li>• Link State ID — 标识路由器 ID。</li> <li>• Advertising Router — 标识通告路由器的 ID。</li> <li>• LS Seq Number — 标识 LS 序列号。这标识了旧的或重复的 LSA。</li> <li>• Checksum — 显示 LSA 的完整内容的 Fletcher 校验和。</li> <li>• Length — 显示 LSA 长度 (以字节为单位)。</li> <li>• Opaque Type — 标识不透明类型字段, 即 LS ID 的前 8 位。</li> <li>• Opaque ID — 标识不透明的类型特定 ID, 即 LS ID 的剩余 24 位。</li> </ul> |
| 示例     | <pre> OS10# show ip ospf 100 database opaque-as        OSPF Router with ID (1.1.1.1) (Process ID 100)                Type-11 AS Opaque  LS age: 3600 Options: (No TOS-Capability, No DC) LS type: Type-11 AS Opaque Link State ID: 8.1.1.3 Advertising Router: 2.2.2.2 LS Seq Number: 0x8000000D Checksum: 0x61D3 Length: 36 Opaque Type: 8 Opaque ID: 65795 </pre>                                                                                                                    |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

show ip ospf database opaque-link

显示有关不透明链路类型 9 LSA 的信息。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show ip ospf [<i>process-id</i>] [<i>vrf vrf-name</i>] database opaque-link</code>                                                                                                                                                                                                                                                                                                                                                                                               |
| 参数     | <ul style="list-style-type: none"> <li>• <i>process-id</i> — (可选) 显示 OSPF 进程 ID 的不透明链路类型 9 LSA 信息。如果未输入进程 ID, 则此命令仅适用于第一个 OSPF 过程。</li> <li>• <i>vrf vrf-name</i> — (可选) 显示与 VRF 对应的 OSPF 进程 ID 的不透明链路类型 9 LSA 信息。</li> </ul>                                                                                                                                                                                                                                                          |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 使用情况信息 | <ul style="list-style-type: none"> <li>• LS Age — 显示 LS 时限。</li> <li>• Options — 显示路由器上可用的可选功能。</li> <li>• LS Type — 显示 LS 类型。</li> <li>• Link State ID — 标识路由器 ID。</li> <li>• Advertising Router — 标识通告路由器的 ID。</li> <li>• LS Seq Number — 标识 LS 序列号。这标识了旧的或重复的 LSA。</li> <li>• Checksum — 显示 LSA 的完整内容的 Fletcher 校验和。</li> <li>• Length — 显示 LSA 长度 (以字节为单位)。</li> <li>• Opaque Type — 标识不透明类型字段, 即 LS ID 的前 8 位。</li> <li>• Opaque ID — 标识不透明的类型特定 ID, 即 LS ID 的剩余 24 位。</li> </ul> |
| 示例     | <pre> OS10# show ip ospf 100 database opaque-link       OSPF Router with ID (1.1.1.1) (Process ID 100) </pre>                                                                                                                                                                                                                                                                                                                                                                          |



```

Type-9 Link Local Opaque (Area 0.0.0.1)
LS age: 3600
Options: (No TOS-Capability, No DC)
LS type: Type-9 Link Local Opaque
Link State ID: 8.1.1.1
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000007
Checksum: 0x9DA1
Length: 28
Opaque Type: 8
Opaque ID: 65793

```

### 支持的版本

10.2.0E or later

## show ip ospf database router

显示有关路由器类型 1 LSA 的信息。

### 语法

```
show ip ospf process-id [vrf vrf-name] database router
```

### 参数

- *process-id* — (可选) 显示 OSPF 进程 ID 的路由器类型 1 LSA。如果未输入进程 ID，则此命令仅适用于第一个 OSPF 过程。
- *vrf vrf-name* — (可选) 显示与 VRF 对应的 OSPF 进程 ID 的路由器类型 1 LSA。

### 默认

未配置

### 命令模式

EXEC

### 使用情况信息

输出：

- LS age — 显示 LS 年限。
- Options — 显示可选功能。
- LS Type — 显示 LS 类型。
- Link State ID — 标识路由器 ID。
- Advertising Router — 标识通告路由器的 ID。
- LS Seq Number — 标识 LS 序列号。这标识了旧的或重复的 LSA。
- Checksum — 显示 LSA 的完整内容的 Fletcher 校验和。
- Length — 显示 LSA 长度（以字节为单位）。
- TOS — 显示 ToS 选项。唯一可用的选项为零。
- Metric — 显示 LSA 指标。

### 示例

```

OS10# show ip ospf 10 database router

 OSPF Router with ID (111.2.1.1) (Process ID 10)

 Router (Area 0.0.0.0)

LS age: 1419
Options: (No TOS-capability, No DC, E)
LS type: Router
Link State ID: 111.2.1.1
Advertising Router: 111.2.1.1
LS Seq Number: 0x8000000d
Checksum: 0x9bf2
Length: 60
AS Boundary Router
Number of Links: 3

Link connected to: a Transit Network
(Link ID) Designated Router address: 110.1.1.2
(Link Data) Router Interface address: 110.1.1.1
Number of TOS metric: 0
TOS 0 Metric: 1

Link connected to: a Transit Network

```

```
(Link ID) Designated Router address: 111.1.1.1
(Link Data) Router Interface address: 111.1.1.1
Number of TOS metric: 0
TOS 0 Metric: 1

Link connected to: a Transit Network
(Link ID) Designated Router address: 111.2.1.1
(Link Data) Router Interface address: 111.2.1.1
Number of TOS metric: 0
TOS 0 Metric: 1
```

**支持的版本** 10.2.0E or later

## show ip ospf database summary

显示网络摘要类型 3 LSA 路由信息。

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>show ip ospf [process-id] [vrf vrf-name] database summary</code>                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>process-id</code> — (可选) 显示特定 OSPF 进程 ID 的 LSA 信息。如果未输入进程 ID，则此命令仅适用于第一个 OSPF 过程。</li> <li><code>vrf vrf-name</code> — (可选) 显示与 VRF 对应的指定 OSPF 进程 ID 的 LSA 信息。</li> </ul>                                                                                                                                                                                                                                              |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>命令模式</b>   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>使用情况信息</b> | <ul style="list-style-type: none"> <li>LS Age — 显示 LS 年限。</li> <li>Options — 显示路由器上可用的可选功能。</li> <li>LS Type — 显示 LS 类型。</li> <li>Link State ID — 标识路由器 ID。</li> <li>Advertising Router — 标识通告路由器的 ID。</li> <li>LS Seq Number — 标识 LS 序列号。这标识了旧的或重复的 LSA。</li> <li>Checksum — 显示 LSA 的完整内容的 Fletcher 校验和。</li> <li>Length — 显示 LSA 长度 (以字节为单位)。</li> <li>Network Mask — 标识在该区域上实施的网络掩码。</li> <li>TOS — 显示 ToS 选项。唯一可用的选项为零。</li> <li>Metric — 显示 LSA 指标。</li> </ul> |

### 示例

```
OS10# show ip ospf 10 database summary
 OSPF Router with ID (111.2.1.1) (Process ID 10)

 Summary Network (Area 0.0.0.0)

LS age: 623
Options: (No TOS-capability, No DC)
C: Summary Network
Link State ID: 115.1.1.0
Advertising Router: 111.111.111.1
LS Seq Number: 0x800001e8
Checksum: 0x4a67
Length: 28
Network Mask: /24
 TOS: 0 Metric: 0
```

**支持的版本** 10.2.0E or later

## show ip ospf interface

显示已配置的 OSPF 接口。必须启用 OSPF 才能显示输出。

|           |                                                                                                                                                         |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b> | <code>show ip ospf interface [process-id] [vrf vrf-name] interface</code> 或 <code>show ip ospf [process-id] [vrf vrf-name] interface [interface]</code> |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------|

- 参数**
- *process-id* — (可选) 显示 OSPF 进程 ID 的信息。如果未输入进程 ID，则此命令仅适用于第一个 OSPF 过程。
  - *vrf vrf-name* — (可选) 显示与 VRF 对应的 OSPF 实例的信息。
  - *interface* — (可选) 输入接口信息：
    - *ethernet* — 输入以太网接口信息，从 1 到 48。
    - *port channel* — 输入端口通道接口编号，从 1 到 128。
    - *vlan* — 输入 VLAN 接口编号，从 1 到 4093。

**默认** 未配置

**命令模式** EXEC

**示例**

```
OS10# show ip ospf 10 interface
ethernet1/1/1 is up, line protocol is up
Internet Address 110.1.1.1/24, Area 0.0.0.0
Process ID 10, Router ID 1.1.1.1, Network Type broadcast, Cost: 10
Transmit Delay is 1 sec, State WAIT, Priority 1
BFD enabled(Interface level) Interval 300 Min_rx 300 Multiplier 3 Role
Active
Designated Router (ID) , Interface address 0.0.0.0
Backup Designated router (ID) , Interface address 0.0.0.0
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Neighbor Count is 0, Adjacent neighbor count is 0
```

**支持的版本** 10.2.0E or later

## show ip ospf routes

显示从邻居接收的 OSPF 路由以及开销、下一中继站、区域、接口和路由类型等参数。

**语法** `show ip ospf [process-id] [vrf vrf-name] routes [prefix IP-prefix]`

- 参数**
- *process-id* — (可选) 输入 OSPFv2 进程 ID，以查看特定于 ID 的信息。
  - *vrf vrf-name* — (可选) 输入关键字 *vrf*，后跟 VRF 的名称，以显示在已配置 VRF 中 OSPF 计算的路由。
  - *IP-prefix* — (可选) 指定 IP 地址，以查看特定于 IP 地址的信息。

**默认** 无

**命令模式** EXEC

**使用情况信息** 显示每个邻居和接口的成本指标。

**示例**

```
OS10# show ip ospf 10 routes
Prefix Cost Nexthop Interface Area Type
110.1.1.0 1 0.0.0.0 vlan3050 0.0.0.0 intra-area
111.1.1.0 1 0.0.0.0 vlan3051 0.0.0.0 intra-area
111.2.1.0 1 0.0.0.0 vlan3053 0.0.0.0 intra-area
```

**支持的版本** 10.2.0E or later

## show ip ospf statistics

显示 OSPF 流量统计信息。

**语法** `show ip ospf [instance-number] [vrf vrf-name] statistics [interface interface]`

- 参数**
- *instance-number* — (可选) 输入 OSPF 的实例编号，从 1 到 65535。
  - *vrf vrf-name* — (可选) 输入关键字 *vrf*，后跟 VRF 的名称，以显示与该 VRF 对应的 OSPF 流量统计信息。
  - *interface interface* — (可选) 输入接口信息：
    - *ethernet node/slot/port[:subport]* — 输入以太网端口接口。

- port-channel *number* — 输入端口通道接口编号，从 1 到 128。
- vlan *vlan-id* — 输入 VLAN ID 号，从 1 到 4093。

|        |                                                        |
|--------|--------------------------------------------------------|
| 默认     | 未配置                                                    |
| 命令模式   | EXEC                                                   |
| 使用情况信息 | 此命令将显示指定实例或接口的 OSPFv2 流量统计信息，或者所有 OSPFv2 实例和接口的流量统计信息。 |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show ip ospf 10 statistics Interface vlan3050   Receive Statistics     rx-invalid          0      rx-invalid-bytes      0     rx-hello            0      rx-hello-bytes      0     rx-db-des           0      rx-db-des-bytes     0     rx-ls-req           0      rx-ls-req-bytes     0     rx-ls-upd           0      rx-ls-upd-bytes     0     rx-ls-ack           0      rx-ls-ack-bytes     0   Transmit Statistics     tx-failed           0      tx-failed-bytes     0     tx-hello            0      tx-hello-bytes      0     tx-db-des           0      tx-db-des-bytes     0     tx-ls-req           0      tx-ls-req-bytes     0     tx-ls-upd           0      tx-ls-upd-bytes     0     tx-ls-ack           0      tx-ls-ack-bytes     0   Error packets (Receive statistics)     bad-src             0      dupe-id             0      hello-err     mtu-mismatch        0      nbr-ignored         0      wrong-proto     resource-err        0      bad-lsa-len         0      lsa-bad-type     lsa-bad-len         0      lsa-bad-cksum       0      auth-fail     netmask-mismatch   0      hello-tmr-mismatch  0      dead-ivl-mismatch     options-mismatch    0      nbr-admin-down      0      own-hello-drop     self-orig           0      wrong-length        0      checksum-error     version-mismatch    0      area-mismatch       0</pre> |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|

show ip ospf topology

显示直接连接到 OSPF 区域的路由器。

|        |                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show ip ospf [ <i>process-id</i> ] [ <i>vrf vrf-name</i> ] topology                                                                                                                           |
| 参数     | <ul style="list-style-type: none"><li>• <i>process-id</i> — (可选) 显示 OSPF 进程信息。如果未输入进程 ID，则此操作仅适用于第一个 OSPF 过程。</li><li>• <i>vrf vrf-name</i> — (可选) 在已配置的 VRF 中显示直接连接的 OSPF 区域中的路由器。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                           |
| 命令模式   | EXEC                                                                                                                                                                                          |
| 使用情况信息 | “E”标记输出指示所列的路由器为 ASBR。“B”标记指示所列的路由器为 ABR。如果标记字段同时显示了 E 和 B，则表示所列的路由器同时为 ASBR 和 ABR。                                                                                                           |

|    |                                                                                                                                                                                                                                                                                    |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show ip ospf 10 topology  Router ID      Flags      Cost  Nexthop      Interface  Area 111.111.111.1  -/B/-/    1     111.1.1.2    V1 3051    0 111.111.111.2  -/B/-/    1     111.2.1.2    V1 3053    0 112.2.1.1      E/-/-/    1     110.1.1.2    V1 3050    0</pre> |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|               |        |   |           |         |   |
|---------------|--------|---|-----------|---------|---|
| 112.112.112.1 | -/B/-/ | 2 | 110.1.1.2 | V1 3050 | 0 |
| 112.112.112.2 | -/B/-/ | 2 | 110.1.1.2 | V1 3050 | 0 |

**支持的版本** 10.2.0E or later

## summary-address

为 ASBR 配置一个摘要地址，以通告作为指定地址范围涵盖的所有重新分发路由的聚合的一个外部路由。

**语法** `summary-address ip-address/mask [not-advertise | tag tag-value]`

- 参数**
- `ip-address/mask`— 输入要与掩码一起汇总的 IP 地址。
  - `not-advertise`— (可选) 抑制与网络前缀/掩码不匹配的 IP 地址。
  - `tag-value`— (可选) 输入一个值，以匹配通过路由映射重新分配的路由，从 1 到 65535。

**默认值)** 未配置

**命令模式** ROUTER-OSPF

**使用情况信息** 此命令的 `no` 版本将禁用摘要地址。

**示例**

```
OS10(config)# router ospf 100
OS10(config-router-ospf-100)# summary-address 10.0.0.0/8 not-advertise
```

**支持的版本** 10.3.0E or later

## timers lsa arrival

配置 LSA 验收隔。

**语法** `timers lsa arrival arrival-time`

**参数** `arrival-time` — 设置接收 LSA 之间的间隔 (以毫秒为单位)，从 0 到 600000。

**默认** 1000 毫秒

**命令模式** ROUTER-OSPF

**使用情况信息** 设置在重复接收 LSA 之间的 LSA 到达时间可确保系统获得足够的时间来接受 LSA。此命令的版本 `no` 会将该值重置为默认值。

**示例**

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# timers lsa arrival 2000
```

**支持的版本** 10.2.0E or later

## timers spf

启用最短路径优先 (SPF) 限制，以便在发生拓扑更改时延迟 SPF 计算。

**语法** `timers spf [start-time [hold-time [max-wait]]]`

- 参数**
- `start-time` — 设置初始 SPF 延迟 (以毫秒为单位)，从 1 到 600000；默认值 1000。
  - `hold-time` — 设置两个 SPF 计算之间的额外保留时间，从 1 到 600000；默认值 10000。
  - `max-wait` — 设置两次 SPF 计算之间的最长等待时间，从 1 到 600000；默认值 10000。

- 默认**
- `start-time` — 1000 毫秒
  - `hold-time` — 10000 毫秒
  - `max-wait` — 10000 毫秒

**命令模式** ROUTER-OSPF

**使用情况信息** 默认情况下，OSPF 实例中的 SPF 计时器已禁用。

使用 SPF 限制在网络不稳定期间延迟 SPF 计算。在 OSPF 网络中，拓扑更改事件会在开始时间后触发 SPF 计算。当开始计时器完成时，保留时间可能会延迟另一次 SPF 计算。当挂起计时器正在运行时：

- 每次发生拓扑更改时，SPF 计算会延迟两倍配置的保留时间，最多可达最长等待时间。
- 如果未发生任何拓扑更改，将执行 SPF 计算，并且保留计时器将重置为其配置的值。

如果未指定开始时间、保存时间或最大等待值，则将使用默认值。此命令的 `no` 版本会移除已配置的 SPF 计时器，并在 OSPF 实例中禁用 SPF 限制。

#### 示例

```
OS10(config)# router ospf 100
OS10(config-router-ospf-100)# timers spf 1200 2300 3400
OS10(config-router-ospf-100)# do show ip ospf

Routing Process ospf 100 with ID 12.1.1.1
Supports only single TOS (TOS0) routes
It is Flooding according to RFC 2328
SPF schedule delay 1200 msec, Hold time between two SPF's 2300 msec
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
Area (0.0.0.1)
Number of interface in this area is 1
SPF algorithm executed 1 times
```

#### 支持的版本

10.4.0E(R1) or later

## timers throttle lsa all

配置 LSA 传输间隔。

#### 语法

```
timers lsa all [start-interval | hold-interval | max-interval]
```

#### 参数

- *start-interval* — 设置初始发送和重新发送相同 LSA 的时间间隔（以毫秒为单位），从 0 到 600000。
- *hold-interval* — 设置发送相同 LSA 的下一个间隔（以毫秒为单位）。这是在尝试开始时间间隔后发送相同 LSA 之间的时间，从 1 到 600,000。
- *max-interval* — 设置系统在发送 LSA 之前等待的最长时间（以毫秒为单位），从 1 到 600000。
- 

#### 默认

- 开始-间隔 — 0 毫秒
- 保留-间隔 — 5000 毫秒
- 最大-间隔 — 5000 毫秒

#### 命令模式

ROUTER-OSPF

#### 使用情况信息

此命令的 `no` 版本将移除 LSA 传输计时器。

#### 示例

```
OS10(config)# router ospf 10
OS10(config-router-ospf-10)# timers throttle lsa all 100 300 1000
```

#### 支持的版本

10.2.0E or later

## OSPFv3

OSPFv3 是支持 IPv6 单播地址系列 (AF) 的 IPv6 链路状态路由协议。OSPFv3 默认已禁用。您必须至少配置一个接口（物理或环回）。当为一个或多个接口启用 OSPFv3 时，OSPF 进程将自动启动。除 *area 0* 以外的任何区域都可以为其分配任何数字 ID。

## 启用 OSPFv3

1. 在 CONFIGURATION 模式下全局启用 OSPFv3 并配置 OSPFv3 实例。

```
router ospfv3 instance-number
```

2. 输入接口信息以在 INTERFACE 模式下配置 OSPFv3 接口。

```
interface ethernet node/slot/port[:subport]
```

3. 在 INTERFACE 模式下启用接口。

```
no shutdown
```

4. 禁用默认的交换机端口配置，并将其从接口或 INTERFACE 模式中的 LAG 端口移除。

```
no switchport
```

5. 在 INTERFACE 模式下启用接口上的 OSPFv3。

```
ipv6 ospfv3 process-id area area-id
```

- *process-id* — 输入特定 OSPFv3 进程的 OSPFv3 进程 ID，从 1 到 65535。
- *area-id* — 将 OSPF 区域 ID 输入为 A.B.C.D 格式或数字（从 1 到 65535）的 IP 地址。

### 启用 OSPFv3

```
OS10(config)# router ospfv3 100
OS10(config-router-ospfv3-100)# exit
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# ipv6 ospfv3 300 area 0.0.0.0
```

## 在非默认 VRF 实例中启用 OSPFv3

1. 创建要在其中启用 OSPFv3 的非默认 VRF 实例：

```
ip vrf vrf-name
CONFIGURATION 模式
```

2. 在您之前创建的非默认 VRF 实例中启用 OSPFv3，并在 VRF CONFIGURATION 模式下配置 OSPFv3 实例。

```
router ospfv3 instance-number vrf vrf-name
```

3. 输入接口信息以在 INTERFACE 模式下配置 OSPFv3 接口。

```
interface ethernet node/slot/port[:subport]
```

4. 在 INTERFACE 模式下启用接口。

```
no shutdown
```

5. 禁用默认的交换机端口配置，并将其从接口或 INTERFACE 模式中的 LAG 端口移除。

```
no switchport
```

6. 将接口与您之前创建的非默认 VRF 实例关联。

```
ip vrf forwarding vrf-name
```

7. 在接口上启用 OSPFv3。

```
ipv6 ospfv3 process-id area area-id
```

- *process-id* — 输入特定 OSPFv3 进程的 OSPFv3 进程 ID，从 1 到 65535。

- *area-id* — 将 OSPF 区域 ID 输入为 A.B.C.D 格式或数字 (从 1 到 65535) 的 IP 地址。

## 启用 OSPFv3

```
OS10(config)# ip vrf vrf-blue
OS10(config-vrf-blue)# router ospfv3 100 vrf vrf-blue
OS10(config-router-ospfv3-100)# exit
OS10(config)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# ip vrf forwarding vrf-blue
OS10(conf-if-eth1/1/1)# ipv6 ospfv3 300 area 0.0.0.0
```

### 注:

如果您想要将与一个 VRF 实例相关联的接口移至另一个默认或非默认 VRF 实例, 则必须先删除该接口上已经存在的 OSPF 或 Layer3 配置。如果将接口从一个 VRF 实例移至另一个实例, 而不删除这些现有的 Layer3 或 OSPF 配置, 则这些配置不会在新的 VRF 实例中生效。

请考虑在默认 VRF 实例上配置了 OSPF 实例 100 的情况, 并在名为 VRF-Red 的非默认 VRF 实例上配置 OSPF 实例 200。默认 VRF 实例上的接口 eth1/1/1 连接到 OSPF 进程 100 区域 1。在这种情况下, 如果您想要将 eth1/1/1 从默认 VRF 实例移至 VRF-Red, 则必须先移除接口 eth1/1/1 当前连接到的 OSPF 区域配置。

## 分配路由器 ID

您可以为 OSPFv3 进程分配路由器 ID。为每个路由器配置 IP 地址格式的任意值。每个路由器 ID 必须是唯一的。为活动的 OSPFv3 路由器进程使用固定的路由器 ID。更改路由器 ID 会导致现有 OSPFv3 邻接。新的路由器 ID 将立即变为有效。

- 在 ROUTER-OSPFv3 模式下为 OSPFv3 进程分配路由器 ID

```
router-id ip-address
```

## 分配路由器 ID

```
OS10(config)# router ospfv3 100
OS10(config-router-ospfv3-100)# router-id 10.10.1.5
```

## 查看 OSPFv3 状态

```
OS10# show ipv6 ospf
Routing Process ospfv3 100 with ID 10.10.1.5
It is an Area Border Router
Min LSA origination 5000 msec, Min LSA arrival 1000 msec
Min LSA hold time 0 msec, Max LSA wait time 0 msec
Number of area in this router is 2, normal 2 stub 0 nssa
Area (0.0.0.0)
 Number of interface in this area is 1
 SPF algorithm executed 42 times
Area (0.0.0.1)
 Number of interface in this area is 1
 SPF algorithm executed 42 times
```

## 配置存根区域

类型 5 LSA 不会泛洪至存根区域。ABR 将默认路由通告到它所连接的存根区域。存根区域路由器使用默认路由到达外部目标。

1. 启用 OSPFv3 路由并进入 ROUTER-OSPFv3 模式, 从 1 到 65535。

```
router ospfv3 instance number
```

2. 在 ROUTER-OSPFv3 模式下将区域配置为存根区域。

```
area area-id stub [no-summary]
```

- *area-id* — 采用 A.B.C.D 格式或数字将 OSPFv3 区域 ID 输入为 IP 地址, 从 1 到 65535。



- no-summary — (可选) 输入以防止 ABR 将摘要 LSA 发送到存根区域。

## 配置存根区域

```
OS10(config)# router ospfv3 10
OS10(conf-router-ospf-10)# area 10.10.5.1 stub no-summary
```

## 查看存根区域配置

```
OS10# show running-configuration ospfv3
!
interface ethernet1/1/3
ipv6 ospf 65 area 0.0.0.2
!
router ospfv3 65
area 0.0.0.2 stub no-summary

OS10# show ipv6 ospf database
 OSPF Router with ID (199.205.134.103) (Process ID 65)

Router Link States (Area 0.0.0.2)

ADV Router Age Seq# Fragment ID Link count Bits

199.205.134.103 32 0x80000002 0 1 B
202.254.156.15 33 0x80000002 0 1 B

Net Link States (Area 0.0.0.2)

ADV Router Age Seq# Link ID Rtr count

202.254.156.15 38 0x80000001 12 2

Inter Area Prefix Link States (Area 0.0.0.2)

ADV Router Age Seq# Prefix

202.254.156.15 93 0x80000001 ::/0

Intra Area Prefix Link States (Area 0.0.0.2)

ADV Router Age Seq# Link ID Ref-lstype Ref-LSID

202.254.156.15 34 0x80000003 65536 0x2002 12

Link (Type-8) Link States (Area 0.0.0.2)

ADV Router Age Seq# Link ID Interface

199.205.134.103 42 0x80000001 12 ethernet1/1/3
202.254.156.15 54 0x80000001 12 ethernet1/1/3
```

## 启用被动接口

被动接口是不发送或接收路由信息的接口。将接口配置为被动接口可禁止接收和发送路由更新。

虽然被动接口不会发送或接收路由更新，但该接口上的网络包含在通过其他接口发送的 OSPF 更新中。您可以使用 `no ipv6 ospf passive` 命令从被动接口移除接口。

1. 在 INTERFACE 模式下输入接口类型。

```
interface ethernet node/slot/port[:subport]
```

2. 在 INTERFACE 模式下将接口配置为被动接口。

```
ipv6 ospf passive
```

## 配置被动接口

```
OS10(config)# interface ethernet 1/1/6
OS10(conf-if-eth1/1/6)# ipv6 ospf passive
```

## 查看被动接口

```
OS10# show running-configuraiton
!!!
!!
interface ethernet1/1/1
 ip address 10.10.10.1/24
 no switchport
 no shutdown
 ipv6 ospf 100 area 0
 ipv6 ospf passive
!!
!
```

## 接口 OSPFv3 参数

接口参数值在所有接口之间必须一致，以避免路由错误。例如，为 OSPF 网络中所有路由器上的问候数据包设置相同的时间间隔，以防止 OSPF 邻居配置错误。

1. 输入接口以在 CONFIGURATION 模式下更改 OSPFv3 参数。

```
interface interface-name
```

2. 在 INTERFACE 模式下，将与 OSPFv3 流量相关联的成本更改为 1 到 65535，默认值取决于接口速度。

```
ipv6 ospf cost
```

3. 在 INTERFACE 模式下，更改声明邻居停顿之前路由器等待的时间间隔，从 1 到 65535，默认值为 40。失效间隔必须为问候间隔的四倍。OSPFv3 网络中的所有路由器上的停顿时间间隔必须相同。

```
ipv6 ospf dead-interval seconds
```

4. 在 INTERFACE 模式下，更改问候数据包传输延的时间间隔（以秒为单位），从 1 到 65535，默认值为 10。OSPFv3 网络中的所有路由器上的问候时间间隔必须相同。

```
ipv6 ospf hello-interval seconds
```

5. 在 INTERFACE 模式下更改接口的优先级，以确定 OSPFv3 广播网络的 DR，从 0 到 255，默认值为 1。

```
ipv6 ospf priority number
```

## 更改 OSPFv3 接口参数

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 ospf hello-interval 5
OS10(conf-if-eth1/1/1)# ipv6 ospf dead-interval 20
OS10(conf-if-eth1/1/1)# ipv6 ospf priority 4
```

## 查看 OSPFv3 接口参数

```
OS10# show ipv6 ospf interface
ethernet1/1/1 is up, line protocol is up
 Link Local Address fe80::20c:29ff:fe0a:d59/64, Interface ID 5
 Area 0.0.0.0, Process ID 200, Instance ID 0, Router ID 10.0.0.2
 Network Type broadcast, Cost: 1
 Transmit Delay is 1 sec, State BDR, Priority 1
 Designated Router on this network is 2.2.2.2
 Backup Designated router on this network is 10.0.0.2 (local)
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 2.2.2.2(Designated Router)
```

## 默认路由

您可以生成外部默认路由并将默认信息分发至 OSPFv3 路由域。

- 在 OSPFv3 模式下使用 `default-information originate [always]` 命令生成默认路由。

### 配置默认路由

```
OS10(config)# router ospfv3 100
OS10(config-router-ospf-100)# default-information originate always
```

### 查看默认路由配置

```
OS10(config-router-ospf-100)# show configuration
!
router ospfv3 100
 default-information originate always
```

## OSPFv3 IPsec 身份验证和加密

与 OSPFv2 不同，OSPFv3 在其协议标头中没有身份验证字段来提供安全性。为了提供身份验证和机密性，OSPFv3 使用 IP 安全 (IPsec) — 一组用于对数据包进行身份验证和加密的安全协议。OS10 OSPFv3 使用 IPv6 身份验证标头 (AH) 或 IPv6 封装安全有效负载 (ESP) 来支持 IPsec。

- AH 身份验证会验证数据在传输过程中不会更改，并确保用户与预期的个人或组织进行通信。在 IP 标头之后插入身份验证标头，其值为 51。支持 MD5 和 SHA1 身份验证类型；支持加密和未加密密钥。
- ESP 加密可封装数据，从而实现数据报中遵循的数据保护。在 IP 标头之后和下一个层协议标头之前已插入 ESP 扩展名标头。支持 3DES、DES、AES-CBC 和 NULL 加密算法；支持加密和未加密密钥。

在物理、端口通道或 VLAN 接口上或在 OSPFv3 区域中应用 IPsec 身份验证或加密。每个配置包含一个安全策略索引 (SPI) 和 OSPFv3 数据包验证密钥。配置 OSPFv3 的 IPsec 协议后，IPsec 操作对用户不可见。

您一次只能在一个接口或某个区域上启用一种身份验证或加密安全协议。使用 `ipv6 ospf authentication` 命令启用 IPsec AH；使用 `ipv6 ospf encryption` 命令启用 IPsec ESP。

- 默认情况下，将在该区域中的所有接口上继承为区域配置的安全策略。
- 在接口上配置的安全策略将覆盖为其分配接口的区域的任何区域级别配置的安全性。
- 已配置的身份验证或加密策略适用于在接口或区域中传输的所有 OSPFv3 数据包。OSPFv3 接口上的入站和出站流量中的 IPsec 安全关联相同。
- 由于标头包含具有可变长度的字段，因此没有最大 AH 或 ESP 标头长度。

## 在接口上配置 IPsec 身份验证

**前提条件：**在 OSPFv3 接口上启用 IPsec 身份验证之前，必须在全局范围内启用 IPv6 单播路由、启用接口上的 OSPFv3，并将其分配给某个区域。

对于路由器上的一个 IPsec 身份验证或加密安全策略，SPI 值必须是唯一的。您不能在另一个接口上配置相同的 SPI 值，即使它使用相同的身份验证或加密算法也是如此。

您不能在接口上同时使用 IPsec MD5 或 SHA1 身份验证类型和 `null` 设置。这些设置相互排斥。

- 在接口模式下为 OSPFv3 数据包启用 IPsec 身份验证。

```
ipv6 ospf authentication {null | ipsec spi number {MD5 | SHA1} key}
```

- `null` — 禁止在接口上继承为区域配置的身份验证策略。只有在配置 IPsec 区域身份验证时，才能使用此参数。
- `ipsec spi number` — 输入一个唯一的安全策略索引 (SPI) 值，从 256 到 4294967295。
- `md5` — 启用消息摘要 5 (MD5) 身份验证。
- `sha1` — 启用安全哈希算法 1 (SHA-1) 身份验证。
- `key` — 输入在验证类型中使用的文本字符串。所有邻接的 OSPFv3 路由器必须共享密钥以交换信息。仅支持非加密密钥。对于 MD5 身份验证，非加密的密钥必须是 32 位明文十六进制数字。对于 SHA-1 身份验证，非加密密钥必须是 40 位十六进制数字。不支持加密密钥。

要删除 IPsec 身份验证策略，请使用 `no ipv6 ospf authentication ipsec spi number` 或 `no ipv6 ospf authentication null` 命令。

## 在接口上配置 IPsec 身份验证

```
OS10(conf-if-eth1/1/1)# ipv6 ospf authentication ipsec spi 400 md5
12345678123456781234567812345678
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
ipv6 ospf authentication ipsec spi 400 md5 12345678123456781234567812345678
no switchport
no shutdown
ipv6 address 1::1/64
```

## 接口上的 IPsec 加密

**前提条件:** 在 OSPFv3 接口上启用 IPsec 加密之前, 必须在全局范围内启用 IPv6 单播路由、启用接口上的 OSPFv3, 并将其分配给某个区域。

在接口上配置加密时, 同时启用了 IPsec 加密和身份验证。如果您已使用 `ipv6 ospf authentication ipsec` 命令配置了用于 IPsec 身份验证的接口, 则不能配置加密。要配置加密, 必须先删除身份验证策略。

- 在接口模式下为 OSPFv3 数据包启用 IPsec 加密。

```
ipv6 ospf encryption ipsec spi number esp encryption-type
key authentication-type key
```

- `ipsec spi number` — 输入一个唯一的安全策略索引 (SPI) 值, 从 256 到 4294967295。
- `esp encryption-type key` — 输入与 ESP (3DES、DES、AES 或 NULL) 一起使用的加密算法。对于 AES-CBC, 仅支持 AES-128 和 AES-192 密码。
- `key` — 输入加密算法中使用的文本字符串。所有邻接的 OSPFv3 路由器必须共享密钥以加密信息。仅支持非加密密钥。非加密密钥的所需长度为: 3DES-48 位十六进制数字; DES — 16 位十六进制数字; AES-CBC — 32 位十六进制数字适用于 AES-128, 48 位十六进制数字适用于 AES-192。
- `authentication-type key` — 输入要使用的加密身份验证 MD5 或 SHA1 算法。
- `key` — 输入身份验证算法中使用的文本字符串。所有邻接的 OSPFv3 路由器必须共享密钥以交换信息。仅支持非加密密钥。对于 MD5 身份验证, 非加密的密钥必须是 32 位明文十六进制数字。对于 SHA1 身份验证, 非加密密钥必须是 40 位十六进制数字。不支持加密密钥。

要删除 IPsec 加密策略, 请使用 `no ipv6 ospf encryption ipsec spi number` 或 `no ipv6 ospf encryption null` 命令。

## 在接口上配置 IPsec 加密

```
OS10(conf-if-eth1/1/1)# ipv6 ospf encryption ipsec spi 500 esp des 1234567812345678 md5
12345678123456781234567812345678
OS10(conf-if-eth1/1/1)# show configuration
!
interface ethernet1/1/1
ipv6 ospf encryption ipsec spi 500 esp des 1234567812345678 md5
12345678123456781234567812345678
no switchport
no shutdown
ipv6 address 1::1/64
```

## 配置 OSPFv3 的 IPsec 身份验证区域

**前提条件:** 在为 OSPFv3 区域启用 IPsec 身份验证之前, 必须在每个路由器上全局启用 OSPFv3。

- 在路由器 OSPFv3 模式下为区域中的 OSPFv3 数据包启用 IPsec 身份验证。

```
area area-id authentication ipsec spi number {MD5 | SHA1} key
```

- `area area-id` — 输入区域 ID 作为编号或 IPv6 前缀。
- `ipsec spi number` — 输入一个唯一的安全策略索引 (SPI) 值, 从 256 到 4294967295。
- `md5` — 启用消息摘要 5 (MD5) 身份验证。
- `sha1` — 启用安全哈希算法 1 (SHA1) 身份验证。

- *key* — 输入在验证类型中使用的文本字符串。该区域中所有 OSPFv3 路由器共享该密钥以交换信息。仅支持非加密密钥。对于 MD5 身份验证，非加密的密钥必须是 32 位明文十六进制数字。对于 SHA1 身份验证，非加密密钥必须是 40 位十六进制数字。不支持加密密钥。

要删除 IPsec 身份验证策略，请使用 `no area area-id authentication ipsec spi number` 命令。

### 为 OSPFv3 区域配置 IPsec 身份验证

```
OS10(config-router-ospfv3-100)# area 1 authentication ipsec spi 400 md5
12345678123456781234567812345678
OS10(config-router-ospfv3-100)# show configuration
!
router ospfv3 100
area 0.0.0.1 authentication ipsec spi 400 md5 12345678123456781234567812345678
```

## OSPFv3 区域的 IPsec 加密

**前提条件：**在为 OSPFv3 区域启用 IPsec 加密之前，必须在每个路由器上全局启用 OSPFv3。

在区域级别配置加密时，同时启用 IPsec 加密和身份验证。如果已使用 `area ospf authentication ipsec` 命令配置了 IPsec 区域身份验证，则不能配置加密。要配置加密，必须先删除身份验证策略。

- 在路由器 OSPFv3 模式下为区域中的 OSPFv3 数据包启用 IPsec 加密。

```
area area-id encryption ipsec spi number esp encryption-type key
authentication-type key
```

- *area area-id* — 输入区域 ID 作为编号或 IPv6 前缀。
- *ipsec spi number* — 输入一个唯一的安全策略索引 (SPI) 值，从 256 到 4294967295。
- *esp encryption-type* — 输入与 ESP (3DES、DES、AES 或 NULL) 一起使用的加密算法。对于 AES-CBC，仅支持 AES-128 和 AES-192 密码。
- *key* — 输入加密算法中使用的文本字符串。所有邻接的 OSPFv3 路由器必须共享密钥以加密信息。仅支持非加密密钥。非加密密钥的所需长度为：3DES-48 位十六进制数字；DES — 16 位十六进制数字；AES-CBC — 32 位十六进制数字适用于 AES-128，48 位十六进制数字适用于 AES-192。
- *authentication-type* — 输入要使用的加密身份验证 MD5 或 SHA1 算法。
- *key* — 输入身份验证算法中使用的文本字符串。所有邻接的 OSPFv3 路由器必须共享密钥以交换信息。仅支持非加密密钥。对于 MD5 身份验证，非加密的密钥必须是 32 位明文十六进制数字。对于 SHA1 身份验证，非加密密钥必须是 40 位十六进制数字。不支持加密密钥。

要删除 IPsec 加密策略，请使用 `no area area-id encryption ipsec spi number` 命令。

### 配置 OSPFv3 区域的 IPsec 加密

```
OS10(config-router-ospfv3-100)# area 1 encryption ipsec spi 401 esp des 1234567812345678
md5
12345678123456781234567812345678
OS10(config-router-ospfv3-100)# show configuration
!
router ospfv3 100
area 0.0.0.1 encryption ipsec spi 401 esp des 1234567812345678 md5
12345678123456781234567812345678
```

## OSPFv3 故障处理

您可以对 OSPFv3 操作进行故障处理，并查看有关中断进程的典型问题。

- 是否全局启用 OSPFv3？
- 在接口上是否已启用 OSPFv3？
- 是否正确建立了邻区？
- 是否已针对 L3 正确配置了接口？
- 路由器是否是正确的区域类型？
- OSPF 数据库中是否包括 OSPF 路由？
- 除了 OSPF 数据库外，路由表中是否还包括 OSPF 路由？
- 是否可以对相邻路由器接口的链路本地 IPv6 地址执行 ping 命令？

## 使用 show 命令对 OSPFv3 进行故障处理

- 查看在 EXEC 模式下已启用的所有 OSPF 进程 ID 的摘要。

```
show running-configuration ospfv3
```

- 以 EXEC 模式查看 IP 路由的摘要信息。

```
show ipv6 route summary
```

- 以 EXEC 模式查看 OSPF 数据库的摘要信息。

```
show ipv6 ospf database
```

- 以 EXEC 模式查看连接到本地路由器的 OSPF 邻居的配置。

```
show ipv6 ospf neighbor
```

## 查看 OSPF 配置

```
OS10# show running-configuration ospfv3
!
interface ethernet1/1/1
ip ospf 100 area 0.0.0.0
!
router ospf 100
log-adjacency-changes
```

## OSPFv3 命令

### area authentication

为 OSPFv3 区域配置身份验证。

|        |                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>area area-id authentication ipsec spi number {MD5   SHA1} key</code>                                                                                                                                                                                                                                                     |
| 参数     | <ul style="list-style-type: none"><li>• <code>area area-id</code> — 输入区域 ID 作为编号或 IPv6 前缀。</li><li>• <code>ipsec spi number</code> — 输入一个唯一的安全策略索引 (SPI) 值, 从 256 到 4294967295。</li><li>• <code>md5</code> — 启用 MD5 身份验证。</li><li>• <code>sha1</code> — 启用 SHA1 身份验证。</li><li>• <code>key</code> — 输入在验证类型中使用的文本字符串。</li></ul> |
| 默认     | 未配置 OSPFv3 区域身份验证。                                                                                                                                                                                                                                                                                                             |
| 命令模式   | ROUTER-OSPFv3                                                                                                                                                                                                                                                                                                                  |
| 使用情况信息 | <ul style="list-style-type: none"><li>• 在为 OSPFv3 区域启用 IPsec 身份验证之前, 必须在每个路由器上全局启用 OSPFv3。</li><li>• 该区域中所有 OSPFv3 路由器必须共享相同的身份验证密钥以交换信息。仅支持非加密密钥。对于 MD5 身份验证, 非加密的密钥必须是 32 位明文十六进制数字。对于 SHA1 身份验证, 非加密密钥必须是 40 位十六进制数字。不支持加密密钥。</li></ul>                                                                                     |
| 示例     | <pre>OS10(config-router-ospfv3-100)# area 1 authentication ipsec spi 400 md5 1234567812345678123456781234567812345678</pre>                                                                                                                                                                                                    |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                                                                                                                                                           |

### area encryption

配置 OSPFv3 区域的加密。

|    |                                                                                                       |
|----|-------------------------------------------------------------------------------------------------------|
| 语法 | <code>area area-id encryption ipsec spi number esp encryption-type key authentication-type key</code> |
| 参数 | <ul style="list-style-type: none"><li>• <code>area area-id</code> — 输入区域 ID 作为编号或 IPv6 前缀。</li></ul>  |

- `ipsec spi number` — 输入一个唯一的安全策略索引号，从 256 到 4294967295。
- `esp encryption-type` — 输入与 ESP (3DES、DES、AES 或 NULL) 一起使用的加密算法。对于 AES-CBC，仅支持 AES-128 和 AES-192 密码。
- `key` — 输入加密算法中使用的文本字符串。
- `authentication-type` — 输入要使用的加密身份验证 MD5 或 SHA1 算法。
- `key` — 输入身份验证算法中使用的文本字符串。

**默认** OSPFv3 区域加密未配置。

**命令模式** ROUTER-OSPFv3

**使用情况信息**

- 在为 OSPFv3 区域启用 IPsec 加密之前，必须在每个路由器上全局启用 OSPFv3。
- 在区域级别配置加密时，同时启用 IPsec 加密和身份验证。如果已使用 `area ospf authentication ipsec` 命令配置了 IPsec 区域身份验证，则不能配置加密。要配置加密，必须先删除身份验证策略。
- 该区域中所有 OSPFv3 路由器必须共享相同的加密密钥以解密信息。仅支持非加密密钥。非加密密钥的所需长度为：3DES-48 位十六进制数字；DES — 16 位十六进制数字；AES-CBC — 32 位十六进制数字适用于 AES-128，48 位十六进制数字适用于 AES-192。
- 该区域中所有 OSPFv3 路由器必须共享相同的身份验证密钥以交换信息。仅支持非加密密钥。对于 MD5 身份验证，非加密的密钥必须是 32 位明文十六进制数字。对于 SHA1 身份验证，非加密密钥必须是 40 位十六进制数字。不支持加密密钥。

**示例**

```
OS10(config-router-ospfv3-100)# area 1 encryption ipsec spi 401 esp des
1234567812345678 md5
12345678123456781234567812345678
```

**支持的版本** 10.4.0E(R1) or later

## area stub

将区域定义为 OSPF 存根区域。

**语法** `area area-id stub [no-summary]`

**参数**

- `area-id` — 采用 A.B.C.D 格式或数字将 OSPFv3 区域 ID 设置为 IP 地址，从 1 到 65535。
- `no-summary` — (可选) 防止 ABR 将摘要发送至存根区域。

**默认** 未配置

**命令模式** ROUTER-OSPFv3

**使用情况信息** 此命令的 `no` 版本将删除存根区域。

**示例**

```
OS10(config)# router ospfv3 10
OS10(conf-router-ospfv3-10)# area 10.10.1.5 stub
```

**支持的版本** 10.3.0E or later

## auto-cost reference-bandwidth

基于配置的自动成本参考带宽值计算接口的默认指标。

**语法** `auto-cost reference-bandwidth value`

**参数** `value` — 输入参考带宽值以计算 OSPFv3 接口成本 (以每秒兆位数为单位)，从 1 到 4294967。

**默认** 100000

**命令模式** ROUTER-OSPFv3

**使用情况信息** 在 INTERFACE 模式下通过 `ipv6 ospf cost` 命令设置的值将覆盖通过 `auto-cost` 命令所产生的成本。此命令的 `no` 版本会将该值重置为默认值。



|       |                                                                                                              |
|-------|--------------------------------------------------------------------------------------------------------------|
| 示例    | <pre>OS10(config)# router ospfv3 100 OS10(config-router-ospfv3-100)# auto-cost reference-bandwidth 150</pre> |
| 支持的版本 | 10.3.0E or later                                                                                             |

### clear ipv6 ospf process

清除所有 OSPFv3 路由表。

|        |                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>clear ipv6 ospf {instance-number} [vrf vrf-name] process</code>                                                                                                                                           |
| 参数     | <ul style="list-style-type: none"> <li><code>instance-number</code> — 输入 OSPFv3 实例编号，从 1 到 65535。</li> <li><code>vrf vrf-name</code> — (可选) 输入关键字 <code>vrf</code>，后跟 VRF 的名称，以清除该 VRF 中的 OSPFv3 进程。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                             |
| 命令模式   | EXEC                                                                                                                                                                                                            |
| 使用情况信息 | 无                                                                                                                                                                                                               |
| 示例     | <pre>OS10# clear ipv6 ospf 3 process</pre>                                                                                                                                                                      |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                |

### clear ipv6 ospf statistics

清除 OSPFv3 流量统计信息。

|        |                                                                                                                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>clear ipv6 ospf [instance-number] [vrf vrf-name] statistics</code>                                                                                                                                               |
| 参数     | <ul style="list-style-type: none"> <li><code>instance-number</code> — (可选) 输入 OSPFv3 实例编号，从 1 到 65535。</li> <li><code>vrf vrf-name</code> — (可选) 输入关键字 <code>VRF</code>，后跟 VRF 的名称，以清除该 VRF 中的 OSPFv3 统计信息。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                    |
| 命令模式   | EXEC                                                                                                                                                                                                                   |
| 使用情况信息 | 此命令清除指定实例或所有已配置的 OSPFv3 实例中的 OSPFv3 流量统计信息，并将其重置为零。                                                                                                                                                                    |
| 示例     | <pre>OS10# clear ipv6 ospf 100 statistics</pre>                                                                                                                                                                        |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                                                   |

### debug ip ospfv3

启用开放式最短路径优先第 3 版 (OSPFv3) 调试，并显示与 OSPFv3 处理相关的消息。

|        |                                                         |
|--------|---------------------------------------------------------|
| 语法     | <code>debug ip ospfv3</code>                            |
| 参数     | 无                                                       |
| 默认     | 无                                                       |
| 命令模式   | EXEC                                                    |
| 使用情况信息 | <code>no debug ip ospfv3</code> 命令将停止显示与处理 OSPFv3 相关的消息 |
| 示例     | <pre>debug ip ospfv3</pre>                              |
| 支持的版本  | OS10 原有命令。                                              |



## default-information originate

生成默认的外部路由信息并分发给 OSPFv3 路由域。

**语法** `default-information originate [always]`

**参数** `always` — (可选) 始终通告默认路由。

**默认** 已禁用

**命令模式** ROUTER-OSPFv3

**使用情况信息** 此命令的 `no` 版本将禁用默认路由的分布。

**示例**

```
OS10(config)# router ospfv3 100
OS10(config-router-ospfv3-100)# default-information originate always
```

**支持的版本** 10.3.0E or later

## ipv6 ospf area

将接口连接到 OSPF 区域。

**语法** `ipv6 ospf process-id area area-id`

**参数**

- `process-id` — 输入特定 OSPFv3 进程的 OSPFv3 进程 ID, 从 1 到 65535。
- `area-id` — 以点分隔的十进制 A.B.C.D 格式输入 OSPFv3 区域 ID, 或者输入一个从 1 到 65535 的区域 ID 号。

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息** 此命令的 `no` 版本将从 OSPFv3 区域中移除接口。

**示例**

```
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)# ipv6 ospf 10 area 1
```

**支持的版本** 10.3.0E or later

## ipv6 ospf authentication

在 IPv6 接口上配置 OSPFv3 身份验证。

**语法** `ipv6 ospf authentication {null | ipsec spi number {MD5 | SHA1} key}`

**参数**

- `null` — 防止在接口上继承区域身份验证。
- `ipsec spi number` — 输入一个唯一的安全策略索引号, 从 256 到 4294967295。
- `md5` — 启用 MD5 身份验证。
- `sha1` — 启用 SHA1 身份验证。
- `key` — 输入身份验证类型使用的文本字符串。

**默认** 未在接口上配置 IPv6 OSPF 身份验证。

**命令模式** INTERFACE

**使用情况信息**

- 在 OSPFv3 接口上启用 IPsec 身份验证之前, 必须在全局范围内启用 IPv6 单播路由、配置 IPv6 地址并启用接口上的 OSPFv3, 并将其分配给某个区域。
- 对于路由器上的一个 IPsec 身份验证或加密安全策略, SPI 值必须是唯一的。您不能在另一个接口上配置相同的 SPI 值, 即使它使用相同的身份验证或加密算法也是如此。
- 您不能在接口上同时使用 IPsec MD5 或 SHA1 身份验证类型和 `null` 设置。这些设置相互排斥。
- 所有邻接的 OSPFv3 路由器必须共享密钥以交换信息。仅支持非加密密钥。对于 MD5 身份验证, 非加密的密钥必须是 32 位明文十六进制数字。对于 SHA1 身份验证, 非加密密钥必须是 40 位十六进制数字。不支持加密密钥。

## 示例

```
OS10(config)# interface ethernet 1/1/6
OS10(conf-if-eth1/1/6)# ipv6 ospf authentication ipsec spi 400 md5
12345678123456781234567812345678
```

## 支持的版本

10.4.0E(R1) or later

## ipv6 ospf cost

更改与接口上的 OSPFv3 流量关联的成本

### 语法

`ipv6 ospf cost cost`

### 参数

*cost* — 输入一个值作为接口的 OSPFv3 成本，从 1 到 65535。

### 默认

基于带宽参考

### 命令模式

INTERFACE

### 使用情况信息

如果未配置，接口成本将基于 `auto-cost` 命令。此命令可通过多个供应商配置 OSPFv3，以确保所有路由器使用相同的成本值。此命令的 `no` 版本会删除 IPv6 OSPF 成本配置。

## 示例

```
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)# ipv6 ospf cost 10
```

## 支持的版本

10.3.0E or later

## ipv6 ospf dead-interval

设置自从路由器收到上次问候数据包以来的时间间隔。超过该时间间隔后，相邻路由器会将路由器声明为失效。

### 语法

`ipv6 ospf dead-interval seconds`

### 参数

*seconds* — 输入停顿间隔值（以秒为单位），从 1 到 65535。

### 默认

40 秒

### 命令模式

INTERFACE

### 使用情况信息

默认情况下，停顿间隔为默认呼叫间隔的四倍。此命令的 `no` 版本会将该值重置为默认值。

## 示例

```
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)# ipv6 ospf dead-interval 10
```

## 支持的版本

10.3.0E or later

## ipv6 ospf encryption

在 IPv6 接口上配置 OSPFv3 加密。

### 语法

`ipv6 ospf encryption {ipsec spi number esp encryption-type key authentication-type key | null}`

### 参数

- *ipsec spi number* — 输入一个唯一的安全策略索引号，从 256 到 4294967295。
- *esp encryption-type* — 输入与 ESP (3DES、DES、AES 或 NULL) 一起使用的加密算法。对于 AES-CBC，仅支持 AES-128 和 AES-192 密码。
- *key* — 输入加密算法中使用的文本字符串。
- *authentication-type* — 输入要使用的加密 MD5 或 SHA1 身份验证算法。
- *key* — 输入身份验证算法中使用的文本字符串。
- *null* — 输入不使用 IPsec 加密的关键字。

### 默认

未在接口上配置 IPv6 OSPF 加密。

### 命令模式

INTERFACE

## 使用情况信息

- 在 OSPFv3 接口上启用 IPsec 身份验证之前，必须在全局范围内启用 IPv6 单播路由、配置 IPv6 地址并启用接口上的 OSPFv3，并将其分配给某个区域。
- 在接口上配置加密时，同时启用了 IPsec 加密和身份验证。如果您已使用 `ipv6 ospf authentication ipsec` 命令配置了用于 IPsec 身份验证的接口，则不能配置加密。要配置加密，必须先删除身份验证策略。
- 所有邻接的 OSPFv3 路由器必须共享相同的加密密钥以解密信息。仅支持非加密密钥。非加密密钥的所需长度为：3DES-48 位十六进制数字；DES — 16 位十六进制数字；AES-CBC — 32 位十六进制数字适用于 AES-128，48 位十六进制数字适用于 AES-192。
- 所有邻接的 OSPFv3 路由器必须共享相同的身份验证密钥以交换信息。仅支持非加密密钥。对于 MD5 身份验证，非加密的密钥必须是 32 位明文十六进制数字。对于 SHA1 身份验证，非加密密钥必须是 40 位十六进制数字。不支持加密密钥。

## 示例

```
OS10(config)# interface ethernet 1/1/6
OS10(conf-if-eth1/1/6)# ipv6 ospf encryption ipsec spi 500 esp des
1234567812345678 md5 12345678123456781234567812345678
```

```
OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# ipv6 ospf encryption null
```

## 支持的版本

10.4.0E(R1) or later

## ipv6 ospf hello-interval

设置在接口上发送的问候数据包之间的时间间隔。

**语法** `ipv6 ospf hello-interval seconds`

**参数** `seconds` — 输入问候间隔值（以秒为单位），从 1 到 65535。

**默认** 10 秒

**命令模式** INTERFACE

**使用情况信息** 网络中的所有路由器都必须具有与问候数据包相同的问候时间间隔。此命令的 `no` 版本会将该值重置为默认值。

## 示例

```
OS10(config)# interface vlan 10
OS10(conf-if-vl-10)# ipv6 ospf hello-interval 30
```

## 支持的版本

10.3.0E or later

## ipv6 ospf network

设置接口的网络类型。

**语法** `ipv6 ospf network {point-to-point | broadcast}`

- 参数**
- `point-to-point` — 将接口设置为点对点网络的一部分。
  - `broadcast` — 将接口设置为广播网络的一部分。

**默认** 广播

**命令模式** INTERFACE

**使用情况信息** 此命令的 `no` 版本会将该值重置为默认值。

## 示例

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ipv6 ospf network broadcast
```

## 支持的版本

10.3.0E or later

### ipv6 ospf passive

将接口配置为被动接口，并禁止接收和发送到被动接口的路由更新。

|        |                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | ipv6 ospf passive                                                                                                                                                                                                                          |
| 参数     | 无                                                                                                                                                                                                                                          |
| 默认     | 未配置                                                                                                                                                                                                                                        |
| 命令模式   | INTERFACE                                                                                                                                                                                                                                  |
| 使用情况信息 | 必须先配置接口，然后才能将接口设置为被动模式。此命令的 no 版本将禁用被动接口配置。<br> <b>注：</b> 由于环回接口为隐式被动，因此不会在环回接口上影响发送和接收 OSPF 路由更新的配置。但是，与这些环回接口相对应的网络信息仍在通过 OSPF 配置的其他接口发送的 OSPF LSA 中发布。 |
| 示例     | <pre>OS10(config)# interface ethernet 1/1/6 OS10(conf-if-eth1/1/6)# ipv6 ospf passive</pre>                                                                                                                                                |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                           |

### ipv6 ospf priority

设置接口的优先级，以确定 OSPFv3 网络的灾难恢复。

|        |                                                                                                |
|--------|------------------------------------------------------------------------------------------------|
| 语法     | ipv6 ospf priority <i>number</i>                                                               |
| 参数     | <i>number</i> — 输入路由器优先级编号，从 0 到 255。                                                          |
| 默认     | 1                                                                                              |
| 命令模式   | INTERFACE                                                                                      |
| 使用情况信息 | 当连接到网络的两个路由器尝试成为灾难恢复时，具有更高路由器优先级的路由器优先。此命令的 no 版本会将该值重置为默认值。                                   |
| 示例     | <pre>OS10(config)# interface ethernet 1/1/6 OS10(conf-if-eth1/1/6)# ipv6 ospf priority 4</pre> |
| 支持的版本  | 10.3.0E or later                                                                               |

### log-adjacency-changes

启用对 OSPFv3 邻接状态更改的 syslog 消息的日志记录。

|        |                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------|
| 语法     | log-adjacency-changes                                                                            |
| 参数     | 无                                                                                                |
| 默认     | 已禁用                                                                                              |
| 命令模式   | ROUTER-OSPFv3                                                                                    |
| 使用情况信息 | 此命令的版本 no 会将该值重置为默认值。                                                                            |
| 示例     | <pre>OS10(config)# router ospfv3 100 OS10(config-router-ospfv3-100)# log-adjacency-changes</pre> |
| 支持的版本  | 10.3.0E or later                                                                                 |

## maximum-paths

允许转发多个路径上的数据包。

|        |                                                                                        |
|--------|----------------------------------------------------------------------------------------|
| 语法     | <code>maximum-paths number</code>                                                      |
| 参数     | <i>number</i> — 输入 OSPFv3 的路径数量 (从 1 到 128)。                                           |
| 默认     | 已禁用                                                                                    |
| 命令模式   | ROUTER-OSPFv3                                                                          |
| 使用情况信息 | 此命令的 <code>no</code> 版本会将该值重置为默认值。                                                     |
| 示例     | <pre>OS10(config)# router ospfv3 OS10(config-router-ospfv3-100)# maximum-paths 1</pre> |
| 支持的版本  | 10.3.0E or later                                                                       |

## redistribute

将来自另一个路由协议或路由实例的信息重新分配到 OSPFv3 进程。

|          |                                                                                                                                                                                                                                                                         |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法       | <code>redistribute {bgp as-number   connected   static} [route-map route-map name]</code>                                                                                                                                                                               |
| 参数       | <ul style="list-style-type: none"><li><i>as-number</i> — 输入自治编号以重新分发整个 OSPFv3 实例的 BGP 路由信息, 从 1 到 4294967295。</li><li><i>route-map name</i> — 输入已配置的路由映射的名称。</li><li><i>connected</i> — 输入要重新分发的接口上来自连接的活动路由的信息。</li><li><i>static</i> — 输入重新分发的接口上来自静态路由的信息。</li></ul> |
| 默认       | 未配置                                                                                                                                                                                                                                                                     |
| 命令模式     | ROUTER-OSPFv3                                                                                                                                                                                                                                                           |
| 使用情况信息   | 重新分发 OSPFv3 时, 不会从 BGP 配置中完全移除该进程。此命令的 <code>no</code> 版本将禁用重新分发配置。                                                                                                                                                                                                     |
| 示例       | <pre>OS10(config)# router ospfv3 100 OS10(config-router-ospfv3-100)# redistribute bgp 4 route-map dell1</pre>                                                                                                                                                           |
| 示例 (已连接) | <pre>OS10((config-router-ospfv3-100)# redistribute connected route-map dell2</pre>                                                                                                                                                                                      |
| 支持的版本    | 10.3.0E or later                                                                                                                                                                                                                                                        |

## router-id

为 OSPFv3 进程配置固定的路由器 ID。

|        |                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>router-id ip-address</code>                                                                                                                |
| 参数     | <i>ip-address</i> — 输入路由器的 IP 地址作为路由器 ID。                                                                                                        |
| 默认     | 未配置                                                                                                                                              |
| 命令模式   | ROUTER-OSPFv3                                                                                                                                    |
| 使用情况信息 | 为每个路由器配置 IP 地址格式的任意值。每个路由器 ID 必须是唯一的。为活动的 OSPFv3 路由器进程使用固定的路由器 ID。更改路由器 ID 会导致现有 OSPFv3 邻接。新的路由器 ID 将立即变为有效。此命令的 <code>no</code> 版本将禁用路由器 ID 配置。 |
| 示例     | <pre>OS10(config)# router ospfv3 10 OS10(config-router-ospfv3-100)# router-id 10.10.1.5</pre>                                                    |
| 支持的版本  | 10.3.0E or later                                                                                                                                 |

## router ospfv3

进入路由器 OSPFv3 模式并配置 OSPFv3 实例。

|        |                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>router ospfv3 instance-number [vrf vrf-name]</code>                                                                                                                                                    |
| 参数     | <ul style="list-style-type: none"><li><code>instance-number</code>— 输入路由器 OSPFv3 实例编号, 从 1 到 65535。</li><li><code>vrf vrf-name</code>— 输入关键字 <code>vrf</code>, 后跟 VRF 的名称, 以便在该 VRF 中配置 OSPFv3 实例。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                          |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                |
| 使用情况信息 | 此命令的 <code>no</code> 版本将删除 OSPFv3 实例。                                                                                                                                                                        |
| 示例     | <pre>OS10(config)# router ospfv3 10 vrf vrf-test</pre>                                                                                                                                                       |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                             |

## show ipv6 ospf

显示 OSPFv3 实例配置信息。

|        |                                                                       |
|--------|-----------------------------------------------------------------------|
| 语法     | <code>show ipv6 ospf [instance-number]</code>                         |
| 参数     | <code>instance-number</code> — (可选) 查看指定实例编号的 OSPFv3 信息, 从 1 到 65535。 |
| 默认     | 无                                                                     |
| 命令模式   | EXEC                                                                  |
| 使用情况信息 | 无                                                                     |
| 示例     |                                                                       |

```
OS10# show ipv6 ospf
Routing Process ospfv3 200 with ID 1.1.1.1
It is an Area Border Router
Min LSA origination 5000 msec, Min LSA arrival 1000 msec
Min LSA hold time 0 msec, Max LSA wait time 0 msec
Number of area in this router is 2, normal 2 stub 0 nssa
 Area (0.0.0.0)
 Number of interface in this area is 1
 SPF algorithm executed 42 times
 Area (0.0.0.1)
 Number of interface in this area is 1
 SPF algorithm executed 42 times
OS10# show ipv6 ospf 200
Routing Process ospfv3 200 with ID 10.0.0.2
Min LSA origination 5000 msec, Min LSA arrival 1000 msec
Min LSA hold time 0 msec, Max LSA wait time 0 msec
Number of area in this router is 1, normal 1 stub 0 nssa
 Area (0.0.0.0)
 Number of interface in this area is 1
 SPF algorithm executed 3 times
```

|       |                  |
|-------|------------------|
| 支持的版本 | 10.3.0E or later |
|-------|------------------|

## show ipv6 ospf database

显示所有 LSA 信息。必须启用 OSPFv3 才能生成输出。

|    |                                                                                                                                                                                                                               |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>show ipv6 ospf process-id [vrf vrf-name] database</code>                                                                                                                                                                |
| 参数 | <ul style="list-style-type: none"><li><code>process-id</code>— 输入 OSPFv3 进程 ID 以查看特定进程。如果未进入进程 ID, 此命令将应用于所有已配置的 OSPFv3 进程。</li><li><code>vrf vrf-name</code>— 输入关键字 <code>vrf</code>, 后跟 VRF 的名称, 以显示该 VRF LSA 信息。</li></ul> |
| 默认 | 未配置                                                                                                                                                                                                                           |

命令模式

使用情况信息

- EXEC
- Link ID — 标识路由器 ID。
  - ADV Router — 标识通告路由器的 ID。
  - Age — 显示 LS 年限。
  - Seq# — 标识 LS 序列号。这标识了旧的或重复的 LSA。
  - Checksum — 显示 LSA 的完整内容的 Fletcher 校验和。
  - Link count — 显示该路由器的接口数量。
  - Rtr Count — 显示路由器计数。
  - Dest RtrID — 显示目标路由器 ID。
  - Interface — 显示接口类型。
  - Prefix — 显示前缀的详细信息。

示例

```
OS10# show ipv6 ospf database
 OSPF Router with ID (10.0.0.2) (Process ID 200)
Router Link States (Area 0.0.0.0)
ADV Router Age Seq# Fragment ID Link count Bits

1.1.1.1 1610 0x80000144 0 1 B
2.2.2.2 1040 0x8000013A 0 1
10.0.0.2 1039 0x80000002 0 1
Net Link States (Area 0.0.0.0)
ADV Router Age Seq# Link ID Rtr count

2.2.2.2 1045 0x80000001 5 2
Inter Area Router States (Area 0.0.0.0)
ADV Router Age Seq# Link ID Dest RtrID

1.1.1.1 1605 0x80000027 1 3.3.3.3
Link (Type-8) Link States (Area 0.0.0.0)
ADV Router Age Seq# Link ID Interface

1.1.1.1 1615 0x80000125 5 ethernet1/1/1
2.2.2.2 1369 0x8000011B 5 ethernet1/1/1
10.0.0.2 1044 0x80000001 5 ethernet1/1/1
Type-5 AS External Link States
ADV Router Age Seq# Prefix

3.3.3.3 3116 0x80000126 400::/64
3.3.3.3 3116 0x80000124 34::/64
```

支持的版本

10.3.0E or later

show ipv6 ospf interface

显示已配置的 OSPFv3 接口。必须启用 OSPFv3 才能显示输出。

语法

```
show ipv6 ospf interface interface [vrf vrf-name]
```

参数

- interface — (可选) 输入接口信息：
  - ethernet — 物理接口，从 1 到 48。
  - port-channel — 端口通道接口，从 1 到 128。
  - vlan — VLAN 接口，从 1 到 4093。
- vrf vrf-name — (可选) 输入关键字 vrf，后跟 VRF 的名称，以清除该 VRF 中配置了已启用 OSPFv3 的接口。

默认

未配置

命令模式

EXEC

示例

```
OS10# show ipv6 ospf interface
ethernet1/1/1 is up, line protocol is up
 Link Local Address fe80::20c:29ff:fe0a:d59/64, Interface ID 5
 Area 0.0.0.0, Process ID 200, Instance ID 0, Router ID 10.0.0.2
 Network Type broadcast, Cost: 1
```

```

Transmit Delay is 1 sec, State BDR, Priority 1
BFD enabled(Interface level) Interval 300 Min_rx 300 Multiplier 3 Role
Active
Designated Router on this network is 2.2.2.2
Backup Designated router on this network is 10.0.0.2 (local)
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 2.2.2.2(Designated Router)

```

**支持的版本** 10.3.0E or later

## show ipv6 ospf neighbor

显示连接到本地路由器的 OSPFv3 邻居的列表。

|               |                                                                                                                                                                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>show ipv6 ospf [vrf vrf-name] neighbor</code>                                                                                                                                                                                                                                                                                         |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>vrf vrf-name</code> — 输入关键字 <code>vrf</code>，后跟 VRF 的名称，以显示该 VRF 中的 OSPFv3 邻居的列表。</li> </ul>                                                                                                                                                                                                   |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                                                         |
| <b>命令模式</b>   | EXEC                                                                                                                                                                                                                                                                                                                                        |
| <b>使用情况信息</b> | <ul style="list-style-type: none"> <li><code>Neighbor ID</code> — 显示邻居路由器 ID。</li> <li><code>Pri</code> — 显示已分配优先级的邻居。</li> <li><code>State</code> — 显示邻居的 OSPF 状态。</li> <li><code>Dead Time</code> — 显示预期的时间，直至系统声明邻居失效。</li> <li><code>Interface ID</code> — 显示邻居接口 ID</li> <li><code>Interface</code> — 显示接口类型、节点/插槽/端口或编号信息。</li> </ul> |

|           |                                                                                                                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>示例</b> | <pre> OS10(conf-if-eth1/1/1)# show ipv6 ospf neighbor Neighbor ID   Pri   State   Dead Time   Interface ID   Interface ----- 2.2.2.2       1     Full/DR  00:00:30    5              ethernet1/1/1 </pre> |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**支持的版本** 10.3.0E or later

## show ipv6 ospf statistics

显示 OSPFv3 流量统计信息。

|               |                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>show ipv6 ospf [instance-number] statistics [interface interface]</code>                                                                                                                                                                                                                                                                                                                                            |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>instance-number</code> — (可选) 输入 OSPFv3 实例编号，从 1 到 65535。</li> <li><code>interface interface</code> — (可选) 输入接口信息： <ul style="list-style-type: none"> <li><code>ethernet node/slot/port[:subport]</code> — 输入以太网端口接口。</li> <li><code>port-channel number</code> — 输入端口通道接口编号，从 1 到 128。</li> <li><code>vlan vlan-id</code> — 输入 VLAN ID 号，从 1 到 4093。</li> </ul> </li> </ul> |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>命令模式</b>   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>使用情况信息</b> | 此命令将显示指定实例或接口的 OSPFv3 流量统计信息，或者所有 OSPFv3 实例和接口的流量统计信息。                                                                                                                                                                                                                                                                                                                                                                    |

|           |                                                                                                                                                                                                                                |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>示例</b> | <pre> OS10# show ipv6 ospf interface ethernet 1/1/1  Interface ethernet1/1/1 Receive Statistics rx-invalid 0 rx-invalid-bytes 0 rx-hello 0 rx-hello-bytes 0 rx-db-des 0 rx-db-des-bytes 0 rx-ls-req 0 rx-ls-req-bytes 0 </pre> |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



```

rx-ls-upd 0 rx-ls-upd-bytes 0
rx-ls-ack 0 rx-ls-ack-bytes 0
Transmit Statistics
tx-hello 1054 tx-hello-bytes 37944
tx-db-des 0 tx-db-des-bytes 0
tx-ls-req 0 tx-ls-req-bytes 0
tx-ls-upd 0 tx-ls-upd-bytes 0
tx-ls-ack 0 tx-ls-ack-bytes 0
Error packets (Receive statistics)
bad-src 0 dupe-id 0 hello-err 0
mtu-mismatch 0 nbr-ignored 0
resource-err 0 bad-lsa-len 0 lsa-bad-type 0
lsa-bad-len 0 lsa-bad-cksum 0
hello-tmr-mismatch 0 dead-ivl-mismatch 0
options-mismatch 0 nbr-admin-down 0 own-hello-drop 0
self-orig 0 wrong-length 0
version-mismatch 0 area-mismatch 0

```

**支持的版本** 10.4.0E(R1) or later

## timers spf (OSPFv3)

启用最短路径优先 (SPF) 限制，以便在发生拓扑更改时延迟 SPF 计算。

**语法** `timers spf [start-time [hold-time [max-wait]]]`

- 参数**
- *start-time* — 设置初始 SPF 延迟（以毫秒为单位），从 1 到 600000；默认值 1000。
  - *hold-time* — 设置两个 SPF 计算之间的额外保留时间，从 1 到 600000；默认值 10000。
  - *max-wait* — 设置两次 SPF 计算之间的最长等待时间，从 1 到 600000；默认值 10000。

- 默认**
- *start-time* — 1000 毫秒
  - *hold-time* — 10000 毫秒
  - *max-wait* — 10000 毫秒

**命令模式** ROUTER-OSPFv3

**使用情况信息** OSPFv2 和 OSPFv3 支持 SPF 限制。默认情况下，OSPF 实例中的 SPF 计时器已禁用。

使用 SPF 限制在网络不稳定期间延迟 SPF 计算。在 OSPF 网络中，拓扑更改事件会在指定的开始时间后触发 SPF 计算。当开始计时器完成时，保留时间可能会延迟另一次 SPF 计算。当挂起计时器正在运行时：

- 每次发生拓扑更改时，SPF 计算会延迟两倍配置的保留时间，最多可达最长等待时间。
- 如果未发生任何拓扑更改，将执行 SPF 计算，并且保留计时器将重置为其配置的值。

如果未指定开始时间、保存时间或最大等待值，则将使用默认值。此命令的 `no` 版本会移除已配置的 SPF 计时器，并在 OSPF 实例中禁用 SPF 限制。

### 示例

```

OS10(config)# router ospfv3 100
OS10(config-router-ospfv3-100)# timers spf 1345 2324 9234

OS10(config-router-ospfv3-100)# do show ipv6 ospf
Routing Process ospfv3 100 with ID 129.240.244.107
SPF schedule delay 1345 msecs, Hold time between two SPFs 2324 msecs
Min LSA origination 5000 msec, Min LSA arrival 1000 msec
Min LSA hold time 0 msec, Max LSA wait time 0 msec
Number of area in this router is 1, normal 1 stub 0 nssa
Area (0.0.0.1)
Number of interface in this area is 1
SPF algorithm executed 2 times

```

**支持的版本** 10.4.0E(R1) or later

# 对象跟踪管理器

OTM 使您可以跟踪第 2 层 (L2) 接口的链路状态，以及 IPv4 和 IPv6 主机的可访问性。您可以提高网络的可用性，并在对象状态停机时缩短恢复时间。

对象跟踪可监控跟踪对象的状态，并传达对感兴趣的客户端应用程序所做的任何更改。OTM 客户端应用程序是虚拟路由器冗余协议 (VRRP) 和基于策略的路由 (PBR)。每个跟踪对象都有一个唯一的标识编号，客户端使用该数字来配置跟踪的对象更改状态时要采取的措施。您还可以选择指定跟踪对象的状态报告更改到客户端应用程序之前的时间延迟。

VRRP 订阅跟踪接口行协议状态的轨道对象。它使用跟踪的对象状态来确定 VRRP 组中 VRRP 路由器的优先级。如果跟踪的状态或接口停机，VRRP 将根据您配置跟踪状态的新优先级来更新优先级。当跟踪状态出现时，VRRP 将恢复虚拟路由器组的原始优先级。

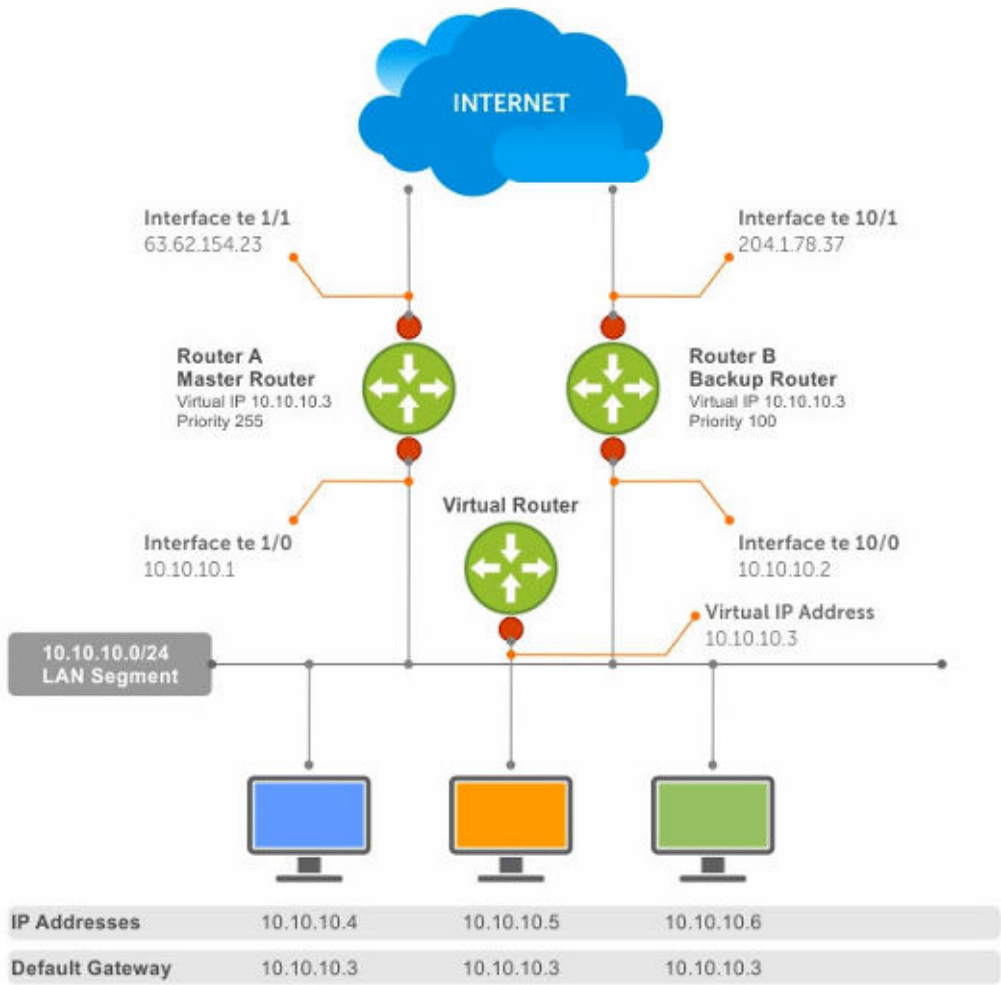


图 8: 对象跟踪

## 接口跟踪

您可以创建一个对象来跟踪 L2 接口的线路协议状态，并监控其正常运行或停止状态。您可以配置最多 500 个对象。每个对象都分配有唯一的 ID。

当链路级别状态为停止时，跟踪的资源状态也将被视为停止。如果链路级别状态为启动，则跟踪的资源状态也被视为启动。对于端口信道或 VLAN 等逻辑接口，如果逻辑接口下的任何物理接口都正常运行，则链路协议状态将视为启动。

可用接口的列表包括：

- ethernet — 物理接口

- port-channel — 端口通道标识符
- VLAN — 虚拟局域网 (VLAN) 标识符
- Loopback — 环回接口标识符
- mgmt — 管理接口

1. 在 CONFIGURATION 模式下配置对象跟踪，从 1 到 500。

```
track object-id
```

2. (可选) 在 OBJECT TRACKING 模式下进入 L2 接口的线路协议状态中进入接口对象跟踪。

```
interface interface line-protocol
```

3. (可选) 在 OBJECT TRACKING 模式下配置在通信已跟踪接口的状态更改之前使用的事件延迟，从 0 到 80 秒；默认值为 0。

```
delay [up seconds] [down seconds]
```

4. (可选) 在 EXEC 模式下查看跟踪的对象信息。

```
show track object-id
```

5. (可选) 在 EXEC 模式下查看所有接口对象的信息。

```
show track interface
```

6. (可选) 在 EXEC 模式下查看所有 IPv4 或 IPv6 下一跳对象信息。

```
show track [ip | ipv6]
```

7. (可选) 在 EXEC 模式下查看对象信息的简要状态。

```
show track brief
```

## 配置对象跟踪

```
OS10(config)# track 1
OS10(conf-track-1)# interface ethernet 1/1/1 line-protocol
OS10(conf-track-1)# delay up 20
OS10(conf-track-1)# delay down 10
OS10(conf-track-1)# do show track 1
Interface ethernet1/1/1 line-protocol
Line protocol is UP
1 changes, Last change 2017-04-26T06:41:36Z
```

## 主机跟踪

如果将 IP 主机配置为跟踪对象，则 ARP 高速缓存中的条目或下一跳地址将确定路由的启动或关闭状态。

如果路由器的下一跳地址存在 ARP 高速缓存条目，则可以访问跟踪的主机。如果在考虑路由之前显示下一跳地址，将会尝试重新生成 ARP 高速缓存条目。

1. 在 CONFIGURATION 模式下配置对象跟踪。

```
track object-id
```

2. 输入主机 IP 地址，以便在 OBJECT TRACKING 模式下访问 IPv4 或 IPv6 路由。

```
[ip | ipv6] host-ip-address reachability
```

3. 配置在 OBJECT TRACKING 模式下传达跟踪的路径更改状态之前使用的时间延迟。

```
delay [up seconds] [down seconds]
```

4. 通过在 OBJECT TRACKING 模式下定期检查可访问性来跟踪主机。

```
reachability-refresh interval
```

5. 在 EXEC 模式下查看跟踪配置和跟踪的对象状态。

```
show track object-id
```

配置 IPv4 主机跟踪

```
OS10 (conf-track-1)# track 2
OS10 (conf-track-2)# ip 1.1.1.1 reachability
OS10 (conf-track-2)# do show track 2
IP Host 1.1.1.1 reachability
Reachability is DOWN
1 changes, Last change 2017-04-26T06:45:31Z
OS10 (conf-track-2)#
```

配置 IPv6 主机跟踪

```
OS10 (conf-track-2)# track 3
OS10 (conf-track-3)# ipv6 20::20 reachability
OS10 (conf-track-3)# delay up 20
OS10 (conf-track-3)# do show track 3
IP Host 20::20 reachability
Reachability is DOWN
1 changes, Last change 2017-04-26T06:47:04Z
OS10 (conf-track-3)#
```

设置跟踪延迟

您可以为每个跟踪的对象配置可选的向上或向下计时器。该计时器允许您设置所跟踪对象状态的更改与客户端通信之前的时间延迟。当状态从向上到向下或从向下变为向上时，时间延迟便会开始。

如果对象的状态在计时器过期之前切换回其先前的状态，则会取消计时器而不通知客户端。如果计时器过期并且对象的状态已更改，则会向客户端发送一条通知。例如，如果向下计时器正在运行，并且某个接口发生故障，则向下计时器已取消。客户端不会收到有关事件的通知。

如果未配置延迟，则会在检测到跟踪对象状态发生变化时发送通知。以秒为单位指定传达状态更改的时间延迟。

对象跟踪

作为客户端，VRRP 可以跟踪最多 20 个接口对象，并且每个 VRRP 组支持 12 个跟踪的接口。您可以为每个跟踪的 VRRP 对象或组接口分配唯一的优先级-成本值，从 1 到 254。

如果跟踪的 VRRP 对象处于停止状态，则将从 VRRP 组优先级中减去优先级成本。如果 VRRP 组路由器充当 owner-master，运行时 VRRP 组优先级保持固定为 255。跟踪对象状态的更改不起作用。

在 VRRP 对象跟踪中，所有跟踪对象和接口的优先级成本之和不能等于或超过 VRRP 组的优先级。

查看跟踪对象

您可以查看当前跟踪的 L2 或 L3 接口或 IPv4 或 IPv6 主机的状态。

查看简要对象跟踪信息

```
OS10# show track brief
```

| TrackID               | Resource         | Parameter     | Status | LastChange            |
|-----------------------|------------------|---------------|--------|-----------------------|
| 1                     | line-protocol    | ethernet1/1/1 | DOWN   |                       |
| 2017-02-03T08:41:25Z1 |                  |               |        |                       |
| 2                     | ipv4-reachablity | 1.1.1.1       | DOWN   |                       |
| 2017-02-03T08:41:43Z1 |                  |               |        |                       |
| 3                     | ipv6-reachablity | 10::10        | DOWN   | 2017-02-03T08:41:55Z1 |

查看所有对象跟踪信息

```
OS10# show track
```

查看接口对象跟踪信息

|                            |                  |               |        |                       |
|----------------------------|------------------|---------------|--------|-----------------------|
| OS10# show track interface |                  |               |        |                       |
| TrackID                    | Resource         | Parameter     | Status | LastChange            |
| -----                      |                  |               |        |                       |
| 1                          | line-protocol    | ethernet1/1/1 | DOWN   |                       |
| 2017-02-03T08:41:25Z1      |                  |               |        |                       |
| OS10# show track ip        |                  |               |        |                       |
| TrackID                    | Resource         | Parameter     | Status | LastChange            |
| -----                      |                  |               |        |                       |
| 2                          | ipv4-reachablity | 1.1.1.1       | DOWN   |                       |
| 2017-02-03T08:41:43Z1      |                  |               |        |                       |
| OS10# show track ipv6      |                  |               |        |                       |
| TrackID                    | Resource         | Parameter     | Status | LastChange            |
| -----                      |                  |               |        |                       |
| 3                          | ipv6-reachablity | 10::10        | DOWN   | 2017-02-03T08:41:55Z1 |

查看 IPv4 下一跳对象跟踪

```
OS10# show track ip
```

查看 IPv6 下一跳对象跟踪

```
OS10# show track ipv6
```

查看正在运行的配置

```
OS10# show running-configuration
```

OTM 命令

delay

配置延迟计时器。

|        |                                             |
|--------|---------------------------------------------|
| 语法     | delay {up   down} seconds                   |
| 参数     | seconds — 以秒为单位输入延迟时间。最多 180 个字符。           |
| 默认     | 未配置                                         |
| 命令模式   | CONFIGURATION                               |
| 使用情况信息 | 无                                           |
| 示例     | OS10(conf-track-100)# delay up 200 down 100 |
| 支持的版本  | 10.3.0E or later                            |

interface line-protocol

配置对象以跟踪特定接口的系列协议状态。

|    |                                                                                                                                                                                                                     |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | interface interface line-protocol                                                                                                                                                                                   |
| 参数 | interface — 输入以下接口信息： <ul style="list-style-type: none"><li>• ethernet — 物理接口。</li><li>• port-channel — 输入端口通道标识符。</li><li>• vlan — 输入 VLAN 标识符。</li><li>• loopback — 输入环回接口标识符。</li><li>• mgmt — 输入管理接口。</li></ul> |
| 默认 | 未配置                                                                                                                                                                                                                 |

**命令模式** CONFIGURATION

**使用情况信息** 无

**示例**

```
OS10(conf-track-100)# interface ethernet line-protocol
```

**支持的版本** 10.3.0E or later

## ip reachability

配置对象以跟踪特定下一跳主机的可访问性。

**语法** `ip host-ip-address reachability`

**参数** `host-ip-address` — 输入 IPv4 主机地址。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 无

**示例**

```
OS10(config)# track 100
OS10(conf-track-100)# ip 10.10.10.1 reachability
```

**支持的版本** 10.3.0E or later

## ipv6 reachability

配置对象以跟踪特定下一跳主机的可访问性。

**语法** `ipv6 host-ip-address reachability`

**参数** `host-ip-address` — 输入 IPv6 主机地址。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 无

**示例**

```
OS10(config)# track 200
OS10(conf-track-200)# ipv6 10::1 reachability
```

**支持的版本** 10.3.0E or later

## reachability-refresh

配置可访问性跟踪的轮询间隔。

**语法** `reachability-refresh interval`

**参数** `interval` — 输入轮询间隔值。最大值为 3600 秒。

**默认** 0 秒

**命令模式** CONFIGURATION

**使用情况信息** 将间隔设置为 0 可禁用刷新。

**示例**

```
OS10(conf-track-100)# reachability-refresh 600
```

**支持的版本** 10.3.0E or later

## show track

显示跟踪的对象信息。

|         |                                                                                                                                                                                                                                                                                        |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法      | show track [ <i>brief</i> ] [ <i>object-id</i> ] [ <i>interface</i> ] [ <i>ip</i>   <i>ipv6</i> ]                                                                                                                                                                                      |
| 参数      | <ul style="list-style-type: none"><li>• <i>brief</i> — (可选) 显示简要跟踪的对象信息。</li><li>• <i>object-id</i> — (可选) 显示特定对象 ID 的跟踪对象信息。</li><li>• <i>interface</i> — (可选) 显示所有接口对象的信息。</li><li>• <i>ip</i> — (可选) 显示所有 IPv4 下一跳对象的信息。</li><li>• <i>ipv6</i> — (可选) 显示所有 IPv6 下一跳对象的信息。</li></ul> |
| 默认      | 无                                                                                                                                                                                                                                                                                      |
| 命令模式    | CONFIGURATION                                                                                                                                                                                                                                                                          |
| 使用情况信息  | 无                                                                                                                                                                                                                                                                                      |
| 示例 (简要) |                                                                                                                                                                                                                                                                                        |

```
OS10# show track brief
```

| TrackID               | Resource         | Parameter     | Status | LastChange            |
|-----------------------|------------------|---------------|--------|-----------------------|
| 1                     | line-protocol    | ethernet1/1/1 | DOWN   |                       |
| 2017-02-03T08:41:25Z1 |                  |               |        |                       |
| 2                     | ipv4-reachablity | 1.1.1.1       | DOWN   |                       |
| 2017-02-03T08:41:43Z1 |                  |               |        |                       |
| 3                     | ipv6-reachablity | 10::10        | DOWN   | 2017-02-03T08:41:55Z1 |

支持的版本 10.3.0E or later

## track

配置和管理跟踪的对象。

|        |                                          |
|--------|------------------------------------------|
| 语法     | track <i>object-id</i>                   |
| 参数     | <i>object-id</i> — 输入要跟踪的对象 ID。最大值为 500。 |
| 默认     | 未配置                                      |
| 命令模式   | CONFIGURATION                            |
| 使用情况信息 | 此命令的 <i>no</i> 版本从接口删除跟踪的对象。             |
| 示例     |                                          |

```
OS10# track 100
```

支持的版本 10.3.0E or later

# 基于策略的路由

PBR 提供了一种机制，可根据定义用来基于路由表覆盖交换机转发决策的策略，对 IPv4 和 IPv6 数据包进行重定向。

## 基于策略的路由映射

路由映射是一组有序的规则，用于控制 IP 路由到协议域的重新分发。当您在某个接口上启用 PBR 时，所有 IPv4 或 IPv6 数据包将根据您在路由映射中定义的策略来处理。路由映射中定义的规则基于访问控制列表 (ACL) 和下一跳地址，并且仅适用于在基于策略的路由中使用的 ACL。

您可以创建路由映射，用于指定匹配条件以及满足所有匹配子句的结果操作。创建路由映射后，您可以对特定接口上的该路由映射启用 PBR。路由 — 映射包含可以标记为 *permit* 的 *match* 和 *set* 语句。

## 用于匹配路由映射的访问列表

您可以分配 IPv4 或 IPv6 访问列表以匹配路由映射。IP 访问列表包含根据标头字段匹配流量内容的条件，例如目标 IP 或源 IP。

当 `permit` 或 `deny` 存在于 `access-list` 中时，它会被忽略并且 `route-map` 命令中存在的操作将用于基于策略的路由。路由映射语句中的 `permit` 关键字表示基于策略的路由。路由映射语句中的 `deny` 关键字表示基于交换机的转发决定，即 PBR 异常。仅在基于策略的路由中将访问列表用于数据包匹配条件。

1. 在 CONFIGURATION 模式下分配访问列表以匹配路由映射。

```
ip access-list access-list-name
```

2. 在 IP ACL 模式下设置 IP 地址以匹配访问列表。

```
permit ip ip-address
```

### 配置 IPv4 访问列表以匹配路由映射

```
OS10(config)# ip access-list acl5
OS10(conf-ipv4-acl)# permit ip 10.10.10.0/24 any
```

### 配置 IPv6 访问列表以匹配路由映射

```
OS10(config)# ipv6 access-list acl8
OS10(conf-ipv6-acl)# permit ipv6 10::10 any
```

## 设置地址以匹配路由映射

您可以设置 IPv4 或 IPv6 地址以匹配路由映射。

1. 输入要匹配的 IPv4 或 IPv6 地址，并在路由映射模式下指定访问列表名称。

```
match {ip | ipv6} address access-list-name
```

2. 在路由映射模式中设置下一跳 IP 地址。

```
set {ip | ipv6} next-hop ip-address
```

### 应用匹配并将参数设置为 IPv4 路由映射

```
OS10(conf-route-map)# route-map map1
OS10(conf-route-map)# match ip address acl5
OS10(conf-route-map)# set ip next-hop 10.10.10.10
```

### 应用匹配并将参数设置为 IPv6 路由映射

```
OS10(conf-route-map)# route-map map1
OS10(conf-route-map)# match ipv6 address acl8
OS10(conf-route-map)# set ipv6 next-hop 20::20
```

## 将路由映射分配给接口

您可以将路由映射分配给接口，以便基于 IPv4 或 IPv6 策略的路由至接口。

- 在 INTERFACE 模式下，将基于 IPv4 或 IPv6 策略的路由映射到接口。

```
{ip | ipv6} policy route-map map-name
```

### 为 IPv4 接口分配路由映射

```
OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# ip policy route-map map1
```



## 为 IPv6 接口分配路由映射

```
OS10(conf-if-eth1/1/5)# ipv6 policy route-map map2
```

## 查看 PBR 信息

显示 PBR 信息以验证 IPv4 或 IPv6 配置并查看统计信息。

1. 在 EXEC 模式下查看 IPv4 或 IPv6 PBR 策略信息。

```
show {ip | ipv6} policy name
```

2. 在 EXEC 模式下查看当前 PBR 统计信息。

```
show route-map map-name pbr-statistics
```

3. 在 EXEC 模式下清除所有策略统计信息。

```
clear route-map map-name pbr-statistics
```

### 验证 IPv4 PBR 配置

```
OS10# show ip policy abc
Interface Route-map

ethernet1/1/1 abc
ethernet1/1/3 abc
vlan100 abc
```

### 验证 IPv6 PBR 配置

```
OS10# show ipv6 policy abc
Interface Route-map

ethernet1/1/1 abc
ethernet1/1/3 abc
vlan100 abc
```

### 查看当前 PBR 统计信息

```
show route-map pbr-sample pbr-statistics
route-map pbr-sample, permit, sequence 10

Policy routing matches: 84 packets
```

## 基于策略的按 VRF 的路由

为 IPv4 和 IPv6 流量流的每个 VRF 实例配置 PBR。

基于策略的路由 (PBR) 允许具有特定匹配条件的数据包（例如来自特定源和目标地址的数据包）重新定向到其他下一跳。

您还可以使用 PBR 将到达 VRF 实例的数据包重新定向到可通过不同 VRF 实例访问的下一跳。可将到达任何 VRF 实例的数据包重新定向到默认 VRF 实例或任何其他非默认 VRF 实例。

 **注：**默认和非默认 VRF 实例上支持 PBR；但是，管理 VRF 实例上不支持 PBR。

## 按 VRF 配置 PBR

对于到达 VRF 实例的流量，您可以使用路由映射将此流量重新定向到另一个 VRF 实例上的下一跳。在路由映射中，设置可通过不同 VRF 实例访问的下一跳 IP 地址。当与特定条件匹配的流量到达 VRF 实例时，路由映射配置可将数据包重新定向到可通过另一个 VRF 实例访问的下一跳。要按 VRF 配置 PBR，请执行以下操作：

1. 为 IPv4 或 IPv6 流量创建匹配 ACL 规则。

```
{ip | ipv6} access-list access-list-name
```

2. 允许或拒绝来自具有特定目标的任何源的 IPv4 或 IPv6 流量。

```
permit {ip | ipv6} any ip-address
```

或

```
deny {ip | ipv6} any ip-address
```

3. 配置路由映射，以重新定向到达特定 VRF 实例的流量。

```
route-map route-map-name
```

4. 输入要匹配的 IPv4 或 IPv6 地址，然后指定访问列表名称。

```
match {ip | ipv6} address access-list-name
```

5. 在路由映射中，设置要通过不同 VRF 实例访问 IPv4 或 IPv6 下一跳。

```
set {ip | ipv6} vrf vrf-name next-hop next-hop-ipv4address
```

通过不同的 VRF 实例可访问此下一跳地址。

 **注：**如果在指定的 VRF 实例上可以访问下一跳，则重定向数据包；否则，数据包将遵循常规的路由流程。

6. 将路由映射应用到接口。

```
interface interface-type
```

```
{ip | ipv6} policy route-map route-map-name
```

7. 查看路由映射信息。

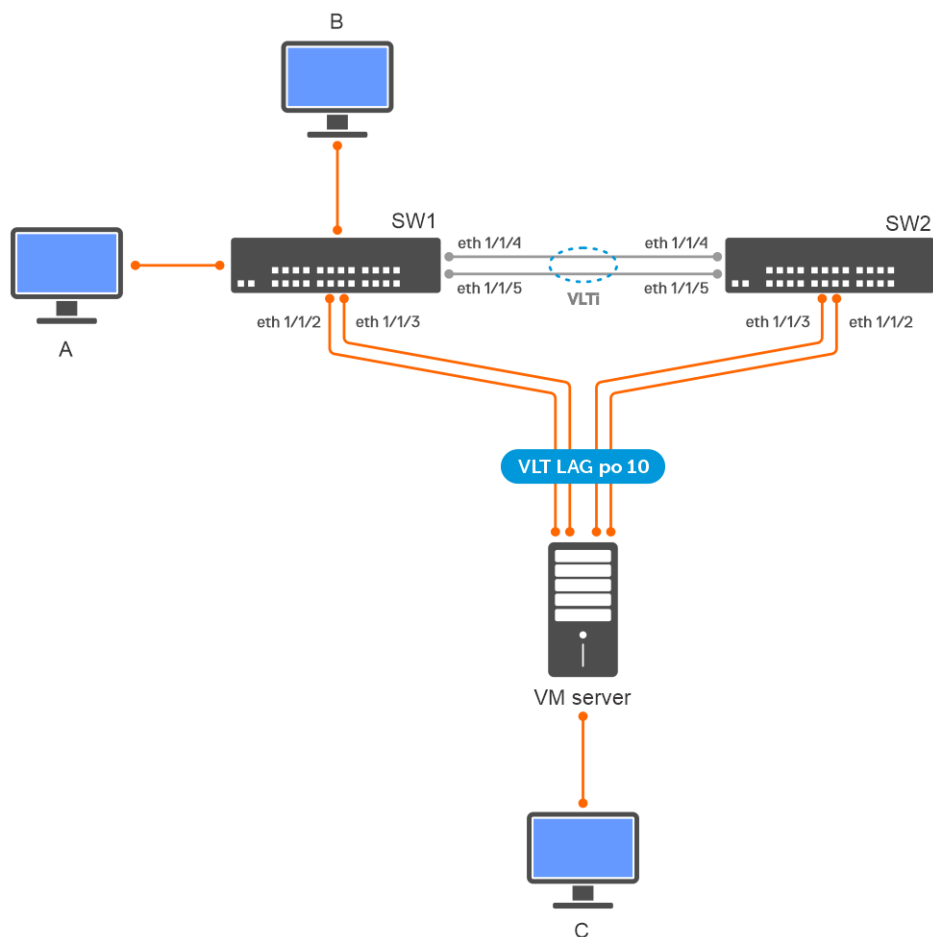
```
show route-map
```

```
OS10(conf-if-vl-40)# do show route-map
route-map test, permit, sequence 10
Match clauses:
ip address (access-lists): acl1
Set clauses:
ip vrf red next-hop 1.1.1.1 track-id 200
```

## PBR 和 VLT

在 VLT 设置中配置 PBR 时，在两个 VLT 对等节点上配置相同的 PBR 规则。

在下面的示例中，流量源自 A，并发往 B。使用 PBR 规则通过 VLT 端口通道将流量重定向至 C。当 VLT 端口通道接口停机时，流量仍然通过 VLT<sub>i</sub> 传输到 C。



## SW 1

### VLAN 配置

- 创建 VLAN 并为其分配充当 VM 中主机的网关的 IP 地址。

```
OS10# configure terminal
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# no shutdown
OS10(conf-if-vl-100)# ip address 10.1.1.1/24
OS10(conf-if-vl-100)# exit
```

- 创建另一个 VLAN 并为其分配 IP 地址。

```
OS10# configure terminal
OS10(config)# interface vlan 200
OS10(conf-if-vl-200)# no shutdown
OS10(conf-if-vl-200)# ip address 10.2.1.1/24
OS10(conf-if-vl-200)# exit
```

### VLT 配置

- 创建 VLT 域并配置 VLTi。

```
OS10(config)# interface range ethernet 1/1/4-1/1/5
OS10(conf-range-eth1/1/4-1/1/5)# no switchport
OS10(conf-range-eth1/1/4-1/1/5)# exit
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# discovery-interface ethernet 1/1/4-1/1/5
```

- 配置 VLT MAC 地址。

```
OS10(conf-vlt-1)# vlt-mac 12:5e:23:2d:76:3e
```

### 3. 指定 VLT 对等节点的管理 IP 地址作为备份链路。

```
OS10(config-vlt-1)# backup destination 10.10.10.2
```

### 4. 配置 VLT 端口通道。

#### SW1 到 VM VLT 端口通道配置

```
OS10(config)# interface port-channel 10
OS10(config-if-po-10)# description SW1ToVM
OS10(config-if-po-10)# vlt-port-channel 10
OS10(config-if-po-10)# switchport mode trunk
OS10(config-if-po-10)# switchport trunk allowed vlan 100,200
OS10(config-if-po-10)# exit
OS10(config)# interface ethernet 1/1/2-1/1/3
OS10(config-if-eth1/1/2-1/1/3)# no shutdown
OS10(config-if-eth1/1/2-1/1/3)# channel-group 10
```

#### SW 1 到服务器配置

```
OS10(config)# interface port-channel 20
OS10(config-if-po-20)# description SW1ToServer
OS10(config-if-po-20)# vlt-port-channel 20
OS10(config-if-po-20)# switchport mode trunk
OS10(config-if-po-20)# switchport trunk allowed vlan 100,200
OS10(config-if-po-20)# exit
OS10(config)# interface ethernet 1/1/1,1/1/6
OS10(config-if-eth1/1/1,1/1/6)# no shutdown
OS10(config-if-eth1/1/1,1/1/6)# channel-group 20
```

#### (可选) 对等节点路由配置

- 配置对等节点路由。

```
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# peer-routing
```

### PBR 配置

在两个 VLT 对等节点的流量入口接口和 VLTi 接口上应用策略。

```
OS10(config)# ip access-list PBR-A2C
OS10(config-ipv4-acl)# permit ip 10.10.10.0/24 any
OS10(config-route-map)# route-map Map1
OS10(config-route-map)# match ip address PBR-A2C
OS10(config-route-map)# set ip next-hop 10.10.20.10
OS10(config-route-map)# exit
OS10(config)# interface ethernet 1/1/4-1/1/6
OS10(config-if-eth1/1/4-1/1/6)# ip policy route-map Map1
```

### SW 2

#### VLAN 配置

- 创建 VLAN 并为其分配充当 VM 中主机的网关的 IP 地址。

```
OS10# configure terminal
OS10(config)# interface vlan 100
OS10(config-if-vl-100)# no shutdown
OS10(config-if-vl-100)# ip address
OS10(config-if-vl-100)# ip address 10.1.1.2/24
OS10(config-if-vl-100)# exit
```

- 创建另一个 VLAN 并为其分配 IP 地址。

```
OS10# configure terminal
OS10(config)# interface vlan 200
OS10(config-if-vl-200)# no shutdown
OS10(config-if-vl-200)# ip address
OS10(config-if-vl-200)# ip address 10.2.1.3/24
OS10(config-if-vl-200)# exit
```

## VLT 配置

### 1. 创建 VLT 域并配置 VLTi。

```
OS10(config)# interface range ethernet 1/1/4-1/1/5
OS10(config-range-eth1/1/4-1/1/5)# no switchport
OS10(config-range-eth1/1/4-1/1/5)# exit
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# discovery-interface ethernet 1/1/4-1/1/5
```

### 2. 配置 VLT MAC 地址。

```
OS10(config-vlt-1)# vlt-mac 12:5e:23:f4:23:54
```

### 3. 指定 VLT 对等节点的管理 IP 地址作为备份链路。

```
OS10(config-vlt-1)# backup destination 10.10.10.1
```

### 4. 配置 VLT 端口通道。

SW2 到 VM VLT 端口通道配置

```
OS10(config)# interface port-channel 10
OS10(config-if-po-10)# description SW2ToVM
OS10(config-if-po-10)# vlt-port-channel 10
OS10(config-if-po-10)# switchport mode trunk
OS10(config-if-po-10)# switchport trunk allowed vlan 100,200
OS10(config-if-po-10)# exit
OS10(config)# interface ethernet 1/1/2-1/1/3
OS10(config-if-eth1/1/2-1/1/3)# no shutdown
OS10(config-if-eth1/1/2-1/1/3)# channel-group 10
```

### (可选) 对等节点路由配置

- 配置对等节点路由。

```
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# peer-routing
```

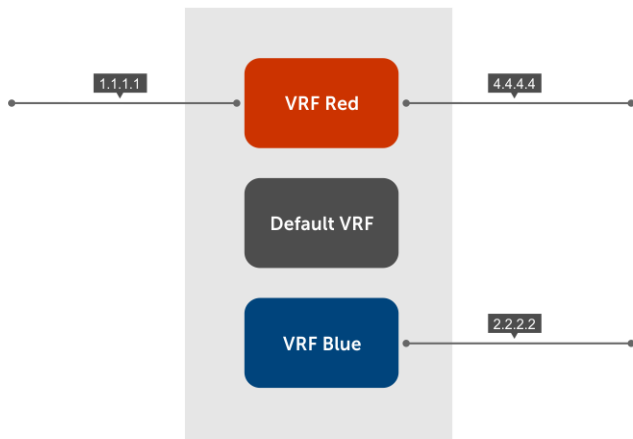
## PBR 配置

在两个 VLT 对等节点的 VLTi 接口上应用策略。

```
OS10(config)# ip access-list PBR-A2C
OS10(config-ipv4-acl)# permit ip 10.10.10.0/24 any
OS10(config-route-map)# route-map Map1
OS10(config-route-map)# match ip address PBR-A2C
OS10(config-route-map)# set ip next-hop 10.10.20.10
OS10(config-route-map)# exit
OS10(config)# interface ethernet 1/1/4-1/1/6
OS10(config-if-eth1/1/4-1/1/6)# ip policy route-map Map1
```

## 配置示例

请考虑通过属于 VRF RED 的 VLAN40 来自源 IP 地址 1.1.1.1 入口的流量情况。此流量的出口接口也位于与 IP 地址 4.4.4.4 相同的 VRF RED 中（如下所示）。



通过使用以下 PBR 配置，您可以通过 VRF BLUE 中的下一跳 IP 地址 2.2.2.2，将流量入口重新定向到可访问的目标 VRF RED：

1. 创建路由映射。

```
OS10(config)# route-map test
```

2. 输入与指定访问列表匹配的 IP 地址。

```
OS10(config-route-map)# match ip 4.4.4.4 acl1
```

3. 将下一跳地址设置为 2.2.2.2，通过 VRF BLUE 可以访问该地址。

```
OS10(config-route-map)#
OS10(config-route-map)# set ip vrf BLUE next-hop 2.2.2.2
OS10(config-route-map)# exit
```

4. 将此规则应用于流量入口所在的接口，在此情况下是 VLAN40。

```
OS10(config)# interface vlan 40
OS10(conf-if-vl-40)#
OS10(conf-if-vl-40)# ip policy route-map test
```

5. (可选) 查看接口上的 PBR 配置。

```
OS10(conf-if-vl-40)# show configuration
!
interface vlan40
no shutdown
ip policy route-map test
!
```

## 跟踪路由可访问性

使用对象跟踪来跟踪 IPv4 或 IPv6 可访问性。要在通过 VRF 实例可访问的路由上配置跟踪，请执行以下操作：

1. 配置对象跟踪。

```
track track-id
```

```
OS10(config)# track 200
```

2. 通过 VRF 实例配置下一跳地址的可访问性。

```
ip ip-address reachablility vrf vrf-name
```

```
OS10(conf-track-200)#
OS10(conf-track-200)# ip 1.1.1.1 reachability vrf red
OS10(conf-track-200)#exit
```

### 3. 配置路由映射。

```
route-map route-map-name
```

```
OS10(config-route-map)#
OS10(config-route-map)# match ip address acl1
```

### 4. 将在步骤 1 中配置的磁道 ID 设置为路由映射。

```
set ip vrf vrf-name nexy-hop next-hop-address track-id track-id-number
```

```
OS10(config-route-map)# set ip vrf red next-hop 1.1.1.1 track-id 200
```

### 5. 对 VRF 实例上的入口流量接口应用路由映射。

```
interface interface-type
ip policy route-map route-map-name
```

```
OS10(config)# interface vlan 40
OS10(config-if-vl-40)#
OS10(config-if-vl-40)# ip policy route-map test
OS10(config-if-vl-40)# show configuration
!
```

**注：**确保配置下一跳 IP 地址跟踪，以及具有相同 VRF 实例的 PBR 下一跳地址。对于同一 VRF 实例中的下一跳地址可访问性，必须为每个 VRF 配置 PBR 和对象跟踪。在 VRF 实例中缺少下一跳 IP 地址跟踪或 PBR 下一跳配置会导致配置错误。但是，系统不会显示一条错误消息来指出配置中的问题。

## 使用 PBR 允许和阻止特定流量

本部分介绍如何使用 PBR 通过接口允许特定流量。

### 配置接口

#### 1. 创建 VLAN 接口。

```
OS10(Config)# interface vlan999
```

#### 2. 启用接口。

```
OS10(Config-if-999)# no shutdown
```

#### 3. 为接口输入一个 IP 地址。

```
OS10(Config-if-999)# ip address 10.99.0.251/16
```

### 定义 PBR 参数

- 创建 ACL 并定义应该为 PBR 处理启用哪些内容。

```
ip access-list TEST-ACL
seq 10 permit tcp any any eq 80
seq 20 permit tcp any any eq 443
seq 30 permit tcp any any eq 21
seq 40 permit icmp any any
```

- 创建 ACL 并定义应从 PBR 处理中排除的内容。

```
ip access-list TEST-ACL-DENY
seq 10 deny tcp 10.99.0.0/16 10.0.0.0/8 eq 80
seq 20 deny tcp 10.99.0.0/16 10.0.0.0/8 eq 443
seq 30 deny tcp 10.99.0.0/16 10.0.0.0/8 eq 21
seq 40 deny icmp 10.99.0.0/16 10.0.0.0/8
```

- 创建路由映射，以阻止特定流量进行 PBR 处理。

```
route-map TEST-RM deny 5
match ip address TEST-ACL-DENY
```

- 创建路由映射以允许流量进行 PBR 处理。

```
route-map TEST-RM permit 10
match ip address TEST-ACL
set ip next-hop 10.0.40.235
```

- 将策略应用到先前创建的接口。

```
ip policy route-map TEST-RM
```

在此配置中，route-map TEST-RM deny 5 配置会阻止与 TEST-ACL-DENY ACL 匹配的流量进行进一步 PBR 处理。此流量使用路由表进行路由。route-map TEST-RM permit 10 配置会发送与 TEST-ACL ACL 匹配的流量，以便进行 PBR 处理。任何与 TEST-ACL ACL 匹配的数据包将转发到 10.0.40.235。

## 查看 PBR 配置

使用 show configuration 命令可查看接口的配置。

```
OS10(conf-if-vl-40)# show configuration
!
interface vlan40
no shutdown
ip policy route-map test
```

使用 show route-map 命令可查看路由映射配置。

```
OS10(config)# do show route-map
route-map map1, permit, sequence 10
Match clauses:
 ipv6 address (access-lists): acl1
Set clauses:
 ipv6 vrf {vrf-name} next-hop 5555::5556

OS10(conf-if-vl-40)# do show route-map
route-map test, permit, sequence 10
Match clauses:
ip address (access-lists): acl1
Set clauses:
ip next-hop 1.1.1.1 track-id 200

OS10(conf-if-vl-40)# do show route-map test
route-map test, permit, sequence 10
Match clauses:
ip address (access-lists): acl1
Set clauses:
ip vrf red next-hop 1.1.1.1 track-id 200
!
```

## PBR 命令

### clear route-map pbr-statistics

清除所有 PBR 计数器。

|               |                                           |
|---------------|-------------------------------------------|
| <b>语法</b>     | clear route-map [map-name] pbr-statistics |
| <b>参数</b>     | map-name— 输入已配置的路由映射的名称。最多 140 个字符。       |
| <b>默认</b>     | 无                                         |
| <b>命令模式</b>   | EXEC                                      |
| <b>使用情况信息</b> | 无                                         |



**示例**

```
OS10# clear route-map map1 pbr-statistics
```

**支持的版本**

10.3.0E or later

## match address

将访问列表与路由映射匹配。

**语法**

```
match {ip | ipv6} address [name]
```

**参数**

*name*— 输入访问列表的名称。最多 140 个字符。

**默认**

未配置

**命令模式**

ROUTE-MAP

**使用情况信息**

无

**示例**

```
OS10(config-route-map)# match ip address acl1
```

**支持的版本**

10.3.0E or later

## policy route-map

将基于 IPv4 或 IPv6 策略的路由的路由映射分配到接口。

**语法**

```
{ip | ipv6} policy route-map [map-name]
```

**参数**

*map-name*— 输入已配置的路由映射的名称。最多 140 个字符。

**默认**

未配置

**命令模式**

INTERFACE

**使用情况信息**

无

**示例**

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# ip policy route-map map1
```

**支持的版本**

10.3.0E or later

## route-map pbr-statistics

启用 PBR 统计信息的计数器。

**语法**

```
route-map [map-name] pbr-statistics
```

**参数**

*map-name*— 输入已配置的路由映射的名称。最多 140 个字符。

**默认**

未配置

**命令模式**

CONFIGURATION

**使用情况信息**

无

**示例**

```
OS10(config)# route-map map1 pbr-statistics
```

**支持的版本**

10.3.0E or later

## set next-hop

为基于策略的路由设置 IPv4 或 IPv6 下一跳地址。

|               |                                                                                                                                                                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>set {ip   ipv6} vrf [vrf-name] next-hop address</code>                                                                                                                                                                                                                                          |
| <b>参数</b>     | <ul style="list-style-type: none"><li><code>vrf vrf-name</code> — 输入关键字，然后是 VRF 的名称，以使下一跳可访问该 VRF。</li><li><code>address</code> — 输入下一跳 IPv4 或 IPv6 地址。</li></ul>                                                                                                                                     |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                   |
| <b>命令模式</b>   | ROUTE-MAP                                                                                                                                                                                                                                                                                             |
| <b>使用情况信息</b> | <p>您必须配置下一跳 IP 地址跟踪，以及具有相同 VRF 实例的 PBR 下一跳地址。对于同一 VRF 实例中的下一跳地址可访问性，必须为每个 VRF 配置 PBR 和对象跟踪。在 VRF 实例中缺少下一跳 IP 地址跟踪或 PBR 下一跳配置会导致配置错误。但是，系统不会显示一条错误消息来指出配置中的问题。</p> <p><code>set {ip   ipv6} next-hop</code> 命令支持 PBR 路由映射配置的多个下一跳地址。如果您为 BGP 路由映射配置输入了多个下一跳条目，或者 RTM 的路由重新分发，则系统将仅使用第一个条目，并忽略其余条目。</p> |

|           |                                                                                                                                                                                                                          |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>示例</b> | <pre>OS10(conf-route-map)# set ip next-hop 10.10.10.10 *Sets the next-hop IP address. OS10(conf-route-map)#set ip vrf red next-hop 2.2.2.2 *The next-hop 2.2.2.2 should be reachable via interface over VRF "red".</pre> |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|              |                  |
|--------------|------------------|
| <b>支持的版本</b> | 10.3.0E or later |
|--------------|------------------|

## set next-hop track

跟踪下一跳 IPv4 或 IPv6 地址对象。

|               |                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>set {ip   ipv6} vrf [vrf-name] next-hop address track track-id</code>                                                                                                                                               |
| <b>参数</b>     | <ul style="list-style-type: none"><li><code>address</code>— 输入 IPv4 或 IPv6 地址。</li><li><code>vrf vrf-name</code> — 输入关键字，然后是 VRF 的名称，以跟踪可通过该 VRF 访问的下一跳地址。</li><li><code>track-id</code>— (可选) 输入 PBR 对象的跟踪 ID。</li></ul> |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                       |
| <b>命令模式</b>   | ROUTE-MAP                                                                                                                                                                                                                 |
| <b>使用情况信息</b> | <p>您必须配置下一跳 IP 地址跟踪，以及具有相同 VRF 实例的 PBR 下一跳地址。对于同一 VRF 实例中的下一跳地址可访问性，必须为每个 VRF 配置 PBR 和对象跟踪。在 VRF 实例中缺少下一跳 IP 地址跟踪或 PBR 下一跳配置会导致配置错误。但是，系统不会显示一条错误消息来指出配置中的问题。</p>                                                         |

|           |                                                                                                                                                                                                                                                                                     |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>示例</b> | <pre>OS10(conf-route-map)# set ip next-hop 10.10.10.10 track-id 12 *Set the track ID configured to the route-map. OS10(conf-route-map)# set ip vrf red next-hop 1.1.1.1 track-id 200 *Sets the track ID configured to track the next-hop reachable through the VRF specified.</pre> |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|              |                  |
|--------------|------------------|
| <b>支持的版本</b> | 10.3.0E or later |
|--------------|------------------|

## show policy

显示策略信息。

|             |                                                        |
|-------------|--------------------------------------------------------|
| <b>语法</b>   | <code>show {ip   ipv6} policy [map-name]</code>        |
| <b>参数</b>   | <code>map-name</code> — (可选) 输入已配置的路由映射的名称。最多 140 个字符。 |
| <b>默认</b>   | 无                                                      |
| <b>命令模式</b> | EXEC                                                   |

使用情况信息 无

示例

```
OS10# show ip policy map-name
```

支持的版本 10.3.0E or later

## show route-map pbr-statistics

显示当前 PBR 统计信息。

语法 `show route-map [map-name] pbr-statistics`

参数 `map-name` — (可选) 输入已配置的路由映射的名称。最多 140 个字符。

默认 无

命令模式 EXEC

使用情况信息 无

示例

```
OS10# show route-map map1 pbr-statistics
```

支持的版本 10.3.0E or later

## 虚拟路由器冗余协议

VRRP 允许您从局域网 (LAN) 上的物理路由器组形成虚拟路由器。在发生硬件故障时，这些虚拟路由平台（主要和备份对）提供冗余性。通过 VRRP 还可以轻松地将虚拟路由器配置为所有主机的默认网关，并避免物理路由器的单点故障。

VRRP：

- 提供虚拟默认路由平台
- 提供负载均衡
- 在单个 LAN 分段上支持多个逻辑 IP 子网
- 启用简单流量路由，而不会出现静态默认路由的单点故障
- 避免出现动态路由和发现协议问题
- 接管失败的默认路由器：
  - 数秒内
  - 最少 VRRP 流量
  - 不与主机进行任何交互

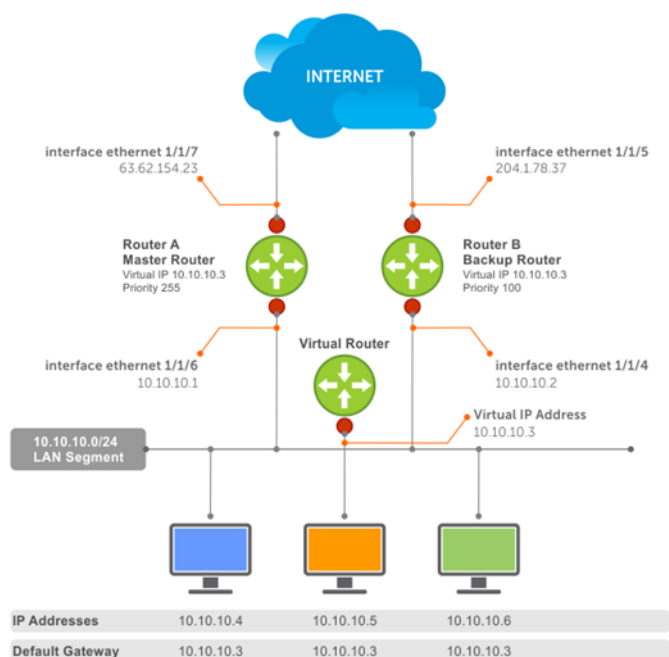
 **注：** VRRP 的默认行是主-主。如果您想要使用 VLAN 上的 VRRP，但不希望 VRRP 的备份网关代表非 VLT 位置中的活动 VRRP 网关流量，请使用 `no vrrp mode active-active` 命令禁用 VRRP 主-主功能。

## 配置

VRRP 指定拥有 LAN 上终端站的下一跳 IP 和 MAC 地址的主要或活动路由器。通过选择过程从虚拟路由器中选择主路由器并将发送的数据包转发到下一跳 IP 地址。如果主路由器出现故障，VRRP 将开始选择过程，以选择一个新的主路由器继续路由流量。

VRRP 数据包使用虚拟路由器 MAC 地址作为源 MAC 地址进行传输。与虚拟路由器关联的虚拟路由器 MAC 地址对于 IPv4 为 00:00:5E:00:01:{VRID} 格式，对于 IPv6 为 00:00:5E:00:02:{VRID} 格式。VRID 是虚拟路由器标识符，允许网络上具有多达 255 个 IPv4 和 IPv6 VRRP 路由器。前四个八位字节为无限制，最后两个 VRID 八位字节对于 IPv4 为 01:{VRID}，对于 IPv6 为 02:{VRID}。最后一个八位字节根据 VRRP 的虚拟路由器标识符发生变化。

### 基本 VRRP 配置



示例显示了使用 VRRP 的典型网络配置。所有主机的默认路由器均设置为虚拟路由器的 IP 地址，而不是将网络 10.10.10.0 上的主机配置为路由器 A 或路由器 B 的 IP 地址作为默认路由器。当 LAN 分段上的任何主机请求互联网访问权限时，它会将数据包发送到虚拟路由器的 IP 地址。

路由器 A 配置为具有虚拟路由器 IP 地址的主路由器，并将所有发送到虚拟路由器的数据包发送到互联网。路由器 B 是备份路由器，并且还使用虚拟路由器 IP 地址进行了配置。

如果主路由器（即路由器 A）不可用（在以太网 1/1/6 上的 LAN 分段与路由器 A 之间的连接发生故障），则备份路由器（即路由器 B）将自动成为主路由器，并响应发送至虚拟 IP 地址的数据包。所有工作站都会继续使用虚拟路由器的 IP 地址来传输发送至互联网的数据包。路由器 B 接收和转发 interface ethernet 1/1/5 上的数据包。在路由器 A 恢复操作之前，VRRP 允许路由器 B 为访问互联网 LAN 分段中的用户提供不间断的服务。

当路由器 A 用于提供网关服务的接口（以太网 1/1/7）停止工作时，路由器 B 不会自动接管。要使路由器 B 成为主路由器，必须配置接口跟踪。当您在接口上配置跟踪并且接口停止工作时，VRRP 组的优先级会降低。VRRP 组的低优先级会触发选择，并且路由器 B 将成为主路由器。有关详细信息，请参阅[接口/对象跟踪](#)。

## 创建虚拟路由器

VRRP 使用 VRID 来识别配置的每个虚拟路由器。在使用 VRRP 之前，必须使用主 IP 地址配置接口并启用。

- 在 INTERFACE 模式下为具有 VRRP 标识符的接口创建虚拟路由器，从 1 到 255。

```
vrrp-group vrrp-id
```

- 在 INTERFACE 模式下删除 VRRP 组。

```
no vrrp-group vrrp-id
```

### 配置 VRRP

```
OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# vrrp-group 254
```

### 验证 VRRP

```
OS10(conf-eth1/1/5-vrid-254)# do show running-configuration
...
!
interface ethernet 1/1/5
ip address 10.10.10.1/24
!
vrrp-group 254
```

```
no shutdown
...
```

## 组版本

配置系统的 VRRP 版本。定义 VRRPv2 — `vrrp version 2` 或 VRRPv3 — `vrrp version 3`。

- 在 INTERFACE 模式下配置 IPv4 的 VRRP 版本。

```
vrrp version
```

### 配置 VRRP 版本 3

```
OS10(config)# vrrp version 3
```

- 将具有最低优先级的交换机设置为 `vrrp version 2`。
- 将具有最高优先级的交换机设置为 `vrrp version 3`。
- 将所有交换机从 `vrrp version 2` 设置为 `vrrp version 3`。

### 将 IPv4 组从 VRRPv2 迁移到 VRRPv3

```
OS10_backup_switch1(config)# vrrp version 2
OS10_backup_switch2(config)# vrrp version 2
```

### 将主交换机设置为 VRRPv3

```
OS10_master_switch(config)# vrrp version 3
```

### 将备份交换机设置为 VRRPv3

```
OS10_backup_switch1(config)# vrrp version 3
OS10_backup_switch2(config)# vrrp version 3
```

## 虚拟 IP 地址

虚拟路由器包含为该 VRRP 组 (VRID) 配置的虚拟 IP 地址。在将虚拟 IP 地址分配给 VRRP 组之前，VRRP 组不会传输 VRRP 数据包。

要激活接口上的 VRRP 组，请为 VRRP 组配置至少一个虚拟 IP 地址。虚拟 IP 地址是虚拟路由器的 IP 地址，不需要 IP 地址掩码。您可以在一个 VRRP 组 (VRID) 上配置最多 10 个虚拟 IP 地址。

这些规则适用于虚拟 IP 地址：

- 虚拟 IP 地址必须与在接口上配置的主要或次要 IP 地址位于同一子网中。虽然单个 VRRP 组可以包含属于接口上配置的多个 IP 子网的虚拟 IP 地址，但 Dell EMC 建议为任何一个 VRRP 组配置属于同一 IP 子网的虚拟 IP 地址。您在其上启用 VRRP 的接口包含 50.1.1.1/24 的主要 IP 地址和 60.1.1.1/24 的辅助 IP 地址。VRRP 组 (VRID 1) 必须包含属于子网 50.1.1.0/24 或子网 60.1.1.0/24 的虚拟地址。
- 如果您在一个接口上配置多个 VRRP 组，则只有其中一个 VRRP 组可以包含接口的主要或次要 IP 地址。

 **注：** OS10 不支持将虚拟 IP 地址配置为与接口的主要或次要 IP 地址相同。不支持优先级 255。

## 配置虚拟 IP 地址

配置虚拟 IP 地址 — 主要 IP 地址和虚拟 IP 地址必须位于同一子网中。

- 在 INTERFACE 模式下配置 VRRP 组，从 1 到 255。

```
vrrp-group vrrp-id
```

- 在 INTERFACE VRRP 模式下为此 VRRP ID 配置虚拟 IP 地址。最多 10 个 IP 地址。

```
virtual-address ip-address1 [...ip-address10]
```

## 配置虚拟 IP 地址

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# no switchport
OS10(config-if-eth1/1/1)# ip address 10.1.1.1/24
OS10(config-if-eth1/1/1)# vrrp-group 10
OS10(config-eth1/1/1-vrid-10)# virtual-address 10.1.1.8
```

## 验证虚拟 IP 地址

```
OS10# show running-configuration
! Version 10.1.9999P.2281
! Last configuration change at Jul 26 12:01:58 2016
!
aaa authentication system:local
!
interface ethernet1/1/1
 ip address 10.1.1.1/24
 no switchport
 no shutdown
!
 vrrp-group 10
 virtual-address 10.1.1.8
!
interface ethernet1/1/2
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/3
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/4
 switchport access vlan 1
--more--
```

## 查看 VRRP 信息

当 VRRP 进程完成初始化时，“State”字段将包含 master 或 backup。

```
OS10# show vrrp brief
Interface Group Priority Preemption State Master-addr Virtual addr(s)

ethernet1/1/1 IPv4 10 100 true master 10.1.1.8 10.1.1.8
```

## 查看 VRRP 组 1

```
OS10# show vrrp 1
Interface : ethernet1/1/1 IPv4 VRID : 1
Primary IP Address : 10.1.1.1 State : master-state
Virtual MAC Address : 00:00:5e:00:01:01
Version : version-3 Priority : 100
Preempt : Hold-time :
Authentication : no-authentication
Virtual IP address :
10.1.1.1
master-transitions : 1 advertise-rcvd : 0
advertise-interval-errors : 0 ip-ttl-errors : 0
priority-zero-pkts-rcvd : 0 priority-zero-pkts-sent : 0
invalid-type-pkts-rcvd : 0 address-list-errors : 0
pkt-length-errors : 0
```

## 在 VRF 中配置虚拟 IP 地址

您可以在非默认 VRF 实例中配置 VRRP 组，并将虚拟地址分配给此组。

要配置特定 VRF 下的 VRRP，请执行以下操作：

1. 创建要在其中配置 VRRP 的非默认 VRF。

```
ip vrf vrf-name
CONFIGURATION 模式
```

2. 在 VRF 配置模式下，输入所需的接口。

```
interface interface-id
VRF CONFIGURATION 模式
```

3. 从 L2 交换模式移除接口。

```
no switchport
INTERFACE CONFIGURATION 模式
```

4. 为您创建的非默认 VRF 分配接口。

```
ip vrf forwarding vrf-name
INTERFACE CONFIGURATION 模式
```

5. 将一个 IP 地址分配给接口。

```
ip address ip-address
INTERFACE CONFIGURATION 模式
```

6. 配置 VRRP 组。

```
vrrp-group group-id
INTERFACE CONFIGURATION 模式
```

7. 为 VRRP ID 配置虚拟 IP 地址。

```
virtual-address ip-address
INTERFACE VRRP 模式
```

```
OS10(config)# ip vrf vrf-test
OS10(config-vrf)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# ip vrf forwarding vrf-test
OS10(conf-if-eth1/1/1)# ip address 10.1.1.1/24
OS10(conf-if-eth1/1/1)# vrrp-group 10
OS10(conf-eth1/1/1-vrid-10)# virtual-address 10.1.1.8
```

从 VRF 移除接口之前，请从与 VRF 关联的接口中删除配置的 VRRP 组。如果不删除已配置的 VRRP 组，这些组在默认 VRF 上保持活动状态，从而导致虚拟 IP 地址配置重复。

## 设置组优先级

具有接口的最高主 IP 地址的路由器将成为**主服务器**。虚拟路由器的默认优先级为 100。如果主路由器发生故障，VRRP 将开始选举过程，以根据下一个优先级选择新的主路由器。如果任何配置的虚拟 IP 地址与接口 IP 地址相匹配，则虚拟路由器优先级将自动设置为 255。

1. 在 INTERFACE 模式下为具有 VRRP 标识符的接口创建虚拟路由器，从 1 到 255。

```
vrrp-group vrrp-id
```

2. 在 INTERFACE VRRP 模式下为 VRRP 组配置优先级编号，从 1 到 254，默认值为 100。

```
priority number
```

### 设置 VRRP 组优先级

```
OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# vrrp-group 254
OS10(conf-eth1/1/5-vrid-254)# priority 200
```

### 验证 VRRP 组优先级

```
OS10(conf-eth1/1/5-vrid-254)# do show vrrp 254

Interface : ethernet1/1/5 IPv4 VRID : 254
Primary IP Address : 10.1.1.1 State : master-state
Virtual MAC Address : 00:00:5e:00:01:01
```

```

Version : version-3 Priority : 200
Preempt : Hold-time :
Authentication : no-authentication
Virtual IP address :
10.1.1.1
master-transitions : 1 advertise-rcvd : 0
advertise-interval-errors : 0 ip-ttl-errors : 0
priority-zero-pkts-rcvd : 0 priority-zero-pkts-sent : 0
invalid-type-pkts-rcvd : 0 address-list-errors : 0
pkt-length-errors : 0

```

## 身份验证

简单身份验证 VRRP 数据包可确保只有受信任的路由器参与 VRRP 进程。启用身份验证时，OS10 在其 VRRP 传输中包括密码。接收路由器使用该密码来验证传输。

您必须使用相同的密码配置 VRRP 组中的所有虚拟路由器。必须启用使用相同密码的身份验证，否则将禁用身份验证。不支持对 VRRPv3 进行身份验证。

1. 在 INTERFACE 模式下为具有 VRRP 标识符的接口创建虚拟路由器，从 1 到 255。

```
vrrp-group vrrp-id
```

2. 在 INTERFACE-VRRP 模式下配置简单文本密码。

```
authentication-type simple-text text
```

simple-text text — 输入关键字和简单文本密码。

### 配置 VRRP 验证

```

OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# vrrp-group 250
OS10(conf-eth1/1/5-vrid-250)# authentication simple-text eureka

```

### 验证 VRRP 身份验证配置

```

OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# vrrp-group 1
OS10(conf-eth1/1/1-vrid-1)# authentication simple-text dell

```

## 禁用抢占

通过禁用抢占进程，防止具有较高优先级的备份路由器成为主路由器。默认情况下，preempt 命令已启用。如果另一个具有较高优先级的路由器联机，命令会强制系统更改主路由器。

您必须使用相同的设置配置 VRRP 组中的所有虚拟路由器。配置启用了抢占的所有路由器或配置已禁用抢占的所有路由器。

1. 在 INTERFACE 模式下为具有 VRRP 标识符的接口创建虚拟路由器，从 1 到 255。

```
vrrp-group vrrp-id
```

2. 阻止优先级较高的任何备份路由器成为 INTERFACE-VRRP 模式下的主路由器。

```
no preempt
```

### 禁用抢占

```

OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# vrrp-group 254
OS10(conf-eth1/1/5-vrid-254)# no preempt

```

### 查看正在运行的配置

```

OS10(conf-eth1/1/5-vrid-254)# do show running-configuration
! Version 10.2.0E

```



```

! Last configuration change at Sep 24
07:17:45 2016
!
debug radius false
snmp-server contact http://www.dell.com/support/softwarecontacts
snmp-server location "United States"
username admin password 6q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/3OJc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIGNs5BKH.
aaa authentication system:local
!
interface ethernet1/1/5
 ip address 1.1.1.1/16
 no switchport
 no shutdown
!
vrrp-group 254
 priority 125
 virtual-address 1.1.1.3
 no preempt
!

```

## 通告间隔

默认情况下，主路由器会每隔一秒钟将 VRRP 通告传输到 VRRP 组的所有成员，表示它是正常运行并且是主路由器。

如果 VRRP 组丢失三个连续通告，则选择过程将开始，并且优先级最高的备份虚拟路由器将转换为主路由器。为避免限制 VRRP 通告数据包，Dell EMC 建议将 VRRP 通告间隔增加到高于默认值 1 秒的值。如果您更改一个路由器上 VRRP 通告之间的时间间隔，请在所有参与的路由器上进行更改。

如果配置 VRRP 版本 2，则必须在多个整秒数内配置计时器值。例如，计时器值为 3 秒或 300 厘秒有效且相当。50 厘秒的时间值无效，因为它不是 1 秒的倍数。如果您使用的是 VRRP 版本 3，则必须以 25 个厘秒的倍数配置计时器值。厘秒为 1/100 秒。

- 在 INTERFACE 模式下为具有 VRRP 标识符的接口创建虚拟路由器，从 1 到 255。

```
vrrp-group vrrp-id
```

- 对于 VRRPv2，在 INTERFACE-VRRP 模式下更改通告间隔设置（以秒为单位），从 1 到 255，默认值为 1。

```
advertise-interval seconds
```

- 对于 VRRPv3，更改通告厘秒间隔设置 INTERFACE-VRRP 模式从 25 到 4075，默认值为 100。

```
advertise-interval centisecs centisecs
```

### 更改通告间隔

```

OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# vrrp-group 1
OS10(conf-eth1/1/1-vrid-1)# advertise-interval centisecs 200

```

### 查看正在运行的配置

```

OS10(conf-eth1/1/1-vrid-1)# do show running-configuration

! Version 10.1.9999P.2281
! Last configuration change at Jul 26 12:22:33 2016
!
aaa authentication system:local
!
interface ethernet1/1/1
 ip address 10.1.1.1/16
 no switchport
 no shutdown
!
vrrp-group 1
 advertisement-interval centisecs 200
 priority 200
 virtual-address 10.1.1.1
!

```

```
interface ethernet1/1/2
 switchport access vlan 1
 no shutdown
```

## 接口/对象跟踪

您可以根据虚拟组监控任何接口的状态。OS10 最多支持 10 个磁道组，并且每个磁道组只能跟踪一个接口。

如果跟踪的接口发生故障，则 VRRP 组的优先级会降低到默认值 10（也称为成本）。如果跟踪的接口状态为增长，则 VRRP 组的优先级按优先级成本增加。

VRRP 组的低优先级可能会触发选择。根据 VRRP 组的优先级选择主/备份 VRRP 路由器，跟踪功能可确保最佳 VRRP 路由器是该组的主节点。跟踪组的优先级成本必须小于 VRRP 组的已配置优先级。如果将 VRRP 组配置为拥有优先级为 255 的所有者路由器，则将禁用该组跟踪，而不考虑跟踪的接口的状态。所有者组的优先级始终保持为 255。

对于虚拟组，请使用 `interface` 命令跟踪任何接口的线路协议状态。输入接口类型和 `node/slot/port[:subport]` 信息，或者 VLAN 编号：

- `ethernet` — 物理接口，从 1 到 48
- `vlan` — VLAN 接口，从 1 到 4093

对于虚拟组，请使用 `track` 命令和对象编号跟踪已配置对象的状态。在创建跟踪对象之前，您还可以使用此命令为 VRRP 组配置跟踪对象。在将所跟踪的对象确定为停止状态之前，不会对 VRRP 组的优先级进行任何更改。

## 配置跟踪

要跟踪 VRRP 组中的对象，请使用以下命令：

1. 在 CONFIGURATION 模式下分配对象跟踪唯一 ID 编号，从 1 到 500。

```
track track-id
```

2. 监控跟踪配置模式下的接口。

```
interface ethernet node/slot/port[:subport]
```

### 配置接口跟踪

```
OS10(config)# track 10
OS10(conf-track-10)# interface ethernet 1/1/7 line-protocol
```

### 查看正在运行的配置

```
OS10(conf-track-10)# do show running-configuration

! Version 10.1.9999P.2281
! Last configuration change at Jul 27 03:24:01 2016
!
aaa authentication system:local
!
interface ethernet1/1/1
 ip address 10.1.1.1/16
 no switchport
 no shutdown
!
vrrp-group 1
 priority 200
 virtual-address 10.1.1.1
!
interface ethernet1/1/2
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/3
 switchport access vlan 1
 no shutdown
!
interface ethernet1/1/4
```

```

switchport access vlan 1
no shutdown
!
interface ethernet1/1/5
switchport access vlan 1
no shutdown
!
interface ethernet1/1/6
switchport access vlan 1
no shutdown
!
.....
interface vlan1
no shutdown
!
interface mgmt1/1/1
no shutdown
!
support-assist
!
track 10
interface ethernet1/1/7 line-protocol

```

要将跟踪对象与 VRRP 组关联，请在 VRRP GROUP CONFIGURATION 模式下使用 VRRP `track` 命令。

## VRRP 命令

### advertise-interval

设置 VRRP 通告之间的时间间隔。

|               |                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>advertise-interval [seconds   centisecs centisecs]</code>                                                                                                           |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>seconds</code> — 输入通告间隔（以秒为单位），从 1 到 255。</li> <li><code>centisecs centisecs</code> — （可选）输入 25 的倍数值，从 25 到 4075。</li> </ul> |
| <b>默认</b>     | 1 秒或 100 厘秒                                                                                                                                                               |
| <b>命令模式</b>   | INTERFACE-VRRP                                                                                                                                                            |
| <b>使用情况信息</b> | Dell EMC 建议保留此命令的默认设置。如果您更改一个路由器上 VRRP 通告之间的时间间隔，请在所有路由器上进行更改。此命令的 <code>no</code> 版本将 VRRP 通告计时器间隔设置回其默认值，1 秒或 100 厘秒。                                                   |
| <b>示例</b>     | <pre>OS10(conf-eth1/1/6-vrid-250)# advertise-interval 120 centisecs 100</pre>                                                                                             |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                                                          |

### authentication-type

启用 VRRP 数据交换的身份验证。

|               |                                                                                   |
|---------------|-----------------------------------------------------------------------------------|
| <b>语法</b>     | <code>authentication-type simple-text password</code>                             |
| <b>参数</b>     | <code>simple-text password</code> — 输入简单文本密码。                                     |
| <b>默认</b>     | 已禁用                                                                               |
| <b>命令模式</b>   | INTERFACE-VRRP                                                                    |
| <b>使用情况信息</b> | 在启用身份验证的情况下，OS10 确保只有受信任的路由器加入自治网络中的路由。此命令的 <code>no</code> 版本将禁用 VRRP 数据交换的身份验证。 |
| <b>示例</b>     | <pre>OS10(conf-ethernet1/1/6-vrid-250)# authentication simple-text eureka</pre>   |

支持的版本 10.2.0E or later

preempt

允许或抢占具有较高优先级值的备份路由器成为主路由器。

|        |                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------------------|
| 语法     | preempt                                                                                                                         |
| 参数     | 无                                                                                                                               |
| 默认     | 已启用                                                                                                                             |
| 命令模式   | INTERFACE-VRRP                                                                                                                  |
| 使用情况信息 | VRRP 使用抢占确定 VRRP 备份路由器成为主节点后会发生的状况。默认状况下启用抢占时，如果备份路由器以高于新的主路由器的优先级联机，则 VRRP 将切换到备份。如果禁用了抢占，则仅在主服务器失败时，VRRP 才切换。此命令的 no 版本将禁用抢占。 |
| 示例     | <pre>OS10 (conf-eth1/1/5-vrid-254) # preempt</pre>                                                                              |
| 支持的版本  | 10.2.0E or later                                                                                                                |

priority

为 VRRP 组分配 VRRP 优先级值。VRRP 在主选择过程中使用此值。

|        |                                                                                      |
|--------|--------------------------------------------------------------------------------------|
| 语法     | priority number                                                                      |
| 参数     | number — 输入优先级值，从 1 到 254。                                                           |
| 默认     | 100                                                                                  |
| 命令模式   | INTERFACE-VRRP                                                                       |
| 使用情况信息 | 为保证 VRRP 组变为主节点，请将 VRRP 组的优先级配置为 254（优先级最高），。OS10 不支持优先级 255。此命令的 no 版本将值重置为默认值 100。 |
| 示例     | <pre>OS10 (conf-eth1/1/5-vrid-254) # priority 200</pre>                              |
| 支持的版本  | 10.2.0E or later                                                                     |

show vrrp

显示 VRRP 组信息。

|        |                                                                                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show vrrp [vrf vrf-name] {brief   vrrp-id   ipv6 group-id}                                                                                                                                                                                                                   |
| 参数     | <ul style="list-style-type: none"><li>vrf vrf-name — 显示与指定的 VRF 对应的 VRRP 组信息。</li><li>brief — 显示系统中所有 VRRP 实例的配置信息。</li><li>vrrp-id — 输入 VRRP 组 ID 编号以查看 VRRP 的 IPv4 组操作状态信息，从 1 到 255。</li><li>ipv6 group-id — （可选）输入 VRRP 组 ID 编号，以查看特定 IPv6 组的操作状态信息，从 1 到 255。</li></ul> |
| 默认     | 所有 IPv4 VRRP 组配置                                                                                                                                                                                                                                                             |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                         |
| 使用情况信息 | 显示所有处于活动状态的 VRRP 组。如果没有 VRRP 组处于活动状态，系统将显示 No Active VRRP group。                                                                                                                                                                                                             |
| 示例（简要） | <pre>OS10 # show vrrp brief Interface      Group Priority Preemption State      Master-addr Virtual addr(s)</pre>                                                                                                                                                            |

```

ethernet1/1/1 1 200 true master-state 10.1.1.1 10.1.1.1
```

示例 (IPv6)

```
OS10 # show vrrp ipv6 1
Interface : ethernet1/1/1 IPv6 VRID : 1
Primary IP Address : 10::1 State : master-state
Virtual MAC Address : 00:00:5e:00:02:01
Version : version-3 Priority : 200
Preempt : Hold-time :
Authentication : no-authentication
Virtual IP address :
10::1
master-transitions : 1 advertise-rcvd : 0
advertise-interval-errors : 0 ip-ttl-errors : 0
priority-zero-pkts-rcvd : 0 priority-zero-pkts-sent : 0
invalid-type-pkts-rcvd : 0 address-list-errors : 0
pkt-length-errors : 0
```

支持的版本 10.2.0E or later

track

为跟踪对象指定唯一标识符。

- 语法** track track-id [priority cost [value]]
- 参数**
- track-id — 输入对象跟踪资源 ID 号，从 1 到 500。
  - priority cost value — (可选) 输入要从优先级值减去的成本值，从 1 到 254。
- 默认** 10
- 命令模式** INTERFACE-VRRP
- 使用情况信息** 如果禁用该接口，则从优先级值中减去成本值并强制实施新的主选举。当优先级值低于备份虚拟路由器中的优先级值时此选举过程适用。您只能将一个跟踪对象与一个 VRRP 组关联。此命令的 no 版本会将该值重置为默认值。

**示例**

```
OS10(conf-eth1/1/5-vrid-254)# track 400
```

**示例 (优先级成本)**

```
OS10(conf-eth1/1/5-vrid-254)# track 400 priority-cost 20
```

支持的版本 10.2.0E or later

track interface

监控接口并降低该接口上的 VRRP 组的优先级值 (如果已禁用)。

- 语法** interface {ethernet node/slot/port[:subport]} [line-protocol]
- 参数**
- ethernet node/slot/port[:subport] — (可选) 输入关键字和要跟踪的接口信息。
  - line-protocol — (可选) 跟踪接口行协议运行状态。
- 默认** 已禁用
- 命令模式** EXEC
- 使用情况信息** 在跟踪接口之前分配对象跟踪唯一 ID 编号。使用 line-protocol 参数跟踪接口操作状态信息。此命令的 no 版本会将该值重置为默认值。

**示例**

```
OS10(config)# track 10
OS10(conf-track-10)# interface ethernet 1/1/5 line-protocol
```

支持的版本 10.2.0E or later

## virtual-address

在 VRRP 组中配置最多 10 个虚拟路由器 IP 地址。为 VRRP 组设置至少一个虚拟 IP 地址，以开始发送 VRRP 数据包。

|        |                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>virtual-address ip-address1 [ip-address2...ip-address10]</code>                                                                                                                                                                           |
| 参数     | <ul style="list-style-type: none"><li><code>ip-address1</code> — 以 A.B.C.D 格式输入虚拟路由器的 IP 地址。IP 地址必须与接口的主 IP 地址位于同一子网中。</li><li><code>ip-address2...ip-address10</code> — (可选) 输入虚拟路由器的最多 9 个附加 IP 地址，用空格分隔。IP 地址必须与接口的主 IP 地址位于同一子网中。</li></ul> |
| 默认     | 已启用                                                                                                                                                                                                                                             |
| 命令模式   | INTERFACE-VRRP                                                                                                                                                                                                                                  |
| 使用情况信息 | 在配置虚拟 IP 地址时，VRRP 组仅变为活动状态，并发送 VRRP 数据包。删除虚拟地址时，VRRP 组将停止发送 VRRP 数据包。您可以对在所有 VRRP 组中配置的虚拟地址执行 ping 操作。此命令的 <code>no</code> 版本将删除系统中配置的一个或多个虚拟地址。                                                                                                |
| 示例     | <pre>OS10(conf-eth1/1/5-vrid-254)# virtual address 10.1.1.15</pre>                                                                                                                                                                              |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                |

## vrrp delay reload

设置在系统重新启动后 VRRP 初始化的延迟时间。

|        |                                                                                |
|--------|--------------------------------------------------------------------------------|
| 语法     | <code>vrrp delay reload seconds</code>                                         |
| 参数     | <code>seconds</code> — 输入 VRRP 重新加载时间的秒数，从 0 到 900。                            |
| 默认     | 0                                                                              |
| 命令模式   | CONFIGURATION                                                                  |
| 使用情况信息 | 零秒的 VRRP 延迟加载时间表示没有延迟。此命令配置适用于所有 VRRP 配置的接口。此命令的 <code>no</code> 版本会将该值重置为默认值。 |
| 示例     | <pre>OS10(config)# vrrp delay reload 5</pre>                                   |
| 支持的版本  | 10.4.0E(R1) or later                                                           |

## vrrp-group

为 IPv4 接口或 VLAN 分配 VRRP 组标识号

|           |                                                                                                                             |
|-----------|-----------------------------------------------------------------------------------------------------------------------------|
| 语法        | <code>vrrp-group vrrp-id</code>                                                                                             |
| 参数        | <code>vrrp-id</code> — 输入一个 VRRP 组标识号，从 1 到 255。                                                                            |
| 默认        | 未配置                                                                                                                         |
| 命令模式      | INTERFACE-VRRP                                                                                                              |
| 使用情况信息    | 在配置虚拟 IP 地址时，VRRP 组仅变为活动状态，并发送 VRRP 数据包。删除虚拟地址时，VRRP 组将停止发送 VRRP 数据包。此命令的 <code>no</code> 版本将移除 <code>vrrp-group</code> 配置。 |
| 示例        | <pre>OS10(conf-if-eth1/1/5)# vrrp-group 254</pre>                                                                           |
| 示例 (VLAN) | <pre>OS10(conf-if-vl-10)# vrrp-group 5</pre>                                                                                |
| 支持的版本     | 10.2.0E or later                                                                                                            |

## vrrp-ipv6-group

为 IPv6 接口分配 VRRP 组标识号。

|               |                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>vrrp-ipv6-group vrrp-id</code>                                                                                             |
| <b>参数</b>     | <code>vrrp-id</code> — 输入 VRRP 组标识号，从 1 到 255。                                                                                   |
| <b>默认</b>     | 未配置                                                                                                                              |
| <b>命令模式</b>   | INTERFACE-VRRP                                                                                                                   |
| <b>使用情况信息</b> | 在配置虚拟 IP 地址时，VRRP 组仅变为活动状态，并发送 VRRP 数据包。删除虚拟地址时，VRRP 组将停止发送 VRRP 数据包。此命令的 <code>no</code> 版本将移除 <code>vrrp-ipv6-group</code> 配置。 |
| <b>示例</b>     | <pre>OS10(conf-if-eth1/1/7)# vrrp-ipv6-group 250</pre>                                                                           |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                 |

## vrrp version

设置 IPv4 组的 VRRP 版本。

|               |                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>vrrp version {2   3}</code>                                                                 |
| <b>参数</b>     | <ul style="list-style-type: none"><li>• 2 — 设置为 VRRP 版本 2。</li><li>• 3 — 设置为 VRRP 版本 3。</li></ul> |
| <b>默认</b>     | 未配置                                                                                               |
| <b>命令模式</b>   | CONFIGURATION                                                                                     |
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本将禁用 IPv4 组的 VRRP 版本。                                                       |
| <b>示例</b>     | <pre>OS10(config)# vrrp version 2</pre>                                                           |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                  |

多播是一种技术，允许网络设备在单次传输中将数据发送给一组感兴趣的接收器。例如，此技术广泛用于流式传输视频。通过多播，您可以更有效地使用网络资源，特别是针对带宽消耗的服务，例如音频和视频传输。

OS10 支持 IPv4 网络中的多播功能，并使用以下协议进行多播分发：

- 互联网组管理协议 (IGMP)
- 协议独立多播 (PIM)

## 重要事项

- OS10 支持多播路由 IGMP 和 IPv4 PIM。此版本的 OS10 不支持 IPv6 PIM。
- OS10 支持默认和非默认 VRF 上 PIM 和 IGMP。
- OS10 不支持 S3048-ON 平台上的多播路由。
- S4248FB-ON 和 S4248FBL-ON 平台上不支持多播泛洪控制。

## 配置多播路由

配置多播路由包含两个步骤，即在第 3 层 (L3) 接口上配置多播路由和启用 PIM 稀疏模式 (PIM-SM)。以下过程介绍了如何配置多播路由。

有关 IGMP 和 PIM 功能配置的详细信息，请参阅[互联网组管理协议](#)和[协议独立多播](#)。

### 注：

多播泛洪限制功能默认已启用。为确保不会发生任何流量丢弃，Dell EMC 建议您执行以下操作之一：

- 禁用在 VLAN 上没有 IGMP 接收器的两个 PIM 路由器的 VLAN 上 IGMP 侦听。
- 将 PIM 路由器之间的接口配置为静态 mrouter 端口。

1. 为 IPv4 网络启用多播路由。

```
OS10# configure terminal
OS10(config)# ip multicast-routing
```

2. 在 VLAN 接口上配置 IP 地址。

```
OS10(config)# interface vlan 2
OS10(conf-if-vl-2)# ip address 1.1.1.2/24
```

3. 在 L3 接口上启用 PIM 稀疏模式。

```
OS10(config)# interface vlan 2
OS10(conf-if-vl-2) ip pim sparse-mode
```

4. 在 CONFIGURATION 模式下，静态配置集合点 (RP) IP 地址，并指定多播组地址范围。可以跨 PIM 域访问 RP IP 地址。

```
OS10(config)# ip pim rp-address 171.1.1.1 group-address 225.1.1.3/32
```

在网络中的所有节点上配置 RP 地址和多播组地址。



# 未知的多播泛洪控制

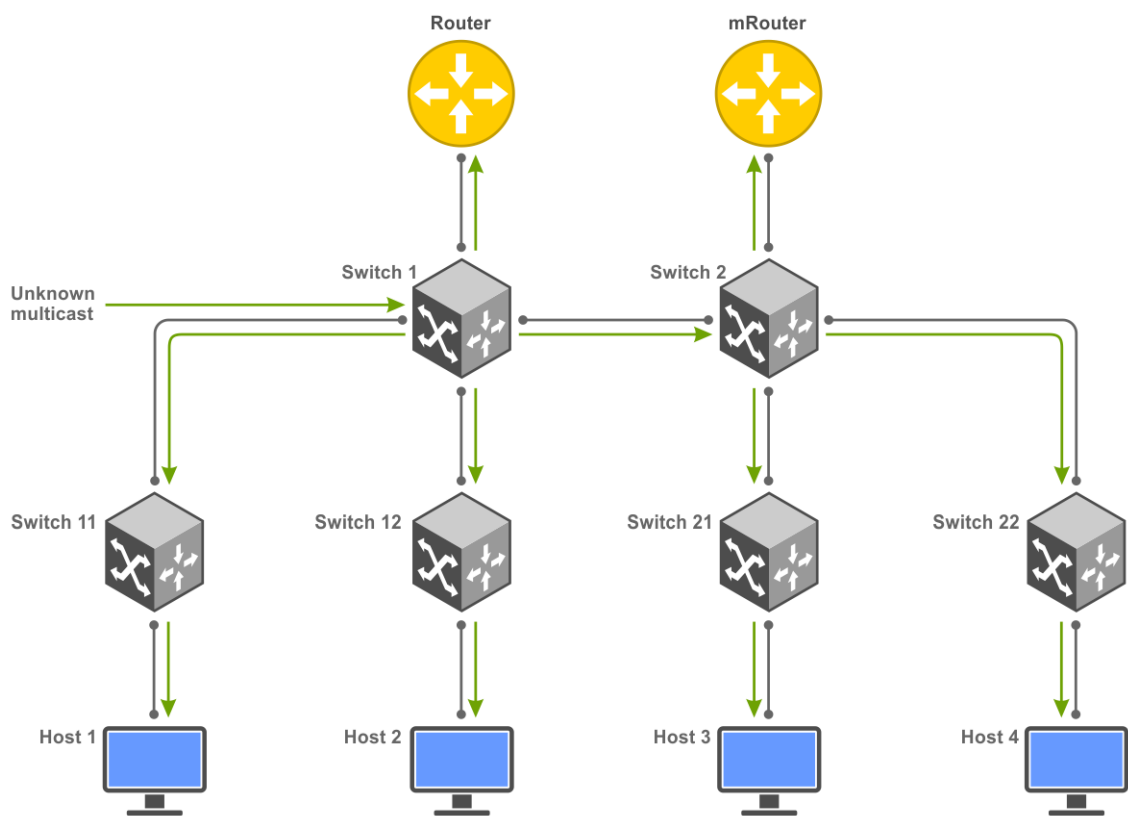
通过未知的多播泛洪控制功能，系统只能将未知的多播数据包转发至多播路由器 (mrouter)。

当您启用多播侦听时，OS10 会将已了解目标的多播帧转发给其预期的收件人。当系统收到其目标未知的多播帧时，将会使特定 VLAN 的所有端口的帧泛洪。接收这些多播帧的所有主机都必须对其进行处理。通过多播泛洪控制，系统仅将未知的多播帧转发到通向 mrouter 的接口。然后，mrouter 可以将流量转发到目标。

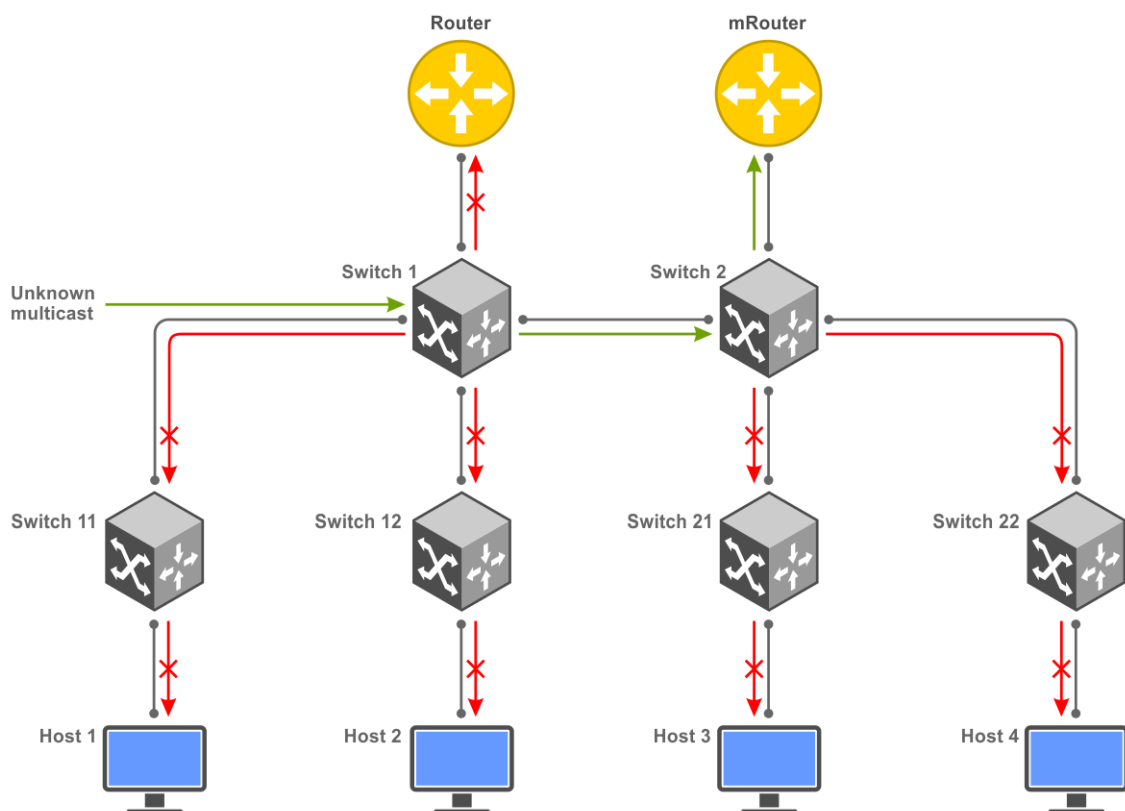
要使多播泛洪控制正常工作，您必须同时在系统上启用 IGMP 和 MLD 侦听。默认情况下，多播泛洪控制、IGMP 侦听和 MLD 侦听均已启用。

**注：**在 Dell EMC PowerSwitch S4248FB-ON 和 S4248FBL-ON 交换机上不支持多播泛洪控制功能。

下文介绍了在所有交换机的所有端口上充斥多播帧的情形。网络中的交换机和主机不需要接收这些帧，因为它们不是预期目标。



通过多播泛洪控制，多播帧（其目标未知）将仅转发到指定的 mrouter 端口。OS10 基于接收 IGMP 成员查询的接口动态了解 mrouter 接口。您也可以使用 `ip igmp snooping mrouter` 和 `ipv6 mld snooping mrouter` 命令静态配置 mrouter 接口。



## 启用多播泛洪控制

默认情况下，OS10 上已启用多播泛洪控制。如果已禁用，请使用以下过程启用多播泛洪控制：

1. 配置 IGMP 侦听。要了解如何配置 IGMP 侦听，请参阅 [IGMP 侦听](#) 部分。
2. 配置 MLD 侦听。要了解如何配置 MLD 侦听，请参阅 [MLD 侦听](#) 部分。
3. 启用多播泛洪控制功能。

```
OS10(config)# multicast snooping flood-restrict
```

## 多播命令

### 多播侦听泛洪限制

为 IGMP 侦听和 MLD 侦听启用多播侦听泛洪控制。

**语法** `multicast snooping flood-restrict`

此命令的 `no` 版本将禁用多播泛洪控制。

**参数** 无

**默认** 已启用

**命令模式** CONFIGURATION

**使用情况信息** 默认情况下，多播侦听泛洪控制、IGMP 侦听和 MLD 侦听功能处于启用状态。

要使多播泛洪限制在 VLAN 上有效，必须在全局和 VLAN 级别启用 IGMP 侦听和 MLD 侦听。

要禁用多播侦听泛洪控制，请使用 `no multicast snooping flood-restrict` 命令。

#### 示例

```
OS10(config)# multicast snooping flood-restrict
```

#### 支持的版本

10.4.3.0 or later

## 互联网组管理协议

互联网组管理协议 (IGMP) 是使用 IPv4 网络建立多播组成员身份的通信协议。OS10 支持 IGMPv1、IGMPv2 和 IGMPv3，以管理 IPv4 网络上的多播组成员身份。

IGMP 定期进行查询（默认情况下，每隔 60 秒）将向所有主机发出成员身份查询。主机在响应查询时，将响应发送回查询器以报告其多播组成员身份。交换机将输入一个条目，以将相应的端口标识为特定多播组的成员。

 **注：**多播路由器是启用了多播功能的第 3 层路由器或交换机。

当主机要加入多播组时，它会将 IGMP 消息发送至多播路由器。

每个网络段都有一个 IGMP 查询器，这是一个多播路由器。多播路由器会定期发送 IGMP 查询，以学习哪些多播组处于活动状态，并且在网络上具有成员。

多播路由器将发送以下类型的查询：

- 常规查询 — 学习多播组的监听器。
- 特定于多播地址的查询 — 学习特定多播地址是否有侦听程序。
- 特定于多播地址和源的查询 — 为了学习多播源的指定列表中是否有包含任何侦听程序的任何源。

主机将以下消息发送至多播路由器：

- 版本 1：成员身份报告
- 版本 2：
  - 版本 1 成员身份报告，用于与版本 1 向后兼容性
  - 版本 2 成员身份报告
  - 离开组消息
- 版本 3：
  - 版本 1 成员身份报告，用于与版本 1 向后兼容性
  - 版本 2 成员身份报告，用于与版本 2 向后兼容性
  - 版本 3 成员身份报告
  - 版本 2 离开组消息

版本 3 提供对源筛选的支持。系统报告仅接收来自特定源地址的数据包或除某些特定源地址以外的所有源（将其发送到特定多播地址除外）。

## 标准合规性

- OS10 符合 RFC 1112、2236 和 3376，分别适用于 IGMP 版本 1、2 和 3。
- OS10 使用版本 3 作为默认 IGMP 版本。版本 3 向后兼容版本 1 和 2。

## 重要事项

- OS10 系统不能用作 IGMP 主机或 IGMP 版本 1 查询者。
- OS10 会在启用 PIM 稀疏模式的接口上自动启用 IGMP。

## 支持的 IGMP 版本

IGMP 有三个版本。版本 3 已停用，并且与版本 2 反向兼容；版本 2 已停用版本 1。

OS10 支持以下 IGMP 版本：

- 路由器 — IGMP 版本 2 和 3。默认值为版本 3。
- 主机 — IGMP 版本 1、2 和 3。

在 IGMP 版本 2 中，主机将在特定组成员身份中表达兴趣 (\*, G)。在 IGMP 版本 3 中，主机将在特定组成员身份中表达兴趣，并指定其需要多播流量的源 (S, G)。

## 查询间隔

IGMP 查询会定期发送常规查询，以发现哪些多播组处于活动状态。组必须至少有一个主机处于活动状态。默认情况下，每 60 秒发送一次定期查询消息。您可以使用 `ip igmp query-interval` 命令配置此值。

要配置查询间隔：

```
OS10# configure terminal
OS10# interface vlan120
OS10(conf-if-vl-120)# ip igmp query-interval 60
```

## 最后成员查询间隔

当 IGMP 查询者收到离开消息时，将发送一组特定的查询消息，以确保网络中的任何其他主机对多播流感兴趣。默认情况下，组特定查询消息每 1000 毫秒发送一次。您可以使用 `ip igmp last-member-query-interval` 命令配置此值。

要配置上次成员查询间隔，请执行以下操作：

```
OS10# configure terminal
OS10# interface vlan120
OS10(conf-if-vl-120)# ip igmp last-member-query-interval 200
```

## 最长响应时间

最长响应时间是查询器在采取操作之前等待查询响应的时量。

当主机收到查询时，它不会立即响应，而是启动延迟计时器。延迟时间设置为介于 0 和最长响应时间之间的随机值。当计时器过期时，主机发送响应；在 IGMP 版本 2 中，如果另一台主机在计时器过期之前响应，则计时器无效，不会发送响应。

查询器将通告查询中的最长响应时间。降低此值会缩短保留延迟，但会增加响应突发性，因为在最长响应时间过期之前将发送所有主机成员身份报告。反之，增加此值可减少突发性，但会增加保留延迟。

要配置最长响应时间：

```
OS10# configure terminal
OS10# interface vlan120
OS10(conf-if-vl-120)# ip igmp query-max-resp-time 20
```

## IGMP 即时离开

如果 IGMP 查询者不会收到对组特定或组和源查询的响应，它将根据配置的查询者可靠性值发送另一个查询。此值决定查询者发送消息的次数。如果查询者没有收到响应，将从该子网的传出接口中移除组。

IGMP 即时离开通过使路由器可以在收到离开消息后立即删除接口上的组成员身份，从而缩短保留延迟的时间。即时离开不会在删除条目之前发送特定于组的或组和源的查询。

要配置 IGMP 即时离开：

```
OS10# configure terminal
OS10# interface vlan14
OS10(conf-if-vl-14)# ip igmp immediate-leave
```

## 选择 IGMP 版本

默认情况下，OS10 将启用 IGMP 版本 3。

如果主机需要 3 以外的 IGMP 版本，请使用以下命令选择不同的 IGMP 版本：

```
OS10# configure terminal
OS10# interface vlan12
OS10(conf-if-vl-12)# ip igmp version 3
```

## 查看已启用 IGMP 的接口和组

要查看已启用 IGMP 的接口和组，请使用以下 show 命令。

要查看已启用 IGMP 的接口：

```
OS10# show ip igmp interface
Vlan103 is up, line protocol is up
Internet address is 2.1.1.2
IGMP is enabled on interface
IGMP version is 3
IGMP query interval is 60 seconds
IGMP querier timeout is 130 seconds
IGMP last member query response interval is 1000 ms
IGMP max response time is 10 seconds
IGMP immediate-leave is disabled on this interface
IGMP joins count: 0
IGMP querying router is 2.1.1.1

Vlan105 is up, line protocol is up
Internet address is 3.1.1.2
IGMP is enabled on interface
IGMP version is 3
IGMP query interval is 60 seconds
IGMP querier timeout is 130 seconds
IGMP last member query response interval is 1000 ms
IGMP max response time is 10 seconds
IGMP immediate-leave is disabled on this interface
IGMP joins count: 0
IGMP querying router is 3.1.1.1

Vlan121 is up, line protocol is up
Internet address is 121.1.1.2
IGMP is enabled on interface
IGMP version is 3
IGMP query interval is 60 seconds
IGMP querier timeout is 130 seconds
IGMP last member query response interval is 1000 ms
IGMP max response time is 10 seconds
IGMP immediate-leave is disabled on this interface
IGMP joins count: 100
IGMP querying router is 121.1.1.2
```

要查看 IGMP 组：

```
OS10# show ip igmp groups
Total Number of Groups: 100
IGMP Connected Group Membership
```

| Group Address | Interface | Mode          | Uptime   | Expires  | Last Reporter |
|---------------|-----------|---------------|----------|----------|---------------|
| 225.1.1.1     | vlan121   | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10    |
| 225.1.1.2     | vlan121   | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10    |
| 225.1.1.3     | vlan121   | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10    |
| 225.1.1.4     | vlan121   | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10    |
| 225.1.1.5     | vlan121   | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10    |
| 225.1.1.6     | vlan121   | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10    |
| 225.1.1.7     | vlan121   | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10    |
| 225.1.1.8     | vlan121   | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10    |
| 225.1.1.9     | vlan121   | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10    |

|            |         |               |          |          |            |
|------------|---------|---------------|----------|----------|------------|
| 225.1.1.10 | vlan121 | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10 |
| 225.1.1.11 | vlan121 | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10 |
| 225.1.1.12 | vlan121 | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10 |
| 225.1.1.13 | vlan121 | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10 |
| 225.1.1.14 | vlan121 | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10 |
| 225.1.1.15 | vlan121 | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10 |
| 225.1.1.16 | vlan121 | IGMPv2-Compat | 12:39:00 | 00:01:58 | 121.1.1.10 |

## IGMP 侦听

IGMP 侦听使用 IGMP 数据包中的信息生成将端口与多播组关联的转发表。当交换机收到多播帧时，它们会将其转发给其预期的接收器。OS10 支持对虚拟局域网 (VLAN) 接口进行 IGMP 侦听。

默认情况下，IGMP 侦听已启用，从 OS10 版本 10.4.3.0 生效。

### 配置 IGMP 侦听

- 在 CONFIGURATION 模式下使用 `ip igmp snooping enable` 命令在全局范围内启用 IGMP 侦听。此命令将对所有 VLAN 接口启用 IGMP 侦听。

i

注:

如果配置了 IGMP 侦听，则 OS10 不支持扩展配置文件 VLAN 配置。要在 IGMP 侦听时使用扩展配置文件配置，请使用 `mode 13` 命令。
- (可选) 在 VLAN INTERFACE 模式下，使用 `no ip igmp snooping` 命令禁用对特定 VLAN 接口的 IGMP 侦听。
- (可选) 默认情况下，多播淹没控制已启用。要禁用多播泛洪限制功能，请在 CONFIGURATION 模式下使用 `no multicast snooping flood-restrict` 命令。要全局重新启用该功能，请在 CONFIGURATION 模式下使用 `multicast snooping flood-restrict` 命令。
- 在网络中，侦听交换机连接到发送 IGMP 查询的多播路由器。在没有多播路由器的第 2 层网络上，您可以将侦听交换机配置为充当查询器。在 VLAN CONFIGURATION 模式下使用 `ip igmp snooping querier` 命令发送查询。
- OS10 将根据接收的 IGMP 成员查询的接口动态学习多播路由器接口。要静态分配多播路由器接口，请在 VLAN INTERFACE 模式下使用 `ip igmp snooping mrouter interface interface-type` 命令。

i

注:

IGMP 侦听会根据接收的 IGMP 查询动态检测 mrouter 接口。如果有多个连接到侦听交换机的多播路由器，其中一个将发送 IGMP 查询，并且连接到该路由器的接口将动态学习为 mrouter 端口。您必须将连接到其他多播路由器的接口配置为静态 mrouter 端口。
- (可选) 在 VLAN INTERFACE 模式下，使用 `ip igmp version version-number` 命令配置 IGMP 版本。
- (可选) 快速离开选项允许 IGMP 侦听交换机在接收离开消息时立即从多播组中删除接口。在 VLAN INTERFACE 模式下，使用 `ip igmp snooping fast-leave` 命令启用快速离开。
- (可选) 在 VLAN INTERFACE 模式下，使用 `ip igmp snooping query-interval query-interval-time` 命令为发送 IGMP 常规查询配置时间间隔。
- (可选) 在 VLAN 接口模式下，使用 `ip igmp snooping query-max-resp-time query-response-time` 命令，配置响应 IGMP 查询中通告的查询的最长时间。
- (可选) 在 VLAN INTERFACE 模式下，使用 `ip igmp snooping last-member-query-interval query-interval-time` 命令，配置在组特定 IGMP 查询消息之间的时间间隔。

### IGMP 侦听配置

```
OS10(config)# ip igmp snooping enable
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ip igmp snooping mrouter interface ethernet 1/1/32
OS10(conf-if-vl-100)# ip igmp snooping querier
OS10(conf-if-vl-100)# ip igmp version 3
OS10(conf-if-vl-100)# ip igmp snooping fast-leave
OS10(conf-if-vl-100)# ip igmp snooping query-interval 60
OS10(conf-if-vl-100)# ip igmp snooping query-max-resp-time 10
OS10(conf-if-vl-100)# ip igmp snooping last-member-query-interval 1000
```

### 查看 IGMP 侦听信息

```
OS10# show ip igmp snooping groups
Total Number of Groups: 480
IGMP Connected Group Membership
Group Address Interface Mode Expires
225.1.0.0 vlan3531 IGMPv2-Compat 00:01:35
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.1 vlan3531 IGMPv2-Compat 00:01:35
```

```

Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.2 vlan3531 IGMPv2-Compat 00:01:35
Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.3 vlan3531 IGMPv2-Compat 00:01:35
Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.4 vlan3531 IGMPv2-Compat 00:01:35
Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.5 vlan3531 IGMPv2-Compat 00:01:35
Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.6 vlan3531 IGMPv2-Compat 00:01:35
Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.7 vlan3531 IGMPv2-Compat 00:01:35
Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.8 vlan3531 IGMPv2-Compat 00:01:35
Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
225.1.0.9 vlan3531 IGMPv2-Compat 00:01:35
Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
--more--

```

<<Output Truncated>>

```

OS10# show ip igmp snooping interface vlan 2
Vlan2 is up, line protocol is up
IGMP version is 3
IGMP snooping is enabled on interface
IGMP snooping query interval is 60 seconds
IGMP snooping querier timeout is 130 seconds
IGMP snooping last member query response interval is 1000 ms
IGMP Snooping max response time is 10 seconds
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is disabled on this interface
Multicast flood-restrict is enabled on this interface

```

```

show ip igmp snooping mrouter
Interface Router Ports
Vlan 100 ethernet 1/1/32

```

## IGMP 命令

### clear ip igmp groups

清除组高速缓存表中的条目。

|        |                                       |
|--------|---------------------------------------|
| 语法     | clear ip igmp [vrf vrf-name] groups   |
| 参数     | vrf vrf-name— 输入关键字 vrf，然后输入 VRF 的名称。 |
| 默认     | 无                                     |
| 命令模式   | EXEC                                  |
| 使用情况信息 | 无                                     |
| 示例     | OS10# clear ip igmp groups            |

支持的版本 10.4.3.0 or later

### ip igmp immediate-leave

启用 IGMP 即时离开。

|    |                         |
|----|-------------------------|
| 语法 | ip igmp immediate-leave |
| 参数 | 无                       |

|               |                                                                                                                                     |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>默认</b>     | 无                                                                                                                                   |
| <b>命令模式</b>   | INTERFACE                                                                                                                           |
| <b>使用情况信息</b> | 在从成员身份数据库删除组之前，查询者会发送一些特定于组的查询。如果需要立即从成员身份数据库中删除组，请使用 <code>ip igmp immediate-leave</code> 命令。此命令的 <code>no</code> 版本将禁用 IGMP 即时离开。 |
| <b>示例</b>     | <pre>OS10# configure terminal OS10# interface vlan11 OS10(conf-if-vl-11)# ip igmp immediate-leave</pre>                             |
| <b>支持的版本</b>  | 10.4.3.0 or later                                                                                                                   |

## ip igmp last-member-query-interval

更改最后成员查询间隔，这是为了响应留下组消息而发送的特定于组的查询中包含的最长响应时间。此最后成员查询间隔是特定于组的查询消息之间的时间间隔。

|               |                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ip igmp last-member-query-interval <i>milliseconds</i></code>                                                    |
| <b>参数</b>     | <i>milliseconds</i> — 输入配置特定于组的查询消息之间的时间间隔的时间量（以毫秒为单位）。范围从 100 到 65535。                                                |
| <b>默认</b>     | 1000 毫秒                                                                                                                |
| <b>命令模式</b>   | INTERFACE                                                                                                              |
| <b>使用情况信息</b> | 无                                                                                                                      |
| <b>示例</b>     | <pre>OS10# configure terminal OS10# interface vlan11 OS10(conf-if-vl-11)# ip igmp last-member-query-interval 200</pre> |
| <b>支持的版本</b>  | 10.4.3.0 or later                                                                                                      |

## ip igmp query-interval

更改查询器发送 IGMP 常规查询的频率。

|               |                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ip igmp query-interval <i>seconds</i></code>                                                        |
| <b>参数</b>     | <i>seconds</i> — 以秒为单位输入配置 IGMP 常规查询的时间间隔的时间量。范围为 1 到 18000。                                              |
| <b>默认</b>     | 60 秒                                                                                                      |
| <b>命令模式</b>   | INTERFACE                                                                                                 |
| <b>使用情况信息</b> | 无                                                                                                         |
| <b>示例</b>     | <pre>OS10# configure terminal OS10# interface vlan12 OS10(conf-if-vl-12)# ip igmp query-interval 60</pre> |
| <b>支持的版本</b>  | 10.4.3.0 or later                                                                                         |

## ip igmp query-max-resp-time

配置在常规查询中通告的最长查询响应时间。

|           |                                                         |
|-----------|---------------------------------------------------------|
| <b>语法</b> | <code>ip igmp query-max-resp-time <i>seconds</i></code> |
| <b>参数</b> | <i>seconds</i> — 输入时间量（以秒为单位），从 1 到 25。                 |
| <b>默认</b> | 10 秒                                                    |



|               |                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------|
| <b>命令模式</b>   | INTERFACE                                                                                                      |
| <b>使用情况信息</b> | IGMP 查询的最长响应时间值必须小于 IGMP 查询间隔值。命令的 <code>no</code> 形式可配置默认值。                                                   |
| <b>示例</b>     | <pre>OS10# configure terminal OS10# interface vlan14 OS10(conf-if-vl-14)# ip igmp query-max-resp-time 20</pre> |
| <b>支持的版本</b>  | 10.4.3.0 or later                                                                                              |

## ip igmp snooping enable

启用全局 IGMP 侦听。

|               |                                                  |
|---------------|--------------------------------------------------|
| <b>语法</b>     | <code>ip igmp snooping enable</code>             |
| <b>参数</b>     | 无                                                |
| <b>默认</b>     | 已启用                                              |
| <b>命令模式</b>   | CONFIGURATION                                    |
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本将禁用 IGMP 侦听。              |
| <b>示例</b>     | <pre>OS10(config)# ip igmp snooping enable</pre> |
| <b>支持的版本</b>  | 10.4.0E(R1) or later                             |

## ip igmp snooping

对指定 VLAN 接口启用 IGMP 侦听。

|               |                                                                                                               |
|---------------|---------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ip igmp snooping</code>                                                                                 |
| <b>参数</b>     | 无                                                                                                             |
| <b>默认</b>     | 取决于全局配置。                                                                                                      |
| <b>命令模式</b>   | VLAN INTERFACE                                                                                                |
| <b>使用情况信息</b> | 当您在全局范围内启用 IGMP 侦听时，该配置适用于所有 VLAN 接口。您可以禁用对指定 VLAN 接口的 IGMP 侦听。此命令的 <code>no</code> 版本将禁用指定 VLAN 接口上 IGMP 侦听。 |
| <b>示例</b>     | <pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# no ip igmp snooping</pre>                         |
| <b>支持的版本</b>  | 10.4.0E(R1) or later                                                                                          |

## ip igmp snooping fast-leave

为指定 VLAN 启用快速离开 IGMP 侦听。

|               |                                                                          |
|---------------|--------------------------------------------------------------------------|
| <b>语法</b>     | <code>ip igmp snooping fast-leave</code>                                 |
| <b>参数</b>     | 无                                                                        |
| <b>默认</b>     | 已禁用                                                                      |
| <b>命令模式</b>   | VLAN INTERFACE                                                           |
| <b>使用情况信息</b> | 快速离开选项允许 IGMP 侦听交换机在接收离开消息时立即从多播组中删除接口。此命令的 <code>no</code> 版本将禁用快速离开功能。 |

### 示例

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ip igmp snooping fast-leave
```

**支持的版本** 10.4.1.0 or later

## ip igmp snooping last-member-query-interval

配置特定于组的 IGMP 查询消息之间的时间间隔。

**语法** `ip igmp snooping last-member-query-interval query-interval-time`

**参数** *query-interval-time*— 输入查询时间间隔（以毫秒为单位），从 100 到 65535。

**默认** 1000 毫秒

**命令模式** VLAN INTERFACE

**使用情况信息** 此命令的 `no` 版本将最后成员查询间隔时间重置为默认值。

### 示例

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ip igmp snooping last-member-query-interval 2500
```

**支持的版本** 10.4.1.0 or later

## ip igmp snooping mrouter

配置指定 VLAN 接口上的多播路由器端口。

**语法** `ip igmp snooping mrouter interface interface-type`

**参数** *interface-type*— 输入接口类型的详细信息。该接口必须是 VLAN 的成员。

**默认** 未配置

**命令模式** VLAN INTERFACE

**使用情况信息** 此命令的 `no` 版本将从 VLAN 成员端口移除多播路由器配置。

### 示例

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ip igmp snooping mrouter interface ethernet 1/1/1
```

**支持的版本** 10.4.0E(R1) or later

## ip igmp snooping querier

为指定的 VLAN 接口启用 IGMP 查询器处理。

**语法** `ip igmp snooping querier`

**参数** 无

**默认** 未配置

**命令模式** VLAN INTERFACE

**使用情况信息** 此命令的 `no` 版本会在 VLAN 接口上禁用 IGMP 查询器。

### 示例

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ip igmp snooping querier
```

**支持的版本** 10.4.0E(R1) or later

## ip igmp snooping query-interval

配置发送 IGMP 常规查询的时间间隔。

|        |                                                                         |
|--------|-------------------------------------------------------------------------|
| 语法     | <code>ip igmp snooping query-interval <i>query-interval-time</i></code> |
| 参数     | <i>query-interval-time</i> — 输入间隔时间（以秒为单位），从 2 到 18000。                 |
| 默认     | 60 秒                                                                    |
| 命令模式   | VLAN INTERFACE                                                          |
| 使用情况信息 | 此命令的 <code>no</code> 版本将查询间隔重置为默认值。                                     |
| 示例     |                                                                         |

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ip igmp snooping query-interval 120
```

支持的版本 10.4.1.0 or later

## ip igmp snooping query-max-resp-time

配置响应 IGMP 查询中通告的查询的最长时间。

|        |                                                                              |
|--------|------------------------------------------------------------------------------|
| 语法     | <code>ip igmp snooping query-max-resp-time <i>query-response-time</i></code> |
| 参数     | <i>query-response-time</i> — 以秒为单位输入查询响应时间，从 1 到 25。                         |
| 默认     | 10 秒                                                                         |
| 命令模式   | VLAN INTERFACE                                                               |
| 使用情况信息 | 此命令的 <code>no</code> 版本将查询响应时间重置为默认值。                                        |
| 示例     |                                                                              |

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ip igmp snooping query-max-resp-time 15
```

支持的版本 10.4.1.0 or later

## ip igmp version

配置 IGMP 版本。

|        |                                                    |
|--------|----------------------------------------------------|
| 语法     | <code>ip igmp version <i>version-number</i></code> |
| 参数     | <i>version-number</i> — 将版本号输入为 2 或 3。             |
| 默认     | 3                                                  |
| 命令模式   | VLAN INTERFACE                                     |
| 使用情况信息 | 此命令的 <code>no</code> 版本将版本号重置为默认值。                 |
| 示例     |                                                    |

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ip igmp version 2
```

支持的版本 10.4.1.0 or later

## show ip igmp groups

显示 IGMP 组。

|    |                                                                                                                                                                              |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>show ip igmp [<i>vrf vrf-name</i>] groups [<i>group-address</i> [<i>detail</i>]   <i>detail</i>   <i>interface-name</i> [<i>group-address</i> [<i>detail</i>]]]</code> |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|        |                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 参数     | <ul style="list-style-type: none"> <li><code>vrf vrf-name</code>— 输入关键字 <code>vrf</code>，然后输入 VRF 的名称。</li> <li><code>group-address</code>— 输入以点分隔的十进制格式的组地址以查看特定的组信息。</li> <li><code>interface-name</code>— 输入接口名称。</li> </ul>                                                                                                                                          |
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                                        |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                     |
| 使用情况信息 | <p><code>show ip igmp groups</code> 命令将显示 IGMP 数据库、所有接口上所有组的已配置条目、特定接口上的所有组或特定接口上特定组。此命令显示以下内容：</p> <ul style="list-style-type: none"> <li>Group address — 列出 IGMP 组的多播地址</li> <li>Interface — 列出接口类型、插槽和端口号</li> <li>Mode — 显示已使用的 IGMP 版本</li> <li>Uptime — 显示组已运行的时间量。</li> <li>Expires — 显示条目过期之前的时间</li> <li>Last reporter — 显示作为 IGMP 组成员的最后一个主机的 IP 地址</li> </ul> |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show ip igmp groups Total Number of Groups: 100 IGMP Connected Group Membership Group Address Interface      Mode           Uptime        Expires       Last Reporter 225.1.1.1      vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.2      vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.3      vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.4      vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.5      vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.6      vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.7      vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.8      vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.9      vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.10     vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.11     vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.12     vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.13     vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.14     vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.15     vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10 225.1.1.16     vlan121        IGMPv2-Compat 12:39:00      00:01:58     121.1.1.10</pre> |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

支持的版本 10.4.3.0 or later

## show ip igmp interface

显示有关所有已启用 IGMP 的接口的信息。

|        |                                                                                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show ip igmp [vrf vrf-name] interface name</code>                                                                                                                                        |
| 参数     | <ul style="list-style-type: none"> <li><code>vrf vrf-name</code>— 输入关键字 <code>vrf</code>，然后输入 VRF 的名称。</li> <li><code>interface name</code>— 输入关键字 <code>interface</code>，然后输入接口名称。</li> </ul> |
| 默认     | 无                                                                                                                                                                                              |
| 命令模式   | EXEC                                                                                                                                                                                           |
| 使用情况信息 | 无                                                                                                                                                                                              |

|    |                                                                                                                                                                                                                                                                                                                                                                                             |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show ip igmp interface Vlan103 is up, line protocol is up Internet address is 2.1.1.2 IGMP is enabled on interface IGMP version is 3 IGMP query interval is 60 seconds IGMP querier timeout is 130 seconds IGMP last member query response interval is 1000 ms IGMP max response time is 10 seconds IGMP immediate-leave is disabled on this interface IGMP joins count: 0</pre> |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```

IGMP querying router is 2.1.1.1

Vlan121 is up, line protocol is up
Internet address is 121.1.1.2
IGMP is enabled on interface
IGMP version is 3
IGMP query interval is 60 seconds
IGMP querier timeout is 130 seconds
IGMP last member query response interval is 1000 ms
IGMP max response time is 10 seconds
IGMP immediate-leave is disabled on this interface
IGMP joins count: 100
IGMP querying router is 121.1.1.2

```

**支持的版本** 10.4.3.0 or later

## show ip igmp snooping groups

显示 IGMP 侦听组成员身份详细信息。

**语法** `show ip igmp snooping groups [detail | [vlan vlan-id [detail | ip-address]]]`

- 参数**
- *vlan-id*— (可选) 输入 VLAN ID, 从 1 到 4093。
  - *detail* — (可选) 输入 *detail* 以显示 IGMPv3 源信息。
  - *ip-address*— (可选) 输入多播组的 IP 地址。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```

OS10# show ip igmp snooping groups
Total Number of Groups: 480
IGMP Connected Group Membership
Group Address Interface Mode
Expires
225.1.0.0 vlan3031 IGMPv2-Compat
00:01:26
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.1 vlan3031 IGMPv2-Compat
00:01:26
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.2 vlan3031 IGMPv2-Compat
00:01:26
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.3 vlan3031 IGMPv2-Compat
00:01:26
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.4 vlan3031 IGMPv2-Compat
00:01:26
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.5 vlan3031 IGMPv2-Compat
00:01:26
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.6 vlan3031 IGMPv2-Compat
00:01:26
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.7 vlan3031 IGMPv2-Compat
00:01:26
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.8 vlan3031 IGMPv2-Compat
00:01:26
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.9 vlan3031 IGMPv2-Compat
00:01:26
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.10 vlan3031 IGMPv2-Compat

```

```
00:01:26
--more--
<<Output Truncated>>
```

#### 示例 (使用 VLAN)

```
OS10# show ip igmp snooping groups vlan 3031
Total Number of Groups: 12
IGMP Connected Group Membership
Group Address Interface Mode
Expires
225.1.0.0 vlan3031 IGMPv2-Compat
00:01:30
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.1 vlan3031 IGMPv2-Compat
00:01:30
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.2 vlan3031 IGMPv2-Compat
00:01:30
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.3 vlan3031 IGMPv2-Compat
00:01:30
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.4 vlan3031 IGMPv2-Compat
00:01:30
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.5 vlan3031 IGMPv2-Compat
00:01:30
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.6 vlan3031 IGMPv2-Compat
00:01:30
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.7 vlan3031 IGMPv2-Compat
00:01:30
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.8 vlan3031 IGMPv2-Compat
00:01:30
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.9 vlan3031 IGMPv2-Compat
00:01:30
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
225.1.0.10 vlan3031 IGMPv2-Compat
00:01:30
--more--
```

#### 示例 (使用 VLAN 和多播 IP 地址)

```
OS10# show ip igmp snooping groups vlan 3031 225.1.0.0
IGMP Connected Group Membership
Group Address Interface Mode
Expires
225.1.0.0 vlan3031 IGMPv2-Compat
00:01:44
 Member-ports :port-channel51,ethernet1/1/51:1,ethernet1/1/52:1
```

#### 示例 (包含详细信息)

```
OS10# show ip igmp snooping groups detail
Interface vlan3041
Group 232.11.0.0
Source List
 101.41.0.21
 Member Port Mode Uptime Expires
 port-channel51 Include 1d:20:26:07 00:01:41
 ethernet1/1/51:1 Include 1d:20:26:05 00:01:46
 ethernet1/1/52:1 Include 1d:20:26:08 00:01:46

Interface vlan3041
Group 232.11.0.1
Source List
 101.41.0.21
 Member Port Mode Uptime Expires
 port-channel51 Include 1d:20:26:07 00:01:41
 ethernet1/1/51:1 Include 1d:20:26:05 00:01:46
```

|                               |             |             |          |
|-------------------------------|-------------|-------------|----------|
| ethernet1/1/52:1              | Include     | 1d:20:26:08 | 00:01:46 |
| Interface                     | vlan3041    |             |          |
| Group                         | 232.11.0.2  |             |          |
| Source List                   | 101.41.0.21 |             |          |
| Member Port                   | Mode        | Uptime      | Expires  |
| port-channel51                | Include     | 1d:20:26:07 | 00:01:41 |
| --more-- <<Output Truncated>> |             |             |          |

## 示例（使用 VLAN）

|                                                     |             |             |          |
|-----------------------------------------------------|-------------|-------------|----------|
| OS10# show ip igmp snooping groups vlan 3041 detail |             |             |          |
| Interface                                           | vlan3041    |             |          |
| Group                                               | 232.11.0.0  |             |          |
| Source List                                         | 101.41.0.21 |             |          |
| Member Port                                         | Mode        | Uptime      | Expires  |
| port-channel51                                      | Include     | 1d:20:26:07 | 00:01:41 |
| ethernet1/1/51:1                                    | Include     | 1d:20:26:05 | 00:01:46 |
| ethernet1/1/52:1                                    | Include     | 1d:20:26:08 | 00:01:46 |
| Interface                                           | vlan3041    |             |          |
| Group                                               | 232.11.0.1  |             |          |
| Source List                                         | 101.41.0.21 |             |          |
| Member Port                                         | Mode        | Uptime      | Expires  |
| port-channel51                                      | Include     | 1d:20:26:07 | 00:01:41 |
| ethernet1/1/51:1                                    | Include     | 1d:20:26:05 | 00:01:46 |
| ethernet1/1/52:1                                    | Include     | 1d:20:26:08 | 00:01:46 |
| Interface                                           | vlan3041    |             |          |
| Group                                               | 232.11.0.2  |             |          |
| Source List                                         | 101.41.0.21 |             |          |
| Member Port                                         | Mode        | Uptime      | Expires  |
| port-channel51                                      | Include     | 1d:20:26:07 | 00:01:41 |
| --more--                                            |             |             |          |

## 示例（使用 VLAN 和多播 IP 地址）

|                                                                |             |             |          |
|----------------------------------------------------------------|-------------|-------------|----------|
| OS10# show ip igmp snooping groups vlan 3041 232.11.0.0 detail |             |             |          |
| Interface                                                      | vlan3041    |             |          |
| Group                                                          | 232.11.0.0  |             |          |
| Source List                                                    | 101.41.0.21 |             |          |
| Member Port                                                    | Mode        | Uptime      | Expires  |
| port-channel51                                                 | Include     | 1d:20:27:36 | 00:01:09 |
| ethernet1/1/51:1                                               | Include     | 1d:20:27:34 | 00:01:07 |
| ethernet1/1/52:1                                               | Include     | 1d:20:27:37 | 00:01:07 |

支持的版本 10.4.0E(R1) or later

## show ip igmp snooping interface

显示 IGMP 侦听接口的详细信息。

**语法** show ip igmp snooping interface [vlan *vlan-id*]

**参数** *vlan-id*—（可选）输入 VLAN ID，从 1 到 4093。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** S4248FB-ON 和 S4248FBL-ON 设备上的多播泛洪控制功能不可。

## 示例

|                                       |        |               |       |
|---------------------------------------|--------|---------------|-------|
| OS10# show ip igmp snooping interface |        |               |       |
| Vlan3031                              | is up, | line protocol | is up |
| IGMP version                          | is 3   |               |       |

```

IGMP snooping is enabled on interface
IGMP snooping query interval is 60 seconds
IGMP snooping querier timeout is 130 seconds
IGMP snooping last member query response interval is 1000 ms
IGMP Snooping max response time is 10 seconds
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is enabled on this interface

Vlan3032 is up, line protocol is up
IGMP version is 3
IGMP snooping is enabled on interface
IGMP snooping query interval is 60 seconds
IGMP snooping querier timeout is 130 seconds
IGMP snooping last member query response interval is 1000 ms
IGMP Snooping max response time is 10 seconds
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is enabled on this interface

Vlan3033 is up, line protocol is up
IGMP version is 3
--more--
<<Output Truncated>>

```

```

OS10# show ip igmp snooping interface
Vlan2 is up, line protocol is up
IGMP version is 3
IGMP snooping is enabled on interface
IGMP snooping query interval is 60 seconds
IGMP snooping querier timeout is 130 seconds
IGMP snooping last member query response interval is 1000 ms
IGMP Snooping max response time is 10 seconds
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is disabled on this interface
Multicast snooping flood-restrict is enabled on this interface

Vlan3 is up, line protocol is up
IGMP version is 3
IGMP snooping is enabled on interface
IGMP snooping query interval is 60 seconds
IGMP snooping querier timeout is 130 seconds
IGMP snooping last member query response interval is 1000 ms
IGMP Snooping max response time is 10 seconds
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is disabled on this interface
Multicast snooping flood-restrict is enabled on this interface

```

## **示例 (使用 VLAN)**

```

OS10# show ip igmp snooping interface vlan 3031
Vlan3031 is up, line protocol is up
IGMP version is 3
IGMP snooping is enabled on interface
IGMP snooping query interval is 60 seconds
IGMP snooping querier timeout is 130 seconds
IGMP snooping last member query response interval is 1000 ms
IGMP Snooping max response time is 10 seconds
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is enabled on this interface

```

```

OS10# show ip igmp snooping interface vlan 3031
Vlan3031 is up, line protocol is up
IGMP version is 3
IGMP snooping is enabled on interface
IGMP snooping query interval is 60 seconds
IGMP snooping querier timeout is 130 seconds
IGMP snooping last member query response interval is 1000 ms
IGMP Snooping max response time is 10 seconds
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is enabled on this interface
Multicast snooping flood-restrict is enabled on this interface

```



**支持的版本** 10.4.0E(R1) or later 更新了命令以显示 10.4.3.0 or later 上的多播泛洪限制状态

## show ip igmp snooping mrouter

显示多播路由器端口的详细信息。

|               |                                                      |
|---------------|------------------------------------------------------|
| <b>语法</b>     | show ip igmp snooping mrouter [vlan <i>vlan-id</i> ] |
| <b>参数</b>     | <i>vlan-id</i> — (可选) 输入 VLAN ID, 从 1 到 4093。        |
| <b>默认</b>     | 未配置                                                  |
| <b>命令模式</b>   | EXEC                                                 |
| <b>使用情况信息</b> | 无                                                    |
| <b>示例</b>     |                                                      |

```
OS10# show ip igmp snooping mrouter
Interface Router Ports
vlan3031 port-channel31
vlan3032 port-channel31
vlan3033 port-channel31
vlan3034 port-channel31
vlan3035 port-channel31
vlan3036 port-channel31
vlan3037 port-channel31
vlan3038 port-channel31
vlan3039 port-channel31
vlan3040 port-channel31
vlan3041 port-channel31
vlan3042 port-channel31
vlan3043 port-channel31
vlan3044 port-channel31
vlan3045 port-channel31
vlan3046 port-channel31
vlan3047 port-channel31
vlan3048 port-channel31
vlan3049 port-channel31
vlan3050 port-channel31
vlan3051 port-channel31
vlan3052 port-channel31
--more--
```

<<Output Truncated>>

### 示例 (使用 VLAN)

```
OS10# show ip igmp snooping mrouter vlan 3031
Interface Router Ports
vlan3031 port-channel31
```

**支持的版本** 10.4.0E(R1) or later

## 多播侦听器发现协议

IPv6 网络使用多播侦听器查找 (MLD) 协议来管理多播组。

OS10 支持 MLDv1 和 MLDv2 以管理 IPv6 网络上的多播组成员身份。

## MLD 侦听

MLD 侦听使用 IGMP 数据包中的信息并生成将端口与多播组关联的转发表。当交换机收到多播帧时，它们会将其转发给其预期的接收器。

OS10 支持对 VLAN 接口进行 MLD 侦听。默认情况下，MLD 侦听已启用，从 OS10 版本 10.4.3.0 生效。

### 配置 MLD 侦听

- 在 CONFIGURATION 模式下, 使用 `ipv6 mld snooping enable` 命令可在全局范围内启用 MLD 侦听。此命令在所有 VLAN 接口上启用 MLDv2 和 MLDv1 侦听。
- (可选) 您可以在 VLAN INTERFACE 模式下使用 `no ipv6 mld snooping` 命令在特定 VLAN 接口上禁用 MLD 侦听。
- (可选) 默认情况下, 多播淹没控制已启用。要禁用多播泛洪限制功能, 请在 CONFIGURATION 模式下使用 `no multicast snooping flood-restrict` 命令。要全局重新启用该功能, 请在 CONFIGURATION 模式下使用 `ip igmp snooping enable` 命令。
- 在网络中, 侦听交换机连接到发送 MLD 查询的多播路由器。在没有多播路由器的第 2 层网络上, 您可以将侦听交换机配置为充当查询器。在 VLAN CONFIGURATION 模式下使用 `ipv6 mld snooping querier` 命令发送查询。
- OS10 将根据接收的 MLD 成员查询的接口动态学习多播路由器接口。要静态分配多播路由器接口, 请在 VLAN INTERFACE 模式下使用 `ipv6 mld snooping mrouter interface interface-type` 命令。
- (可选) 在 VLAN INTERFACE 模式下, 使用 `ipv6 mld version version-number` 命令配置 MLD 版本。
- (可选) 快速离开选项允许 MLD 侦听交换机在接收离开消息时立即从多播组中删除接口。在 VLAN INTERFACE 模式下, 使用 `ipv6 mld snooping fast-leave` 命令启用快速离开。
- (可选) 在 VLAN INTERFACE 模式下, 使用 `ipv6 mld snooping query-interval query-interval-time` 命令为发送 MLD 常规查询配置时间间隔。
- (可选) 在 VLAN 接口模式下, 使用 `ipv6 mld snooping query-max-resp-time query-response-time` 命令, 配置响应 MLD 查询中通告的查询的最长时间。
- (可选) 在 VLAN INTERFACE 模式下, 使用 `ipv6 mld snooping last-member-query-interval query-interval-time` 命令, 配置在组特定 MLD 查询消息之间的时间间隔。

## MLD 侦听配置

```
OS10(config)# ipv6 mld snooping enable
OS10(config)# interface vlan 11
OS10(conf-if-vl-11)# ipv6 mld snooping mrouter interface ethernet 1/1/32
OS10(conf-if-vl-11)# ipv6 mld snooping querier
OS10(conf-if-vl-11)# ipv6 mld version 1
OS10(conf-if-vl-11)# ipv6 mld snooping fast-leave
OS10(conf-if-vl-11)# ipv6 mld snooping query-interval 60
OS10(conf-if-vl-11)# ipv6 mld snooping query-max-resp-time 10
OS10(conf-if-vl-11)# ipv6 mld snooping last-member-query-interval 1000
```

## 查看 MLD 侦听信息

```
OS10# show ipv6 mld snooping groups
Total Number of Groups: 280
MLD Connected Group Membership
Group Address Interface
Mode Expires
ff02::2 vlan3531
Exclude 00:01:38
ff0e:225:1:: vlan3531 MLDv1-
Compat 00:01:52
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::1 vlan3531 MLDv1-
Compat 00:01:52
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::2 vlan3531 MLDv1-
Compat 00:01:52
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::3 vlan3531 MLDv1-
Compat 00:01:52
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::4 vlan3531 MLDv1-
Compat 00:01:52
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::5 vlan3531 MLDv1-
Compat 00:01:52
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff02::2 vlan3532
Exclude 00:01:47
ff0e:225:2:: vlan3532 MLDv1-
Compat 00:01:56
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:2::1 vlan3532 MLDv1-
Compat 00:01:56
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:2::2 vlan3532 MLDv1-
Compat 00:01:56
```

```
Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
--more--
<<Output Truncated>>
```

```
OS10# show ipv6 mld snooping interface vlan 3031
Vlan3031 is up, line protocol is up
MLD version is 2
MLD snooping is enabled on interface
MLD snooping query interval is 60 seconds
MLD snooping querier timeout is 130 seconds
MLD snooping last member query response interval is 1000 ms
MLD snooping max response time is 10 seconds
MLD snooping fast-leave is disabled on this interface
MLD snooping querier is disabled on this interface
```

```
OS10# show ipv6 mld snooping interface vlan 2
Vlan2 is up, line protocol is up
MLD version is 2
MLD snooping is enabled on interface
MLD snooping query interval is 60 seconds
MLD snooping querier timeout is 130 seconds
MLD snooping last member query response interval is 1000 ms
MLD snooping max response time is 10 seconds
MLD snooping fast-leave is disabled on this interface
MLD snooping querier is disabled on this interface
Multicast flood-restrict is enabled on this interface
```

```
OS10# show ipv6 mld snooping mrouter vlan 11
Interface Router Ports
Vlan 11 ethernet 1/1/32
```

## MLD 侦听命令

### ipv6 mld snooping

在指定的 VLAN 接口上启用 MLD 侦听。

**语法**                    ipv6 mld snooping

**参数**                    无

**默认**                    已启用

**命令模式**                VLAN INTERFACE

**使用情况信息**           当您全局启用 MLD 侦听时，配置将应用于所有 VLAN 的接口。您可以禁用对指定 VLAN 接口的 MLD 侦听。此命令的 no 版本将禁用指定的 VLAN 接口上的 MLD 侦听。

**示例**

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# no ipv6 mld snooping
```

**支持的版本**            10.4.1.0 or later

### ipv6 mld snooping enable

启用全局 MLD 侦听。

**语法**                    ipv6 mld snooping enable

**参数**                    无

**默认**                    已启用

**命令模式**                CONFIGURATION

|               |                                                   |
|---------------|---------------------------------------------------|
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本将禁用 MLD 侦听。                |
| <b>示例</b>     | <pre>OS10(config)# ipv6 mld snooping enable</pre> |
| <b>支持的版本</b>  | 10.4.1.0 or later                                 |

## ipv6 mld snooping fast-leave

为指定 VLAN 启用快速离开 MLD 侦听。

|               |                                                                                                |
|---------------|------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ipv6 mld snooping fast-leave</code>                                                      |
| <b>参数</b>     | 无                                                                                              |
| <b>默认</b>     | 已禁用                                                                                            |
| <b>命令模式</b>   | VLAN INTERFACE                                                                                 |
| <b>使用情况信息</b> | 快速离开选项允许 MLD 侦听交换机在接收到 <code>leave</code> 消息时立即从多播组中删除接口。此命令的 <code>no</code> 版本将禁用快速离开功能。     |
| <b>示例</b>     | <pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# ipv6 mld snooping fast-leave</pre> |
| <b>支持的版本</b>  | 10.4.1.0 or later                                                                              |

## ipv6 mld snooping last-member-query-interval

配置特定于组的 MLD 查询消息之间的时间间隔。

|               |                                                                                                                     |
|---------------|---------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ipv6 mld snooping last-member-query-interval <i>query-interval-time</i></code>                                |
| <b>参数</b>     | <i>query-interval-time</i> — 以毫秒为单位输入查询时间间隔，范围为 100 至 65535。                                                        |
| <b>默认</b>     | 1000 毫秒                                                                                                             |
| <b>命令模式</b>   | VLAN INTERFACE                                                                                                      |
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本将最后成员查询间隔时间重置为默认值。                                                                           |
| <b>示例</b>     | <pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# ipv6 mld snooping last-member-query-interval 2500</pre> |
| <b>支持的版本</b>  | 10.4.1.0 or later                                                                                                   |

## ipv6 mld snooping mrouter

将指定的 VLAN 成员端口配置为多播路由器接口。

|               |                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ipv6 mld snooping mrouter interface <i>interface-type</i></code>                                               |
| <b>参数</b>     | <i>interface-type</i> — 输入接口类型的详细信息。该接口应当是 VLAN 的成员。                                                                 |
| <b>默认</b>     | 未配置                                                                                                                  |
| <b>命令模式</b>   | VLAN INTERFACE                                                                                                       |
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本将从 VLAN 成员端口移除多播路由器配置。                                                                        |
| <b>示例</b>     | <pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# ipv6 mld snooping mrouter interface ethernet 1/1/1</pre> |
| <b>支持的版本</b>  | 10.4.1.0 or later                                                                                                    |

## ipv6 mld snooping querier

在指定的 VLAN 接口上启用 MLD 查询器。

|        |                                               |
|--------|-----------------------------------------------|
| 语法     | <code>ipv6 mld snooping querier</code>        |
| 参数     | 无                                             |
| 默认     | 未配置                                           |
| 命令模式   | VLAN INTERFACE                                |
| 使用情况信息 | 此命令的 <code>no</code> 版本会在 VLAN 接口上禁用 MLD 查询器。 |
| 示例     |                                               |

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ipv6 mld snooping querier
```

支持的版本 10.4.1.0 or later

## ipv6 mld snooping query-interval

配置发送 MLD 常规查询的时间间隔。

|        |                                                                          |
|--------|--------------------------------------------------------------------------|
| 语法     | <code>ipv6 mld snooping query-interval <i>query-interval-time</i></code> |
| 参数     | <i>query-interval-time</i> — 输入间隔时间（以秒为单位），范围从 2 到 18000。                |
| 默认     | 60 秒                                                                     |
| 命令模式   | VLAN INTERFACE                                                           |
| 使用情况信息 | 此命令的 <code>no</code> 版本将查询间隔重置为默认值。                                      |
| 示例     |                                                                          |

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ipv6 mld snooping query-interval 120
```

支持的版本 10.4.1.0 or later

## ipv6 mld query-max-resp-time

配置响应 MLD 查询中通告的查询的最长时间。

|        |                                                                               |
|--------|-------------------------------------------------------------------------------|
| 语法     | <code>ipv6 mld snooping query-max-resp-time <i>query-response-time</i></code> |
| 参数     | <i>query-response-time</i> — 以秒为单位输入查询响应时间，从 1 到 25。                          |
| 默认     | 10 秒                                                                          |
| 命令模式   | VLAN INTERFACE                                                                |
| 使用情况信息 | 此命令的 <code>no</code> 版本将查询响应时间重置为默认值。                                         |
| 示例     |                                                                               |

```
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ipv6 mld snooping query-max-resp-time 15
```

支持的版本 10.4.1.0 or later

## ipv6 mld version

配置 MLD 版本。

|    |                                                     |
|----|-----------------------------------------------------|
| 语法 | <code>ipv6 mld version <i>version-number</i></code> |
| 参数 | <i>version-number</i> — 将版本号输入为 1 或 2。              |

|        |                                                                                      |
|--------|--------------------------------------------------------------------------------------|
| 默认     | 2                                                                                    |
| 命令模式   | VLAN INTERFACE                                                                       |
| 使用情况信息 | 此命令的 no 版本将版本号重置为默认值。                                                                |
| 示例     | <pre>OS10(config)# interface vlan 100 OS10(conf-if-vl-100)# ipv6 mld version 1</pre> |
| 支持的版本  | 10.4.1.0 or later                                                                    |

## show ipv6 mld snooping groups

显示 MLD 侦听组成员身份详细信息。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show ipv6 mld snooping groups [vlan vlan-id] [ipv6-address]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"><li>vlan-id— (可选) 输入 VLAN ID, 从 1 到 4093。</li><li>ipv6-address— (可选) 输入多播组的 IPv6 地址。</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 示例     | <pre>OS10# show ipv6 mld snooping groups Total Number of Groups: 280 MLD Connected Group Membership Group Address      Interface Mode               Expires ff02::2           vlan3531 Exclude           00:01:38 ff0e:225:1::      vlan3531      MLDv1- Compat 00:01:52 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52 ff0e:225:1::1     vlan3531      MLDv1- Compat 00:01:52 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52 ff0e:225:1::2     vlan3531      MLDv1- Compat 00:01:52 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52 ff0e:225:1::3     vlan3531      MLDv1- Compat 00:01:52 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52 ff0e:225:1::4     vlan3531      MLDv1- Compat 00:01:52 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52 ff0e:225:1::5     vlan3531      MLDv1- Compat 00:01:52 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52 ff02::2           vlan3532 Exclude           00:01:47 ff0e:225:2::      vlan3532      MLDv1- Compat 00:01:56 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52 ff0e:225:2::1     vlan3532      MLDv1- Compat 00:01:56 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52 ff0e:225:2::2     vlan3532      MLDv1- Compat 00:01:56 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52 --more--</pre> |

|              |                                                                                                                                                                       |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 (使用 VLAN) | <pre>OS10# show ipv6 mld snooping groups vlan 3531 Total Number of Groups: 7 MLD Connected Group Membership Group Address      Interface      Mode      Expires</pre> |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
ff02::2 vlan3531 Exclude 00:02:08
ff0e:225:1:: vlan3531 MLDv1-Compat 00:02:12
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::1 vlan3531 MLDv1-Compat 00:02:12
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::2 vlan3531 MLDv1-Compat 00:02:12
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::3 vlan3531 MLDv1-Compat 00:02:12
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::4 vlan3531 MLDv1-Compat 00:02:12
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
ff0e:225:1::5 vlan3531 MLDv1-Compat 00:02:12
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
```

示例（使用 VLAN 和多播 IP 地址）

```
OS10# show ipv6 mld snooping groups vlan 3531 ff0e:225:1::
MLD Connected Group Membership
Group Address Interface Mode Expires
ff0e:225:1:: vlan3531 MLDv1-Compat 00:01:30
 Member-ports :port-channel41,ethernet1/1/51,ethernet1/1/52
```

支持的版本 10.4.0E(R1) or later

show ipv6 mld snooping groups detail

显示 MLD 源信息以及详细的成员端口信息。

语法

show ipv6 mld snooping groups [vlan *vlan-id*] [group *ipv6-address*] detail

参数

- vlan-id*—（可选）输入 VLAN ID，从 1 到 4093。
- ipv6-address*—（可选）输入多播组的 IPv6 地址。

默认

未配置

命令模式

EXEC

使用情况信息

无

示例

```
OS10# show ipv6 mld snooping groups detail
Interface vlan3041
Group ff02::2
Source List
--
 Member Port Mode Uptime Expires
 port-channel31 Exclude 2d:11:57:08 00:01:44

Interface vlan3041
Group ff3e:232:b::
Source List
2001:101:29::1b
 Member Port Mode Uptime Expires
 port-channel31 Include 2d:11:50:17 00:01:42
 ethernet1/1/51:1 Include 2d:11:50:36 00:01:38
 ethernet1/1/52:1 Include 2d:11:50:36 00:01:25

Interface vlan3041
Group ff3e:232:b::1
Source List
2001:101:29::1b
 Member Port Mode Uptime Expires
 port-channel31 Include 2d:11:50:17 00:01:29
 ethernet1/1/51:1 Include 2d:11:50:36 00:01:25
 ethernet1/1/52:1 Include 2d:11:50:36 00:01:38
--more--
```

示例（使用 VLAN）

```
OS10# show ipv6 mld snooping groups vlan 3041 detail
Interface vlan3041
```

```

Group ff02::2
Source List
--
 Member Port Mode Uptime Expires
 port-channel31 Exclude 2d:11:57:08 00:01:44

Interface vlan3041
Group ff3e:232:b::
Source List
 2001:101:29::1b
 Member Port Mode Uptime Expires
 port-channel31 Include 2d:11:50:17 00:01:42
 ethernet1/1/51:1 Include 2d:11:50:36 00:01:38
 ethernet1/1/52:1 Include 2d:11:50:36 00:01:25

Interface vlan3041
Group ff3e:232:b::1
Source List
 2001:101:29::1b
 Member Port Mode Uptime Expires
 port-channel31 Include 2d:11:50:17 00:01:29
 ethernet1/1/51:1 Include 2d:11:50:36 00:01:25
 ethernet1/1/52:1 Include 2d:11:50:36 00:01:38
--more--

```

### 示例（使用 VLAN 和多播 IP 地址）

```

OS10# show ipv6 mld snooping groups vlan 3041 ff3e:232:b:: detail
Interface vlan3041
Group ff3e:232:b::
Source List
 2001:101:29::1b
 Member Port Mode Uptime Expires
 port-channel31 Include 2d:11:50:53 00:02:01
 ethernet1/1/51:1 Include 2d:11:51:11 00:02:01
 ethernet1/1/52:1 Include 2d:11:51:12 00:01:52

```

**支持的版本** 10.4.1.0 or later

## show ipv6 mld snooping interface

显示 MLD 侦听接口的详细信息。

**语法** show ipv6 mld snooping interface [vlan *vlan-id*]

**参数** *vlan-id*—（可选）输入 VLAN ID，从 1 到 4093。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** S4248FB-ON 和 S4248FBL-ON 设备上的多播泛洪控制功能不可。

### 示例

```

OS10# show ipv6 mld snooping interface vlan 3031
Vlan3031 is up, line protocol is up
MLD version is 2
MLD snooping is enabled on interface
MLD snooping query interval is 60 seconds
MLD snooping querier timeout is 130 seconds
MLD snooping last member query response interval is 1000 ms
MLD snooping max response time is 10 seconds
MLD snooping fast-leave is disabled on this interface
MLD snooping querier is disabled on this interface

```

```

OS10# show ipv6 mld snooping interface vlan 2
Vlan2 is up, line protocol is up
MLD version is 2
MLD snooping is enabled on interface
MLD snooping query interval is 60 seconds

```



```

MLD snooping querier timeout is 130 seconds
MLD snooping last member query response interval is 1000 ms
MLD snooping max response time is 10 seconds
MLD snooping fast-leave is disabled on this interface
MLD snooping querier is disabled on this interface
Multicast flood-restrict is enabled on this interface

```

**支持的版本** 10.4.1.0 or later

## show ipv6 mld snooping mrouter

显示多播路由器端口的详细信息。

**语法** show ipv6 mld snooping mrouter [vlan *vlan-id*]  
**参数** *vlan-id*— (可选) 输入 VLAN ID, 从 1 到 4093。  
**默认** 未配置  
**命令模式** EXEC  
**使用情况信息** 无  
**示例**

```

OS10# show ipv6 mld snooping mrouter vlan 11
Interface Router Ports
Vlan 11 ethernet 1/1/32

```

**支持的版本** 10.4.1.0 or later

## 协议独立多播

协议独立多播 (PIM) 是一组可提供一对多和多对多的信息传输的多播路由协议。PIM 使用其他路由协议的路由信息, 并且不依赖于任何特定的单播路由协议。PIM 使用网络中部署的任何单播路由协议。OS10 支持以下 PIM 模式:

- PIM 稀疏模式 (PIM-SM)
- PIM 源特定多播 (PIM-SSM)

## PIM 术语

表. 43: PIM 术语

| 术语            | 定义                                                   |
|---------------|------------------------------------------------------|
| 集合点 (RP)      | RP 是共享树使用的单个根节点, 称为集合点。                              |
| (*, G)        | (*, G) 是指组的 PIM 表中的条目。                               |
| (S, G)        | (S, G)是指在 PIM 表中的一个条目, 用于 RP 树 (RPT) 上的源和组。          |
| (S, G, RPT)   | (S, G, RPT) 是指 RP 树中的一个条目。                           |
| 第一跳路由器 (FHR)  | FHR 是直接连接到多播源的路由器。                                   |
| 最后一跳路由器 (LHR) | LHR 是多播路径中的最后一个路由器, 并直接连接到多播接收器。                     |
| 中间路由器         | PIM 路由器不是 FHR、RP 或 LHR。                              |
| 共享树 (RPT)     | RPT 是单向多播树, 其根节点为 RP。                                |
| 最短路径树 (SPT)   | SPT 的根节点是多播源。多播流量路由到最短路径上的接收器。此设置可减少 RP 上的网络延迟和流量拥塞。 |

表. 43: PIM 术语 (续)

| 术语           | 定义                        |
|--------------|---------------------------|
| 传出接口 (OIF)   | OIF 是向接收器发送多播数据包的接口。      |
| 传入接口 (IIF)   | IIF 是用于接收源或 RP 的多播数据包的接口。 |
| 反向路径转发 (RPF) | RPF 是路由器用来访问 RP 或多播源的路径。  |

## 标准合规性

OS10 符合以下标准：

- RFC 4601 for PIM-SM
- RFC 3569 for PIM-SSM

## PIM-SM

PIM 稀疏模式 (PIM-SM) 是用于具有稀疏分布的接收器的网络的多播路由协议。接收方必须明确发送加入消息以加入特定组或源。PIM 加入和修剪邮件用于加入和离开多播分发树。

PIM-SM 使用共享树，并且根节点为集合点 (RP)。所有多播源都使用 RP 将流量路由到接收方。最后一跳路由器 (LHR) 向 RP 发送 (\*, G) 加入消息。连接到第一跳路由器的指定路由器 (FHR) 将来自 PIM 控制消息中的多播源的多播数据封装，并通过单播方式将其发送到 RP 作为 PIM 注册消息。RP 发送一个 (S, G) 加入与源的连接。当 RP 收到来自源的本机数据流量时，它会向 FHR 发送一条注册停止消息。

OS10 支持对多播组的 RP 地址进行静态和动态配置。

要使 PIM-SM 状态保持活动状态，所有 PIM 的邻居都会发送定期问候邮件。

您必须在每个参与接口上启用 PIM-SM。确保在系统上启用多播路由。要执行此操作，请在 CONFIGURATION 模式下使用 `ip multicast-routing` 命令。

```
OS10# configure terminal
OS10(config)# interface vlan 100
OS10(conf-if-vl-100)# ip pim sparse-mode
```

## PIM-SSM

PIM-SSM 使用基于源的树。针对将数据发送到多播组的数据的每个多播源构建单独的多播分发树。每个多播分发树都在靠近源的位置拥有作为其根节点的路由器。源将数据直接发送到树的根。PIM-SSM 使接收器可以指定要从中接收数据的源及其要加入的多播组。接收器使用源和组地址对 (S, G) 来标识多播数据流，而不是单独的组地址 (\*, G)。

- i

注：
- PIM SSM 要求接收器支持 IGMP 版本 3。
  - 默认 PIM-SSM 范围为 232.0.0.0/8。始终支持默认范围，并且范围绝不会小于默认值。
  - 如果 PIM-SSM 组范围与候选 RP 通告的多播组范围重叠，则路由器会从 BSR 中选择所学习的 RP 并创建 (\*, G) 条目，而不是 (S, G) 条目。

## PIM-SSM 的优势

PIM-SSM 的优势包括：

- PIM-SSM 将多播流量从单个源转发到子网。其他版本的 PIM 需要接收器订阅组。接收器只接收来自它所感兴趣的源的流量，但从发送至该组的所有源接收流量。PIM-SSM 要求接收方指定它们感兴趣的源，以避免接收不必要的流量。
- 与 PIM-SM 相比，PIM-SSM 效率更高，因为它会立即创建到源的最短路径树 (SPT)，而不是使用共享树。PIM-SM 要求将共享树根置于 RP，因为 IGMPv2 接收器不会在其成员身份报告中表达源信息。多播流量通过 RP 从源传递给接收器，直至最后一跳路由器 (LHR) 获知源地址，此时它将切换到 SPT。

PIM-SSM 使用 IGMPv3。由于接收方订阅源和组，因此 RP 和共享树是不必要的；仅使用 SPT。在 OS10 系统上，可以将 PIM-SM 与 IGMPv3 配合使用，以实现相同的结果，但 PIM-SSM 能够免去不必要的协议开销。

## 配置 PIM-SSM

要为 PIM SSM 配置组范围，请执行以下操作：

**注：**为 SSM 保留 IP 范围 232.0.0.0/8。您不必明确配置此范围。

1. 创建 ACL 规则以指定应使用 SSM 的地址范围。

```
OS10# configure terminal
OS10(config)# ip access-list ssm-1
OS10(config-ipv4-acl)# permit ip any 236.0.0.0/8
OS10(config-ipv4-acl)# exit
```

2. 使用 `ip pim ssm-range` 命令启用 PIM SSM 的地址范围。

```
OS10(config)# ip pim ssm-range ssm-1
```

您可以使用 `show ip pim ssm-range` 命令查看 PIM SSM 配置中添加的组。

```
OS10# show ip pim ssm-range
Group Address / MaskLen
236.0.0.0 / 8
```

## 为 S、G 条目配置到期计时器

您可以在全局范围内配置到期条目的到期计时器。默认情况下，S、G 条目将在 210 秒内过期。

要配置 S、G 到期计时器，请执行以下操作：

```
OS10# configure terminal
OS10(config)# ip pim sparse-mode sg-expiry-timer 500
```

## Configure static rendezvous point

集合点 (RP) 是路由器上的一个接口，可充当特定于组的树的根节点；每个组必须具有 RP。您必须在网络中的所有节点上配置 RP。

要配置静态 RP：

```
OS10# configure terminal
OS10(config)# ip pim rp-address 171.1.1.1 group-address 225.1.1.3/32
```

## 覆盖自举路由器更新

自举路由器 (BSR) 是 PIM 域中的路由器，可帮助自动发现多播网络中给定多播组的集合点 (RP)。PIM 路由器使用 BSR 以获取 RP IP 地址。您还可以静态配置 RP 的 IP 地址。如果为组配置了静态 RP，要使用静态 RP 配置覆盖 BSR 更新，请使用 `ip pim rp-address` 命令中的 `override` 选项。如果未明确使用 `override` 选项，并且：

- 静态 RP 的前缀长度与 BSR 更新中通告的 RP 相同，BSR RP 优先于静态配置的 RP。
- 如果静态 RP 和 BSR RP 的前缀长度不匹配，OS10 将选择具有最高匹配前缀的路由器作为 RP。

要覆盖 BSR 更新，请执行以下操作：

```
OS10# configure terminal
OS10(config)# ip pim rp-address 20.1.1.1 255.1.2.3/24 override
```

**注:** 如果已启用 `override` 选项, 则在不使用 `override` 选项的情况下配置静态 RP 不会移除覆盖配置。您必须使用 `override` 选项删除静态 RP 配置, 然后再次重新配置静态 RP 配置。

要查看多播组的 RP, 请使用 `show ip pim rp` 命令。

```
OS10# show ip pim rp
Group RP

225.1.1.1 171.1.1.1
225.1.1.2 171.1.1.1
225.1.1.3 171.1.1.1
225.1.1.4 171.1.1.1
225.1.1.5 171.1.1.1
225.1.1.6 171.1.1.1
```

要查看多播组范围的 RP, 请使用 `show ip pim rp mapping` 命令。

```
OS10# show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 230.1.1.1/32
RP:14.1.1.1, v2
 Info source: 42.1.1.1, via bootstrap, priority 255
 expires: 00:01:53

Group(s): 231.1.1.1/32
RP: 9.1.1.1, v2
 Info source: 42.1.1.1, via bootstrap, priority 254
 expires: 00:01:54
```

## 使用 BSR 机制配置动态 RP

您可以将域中的 PIM 路由器子集配置为候选 BSR (C-BSR)。BSR 将交换引导数据库消息 (BSM) 以选举 BSR。BSR 会将其状态通知给所有路由器。

域中的每个 PIM 路由器都必须将特定多播组地址映射到同一 RP。对于 BSR, 组到 RP 的映射是动态的。您可以将域中的一个路由器子集配置为 C-RP。每个 PIM 路由器将从 BSR 消息学习的组到 RP 映射列表中选择一个多播组的 RP。

RP 选举过程如下:

1. C-BSR 将公告 BSM 中整个域的候选。每个 BSM 都包含 BSR 优先级。优先级最高的 C-BSR 变为 BSR。
2. 每个 C-RP 将定期 BSR 通告单播至 BSR。每条消息都包含 RP 优先级值和路由器为 C-RP 的多播组范围。
3. BSR 决定了最高效稳定的组到 RP 映射, 称为 RP-set 构造。
4. BSR 会将组到 RP 映射集发送到所有多播路由器。要从一组 RP 中选择 RP, 多播路由器将使用 RFC 4601 中指定的算法。
5. BSR 将组范围到 RP 映射发送到域中的所有路由器。

## 配置说明

- PIM 路由器对于每个 VRF 实例仅支持一个候选 BSR。
- PIM 路由器对于每个 VRF 实例仅支持一个候选 RP。
- 您可以为第 3 层 (L3) VLAN、环回、物理或端口通道接口配置 PIM BSR 候选项和 RP 候选项。系统从此接口派生 IP 地址以确定 BSR 或 RP 地址。
- VXLAN 桥接口上不支持 PIM BSR 和 RP 候选配置。
- **配置候选 BSR 之前:**
  - 全局启用多播路由, 并在路由器之间建立 PIM 邻居关系。确保已填充单播路由表。
  - 在候选 BSR 接口上配置 IP 地址。
- **配置候选 RP 之前:**
  - 全局启用多播路由, 并在路由器之间建立 PIM 邻居关系。确保已填充单播路由表。
  - 确保候选 RP 可以访问您网络中的所有节点。
  - (可选) 配置 ACL, 源为 `any` 和目标为有效的多播组地址。如果未配置 ACL, 则路由器将自己通告为整个多播范围的 RP (224.0.0.0/4)。

**注:**

- 当您不具有任何规则的 ACL 关联到 RP 候选项时, 根据配置顺序, 系统的行为会有所不同:

- 如果您在不先创建任何规则的情况下创建 ACL，然后将其与 RP 候选项关联，则路由器将拒绝所有多播组。
- 如果将 ACL 关联到尚未在系统中创建的 RP 候选项，然后配置不带任何规则的 ACL，则路由器会将自己通告为整个多播范围的 RP (224.0.0.0/4)。
- 请勿在用于 deny RP 候选项的 ACL 中使用规则，因为它没有任何意义。

要使用 BSR 机制配置动态 RP，请执行以下操作：

### 1. 使用 ip pim bsr-candidate 命令配置候选 BSR。

```
OS10# configure terminal
OS10(config)# interface ethernet 1/1/9
OS10(config-if-eth1/1/9)# ip address 10.1.1.8/24
OS10(config-if-eth1/1/9)# no shutdown
OS10(config-if-eth1/1/9)# exit
OS10(config)# ip pim bsr-candidate ethernet 1/1/9 hash-mask-len 31 priority 255
```

要查看 PIM 候选项并选择 BSR：

```
OS10# show ip pim bsr-router

This system is the Bootstrap Router (v2)
BSR address: 10.1.1.8
BSR Priority: 255, Hash mask length: 31
Next bootstrap message in 00:00:57
This system is a candidate BSR
Candidate BSR address: 11.1.1.8, priority: 255, hash mask length: 31
```

### 2. (可选) 配置 BSR 计时器。

```
OS10(config)# ip pim bsr-candidate-timers ethernet 1/1/9 advt-interval 40
```

要查看 BSR 计时器值，请执行以下操作：

```
OS10# show ip pim bsr-router

This system is the Bootstrap Router (v2)
BSR address: 10.1.1.8
BSR Priority: 255, Hash mask length: 31
Next bootstrap message in 00:00:39
This system is a candidate BSR
Candidate BSR address: 11.1.1.8, priority: 255, hash mask length: 31
```

### 3. 配置候选 RP。

```
OS10# configure terminal
OS10(config)# interface loopback 10
OS10(config-if-lo-10)# ip address 10.1.2.8/24
OS10(config-if-lo-10)# no shutdown
OS10(config-if-lo-10)# exit

OS10(config)# ip access-list acl-rp
OS10(config-ipv4-acl)# permit ip any 225.1.1.0/24

OS10(config)# ip pim rp-candidate loopback 10 priority 23 acl acl-rp
```

**注：**系统不会覆盖候选 RP 配置。您必须删除该条目并进行重新配置。例如，在使用优先级配置候选 RP 并将 ACL 与其关联后，要重置优先级并将 ACL 与候选 RP 取消关联，或将候选 RP 重置为默认值，则必须使用 `no ip pim rp-candidate` 命令并重新配置候选 RP。

要查看候选 RP、候选 BSR 和选举的 BSR，请执行以下操作：

```
OS10# show ip pim bsr-router

This system is the Bootstrap Router (v2)
BSR address: 10.1.1.8
BSR Priority: 255, Hash mask length: 31
Next bootstrap message in 00:00:20
This system is a candidate BSR
```

```
Candidate BSR address: 10.1.1.8, priority: 255, hash mask length: 31
Next Cand_RP_advertisement in 00:00:50
RP: 10.1.2.8(loopback10)
```

要查看 RP 映射详细信息，请执行以下操作：

```
OS10# show ip pim rp mapping
Group(s) : 225.1.1.0/24
RP : 10.1.2.8, v2
Info source: 10.1.1.8, via bootstrap, priority 0
expires: 00:00:00
```

#### 4. (可选) 配置 RP 计时器。

```
OS10(config)# ip pim rp-candidate-timers loopback 10 advt-interval 10 hold-time 25
```

要查看候选 RP 详细信息：

```
OS10# show ip pim bsr-router

This system is the Bootstrap Router (v2)
BSR address: 10.1.1.8
BSR Priority: 255, Hash mask length: 31
Next bootstrap message in 00:00:00
This system is a candidate BSR
Candidate BSR address: 10.1.1.8, priority: 255, hash mask length: 31
Next Cand_RP_advertisement in 00:00:09
RP: 10.1.2.8(loopback10)
```

要查看 RP 映射详细信息，请执行以下操作：

```
OS10# show ip pim rp mapping
Group(s) : 225.1.1.0/24
RP : 10.1.2.8, v2
Info source: 10.1.1.8, via bootstrap, priority 23
expires: 00:01:04
```

## 配置指定的路由器优先级

多个 PIM SM 路由器可以连接到单个局域网 (LAN) 段。其中一个路由器选择作为指定的路由器 (DR)。

DR 将使用问候消息进行选择。每个 PIM 路由器通过定期从每个启用 PIM 的接口发送问候邮件来了解其邻居。问候邮件包含其发送的接口 IP 地址和 DR 优先级值。具有最高优先级值的路由器将成为灾难恢复。如果两个路由器的优先级值相同，则具有最高 IP 地址的路由器将为灾难恢复。默认情况下，DR 优先级值为 1，因此 IP 地址可确定灾难恢复。

要配置 DR 优先级，请使用以下命令：

```
OS10# configure terminal
OS10(config)# interface vlan 100
OS10(config-if-vl-100)# ip pim dr-priority 200
```

## PIM 命令

### clear ip pim tib

从 PIM 数据库中清除 PIM 树信息。

|      |                                       |
|------|---------------------------------------|
| 语法   | clear ip pim [vrf vrf-name] tib       |
| 参数   | vrf vrf-name— 输入关键字 vrf，然后输入 VRF 的名称。 |
| 默认   | 无                                     |
| 命令模式 | EXEC PRIVILEGE                        |

#### 使用情况信息

在节点上运行此命令时，会删除：

- 来自 PIM 树信息库 (TIB) 的所有多播路由
- 整个多播路由表和数据平面中的所有条目

使用 VLT 多播路由的情况下，在本地 VLT 节点上运行此命令时，将会删除：

- 来自本地 PIM 的所有多播路由 TIB
- 数据平面中的所有本地 mroute 条目
- 从 VLT 对等节点中同步的 mroute 条目

#### 示例

```
OS10# clear ip pim vrf vrf1 tib
```

#### 支持的版本

10.4.3.0 or later

## ip multicast-routing

启用 IP 多播转发。

#### 语法

```
ip multicast-routing [vrf vrf-name]
```

#### 参数

*vrf vrf-name*— 输入关键字 *vrf*，然后输入 VRF 的名称。

#### 默认

无

#### 命令模式

CONFIGURATION

#### 使用情况信息

启用 IP 多播后，启用接口上的 IGMP 和 PIM。要执行此操作，请在 INTERFACE 模式下使用 `ip pim sparse-mode` 命令。命令的 `no` 形式将禁用 IP 多播转发。

#### 示例

```
OS10# configure terminal
OS10(config)# ip multicast-routing
```

#### 支持的版本

10.4.3.0 or later

## ip pim bsr-candidate

将路由器配置为 IPv4 PIM BSR 候选对象。

#### 语法

```
ip pim [vrf vrf-name] bsr-candidate {ethernet node/slot/port[:subport] |
loopback loopback-interface-number | vlan vlan-number | port-channel port-
channel-number} [hash-mask-len length] [priority priority-value]

no ip pim [vrf vrf-name] bsr-candidate
```

#### 参数

- *vrf vrf-name*— 输入关键字 *vrf*，然后输入 VRF 的名称。
- *loopback-interface-number*— 输入 0 至 16383 之间的值。
- *vlan-number*— 输入 1 至 4093 之间的值。
- *port-channel-number*— 输入 1 至 128 之间的值。
- *length*— 输入 0 至 32 之间的值。
- *priority-value*— 输入 0 至 255 之间的值。

#### 默认

- 哈希掩码长度为 30。
- 优先级为 64。

#### 命令模式

CONFIGURATION

#### 使用情况信息

系统会将指定接口的 IP 地址通告为 BSR 消息中的 BSR IP 地址。命令的 `no` 形式会从候选 BSR 中移除路由器。请勿以命令的 `no` 形式指定参数。

|       |                                                                                                                         |
|-------|-------------------------------------------------------------------------------------------------------------------------|
| 示例    | <pre>OS10# configure terminal OS10(config)# ip pim vrf red bsr-candidate loopback 10 hash-mask-len 31 priority 11</pre> |
| 支持的版本 | 10.5.0 or later                                                                                                         |

## ip pim bsr-candidate-timers

配置候选 BSR 通告之间的时间间隔。

|        |                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip pim [vrf <i>vrf-name</i>] bsr-candidate-timers {ethernet <i>node/slot/port[:subport]</i>   loopback <i>loopback-interface-number</i>   vlan <i>vlan-number</i>   port-channel <i>port-channel-number</i>} advt-interval <i>interval-value</i></code>                                                                                                            |
| 参数     | <ul style="list-style-type: none"> <li><code>vrf <i>vrf-name</i></code>— 输入关键字 <code>vrf</code>，然后输入 VRF 的名称。</li> <li><code>loopback-interface-number</code>— 输入 0 至 16383 之间的值。</li> <li><code>vlan-number</code>— 输入 1 至 4093 之间的值。</li> <li><code>port-channel-number</code>— 输入 1 至 128 之间的值。</li> <li><code>interval-value</code>— 输入 1 至 2147483 之间的值。</li> </ul> |
| 默认     | <ul style="list-style-type: none"> <li>通告间隔默认值为 60 秒。</li> </ul>                                                                                                                                                                                                                                                                                                         |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                            |
| 使用情况信息 | 使用此命令可调整定期 BSR 通告之间的时间间隔。命令的 <code>no</code> 形式将候选 BSR 通告间隔重置为默认值。请勿以命令的 <code>no</code> 形式指定参数。                                                                                                                                                                                                                                                                         |
| 示例     | <pre>OS10(config)# ip pim vrf red bsr-candidate-timers loopback 10 advt- interval 40</pre>                                                                                                                                                                                                                                                                               |
| 支持的版本  | 10.5.0 or later                                                                                                                                                                                                                                                                                                                                                          |

## ip pim bsr-timeout

配置 BSR 超时值。

|        |                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <pre>ip pim [vrf <i>vrf-name</i>] bsr-timeout <i>value</i> no ip pim [vrf <i>vrf-name</i>] bsr-timeout</pre>                                                               |
| 参数     | <ul style="list-style-type: none"> <li><code>vrf <i>vrf-name</i></code>— 输入关键字 <code>vrf</code>，然后输入 VRF 的名称。</li> <li><code>value</code>— 输入 0 至 2147483 之间的值。</li> </ul> |
| 默认     | 130 s                                                                                                                                                                      |
| 命令模式   | CONFIGURATION                                                                                                                                                              |
| 使用情况信息 | 命令的 <code>no</code> 形式将 BSR 超时重置为其默认值。                                                                                                                                     |
| 示例     | <pre>OS10# configure terminal OS10(config)# ip pim vrf red bsr-timeout 140</pre>                                                                                           |
| 支持的版本  | 10.5.0 or later                                                                                                                                                            |

## ip pim dr-priority

更改接口的指定路由器 (DR) 优先级。

|    |                                                       |
|----|-------------------------------------------------------|
| 语法 | <code>ip pim dr-priority <i>priority-value</i></code> |
| 参数 | <code>priority-value</code> — 输入从 0 到 4294967295 的编号。 |



|        |                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------|
| 默认     | 1                                                                                                                       |
| 命令模式   | INTERFACE CONFIGURATION                                                                                                 |
| 使用情况信息 | <p>分配给接口的最高值的路由器将成为灾难恢复。如果两个接口具有相同的 DR 优先级值，则具有最高 IP 地址的接口将成为灾难恢复。</p> <p>此命令的 <code>no</code> 形式将移除分配给接口的 DR 优先级值。</p> |
| 示例     | <pre>OS10# configure terminal OS10(config)# interface vlan 1 OS10(config-if-vl-1)# ip pim dr-priority 200</pre>         |
| 支持的版本  | 10.4.3.0 or later                                                                                                       |

## ip pim query-interval

更改 PIM 路由器查询消息的频率。

|        |                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip pim query-interval seconds</code>                                                                        |
| 参数     | <code>seconds</code> — 输入在从每个启用 PIM 的接口发送 PIM 问候数据包之前路由器等待的时间量（以秒为单位），从 2 到 18000。                                |
| 默认     | 30 秒                                                                                                              |
| 命令模式   | INTERFACE CONFIGURATION                                                                                           |
| 使用情况信息 | 此命令的 <code>no</code> 形式会将 PIM 路由器查询消息的频率返回为默认值。                                                                   |
| 示例     | <pre>OS10# configure terminal OS10(config)# interface vlan 1 OS10(config-if-vl-1)# ip pim query-interval 20</pre> |
| 支持的版本  | 10.4.3.0 or later                                                                                                 |

## ip pim rp-address

为组配置静态 PIM RP 地址。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip pim [vrf vrf-name] rp-address address {group-address group-address mask} [override]</code>                                                                                                                                                                                                                                                                                                                                        |
| 参数     | <ul style="list-style-type: none"> <li><code>vrf vrf-name</code>— 输入关键字 <code>vrf</code>，然后输入 VRF 的名称。</li> <li><code>rp-address address</code>— 输入关键字 <code>address</code>，以点分隔的十进制格式 (A.B.C.D) 的 RP 地址。</li> <li><code>group-address group-address mask</code>— 输入关键字 <code>group-address</code>，然后是以点分隔的十进制格式 (/xx) 的组地址掩码，用于将组地址分配给 RP。</li> <li><code>[override]</code> — 使用具有相同前缀长度的组的静态 RP 覆盖 BSR 更新。</li> </ul>                    |
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 使用情况信息 | <p>第一跳路由器使用此地址来代表源多播主机发送注册数据包。RP 地址按其输入的顺序存储。RP 将根据组的更长的前缀匹配进行选择。您可以指定将给定节点配置为 RP 的组地址范围。RP 选择不依赖于静态或动态 RP 分配。</p> <p>如果已为组配置了静态 RP，请使用 <code>override</code> 选项将 BSR 更新替换为静态 RP 配置。</p> <p>如果未明确使用 <code>override</code> 选项，并且：</p> <ul style="list-style-type: none"> <li>静态 RP 的前缀长度与 BSR RP 相同，BSR RP 优先于静态配置的 RP。</li> <li>如果静态 RP 和 BSR RP 的前缀长度不匹配，OS10 将选择具有最高匹配前缀的路由器作为 RP。</li> </ul> <p>此命令的 <code>no</code> 形式将移除静态 RP 配置。</p> |

## 示例

```
OS10# configure terminal
OS10(config)# ip pim rp-address 171.1.1.1 group-address 225.1.1.3/32
override
```

## 支持的版本

10.4.3.0 or later

# ip pim rp-candidate

将路由器配置为 IPv4 PIM RP 候选项。

## 语法

```
ip pim [vrf vrf-name] rp-candidate {ethernet node/slot/port[:subport] |
loopback loopback-interface-number | vlan vlan-number | port-channel port-
channel-number} [priority priority-value] [acl acl-name]
```

## 参数

- *vrf vrf-name*— 输入关键字 *vrf*，然后输入 VRF 的名称。
- *loopback-interface-number*— 输入 0 至 16383 之间的值。
- *vlan-number*— 输入 1 至 4093 之间的值。
- *port-channel-number*— 输入 1 至 128 之间的值。
- *priority-value*— 输入 0 至 255 之间的值。
- *acl-name*— 标准 ACL 名称

## 默认

优先级为 192。

## 命令模式

CONFIGURATION

## 使用情况信息

指定接口以获取候选 RP 地址。访问列表 *acl-name* 可添加此候选 RP 可为其提供服务的一系列组地址。

如果您未指定访问列表，则 C-RP 会将自身通告给整个多播范围，224.0.0.0/4。

如果指定访问列表，则 C-RP 仅通告访问列表允许的组范围。

命令的 *no* 形式是从 C-RP 中移除路由器。您必须使用此命令的 *no* 形式指定参数。

## 示例

```
OS10# configure terminal
OS10(config)# ip pim vrf red rp-candidate loopback 10 priority 11 acl rp-
grp
```

## 支持的版本

10.5.0 or later

# ip pim rp-candidate-timers

配置定期的候选 RP 通告之间的时间间隔。

## 语法

```
ip pim [vrf vrf-name] rp-candidate-timers {ethernet node/slot/
port[:subport] | loopback loopback-interface-number | vlan vlan-number |
port-channel port-channel-number} {advt-interval interval-value} [hold-time
hold-time-value]
```

## 参数

- *vrf vrf-name*— 输入关键字 *vrf*，然后输入 VRF 的名称。
- *loopback-interface-number*— 输入 0 至 16383 之间的值。
- *vlan-number*— 输入 1 至 4093 之间的值。
- *port-channel-number*— 输入 1 至 128 之间的值。
- *interval-value*— 输入 1 至 26214 之间的值。
- *hold-time-value*— 输入 1 至 65535 之间的值。

 **注：**保留时间必须大于通告时间间隔。

## 默认

- 通告间隔为 60 秒。
- 暂存时间值为 150 秒。

## 命令模式

CONFIGURATION

|               |                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>使用情况信息</b> | 使用此命令可调整候选 RP 通告之间的时间间隔。在暂存时间值到期之前，通告的 RP 条目会保留在节点中。Dell EMC 建议将暂存时间值配置为通告间隔的 2.5 倍。命令的 <code>no</code> 形式将候选 RP 计时器重置为默认值。     |
| <b>示例</b>     | <pre>OS10# configure terminal OS10(config)# ip pim vrf red rp-candidate-timers loopback 10 advt- interval 30 hold-time 80</pre> |
| <b>支持的版本</b>  | 10.5.0 or later                                                                                                                 |

## ip pim sparse-mode

在接口上启用 PIM 稀疏模式和 IGMP。

|               |                                                                                                                                                                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ip pim sparse-mode</code>                                                                                                                                                                                                                                                                                                           |
| <b>参数</b>     | 无                                                                                                                                                                                                                                                                                                                                         |
| <b>默认</b>     | 已禁用                                                                                                                                                                                                                                                                                                                                       |
| <b>命令模式</b>   | INTERFACE CONFIGURATION                                                                                                                                                                                                                                                                                                                   |
| <b>使用情况信息</b> | <p>在启用 PIM 稀疏模式之前，请确保：</p> <ul style="list-style-type: none"> <li>使用 <code>ip multicast-routing</code> 命令全局启用多播。</li> <li>接口已启用。使用 <code>no shutdown</code> 命令可启用接口。</li> <li>接口在第 3 层模式下。PIM-SM 仅在第 3 层接口上启用。在接口上配置 PIM 之前，请使用 <code>no switchport</code> 命令将接口从第 2 层更改为第 3 层模式。</li> </ul> <p>使用命令的 <code>no</code> 形式可禁用 PIM 稀疏模式。</p> |

|              |                                                                                                                                                         |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>示例</b>    | <pre>OS10# configure terminal OS10(config)# interface vlan 2 OS10(config-if-vl-2)# ip address 1.1.1.2/24 OS10(config-if-vl-2)# ip pim sparse-mode</pre> |
| <b>支持的版本</b> | 10.4.3.0 or later                                                                                                                                       |

## ip pim sparse-mode sg-expiry-timer

为所有源全局启用到期计时器。

|               |                                                                                                                                                                             |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ip pim [vrf vrf-name] sparse-mode sg-expiry-timer seconds</code>                                                                                                      |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>vrf vrf-name</code>— 输入关键字 <code>vrf</code>，然后输入 VRF 的名称。</li> <li><code>seconds</code>— 输入保留的秒数。范围为 211 到 65535 秒。</li> </ul> |
| <b>默认</b>     | 210 秒                                                                                                                                                                       |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                                                               |
| <b>使用情况信息</b> | 此命令将配置所有 S、G 条目的到期计时器。                                                                                                                                                      |

|              |                                                                                          |
|--------------|------------------------------------------------------------------------------------------|
| <b>示例</b>    | <pre>OS10# configure terminal OS10(config)# ip pim sparse-mode sg-expiry-timer 500</pre> |
| <b>支持的版本</b> | 10.4.3.0 or later                                                                        |

## ip pim ssm-range

使用访问列表指定 SSM 组范围。

|        |                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip pim [vrf vrf-name] ssm-range {access-list-name}</code>                                                                                                   |
| 参数     | <ul style="list-style-type: none"><li><code>vrf vrf-name</code>— 输入关键字 <code>vrf</code>，然后输入 VRF 的名称。</li><li><code>access-list-name</code>— 输入访问列表的名称。</li></ul> |
| 默认     | 232.0.0.0/8                                                                                                                                                       |
| 命令模式   | CONFIGURATION                                                                                                                                                     |
| 使用情况信息 | 当 ACL 规则更改时，ACL 和 PIM 模块会自动应用新规则。移除 SSM ACL 时，PIM-SSM 仅支持默认的 SSM 范围。                                                                                              |
| 示例     | <pre>OS10# configure terminal OS10(config)# ip pim ssm-range ssm</pre>                                                                                            |
| 支持的版本  | 10.4.3.0 or later                                                                                                                                                 |

## show ip pim bsr-router

显示有关自举路由器的信息。

|        |                                                                                                                                                                                                                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show ip pim [vrf vrf-name] bsr-router</code>                                                                                                                                                                                                                                                                          |
| 参数     | <code>vrf vrf-name</code> — 输入关键字 <code>vrf</code> ，然后输入 VRF 的名称。                                                                                                                                                                                                                                                           |
| 默认     | 无                                                                                                                                                                                                                                                                                                                           |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                        |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                                           |
| 示例     | <pre>OS10# show ip pim bsr-router  PIMv2 Bootstrap information BSR address: 101.0.0.1 BSR Priority: 199, Hash mask length: 31 Expires: 00:00:24 This system is a candidate BSR Candidate BSR address: 104.0.0.1, priority: 99, hash mask length: 31 Next Cand_RP advertisement in 00:00:15 RP: 104.0.0.1(loopback101)</pre> |
| 支持的版本  | 10.5.0 or later                                                                                                                                                                                                                                                                                                             |

## show ip pim interface

显示有关启用 IP PIM 接口的信息。

|        |                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show ip pim [vrf vrf-name] interface</code>                                                                                                                                                                                                                                                                                                                             |
| 参数     | <code>vrf vrf-name</code> — 输入关键字 <code>vrf</code> ，然后输入 VRF 的名称。                                                                                                                                                                                                                                                                                                             |
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                                             |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | <p><code>show ip pim interface</code> 命令将显示以下内容：</p> <ul style="list-style-type: none"><li><code>Address</code> — 已启用 IP PIM 接口的 IP 地址</li><li><code>Interface</code> — 具有插槽/端口信息或 VLAN/端口通道 ID 的接口类型</li><li><code>Version/Mode</code> — PIM 版本号和模式；对于 PIM 版本 2 是 <code>v2</code>，对于 PIM 稀疏模式是 <code>s</code></li><li><code>Nbr Count</code> — 已启用 PIM 的接口上的活动邻居计数</li></ul> |

- Query interval — 该接口上路由器查询消息的查询间隔
- DR priority — 在该接口上配置的指定路由器优先级值
- DR — 该接口的 DR 的 IP 地址

#### 示例

```
OS10# show ip pim interface
Address Interface Ver/Mode Nbr Count Query Intvl DR Prio DR

2.2.2.2 vlan103 v2/S 1 30 1 2.2.2.2
3.3.3.2 vlan105 v2/S 1 30 1 3.3.3.2
122.1.1.2 vlan121 v2/S 0 30 1 122.1.1.2
```

**支持的版本** 10.4.3.0 or later

## show ip pim mcache

显示从 VLT 对等节点和本地路由信息同步的路由。

**语法** `show ip pim [vrf vrf-name] mcache [group-address [source-address]] [vlt]`

- 参数**
- vrf vrf-name— 输入关键字 vrf，然后输入 VRF 的名称。
  - group-address— 输入以点分隔的十进制格式 (A.B.C.D) 的多播组地址。
  - source-address— 输入以点分隔的十进制格式 (A.B.C.D) 的多播源地址。

**默认** 无

**命令模式** EXEC

**使用情况信息** 此命令提供了有关多播路由的传入和传出接口的详细信息。

#### 示例

```
OS10# show ip pim mcache vlt
PIM Multicast Routing Cache Table

Flags: S - Synced

(*, 225.1.1.1), flags: S
 Incoming interface: Vlan 502
 outgoing interface list:
 Vlan 2002 (S)

(2.2.2.2, 225.1.1.1), flags: S
 Incoming interface: Vlan 501
 outgoing interface list:
 Vlan 1000, Vlan 2003 (S)
```

```
OS10# show ip pim mcache
PIM Multicast Routing Cache Table

(*, 225.1.1.1)
 Incoming interface : vlan105
 Outgoing interface list :
 vlan121

(101.1.1.10,225.1.1.1)
 Incoming interface : vlan103
 Outgoing interface list :
 vlan121
```

**支持的版本** 10.4.3.0 or later

## show ip pim neighbor

显示 PIM 邻居。

**语法** `show ip pim [vrf vrf-name] neighbor`

参数

默认

命令模式

使用情况信息

示例

支持的版本

vrf vrf-name—Enter the keyword vrf, then the name of the VRF.

无

EXEC

此命令显示以下内容：

- Neighbor address — PIM 邻居的 IP 地址
- Interface — 包含 PIM 邻居的插槽/端口信息或 VLAN/端口通道 ID 的接口类型
- Uptime/expires — PIM 邻居已启动的时间量
- Version — PIM 版本号；v2 适用于 PIM 版本 2
- DR priority/Mode — 指定的路由器优先级值和模式。默认的指定路由器优先级为 1 和 S（对于稀疏模式）

OS10# show ip pim neighbor

| Neighbor Address | Interface | Uptime/Expires    | Ver | DR Priority/Mode |
|------------------|-----------|-------------------|-----|------------------|
| 2.1.1.1          | vlan103   | 13:05:58/00:01:19 | v2  | 1 / S            |
| 3.1.1.1          | vlan105   | 13:05:58/00:01:17 | v2  | 1 / S            |

10.4.3.0 or later

show ip pim rp

显示有关所有多播组到 RP 映射的简要信息。

| 语法         | show ip pim [vrf vrf-name] rp [mapping   group-address]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|------------|-----------|------------|-----------|------------|-----------|------------|-----------|
| 参数         | <ul style="list-style-type: none"><li>• vrf vrf-name— 输入关键字 vrf, 然后输入 VRF 的名称。</li><li>• mapping — 输入关键字 mapping 以将多播组显示到 rp 映射, 以及有关如何了解 rp 的信息。</li><li>• group-address— 以点分隔的十进制格式输入多播组地址掩码, 以查看特定组的 RP (A.B.C.D)。</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 默认         | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 命令模式       | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 使用情况信息     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 示例         | <div>OS10# show ip pim rp</div> <table><thead><tr><th>Group</th><th>RP</th></tr></thead><tbody><tr><td>225.1.1.1</td><td>171.1.1.1</td></tr><tr><td>225.1.1.2</td><td>171.1.1.1</td></tr><tr><td>225.1.1.3</td><td>171.1.1.1</td></tr><tr><td>225.1.1.4</td><td>171.1.1.1</td></tr><tr><td>225.1.1.5</td><td>171.1.1.1</td></tr><tr><td>225.1.1.6</td><td>171.1.1.1</td></tr><tr><td>225.1.1.7</td><td>171.1.1.1</td></tr><tr><td>225.1.1.8</td><td>171.1.1.1</td></tr><tr><td>225.1.1.9</td><td>171.1.1.1</td></tr><tr><td>225.1.1.10</td><td>171.1.1.1</td></tr><tr><td>225.1.1.11</td><td>171.1.1.1</td></tr><tr><td>225.1.1.12</td><td>171.1.1.1</td></tr><tr><td>225.1.1.13</td><td>171.1.1.1</td></tr></tbody></table> <div>OS10# show ip pim rp mapping</div> <div>PIM Group-to-RP Mappings</div> <div>Group(s): 230.1.1.1/32</div> <div>RP: 14.1.1.1, v2</div> <div>Info source: 42.1.1.1, via bootstrap, priority 255</div> <div>expires: 00:01:53</div> <div>Group(s): 231.1.1.1/32</div> <div>RP: 9.1.1.1, v2</div> | Group | RP | 225.1.1.1 | 171.1.1.1 | 225.1.1.2 | 171.1.1.1 | 225.1.1.3 | 171.1.1.1 | 225.1.1.4 | 171.1.1.1 | 225.1.1.5 | 171.1.1.1 | 225.1.1.6 | 171.1.1.1 | 225.1.1.7 | 171.1.1.1 | 225.1.1.8 | 171.1.1.1 | 225.1.1.9 | 171.1.1.1 | 225.1.1.10 | 171.1.1.1 | 225.1.1.11 | 171.1.1.1 | 225.1.1.12 | 171.1.1.1 | 225.1.1.13 | 171.1.1.1 |
| Group      | RP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.1  | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.2  | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.3  | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.4  | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.5  | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.6  | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.7  | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.8  | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.9  | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.10 | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.11 | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.12 | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |
| 225.1.1.13 | 171.1.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |    |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |           |            |           |            |           |            |           |            |           |

```
Info source: 42.1.1.1, via bootstrap, priority 254
expires: 00:01:54
```

**支持的版本** 10.4.3.0 or later

## show ip pim ssm-range

显示使用 SSM 范围功能添加的非默认组。

**语法** `show ip pim [vrf vrf-name] ssm-range`

**参数** `vrf vrf-name`— 输入关键字 `vrf`，然后输入 VRF 的名称。

**默认** 无

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# show ip pim ssm-range
Group Address / MaskLen
224.1.1.1 / 32
```

**支持的版本** 10.4.3.0 or later

## show ip pim summary

显示 PIM 摘要。

**语法** `show ip pim [vrf vrf-name] summary`

**参数** `vrf vrf-name`— 输入关键字 `vrf`，然后输入 VRF 的名称。

**默认** 无

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# show ip pim summary

Entries in PIM-TIB/MFC : 250/150

Active Modes :
PIM-SM

TIB summary:
50/50 (*,G) entries in PIM-TIB/MFC
100/100 (S,G) entries in PIM-TIB/MFC
100/0 (S,G,Rpt) entries in PIM-TIB/MFC

Interface summary:

4 active PIM interfaces
1 active PIM neighbor

1 RPs
2 sources

Message summary:
150/50 Joins/Prunes sent/received
0/0 Candidate-RP advertisements sent/received
6/4 BSR messages sent/received
0 Null Register messages received
0/50 Register-stop messages sent/received

Data path event summary:
```

```

100 no-cache messages received
50 last-hop switchover messages received
0/0 pim-assert messages sent/received
0/0 register messages sent/received

VLT Multicast summary:
0(*,G) synced entries in MFC
281(S,G) synced entries in MFC
0(S,G,Rpt) synced entries in MFC

```

**支持的版本** 10.4.3.0 or later

## show ip pim tib

显示 PIM 树信息库 (TIB)。

**语法** `show ip pim [vrf vrf-name] tib [group-address [source-address]]`

- 参数**
- `vrf vrf-name`— 输入关键字 `vrf`，然后输入 VRF 的名称。
  - `group-address`— 输入以点分隔的十进制格式 (A.B.C.D) 的组地址。
  - `source-address`— 输入以点分隔的十进制格式 (A.B.C.D) 的源地址。

**默认** 无

**命令模式** EXEC

- 使用情况信息** 此命令显示以下内容：
- S, G — 显示多播 PIM 数据库中的条目
  - uptime — 显示条目在 PIM 路由表中的时间量
  - expires — 显示条目过期和从数据库中删除的时间量
  - RP — 显示输入的 RP 或源的 IP 地址
  - Incoming interface — 显示朝向 RP/源的反向路径转发 (RPF) 接口
  - RPF neighbor — 显示此接口朝向 RP/源的下一跳 IP 地址
  - Outgoing interface list — 列出符合以下条件之一的接口：
    - 组中直接连接的成员
    - 组中静态连接的成员
    - 收到了 (\*, G) 或 (S, G) 加入消息

**示例**

```

OS10# show ip pim tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.1.1), uptime 13:08:24, expires 00:00:12, RP 171.1.1.1, flags:
SCJ
 Incoming interface: vlan105, RPF neighbor 3.1.1.1
 Outgoing interface list:
 vlan121 Forward/Sparse 13:07:53/Never

(101.1.1.10, 225.1.1.1), uptime 13:07:51, expires 00:06:09, flags: T
 Incoming interface: vlan103, RPF neighbor 2.1.1.1
 Outgoing interface list:
 vlan121 Forward/Sparse 13:07:50/Never

```

**支持的版本** 10.4.3.0 or later



## show ip rpf

显示反向路径转发 (RPF) 信息。

|        |                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------|
| 语法     | show ip rpf [vrf vrf-name] [summary]                                                                             |
| 参数     | <ul style="list-style-type: none"><li>vrf vrf-name— 输入关键字 vrf, 然后输入 VRF 的名称。</li><li>summary — RPF 摘要。</li></ul> |
| 默认     | 无                                                                                                                |
| 命令模式   | EXEC                                                                                                             |
| 使用情况信息 | PIM 使用单播路由检查多播源可访问性。PIM 检查每个路由的距离。最短距离的路由是 PIM 为可访问性选择的路由。                                                       |

|    |                                                                                                                                                                                                                                                                                                                         |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show ip rpf RPF information for 101.1.1.10   RPF interface: vlan103   RPF neighbor: 2.1.1.1   RPF route/mask: 101.1.1.0/255.255.255.0   RPF type: Unicast RPF information for 171.1.1.1   RPF interface: vlan105   RPF neighbor: 3.1.1.1   RPF route/mask: 171.1.1.0/255.255.255.0   RPF type: Unicast</pre> |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

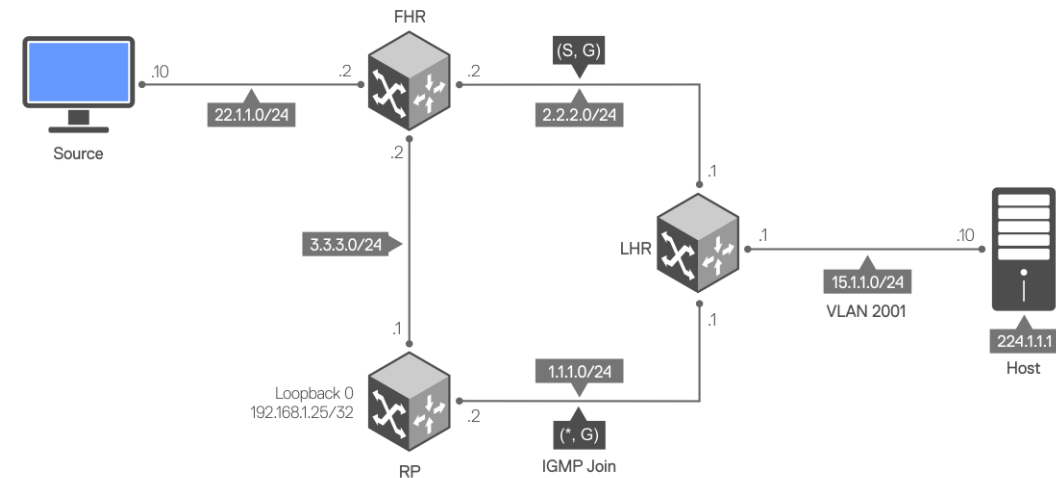
支持的版本 10.4.3.0 or later

## PIM-SM 示例配置

本部分介绍如何使用下图所示的拓扑，在 FHR、RP 和 LHR 节点中启用 PIM SM。

要启用 PIM-SM，请在每个节点（FHR、RP 和 LHR）上执行以下配置：

- 使用 ip multicast-routing 命令在所有节点上启用多播路由
- 使用 ip pim sparse-mode 命令为节点的所有必需第 3 层接口启用 PIM-SM
- 使用 ip pim rp-address 命令在每个多播启用的节点上配置 RP 地址
- 为 PIM-SM 拓扑中节点的每个接口配置 IP 地址
- 为路由更新启用路由协议 (OSPF)



FHR 节点中的示例配置:

```
FHR# configure terminal
FHR(config)#
FHR(config)# ip multicast-routing
FHR(config)# interface ethernet 1/1/31
FHR(config-if-eth1/1/31)# no switchport
FHR(config-if-eth1/1/31)# ip address 3.3.3.2/24
FHR(config-if-eth1/1/31)# ip pim sparse-mode
FHR(config-if-eth1/1/31)# ip ospf 1 area 0
FHR(config-if-eth1/1/31)# exit
FHR(config)#
FHR(config)# interface ethernet 1/1/17
FHR(config-if-eth1/1/17)#
FHR(config-if-eth1/1/17)# no switchport
FHR(config-if-eth1/1/17)# ip address 2.2.2.2/24
FHR(config-if-eth1/1/17)# ip pim sparse-mode
FHR(config-if-eth1/1/17)# ip ospf 1 area 0
FHR(config-if-eth1/1/17)# exit
FHR(config)# router ospf 1
FHR(config-router-ospf-1)# exit
FHR(config)# ip pim rp-address 192.168.1.25 group-address 224.0.0.0/4
FHR(config)#
FHR# configure terminal
FHR(config)# interface ethernet 1/1/48
FHR(config-if-eth1/1/48)# no switchport
FHR(config-if-eth1/1/48)# ip address 22.1.1.2/24
FHR(config-if-eth1/1/48)# ip pim sparse-mode
FHR(config-if-eth1/1/48)# ip ospf 1 area 0
FHR(config-if-eth1/1/48)#
```

show ip pim interface 命令将在 FHR 中显示已启用 PIM 的接口。

| Address  | Interface      | Ver/Mode | Nbr Count | Query Intvl | DR Prio | DR       |
|----------|----------------|----------|-----------|-------------|---------|----------|
| 2.2.2.2  | ethernet1/1/17 | v2/S     | 1         | 30          | 1       | 2.2.2.2  |
| 3.3.3.2  | ethernet1/1/31 | v2/S     | 1         | 30          | 1       | 3.3.3.2  |
| 22.1.1.2 | ethernet1/1/48 | v2/S     | 0         | 30          | 1       | 22.1.1.2 |

show ip pim neighbor 命令将显示 FHR 的 PIM 邻居以及用于访问邻居的接口。

| Neighbor Address | Interface      | Uptime/Expires    | Ver | DR  |
|------------------|----------------|-------------------|-----|-----|
| 2.2.2.1          | ethernet1/1/17 | 00:04:31/00:01:43 | v2  | 1 / |
| 3.3.3.1          | ethernet1/1/31 | 00:05:45/00:01:31 | v2  | 1 / |

show ip pim rp mapping 命令将显示到 RP 映射的多播组以及关于如何了解 RP 的信息。

```
FHR# show ip pim rp mapping
Group(s) : 224.0.0.0/4, Static
RP : 192.168.1.25, v2
```

RP 节点中的示例配置:

```
RP# configure terminal
RP(config)# ip multicast-routing
RP(config)# interface ethernet 1/1/31
RP(config-if-eth1/1/31)# no switchport
RP(config-if-eth1/1/31)# ip address 3.3.3.1/24
RP(config-if-eth1/1/31)# ip pim sparse-mode
RP(config-if-eth1/1/31)# ip ospf 1 area 0
RP(config-if-eth1/1/31)# exit
RP(config)#
RP(config)# interface ethernet 1/1/43
```

```

RP(config-if-eth1/1/43)# no switchport
RP(config-if-eth1/1/43)# ip address 1.1.1.2/24
RP(config-if-eth1/1/43)# ip pim sparse-mode
RP(config-if-eth1/1/43)# ip ospf 1 area 0
RP(config-if-eth1/1/43)# exit
RP(config)#
RP(config)# interface loopback 0
RP(config-if-lo-0)# ip address 192.168.1.25/32
RP(config-if-lo-0)# ip ospf 1 area 0
RP(config-if-lo-0)# exit
RP(config)# ip pim rp-address 192.168.1.25 group-address 224.0.0.0/4
RP(config)# end
RP#
RP# configure terminal
RP(config)# router ospf 1
RP(config-router-ospf-1)# end

```

show ip pim interface 命令用于显示 RP 中已启用 PIM 的接口。

```

RP# show ip pim interface

```

| Address | Interface      | Ver/Mode | Nbr Count | Query Intvl | DR Prio | DR      |
|---------|----------------|----------|-----------|-------------|---------|---------|
| 3.3.3.1 | ethernet1/1/31 | v2/S     | 1         | 30          | 1       | 3.3.3.2 |
| 1.1.1.2 | ethernet1/1/43 | v2/S     | 1         | 30          | 1       | 1.1.1.2 |

```

RP#

```

show ip pim neighbor 命令将显示 RP 的 PIM 邻居以及用于访问邻居的接口。

```

RP# show ip pim neighbor

```

| Neighbor Address | Interface      | Uptime/Expires    | Ver | DR  |
|------------------|----------------|-------------------|-----|-----|
| 3.3.3.2          | ethernet1/1/31 | 00:02:57/00:01:17 | v2  | 1 / |
| 1.1.1.1          | ethernet1/1/43 | 00:06:35/00:01:39 | v2  | 1 / |

```

RP#

```

LHR 节点中的示例配置：

```

LHR# configure terminal
LHR(config)# ip multicast-routing
LHR(config)# interface ethernet 1/1/17
LHR(config-if-eth1/1/17)#
LHR(config-if-eth1/1/17)# no switchport
LHR(config-if-eth1/1/17)# ip address 1.1.1.1/24
LHR(config-if-eth1/1/17)# ip pim sparse-mode
LHR(config-if-eth1/1/17)# ip ospf 1 area 0
LHR(config-if-eth1/1/17)# exit
LHR(config)#
LHR(config)# interface ethernet 1/1/29
LHR(config-if-eth1/1/29)# no switchport
LHR(config-if-eth1/1/29)# ip address 2.2.2.1/24
LHR(config-if-eth1/1/29)# ip pim sparse-mode
LHR(config-if-eth1/1/29)# ip ospf 1 area 0
LHR(config-if-eth1/1/29)# exit
LHR(config)#
LHR(config)# ip pim rp-address 192.168.1.25 group-address 224.0.0.0/4
LHR(config)# end
LHR(config)# interface vlan 2001
LHR(config-if-vl-2001)# no shutdown
LHR(config-if-vl-2001)# ip address 15.1.1.1/24
LHR(config-if-vl-2001)# ip pim sparse-mode
LHR(config-if-vl-2001)# ip ospf 1 area 0
LHR(config-if-vl-2001)# exit
LHR(config)#
LHR(config)# interface ethernet 1/1/38
LHR(config-if-eth1/1/38)# switchport mode trunk
LHR(config-if-eth1/1/38)# no switchport access vlan
LHR(config-if-eth1/1/38)# switchport trunk allowed vlan 2001
LHR(config-if-eth1/1/38)# exit
LHR# configure terminal

```

```
LHR(config)# router ospf 1
LHR(config-router-ospf-1)# end
```

show ip pim interface 命令将在 LHR 中显示已启用 PIM 的接口。

```
LHR# show ip pim interface
Address Interface Ver/Mode Nbr Count Query Intvl DR Prio DR

2.2.2.1 ethernet1/1/1 v2/S 1 30 1 2.2.2.2
1.1.1.1 ethernet1/1/26:1 v2/S 1 30 1 1.1.1.2
15.1.1.1 vlan2001 v2/S 0 30 1 15.1.1.1
```

show ip pim neighbor 命令将显示 LHR 的 PIM 邻居以及用于访问邻居的接口。

```
LHR# show ip pim neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority/Mode

2.2.2.2 ethernet1/1/17 00:02:58/00:01:24 v2 1 / DR S
1.1.1.2 ethernet1/1/29 00:07:49/00:01:31 v2 1 / DR S
```

```
LHR# show ip pim rp mapping
Group(s) : 224.0.0.0/4, Static
RP : 192.168.1.25, v2
```

在收到 IGMP 加入和多播流量后，以下 show 命令输出示例将显示所有节点上的 PIM 状态。

### FHR 节点中的 PIM 状态

show ip pim tib 命令输出将显示 PIM 树信息库 (TIB)。

```
FHR# show ip pim tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(22.1.1.10, 224.1.1.1), uptime 00:02:20, expires 00:01:09, flags: T
Incoming interface: ethernet1/1/48, RPF neighbor 0.0.0.0
Outgoing interface list:
 ethernet1/1/17 Forward/Sparse 00:00:19/00:03:10
```

show ip pim mcache 命令输出将显示多播路由条目。

```
FHR# show ip pim mcache
PIM Multicast Routing Cache Table

(22.1.1.10,224.1.1.1)
Incoming interface : ethernet1/1/48
Outgoing interface list :
 ethernet1/1/17
```

### RP 节点中的 PIM 状态

```
RP# show ip pim tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 224.1.1.1), uptime 00:00:57, expires 00:00:00, RP 192.168.1.25, flags: S
Incoming interface: Null, RPF neighbor 0.0.0.0
Outgoing interface list:
```

```
(22.1.1.10, 224.1.1.1), uptime 00:02:58, expires 00:03:06, flags: P
Incoming interface: ethernet1/1/31, RPF neighbor 3.3.3.2
Outgoing interface list:
```

## LHR 节点中的 IGMP 和 PIM 状态

show ip igmp groups 命令输出将显示 IGMP 数据库。

```
LHR# show ip igmp groups
Total Number of Groups: 1
IGMP Connected Group Membership
Group Address Interface Mode
Uptime Expires Last Reporter
224.1.1.1 vlan2001 IGMPv2-Compat
00:00:01 00:01:59 15.1.1.10
LHR#
```

```
LHR# show ip pim tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 224.1.1.1), uptime 00:00:05, expires 00:00:54, RP 192.168.1.25, flags: SCJ
Incoming interface: ethernet1/1/29, RPF neighbor 1.1.1.2
Outgoing interface list:
 vlan2001 Forward/Sparse 00:00:05/Never

(22.1.1.10, 224.1.1.1), uptime 00:00:05, expires 00:03:24, flags: T
Incoming interface: ethernet1/1/17, RPF neighbor 2.2.2.2
Outgoing interface list:
 vlan2001 Forward/Sparse 00:00:05/Never
```

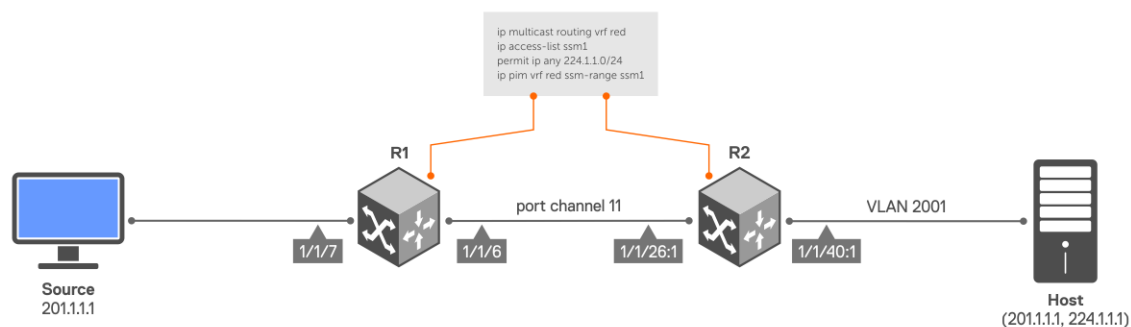
```
LHR# show ip pim mcache
PIM Multicast Routing Cache Table

(*, 224.1.1.1)
Incoming interface : ethernet1/1/29
Outgoing interface list :
 vlan2001

(22.1.1.10, 224.1.1.1)
Incoming interface : ethernet1/1/17
Outgoing interface list :
 vlan2001
```

## PIM-SSM 示例配置

本部分介绍如何使用下图所示的拓扑来启用 PIM SSM。



要启用 PIM SSM，请在 R1 和 R2 上执行以下配置：

## R1 上的示例配置:

```
R1# configure terminal
R1(config)# ip vrf red
R1(config-vrf)# end

R1# configure terminal
R1(config)# interface port-channel 11
R1(config-if-po-11)# no switchport
R1(config-if-po-11)# ip vrf forwarding red
R1(config-if-po-11)# end

R1# configure terminal
R1(config)# interface ethernet 1/1/6
R1(config-if-eth1/1/6)# no ip vrf forwarding
R1(config-if-eth1/1/6)# no switchport
R1(config-if-eth1/1/6)# channel-group 11
R1(config-if-eth1/1/6)# end

R1# configure terminal
R1(config)# interface ethernet 1/1/7
R1(config-if-eth1/1/7)# no switchport
R1(config-if-eth1/1/7)# interface ethernet 1/1/7
R1(config-if-eth1/1/7)# ip vrf forwarding red
R1(config-if-eth1/1/7)# ip address 201.1.1.2/24
R1(config-if-eth1/1/7)# ip pim sparse-mode
R1(config-if-eth1/1/7)# no shutdown
R1(config-if-eth1/1/7)# end

R1# configure terminal
R1(config)# interface port-channel 11
R1(config-if-po-11)# no switchport
R1(config-if-po-11)# interface port-channel 11
R1(config-if-po-11)# ip vrf forwarding red
R1(config-if-po-11)# ip address 193.1.1.1/24
R1(config-if-po-11)# ip pim sparse-mode
R1(config-if-po-11)# no shutdown
R1(config-if-po-11)# end

R1# configure terminal
R1(config)# interface Lo0
R1(config-if-lo-0)# ip vrf forwarding red
R1(config-if-lo-0)# ip address 2.2.2.2/32
R1(config-if-lo-0)# ip pim sparse-mode
R1(config-if-lo-0)# no shutdown
R1(config-if-lo-0)# end

R1# configure terminal
R1(config)# router ospf 100 vrf red
R1(config-router-ospf-100)# interface ethernet 1/1/7
R1(config-if-eth1/1/7)# ip ospf 100 area 0
R1(config-if-eth1/1/7)# end

R1# configure terminal
R1(config)# router ospf 100 vrf red
R1(config-router-ospf-100)# interface port-channel 11
R1(config-if-po-11)# ip ospf 100 area 0
R1(config-if-po-11)# end

R1# configure terminal
R1(config)# ip multicast-routing vrf red
R1(config)# end

R1# configure terminal
R1(config)# ip access-list test
R1(config-ip4-acl)# permit ip any 224.1.1.0/24
R1(config-ip4-acl)# exit

R1(config)# ip pim vrf red ssm-range test
R1(config)# end
```

## R2 上的示例配置:

```
R2# configure terminal
R2(config)# ip vrf red
R2(conf-vrf)# end

R2# configure terminal
R2(config)# interface vlan 2001
R2(conf-if-vl-2001)# ip vrf forwarding red
R2(conf-if-vl-2001)# end

R2# configure terminal
R2(config)# interface ethernet 1/1/40:1
R2(conf-if-eth1/1/40:1)# no ip vrf forwarding
R2(conf-if-eth1/1/40:1)# switchport mode trunk
R2(conf-if-eth1/1/40:1)# switchport trunk allowed vlan 2001
R2(conf-if-eth1/1/40:1)# end

R2# configure terminal
R2(config)# interface port-channel 11
R2(conf-if-po-11)# no switchport
R2(conf-if-po-11)# ip vrf forwarding red
R2(conf-if-po-11)# end

R2# configure terminal
R2(config)# interface ethernet 1/1/26:1
R2(conf-if-eth1/1/26:1)# no ip vrf forwarding
R2(conf-if-eth1/1/26:1)# no switchport
R2(conf-if-eth1/1/26:1)# channel-group 11
R2(conf-if-eth1/1/26:1)# end

R2# configure terminal
R2(config)# interface vlan 2001
R2(conf-if-vl-2001)# ip vrf forwarding red
R2(conf-if-vl-2001)# ip address 208.1.1.2/24
R2(conf-if-vl-2001)# ip pim sparse-mode
R2(conf-if-vl-2001)# no shutdown
R2(conf-if-vl-2001)# end

R2# configure terminal
R2(config)# interface port-channel 11
R2(conf-if-po-11)# no switchport
R2(conf-if-po-11)# interface port-channel 11
R2(conf-if-po-11)# ip vrf forwarding red
R2(conf-if-po-11)# ip address 193.1.1.2/24
R2(conf-if-po-11)# ip pim sparse-mode
R2(conf-if-po-11)# no shutdown
R2(conf-if-po-11)# end

R2# configure terminal
R2(config)# interface Lo0
R2(conf-if-lo-0)# ip vrf forwarding red
R2(conf-if-lo-0)# ip address 4.4.4.4/32
R2(conf-if-lo-0)# ip pim sparse-mode
R2(conf-if-lo-0)# no shutdown
R2(conf-if-lo-0)# end

R2# configure terminal
R2(config)# router ospf 100 vrf red
R2(config-router-ospf-100)# interface vlan 2001
R2(conf-if-vl-2001)# ip ospf 100 area 0
R2(conf-if-vl-2001)# end

R2# configure terminal
R2(config)# router ospf 100 vrf red
R2(config-router-ospf-100)# interface port-channel 11
R2(conf-if-po-11)# ip ospf 100 area 0
R2(conf-if-po-11)# end

R2# configure terminal
R2(config)# ip multicast-routing vrf red
R2(config)# end
```

```
R2# configure terminal
R2(config)# ip access-list test
R2(config-ipv4-acl)# permit ip any 224.1.1.0/24
R2(config-ipv4-acl)# exit
R2(config)# ip pim vrf red ssm-range test
R2(config)# end
```

## 验证配置

要验证配置，请在 R1 上使用以下 show 命令：

show ip pim vrf red neighbor 命令用于显示 R1 的 PIM 邻居和通过其到达邻居的接口。

```
R1# show ip pim vrf red neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority / Mode

193.1.1.2 port-channel11 02:34:33/00:01:17 v2 1 / DR S
```

show ip pim vrf red ssm-range 命令将显示指定的多播地址范围。

```
R1# show ip pim vrf red ssm-range
Group Address / MaskLen
224.1.1.0 / 24
```

show ip pim vrf red tib 命令输出将显示 PIM 树信息库 (TIB)。

```
R1# show ip pim vrf red tib
PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(201.1.1.1, 224.1.1.1), uptime 00:19:42, expires 00:00:47, flags: T
Incoming interface: ethernet1/1/7, RPF neighbor 0.0.0.0
Outgoing interface list:
port-channel11 Forward/Sparse 00:00:37/00:02:52
```

show ip pim vrf red mcache 命令输出将显示多播路由条目。

```
R1# show ip pim vrf red mcache
PIM Multicast Routing Cache Table
(201.1.1.1, 224.1.1.1)
Incoming interface : ethernet1/1/7
Outgoing interface list :
port-channel11
```

在 R2 上使用以下 show 命令：

show ip igmp vrf red groups 命令输出将显示 IGMP 数据库。

```
R2# show ip igmp vrf red groups
Total Number of Groups: 1
IGMP Connected Group Membership
Group Address Interface Mode Uptime Expires Last Reporter
224.1.1.1 vlan2001 Include 00:00:03 Never 208.1.1.1
```

show ip pim vrf red tib 命令输出将显示 PIM 树信息库 (TIB)。

```
R2# show ip pim vrf red tib
PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(201.1.1.1, 224.1.1.1), uptime 00:00:06, expires 00:03:23, flags: CT
Incoming interface: port-channel11, RPF neighbor 193.1.1.1
```



```
Outgoing interface list:
vlan2001 Forward/Sparse 00:00:06/Never
```

show ip pim vrf red neighbor 命令用于显示 R2 的 PIM 邻居和通过其到达邻居的接口。

```
R2# show ip pim vrf red neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority / Mode

193.1.1.1 port-channel11 02:34:15/00:01:29 v2 1/ S
```

show ip pim vrf red ssm-range 命令将显示指定的多播地址范围。

```
R2# show ip pim vrf red ssm-range
Group Address / MaskLen
224.1.1.0 / 24
```

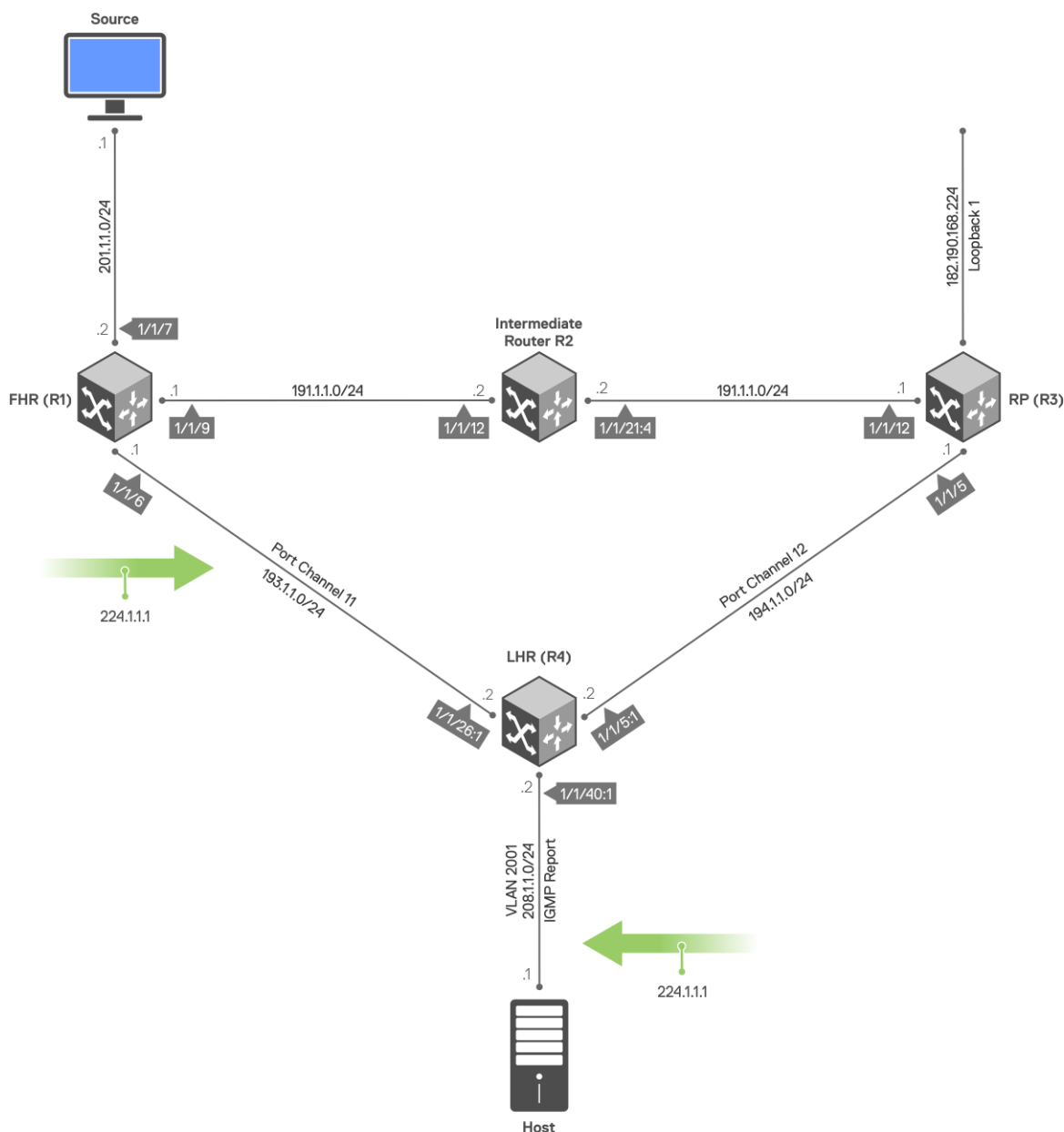
show ip pim vrf red mcache 命令输出将显示多播路由条目。

```
R2# show ip pim vrf red mcache
PIM Multicast Routing Cache Table

(201.1.1.1, 224.1.1.1)
Incoming interface : port-channel11
Outgoing interface list :
vlan2001
```

# 多播 VRF 配置示例

本部分介绍如何使用下图所示的拓扑，在非默认 VRF 实例中配置 IPv4 多播。



在每个节点 — R1、R2、R3 和 R4 上，执行以下配置。

**R1 上的示例配置：**

```
R1# configure terminal
R1(config)# ip vrf red
R1(conf-vrf)# end

R1# configure terminal
R1(config)# interface port-channel 11
R1(conf-if-po-11)# no switchport
R1(conf-if-po-11)# ip vrf forwarding red
R1(conf-if-po-11)# end

R1# configure terminal
R1(config)# interface ethernet 1/1/6
R1(conf-if-eth1/1/6)# no ip vrf forwarding
```

```

R1(conf-if-eth1/1/6)# no switchport
R1(conf-if-eth1/1/6)# channel-group 11
R1(conf-if-eth1/1/6)# end

R1# configure terminal
R1(config)# interface ethernet 1/1/7
R1(conf-if-eth1/1/7)# no switchport
R1(conf-if-eth1/1/7)# interface ethernet 1/1/7
R1(conf-if-eth1/1/7)# ip vrf forwarding red
R1(conf-if-eth1/1/7)# ip address 201.1.1.2/24
R1(conf-if-eth1/1/7)# ip pim sparse-mode
R1(conf-if-eth1/1/7)# no shutdown
R1(conf-if-eth1/1/7)# end

R1# configure terminal
R1(config)# interface ethernet 1/1/9
R1(conf-if-eth1/1/9)# no switchport
R1(conf-if-eth1/1/9)# interface ethernet 1/1/9
R1(conf-if-eth1/1/9)# ip vrf forwarding red
R1(conf-if-eth1/1/9)# ip address 191.1.1.1/24
R1(conf-if-eth1/1/9)# ip pim sparse-mode
R1(conf-if-eth1/1/9)# no shutdown
R1(conf-if-eth1/1/9)# end

R1# configure terminal
R1(config)# interface port-channel 11
R1(conf-if-po-11)# no switchport
R1(conf-if-po-11)# interface port-channel 11
R1(conf-if-po-11)# ip vrf forwarding red
R1(conf-if-po-11)# ip address 193.1.1.1/24
R1(conf-if-po-11)# ip pim sparse-mode
R1(conf-if-po-11)# no shutdown
R1(conf-if-po-11)# end

R1# configure terminal
R1(config)# interface Lo0
R1(conf-if-lo-0)# ip vrf forwarding red
R1(conf-if-lo-0)# ip address 2.2.2.2/32
R1(conf-if-lo-0)# ip pim sparse-mode
R1(conf-if-lo-0)# no shutdown
R1(conf-if-lo-0)# end

R1# configure terminal
R1(config)# router ospf 100 vrf red
R1(config-router-ospf-100)# interface ethernet 1/1/7
R1(conf-if-eth1/1/7)# ip ospf 100 area 0
R1(conf-if-eth1/1/7)# end

R1# configure terminal
R1(config)# router ospf 100 vrf red
R1(config-router-ospf-100)# interface ethernet 1/1/9
R1(conf-if-eth1/1/9)# ip ospf 100 area 0
R1(conf-if-eth1/1/9)# end

R1# configure terminal
R1(config)# router ospf 100 vrf red
R1(config-router-ospf-100)# interface port-channel 11
R1(conf-if-po-11)# ip ospf 100 area 0
R1(conf-if-po-11)# end

R1# configure terminal
R1(config)# ip multicast-routing vrf red
R1(config)# end

R1# configure terminal
R1(config)# ip pim vrf red rp-address 182.190.168.224 group-address 224.0.0.0/4
R1(config)# end

```

## R2 上的示例配置:

```

R2# configure terminal
R2(config)# ip vrf red
R2(config-vrf)# end

```

```

R2# configure terminal
R2(config)# interface vlan 1001
R2(conf-if-vl-1001)# ip vrf forwarding red
R2(conf-if-vl-1001)# end

R2# configure terminal
R2(config)# interface ethernet 1/1/21:4
R2(conf-if-eth1/1/21:4)# switchport mode trunk
R2(conf-if-eth1/1/21:4)# switchport trunk allowed vlan 1001
R2(conf-if-eth1/1/21:4)# end

R2# configure terminal
R2(config)# interface ethernet 1/1/12:1
R2(conf-if-eth1/1/12:1)# no switchport
R2(conf-if-eth1/1/12:1)# ip vrf forwarding red
R2(conf-if-eth1/1/12:1)# ip address 191.1.1.2/24
R2(conf-if-eth1/1/12:1)# ip pim sparse-mode
R2(conf-if-eth1/1/12:1)# no shutdown
R2(conf-if-eth1/1/12:1)# end

R2# configure terminal
R2(config)# interface vlan 1001
R2(conf-if-vl-1001)# ip vrf forwarding red
R2(conf-if-vl-1001)# ip address 192.1.1.2/24
R2(conf-if-vl-1001)# ip pim sparse-mode
R2(conf-if-vl-1001)# no shutdown
R2(conf-if-vl-1001)# end

R2# configure terminal
R2(config)# interface Lo0
R2(conf-if-lo-0)# ip vrf forwarding red
R2(conf-if-lo-0)# ip address 1.1.1.1/32
R2(conf-if-lo-0)# ip pim sparse-mode
R2(conf-if-lo-0)# no shutdown
R2(conf-if-lo-0)# end

R2# configure terminal
R2(config)# router ospf 100 vrf red
R2(config-router-ospf-100)# interface ethernet 1/1/12:1
R2(conf-if-eth1/1/12:1)# ip ospf 100 area 0
R2(conf-if-eth1/1/12:1)# end

R2# configure terminal
R2(config)# router ospf 100 vrf red
R2(config-router-ospf-100)# interface vlan 1001
R2(conf-if-vl-1001)# ip ospf 100 area 0
R2(conf-if-vl-1001)# end

R2# configure terminal
R2(config)# ip multicast-routing vrf red
R2(config)# end

R2# configure terminal
R2(config)# ip pim vrf red rp-address 182.190.168.224 group-address 224.0.0.0/4
R2(config)# end

```

### R3 上的示例配置:

```

R3# configure terminal
R3(config)# ip vrf red
R3(conf-vrf)# end

R3# configure terminal
R3(config)# interface vlan 1001
R3(conf-if-vl-1001)# ip vrf forwarding red
R3(conf-if-vl-1001)# end

R3# configure terminal
R3(config)# interface ethernet 1/1/12
R3(conf-if-eth1/1/12)# no ip vrf forwarding
R3(conf-if-eth1/1/12)# switchport mode trunk
R3(conf-if-eth1/1/12)# switchport trunk allowed vlan 1001

```

```

R3(config-if-eth1/1/12)# end

R3# configure terminal
R3(config)# interface port-channel 12
R3(config-if-po-12)# no switchport
R3(config-if-po-12)# ip vrf forwarding red
R3(config-if-po-12)# end
R3# configure terminal
R3(config)# interface ethernet 1/1/5
R3(config-if-eth1/1/5)# no ip vrf forwarding
R3(config-if-eth1/1/5)# no switchport
R3(config-if-eth1/1/5)# channel-group 12
R3(config-if-eth1/1/5)# end

R3# configure terminal
R3(config)# interface vlan 1001
R3(config-if-vl-1001)# ip vrf forwarding red
R3(config-if-vl-1001)# ip address 192.1.1.1/24
R3(config-if-vl-1001)# ip pim sparse-mode
R3(config-if-vl-1001)# no shutdown
R3(config-if-vl-1001)# end

R3# configure terminal
R3(config)# interface port-channel 12
R3(config-if-po-12)# no switchport
R3(config-if-po-12)# interface port-channel 12
R3(config-if-po-12)# ip vrf forwarding red
R3(config-if-po-12)# ip address 194.1.1.1/24
R3(config-if-po-12)# ip pim sparse-mode
R3(config-if-po-12)# no shutdown
R3(config-if-po-12)# end

R3# configure terminal
R3(config)# interface Lo0
R3(config-if-lo-0)# ip vrf forwarding red
R3(config-if-lo-0)# ip address 3.3.3.3/32
R3(config-if-lo-0)# ip pim sparse-mode
R3(config-if-lo-0)# no shutdown
R3(config-if-lo-0)# end

R3# configure terminal
R3(config)# router ospf 100 vrf red
R3(config-router-ospf-100)# interface vlan 1001
R3(config-if-vl-1001)# ip ospf 100 area 0
R3(config-if-vl-1001)# end

R3# configure terminal
R3(config)# router ospf 100 vrf red
R3(config-router-ospf-100)# interface port-channel 12
R3(config-if-po-12)# ip ospf 100 area 0
R3(config-if-po-12)# end

R3# configure terminal
R3(config)# router ospf 100 vrf red
R3(config-router-ospf-100)# interface Lo1
R3(config-if-lo-1)# ip ospf 100 area 0
R3(config-if-lo-1)# end

R3# configure terminal
R3(config)# ip multicast-routing vrf red
R3(config)# end

R3# configure terminal
R3(config)# interface Lo1
R3(config-if-lo-1)# ip vrf forwarding red
R3(config-if-lo-1)# ip address 182.190.168.224/32
R3(config-if-lo-1)# ip pim sparse-mode
R3(config-if-lo-1)# no shutdown
R3(config-if-lo-1)# end

R3# configure terminal
R3(config)# ip pim vrf red rp-address 182.190.168.224 group-address 224.0.0.0/4
R3(config)# end

```

## R4 上的示例配置:

```
R4# configure terminal
R4(config)# ip vrf red
R4(config-vrf)# end

R4# configure terminal
R4(config)# interface vlan 2001
R4(config-if-vl-2001)# ip vrf forwarding red
R4(config-if-vl-2001)# end

R4# configure terminal
R4(config)# interface ethernet 1/1/40:1
R4(config-if-eth1/1/40:1)# no ip vrf forwarding
R4(config-if-eth1/1/40:1)# switchport mode trunk
R4(config-if-eth1/1/40:1)# switchport trunk allowed vlan 2001
R4(config-if-eth1/1/40:1)# end

R4# configure terminal
R4(config)# interface port-channel 11
R4(config-if-po-11)# no switchport
R4(config-if-po-11)# ip vrf forwarding red
R4(config-if-po-11)# end
R4# configure terminal
R4(config)# interface port-channel 12
R4(config-if-po-12)# no switchport
R4(config-if-po-12)# ip vrf forwarding red
R4(config-if-po-12)# end

R4# configure terminal
R4(config)# interface ethernet 1/1/26:1
R4(config-if-eth1/1/26:1)# no ip vrf forwarding
R4(config-if-eth1/1/26:1)# no switchport
R4(config-if-eth1/1/26:1)# channel-group 11
R4(config-if-eth1/1/26:1)# end

R4# configure terminal
R4(config)# interface ethernet 1/1/5:1
R4(config-if-eth1/1/5:1)# no ip vrf forwarding
R4(config-if-eth1/1/5:1)# no switchport
R4(config-if-eth1/1/5:1)# channel-group 12
R4(config-if-eth1/1/5:1)# end

R4# configure terminal
R4(config)# interface vlan 2001
R4(config-if-vl-2001)# ip vrf forwarding red
R4(config-if-vl-2001)# ip address 208.1.1.2/24
R4(config-if-vl-2001)# ip pim sparse-mode
R4(config-if-vl-2001)# no shutdown
R4(config-if-vl-2001)# end

R4# configure terminal
R4(config)# interface port-channel 11
R4(config-if-po-11)# no switchport
R4(config-if-po-11)# interface port-channel 11
R4(config-if-po-11)# ip vrf forwarding red
R4(config-if-po-11)# ip address 193.1.1.2/24
R4(config-if-po-11)# ip pim sparse-mode
R4(config-if-po-11)# no shutdown
R4(config-if-po-11)# end

R4# configure terminal
R4(config)# interface port-channel 12
R4(config-if-po-12)# no switchport
R4(config-if-po-12)# interface port-channel 12
R4(config-if-po-12)# ip vrf forwarding red
R4(config-if-po-12)# ip address 194.1.1.2/24
R4(config-if-po-12)# ip pim sparse-mode
R4(config-if-po-12)# no shutdown
R4(config-if-po-12)# end

R4# configure terminal
```

```

R4(config)# interface Lo0
R4(config-if-lo-0)# ip vrf forwarding red
R4(config-if-lo-0)# ip address 4.4.4.4/32
R4(config-if-lo-0)# ip pim sparse-mode
R4(config-if-lo-0)# no shutdown
R4(config-if-lo-0)# end

R4# configure terminal
R4(config)# router ospf 100 vrf red
R4(config-router-ospf-100)# interface vlan 2001
R4(config-if-vl-2001)# ip ospf 100 area 0
R4(config-if-vl-2001)# end

R4# configure terminal
R4(config)# router ospf 100 vrf red
R4(config-router-ospf-100)# interface port-channel 11
R4(config-if-po-11)# ip ospf 100 area 0
R4(config-if-po-11)# end

R4# configure terminal
R4(config)# router ospf 100 vrf red
R4(config-router-ospf-100)# interface port-channel 12
R4(config-if-po-12)# ip ospf 100 area 0
R4(config-if-po-12)# end

R4# configure terminal
R4(config)# ip multicast-routing vrf red
R4(config)# end

R4# configure terminal
R4(config)# ip pim vrf red rp-address 182.190.168.224 group-address 224.0.0.0/4
R4(config)# end

```

## 验证配置

要验证配置，请使用以下 show 命令。

### 第一跳路由器 (R1)

```

R1# show ip pim vrf red neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority / Mode

191.1.1.2 ethernet1/1/9 02:13:21/00:01:25 v2 1/ DR S
193.1.1.2 port-channel11 02:15:29/00:01:22 v2 1/ DR S

```

```

R1# show ip pim vrf red tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(201.1.1.1, 224.1.1.1), uptime 00:00:33, expires 00:02:56, flags: FT
 Incoming interface: ethernet1/1/7, RPF neighbor 0.0.0.0
 Outgoing interface list:
 port-channel11 Forward/Sparse 00:00:33/00:02:56

```

```

R1# show ip pim vrf red rp
Group RP

```

```

224.1.1.1 182.190.168.224
```

```
R1# show ip pim vrf red rp mapping
Group(s) : 224.0.0.0/4, Static
RP : 182.190.168.224, v2
```

```
R1# show ip pim vrf red mcache
PIM Multicast Routing Cache Table

(201.1.1.1, 224.1.1.1)
Incoming interface : ethernet1/1/7
Outgoing interface list :
port-channel11
```

### 集合点 (R3)

```
R3# show ip pim vrf red neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority / Mode

192.1.1.2 vlan1001 02:11:46/00:01:33 v2 1/ DR S
194.1.1.2 port-channel12 02:14:12/00:01:33 v2 1/ DR S
```

```
R3# show ip pim vrf red tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 224.1.1.1), uptime 00:01:48, expires 00:00:00, RP 182.190.168.224, flags: S
Incoming interface: Null, RPF neighbor 0.0.0.0
Outgoing interface list:
port-channel12 Forward/Sparse 00:01:48/00:02:41
```

```
R3# show ip pim vrf red mcache
PIM Multicast Routing Cache Table

(*, 224.1.1.1)
Incoming interface :
Outgoing interface list :
port-channel12
```

```
R3# show ip rpf vrf red
RPF information for 182.190.168.224
RPF interface:
RPF neighbor: 0.0.0.0
RPF route/mask: 0.0.0.0/0.0.0.0
RPF type: Unicast
```

```
R3# show ip pim vrf red rp mapping
Group(s) : 224.0.0.0/4, Static
RP : 182.190.168.224, v2
```

```
R3# show ip pim vrf red rp
Group RP

224.1.1.1 182.190.168.224
```

```
R3# show ip pim vrf red rp
Group RP
```



```

224.1.1.1 182.190.168.224
```

```
R3# show ip pim vrf red tib
```

```
PIM Multicast Routing Table
```

```
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
```

```
Timers: Uptime/Expires
```

```
Interface state: Interface, next-Hop, State/Mode
```

```
(* , 224.1.1.1), uptime 00:04:41, expires 00:00:00, RP 182.190.168.224, flags: S
Incoming interface: Null, RPF neighbor 0.0.0.0
Outgoing interface list:
 port-channel12 Forward/Sparse 00:04:41/00:02:48
```

```
(201.1.1.1, 224.1.1.1), uptime 00:01:55, expires 00:02:29, flags: P
Incoming interface: port-channel12, RPF neighbor 194.1.1.2
Outgoing interface list:
```

```
R3# show ip pim vrf red mcache
```

```
PIM Multicast Routing Cache Table
```

```
(* , 224.1.1.1)
Incoming interface :
Outgoing interface list :
 port-channel12
```

#### 最后一跳路由器 (R4)

```
R4# show ip pim vrf red neighbor
```

| Neighbor Address | Interface      | Uptime/Expires    | Ver | DR | Priority | Mode |
|------------------|----------------|-------------------|-----|----|----------|------|
| 193.1.1.1        | port-channel11 | 02:11:48/00:01:26 | v2  | 1  |          | / S  |
| 194.1.1.1        | port-channel12 | 02:12:07/00:01:41 | v2  | 1  |          | / S  |

```
R4# show ip pim vrf red rp mapping
```

```
Group(s) : 224.0.0.0/4, Static
```

```
RP : 182.190.168.224, v2
```

```
R4# show ip pim vrf red rp
```

| Group     | RP              |
|-----------|-----------------|
| 224.1.1.1 | 182.190.168.224 |

```
R4# show ip igmp vrf red groups
```

```
Total Number of Groups: 1
```

```
IGMP Connected Group Membership
```

| Group Address | Expires  | Interface | Mode          |
|---------------|----------|-----------|---------------|
| 224.1.1.1     | 00:02:07 | vlan2001  | IGMPv2-Compat |
| 00:00:18      |          | 208.1.1.1 |               |

```
R4# show ip rpf vrf red
```

```
RPF information for 182.190.168.224
```

```
 RPF interface: port-channel12
```

```
 RPF neighbor: 194.1.1.1
```

```
 RPF route/mask: 182.190.168.224/255.255.255.255
```

```
 RPF type: Unicast
```

```
R4# show ip pim vrf red tib
```

```
PIM Multicast Routing Table
```

```
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
```

```
Timers: Uptime/Expires
```

```
Interface state: Interface, next-Hop, State/Mode
```

```
(*, 224.1.1.1), uptime 00:05:44, expires 00:00:15, RP 182.190.168.224, flags: SCJ
Incoming interface: port-channel12, RPF neighbor 194.1.1.1
Outgoing interface list:
 vlan2001 Forward/Sparse 00:05:44/Never

(201.1.1.1, 224.1.1.1), uptime 00:02:58, expires 00:00:31, flags: CT
Incoming interface: port-channel11, RPF neighbor 193.1.1.1
Outgoing interface list:
 vlan2001 Forward/Sparse 00:02:58/Never

R4# show ip pim vrf red mcache
PIM Multicast Routing Cache Table

(*, 224.1.1.1)
Incoming interface : port-channel12
Outgoing interface list :
 vlan2001

(201.1.1.1, 224.1.1.1)
Incoming interface : port-channel11
Outgoing interface list :
 vlan2001

R4# show ip pim vrf red summary

Entries in PIM-TIB/MFC: 3/2

Active Modes:
 PIM-SM

Interface summary:
 4 active PIM interfaces
 0 passive PIM interfaces
 2 active PIM neighbor

TIB Summary:
 1/1 (*,G) entries in PIM-TIB/MFC
 1/1 (S,G) entries in PIM-TIB/MFC
 1/0 (S,G,Rpt) entries in PIM-TIB/MFC

 1 RP
 1 sources

Message Summary:
 81268/13033 Joins/Prunes sent/received
 0 Null Register messages received
 0/0 Register-stop messages sent/received

Data path event summary:
 0/0 pim-assert messages sent/received
 0/0 register messages sent/received
```

## VLT 多播路由

OS10 支持 IPv4 网络的 VLT 域中的多播路由。当 VLT 对等节点或 VLTi 链路停机时，此功能可提供对多播路由流量的弹性。

### 多播路由表同步

多播路由协议不会在对等 VLT 节点之间交换多播路由。每个 VLT 节点独立于对等 VLT 节点运行 PIM 协议。因此，PIM 状态不会在节点之间同步。但是，OS10 会将多播路由表与在对等 VLT 节点之间每个节点上学习的 PIM 的路由进行同步。多播路由表同步：

- 避免通过 VLTi 链路进行非优化转发。表同步允许将传入流量发送到设备中本地路由的错误对等节点。
- 在 VLT 节点发生故障时提供流量弹性。在 PIM 协议重新融合并构建新树之前，将转发流量。

## IGMP 消息同步

VLT 节点使用 VLTi 链路在其对等节点之间同步 IGMP 消息。在其中一个 VLT 节点上接收到的任何 IGMP 加入消息都会与对等节点同步。因此，VLT 域中的 IGMP 表是相同的。

## 出口掩码

当来自源的多播流量到达其中一个 VLT 对等节点时，将使用本地路由或切换功能并通过 VLTi 链路将其发送到下游接收器。对等节点的 VLTi 链路上的端口块会丢弃多播流量。此端口块也称为出口掩码，可避免两个 VLT 节点的 VLT 端口通道上存在重复的流量转发。但是，如果接收器连接到对等节点，则系统会将多播流量转发至接收器。

## 跨区 VLAN

在两个 VLT 对等节点上配置的任何 VLAN 都称为一个跨区 VLAN。VLT 互连 (VLTi) 端口将自动添加为跨区 VLAN 的成员。连接到跨区 VLAN 子网上的至少一个 VLT 节点的任何相邻路由器均可直接从 L3 级别的两个 VLT 对等节点访问。

- 跨区 VLAN L3 接口：如果您对两个 VLT 节点上的每个跨区 VLAN L3 接口启用 PIM，则接口为一个跨区 VLAN L3 接口。
  - 跨区 VLT VLAN L3 接口：包括至少有一个 VLT 端口配置为端口通道成员的所有跨区 L3 VLAN。
  - 跨区非 VLT VLAN L3 接口：包括未将 VLT 端口配置为端口通道成员的所有跨区 VLAN。
- 非跨区 L3 接口：所有未将 VLT 端口配置为端口通道成员的点对点接口或 L3 VLAN。

有关详情，请参阅[部署注意事项](#)。

## 部署注意事项

Dell EMC 建议执行以下操作：

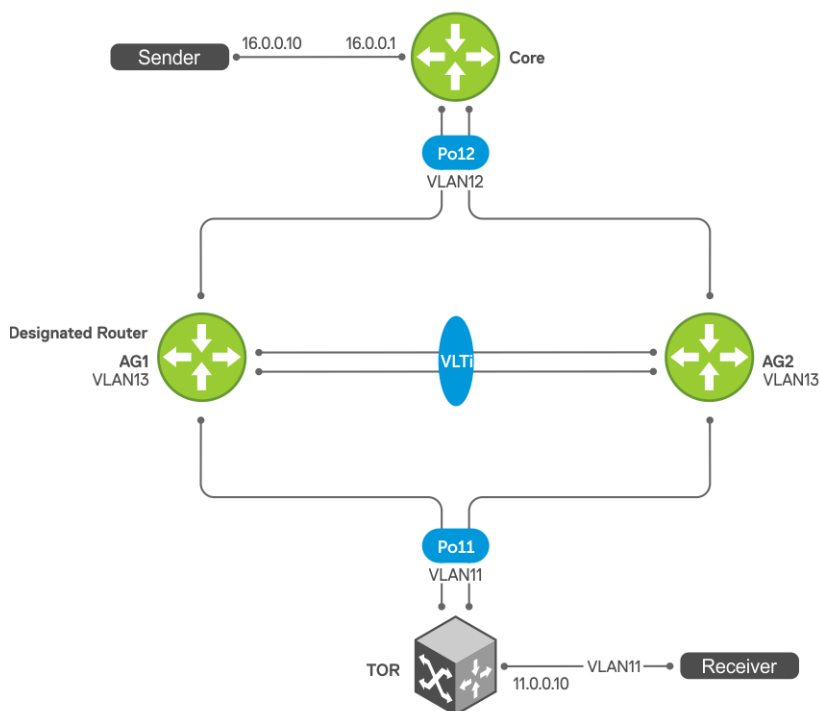
- 在已启用 VLT 的 PIM 路由器中，当有多个 PIM 跨区路径到达源或 RP 时，不支持多播路由。仅配置一个 PIM 跨区路径以到达聚合或主干中的任何 PIM 路由器。
- 如果源连接到 VLT 对等节点的非跨区接口，并且从两个 VLT 节点的跨区接口可访问 RP，则接收方可能会收到重复流量。为避免出现重复流量，请将源配置为可在跨区接口上访问。
- 为获得更好的融合，上游传入接口 (IIF) 和下游传出接口 (OIF) 必须是跨区 VLAN。
- 在 VLT 部署中，Dell EMC 建议不要通过使用 `ip pim dr-priority` 命令配置非默认值来更改 PIM 指定的路由器。
- 在大规模多播部署中，您可能会看到频繁的多播控制流量猝发。对于此类部署，Dell EMC 建议您在所有 PIM 路由器上使用控制平面监察来增加队列 2 的突发大小。有关如何将 QoS 策略配置为速率限制控制平面流量的详细信息，请参阅[配置控制平面监察](#)。

 **注：**OS10 不支持任播 RP。

## 示例：跨区 L3 VLAN IIF

本部分介绍如何使用下图所示的拓扑在四节点设置 (core、AG1、AG2 和 ToR) 中配置 VLT 多播路由：

- Core、AG1 和 AG2 是 VLT 域中的多播路由器。
- ToR 是启用了 IGMP 的 L2 交换机。
- OSPF 是单播路由协议。



## 核心上的配置示例：

```

core# configure terminal
core(config)# ip multicast-routing
core(config)# ip pim rp-address 103.0.0.3 group-address 224.0.0.0/4
core(config)# router ospf 100
core(config-router-ospf-100)# exit

core(config)# interface ethernet 1/1/32:1
core(conf-if-eth1/1/32:1)# no shutdown
core(conf-if-eth1/1/32:1)# no switchport
core(conf-if-eth1/1/32:1)# ip address 16.0.0.1/24
core(conf-if-eth1/1/32:1)# flowcontrol receive off
core(conf-if-eth1/1/32:1)# ip pim sparse-mode
core(conf-if-eth1/1/32:1)# ip ospf 100 area 0.0.0.0
core(conf-if-eth1/1/32:1)# exit

core(config)# interface vlan 12
core(conf-if-vl-12)# no shutdown
core(conf-if-vl-12)# ip address 12.0.0.3/24
core(conf-if-vl-12)# ip pim sparse-mode
core(conf-if-vl-12)# ip pim dr-priority 1000
core(conf-if-vl-12)# ip ospf 100 area 0.0.0.0
core(conf-if-vl-12)# exit

core(config)# interface loopback 103
core(conf-if-lo-103)# no shutdown
core(conf-if-lo-103)# ip address 103.0.0.3/32
core(conf-if-lo-103)# ip pim sparse-mode
core(conf-if-lo-103)# ip ospf 100 area 0.0.0.0
core(conf-if-lo-103)# exit

```

### 核心和接口的 PIM 邻居以到达邻居

show ip pim neighbor 命令将显示核心和接口的 PIM 邻居以到达邻居。

```

core# show ip pim neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority / Mode

```

|          |        |                   |    |    |     |
|----------|--------|-------------------|----|----|-----|
| 12.0.0.1 | vlan12 | 00:01:06/00:01:43 | v2 | 10 | / S |
| 12.0.0.2 | vlan12 | 00:01:03/00:01:42 | v2 | 10 | / S |

## 核心中的 PIM 状态

show ip pim tib 命令的输出。

```
core# show ip pim tib
PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.1.1), uptime 00:04:16, expires 00:00:00, RP 103.0.0.3, flags: S
 Incoming interface: Null, RPF neighbor 0.0.0.0
 Outgoing interface list:
 vlan12 Forward/Sparse 00:04:16/00:03:13
```

## 以下 show 命令输出显示流启动后的流量:

show ip pim tib 命令输出将显示 PIM 树信息库 (TIB)。

```
core# show ip pim tib
PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.1.1), uptime 00:09:54, expires 00:00:00, RP 103.0.0.3, flags: S
 Incoming interface: Null, RPF neighbor 0.0.0.0
 Outgoing interface list:
 vlan12 Forward/Sparse 00:09:54/00:02:35

(16.0.0.10, 225.1.1.1), uptime 00:00:34, expires 00:02:55, flags: FT
 Incoming interface: ethernet1/1/32:1, RPF neighbor 0.0.0.0
 Outgoing interface list:
 vlan12 Forward/Sparse 00:00:34/00:02:55
```

show ip pim mcache 命令输出将显示多播路由条目。

```
core# show ip pim mcache
PIM Multicast Routing Cache Table

(16.0.0.10, 225.1.1.1)
 Incoming interface : ethernet1/1/32:1
 Outgoing interface list :
 vlan12
```

## AG1 上的配置示例:

```
AG1# configure terminal
AG1(config)# ip multicast-routing
AG1 (config)# ip pim rp-address 103.0.0.3 group-address 224.0.0.0/4
AG1(config)# router ospf 100
AG1(config-router-ospf-100)# exit

AG1(config)# vlt-domain 255
AG1(conf-vlt-255)# backup destination 10.16.132.147
AG1(conf-vlt-255)# discovery-interface ethernet1/1/31:1,1/1/31:4
AG1(conf-vlt-255)# peer-routing
AG1(conf-vlt-255)# primary-priority 1
AG1(conf-vlt-255)# vlt-mac 00:00:00:11:11:11
AG1(conf-vlt-255)# exit
```

```

AG1(config)# interface ethernet 1/1/32:1
AG1(conf-if-eth1/1/32:1)# no shutdown
AG1(conf-if-eth1/1/32:1)# no switchport
AG1(conf-if-eth1/1/32:1)# ip address 16.0.0.1/24
AG1(conf-if-eth1/1/32:1)# flowcontrol receive off
AG1(conf-if-eth1/1/32:1)# ip pim sparse-mode
AG1(conf-if-eth1/1/32:1)# ip ospf 100 area 0.0.0.0
AG1(conf-if-eth1/1/32:1)# exit

```

```

AG1(config)# interface vlan 11
AG1(conf-if-vlan-11)# no shutdown
AG1(conf-if-vlan-11)# ip address 11.0.0.1/24
AG1(conf-if-vlan-11)# ip pim sparse-mode
AG1(conf-if-vlan-11)# ip pim dr-priority 1000
AG1(conf-if-vlan-11)# ip ospf 100 area 0.0.0.0
AG1(conf-if-vlan-11)# ip ospf cost 3000
AG1(conf-if-vlan-11)# exit

```

```

AG1(config)# interface vlan 12
AG1(conf-if-vlan-12)# no shutdown
AG1(conf-if-vlan-12)# ip address 12.0.0.1/24
AG1(conf-if-vlan-12)# ip pim sparse-mode
AG1(conf-if-vlan-12)# ip pim dr-priority 10
AG1(conf-if-vlan-12)# ip ospf 100 area 0.0.0.0
AG1(conf-if-vlan-12)# exit

```

```

AG1(config)# interface vlan 13
AG1(conf-if-vlan-13)# no shutdown
AG1(conf-if-vlan-13)# ip address 13.0.0.1/24
AG1(conf-if-vlan-13)# ip pim sparse-mode
AG1(conf-if-vlan-13)# ip pim dr-priority 10
AG1(conf-if-vlan-13)# ip ospf 100 area 0.0.0.0
AG1(conf-if-vlan-13)# ip ospf cost 4000
AG1(conf-if-vlan-13)# exit

```

```

AG1(config)# interface loopback 101
AG1(conf-if-lo-101)# no shutdown
AG1(conf-if-lo-101)# ip address 101.0.0.1/32
AG1(conf-if-lo-101)# ip pim sparse-mode
AG1(conf-if-lo-101)# ip ospf 100 area 0.0.0.0
AG1(conf-if-lo-101)# exit

```

```

AG1(config)# interface port-channel11
AG1(conf-if-po-11)# no shutdown
AG1(conf-if-po-11)# switchport mode trunk
AG1(conf-if-po-11)# switchport trunk allowed vlan 11
AG1(conf-if-po-11)# vlt-port-channel 11
AG1(conf-if-po-11)# exit

```

```

AG1(config)# interface port-channel12
AG1(conf-if-po-12)# no shutdown
AG1(conf-if-po-12)# switchport mode trunk
AG1(conf-if-po-12)# switchport access vlan 1
AG1(conf-if-po-12)# switchport trunk allowed vlan 12
AG1(conf-if-po-12)# vlt-port-channel 12
AG1(conf-if-po-12)# exit

```

## AG1 和接口的 PIM 邻居以到达邻居

show ip pim neighbor 命令将显示 AG1 和接口的 PIM 邻居以到达邻居。

```

AG1# show ip pim neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority / Mode

11.0.0.2 vlan11 00:00:43/00:01:33 v2 10 / S
12.0.0.2 vlan12 00:01:01/00:01:44 v2 10 / S
12.0.0.3 vlan12 00:01:01/00:01:43 v2 1000 / DR S
13.0.0.2 vlan13 00:01:02/00:01:42 v2 1000 / DR S

```

## AG1 中的 IGMP 和 PIM 状态

show ip igmp groups 命令输出将显示 IGMP 数据库。

```
AG1# show ip igmp groups
Total Number of Groups: 1
IGMP Connected Group Membership
Group Address Interface Mode
Uptime Expires Last Reporter
225.1.1.1 vlan11 Exclude
00:01:55 00:01:53 0.0.0.0
```

show ip pim tib 命令输出将显示 PIM 树信息库 (TIB)。

```
AG1# show ip pim tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.1.1), uptime 00:02:05, expires 00:00:54, RP 103.0.0.3, flags: SCJ
Incoming interface: vlan12, RPF neighbor 12.0.0.3
Outgoing interface list:
 vlan11 Forward/Sparse 00:02:05/Never
```

show ip pim mcache 命令输出将显示多播路由条目。

```
AG1# show ip pim mcache
PIM Multicast Routing Cache Table

(*, 225.1.1.1)
Incoming interface : vlan12
Outgoing interface list :
 vlan11

AG1-VLT-NODE-1# show ip pim mcache vlt
PIM Multicast Routing Cache Table
Flags: S - Synced

(*, 225.1.1.1)
Incoming interface : vlan12
Outgoing interface list :
 vlan11
```

以下 show 命令输出显示流量流建立后的流量：

show ip pim tib 命令将显示 PIM 树信息库。

```
AG1# show ip pim tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.1.1), uptime 00:10:15, expires 00:00:44, RP 103.0.0.3, flags: SCJ
Incoming interface: vlan12, RPF neighbor 12.0.0.3
Outgoing interface list:
 vlan11 Forward/Sparse 00:10:15/Never

(16.0.0.10, 225.1.1.1), uptime 00:00:55, expires 00:02:34, flags: CT
Incoming interface: vlan12, RPF neighbor 12.0.0.3
Outgoing interface list:
 vlan11 Forward/Sparse 00:00:55/Never
```

show ip pim mcache 命令将显示多播路由条目。

```
AG1# show ip pim mcache
PIM Multicast Routing Cache Table

(*, 225.1.1.1)
 Incoming interface : vlan12
 Outgoing interface list :
 vlan11

(16.0.0.10, 225.1.1.1)
 Incoming interface : vlan12
 Outgoing interface list :
 vlan11
```

show ip pim mcache vlt 命令将显示多播路由条目。

```
AG1# show ip pim mcache vlt
PIM Multicast Routing Cache Table
Flags: S - Synced

(*, 225.1.1.1)
 Incoming interface : vlan12
 Outgoing interface list :
 vlan11

(16.0.0.10, 225.1.1.1)
 Incoming interface : vlan12
 Outgoing interface list :
 vlan11
```

## AG2 上的配置示例:

```
AG2# configure terminal
AG2(config)# ip multicast-routing
AG2 (config)# ip pim rp-address 103.0.0.3 group-address 224.0.0.0/4
AG2(config)# router ospf 100
AG2(config-router-ospf-100)# exit

AG2(config)# vlt-domain 255
AG2(conf-vlt-255)# backup destination 10.16.132.153
AG2(conf-vlt-255)# discovery-interface ethernet1/1/31:1,1/1/31:4
AG2(conf-vlt-255)# peer-routing
AG2(conf-vlt-255)# vlt-mac 00:00:00:11:11:11
AG2(conf-vlt-255)# exit

AG2(config)# interface ethernet 1/1/32:1
AG2(conf-if-eth1/1/32:1)# no shutdown
AG2(conf-if-eth1/1/32:1)# no switchport
AG2(conf-if-eth1/1/32:1)# ip address 16.0.0.1/24
AG2(conf-if-eth1/1/32:1)# flowcontrol receive off
AG2(conf-if-eth1/1/32:1)# ip pim sparse-mode
AG2(conf-if-eth1/1/32:1)# ip ospf 100 area 0.0.0.0
AG2(conf-if-eth1/1/32:1)# exit

AG2(config)# interface vlan 11
AG2(conf-if-vlan-11)# no shutdown
AG2(conf-if-vlan-11)# ip address 11.0.0.2/24
AG2(conf-if-vlan-11)# ip pim sparse-mode
AG2(conf-if-vlan-11)# ip pim dr-priority 10
AG2(conf-if-vlan-11)# ip ospf 100 area 0.0.0.0
AG2(conf-if-vlan-11)# ip ospf cost 3000
AG2(conf-if-vlan-11)# exit

AG2(config)# interface vlan 12
AG2(conf-if-vlan-12)# no shutdown
AG2(conf-if-vlan-12)# ip address 12.0.0.2/24
AG2(conf-if-vlan-12)# ip pim sparse-mode
AG2(conf-if-vlan-12)# ip pim dr-priority 10
```



```

AG2(conf-if-vlan-12)# ip ospf 100 area 0.0.0.0
AG2(conf-if-vlan-12)# exit

AG2(config)# interface vlan 13
AG2(conf-if-vlan-13)# no shutdown
AG2(conf-if-vlan-13)# ip address 13.0.0.2/24
AG2(conf-if-vlan-13)# ip pim sparse-mode
AG2(conf-if-vlan-13)# ip pim dr-priority 1000
AG2(conf-if-vlan-13)# ip ospf 100 area 0.0.0.0
AG2(conf-if-vlan-13)# ip ospf cost 4000
AG2(conf-if-vlan-13)# exit

AG2(config)# interface loopback 102
AG2(conf-if-lo-102)# no shutdown
AG2(conf-if-lo-102)# ip address 102.0.0.2/32
AG2(conf-if-lo-102)# ip pim sparse-mode
AG2(conf-if-lo-102)# ip ospf 100 area 0.0.0.0
AG2(conf-if-lo-102)# exit

AG2(config)# interface port-channel11
AG2(conf-if-po-11)# no shutdown
AG2(conf-if-po-11)# switchport mode trunk
AG2(conf-if-po-11)# switchport access vlan 1
AG2(conf-if-po-11)# switchport trunk allowed vlan 11
AG2(conf-if-po-11)# vlt-port-channel 11
AG2(conf-if-po-11)# exit

AG2(config)# interface port-channel12
AG2(conf-if-po-12)# no shutdown
AG2(conf-if-po-12)# switchport mode trunk
AG2(conf-if-po-12)# switchport access vlan 1
AG2(conf-if-po-12)# switchport trunk allowed vlan 12
AG2(conf-if-po-12)# vlt-port-channel 12
AG2(conf-if-po-12)# exit

```

## AG2 和接口的 PIM 邻居以到达邻居

show ip pim neighbor 命令将显示 AG2 和接口的 PIM 邻居以到达邻居。

```

AG2# show ip pim neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority / Mode

11.0.0.1 vlan11 00:00:38/00:01:36 v2 1000 / DR S
12.0.0.1 vlan12 00:01:00/00:01:19 v2 10 / S
12.0.0.3 vlan12 00:01:06/00:01:18 v2 1000 / DR S
13.0.0.1 vlan13 00:01:00/00:01:19 v2 10 / S

```

## AG2 中的 IGMP 和 PIM 状态

show ip igmp groups 命令输出将显示 IGMP 数据库。

```

AG2# show ip igmp groups
Total Number of Groups: 1
IGMP Connected Group Membership
Group Address Interface Mode
Uptime Expires Last Reporter
225.1.1.1 vlan11 Exclude
00:02:00 00:01:47 0.0.0.0

```

show ip pim tib 命令的输出。

```

AG2# show ip pim tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.1.1), uptime 00:02:15, expires 00:00:00, RP 103.0.0.3, flags: SC
Incoming interface: vlan12, RPF neighbor 12.0.0.3

```

```
Outgoing interface list:
 vlan11 Forward/Sparse 00:02:15/Never
```

show ip pim mcache 命令输出将显示多播路由条目。

```
AG2# show ip pim mcache
PIM Multicast Routing Cache Table
```

```
(*, 225.1.1.1)
 Incoming interface : vlan12
 Outgoing interface list :
 vlan11
```

```
AG2# show ip pim mcache vlt
PIM Multicast Routing Cache Table
Flags: S - Synced
```

```
(*, 225.1.1.1), flags: S
 Incoming interface : vlan12
 Outgoing interface list :
 vlan11 (S)
```

以下 show 命令输出显示流量流建立后的同步状态：

```
AG2# show ip pim tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.1.1), uptime 00:10:30, expires 00:00:00, RP 103.0.0.3, flags: SC
 Incoming interface: vlan12, RPF neighbor 12.0.0.3
 Outgoing interface list:
 vlan11 Forward/Sparse 00:10:30/Never
```

```
AG2# show ip pim mcache
PIM Multicast Routing Cache Table

(*, 225.1.1.1)
 Incoming interface : vlan12
 Outgoing interface list :
 vlan11

(16.0.0.10, 225.1.1.1)
 Incoming interface : vlan12
 Outgoing interface list :
 vlan11
```

```
AG2# show ip pim mcache vlt
PIM Multicast Routing Cache Table
Flags: S - Synced

(*, 225.1.1.1), flags: S
 Incoming interface : vlan12
 Outgoing interface list :
 vlan11 (S)

(16.0.0.10, 225.1.1.1), flags: S
 Incoming interface : vlan12
 Outgoing interface list :
 vlan11 (S)
```

## TOR 上的配置示例：

```
TOR# configure terminal
TOR(config)# ip igmp snooping enable

TOR(config)# interface vlan 11
TOR(config-if-vlan-11)# no shutdown
TOR(config-if-vlan-11)# exit

TOR(config)# interface port-channel 11
TOR(config-if-po-11)# no shutdown
TOR(config-if-po-11)# switchport mode trunk
TOR(config-if-po-11)# switchport access vlan 1
TOR(config-if-po-11)# switchport trunk allowed vlan 11
TOR(config-if-po-11)# exit

TOR(config)# interface ethernet 1/1/32:1
TOR(config-if-eth1/1/32:1)# no shutdown
TOR(config-if-eth1/1/32:1)# switchport mode trunk
TOR(config-if-eth1/1/32:1)# switchport access vlan 1
TOR(config-if-eth1/1/32:1)# switchport trunk allowed vlan 11
TOR(config-if-eth1/1/32:1)# flowcontrol receive off
TOR(config-if-eth1/1/32:1)# exit
```

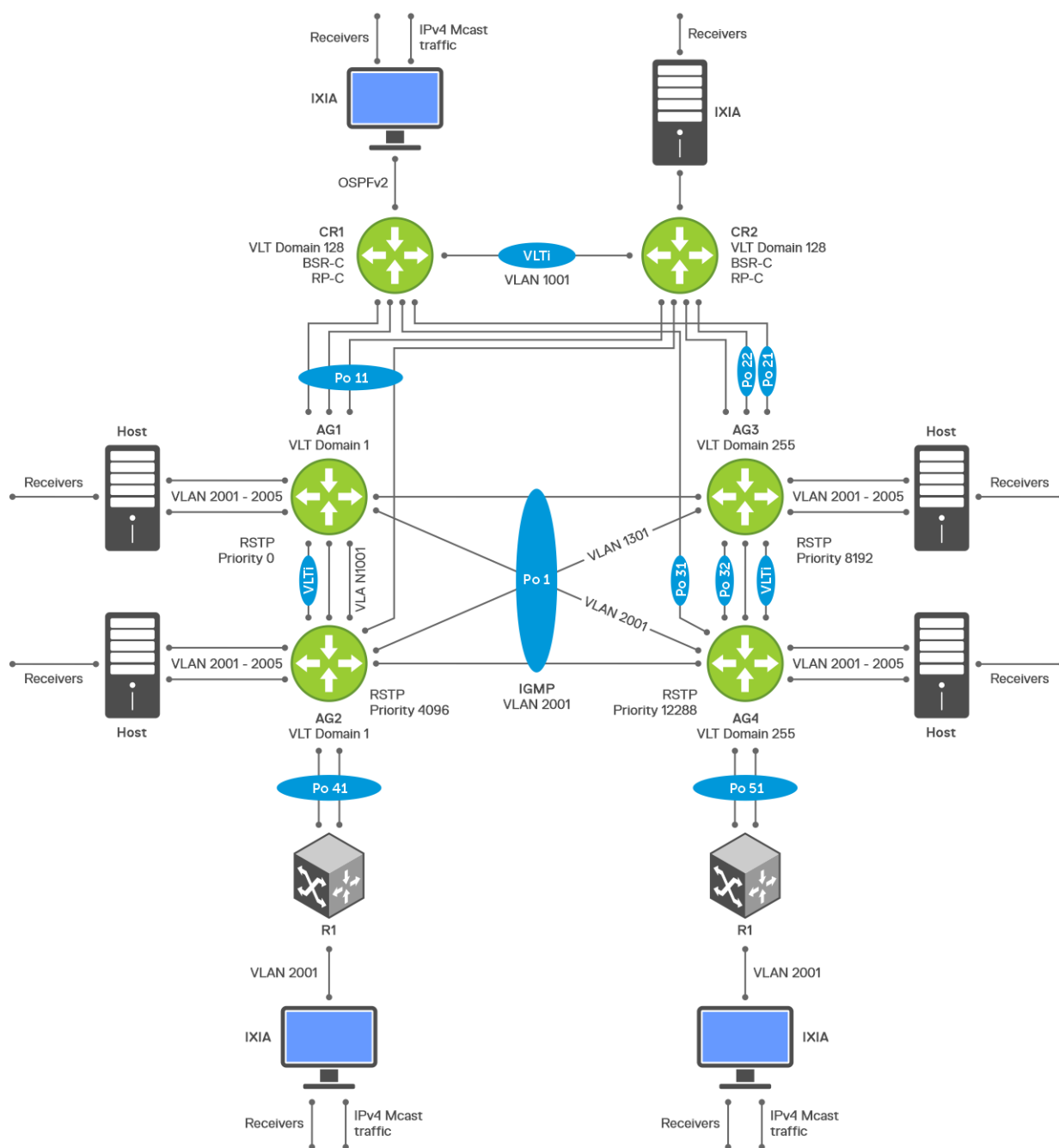
### TOR 上的 IGMP 侦听信息

以下命令将显示 IGMP 侦听组成员身份详细信息：

```
ToR# show ip igmp snooping groups
Total Number of Groups: 1
IGMP Connected Group Membership
Group Address Interface Mode Expires
225.1.1.1 vlan11 IGMPv2-Compat 00:02:09
Member-ports :ethernet1/1/32:1
```

## 示例：方形 VLT 拓扑中的主动-主动 PIM

在方形 VLT 环境中，以下拓扑使用主动/主动 PIM：



- CR1、CR2、AG1、AG2、AG3 和 AG4 是多播路由器。
- CR1 和 CR2 是 BSR 和 RP 节点。
- TR1 和 TR2 是已启用 IGMP 的 L2 节点。
- OSPFv2 是单播路由协议。

## CR1 交换机

### 1. 配置 RSTP。

```
CR1(config)# spanning-tree disable
```

### 2. 配置 VLT 域。

```
CR1(config)# interface ethernet 1/1/27:2
CR1(conf-if-eth1/1/27:2)# no switchport

CR1(config)# vlt-domain 128
```

```
CR1(conf-vlt-128)# backup destination 10.222.208.160
CR1(conf-vlt-128)# discovery-interface ethernet1/1/27:2
CR1(conf-vlt-128)# peer-routing
CR1(conf-vlt-128)# primary-priority 1
CR1(conf-vlt-128)# vlt-mac 9a:00:00:aa:aa:aa
```

3. 配置朝向 AG1 和 AG2 的端口通道接口。

```
CR1(config)# interface port-channel 11

CR1(config)# interface ethernet 1/1/1:1
CR1(conf-if-eth1/1/1:1)# channel-group 11 mode active

CR1(config)# interface ethernet 1/1/9:1
CR1(conf-if-eth1/1/9:1)# channel-group 11 mode active

CR1(config)# interface port-channel 11
CR1(conf-if-po-11)# vlt-port-channel 11
```

4. 配置朝向 AG3 的端口通道接口。

```
CR1(config)# interface port-channel 21

CR1(config)# interface ethernet 1/1/25:1
CR1(conf-if-eth1/1/25:1)# channel-group 21 mode active
```

5. 配置朝向 AG4 的端口通道接口。

```
CR1(config)# interface port-channel 31

CR1(config)# interface ethernet 1/1/17:1
CR1(conf-if-eth1/1/17:1)# channel-group 31 mode active
```

6. 配置环回接口并启用 PIM 稀疏模式。

```
CR1(config)# interface loopback 1
CR1(conf-if-lo-1)# ip address 10.1.100.5/32
CR1(conf-if-lo-1)# ip pim sparse-mode
```

7. 启用默认 VRF 上的多播路由。

```
CR1(config)# ip multicast-routing
```

8. 启用 BSR。

```
CR1(config)# ip pim bsr-candidate loopback1 hash-mask-len 31 priority 199
```

9. 启用 RP 候选。

```
CR1(config)# ip pim rp-candidate loopback1 priority 100 acl mcast_acl
```

10. 配置 RP 映射的访问列表。

```
CR1(config)# ip access-list mcast_acl
CR1(config-ip4-acl)# permit ip any 225.0.0.0/8
```

11. 为单播路由配置 OSPF。

```
CR1(config)# router ospf 1
CR1(config-router-ospf-1)# log-adjacency-changes
CR1(config-router-ospf-1)# redistribute connected
CR1(config-router-ospf-1)# router-id 10.1.100.5
```

12. 配置 VLAN 上的 IP 地址、OSPF 进程和 PIM-SM。

- VLAN 100 朝向 CR2

```
CR1(config)# interface vlan 100
CR1(conf-if-vl-100)# ip address 10.1.1.5/24
CR1(conf-if-vl-100)# ip ospf 1 area 0.0.0.0
CR1(conf-if-vl-100)# ip pim sparse-mode
CR1(conf-if-vl-100)# ip pim dr-priority 1
```

- VLAN 1001 朝向 AG1 和 AG2

```
CR1(config)# interface vlan 1001
CR1(conf-if-vl-1001)# ip address 10.1.2.5/24
CR1(conf-if-vl-1001)# ip ospf 1 area 0.0.0.0
CR1(conf-if-vl-1001)# ip pim sparse-mode
CR1(conf-if-vl-1001)# ip igmp snooping mrouter interface port-channel11
```

- VLAN 1101 朝向 AG3

```
CR1(config)# interface vlan 1101
CR1(conf-if-vl-1101)# ip address 10.1.3.5/24
CR1(conf-if-vl-1101)# ip ospf 1 area 0.0.0.0
CR1(conf-if-vl-1101)# ip pim sparse-mode
CR1(conf-if-vl-1101)# ip ospf cost 65535
CR1(conf-if-vl-1101)# ip igmp snooping mrouter interface port-channel21
```

- VLAN 1201 朝向 AG4

```
CR1(config)# interface vlan 1201
CR1(conf-if-vl-1201)# ip address 10.1.4.5/24
CR1(conf-if-vl-1201)# ip ospf 1 area 0.0.0.0
CR1(conf-if-vl-1201)# ip pim sparse-mode
CR1(conf-if-vl-1201)# ip ospf cost 65535
CR1(conf-if-vl-1201)# ip igmp snooping mrouter interface port-channel31
```

### 13. 将接口配置为 VLAN 中继端口，并指定允许的 VLAN。

```
CR1(config)# interface port-channel 11
CR1(conf-if-po-11)# switchport mode trunk
CR1(conf-if-po-11)# switchport trunk allowed vlan 1001
```

```
CR1(config)# interface port-channel 21
CR1(conf-if-po-21)# switchport mode trunk
CR1(conf-if-po-21)# switchport trunk allowed vlan 1101
```

```
CR1(config)# interface port-channel 31
CR1(conf-if-po-31)# switchport mode trunk
CR1(conf-if-po-31)# switchport trunk allowed vlan 1201
```

```
CR1(config)# interface ethernet 1/1/28:1
CR1(conf-if-eth1/1/28:1)# switchport mode trunk
CR1(conf-if-eth1/1/28:1)# switchport trunk allowed vlan 100
```

```
CR1(config)# interface ethernet 1/1/28:3
CR1(conf-if-eth1/1/28:3)# switchport mode trunk
CR1(conf-if-eth1/1/28:3)# switchport trunk allowed vlan 100
```

## CR2 交换机

### 1. 配置 RSTP。

```
CR2(config)# spanning-tree disable
```

### 2. 配置 VLT 域。

```
CR2(config)# interface ethernet 1/1/27:2
CR2(conf-if-eth1/1/27:2)# no switchport

CR2(config)# vlt-domain 128
CR2(conf-vlt-128)# backup destination 10.222.208.238
CR2(conf-vlt-128)# discovery-interface ethernet1/1/27:2
CR2(conf-vlt-128)# peer-routing
CR2(conf-vlt-128)# primary-priority 65535
CR2(conf-vlt-128)# vlt-mac 9a:00:00:aa:aa:aa
```

3. 配置朝向 AG1 和 AG2 的端口通道接口。

```
CR2(config)# interface port-channel 11

CR2(config)# interface ethernet 1/1/1:1
CR2(conf-if-eth1/1/1:1)# channel-group 11 mode active

CR2(config)# interface ethernet 1/1/9:1
CR2(conf-if-eth1/1/9:1)# channel-group 11 mode active

CR2(config)# interface port-channel 11
CR2(conf-if-po-11)# vlt-port-channel 11
```

4. 配置朝向 AG3 的端口通道接口。

```
CR2(config)# interface port-channel 22

CR2(config)# interface ethernet 1/1/25:1
CR2(conf-if-eth1/1/25:1)# channel-group 22 mode active
```

5. 配置朝向 AG4 的端口通道接口。

```
CR2(config)# interface port-channel 32

CR2(config)# interface ethernet 1/1/17:1
CR2(conf-if-eth1/1/17:1)# channel-group 32 mode active
```

6. 配置环回接口并启用 PIM-SM。

```
CR2(config)# interface loopback 1
CR2(conf-if-lo-1)# ip address 10.1.100.6/32
CR2(conf-if-lo-1)# ip pim sparse-mode
```

7. 启用默认 VRF 上的多播路由。

```
CR2(config)# ip multicast-routing
```

8. 启用 BSR。此路由器将成为选择的 BSR。

```
CR2(config)# ip pim bsr-candidate loopback1 hash-mask-len 31 priority 99
```

9. 启用 RP 候选。

```
CR2(config)# ip pim rp-candidate loopback1 priority 100 acl mcast_acl
```

10. 配置 RP 映射的访问列表。

```
CR2(config)# ip access-list mcast_acl
CR2(config-ipv4-acl)# permit ip any 225.0.0.0/8
```

11. 为单播路由配置 OSPF。

```
CR2(config)# router ospf 1
CR2(config-router-ospf-1)# log-adjacency-changes
CR2(config-router-ospf-1)# redistribute connected
CR2(config-router-ospf-1)# router-id 10.1.100.6
```

12. 配置 VLAN 上的 IP 地址、OSPF 进程和 PIM 稀疏模式。

- VLAN 100 朝向 CR1

```
CR2(config)# interface vlan 100
CR2(conf-if-vl-100)# ip address 10.1.1.6/24
CR2(conf-if-vl-100)# ip ospf 1 area 0.0.0.0
CR2(conf-if-vl-100)# ip pim sparse-mode
CR2(conf-if-vl-100)# ip pim dr-priority 4294967295
```

- VLAN 1001 朝向 AG1 和 AG2

```
CR2(config)# interface vlan 1001
CR2(conf-if-vl-1001)# ip address 10.1.2.6/24
CR2(conf-if-vl-1001)# ip ospf 1 area 0.0.0.0
```

```
CR2(conf-if-vl-1001)# ip pim sparse-mode
CR2(conf-if-vl-1001)# ip igmp snooping mrouter interface port-channel11
```

- VLAN 1151 朝向 AG3

```
CR2(config)# interface vlan 1151
CR2(conf-if-vl-1151)# ip address 10.110.1.5/24
CR2(conf-if-vl-1151)# ip ospf 1 area 0.0.0.0
CR2(conf-if-vl-1151)# ip pim sparse-mode
CR2(conf-if-vl-1151)# ip ospf cost 65535
CR2(conf-if-vl-1151)# ip igmp snooping mrouter interface port-channel22
```

- VLAN 1251 朝向 AG4

```
CR2(config)# interface vlan 1251
CR2(conf-if-vl-1251)# ip address 10.192.168.5/24
CR2(conf-if-vl-1251)# ip ospf 1 area 0.0.0.0
CR2(conf-if-vl-1251)# ip pim sparse-mode
CR2(conf-if-vl-1251)# ip ospf cost 65535
CR2(conf-if-vl-1251)# ip igmp snooping mrouter interface port-channel32
```

### 13. 将接口配置为 VLAN 中继端口，并指定允许的 VLAN。

```
CR2(config)# interface port-channel 11
CR2(conf-if-po-11)# switchport mode trunk
CR2(conf-if-po-11)# switchport trunk allowed vlan 1001
```

```
CR2(config)# interface port-channel 22
CR2(conf-if-po-22)# switchport mode trunk
CR2(conf-if-po-22)# switchport trunk allowed vlan 1151
```

```
CR2(config)# interface port-channel 32
CR2(conf-if-po-32)# switchport mode trunk
CR2(conf-if-po-32)# switchport trunk allowed vlan 1251
```

```
CR2(config)# interface ethernet 1/1/28:2
CR2(conf-if-eth1/1/28:2)# switchport mode trunk
CR2(conf-if-eth1/1/28:2)# switchport trunk allowed vlan 100
```

```
CR2(config)# interface ethernet 1/1/28:4
CR2(conf-if-eth1/1/28:4)# switchport mode trunk
CR2(conf-if-eth1/1/28:4)# switchport trunk allowed vlan 100
```

## AG1 交换机

### 1. 配置 RSTP。

```
AG1(config)# spanning-tree mode rstp
AG1(config)# spanning-tree rstp priority 0
```

### 2. 配置 VLT 域。

```
AG1(config)# interface ethernet 1/1/25:1
AG1(conf-if-eth1/1/25:1)# no switchport

AG1(config)# vlt-domain 1
AG1(conf-vlt-1)# backup destination 10.222.208.211
AG1(conf-vlt-1)# discovery-interface ethernet1/1/25:1
AG1(conf-vlt-1)# peer-routing
AG1(conf-vlt-1)# primary-priority 1
AG1(conf-vlt-1)# vlt-mac de:11:de:11:de:11
```

### 3. 配置朝向 CR1 和 CR2 的端口通道接口。

```
AG1(config)# interface port-channel 11
AG1(config)# interface ethernet 1/1/1:1
```



```
AG1(config-if-eth1/1/1:1)# channel-group 11 mode active

AG1(config)# interface ethernet 1/1/3:1
AG1(config-if-eth1/1/3:1)# channel-group 11 mode active

AG1(config)# interface port-channel 11
AG1(config-if-po-11)# vlt-port-channel 11
AG1(config-if-po-11)# spanning-tree disable
```

#### 4. 配置朝向 AG3 和 AG4 的端口通道接口。

```
AG1(config)# interface port-channel 1
AG1(config-if-po-1)# vlt-port-channel 1

AG1(config)# interface ethernet 1/1/24:1
AG1(config-if-eth1/1/24:1)# channel-group 1 mode active

AG1(config)# interface ethernet 1/1/26:1
AG1(config-if-eth1/1/26:1)# channel-group 1 mode active
```

#### 5. 配置朝向 TR1 的端口通道接口。

```
AG1(config)# interface port-channel 41
AG1(config-if-po-41)# vlt-port-channel 41

AG1(config)# interface ethernet 1/1/17:1
AG1(config-if-eth1/1/17:1)# channel-group 41 mode active
```

#### 6. 配置环回接口并启用 PIM-SM。

```
AG1(config)# interface loopback 1
AG1(config-if-lo-1)# ip address 10.1.100.1/32
AG1(config-if-lo-1)# ip pim sparse-mode
```

#### 7. 启用默认 VRF 上的多播路由。

```
AG1(config)# ip multicast-routing
```

#### 8. 为单播路由配置 OSPF。

```
AG1(config)# router ospf 1
AG1(config-router-ospf-1)# log-adjacency-changes
AG1(config-router-ospf-1)# redistribute connected
AG1(config-router-ospf-1)# router-id 10.1.100.1
```

#### 9. 配置 VLAN 上的 IP 地址、OSPF 进程和 PIM-SM。

- VLAN 1001 朝向 CR1 和 CR2

```
AG1(config)# interface vlan 1001
AG1(config-if-vl-1001)# ip address 10.1.2.1/24
AG1(config-if-vl-1001)# ip ospf 1 area 0.0.0.0
AG1(config-if-vl-1001)# ip pim sparse-mode
AG1(config-if-vl-1001)# ip igmp snooping mrouter interface port-channel11
```

- VLAN 1301 朝向 AG3 和 AG4

```
AG1(config)# interface vlan 1301
AG1(config-if-vl-1301)# ip address 10.112.1.1/24
AG1(config-if-vl-1301)# ip ospf 1 area 0.0.0.0
AG1(config-if-vl-1301)# ip pim sparse-mode
AG1(config-if-vl-1301)# ip igmp snooping mrouter interface port-channel11
```

- VLAN 2001 朝向 TR1

```
AG1(config)# interface vlan 2001
AG1(config-if-vl-2001)# ip address 192.168.1.1/24
AG1(config-if-vl-2001)# ip pim sparse-mode
AG1(config-if-vl-2001)# ip pim dr-priority 4294967295
AG1(config-if-vl-2001)# ip igmp snooping mrouter interface port-channel11
```

## 10. 将接口配置为 VLAN 中继端口，并指定允许的 VLAN。

```
AG1(config)# interface port-channel 11
AG1(conf-if-po-11)# switchport mode trunk
AG1(conf-if-po-11)# switchport trunk allowed vlan 1001
```

```
AG1(config)# interface port-channel 1
AG1(conf-if-po-1)# switchport mode trunk
AG1(conf-if-po-1)# switchport trunk allowed vlan 1301,2001
```

```
AG1(config)# interface port-channel 41
AG1(conf-if-po-41)# switchport mode trunk
AG1(conf-if-po-41)# switchport trunk allowed vlan 2001
```

```
AG1(config)# interface ethernet 1/1/6:2
AG1(conf-if-eth1/1/6:2)# switchport mode trunk
AG1(conf-if-eth1/1/6:2)# switchport trunk allowed vlan 2001
AG1(conf-if-eth1/1/6:2)# spanning-tree port type edge
```

## AG2 交换机

### 1. 配置 RSTP。

```
AG2(config)# spanning-tree mode rstp
AG2(config)# spanning-tree rstp priority 4096
```

### 2. 配置 VLT 域。

```
AG2(config)# interface ethernet 1/1/25:1
AG2(conf-if-eth1/1/25:1)# no switchport

AG2(config)# vlt-domain 1
AG2(conf-vlt-1)# backup destination 10.16.208.218
AG2(conf-vlt-1)# discovery-interface ethernet1/1/25:1
AG2(conf-vlt-1)# peer-routing
AG2(conf-vlt-1)# primary-priority 65535
AG2(conf-vlt-1)# vlt-mac de:11:de:11:de:11
```

### 3. 配置朝向 CR1 和 CR2 的端口通道接口。

```
AG2(config)# interface port-channel 11

AG2(config)# interface ethernet 1/1/1:1
AG2(conf-if-eth1/1/1:1)# channel-group 11 mode active

AG2(config)# interface ethernet 1/1/3:1
AG2(conf-if-eth1/1/3:1)# channel-group 11 mode active

AG2(config)# interface port-channel 11
AG2(conf-if-po-11)# vlt-port-channel 11
AG2(conf-if-po-11)# spanning-tree disable
```

### 4. 配置朝向 AG3 和 AG4 的端口通道接口。

```
AG2(config)# interface port-channel 1
AG2(conf-if-po-1)# vlt-port-channel 1

AG2(config)# interface ethernet 1/1/24:1
AG2(conf-if-eth1/1/24:1)# channel-group 1 mode active

AG2(config)# interface ethernet 1/1/26:1
AG2(conf-if-eth1/1/26:1)# channel-group 1 mode active
```

### 5. 配置朝向 TR1 的端口通道接口。

```
AG2(config)# interface port-channel 41
AG2(conf-if-po-41)# vlt-port-channel 41
```

```
AG2(config)# interface ethernet 1/1/17:1
AG2(conf-if-eth1/1/17:1)# channel-group 41 mode active
```

#### 6. 配置环回接口并启用 PIM-SM。

```
AG2(config)# interface loopback 1
AG2(conf-if-lo-1)# ip address 10.1.100.2/32
AG2(conf-if-lo-1)# ip pim sparse-mode
```

#### 7. 启用默认 VRF 上的多播路由。

```
AG2(config)# ip multicast-routing
```

#### 8. 为单播路由配置 OSPF。

```
AG2(config)# router ospf 1
AG2(config-router-ospf-1)# log-adjacency-changes
AG2(config-router-ospf-1)# redistribute connected
AG2(config-router-ospf-1)# router-id 10.1.100.2
```

#### 9. 配置 VLAN 上的 IP 地址、OSPF 进程和 PIM-SM。

- VLAN 1001 朝向 CR1 和 CR2

```
AG2(config)# interface vlan 1001
AG2(conf-if-vl-1001)# ip address 10.1.2.2/24
AG2(conf-if-vl-1001)# ip ospf 1 area 0.0.0.0
AG2(conf-if-vl-1001)# ip pim sparse-mode
AG2(conf-if-vl-1001)# ip igmp snooping mrouter interface port-channel11
```

- VLAN 1301 朝向 AG3 和 AG4

```
AG2(config)# interface vlan 1301
AG2(conf-if-vl-1301)# ip address 10.112.1.2/24
AG2(conf-if-vl-1301)# ip ospf 1 area 0.0.0.0
AG2(conf-if-vl-1301)# ip pim sparse-mode
AG2(conf-if-vl-1301)# ip igmp snooping mrouter interface port-channel11
```

- VLAN 2001 朝向 TR1

```
AG2(config)# interface vlan 2001
AG2(conf-if-vl-2001)# ip address 192.168.1.2/24
AG2(conf-if-vl-2001)# ip pim sparse-mode
AG2(conf-if-vl-2001)# ip pim dr-priority 4294967290
AG2(conf-if-vl-2001)# ip igmp snooping mrouter interface port-channel11
```

#### 10. 将接口配置为 VLAN 中继端口，并指定允许的 VLAN。

```
AG2(config)# interface port-channel 11
AG2(conf-if-po-11)# switchport mode trunk
AG2(conf-if-po-11)# switchport trunk allowed vlan 1001
```

```
AG2(config)# interface port-channel 1
AG2(conf-if-po-1)# switchport mode trunk
AG2(conf-if-po-1)# switchport trunk allowed vlan 1301,2001
```

```
AG2(config)# interface port-channel 41
AG2(conf-if-po-41)# switchport mode trunk
AG2(conf-if-po-41)# switchport trunk allowed vlan 2001
```

```
AG2(config)# interface ethernet 1/1/6:2
AG2(conf-if-eth1/1/6:2)# switchport mode trunk
AG2(conf-if-eth1/1/6:2)# switchport trunk allowed vlan 2001
AG2(conf-if-eth1/1/6:2)# spanning-tree port type edge
```

## AG3 交换机

### 1. 配置 RSTP。

```
AG3(config)# spanning-tree mode rstp
AG3(config)# spanning-tree rstp priority 8192
```

### 2. 配置 VLT 域。

```
AG3(config)# interface ethernet 1/1/25:1
AG3(conf-if-eth1/1/25:1)# no switchport

AG3(config)# vlt-domain 1
AG3(conf-vlt-255)# backup destination 10.222.208.39
AG3(conf-vlt-255)# discovery-interface ethernet1/1/25:1
AG3(conf-vlt-255)# peer-routing
AG3(conf-vlt-255)# primary-priority 1
AG3(conf-vlt-255)# vlt-mac f0:ce:10:f0:ce:10
```

### 3. 配置朝向 CR1 的端口通道接口。

```
AG3(config)# interface port-channel 21

AG3(config)# interface ethernet 1/1/1:1
AG3(conf-if-eth1/1/1:1)# channel-group 21 mode active
```

### 4. 配置朝向 CR2 的端口通道接口。

```
AG3(config)# interface port-channel 22

AG3(config)# interface ethernet 1/1/4:1
AG3(conf-if-eth1/1/4:1)# channel-group 22 mode active
```

### 5. 配置朝向 AG3 和 AG4 的端口通道接口。

```
AG3(config)# interface port-channel 1
AG3(conf-if-po-1)# vlt-port-channel 1

AG3(config)# interface ethernet 1/1/24:1
AG3(conf-if-eth1/1/24:1)# channel-group 1 mode active

AG3(config)# interface ethernet 1/1/26:1
AG3(conf-if-eth1/1/26:1)# channel-group 1 mode active
```

### 6. 配置朝向 TR2 的端口通道接口。

```
AG3(config)# interface port-channel 51
AG3(conf-if-po-51)# vlt-port-channel 51

AG3(config)# interface ethernet 1/1/17:1
AG3(conf-if-eth1/1/17:1)# channel-group 51 mode active
```

### 7. 启用默认 VRF 上的多播路由。

```
AG3(config)# ip multicast-routing
```

### 8. 为单播路由配置 OSPF。

```
AG3(config)# router ospf 1
AG3(config-router-ospf-1)# log-adjacency-changes
AG3(config-router-ospf-1)# redistribute connected
AG3(config-router-ospf-1)# router-id 10.1.100.3
```

### 9. 配置 VLAN 上的 IP 地址、OSPF 进程和 PIM-SM。

- VLAN 1101 朝向 CR1

```
AG3(config)# interface vlan 1101
AG3(conf-if-vl-1101)# ip address 10.1.3.3/24
AG3(conf-if-vl-1101)# ip ospf 1 area 0.0.0.0
```

```
AG3(conf-if-vl-1101)# ip pim sparse-mode
AG3(conf-if-vl-1101)# ip igmp snooping mrouter interface port-channel21
```

- VLAN 1151 朝向 CR2

```
AG3(config)# interface vlan 1151
AG3(conf-if-vl-1151)# ip address 10.110.1.3/24
AG3(conf-if-vl-1151)# ip ospf 1 area 0.0.0.0
AG3(conf-if-vl-1151)# ip pim sparse-mode
AG3(conf-if-vl-1151)# ip igmp snooping mrouter interface port-channel22
```

- VLAN 1301 朝向 AG1 和 AG2

```
AG3(config)# interface vlan 1301
AG3(conf-if-vl-1301)# ip address 10.112.1.3/24
AG3(conf-if-vl-1301)# ip ospf 1 area 0.0.0.0
AG3(conf-if-vl-1301)# ip pim sparse-mode
AG3(conf-if-vl-1301)# ip igmp snooping mrouter interface port-channel1
```

- VLAN 2001 朝向 TR2

```
AG3(config)# interface vlan 2001
AG3(conf-if-vl-2001)# ip address 192.168.1.3/24
AG3(conf-if-vl-2001)# ip pim sparse-mode
AG3(conf-if-vl-2001)# ip pim dr-priority 100000
AG3(conf-if-vl-2001)# ip igmp snooping mrouter interface port-channel1
```

## 10. 将接口配置为 VLAN 中继端口，并指定允许的 VLAN。

```
AG3(config)# interface port-channel 21
AG3(conf-if-po-21)# switchport mode trunk
AG3(conf-if-po-21)# switchport trunk allowed vlan 1101
AG3(conf-if-po-21)# spanning-tree disable
```

```
AG3(config)# interface port-channel 22
AG3(conf-if-po-22)# switchport mode trunk
AG3(conf-if-po-22)# switchport trunk allowed vlan 1201
AG3(conf-if-po-22)# spanning-tree disable
```

```
AG3(config)# interface port-channel 1
AG3(conf-if-po-1)# switchport mode trunk
AG3(conf-if-po-1)# switchport trunk allowed vlan 1301,2001
```

```
AG3(config)# interface port-channel 51
AG3(conf-if-po-51)# switchport mode trunk
AG3(conf-if-po-51)# switchport trunk allowed vlan 2001
```

```
AG3(config)# interface ethernet 1/1/32:2
AG3(conf-if-eth1/1/32:2)# switchport mode trunk
AG3(conf-if-eth1/1/32:2)# switchport trunk allowed vlan 2001
AG3(conf-if-eth1/1/32:2)# spanning-tree port type edge
```

## AG4 交换机

### 1. 配置 RSTP。

```
AG4(config)# spanning-tree mode rstp
AG4(config)# spanning-tree rstp priority 12288
```

### 2. 配置 VLT 域。

```
AG4(config)# interface ethernet 1/1/25:1
AG4(conf-if-eth1/1/25:1)# no switchport

AG4(config)# vlt-domain 1
AG4(conf-vlt-255)# backup destination 10.222.208.219
AG4(conf-vlt-255)# discovery-interface ethernet1/1/25:1
```

```
AG4(config-vlt-255)# peer-routing
AG4(config-vlt-255)# primary-priority 65535
AG4(config-vlt-255)# vlt-mac f0:ce:10:f0:ce:10
```

3. 配置朝向 CR1 的端口通道接口。

```
AG4(config)# interface port-channel 31
AG4(config)# interface ethernet 1/1/1:1
AG4(config-if-eth1/1/1:1)# channel-group 31 mode active
```

4. 配置朝向 CR2 的端口通道接口。

```
AG4(config)# interface port-channel 32
AG4(config)# interface ethernet 1/1/4:1
AG4(config-if-eth1/1/4:1)# channel-group 32 mode active
```

5. 配置朝向 AG3 和 AG4 的端口通道接口。

```
AG4(config)# interface port-channel 1
AG4(config-if-po-1)# vlt-port-channel 1

AG4(config)# interface ethernet 1/1/24:1
AG4(config-if-eth1/1/24:1)# channel-group 1 mode active

AG4(config)# interface ethernet 1/1/26:1
AG4(config-if-eth1/1/26:1)# channel-group 1 mode active
```

6. 配置朝向 TR2 的端口通道接口。

```
AG4(config)# interface port-channel 51
AG4(config-if-po-51)# vlt-port-channel 51

AG4(config)# interface ethernet 1/1/17:1
AG4(config-if-eth1/1/17:1)# channel-group 51 mode active
```

7. 启用默认 VRF 上的多播路由。

```
AG4(config)# ip multicast-routing
```

8. 为单播路由配置 OSPF。

```
AG4(config)# router ospf 1
AG4(config-router-ospf-1)# log-adjacency-changes
AG4(config-router-ospf-1)# redistribute connected
AG4(config-router-ospf-1)# router-id 10.1.100.4
```

9. 配置 VLAN 上的 IP 地址、OSPF 进程和 PIM-SM。

- VLAN 1201 朝向 CR1

```
AG4(config)# interface vlan 1201
AG4(config-if-vl-1201)# ip address 10.1.4.4/24
AG4(config-if-vl-1201)# ip ospf 1 area 0.0.0.0
AG4(config-if-vl-1201)# ip pim sparse-mode
AG4(config-if-vl-1201)# ip igmp snooping mrouter interface port-channel31
```

- VLAN 1251 朝向 CR2

```
AG4(config)# interface vlan 1251
AG4(config-if-vl-1251)# ip address 10.192.168.4/24
AG4(config-if-vl-1251)# ip ospf 1 area 0.0.0.0
AG4(config-if-vl-1251)# ip pim sparse-mode
AG4(config-if-vl-1251)# ip igmp snooping mrouter interface port-channel32
```

- VLAN 1301 朝向 AG1 和 AG2

```
AG4(config)# interface vlan 1301
AG4(config-if-vl-1301)# ip address 10.112.1.4/24
AG4(config-if-vl-1301)# ip ospf 1 area 0.0.0.0
```

```
AG4(conf-if-vl-1301)# ip pim sparse-mode
AG4(conf-if-vl-1301)# ip igmp snooping mrouter interface port-channel1
```

- VLAN 2001 朝向 TR2

```
AG4(config)# interface vlan 2001
AG4(conf-if-vl-2001)# ip address 192.168.1.4/24
AG4(conf-if-vl-2001)# ip pim sparse-mode
AG4(conf-if-vl-2001)# ip igmp snooping mrouter interface port-channel1
```

## 10. 将接口配置为 VLAN 中继端口，并指定允许的 VLAN。

```
AG4(config)# interface port-channel 31
AG4(conf-if-po-31)# switchport mode trunk
AG4(conf-if-po-31)# switchport trunk allowed vlan 1201
AG4(conf-if-po-31)# spanning-tree disable
```

```
AG4(config)# interface port-channel 32
AG4(conf-if-po-32)# switchport mode trunk
AG4(conf-if-po-32)# switchport trunk allowed vlan 1251
AG4(conf-if-po-32)# spanning-tree disable
```

```
AG4(config)# interface port-channel 1
AG4(conf-if-po-1)# switchport mode trunk
AG4(conf-if-po-1)# switchport trunk allowed vlan 1301,2001
```

```
AG4(config)# interface port-channel 51
AG4(conf-if-po-51)# switchport mode trunk
AG4(conf-if-po-51)# switchport trunk allowed vlan 2001
```

```
AG4(config)# interface ethernet 1/1/32:2
AG4(conf-if-eth1/1/32:2)# switchport mode trunk
AG4(conf-if-eth1/1/32:2)# switchport trunk allowed vlan 2001
AG4(conf-if-eth1/1/32:2)# spanning-tree port type edge
```

## TR1 交换机

### 1. 配置 RSTP。

```
TR1(config)# spanning-tree mode rstp
```

### 2. 配置朝向 AG1 的端口通道接口。

```
TR1(config)# interface port-channel 41
TR1(config)# interface ethernet 1/1/39
TR1(conf-if-eth1/1/39)# channel-group 41 mode active
```

### 3. 配置朝向 AG2 的端口通道接口。

```
TR1(config)# interface ethernet 1/1/27:1
TR1(conf-if-eth1/1/27:1)# channel-group 41 mode active
```

### 4. 朝向 AG1 和 AG2 配置 VLAN 2001。

```
TR1(config)# interface vlan 2001
```

### 5. 将接口配置为 VLAN 中继端口，并指定允许的 VLAN。

```
TR1(config)# interface port-channel 41
TR1(conf-if-po-41)# switchport mode trunk
TR1(conf-if-po-41)# switchport trunk allowed vlan 2001
```

```
TR1(config)# interface ethernet 1/1/31
TR1(conf-if-eth1/1/31)# switchport mode trunk
```

```
TR1(conf-if-eth1/1/31)# switchport trunk allowed vlan 2001
TR1(conf-if-eth1/1/31)# spanning-tree port type edge
```

```
TR1(config)# interface ethernet 1/1/32
TR1(conf-if-eth1/1/32)# switchport mode trunk
TR1(conf-if-eth1/1/32)# switchport trunk allowed vlan 2001
TR1(conf-if-eth1/1/32)# spanning-tree port type edge
```

## TR2 交换机

### 1. 配置 RSTP。

```
TR2(config)# spanning-tree mode rstp
```

### 2. 配置朝向 AG3 的端口通道接口。

```
TR2(config)# interface port-channel 51
TR2(config)# interface ethernet 1/1/1
TR2(conf-if-eth1/1/1)# channel-group 51 mode active
```

### 3. 配置朝向 AG4 的端口通道接口。

```
TR2(config)# interface ethernet 1/1/25:1
TR2(conf-if-eth1/1/25:1)# channel-group 51 mode active
```

### 4. 朝向 AG1 和 AG2 配置 VLAN 2001。

```
TR2(config)# interface vlan 2001
```

### 5. 将接口配置为 VLAN 中继端口，并指定允许的 VLAN。

```
TR2(config)# interface port-channel 51
TR2(conf-if-po-51)# switchport mode trunk
TR2(conf-if-po-51)# switchport trunk allowed vlan 2001
```

```
TR2(config)# interface ethernet 1/1/21
TR2(conf-if-eth1/1/31)# switchport mode trunk
TR2(conf-if-eth1/1/31)# switchport trunk allowed vlan 2001
TR2(conf-if-eth1/1/31)# spanning-tree port type edge
```

```
TR2(config)# interface ethernet 1/1/22
TR2(conf-if-eth1/1/32)# switchport mode trunk
TR2(conf-if-eth1/1/32)# switchport trunk allowed vlan 2001
TR2(conf-if-eth1/1/32)# spanning-tree port type edge
```

## 验证配置

您可以使用以下 `show` 命令验证配置。

### CR1

`show ip pim interface` 命令将显示节点上已启用 PIM 的接口。

```
CR1# show ip pim interface
Address Interface Ver/Mode Nbr Count Query Intvl DR Prio DR

10.1.1.5 vlan100 v2/S 1 30 1 10.1.1.6
10.1.3.5 vlan1101 v2/S 1 30 1 10.1.3.5
10.1.4.5 vlan1201 v2/S 1 30 1 10.1.4.5
10.1.2.5 vlan1001 v2/S 3 30 1 10.1.2.6
```



show ip pim neighbor 命令将显示节点的 PIM 邻居和接口，以访问邻居。

```
CR1# show ip pim neighbor
```

| Neighbor Address | Interface | Uptime/Expires    | Ver | DR Priority | Mode   |
|------------------|-----------|-------------------|-----|-------------|--------|
| 10.1.1.6         | vlan100   | 00:24:19/00:01:25 | v2  | 4294967295  | / DR   |
| S                |           |                   |     |             |        |
| 10.1.3.3         | vlan1101  | 00:20:28/00:01:18 | v2  | 1           | /      |
| S                |           |                   |     |             |        |
| 10.1.4.4         | vlan1201  | 00:18:21/00:01:24 | v2  | 1           | /      |
| S                |           |                   |     |             |        |
| 10.1.2.1         | vlan1001  | 00:22:12/00:01:36 | v2  | 1           | /      |
| S                |           |                   |     |             |        |
| 10.1.2.2         | vlan1001  | 00:17:38/00:01:36 | v2  | 1           | /      |
| S                |           |                   |     |             |        |
| 10.1.2.6         | vlan1001  | 00:24:17/00:01:36 | v2  | 1           | / DR S |

show ip pim summary 命令将显示 PIM 摘要。

```
CR1# show ip pim summary
```

|                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Entries in PIM-TIB/MFC: 96/52                                                                                                                                                                                                           |
| Active Modes:<br>PIM-SM                                                                                                                                                                                                                 |
| Interface summary:<br>4 active PIM interfaces<br>0 passive PIM interfaces<br>6 active PIM neighbor                                                                                                                                      |
| TIB Summary:<br>20/12 (*,G) entries in PIM-TIB/MFC<br>40/40 (S,G) entries in PIM-TIB/MFC<br>36/0 (S,G,Rpt) entries in PIM-TIB/MFC<br><br>2 RP<br>3 sources<br>0 Register states                                                         |
| Message Summary:<br>189/770 Joins/Prunes sent/received<br>0/56 Candidate-RP advertisements sent/received<br>420/112 BSR messages sent/received<br><br>267 Null Register messages received<br>357/0 Register-stop messages sent/received |
| Data path event summary:<br>0 last-hop switchover messages received<br>28/28 pim-assert messages sent/received<br>0/119 register messages sent/received                                                                                 |
| VLT Multicast summary:<br>0(*,G) synced entries in MFC<br>20(S,G) synced entries in MFC<br>0(S,G,Rpt) synced entries in MFC                                                                                                             |

show ip pim tib 命令将显示 PIM 树信息库 (TIB)。

```
CR1# show ip pim tib
```

|                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PIM Multicast Routing Table                                                                                                                                   |
| Flags: S - Sparse, C - Connected, L - Local, P - Pruned,<br>R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,<br>K - Ack-Pending state        |
| Timers: Uptime/Expires                                                                                                                                        |
| Interface state: Interface, next-Hop, State/Mode                                                                                                              |
| (*, 225.1.0.0), uptime 01:42:49, expires 00:00:00, RP 10.1.100.6, flags: SC<br>Incoming interface: vlan100, RPF neighbor 10.1.1.6<br>Outgoing interface list: |

```
(172.16.1.201, 225.1.0.0), uptime 01:24:45, expires 00:02:46, flags: CTP
Incoming interface: vlan100, RPF neighbor 0.0.0.0
Outgoing interface list:
```

show ip pim mcache 命令将显示多播路由条目。

```
CR1# show ip pim mcache
PIM Multicast Routing Cache Table

(192.168.1.201, 225.1.0.0)
Incoming interface : vlan1001
Outgoing interface list :
vlan1

(192.168.1.202, 225.1.0.0)
Incoming interface : vlan1001
Outgoing interface list :
vlan1

(172.16.1.201, 225.1.0.0)
Incoming interface : vlan1
Outgoing interface list :
vlan1001
```

show ip pim mcache vlt 命令将显示 VLT 对等节点之间同步的多播路由条目。

```
CR1# show ip pim mcache vlt | no-more
PIM Multicast Routing Cache Table
Flags: S - Synced

(192.168.1.201, 225.1.0.0), flags: S
Incoming interface : vlan1001
Outgoing interface list :
vlan100 (S)

(192.168.1.202, 225.1.0.0), flags: S
Incoming interface : vlan1001
Outgoing interface list :
vlan100 (S)

(172.16.1.201, 225.1.0.0)
Incoming interface : vlan1
Outgoing interface list :
vlan1001 (S)
```

show ip pim bsr-router 命令将显示有关 BSR 的信息。

```
CR1# show ip pim bsr-router

This system is the Bootstrap Router (v2)
BSR address: 10.1.100.5
BSR Priority: 199, Hash mask length: 31
Next bootstrap message in 00:00:12
This system is a candidate BSR
Candidate BSR address: 10.1.100.5, priority: 199, hash mask length: 31
Next Cand_RP_advertisement in 00:00:24
RP: 10.1.100.5(loopback1)
```

show ip pim rp 命令将显示有关所有多播组到 RP 映射的信息。

```
CR1# show ip pim rp
Group RP
```

```

225.1.0.0 10.1.100.6
```

```
CR1# show ip pim rp mapping
Group(s) : 225.0.0.0/8
RP : 10.1.100.5, v2
Info source: 10.1.100.5, via bootstrap, priority 100
expires: 00:00:56
Group(s) : 225.0.0.0/8
RP : 10.1.100.6, v2
Info source: 10.1.100.5, via bootstrap, priority 100
expires: 00:01:07
```

show ip igmp snooping groups 命令将显示 IGMP 数据库。

```
CR1# show ip igmp snooping groups
Total Number of Groups: 320
```

```
CR1# show ip igmp snooping groups vlan 1 225.1.0.0 detail
Interface vlan1
Group 225.1.0.0
Source List
--
Member Port Mode Uptime
Expires
port-channel1000 IGMPv2-Compat 01:56:53
00:02:07
ethernet1/1/28:1 IGMPv2-Compat 01:56:53 00:02:03
```

## CR2

show ip pim interface 命令将显示节点上已启用 PIM 的接口。

```
CR2# show ip pim interface
Address Interface Ver/Mode Nbr Count Query Intvl DR Prio DR

10.1.1.6 vlan100 v2/S 1 30 4294967295
10.1.1.6
10.110.1.5 vlan1151 v2/S 1 30 1
10.110.1.5
10.192.168.5 vlan1251 v2/S 1 30 1
10.192.168.5
10.1.2.6 vlan1001 v2/S 3 30 1 10.1.2.6
```

show ip pim neighbor 命令将显示节点的 PIM 邻居和接口，以访问邻居。

```
CR2# show ip pim neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority / Mode

10.1.1.5 vlan100 00:26:16/00:01:28 v2 1 / S
10.110.1.3 vlan1151 00:22:17/00:01:29 v2 1 / S
10.192.168.4 vlan1251 00:20:13/00:01:31 v2 1 / S
10.1.2.1 vlan1001 00:24:09/00:01:39 v2 1 / S
10.1.2.2 vlan1001 00:19:35/00:01:39 v2 1 / S
10.1.2.5 vlan1001 00:26:14/00:01:42 v2 1 / S
```

show ip pim summary 命令将显示 PIM 摘要。

```
CR2# show ip pim summary

Entries in PIM-TIB/MFC: 98/59

Active Modes:
PIM-SM

Interface summary:
4 active PIM interfaces
0 passive PIM interfaces
6 active PIM neighbor
```

```

TIB Summary:
 20/20 (*,G) entries in PIM-TIB/MFC
 39/39 (S,G) entries in PIM-TIB/MFC
 39/0 (S,G,Rpt) entries in PIM-TIB/MFC

 2 RP
 3 sources
 16 Register states

Message Summary:
 208/885 Joins/Prunes sent/received
 60/0 Candidate-RP advertisements sent/received
 310/405 BSR messages sent/received

 205 Null Register messages received
 268/181 Register-stop messages sent/received

Data path event summary:
 11 last-hop switchover messages received
 28/28 pim-assert messages sent/received
 186/79 register messages sent/received

VLT Multicast summary:
 0(*,G) synced entries in MFC
 21(S,G) synced entries in MFC
 0(S,G,Rpt) synced entries in MFC

```

show ip pim tib 命令将显示 PIM 树信息库 (TIB)。

```

CR2# show ip pim tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.0.0), uptime 01:43:37, expires 00:00:00, RP 10.1.100.6, flags: SC
Incoming interface: Null, RPF neighbor 0.0.0.0
Outgoing interface list:
 vlan100 Forward/Sparse 01:43:37/Never
 vlan1001 Forward/Sparse 01:39:18/00:03:08
 vlan1251 Forward/Sparse 01:25:23/00:03:06

(192.168.1.201, 225.1.0.0), uptime 01:25:24, expires 00:02:42, flags: CT
Incoming interface: vlan1001, RPF neighbor 10.1.2.2
Outgoing interface list:
 vlan100 Forward/Sparse 01:25:24/Never

(192.168.1.202, 225.1.0.0), uptime 01:25:24, expires 00:02:56, flags: CT
Incoming interface: vlan1001, RPF neighbor 10.1.2.2
Outgoing interface list:
 vlan100 Forward/Sparse 01:25:24/Never

(172.16.1.201, 225.1.0.0), uptime 01:25:24, expires 00:02:57, flags: CFT
Incoming interface: vlan100, RPF neighbor 0.0.0.0
Outgoing interface list:
 vlan1001 Forward/Sparse 01:25:24/00:03:13
 vlan1251 Forward/Sparse 01:25:23/00:03:06

```

show ip pim mcache 命令将显示多播路由条目。

```

CR2# show ip pim mcache
PIM Multicast Routing Cache Table

(192.168.1.201, 225.1.0.0)
Incoming interface : vlan1001

```

```

Outgoing interface list :
 vlan1
(192.168.1.202, 225.1.0.0)
 Incoming interface : vlan1001
 Outgoing interface list :
 vlan1
(172.16.1.201, 225.1.0.0)
 Incoming interface : vlan1
 Outgoing interface list :
 vlan1001
 vlan1251

```

show ip pim mcache vlt 命令将显示 VLT 对等节点之间同步的多播路由条目。

```

CR2# show ip pim mcache vlt
PIM Multicast Routing Cache Table
Flags: S - Synced

(192.168.1.201, 225.1.0.0)
 Incoming interface : vlan1001
 Outgoing interface list :
 vlan1
(192.168.1.202, 225.1.0.0)
 Incoming interface : vlan1001
 Outgoing interface list :
 vlan1
(172.16.1.201, 225.1.0.0)
 Incoming interface : vlan1
 Outgoing interface list :
 vlan1001

```

show ip pim bsr-router 命令将显示有关 BSR 的信息。

```

CR2# show ip pim bsr-router

PIMv2 Bootstrap information
 BSR address: 10.1.100.5
 BSR Priority: 199, Hash mask length: 31
 Expires: 00:00:17
 This system is a candidate BSR
 Candidate BSR address: 10.1.100.6, priority: 99, hash mask length: 31
 Next Cand RP advertisement in 00:00:24
 RP: 10.1.100.6(loopback1)

```

show ip pim rp mapping 命令将显示有关所有多播组到 RP 映射的信息。

```

CR2# show ip pim rp
Group RP

225.1.0.0 10.1.100.6

```

```

CR2# show ip pim rp mapping
Group(s) : 225.0.0.0/8
RP : 10.1.100.5, v2
 Info source: 10.1.100.5, via bootstrap, priority 100
 expires: 00:00:58
Group(s) : 225.0.0.0/8
RP : 10.1.100.6, v2
 Info source: 10.1.100.5, via bootstrap, priority 100
 expires: 00:00:39

```

show ip igmp snooping groups 命令将显示 IGMP 数据库。

```
CR2# show ip igmp snooping groups
Total Number of Groups: 320

CR2# show ip igmp snooping groups vlan 1 225.1.0.0 detail
Interface vlan1
Group 225.1.0.0
Source List
--
 Member Port Mode Uptime
Expires
 port-channel1000 IGMPv2-Compat 01:57:20
00:01:39
 ethernet1/1/28:4 IGMPv2-Compat 01:57:31 00:01:39
```

AG1

show ip pim interface 命令将显示节点上已启用 PIM 的接口。

```
AG1# show ip pim interface
Address Interface Ver/Mode Nbr Count Query Intvl DR Prio DR

10.1.2.1 vlan1001 v2/S 3 30 1 10.1.2.6
10.112.1.1 vlan1301 v2/S 3 30 1 10.112.1.4
192.168.1.4 vlan2001 v2/S 3 30 4294967295 192.168.1.4
```

show ip pim neighbor 命令将显示节点的 PIM 邻居和接口，以访问邻居。

```
AG1# show ip pim neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority / Mode

10.1.2.2 vlan1001 00:19:45/00:01:29 v2 1 / S
10.1.2.5 vlan1001 00:24:18/00:01:32 v2 1 / S
10.1.2.6 vlan1001 00:24:19/00:01:29 v2 1 / DR S
10.112.1.2 vlan1301 00:19:52/00:01:22 v2 1 / S
10.112.1.3 vlan1301 00:22:14/00:01:24 v2 1 / S
10.112.1.4 vlan1301 00:20:38/00:01:22 v2 1 / DR S
192.168.1.3 vlan2001 00:19:51/00:01:23 v2 4294967290 / S
192.168.1.2 vlan2001 00:22:11/00:01:23 v2 100000 / S
192.168.1.1 vlan2001 00:20:36/00:01:25 v2 1 / S
```

show ip pim summary 命令将显示 PIM 摘要。

```
AG1# show ip pim summary

Entries in PIM-TIB/MFC: 140/80

Active Modes:
 PIM-SM

Interface summary:
 7 active PIM interfaces
 0 passive PIM interfaces
 21 active PIM neighbor

TIB Summary:
 20/20 (*,G) entries in PIM-TIB/MFC
 60/60 (S,G) entries in PIM-TIB/MFC
 60/0 (S,G,Rpt) entries in PIM-TIB/MFC

 2 RP
 3 sources
 40 Register states

Message Summary:
 418/386 Joins/Prunes sent/received
 0/0 Candidate-RP advertisements sent/received
 597/1827 BSR messages sent/received
```

```
0 Null Register messages received
0/459 Register-stop messages sent/received
```

Data path event summary:

```
20 last-hop switchover messages received
23/159 pim-assert messages sent/received
499/0 register messages sent/received
```

VLT Multicast summary:

```
0(*,G) synced entries in MFC
0(S,G) synced entries in MFC
0(S,G,Rpt) synced entries in MFC
```

show ip pim tib 命令将显示 PIM 树信息库 (TIB)。

```
AG1# show ip pim tib
```

PIM Multicast Routing Table

Flags: S - Sparse, C - Connected, L - Local, P - Pruned,  
R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,  
K - Ack-Pending state

Timers: Uptime/Expires

Interface state: Interface, next-Hop, State/Mode

```
(* , 225.1.0.0), uptime 01:39:47, expires 00:00:09, RP 10.1.100.6, flags: SCJ
```

Incoming interface: vlan1001, RPF neighbor 10.1.2.6

Outgoing interface list:

```
vlan2001 Forward/Sparse 01:39:47/Never
vlan2002 Forward/Sparse 01:39:41/Never
vlan2003 Forward/Sparse 01:39:44/Never
vlan2004 Forward/Sparse 01:39:44/Never
vlan2005 Forward/Sparse 01:39:43/Never
```

```
(192.168.1.201, 225.1.0.0), uptime 01:25:53, expires 00:01:14, flags: CFT
```

Incoming interface: vlan2001, RPF neighbor 0.0.0.0

Outgoing interface list:

```
vlan2002 Forward/Sparse 01:25:53/Never
vlan2003 Forward/Sparse 01:25:53/Never
vlan2004 Forward/Sparse 01:25:53/Never
vlan2005 Forward/Sparse 01:25:53/Never
```

```
(192.168.1.202, 225.1.0.0), uptime 01:25:53, expires 00:01:14, flags: CFT
```

Incoming interface: vlan2001, RPF neighbor 0.0.0.0

Outgoing interface list:

```
vlan2002 Forward/Sparse 01:25:53/Never
vlan2003 Forward/Sparse 01:25:53/Never
vlan2004 Forward/Sparse 01:25:53/Never
vlan2005 Forward/Sparse 01:25:53/Never
```

```
(172.16.1.201, 225.1.0.0), uptime 01:22:46, expires 00:01:15, flags: CT
```

Incoming interface: vlan1001, RPF neighbor 10.1.2.6

Outgoing interface list:

```
vlan2002 Forward/Sparse 01:22:46/Never
vlan2003 Forward/Sparse 01:22:46/Never
vlan2004 Forward/Sparse 01:22:46/Never
vlan2005 Forward/Sparse 01:22:46/Never
```

show ip pim mcache 命令将显示多播路由条目。

```
AG1# show ip pim mcache
```

PIM Multicast Routing Cache Table

```
(* , 225.1.0.0)
```

Incoming interface : vlan1001

Outgoing interface list :

```
vlan2002
vlan2003
vlan2004
vlan2005
```

```
(192.168.1.201, 225.1.0.0)
Incoming interface : vlan2001
Outgoing interface list :
vlan1001
vlan2002
vlan2003
vlan2004
vlan2005

(192.168.1.202, 225.1.0.0)
Incoming interface : vlan2001
Outgoing interface list :
vlan1001
vlan2002
vlan2003
vlan2004
vlan2005

(172.16.1.201, 225.1.0.0)
Incoming interface : vlan1001
Outgoing interface list :
vlan2002
vlan2003
vlan2004
vlan2005
```

show ip pim mcache vlt 命令将显示 VLT 对等节点之间同步的多播路由条目。

```
AG1# show ip pim mcache vlt | no-more
PIM Multicast Routing Cache Table
Flags: S - Synced

(*, 225.1.0.0)
Incoming interface : vlan1001
Outgoing interface list :
vlan2002
vlan2003
vlan2004
vlan2005

(192.168.1.201, 225.1.0.0)
Incoming interface : vlan2001
Outgoing interface list :
vlan1001 (S)
vlan2002
vlan2003
vlan2004
vlan2005

(192.168.1.202, 225.1.0.0)
Incoming interface : vlan2001
Outgoing interface list :
vlan1001 (S)
vlan2002
vlan2003
vlan2004
vlan2005

(172.16.1.201, 225.1.0.0)
Incoming interface : vlan1001
Outgoing interface list :
vlan2002
vlan2003
vlan2004
vlan2005
```

show ip pim bsr-router 命令将显示有关 BSR 的信息。

```
AG1# show ip pim bsr-router

PIMv2 Bootstrap information
```



```
BSR address: 10.1.100.5
BSR Priority: 199, Hash mask length: 31
Expires: 00:00:23
```

show ip pim rp mapping 命令将显示有关所有多播组到 RP 映射的信息。

```
AG1# show ip pim rp
Group RP

225.1.0.0 10.1.100.6
```

```
AG1# show ip pim rp mapping
Group(s) : 225.0.0.0/8
RP : 10.1.100.5, v2
 Info source: 10.1.100.5, via bootstrap, priority 100
 expires: 00:00:45
Group(s) : 225.0.0.0/8
RP : 10.1.100.6, v2
 Info source: 10.1.100.5, via bootstrap, priority 100
 expires: 00:00:56
```

show ip igmp snooping groups 命令将显示 IGMP 数据库。

```
AG1# show ip igmp snooping groups
Total Number of Groups: 1600
```

```
AG1# show ip igmp snooping groups vlan 2001 225.1.0.0 detail
Interface vlan2001
Group 225.1.0.0
Source List
--
 Member Port Mode Uptime
Expires
 port-channel1 Exclude 01:53:40
00:01:35
 port-channel1000 IGMPv2-Compat 01:53:16
00:01:41
 port-channel41 Exclude 01:53:37
00:01:37
 ethernet1/1/6:2 IGMPv2-Compat 01:53:34 00:01:41
```

## AG2

show ip pim interface 命令将显示节点上已启用 PIM 的接口。

```
AG2# show ip pim interface
Address Interface Ver/Mode Nbr Count Query Intvl DR Prio DR

192.168.1.3 vlan2001 v2/S 3 30 4294967290 192.168.1.4
10.112.1.2 vlan1301 v2/S 3 30 1 10.112.1.4
10.1.2.2 vlan1001 v2/S 3 30 1 10.1.2.6
```

show ip pim neighbor 命令将显示节点的 PIM 邻居和接口，以访问邻居。

```
AG2# show ip pim neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority / Mode

192.168.1.4 vlan2001 00:21:42/00:01:38 v2 4294967295 / DR S
192.168.1.2 vlan2001 00:21:50/00:01:38 v2 100000 / S
192.168.1.1 vlan2001 00:20:39/00:01:39 v2 1 / S
10.112.1.1 vlan1301 00:22:29/00:01:40 v2 1 / S
10.112.1.3 vlan1301 00:22:29/00:01:38 v2 1 / S
10.112.1.4 vlan1301 00:20:39/00:01:36 v2 1 / DR S
10.1.2.1 vlan1001 00:22:44/00:01:44 v2 1 / S
10.1.2.5 vlan1001 00:22:33/00:01:17 v2 1 / S
10.1.2.6 vlan1001 00:22:34/00:01:44 v2 1 / DR S
```

show ip pim summary 命令将显示 PIM 摘要。

```
AG2# show ip pim summary

Entries in PIM-TIB/MFC: 60/40

Active Modes:
 PIM-SM

Interface summary:
 7 active PIM interfaces
 0 passive PIM interfaces
 21 active PIM neighbor

TIB Summary:
 20/0 (*,G) entries in PIM-TIB/MFC
 40/40 (S,G) entries in PIM-TIB/MFC
 0/0 (S,G,Rpt) entries in PIM-TIB/MFC

 2 RP
 2 sources
 0 Register states

Message Summary:
 63/775 Joins/Prunes sent/received
 0/0 Candidate-RP advertisements sent/received
 587/1895 BSR messages sent/received

 0 Null Register messages received
 0/0 Register-stop messages sent/received

Data path event summary:
 0 last-hop switchover messages received
 22/162 pim-assert messages sent/received
 0/0 register messages sent/received

VLT Multicast summary:
 20(*,G) synced entries in MFC
 20(S,G) synced entries in MFC
 0(S,G,Rpt) synced entries in MFC
```

show ip pim tib 命令将显示 PIM 树信息库 (TIB)。

```
AG2# show ip pim tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.0.0), uptime 01:40:01, expires 00:00:00, RP 10.1.100.6, flags: SC
 Incoming interface: vlan1001, RPF neighbor 10.1.2.6
 Outgoing interface list:
 vlan2001 Forward/Sparse 01:39:57/Never
 vlan2002 Forward/Sparse 01:40:01/Never
 vlan2003 Forward/Sparse 01:39:55/Never
 vlan2004 Forward/Sparse 01:39:51/Never
 vlan2005 Forward/Sparse 01:39:52/Never

(192.168.1.201, 225.1.0.0), uptime 01:26:21, expires 00:01:10, flags: CT
 Incoming interface: vlan2001, RPF neighbor 0.0.0.0
 Outgoing interface list:
 vlan1001 Forward/Sparse 01:26:21/00:03:09

(192.168.1.202, 225.1.0.0), uptime 01:26:21, expires 00:01:10, flags: CT
 Incoming interface: vlan2001, RPF neighbor 0.0.0.0
 Outgoing interface list:
 vlan1001 Forward/Sparse 01:26:21/00:03:09
```

show ip pim mcache 命令将显示多播路由条目。

```
AG2# show ip pim mcache
PIM Multicast Routing Cache Table

(*, 225.1.0.0)
 Incoming interface : vlan1001
 Outgoing interface list :
 vlan2002
 vlan2003
 vlan2004
 vlan2005

(192.168.1.201, 225.1.0.0)
 Incoming interface : vlan2001
 Outgoing interface list :
 vlan1001
 vlan2002
 vlan2003
 vlan2004
 vlan2005

(192.168.1.202, 225.1.0.0)
 Incoming interface : vlan2001
 Outgoing interface list :
 vlan1001
 vlan2002
 vlan2003
 vlan2004
 vlan2005

(172.16.1.201, 225.1.0.0)
 Incoming interface : vlan1001
 Outgoing interface list :
 vlan2002
 vlan2003
 vlan2004
 vlan2005
```

show ip pim mcache vlt 命令将显示 VLT 对等节点之间同步的多播路由条目。

```
AG2# show ip pim mcache vlt | no-more
PIM Multicast Routing Cache Table
Flags: S - Synced

(*, 225.1.0.0), flags: S
 Incoming interface : vlan1001
 Outgoing interface list :
 vlan2002 (S)
 vlan2003 (S)
 vlan2004 (S)
 vlan2005 (S)

(192.168.1.201, 225.1.0.0)
 Incoming interface : vlan2001
 Outgoing interface list :
 vlan1001
 vlan2002 (S)
 vlan2003 (S)
 vlan2004 (S)
 vlan2005 (S)

(192.168.1.202, 225.1.0.0)
 Incoming interface : vlan2001
 Outgoing interface list :
 vlan1001
 vlan2002 (S)
 vlan2003 (S)
 vlan2004 (S)
 vlan2005 (S)

(172.16.1.201, 225.1.0.0), flags: S
```

```
Incoming interface : vlan1001
Outgoing interface list :
 vlan2002 (S)
 vlan2003 (S)
 vlan2004 (S)
 vlan2005 (S)
```

show ip pim bsr-router 命令将显示有关 BSR 的信息。

```
AG2# show ip pim bsr-router

PIMv2 Bootstrap information
 BSR address: 10.1.100.5
 BSR Priority: 199, Hash mask length: 31
 Expires: 00:00:26
```

show ip pim rp mapping 命令将显示有关所有多播组到 RP 映射的信息。

```
AG2# show ip pim rp
Group RP

225.1.0.0 10.1.100.6
```

```
AG2# show ip pim rp mapping
Group(s) : 225.0.0.0/8
RP : 10.1.100.5, v2
 Info source: 10.1.100.5, via bootstrap, priority 100
 expires: 00:01:03
Group(s) : 225.0.0.0/8
RP : 10.1.100.6, v2
 Info source: 10.1.100.5, via bootstrap, priority 100
 expires: 00:00:44
```

show ip igmp snooping groups 命令将显示 IGMP 数据库。

```
AG2# show ip igmp snooping groups
Total Number of Groups: 1600
```

```
AG2# show ip igmp snooping groups vlan 2001 225.1.0.0 detail
Interface vlan2001
Group 225.1.0.0
Source List
--
 Member Port Mode Uptime
Expires
 port-channel1 Exclude 01:51:31
00:01:30
 port-channel1000 IGMPv2-Compat 01:53:27
00:01:36
 port-channel41 Exclude 01:50:30
00:01:32
 ethernet1/1/6:2 IGMPv2-Compat 01:51:28 00:01:30
```

### AG3

show ip pim interface 命令将显示节点上已启用 PIM 的接口。

```
AG3# show ip pim interface
Address Interface Ver/Mode Nbr Count Query Intvl DR Prio DR

10.112.1.3 vlan1301 v2/S 3 30 1 10.112.1.4
192.168.1.2 vlan2001 v2/S 3 30 100000 192.168.1.4
10.110.1.3 vlan1151 v2/S 1 30 1 10.110.1.5
10.1.3.3 vlan1101 v2/S 1 30 1 10.1.3.5
```

show ip pim neighbor 命令将显示节点的 PIM 邻居和接口，以访问邻居。

```
AG3# show ip pim neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority / Mode
```

```

10.112.1.1 vlan1301 00:22:45/00:01:24 v2 1 / S
10.112.1.2 vlan1301 00:20:24/00:01:20 v2 1 / S
10.112.1.4 vlan1301 00:21:09/00:01:20 v2 1 / DR S
192.168.1.4 vlan2001 00:22:47/00:01:22 v2 4294967295 / DR S
192.168.1.3 vlan2001 00:20:22/00:01:22 v2 4294967290 / S
192.168.1.1 vlan2001 00:21:07/00:01:23 v2 1 / S
10.110.1.5 vlan1151 00:22:58/00:01:16 v2 1 / DR S
10.1.3.5 vlan1101 00:23:05/00:01:38 v2 1 / DR S

```

show ip pim summary 命令将显示 PIM 摘要。

```

AG3# show ip pim summary

Entries in PIM-TIB/MFC: 60/40

Active Modes:
 PIM-SM

Interface summary:
 8 active PIM interfaces
 0 passive PIM interfaces
 20 active PIM neighbor

TIB Summary:
 20/0 (*,G) entries in PIM-TIB/MFC
 40/40 (S,G) entries in PIM-TIB/MFC
 0/0 (S,G,Rpt) entries in PIM-TIB/MFC

 2 RP
 2 sources
 0 Register states

Message Summary:
 40/20 Joins/Prunes sent/received
 0/0 Candidate-RP advertisements sent/received
 680/1899 BSR messages sent/received

 0 Null Register messages received
 0/0 Register-stop messages sent/received

Data path event summary:
 0 last-hop switchover messages received
 22/164 pim-assert messages sent/received
 0/0 register messages sent/received

VLT Multicast summary:
 0(*,G) synced entries in MFC
 0(S,G) synced entries in MFC
 0(S,G,Rpt) synced entries in MFC

```

show ip pim tib 命令将显示 PIM 树信息库 (TIB)。

```

AG3# show ip pim tib

PIM Multicast Routing Table
Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.0.0), uptime 01:39:57, expires 00:00:00, RP 10.1.100.6, flags: SC
Incoming interface: vlan1151, RPF neighbor 10.110.1.5
Outgoing interface list:
 vlan2001 Forward/Sparse 01:39:57/Never
 vlan2002 Forward/Sparse 01:39:57/Never
 vlan2003 Forward/Sparse 01:39:57/Never
 vlan2004 Forward/Sparse 01:39:57/Never
 vlan2005 Forward/Sparse 01:39:57/Never

```

```
(192.168.1.201, 225.1.0.0), uptime 01:26:40, expires 00:00:52, flags: CTP
Incoming interface: vlan2001, RPF neighbor 0.0.0.0
Outgoing interface list:
```

```
(192.168.1.202, 225.1.0.0), uptime 01:26:40, expires 00:00:52, flags: CTP
Incoming interface: vlan2001, RPF neighbor 0.0.0.0
Outgoing interface list:
```

show ip pim mcache 命令将显示多播路由条目。

```
AG3# show ip pim mcache
PIM Multicast Routing Cache Table

(192.168.1.201, 225.1.0.0)
Incoming interface : vlan2001
Outgoing interface list :

(192.168.1.202, 225.1.0.0)
Incoming interface : vlan2001
Outgoing interface list :
```

show ip pim bsr-router 命令将显示有关 BSR 的信息。

```
AG3# show ip pim bsr-router

PIMv2 Bootstrap information
BSR address: 10.1.100.5
BSR Priority: 199, Hash mask length: 31
Expires: 00:00:30
```

show ip pim rp mapping 命令将显示有关所有多播组到 RP 映射的信息。

```
AG3# show ip pim rp
Group RP

225.1.0.0 10.1.100.6
```

```
AG3# show ip pim rp mapping
Group(s) : 225.0.0.0/8
RP : 10.1.100.5, v2
Info source: 10.1.100.5, via bootstrap, priority 100
expires: 00:00:43
Group(s) : 225.0.0.0/8
RP : 10.1.100.6, v2
Info source: 10.1.100.5, via bootstrap, priority 100
expires: 00:00:54
```

show ip igmp snooping groups 命令将显示 IGMP 数据库。

```
AG3# show ip igmp snooping groups
Total Number of Groups: 1600
```

```
AG3# show ip igmp snooping groups vlan 2001 225.1.0.0 detail
Interface vlan2001
Group 225.1.0.0
Source List
--
Member Port Mode Uptime
Expires
port-channel1 Exclude 01:53:46
00:01:28
port-channel1000 IGMPv2-Compat 01:54:04
00:01:29
port-channel51 Exclude 01:54:40
00:01:23
ethernet1/1/32:2 IGMPv2-Compat 01:54:04 00:01:28
```

## AG4

show ip pim interface 命令将显示节点上已启用 PIM 的接口。

```
AG4# show ip pim interface
Address Interface Ver/Mode Nbr Count Query Intvl DR Prio DR

10.1.4.4 vlan1201 v2/S 1 30 1 10.1.4.5
10.112.1.4 vlan1301 v2/S 3 30 1 10.112.1.4
192.168.1.1 vlan2001 v2/S 3 30 1 192.168.1.4
10.192.168.4 vlan1251 v2/S 1 30 1 10.192.168.5
```

show ip pim neighbor 命令将显示节点的 PIM 邻居和接口，以访问邻居。

```
AG4# show ip pim neighbor
Neighbor Address Interface Uptime/Expires Ver DR Priority / Mode

10.1.4.5 vlan1201 00:22:44/00:01:35 v2 1 / DR S
10.112.1.1 vlan1301 00:22:52/00:01:43 v2 1 / S
10.112.1.2 vlan1301 00:20:35/00:01:40 v2 1 / S
10.112.1.3 vlan1301 00:23:26/00:01:42 v2 1 / S
192.168.1.4 vlan2001 00:22:52/00:01:41 v2 4294967295 / DR S
192.168.1.3 vlan2001 00:20:33/00:01:41 v2 4294967290 / S
192.168.1.2 vlan2001 00:23:50/00:01:41 v2 100000 / S
10.192.168.5 vlan1251 00:22:37/00:01:39 v2 1 / DR S
```

show ip pim summary 命令将显示 PIM 摘要。

```
AG4# show ip pim summary

Entries in PIM-TIB/MFC: 140/80

Active Modes:
 PIM-SM

Interface summary:
 8 active PIM interfaces
 0 passive PIM interfaces
 20 active PIM neighbor

TIB Summary:
 20/20 (*,G) entries in PIM-TIB/MFC
 60/60 (S,G) entries in PIM-TIB/MFC
 60/0 (S,G,Rpt) entries in PIM-TIB/MFC

 2 RP
 3 sources
 0 Register states

Message Summary:
 389/0 Joins/Prunes sent/received
 0/0 Candidate-RP advertisements sent/received
 687/1944 BSR messages sent/received

 0 Null Register messages received
 0/0 Register-stop messages sent/received

Data path event summary:
 22 last-hop switchover messages received
 120/67 pim-assert messages sent/received
 0/0 register messages sent/received

VLT Multicast summary:
 0(*,G) synced entries in MFC
 0(S,G) synced entries in MFC
 0(S,G,Rpt) synced entries in MFC
```

show ip pim tib 命令将显示 PIM 树信息库 (TIB)。

```
AG4# show ip pim tib

PIM Multicast Routing Table
```

```

Flags: S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register Flag, T - SPT-bit set, J - Join SPT,
 K - Ack-Pending state
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.0.0), uptime 01:40:17, expires 00:00:58, RP 10.1.100.6, flags: SCJ
Incoming interface: vlan1251, RPF neighbor 10.192.168.5
Outgoing interface list:
 vlan2001 Forward/Sparse 01:40:17/Never
 vlan2002 Forward/Sparse 01:40:09/Never
 vlan2003 Forward/Sparse 01:40:04/Never
 vlan2004 Forward/Sparse 01:40:04/Never
 vlan2005 Forward/Sparse 01:40:04/Never

(192.168.1.201, 225.1.0.0), uptime 01:27:01, expires 00:00:30, flags: CTP
Incoming interface: vlan2001, RPF neighbor 0.0.0.0
Outgoing interface list:

(192.168.1.202, 225.1.0.0), uptime 01:27:01, expires 00:00:30, flags: CTP
Incoming interface: vlan2001, RPF neighbor 0.0.0.0
Outgoing interface list:

(172.16.1.201, 225.1.0.0), uptime 01:27:01, expires 00:00:31, flags: CT
Incoming interface: vlan1251, RPF neighbor 10.192.168.5
Outgoing interface list:
 vlan2001 Forward/Sparse 01:27:01/Never

```

show ip pim mcache 命令将显示多播路由条目。

```

AG4# show ip pim mcache
PIM Multicast Routing Cache Table

(*, 225.1.0.0)
Incoming interface : vlan1251
Outgoing interface list :
 vlan2001

(192.168.1.201, 225.1.0.0)
Incoming interface : vlan2001
Outgoing interface list :

(192.168.1.202, 225.1.0.0)
Incoming interface : vlan2001
Outgoing interface list :

(172.16.1.201, 225.1.0.0)
Incoming interface : vlan1251
Outgoing interface list :
 vlan2001

```

show ip pim bsr-router 命令将显示有关 BSR 的信息。

```

AG4# show ip pim bsr-router

PIMv2 Bootstrap information
BSR address: 10.1.100.5
BSR Priority: 199, Hash mask length: 31
Expires: 00:00:20

```

show ip pim rp mapping 命令将显示有关所有多播组到 RP 映射的信息。

```

AG4# show ip pim rp
Group RP

```



```

225.1.0.0 10.1.100.6
```

```
AG4# show ip pim rp mapping
Group(s) : 225.0.0.0/8
RP : 10.1.100.5, v2
 Info source: 10.1.100.5, via bootstrap, priority 100
 expires: 00:01:02
Group(s) : 225.0.0.0/8
RP : 10.1.100.6, v2
 Info source: 10.1.100.5, via bootstrap, priority 100
 expires: 00:00:43
```

show ip igmp snooping groups 命令将显示 IGMP 数据库。

```
AG4# show ip igmp snooping groups
Total Number of Groups: 1600
```

```
AG4# show ip igmp snooping groups vlan 2001 225.1.0.0 detail
Interface vlan2001
Group 225.1.0.0
Source List
--
Member Port Mode Uptime
Expires
port-channel1 Exclude 01:52:34
00:01:26
port-channel1000 IGMPv2-Compat 01:54:04
00:01:27
port-channel51 Exclude 01:52:49
00:01:21
ethernet1/1/32:2 IGMPv2-Compat 01:53:42 00:01:27
```

## TR1

show ip igmp snooping groups 命令将显示 IGMP 数据库。

```
TR1# show ip igmp snooping groups
Total Number of Groups: 1600
```

```
TR1# show ip igmp snooping groups vlan 2001 225.1.0.0 detail
Interface vlan2001
Group 225.1.0.0
Source List
--
Member Port Mode Uptime
Expires
ethernet1/1/31 IGMPv2-Compat 01:56:02
00:01:17
ethernet1/1/32 IGMPv2-Compat 01:56:02 00:01:21
```

## TR2

show ip igmp snooping groups 命令将显示 IGMP 数据库。

```
TR2# show ip igmp snooping groups
Total Number of Groups: 1600
```

```
TR2# show ip igmp snooping groups vlan 2001
Total Number of Groups: 20
IGMP Connected Group Membership
Group Address Interface Mode
Expires
225.1.0.0 vlan2001 IGMPv2-Compat
00:01:36
Member-ports :ethernet1/1/21,ethernet1/1/22
225.1.0.1 vlan2001 IGMPv2-Compat
00:01:36
Member-ports :ethernet1/1/21,ethernet1/1/22
```

```
225.1.0.2 vlan2001 IGMPv2-Compat
00:01:36
 Member-ports :ethernet1/1/21,ethernet1/1/22

<<Output_truncated>>
```

## VLT 多播路由显示命令

### show vlt inconsistency ip mcache

显示有关本地和对等 VLT 节点之间不匹配的 IIF 路由的信息。

|        |                                  |
|--------|----------------------------------|
| 语法     | show vlt inconsistency ip mcache |
| 参数     | 无                                |
| 默认     | 无                                |
| 命令模式   | EXEC                             |
| 使用情况信息 | 无                                |
| 示例     |                                  |

```
OS10# show vlt inconsistency ip mcache

Spanned Multicast routing IIF inconsistency:
Multicast Route Local IIF Peer IIF
(22.22.22.200, 225.1.1.2) Vlan 5 Vlan6
(*, 225.1.1.2) Vlan 15 ethernet 1/1/1
```

支持的版本 10.5.0 or later

### show vlt mismatch

显示 VLT 对等节点之间的配置不匹配。

|        |                                     |
|--------|-------------------------------------|
| 语法     | show vlt {domain-id   all} mismatch |
| 参数     | domain-id— 输入 VLT 域 ID，从 1 到 255。   |
| 默认     | 无                                   |
| 命令模式   | EXEC                                |
| 使用情况信息 | show vlt mismatch 命令将显示多播配置不匹配。     |
| 示例     |                                     |

```
OS10# show vlt all mismatch

Multicast routing mismatches:
Global status:
Parameter VRF Local Peer

V4 Multicast default Enabled Disabled

Vlan status
VlanId Local IPv4 Peer Local IPv6 Peer

Vlan 11 Enabled Disabled Disabled Disabled
Vlan 12 Enabled Disabled Disabled Disabled
Vlan 13 Enabled Disabled Disabled Disabled
```

支持的版本 10.5.0 or later

# VXLAN

虚拟可扩展 LAN (VXLAN) 通过虚拟化数据中心内的底层第 3 层 (L3) 传输网络扩展第 2 层 (L2) 服务器连接。虚拟化数据中心包含多租户环境中的虚拟机 (VM)。OS10 支持 VXLAN，如 RFC 7348 中所述。

通过将 L2 框架封装在 L3 数据包中，VXLAN 可在现有 L3 网络上提供 L2 覆盖机制。VXLAN 共享转发域允许租户 L2 数据段中的主机（如虚拟和物理机）通过共享 IP 网络进行通信。每个租户的 L2 数据段由称为 VXLAN 网络标识符 (VNI) 的 24 位 ID 进行标识。

OS10 交换机部署为 VXLAN 网关，用于在对服务器流量进行隧道操作时在 L3 数据包中对 L2 框架进行封装/取消封装。在此角色中，OS10 交换机作为 VXLAN 隧道端点 (VTEP) 运行。使用 VXLAN 隧道，服务器 VLAN 数据段通过扩展的 L2 转发域进行通信。

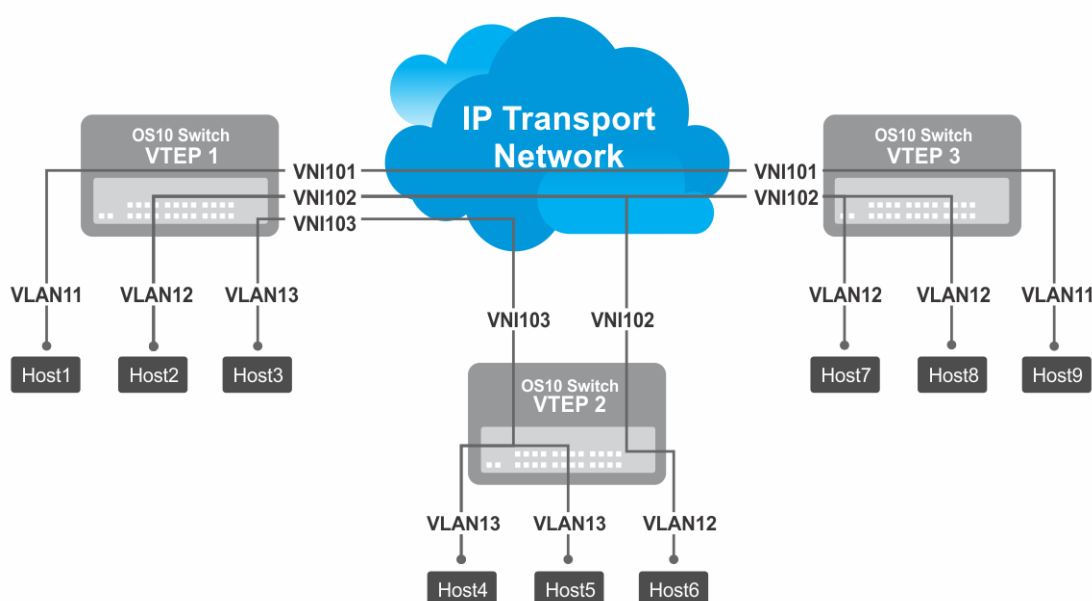


图 9: VXLAN 拓扑

**注:** 此功能在 Z9332F-ON 平台上不受支持。

## VXLAN 概念

### 网络虚拟化叠加 (NVO)

覆盖网络通过基础 L3 IP 网络在租户段中的服务器虚拟机 (VM) 之间扩展了 L2 连接。租户段可以是在基础网络间分布的一组主机或服务器。

- NVO 覆盖网络使用独立的 L2 桥域（虚拟网络）—— 独立于传统 VLAN 转发。
- NVO 基础网络在默认 VRF 中使用现有 L3 基础架构和路由协议运行。

### 虚拟可扩展 LAN (VXLAN)

一种网络虚拟化叠加类型，用于将租户有效负载封装到 IP UDP 数据包中，以用于跨 IP 基础网络进行传输。

### VXLAN 网络标识符 (VNI)

用于标识租户段并在 VXLAN 封装的数据包中传输的 24 位 ID 编号。

### VXLAN 隧道端点 (VTEP)

已连接的终端主机分配给虚拟网络的交换机。虚拟网络映射到 VXLAN 段。本地和远程 VTEP 针对终端主机之间的流量执行封装和取消封装的 VXLAN 标头。VTEP 也称为网络虚拟化边缘 (NVE) 节点。

|                       |                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>桥域</b>             | <p>一个 L2 域，它从成员接口接收数据包，并根据数据包的目标 MAC 地址将数据包转发到其他成员接口，或使数据包在其他成员接口泛洪。OS10 支持两种类型的桥域：简单 VLAN 和虚拟网络。</p> <ul style="list-style-type: none"> <li>简单 VLAN：VLAN ID 表示的网桥域。所有成员端口上的流量都分配有相同的 VLAN ID。</li> <li>虚拟网络：虚拟网络 ID (VNID) 表示的网桥域。虚拟网络支持在 <i>交换机限定的 VLAN</i> 中使用单个 VLAN ID，或者在 <i>端口限定的 VLAN</i> 中使用多个（端口、VLAN）对的叠加封装和映射。</li> </ul> |
| <b>分布式路由</b>          | <p>虚拟网络中的所有 VTEP 都执行跨网段路由，并以两种可能的模式充当 L3 网关：</p> <ul style="list-style-type: none"> <li>非对称路由：所有 VTEP 都可以执行路由。仅在入口 VTEP 上进行路由决策。出口 VTEP 可执行桥接。</li> <li>对称路由：所有 VTEP 都执行路由。在入口和出口 VTEP 上进行路由决策。</li> </ul>                                                                                                                            |
| <b>虚拟网络</b>           | 在 OS10 中，覆盖网络中的每个 L2 泛洪域均表示为 <i>虚拟网络</i> 。                                                                                                                                                                                                                                                                                            |
| <b>虚拟网络标识符 (VNID)</b> | 在 OS10 中标识虚拟网络的 16 位 ID 编号。                                                                                                                                                                                                                                                                                                           |
| <b>虚拟网络接口</b>         | 将虚拟网络桥连接到租户 VRF 路由实例的路由器接口。                                                                                                                                                                                                                                                                                                           |
| <b>访问端口</b>           | VTEP 交换机上连接到终端主机且属于覆盖网络的端口。                                                                                                                                                                                                                                                                                                           |
| <b>网络端口</b>           | VTEP 交换机上连接到基础网络的端口。                                                                                                                                                                                                                                                                                                                  |
| <b>交换机限定的 VLAN</b>    | <p>映射到 OS10 中的虚拟网络 ID (VNID) 的 VLAN。VLAN 的所有成员端口都会自动添加到虚拟网络。</p> <ul style="list-style-type: none"> <li>您只能将一个 VLAN ID 映射到虚拟网络。</li> <li>理想情况下，适用于通过 VXLAN 扩展 IP 结构的现有租户 VLAN。</li> </ul>                                                                                                                                             |
| <b>端口限定的 VLAN</b>     | <p>在 OS10 中映射到虚拟网络 ID (VNID) 的端口、VLAN 对。使用关联的标记 VLAN 或未标记的成员将单个成员接口分配给虚拟网络。使用端口限定的 VLAN，您可以配置：</p> <ul style="list-style-type: none"> <li>到不同虚拟网络的不同访问接口上相同的 VLAN ID。</li> <li>到相同虚拟网络的不同访问接口上不同的 VLAN ID。</li> </ul>                                                                                                                 |

## VXLAN 即 NVO 解决方案

网络虚拟化叠加 (NVO) 是一种解决方案，可满足多租户数据中心的要求，尤其是一个包含虚拟化主机的解决方案。NVO 网络是覆盖网络，用于在基础 IP 网络上属于租户段的虚拟机之间扩展 L2 连接。每个租户的有效负载均封装在原始 VTEP 的 IP 数据包中。要访问有效负载，租户有效负载将在目标 VTEP 上去除封装。每个租户段也称为 *虚拟网络*，并在使用虚拟网络 ID (VNID) 的 OS10 中唯一标识。

VXLAN 是一种用作 NVO 解决方案的封装类型。VXLAN 将租户有效负载封装到 IP UDP 数据包，以用于跨 IP 基础网络进行传输。在 OS10 中，为每个虚拟网络分配了一个 24 位编号，该数字称为 VXLAN 封装的数据包携带的 *VXLAN 网络标识符 (VNI)*。VNI 在所有 VTEP 上唯一标识租户段。OS10 将 ASIC 表格设置为：

- 支持在 L3 网络中创建 L2 桥泛洪域。
- 促进本地端口之间的数据包转发以及从本地设备到远程设备的隧道数据包。

## 配置 VXLAN

要使用 VXLAN 扩展 L2 租户段，请在每个 VTEP 交换机上执行以下配置步骤：

1. 配置封装 VXLAN 数据包中使用的源 IP 地址。
2. 配置虚拟网络并分配 VXLAN VNI。
3. 配置 VLAN 标记的访问端口。
4. 配置未标记的访问端口。
5. （可选）为不同虚拟网络上的主机启用路由。
6. 将本地 VXLAN 源 IP 地址通告到远程 VTEP。
7. （可选）配置 VLT。

## 在 VTEP 上配置源 IP 地址

当您交换机配置为 VXLAN 隧道端点 (VTEP) 时，请配置一个环回接口，其 IP 地址用作封装的数据包标头中的源 IP 地址。只有分配到网络虚拟化边缘 (NVE) 实例的环回接口用作源 VXLAN 接口。

- 如果交换机上至少有一个已分配给虚拟网络 ID (VNID) 的 VXLAN 网络 ID (VNI)，请勿重新配置分配给源接口的 VXLAN 源接口或 IP 地址。
- 必须可以从远程 VTEP 访问源环回 IP 地址。
- 不支持将 IPv6 地址用作源 VXLAN 地址。
- 请勿将源环回接口分配给非默认的 VRF 实例。
- 仅在默认 VRF 中支持远程隧道端点的基础可访问性。

1. 在 CONFIGURATION 模式下将环回接口配置为用作源 VXLAN 隧道端点。范围从 0 到 255。

```
interface loopback number
```

2. 在 INTERFACE 模式下的环回接口上配置 IP 地址。IP 地址允许源 VTEP 通过 L3 传输网络发送 VXLAN 帧。

```
ip address ip-address/mask
```

3. 返回 CONFIGURATION 模式。

```
exit
```

4. 从 CONFIGURATION 模式进入 NVE 模式。NVE 模式允许您在交换机上配置 VXLAN 隧道端点。

```
nve
```

5. 在 NVE 模式下，将环回接口配置为交换机上所有虚拟网络的源隧道端点。

```
source-interface loopback number
```

6. 返回 CONFIGURATION 模式。

```
exit
```

## 配置 VXLAN 虚拟网络

要创建 VXLAN，请将 VXLAN 段 ID (VNI) 分配给虚拟网络 ID (VNID) 并配置远程 VTEP。唯一的 2 字节 VNID 将标识虚拟网络。您不能将同一个 VXLAN VNI 分配给多个虚拟网络。手动配置静态 VXLAN 中的 VXLAN 隧道端点或使用 BGP EVPN 自动查找 VXLAN 隧道端点。

1. 在 CONFIGURATION 模式下创建虚拟网络桥域。有效的 VNID 编号从 1 到 65535。

```
virtual-network vn-id
```

2. 在 VIRTUAL-NETWORK 模式下将 VXLAN VNI 分配给虚拟网络。范围从 1 到 16777215。在每个 VTEP 交换机上为同一个租户段配置 VNI。

```
vxlan-vni vni
```

3. (可选) 如果使用 BGP EVPN for VXLAN，则无需执行此步骤 — 要设置静态 VXLAN，请在 VXLAN-VNI 模式下配置远程 VTEP 的源 IP 地址。您可以为 VXLAN VNI 配置多达 1024 个远程 VTEP 地址。

```
remote-vtep ip-address
```

配置远程 VTEP 后，当 IP 路由到基础 IP 网络中的远程 VTEP IP 地址的路径已知时，虚拟网络将发送和接收来自或到达下游服务器和主机的 VXLAN 封装流量。在访问接口上接收到的所有广播、多播和未知单播 (BUM) 流量都会复制，并发送到所有已配置的远程 VTEP。每个数据包的标头中都包含 VXLAN VNI。

默认情况下，从远程 VTEP 学习 MAC 已启用并未知的单播数据包将泛洪到所有远程 VTEP。要配置额外的远程 VTEP，请重新输入 `remote-vtep ip-address` 命令。

4. 返回 VIRTUAL-NETWORK 模式。

```
exit
```

5. 返回 CONFIGURATION 模式。

```
exit
```

## 配置 VLAN 标记的访问端口

使用交换机限定的 VLAN 或端口限定的 VLAN 配置 VXLAN 覆盖网络中的本地访问端口。仅支持一种方法。您不能使用交换机限定的和端口限定的 VLAN 将标记的 VLAN 成员接口分配给虚拟网络。

- 要使用交换机限定的 VLAN 将 VLAN 标记的成员端口添加到虚拟网络，请执行以下操作：
  1. 在 VLAN 接口模式下，将 VLAN 分配给虚拟网络。

```
interface vlan vlan-id
virtual-network vn-id
```

2. 在接口模式下将端口接口配置为 VLAN 的主干成员。

```
interface ethernet node/slot/port[:subport]
switchport mode trunk
switchport trunk allowed-vlan vlan-id
exit
```

分配给 VLAN 的本地物理端口通过虚拟网络传输数据包。

**注：**分配给虚拟网络的交换机限定的 VLAN 不能具有配置的 IP 地址，并且不能加入 L3 路由；例如：

```
OS10(config)# interface vlan 102
OS10(conf-if-vlan-5)# ip address 1.1.1.1/24
% Error: vlan102, IP address cannot be configured for VLAN attached to Virtual
Network.
```

- 要使用端口限定的 VLAN 将 VLAN 标记的成员端口添加到虚拟网络，请执行以下操作：
  1. 在接口模式下将接口配置为主干成员。

```
interface ethernet node/slot/port[:subport]
switchport mode trunk
exit
```

2. 在 VIRTUAL-NETWORK 模式下，将主干成员接口分配为端口，将 VLAN ID 对分配给虚拟网络。针对接口上的虚拟网络发送和接收的所有流量都带有 VLAN 标记。连接到不同交换机接口的多个租户可以具有相同的 vlan-tag VLAN ID。

```
virtual-network vn-id
member-interface ethernet node/slot/port[:subport] vlan-tag vlan-id
```

端口 VLAN 对将开始通过虚拟网络传输数据包。

3. 重复步骤 1 和 2，以将额外的成员端口、VLAN 对分配到虚拟网络。
  - 您不能将同一端口、VLAN 成员接口对分配到多个虚拟网络。
  - 您可以将具有不同成员接口的相同 vlan-tag VLAN ID 分配到不同的虚拟网络。
  - 您可以将具有不同 vlan-tag VLAN ID 的成员接口分配到不同的虚拟网络。

从 VXLAN 隧道中传输的数据包中删除 VLAN ID 标签。在将每个数据包从隧道的出口源接口发送之前，会将 VXLAN VNI 封装在数据包标头中。在远程 VTEP 中，VXLAN VNI 被删除，并且数据包在虚拟网络桥域上传输。VLAN ID 使用与 VTEP 上的虚拟网络出口接口关联的 VLAN ID 进行重新生成，并且包含在数据包标头中。

## 配置未标记的访问端口

使用交换机限定的 VLAN 或端口限定的 VLAN，将未标记的访问端口添加到 VXLAN 覆盖网络中。仅支持一种方法。

- 要使用交换机限定的 VLAN 将未标记的成员端口添加到虚拟网络，请执行以下操作：
  1. 在 VLAN 接口模式下，将 VLAN 分配给虚拟网络。

```
interface vlan vlan-id
virtual-network vn-id
exit
```

2. 在接口模式下将端口接口配置为 VLAN 的访问成员。

```
interface ethernet node/slot/port[:subport]
switchport access vlan vlan-id
exit
```

通过虚拟网络传输的未标记端口上接收的数据包。

- 要使用端口限定的 VLAN 将未标记的成员端口添加到虚拟网络，请执行以下操作：

1. 创建保留 VLAN ID，以便在 CONFIGURATION 模式下将成员接口上的未标记流量分配给虚拟网络。在内部对属于虚拟网络的交换机上的所有未标记成员接口使用 VLAN ID。

```
virtual-network untagged-vlan untagged-vlan-id
```

2. 将端口接口配置为主干成员，并在接口模式下移除访问 VLAN。

```
interface ethernet node/slot/port[:subport]
switchport mode trunk
no switchport access vlan
exit
```

3. 在 VIRTUAL-NETWORK 模式下，将中继接口分配为虚拟网络的未标记成员。您不能对传统 VLAN 或虚拟网络成员接口上的标记流量使用保留的 VLAN ID。

```
virtual-network vn-id
member-interface ethernet node/slot/port[:subport] untagged
exit
```

如果至少有一个未标记的成员接口分配给虚拟网络，您将无法删除保留未标记的 VLAN ID。如果重新配置保留的未标记 VLAN ID，您必须重新配置虚拟网络中的所有未标记成员接口，才能使用新 ID 或重新加载交换机。

## 在虚拟网络之间启用覆盖路由

之前的部分介绍了 VTEP 如何在虚拟网络上同一 L2 租户段中的主机之间切换流量，以及如何通过 IP 基础结构传输流量。本部分介绍了属于同一租户 VRF 的不同 L2 数据段中的主机如何相互通信。

 **注：**在 S4248-ON 交换机上，静态 VXLAN 不支持虚网之间的 IPv6 覆盖路由。但是，BGP EVPN 支持 IPv6 覆盖路由。

每个租户都分配有一个 VRF，并且每个虚拟网络接口都分配有租户 VRF 中的 IP 子网。VTEP 充当 L3 网关，在将流量封装在 VXLAN 标头之前将流量从一个租户子网路由到另一个租户子网，并将其通过 IP 基础结构进行传输。

要启用虚拟网络之间的流量路由，请为每个虚拟网络配置一个接口，并将其与租户 VRF 关联。在与虚拟网络关联的 IP 子网范围内，将唯一的 IP 地址分配给每个 VTEP 上的每个虚拟网络接口。

要在 VTEP 上启用高效的流量转发，OS10 支持分布式网关路由。分布式网关意味着多个 VTEP 充当租户子网的网关路由器。离主机最近的 VTEP 充当网关路由器。要支持在不同 VTEP 上无缝迁移主机和虚拟机，请在所有 VTEP 上为每个虚拟网络配置一个通用虚拟 IP 地址，即任意广播 IP 地址。使用此任意广播 IP 地址作为 VM 上的网关 IP 地址。

要在每个租户都有其各自的 L2 分段时支持多个租户，请为每个租户配置不同的 IP VRF。所有租户在默认 VRF 中共享同一 VXLAN 基础 IP 结构。

1. 在配置模式下创建用于覆盖路由的非默认 VRF 实例。对于多租户，请为每个租户创建 VRF 实例。

```
ip vrf tenant-vrf-name
exit
```

2. 配置任意广播网关 MAC 地址 — 在配置模式下的所有 VXLAN 虚拟网络中使用所有 VTEP。

当 VM 为 VXLAN 虚拟网络中的任意广播网关 IP 地址发送地址解析协议 (ARP) 请求时，最接近的 VTEP 将使用配置的任意广播 MAC 地址进行响应。在所有 VTEP 上配置相同的 MAC 地址，以便在 VM 迁移到不同的 VTEP 时，任意广播网关 MAC 地址保持相同。由于配置的 MAC 地址会自动用于所有 VXLAN 虚拟网络，请在全局配置模式下进行配置。

```
ip virtual-router mac-address mac-address
```

3. 配置虚拟网络接口，将其分配给租户 VRF 并配置 IP 地址。

接口 IP 地址在每个 VTEP 上必须唯一，包括 VLT 对中的 VTEP。您可以在虚拟网络接口上配置 IPv6 地址。在同一个 VTEP 上配置的不同虚拟网络接口必须在不同的子网中具有虚拟网络 IP 地址。如果未将虚拟网络接口分配给租户 VRF，则会将其分配给默认 VRF。

```
interface virtual-network vn-id
ip vrf forwarding tenant-vrf-name
ip address ip-address/mask
no shutdown
exit
```



4. 在 INTERFACE-VIRTUAL-NETWORK 模式下为每个虚拟网络配置任意广播网关 IPv4 或 IPv6 地址。此任意广播 IP 地址必须与步骤 3 中虚拟网络接口的 IP 地址位于同一子网中。

配置与虚拟网络中所有 VTEP 上的任意广播 IP 地址相同的 IPv4 或 IPv6 地址。所有主机都使用任意广播网关 IP 地址作为连接到在步骤 3 中配置的虚拟网络接口的子网中的默认网关 IP 地址。在所有下游 VM 上配置任意广播网关 IP 地址。通过使用相同的任意广播网关 IP 地址，主机虚拟机可从一个 VTEP 移到 VXLAN 中的另一个 VTEP。Dell EMC 建议在 VLT 和非 VLT VXLAN 配置中使用任意广播网关。

```
interface virtual-network vn-id
ip virtual-router address ip-address
```

虚拟网络路由的配置说明:

- VXLAN 覆盖路由包括在入口 VTEP 上路由租户流量，并在出口 VTEP 上桥接流量。入口 VTEP 了解 ARP 条目，并将租户虚拟机的所有目标 IP 地址与覆盖中的相应虚拟机关联 MAC 地址。在入口 VTEP 中，为每个目标 IP 子网配置虚拟网络，即使 IP 子网没有本地连接的主机。
- 覆盖网络中的虚拟网络接口上不支持仅开放最短路径优先 (OSPF) 和 BGP 等路由协议。但是，支持指向虚拟网络接口或属于虚拟网络子网的下一跳 IP 地址的静态路由。
- 在叠加中添加静态路由时，属于虚拟网络子网的任何下一跳 IP 地址都必须是该路由的唯一下一跳，并且不能是多个 ECMP 下一跳之一。例如，如果您逐一输入以下配置命令，其中 10.250.0.0/16 是一个虚拟网络子网，则只有第一个下一跳在交换机上处于活动状态。

```
OS10(config)# ip route 0.0.0.0/0 10.250.0.101
OS10(config)# ip route 0.0.0.0/0 10.250.0.102
```

如果下一跳是 VLT 域中的双穴 VTEP，则解决方法是在这两个 VTEP 上配置相同的任意广播网关 IP 地址，并使用此地址作为下一跳 IP 地址。

- 虚拟网络中不支持 VLT 对等路由。数据包将发送到虚拟网络对等 MAC 地址 L2 交换机，而不是 IP 路由。要在虚拟网络中实现主动-主动对等节点路由，请在 VLT VTEP 上配置相同的虚拟任意广播网关 IP 和 MAC 地址，并使用任意广播 IP 作为虚拟机上的默认网关。
- 虚拟网络接口上不支持虚拟路由器冗余协议 (VRRP)。配置虚拟任意广播网关 IP 地址，以便在两个 VTEP VLT 对等节点上共享单个网关 IP 地址，并使用任意广播 IP 作为虚拟机上的默认网关。
- 虚拟网络接口上不支持互联网组管理协议 (IGMP) 和协议独立多播 (PIM)。
- 不支持在 VXLAN 终止后将传入 VXLAN 封装的流量的 IP 路由发送到覆盖网络。

下表显示了如何在包含三个虚拟网络和多个 VTEP 的数据中心中使用任意广播网关 IP 和 MAC 地址:

- 为所有虚拟网络中的所有 VTEP 全局配置任意广播 MAC 地址。例如，如果使用三个虚拟网络中的三个 VTEP 交换机:

表. 44: 所有 VTEP 的 MAC 地址

| 虚拟网络    | VTEP   | 任意广播网关 MAC 地址     |
|---------|--------|-------------------|
| VNID 11 | VTEP 1 | 00.11.22.33.44.55 |
|         | VTEP 2 | 00.11.22.33.44.55 |
|         | VTEP 3 | 00.11.22.33.44.55 |
| VNID 12 | VTEP 1 | 00.11.22.33.44.55 |
|         | VTEP 2 | 00.11.22.33.44.55 |
|         | VTEP 3 | 00.11.22.33.44.55 |
| VNID 13 | VTEP 1 | 00.11.22.33.44.55 |
|         | VTEP 2 | 00.11.22.33.44.55 |
|         | VTEP 3 | 00.11.22.33.44.55 |

- 在所有虚拟网络上的每个 VTEP 上的虚拟网络接口上配置唯一的 IP 地址。在虚拟网络子网中的所有 VTEP 上配置相同的任意广播网关 IP 地址。例如:

表. 45: 每个 VTEP 上的虚拟网络接口上的 IP 地址

| 虚拟网络    | VTEP   | 虚拟网络 IP 地址  | 任意广播网关 IP 地址 |
|---------|--------|-------------|--------------|
| VNID 11 | VTEP 1 | 10.10.1.201 | 10.10.1.254  |
|         | VTEP 2 | 10.10.1.202 | 10.10.1.254  |



表. 45: 每个 VTEP 上的虚拟网络接口上的 IP 地址 (续)

| 虚拟网络    | VTEP   | 虚拟网络 IP 地址  | 任意广播网关 IP 地址 |
|---------|--------|-------------|--------------|
|         | VTEP 3 | 10.10.1.203 | 10.10.1.254  |
| VNID 12 | VTEP 1 | 10.20.1.201 | 10.20.1.254  |
|         | VTEP 2 | 10.20.1.202 | 10.20.1.254  |
|         | VTEP 3 | 10.20.1.203 | 10.20.1.254  |
| VNID 13 | VTEP 1 | 10.30.1.201 | 10.30.1.254  |
|         | VTEP 2 | 10.30.1.202 | 10.30.1.254  |
|         | VTEP 3 | 10.30.1.203 | 10.30.1.254  |

## 通告 VXLAN 源 IP 地址

- 将本地源隧道接口的 IP 地址通告至使用现有路由基础架构的基础 IP 网络中的所有 VTEP。本示例使用 OSPF 以通告以太网 1/1/3 上的 VXLAN 源 IP 地址，这是面向基础网络的接口：

```

OS10(config)# router ospf 100
OS10(config-ospf)# router-id 110.111.170.195
OS10(config-ospf)# exit
OS10(config)# interface ethernet1/1/3
OS10(config-if-eth1/1/3)# ip ospf 100 area 0.0.0.0
OS10(config-if-eth1/1/3)# exit
OS10(config)# interface loopback 1
OS10(config-if-lo-1)# ip ospf 100 area 0.0.0.0

```

基础 IP 网络中的每个 VTEP 交换机都会学习 VXLAN 源接口的 IP 地址。如果无法访问远程 VTEP 交换机，其状态将在 `show nve remote-vtep` 输出中显示为 DOWN。

- 在接口模式下，在面向 L3 基础网络的接口上配置的 MTU 值至少比面向服务器的链接上的 MTU 高 50 字节，以允许 VXLAN 封装。范围从 1312 到 9216。

```

mtu value

```

- 返回 CONFIGURATION 模式。

```

exit

```

## 配置 VLT

(可选) 在 VLT 域中使用 VXLAN，请配置 VLT 域 — 包括 VLT 互连 (VLTi) 接口、备份心跳信号和 VLT MAC 地址 (如 *OS10 Enterprise Edition User Guide*) 中的*虚拟链路中继*部分中所述) 。

所需的 VLT VXLAN 配置：

- VTEP 源环回接口的 IP 地址在 VLT 对等节点上必须相同。
- 如果使用端口限定的 VLAN 将标记的访问接口分配给虚拟网络，要识别属于每个虚拟网络的流量，则必须为 VLT 互连 (VLTi) 链路配置唯一的 VLAN ID。
- 配置 VLAN 以在 VIRTUAL-NETWORK 模式中通过 VLTi 链路传输 VXLAN 流量。从 VLTi 上的虚拟网络发送和接收的所有流量都将携带 VLTi VLAN ID 标记。

在两个 VLT 同行上配置相同的 VLTi VLAN ID。您不能将现有 VLAN 的 ID 用于 VLT 对等节点或保留的未标记 VLAN ID。您可以使用 VLTi VLAN ID 将已标记或未标记的访问接口分配给虚拟网络。

```

virtual-network vn-id
vlti-vlan vlan-id

```

- 虽然 VXLAN 虚拟网络没有连接到下游服务器的访问端口成员，但您必须配置交换机限定的 VLAN 或 VLTi VLAN。此 VLAN 的存在可确保 VLTi 链路作为虚拟网络的成员添加，以便从 VXLAN 隧道接收的错误哈希 ARP 数据包到达目标 VLT 节点。

妥善做法：

- 如果 VLT 对等节点失去与承载 L3 网络之间的连接，它将继续通过专用 L3 VLAN 上的 VLTi 链路，将路由流量传输到另一个 VLT 对等节点上的网络。在承载网络中的 VLT 对等节点之间配置 L3 VLAN，并在 VLAN 上启用路由；例如：

```
OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 41.1.1.1/24
OS10(config-if-vl-4000)# ip ospf 1 area 0.0.0.0
```

- 要在 VLT 对等节点启动并加入现有 VLT 域或 VLTi 链路出现故障并且 VLT 对等节点仍然由 VLT 心跳检测到的情况下降低流量损失，请创建一个上行链路状态组。将对等控制器上的所有访问 VLT 端口通道配置为上游链路。将所有面向网络的链路配置为下游链路。例如：

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# enable
OS10(conf-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
OS10(conf-uplink-state-group-1)# upstream port-channel 10
```

## L3 VXLAN 路由扩展

S4100-ON 系列、S5200-ON 系列、S4048T-ON 和 S6010-ON 交换机支持本机 VxLAN 路由 — 传入隧道和传出隧道 (RIOT)。RIOT 需要为覆盖路由保留专用硬件资源。您不能将这些专用资源用于基础路由。

每个覆盖 ARP 条目都需要在硬件中路由下一跳，以将目标租户 VM IP 地址绑定到相应的租户 VM MAC 地址和 VNI。分配给 IP 子网的每个虚拟网络接口都需要硬件中的路由接口。

OS10 支持预设配置文件以重新分配为覆盖 ARP 条目保留的资源数量。为每种预设模式保留的条目数因 OS10 交换机而异。

表. 46: 路由在 OS10 交换机上保留下一跳

| OS10 交换机                 | 叠加下一跳条目 | 基础下一跳条目 | 叠加 L3 RIF 条目 | 基础 L3 RIF 条目 |
|--------------------------|---------|---------|--------------|--------------|
| S41xx-ON 系列：             | —       | —       | —            | —            |
| default-overlay-routing  | 4096    | 28672   | 2048         | 10240        |
| disable-overlay-routing  | 0       | 32768   | 0            | 12288        |
| balanced-overlay-routing | 16384   | 16384   | 6144         | 6144         |
| scaled-overlay-routing   | 24576   | 8192    | 10240        | 2048         |
| S4048T-ON 和 S6010-ON：    | —       | —       | —            | —            |
| default-overlay-routing  | 8192    | 4096    | 2048         | 2048         |
| disable-overlay-routing  | 0       | 49152   | 49152        | 0            |
| balanced-overlay-routing | 24576   | 24576   | 24576        | 6144         |
| scaled-overlay-routing   | 40960   | 8192    | 8192         | 10240        |
| S52xx-ON 系列：             | —       | —       | —            | —            |
| default-overlay-routing  | 8192    | 57344   | 2048         | 14336        |
| disable-overlay-routing  | 0       | 65536   | 0            | 16384        |
| balanced-overlay-routing | 32768   | 32768   | 8192         | 8192         |
| scaled-overlay-routing   | 53248   | 12288   | 12288        | 4096         |
| S4248-ON：                | —       | —       | —            | —            |
| default-overlay-routing  | 20480   | 110592  | 4096         | 28672        |

 注: S4248-ON 交换机支持一个默认配置文件，以保留用于叠加 ARP 条目的源。

要在配置覆盖路由配置文件后激活配置文件，请保存配置并重新加载交换机。

## 配置覆盖路由配置文件

- 在 CONFIGURATION 模式下，启用覆盖路由配置文件或禁用配置的配置文件并返回默认值。

```
OS10(config)# hardware overlay-routing-profile {disable-overlay-routing | balanced-
overlay-routing |
scaled-overlay-routing}
```

## 显示覆盖路由配置文件

- 在不同的配置文件中查看可用于覆盖路由的硬件资源；例如，在 S5200-ON 系列中：

```
OS10# show hardware overlay-routing-profile mode all
Mode Overlay Next-hop Underlay Next-hop Overlay L3 RIF
Underlay L3 RIF
Entries Entries Entries Entries Entries
default-overlay-routing 8192 57344 2048
14336
disable-overlay-routing 0 65536 0
16384
balanced-overlay-routing 32768 32768 8192
8192
scaled-overlay-routing 53248 12288 12288 4096
```

- 查看当前配置的覆盖路由配置文件；例如，在 S5200-ON 系列中：

```
show hardware overlay-routing-profile mode
Setting Mode Overlay Underlay Overlay Underlay
Next-hop Next-hop L3 RIF L3 RIF
Entries Entries Entries Entries
Current default-overlay-routing 8192 57344 2048 14336
Next-boot default-overlay-routing 8192 57344 2048 14336
```

# VTEP 上的 DHCP 中继

叠加中主机上的动态主机配置协议 (DHCP) 客户端使用 VTEP 交换机上的 DHCP 中继与 DHCP 服务器进行通信。在 OS10 中，仅在基础网络中找到 DHCP 服务器时，VTEP 上才支持 DHCP 中继。为了无缝工作，VTEP DHCP 中继会将中继接口的虚拟网络 IP 地址传输到 DHCP 服务器。

默认情况下，DHCP 使用 `giaddr` 数据包字段将这些地址传送到服务器。在 VxLAN 中，在同一默认 VRF 中具有叠加和基础子网，VTEP 上的 DHCP 中继可在无用户干预的情况下运行。但是，在基础和叠加位于不同 VRF 中的 VxLAN 中，默认 DHCP 方法不成功。IP 租户子网位于叠加地址空间中。VTEP 可访问的 IP 地址在基础地址空间中。要从 VTEP 可访问的 IP 地址单独传输客户端的 IP 子网，必须在 DHCP 中继代理选项 82 中配置额外的 DHCP 子选项 (5 或 151)。

由于 OS10 不支持 DHCP 中继代理选项 82 中的必需子选项，因此 `giaddr` 数据包字段必须包含中继接口的虚拟网络 IP 地址，并且必须可以从基础中的 DHCP 服务器访问此 IP 地址。用作 DHCP 中继的每个 VTEP 必须使用路由泄露机制作为通向基础的路由来安装其虚拟网络 IP 地址，并通告给所有基础路由器（包括主干交换机）的路由。

同样，必须可以从叠加中的客户端租户 VRF 访问基础 VRF 中的 DHCP 服务器。在基础默认 VRF 中配置 DHCP 服务器子网的静态路由，并将静态路由泄露到叠加中的客户端租户 VRF。此配置可在虚拟网络中设置客户端与 DHCP 服务器之间的双向通信。如果 VxLAN 叠加子网和基础子网在同一默认 VRF 中，则无需进行路由泄露配置。

## 在 VTEP 上配置 DHCP 中继

- 在默认 VRF 中，将非默认租户 VRF 中的虚拟网络中继接口的 IP 地址配置为静态路由。

```
OS10(config)# ip route 10.10.0.2/32 interface virtual-network 10
```

- 配置到租户 VRF 中 DHCP 服务器接口的静态 IP 路由。

```
OS10(config)# ip route vrf tenant01 40.1.1.0/24 interface vlan40
```

- 在租户 VRF 的虚拟网络接口上配置 DHCP 中继。

```
OS10(config)# interface virtual-network 10
OS10(conf-if-vn-10)# ip helper-address 40.1.1.1 vrf tenant01
```

# 查看 VXLAN 配置

使用 show 命令可验证 VXLAN 配置和监控 VXLAN 操作。

## 查看 VXLAN 虚拟网络

```
OS10# show virtual-network
Codes: DP - MAC-learn Dataplane, CP - MAC-learn Controlplane, UUD - Unknown-Unicast-Drop
Un-tagged VLAN: 888
Virtual Network: 60000
 VLTi-VLAN: 2500
 Members:
 VLAN 1000: port-channel1, ethernet1/1/9, ethernet1/1/10
 VLAN 2500: port-channel1000
VxLAN Virtual Network Identifier: 16775000
Source Interface: loopback100(222.222.222.222)
Remote-VTEPs (flood-list): 55.55.55.55(DP),77.1.1.1(DP)
```

## 查看 VXLAN 虚拟网络端口

```
OS10# show virtual-network interface ethernet 1/1/1
Interface Vlan Virtual-network
ethernet1/1/1 100 1000
ethernet1/1/1 200 2000
ethernet1/1/1 300 3000
```

## 查看 VXLAN 虚拟网络 VLAN

```
OS10# show virtual-network vlan 100
Vlan Virtual-network Interface
100 1000 ethernet1/1/1,ethernet1/1/2
100 5000 ethernet1/1/2
```

## 查看 VXLAN 虚拟网络 VLAN

```
OS10# show vlan
Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring VLANs,
@ - Attached to Virtual Network
Q: A - Access (Untagged), T - Tagged

NUM Status Description Q Ports
* 1 up A Eth1/1/1-1/1/48
@ 100 up T Eth1/1/2,Eth1/1/3
 A Eth1/1/1
@ 101 up T port-channel5
200 up T Eth1/1/11-1/1/15
```

## 查看 VXLAN 虚拟网络统计信息

```
OS10# show virtual-network counters
Virtual-Network Input (Packets/Bytes) Output (Packets/Bytes)
1000 857/8570 257/23709
2000 457/3570 277/13709
```

```
OS10# show virtual-network counters interface 1/1/3 vlan 100
Virtual-Network Input (Packets/Bytes) Output (Packets/Bytes)
1000 857/8570 257/23709
2000 457/3570 277/13709
```

 **注:** 使用 flex 计数器，OS10 可能会在 Output 字段中显示更多数据包，但其他数据包将不会。准确数，使用 Output Bytes 数字。

## 查看 VXLAN 远程 VTEP

```
OS10# show nve remote-vtep summary
Remote-VTEP State
```

```

2.2.2.2 up
```

```
OS10# show nve remote-vtep
Codes: DP - MAC-learn Dataplane, CP - MAC-learn Controlplane, UUD - Unknown-Unicast-Drop
IP Address: 2.2.2.2, State: up, Encap: VxLAN
VNI list: 10000(DP), 200(DP), 300(DP)
```

### 查看远程 VTEP 上的 VXLAN 统计信息

```
OS10# show nve remote-vtep counters
Remote-VTEP Input (Packets/Bytes) Output (Packets/Bytes)

10.10.10.10 857/8570 257/23709
20.20.20.20 457/3570 277/13709
```

### 按 VNID 查看 VXLAN 虚拟网络

```
OS10# show nve vxlan-vni
VNI Virtual-Network Source-IP Remote-VTEPs

101 101 44.44.44.44 11.11.11.11,22.22.22.22,33.33.33.33
102 102 44.44.44.44 11.11.11.11,22.22.22.22,33.33.33.33
103 103 44.44.44.44 11.11.11.11,22.22.22.22,33.33.33.33
104 104 44.44.44.44 11.11.11.11,22.22.22.22,33.33.33.33
```

### 查看虚拟网络之间的 VXLAN 路由

show ip arp vrf 和 show ipv6 neighbors vrf 命令输出将显示有关在交换机的非默认 VRF 中学习的 IPv4 和 IPv6 邻居的信息。show ip route vrf 命令将显示 IPv4 和 IPv6 的路由。

```
OS10# show ip arp vrf tenant1
Address Hardware address Interface Egress Interface

111.0.0.2 00:c5:15:02:12:f1 virtual-network20 ethernet1/1/5
111.0.0.3 00:c5:15:02:12:a2 virtual-network20 port-channel5
111.0.0.4 00:12:98:1f:34:11 virtual-network20 VXLAN(20.0.0.1)
121.0.0.3 00:12:28:1f:34:15 virtual-network20 port-channel5
121.0.0.4 00:f2:34:ac:34:09 virtual-network20 VXLAN(20.0.0.1)

OS10# show ipv6 neighbors vrf tenant1
IPv6 Address Hardware Address State Interface Egress Interface

200::2 00:12:28:1f:34:15 STALE virtual-network40 port-channel5
200::f 00:f2:34:ac:34:09 REACH virtual-network40 VXLAN(20.0.0.1)
```

```
OS10# show ip route vrf vrf_1
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, * - candidate default,
 + - summary route, > - non-active route
Gateway of last resort is not set
Destination Gateway Dist/Metric Last Change

C 100.1.0.0/16 via 100.1.1.4 virtual-network60000 0/0 00:36:24
C 100.33.0.0/16 via 100.33.1.4 virtual-network60032 0/0 00:36:23
C 100.65.0.0/16 via 100.65.1.4 virtual-network60064 0/0 00:36:22
C 100.97.0.0/16 via 100.97.1.4 virtual-network60096 0/0 00:36:21

OS10# show ipv6 route vrf vrf_1
Codes: C - connected
 S - static
 B - BGP, IN - internal BGP, EX - external BGP
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, * - candidate default,
 + - summary route, > - non-active route
```

```

Gateway of last resort is not set
 Destination Gateway Dist/Metric Last Change

C 1000:100:10:1::/64 via 1000:100:10:1::4 virtual-network60000 0/0 00:37:08
C 1000:100:10:21::/64 via 1000:100:10:21::4 virtual-network60032 0/0 00:37:07
C 1000:100:10:41::/64 via 1000:100:10:41::4 virtual-network60064 0/0 00:37:06
C 1000:100:10:61::/64 via 1000:100:10:61::4 virtual-network60096 0/0 00:37:05

```

## VXLAN MAC 地址

使用 `show mac address-table virtual-network` 或 `show mac address-table extended` 命令可显示在 VXLAN 虚拟网络上或在 VXLAN 虚拟网络 and 传统 VLAN 上获知的 MAC 地址。

使用 `clear mac address-table dynamic virtual-network` 和 `clear mac address-table dynamic nve remote-vtep` 命令可从 MAC 地址虚拟网络表中删除地址条目。

**注：**即使将交换机范围的 VLAN 中的端口分配给 VXLAN 虚拟网络，已有的 `show mac address-table` 和 `clear mac-address-table` 命令也不会显示和清除虚拟网络域中的 MAC 地址。

### 显示 VXLAN MAC 地址

表. 47: 显示 VXLAN MAC 地址

| 命令                                                                                                                                                                                        | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>show mac address-table virtual-network [vn-id   local   remote   static   dynamic   address mac-address   interface {ethernet node/slot/port:subport   port-channel number}]</code> | <p>显示在所有或指定虚拟网络上获知的所有 MAC 地址。</p> <p><i>vn-id</i>: 仅显示有关指定虚拟网络的信息。</p> <p><i>local</i>: 仅显示本地获知的 MAC 地址。</p> <p><i>remote</i>: 仅显示远程 MAC 地址。</p> <p><i>static</i>: 仅显示静态 MAC 地址。</p> <p><i>dynamic</i>: 仅显示动态 MAC 地址。</p> <p><i>address mac-address</i>: 仅显示有关指定 MAC 地址的信息。</p> <p><i>interface ethernet node/slot/port:subport</i>: 仅显示在指定接口上获知的 MAC 地址。</p> <p><i>interface port-channel number</i>: 仅显示在指定端口通道上获知的 MAC 地址。</p> |
| <code>show mac address-table extended [address mac-address   interface {ethernet node/slot/port:subport   port-channel number}   static   dynamic]</code>                                 | <p>显示在所有 VLAN 和 VXLAN 上获知的 MAC 地址（默认值）。</p> <p><i>address mac-address</i>: 仅显示有关指定 MAC 地址的信息。</p> <p><i>interface ethernet node/slot/port:subport</i>: 仅显示在指定接口上获知的 MAC 地址。</p> <p><i>interface port-channel number</i>: 仅显示在指定端口通道上获知的 MAC 地址。</p> <p><i>static</i>: 仅显示静态 MAC 地址。</p> <p><i>dynamic</i>: 仅显示动态 MAC 地址。</p>                                                                                                      |
| <code>show mac address-table nve {vxlan-vni vn-id   remote-vtep ip-address}</code>                                                                                                        | <p><i>vxlan-vni vn-id</i>: 显示在 NVE 上从指定的 VXLAN 虚拟网络 ID 中获知的 MAC 地址。</p> <p><i>remote-vtep ip-address</i>: 显示在 NVE 上从指定的远程 VTEP 获知的 MAC 地址。</p>                                                                                                                                                                                                                                                                                    |
| <code>show mac address-table count virtual-network [dynamic   local   remote   static   interface]</code>                                                                                 | 显示在所有虚拟网络上获知的 MAC 地址的数量（默认值）。                                                                                                                                                                                                                                                                                                                                                                                                     |

表. 47: 显示 VXLAN MAC 地址 (续)

| 命令                                                                                                                   | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>{ethernet node/slot/port:subport   port-channel number}   vn-id]</code>                                        | <p><code>dynamic</code>: 显示在所有或指定虚拟网络上获知的动态 MAC 地址的数量。</p> <p><code>local</code>: 显示本地获知的 MAC 地址的数量。</p> <p><code>remote</code>: 显示在所有或指定虚拟网络上获知的远程 MAC 地址的数量。</p> <p><code>static</code>: 显示在所有或指定虚拟网络上获知的静态 MAC 地址的数量。</p> <p><code>interface ethernet node/slot/port:subport</code>: 显示在指定接口上获知的 MAC 地址的数量。</p> <p><code>interface port-channel number</code>: 显示在指定端口通道上获知的 MAC 地址的数量。</p> <p><code>vn-id</code>: 显示指定虚拟网络上获知的 MAC 地址的数量。</p> |
| <code>show mac address-table count nve {remote-vtep ip-address   vxlan-vni vn-id}</code>                             | <p>显示为虚拟网络或远程 VTEP 获知的 MAC 地址的数量。</p> <p><code>remote-vtep ip-address</code>: 显示在指定的远程 VTEP 上获知的 MAC 地址的数量。</p> <p><code>vxlan-vni vn-id</code>: 显示在指定 VXLAN 虚拟网络上获知的 MAC 地址的数量。</p>                                                                                                                                                                                                                                                              |
| <code>show mac address-table count extended [interface ethernet node/slot/port:subport   port-channel number]</code> | <p>显示在所有 VLAN 和 VXLAN 虚拟网络上获知的 MAC 地址的数量。</p> <p><code>interface ethernet node/slot/port:subport</code>: 显示在指定接口上从 VLAN 和 VXLAN 获知的 MAC 地址的数量。</p> <p><code>port-channel number</code>: 显示在指定端口通道上从 VLAN 和 VXLAN 获知的 MAC 地址的数量。</p>                                                                                                                                                                                                               |

## 清除 VXLAN MAC 地址

表. 48: 清除 VXLAN MAC 地址

| 命令                                                                                                                                                                             | 说明                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>clear mac address-table dynamic virtual-network [interface {ethernet node/slot/port:subport   port-channel number}   local   vn-id [address mac-address   local]]</code> | <p>清除在所有 VXLAN 虚拟网络上获知的所有 MAC 地址。</p> <p><code>interface ethernet node/slot/port:subport</code>: 仅清除在指定接口上获知的 MAC 地址。</p> <p><code>interface port-channel number</code>: 仅清除在指定端口通道上获知的 MAC 地址。</p> <p><code>local</code>: 仅清除本地获知的 MAC 地址。</p> <p><code>vn-id</code>: 仅清除在指定虚拟网络上获知的 MAC 地址。</p> <p><code>vn-id address mac-address</code>: 仅清除在指定虚拟网络上获知的 MAC 地址。</p> |
| <code>clear mac address-table dynamic nve remote-vtep ip-address</code>                                                                                                        | 清除从指定的远程 VTEP 获知的所有 MAC 地址。                                                                                                                                                                                                                                                                                                                                             |

# VXLAN 命令

## hardware overlay-routing-profile

配置 VXLAN 覆盖路由的保留 ARP 表条目的数量。

|        |                                                                                                                                                                                                 |                                                                                                                                                                            |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>hardware overlay-routing-profile {balanced-overlay-routing   scaled-overlay-routing   disable-overlay-routing}</code>                                                                     |                                                                                                                                                                            |
| 参数     | <b>balanced-overlay-routing</b>                                                                                                                                                                 | 为平衡的 VXLAN 租户路由保留路由条目： <ul style="list-style-type: none"><li>• S4048T-ON 和 S6010-ON: 24576 条目</li><li>• S4100-ON 系列: 16384 条目</li><li>• S5200-ON 系列交换机: 32768 条目</li></ul> |
|        | <b>scaled-overlay-routing</b>                                                                                                                                                                   | 为缩放的 VXLAN 租户路由保留路由条目： <ul style="list-style-type: none"><li>• S4048T-ON 和 S6010-ON: 36864 条目</li><li>• S4100-ON 系列: 24576 条目</li><li>• S5200-ON 系列交换机: 53248 条目</li></ul> |
|        | <b>disable-overlay-routing</b>                                                                                                                                                                  | 为覆盖路由分配 0 下一跳条目并为基础路由分配所有下一跳条目。                                                                                                                                            |
| 默认     | S4048T-ON 和 S6010-ON 交换机可保留 8192 ARP 表条目。<br>S4100-ON 系列交换机可保留 4096 ARP 表条目。<br>S5200-ON 系列交换机可保留 8192 ARP 表条目。                                                                                 |                                                                                                                                                                            |
| 命令模式   | CONFIGURATION                                                                                                                                                                                   |                                                                                                                                                                            |
| 使用情况信息 | 配置文件中的保留表条目数根据 OS10 交换机的不同而有所不同。要查看交换机的可用覆盖路由配置文件，请使用 <code>show hardware overlay-routing-profile mode all</code> 命令。配置配置文件后，重新加载交换机以激活配置文件。命令的 <code>no</code> 形式将禁用已配置的配置文件并恢复默认的保留 ARP 表条目数。 |                                                                                                                                                                            |
| 示例     | <pre>OS10(config)# hardware overlay-routing-profile balanced-overlay-routing OS10(config)# exit OS10# write memory OS10# reload</pre>                                                           |                                                                                                                                                                            |
| 支持的版本  | 10.4.3.0 or later                                                                                                                                                                               |                                                                                                                                                                            |

## interface virtual-network

配置虚拟网络路由器接口。

|        |                                                                                                              |                          |
|--------|--------------------------------------------------------------------------------------------------------------|--------------------------|
| 语法     | <code>interface virtual-network vn-id</code>                                                                 |                          |
| 参数     | <b>virtual-network vn-id</b>                                                                                 | 输入一个虚拟网络 ID，从 1 到 65535。 |
| 默认     | 未配置                                                                                                          |                          |
| 命令模式   | CONFIGURATION                                                                                                |                          |
| 使用情况信息 | 配置虚拟网络路由器接口以启用连接到虚拟网络的主机，从而将流量路由到同一 VRF 中另一个虚拟网络上的主机。虚拟网络 IP 地址在每个 VTEP 上必须唯一，包括 VTEP 成对 VLT。                |                          |
| 示例     | <pre>OS10(config)# interface virtual-network 10000 OS10(config-if-vn-10000)# ip vrf forwarding tenant1</pre> |                          |



```
OS10(config-if-vn-10000)# ip address 10.1.0.1/16
OS10(config-if-vn-10000)# no shutdown
```

**支持的版本** 10.4.3.0 or later

## ip virtual-router address

为 VXLAN 虚拟网络配置任意广播网关 IP 地址。

**语法** `ip virtual-router address ip-address`

**参数** `address ip-address` 输入任意广播 L3 网关的 IP 地址。

**默认** 未配置

**命令模式** INTERFACE-VIRTUAL-NETWORK

**使用情况信息** 在 VXLAN 虚拟网络中的所有 VTEP 上配置相同的任意广播网关 IP 地址。如果主机虚拟机在 VXLAN 中从一个 VTEP 移到另一个 VTEP，请使用任意广播网关 IP 地址作为默认网关 IP 地址。任意广播网关 IP 地址必须与虚拟网络路由器接口的 IP 地址位于同一子网中。

**示例**

```
OS10(config)# interface virtual-network 10000
OS10(config-if-vn-10000)# ip virtual-router address 10.1.0.100
```

**支持的版本** 10.4.3.0 or later

## ip virtual-router mac-address

配置 VXLAN 路由的任意广播 L3 网关的 MAC 地址。

**语法** `ip virtual-router mac-address mac-address`

**参数** `mac-address mac-address` 输入任意广播 L3 网关的 MAC 地址。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 在所有 VTEP 上配置相同的 MAC 地址，以便在 VM 迁移到不同的 VTEP 时，任意广播网关 MAC 地址保持相同。由于配置的 MAC 地址会自动用于所有 VXLAN 虚拟网络，请在全局配置模式下进行配置。

**示例**

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

**支持的版本** 10.4.3.0 or later

## member-interface

将成员接口上的未标记或已标记 VLAN 流量分配给虚拟网络。

**语法** `member-interface {ethernet node/slot/port[:subport] | port-channel number} {vlan-tag vlan-id | untagged}`

**参数** `ethernet node/slot/port[:subport]` 将指定的接口分配给虚拟网络。

|                            |                                                                                                                                                                          |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>port-channel number</b> | 将指定的端口通道分配给虚拟网络。                                                                                                                                                         |
| <b>untagged</b>            | 将接口或端口通道上的未标记流量分配给虚拟网络。                                                                                                                                                  |
| <b>vlan-tag vlan-id</b>    | 将指定 VLAN 上的标记流量分配给虚拟网络。                                                                                                                                                  |
| <b>默认</b>                  | 未配置                                                                                                                                                                      |
| <b>命令模式</b>                | VIRTUAL-NETWORK                                                                                                                                                          |
| <b>使用情况信息</b>              | 使用此命令可将同一 VLAN 或接口上的流量分配给不同的虚拟网络。此命令的 no 版本将移除配置的值。                                                                                                                      |
| <b>示例</b>                  | <pre>OS10(config)# virtual-network 10000 OS10(config-vn)# member-interface port-channel 10 vlan-tag 200 OS10(config-vn)# member-interface port-channel 20 untagged</pre> |
| <b>支持的版本</b>               | 10.4.2.0 or later                                                                                                                                                        |

nve

进入网络虚拟化边缘 (NVE) 配置模式以配置源 VXLAN 隧道端点。

|               |                                        |
|---------------|----------------------------------------|
| <b>语法</b>     | nve                                    |
| <b>参数</b>     | 无                                      |
| <b>默认</b>     | 无                                      |
| <b>命令模式</b>   | CONFIGURATION                          |
| <b>使用情况信息</b> | 在 NVE 模式下，为交换机上的所有虚拟网络配置源隧道端点。         |
| <b>示例</b>     | <pre>OS10# nve OS10(config-nve)#</pre> |
| <b>支持的版本</b>  | 10.4.2.0 or later                      |

remote-vtep

配置 VXLAN 网络中的远程隧道端点的 IP 地址。

|               |                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | remote-vtep ip-address                                                                                                                                     |
| <b>参数</b>     | ip-address — 输入远程虚拟隧道端点 (VTEP) 的 IP 地址。                                                                                                                    |
| <b>默认</b>     | 未配置                                                                                                                                                        |
| <b>命令模式</b>   | VIRTUAL-NETWORK VXLAN-VNI                                                                                                                                  |
| <b>使用情况信息</b> | 配置远程 VTEP 后，VXLAN 虚拟网络将启用，以开始发送服务器流量。您可以配置多个远程 VTEP。访问接口上接收到的所有广播、多播和未知单播 (BUM) 流量均复制到远程 VTEP 上。此命令的 no 版本将移除配置的值。                                         |
| <b>示例</b>     | <pre>OS10(config-vn-vxlan-vni)# remote-vtep 20.20.20.1 OS10(config-vn-vxlan-vni-remote-vtep)# exit OS10(config-vn-vxlan-vni)# remote-vtep 30.20.20.1</pre> |
| <b>支持的版本</b>  | 10.4.2.0 or later                                                                                                                                          |

# show hardware overlay-routing-profile mode

显示在不同配置文件中可用于覆盖路由的硬件资源的数量。

|        |                                                                                                                      |                               |  |
|--------|----------------------------------------------------------------------------------------------------------------------|-------------------------------|--|
| 语法     | show hardware overlay-routing-profile mode [all]                                                                     |                               |  |
| 参数     | all                                                                                                                  | 查看每个硬件分区中可用于覆盖路由配置文件的租户条目的数量。 |  |
| 默认     | 未配置                                                                                                                  |                               |  |
| 命令模式   | EXEC                                                                                                                 |                               |  |
| 使用情况信息 | 对于 S4100-ON 系列、S5200-ON 系列、S4048T-ON、S4248-ON 和 S6010-ON 交换机，L3 VXLAN 覆盖路由将需要保留硬件资源。配置文件中的保留表条目数根据 OS10 交换机的不同而有所不同。 |                               |  |

## 示例 (S5200-ON 系列)

```
OS10# show hardware overlay-routing-profile mode all
Mode
Overlay Next-hop L3 RIF Underlay L3 RIF
Entries Entries Entries Entries
default-overlay-routing 8192 57344 2048 14336
disable-overlay-routing 0 65536 0 16384
balanced-overlay-routing 32768 32768 8192 8192
scaled-overlay-routing 53248 12288 12288 4096

show hardware overlay-routing-profile mode
Setting Mode Overlay Next-hop L3 RIF Underlay L3 RIF
Entries Entries Entries Entries
Current default-overlay-routing 8192 57344 2048 14336
Next-boot default-overlay-routing 8192 57344 2048 14336
```

支持的版本 10.4.3.0 or later

# show interface virtual-network

显示虚拟网络路由器接口和数据包统计信息的配置。

|        |                                            |                          |  |
|--------|--------------------------------------------|--------------------------|--|
| 语法     | show interface virtual-network [vn-id]     |                          |  |
| 参数     | <b>vn-id</b>                               | 输入一个虚拟网络 ID，从 1 到 65535。 |  |
| 默认     | 未配置                                        |                          |  |
| 命令模式   | EXEC                                       |                          |  |
| 使用情况信息 | 使用此命令可显示用于在虚拟网络中路由流量的虚拟网络 IP 地址。还会显示流量计数器。 |                          |  |
| 示例     |                                            |                          |  |

```
show interface virtual-network 102
Virtual-network 102 is up, line protocol is up
Address is 14:18:77:25:6f:84, Current address is 14:18:77:25:6f:84
Interface index is 66
Internet address is 12.12.12.2/24
Mode of IPv4 Address Assignment: MANUAL
Interface IPv6 oper status: Enabled
Link local IPv6 address: fe80::1618:77ff:fe25:6eb9/64
MTU 1532 bytes, IP MTU 1500 bytes
ARP type: ARPA, ARP Timeout: 60
Last clearing of "show interface" counters: 10:24:21
Queuing strategy: fifo
Input statistics:
89 packets, 10056 octets
Output statistics:
207 packets, 7376 octets
Time since last interface status change: 10:23:21
```

支持的版本 10.4.3.0 or later

## show nve remote-vtep

显示有关远程 VXLAN 隧道端点的信息。

**语法** `show nve remote-vtep [ip-address | summary | counters]`

**参数**

- ip-address** 显示有关指定的远程 VTEP 的详细信息。
- summary** 显示有关远程 VTEP 的汇总信息。
- counters** 显示有关远程 VTEP 流量的统计信息。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 使用此命令可显示每个远程 VTEP 的 IP 地址、运行状态和配置的 VXLAN。同时还会显示用于每个 VXLAN ID (VNI) 的远程 MAC 学习和未知的单播丢弃设置。

**示例**

```
OS10# show nve remote-vtep summary
Remote-VTEP State

2.2.2.2 up
```

```
OS10# show nve remote-vtep
Codes: DP - MAC-learn Dataplane, CP - MAC-learn Controlplane, UUD -
Unknown-Unicast-Drop
IP Address: 2.2.2.2, State: up, Encap: VxLAN
VNI list: 10000 (DP), 200 (DP), 300 (DP)
```

支持的版本 10.4.2.0 or later

## show nve remote-vtep counters

显示远程 VTEP 的 VXLAN 数据包统计信息。

**语法** `show nve remote-vtep [ip-address] counters`

**参数**

- ip-address** — 输入远程 VTEP 的 IP 地址。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 使用此命令可显示远程 VTEP 上的 VXLAN 流量的输入和输出统计信息。VTEP 通过其 IP 地址进行标识。使用 `clear nve remote-vtep [ip-address] counters` 命令可清除 VXLAN 数据包统计信息。

**示例**

```
OS10# show nve remote-vtep counters
Peer Input (Packets/Bytes) Output (Packets/Bytes)
10.10.10.10 857/8570 257/23709
20.20.20.20 457/3570 277/13709
```

支持的版本 10.4.2.0 或更高版本

## show nve vxlan-vni

显示有关交换机上的 VXLAN 虚拟网络的信息。

**语法** `show nve vxlan-vni`

**参数** 无

|        |                                                                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | 未配置                                                                                                                                                                                                                                                               |
| 命令模式   | EXEC                                                                                                                                                                                                                                                              |
| 使用情况信息 | 使用此命令可显示有关已配置的 VXLAN 虚拟网络的信息。每个 VXLAN 虚拟网络由其虚拟网络 ID 标识。                                                                                                                                                                                                           |
| 示例     | <pre>OS10# show nve vxlan-vni VNI      Virtual-Network      Source-IP      Remote-VTEPs ----- 10000    1                    1.1.1.1        2.2.2.2 200      2                    1.1.1.1        2.2.2.2 300      300                 1.1.1.1        2.2.2.2</pre> |
| 支持的版本  | 10.4.2.0 or later                                                                                                                                                                                                                                                 |

## show virtual-network

显示虚拟网络配置，包括所有 VXLAN 配置。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show virtual-network [vn-id]                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 参数     | <b>vn-id</b> 输入一个虚拟网络 ID，从 1 到 65535。                                                                                                                                                                                                                                                                                                                                                                                                        |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | 使用此命令可显示 VXLAN 虚拟网络的 VNID、端口成员、源接口和远程隧道端点。                                                                                                                                                                                                                                                                                                                                                                                                   |
| 示例     | <pre>OS10# show virtual-network Codes: DP - MAC-learn Dataplane, CP - MAC-learn Controlplane, UUD - Unknown-Unicast-Drop Un-tagged VLAN: 888 Virtual Network: 60000 VLTi-VLAN: 2500 Members:   VLAN 1000: port-channel1, ethernet1/1/9, ethernet1/1/10   VLAN 2500: port-channel1000 VxLAN Virtual Network Identifier: 16775000 Source Interface: loopback100(222.222.222.222) Remote-VTEPs (flood-list): 55.55.55.55(DP),77.1.1.1(DP)</pre> |
| 支持的版本  | 10.4.2.0 or later                                                                                                                                                                                                                                                                                                                                                                                                                            |

## show virtual-network counters

显示虚拟网络的数据包统计信息。

|        |                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show virtual-network [vn-id] counters                                                                                                                                                                                                   |
| 参数     | <b>vn-id</b> 输入一个虚拟网络 ID，从 1 到 65535。                                                                                                                                                                                                   |
| 默认     | 未配置                                                                                                                                                                                                                                     |
| 命令模式   | EXEC                                                                                                                                                                                                                                    |
| 使用情况信息 | 使用此命令可以监控虚拟网络（包括 VXLAN）上的数据包吞吐量。使用 clear virtual-network counters 命令可清除虚拟网络计数器。                                                                                                                                                         |
| 示例     | <pre>OS10# show virtual-network counters Virtual-Network      Input (Packets/Bytes)      Output (Packets/Bytes) 1000                 857/8570                  257/23709 2000                 457/3570                  277/13709</pre> |

支持的版本 10.4.2.0 或更高版本

## show virtual-network interface counters

显示成员端口、端口通道或 VXLAN 虚拟网络中 VLAN 的数据包统计信息。

|        |                                                                                                                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show virtual-network interface {ethernet node/slot/port:subport   port-channel number} [vlan vlan-id] counters</code>                                                                                                                                                                                                                                |
| 参数     | <div><div><code>interface</code>      输入以太网接口的端口信息。<br/><code>ethernet</code><br/><code>node/slot/</code><br/><code>port[:subport]</code><br/><code>]</code></div><div><code>interface</code>      输入端口通道号，从 1 到 128。<br/><code>port-channel</code><br/><code>number</code></div><div><code>vlan vlan-id</code>    (可选) 输入 VLAN ID，从 1 到 4093。</div></div> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                        |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                       |
| 使用情况信息 | 使用此命令可监控属于 VXLAN 虚拟网络成员的端口接口上的数据包吞吐量。将 VLAN 成员接口仅分配给一个虚拟网络。要清除成员端口上的 VXLAN 数据包计数器 VLAN 或虚拟网络的成员，请使用 <code>clear virtual-network interface {ethernet node/slot/port:subport   port-channel number} [vlan vlan-id] counters</code> 命令。                                                                                                                       |

|    |                                                                                                                                                                                                          |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show virtual-network interface 1/1/3 vlan 100 counters Virtual-Network      Input (Packets/Bytes)      Output (Packets/Bytes) 2000                  457/3570                  277/13709</pre> |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

支持的版本 10.4.2.0 or later

## show virtual-network interface

显示分配了端口的 VXLAN 虚拟网络和服务器 VLAN。

|        |                                                                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show virtual-network interface {ethernet node/slot/port:subport   port-channel number}</code>                                                                                                                                                                                     |
| 参数     | <div><div><code>interface</code>      输入以太网接口的端口信息。<br/><code>ethernet</code><br/><code>node/slot/</code><br/><code>port[:subport]</code><br/><code>]</code></div><div><code>interface</code>      输入端口通道号，从 1 到 128。<br/><code>port-channel</code><br/><code>number</code></div></div> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                     |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                    |
| 使用情况信息 | 使用此命令可验证连接到下游服务器的以太网端口是其成员的 VXLAN VLAN。                                                                                                                                                                                                                                                 |
| 示例     | <pre>OS10# show virtual-network interface ethernet 1/1/1 Interface      Vlan      Virtual-network ethernet1/1/1  100      1000</pre>                                                                                                                                                    |

|               |     |      |
|---------------|-----|------|
| ethernet1/1/1 | 200 | 2000 |
| ethernet1/1/1 | 300 | 3000 |

支持的版本 10.4.2.0 or later

## show virtual-network vlan

显示分配了 VLAN 的 VXLAN 虚拟网络。

- 语法 show virtual-network vlan *vlan-id*
- 参数 **vlan *vlan-id*** 输入 VLAN ID, 从 1 到 4093。
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 使用此命令可以验证分配了 VLAN 的 VXLAN 虚拟网络, 包括连接到下游服务器的端口成员。
- 示例

```
OS10# show show virtual-network 100
Vlan Virtual-network Interface
100 1000 ethernet1/1/1,ethernet1/1/2
```

支持的版本 10.4.2.0 or later

## show vlan (virtual network)

显示分配给虚拟网络的 VLAN。

- 语法 show vlan
- 参数 无
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 使用此命令可显示通过虚拟网络传输 VXLAN 数据包的 VLAN 端口接口。
- 示例

```
OS10# show vlan
Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring
VLANs,
@ - Attached to Virtual Network
Q: A - Access (Untagged), T - Tagged

 NUM Status Description Q Ports
* 1 up A Eth1/1/1-1/1/48
@ 100 up T Eth1/1/2,Eth1/1/3
A Eth1/1/1
@ 101 up T port-channel5
200 up T Eth1/1/11-1/1/15
```

支持的版本 10.4.2.0 or later

## source-interface loopback

将专用环回接口配置为源 VTEP。

- 语法 source-interface loopback *number*
- 参数 **loopback *number*** 输入用作 VXLAN 虚拟隧道源接口的环回接口, 从 0 到 16383。

|        |                                                                                                                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | 未配置                                                                                                                                                                                                                                                     |
| 命令模式   | NVE-INSTANCE                                                                                                                                                                                                                                            |
| 使用情况信息 | 环回接口的 IP 地址用作从交换机作为 NVE VTEP 发送的封装数据包中的源 IP 地址。 <ul style="list-style-type: none"><li>环回接口必须配置 IP 地址。必须可以从远程 VTEP 访问环回 IP 地址。</li><li>如果为 NVE 实例配置了至少一个 VXLAN 虚拟网络 ID (VNID)，则无法更改源接口。</li></ul> 在 NVE 模式下使用此命令可覆盖以前配置的值并重新配置源 IP 地址。此命令的 no 版本将移除配置的值。 |
| 示例     | <pre>OS10(config-nve)# source-interface loopback 1</pre>                                                                                                                                                                                                |
| 支持的版本  | 10.4.2.0 or later                                                                                                                                                                                                                                       |

## virtual-network

为 VXLAN 隧道创建虚拟网络。

|        |                                                                         |
|--------|-------------------------------------------------------------------------|
| 语法     | virtual-network <i>vn-id</i>                                            |
| 参数     | <b><i>vn-id</i></b> 输入虚拟网络 ID，从 1 到 65535。                              |
| 默认     | 未配置                                                                     |
| 命令模式   | CONFIGURATION                                                           |
| 使用情况信息 | 虚拟网络作为 L2 桥接域运行。要将 VXLAN 添加到虚拟网络，请使用 vxlan-vni 命令。此命令的 no 版本将移除配置的虚拟网络。 |
| 示例     | <pre>OS10(config)# virtual-network 1000 OS10(config-vn)#</pre>          |
| 支持的版本  | 10.4.2.0 or later                                                       |

## virtual-network untagged-vlan

配置用于内部使用的专用 VLAN 以在交换机上的虚拟网络中的成员端口上传输未标记流量。

|        |                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------|
| 语法     | virtual-network untagged-vlan <i>vlan-id</i>                                                              |
| 参数     | <b><i>id</i></b> 输入保留的未标记 VLAN ID，从 1 到 4093。                                                             |
| 默认     | 未配置                                                                                                       |
| 命令模式   | CONFIGURATION                                                                                             |
| 使用情况信息 | 在内部对属于虚拟网络的所有未标记成员接口使用未标记的 VLAN ID。您不能将保留的未标记 VLAN ID 用于简单的 VLAN 桥，也不能用于虚拟网络成员接口上的标记流量。此命令的 no 版本将移除配置的值。 |
| 示例     | <pre>OS10(config)# virtual-network untagged-vlan 10</pre>                                                 |
| 支持的版本  | 10.4.2.0 or later                                                                                         |

## vxlan-vni

将 VXLAN ID 分配给虚拟网络。

|    |                      |
|----|----------------------|
| 语法 | vxlan-vni <i>vni</i> |
|----|----------------------|



|        |                                                                        |
|--------|------------------------------------------------------------------------|
| 参数     | <b>vni</b> 输入虚拟网络的 VXLAN ID，从 1 到 16777215。                            |
| 默认     | 未配置                                                                    |
| 命令模式   | VIRTUAL-NETWORK                                                        |
| 使用情况信息 | 此命令将 VXLAN ID 编号与虚拟网络关联。此命令的 <code>no</code> 版本将移除配置的 ID。              |
| 示例     | <pre>OS10(conf-vn-100)# vxlan-vni 100 OS10(config-vn-vxlan-vni)#</pre> |
| 支持的版本  | 10.4.2.0 or later                                                      |

## VXLAN MAC 命令

### clear mac address-table dynamic nve remote-vtep

清除从远程 VTEP 学习的所有 MAC 地址。

|        |                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>clear mac address-table dynamic nve remote-vtep ip-address</code>                                            |
| 参数     | <b>remote-vtep</b> 清除从指定的远程 VTEP 学习的 MAC 地址。<br><b>ip-address</b>                                                  |
| 默认     | 未配置                                                                                                                |
| 命令模式   | EXEC                                                                                                               |
| 使用情况信息 | 要显示从远程 VTEP 学习的 MAC 地址，请使用 <code>show mac address-table nve remote-vtep</code> 命令。使用此命令可删除从远程 VTEP 学习的所有 MAC 地址条目。 |
| 示例     | <pre>OS10# clear mac address-table dynamic nve remote-vtep 32.1.1.1</pre>                                          |
| 支持的版本  | 10.4.2.0 or later                                                                                                  |

### clear mac address-table dynamic virtual-network

清除在所有或指定的 VXLAN 虚拟网络上获知的 MAC 地址。

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>clear mac address-table dynamic virtual-network [interface {ethernet node/slot/port:subport   port-channel number}   local   vn-id [address mac-address   local]]</code>                                                                                                                                                                                                                                                     |
| 参数 | <b>interface</b> 清除在指定接口上获知的所有 MAC 地址。<br><b>ethernet</b><br><b>node/slot/</b><br><b>port[:subport]</b><br><b>]</b><br><b>interface</b> 清除在指定端口通道上获知的所有 MAC 地址。<br><b>port-channel</b><br><b>number</b><br><b>virtual-</b><br><b>network vn-id</b> 清除所有已在指定虚拟网络上获知的 MAC 地址，从 1 到 65535。<br><b>local</b> 仅清除本地获知的 MAC 地址。<br><b>vn-id</b> 清除指定虚拟网络上获知的 MAC 地址，从 1 到 65535。<br><b>vn-id local</b> 清除指定虚拟网络上本地获知的 MAC 地址，从 1 到 65535。 |

|        |                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <b><code>vn-id address</code></b> 仅清除在指定虚拟网络中获知的 MAC 地址条目。以 <code>EEEE.EEEE.EEEE</code> 格式输入<br><b><code>mac-address</code></b> MAC 地址。                           |
| 默认     | 未配置                                                                                                                                                               |
| 命令模式   | EXEC                                                                                                                                                              |
| 使用情况信息 | 使用此命令时，不使用可选参数，以从 MAC 地址表中删除仅在虚拟网络桥上获知的所有动态 MAC 地址条目。此命令不会删除在简单 VLAN 桥上获知的 MAC 地址条目。使用 <code>show mac address-table virtual-network</code> 命令将显示在虚拟网络上获知的 MAC 地址。 |
| 示例     | <pre>OS10# clear mac address-table dynamic virtual-network</pre>                                                                                                  |
| 支持的版本  | 10.4.2.0 or later                                                                                                                                                 |

## show mac address-table count extended

显示在所有 VLAN 和 VXLAN 虚拟网络上获知的 MAC 地址的数量。

|        |                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show mac address-table count extended [interface {ethernet <i>node/slot/port:subport</i>   port-channel <i>number</i>}]</code>                                                                                                                                                                                                                                                    |
| 参数     | <div> <b><code>interface</code></b> 显示在指定接口的所有 VLAN 和 VXLAN 上获知的 MAC 地址的数量。<br/> <b><code>ethernet</code></b><br/> <b><code>node/slot/</code></b><br/> <b><code>port[:subport]</code></b><br/> <b><code>]</code></b> </div> <div> <b><code>interface</code></b> 显示在指定端口通道上的所有 VLAN 和 VXLAN 上获知的 MAC 地址的数量。<br/> <b><code>port-channel</code></b><br/> <b><code>number</code></b> </div> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                     |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                    |
| 使用情况信息 | 使用此命令可显示在所有 VLAN 和 VXLAN 虚拟网络上获知的 MAC 地址条目的数量。                                                                                                                                                                                                                                                                                                                                          |
| 示例     | <pre>OS10# show mac address-table count extended MAC Entries for all vlans : Dynamic Address Count :           10 Static Address (User-defined) Count :    2 Total MAC Addresses in Use:         12</pre>                                                                                                                                                                               |
| 支持的版本  | 10.4.2.0 or later                                                                                                                                                                                                                                                                                                                                                                       |

## show mac address-table count nve

显示在 VXLAN 虚拟网络或远程 VXLAN 隧道端点上学习的 MAC 地址的数量。

|      |                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | <code>show mac address-table count nve {vxlan-vni <i>vni</i>   remote-vtep <i>ip-address</i>}</code>                                                                                              |
| 参数   | <div> <b><code>vxlan-vni vni</code></b> 显示已在指定的 VXLAN 虚拟网络上学习的 MAC 地址，从 1 到 16,777,215。<br/> <b><code>remote-vtep</code></b> 显示从指定的远程 VTEP 学习的 MAC 地址。<br/> <b><code>ip-address</code></b> </div> |
| 默认   | 未配置                                                                                                                                                                                               |
| 命令模式 | EXEC                                                                                                                                                                                              |

**使用情况信息** 使用 `clear mac address-table dynamic nve remote-vtep` 命令可从远程 VTEP 删除学习的所有 MAC 地址条目。使用 `clear mac address-table dynamic virtual-network vn-id` 命令可删除在虚拟网络桥上学习的所有动态 MAC 地址条目。

**示例**

```
OS10# show mac address-table count nve vxlan-vni 1001
MAC Entries for all vlans :
Dynamic Address Count : 1
Static Address (User-defined) Count : 0
Total MAC Addresses in Use: 1

OS10# show mac address-table count nve remote-vtep 32.1.1.1
MAC Entries for all vlans :
Dynamic Address Count : 2
Static Address (User-defined) Count : 0
Total MAC Addresses in Use: 2
```

**支持的版本** 10.4.2.0 or later

## show mac address-table count virtual-network

显示在虚拟网络上学习的 MAC 地址数。

**语法** `show mac address-table count virtual-network [dynamic | local | remote | static | interface {ethernet node/slot/port:subport | port-channel number} | vn-id]`

|           |                                                                           |                                     |
|-----------|---------------------------------------------------------------------------|-------------------------------------|
| <b>参数</b> | <b>dynamic</b>                                                            | 显示 MAC 地址的本地已动态学习的数量。               |
|           | <b>local</b>                                                              | 显示本地 MAC 地址的数量。                     |
|           | <b>remote</b>                                                             | 显示从远程 VTEP 学习的 MAC 地址的数量。           |
|           | <b>static</b>                                                             | 显示本地静态配置 MAC 地址的数量。                 |
|           | <b>interface</b>                                                          | 显示在指定接口上学习的 MAC 地址的数量。              |
|           | <b>ethernet</b><br><b>node/slot/</b><br><b>port[:subport]</b><br><b>]</b> |                                     |
|           | <b>interface</b><br><b>port-channel</b><br><b>number</b>                  | 显示在指定端口通道上学习的 MAC 地址的数量。            |
|           | <b>vn-id</b>                                                              | 显示指定虚拟网络上学习的 MAC 地址的数量，从 1 到 65535。 |

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 使用此命令可显示在 MAC 地址表中的虚拟网络上学习的 MAC 地址条目的数量。

**示例**

```
OS10# show mac address-table count virtual-network
MAC Entries for all vlans :
Dynamic Address Count : 8
Static Address (User-defined) Count : 0
Total MAC Addresses in Use: 8
```

**支持的版本** 10.4.2.0 or later

## show mac address-table extended

显示在所有 VLAN 和 VXLAN 上了解到的 MAC 地址。

|        |                                                                                                                                              |                        |  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------|--|
| 语法     | show mac address-table extended [address mac-address   interface {ethernet node/slot/port:subport   port-channel number}   static   dynamic] |                        |  |
| 参数     | address mac-address                                                                                                                          | 仅显示有关指定 MAC 地址的信息。     |  |
|        | interface ethernet node/slot/port[:subport]                                                                                                  | 仅显示在指定接口上学习的 MAC 地址。   |  |
|        | interface port-channel number                                                                                                                | 仅显示在指定端口通道上学习的 MAC 地址。 |  |
|        | static                                                                                                                                       | 仅显示静态 MAC 地址。          |  |
|        | dynamic                                                                                                                                      | 仅显示动态 MAC 地址。          |  |
| 默认     | 未配置                                                                                                                                          |                        |  |
| 命令模式   | EXEC                                                                                                                                         |                        |  |
| 使用情况信息 | 默认情况下，从远程 VTEP 进行 MAC 学习已启用。使用此命令以验证是否在交换机上的 VXLAN 虚拟网络和 VLAN 上学习 MAC 地址。show mac address-table 命令仅显示在 LAN 端口和 VLAN 接口上学习的 MAC 地址。           |                        |  |

示例

| OS10# show mac address-table extended |        |                   |         |                       |
|---------------------------------------|--------|-------------------|---------|-----------------------|
| Virtual-Network                       | VlanId | MAC Address       | Type    | Interface/Remote-VTEP |
| -                                     | 500    | 00:00:00:00:11:11 | dynamic | ethernet1/1/31:1      |
| -                                     | 500    | 00:00:00:00:44:44 | dynamic | port-channel1000      |
| -                                     | 1      | aa:bb:cc:dd:f0:03 | static  | port-channel1000      |
| -                                     | 500    | aa:bb:cc:dd:f0:03 | static  | port-channel1000      |
| -                                     | 4000   | aa:bb:cc:dd:f0:03 | static  | port-channel1000      |
| 10000                                 |        | 00:00:00:00:00:11 | dynamic | ethernet1/1/31:1      |
| 10000                                 | 100    | 00:00:00:00:00:44 | dynamic | port-channel1000      |
| 10000                                 | 100    | 00:00:00:00:00:55 | dynamic | port-channel10        |
| 10000                                 |        | 00:00:00:00:00:77 | dynamic | VxLAN(32.1.1.1)       |
| 20000                                 | 300    | 00:00:00:00:00:22 | dynamic | port-channel100       |
| 20000                                 | 300    | 00:00:00:00:00:33 | dynamic | port-channel1000      |
| 20000                                 | 300    | 00:00:00:00:00:66 | dynamic | port-channel10        |
| 20000                                 |        | 00:00:00:00:00:88 | dynamic | VxLAN(32.1.1.1)       |

支持的版本 10.4.2.0 or later

## show mac address-table nve

显示在 VXLAN 虚拟网络或远程 VXLAN 隧道端点上学习的 MAC 地址。

|      |                                                                     |                                                 |  |
|------|---------------------------------------------------------------------|-------------------------------------------------|--|
| 语法   | show mac address-table nve {vxlan-vni vni   remote-vtep ip-address} |                                                 |  |
| 参数   | <b>vxlan-vni vni</b>                                                | 显示已在指定的 VXLAN 虚拟网络上学习的 MAC 地址，从 1 到 16,777,215。 |  |
|      | <b>remote-vtep ip-address</b>                                       | 显示从指定的远程 VTEP 学习的 MAC 地址。                       |  |
| 默认   | 未配置                                                                 |                                                 |  |
| 命令模式 | EXEC                                                                |                                                 |  |

**使用情况信息** 使用 `clear mac address-table dynamic nve remote-vtep 32.1.1.1` 命令可从远程 VTEP 删除学习的所有 MAC 地址条目。使用 `clear mac address-table dynamic virtual-network vn-id` 命令可删除在虚拟网络桥上学习的所有动态 MAC 地址条目。

**示例**

```
OS10# show mac address-table nve remote-vtep 32.1.1.1
Virtual-Network VNI MAC Address Type Remote-VTEP

10000 9999 00:00:00:00:00:77 dynamic VxLAN(32.1.1.1)
20000 19999 00:00:00:00:00:88 dynamic VxLAN(32.1.1.1)

OS10# show mac address-table nve vxlan-vni 9999
Virtual-Network VNI MAC Address Type Remote-VTEP

10000 9999 00:00:00:00:00:77 dynamic VxLAN(32.1.1.1)
```

**支持的版本** 10.4.2.0 or later

## show mac address-table virtual-network

显示在所有或指定虚拟网络上学习的 MAC 地址。

**语法** `show mac address-table virtual-network [vn-id | local | remote | static | dynamic | address mac-address | interface {ethernet node/slot/port:subport | port-channel number}]`

**参数**

|                                                    |                                                              |
|----------------------------------------------------|--------------------------------------------------------------|
| <b>vn-id</b>                                       | 仅显示有关指定的虚拟网络的信息。                                             |
| <b>local</b>                                       | 仅显示本地学习的 MAC 地址。                                             |
| <b>remote</b>                                      | 仅显示远程 MAC 地址。                                                |
| <b>static</b>                                      | 仅显示静态 MAC 地址。                                                |
| <b>dynamic</b>                                     | 仅显示动态 MAC 地址。                                                |
| <b>address mac-address</b>                         | 仅显示有关指定 MAC 地址的信息。以 <code>EEEE.EEEE.EEEE</code> 格式输入 MAC 地址。 |
| <b>interface ethernet node/slot/port[:subport]</b> | 仅显示在指定接口上学习的 MAC 地址。                                         |
| <b>interface port-channel number</b>               | 仅显示在指定端口通道上学习的 MAC 地址。                                       |

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 使用此命令验证在 VXLAN 虚拟网络上学习到的 MAC 地址。默认情况下，从远程 VTEP 进行 MAC 学习已启用。

**示例**

```
OS10# show mac address-table virtual-network
Virtual-Network VlanId MAC Address Type Interface/Remote-VTEP

10000 00:00:00:00:00:11 dynamic ethernet1/1/31:1
10000 100 00:00:00:00:00:44 dynamic port-channel1000
10000 100 00:00:00:00:00:55 dynamic port-channel10
10000 00:00:00:00:00:77 dynamic VxLAN(32.1.1.1)
10000 100 34:a0:a0:a1:a2:f6 dynamic port-channel10
20000 300 00:00:00:00:00:22 dynamic port-channel100
20000 300 00:00:00:00:00:33 dynamic port-channel1000
20000 300 00:00:00:00:00:66 dynamic port-channel10
```

|       |     |                   |         |                 |
|-------|-----|-------------------|---------|-----------------|
| 20000 |     | 00:00:00:00:00:88 | dynamic | VxLAN(32.1.1.1) |
| 20000 | 300 | 34:a0:a0:a1:a2:f6 | dynamic | port-channel10  |

支持的版本10.4.2.0 or later

## 示例：VXLAN 和静态 VTEP

在此示例中，使用了典型的 Clos 分支-主干拓扑，并在 VLT 双主页域中使用静态 VXLAN 隧道端点 (VTEP)。单个交换机配置显示如何设置端到端 VXLAN。基础 IP 网络路由使用 OSPF 进行通告。

- 在 VTEP 1 和 2 上，使用交换机限定的 VLAN 配置将访问端口分配给虚拟网络。
- 在 VTEP 3 和 4 上，使用端口限定的 VLAN 配置将访问端口分配给虚拟网络。
- 在 VTEP 上配置不同 IP 子网中的主机之间的覆盖路由。

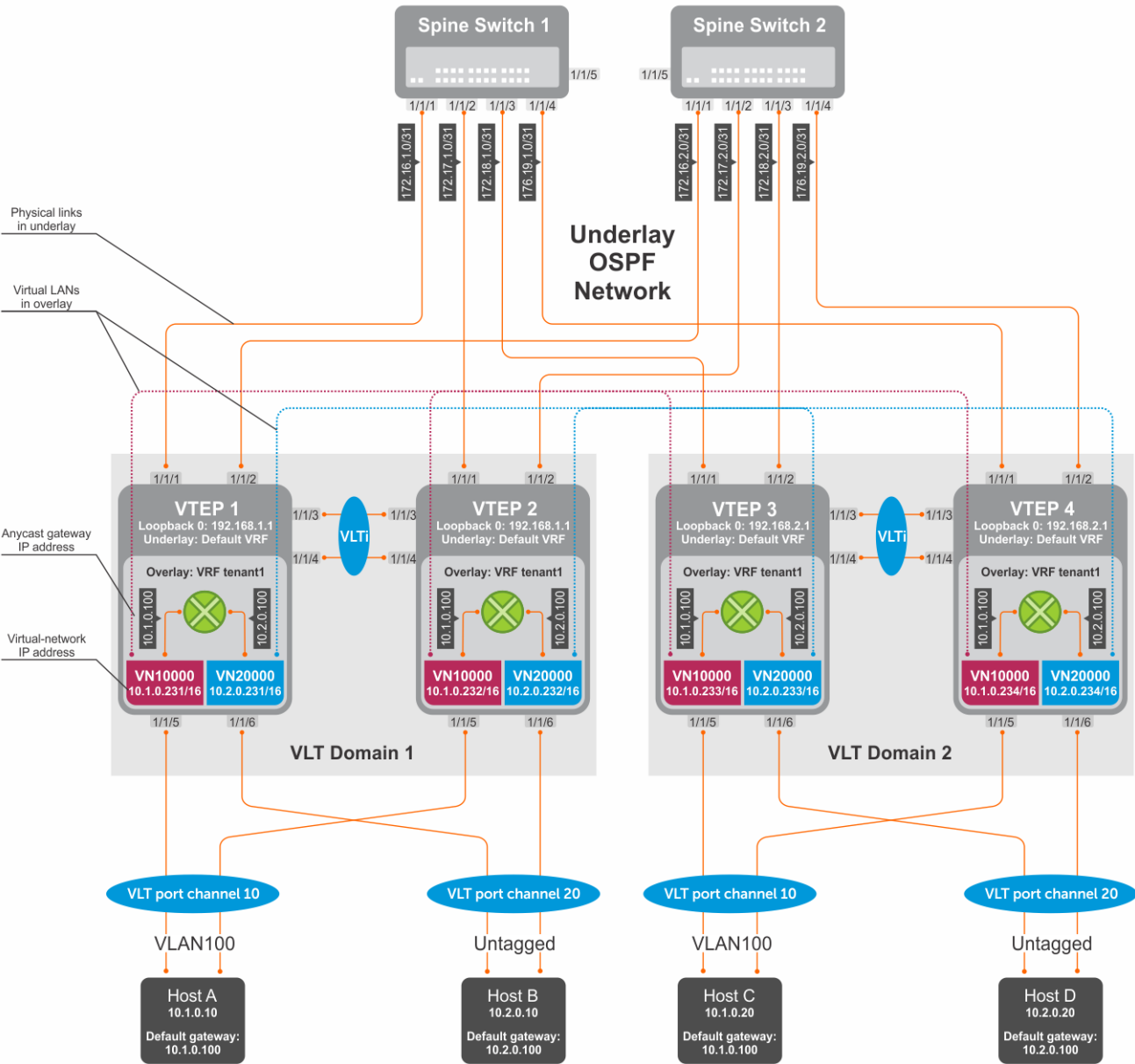


图 10: 静态 VXLAN 使用情形

# VTEP 1 分支交换机

## 1. 配置基础 OSPF 协议

请勿在步骤 2 中为路由器 ID 和源环回接口配置相同的 IP 地址。

```
OS10(config)# router ospf 1
OS10(config-router-ospf-1)# router-id 172.16.0.1
OS10(config-router-ospf-1)# exit
```

## 2. 配置环回接口

```
OS10(config)# interface loopback0
OS10(conf-if-lo-0)# no shutdown
OS10(conf-if-lo-0)# ip address 192.168.1.1/32
OS10(conf-if-lo-0)# ip ospf 1 area 0.0.0.0
OS10(conf-if-lo-0)# exit
```

## 3. 将环回接口配置为 VXLAN 源隧道接口

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback0
OS10(config-nve)# exit
```

## 4. 使用静态 VTEP 配置 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vxlan-vni 10000
OS10(config-vn-vxlan-vni)# remote-vtep 192.168.2.1
OS10(config-vn-vxlan-vni-remote-vtep)# exit
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vxlan-vni 20000
OS10(config-vn-vxlan-vni)# remote-vtep 192.168.2.1
OS10(config-vn-vxlan-vni-remote-vtep)# exit
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-20000)# exit
```

## 5. 将 VLAN 成员接口分配给虚拟网络

使用交换机限定的 VLAN 到 VNI 映射：

```
OS10(config)# interface vlan100
OS10(config-if-vl-100)# virtual-network 10000
OS10(config-if-vl-100)# no shutdown
OS10(config-if-vl-100)# exit
OS10(config)# interface vlan200
OS10(config-if-vl-100)# virtual-network 20000
OS10(config-if-vl-100)# no shutdown
OS10(config-if-vl-100)# exit
```

## 6. 针对交换机限定的 VLAN 至 VNI 映射将访问端口配置为 VLAN 成员

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode trunk
OS10(conf-if-po-10)# switchport trunk allowed vlan 100
OS10(conf-if-po-10)# exit

OS10(config)# interface ethernet1/1/5
OS10(conf-if-eth1/1/5)# no shutdown
OS10(conf-if-eth1/1/5)# channel-group 10 mode active
OS10(conf-if-eth1/1/5)# no switchport
OS10(conf-if-eth1/1/5)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# no shutdown
OS10(conf-if-po-20)# switchport access vlan 200
OS10(conf-if-po-20)# exit
```

```
OS10(config)# interface ethernet1/1/6
OS10(config-if-eth1/1/6)# no shutdown
OS10(config-if-eth1/1/6)# channel-group 20 mode active
OS10(config-if-eth1/1/6)# no switchport
OS10(config-if-eth1/1/6)# exit
```

## 7. 配置面向上游网络的端口

```
OS10(config)# interface ethernet1/1/1
OS10(config-if-eth1/1/1)# no shutdown
OS10(config-if-eth1/1/1)# no switchport
OS10(config-if-eth1/1/1)# mtu 1650
OS10(config-if-eth1/1/1)# ip address 172.16.1.0/31
OS10(config-if-eth1/1/1)# ip ospf 1 area 0.0.0.0
OS10(config-if-eth1/1/1)# exit
```

```
OS10(config)# interface ethernet1/1/2
OS10(config-if-eth1/1/2)# no shutdown
OS10(config-if-eth1/1/2)# no switchport
OS10(config-if-eth1/1/2)# mtu 1650
OS10(config-if-eth1/1/2)# ip address 172.16.2.0/31
OS10(config-if-eth1/1/2)# ip ospf 1 area 0.0.0.0
OS10(config-if-eth1/1/2)# exit
```

## 8. 配置 VLT

### 配置专用 L3 承载路径，以在发生网络故障时访问 VLT 对等方

```
OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 172.16.250.1/30
OS10(config-if-vl-4000)# ip ospf 1 area 0.0.0.0
OS10(config-if-vl-4000)# exit
```

### 配置 VLT 端口通道

```
OS10(config)# interface port-channel10
OS10(config-if-po-10)# vlt-port-channel 10
OS10(config-if-po-10)# exit

OS10(config)# interface port-channel20
OS10(config-if-po-20)# vlt-port-channel 20
OS10(config-if-po-20)# exit
```

### 配置 VLTi 成员链路

```
OS10(config)# interface ethernet1/1/3
OS10(config-if-eth1/1/3)# no shutdown
OS10(config-if-eth1/1/3)# no switchport
OS10(config-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(config-if-eth1/1/4)# no shutdown
OS10(config-if-eth1/1/4)# no switchport
OS10(config-if-eth1/1/4)# exit
```

### 配置 VLT 域

```
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# backup destination 10.16.150.1
OS10(config-vlt-1)# discovery-interface ethernet1/1/3,1/1/4
OS10(config-vlt-1)# vlt-mac aa:bb:cc:dd:ee:ff
OS10(config-vlt-1)# exit
```

### 使用上行链路 VLT 端口和下行链路网络端口配置 UFD

```
OS10(config)# uplink-state-group 1
OS10(config-uplink-state-group-1)# enable
OS10(config-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
```



```
OS10(config-uplink-state-group-1)# upstream port-channel10
OS10(config-uplink-state-group-1)# upstream port-channel20
OS10(config-uplink-state-group-1)# exit
```

## 9. 配置叠加 IP 路由

### 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(config-vrf)# exit
```

### 为所有 VTEP 配置任意广播 L3 网关 MAC 地址

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

### 使用每个虚拟网络的任意广播网关 IP 地址配置路由

```
OS10(config)# interface virtual-network 10000
OS10(config-if-vn-10000)# ip vrf forwarding tenant1
OS10(config-if-vn-10000)# ip address 10.1.0.231/16
OS10(config-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(config-if-vn-10000)# no shutdown
OS10(config-if-vn-10000)# exit
OS10(config)# interface virtual-network 20000
OS10(config-if-vn-20000)# ip vrf forwarding tenant1
OS10(config-if-vn-20000)# ip address 10.2.0.231/16
OS10(config-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(config-if-vn-20000)# no shutdown
OS10(config-if-vn-20000)# exit
```

## VTEP 2 分支交换机

### 1. 配置基础 OSPF 协议

请勿在其他 VTEP 交换机上配置相同的路由器 ID。

```
OS10(config)# router ospf 1
OS10(config-router-ospf-1)# router-id 172.17.0.1
OS10(config-router-ospf-1)# exit
```

### 2. 配置环回接口

源接口 IP 地址必须与 VLT 对等节点上的源接口 IP 地址相同。

```
OS10(config)# interface loopback0
OS10(config-if-lo-0)# no shutdown
OS10(config-if-lo-0)# ip address 192.168.1.1/32
OS10(config-if-lo-0)# ip ospf 1 area 0.0.0.0
OS10(config-if-lo-0)# exit
```

### 3. 将环回接口配置为 VXLAN 源隧道接口

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback0
OS10(config-nve)# exit
```

### 4. 使用静态 VTEP 配置 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vxlan-vni 10000
OS10(config-vn-vxlan-vni)# remote-vtep 192.168.2.1
OS10(config-vn-vxlan-vni-remote-vtep)# exit
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vxlan-vni 20000
OS10(config-vn-vxlan-vni)# remote-vtep 192.168.2.1
OS10(config-vn-vxlan-vni-remote-vtep)# exit
```

```
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-20000)# exit
```

## 5. 将交换机限定的 VLAN 分配给虚拟网络

```
OS10(config)# interface vlan100
OS10(config-if-vl-100)# virtual-network 10000
OS10(config-if-vl-100)# no shutdown
OS10(config-if-vl-100)# exit
OS10(config)# interface vlan200
OS10(config-if-vl-100)# virtual-network 20000
OS10(config-if-vl-100)# no shutdown
OS10(config-if-vl-100)# exit
```

## 6. 将访问端口配置为 VLAN 成员

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode access
OS10(conf-if-po-10)# switchport access vlan 200
OS10(conf-if-po-10)# exit

OS10(config)# interface ethernet1/1/5
OS10(conf-if-eth1/1/5)# no shutdown
OS10(conf-if-eth1/1/5)# channel-group 10 mode active
OS10(conf-if-eth1/1/5)# no switchport
OS10(conf-if-eth1/1/5)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# no shutdown
OS10(conf-if-po-20)# switchport mode access
OS10(conf-if-po-20)# switchport access vlan 200
OS10(conf-if-po-20)# exit

OS10(config)# interface ethernet1/1/6
OS10(conf-if-eth1/1/6)# no shutdown
OS10(conf-if-eth1/1/6)# channel-group 20 mode active
OS10(conf-if-eth1/1/6)# no switchport
OS10(conf-if-eth1/1/6)# exit
```

## 7. 配置面向上游网络的端口

```
OS10(config)# interface ethernet1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/1)# ip address 172.17.1.0/31
OS10(conf-if-eth1/1/1)# ip ospf 1 area 0.0.0.0
OS10(conf-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/2)# ip address 172.17.2.0/31
OS10(conf-if-eth1/1/2)# ip ospf 1 area 0.0.0.0
OS10(conf-if-eth1/1/2)# exit
```

## 8. 配置 VLT

### 配置专用 L3 承载路径，以在发生网络故障时访问 VLT 对等节点

```
OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 172.16.250.2/30
OS10(config-if-vl-4000)# ip ospf 1 area 0.0.0.0
OS10(config-if-vl-4000)# exit
```

## 配置 VLT 端口通道

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# vlt port-channel 10
OS10(conf-if-po-10)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# vlt port-channel 20
OS10(conf-if-po-20)# exit
```

## 配置 VLTi 成员链路

```
OS10(config)# interface ethernet1/1/3
OS10(conf-if-eth1/1/3)# no shutdown
OS10(conf-if-eth1/1/3)# no switchport
OS10(conf-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(conf-if-eth1/1/4)# no shutdown
OS10(conf-if-eth1/1/4)# no switchport
OS10(conf-if-eth1/1/4)# exit
```

## 配置 VLT 域

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.150.2
OS10(conf-vlt-1)# discovery-interface ethernet1/1/3,1/1/4
OS10(conf-vlt-1)# vlt-mac aa:bb:cc:dd:ee:ff
OS10(conf-vlt-1)# exit
```

## 使用上行链路 VLT 端口和下行链路网络端口配置 UFD

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# enable
OS10(conf-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
OS10(conf-uplink-state-group-1)# upstream port-channel10
OS10(conf-uplink-state-group-1)# upstream port-channel20
OS10(conf-uplink-state-group-1)# exit
```

## 9. 配置叠加 IP 路由

### 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(conf-vrf)# exit
```

### 为所有 VTEP 配置任意广播 L3 网关 MAC 地址

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

### 使用每个虚拟网络的任意广播网关 IP 地址配置路由

```
OS10(config)# interface virtual-network 10000
OS10(config-if-vn-10000)# ip vrf forwarding tenant1
OS10(config-if-vn-10000)# ip address 10.1.0.232/16
OS10(config-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(config-if-vn-10000)# no shutdown
OS10(config-if-vn-10000)# exit
OS10(config)# interface virtual-network 20000
OS10(config-if-vn-20000)# ip vrf forwarding tenant1
OS10(config-if-vn-20000)# ip address 10.2.0.232/16
OS10(config-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(config-if-vn-20000)# no shutdown
OS10(config-if-vn-20000)# exit
```

## VTEP 3 分支交换机

### 1. 配置基础 OSPF 协议

请勿在步骤 2 中为路由器 ID 和源环回接口配置相同的 IP 地址。

```
OS10(config)# router ospf 1
OS10(config-router-ospf-1)# router-id 172.18.0.1
OS10(config-router-ospf-1)# exit
```

### 2. 配置环回接口

```
OS10(config)# interface loopback0
OS10(conf-if-lo-0)# no shutdown
OS10(conf-if-lo-0)# ip address 192.168.2.1/32
OS10(conf-if-lo-0)# ip ospf 1 area 0.0.0.0
OS10(conf-if-lo-0)# exit
```

### 3. 将环回接口配置为 VXLAN 源隧道接口

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback0
OS10(config-nve)# exit
```

### 4. 使用静态 VTEP 配置 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vxlan-vni 10000
OS10(config-vn-vxlan-vni)# remote-vtep 192.168.1.1
OS10(config-vn-vxlan-vni-remote-vtep)# exit
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vxlan-vni 20000
OS10(config-vn-vxlan-vni)# remote-vtep 192.168.1.1
OS10(config-vn-vxlan-vni-remote-vtep)# exit
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-20000)# exit
```

### 5. 为未标记成员接口配置保留的 VLAN ID

```
OS10(config)# virtual-network untagged-vlan 1000
```

### 6. 配置访问端口

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode trunk
OS10(conf-if-po-10)# no switchport access vlan
OS10(conf-if-po-10)# exit

OS10(config)# interface ethernet1/1/5
OS10(conf-if-eth1/1/5)# no shutdown
OS10(conf-if-eth1/1/5)# channel-group 10 mode active
OS10(conf-if-eth1/1/5)# no switchport
OS10(conf-if-eth1/1/5)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# no shutdown
OS10(conf-if-po-20)# switchport mode trunk
OS10(conf-if-po-20)# no switchport access vlan
OS10(conf-if-po-20)# exit

OS10(config)# interface ethernet1/1/6
OS10(conf-if-eth1/1/6)# no shutdown
OS10(conf-if-eth1/1/6)# channel-group 20 mode active
OS10(conf-if-eth1/1/6)# no switchport
OS10(conf-if-eth1/1/6)# exit
```

## 7. 将访问端口添加到 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# member-interface port-channel 10 vlan-tag 100
OS10(config-vn-10000)# exit
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# member-interface port-channel 20 untagged
OS10(config-vn-20000)# exit
```

**注：**此步骤显示如何使用端口限定的 VLAN 到 VNI 映射添加访问端口。您还可以使用交换机限定的 VLAN 到 VNI 映射添加访问端口。但是，不能同时使用这两种方法；您必须使用端口限定的或交换机限定的 VLAN 到 VNI 映射。

## 8. 配置面向上游网络的端口

```
OS10(config)# interface ethernet1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/1)# ip address 172.18.1.0/31
OS10(conf-if-eth1/1/1)# ip ospf 1 area 0.0.0.0
OS10(conf-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# mtu 1650
OS10(conf-if-eth1/1/2)# ip address 172.18.2.0/31
OS10(conf-if-eth1/1/2)# ip ospf 1 area 0.0.0.0
OS10(conf-if-eth1/1/2)# exit
```

## 9. 配置 VLT

### 为 VXLAN 虚拟网络配置 VLTi VLAN

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vlti-vlan 100
OS10(config-vn-10000)# exit
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vlti-vlan 200
OS10(config-vn-20000)# exit
```

### 配置专用 L3 承载路径，以在发生网络故障时访问 VLT 对等节点

```
OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 172.16.250.9/30
OS10(config-if-vl-4000)# ip ospf 1 area 0.0.0.0
OS10(config-if-vl-4000)# exit
```

### 配置 VLT 端口通道

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# vlt port-channel 10
OS10(conf-if-po-10)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# vlt port-channel 20
OS10(conf-if-po-20)# exit
```

### 配置 VLTi 成员链路

```
OS10(config)# interface ethernet1/1/3
OS10(conf-if-eth1/1/3)# no shutdown
OS10(conf-if-eth1/1/3)# no switchport
OS10(conf-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(conf-if-eth1/1/4)# no shutdown
OS10(conf-if-eth1/1/4)# no switchport
OS10(conf-if-eth1/1/4)# exit
```

## 配置 VLT 域

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.150.3
OS10(conf-vlt-1)# discovery-interface ethernet1/1/3,1/1/4
OS10(conf-vlt-1)# vlt-mac aa:bb:dd:cc:ff:ee
OS10(conf-vlt-1)# exit
```

## 使用上行链路 VLT 端口和下行链路网络端口配置 UFD

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# enable
OS10(conf-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
OS10(conf-uplink-state-group-1)# upstream port-channel10
OS10(conf-uplink-state-group-1)# upstream port-channel20
OS10(conf-uplink-state-group-1)# exit
```

## 10. 配置叠加 IP 路由

### 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(conf-vrf)# exit
```

### 配置任意广播 L3 网关

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

### 使用每个虚拟网络的任意广播网关 IP 地址配置路由

```
OS10(config)# interface virtual-network 10000
OS10(config-if-vn-10000)# ip vrf forwarding tenant1
OS10(config-if-vn-10000)# ip address 10.1.0.233/16
OS10(config-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(config-if-vn-10000)# no shutdown
OS10(config-if-vn-10000)# exit
OS10(config)# interface virtual-network 20000
OS10(config-if-vn-20000)# ip vrf forwarding tenant1
OS10(config-if-vn-20000)# ip address 10.2.0.233/16
OS10(config-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(config-if-vn-20000)# no shutdown
OS10(config-if-vn-20000)# exit
```

# VTEP 4 分支交换机

## 1. 配置基础 OSPF 协议

请勿在步骤 2 中为路由器 ID 和源环回接口配置相同的 IP 地址。

```
OS10(config)# router ospf 1
OS10(config-router-ospf-1)# router-id 172.19.0.1
OS10(config-router-ospf-1)# exit
```

## 2. 配置环回接口

```
OS10(config)# interface loopback0
OS10(conf-if-lo-0)# no shutdown
OS10(conf-if-lo-0)# ip address 192.168.2.1/32
OS10(conf-if-lo-0)# ip ospf 1 area 0.0.0.0
OS10(conf-if-lo-0)# exit
```

## 3. 将环回接口配置为 VXLAN 源隧道接口

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback0
OS10(config-nve)# exit
```

#### 4. 使用静态 VTEP 配置 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vxlan-vni 10000
OS10(config-vn-vxlan-vni)# remote-vtep 192.168.1.1
OS10(config-vn-vxlan-vni-remote-vtep)# exit
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vxlan-vni 20000
OS10(config-vn-vxlan-vni)# remote-vtep 192.168.1.1
OS10(config-vn-vxlan-vni-remote-vtep)# exit
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-20000)# exit
```

#### 5. 为未标记成员接口配置保留的 VLAN ID

```
OS10(config)# virtual-network untagged-vlan 1000
```

#### 6. 配置访问端口

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode trunk
OS10(conf-if-po-10)# no switchport access vlan
OS10(conf-if-po-10)# exit

OS10(config)# interface ethernet1/1/5
OS10(conf-if-eth1/1/5)# no shutdown
OS10(conf-if-eth1/1/5)# channel-group 10 mode active
OS10(conf-if-eth1/1/5)# no switchport
OS10(conf-if-eth1/1/5)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# no shutdown
OS10(conf-if-po-20)# switchport mode trunk
OS10(conf-if-po-20)# no switchport access vlan
OS10(conf-if-po-20)# exit

OS10(config)# interface ethernet1/1/6
OS10(conf-if-eth1/1/6)# no shutdown
OS10(conf-if-eth1/1/6)# channel-group 20 mode active
OS10(conf-if-eth1/1/6)# no switchport
OS10(conf-if-eth1/1/6)# exit
```

#### 7. 将访问端口添加到 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# member-interface port-channel 10 vlan-tag 100
OS10(config-vn-10000)# exit
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# member-interface port-channel 20 untagged
OS10(config-vn-20000)# exit
```

#### 8. 配置面向上游网络的端口

```
OS10(config)# interface ethernet1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/1)# ip address 172.19.1.0/31
OS10(conf-if-eth1/1/1)# ip ospf 1 area 0.0.0.0
OS10(conf-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# mtu 1650
OS10(conf-if-eth1/1/2)# ip address 172.19.2.0/31
```

```
OS10(config-if-eth1/1/2)# ip ospf 1 area 0.0.0.0
OS10(config-if-eth1/1/2)# exit
```

## 9. 配置 VLT

### 为 VXLAN 虚拟网络配置 VLTi VLAN

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vlti-vlan 200
OS10(config-vn-10000)# exit
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vlti-vlan 100
OS10(config-vn-20000)# exit
```

### 配置专用 L3 承载路径，以在发生网络故障时访问 VLT 对等节点

```
OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 172.16.250.10/30
OS10(config-if-vl-4000)# ip ospf 1 area 0.0.0.0
OS10(config-if-vl-4000)# exit
```

### 配置 VLT 端口通道

```
OS10(config)# interface port-channel10
OS10(config-if-po-10)# vlt port-channel 10
OS10(config-if-po-10)# exit

OS10(config)# interface port-channel20
OS10(config-if-po-20)# vlt port-channel 20
OS10(config-if-po-20)# exit
```

### 配置 VLTi 成员链路

```
OS10(config)# interface ethernet1/1/3
OS10(config-if-eth1/1/3)# no shutdown
OS10(config-if-eth1/1/3)# no switchport
OS10(config-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(config-if-eth1/1/4)# no shutdown
OS10(config-if-eth1/1/4)# no switchport
OS10(config-if-eth1/1/4)# exit
```

### 配置 VLT 域

```
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# backup destination 10.16.150.4
OS10(config-vlt-1)# discovery-interface ethernet1/1/3,1/1/4
OS10(config-vlt-1)# vlt-mac aa:bb:dd:cc:ff:ee
OS10(config-vlt-1)# exit
```

### 使用上行链路 VLT 端口和下行链路网络端口配置 UFD

```
OS10(config)# uplink-state-group 1
OS10(config-uplink-state-group-1)# enable
OS10(config-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
OS10(config-uplink-state-group-1)# upstream port-channel10
OS10(config-uplink-state-group-1)# upstream port-channel20
OS10(config-uplink-state-group-1)# exit
```

## 10. 配置叠加 IP 路由

### 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(config-vrf)# exit
```



## 为所有虚拟网络中的所有 VTEP 配置任意广播 L3 网关

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

## 使用每个虚拟网络的任意广播网关 IP 地址配置路由

```
OS10(config)# interface virtual-network 10000
OS10(config-if-vn-10000)# ip vrf forwarding tenant1
OS10(config-if-vn-10000)# ip address 10.1.0.234/16
OS10(config-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(config-if-vn-10000)# no shutdown
OS10(config-if-vn-10000)# exit
OS10(config)# interface virtual-network 20000
OS10(config-if-vn-20000)# ip vrf forwarding tenant1
OS10(config-if-vn-20000)# ip address 10.2.0.234/16
OS10(config-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(config-if-vn-20000)# no shutdown
OS10(config-if-vn-20000)# exit
```

# 主干交换机 1

## 1. 在承载链路上配置指向分支交换机的下游端口

```
OS10(config)# interface ethernet1/1/1
OS10(config-if-eth1/1/1)# no shutdown
OS10(config-if-eth1/1/1)# no switchport
OS10(config-if-eth1/1/1)# ip address 172.16.1.1/31
OS10(config-if-eth1/1/1)# ip ospf 1 area 0.0.0.0
OS10(config-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(config-if-eth1/1/2)# no shutdown
OS10(config-if-eth1/1/2)# no switchport
OS10(config-if-eth1/1/2)# ip address 172.17.1.1/31
OS10(config-if-eth1/1/2)# ip ospf 1 area 0.0.0.0
OS10(config-if-eth1/1/2)# exit

OS10(config)# interface ethernet1/1/3
OS10(config-if-eth1/1/3)# no shutdown
OS10(config-if-eth1/1/3)# no switchport
OS10(config-if-eth1/1/3)# ip address 172.18.1.1/31
OS10(config-if-eth1/1/3)# ip ospf 1 area 0.0.0.0
OS10(config-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(config-if-eth1/1/4)# no shutdown
OS10(config-if-eth1/1/4)# no switchport
OS10(config-if-eth1/1/4)# ip address 172.19.1.1/31
OS10(config-if-eth1/1/4)# ip ospf 1 area 0.0.0.0
OS10(config-if-eth1/1/4)# exit
```

## 2. 配置基础 OSPF 协议

```
OS10(config)# router ospf 1
OS10(config-router-ospf-1)# router-id 172.200.0.1
OS10(config-router-ospf-1)# exit
```

# 主干交换机 2

## 1. 在承载链路上配置指向分支交换机的下游端口

```
OS10(config)# interface ethernet1/1/1
OS10(config-if-eth1/1/1)# no shutdown
OS10(config-if-eth1/1/1)# no switchport
OS10(config-if-eth1/1/1)# ip address 172.16.2.1/31
OS10(config-if-eth1/1/1)# ip ospf 1 area 0.0.0.0
```

```

OS10(config-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(config-if-eth1/1/2)# no shutdown
OS10(config-if-eth1/1/2)# no switchport
OS10(config-if-eth1/1/2)# ip address 172.17.2.1/31
OS10(config-if-eth1/1/2)# ip ospf 1 area 0.0.0.0
OS10(config-if-eth1/1/2)# exit

OS10(config)# interface ethernet1/1/3
OS10(config-if-eth1/1/3)# no shutdown
OS10(config-if-eth1/1/3)# no switchport
OS10(config-if-eth1/1/3)# ip address 172.18.2.1/31
OS10(config-if-eth1/1/3)# ip ospf 1 area 0.0.0.0
OS10(config-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(config-if-eth1/1/4)# no shutdown
OS10(config-if-eth1/1/4)# no switchport
OS10(config-if-eth1/1/4)# ip address 172.19.2.1/31
OS10(config-if-eth1/1/4)# ip ospf 1 area 0.0.0.0
OS10(config-if-eth1/1/4)# exit

```

## 2. 配置基础 OSPF 协议

```

OS10(config)# router ospf 1
OS10(config-router-ospf-1)# router-id 172.201.0.1
OS10(config-router-ospf-1)# exit

```

# BGP EVPN for VXLAN

以太网虚拟专用网络 (EVPN) 是 VXLAN 的控制平面，可减少网络泛洪并解决可扩展性问题。EVPN 使用 MP BGP 在 VTEP 之间交换信息。EVPN 是在 RFC 7432 中引入的，并且基于 BGP MPLS 的 VPN。RFC 8365 介绍了基于 VXLAN 的 EVPN。

MP BGP EVPN 控制平面提供基于协议的远程 VTEP 查找以及 MAC 和 ARP 获知。此配置可减少与 L2 未知单播流量相关的泛洪。主机 MAC 和 IP 可访问性信息的分发支持虚拟机 (VM) 移动性和可扩展的 VXLAN 覆盖网络设计。

BGP EVPN 协议将 MAC 地址和 ARP/邻居地址分组到 EVPN 实例 (EVI) 下，以便在 VTEP 之间交换它们。在 OS10 中，每个 EVI 在 1:1 映射中与一个 VXLAN VNI 关联。

## 基于 BGP EVPN 的 VXLAN 的优势

- 通过启用端主机 L2 和 L3 可访问性信息的控制平面获知，消除了 VTEP 发现的泛洪和获知方法。
- 通过本地 VTEP 上基于 EVPN 的 MAC 和 IP 路由通告，最大限度地减少未知单播和广播流量的网络泛洪。
- 为主机移动性提供支持。

# BGP EVPN 与静态 VXLAN 比较

OS10 支持两种类型的 VXLAN NVO 覆盖网络：

- 静态 VXLAN
- BGP EVPN

为 VXLAN 配置和操作静态 VXLAN 和 BGP EVPN，方法是：

- 手动配置覆盖和基础网络。
- 手动配置每个虚拟网络和 VNI。
- 手动配置虚拟网络中的访问端口成员身份。
- 现有的路由协议可提供和了解对 VTEP 对等的基础可访问性。

但是，静态 VXLAN 和 BGP EVPN for VXLAN 与所述不同：

表. 49: 静态 VXLAN 与 VXLAN BGP EVPN 之间的差异

| 静态 VXLAN                                      | VXLAN BGP EVPN                                                                                 |
|-----------------------------------------------|------------------------------------------------------------------------------------------------|
| 要开始向远程 VTEP 发送和接收虚拟网络流量，请手动将 VTEP 配置为虚拟网络的成员。 | 无需执行手动配置。每个远程 VTEP 都将自动作为从远程 VTEP 接收的 EVPN 路由中的虚拟网络成员学习。学习远程 VTEP 地址后，VXLAN 流量将发送到 VTEP，并从中接收。 |
| 数据包在数据平面中的 VXLAN 标头解封后学习远程主机。                 | 在使用 BGP EVPN 类型 2 路由和 MAC/IP 通告的控制平面中学习远程主机 MAC 地址。                                            |

VXLAN BGP EVPN 操作

EVPN 地址系列允许 VXLAN 在外部边界网关协议 (eBGP) 和内部边界网关协议 (iBGP) 会话中传送 EVPN 路由。在数据中心网络中，在 IP 基础网络和 EVPN 中使用 eBGP 或 iBGP 进行路由交换。

以下 BGP EVPN 拓扑示例显示了分支-主干数据中心网络，其中 eBGP 在 IP 基础网络中交换 IP 路由，并在 VXLAN 覆盖网络中交换 EVPN 路由。所有主干节点均位于自治系统 — AS 65535。所有分支节点都位于另一个自治系统 — AS 65000。

要通告基础 IP 路由，请使用接口 IP 地址在分支节点和主干节点之间建立 eBGP 对等会话。要通告 EVPN 路由，分支和主干节点之间的 eBGP 对等会话使用环回 IP 地址。

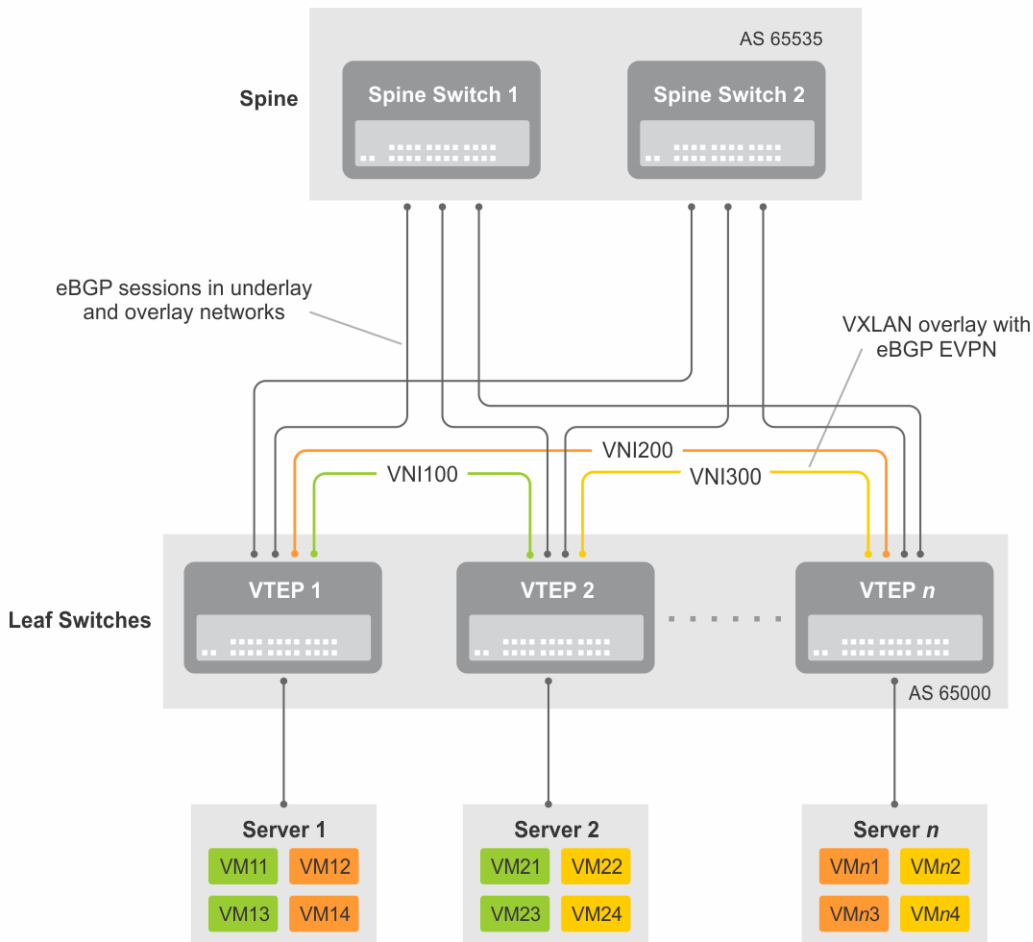


图 11: BGP EVPN 拓扑

分支节点

分支节点通常是数据中心网络中的架顶式 (ToR) 交换机。它们充当 VXLAN 隧道端点并执行 VXLAN 封装和解封。分支节点还将加入 MP BGP EVPN，以支持控制平面和数据平面功能。

控制平面功能包括：

- 使用基础网络中的任何路由协议启动并维护路由邻接。

- 向所有 MP-BGP EVPN 对等节点通告本地已知的路由。
- 处理从远程 MP-BGP EVPN 对等节点收到的路由，并将其安装在本地转发平面上。

数据平面功能包括：

- 使用 VXLAN 标头封装服务器流量，并将数据包转发到基础网络。
- 解封从远程 VTEP 接收的 VXLAN 数据包并将本机数据包转发到下游主机。
- 执行基础路由处理，包括基于外部 IP 地址的路由。

### 主干节点

主干节点的角色根据其控制平面和数据平面功能而变化。主干节点将加入基础路由处理以转发数据包，并加入覆盖网络以向所有 MP-BGP 对等节点通告 EVPN 路由。

控制平面功能包括：

- 与所有邻居分支节点发起 BGP 对等。
- BGP 路由将向所有 BGP 对等方通告。
- 通过基础网络中的所有分支和主干节点启动和维护路由邻接。

数据平面功能包括：

- 仅基于 VXLAN 封装数据包中的外部标头执行基础路由处理。
- 不执行 VXLAN 封装或解封。

在每个 VTEP 上运行的 BGP EVPN 将侦听本地叠加中的路由信息交换，将已知的路由编码为 BGP EVPN 路由，并将其插入 BGP 以向对等方通告。隧道端点通告为类型 3 EVPN 路由。MAC/IP 地址通告为类型 2 EVPN 路由。

### EVPN 实例

EVPN 实例 (EVI) 跨越了加入以太网 VPN 的 VTEP。使用 EVPN 通告的每个虚拟网络租户段必须与 EVI 相关联。在 OS10 中，在自动 EVI 或手动配置模式下配置 EVI。

- 自动 EVI — 在 VTEP 上配置虚拟网络后，自动 EVI 模式会自动创建 EVPN 实例。路由标识 (RD) 和路由目标 (RT) 值会自动生成：
  - EVI ID 自动生成的值与 VTEP 上配置的虚拟网络 ID (VNID) 相同，并与 VXLAN 网络 ID (VNI) 关联。
  - 路由标识将为每个 EVI ID 自动生成。路由标识将维护不同 EVPN 实例之间的 EVPN 路由的唯一性。
  - 路由目标导入和导出值将为每个 EVI ID 自动生成。路由目标将决定 EVPN 路由在 EVPN 实例之间的分布方式。
- 手动 EVI 配置 — 要指定 RD 和 RT 值，请手动配置 EVPN 实例并使用 VXLAN VNI 将每个 EVI 与叠加虚拟网络关联。仅当您配置虚拟网络、RD 和 RT 值时，EVI 才会激活。

在手动 EVI 配置中，您可以手动配置 RD 和 RT 或将其自动配置。

### 路由标识

RD 是唯一标识 EVI 的 8 字节标识符。每个 EVPN 路由都以唯一的 RD 为前缀，并在 BGP 对等方之间交换，使租户路由在网络中是唯一的。通过这种方法，支持租户之间的重叠地址空间。

您可以为每个 EVI 自动生成或手动配置 RD。在自动 EVI 模式下，RD 将自动生成。在手动 EVI 配置模式下，您可以自动生成或手动配置 RD。

如 RFC 7432 中所指定，手动配置的 RD 将采用以下格式进行编码：*4-octet-ipv4-address:2-octet-number* 自动生成的 RD 的格式为：*vtep-ip-address:evi*。

### 路由目标

当 RD 保持不同 EVI 之间的 EVPN 路由的唯一性时，RT 会控制 EVPN 路由在 EVI 之间的分布方式。每个 EVI 都配置有导入和导出 RT 值。EVI 的 BGP EVPN 路由将通告 EVI 携带与 EVI 相关联的导出 RT。接收 VTEP 会将 BGP EVPN 路由中的信息下载到具有匹配导入 RT 值的 EVI。

您可以为每个 EVI 自动生成或手动配置 RT 导入和导出。在自动 EVI 模式中，RT 将自动生成。在手动 EVI 配置模式下，您可以自动生成或手动配置 RT。

RT 包含 2-八字节 *type* 和 6-八字节 *value*。如果您自动配置 RT，则编码格式与 2 字节和 4 字节 AS 编号 (ASN) 不同：

- 对于 2 字节 ASN，RT *type* 设置为 0200 (在 RFC 4364 中为类型 0)。在 RFC 8365 的 5.1.2.1 部分中，RT 值的编码格式为：*2-octet-ASN: 4-octet-number*，其中以下值用于 *4-octet-number* 字段：
  - 类型：1
  - D-ID：0
  - 服务 ID：VNI
- 对于 4 字节 ASN，OS10 可以为 2 字节和 4 字节 ASN 自动配置 RT。RT *type* 设置为 0202 (在 RFC 4364 中为类型 2)。RT *value* 的编码格式为：*4-octet-ASN: 2-octet-number*，其中 *2-octet-number* 字段中包含 EVI ID。在自动 EVI 模式中，EVI ID 与虚拟网络 ID (VNID) 相同。因此，在 4 字节 ASN 部署中，如果所有 VTEP 上的 VNID 至 VNI 映射相同，则 OS10 支持 RT 自动配置。

## 为 VXLAN 配置 BGP EVPN

要在 VXLAN 覆盖网络中设置 BGP EVPN 服务，请执行以下操作：

1. 配置 VXLAN 覆盖网络。如果为 VXLAN 虚拟网络启用路由，将自动启用 BGP EVPN 的集成路由和桥接 (IRB)。有关详细信息，请参阅[配置 VXLAN](#)。
2. 配置 BGP 以通告 EVPN 路由。
3. 配置 EVPN，包括与 EVPN 实例关联的 VNI、RD 和 RT 值。
4. 验证 BGP EVPN 配置。

### 配置

1. 配置 BGP 以通告 EVPN 路由。

EVPN 要求您在基础网络中的分支节点和主干节点之间建立 MP BGP 会话。在每个主干和分支节点上，配置至少两个 BGP 对等会话：

- 基础网络中直接连接的 BGP 对等体，使用 IPv4 单播地址系列来通告 VTEP 和环回 IP 地址。
- 覆盖网络中的 BGP 对等体，用于使用 EVPN 地址系列通告覆盖信息。在覆盖网络中的 BGP 对等会话中，仅激活 EVPN 地址系列。

对于基础网络中的每个 BGP 对等会话：

- a. 在 CONFIGURATION 模式下创建 BGP 实例。您将进入路由器 BGP 配置模式。

```
router bgp as-number
```

- b. 在 ROUTER-BGP 模式下为 BGP 实例分配 IP 地址。

```
router-id ip-address
```

- c. 从 ROUTER-BGP 进入 IPv4 地址系列配置模式。

```
address-family ipv4 unicast
```

- d. 在 ROUTER-BGP-ADDRESS-FAMILY 模式下，向地址系列中的 BGP 对等体通告 IPv4 前缀。

```
network ip-address/mask
```

- e. 返回到 ROUTER-BGP 模式。

```
exit
```

- f. 在 ROUTER-BGP 模式下配置 BGP 对等体地址。

```
neighbor ip-address
```

- g. 在 ROUTER-BGP-NEIGHBOR 模式下将 BGP 邻居分配给自治系统。

```
remote-as as-number
```

- h. 在 ROUTER-BGP-NEIGHBOR 模式下启用与 BGP 邻居的对等会话。

```
no shutdown
```

- i. 返回到 ROUTER-BGP 模式。

```
exit
```

对于覆盖网络中的每个 BGP 对等会话：

- a. 使用在 ROUTER-BGP 模式下的 VTEP 上的环回 IP 地址配置 BGP 对等。

```
neighbor loopback-ip-address
```

- b. 为 ROUTER-BGP-NEIGHBOR 模式中的自治系统分配 BGP 邻居环回地址。邻居环回 IP 地址是远程 VTEP 上的源接口。

```
remote-as as-number
```

- c. 使用本地环回地址作为发送至 ROUTER-BGP-NEIGHBOR 模式下的邻居的 BGP 数据包中的源地址。

```
update-source loopback0
```

- d. 在 ROUTER-BGP-NEIGHBOR 模式下将扩展社区属性发送至 BGP 邻居。

```
send-community extended
```

- e. 在 ROUTER-BGP-NEIGHBOR 模式下启用与 BGP 邻居的对等会话。

```
no shutdown
```

- f. 配置 L2 VPN EVPN 地址系列，以便在路由器的 ROUTER-BGP-NEIGHBOR 模式下进行基于 VXLAN 主机的路由到 BGP 对等。

```
address-family l2vpn evpn
```

- g. 在 ROUTER-BGP-NEIGHBOR 模式下启用 L2VPN EVPN 地址与 BGP 邻居的交换。

```
activate
```

- h. 返回到 ROUTER-BGP 模式。

```
exit
```

- i. 从 ROUTER-BGP 进入 IPv4 地址系列配置模式。

```
address-family ipv4 unicast
```

- j. 在 ROUTER-BGP 模式下禁用与 BGP 对等主机的 IPv4 地址交换。

```
no activate
```

- k. 返回到 ROUTER-BGP-NEIGHBOR 模式。

```
exit
```

- l. (可选) 如果在同一 ASN 中配置了所有分支交换机：

- 在每个分支交换机上，从 ROUTER-BGP-NEIGHBOR 模式进入 L2VPN EVPN 地址系列配置模式。激活 L2VPN EVPN 地址与 BGP 对等主机的交换。配置交换机以接受在 ROUTER-BGP-NEIGHBOR-AF 模式下从对等方收到的更新中的路由和本地 AS 编号。

```
OS10(config-router-bgp-neighbor)# address-family l2vpn evpn
OS10(config-router-neighbor-af)# activate
OS10(config-router-neighbor-af)# allowas-in 1
OS10(config-router-neighbor-af)# exit
OS10(config-router-bgp-neighbor)# exit
```

- 在每个主干交换机上，在 ROUTER-BGP-NEIGHBOR-AF 模式中禁用到分支交换机邻近的发送方回路检测。

```
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no sender-side-loop-detection
OS10(conf-router-neighbor-af)# exit
```

- m. (可选) 在 VLT 部署中的每个分支交换机上，在 ROUTER-BGP-NEIGHBOR 模式下配置多跳对等路由的数量，以确保 BGP EVPN 对等会话在所有与主干交换机的本地链路关闭时通过 VLT VTEP 对等主机建立。

```
OS10(conf-router-neighbor)# ebgp-multihop 1
```

## 2. 配置 EVPN。

EVPN 实例 (EVI) 跨多个参与 EVPN 的 VTEP。在 OS10 中，在自动 EVI 或手动配置模式下配置 EVI。

### • 自动 EVI 模式

- a. 在 CONFIGURATION 模式下启用 EVPN 控制面板。

```
evpn
```

- b. 为 EVPN 模式下启用叠加虚拟网络的自动 EVI 创建。只有当 BGP EVPN 与 2 字节 AS 编号一起使用并且 EVPN 地址系列已启用至少一个 BGP 实例时，才支持自动 EVI 创建。不允许在自动 EVI 模式下进行进一步的手动配置。

```
auto-evi
```

### • 手动 EVI 配置模式

- a. 在 CONFIGURATION 模式下启用 EVPN 控制面板。

```
evpn
```

- b. 在 EVPN 模式中手动创建 EVPN 实例。范围是从 1 到 65535。

```
evi id
```

- c. 在 EVPN EVI 模式下配置路由区分器。

```
rd {A.B.C.D:[1-65535] | auto}
```

其中:

- o rd A.B.C.D:[1-65535] 使用 4 个八位字节 IPv4 地址配置 RD, 然后是 2 个八位字节数字。
- o rd auto 将自动生成 RD。

- d. 配置 EVPN EVI 模式下的 RT 值。

```
route-target {auto | value [asn4] {import | export | both}}
```

其中:

- o route-target auto 将自动为 EVPN 路由配置导入和导出值。
- o route-target value [asn4]{import | export | both} 以 2-octet-ASN:4-octet-number 或 4-octet-ASN:2-octet-number 格式为 EVPN 路由配置导入或导出值。
  - 2-octet ASN 编号为 1 到 65535。
  - 4-octet ASN 编号为 1 到 4294967295。

要为 RT 导入和导出值配置相同的值, 请使用 both 选项。asn4 将通告一个 2 字节 AS 编号作为 4 字节路由目标值。如果指定 asn4 选项, 请在 EVPN EVI 模式下配置与 EVPN 实例关联的 VXLAN 网络 ID, 从 1 到 16777215。配置为 VXLAN 虚拟网络配置的相同 VNI 值。有关详细信息, 请参阅[配置 VXLAN](#)。

```
vni vni
```

### 3. 验证 BGP EVPN 配置。

#### 显示 EVPN 实例配置

```
OS10# show evpn evi 1
EVI : 65447, State : up
 Bridge-Domain : (Virtual-Network)100, (VNI)100
 Route-Distinguisher : 1:110.111.170.102:65447(auto)
 Route-Targets : 0:101:268435556(auto) both
 Inclusive Multicast : 110.111.170.107
```

#### 显示 EVPN 实例的 VXLAN 叠加

```
OS10# show evpn vxlan-vni
VXLAN-VNI EVI Virtual-Network-Instance
100001 1 1
100010 2 2
```

#### 在 EVPN 实例中显示 BGP 邻居

```
OS10# show ip bgp neighbors 110.111.170.102
BGP neighbor is 110.111.170.102, remote AS 100, local AS 100 internal link
BGP version 4, remote router ID 110.111.170.102
BGP state ESTABLISHED, in this state for 04:02:59
Last read 00:21:21 seconds
Hold time is 180, keepalive interval is 60 seconds
Configured hold time is 180, keepalive interval is 60 seconds
Fall-over disabled

Received 311 messages
 2 opens, 2 notifications, 3 updates
 304 keepalives, 0 route refresh requests
Sent 307 messages
 4 opens, 0 notifications, 2 updates
 301 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
Minimum time before advertisements start is 0 seconds
```

```

Capabilities received from neighbor for IPv4 Unicast:
MULTIPROTO_EXT(1)
ROUTE_REFRESH(2)
CISCO_ROUTE_REFRESH(128)
4 OCTET AS(65)
MP_L2VPN_EVPN
Capabilities advertised to neighbor for IPv4 Unicast:
MULTIPROTO_EXT(1)
ROUTE_REFRESH(2)
CISCO_ROUTE_REFRESH(128)
4 OCTET AS(65)
MP_L2VPN_EVPN
Prefixes accepted 1, Prefixes advertised 1
Connections established 2; dropped 0
Last reset never
Prefixes ignored due to:
 Martian address 0, Our own AS in AS-PATH 0
 Invalid Nexthop 0, Invalid AS-PATH length 0
 Wellknown community 0, Locally originated 0

Local host: 110.111.180.195, Local port: 43081
Foreign host: 110.111.170.102, Foreign port: 179

```

## 显示 BGP L2VPN EVPN 地址系列

```

OS10# show ip bgp l2vpn evpn
BGP local RIB : Routes to be Added , Replaced , Withdrawn
BGP local router ID is 110.111.170.102
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed/network, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network Next Hop Metric LocPrf Weight Path
*>r Route distinguisher: 110.111.170.102:65447
[3]:[0]:[32]:[110.111.170.102]/152 110.111.170.102 0 100 32768 ?
*> Route distinguisher: 110.111.170.107:64536
[3]:[0]:[32]:[110.111.170.107]/152 110.111.170.107 0 100 0 100 101 ?

```

## 显示主机 MAC 地址的 EVPN 路由

```

OS10# show evpn mac
Type -(lcl): Local (rmt): remote

EVI Mac-Address Type Seq-No Interface/Next-Hop
50 00:00:00:aa:aa:aa rmt 0 55.1.1.3
50 00:00:00:cc:cc:cc lcl 0 ethernet1/1/8:1

OS10# show evpn mac evi 50
Type -(lcl): Local (rmt): remote

EVI Mac-Address Type Seq-No Interface/Next-Hop
50 00:00:00:aa:aa:aa rmt 0 55.1.1.3
50 00:00:00:cc:cc:cc lcl 0 ethernet1/1/8:1

```

## VXLAN BGP EVPN 路由

本部分介绍 EVPN 如何在与 VTEP 上属于同一个租户的 EVI 相关联的 L2 数据段之间实施覆盖路由。IETF draft draft-ietf-bess-evpn-inter-subnet-forwarding-05 介绍 evpn 子网间转发、集成的路由和桥接 (IRB) 以及如何在 L2 租户域之间使用 IP 路由。

您可以通过为每个租户分配 VRF、创建虚拟网络接口和将 VRF 中的 IP 子网分配给每个虚拟网络接口来设置覆盖路由。VTEP 充当 L3 网关，在将流量封装在 VXLAN 标头之前将流量从一个租户子网路由到另一个租户子网，并将其通过基础结构进行传输。在与 EVI 关联的虚拟网络上，仅在创建虚拟网络接口后启用 EVPN IRB。

为虚拟网络/EVI 启用 IRB 时，每个 VTEP 上的 EVPN 操作还会向所有其他 EVPN 通告已启用 VTEP 的虚拟网络上获知的本地租户 IP MAC 绑定。本地租户 IP MAC 绑定可从 ARP 或 ICMPv6 协议操作获知。它们作为 EVPN 类型 2 BGP 路由更新通告给其他 VTEP，每个客户端都会在数据平面中将其导入和安装为 ARP/IPv6 邻居条目。

要在 VTEP 上启用高效的流量转发，OS10 支持分布式网关路由。分布式网关允许多个 VTEP 充当租户子网的网关路由器。最接近主机的 VTEP 用作其网关路由器。



要为 BGP EVPN 启用 L3 网关/IRB 功能，请配置 VXLAN 覆盖网络并在交换机上启用路由：

1. 为覆盖路由创建非默认的 VRF 实例。对于多租户，请为每个租户创建 VRF 实例。
2. 全局配置所有 VTEP 使用的任意广播网关 MAC 地址。
3. 针对每个虚拟网络配置虚拟网络接口，（可选）将其分配给租户 VRF 并配置 IP 地址。然后启用该接口。
4. 为每个虚拟网络配置任意广播网关 IP 地址。OS10 支持分布式网关路由。

对于连接到每个 VTEP 的租户、虚拟机和服务器的，EVPN 支持不同类型的 IRB 路由：

- 集中式路由：对于每个租户子网，将一个 VTEP 指定为 L3 网关，以执行 IRB 间子网路由。所有其他 VTEP 执行 L2 桥接。
- 分布式路由：对于每个租户子网，所有 VTEP 都会为连接到 VTEP 的租户 VM 和服务器的执行 L3 网关路由。在大型多租户网络中，分布式路由允许更高效的带宽使用和流量转发。IRB 路由的执行方式如下：
  - 仅在入口 VTEP 上。
  - 在入口和出口 VTEP 上。

## 非对称 IRB 路由

在非对称 IRB 路由中，IRB 路由仅在入口 VTEP 上执行。出口 VTEP 在租户子网中执行 L2 桥接。

入口 VTEP 直接将数据包路由到目标虚拟网络 VNI 中的目标主机 MAC 地址。出口 VTEP 仅通过删除 VXLAN 标头并将数据包转发到本地第二层域（使用 VNI 到 VLAN 映射）将数据包发送到主机。

入口 VTEP 配置有所有目标虚拟网络，并且其硬件表中的所有目标主机都具有 ARP 条目和 MAC 地址。每个 VTEP 使用本地地址 ARP 侦听以及来自远程 VTEP 的类型 2 路由通告来了解主机 MAC 和 MAC 到 IP 的绑定。

对于使用非对称 IRB 的 VXLAN BGP EVPN 示例，请参阅[示例：VXLAN 和 BGP EVPN](#)，[示例：VXLAN BGP EVPN — 多 AS 拓扑](#)。

## BGP EVPN 和 VLT

OS10 在您配置为 VTEP 的 VLT 对等节点之间支持 BGP EVPN 操作。有关设置 VLT for VXLAN 的配置和妥善做法的详细信息，请参阅[配置 VXLAN — 配置 VLT](#)。此信息也应用于 BGP EVPN for VXLAN。

当到基础 L3 网络的连接丢失时，Dell EMC 建议为专用 L3 VLAN 上 VLT 对中 VTEP 之间的 IPv4 地址系列配置 iBGP 对等互连。不需要在 VLT 对中 VTEP 之间的 iBGP 对等会话上启用 EVPN 地址系列，因为在环回接口上将执行 EVPN 与主干交换机之间的对等互连。

VLT 对中的两个 VTEP 均通告相同的 EVPN 路由，如果其中一个 VTEP 对等节点发生故障，则会提供冗余。要设置冗余 EVPN 路由通告，请针对 VLT 对中两个 VTEP 上的每个 VNI 配置相同的 EVI、RD 和 RT 值，包括：

- 在自动 EVI 模式下，如果两个 VTEP 对等节点上的 VNID 至 VNI 关联相同，则会自动确保这一相同的配置。
- 在手动 EVI 模式下，您必须在两个 VTEP 对等节点上配置相同的 EVI 至 VNID 关联。
- 在手动 EVI 模式下，您必须在两个 VTEP 对等节点上配置相同的 RD 和 RT 值。

在 EVPN 配置中，增加 VLT 延迟恢复计时器，以允许建立 BGP EVPN 邻接并允许通过 EVPN 下载远程 MAC 和邻居条目以及安装在数据平面。VLT 延迟还原将确定 VLT LAG 在启动时保持运行状态的时间，以允许数据平面设置和转发流量，从而在 VLT 对等节点启动并加入 VLT 域时最小化流量损失。

有关 BGP EVPN VLT 配置示例，请参阅[示例：VXLAN 和 BGP EVPN](#)。

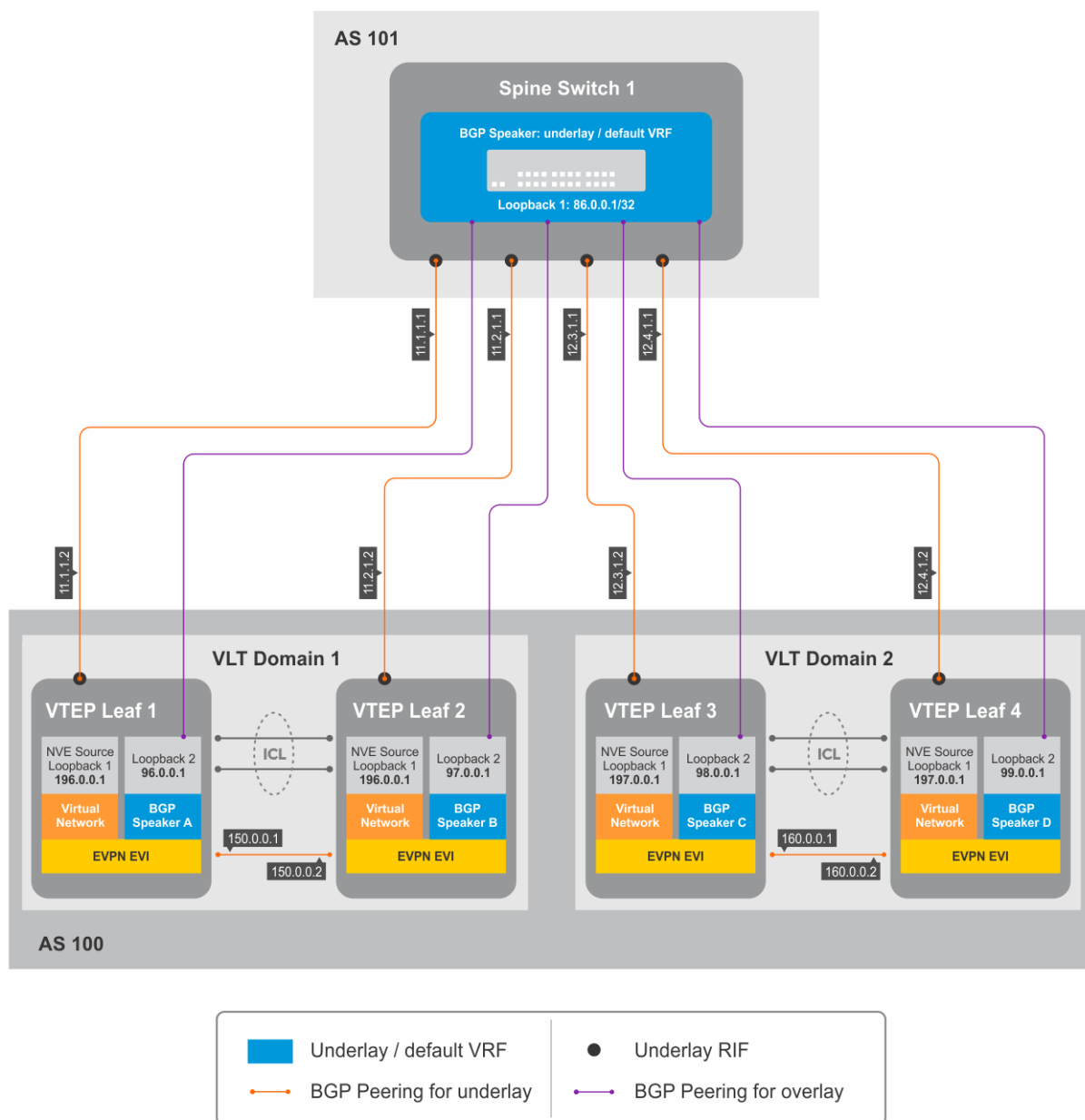


图 12: VLT 域中的 BGP EVPN

## VXLAN BGP 命令

### 激活 (l2vpn evpn)

使用 BGP 邻居或对等组启用 L2 VPN EVPN 地址系列信息的交换。

语法 activate

参数 无

默认 未配置

命令模式 ROUTER-BGP-NEIGHBOR-AF

使用情况信息 使用此命令可以为具有 BGP 邻居的基于 VXLAN 主机的路由交换 L2 VPN EVPN 地址信息。默认情况下，IPv4 单播地址系列已启用。使用此命令的 no 版本可禁用带有邻居的地址系列。

## 示例

```
OS10(config-router-neighbor)# address-family l2vpn evpn unicast
OS10(config-router-bgp-neighbor-af)# activate
```

**支持的版本** 10.2.0E or later

## address-family l2vpn evpn

配置 L2 VPN EVPN 地址系列，以用于基于 VXLAN 主机的路由到 BGP 邻居。

**语法** address-family l2vpn evpn

**参数** 无

**默认** 未配置

**命令模式** ROUTER-NEIGHBOR

**使用情况信息** 要在 VXLAN 中使用 BGP EVPN 服务，必须在 VTEP 上配置和启用 L2VPN EVPN 地址系列，以支持基于主机的路由到每个 BGP 邻居。

## 示例

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 45.0.0.1
OS10(config-router-neighbor)# address-family l2vpn evpn
```

**支持的版本** 10.4.2.0 or later

## allowas-in

配置在交换机拒绝路由之前，本地 AS 编号在 BGP AS\_PATH 路径属性中可以出现的次数。

**语法** allowas-in as-number

**参数** as-number— 输入局部变量的次数，从 1 到 10。

**默认** 已禁用

**命令模式** ROUTER-BPG-NEIGHBOR-AF

**使用情况信息** 使用此命令可启用 BGP 扬声器，以接受更新中对等体收到的指定次数的本地 AS 数字。此命令的 no 版本会将该值重置为默认值。

## 示例 (IPv4)

```
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# allowas-in 5
```

## 示例 (IPv6)

```
OS10(config-router-template)# address-family ipv6 unicast
OS10(config-router-bgp-template-af)# allowas-in 5
```

**支持的版本** 10.3.0E or later

## sender-side-loop-detection

为 BGP 邻居启用发送方回路检测过程。

**语法** sender-side-loop-detection

**参数** 无

**默认** 已启用

**命令模式** ROUTER-BGP-NEIGHBOR-AF

**使用情况信息** 在开始通告路由之前，此命令可帮助根据 AS 路径检测路由环路。要将邻居配置为接受路由，请使用 neighbor allowas-in 命令。此命令的 no 版本将禁用该邻居的发送方回路检测。

示例 (IPv4)

```
OS10(conf-router-bgp-102)# neighbor 3.3.3.1
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-bgp-neighbor-af)# sender-side-loop-detection
```

示例 (IPv6)

```
OS10(conf-router-bgp-102)# neighbor 32::1
OS10(conf-router-neighbor)# address-family ipv6 unicast
OS10(conf-router-bgp-neighbor-af)# no sender-side-loop-detection
```

支持的版本 10.3.0E or later

show ip bgp l2vpn evpn

显示 EVPN 实例中 L2VPN EVPN 地址系列中的内部 BGP 路由。

语法 show ip bgp l2vpn evpn [summary | neighbors [ip-address]]

- 参数
- summary** 显示 L2VPN 地址系列中与远程 VTEP 交换的 BGP 路由的摘要。
  - neighbors** 显示与 L2VPN 地址系列交换中的 BGP 路由的远程 VTEP。
  - ip-address** 显示有关特定邻居的信息。
  - interface** 显示通过未编号的邻居获知的 BGP 信息。
  - interface-type**

默认 未配置

命令模式 EXEC

使用情况信息 使用此命令可显示交换机上 EVPN 实例中用于 L2VPN EVPN 地址系列的 BGP 路由。

示例

```
OS10# show ip bgp l2vpn evpn
BGP local RIB : Routes to be Added , Replaced , Withdrawn
BGP local router ID is 110.111.170.102
Status codes: s suppressed, S stale, d dampened, h history, * valid, >
best
Path source: I - internal, a - aggregate, c - confed-external,
r - redistributed/network, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf
Weight Path
*>r Route distinguisher: 110.111.170.102:65447
[3]:[0]:[32]:[110.111.170.102]/152 110.111.170.102 0 100
32768 ?
*> Route distinguisher: 110.111.170.107:64536
[3]:[0]:[32]:[110.111.170.107]/152 110.111.170.107 0 100
0 100 101 ?
```

```
OS10# show ip bgp l2vpn evpn summary
BGP router identifier 2.2.2.2 local AS number 4294967295
Neighbor AS MsgRcvd MsgSent Up/Down State/
Pfx
3.3.3.3 4294967295 2831 9130 05:57:27 504
4.4.4.4 4294967295 2364 9586 05:56:43 504
5.5.5.5 4294967295 4947 8399 01:10:39 11514
6.6.6.6 4294967295 2413 7310 05:51:56 504
```

```
OS10# show ip bgp l2vpn evpn neighbors
BGP neighbor is 3.3.3.3, remote AS 4294967295, local AS 4294967295
internal link

BGP version 4, remote router ID 3.3.3.3
BGP state ESTABLISHED, in this state for 06:21:55
Last read 00:37:43 seconds
```

```

Hold time is 180, keepalive interval is 60 seconds
Configured hold time is 180, keepalive interval is 60 seconds
Fall-over disabled
Route reflector client

Received 2860 messages
 1 opens, 0 notifications, 2422 updates
 437 keepalives, 0 route refresh requests
Sent 32996 messages
 1 opens, 0 notifications, 32565 updates
 430 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv4 Unicast:
 ROUTE_REFRESH(2)
 CISCO_ROUTE_REFRESH(128)
 4 OCTET AS(65)
 MP_L2VPN_EVPN(1)
Capabilities advertised to neighbor for IPv4 Unicast:
 ROUTE_REFRESH(2)
 CISCO_ROUTE_REFRESH(128)
 4 OCTET AS(65)
 MP_L2VPN_EVPN(1)
Prefixes accepted 504, Prefixes advertised 13012
Connections established 1; dropped 0
Last reset never
Local host: 2.2.2.2, Local port: 37853
Foreign host: 3.3.3.3, Foreign port: 179
...

```

**支持的版本** 10.4.2.0 or later

## VXLAN EVPN 命令

### auto-evi

自动创建 EVPN 实例，包括路由标识符 (RD) 和路由目标 (RT) 值。

**语法** auto-evi

**参数** 无

**默认** 未配置

**命令模式** EVPN

**使用情况信息** 在运行 BGP 和 2 字节或 4 字节自治系统的部署中，当您在覆盖网络专供的 VTEP 上创建虚拟网络时，自动 EVI 将自动创建 EVPN 实例。在自动 EVI 模式下，RD 和 RT 值会自动生成：

- 对于 2 字节自治系统：
  - RD 自动配置为覆盖网络源 IP 地址和自动生成的 EVI 索引中的类型 1。
  - RT 自动配置为 2 字节 AS 与 3 字节 VNI 的类型 0 — 类型编码为 0x0002。
- 对于 4 字节自治系统：
  - RD 自动配置为覆盖网络源 IP 地址和自动生成的 EVI 索引中的类型 1。
  - RT 自动配置为 4 字节 AS 与 2 字节 EVI 的类型 2 — 类型编码为 0x0202。

### 示例

```

OS10(config)# evpn
OS10(config-evpn)# auto-evi

```

**支持的版本** 10.4.2.0 or later

## evi

在 EVPN 模式下创建 EVPN 实例 (EVI)。

|        |                                                                                                                              |                             |
|--------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| 语法     | <code>evi id</code>                                                                                                          |                             |
| 参数     | <code>id</code>                                                                                                              | 输入 EVPN 实例 ID, 从 1 到 65535。 |
| 默认     | 未配置                                                                                                                          |                             |
| 命令模式   | EVPN                                                                                                                         |                             |
| 使用情况信息 | 如果 MP BGP 网络使用 4 字节自治系统或指定 RD 和 RT 值, 请手动配置 EVPN 实例并将每个 EVI 与叠加 VXLAN 虚拟网络关联。仅当您配置 VXLAN 网络 ID (VNI)、RD、RT 和虚拟网络时, EVI 才会激活。 |                             |
| 示例     | <pre>OS10(config)# evpn OS10(config-evpn)# evi 10 OS10(config-evpn-evi)#</pre>                                               |                             |
| 支持的版本  | 10.4.2.0 or later                                                                                                            |                             |

## evpn

为 VXLAN 启用 EVPN 控制平面。

|        |                                                                                                              |  |
|--------|--------------------------------------------------------------------------------------------------------------|--|
| 语法     | <code>evpn</code>                                                                                            |  |
| 参数     | 无                                                                                                            |  |
| 默认     | 未配置                                                                                                          |  |
| 命令模式   | CONFIGURATION                                                                                                |  |
| 使用情况信息 | 启用 EVPN 会触发 BGP 将 EVPN 功能与 AFI = 25 和 SAFI = 70 一起通告到自治系统中的所有 BGP 对等节点。此命令的 <code>no</code> 版本将禁用交换机上的 EVPN。 |  |
| 示例     | <pre>OS10(config)# evpn OS10(config-evpn)#</pre>                                                             |  |
| 支持的版本  | 10.4.2.0 or later                                                                                            |  |

## rd

配置 EVPN 路由使用的路由标识 (RD) 值。

|        |                                                                                                               |                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 语法     | <code>rd {A.B.C.D:[1-65535]   auto}</code>                                                                    |                                                                             |
| 参数     | <code>A.B.C.D:</code><br><code>[1-65535]</code><br><code>auto</code>                                          | 使用 4 个八位字节 IPv4 地址手动配置 RD, 然后是从 1 到 65535 的 2 个八位字节数字。<br><br>将 RD 配置为自动生成。 |
| 默认     | 未配置                                                                                                           |                                                                             |
| 命令模式   | EVPN-EVI 和 EVPN-VRF                                                                                           |                                                                             |
| 使用情况信息 | RD 在不同 EVPN 实例之间保持 EVPN 路由的唯一性。在用于 EVPN 对称 IRB 流量的租户 VRF 中配置路由标识。RD 自动配置为覆盖网络源 IP 地址和自动生成的 EVPN 实例 ID 中的类型 1。 |                                                                             |
| 示例     | <pre>OS10(config)# evpn OS10(config-evpn)# evi 10</pre>                                                       |                                                                             |

```
OS10(config-evpn-evi)# vni 10000
OS10(config-evpn-evi)# rd 111.111.111.111:65535
```

```
OS10(config)# evpn
OS10(config-evpn)# vrf vrf-blue
OS10(config-evpn-vrf-vrf-blue)# rd 111.111.111.111:65000
```

**支持的版本** 10.4.2.0 or later

## route-target

配置 EVPN 路由使用的路由目标 (RT) 值。

**语法** route-target {auto | value {import | export | both} [asn4]}

**参数**

|                                       |                                                                                                                                           |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>value {import   export   both}</b> | 以 <i>2-octet-ASN:4-octet-number</i> 或 <i>4-octet-ASN:2-octet-number</i> 格式配置 RT 导入或导出值或两个值。                                               |
|                                       | <ul style="list-style-type: none"> <li>• <i>2-octet</i> ASN 或编号为 1 到 65535。</li> <li>• <i>4-octet</i> ASN 或编号为 1 到 4294967295。</li> </ul> |
| <b>auto</b>                           | 将 RT 导入和导出值配置为自动生成。                                                                                                                       |
| <b>asn4</b>                           | (可选) 在 RT 值中通告 4 字节 AS 编号。                                                                                                                |

**默认** 未配置

**命令模式** EVPN-EVI 和 EVPN-VRF

**使用情况信息** RT 确定了 EVPN 路由在 EVPN 实例之间的分布方式。使用导入和导出值配置每个 RT。当 EVPN 路由通告时，为导出配置的 RT 导出值会连接到每个路由。接收 VTEP 将路由导出值与本地 RT 导入值进行比较。如果值匹配，路由将下载并安装在 VTEP 上。

- 对于 2 字节自治系统，RT 从 2 字节 AS 和 3 字节 VNI 自动配置为类型 0 — 类型编码为 0x0002。
- 对于 4 字节自治系统，RT 从 4 字节 AS 和 2 字节 EVI 自动配置为类型 2 — 类型编码为 0x0202。

在租户 VRF 中配置用于 EVPN 对称 IRB 流量的路由目标。

**示例**

```
OS10(config)# evpn
OS10(config-evpn)# evi 10
OS10(config-evpn-evi)# vni 10000
OS10(config-evpn-evi)# rd 111.111.111.111:65535
OS10(config-evpn-evi)# route-target 1:3 both
```

```
OS10(config)# evpn
OS10(config-evpn)# vrf vrf-blue
OS10(config-evpn-vrf-vrf-blue)# route-target auto
```

**支持的版本** 10.4.2.0 or later

## show evpn evi

显示 EVPN 实例的配置设置。

**语法** show evpn evi [id]

**参数** id — (可选) 输入 EVPN 实例 ID，从 1 到 65535。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 使用此命令可以验证 EVPN 实例状态、关联的 VXLAN 虚拟网络以及 BGP EVPN 路由在 EVI 中使用的 RD 和 RT 值。此外，还会显示集成路由和桥接 (IRB) 的状态和用于 EVPN 流量的 VRF。

示例

```
OS10# show evpn evi 101
EVI : 101, State : up
 Bridge-Domain : Virtual-Network 101, VNI 101
 Route-Distinguisher : 1:95.0.0.4:101(auto)
 Route-Targets : 0:101:268435556(auto) both
 Inclusive Multicast : 95.0.0.3
 IRB : Enabled(VRF: default)
```

支持的版本 10.4.2.0 or later

show evpn mac

显示主机 MAC 地址的 BGP EVPN 路由。

语法

```
show evpn mac {count | mac-address nn.nn.nn.nn | evi id [mac-address
nn.nn.nn.nn | count | next-hop ip-address count]}
```

参数

- count — 显示 EVPN 实例中的本地和远程主机 MAC 地址的总数。
- mac-address nn.nn.nn.nn — 显示特定 48 位主机 MAC 地址的 BGP EVPN 路由。
- evi id — 显示指定 EVPN 实例中的主机 MAC 地址和下一跳，从 1 到 65535。要筛选输出，请显示 EVPN ID 或下一中继站 IP 地址的主机的信息 MAC 地址计数，以及指定 MAC 地址的 BGP 路由。

默认

未配置

命令模式

EXEC

使用情况信息

使用此命令可显示 EVPN 实例中的主机 MAC 地址的 BGP 路由。

示例

```
OS10# show evpn mac
Type -(lcl): Local (rmt): remote

EVI Mac-Address Type Seq-No Interface/Next-Hop
50 00:00:00:aa:aa:aa rmt 0 55.1.1.3

OS10# show evpn mac count

Total MAC Entries :
 Local MAC Address Count : 2
 Remote MAC Address Count : 5

OS10# show evpn mac evi 811 count

EVI 811 MAC Entries :
 Local MAC Address Count : 1
 Remote MAC Address Count : 2

OS10# show evpn mac evi 811 next-hop 80.80.1.8 count

EVI 811 next-hop 80.80.1.8 MAC Entries :
 Remote MAC Address Count : 2
```

支持的版本 10.4.2.0 or later

show evpn mac-ip

显示用于主机 MAC IP 地址绑定的 BGP EVPN 类型 2 路由。

语法

```
show evpn mac-ip [count | evi evi [mac-address mac-address] | mac-address
mac-address | next-hop ip-address]
```

参数

- count — 显示 EVPN 中的 MAC 地址总数 MAC IP 地址绑定。



- `evi evi` — 输入 EVPN 实例 ID, 从 1 到 65535。
- `host ip-address` — 输入通过 EVPN 路由进行通信的主机的 IP 地址。
- `mac-address mac-address` — 输入通过 EVPN 路由 (采用格式 `nn:nn:nn:nn:nn`) 进行通信的主机的 MAC 地址。
- `next-hop ip-address` — 输入下一跳交换机的 IP 地址。

默认

命令模式

使用情况信息

示例

未配置

EXEC

使用此命令查看 VXLAN 租户段中的主机通信的 MAC IP 地址绑定。

```
OS10# show evpn mac-ip
```

```
Type -(lcl): Local (rmt): remote
```

| EVI | Mac-Address       | Type | Seq-No | Host-IP       | Interface/Next-Hop |
|-----|-------------------|------|--------|---------------|--------------------|
| 101 | 14:18:77:0c:e5:a3 | rmt  | 0      | 11.11.11.3    | 95.0.0.5           |
| 101 | 14:18:77:0c:e5:a3 | rmt  | 0      | 2001:11::11:3 | 95.0.0.5           |
| 101 | 14:18:77:25:4e:84 | rmt  | 0      | 55.55.55.1    | 95.0.0.3           |
| 101 | 14:18:77:25:6f:84 | lcl  | 0      | 11.11.11.2    |                    |
| 101 | 14:18:77:25:6f:84 | lcl  | 0      | 2001:11::11:2 |                    |
| 102 | 14:18:77:0c:e5:a4 | rmt  | 0      | 12.12.12.3    | 95.0.0.5           |
| 102 | 14:18:77:0c:e5:a4 | rmt  | 0      | 2001:12::12:3 | 95.0.0.5           |
| 102 | 14:18:77:25:4d:b9 | rmt  | 0      | 12.12.12.1    | 95.0.0.3           |
| 102 | 14:18:77:25:6e:b9 | lcl  | 0      | 12.12.12.2    |                    |
| 103 | 14:18:77:25:4e:84 | rmt  | 0      | 13.13.13.1    | 95.0.0.3           |
| 103 | 14:18:77:25:4e:84 | rmt  | 0      | 2001:13::13:1 | 95.0.0.3           |
| 103 | 14:18:77:25:6f:84 | lcl  | 0      | 13.13.13.2    |                    |
| 103 | 14:18:77:25:6f:84 | lcl  | 0      | 2001:13::13:2 |                    |
| 104 | 14:18:77:25:4d:b9 | rmt  | 0      | 14.14.14.1    | 95.0.0.3           |
| 104 | 14:18:77:25:4d:b9 | rmt  | 0      | 2001:14::14:1 | 95.0.0.3           |
| 104 | 14:18:77:25:6e:b9 | lcl  | 0      | 14.14.14.2    |                    |
| 104 | 14:18:77:25:6e:b9 | lcl  | 0      | 2001:14::14:2 |                    |
| 105 | 14:18:77:25:4d:b9 | rmt  | 0      | 15.15.15.1    | 95.0.0.3           |
| 105 | 14:18:77:25:4d:b9 | rmt  | 0      | 2001:15::15:1 | 95.0.0.3           |
| 105 | 14:18:77:25:6e:b9 | lcl  | 0      | 15.15.15.2    |                    |
| 105 | 14:18:77:25:6e:b9 | lcl  | 0      | 2001:15::15:2 |                    |
| 106 | 14:18:77:25:4e:84 | rmt  | 0      | 16.16.16.1    | 95.0.0.3           |
| 106 | 14:18:77:25:4e:84 | rmt  | 0      | 2001:16::16:1 | 95.0.0.3           |
| 106 | 14:18:77:25:6f:84 | lcl  | 0      | 16.16.16.2    |                    |
| 106 | 14:18:77:25:6f:84 | lcl  | 0      | 2001:16::16:2 |                    |

```
OS10# show evpn mac-ip evi 104
```

```
Type -(lcl): Local (rmt): remote
```

| EVI | Mac-Address       | Type | Seq-No | Host-IP       | Interface/Next-Hop |
|-----|-------------------|------|--------|---------------|--------------------|
| 104 | 14:18:77:25:4d:b9 | rmt  | 0      | 14.14.14.1    | 95.0.0.3           |
| 104 | 14:18:77:25:4d:b9 | rmt  | 0      | 2001:14::14:1 | 95.0.0.3           |
| 104 | 14:18:77:25:6e:b9 | lcl  | 0      | 14.14.14.2    |                    |
| 104 | 14:18:77:25:6e:b9 | lcl  | 0      | 2001:14::14:2 |                    |

```
OS10# show evpn mac-ip evi 101 mac-address 14:18:77:0c:e5:a3
```

```
Type -(lcl): Local (rmt): remote
```

| EVI | Mac-Address       | Type | Seq-No | Host-IP       | Interface/Next-Hop |
|-----|-------------------|------|--------|---------------|--------------------|
| 101 | 14:18:77:0c:e5:a3 | rmt  | 0      | 11.11.11.3    | 95.0.0.5           |
| 101 | 14:18:77:0c:e5:a3 | rmt  | 0      | 2001:11::11:3 | 95.0.0.5           |

```
OS10# show evpn mac-ip mac-address 14:18:77:25:4e:84
```

```
Type -(lcl): Local (rmt): remote
```

| EVI | Mac-Address | Type | Seq-No | Host-IP | Interface/Next-Hop |
|-----|-------------|------|--------|---------|--------------------|
|-----|-------------|------|--------|---------|--------------------|

|     |                   |     |   |               |          |
|-----|-------------------|-----|---|---------------|----------|
| 101 | 14:18:77:25:4e:84 | rmt | 0 | 55.55.55.1    | 95.0.0.3 |
| 103 | 14:18:77:25:4e:84 | rmt | 0 | 13.13.13.1    | 95.0.0.3 |
| 103 | 14:18:77:25:4e:84 | rmt | 0 | 2001:13::13:1 | 95.0.0.3 |
| 106 | 14:18:77:25:4e:84 | rmt | 0 | 16.16.16.1    | 95.0.0.3 |
| 106 | 14:18:77:25:4e:84 | rmt | 0 | 2001:16::16:1 | 95.0.0.3 |

**支持的版本** 10.4.3.0 or later

## show evpn vrf

显示用于在 VXLAN 覆盖网络中转发 EVPN 路由的 VRF 实例。

**语法** `show evpn vrf [vrf-name]`

**参数** `vrf-name` — (可选) 输入非默认租户 VRF 实例的名称。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 使用此命令可以验证在 EVPN 实例中用于在 VXLAN 中交换 BGP EVPN 路由的租户 VRF 实例。

**示例**

```
show evpn vrf
```

| VXLAN-VNI | EVI | Virtual-Network-Instance | VRF-Name |
|-----------|-----|--------------------------|----------|
| 102       | 102 | 102                      | blue     |
| 103       | 103 | 103                      | default  |
| 104       | 104 | 104                      | blue     |
| 106       | 106 | 106                      | default  |
| 105       | 105 | 105                      | blue     |
| 101       | 101 | 101                      | default  |

**支持的版本** 10.4.3.0 or later

## show evpn vxlan-vni

显示 EVPN 实例的 VXLAN 覆盖网络。

**语法** `show evpn vxlan-vni [vni]`

**参数** `vni` — (可选) 输入 VXLAN 虚拟网络 ID, 从 1 到 16777215。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 使用此命令可以验证 EVPN 实例使用的 VXLAN 虚拟网络和桥域。

**示例**

```
OS10# show evpn vxlan-vni
```

| VXLAN-VNI | EVI   | Bridge-Domain |
|-----------|-------|---------------|
| 100       | 65447 | 65447         |

**支持的版本** 10.4.2.0 or later

## 示例：VXLAN 和 BGP EVPN

以下带有 BGP EVPN 的 VXLAN 示例使用 Clos 分支-主干拓扑和 VXLAN 隧道端点 (VTEP)。单个交换机配置显示如何设置端到端 VXLAN。eBGP 用于交换 IP 承载网络中的 IP 路由和 VXLAN 覆盖网络中的 EVPN 路由。所有主干节点均位于自治系统 — AS 101。所有分支节点都位于另一个自治系统 — AS 100。

- 在 VTEP 1 和 2 上：使用交换机限定的 VLAN 将访问端口分配给虚拟网络。EVPN 使用自动 EVI 模式进行配置。
- 在 VTEP 3 和 4 上：使用端口限定的 VLAN 将访问端口分配给虚拟网络。使用手动配置模式来配置 EVPN 实例。使用自动模式配置 RD 和 RT。

所有 VTEP 执行非对称 IRB 路由，其中：

- IRB 路由仅在入口 VTEP 上执行。
- 出口 VTEP 执行 IRB 桥接。

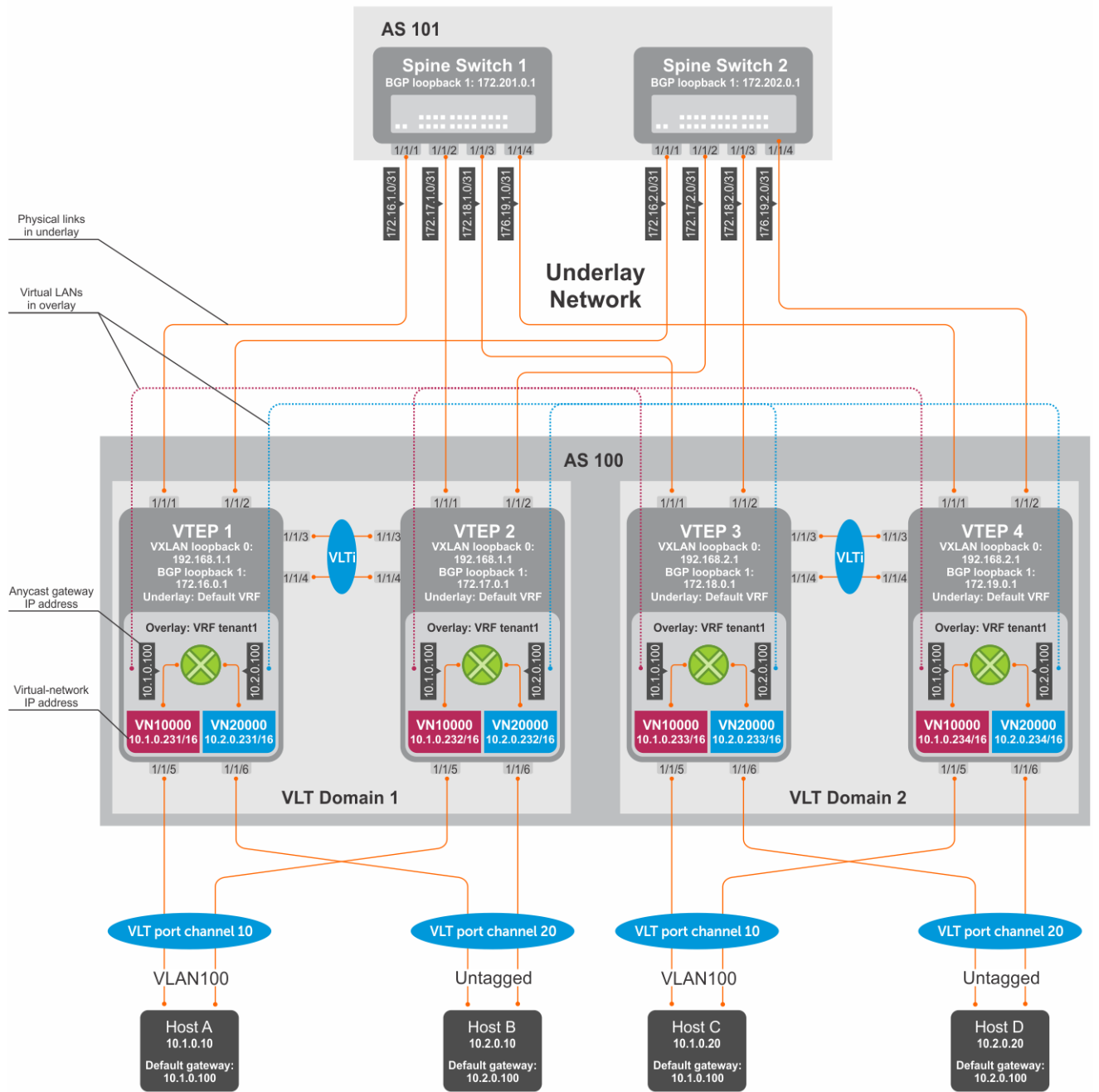


图 13: VXLAN BGP EVPN 使用情形

## VTEP 1 分支交换机

### 1. 使用与 VLT 对等方相同的 IP 地址为承载 VXLAN 配置环回接口

```
OS10(config)# interface loopback0
OS10(conf-if-lo-0)# no shutdown
OS10(conf-if-lo-0)# ip address 192.168.1.1/32
OS10(conf-if-lo-0)# exit
```

## 2. 将环回接口配置为 VXLAN 源隧道接口

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback0
OS10(config-nve)# exit
```

## 3. 配置 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vxlan-vni 10000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vxlan-vni 20000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-20000)# exit
```

## 4. 将 VLAN 成员接口分配给虚拟网络

使用交换机限定的 VLAN 到 VNI 映射：

```
OS10(config)# interface vlan100
OS10(config-if-vl-100)# virtual-network 10000
OS10(config-if-vl-100)# no shutdown
OS10(config-if-vl-100)# exit
OS10(config)# interface vlan200
OS10(config-if-vl-200)# virtual-network 20000
OS10(config-if-vl-200)# no shutdown
OS10(config-if-vl-200)# exit
```

## 5. 针对交换机限定的 VLAN 至 VNI 映射将访问端口配置为 VLAN 成员

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode trunk
OS10(conf-if-po-10)# switchport trunk allowed vlan 100
OS10(conf-if-po-10)# no switchport access vlan
OS10(conf-if-po-10)# exit

OS10(config)# interface ethernet1/1/5
OS10(conf-if-eth1/1/5)# no shutdown
OS10(conf-if-eth1/1/5)# channel-group 10 mode active
OS10(conf-if-eth1/1/5)# no switchport
OS10(conf-if-eth1/1/5)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# no shutdown
OS10(conf-if-po-20)# switchport mode trunk
OS10(conf-if-po-20)# switchport access vlan 200
OS10(conf-if-po-20)# exit

OS10(config)# interface ethernet1/1/6
OS10(conf-if-eth1/1/6)# no shutdown
OS10(conf-if-eth1/1/6)# channel-group 20 mode active
OS10(conf-if-eth1/1/6)# no switchport
OS10(conf-if-eth1/1/6)# exit
```

## 6. 配置面向上游网络的端口

```
OS10(config)# interface ethernet1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/1)# ip address 172.16.1.0/31
OS10(conf-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# mtu 1650
```

```
OS10(config-if-eth1/1/2)# ip address 172.16.2.0/31
OS10(config-if-eth1/1/2)# exit
```

## 7. 配置 eBGP

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# router-id 172.16.0.1
OS10(config-router-bgp-100)# address-family ipv4 unicast
OS10(config-router-bgp-af)# redistribute connected
OS10(config-router-bgp-af)# exit
```

## 8. 针对 IPv4 点对点等配置 eBGP

```
OS10(config-router-bgp-100)# neighbor 172.16.1.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-100)# neighbor 172.16.2.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 9. 为 BGP EVPN 对等配置与 VLT 对等方 IP 地址不同的环回接口

```
OS10(config)# interface loopback1
OS10(config-if-lo-1)# no shutdown
OS10(config-if-lo-1)# ip address 172.16.0.1/32
OS10(config-if-lo-1)# exit
```

## 10. 配置 BGP EVPN 对等

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172.201.0.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-100)# neighbor 172.202.0.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 11. 配置 EVPN

使用自动 EVI 模式配置 EVPN 实例、RD 和 RT:

```
OS10(config)# evpn
OS10(config-evpn)# auto-evi
OS10(config-evpn)# exit
```

## 12. 配置 VLT

配置专用 L3 承载路径, 以在发生网络故障时访问 VLT 对等节点

```
OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 172.16.250.0/31
OS10(config-if-vl-4000)# exit
```

配置 VLT 端口通道

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# vlt-port-channel 10
OS10(conf-if-po-10)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# vlt-port-channel 20
OS10(conf-if-po-20)# exit
```

配置 VLTi 成员链路

```
OOS10(config)# interface ethernet1/1/3
OS10(conf-if-eth1/1/3)# no shutdown
OS10(conf-if-eth1/1/3)# no switchport
OS10(conf-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(conf-if-eth1/1/4)# no shutdown
OS10(conf-if-eth1/1/4)# no switchport
OS10(conf-if-eth1/1/4)# exit
```

配置 VLT 域

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.150.1
OS10(conf-vlt-1)# discovery-interface ethernet1/1/3,1/1/4
OS10(conf-vlt-1)# vlt-mac aa:bb:cc:dd:ee:ff
OS10(conf-vlt-1)# exit
```

使用上行链路 VLT 端口和下行链路网络端口配置 UFD

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# enable
OS10(conf-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
OS10(conf-uplink-state-group-1)# upstream port-channel10
OS10(conf-uplink-state-group-1)# upstream port-channel20
OS10(conf-uplink-state-group-1)# exit
```

在 VLT 对等方之间配置 iBGP IPv4 对等

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172.16.250.1
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 13. 在覆盖网络中配置 IP 切换

## 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(conf-vrf)# exit
```

## 配置任意广播网关 MAC 地址

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

## 在虚拟网络上配置路由

```
OS10(config)# interface virtual-network 10000
OS10(conf-if-vn-10000)# ip vrf forwarding tenant1
OS10(conf-if-vn-10000)# ip address 10.1.0.231/16
OS10(conf-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(conf-if-vn-10000)# no shutdown
OS10(conf-if-vn-10000)# exit

OS10(config)# interface virtual-network 20000
OS10(conf-if-vn-20000)# ip vrf forwarding tenant1
OS10(conf-if-vn-20000)# ip address 10.2.0.231/16
OS10(conf-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(conf-if-vn-20000)# no shutdown
OS10(conf-if-vn-20000)# exit
```

## VTEP 2 分支交换机

### 1. 使用与 VLT 对等方相同的 IP 地址为承载 VXLAN 配置环回接口

```
OS10(config)# interface loopback0
OS10(conf-if-lo-0)# no shutdown
OS10(conf-if-lo-0)# ip address 192.168.1.1/32
OS10(conf-if-lo-0)# exit
```

### 2. 将环回接口配置为 VXLAN 源隧道接口

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback0
OS10(config-nve)# exit
```

### 3. 配置 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vxlan-vni 10000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn)# exit
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vxlan-vni 20000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-20000)# exit
```

### 4. 将 VLAN 成员接口分配给虚拟网络

使用交换机限定的 VLAN 到 VNI 映射：

```
OS10(config)# interface vlan100
OS10(config-if-vl-100)# virtual-network 10000
OS10(config-if-vl-100)# no shutdown
OS10(config-if-vl-100)# exit
OS10(config)# interface vlan200
OS10(config-if-vl-200)# virtual-network 20000
OS10(config-if-vl-200)# no shutdown
OS10(config-if-vl-200)# exit
```

## 5. 针对交换机限定的 VLAN 至 VNI 映射将访问端口配置为 VLAN 成员

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode trunk
OS10(conf-if-po-10)# switchport trunk allowed vlan 100
OS10(conf-if-po-10)# no switchport access vlan
OS10(conf-if-po-10)# exit

OS10(config)# interface ethernet1/1/5
OS10(conf-if-eth1/1/5)# no shutdown
OS10(conf-if-eth1/1/5)# channel-group 10 mode active
OS10(conf-if-eth1/1/5)# no switchport
OS10(conf-if-eth1/1/5)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# no shutdown
OS10(conf-if-po-20)# switchport mode trunk
OS10(conf-if-po-20)# switchport access vlan 200
OS10(conf-if-po-20)# exit

OS10(config)# interface ethernet1/1/6
OS10(conf-if-eth1/1/6)# no shutdown
OS10(conf-if-eth1/1/6)# channel-group 20 mode active
OS10(conf-if-eth1/1/6)# no switchport
OS10(conf-if-eth1/1/6)# exit
```

## 6. 配置面向上游网络的端口

```
OS10(config)# interface ethernet1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/1)# ip address 172.17.1.0/31
OS10(conf-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# mtu 1650
OS10(conf-if-eth1/1/2)# ip address 172.17.2.0/31
OS10(conf-if-eth1/1/2)# exit
```

## 7. 配置 eBGP

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# router-id 172.17.0.1
OS10(config-router-bgp-100)# address-family ipv4 unicast
OS10(configure-router-bgp-af)# redistribute connected
OS10(configure-router-bgp-af)# exit
```

## 8. 针对 IPv4 点对点对等配置 eBGP

```
OS10(config-router-bgp-100)# neighbor 172.17.1.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-100)# neighbor 172.17.2.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```



## 9. 为 BGP EVPN 对等配置环回接口与 VLT 对等 IP 地址不同

```
OS10(config)# interface loopback1
OS10(conf-if-lo-1)# no shutdown
OS10(conf-if-lo-1)# ip address 172.17.0.1/32
OS10(conf-if-lo-1)# exit
```

## 10. 配置 BGP EVPN 对等

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172.201.0.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-100)# neighbor 172.202.0.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-bgp-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 11. 配置 EVPN

使用自动 EVI 模式配置 EVPN 实例、RD 和 RT:

```
OS10(config)# evpn
OS10(config-evpn)# auto-evi
OS10(config-evpn)# exit
```

## 12. 配置 VLT

配置专用 L3 承载路径, 以在发生网络故障时访问 VLT 对等方

```
OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 172.16.250.1/31
OS10(config-if-vl-4000)# exit
```

### 配置 VLT 端口通道

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# vlt-port-channel 10
OS10(conf-if-po-10)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# vlt-port-channel 20
OS10(conf-if-po-20)# exit
```

## 配置 VLTi 成员链路

```
OS10(config)# interface ethernet1/1/3
OS10(conf-if-eth1/1/3)# no shutdown
OS10(conf-if-eth1/1/3)# no switchport
OS10(conf-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(conf-if-eth1/1/4)# no shutdown
OS10(conf-if-eth1/1/4)# no switchport
OS10(conf-if-eth1/1/4)# exit
```

## 配置 VLT 域

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.150.2
OS10(conf-vlt-1)# discovery-interface ethernet1/1/3,1/1/4
OS10(conf-vlt-1)# vlt-mac aa:bb:cc:dd:ee:ff
OS10(conf-vlt-1)# exit
```

## 使用上行链路 VLT 端口和下行链路网络端口配置 UFD

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# enable
OS10(conf-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
OS10(conf-uplink-state-group-1)# upstream port-channel10
OS10(conf-uplink-state-group-1)# upstream port-channel20
OS10(conf-uplink-state-group-1)# exit
```

## 在 VLT 对等方之间配置 iBGP IPv4 对等

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172.16.250.0
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 13. 在覆盖网络中配置 IP 切换

### 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(conf-vrf)# exit
```

### 配置任意广播网关 MAC 地址

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

### 在虚拟网络上配置路由

```
OS10(config)# interface virtual-network 10000
OS10(conf-if-vn-10000)# ip vrf forwarding tenant1
OS10(conf-if-vn-10000)# ip address 10.1.0.232/16
OS10(conf-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(conf-if-vn-10000)# no shutdown
OS10(conf-if-vn-10000)# exit

OS10(config)# interface virtual-network 20000
OS10(conf-if-vn-20000)# ip vrf forwarding tenant1
OS10(conf-if-vn-20000)# ip address 10.2.0.232/16
OS10(conf-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(conf-if-vn-20000)# no shutdown
OS10(conf-if-vn-20000)# exit
```

## VTEP 3 分支交换机

### 1. 使用与 VLT 对等方相同的 IP 地址为承载 VXLAN 配置环回接口

```
OS10(config)# interface loopback0
OS10(config-if-lo-0)# no shutdown
OS10(config-if-lo-0)# ip address 192.168.2.1/32
OS10(config-if-lo-0)# exit
```

### 2. 将环回接口配置为 VXLAN 源隧道接口

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback0
OS10(config-nve)# exit
```

### 3. 配置 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vxlan-vni 10000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit
```

```
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vxlan-vni 20000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-20000)# exit
```

### 4. 为未标记成员身份配置未使用的 VLAN ID

```
OS10(config)# virtual-network untagged-vlan 1000
```

### 5. 针对端口限定的 VLAN 至 VNI 映射将访问端口配置为 VLAN 成员

```
OS10(config)# interface port-channel10
OS10(config-if-po-10)# no shutdown
OS10(config-if-po-10)# switchport mode trunk
OS10(config-if-po-10)# no switchport access vlan
OS10(config-if-po-10)# exit

OS10(config)# interface ethernet1/1/5
OS10(config-if-eth1/1/5)# no shutdown
OS10(config-if-eth1/1/5)# channel-group 10 mode active
OS10(config-if-eth1/1/5)# no switchport
OS10(config-if-eth1/1/5)# exit

OS10(config)# interface port-channel20
OS10(config-if-po-20)# no shutdown
OS10(config-if-po-20)# switchport mode trunk
OS10(config-if-po-20)# no switchport access vlan
OS10(config-if-po-20)# exit

OS10(config)# interface ethernet1/1/6
OS10(config-if-eth1/1/6)# no shutdown
OS10(config-if-eth1/1/6)# channel-group 20 mode active
OS10(config-if-eth1/1/6)# no switchport
OS10(config-if-eth1/1/6)# exit
```

### 6. 将访问端口添加到虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# member-interface port-channel 10 vlan-tag 100
OS10(config-vn-10000)# exit

OS10(config)# virtual-network 20000
OS10(config-vn-20000)# member-interface port-channel 20 untagged
OS10(config-vn-20000)# exit
```

## 7. 配置面向上游网络的端口

```
OS10(config)# interface ethernet1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/1)# ip address 172.18.1.0/31
OS10(conf-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/2)# ip address 172.18.2.0/31
OS10(conf-if-eth1/1/2)# exit
```

## 8. 配置 eBGP

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# router-id 172.18.0.1
OS10(config-router-bgp-100)# address-family ipv4 unicast
OS10(configure-router-bgp-af)# redistribute connected
OS10(configure-router-bgp-af)# exit
```

## 9. 针对 IPv4 点对点等配置 eBGP

```
OS10(config-router-bgp-100)# neighbor 172.18.1.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-100)# neighbor 172.18.2.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 10. 为 BGP EVPN 对等配置环回接口与 VLT 对等主机 IP 地址不同

```
OS10(config)# interface loopback1
OS10(conf-if-lo-1)# no shutdown
OS10(conf-if-lo-1)# ip address 172.18.0.1/32
OS10(conf-if-lo-1)# exit
```

## 11. 配置 BGP EVPN 对等

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172.201.0.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-100)# neighbor 172.202.0.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# ebgp-multihop 4
```

```

OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit

```

## 12. 配置 EVPN

在手动配置模式下配置 EVPN 实例，在自动模式下配置 RD 和 RT 配置：

```

OS10(config)# evpn
OS10(config-evpn)# evi 10000
OS10(config-evpn-evi-10000)# vni 10000
OS10(config-evpn-evi-10000)# rd auto
OS10(config-evpn-evi-10000)# route-target auto
OS10(config-evpn-evi-10000)# exit

OS10(config-evpn)# evi 20000
OS10(config-evpn-evi-20000)# vni 20000
OS10(config-evpn-evi-20000)# rd auto
OS10(config-evpn-evi-20000)# route-target auto
OS10(config-evpn-evi-20000)# exit
OS10(config-evpn)# exit

```

## 13. 配置 VLT

### 为虚拟网络配置 VLTi VLAN

```

OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vlti-vlan 100
OS10(config-vn-10000)# exit

OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vlti-vlan 200
OS10(config-vn-20000)# exit

```

### 配置专用 L3 承载路径，以在发生网络故障时访问 VLT 对等方

```

OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 172.16.250.10/31
OS10(config-if-vl-4000)# exit

```

### 配置 VLT 端口通道

```

OS10(config)# interface port-channel10
OS10(conf-if-po-10)# vlt-port-channel 10
OS10(conf-if-po-10)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# vlt-port-channel 20
OS10(conf-if-po-20)# exit

```

### 配置 VLTi 成员链路

```

OOS10(config)# interface ethernet1/1/3
OS10(conf-if-eth1/1/3)# no shutdown
OS10(conf-if-eth1/1/3)# no switchport
OS10(conf-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(conf-if-eth1/1/4)# no shutdown
OS10(conf-if-eth1/1/4)# no switchport
OS10(conf-if-eth1/1/4)# exit

```

## 配置 VLT 域

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.150.3
OS10(conf-vlt-1)# discovery-interface ethernet1/1/3,1/1/4
OS10(conf-vlt-1)# vlt-mac aa:bb:cc:dd:ff:ee
OS10(conf-vlt-1)# exit
```

## 使用上行链路 VLT 端口和下行链路网络端口配置 UFD

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# enable
OS10(conf-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
OS10(conf-uplink-state-group-1)# upstream port-channel10
OS10(conf-uplink-state-group-1)# upstream port-channel20
OS10(conf-uplink-state-group-1)# exit
```

## 在 VLT 对等方之间配置 iBGP IPv4 对等

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172.16.250.11
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 14. 在覆盖网络中配置 IP 路由

### 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(conf-vrf)# exit
```

### 配置任意广播网关 MAC 地址

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

### 在虚拟网络上配置路由

```
OS10(config)# interface virtual-network 10000
OS10(conf-if-vn-10000)# ip vrf forwarding tenant1
OS10(conf-if-vn-10000)# ip address 10.1.0.233/16
OS10(conf-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(conf-if-vn-10000)# no shutdown
OS10(conf-if-vn-10000)# exit

OS10(config)# interface virtual-network 20000
OS10(conf-if-vn-20000)# ip vrf forwarding tenant1
OS10(conf-if-vn-20000)# ip address 10.2.0.233/16
OS10(conf-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(conf-if-vn-20000)# no shutdown
OS10(conf-if-vn-20000)# exit
```

## VTEP 4 分支交换机

### 1. 使用与 VLT 对等方相同的 IP 地址为承载 VXLAN 配置环回接口

```
OS10(config)# interface loopback0
OS10(conf-if-lo-0)# no shutdown
OS10(conf-if-lo-0)# ip address 192.168.2.1/32
OS10(conf-if-lo-0)# exit
```

### 2. 将环回接口配置为 VXLAN 源隧道接口

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback0
OS10(config-nve)# exit
```

### 3. 配置 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vxlan-vni 10000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit

OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vxlan-vni 20000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-20000)# exit
```

### 4. 为未标记成员身份配置未使用的 VLAN ID

```
OS10(config)# virtual-network untagged-vlan 1000
```

### 5. 针对端口限定的 VLAN 至 VNI 映射将访问端口配置为 VLAN 成员

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode trunk
OS10(conf-if-po-10)# no switchport access vlan
OS10(conf-if-po-10)# exit

OS10(config)# interface ethernet1/1/5
OS10(conf-if-eth1/1/5)# no shutdown
OS10(conf-if-eth1/1/5)# channel-group 10 mode active
OS10(conf-if-eth1/1/5)# no switchport
OS10(conf-if-eth1/1/5)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# no shutdown
OS10(conf-if-po-20)# switchport mode trunk
OS10(conf-if-po-20)# no switchport access vlan
OS10(conf-if-po-20)# exit

OS10(config)# interface ethernet1/1/6
OS10(conf-if-eth1/1/6)# no shutdown
OS10(conf-if-eth1/1/6)# channel-group 20 mode active
OS10(conf-if-eth1/1/6)# no switchport
OS10(conf-if-eth1/1/6)# exit
```

### 6. 将访问端口添加到虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# member-interface port-channel 10 vlan-tag 100
OS10(config-vn)# exit

OS10(config)# virtual-network 20000
OS10(config-vn-20000)# member-interface port-channel 20 untagged
OS10(config-vn)# exit
```

### 7. 配置面向上游网络的端口

```
OS10(config)# interface ethernet1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/1)# ip address 172.19.1.0/31
OS10(conf-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# mtu 1650
OS10(conf-if-eth1/1/2)# ip address 172.19.2.0/31
OS10(conf-if-eth1/1/2)# exit
```

## 8. 配置 eBGP

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# router-id 172.19.0.1
OS10(config-router-bgp-100)# address-family ipv4 unicast
OS10(configure-router-bgp-af)# redistribute connected
OS10(configure-router-bgp-af)# exit
```

## 9. 针对 IPv4 点对点对等配置 eBGP

```
OS10(config-router-bgp-100)# neighbor 172.19.1.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-100)# neighbor 172.19.2.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 10. 为 BGP EVPN 对等配置与 VLT 对等方 IP 地址不同的环回接口

```
OS10(config)# interface loopback1
OS10(conf-if-lo-1)# no shutdown
OS10(conf-if-lo-1)# ip address 172.19.0.1/32
OS10(conf-if-lo-1)# exit
```

## 11. 配置 BGP EVPN 对等

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172.201.0.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-100)# neighbor 172.202.0.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# allowas-in 1
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 12. 配置 EVPN



在手动配置模式下配置 EVPN 实例，在自动模式下配置 RD 和 RT 配置：

```
OS10(config)# evpn
OS10(config-evpn)# evi 10000
OS10(config-evpn-evi-10000)# vni 10000
OS10(config-evpn-evi-10000)# rd auto
OS10(config-evpn-evi-10000)# route-target auto
OS10(config-evpn-evi-10000)# exit

OS10(config-evpn)# evi 20000
OS10(config-evpn-evi-20000)# vni 20000
OS10(config-evpn-evi-20000)# rd auto
OS10(config-evpn-evi-20000)# route-target auto
OS10(config-evpn-evi-20000)# exit
OS10(config-evpn)# exit
```

### 13. 配置 VLT

#### 为虚拟网络配置 VLTi VLAN

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vlti-vlan 100
OS10(config-vn-10000)# exit

OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vlti-vlan 200
OS10(config-vn-20000)# exit
```

#### 配置专用 L3 承载路径，以在发生网络故障时访问 VLT 对等方

```
OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 172.16.250.11/31
OS10(config-if-vl-4000)# exit
```

#### 配置 VLT 端口通道

```
OS10(config)# interface port-channel10
OS10(config-if-po-10)# vlt-port-channel 10
OS10(config-if-po-10)# exit

OS10(config)# interface port-channel20
OS10(config-if-po-20)# vlt-port-channel 20
OS10(config-if-po-20)# exit
```

#### 配置 VLTi 成员链路

```
OOS10(config)# interface ethernet1/1/3
OS10(config-if-eth1/1/3)# no shutdown
OS10(config-if-eth1/1/3)# no switchport
OS10(config-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(config-if-eth1/1/4)# no shutdown
OS10(config-if-eth1/1/4)# no switchport
OS10(config-if-eth1/1/4)# exit
```

#### 配置 VLT 域

```
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# backup destination 10.16.150.4
OS10(config-vlt-1)# discovery-interface ethernet1/1/3,1/1/4
OS10(config-vlt-1)# vlt-mac aa:bb:cc:dd:ff:ee
OS10(config-vlt-1)# exit
```

#### 使用上行链路 VLT 端口和下行链路网络端口配置 UFD

```
OS10(config)# uplink-state-group 1
OS10(config-uplink-state-group-1)# enable
OS10(config-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
```

```
OS10(config-uplink-state-group-1)# upstream port-channel10
OS10(config-uplink-state-group-1)# upstream port-channel20
OS10(config-uplink-state-group-1)# exit
```

## 在 VLT 对等方之间配置 iBGP IPv4 对等

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172.16.250.10
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 14. 在覆盖网络中配置 IP 路由

### 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(config-vrf)# exit
```

### 配置任意广播网关 MAC 地址

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

### 在虚拟网络上配置路由

```
OS10(config)# interface virtual-network 10000
OS10(config-if-vn-10000)# ip vrf forwarding tenant1
OS10(config-if-vn-10000)# ip address 10.1.0.234/16
OS10(config-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(config-if-vn-10000)# no shutdown
OS10(config-if-vn-10000)# exit

OS10(config)# interface virtual-network 20000
OS10(config-if-vn-20000)# ip vrf forwarding tenant1
OS10(config-if-vn-20000)# ip address 10.2.0.234/16
OS10(config-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(config-if-vn-20000)# no shutdown
OS10(config-if-vn-20000)# exit
```

## 主干交换机 1

### 1. 在承载链路上配置指向分支交换机的下游端口

```
OS10(config)# interface ethernet1/1/1
OS10(config-if-eth1/1/1)# no shutdown
OS10(config-if-eth1/1/1)# no switchport
OS10(config-if-eth1/1/1)# ip address 172.16.1.1/31
OS10(config-if-eth1/1/1)# exit
OS10(config)# interface ethernet1/1/2
OS10(config-if-eth1/1/2)# no shutdown
OS10(config-if-eth1/1/2)# no switchport
OS10(config-if-eth1/1/2)# ip address 172.17.1.1/31
OS10(config-if-eth1/1/2)# exit
OS10(config)# interface ethernet1/1/3
OS10(config-if-eth1/1/3)# no shutdown
OS10(config-if-eth1/1/3)# no switchport
OS10(config-if-eth1/1/3)# ip address 172.18.1.1/31
OS10(config-if-eth1/1/3)# exit
OS10(config)# interface ethernet1/1/4
OS10(config-if-eth1/1/4)# no shutdown
OS10(config-if-eth1/1/4)# no switchport
OS10(config-if-eth1/1/4)# ip address 172.19.1.1/31
OS10(config-if-eth1/1/4)# exit
```

## 2. 配置 eBGP

```
OS10(config)# router bgp 101
OS10(config-router-bgp-101)# router-id 172.201.0.1
OS10(config-router-bgp-101)# address-family ipv4 unicast
OS10(configure-router-bgpv4-af)# redistribute connected
OS10(configure-router-bgpv4-af)# exit
```

## 3. 在 P2P 链路上配置 eBGP IPv4 对等节点会话

```
OS10(config-router-bgp-101)# neighbor 172.16.1.0
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-neighbor-af)# no sender-side-loop-detection
OS10(config-router-neighbor-af)# exit
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-101)# neighbor 172.17.1.0
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-neighbor-af)# no sender-side-loop-detection
OS10(config-router-neighbor-af)# exit
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-101)# neighbor 172.18.1.0
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-neighbor-af)# no sender-side-loop-detection
OS10(config-router-neighbor-af)# exit
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-101)# neighbor 172.19.1.0
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-neighbor-af)# no sender-side-loop-detection
OS10(config-router-neighbor-af)# exit
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-101)# exit
```

## 4. 为 BGP EVPN 对等节点配置环回接口

```
OS10(config)# interface loopback1
OS10(config-if-lo-1)# no shutdown
OS10(config-if-lo-1)# ip address 172.201.0.1/32
OS10(config-if-lo-1)# exit
```

## 5. 配置 BGP EVPN 对等节点会话

```
OS10(config)# router bgp 101
OS10(config-router-bgp-101)# neighbor 172.16.0.1
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-neighbor-af)# no activate
OS10(config-router-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-neighbor-af)# no sender-side-loop-detection
OS10(config-router-neighbor-af)# activate
OS10(config-router-neighbor-af)# exit

OS10(config-router-bgp-101)# neighbor 172.17.0.1
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# send-community extended
```

```

OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-neighbor-af)# no activate
OS10(config-router-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-neighbor-af)# no sender-side-loop-detection
OS10(config-router-neighbor-af)# activate
OS10(config-router-neighbor-af)# exit

OS10(config-router-bgp-101)# neighbor 172.18.0.1
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-neighbor-af)# no activate
OS10(config-router-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-neighbor-af)# no sender-side-loop-detection
OS10(config-router-neighbor-af)# activate
OS10(config-router-neighbor-af)# exit

OS10(config-router-bgp-101)# neighbor 172.19.0.1
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-neighbor-af)# no activate
OS10(config-router-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-neighbor-af)# no sender-side-loop-detection
OS10(config-router-neighbor-af)# activate
OS10(config-router-neighbor-af)# exit

```

## 主干交换机 2

### 1. 在承载链路上配置指向分支交换机的下游端口

```

OS10(config)# interface ethernet1/1/1
OS10(config-if-eth1/1/1)# no shutdown
OS10(config-if-eth1/1/1)# no switchport
OS10(config-if-eth1/1/1)# ip address 172.16.2.1/31
OS10(config-if-eth1/1/1)# exit
OS10(config)# interface ethernet1/1/2
OS10(config-if-eth1/1/2)# no shutdown
OS10(config-if-eth1/1/2)# no switchport
OS10(config-if-eth1/1/2)# ip address 172.17.2.1/31
OS10(config-if-eth1/1/2)# exit
OS10(config)# interface ethernet1/1/3
OS10(config-if-eth1/1/3)# no shutdown
OS10(config-if-eth1/1/3)# no switchport
OS10(config-if-eth1/1/3)# ip address 172.18.2.1/31
OS10(config-if-eth1/1/3)# exit
OS10(config)# interface ethernet1/1/4
OS10(config-if-eth1/1/4)# no shutdown
OS10(config-if-eth1/1/4)# no switchport
OS10(config-if-eth1/1/4)# ip address 172.19.2.1/31
OS10(config-if-eth1/1/4)# exit

```

### 2. 配置 eBGP

```

OS10(config)# router bgp 101
OS10(config-router-bgp-101)# router-id 172.202.0.1
OS10(config-router-bgp-101)# address-family ipv4 unicast

```

```
OS10(configure-router-bgpv4-af)# redistribute connected
OS10(configure-router-bgpv4-af)# exit
```

### 3. 在 P2P 链路上配置 eBGP IPv4 对等节点会话

```
OS10(conf-router-bgp-101)# neighbor 172.16.2.0
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no sender-side-loop-detection
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# exit

OS10(conf-router-bgp-101)# neighbor 172.17.2.0
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no sender-side-loop-detection
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# exit

OS10(conf-router-bgp-101)# neighbor 172.18.2.0
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no sender-side-loop-detection
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# exit

OS10(conf-router-bgp-101)# neighbor 172.19.2.0
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no sender-side-loop-detection
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# exit
OS10(conf-router-bgp-101)# exit
```

### 4. 为 BGP EVPN 对等节点配置环回接口

```
OS10(config)# interface loopback1
OS10(conf-if-lo-1)# no shutdown
OS10(conf-if-lo-1)# ip address 172.202.0.1/32
OS10(conf-if-lo-1)# exit
```

### 5. 配置 BGP EVPN 对等节点会话

```
OS10(config)# router bgp 101
OS10(conf-router-bgp-101)# neighbor 172.16.0.1
OS10(conf-router-neighbor)# ebgp-multihop 4
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# send-community extended
OS10(conf-router-neighbor)# update-source loopback1
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no activate
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# address-family l2vpn evpn
OS10(conf-router-neighbor-af)# no sender-side-loop-detection
OS10(conf-router-neighbor-af)# activate
OS10(conf-router-neighbor-af)# exit

OS10(conf-router-bgp-101)# neighbor 172.17.0.1
OS10(conf-router-neighbor)# ebgp-multihop 4
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# send-community extended
OS10(conf-router-neighbor)# update-source loopback1
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no activate
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# address-family l2vpn evpn
```

```

OS10(conf-router-neighbor-af)# no sender-side-loop-detection
OS10(conf-router-neighbor-af)# activate
OS10(conf-router-neighbor-af)# exit

OS10(conf-router-bgp-101)# neighbor 172.18.0.1
OS10(conf-router-neighbor)# ebgp-multihop 4
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# send-community extended
OS10(conf-router-neighbor)# update-source loopback1
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no activate
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# address-family l2vpn evpn
OS10(conf-router-neighbor-af)# no sender-side-loop-detection
OS10(conf-router-neighbor-af)# activate
OS10(conf-router-neighbor-af)# exit

OS10(conf-router-bgp-101)# neighbor 172.19.0.1
OS10(conf-router-neighbor)# ebgp-multihop 4
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# send-community extended
OS10(conf-router-neighbor)# update-source loopback1
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no activate
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# address-family l2vpn evpn
OS10(conf-router-neighbor-af)# no sender-side-loop-detection
OS10(conf-router-neighbor-af)# activate
OS10(conf-router-neighbor-af)# exit

```

## 使用 BGP EVPN 配置验证 VXLAN

### 1. 验证虚拟网络配置

```

LEAF1# show virtual-network
Codes: DP - MAC-learn Dataplane, CP - MAC-learn Controlplane, UUD - Unknown-Unicast-Drop
Virtual Network: 10000
 Members:
 VLAN 100: port-channel10, port-channel1000
 VxLAN Virtual Network Identifier: 10000
 Source Interface: loopback0(192.168.1.1)
 Remote-VTEPs (flood-list): 192.168.2.1(CP)

Virtual Network: 20000
 Members:
 Untagged: port-channel20
 VLAN 200: port-channel1000
 VxLAN Virtual Network Identifier: 20000
 Source Interface: loopback0(192.168.1.1)
 Remote-VTEPs (flood-list): 192.168.2.1(CP)
LEAF1#

```

### 2. 验证 EVPN 配置和 EVPN 参数

```

LEAF1# show evpn evi

EVI : 10000, State : up
 Bridge-Domain : Virtual-Network 10000, VNI 10000
 Route-Distinguisher : 1:192.168.1.1:10000(auto)
 Route-Targets : 0:100:268445456(auto) both
 Inclusive Multicast : 192.168.2.1
 IRB : Enabled(tenant1)

EVI : 20000, State : up
 Bridge-Domain : Virtual-Network 20000, VNI 20000
 Route-Distinguisher : 1:192.168.1.1:20000(auto)
 Route-Targets : 0:100:268455456(auto) both
 Inclusive Multicast : 192.168.2.1

```

```
IRB : Enabled(tenant1)
LEAF1#
```

### 3. 验证分支和主干节点之间的 BGP EVPN 邻居

```
LEAF1# show ip bgp l2vpn evpn summary
BGP router identifier 172.16.0.1 local AS number 100
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx
172.201.0.1 101 1132 1116 13:29:00 27
172.202.0.1 101 1131 1118 13:29:02 28
LEAF1#
```

### 4. 检查主机 A 和主机 B 之间的连接

```
root@HOST-A:~# ping 10.2.0.10 -c 5
PING 10.2.0.10 (10.2.0.10) 56(84) bytes of data.
64 bytes from 10.2.0.10: icmp_seq=1 ttl=63 time=0.824 ms
64 bytes from 10.2.0.10: icmp_seq=2 ttl=63 time=0.847 ms
64 bytes from 10.2.0.10: icmp_seq=3 ttl=63 time=0.835 ms
64 bytes from 10.2.0.10: icmp_seq=4 ttl=63 time=0.944 ms
64 bytes from 10.2.0.10: icmp_seq=5 ttl=63 time=0.806 ms

--- 10.2.0.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.806/0.851/0.944/0.051 ms
root@HOST-A:~#
```

### 5. 检查主机 A 和主机 C 之间的连接

```
root@HOST-A:~# ping 10.1.0.20 -c 5
PING 10.1.0.20 (10.1.0.20) 56(84) bytes of data.
64 bytes from 10.1.0.20: icmp_seq=1 ttl=64 time=0.741 ms
64 bytes from 10.1.0.20: icmp_seq=2 ttl=64 time=0.737 ms
64 bytes from 10.1.0.20: icmp_seq=3 ttl=64 time=0.772 ms
64 bytes from 10.1.0.20: icmp_seq=4 ttl=64 time=0.799 ms
64 bytes from 10.1.0.20: icmp_seq=5 ttl=64 time=0.866 ms

--- 10.1.0.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4061ms
rtt min/avg/max/mdev = 0.737/0.783/0.866/0.047 ms
root@HOST-A:~#
```

### 6. 检查主机 A 和主机 D 之间的连接

```
root@HOST-A:~# ping 10.2.0.20 -c 5
PING 10.2.0.20 (10.2.0.20) 56(84) bytes of data.
64 bytes from 10.2.0.20: icmp_seq=1 ttl=63 time=0.707 ms
64 bytes from 10.2.0.20: icmp_seq=2 ttl=63 time=0.671 ms
64 bytes from 10.2.0.20: icmp_seq=3 ttl=63 time=0.687 ms
64 bytes from 10.2.0.20: icmp_seq=4 ttl=63 time=0.640 ms
64 bytes from 10.2.0.20: icmp_seq=5 ttl=63 time=0.644 ms

--- 10.2.0.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4089ms
rtt min/avg/max/mdev = 0.640/0.669/0.707/0.041 ms
root@HOST-A:~#
```

 **注：**按照步骤 1 至 6 检查其他主机组合与主机之间的 ping 连接，并通过不同的虚拟网络 IP 地址检查主机之间的连接。

## 示例：VXLAN BGP EVPN — 多 AS 拓扑

以下带有 BGP EVPN 的 VXLAN 示例使用 Clos 分支-主干示例。单个交换机配置显示如何设置端到端 VXLAN。eBGP 用于交换 IP 承载网络中的 IP 路由和 VXLAN 覆盖网络中的 EVPN 路由。所有 VTEP 执行非对称 IRB 路由，其中：

- IRB 路由仅在入口 VTEP 上执行。
- 出口 VTEP 执行 IRB 桥接。

在此示例中，位于主干网络中的每个节点和分支网络中的每个 VTEP 都属于不同的自治系统。主干交换机 1 的形式为 101。主干交换机 2 的形式为 102。对于分支节点，VLT 域 1 为 AS 99；VLT 域 2 为 AS 100。

- 在 VTEP 1 和 2 上：使用交换机限定的 VLAN 将访问端口分配给虚拟网络。EVPN 实例以及 RD 和 RT 值在手动模式下配置。
- 在 VTEP 3 和 4 上：使用端口限定的 VLAN 将访问端口分配给虚拟网络。EVPN 实例以及 RD 和 RT 值在手动模式下配置。

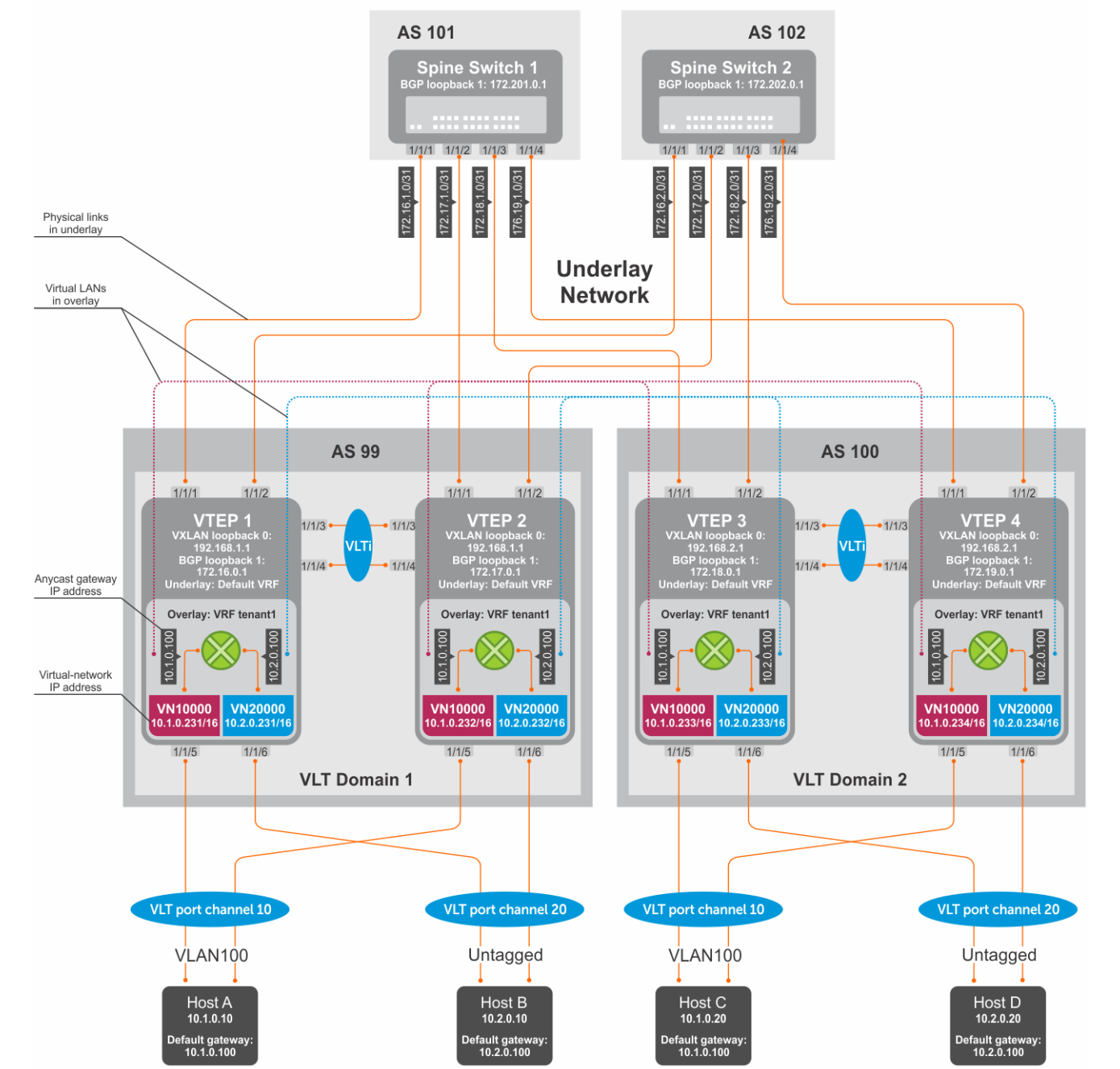


图 14: 带多 AS 的 VXLAN BGP EVPN

## VTEP 1 分支交换机

### 1. 使用与 VLT 对等方相同的 IP 地址为承载 VXLAN 配置环回接口

```
OS10(config)# interface loopback0
OS10(conf-if-lo-0)# no shutdown
OS10(conf-if-lo-0)# ip address 192.168.1.1/32
OS10(conf-if-lo-0)# exit
```



## 2. 将环回接口配置为 VXLAN 源隧道接口

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback0
OS10(config-nve)# exit
```

## 3. 配置 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vxlan-vni 10000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vxlan-vni 20000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-20000)# exit
```

## 4. 将 VLAN 成员接口分配给虚拟网络

使用交换机限定的 VLAN 到 VNI 映射：

```
OS10(config)# interface vlan100
OS10(config-if-vl-100)# virtual-network 10000
OS10(config-if-vl-100)# no shutdown
OS10(config-if-vl-100)# exit
OS10(config)# interface vlan200
OS10(config-if-vl-200)# virtual-network 20000
OS10(config-if-vl-200)# no shutdown
OS10(config-if-vl-200)# exit
```

## 5. 针对交换机限定的 VLAN 至 VNI 映射将访问端口配置为 VLAN 成员

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode trunk
OS10(conf-if-po-10)# switchport trunk allowed vlan 100
OS10(conf-if-po-10)# no switchport access vlan
OS10(conf-if-po-10)# exit

OS10(config)# interface ethernet1/1/5
OS10(conf-if-eth1/1/5)# no shutdown
OS10(conf-if-eth1/1/5)# channel-group 10 mode active
OS10(conf-if-eth1/1/5)# no switchport
OS10(conf-if-eth1/1/5)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# no shutdown
OS10(conf-if-po-20)# switchport mode trunk
OS10(conf-if-po-20)# switchport access vlan 200
OS10(conf-if-po-20)# exit

OS10(config)# interface ethernet1/1/6
OS10(conf-if-eth1/1/6)# no shutdown
OS10(conf-if-eth1/1/6)# channel-group 20 mode active
OS10(conf-if-eth1/1/6)# no switchport
OS10(conf-if-eth1/1/6)# exit
```

## 6. 配置面向上游网络的端口

```
OS10(config)# interface ethernet1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/1)# ip address 172.16.1.0/31
OS10(conf-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# mtu 1650
```

```
OS10(config-if-eth1/1/2)# ip address 172.16.2.0/31
OS10(config-if-eth1/1/2)# exit
```

## 7. 配置 eBGP

```
OS10(config)# router bgp 99
OS10(config-router-bgp-99)# router-id 172.16.0.1
OS10(config-router-bgp-99)# address-family ipv4 unicast
OS10(config-router-bgp-af)# redistribute connected
OS10(config-router-bgp-af)# exit
```

## 8. 针对 IPv4 点对点对等配置 eBGP

```
OS10(config-router-bgp-99)# neighbor 172.16.1.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-99)# neighbor 172.16.2.1
OS10(config-router-neighbor)# remote-as 102
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-99)# exit
```

## 9. 为 BGP EVPN 对等配置与 VLT 对等方 IP 地址不同的环回接口

```
OS10(config)# interface loopback1
OS10(config-if-lo-1)# no shutdown
OS10(config-if-lo-1)# ip address 172.16.0.1/32
OS10(config-if-lo-1)# exit
```

## 10. 配置 BGP EVPN 对等

```
OS10(config)# router bgp 99
OS10(config-router-bgp-99)# neighbor 172.201.0.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-99)# neighbor 172.202.0.1
OS10(config-router-neighbor)# remote-as 102
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 11. 配置 EVPN

在手动模式下配置 EVPN 实例、RD 和 RT 值：

```
OS10(config)# evpn
OS10(config-evpn)# evi 10000
OS10(config-evpn-evi-10000)# vni 10000
OS10(config-evpn-evi-10000)# rd 192.168.1.1:10000
OS10(config-evpn-evi-10000)# route-target 99:10000 both
```

```

OS10(config-evpn-evi-10000)# route-target 100:10000 import
OS10(config-evpn-evi-10000)#exit

OS10(config-evpn)# evi 20000
OS10(config-evpn-evi-20000)# vni 20000
OS10(config-evpn-evi-20000)# rd 192.168.1.1:20000
OS10(config-evpn-evi-20000)# route-target 99:20000 both
OS10(config-evpn-evi-20000)# route-target 100:20000 import
OS10(config-evpn-evi-20000)#exit
OS10(config-evpn)#

```

## 12. 配置 VLT

### 配置专用 L3 承载路径，以在发生网络故障时访问 VLT 对等方

```

OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 172.16.250.0/31
OS10(config-if-vl-4000)# exit

```

### 配置 VLT 端口通道

```

OS10(config)# interface port-channel10
OS10(conf-if-po-10)# vlt-port-channel 10
OS10(conf-if-po-10)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# vlt-port-channel 20
OS10(conf-if-po-20)# exit

```

### 配置 VLTi 成员链路

```

OOS10(config)# interface ethernet1/1/3
OS10(conf-if-eth1/1/3)# no shutdown
OS10(conf-if-eth1/1/3)# no switchport
OS10(conf-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(conf-if-eth1/1/4)# no shutdown
OS10(conf-if-eth1/1/4)# no switchport
OS10(conf-if-eth1/1/4)# exit

```

### 配置 VLT 域

```

OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.150.1
OS10(conf-vlt-1)# discovery-interface ethernet1/1/3,1/1/4
OS10(conf-vlt-1)# vlt-mac aa:bb:cc:dd:ee:ff
OS10(conf-vlt-1)# exit

```

### 使用上行链路 VLT 端口和下行链路网络端口配置 UFD

```

OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# enable
OS10(conf-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
OS10(conf-uplink-state-group-1)# upstream port-channel10
OS10(conf-uplink-state-group-1)# upstream port-channel20
OS10(conf-uplink-state-group-1)# exit

```

### 在 VLT 对等方之间配置 iBGP IPv4 对等

```

OS10(config)# router bgp 99
OS10(config-router-bgp-99)# neighbor 172.16.250.1
OS10(config-router-neighbor)# remote-as 99
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-99)# exit

```

## 13. 在覆盖网络中配置 IP 切换

## 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(conf-vrf)# exit
```

## 配置任意广播网关 MAC 地址

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

## 在虚拟网络上配置路由

```
OS10(config)# interface virtual-network10000
OS10(conf-if-vn-10000)# ip vrf forwarding tenant1
OS10(conf-if-vn-10000)# ip address 10.1.0.231/16
OS10(conf-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(conf-if-vn-10000)# no shutdown
OS10(conf-if-vn-10000)# exit

OS10(config)# interface virtual-network20000
OS10(conf-if-vn-20000)# ip vrf forwarding tenant1
OS10(conf-if-vn-20000)# ip address 10.2.0.231/16
OS10(conf-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(conf-if-vn-20000)# no shutdown
OS10(conf-if-vn-20000)# exit
```

## VTEP 2 分支交换机

### 1. 使用与 VLT 对等方相同的 IP 地址为承载 VXLAN 配置环回接口

```
OS10(config)# interface loopback0
OS10(conf-if-lo-0)# no shutdown
OS10(conf-if-lo-0)# ip address 192.168.1.1/32
OS10(conf-if-lo-0)# exit
```

### 2. 将环回接口配置为 VXLAN 源隧道接口

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback0
OS10(config-nve)# exit
```

### 3. 配置 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vxlan-vni 10000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn)# exit
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vxlan-vni 20000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-20000)# exit
```

### 4. 将 VLAN 成员接口分配给虚拟网络

使用交换机限定的 VLAN 到 VNI 映射：

```
OS10(config)# interface vlan100
OS10(config-if-vl-100)# virtual-network 10000
OS10(config-if-vl-100)# no shutdown
OS10(config-if-vl-100)# exit
OS10(config)# interface vlan200
OS10(config-if-vl-200)# virtual-network 20000
OS10(config-if-vl-200)# no shutdown
OS10(config-if-vl-200)# exit
```

## 5. 针对交换机限定的 VLAN 至 VNI 映射将访问端口配置为 VLAN 成员

```
OS10(config)# interface port-channel10
OS10(config-if-po-10)# no shutdown
OS10(config-if-po-10)# switchport mode trunk
OS10(config-if-po-10)# switchport trunk allowed vlan 100
OS10(config-if-po-10)# no switchport access vlan
OS10(config-if-po-10)# exit

OS10(config)# interface ethernet1/1/5
OS10(config-if-eth1/1/5)# no shutdown
OS10(config-if-eth1/1/5)# channel-group 10 mode active
OS10(config-if-eth1/1/5)# no switchport
OS10(config-if-eth1/1/5)# exit

OS10(config)# interface port-channel20
OS10(config-if-po-20)# no shutdown
OS10(config-if-po-20)# switchport mode trunk
OS10(config-if-po-20)# switchport access vlan 200
OS10(config-if-po-20)# exit

OS10(config)# interface ethernet1/1/6
OS10(config-if-eth1/1/6)# no shutdown
OS10(config-if-eth1/1/6)# channel-group 20 mode active
OS10(config-if-eth1/1/6)# no switchport
OS10(config-if-eth1/1/6)# exit
```

## 6. 配置面向上游网络的端口

```
OS10(config)# interface ethernet1/1/1
OS10(config-if-eth1/1/1)# no shutdown
OS10(config-if-eth1/1/1)# no switchport
OS10(config-if-eth1/1/1)# mtu 1650
OS10(config-if-eth1/1/1)# ip address 172.17.1.0/31
OS10(config-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(config-if-eth1/1/2)# no shutdown
OS10(config-if-eth1/1/2)# no switchport
OS10(config-if-eth1/1/2)# mtu 1650
OS10(config-if-eth1/1/2)# ip address 172.17.2.0/31
OS10(config-if-eth1/1/2)# exit
```

## 7. 配置 eBGP

```
OS10(config)# router bgp 99
OS10(config-router-bgp-99)# router-id 172.17.0.1
OS10(config-router-bgp-99)# address-family ipv4 unicast
OS10(config-router-bgp-af)# redistribute connected
OS10(config-router-bgp-af)# exit
```

## 8. 针对 IPv4 点对点等配置 eBGP

```
OS10(config-router-bgp-99)# neighbor 172.17.1.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-99)# neighbor 172.17.2.1
OS10(config-router-neighbor)# remote-as 102
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-99)# exit
```

## 9. 为 BGP EVPN 对等配置环回接口与 VLT 对等 IP 地址不同

```
OS10(config)# interface loopback1
OS10(config-if-lo-1)# no shutdown
OS10(config-if-lo-1)# ip address 172.17.0.1/32
OS10(config-if-lo-1)# exit
```

## 10. 配置 BGP EVPN 对等

```
OS10(config)# router bgp 99
OS10(config-router-bgp-99)# neighbor 172.201.0.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-99)# neighbor 172.202.0.1
OS10(config-router-neighbor)# remote-as 102
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-bgp-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-bgp-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-99)# exit
```

## 11. 配置 EVPN

在手动模式下配置 EVPN 实例、RD 和 RT:

```
OS10(config)# evpn
OS10(config-evpn)# evi 10000
OS10(config-evpn-evi-10000)# vni 10000
OS10(config-evpn-evi-10000)# rd 192.168.1.1:10000
OS10(config-evpn-evi-10000)# route-target 99:10000 both
OS10(config-evpn-evi-10000)# route-target 100:10000 import
OS10(config-evpn-evi-10000)#exit

OS10(config-evpn)# evi 20000
OS10(config-evpn-evi-20000)# vni 20000
OS10(config-evpn-evi-20000)# rd 192.168.1.1:20000
OS10(config-evpn-evi-20000)# route-target 99:20000 both
OS10(config-evpn-evi-20000)# route-target 100:20000 import
OS10(config-evpn-evi-20000)#exit
OS10(config-evpn)#
```

## 12. 配置 VLT

配置专用 L3 承载路径, 以在发生网络故障时访问 VLT 对等方

```
OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 172.16.250.1/31
OS10(config-if-vl-4000)# exit
```

### 配置 VLT 端口通道

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# vlt-port-channel 10
OS10(conf-if-po-10)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# vlt-port-channel 20
OS10(conf-if-po-20)# exit
```

## 配置 VLTi 成员链路

```
OOS10(config)# interface ethernet1/1/3
OS10(conf-if-eth1/1/3)# no shutdown
OS10(conf-if-eth1/1/3)# no switchport
OS10(conf-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(conf-if-eth1/1/4)# no shutdown
OS10(conf-if-eth1/1/4)# no switchport
OS10(conf-if-eth1/1/4)# exit
```

## 配置 VLT 域

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.150.2
OS10(conf-vlt-1)# discovery-interface ethernet1/1/3,1/1/4
OS10(conf-vlt-1)# vlt-mac aa:bb:cc:dd:ee:ff
OS10(conf-vlt-1)# exit
```

## 使用上行链路 VLT 端口和下行链路网络端口配置 UFD

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# enable
OS10(conf-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
OS10(conf-uplink-state-group-1)# upstream port-channel10
OS10(conf-uplink-state-group-1)# upstream port-channel20
OS10(conf-uplink-state-group-1)# exit
```

## 在 VLT 对等方之间配置 iBGP IPv4 对等

```
OS10(config)# router bgp 99
OS10(config-router-bgp-99)# neighbor 172.16.250.0
OS10(config-router-neighbor)# remote-as 99
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-99)# exit
```

## 13. 在覆盖网络中配置 IP 切换

### 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(conf-vrf)# exit
```

### 配置任意广播网关 MAC 地址

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

### 在虚拟网络上配置路由

```
OS10(config)# interface virtual-network10000
OS10(conf-if-vn-10000)# ip vrf forwarding tenant1
OS10(conf-if-vn-10000)# ip address 10.1.0.232/16
OS10(conf-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(conf-if-vn-10000)# no shutdown
OS10(conf-if-vn-10000)# exit

OS10(config)# interface virtual-network20000
OS10(conf-if-vn-20000)# ip vrf forwarding tenant1
OS10(conf-if-vn-20000)# ip address 10.2.0.232/16
OS10(conf-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(conf-if-vn-20000)# no shutdown
OS10(conf-if-vn-20000)# exit
```

## VTEP 3 分支交换机

### 1. 使用与 VLT 对等方相同的 IP 地址为承载 VXLAN 配置环回接口

```
OS10(config)# interface loopback0
OS10(config-if-lo-0)# no shutdown
OS10(config-if-lo-0)# ip address 192.168.2.1/32
OS10(config-if-lo-0)# exit
```

### 2. 将环回接口配置为 VXLAN 源隧道接口

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback0
OS10(config-nve)# exit
```

### 3. 配置 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vxlan-vni 10000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit
```

```
OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vxlan-vni 20000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-20000)# exit
```

### 4. 为未标记成员身份配置未使用的 VLAN ID

```
OS10(config)# virtual-network untagged-vlan 1000
```

### 5. 针对端口限定的 VLAN 至 VNI 映射将访问端口配置为 VLAN 成员

```
OS10(config)# interface port-channel10
OS10(config-if-po-10)# no shutdown
OS10(config-if-po-10)# switchport mode trunk
OS10(config-if-po-10)# no switchport access vlan
OS10(config-if-po-10)# exit

OS10(config)# interface ethernet1/1/5
OS10(config-if-eth1/1/5)# no shutdown
OS10(config-if-eth1/1/5)# channel-group 10 mode active
OS10(config-if-eth1/1/5)# no switchport
OS10(config-if-eth1/1/5)# exit

OS10(config)# interface port-channel20
OS10(config-if-po-20)# no shutdown
OS10(config-if-po-20)# switchport mode trunk
OS10(config-if-po-20)# no switchport access vlan
OS10(config-if-po-20)# exit

OS10(config)# interface ethernet1/1/6
OS10(config-if-eth1/1/6)# no shutdown
OS10(config-if-eth1/1/6)# channel-group 20 mode active
OS10(config-if-eth1/1/6)# no switchport
OS10(config-if-eth1/1/6)# exit
```

### 6. 将访问端口添加到虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# member-interface port-channel 10 vlan-tag 100
OS10(config-vn-10000)# exit

OS10(config)# virtual-network 20000
OS10(config-vn-20000)# member-interface port-channel 20 untagged
OS10(config-vn-20000)# exit
```



## 7. 配置面向上游网络的端口

```
OS10(config)# interface ethernet1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/1)# ip address 172.18.1.0/31
OS10(conf-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/2)# ip address 172.18.2.0/31
OS10(conf-if-eth1/1/2)# exit
```

## 8. 配置 eBGP

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# router-id 172.18.0.1
OS10(config-router-bgp-100)# address-family ipv4 unicast
OS10(configure-router-bgp-af)# redistribute connected
OS10(configure-router-bgp-af)# exit
```

## 9. 针对 IPv4 点对点等配置 eBGP

```
OS10(config-router-bgp-100)# neighbor 172.18.1.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-100)# neighbor 172.18.2.1
OS10(config-router-neighbor)# remote-as 102
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 10. 为 BGP EVPN 对等配置环回接口与 VLT 对等 IP 地址不同

```
OS10(config)# interface loopback1
OS10(conf-if-lo-1)# no shutdown
OS10(conf-if-lo-1)# ip address 172.18.0.1/32
OS10(conf-if-lo-1)# exit
```

## 11. 配置 BGP EVPN 对等

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172.201.0.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-100)# neighbor 172.202.0.1
OS10(config-router-neighbor)# remote-as 102
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
```

```
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 12. 配置 EVPN

在手动模式下配置 EVPN 实例、RD 和 RT：

```
OS10(config)# evpn
OS10(config-evpn)# evi 10000
OS10(config-evpn-evi-10000)# vni 10000
OS10(config-evpn-evi-10000)# rd 192.168.2.1:10000
OS10(config-evpn-evi-10000)# route-target 99:10000 import
OS10(config-evpn-evi-10000)# route-target 100:10000 both
OS10(config-evpn-evi-10000)# exit

OS10(config-evpn)# evi 20000
OS10(config-evpn-evi-20000)# vni 20000
OS10(config-evpn-evi-20000)# rd 192.168.2.1:20000
OS10(config-evpn-evi-20000)# route-target 99:20000 import
OS10(config-evpn-evi-20000)# route-target 100:20000 both
OS10(config-evpn-evi-20000)# exit
OS10(config-evpn)#
```

## 13. 配置 VLT

### 为虚拟网络配置 VLTi VLAN

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vlti-vlan 100
OS10(config-vn-10000)# exit

OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vlti-vlan 200
OS10(config-vn-20000)# exit
```

### 配置专用 L3 承载路径，以在发生网络故障时访问 VLT 对等方

```
OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 172.16.250.10/31
OS10(config-if-vl-4000)# exit
```

### 配置 VLT 端口通道

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# vlt-port-channel 10
OS10(conf-if-po-10)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# vlt-port-channel 20
OS10(conf-if-po-20)# exit
```

### 配置 VLTi 成员链路

```
OOS10(config)# interface ethernet1/1/3
OS10(conf-if-eth1/1/3)# no shutdown
OS10(conf-if-eth1/1/3)# no switchport
OS10(conf-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(conf-if-eth1/1/4)# no shutdown
OS10(conf-if-eth1/1/4)# no switchport
OS10(conf-if-eth1/1/4)# exit
```

### 配置 VLT 域

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.150.3
OS10(conf-vlt-1)# discovery-interface ethernet1/1/3,1/1/4
```

```
OS10(config-vlt-1)# vlt-mac aa:bb:cc:dd:ff:ee
OS10(config-vlt-1)# exit
```

### 使用上行链路 VLT 端口和下行链路网络端口配置 UFD

```
OS10(config)# uplink-state-group 1
OS10(config-uplink-state-group-1)# enable
OS10(config-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
OS10(config-uplink-state-group-1)# upstream port-channel10
OS10(config-uplink-state-group-1)# upstream port-channel20
OS10(config-uplink-state-group-1)# exit
```

### 在 VLT 对等方之间配置 iBGP IPv4 对等

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172.16.250.11
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 14. 在覆盖网络中配置 IP 路由

### 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(config-vrf)# exit
```

### 配置任意广播网关 MAC 地址

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

### 在虚拟网络上配置路由

```
OS10(config)# interface virtual-network10000
OS10(config-if-vn-10000)# ip vrf forwarding tenant1
OS10(config-if-vn-10000)# ip address 10.1.0.233/16
OS10(config-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(config-if-vn-10000)# no shutdown
OS10(config-if-vn-10000)# exit

OS10(config)# interface virtual-network20000
OS10(config-if-vn-20000)# ip vrf forwarding tenant1
OS10(config-if-vn-20000)# ip address 10.2.0.233/16
OS10(config-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(config-if-vn-20000)# no shutdown
OS10(config-if-vn-20000)# exit
```

## VTEP 4 分支交换机

### 1. 使用与 VLT 对等方相同的 IP 地址为承载 VXLAN 配置环回接口

```
OS10(config)# interface loopback0
OS10(config-if-lo-0)# no shutdown
OS10(config-if-lo-0)# ip address 192.168.2.1/32
OS10(config-if-lo-0)# exit
```

### 2. 将环回接口配置为 VXLAN 源隧道接口

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback0
OS10(config-nve)# exit
```

### 3. 配置 VXLAN 虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vxlan-vni 10000
```

```
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit

OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vxlan-vni 20000
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-20000)# exit
```

#### 4. 为未标记成员身份配置未使用的 VLAN ID

```
OS10(config)# virtual-network untagged-vlan 1000
```

#### 5. 针对端口限定的 VLAN 至 VNI 映射将访问端口配置为 VLAN 成员

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# no shutdown
OS10(conf-if-po-10)# switchport mode trunk
OS10(conf-if-po-10)# no switchport access vlan
OS10(conf-if-po-10)# exit

OS10(config)# interface ethernet1/1/5
OS10(conf-if-eth1/1/5)# no shutdown
OS10(conf-if-eth1/1/5)# channel-group 10 mode active
OS10(conf-if-eth1/1/5)# no switchport
OS10(conf-if-eth1/1/5)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# no shutdown
OS10(conf-if-po-20)# switchport mode trunk
OS10(conf-if-po-20)# no switchport access vlan
OS10(conf-if-po-20)# exit

OS10(config)# interface ethernet1/1/6
OS10(conf-if-eth1/1/6)# no shutdown
OS10(conf-if-eth1/1/6)# channel-group 20 mode active
OS10(conf-if-eth1/1/6)# no switchport
OS10(conf-if-eth1/1/6)# exit
```

#### 6. 将访问端口添加到虚拟网络

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# member-interface port-channel 10 vlan-tag 100
OS10(config-vn)# exit

OS10(config)# virtual-network 20000
OS10(config-vn-20000)# member-interface port-channel 20 untagged
OS10(config-vn)# exit
```

#### 7. 配置面向上游网络的端口

```
OS10(config)# interface ethernet1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# mtu 1650
OS10(conf-if-eth1/1/1)# ip address 172.19.1.0/31
OS10(conf-if-eth1/1/1)# exit

OS10(config)# interface ethernet1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# mtu 1650
OS10(conf-if-eth1/1/2)# ip address 172.19.2.0/31
OS10(conf-if-eth1/1/2)# exit
```

#### 8. 配置 eBGP

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# router-id 172.19.0.1
OS10(config-router-bgp-100)# address-family ipv4 unicast
```

```
OS10(configure-router-bgp-af)# redistribute connected
OS10(configure-router-bgp-af)# exit
```

## 9. 针对 IPv4 点对点等配置 eBGP

```
OS10(config-router-bgp-100)# neighbor 172.19.1.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-100)# neighbor 172.19.2.1
OS10(config-router-neighbor)# remote-as 102
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 10. 为 BGP EVPN 对等配置与 VLT 对等方 IP 地址不同的环回接口

```
OS10(config)# interface loopback1
OS10(conf-if-lo-1)# no shutdown
OS10(conf-if-lo-1)# ip address 172.19.0.1/32
OS10(conf-if-lo-1)# exit
```

## 11. 配置 BGP EVPN 对等

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172.201.0.1
OS10(config-router-neighbor)# remote-as 101
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-100)# neighbor 172.202.0.1
OS10(config-router-neighbor)# remote-as 102
OS10(config-router-neighbor)# ebgp-multihop 4
OS10(config-router-neighbor)# send-community extended
OS10(config-router-neighbor)# update-source loopback1
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-bgp-neighbor-af)# no activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-bgp-neighbor-af)# activate
OS10(config-router-bgp-neighbor-af)# exit
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 12. 配置 EVPN

在手动配置模式下配置 EVPN 实例、RD 和 RT:

```
OS10(config)# evpn
OS10(config-evpn)# evi 10000
OS10(config-evpn-evi-10000)# vni 10000
OS10(config-evpn-evi-10000)# rd 192.168.2.1:10000
OS10(config-evpn-evi-10000)# route-target 99:10000 import
OS10(config-evpn-evi-10000)# route-target 100:10000 both
OS10(config-evpn-evi-10000)# exit

OS10(config-evpn)# evi 20000
OS10(config-evpn-evi-20000)# vni 20000
OS10(config-evpn-evi-20000)# rd 192.168.2.1:20000
OS10(config-evpn-evi-20000)# route-target 99:20000 import
```

```
OS10(config-evpn-evi-20000)# route-target 100:20000 both
OS10(config-evpn-evi-20000)#exit
OS10(config-evpn)#
```

### 13. 配置 VLT

#### 为虚拟网络配置 VLTi VLAN

```
OS10(config)# virtual-network 10000
OS10(config-vn-10000)# vlti-vlan 100
OS10(config-vn-10000)# exit

OS10(config)# virtual-network 20000
OS10(config-vn-20000)# vlti-vlan 200
OS10(config-vn-20000)# exit
```

#### 配置专用 L3 承载路径，以在发生网络故障时访问 VLT 对等方

```
OS10(config)# interface vlan4000
OS10(config-if-vl-4000)# no shutdown
OS10(config-if-vl-4000)# ip address 172.16.250.11/31
OS10(config-if-vl-4000)# exit
```

#### 配置 VLT 端口通道

```
OS10(config)# interface port-channel10
OS10(conf-if-po-10)# vlt-port-channel 10
OS10(conf-if-po-10)# exit

OS10(config)# interface port-channel20
OS10(conf-if-po-20)# vlt-port-channel 20
OS10(conf-if-po-20)# exit
```

#### 配置 VLTi 成员链路

```
OOS10(config)# interface ethernet1/1/3
OS10(conf-if-eth1/1/3)# no shutdown
OS10(conf-if-eth1/1/3)# no switchport
OS10(conf-if-eth1/1/3)# exit

OS10(config)# interface ethernet1/1/4
OS10(conf-if-eth1/1/4)# no shutdown
OS10(conf-if-eth1/1/4)# no switchport
OS10(conf-if-eth1/1/4)# exit
```

#### 配置 VLT 域

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.150.4
OS10(conf-vlt-1)# discovery-interface ethernet1/1/3,1/1/4
OS10(conf-vlt-1)# vlt-mac aa:bb:cc:dd:ff:ee
OS10(conf-vlt-1)# exit
```

#### 使用上行链路 VLT 端口和下行链路网络端口配置 UFD

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# enable
OS10(conf-uplink-state-group-1)# downstream ethernet1/1/1-1/1/2
OS10(conf-uplink-state-group-1)# upstream port-channel10
OS10(conf-uplink-state-group-1)# upstream port-channel20
OS10(conf-uplink-state-group-1)# exit
```

#### 在 VLT 对等方之间配置 iBGP IPv4 对等

```
OS10(config)# router bgp 100
OS10(config-router-bgp-100)# neighbor 172.16.250.10
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
```

```
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-100)# exit
```

## 14. 在覆盖网络中配置 IP 路由

### 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(conf-vrf)# exit
```

### 配置任意广播网关 MAC 地址

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

### 在虚拟网络上配置路由

```
OS10(config)# interface virtual-network10000
OS10(conf-if-vn-10000)# ip vrf forwarding tenant1
OS10(conf-if-vn-10000)# ip address 10.1.0.234/16
OS10(conf-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(conf-if-vn-10000)# no shutdown
OS10(conf-if-vn-10000)# exit

OS10(config)# interface virtual-network20000
OS10(conf-if-vn-20000)# ip vrf forwarding tenant1
OS10(conf-if-vn-20000)# ip address 10.2.0.234/16
OS10(conf-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(conf-if-vn-20000)# no shutdown
OS10(conf-if-vn-20000)# exit
```

## 主干交换机 1

### 1. 在承载链路上配置指向分支交换机的下游端口

```
OS10(config)# interface ethernet1/1/1
OS10(conf-if-eth1/1/1)# no shutdown
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# ip address 172.16.1.1/31
OS10(conf-if-eth1/1/1)# exit
OS10(config)# interface ethernet1/1/2
OS10(conf-if-eth1/1/2)# no shutdown
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# ip address 172.17.1.1/31
OS10(conf-if-eth1/1/2)# exit
OS10(config)# interface ethernet1/1/3
OS10(conf-if-eth1/1/3)# no shutdown
OS10(conf-if-eth1/1/3)# no switchport
OS10(conf-if-eth1/1/3)# ip address 172.18.1.1/31
OS10(conf-if-eth1/1/3)# exit
OS10(config)# interface ethernet1/1/4
OS10(conf-if-eth1/1/4)# no shutdown
OS10(conf-if-eth1/1/4)# no switchport
OS10(conf-if-eth1/1/4)# ip address 172.19.1.1/31
OS10(conf-if-eth1/1/4)# exit
```

### 2. 配置 eBGP

```
OS10(config)# router bgp 101
OS10(config-router-bgp-101)# router-id 172.201.0.1
OS10(config-router-bgp-101)# address-family ipv4 unicast
OS10(configure-router-bgpv4-af)# redistribute connected
OS10(configure-router-bgpv4-af)# exit
```

### 3. 在 P2P 链路上配置 eBGP IPv4 对等节点会话

```
OS10(conf-router-bgp-101)# neighbor 172.16.1.0
OS10(conf-router-neighbor)# remote-as 99
OS10(conf-router-neighbor)# no shutdown
```

```

OS10(conf-router-neighbor)# exit

OS10(conf-router-bgp-101)# neighbor 172.17.1.0
OS10(conf-router-neighbor)# remote-as 99
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# exit

OS10(conf-router-bgp-101)# neighbor 172.18.1.0
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# exit

OS10(conf-router-bgp-101)# neighbor 172.19.1.0
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# exit
OS10(conf-router-bgp-101)# exit

```

#### 4. 为 BGP EVPN 对等节点配置环回接口

```

OS10(config)# interface loopback1
OS10(config-if-lo-1)# no shutdown
OS10(config-if-lo-1)# ip address 172.201.0.1/32
OS10(config-if-lo-1)# exit

```

#### 5. 配置 BGP EVPN 对等节点会话

```

OS10(config)# router bgp 101
OS10(conf-router-bgp-101)# neighbor 172.16.0.1
OS10(conf-router-neighbor)# ebgp-multihop 4
OS10(conf-router-neighbor)# remote-as 99
OS10(conf-router-neighbor)# send-community extended
OS10(conf-router-neighbor)# update-source loopback1
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no activate
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# address-family l2vpn evpn
OS10(conf-router-neighbor-af)# activate
OS10(conf-router-neighbor-af)# exit

OS10(conf-router-bgp-101)# neighbor 172.17.0.1
OS10(conf-router-neighbor)# ebgp-multihop 4
OS10(conf-router-neighbor)# remote-as 99
OS10(conf-router-neighbor)# send-community extended
OS10(conf-router-neighbor)# update-source loopback1
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no activate
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# address-family l2vpn evpn
OS10(conf-router-neighbor-af)# activate
OS10(conf-router-neighbor-af)# exit

OS10(conf-router-bgp-101)# neighbor 172.18.0.1
OS10(conf-router-neighbor)# ebgp-multihop 4
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# send-community extended
OS10(conf-router-neighbor)# update-source loopback1
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no activate
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# address-family l2vpn evpn
OS10(conf-router-neighbor-af)# activate
OS10(conf-router-neighbor-af)# exit

OS10(conf-router-bgp-101)# neighbor 172.19.0.1
OS10(conf-router-neighbor)# ebgp-multihop 4
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# send-community extended
OS10(conf-router-neighbor)# update-source loopback1

```



```
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# address-family ipv4 unicast
OS10(config-router-neighbor-af)# no activate
OS10(config-router-neighbor-af)# exit
OS10(config-router-neighbor)# address-family l2vpn evpn
OS10(config-router-neighbor-af)# activate
OS10(config-router-neighbor-af)# exit
```

## 主干交换机 2

### 1. 在承载链路上配置指向分支交换机的下游端口

```
OS10(config)# interface ethernet1/1/1
OS10(config-if-eth1/1/1)# no shutdown
OS10(config-if-eth1/1/1)# no switchport
OS10(config-if-eth1/1/1)# ip address 172.16.2.1/31
OS10(config-if-eth1/1/1)# exit
OS10(config)# interface ethernet1/1/2
OS10(config-if-eth1/1/2)# no shutdown
OS10(config-if-eth1/1/2)# no switchport
OS10(config-if-eth1/1/2)# ip address 172.17.2.1/31
OS10(config-if-eth1/1/2)# exit
OS10(config)# interface ethernet1/1/3
OS10(config-if-eth1/1/3)# no shutdown
OS10(config-if-eth1/1/3)# no switchport
OS10(config-if-eth1/1/3)# ip address 172.18.2.1/31
OS10(config-if-eth1/1/3)# exit
OS10(config)# interface ethernet1/1/4
OS10(config-if-eth1/1/4)# no shutdown
OS10(config-if-eth1/1/4)# no switchport
OS10(config-if-eth1/1/4)# ip address 172.19.2.1/31
OS10(config-if-eth1/1/4)# exit
```

### 2. 配置 eBGP

```
OS10(config)# router bgp 102
OS10(config-router-bgp-102)# router-id 172.202.0.1
OS10(config-router-bgp-102)# address-family ipv4 unicast
OS10(configure-router-bgpv4-af)# redistribute connected
OS10(configure-router-bgpv4-af)# exit
```

### 3. 在 P2P 链路上配置 eBGP IPv4 对等节点会话

```
OS10(config-router-bgp-102)# neighbor 172.16.2.0
OS10(config-router-neighbor)# remote-as 99
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-102)# neighbor 172.17.2.0
OS10(config-router-neighbor)# remote-as 99
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-102)# neighbor 172.18.2.0
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit

OS10(config-router-bgp-102)# neighbor 172.19.2.0
OS10(config-router-neighbor)# remote-as 100
OS10(config-router-neighbor)# no shutdown
OS10(config-router-neighbor)# exit
OS10(config-router-bgp-102)# exit
```

### 4. 为 BGP EVPN 对等节点配置环回接口

```
OS10(config)# interface loopback1
OS10(config-if-lo-1)# no shutdown
```

```
OS10(conf-if-lo-1)# ip address 172.202.0.1/32
OS10(conf-if-lo-1)# exit
```

## 5. 配置 BGP EVPN 对等节点会话

```
OS10(config)# router bgp 102
OS10(conf-router-bgp-102)# neighbor 172.16.0.1
OS10(conf-router-neighbor)# ebgp-multihop 4
OS10(conf-router-neighbor)# remote-as 99
OS10(conf-router-neighbor)# send-community extended
OS10(conf-router-neighbor)# update-source loopback1
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no activate
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# address-family l2vpn evpn
OS10(conf-router-neighbor-af)# activate
OS10(conf-router-neighbor-af)# exit

OS10(conf-router-bgp-102)# neighbor 172.17.0.1
OS10(conf-router-neighbor)# ebgp-multihop 4
OS10(conf-router-neighbor)# remote-as 99
OS10(conf-router-neighbor)# send-community extended
OS10(conf-router-neighbor)# update-source loopback1
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no activate
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# address-family l2vpn evpn
OS10(conf-router-neighbor-af)# activate
OS10(conf-router-neighbor-af)# exit

OS10(conf-router-bgp-102)# neighbor 172.18.0.1
OS10(conf-router-neighbor)# ebgp-multihop 4
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# send-community extended
OS10(conf-router-neighbor)# update-source loopback1
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no activate
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# address-family l2vpn evpn
OS10(conf-router-neighbor-af)# activate
OS10(conf-router-neighbor-af)# exit

OS10(conf-router-bgp-102)# neighbor 172.19.0.1
OS10(conf-router-neighbor)# ebgp-multihop 4
OS10(conf-router-neighbor)# remote-as 100
OS10(conf-router-neighbor)# send-community extended
OS10(conf-router-neighbor)# update-source loopback1
OS10(conf-router-neighbor)# no shutdown
OS10(conf-router-neighbor)# address-family ipv4 unicast
OS10(conf-router-neighbor-af)# no activate
OS10(conf-router-neighbor-af)# exit
OS10(conf-router-neighbor)# address-family l2vpn evpn
OS10(conf-router-neighbor-af)# activate
OS10(conf-router-neighbor-af)# exit
```

## VXLAN BGP EVPN 和 BGP EVPN — 多 AS 拓扑

### 1. 验证虚拟网络配置

```
LEAF1# show virtual-network
Codes: DP - MAC-learn Dataplane, CP - MAC-learn Controlplane, UUD - Unknown-Unicast-Drop
Virtual Network: 10000
Members:
 VLAN 100: port-channel10, port-channel1000
VxLAN Virtual Network Identifier: 10000
Source Interface: loopback0(192.168.1.1)
Remote-VTEPs (flood-list): 192.168.2.1(CP)
```

```
Virtual Network: 20000
Members:
 Untagged: port-channel20
VLAN 200: port-channel1000
 VxLAN Virtual Network Identifier: 20000
 Source Interface: loopback0(192.168.1.1)
 Remote-VTEPs (flood-list): 192.168.2.1(CP)
LEAF1#
```

## 2. 验证 EVPN 配置和 EVPN 参数

```
LEAF1# show evpn evi

EVI : 10000, State : up
 Bridge-Domain : Virtual-Network 10000, VNI 10000
 Route-Distinguisher : 1:192.168.1.1:10000
 Route-Targets : 0:99:10000 both, 0:100:10000 import
 Inclusive Multicast : 192.168.2.1
 IRB : Enabled(tenant1)

EVI : 20000, State : up
 Bridge-Domain : Virtual-Network 20000, VNI 20000
 Route-Distinguisher : 1:192.168.1.1:20000
 Route-Targets : 0:99:10000 both, 0:100:10000 import
 Inclusive Multicast : 192.168.2.1
 IRB : Enabled(tenant1)
LEAF1#
```

## 3. 验证分支和主干节点之间的 BGP EVPN 邻居

```
LEAF1# show ip bgp l2vpn evpn summary
BGP router identifier 172.16.0.1 local AS number 99
Neighbor AS MsgRcvd MsgSent Up/Down State/Pfx
172.201.0.1 101 1132 1116 13:29:00 27
172.202.0.1 102 1131 1118 13:29:02 28
LEAF1#
```

## 4. 检查主机 A 和主机 B 之间的连接

```
root@HOST-A:~# ping 10.2.0.10 -c 5
PING 10.2.0.10 (10.2.0.10) 56(84) bytes of data.
64 bytes from 10.2.0.10: icmp_seq=1 ttl=63 time=0.824 ms
64 bytes from 10.2.0.10: icmp_seq=2 ttl=63 time=0.847 ms
64 bytes from 10.2.0.10: icmp_seq=3 ttl=63 time=0.835 ms
64 bytes from 10.2.0.10: icmp_seq=4 ttl=63 time=0.944 ms
64 bytes from 10.2.0.10: icmp_seq=5 ttl=63 time=0.806 ms

--- 10.2.0.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.806/0.851/0.944/0.051 ms
root@HOST-A:~#
```

## 5. 检查主机 A 和主机 C 之间的连接

```
root@HOST-A:~# ping 10.1.0.20 -c 5
PING 10.1.0.20 (10.1.0.20) 56(84) bytes of data.
64 bytes from 10.1.0.20: icmp_seq=1 ttl=64 time=0.741 ms
64 bytes from 10.1.0.20: icmp_seq=2 ttl=64 time=0.737 ms
64 bytes from 10.1.0.20: icmp_seq=3 ttl=64 time=0.772 ms
64 bytes from 10.1.0.20: icmp_seq=4 ttl=64 time=0.799 ms
64 bytes from 10.1.0.20: icmp_seq=5 ttl=64 time=0.866 ms

--- 10.1.0.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4061ms
rtt min/avg/max/mdev = 0.737/0.783/0.866/0.047 ms
root@HOST-A:~#
```

## 6. 检查主机 A 和主机 D 之间的连接

```
root@HOST-A:~# ping 10.2.0.20 -c 5
PING 10.2.0.20 (10.2.0.20) 56(84) bytes of data.
64 bytes from 10.2.0.20: icmp_seq=1 ttl=63 time=0.707 ms
64 bytes from 10.2.0.20: icmp_seq=2 ttl=63 time=0.671 ms
64 bytes from 10.2.0.20: icmp_seq=3 ttl=63 time=0.687 ms
64 bytes from 10.2.0.20: icmp_seq=4 ttl=63 time=0.640 ms
64 bytes from 10.2.0.20: icmp_seq=5 ttl=63 time=0.644 ms

--- 10.2.0.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4089ms
rtt min/avg/max/mdev = 0.640/0.669/0.707/0.041 ms
root@HOST-A:~#
```

 **注：**按照步骤 1 至 6 检查其他主机组合与主机之间的 ping 连接，并通过不同的虚拟网络 IP 地址检查主机之间的连接。

## 示例：VXLAN BGP EVPN — 集中化 L3 网关

以下带有 BGP EVPN 的 VXLAN 示例使用一个集中式第 3 层网关来执行虚拟网络路由。它基于示例配置，[例如：VXLAN BGP EVPN — 多 AS 拓扑](#)。

在 VXLAN BGP EVPN 多 AS 拓扑中，所有 VTEP 都配置为执行分布式 L3 网关路由，在其中，每个 VTEP 都将路由 VXLAN 流量。通过入口 VTEP 进行路由决策。

但是，在多租户网络中，某些 VTEP 只能在第二层 VXLAN 模式下运行，并且仅执行第二层功能。在这种情况下，请在支持第 3 层 VXLAN 功能的第 3 层 VTEP 上配置用于第二层 VTEP 的路由。第 2 层 VXLAN 支持的 VTEP 直接或通过 IP 基础结构与集中式第 3 层网关相连。第 2 层 VTEP 上的任何入口路由流量均切换到第 3 层集中式网关。集中式网关将进行所有路由决策，以将 VXLAN 流量转发到目标第二层 VTEP。

以下适用于 VXLAN BGP EVPN 的集中式 L3 网关示例使用 Clos 分支-主干拓扑。在此示例中：

- VLT 1 中的 VTEP 1 和 VTEP 2 作为 L2 网关运行。
- VLT 2 中的 VTEP 3 和 VTEP 4 作为集中式 L3 网关运行。
- 主机 A 和主机 B 连接到 L2 网关。L2 网关通过 IP 基础结构连接到集中式 L3 网关。
- 您必须在集中式 L3 网关 VTEP 中配置虚拟网络的 IP 地址和任意广播 IP 地址。不需要在 L2 网关 VTEP 中配置这些地址。

在 L2 VTEP 上不执行租户 L3 流量的路由。L2 VTEP 将租户流量转发到 VLT 2 中的集中式 L3 网关。L3 网关将路由 L2 租户段之间的流量。

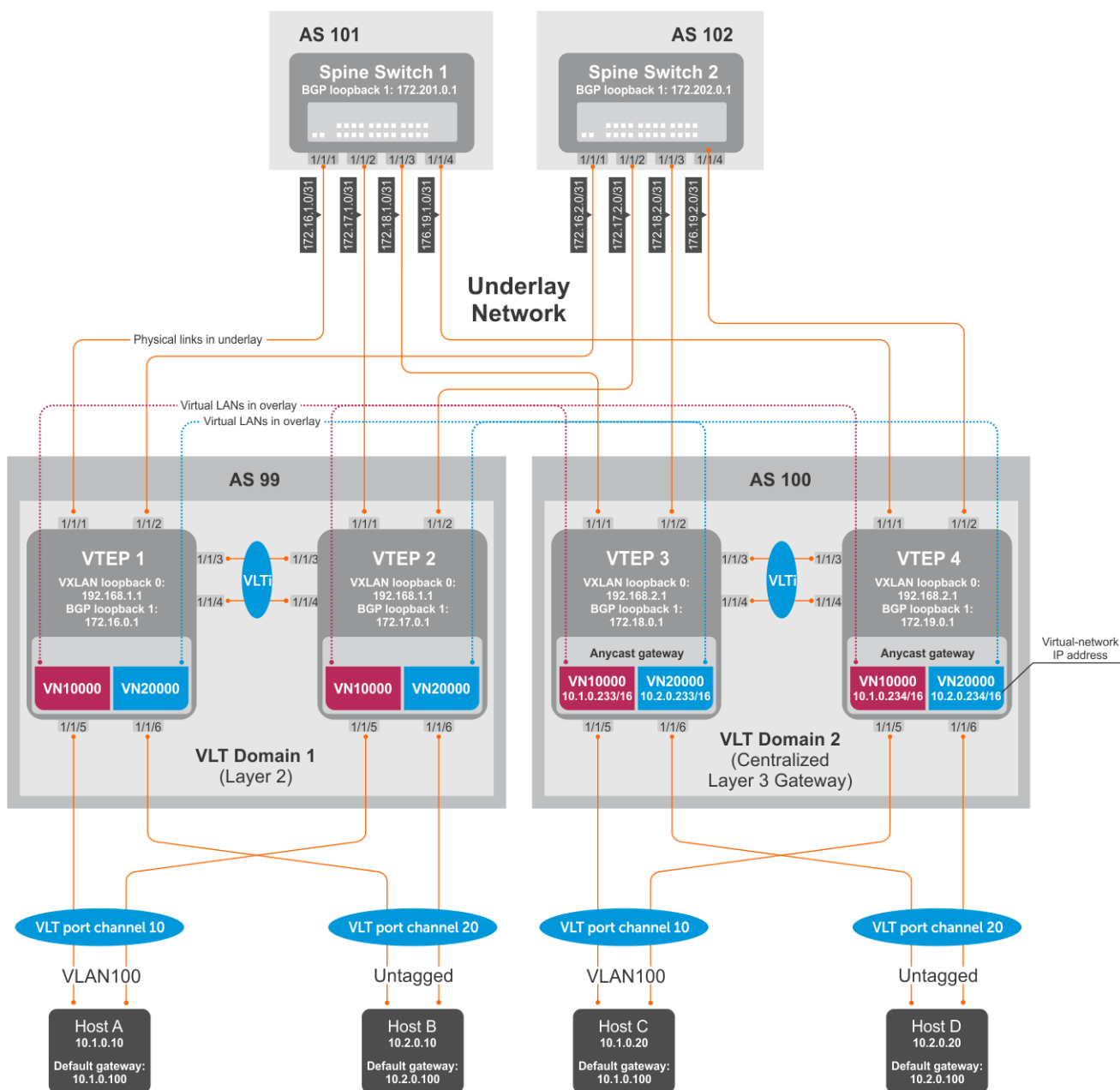


图 15: VXLAN BGP EVPN 与集中式 L3 网关

**注:** 适用于 VXLAN BGP EVPN 的集中式 L3 网关示例使用与示例: [VXLAN BGP EVPN — 多拓扑](#)中相同的配置步骤。将每个主干和分支交换机配置为多 AS 拓扑示例中的各项，以下除外：

- 由于 VTEP 1 和 2 仅在第二层 VXLAN 模式下运行，因此不要在覆盖网络中配置 IP 切换。此步骤包含使用 IP 地址、任意广播 IP 地址和任意广播网关 MAC 地址配置虚拟网络接口。
- 仅在 VTEP 3 和 4 上配置覆盖网络中的 IP 切换。

## VTEP 3 分支交换机

### 14. 在覆盖网络中配置 IP 切换

#### 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(conf-vrf)# exit
```

## 配置任意广播网关 MAC 地址

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

## 在虚拟网络上配置路由

```
OS10(config)# interface virtual-network10000
OS10(conf-if-vn-10000)# ip vrf forwarding tenant1
OS10(conf-if-vn-10000)# ip address 10.1.0.233/16
OS10(conf-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(conf-if-vn-10000)# no shutdown
OS10(conf-if-vn-10000)# exit

OS10(config)# interface virtual-network20000
OS10(conf-if-vn-20000)# ip vrf forwarding tenant1
OS10(conf-if-vn-20000)# ip address 10.2.0.233/16
OS10(conf-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(conf-if-vn-20000)# no shutdown
OS10(conf-if-vn-20000)# exit
```

## VTEP 4 分支交换机

### 14. 在覆盖网络中配置 IP 切换

#### 创建租户 VRF

```
OS10(config)# ip vrf tenant1
OS10(conf-vrf)# exit
```

## 配置任意广播网关 MAC 地址

```
OS10(config)# ip virtual-router mac-address 00:01:01:01:01:01
```

## 在虚拟网络上配置路由

```
OS10(config)# interface virtual-network10000
OS10(conf-if-vn-10000)# ip vrf forwarding tenant1
OS10(conf-if-vn-10000)# ip address 10.1.0.234/16
OS10(conf-if-vn-10000)# ip virtual-router address 10.1.0.100
OS10(conf-if-vn-10000)# no shutdown
OS10(conf-if-vn-10000)# exit

OS10(config)# interface virtual-network20000
OS10(conf-if-vn-20000)# ip vrf forwarding tenant1
OS10(conf-if-vn-20000)# ip address 10.2.0.234/16
OS10(conf-if-vn-20000)# ip virtual-router address 10.2.0.100
OS10(conf-if-vn-20000)# no shutdown
OS10(conf-if-vn-20000)# exit
```

## 示例：VXLAN BGP EVPN — 带有非对称 IRB 的边界分支网关

此 VXLAN BGP EVPN 示例显示了如何将 VXLAN 流量传输到外部网络。来自预定到达互联网的租户主机的流量通过 L3 VTEP 和 IP 基础结构传输到边界分支网关。

**注：**VXLAN 解除封装后，虚拟网络和租户 VLAN 之间的路由仅在 S4200-ON 系列和 S5200-ON 系列上受支持（由于 NPU 功能）。在支持 VXLAN 路由的其他 Dell EMC 交换机上（例如 S4048T-ON、S6010-ON 和 S4100-ON 系列），仅在虚拟网络之间执行解除封装后的路由。您可以将出口虚拟网络连接 to 外部路由器中的 VLAN，该路由器连接到外部网络。

在下面的示例中，VLT 域 1 是 VLT VTEP。VLT 域 2 是边界分支 VLT VTEP 对。数据中心网络中的所有虚拟网络都在具有虚拟网络 IP 和任意广播 IP 网关地址的所有 VTEP 中进行配置。

配置专用虚拟网络以将 VXLAN 流量发送到所有 VTEP 上的外部网络。仅在 VLT 域 2 中的边界分支 VTEP 对上配置专用虚拟网络的任意广播 L3 网关。对于非对称 IRB，请在所有 VTEP 上配置静态默认路由，边界分支 VTEP 除外。这将允许预定发送到外部网络的流量传输到边界分支 VTEP 上的专用虚拟网络的任意广播 L3 地址。在边界分支上配置了不同的静态路由。使用此第二个静态路由，到外部网络的流量将在出口 VLAN 到 WAN 路由器或互联网地址上传输。

当 VLT 域 1 收到发送至外部网络的流量时，流量会路由到入口 VTEP 中的专用虚拟网络，并发送到边界分支 VTEP。在边界分支 VTEP 中，流量将路由到外部 WAN 路由器连接到的 VLAN 或直接连接到互联网。同样，发送到 VXLAN 虚拟网络的任何流量（在边界分支 VTEP 上收到）都将路由到目标虚拟网络。

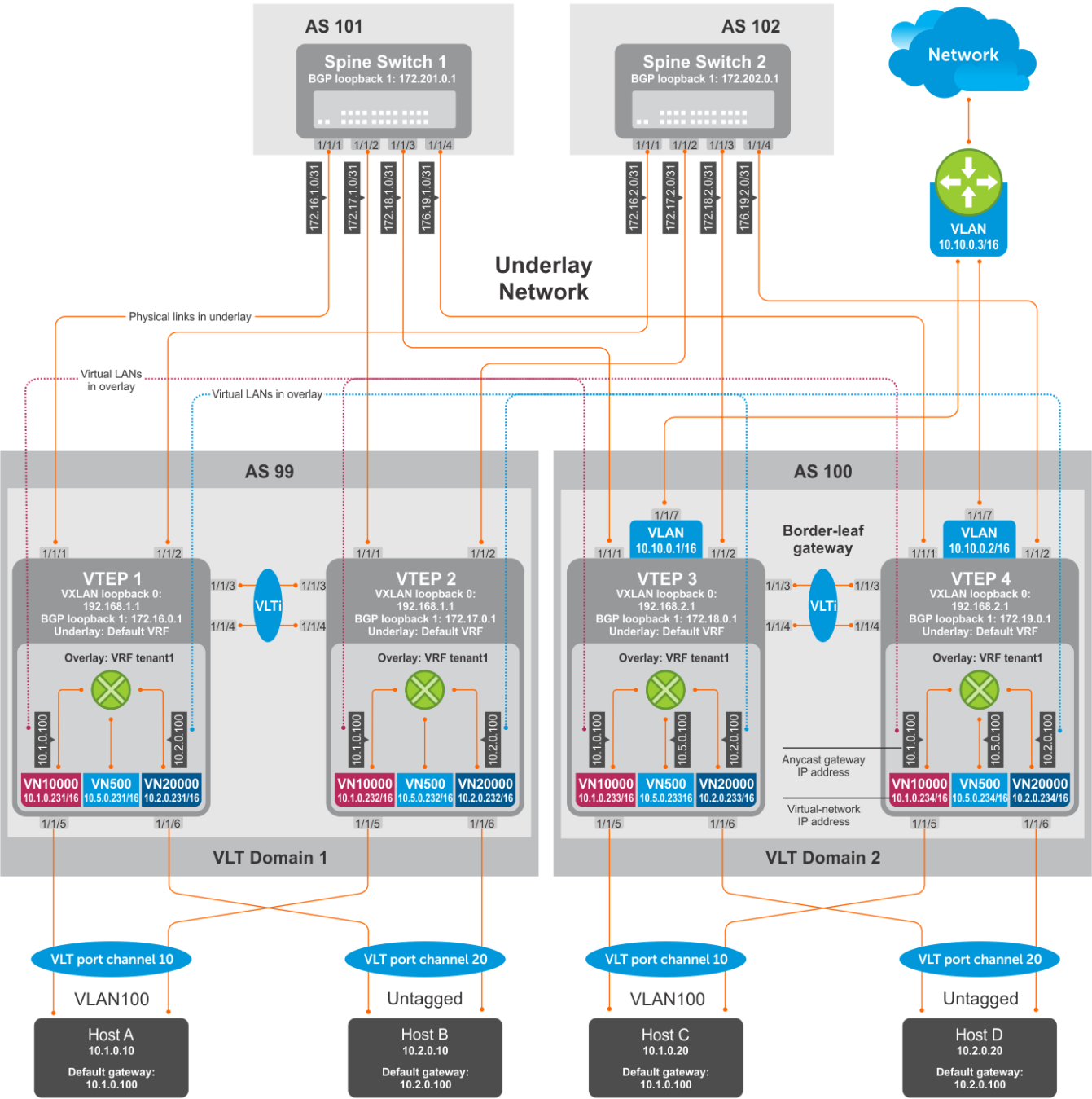


图 16: VXLAN BGP EVPN，带边界分支网关

① 注：适用于 VXLAN BGP EVPN 的边界分支网关示例使用与示例：VXLAN BGP EVPN — 多拓扑中相同的配置步骤。按照多拓扑示例配置每个主干和分支交换机，然后在每个 VTEP 上添加以下额外的配置步骤。

### VTEP 1 分支交换机

#### 14. 配置专用 VXLAN 虚拟网络。

```
OS10(config)# virtual-network 500
OS10(config-vn-500)# vxlan-vni 500
```

```
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit
```

**15. 在虚拟网络上配置路由。**

```
OS10(config)# interface virtual-network 500
OS10(conf-if-vn-10000)# ip vrf forwarding tenant1
OS10(conf-if-vn-10000)# ip address 10.5.0.231/16
```

**16. 为发送到专用虚拟网络的任意广播 MAC 地址的出站流量配置静态路由。**

```
OS10(config)#ip route 0.0.0.0/0 10.5.0.100
```

## VTEP 2 分支交换机

**14. 配置专用 VXLAN 虚拟网络。**

```
OS10(config)# virtual-network 500
OS10(config-vn-500)# vxlan-vni 500
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit
```

**15. 在虚拟网络上配置路由。**

```
OS10(config)# interface virtual-network 500
OS10(conf-if-vn-10000)# ip vrf forwarding tenant2
OS10(conf-if-vn-10000)# ip address 10.5.0.232/16
```

**16. 为发送到专用虚拟网络的任意广播 MAC 地址的出站流量配置静态路由。**

```
OS10(config)#ip route 0.0.0.0/0 10.5.0.100
```

## VTEP 3 分支交换机

**14. 配置专用 VXLAN 虚拟网络。**

```
OS10(config)# virtual-network 500
OS10(config-vn-500)# vxlan-vni 500
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit
```

**15. 配置边界分支 VTEP 上的任意广播网关 MAC 地址。此 MAC 地址必须不同于在非边界分支 VTEP 上配置的任意广播网关 MAC 地址。**

```
OS10(config)# ip virtual-router mac-address 00:02:02:02:02:02
```

**16. 在虚拟网络上配置路由。**

```
OS10(config)# interface virtual-network 500
OS10(conf-if-vn-10000)# ip vrf forwarding tenant1
OS10(conf-if-vn-10000)# ip address 10.5.0.233/16
OS10(conf-if-vn-10000)# ip virtual-router address 10.5.0.100
OS10(conf-if-vn-10000)# no shutdown
OS10(conf-if-vn-10000)# exit
```

**17. 配置外部连接的 VLAN。**

```
OS10(conf)#interface vlan 200
OS10(conf-if-vlan)#ip address 10.10.0.1/16
OS10(conf-if-vlan)#no shutdown
OS10(conf-if-vlan)#exit

OS10(conf)#interface ethernet 1/1/7
```



```
switchport mode trunk
switchport trunk allowed vlan 200
```

#### 18. 为发送到 VLAN 200 的出站流量配置静态路由。

```
OS10(config)#ip route 0.0.0.0/0 10.10.0.3
```

## VTEP 4 分支交换机

#### 14. 配置专用 VXLAN 虚拟网络。

```
OS10(config)# virtual-network 500
OS10(config-vn-500)# vxlan-vni 500
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-10000)# exit
```

#### 15. 配置边界分支 VTEP 上的任意广播网关 MAC 地址。此 MAC 地址必须不同于在非边界分支 VTEP 上配置的任意广播网关 MAC 地址。

```
OS10(config)# ip virtual-router mac-address 00:02:02:02:02:02
```

#### 16. 在虚拟网络上配置路由。

```
OS10(config)# interface virtual-network 500
OS10(conf-if-vn-10000)# ip vrf forwarding tenant1
OS10(conf-if-vn-10000)# ip address 10.5.0.234/16
OS10(conf-if-vn-10000)# ip virtual-router address 10.5.0.100
OS10(conf-if-vn-10000)# no shutdown
OS10(conf-if-vn-10000)# exit
```

#### 17. 配置外部连接的 VLAN。

```
OS10(conf)#interface vlan 200
OS10(conf-if-vlan)#ip address 10.10.0.2/16
OS10(conf-if-vlan)#no shutdown
OS10(conf-if-vlan)#exit

OS10(conf)#interface ethernet 1/1/7
switchport mode trunk
switchport trunk allowed vlan 200
```

#### 18. 为发送到 VLAN 200 的出站流量配置静态路由。

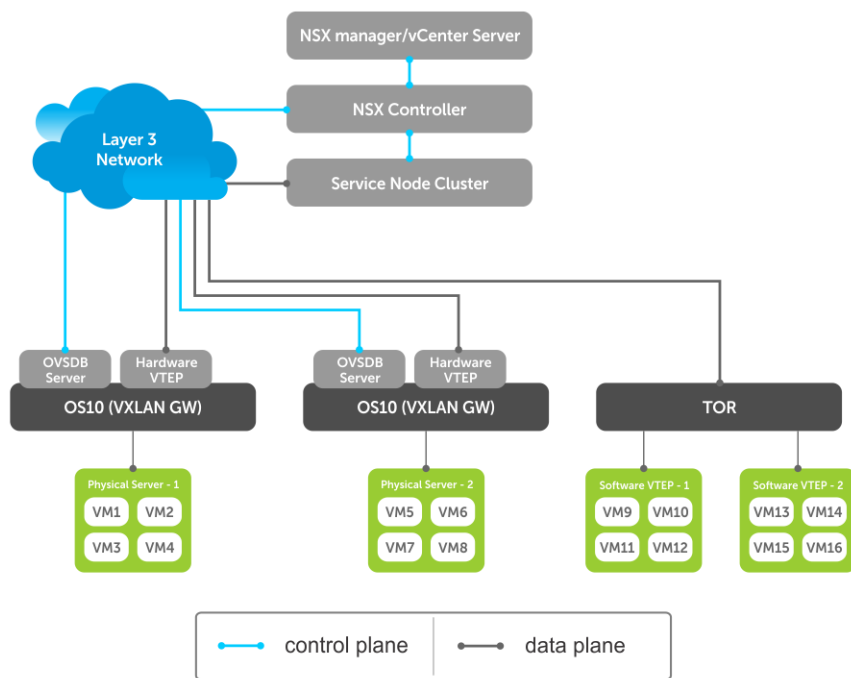
```
OS10(config)#ip route 0.0.0.0/0 10.10.0.3
```

## 控制器调配的 VXLAN

OS10 使用 Open vSwitch Database (OVSDb) 控制器支持 VXLAN 调配。当前，仅受支持的 OVSDb 控制器是 VMware NSX 控制器。在控制器调配的 VXLAN 中，控制器将管理 VXLAN 相关的配置和其他控制平面操作，例如 MAC 地址传播。

**注：**控制器调配的 VXLAN 在 S3048-ON 交换机上不受支持。此外，控制器调配的 VXLAN 在 VLT 域中配置端点的 VTEP 上不受支持。不支持独立模式下的 VTEP。

#### 控制器调配的 VXLAN



NSX 控制器将通过安全套接层 (SSL) 连接使用 OVSDb 管理协议与 OS10 VTEP 通信。在控制器与 VTEP 之间建立通信涉及在 VTEP 生成 SSL 证书并将证书复制到 NSX 控制器。进行 SSL 身份验证后，将在控制器与 VTEP 之间建立通过 SSL 的安全连接。然后，VTEP 将接收和处理来自控制器的进程和配置。

### 控制器调配的 VXLAN：手动配置

您必须使用 OS10 CLI 手动配置基础网络：

- 配置用于基础路由的 L3 路由。对 VTEP 对等节点的基础访问使用配置的路由协议进行学习。
- 配置默认 VRF 中用作 VTEP 源 IP 地址的环回接口，用于基于控制器的调配。
- 分配将由控制器管理的 VTEP 接口。

### 控制器调配的 VXLAN：自动调配

控制器将自动调配

- L2 覆盖网络
- VXLAN 虚拟网络，包括 VTEP 源地址
- 本地访问端口位于虚拟网络中

OS10 VTEP 使用 OVSDb 协议，将 VXLAN 访问端口的服务器 MAC 地址的添加或删除发送到 NSX 控制器。然后，控制器将信息传输到 VTEP 对等节点。VTEP 将编程相应的转发表。

## 配置控制器调配的 VXLAN

要配置 NSX 控制器，请在每个 OS10 VTEP 上执行以下步骤：

1. 配置用于基于控制器的 VXLAN 调配的源接口。将一个 IPv4 地址分配给环回接口。将环回接口分配给 NVE 实例。环回接口必须属于默认的 VRF。有关详细信息，请参阅[在 VTEP 上配置源 IP 地址](#)。
2. 配置 NSX 控制器可访问性。
3. 分配要由控制器管理的本地访问接口。使用 OS10 CLI 创建的成员访问接口的 VLAN ID 必须与由 NSX 控制器为虚拟网络创建的端口限定的 VLAN 的 VLAN ID 不同。
4. (可选) 在 NSX 和 VTEP 中启用 BFD。OS10 符合 RFC5880 双向转发检测。

### 配置说明

- 如果 OS10 交换机在纯 OpenFlow 模式下运行，则不支持 NSX 控制器调配的 VXLAN。
- 一次仅支持一种 VxLAN 调配模式：基于 NSX 控制器的静态 VXLAN 或 BGP EVPN。
- OS10 交换机不会将 VXLAN 访问端口统计信息发送至 NSX 控制器。
- 控制器调配的 VXLAN 在 VLT 域中配置为对等节点的 VTEP 上不受支持。仅支持独立模式下的 VTEP。

## 指定控制器可访问性信息

在 OS10 VTEP 中，控制器配置命令会初始化到基于 OVSDB 的控制器连接。

OS10 一次仅支持一个控制器连接。

 **注：**当前，支持的基于 OVSDB 的控制器仅限 NSX。

要在 OS10 VTEP 上配置 OVSDB 控制器，请执行以下操作：

1. 在 CONFIGURATION 模式下启用 VXLAN。  
`OS10(config)# nve`
2. 将模式更改为 CONFIGURATION-NVE-OVSDB，以配置控制器参数。  
`OS10(config-nve)# controller ovssdb`
3. 在 CONFIGURATION-NVE-OVSDB 模式下，指定 IP 地址、OVSDB 控制器端口和 SSL 作为 OS10 VTEP 与控制器之间的安全连接协议。  
`OS10(config-nve-ovssdb)# ip ip-address port port-number ssl`  
端口号的范围从 0 到 65535。将端口号配置为 6640，将连接类型配置为 SSL。
4. （可选）指定时间间隔（以毫秒 [ms] 为单位）。这是交换机在尝试连接到控制器之间等待的持续时间。  
`OS10(config-nve-ovssdb)# max-backoff interval`  
范围为 1000 到 180000 毫秒。默认值为 8000 毫秒。

```
OS10# configure terminal
OS10(config)# nve
OS10(config-nve)# controller ovssdb
OS10(config-nve-ovssdb)# ip 10.11.66.110 port 6640 ssl
```

## 分配要由控制器管理的接口

在 VTEP 中，为要管理的 OVSDB 控制器明确分配接口。

在分配接口之前，请考虑以下事项：

- 该接口必须处于 Switchport 中继模式。
- 接口不能是任何 VLAN 的成员
- 接口不能是端口通道的成员

当分配要由控制器管理的接口时，如果不满足以上条件，系统会返回错误消息。

分配接口后，您将无法执行以下操作：

- 从 Switchport 中继模式中移除接口
- 添加接口作为任何 VLAN 的成员
- 如果接口具有由控制器配置的活动端口限定的 VLAN（端口、VLAN）对，则从控制器配置中移除该接口。

要分配由 OVSDB 控制器管理的接口，请执行以下操作：

1. 从 CONFIGURATION 模式配置接口。  
`OS10(config)# interface ethernet 1/1/1`
2. 在 INTERFACE 模式下配置 L2 中继。  
`OS10(config-if-eth1/1/1)# switchport mode trunk`
3. 在 INTERFACE 模式下配置分配给 L2 中继端口的访问 VLAN。  
`OS10(config-if-eth1/1/1)# no switchport access vlan`
4. 为控制器分配接口。  
`OS10(config-if-eth1/1/1)# nve-controller`

要查看控制器信息以及控制器管理的端口，请使用 `show nve controller` 命令。

```
OS10# show nve controller

Management IP : 10.16.140.29/16
Gateway IP : 55.55.5.5
Max Backoff : 1000
```

```
Configured Controller : 10.16.140.172:6640 ssl (connected)

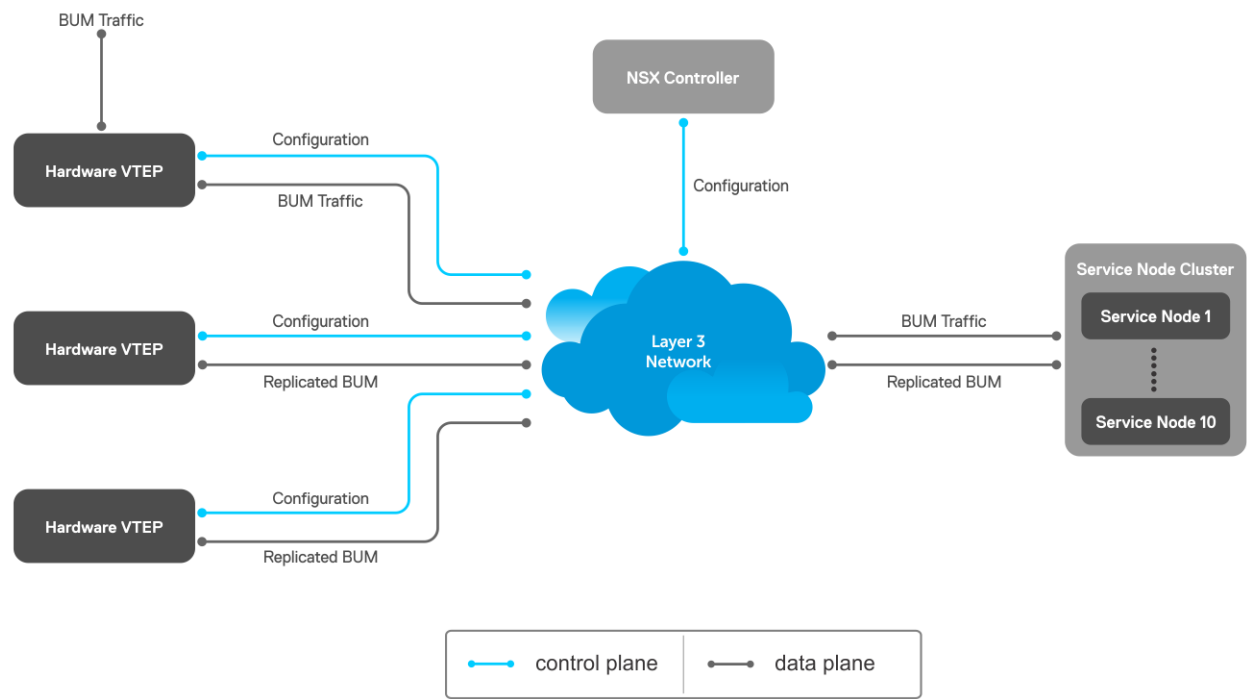
Controller Cluster
IP Port Protocol Connected State Max-Backoff
10.16.140.173 6640 ssl true ACTIVE 1000
10.16.140.171 6640 ssl false BACKOFF 1000
10.16.140.172 6640 ssl true ACTIVE 1000

NVE Controller Ports
ethernet1/1/1:1
ethernet1/1/15
```

## 服务节点

在已调配 NSX 的 VXLAN 环境中，服务节点将复制向所有其他 VTEP 输入 OS10 VTEP 的 L2 广播、未知-单播和多播 (BUM) 流量。要使 BUM 流量的服务节点复制正常工作，您需要在服务节点和 VTEP 之间建立 IP 连接，以便来自 VTEP 的 BUM 流量利用服务节点通过 VXLAN 覆盖访问其他远程 VTEP。NSX 控制器将管理服务节点群集，并通过 OVSDb 协议将节点的 IP 地址发送到 VTEP。服务节点群集将提供冗余，还有助于跨服务节点对 BUM 流量进行负载均衡。

下面显示了在控制器调配的 VXLAN 环境中的 BUM 流量复制：



由于 VTEP 依赖于服务节点来复制 BUM 流量，因此我们需要一种机制来监控 VTEP 与服务节点之间的连接。BFD 可用于监控 VTEP 与服务节点之间的连接，并检测故障。NSX 控制器提供用于在 VTEP 和服务节点之间启动 BFD 会话的参数，例如最小 TX 和 RX 间隔以及乘数。要建立 BFD 会话，请在控制器和 VTEP 上启用 BFD。要在 VTEP 中启用 BFD，请使用 `bfd enable` 命令。

**注：**在控制器调配的 VXLAN 中，VTEP 使用控制器提供的参数而不是在 VTEP 上配置的参数与服务节点建立 BFD 会话。

如果 VTEP 中未启用 BFD，则 VTEP 将使用 IP 可访问性信息来监控与服务节点的连接。

要查看已建立的会话，请使用 `show bfd neighbors` 命令。

```
OS10# show bfd neighbors
* - Active session role

LocalAddr RemoteAddr Interface State RxInt TxInt Mult VRF Clients

```

|   |           |         |                  |    |      |      |   |         |       |
|---|-----------|---------|------------------|----|------|------|---|---------|-------|
| * | 55.55.5.5 | 2.2.2.2 | virtual-network0 | up | 1000 | 1000 | 3 | default | vxlan |
| * | 55.55.5.5 | 2.2.2.3 | virtual-network0 | up | 1000 | 1000 | 3 | default | vxlan |

## 查看复制器

要查看复制器的状态，请使用 `show nve replicators` 命令。

- 显示包含从控制器收到的复制器的详细信息的输出。

```
OS10# show nve replicators
Codes: * - Active Replicator

BFD Status:Enabled
Replicators State

2.2.2.3 Up
2.2.2.2 Up
```

- 显示有关 VNID 可用复制器的详细信息的输出。

```
OS10# show nve replicators vnid 10009
Codes: * - Active Replicator

BFD Status:Enabled
Replicators State

2.2.2.3 Up
2.2.2.2* Up
```

\* — 指示 VTEP 针对特定 VNID 发送 BUM 流量的复制器。

## 从 VMware vCenter 配置和控制 VXLAN

您可以在 VMware vCenter GUI 配置和控制 VXLAN。完成以下步骤：

- 在 CONFIGURATION 模式下，在 OS10 交换机上生成 SSL 证书。

```
OS10# nve controller ssl-key-generate
```

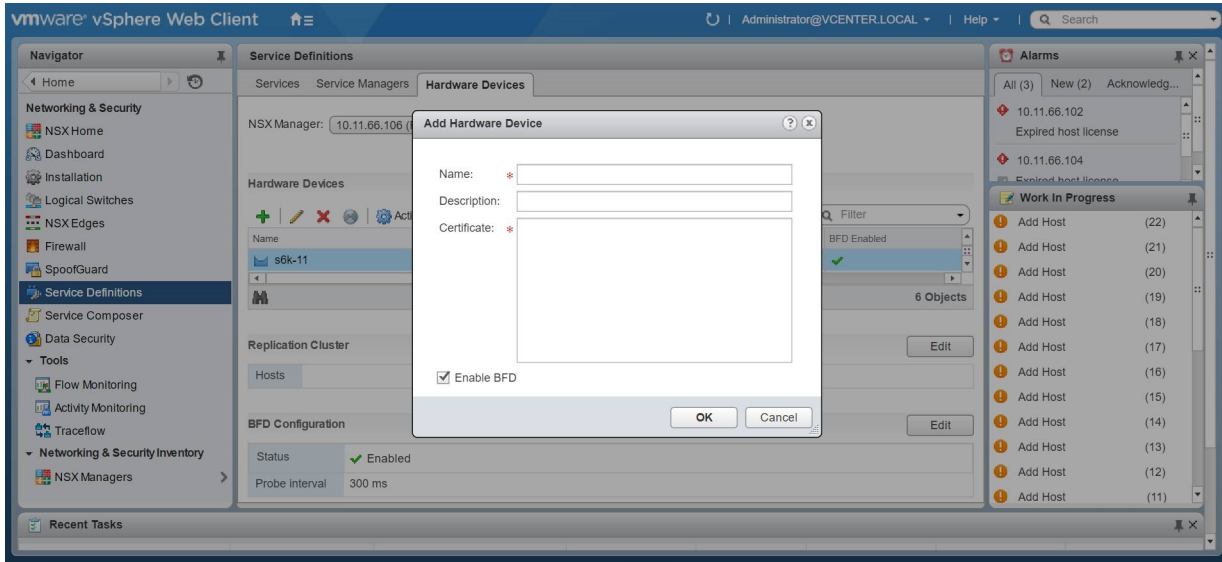
使用 `show nve controller ssl-certificate` 命令可验证或查看证书。

```
OS10# show nve controller ssl-certificate
-----BEGIN CERTIFICATE-----
MIIDgDCCAmgCAQMwDQYJKoZIhvcNAQENBQAwgYExCzAJBgNVBAYTAlVTMQswCQYD
VQQIDAJDQTEVMBMGA1UECgwMT3BlbiB2U3dpdGNoMREwDwYDVQQLEDAhZD210Y2hj
YTE7MDkGA1UEAwwyTlZTIHN3aXRjaGNoIENBIENlcnRpZmljYXRlICgyMDE4IFNl
cCAyMyAwMzo0NzoyMCKwHhcNMjgwOTI0MTYzMDUyWhcNMjgwOTI0MTYzMDUyWjCB
iTELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAkNBMRUwEwYDVQQKDAxPcGVuIHZTd210
Y2gxHzAdBgNVBASMFk9wZW4gd1N3aXRjaCBjZXJ0aWZpZXIwNTAzBgNVBAMMLGRl
bGwgaWQ6MGVlZmUyWmMwLTkzOTEtN2RlMmMwY2JmMTJjMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAsMlD4c4fWwy+5t6VScjizlkFsNzEBOK5PJyI3B6Re
RK/J14Fdxio1YmzG0YObjxiwjpUYEsqPL3Nvh0f10KMqwgqJVBdf6sXWHUVw+9A7c
IfRh0aRI+HIYyUC4YD48GlnVnaCqhYyA0tcMzJm4r2k7A7wJUL0pDXiqS3uJwGmf
xlhvmFio8EeHM/Z79DkBRD6FUMwacAnb3yCIKZH50AWq7qRmmGNZOgYUT+8oaj5tO/
hEQfDYuv32E5z4d3FhiBJMFT86T4YvpJYyJkiKmaQWInkthLV3VxEMXI5vJQclMh
wYbKfPB4hh3+qdS5o+uVco76CVrcWi7rO3XmsBkbnQIDAQABMA0GCSqGSIb3DQEB
DQUAA4IBAQAUFVD20GcHD8zdpYf0YaP4b6TuonUzF0jwoV+Qr9b4kOjEBGuoPdev
X3AeV/dvAa2Q6oliOBM5z74NgHizhr067pFP841Nv7DAVb7cPHHSSTTSeeJjIVMh0k
v0KkVefsYuI4r1jqJxu0GZgBinqehXxVKlceouLvwbhb1MFYXN3lcE2AXR746q1V
ic6stNkxf3nrlOpSDz3P4VOnbAnIrY+SvUVmAT0tdrowH99y2AzoAxUH0dWsH8Ej
CFch7VilmCVVhyghXdfyl6lv/F6vMRwj343BpBW3QsGj68ROX0ILrtOz/2q5oUb/rp
Jd15KFFN3itT/xYBfZ1ZdLYd5F
-----END CERTIFICATE-----
```

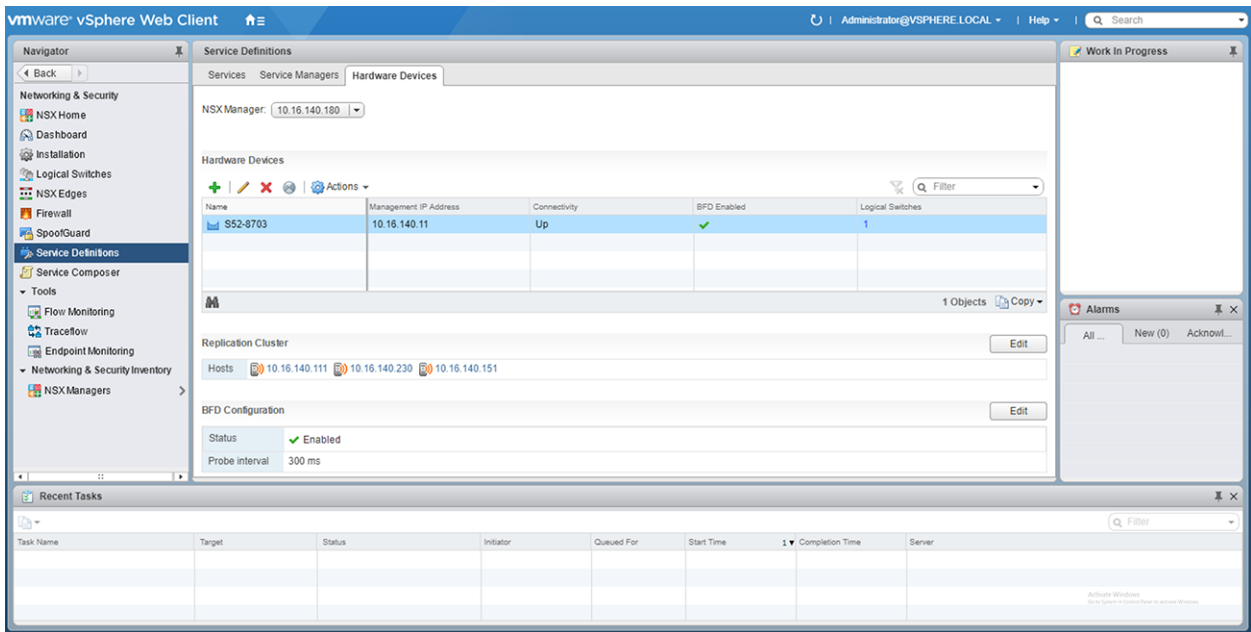
- 在 VMware vCenter 控制台中创建 VXLAN 网关。

以下步骤将配置 VXLAN 网关：

- 打开浏览器窗口，输入 vCenter 的 IP 地址，然后登录 VMware vCenter。
- 单击左侧导航窗格中的 **Service Definitions**。
- 单击 **Hardware Devices** 选项卡。
- 单击 **Hardware Devices** 下的绿色 + 图标以添加设备。此时，**Add Hardware Device** 对话框窗口会打开。
- 在 **Name** 框中输入设备的名称，并复制 OS10 交换机中生成的证书，并将其粘贴到 **Certificate** 框，然后单击 **OK**。



如果在 VTEP 和 NSX 控制器之间成功建立连接，则控制台将显示控制器与 VTEP 的管理 IP 地址之间的当前连接状态。

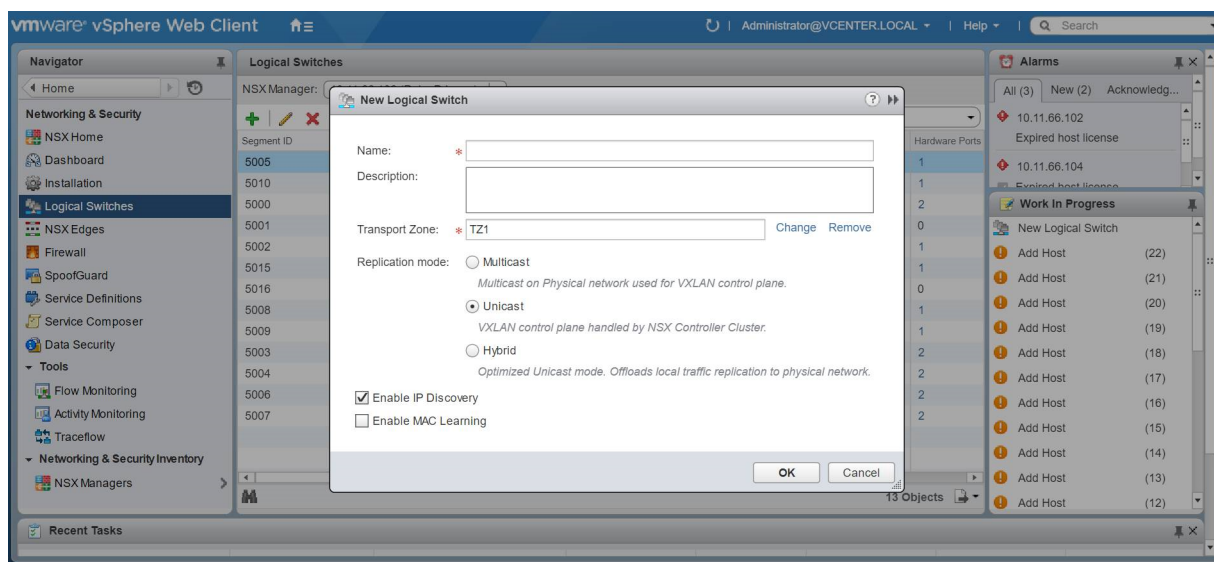


### 3. 创建逻辑交换机。

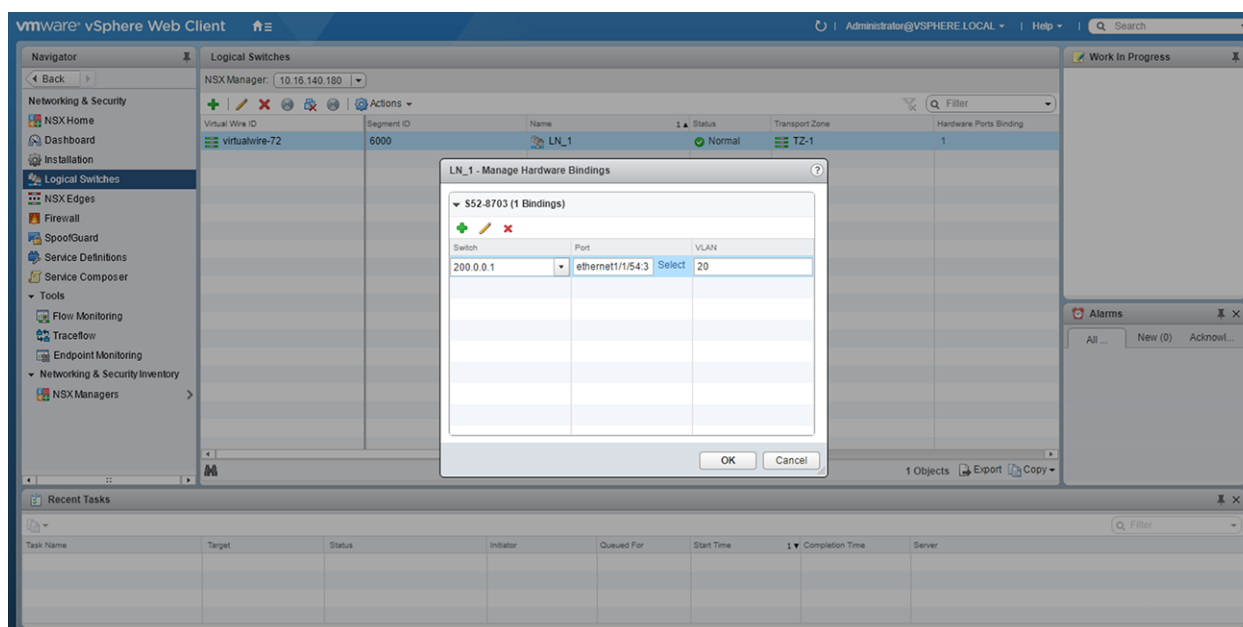
您可以创建逻辑网络，将其用作在物理和虚拟基础架构上进行虚拟化和非虚拟化服务器工作负载的转发域。

以下步骤可为 NSX 控制器管理配置逻辑交换机。

- 从左侧导航窗格中单击 **Logical Switches**。
- 单击 **Logical Switches** 下的绿色 + 图标。此时将打开 **New Logical Switch** 对话框窗口。
- 输入名称并选择 **Unicast** 作为复制模式，然后单击 **OK**



4. 创建逻辑交换机端口，为虚拟机接口 (VIF) 和外部网络的 L2 网关连接提供逻辑连接点。

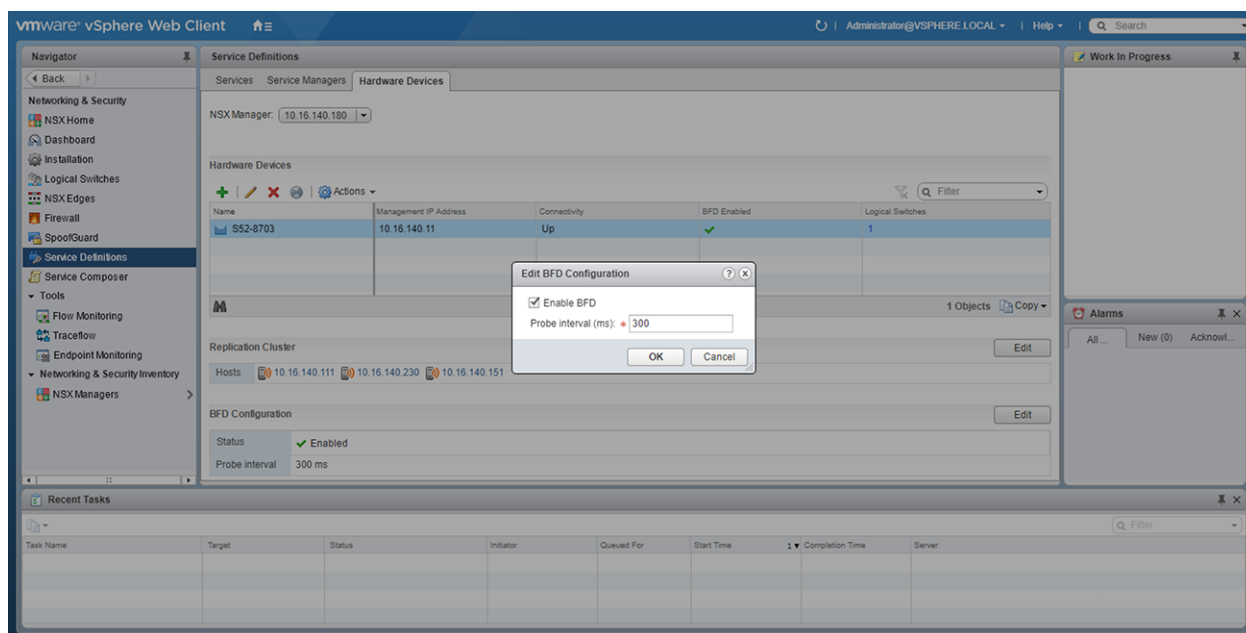


5. (可选) 全局启用或禁用 BFD。
 

以下步骤将启用或禁用控制器中的 BFD 配置。

  - a. 单击左侧导航窗格中的 **Service Definitions**。
  - b. 单击 **Hardware Devices** 选项卡。
  - c. 单击 **BFD Configuration** 中的 **Edit** 按钮。
  - d. 如果需要，选中或清除 **ENABLE BFD** 复选框并提供 **Probe interval** (以毫秒为单位)。



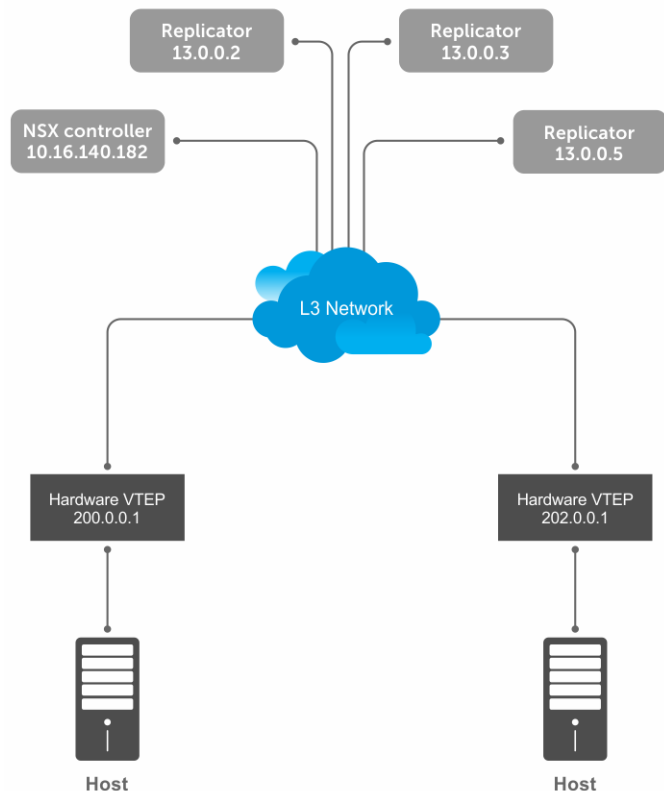


在服务器虚拟机上配置 VMware NSX 控制器后，从 VXLAN 网关 交换机连接到该控制器。

有关 VTEP 中的 NSX 控制器配置的详细信息，请参阅[配置与 OVSDB 控制器的连接](#)。有关 NSX 控制器配置的详细信息，请参阅 VMware 提供的 *NSX User Guide*。

## 示例：具有控制器配置的 VXLAN

此示例显示了在 VXLAN 环境中部署的简单 NSX 控制器和硬件 OS10 VTEP。



要配置 NSX 控制器调配的 VXLAN，请执行以下操作：

- 在 OS10 VTEP 中配置控制器和要由控制器管理的接口。



- 在 VMware vCenter 中配置 NSX 控制器。有关使用 GUI 配置 NSX 控制器的详细信息，请参阅[从 VMware vCenter 配置和控制 VXLAN](#)。

您必须使用控制器配置来配置 OS10 VTEP，以便 VTEP 可以与 NSX 控制器通信。NSX 控制器将处理 VXLAN 环境中的配置和控制面操作。

## VTEP 1

1. 在基础中配置 OSPF 协议。

```
OS10# configure terminal
OS10(config)# router ospf 1
OS10(config)# exit
OS10(config)# interface ethernet 1/1/55:1
OS10(config-if-eth1/1/55:1)# no switchport
OS10(config-if-eth1/1/55:1)# ip ospf 1 area 0.0.0.0
OS10(config-if-eth1/1/55:1)# exit
```

2. 配置环回接口。

```
OS10(config)# interface loopback 1
OS10(config-if-lo-1)# no shutdown
OS10(config-if-lo-1)# ip address 200.0.0.1/32
OS10(config-if-lo-1)# exit
```

3. 创建 NVE 实例并将环回接口配置为 VXLAN 源隧道接口。

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback 1
```

4. 指定 NSX 控制器可访问性信息。

```
OS10(config-nve)# controller ovssdb
OS10(config-nve-ovssdb)# ip 10.16.140.182 port 6640 ssl
OS10(config-nve-ovssdb)# max-backoff 10000
OS10(config-nve-ovssdb)# exit
```

5. 分配要由控制器管理的接口。

```
OS10(config)# interface ethernet 1/1/54:3
OS10(config-if-eth1/1/54:3)# switchport mode trunk
OS10(config-if-eth1/1/54:3)# no switchport access vlan
OS10(config-if-eth1/1/54:3)# nve-controller
```

6. (可选) 启用 BFD。

```
OS10(config)# bfd enable
```

## VTEP 2

1. 在基础中配置 OSPF 协议。

```
OS10# configure terminal
OS10(config)# router ospf 1
OS10(config)# exit
OS10(config)# interface ethernet 1/1/23:1
OS10(config-if-eth1/1/23:1)# no switchport
OS10(config-if-eth1/1/23:1)# ip ospf 1 area 0.0.0.0
OS10(config-if-eth1/1/23:1)# exit
```

2. 配置环回接口。

```
OS10(config)# interface loopback 1
OS10(config-if-lo-1)# no shutdown
OS10(config-if-lo-1)# ip address 202.0.0.1/32
OS10(config-if-lo-1)# exit
```

### 3. 创建 NVE 实例并将环回接口配置为 VXLAN 源隧道接口。

```
OS10(config)# nve
OS10(config-nve)# source-interface loopback 1
```

### 4. 指定 NSX 控制器可访问性信息。

```
OS10(config-nve)# controller ovssdb
OS10(config-nve-ovssdb)# ip 10.16.140.182 port 6640 ssl
OS10(config-nve-ovssdb)# max-backoff 10000
OS10(config-nve-ovssdb)# exit
```

### 5. 分配要由控制器管理的接口。

```
OS10(config)# interface ethernet 1/1/25:3
OS10(config-if-eth1/1/25:3)# switchport mode trunk
OS10(config-if-eth1/1/25:3)# no switchport access vlan
OS10(config-if-eth1/1/25:3)# nve-controller
```

### 6. (可选) 启用 BFD。

```
OS10(config)# bfd enable
```

## 验证控制器配置

### VTEP 1

要查看有关 VTEP 1 上基于控制器的信息，请使用 `show nve controller` 命令。

```
OS10# show nve controller

Management IP : 10.16.140.11/16
Gateway IP : 200.0.0.1
Max Backoff : 10000
Configured Controller : 10.16.140.181:6640 ssl (connected)

Controller Cluster
IP Port Protocol Connected State Max-Backoff
10.16.140.182 6640 ssl true ACTIVE 10000
10.16.140.183 6640 ssl true ACTIVE 10000
10.16.140.181 6640 ssl true ACTIVE 10000

NVE Controller Ports
ethernet1/1/54:3
```

要显示 VXLAN 的 VNID、端口成员、源接口和远程 VTEP，请使用 `show virtual-network` 命令。

```
OS10# show virtual-network
Codes: DP - MAC-learn Dataplane, CP - MAC-learn Controlplane, UUD - Unknown-Unicast-Drop
Virtual Network: 0
Members:

Virtual Network: 6000
Members:
 VLAN 20: ethernet1/1/54:3
 VxLAN Virtual Network Identifier: 6000
 Source Interface: loopback1(200.0.0.1)
 Remote-VTEPs (flood-list): 13.0.0.5(CP)
```

要查看 VXLAN 中的所有复制器及其状态，请使用 `show nve replicators` 命令。

```
OS10# show nve replicators
Codes: * - Active Replicator

BFD Status:Disabled
Replicators State

```

```
13.0.0.5 Up
13.0.0.3 Up
13.0.0.2 Up
```

要查看远程 VTEP 状态, 请使用 `show nve remote-vtep` 命令。

```
OS10# show nve remote-vtep
IP Address: 13.0.0.2, State: up, Encap: VxLAN
 VNI list: ,6000
IP Address: 13.0.0.3, State: up, Encap: VxLAN
 VNI list: ,6000
IP Address: 13.0.0.5, State: up, Encap: VxLAN
 VNI list: ,6000
IP Address: 202.0.0.1, State: up, Encap: Vxlan
 VNI list: 6000
```

## VTEP 2

```
OS10# show nve controller

Management IP : 10.16.140.13/16
Gateway IP : 202.0.0.1
Max Backoff : 10000
Configured Controller : 10.16.140.181:6640 ssl (connected)

Controller Cluster
IP Port Protocol Connected State Max-Backoff
10.16.140.182 6640 ssl true ACTIVE 10000
10.16.140.183 6640 ssl true ACTIVE 10000
10.16.140.181 6640 ssl true ACTIVE 10000

NVE Controller Ports
ethernet1/1/25:3
```

要显示 VXLAN 的 VNID、端口成员、源接口和远程 VTEP, 请使用 `show virtual-network` 命令。

```
OS10# show virtual-network
Codes: DP - MAC-learn Dataplane, CP - MAC-learn Controlplane, UUD - Unknown-Unicast-Drop
Virtual Network: 0
 Members:

Virtual Network: 6000
 Members:
 VLAN 20: ethernet1/1/25:3
 VxLAN Virtual Network Identifier: 6000
 Source Interface: loopback1(202.0.0.1)
 Remote-VTEPs (flood-list): 13.0.0.5(CP)
```

要查看 VXLAN 中的所有复制器及其状态, 请使用 `show nve replicators` 命令。

```
OS10# show nve replicators
Codes: * - Active Replicator

BFD Status:Disabled
Replicators State

13.0.0.5 Up
13.0.0.3 Up
13.0.0.2 Up
```

要查看远程 VTEP 状态, 请使用 `show nve remote-vtep` 命令。

```
OS10# show nve remote-vtep
IP Address: 13.0.0.2, State: up, Encap: VxLAN
 VNI list: ,6000
IP Address: 13.0.0.3, State: up, Encap: VxLAN
 VNI list: ,6000
IP Address: 13.0.0.5, State: up, Encap: VxLAN
```

```
VNI list: ,6000
IP Address: 200.0.0.1, State: up, Encap: Vxlan
VNI list: 6000
```

## VXLAN 控制器命令

### controller ovsdb

将模式更改为 CONFIGURATION-NVE-OVSDB，以配置控制器参数。

**语法** `controller ovsdb`

**参数** 无

**默认** 无

**命令模式** CONFIGURATION-NVE

**使用情况信息** 控制器配置在 OS10 交换机上启动 OVSDB 服务。

此命令的 `no` 版本将停止 OVSDB 服务。如果有任何端口配置为控制器管理端口或 IP 地址配置，则 `no` 版本命令将失败。

 **注:** 从设备中移除控制器配置之前，必须删除所有控制器管理的端口和 IP 地址配置。

#### 示例

```
OS10(config)# nve
OS10(config-nve)# controller ovsdb
```

**支持的版本** 10.4.3.0 or later

### ip port ssl

在交换机中配置 OVSDB 控制器可访问性信息，如 IP 地址、端口号和会话的连接类型。

**语法** `ip ip-address port port-number ssl`

**参数**

- `ip-address` — 指定要连接的 OVSDB 控制器的 IP 地址。
- `port-number` — 指定建立 OVSDB 控制器连接的端口号。

**默认** 对于基于 OVSDB 的控制器，请配置以下各项：

- 端口号 6640
- 连接类型 SSL

**命令模式** CONFIGURATION-NVE-OVSDB

**使用情况信息** 当前，仅受支持的 OVSDB 控制器是 NSX 控制器。此命令的 `no` 版本将移除到 OVSDB 控制器的连接。

#### 示例

```
OS10(config)# nve
OS10(config-nve)# controller ovsdb
OS10(config-nve-ovsdb)# ip 10.11.66.110 port 6640 ssl
```

**支持的版本** 10.4.3.0 or later

### max-backoff

配置时间间隔，以毫秒 (ms) 为单位。这是交换机在尝试连接到控制器之间等待的持续时间。

**语法** `max-backoff interval`

|               |                                                                                                               |
|---------------|---------------------------------------------------------------------------------------------------------------|
| <b>参数</b>     | <i>interval</i> — 输入时间量，以毫秒为单位。这是交换机在尝试与控制器连接之间的等待时间，从 1000 到 180000 ms。                                      |
| <b>默认</b>     | 8000 ms                                                                                                       |
| <b>命令模式</b>   | CONFIGURATION-NVE-OVSDB                                                                                       |
| <b>使用情况信息</b> | 此命令的 <b>no</b> 版本将替换交换机中的默认最长等待时间配置。                                                                          |
| <b>示例</b>     | <pre> OS10(config)# nve OS10(config-nve)# controller ovssdb OS10(config-nve-ovssdb)# max-backoff 40000 </pre> |
| <b>支持的版本</b>  | 10.4.3.0 or later                                                                                             |

## nve-controller

分配要由控制器管理的接口。

|               |                                                                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>nve-controller</code>                                                                                                                                                                                    |
| <b>参数</b>     | 无                                                                                                                                                                                                              |
| <b>默认</b>     | 无                                                                                                                                                                                                              |
| <b>命令模式</b>   | INTERFACE                                                                                                                                                                                                      |
| <b>使用情况信息</b> | 在将接口添加到控制器时，接口必须处于 Switchport 中继模式。如果接口未处于 Switchport 中继模式，则系统会显示以下错误消息：                                                                                                                                       |
|               | <pre>% Error: Interface ethernet1/1/1, must be in switchport trunk for controller mode.</pre>                                                                                                                  |
|               | <p> <b>注：</b>如果接口具有由控制器配置的活动端口限定 VLAN（端口、VLAN）对，则不能从控制器中删除接口。</p> <p>此命令的 <b>no</b> 版本将从控制器中删除接口，并删除与该接口关联的任何 VXLAN 绑定。</p> |
| <b>示例</b>     | <pre> OS10(config)# interface ethernet 1/1/1 OS10(config-if-eth1/1/1)# nve-controller </pre>                                                                                                                   |
| <b>支持的版本</b>  | 10.4.3.0 or later                                                                                                                                                                                              |

## nve controller ssl-key-generate

为 OVSSDB 服务器生成 SSL 证书，以设置与控制器的 SSL 连接。

|               |                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>nve controller ssl-key-generate</code>                                                        |
| <b>参数</b>     | 无                                                                                                   |
| <b>默认</b>     | 无                                                                                                   |
| <b>命令模式</b>   | EXEC                                                                                                |
| <b>使用情况信息</b> | 此命令仅适用于 <code>sysadmin</code> 和 <code>secadmin</code> 角色。此命令将生成 SSL 证书并重新启动 OVSSDB 服务器，以开始使用新生成的证书。 |
| <b>示例</b>     | <pre> OS10# nve controller ssl-key-generate </pre>                                                  |
| <b>支持的版本</b>  | 10.4.3.0 or later                                                                                   |

## show nve controller

显示有关控制器和控制器管理接口的信息。

|      |                     |
|------|---------------------|
| 语法   | show nve controller |
| 参数   | 无                   |
| 默认   | 无                   |
| 命令模式 | EXEC                |
| 示例   |                     |

```
OS10# show nve controller

Management IP : 10.16.140.29/16
Gateway IP : 55.55.5.5
Max Backoff : 1000
Configured Controller : 10.16.140.172:6640 ssl (connected)

Controller Cluster
IP Port Protocol Connected State Max-
Backoff
10.16.140.173 6640 ssl true ACTIVE 1000
10.16.140.171 6640 ssl false BACKOFF 1000
10.16.140.172 6640 ssl true ACTIVE 1000

NVE Controller Ports
ethernet1/1/1:1
ethernet1/1/15
```

|       |                   |
|-------|-------------------|
| 支持的版本 | 10.4.3.0 or later |
|-------|-------------------|

## show nve controller ssl-certificate

显示系统中生成的 SSL 证书。

|        |                                     |
|--------|-------------------------------------|
| 语法     | show nve controller ssl-certificate |
| 参数     | 无                                   |
| 默认     | 无                                   |
| 命令模式   | EXEC                                |
| 使用情况信息 | 此命令仅适用于 sysadmin 和 secadmin 角色。     |
| 示例     |                                     |

```
OS10# show nve controller
-----BEGIN CERTIFICATE-----
MIIDGgDCCAmgCAQMwDQYJKoZIhvcNAQENBQAwgYExCzAJBgNVBAYTA1VTMQswCQYD
VQQIDAJDQTEVMBMGA1UECgwMT3BlbiB2U3dpdGNoMREwDwYDVQQLEDAhZd2l0Y2hj
YTE7MDkGA1UEAwwyT1ZTIHN3aXRjaGNhIENBIENlcnRpZmljYXRlICgyMDE4IFNl
cCAyMyAwMzo0NzoyMCKwHhcNMjgwOTI0MTYzMDUyWhcNMjgwOTI0MTYzMDUyWjCB
iTElMAkGA1UEBhMCVVMxCzAJBgNVBAGMAkNBMRUwEwYDVQQKDAxPcGVuIHZTd2l0
Y2gxH2gAdBgNVBASMFk9wZW4gd1N3aXRjaCBjZXJ0aWZpZXIuNTAzBgNVBAMMLGRl
bGwgaWQ6MGVlZmUwYWMtNGJjOC00MmVmLTkzOTEtN2RlMmMwY2JmMTJjMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsMlD4c4fWwy+5t6VScjizlkFsNzE
BOK5PJyI3B6ReRK/J14Fdxio1YmzG0Y0bjxiwjpuYEsqPL3Nvh0f10KMqwqJVBdf
6sXWHUVw+9A7cIfRh0aRI+HIYyUC4YD48GlnVnaCqhXyAa0tcMzJm4r2k7AjjU1
0pDXiqS3uJwGmfxlhvmFio8EeHM/Z79DkBRD6FUMwacAnb3yCIKZH50AWq7qRmmG
NZOgyYUT+8oaJ5t0/hEQfDYuv32E5z4d3FhiBJMFT86T4YvpJYyJkiKmaQWInkthL
V3VxEMXI5vJQclMhwYbKfPB4hh3+qdS5o+uVco76CVrcWi7rO3XmsBkbnQIDAQAB
MA0GCSqGSIb3DQEBDQUAA4IBAQAuFVD20GcHD8zdpYf0YaP4b6TuonUzF0jwoV+
Qr9b4kOjEBGuoPdevX3AeV/dvAa2Q6o1iOBM5z74NgHizhr067pFP841Nv7DAVb7
cPHHSSTTSeeJjIVMh0kv0KkVefsYuI4rljqJxu0GZgBinqehXxVKlceouLvwbbh1
MFYXN3lcE2AXR746q1Vlc6stNkxf3nr1OpSDz3P4VOnbAnIrY+SvUVmAT0tdrowH
99y2AzoAxUHodWsH8EjCFch7VilmCVVhyghXdfyl6lv/F6vMRwjc343BpBW3QsGj
68ROX0ILRtOz/2q5oUb/rpJd15KFFN3itT/xYBfZ1ZdLYd5F
-----END CERTIFICATE-----
```

支持的版本 10.4.3.0 or later

show nve replicators

显示所有复制器及其状态。

- 语法 show nve replicators [vnid vnid]
- 参数 无
- 默认 无
- 命令模式 EXEC
- 使用情况信息 指定 VNID 时，输出将显示有关可用于 VNID 的服务节点的详细信息。

示例（不带 VNID）

```
OS10# show nve replicators
Codes: * - Active Replicator

BFD Status:Enabled
Replicators State

2.2.2.3 Up
2.2.2.2 Up

OS10# show nve replicators
```

示例（带 VNID）

```
OS10# show nve replicators vnid 10009
Codes: * - Active Replicator

BFD Status:Enabled
Replicators State

2.2.2.3 Up
2.2.2.2* Up
```

\* — 指示 VTEP 向其发送特定 VNID 的 BUM 流量的服务节点。

支持的版本 10.4.3.0 or later

show ovssdb-tables mac-local-ucast

显示有关本地 MAC 地址条目的信息，包括每个 MAC 地址、IP 地址、本地交换机名称和 VNID。

- 语法 show ovssdb-tables mac-local-ucast
- 参数 无
- 默认 无
- 命令模式 EXEC
- 使用情况信息 此命令仅适用于 netadmin、sysadmin 和 secadmin 角色。

示例

```
OS10# show ovssdb-tables mac-local-ucast
Count : 1356
Ucast_Macs_Local table
MAC _uuid ipaddr locator
logical_switch

"00:00:09:00:00:00" 948d2357-9a68-49b2-b5b2-a6a9beaec17a "" bb43d2ec-1e60-4367-9840-648a8cc8acff
f8994210-e29d-4ad4-90fb-557c30f83769
"00:00:09:00:00:01" 4e620093-311a-420e-957f-fbd2bb63f20a "" bb43d2ec-1e60-4367-9840-648a8cc8acff
f8994210-e29d-4ad4-90fb-557c30f83769
"00:00:09:00:00:02" 3846973c-2b29-4c84-af39-dfe7513cdb3d "" bb43d2ec-1e60-4367-9840-648a8cc8acff
f8994210-e29d-4ad4-90fb-557c30f83769
```

支持的版本 10.4.3.0 or later

## show ovssdb-tables mac-remote-ucast

显示有关远程 MAC 地址条目的信息，包括每个 MAC 地址、IP 地址、本地交换机名称和 VNID。

|        |                                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show ovssdb-tables mac-remote-ucast                                                                                                                                                                                                                                                          |
| 参数     | 无                                                                                                                                                                                                                                                                                            |
| 默认     | 无                                                                                                                                                                                                                                                                                            |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | 此命令仅适用于 netadmin、sysadmin 和 secadmin 角色。                                                                                                                                                                                                                                                     |
| 示例     | <pre>OS10# show ovssdb-tables mac-remote-ucast Count : 1 Ucast_Macs_Remote table MAC          _uuid          ipaddr locator logical_switch ----- "00:50:56:8a:b4:c8" 61fa240b-e6a3-4d8e-a693-dd2468e6f308 "" 3105e34b-a273-4193-a60f-51d9cee91403 6932fc02-fb12-4a22-9ec2-f0e2b20df476</pre> |

支持的版本 10.4.3.0 or later

## show ovssdb-tables manager

显示有关控制器列表和相应控制器连接详细信息的信息。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show ovssdb-tables manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 使用情况信息 | 此命令仅适用于 netadmin、sysadmin 和 secadmin 角色。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 示例     | <pre>OS10# show ovssdb-tables manager Count : 3 Manager table _uuid          inactivity_probe is_connected max_backoff other_config status target ----- ----- 478ec8ca-9c5a-4d29-9069-633af6c48002 [] false 1000 {} {state=BACKOFF} "ssl:10.16.140.171:6640" 52f2b491-6372-43e0-98ed-5c4ab0ca8542 [] true 1000 {} {sec_since_connect="37831", sec_since_disconnect="37832", state=ACTIVE} "ssl:10.16.140.173:6640" 7b8a7e36-6221-4297-b85e-51f910abcb5c [] true 1000 {} {sec_since_connect="87", sec_since_disconnect="99", state=ACTIVE} "ssl:10.16.140.172:6640" OS10#</pre> |

支持的版本 10.4.3.0 or later

## show ovssdb-tables tunnel

显示有关物理交换机为服务节点创建的隧道的信息。

|    |                           |
|----|---------------------------|
| 语法 | show ovssdb-tables tunnel |
| 参数 | 无                         |



默认

命令模式

使用情况信息

示例

无

EXEC

此命令仅适用于 netadmin、sysadmin 和 secadmin 角色。

```
OS10# show ovsdb-tables tunnel
Count : 2
Tunnel table
 uuid bfd_config_local bfd_params
 bfd_config_remote
 bfd_status
 local remote

8025d953-acf5-4091-9fa2-75d41953b397 {bfd_dst_ip="55.55.5.5", bfd_dst_mac="00:23:20:00:00:01"} {bfd_dst_ip="2.2.2.2",
bfd_dst_mac="00:50:56:65:b2:3c"} {enable="true", forwarding_if_rx="true", min_rx="1000"} {diagnostic="No Diagnostic",
enabled="true", forwarding="true", remote_state=up, state=up} bb43d2ec-1e60-4367-9840-648a8cc8acff
2d8963da-24d0-4fbd-81e2-fb1a7bba88fd
9853f77a-9db7-47f5-8203-b5b8895d15bd {bfd_dst_ip="55.55.5.5", bfd_dst_mac="00:23:20:00:00:01"} {bfd_dst_ip="2.2.2.3",
bfd_dst_mac="00:50:56:6e:56:9b"} {enable="true", forwarding_if_rx="true", min_rx="1000"} {diagnostic="No Diagnostic",
enabled="true", forwarding="true", remote_state=up, state=up} bb43d2ec-1e60-4367-9840-648a8cc8acff 5eee586b-
e0aa-442b-83ea-16633ec41230
```

支持的版本

10.4.3.0 or later

## UFT 模式

第 2 层 (L2) 网络中的交换机可能需要较大的 MAC 地址表大小，而第 3 层 (L3) 网络中的交换机可能需要较大的路由表大小。统一转发表 (UFT) 可提供配置内部 L2/L3 转发表大小的灵活性。

OS10 支持转发表的多重 UFT 模式。默认情况下，OS10 选择一种 UFT 模式，可为所有表提供合理的大小。受支持的 UFT 模式包括：默认值、scaled-l2-switch、scaled-l3-hosts 和 scaled-l3-routes。

 **注：**此功能在 Z9332F-ON 平台上不受支持。

**表. 50: UFT 模式 — S4048-ON、S4048T-ON、S6010-ON 的表大小**

| UFT 模式           | L2 MAC 表大小 | L3 主机表大小 | L3 路由表大小 |
|------------------|------------|----------|----------|
| Scaled-l2-switch | 294912     | 16384    | 16384    |
| Scaled-l3-hosts  | 98304      | 212992   | 98304    |
| Scaled-l3-routes | 32768      | 16384    | 131072   |
| 默认               | 163840     | 147456   | 16384    |

**表. 51: UFT 模式 — S3048-ON 的表大小**

| UFT 模式           | L2 MAC 表大小 | L3 主机表大小 | L3 路由表大小 |
|------------------|------------|----------|----------|
| Scaled-l2-switch | 40960      | 2048     | 8192     |
| Scaled-l3-hosts  | 8192       | 18432    | 8192     |
| 默认               | 28672      | 8192     | 8192     |

**表. 52: UFT 模式 — S41XX-ON 系列的表大小**

| UFT 模式           | L2 MAC 表大小 | L3 主机表大小 | L3 路由表大小 |
|------------------|------------|----------|----------|
| Scaled-l2-switch | 278528     | 4096     | 16384    |
| Scaled-l3-hosts  | 16384      | 266240   | 16384    |
| Scaled-l3-routes | 16384      | 4096     | 262144   |
| 默认               | 81920      | 69632    | 131072   |

**表. 53: UFT 模式 — Z9100-ON 的表大小**

| UFT 模式           | L2 MAC 表大小 | L3 主机表大小 | L3 路由表大小 |
|------------------|------------|----------|----------|
| Scaled-l2-switch | 139264     | 8192     | 16384    |
| Scaled-l3-hosts  | 8192       | 139264   | 16384    |
| Scaled-l3-routes | 8192       | 8192     | 131072   |
| 默认               | 73728      | 73728    | 16384    |

表. 54: UFT 模式 — Z9264F-ON 的表大小

| UFT 模式           | L2 MAC 表大小 | L3 主机表大小 | L3 路由表大小 |
|------------------|------------|----------|----------|
| Scaled-l2-switch | 270336     | 8192     | 32768    |
| Scaled-l3-hosts  | 8192       | 270336   | 32768    |
| Scaled-l3-routes | 8192       | 8192     | 262144   |
| 默认               | 139264     | 139264   | 32768    |

表. 55: UFT 模式 — S52XX-ON 系列的表大小

| UFT 模式           | L2 MAC 表大小 | L3 主机表大小 | L3 路由表大小 |
|------------------|------------|----------|----------|
| Scaled-l2-switch | 294912     | 16384    | 16384    |
| Scaled-l3-hosts  | 32768      | 278528   | 16384    |
| Scaled-l3-routes | 32768      | 16384    | 389120   |
| 默认               | 163840     | 147456   | 16384    |

表. 56: UFT 模式 — S42xxFB-ON 的表大小

| UFT 模式 | L2 MAC 表大小 | L3 主机表大小 | L3 路由表大小 |
|--------|------------|----------|----------|
| 默认     | 250 K      | 48 K     | 130 K    |

表. 57: UFT 模式 — S42xxFBL-ON 的表大小

| UFT 模式 | L2 MAC 表大小 | L3 主机表大小 | L3 路由表大小 |
|--------|------------|----------|----------|
| 默认     | 250 K      | 48 K     | 2 百万     |

 注: 对于 Scaled-l3-routes 模式, L3 路由表大小可能会因正在安装的路由而异。

## 配置 UFT 模式

可用的 UFT 模式包括 L2 MAC 表、L3 主机表或 L3 路由表大小。保存配置并重新加载交换机, 以使配置更改生效。

- 在 CONFIGURATION 模式下选择一种模式以初始化大表大小。

```
hardware forwarding-table mode [scaled-l2 | scaled-l3-routes | scaled-l3-hosts]
```

- 在 CONFIGURATION 模式下禁用 UFT 模式。

```
no hardware forwarding-table
```

### 配置 UFT 模式

```
OS10(config)# hardware forwarding-table mode scaled-l3-hosts
OS10(config)# exit
OS10# write memory
OS10# reload
```

### 查看 UFT 模式信息

```
OS10# show hardware forwarding-table mode
Current Settings
Mode default-mode
L2 MAC Entries : 163840
Next-boot Settings
scaled-l3-hosts
98304
```

|                  |   |        |        |
|------------------|---|--------|--------|
| L3 Host Entries  | : | 147456 | 212992 |
| L3 Route Entries | : | 32768  | 98304  |

## 查看所有模式的 UFT 信息

```
OS10# show hardware forwarding-table mode all
Mode default scaled-l2 scaled-l3-routes scaled-l3-hosts
L2 MAC Entries 163840 294912 32768 98304
L3 Host Entries 147456 16384 16384 212992
L3 Route Entries 32768 32768 131072 98304
```

## IPv6 扩展前缀路由

包含掩码在 /64 至 /128 之间的前缀路由的 IPv6 地址被称为 IPv6 扩展前缀路由。这些路由要求在最长前缀匹配 (LPM) 表中输入密钥大小的两倍。

您可以使用 `hardware l3 ipv6-extended-prefix prefix-number` 命令配置扩展前缀的路由条目数量。

保存并重新加载交换机，以使设置生效。

### 配置 IPv6 扩展前缀路由

```
OS10# configure terminal
OS10(config)# hardware l3 ipv6-extended-prefix 2048
% Warning: IPv6 Extended Prefix Installation will be applied only after a save and reload.
OS10(config)# do write memory
OS10(config)# reload
```

### 查看 IPv6 扩展前缀路由配置

```
OS10# show running-configuration | grep hardware
hardware l3 ipv6-extended-prefix 2048
```

重新加载之前的配置：

|                                 |                  |                    |
|---------------------------------|------------------|--------------------|
| OS10# show hardware l3          | Current Settings | Next-boot Settings |
| IPv6 Extended Prefix Entries: 0 |                  | 2048               |

重新加载之后的配置：

|                                    |                  |                    |
|------------------------------------|------------------|--------------------|
| OS10# show hardware l3             | Current Settings | Next-boot Settings |
| IPv6 Extended Prefix Entries: 2048 |                  | 2048               |

命令的 `no` 版本将移除 IPv6 扩展前缀路由配置。保存并重新加载交换机以移除配置。

```
OS10(config)# no hardware l3 ipv6-extended-prefix
% Warning: Un-configuring IPv6 Extended Prefix will be applied only after a save and reload.
```

## UFT 命令

### hardware forwarding-table mode

选择一种模式以初始化最大可扩展性大小。可用的选项包括：扩展的 L2 MAC 地址表、扩展的 L3 路由表或扩展的 L3 主机表。

**语法** `hardware forwarding-table mode {scaled-l2 | scaled-l3-routes | scaled-l3-hosts}`

**参数**

- `scaled-l2` — 输入 L2 MAC 地址表大小。

- `scaled-l3-routes` — 输入 L3 路由表大小。
- `scaled-l3-hosts` — 输入 L3 主机表大小。

**默认** 默认参数因平台而异。请参阅 [UFT 模式](#) 页面上的 894。

**命令模式** CONFIGURATION

**使用情况信息** 根据您的网络环境要求配置内部 L2 和 L3 转发表的大小。要应用更改，请重新加载交换机。  
此命令的 `no` 版本将 UFT 模式重置为默认值。

**示例**

```
OS10(config)# hardware forwarding-table mode scaled-l3-hosts
```

**支持的版本** 10.3.0E or later

## hardware l3 ipv6-extended-prefix

配置 IPv6 扩展前缀路由的路由条目的最大数量。

**语法** `hardware l3 ipv6-extended-prefix prefix-number`

**参数** *prefix-number* — 输入 IPv6 扩展前缀路由的路由条目的最大数量。可用选项包括：1024、2048 或 3072。

**默认** 无

**命令模式** CONFIGURATION

**使用情况信息** 保存并重新加载交换机，以使设置生效。命令的 `no` 版本将移除 IPv6 扩展前缀路由配置。

**示例**

```
OS10# configure terminal
OS10(config)# hardware l3 ipv6-extended-prefix 2048
% Warning: IPv6 Extended Prefix Installation will be applied only after
a save and reload.
OS10(config)# do write memory
OS10(config)# reload
```

**支持的版本** 10.4.1.0 or later

## show hardware forwarding-table mode

显示当前硬件转发表模式以及在下一引导后的模式。

**语法** `show hardware forwarding-table mode`

**参数** 无

**默认** 无

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# show hardware forwarding-table mode
```

|                  | Current Settings | Next-boot Settings |
|------------------|------------------|--------------------|
| Mode             | default-mode     | scaled-l3-hosts    |
| L2 MAC Entries   | 163840           | 98304              |
| L3 Host Entries  | 147456           | 212992             |
| L3 Route Entries | 32768            | 98304              |

**支持的版本** 10.3.0E or later

## show hardware forwarding-table mode all

显示硬件转发表模式的表大小。

|        |                                                                                                                                                                                                                                                                                                                                                                |  |  |  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
| 语法     | show hardware forwarding-table mode all                                                                                                                                                                                                                                                                                                                        |  |  |  |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                              |  |  |  |
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                              |  |  |  |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                           |  |  |  |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                                                                              |  |  |  |
| 示例     | <pre>OS10# show hardware forwarding-table mode all Mode                default      scaled-l2    scaled-l3-routes    scaled- l3-hosts L2 MAC Entries      163840      294912      32768               98304 L3 Host Entries     147456      16384       16384               212992 L3 Route Entries    32768       32768       131072              98304</pre> |  |  |  |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                               |  |  |  |

## show hardware l3

显示 IPv6 扩展前缀路由配置。

|        |                                                                                                                         |  |
|--------|-------------------------------------------------------------------------------------------------------------------------|--|
| 语法     | show hardware l3                                                                                                        |  |
| 参数     | 无                                                                                                                       |  |
| 默认     | 无                                                                                                                       |  |
| 命令模式   | EXEC                                                                                                                    |  |
| 使用情况信息 | 无                                                                                                                       |  |
| 示例     | <pre>OS10# show hardware l3 Current Settings      Next-boot Settings IPv6 Extended Prefix Entries: 2048      2048</pre> |  |
| 支持的版本  | 10.4.1.0 or later                                                                                                       |  |

身份验证、授权和核算 (AAA) 服务保护网络可防止未经授权的访问。除了本地身份验证，OS10 还支持远程身份验证拨号用户服务 (RADIUS) 和终端访问控制器访问控制系统 (TACACS+) 客户端/服务器身份验证系统。对于 RADIUS 和 TACACS+，OS10 交换机用作客户端，并向包含所有用户身份验证和网络服务访问信息的服务器发送身份验证请求。

RADIUS 或 TACACS+ 服务器提供：用户凭据身份验证、使用基于角色的权限的授权和核算服务。您可以为不同的登录方法和用户配置使用的安全协议。与 TACACS+ 相比，RADIUS 提供有限的授权和核算服务。如果您使用的是 RADIUS 或 TACACS+ 安全服务器，请按照服务器说明文件中的步骤在服务器上配置所需的安全参数。

### AAA 配置

在交换机上，AAA 配置包括设置访问控制和核算服务：

1. 配置用于允许访问交换机的身份验证方法。
2. 为经过身份验证的用户配置命令授权级别。
3. 为用户会话配置安全设置。
4. 启用 AAA 核算。

## AAA 身份验证

OS10 交换机使用一系列身份验证方法来定义身份验证类型及其应用顺序。默认情况下，OS10 仅使用 `local` 身份验证方法。

方法列表中的身份验证方法按配置的顺序执行。重新输入更改订单的方法。`local` 身份验证方法仍保持启用状态，即使您使用 `no aaa authentication login {console | default}` 命令删除列表中的所有已配置方法。

**注：**如果您在以 SmartFabric 模式工作的 Dell EMC PowerEdge MX7000 以太网模块 (MX9116n 网络引擎和 MX5108n 以太网交换机) 上配置多个身份验证方法，则必须将本地身份验证配置为列表中的第一种方法。

- 在 CONFIGURATION 模式下配置 AAA 身份验证方法。

```
aaa authentication login {console | default} {local | group radius | group tacacs+}
```

- o `console` — 配置控制台登录的身份验证方法。
- o `default` — 配置非控制台身份验证方法，如 SSH 和 Telnet 登录。
- o `local` — 使用通过 `username password role` 命令配置的本地用户名、密码和角色条目。
- o `group radius` — 使用 `radius-server host` 命令配置 RADIUS 服务器。
- o `group tacacs+` — 使用 `tacacs-server host` 命令配置 TACACS+ 服务器。

### 在服务器上配置用户角色

如果控制台用户使用 RADIUS 或 TACACS+ 身份验证登录，则将应用在 RADIUS 或 TACACS+ 服务器上为用户配置的角色。如果身份验证服务器上未配置任何角色，则用户身份验证失败。

此外，您必须使用特定于供应商的属性 (VSA) 配置 RADIUS 或 TACACS+ 服务器上的用户角色，否则身份验证将失败。Dell EMC 的供应商 ID 为 674。使用 `Name = Dell-group-name`，`OID = 2`，`Type = string` 创建 VSA。`Dell-group-name` 的有效值为 `sysadmin`、`secadmin`、`netadmin` 和 `netoperator`。在 RADIUS 或 TACACS+ 服务器上创建用户时，请使用 VSA `Dell-group-name` 值。

有关如何在 RADIUS 或 TACACS+ 服务器上配置特定于供应商的属性的详细信息，请参阅相应的 RADIUS 或 TACACS+ 服务器说明文件。

### 配置 AAA 身份验证

```
OS10(config)# aaa authentication login default group radius local
OS10(config)# do show running-configuration aaa
aaa authentication login default group radius local
aaa authentication login console local
```

## 移除 AAA 身份验证方法

```
OS10(config)# no aaa authentication login default
OS10(config)# do show running-configuration aaa
aaa authentication login default local
aaa authentication login console local
```

# 用户重新身份验证

为防止用户访问资源并执行未授权执行的任务，OS10 允许您在身份验证方法或服务器更改时再次登录，从而要求用户重新进行身份验证，例如：

- 使用 `radius-server host` 命令添加或删除 RADIUS 服务器
- 使用 `aaa authentication login {console | default} {local | group radius | group tacacs+}` 命令添加或删除身份验证方法

默认情况下，用户重新身份验证已禁用。您可以启用此功能，以便在执行上述任一操作时需要重新进行用户身份验证。在这些情况下，已登录用户会从交换机中注销，并且所有 OS10 会话将终止。

## 启用用户重新身份验证

- 在 CONFIGURATION 模式下启用用户重新身份验证。

```
aaa re-authenticate enable
```

此命令的 `no` 版本会禁用用户重新身份验证。

# 密码强度

默认情况下，使用 `username password role` 和 `enable password priv-lvl` 命令配置的密码必须至少包含 9 个字母数字字符。要增加密码强度，您可以使用 `password-attributes` 命令创建更强的密码规则。这些密码规则适用于用户名和权限级别密码配置。

输入命令时，至少需要一个参数。输入此 `character-restriction` 参数时，至少需要一个选项。

- 在 CONFIGURATION 模式下创建更强的密码规则。

```
password-attributes {[min-length number] [character-restriction {[upper number]
[lower number][numeric number] [special-char number]}]}
```

- `min-length number` — 输入最小字母数字字符数，从 6 到 32；默认值为 9。
- `character-restriction` — 在密码中输入字母数字字符的要求：
  - `upper number` — 需要最小大写字母数，从 0 到 31；默认值为 0。
  - `lower number` — 需要最小小写字母数，从 0 到 31；默认值为 0。
  - `numeric number` — 需要最小数字字符数，从 0 到 31；默认值为 0。
  - `special-char number` — 需要最小特殊字符数，从 0 到 31；默认值为 0。

要关闭使用 `password-attributes` 命令启用的强密码检查，请使用 `service simple-password` 命令。除了最低 9 个字符要求以外，没有密码规则应用于用户名和权限级别密码。要恢复为配置的 `password-attributes` 的设置，请使用 `no service simple-password` 命令。

## 创建强密码规则

```
OS10(config)# password-attributes min-length 7 character-restriction upper 4 numeric 2
```

## 显示密码规则

```
OS10# show running-configuration password-attributes
password-attributes min-length 7 character-restriction upper 4 numeric 2
```

## 禁用强密码检查

```
OS10(config)# password-attributes min-length 7 character-restriction upper 4 numeric 2
OS10(config)# username admin2 password 4newhire4 role sysadmin
%Error: Password fail: it does not contain enough DIFFERENT characters
```



```
OS10(config)# enable password 0 4newhire4 priv-lvl 5
%Error: Password it does not contain enough DIFFERENT characters.
OS10(config)# service simple-password
OS10(config)# username admin2 password 4newhire4 role sysadmin
OS10(config)# enable password 0 4newhire4 priv-lvl 5
```

### 重新启用强密码检查

```
OS10(config)# no service simple-password
```

## 简单密码检查

默认情况下, 在使用 `username username password password role role [priv-lvl privilege-level]` 命令配置用户名密码时, OS10 使用强密码检查。

要关闭强密码检查并配置简单的密码不受限制, 请使用 `service simple-password` 命令。

要禁用简单密码检查并返回默认的强密码检查, 请使用 `no service simple-password` 命令。

- 在 CONFIGURATION 模式下输入命令。

```
service simple-password
```

### 启用简单密码检查

```
OS10(config)# username abhishek password madmiamadam role sysadmin
%Error: Password fail: it does not contain enough DIFFERENT characters
OS10(config)# service simple-password
OS10(config)# username abhishek password madmiamadam role sysadmin
OS10(config)#
```

## 隐匿密码

要在 `show` 命令输出中隐匿密码, 以便不显示文本字符, 请使用 `service obscure-password` 命令。命令将隐匿为用户名、NTP、BGP、SNMP、RADIUS 服务器和 TACACS+ 服务器配置的密码。要禁用隐匿密码功能, 请使用 `no service obscure-password` 命令。

- 在 CONFIGURATION 模式下输入命令。

```
service obscure-password
```

### 隐匿 OS10 密码

```
OS10(config)# service obscure-password

OS10(config)# show running-configuration users
username admin password **** role sysadmin priv-lvl 15
username test1 password **** role sysadmin priv-lvl 15

OS10(config)# show running-configuration radius-server
radius-server host 10.2.2.2 key 9 ****

OS10(config)# show running-configuration tacacs-server
tacacs-server host 10.1.1.1 auth-port 7777 key 9 ****
```

### 禁用隐匿密码

```
OS10(config)# no service obscure-password

OS10(config)# show running-configuration users
username admin password 6q9QBeYjZ$jjfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD7/
VKx8SloIhp4NoGzsOI/UNwh8WVuxwfd9q4pWlIgNs5BKH role sysadmin priv-lvl 15
username test1 password 6rounds=656000$50vutEWA9w3ImvF.
$2pSDnaINYTKCQ6WAlJqeabiFQNRvUgui3.
6vR2e.L/D7DBwnV0QtY.KtOBTZAIDDT5.AFWxQHVgs2/V3jC3yG1 role sysadmin priv-lvl 15
```

```
OS10(config)# show running-configuration radius-server
radius-server host 10.2.2.2 key 9
3c0e479bd43bb5baf4ebb16e1317a845f01f832e25a03836c70bd26b9754d6a0

OS10(config)# show running-configuration tacacs-server
tacacs-server host 10.1.1.1 auth-port 7777 key 9
27ca79bf3cbf351708c8d19caf50815661dcd0638719a06c865e88090d03558b
```

## 基于角色的访问控制

RBAC 为访问和授权提供控制。用户将根据定义的角色（而不是其单独的系统用户 ID）获得权限。根据作业功能创建用户角色，以帮助用户执行其关联的作业功能。您只能为每个用户分配一个角色，并且许多用户可以具有相同的角色。用户角色在登录时对用户进行身份认证和授权，并将用户置于 EXEC 模式。有关详细信息，请参阅 [CLI 基础知识](#)。

OS10 支持四个预定义的角色：`sysadmin`、`secadmin`、`netadmin` 和 `netoperator`。每个用户角色可分配用于确定用户可输入的命令以及用户可执行的操作的权限。RBAC 提供了一种简单高效的方式来管理用户权限。如果用户角色与某个命令允许的用户角色匹配，将授予命令授权。

OS10 RBAC 型号提供了责任和更高的安全性。它限制了每个角色的权限，从而允许您对任务进行分区。为了获得更高的安全性，只有一些用户角色可以查看事件、审核和安全系统日志。

## 分配用户角色

要限制 OS10 系统访问，请在配置每个用户时分配一个角色。

- 在 CONFIGURATION 模式下输入用户名、密码和角色。

```
username username password password role role
```

- `username username` — 输入文本字符串。最多 32 个字母数字字符；最少 1 个字符。
- `password password` — 输入文本字符串。最多 32 个字母数字字符；最少 9 个字符。
- `role role` — 输入用户角色：
  - `sysadmin` — 对系统中所有命令的完全访问权限、对操作文件系统的命令的独占访问权限，以及对系统 shell 的访问权限。系统管理员可以创建用户 ID 和用户角色。
  - `secadmin` — 对设置安全策略和系统访问权限的配置命令的完全访问权限，如密码强度、AAA 授权和加密密钥。安全管理员可以显示安全信息，如加密密钥、登录统计信息和日志信息。
  - `netadmin` — 对管理流经交换机（如路由、接口和 ACL）的流量的配置命令的完全访问权限。网络管理员无法访问安全功能的配置命令或查看安全信息。
  - `netoperator` — 访问 EXEC 模式以查看当前配置。网络操作员无法修改交换机上的配置设置。

### 创建用户和分配角色

```
OS10(config)# username smith password silver403! role sysadmin
```

### 查看用户

```
OS10# show users
```

| Index | Line  | User  | Role     | Application | Idle | Login-Time            | Location         |
|-------|-------|-------|----------|-------------|------|-----------------------|------------------|
| 1     | ttyS  | root  | root     | -bash       | >24h | 2018-05-23 T23:05:03Z | console          |
| 2     | pts/0 | admin | sysadmin | bash        | 1.1s | 2018-05-30 T20:04:27Z | 10.14.1.214[ssh] |

## 引导加载程序保护

为防止未经授权的用户访问您的交换机，请使用 GRUB 密码来保护引导加载程序。OS10 允许您启用、禁用和查看启动程序保护。

此功能仅适用于 `sysadmin` 和 `secadmin` 角色。

 **警告:** 启用引导加载程序保护时，请保留已配置的用户名和密码的副本。如果没有已配置的凭据，您将无法访问交换机。

- 在 EXEC 模式下启用引导加载程序保护。使用 `boot protect enable` 命令配置用户名和密码。您可以为每个交换机配置最多三个用户。

```
OS10# boot protect enable username root password calvin
```

通过使用 `boot protect disable` 命令禁用指定用户的引导加载程序保护。

### 启用引导加载程序保护

```
OS10# boot protect enable username root password calvin
```

### 禁用引导加载程序保护

```
OS10# boot protect disable username root
```

### 显示引导加载程序保护

```
OS10# show boot protect
Boot protection enabled
Authorized users: root linuxadmin admin
```

## Linux 管理员用户配置

OS10 支持两个出厂默认用户：admin 和 linuxadmin。使用 admin 用户名登录命令行接口。使用 linuxadmin 用户名访问 Linux shell。

要从 CLI 管理默认 linuxadmin 用户，您可以执行以下操作：

- 配置丢失或忘记的 linuxadmin 密码。
- 禁用 linuxadmin 用户。

 **注:** 只能在根文件系统下配置 linuxadmin 用户，而不是在根文件系统下的其他 Linux 用户。

### 从 CLI 配置 linuxadmin 密码

要配置 linuxadmin 用户的密码，请在 CONFIGURATION 模式下使用 `system-user linuxadmin password {clear-text-password | hashed-password}` 命令。使用 `write memory` 命令保存新密码。例如：

```
OS10(config)# system-user linuxadmin password Dell@admin10!@
OS10(config)# exit
OS10# write memory
```

```
OS10(config)# system-user linuxadmin password
$6$3M55wOYy$Sw1V90k3GE4Hmf6h1ARH.dBHy9gpEFYUvdu15ZpnCYzt.nJjFm0VIZ/
rQvvJeX6krRtfYs2ZqBl6TkmLGAwTM
OS10(config)# exit
OS10# write memory
```

通过 CLI 配置的 linuxadmin 密码优先于通过 Linux shell 配置的密码进行重新引导。

使用 `show running-configuration` 命令验证 linuxadmin 密码。

```
OS10# show running-configuration
system-user linuxadmin password
$6$5DdOHYg5$JCElvMSmkQOrbh31U74PIpv71yOgRmba1IxhkYibppMXs1KM4Y.gbTPcxyMP/PHUkMc5rdk/
ZLv9Sfv3ALtB61
```

### 禁用 linuxadmin 用户

要禁用或锁定 linuxadmin 用户，请在 CONFIGURATION 模式下使用 `system-user linuxadmin disable` 命令。

```
OS10(config)# system-user linuxadmin disable
```

要重新启用或解锁 linuxadmin 用户，请在 CONFIGURATION 模式下使用 `no system-user linuxadmin disable` 命令。

```
OS10(config)# no system-user linuxadmin disable
```

## AAA 身份验证

OS10 交换机使用一系列身份验证方法来定义身份验证类型及其应用顺序。默认情况下，OS10 仅使用 `local` 身份验证方法。

方法列表中的身份验证方法按配置的顺序执行。重新输入更改订单的方法。`local` 身份验证方法仍保持启用状态，即使您使用 `no aaa authentication login {console | default}` 命令删除列表中的所有已配置方法。

**注：**如果您在以 SmartFabric 模式工作的 Dell EMC PowerEdge MX7000 以太网模块（MX9116n 网交引擎和 MX5108n 以太网交换机）上配置多个身份验证方法，必须将本地身份验证配置列表中的第一种方法。

- 在 CONFIGURATION 模式下配置 AAA 身份验证方法。

```
aaa authentication login {console | default} {local | group radius | group tacacs+}
```

- `console` — 配置控制台登录的身份验证方法。
- `default` — 配置非控制台身份验证方法，如 SSH 和 Telnet 登录。
- `local` — 使用通过 `username password role` 命令配置的本地用户名、密码和角色条目。
- `group radius` — 使用 `radius-server host` 命令配置 RADIUS 服务器。
- `group tacacs+` — 使用 `tacacs-server host` 命令配置 TACACS+ 服务器。

### 在服务器上配置用户角色

如果控制台用户使用 RADIUS 或 TACACS+ 身份验证登录，则将应用在 RADIUS 或 TACACS+ 服务器上为用户配置的角色。如果身份验证服务器上未配置任何角色，则用户身份验证失败。

此外，您必须使用特定于供应商的属性 (VSA) 配置 RADIUS 或 TACACS+ 服务器上的用户角色，否则身份验证将失败。Dell EMC 的供应商 ID 为 674。使用 `Name = Dell-group-name`，`OID = 2`，`Type = string` 创建 VSA。`Dell-group-name` 的有效值为 `sysadmin`、`secadmin`、`netadmin` 和 `netoperator`。在 RADIUS 或 TACACS+ 服务器上创建用户时，请使用 VSA `Dell-group-name` 值。

有关如何在 RADIUS 或 TACACS+ 服务器上配置特定于供应商的属性的详细信息，请参阅相应的 RADIUS 或 TACACS+ 服务器说明文件。

### 配置 AAA 身份验证

```
OS10(config)# aaa authentication login default group radius local
OS10(config)# do show running-configuration aaa
aaa authentication login default group radius local
aaa authentication login console local
```

### 移除 AAA 身份验证方法

```
OS10(config)# no aaa authentication login default
OS10(config)# do show running-configuration aaa
aaa authentication login default local
aaa authentication login console local
```

## RADIUS 身份验证

要配置 RADIUS 服务器进行身份验证，请输入服务器的 IP 地址或主机名称，以及用于在 RADIUS 主机上验证 OS10 交换机的密钥。您可以以纯文本或加密格式输入身份验证密钥。您可以在服务器上更改用户数据报协议 (UDP) 端口号。

- 在 CONFIGURATION 模式下配置 RADIUS 身份验证服务器。默认情况下，RADIUS 服务器使用 UDP 端口 1812。

```
radius-server host {hostname | ip-address} key {0 authentication-key | 9
authentication-key | authentication-key} [auth-port port-number]
```

要配置多个 RADIUS 服务器，请多次重新输入 `radius-server host` 命令。如果配置多个 RADIUS 服务器，OS10 会按照配置的顺序尝试连接。OS10 交换机一次连接一个配置的 RADIUS 服务器，直到 RADIUS 服务器通过接受或拒绝响应进行响应。交换机尝试在配置的重新传输重试次数和超时期限内与服务器连接。

为 RADIUS 服务器上允许的超时和重新传输尝试配置全局设置。默认情况下，OS10 支持三重 RADIUS 身份验证尝试，并在五秒后超时。未配置任何源接口。默认 VRF 实例用于联系 RADIUS 服务器。

**注：**您不能同时为 RADIUS 身份验证同时配置非默认 VRF 实例和源接口。

**注：**在非默认 VRF 上不支持使用主机名称配置的 RADIUS 服务器。

- 在 CONFIGURATION 模式下，配置 OS10 重新传输 RADIUS 身份验证请求的次数，重试次数可以为 0 到 100；默认值为 3。

```
radius-server retransmit retries
```

- 在 CONFIGURATION 模式下，配置用于等待来自 RADIUS 服务器的身份验证响应的超时期间，范围为 0 至 1000 秒；默认值为 5。

```
radius-server timeout seconds
```

- （可选）指定一个接口，其 IP 地址用作在 CONFIGURATION 模式中使用 RADIUS 服务器进行用户身份验证的源 IP 地址。默认情况下，未配置任何源接口。OS10 选择将数据包发送到 RADIUS 服务器的任何接口的源 IP 地址。

一个接口可以有两个 IPv4 地址和多个 IPv6 地址。所选 OS10 源接口与 RADIUS 服务器 IP 地址（IPv4 或 IPv6）的版本相匹配。

- 对于 IPv4 RADIUS 服务器，使用主 IPv4 地址。
- 对于 IPv6 服务器，将使用在接口上配置的任何全局 IPv6 地址。
- 如果未配置与 RADIUS 服务器相同的 IP 版本的地址，则使用管理接口的 IP 地址执行 RADIUS 身份验证（不使用源接口）。管理 IP 地址用作交换机上的 RADIUS 网络访问服务器 (NAS) IP 地址。

```
ip radius source-interface interface
```

在 RADIUS 服务器上，您必须使用 Linux 命令行更新配置的 IP 路由，以便源接口路由匹配 NAS IP 路由。

如果 OS10 使用 RADIUS 服务器 VRF 实例，则不支持 RADIUS 服务器源接口，因此无法进行配置。

- （可选）默认情况下，交换机使用默认 VRF 实例与 RADIUS 服务器进行通信。您可以选择在 CONFIGURATION 模式下配置非默认或管理 VRF 实例以进行 RADIUS 身份验证。

```
radius-server vrf management
radius-server vrf vrf-name
```

## 配置 RADIUS 服务器

```
OS10(config)# radius-server host 1.2.4.5 key secret1
OS10(config)# radius-server retransmit 10
OS10(config)# radius-server timeout 10
OS10(config)# ip radius source-interface mgmt 1/1/1
```

## 为非默认 VRF 配置 RADIUS 服务器

```
OS10(config)# ip vrf blue
OS10(conf-vrf)# exit
OS10(config)# radius-server vrf blue
```

## 查看 RADIUS 服务器配置

```
OS10# show running-configuration
...
radius-server host 1.2.4.5 key 9
3a95c26b2a5b96a6b80036839f296babe03560f4b0b7220d6454b3e71bdfc59b
radius-server retransmit 10
radius-server timeout 10
ip radius source-interface mgmt 1/1/1
...
```

## 删除 RADIUS 服务器

```
OS10# no radius-server host 1.2.4.5
```

# RADIUS over TLS 身份验证

传统的基于 RADIUS 的用户身份验证通过 UDP 运行，并使用 MD5 消息摘要算法来实现安全通信。要在 RADIUS 用户身份验证交换中提供增强的安全性，RFC 6614 定义了通过传输层安全 (TLS) 协议进行的 RADIUS。RADIUS over TLS 可在 TLS 连接中保护整个身份验证交换，并通过以下方式提供额外的安全性：

- 使用公钥基础设施 (PKI) 证书可以执行客户端和服务器的相互身份验证
- 加密整个身份验证交换，以使用户 ID 和密码均不易发现

RADIUS over TLS 身份验证需要在证书认证机构上配置 X.509v3 PKI 证书并安装在交换机上。有关详细信息，包括 RADIUS over TLS 的完整使用情形，请参阅 [X.509v3 证书](#)。

**注：**如果您使用 `crypto fips enable` 命令启用 FIPS，RADIUS over TLS 在 FIPS 模式下运行。在 FIPS 模式中，RADIUS over TLS 需要在交换机上安装符合 FIPS 的证书和密钥对。在非 FIPS 模式中，RADIUS over TLS 需要将证书安装为非 FIPS 证书。有关如何安装与 FIPS 兼容和非 FIPS 证书的信息，请参阅[请求和安装主机证书](#)。

要配置 RADIUS over TLS 用户身份验证，请使用 `radius-server host tls` 命令。输入服务器的 IP 地址或主机名称，以及用于验证 RADIUS 主机上的 OS10 交换机的共享密钥。您必须输入要与 RADIUS over TLS 身份验证一起使用的 X.509v3 安全配置文件的名称 — 请参阅[安全配置文件](#)。您可以以纯文本或加密格式输入身份验证密钥。默认情况下，RADIUS over TLS 连接使用 TCP 端口 2083，并且要求身份验证密钥为 `radsec`。您可以更改服务器上的 TCP 端口号。

- 在 CONFIGURATION 模式下的 RADIUS 服务器上配置 RADIUS over TLS 身份验证。

```
radius-server host {hostname | ip-address} tls security-profile profile-name
[auth-port port-number] key {0 authentication-key | 9 authentication-key |
authentication-key}
```

要为 RADIUS over TLS 身份验证配置多个 RADIUS 服务器，请多次重新输入 `radius-server host tls` 命令。如果配置多个 RADIUS 服务器，OS10 会按照配置的顺序尝试连接。OS10 交换机一次连接一个配置的 RADIUS 服务器，直到 RADIUS 服务器通过接受或拒绝响应进行响应。交换机尝试在配置的重新传输重试次数和超时期限内与服务器连接。

安全配置文件可确定交换机上的 X.509v3 证书，用于使用 RADIUS 服务器进行 TLS 身份验证。要为 OS10 应用程序配置安全配置文件，请参阅[安全配置文件](#)。

为 RADIUS 服务器上允许的超时和重新传输尝试配置全局设置，如 [RADIUS 身份验证](#) 中所述。

## 配置 RADIUS over TLS 身份验证服务器

```
OS10(config)# radius-server host 1.2.4.5 tls security-profile radius-prof key radsec
OS10(config)# radius-server retransmit 10
OS10(config)# radius-server timeout 10
```

# TACACS+ 身份验证

通过输入服务器 IP 地址或主机名称来配置 TACACS+ 身份验证服务器。您还必须为用于验证 TACACS+ 主机上的 OS10 交换机的密钥输入文本字符串。传输控制协议 (TCP) 端口条目是可选的。

TACACS+ 通过加密从交换机发送到身份验证服务器的数据包中的整个协议部分，提供更高的数据安全性。RADIUS 仅加密密码。

- 在 CONFIGURATION 模式下配置 TACACS+ 身份验证服务器。默认情况下，TACACS+ 服务器使用 TCP 端口 49 进行身份验证。

```
tacacs-server host {hostname | ip-address} key {0 authentication-key | 9
authentication-key | authentication-key} [auth-port port-number]
```

重新输入 `tacacs-server host` 命令多次，以配置多个 TACACS+ 服务器。如果您配置多个 TACACS+ 服务器，OS10 会尝试按配置的顺序进行连接。OS10 交换机一次连接一个配置的 TACACS+ 服务器，直到 TACACS+ 服务器使用接受或拒绝响应进行响应。



配置 TACACS+ 服务器上允许的全局超时设置。默认情况下，OS10 在五秒后超时。未配置任何源接口。默认 VRF 实例用于联系 TACACS+ 服务器。

**注:** 您不能同时为 TACACS+ 身份验证配置非默认 VRF 实例和源接口。

**注:** 在非默认 VRF 上不支持使用主机名称配置的 TACACS+ 服务器。

- 在 CONFIGURATION 模式下，配置用于等待来自 TACACS+ 服务器的身份验证响应的全局超时，从 1 到 1000 秒；默认值为 5。

```
tacacs-server timeout seconds
```

- (可选) 指定一个接口，其 IP 地址用作在 CONFIGURATION 模式中使用 TACACS+ 服务器进行用户身份验证的源 IP 地址。默认情况下，未配置任何源接口。OS10 选择将数据包发送到 TACACS+ 服务器的任何接口的源 IP 地址。

**注:** 如果配置的源接口没有 IP 地址，则使用管理接口的 IP 地址。

```
ip tacacs source-interface interface
```

- (可选) 默认情况下，交换机使用默认 VRF 实例与 TACACS+ 服务器进行通信。您可以选择在 CONFIGURATION 模式下配置非默认或管理 VRF 实例以进行 TACACS+ 身份验证。

```
tacacs-server vrf management
tacacs-server vrf vrf-name
```

## 配置 TACACS+ 服务器

```
OS10(config)# tacacs-server host 1.2.4.5 key mysecret
OS10(config)# ip tacacs source-interface loopback 2
```

## 为非默认 VRF 配置 TACACS+ 服务器

```
OS10(config)# ip vrf blue
OS10(conf-vrf)# exit
OS10(config)# tacacs-server vrf blue
```

## 查看 TACACS+ 服务器配置

```
OS10# show running-configuration
...
tacacs-server host 1.2.4.5 key 9
3a95c26b2a5b96a6b80036839f296babe03560f4b0b7220d6454b3e71bdfc59b
ip tacacs source-interface loopback 2
...
```

## 删除 TACACS+ 服务器

```
OS10# no tacacs-server host 1.2.4.5
```

# 未知用户角色

当 RADIUS 或 TACACS+ 服务器对用户进行身份验证时，它可能会返回未知用户角色，或可能缺少角色。在这些情况下，默认情况下，OS10 将 `netoperator` 角色和关联权限分配给用户。您可以重新配置默认分配的角色。此外，您可以配置未知的 RADIUS 或 TACACS+ 用户角色名称，以继承现有 OS10 系统定义的角色角色的权限。

- 在 CONFIGURATION 模式下重新配置默认 OS10 用户角色。

```
userrole {default | name} inherit existing-role-name
```

- `default inherit` — 重新配置已分配给具有缺失或未知角色的认证用户的默认权限。
- `name inherit` — 输入从 OS10 用户角色继承权限的 RADIUS 或 TACACS+ 用户角色的名称；最多 32 个字符。
- `existing-role-name` — 分配与现有的 OS10 用户角色关联的权限：
  - `sysadmin` — 对系统中所有命令的完全访问权限、对操作文件系统的命令的独占访问权限，以及对系统 shell 的访问权限。系统管理员可以创建用户 ID 和用户角色。

- `secadmin` — 对设置安全策略和系统访问权限的配置命令的完全访问权限，如密码强度、AAA 授权和加密密钥。安全管理员可以显示安全信息，如加密密钥、登录统计信息和日志信息。
- `netadmin` — 对管理流经交换机（如路由、接口和 ACL）的流量的配置命令的完全访问权限。网络管理员无法访问安全功能的配置命令或查看安全信息。
- `netoperator` — 仅访问 EXEC 模式以查看当前配置。网络操作员无法修改交换机上的配置设置。

### 重新配置未知用户角色的权限

```
OS10(config)# userrole default inherit sysadmin
```

### 为 RADIUS 或 TACACS+ 用户角色配置权限

```
OS10(config)# userrole tacacsadmin inherit netadmin
```

## SSH 服务器

在 OS10 中，安全 shell 服务器允许 SSH 客户端通过安全的加密连接访问 OS10 交换机。SSH 服务器使用 RADIUS 质询/响应、受信任的主机文件、本地存储的密码和公钥对远程客户端进行身份验证。

### 配置 SSH 服务器

- 默认情况下，SSH 服务器已启用。您可以使用 `no ip ssh server enable` 命令禁用 SSH 服务器。
- 默认情况下，质询响应身份验证已禁用。要启用，请使用 `ip ssh server challenge-response-authentication` 命令。
- 默认情况下，基于主机的身份验证已禁用。要启用，请使用 `ip ssh server hostbased-authentication` 命令。
- 默认情况下，密码身份验证已启用。要禁用，请使用 `no ip ssh server password-authentication` 命令。
- 默认情况下，公钥身份验证已启用。要禁用，请使用 `no ip ssh server pubkey-authentication` 命令。
- 默认情况下，不使用密码的登录已禁用。要启用，请使用 `username sshkey` 或 `username sshkey filename` 命令。
- 使用 `ip ssh server cipher cipher-list` 命令配置加密算法的列表。
- 使用 `ip ssh server kex key-exchange-algorithm` 命令配置密钥交换算法。
- 使用 `ip ssh server mac hmac-algorithm` 命令配置哈希消息身份验证代码 (HMAC) 算法。
- 使用 `ip ssh server port port-number` 命令配置 SSH 服务器侦听端口。
- 使用 `ip ssh server vrf` 命令将 SSH 服务器配置为可在管理 VRF 上访问。
- 使用 `ip ssh server login-grace-time seconds` 命令配置 SSH 登录超时，从 0 到 300；默认值为 60。要重设默认 SSH 提示计时器，请使用 `no ip ssh server login-grace-time` 命令。
- 使用 `ip ssh server max-auth-tries number` 命令配置身份验证尝试的最大数量，从 0 到 10；默认值为 6。要重置默认值，请使用 `no ip ssh server max-auth-tries` 命令。

`max-auth-tries` 值包括所有身份验证尝试，包括公钥和密码。如果同时启用了基于公钥的身份验证和密码身份验证，则公钥身份验证为默认设置，并首先尝试。如果失败，`max-auth-tries` 的数量将减少 1。在此情况下，如果您配置了 `ip ssh server max-auth-tries 1`，则不会显示密码提示。

### 重新生成公钥

启用时，默认情况下，SSH 服务器会生成公钥并将其用于客户端身份验证：

- Rivest、Shamir 和 Adelman (RSA) 密钥（使用 2048 位）。
- 椭圆曲线数字签名算法 (ECDSA) 密钥（使用 256 位）
- Ed25519 密钥（使用 256 位）

 **注：**OS10 SSH 服务器不支持 RSA1 和 DSA 密钥。

SSH 客户端必须交换相同公钥才能建立与 OS10 交换机的安全 SSH 连接。如有必要，您可以使用自定义的位大小重新生成 SSH 服务器使用的密钥。您不能更改 Ed25519 密钥的默认大小。`crypto key generate` 命令仅适用于 `sysadmin` 和 `secadmin` 角色。

1. 在 EXEC 模式下重新生成 SSH 服务器的密钥。

```
crypto ssh-key generate {rsa {2048|3072|4096} | ecdsa {256|384|521} | ed25519}
```

2. 在提示符处输入 `yes` 以覆盖现有密钥。

```
Host key already exists. Overwrite [confirm yes/no]:yes
Generated 2048-bit RSA key
```



3. 在 EXEC 模式下显示 SSH 公钥。

```
show crypto ssh-key
```

重新生成 SSH 服务器密钥后，禁用并重新启用 SSH 服务器以使用新密钥。重新启动 SSH 服务器不会影响当前 OS10 会话。

## 虚拟终端行 ACL

要限制 Telnet 和 SSH 到交换机的连接，请在虚拟终端线路上应用访问列表 (VTY)。

1. 使用 permit 或 deny 筛选器创建 IPv4 或 IPv6 访问列表；例如：

```
OS10(config)# ip access-list permit10
OS10(config-ipv4-acl)# permit ip 172.16.0.0 255.255.0.0 any
OS10(config-ipv4-acl)# exit
OS10(config)#
```

2. 在 CONFIGURATION 模式下使用 line vty 命令进入 VTY 模式。

```
OS10(config)# line vty
OS10(config-line-vty)#
```

3. 在 LINE-VTY 模式下使用 {ip | ipv6} access-class access-list-name 命令将访问列表应用到 VTY 行。

```
OS10(config-line-vty)# ip access-class permit10
```

### 查看 VTY ACL 配置

```
OS10(config-line-vty)# show configuration
!
line vty
 ip access-class permit10
 ipv6 access-class deny10
OS10(config-line-vty)#
```

## 限制 SNMP 访问

要筛选交换机上的 SNMP 请求，请将访问列表分配给 SNMP 社区。同时支持 IPv4 和 IPv6 访问列表。

1. 使用 permit 或 deny 筛选器创建访问列表；例如：

```
OS10(config)# ip access-list snmp-read-only-acl
OS10(config-ipv4-acl)# permit ip 172.16.0.0 255.255.0.0 any
OS10(config-ipv4-acl)# exit
OS10(config)#
```

2. 在 CONFIGURATION 模式下将 ACL 应用于 SNMP 社区。

```
OS10(config)# snmp-server community public ro acl snmp-read-only-acl
```

### 查看 SNMP ACL 配置

```
OS10# show snmp community
Community : public
Access : read-only
ACL : snmp-read-only-acl
```

## 启用 AAA 核算

要记录有关所有用户输入的命令的信息，请使用 AAA 核算功能 - 不支持 RADIUS 核算。在使用 console 选项的控制台连接和使用 default 选项的远程连接（如 Telnet 和 SSH）上，AAA 核算将记录 OS10 会话中的登录和命令信息。

AAA 核算会发送核算消息：

- 使用 `start-stop` 选项在进程开始时发送开始通知，并进程在结束时发送停止通知
- 使用 `stop-only` 选项在进程结束时仅发送停止通知
- 使用 `none` 选项不发送任何核算通知
- 使用 `logging` 选项记录 `syslog` 中的所有核算通知
- 使用 `group tacacs+` 选项记录配置的 TACACS+ 服务器中的所有核算通知

#### 启用 AAA 核算

- 在 CONFIGURATION 模式下启用 AAA 核算。

```
aaa accounting commands all {console | default} {start-stop | stop-only | none}
[logging] [group tacacs+]
```

此命令的 `no` 版本可禁用 AAA 核算。

## 启用用户锁定

默认情况下，在交换机上最多支持三次连续失败的密码尝试。可将限制设置为用户 ID 的指定锁定期限内允许的最大密码重试次数。

此功能仅适用于 `sysadmin` 和 `secadmin` 角色。

- 在 CONFIGURATION 模式下配置用户锁定设置。

```
password-attributes {[max-retry number] [lockout-period minutes]}
```

- `max-retry number` — 设置用户锁定之前连续失败登录尝试的最大次数，从 0 到 16；默认值为 3。
- `lockout-period minutes` — 设置用户 ID 在超过失败登录尝试的最大次数后禁止访问系统的时间量，从 0 到 43200；默认值为 0。

当用户由于超过失败登录尝试的最大次数而被锁定时，其他用户仍可访问该交换机。

默认情况下 `lockout-period minutes` 为 0；锁定期间未配置。失败的登录尝试不会锁定用户。

#### 配置用户锁定

```
OS10(config)# password-attributes max-retry 4 lockout period 360
```

## 限制并发登录会话

为避免同一用户 ID 的交换机上存在无限数量的活动会话，请限制控制台和远程连接的数量。通过将终端仿真程序连接到交换机上的控制台串行端口，从控制台连接登录。通过虚拟终端线路远程登录交换机，如 Telnet 和 SSH。

- 在 CONFIGURATION 模式下配置并发登录会话的最大数量。

```
OS10(config)# login concurrent-session limit number
```

- `limit number` — 设置用户 ID 允许的最大并发登录会话数，从 1 到 12；默认值为 10。

当您配置允许的并发登录会话的最大数量时，请考虑以下事项：

- 每个远程 VTY 连接将计数为一个登录会话。
- 连接的控制台上的终端仿真程序中的所有登录会话均计数为一个会话。

#### 配置并发登录会话

```
OS10(config)# login concurrent-session limit 4
```

如果您在并发会话的最大数量处于活动状态后登录到交换机，则会显示一条错误消息。要登录到系统，请关闭某个现有会话。

```
OS10(config)# login concurrent-session limit 4

Too many logins for 'admin'.
Last login: Wed Jan 31 20:37:34 2018 from 10.14.1.213
Connection to 10.11.178.26 closed.
Current sessions for user admin:
```

| Line    | Location   |
|---------|------------|
| 2 vty 0 | 10.14.1.97 |
| 3 vty 1 | 10.14.1.97 |
| 4 vty 2 | 10.14.1.97 |
| 5 vty 3 | 10.14.1.97 |

## 启用登录统计信息

要监控系统安全，请允许用户在登录系统时查看自己的登录统计信息。大量登录失败或不常见的登录位置可能表示系统黑客。启用在用户成功登录后显示启用登录信息；例如：

```
OS10 login: admin
Password:
Last login: Thu Nov 2 16:02:44 UTC 2017 on ttyS1
Linux OS10 3.16.43 #2 SMP Debian 3.16.43-2+deb8u5 x86_64
...
Time-frame for statistics : 25 days
Role changed since last login : false
Failures since last login : 0
Failures in time period : 1
Successes in time period : 14
OS10#
```

此功能仅适用于 `sysadmin` 和 `secadmin` 角色。

- 在 CONFIGURATION 模式下启用登录信息显示。

```
login-statistics enable
```

要显示有关用户登录的信息，请使用 `show login-statistics` 命令。

### 启用登录统计信息

```
OS10(config)# login-statistics enable
```

要禁用登录统计信息，请使用 `no login-statistics enable` 命令。

## 权限级别

控制对交换机的终端访问是一种保护设备和网络的方法。为提高安全性，您可以使用权限级别限制用户对命令子集的访问。

配置权限级别、向其添加命令，并使用密码限制对命令行的访问。系统支持 16 种权限级别：

- 级别 0 — 向用户提供最低权限，以限制对基本命令的访问。
- 级别 1 — 提供对一组 `show` 命令和某些操作（例如 `ping`、`traceroute` 等）的访问权限。
- 级别 15 — 提供对特定用户角色的所有可用命令的访问权限。
- 级别 0、1 和 15 — 系统配置的权限级别和预定义的命令集。
- 级别 2 至 14 — 未配置。您可以为不同用户或访问权限自定义这些级别。

权限级别继承所有较低级别上支持的命令。以用户角色登录后，用户可以访问分配给其权限级别和更低级别的命令。

对于分配了 `sysadmin`、`netadmin` 和 `secadmin` 角色的用户，您不能配置低于级别 2 的权限。您可以配置权限级别为 0 或 1 的 `netoperator` 用户。

将命令分配给权限级别后，使用 `username` 命令为用户分配权限级别。使用 `enable password privilege-level` 命令在权限级别之间切换，并访问每个级别支持的命令。`disable` 命令可将用户转到较低级别。

当远程用户登录时，OS10 会在本地系统中检查是否匹配。如果找到本地用户条目，则会将本地用户的权限级别应用于登录会话的远程用户。如果在本地系统中未找到匹配项，则 OS10 将根据远程用户的角色分配默认权限级别：

- `sysadmin`、`secadmin` 和 `netadmin` 角色：级别 15
- `netoperator` 角色：级别 1

 **注：**系统中的本地用户和登录的远程用户的角色在两端都必须相同。

## 配置权限级别

要限制 CLI 访问，请为用户角色创建所需的权限级别，将命令分配给每个级别，并为用户分配权限级别。

1. 在 CONFIGURATION 模式下创建权限级别。

```
privilege mode priv-lvl privilege-level command-string
```

- *mode* — 输入用于访问 CLI 模式的权限模式：
  - *exec* — 访问 EXEC 模式。
  - *configure* — 访问类别映射、DHCP、日志记录、监控、openflow、策略映射、QOS、支持协助、遥测、CoS、位图、UFD、VLT、VN、VRF、WRED 和别名模式。
  - *interface* — 访问以太网、光纤通道、环回、管理、空、端口组、延迟、分解、范围、端口通道和 VLAN 模式。
  - *route-map* — 访问路由映射模式。
  - *router* — 访问路由器 bgp 和路由器 ospf 模式。
  - *line* — 访问 line-vty 模式。
- *priv-lvl privilege-level* — 输入权限级别的数量，从 2 到 14。
- *command-string* — 输入权限级别支持的命令。

2. 创建用户名、密码和角色，并在 CONFIGURATION 模式下分配权限级别。

```
username username password password role role priv-lvl privilege-level
```

- *username username* — 输入文本字符串；最多 32 个字母数字字符；至少一个字符。
- *password password* — 输入文本字符串；最多 32 个字母数字字符，最少 9 个字符。
- *role role* — 输入用户角色：
  - *sysadmin* — 对系统中所有命令的完全访问权限、对操作文件系统的命令的独占访问权限，以及对系统 shell 的访问权限。系统管理员可以创建用户 ID 和用户角色。
  - *secadmin* — 对设置安全策略和系统访问权限的配置命令的完全访问权限，如密码强度、AAA 授权和加密密钥。安全管理员可以显示安全信息，如加密密钥、登录统计信息和日志信息。
  - *netadmin* — 对管理流经交换机（如路由、接口和 ACL）的流量的配置命令的完全访问权限。网络管理员无法访问安全功能的配置命令或查看安全信息。
  - *netoperator* — 访问 EXEC 模式以查看当前配置。网络操作员无法修改交换机上的配置设置。
- *priv-lvl privilege-level* — 输入权限级别，从 0 到 15。如果未指定 *priv-lvl* 选项，系统将为 *netoperator* 用户分配用户的权限级别 1，为 *sysadmin*、*secadmin* 和 *netadmin* 用户分配权限级别 15。

下面是配置权限级别并将其分配给用户的示例：

```
OS10(config)# privilege exec priv-lvl 12 "show version"
OS10(config)# privilege exec priv-lvl 12 "configure terminal"
OS10(config)# privilege configure priv-lvl 12 "interface ethernet"
OS10(config)# privilege interface priv-lvl 12 "ip address"
OS10(config)# username delluser password 6Yij02Phe2n6whp7b$ladskj0HowijIlkajg981 role
secadmin priv-lvl 12
```

以下示例显示了当前用户的权限级别：

```
OS10# show privilege
Current privilege level is 15.
```

以下示例显示登录 OS10 的所有用户的权限级别：

```
OS10# show users
```

| Index | Line  | User  | Role     | Application | Idle | Login-Time            | Location         | Privilege |
|-------|-------|-------|----------|-------------|------|-----------------------|------------------|-----------|
| 1     | pts/0 | admin | sysadmin | bash        | >24h | 2018-09-08 T06:51:37Z | 10.14.1.91 [ssh] | 15        |
| 2     | pts/1 | netad | netadmin | bash        | >24h | 2018-09-08 T06:54:33Z | 10.14.1.91 [ssh] | 10        |

## 配置启用密码

为用户配置权限级别后，将命令分配给每个级别和启用密码以访问每个级别：

1. 配置权限级别，并在 CONFIGURATION 模式中为其分配命令。

```
privilege mode priv-lvl privilege-level command-string
```

- *mode* — 输入用于访问 CLI 模式的权限模式：
  - *exec* — 访问 EXEC 模式。
  - *configure* — 访问类别映射、DHCP、日志记录、监控、openflow、策略映射、QOS、支持协助、遥测、CoS、位图、UFD、VLT、VN、VRF、WRED 和别名模式。
  - *interface* — 访问以太网、光纤通道、环回、管理、空、端口组、延迟、分解、范围、端口通道和 VLAN 模式。
  - *route-map* — 访问路由映射模式。
  - *router* — 访问路由器 bgp 和路由器 ospf 模式。
  - *line* — 访问 line-vty 模式。
- *priv-lvl privilege-level* — 输入权限级别的数量，从 2 到 14。
- *command-string* — 输入权限级别支持的命令。

对于 *sysadmin*、*netadmin* 和 *secadmin* 角色，您不能配置小于 2 的权限级别。

## 2. 为 CONFIGURATION 模式下的每个权限级别配置启用密码。

```
enable password encryption-type password-string priv-lvl privilege-level
```

- *encryption-type* — 输入密码条目的加密类型：
  - 0 — 使用纯文本而不使用密码加密。
  - sha-256 — 使用 SHA-256 算法加密密码。
  - sha-512 — 使用 SHA-512 算法加密密码。
- *priv-lvl privilege-level* — 输入权限级别，从 1 到 15。

```
OS10(config)# privilege exec priv-lvl 3 "show version"
OS10(config)# enable password 0 P@$w0Rd priv-lvl 3
```

```
OS10(config)# privilege exec priv-lvl 12 "configure terminal"
OS10(config)# privilege configure priv-lvl 12 route-map
OS10(config)# privilege route-map priv-lvl 12 "set local-preference"
OS10(config)# enable password sha-256 $5$2uThib1o$84p.tykjnz/w7j26ymoKBjrb7uepkUB priv-lvl 12
```

# 审核日志

要监控交换机上的用户活动和配置更改，请启用审核日志。只有 *sysadmin* 和 *secadmin* 角色可以启用、查看和清除审核日志。

审核日志记录了配置和安全事件，包括：

- 用户在交换机上登录和注销、登录失败以及用户的并发登录尝试
- 记录了基于用户的配置更改以及更改的用户 ID、日期和时间。未记录特定参数更改。
- 建立安全流量流（如 SSH）和安全流违规
- 证书问题，包括用户访问和使用 *crypto* 命令对证书的安装进行的更改
- 添加和删除用户

审核日志条目保存在本地，并发送到已配置的系统日志服务器。要设置 Syslog 服务器，请参阅[系统日志记录](#)。

## 启用审核日志

- 在 CONFIGURATION 模式下的 Syslog 服务器上的审核日志中启用配置和安全事件记录。

```
logging audit enable
```

要禁用审核日志记录功能，请使用 *no logging audit enable* 命令。

## 查看审核日志

- 在 EXEC 模式下显示审核日志条目。默认情况下，显示 24 个条目，从最早的事件开始。输入 *reverse* 以显示从最近事件开始的条目。您可以更改显示的条目数。

```
show logging audit [reverse] [number]
```

## 清除审核日志

- 在 CONFIGURATION 模式下清除审核日志中的所有事件。

```
clear logging audit
```

## 示例

```
OS10(config)# logging audit enable
OS10(config)# exit

OS10# show logging audit 4
<14>1 2019-02-14T13:15:06.283337+00:00 OS10 audispd - - - Node.1-Unit.1:PRI [audit],
Dell EMC (OS10) node=OS10 type=USER_END msg=audit(1550150106.277:597): pid=7908 uid=0
aid=4294967295 ses=4294967295 msg='op=PAM:session_close acct="admin" exe="/bin/su"
hostname=? addr=? terminal=??? res=success'
<110>1 2019-02-14T13:15:16.331515+00:00 OS10 .clish 7412 - - Node.1-Unit.1:PRI [audit],
User admin on console used cmd: 'crypto security-profile mltestprofile' - success
<110>1 2019-02-14T13:15:21.794529+00:00 OS10 .clish 7412 - - Node.1-Unit.1:PRI [audit],
User admin on console used cmd: 'exit' - success
<110>1 2019-02-14T13:16:05.882555+00:00 OS10 .clish 7412 - - Node.1-Unit.1:PRI [audit],
User admin on console used cmd: 'exit' - success

OS10# show logging audit reverse 4
<110>1 2019-02-14T13:16:05.882555+00:00 OS10 .clish 7412 - - Node.1-Unit.1:PRI [audit],
User admin on console used cmd: 'exit' - success
<110>1 2019-02-14T13:15:21.794529+00:00 OS10 .clish 7412 - - Node.1-Unit.1:PRI [audit],
User admin on console used cmd: 'exit' - success
<110>1 2019-02-14T13:15:16.331515+00:00 OS10 .clish 7412 - - Node.1-Unit.1:PRI [audit],
User admin on console used cmd: 'crypto security-profile mltestprofile' - success
<14>1 2019-02-14T13:15:06.283337+00:00 OS10 audispd - - - Node.1-Unit.1:PRI [audit],
Dell EMC (OS10) node=OS10 type=USER_END msg=audit(1550150106.277:597): pid=7908 uid=0
aid=4294967295 ses=4294967295 msg='op=PAM:session_close acct="admin" exe="/bin/su"
hostname=? addr=? terminal=??? res=success'OS10# show logging audit reverse 10
```

# 安全命令

## aaa accounting

启用 AAA 核算。

**语法**                   aaa accounting commands all {console | default} {start-stop | stop-only | none} [logging] [group tacacs+]

- 参数**
- **commands all** — 记录用户输入的所有命令。RADIUS 核算不支持此选项。
  - **console** — 在控制台连接上的 OS10 会话中记录所有用户身份验证和登录或所有用户输入的命令。
  - **default** — 在远程连接的 OS10 会话中记录所有用户身份验证和登录或所有用户输入的命令；例如，Telnet 和 SSH。
  - **start-stop** — 当进程开始时发送开始通知，并在进程结束时发出停止通知。
  - **stop-only** — 在进程结束时仅发送停止通知。
  - **none** — 未发送任何核算通知。
  - **logging** — 记录 syslog 中的所有核算通知。
  - **group tacacs+** — 记录第一个可访问 TACACS+ 服务器上的所有核算通知。

**默认**                   AAA 核算处于禁用状态。

**命令模式**           CONFIGURATION

**使用情况信息**       您可以在 syslog 和 TACACS+ 服务器上启用核算事件的记录。

从版本 10.4.1.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 no 版本可禁用 AAA 核算。

## 示例

```
OS10(config)# aaa accounting commands all console start-stop logging
group tacacs+
```

## 支持的版本

10.4.1.0 or later

# aaa authentication login

为控制台、SSH 和 Telnet 登录配置 AAA 身份验证方法。

## 语法

```
aaa authentication login {console | default} {local | group radius | group
tacacs+}
```

## 参数

- console — 配置控制台登录的身份验证方法。
- default — 配置 SSH 和 Telnet 登录的身份验证方法。
- local — 使用通过 username password role 命令配置的本地用户名、密码和角色条目。
- group radius — 使用通过 radius-server host 命令配置的 RADIUS 服务器。
- group tacacs+ — 使用通过 tacacs-server host 命令配置的 TACACS+ 服务器。

## 默认

本地身份验证

## 命令模式

CONFIGURATION

## 使用情况信息

**注:** 如果您在以 SmartFabric 模式工作的 Dell EMC PowerEdge MX7000 以太网模块（例如 MX9116n 结构交换引擎和 MX5108n 以太网交换机）上配置多个身份验证方法，则必须将本地身份验证配置为列表中的第一种方法。

从版本 10.4.1.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 no 版本将移除所有已配置的身份验证方法，并且默认为使用本地身份验证。

## 示例

```
OS10(config)# aaa authentication login default group radius local
OS10(config)# do show running-configuration aaa
aaa authentication login default group radius local
aaa authentication login console local
```

```
OS10(config)# no aaa authentication login default
OS10(config)# do show running-configuration aaa
aaa authentication login default local
aaa authentication login console local
```

## 支持的版本

10.4.1.0 or later

# aaa re-authenticate enable

身份验证方法或服务器发生更改后，要求用户重新进行身份验证。

## 语法

```
aaa re-authenticate enable
```

## 参数

无

## 默认

已禁用

## 命令模式

EXEC

## 使用情况信息

启用用户重新身份验证并更改身份验证方法或服务器后，用户将从交换机中注销，并提示您再次登录以重新进行身份验证。用户重新身份验证的触发者为：

- 使用 radius-server host 命令添加或删除作为配置的服务器主机的 RADIUS 服务器。
- 使用 aaa authentication [local | radius] 命令添加或删除身份验证方法。

从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。



命令的 `no` 版本将禁用用户重新身份验证。

**示例**

```
OS10(config)# aaa re-authenticate enable
```

**支持的版本**

10.4.0E(R1) or later

## boot protect disable username

允许您禁用引导加载程序保护。

**语法** `boot protect disable username username`

**参数** 无

**默认** 已禁用

**命令模式** EXEC

**使用情况信息** 您可以为每个单独用户禁用引导加载程序保护。

**示例**

```
OS10# boot protect disable username root
```

**支持的版本**

10.4.3.0 或更高版本

## boot protect enable username password

允许您启用引导加载程序保护。

**语法** `boot protect enable username username password password`

**参数**

- *username* — 输入用户名以提供对引导加载程序保护的访问权限。
- *password* — 输入指定用户名的密码。

**默认** 已禁用

**命令模式** EXEC

**使用情况信息** 您可以通过执行以下命令启用引导加载程序保护。您最多可以配置三个用户名/密码对以进行引导加载程序保护。

**示例**

```
OS10# boot protect enable username root password calvin
```

**支持的版本**

10.4.3.0 或更高版本

## clear logging audit

删除审核日志中的所有事件。

**语法** `clear logging audit`

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 要显示审核日志的内容，请使用 `show logging audit` 命令。

**示例**

```
OS10# clear logging audit
Proceed to clear all audit log messages [confirm yes/no(default)]:yes
```



支持的版本 10.4.3.0 or later

## crypto ssh-key generate

重新生成 SSH 身份验证中使用的公钥。

|        |                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>crypto ssh-key generate {rsa bits   ecdsa bits   ed25519}</code>                                                                                                                                                                                           |
| 参数     | <ul style="list-style-type: none"><li><code>rsa bits</code> — 重新生成具有指定的位大小（2048、3072 或 4096）的 RSA 密钥；默认 2048。</li><li><code>ecdsa bits</code> — 重新生成具有指定的位大小（256、384 或 521）的 ECDSA 密钥；默认 256。</li><li><code>ed25519</code> — 重新生成具有默认的位大小的 Ed25519 密钥。</li></ul> |
| 默认     | SSH 服务器使用默认的公钥长度进行客户端身份验证： <ul style="list-style-type: none"><li>RSA 密钥：2048 位</li><li>ECDSA 密钥：256 位</li><li>Ed25519 密钥：256 位</li></ul>                                                                                                                         |
| 命令模式   | EXEC                                                                                                                                                                                                                                                             |
| 使用情况信息 | 如有必要，您可以使用自定义的位大小重新生成 SSH 服务器使用的公钥。您不能更改 Ed25519 密钥的默认大小。 <code>crypto ssh-key generate</code> 命令仅适用于 <code>sysadmin</code> 和 <code>secadmin</code> 角色。                                                                                                          |
| 示例     | <pre>OS10# crypto ssh-key generate rsa 4096 Host key already exists. Overwrite [confirm yes/no]:yes Generated 4096-bit RSA key OS10#</pre>                                                                                                                       |

支持的版本 10.4.1.0 or later

## disable

降低权限级别。

|        |                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------|
| 语法     | <code>disable privilege-level</code>                                                            |
| 参数     | <ul style="list-style-type: none"><li><code>privilege-level</code> — 输入权限级别，从 0 到 15。</li></ul> |
| 默认     | 1                                                                                               |
| 命令模式   | 特权 EXEC                                                                                         |
| 使用情况信息 | 如果未指定权限级别，系统将分配 1 级。                                                                            |
| 示例     | <pre>OS10# disable  OS10# disable 6</pre>                                                       |

支持的版本 10.4.3.0 or later

## enable

启用特定权限级别。

|      |                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------|
| 语法   | <code>enable privilege-level</code>                                                                 |
| 参数   | <ul style="list-style-type: none"><li><code>privilege-level</code> — 输入已配置的权限级别，从 0 到 15。</li></ul> |
| 默认   | 15                                                                                                  |
| 命令模式 | Exec                                                                                                |

## 使用情况信息

Dell EMC Networking 建议使用 `enable password` 命令配置权限级别为 15 的密码。如果未配置某个级别的密码，您可以在不输入密码的情况下切换到该级别，除非密码配置了最高的中间级别。如果为中间级别配置了密码，则在出现提示时输入该密码。要访问权限级别 15，必须配置 `enable password` 命令。如果未配置权限级别为 15 的密码，则无法输入级别 15。对于权限级别 0 至 14，`enable password` 命令为可选项。

权限级别从所有较低级别继承所有允许的命令。例如，如果您使用 `enable 10` 命令登录到权限级别 10，则分配给权限级别 10 和更低级别的所有命令均可供使用。

## 示例

```
OS10# enable
```

```
OS10# enable 10
```

## 支持的版本

10.4.3.0 or later

# enable password priv-lvl

为权限级别设置密码。

## 语法

```
enable password encryption-type password-string priv-lvl privilege-level
```

## 参数

- encryption-type* — 输入密码加密的类型：
  - 0 — 使用未加密的密码。
  - sha-256 — 使用 SHA-256 加密的密码。
  - sha-512 — 使用 SHA-512 加密的密码。
- priv-lvl privilege-level* — 输入权限编号，从 1 到 15。

## 默认

未配置

## 命令模式

CONFIGURATION

## 使用情况信息

要增加所需的密码强度，请使用 `password-attributes` 命令创建更强的密码规则。此命令的 `no` 版本将移除权限级别密码。

## 示例

```
OS10(conf)# enable password 0 P@$$w0Rd priv-lvl 12
```

```
OS10(conf)# enable password sha-256 $5$2uThib1o$84p.tykjnz/
w7j26ymoKBjrb7uepkUB priv-lvl 12
```

```
OS10(conf)# enable password sha-512
6Yij02Phe2n6whp7b$ladskj0HowijIlkajg981 priv-lvl 12
```

```
OS10# enable 12
password:
OS10# show privilege
Current privilege level is 12.
```

## 支持的版本

10.4.3.0 or later

# ip access-class

使用 IPv4 访问列表筛选虚拟终端线路中的连接。

## 语法

```
ip access-class access-list-name
```

## 参数

*access-list-name* — 输入访问列表名称。

## 默认

未配置

## 命令模式

LINE VTY CONFIGURATION

**使用情况信息** 此命令的 `no` 版本将移除筛选器。

**示例**

```
OS10(config)# line vty
OS10(config-line-vty)# ip access-class deny10
```

**支持的版本** 10.4.0E(R1) or later

## ip radius source-interface

指定 IP 地址用作 RADIUS 服务器进行用户身份验证的 IP 地址的接口。

**语法** `ip radius source-interface interface`

**参数**

`interface:`

- `ethernet node/slot/port[:subport]` — 输入物理以太网接口。
- `loopback number` — 输入环回接口, 从 0 到 16383。
- `mgmt 1/1/1` — 输入管理接口。
- `port-channel channel-id` — 输入端口通道 ID, 从 1 到 28。
- `vlan vlan-id` — 输入 VLAN ID, 从 1 到 4093。

**默认** 未配置。

**命令模式** CONFIGURATION

**使用情况信息** 默认情况下, 未配置任何源接口。OS10 选择源 IP 地址作为将数据包发送到 RADIUS 服务器的接口的 IP 地址。此命令的 `no` 版本将移除配置的源接口。

**示例**

```
OS10(config)# ip radius source-interface ethernet 1/1/10
```

**支持的版本** 10.4.3.1 或更高版本

## ip tacacs source-interface

指定 IP 地址用作 TACACS+ 服务器进行用户身份验证的 IP 地址的接口。

**语法** `ip tacacs source-interface interface`

**参数**

`interface:`

- `ethernet node/slot/port[:subport]` — 输入物理以太网接口。
- `loopback number` — 输入环回接口, 从 0 到 16383。
- `mgmt 1/1/1` — 输入管理接口。
- `port-channel channel-id` — 输入端口通道 ID, 从 1 到 28。
- `vlan vlan-id` — 输入 VLAN ID, 从 1 到 4093。

**默认** 未配置。

**命令模式** CONFIGURATION

**使用情况信息** 默认情况下, 未配置任何源接口。OS10 选择源 IP 地址作为将数据包发送到 TACACS+ 服务器的接口的 IP 地址。此命令的 `no` 版本将移除配置的源接口。

**示例**

```
OS10(config)# ip tacacs source-interface ethernet 1/1/10
```

**支持的版本** 10.4.1.0 or later

## ipv6 access-class

使用 IPv6 访问列表可筛选虚拟终端线路中的连接。

**语法** `ipv6 access-class access-list-name`

**参数** *access-list-name* — 输入访问列表名称。

**默认** 未配置

**命令模式** LINE VTY CONFIGURATION

**使用情况信息** 此命令的 *no* 版本将移除筛选器。

**示例**

```
OS10(config)# line vty
OS10(config-line-vty)# ipv6 access-class permit10
```

**支持的版本** 10.4.0E(R1) or later

## ip ssh server challenge-response-authentication

在 SSH 服务器中启用质询响应身份验证。

**语法** *ip ssh server challenge-response-authentication*

**参数** 无

**默认** 已禁用

**命令模式** CONFIGURATION

**使用情况信息** 从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 *no* 版本将禁用质询响应身份验证。

**示例**

```
OS10(config)# ip ssh server challenge-response-authentication
```

**支持的版本** 10.3.0E or later

## ip ssh server cipher

在 SSH 服务器中配置密码算法的列表。

**语法** *ip ssh server cipher cipher-list*

**参数** *cipher-list* — 输入加密算法的列表。用空格分隔多个条目。SSH 服务器支持的密码算法如下：

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com
- blowfish-cbc
- cast128-cbc
- chacha20-poly1305@opens

**默认**

- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com
- chacha20-poly1305@opens

**命令模式** CONFIGURATION

|               |                                                                                                                                |
|---------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>使用情况信息</b> | 从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。<br>此命令的 <code>no</code> 版本将移除配置。 |
| <b>示例</b>     | <pre>OS10(config)# ip ssh server cipher 3des-cbc aes128-cbc</pre>                                                              |
| <b>支持的版本</b>  | 10.3.0E or later                                                                                                               |

## ip ssh server enable

启用 SSH 服务器。

|               |                                                                                                                                      |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ip ssh server enable</code>                                                                                                    |
| <b>参数</b>     | 无                                                                                                                                    |
| <b>默认</b>     | 已启用                                                                                                                                  |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                        |
| <b>使用情况信息</b> | 从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。<br>此命令的 <code>no</code> 版本将禁用 SSH 服务器。 |
| <b>示例</b>     | <pre>OS10(config)# ip ssh server enable</pre>                                                                                        |
| <b>支持的版本</b>  | 10.3.0E or later                                                                                                                     |

## ip ssh server hostbased-authentication

在 SSH 服务器中启用基于主机的身份验证。

|               |                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>ip ssh server hostbased-authentication</code>                                                                                   |
| <b>参数</b>     | 无                                                                                                                                     |
| <b>默认</b>     | 已禁用                                                                                                                                   |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                         |
| <b>使用情况信息</b> | 从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。<br>此命令的 <code>no</code> 版本将禁用基于主机的身份验证。 |
| <b>示例</b>     | <pre>OS10(config)# ip ssh server hostbased-authentication</pre>                                                                       |
| <b>支持的版本</b>  | 10.3.0E or later                                                                                                                      |

## ip ssh server kex

配置 SSH 服务器中使用的密钥交换算法。

|           |                                                                                                                                                                                                                                                                 |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b> | <code>ip ssh server kex <i>key-exchange-algorithm</i></code>                                                                                                                                                                                                    |
| <b>参数</b> | <i>key-exchange-algorithm</i> — 输入由空格分隔的受支持的密钥交换算法。SSH 服务器支持以下密钥交换算法： <ul style="list-style-type: none"> <li>• <code>curve25519-sha256</code></li> <li>• <code>diffie-hellman-group1-sha1</code></li> <li>• <code>diffie-hellman-group14-sha1</code></li> </ul> |

|        |                                                                                                                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <ul style="list-style-type: none"> <li>• diffie-hellman-group-exchange-sha1</li> <li>• diffie-hellman-group-exchange-sha256</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp521</li> </ul>                       |
| 默认     | <ul style="list-style-type: none"> <li>• curve25519-sha256</li> <li>• diffie-hellman-group14-sha1</li> <li>• diffie-hellman-group-exchange-sha256</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp521</li> </ul> |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                          |
| 使用情况信息 | <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p> <p>此命令的 <code>no</code> 版本将移除配置。</p>                                                                                                              |
| 示例     | <pre>OS10(config)# ip ssh server kex curve25519-sha256 diffie-hellman-group1-sha1</pre>                                                                                                                                                                |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                       |

## ip ssh server mac

配置 SSH 服务器中使用的哈希消息身份验证代码 (HMAC) 算法。

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>ip ssh server mac <i>hmac-algorithm</i></code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 参数 | <p><i>hmac-algorithm</i> — 输入由空格分隔的受支持的 HMAC 算法。SSH 服务器支持以下 HMAC 算法：</p> <ul style="list-style-type: none"> <li>• hmac-md5</li> <li>• hmac-md5-96</li> <li>• hmac-ripemd160</li> <li>• hmac-sha1</li> <li>• hmac-sha1-96</li> <li>• hmac-sha2-256</li> <li>• hmac-sha2-512</li> <li>• umac-64@openssh.com</li> <li>• umac-128@openssh.com</li> <li>• hmac-md5-etm@openssh.com</li> <li>• hmac-md5-96-etm@openssh.com</li> <li>• hmac-ripemd160-etm@openssh.com</li> <li>• hmac-sha1-etm@openssh.com</li> <li>• hmac-sha1-96-etm@openssh.com</li> <li>• hmac-sha2-256-etm@openssh.com</li> <li>• hmac-sha2-512-etm@openssh.com</li> <li>• umac-64-etm@openssh.com</li> <li>• umac-128-etm@openssh.com</li> </ul> |
| 默认 | <ul style="list-style-type: none"> <li>• hmac-sha1</li> <li>• hmac-sha2-256</li> <li>• hmac-sha2-512</li> <li>• umac-64@openssh.com</li> <li>• umac-128@openssh.com</li> <li>• hmac-sha1-etm@openssh.com</li> <li>• hmac-sha2-256-etm@openssh.com</li> <li>• hmac-sha2-512-etm@openssh.com</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                           |

- umac-64-etm@openssh.com
- umac-128-etm@openssh.com

#### 命令模式

CONFIGURATION

#### 使用情况信息

从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 `no` 版本将移除配置。

#### 示例

```
OS10(config)# ip ssh server mac hmac-md5 hmac-md5-96 hmac-ripemd160
```

#### 支持的版本

10.3.0E or later

## ip ssh server password-authentication

在 SSH 服务器中启用密码身份验证。

#### 语法

```
ip ssh server password-authentication
```

#### 参数

无

#### 默认

已启用

#### 命令模式

CONFIGURATION

#### 使用情况信息

从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 `no` 版本将禁用密码身份验证。

#### 示例

```
OS10(config)# ip ssh server password-authentication
```

#### 支持的版本

10.3.0E or later

## ip ssh server port

配置 SSH 服务器侦听端口。

#### 语法

```
ip ssh server port port-number
```

#### 参数

*port-number* — 输入侦听端口号，从 1 到 65535。

#### 默认

22

#### 命令模式

CONFIGURATION

#### 使用情况信息

从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 `no` 版本将移除配置。

#### 示例

```
OS10(config)# ip ssh server port 255
```

#### 支持的版本

10.3.0E or later

## ip ssh server pubkey-authentication

为 SSH 服务器启用公钥身份验证。

#### 语法

```
ip ssh server pubkey-authentication
```

#### 参数

无

|        |                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------|
| 默认     | 已启用                                                                                                                   |
| 命令模式   | CONFIGURATION                                                                                                         |
| 使用情况信息 | 从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。<br>此命令的 no 版本将禁用公钥身份验证。 |
| 示例     | <pre>OS10(config)# ip ssh server pubkey-authentication</pre>                                                          |
| 支持的版本  | 10.3.0E or later                                                                                                      |

## ip ssh server vrf

为管理或非默认 VRF 实例配置 SSH 服务器。

|        |                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip ssh server vrf {management   vrf vrf-name}</code>                                                                                                        |
| 参数     | <ul style="list-style-type: none"> <li><code>management</code> — 将管理 VRF 实例配置为访问 SSH 服务器。</li> <li><code>vrf vrf-name</code> — 输入用于访问 SSH 服务器的 VRF 实例。</li> </ul> |
| 默认     | 未配置                                                                                                                                                               |
| 命令模式   | CONFIGURATION                                                                                                                                                     |
| 使用情况信息 | SSH 服务器使用管理 VRF。                                                                                                                                                  |
| 示例     | <pre>OS10(config)# ip ssh server vrf management OS10(config)# ip ssh server vrf vrf-blue</pre>                                                                    |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                              |

## line vty

进入虚拟终端线路模式以访问虚拟终端 (VTY)。

|        |                                                          |
|--------|----------------------------------------------------------|
| 语法     | <code>line vty</code>                                    |
| 参数     | 无                                                        |
| 默认     | 未配置                                                      |
| 命令模式   | CONFIGURATION                                            |
| 使用情况信息 | 无                                                        |
| 示例     | <pre>OS10(config)# line vty OS10(config-line-vty)#</pre> |
| 支持的版本  | 10.4.0E(R1) or later                                     |

## logging audit enable

允许在审核日志中记录配置和安全事件。

|      |                                   |
|------|-----------------------------------|
| 语法   | <code>logging audit enable</code> |
| 参数   | 无                                 |
| 默认   | 未配置                               |
| 命令模式 | CONFIGURATION                     |



|               |                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>使用情况信息</b> | 审核日志条目保存在本地，并发送到已配置的系统日志服务器。只有 <code>sysadmin</code> 和 <code>secadmin</code> 角色可以启用审核日志。命令的 <code>no</code> 版本将禁用审核日志记录。 |
| <b>示例</b>     | <pre>OS10(config)# logging audit enable</pre>                                                                            |
| <b>支持的版本</b>  | 10.4.3.0 or later                                                                                                        |

## login concurrent-session limit

配置用户 ID 所允许的最大并发登录会话数。

|               |                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>login concurrent-session limit <i>number</i></code>                                                                                                                                 |
| <b>参数</b>     | 限制 <i>number</i> — 输入并发登录会话的限制，从 1 到 12。                                                                                                                                                  |
| <b>默认</b>     | 10 个并发登录会话                                                                                                                                                                                |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                                                                             |
| <b>使用情况信息</b> | 同一用户 ID 的并发登录会话总数包括所有控制台和远程连接，其中： <ul style="list-style-type: none"> <li>每个远程 VTY 连接将计数为一个登录会话。</li> <li>连接的控制台上的终端仿真程序中的所有登录会话均计数为一个会话。</li> </ul> 命令的 <code>no</code> 版本将禁用已配置的允许登录会话数。 |

**示例**

```
OS10(config)# login concurrent-session limit 7
```

**支持的版本** 10.4.1.0 or later

## login-statistics enable

支持向用户显示登录统计信息。

|               |                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>login-statistics enable</code>                                                                                                                             |
| <b>参数</b>     | 无                                                                                                                                                                |
| <b>默认</b>     | 已禁用                                                                                                                                                              |
| <b>命令模式</b>   | CONFIGURATION                                                                                                                                                    |
| <b>使用情况信息</b> | 只有 <code>sysadmin</code> 和 <code>secadmin</code> 角色可以访问此命令。启用时，将在成功登录后显示用户登录信息，包括成功和失败登录次数、角色更改以及用户上次登录的时间。 <code>no login-statistics enable</code> 命令将禁用登录统计信息。 |

**示例**

```
OS10(config)# login-statistics enable
```

**支持的版本** 10.4.0E(R1) or later

## mac address-table static

为 L2 MAC 地址表配置静态条目。

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b> | <code>mac address-table static <i>mac-address</i> vlan <i>vlan-id</i> interface {<i>ethernet node/slot/port[:subport]</i>   <i>port-channel number</i>}</code>                                                                                                                                                                                                                                                                                                 |
| <b>参数</b> | <ul style="list-style-type: none"> <li><code>mac-address</code> — 以 <code>nn:nn:nn:nn:nn:nn</code> 格式输入要添加到表的 MAC 地址。</li> <li><code>vlan <i>vlan-id</i></code> — 输入要将静态 MAC 地址应用到的 VLAN，从 1 到 4093。</li> <li><code>interface</code> — 输入接口类型： <ul style="list-style-type: none"> <li><code>ethernet <i>node/slot/port[:subport]</i></code> — 输入以太网信息。</li> <li><code>port-channel <i>channel-number</i></code> — 输入端口通道接口编号，从 1 到 128。</li> </ul> </li> </ul> |

|        |                                    |
|--------|------------------------------------|
| 默认     | 未配置                                |
| 命令模式   | CONFIGURATION                      |
| 使用情况信息 | 此命令的 <code>no</code> 版本会将该值重置为默认值。 |

#### 示例 (VLAN)

```
OS10(config)# mac address-table static 34:17:eb:f2:ab:c6 vlan 1
interface ethernet 1/1/30
```

#### 示例 (端口通道)

```
OS10(config)# mac address-table static 34:17:eb:02:8c:33 vlan 10
interface port-channel 1
```

支持的版本 10.2.0E or later

## password-attributes

配置密码条目的规则。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>password-attributes {[min-length <i>number</i>] [character-restriction {[upper <i>number</i>] [lower <i>number</i>] [numeric <i>number</i>] [special-char <i>number</i>]}]}</code>                                                                                                                                                                                                                                                                                                                                                                           |
| 参数     | <ul style="list-style-type: none"> <li><code>min-length <i>number</i></code> — (可选) 设置所需字母数字字符的最小数量, 从 6 到 32; 默认值为 9。</li> <li><code>character-restriction</code>: <ul style="list-style-type: none"> <li><code>upper <i>number</i></code> — (可选) 设置最小大写字符数, 从 0 到 31; 默认值为 0。</li> <li><code>lower <i>number</i></code> — (可选) 设置所需的最小小写字符数, 从 0 到 31; 默认值为 0。</li> <li><code>numeric <i>number</i></code> — (可选) 设置所需的最小数字字符数, 从 0 到 31; 默认值为 0。</li> <li><code>special-char <i>number</i></code> — (可选) 设置所需的最小特殊字符数, 从 0 到 31; 默认值为 0。</li> </ul> </li> </ul> |
| 默认     | <ul style="list-style-type: none"> <li>最小长度: 9 个字符</li> <li>大写字符: 0</li> <li>小写字符: 0</li> <li>数字字符: 0</li> <li>特殊字符: 0</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 使用情况信息 | <p>默认情况下, 使用 <code>username password</code> 命令配置的密码必须至少包含 9 个字母数字字符。</p> <p>使用此命令可增加密码强度。输入命令时, 至少需要一个参数。输入此 <code>character-restriction</code> 参数时, 至少需要一个选项。</p> <p>要将参数重设为默认值, 请使用 <code>no password-attributes</code> 命令。</p> <p>从版本 10.4.0E(R3S) 开始, 在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始, 在 SmartFabric 模式下也受支持。</p>                                                                                                                                                                                                                           |
| 示例     | <pre>OS10(config)# password-attributes min-length 6 character-restriction upper 2 lower 2 numeric 2</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## password-attributes max-retry lockout-period

配置最多连续失败登录尝试次数和用户 ID 的锁定期限。

|    |                                                                                                                                                                                                                                           |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>password-attributes {[max-retry <i>number</i>] [lockout-period <i>minutes</i>]}</code>                                                                                                                                              |
| 参数 | <ul style="list-style-type: none"> <li><code>max-retry <i>number</i></code> — (可选) 设置用户锁定之前连续失败登录尝试的最大次数, 从 0 到 16。</li> <li><code>lockout-period <i>minutes</i></code> — (可选) 设置用户 ID 在超过失败登录尝试的最大次数后禁止访问系统的时间量, 从 0 到 43200。</li> </ul> |
| 默认 | <ul style="list-style-type: none"> <li>最大重试次数: 3</li> </ul>                                                                                                                                                                               |

- 锁定期：0 — 未配置锁定期。失败的登录尝试不会锁定用户。

#### 命令模式

CONFIGURATION

#### 使用情况信息

要删除已配置的 `max-retry` 或 `lockout-period` 设置，请使用 `no password-attributes {max-retry | lockout-period}` 命令。

当用户由于超过失败登录尝试的最大次数而被锁定时，其他用户仍可访问该交换机。

从版本 10.4.1.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

#### 示例

```
OS10(config)# password-attributes max-retry 5 lockout-period 30
```

#### 支持的版本

10.4.1.0 or later

## privilege

创建权限级别并与命令关联。

#### 语法

```
privilege mode priv-lvl privilege-level command-string
```

#### 参数

- `mode` — 输入用于访问 CLI 模式的权限模式：
  - `exec` — 访问 EXEC 模式。
  - `configure` — 访问类别映射、DHCP、日志记录、监控、openflow、策略映射、QOS、支持协助、遥测、CoS、位图、UFD、VLT、VN、VRF、WRED 和别名模式。
  - `interface` — 访问以太网、光纤通道、环回、管理、空、端口组、延迟、分解、范围、端口通道和 VLAN 模式。
  - `route-map` — 访问路由映射模式。
  - `router` — 访问路由器 bgp 和路由器 ospf 模式。
  - `line` — 访问 line-vty 模式。
- `priv-lvl privilege-level` — 输入权限级别的数量，从 2 到 14。
- `command-string` — 输入权限级别支持的命令。

#### 默认

未配置

#### 命令模式

CONFIGURATION

#### 使用情况信息

对于分配了 `sysadminnetadmin` 和 `secadmin` 角色的用户，您不能配置低于级别 2 的权限。

如果与权限级别关联的命令有空格，请使用双引号 (") 输入命令。如果某个命令没有空格或包含用连字符分隔的关键字，则无需使用双引号。

此命令的 `no` 版本将从权限级别移除命令。

#### 示例

```
OS10(config)# privilege exec priv-lvl 3 "configure terminal"
OS10(config)# privilege configure priv-lvl 3 "interface ethernet"
OS10(config)# privilege interface priv-lvl 3 "ip address"
OS10(config)# privilege configure priv-lvl 3 route-map
OS10(config)# privilege route-map priv-lvl 3 "set local-preference"
```

#### 支持的版本

10.4.3.0 or later

## radius-server host

配置 RADIUS 服务器和用于对服务器上的交换机进行身份验证的密钥。

#### 语法

```
radius-server host {hostname | ip-address} key {0 authentication-key | 9 authentication-key | authentication-key} [auth-port port-number]
```

#### 参数

- `hostname` — 输入 RADIUS 服务器的主机名称。
- `ip-address` — 输入 RADIUS 服务器的 IPv4 (A.B.C.D) 或 IPv6 (x:x:x:x::x) 地址。
- `key 0 authentication-key` — 以纯文本格式输入身份验证密钥。最多 42 个字符。

- `key 9 authentication-key` — 以加密格式输入身份验证密钥。最多 128 个字符。
- `authentication-key` — 以纯文本格式输入身份验证。最多 42 个字符。不需要在密钥之前输入 0。
- `auth-port port-number` — (可选) 输入用于身份验证的服务器上使用的 UDP 端口, 从 0 到 65535, 默认值为 1812。

|        |                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                  |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                        |
| 使用情况信息 | <p>身份验证密钥必须与 RADIUS 服务器上配置的密钥相匹配。您不能在密钥中输入空格。<code>show running-configuration</code> 输出以加密格式显示未加密密钥和加密密钥。使用 <code>radius-server retransmit</code> 和 <code>radius-server timeout</code> 命令为 RADIUS 服务器上允许的超时和重新传输尝试配置全局设置。</p> <p>从版本 10.4.0E(R3S) 开始, 在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始, 在 SmartFabric 模式下也受支持。</p> <p>此命令的 <code>no</code> 版本将移除 RADIUS 服务器配置。</p> |
| 示例     | <pre>OS10(config)# radius-server host 1.5.6.4 key secret1</pre>                                                                                                                                                                                                                                                                                                                      |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                     |

## radius-server host tls

配置用于 RADIUS over TLS 用户身份验证和安全通信的 RADIUS 服务器。对于 RADIUS over TLS 身份验证, 需要使用 X.509v3 证书的 `radsec` 共享密钥和安全配置文件。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <pre>radius-server host {hostname   ip-address} tls security-profile profile-name [auth-port tcp-port-number] key {0 authentication-key   9 authentication-key   authentication-key}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 参数     | <ul style="list-style-type: none"> <li>• <code>hostname</code> — 输入 RADIUS 服务器的主机名称。</li> <li>• <code>ip-address</code> — 输入 RADIUS 服务器的 IPv4 (A.B.C.D) 或 IPv6 (x:x:x:x::x) 地址。</li> <li>• <code>tls</code> — 输入 <code>tls</code> 以使用 TLS 协议保护 RADIUS 服务器通信。</li> <li>• <code>security-profile profile-name</code> — 输入要与 RADIUS over TLS 身份验证一起使用的 X.509v3 安全配置文件的名称。要为 OS10 应用程序配置安全配置文件, 请参阅<a href="#">安全配置文件</a>。</li> <li>• <code>auth-port tcp-port-number</code> — (可选) 输入服务器用于身份验证的 TCP 端口号。范围从 0 到 65535。默认值为 2083。</li> <li>• <code>key 0 authentication-key</code> — 以纯文本形式输入 <code>radsec</code> 共享密钥。</li> <li>• <code>key 9 authentication-key</code> — 以加密格式输入 <code>radsec</code> 共享密钥。</li> <li>• <code>authentication-key</code> — 以纯文本形式输入 <code>radsec</code> 共享密钥。不需要在密钥之前输入 0。</li> </ul> |
| 默认     | RADIUS 服务器上用于 RADIUS over TLS 通信的 TCP 端口 2083                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 使用情况信息 | <p>对于 RADIUS over TLS 身份验证, 在服务器和 OS10 交换机上配置 <code>radsec</code> 共享密钥。<code>show running-configuration</code> 输出以加密格式显示未加密密钥和加密密钥。使用 <code>radius-server retransmit</code> 和 <code>radius-server timeout</code> 命令为 RADIUS over TLS 服务器上允许的超时和重新传输尝试配置全局设置。</p> <p>RADIUS over TLS 身份验证需要在证书认证机构上配置 X.509v3 PKI 证书并安装在交换机上。有关详细信息, 包括完整的 RADIUS over TLS 示例, 请参阅<a href="#">X.509v3 证书</a>。</p> <p>从版本 10.4.3.0 开始, 在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始, 在 SmartFabric 模式下也受支持。</p> <p>此命令的 <code>no</code> 版本将从 RADIUS over TLS 通信移除 RADIUS 服务器。</p>                                                                                                                                                                                                                                            |
| 示例     | <pre>OS10(config)# radius-server host 1.5.6.4 tls security-profile radius-admin key radsec</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 支持的版本  | 10.4.3.0 or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## radius-server retransmit

配置 RADIUS 服务器上允许的身份验证尝试次数。

|        |                                                                                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>radius-server retransmit retries</code>                                                                                                                                                  |
| 参数     | <code>retries</code> — 输入重试尝试次数，从 0 到 100。                                                                                                                                                     |
| 默认     | OS10 交换机重新传输 RADIUS 身份验证请求三次。                                                                                                                                                                  |
| 命令模式   | CONFIGURATION                                                                                                                                                                                  |
| 使用情况信息 | <p>使用此命令全局配置 RADIUS 服务器上的身份验证请求允许的重新传输尝试次数。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p> <p>此命令的 <code>no</code> 版本会将该值重置为默认值。</p> |
| 示例     | <pre>OS10(config)# radius-server retransmit 50</pre>                                                                                                                                           |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                               |

## radius-server timeout

配置用于重新发送 RADIUS 身份验证请求的超时。

|        |                                                                                                                                                                                     |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>radius-server timeout seconds</code>                                                                                                                                          |
| 参数     | <code>seconds</code> — 以秒为单位输入重新传输的时间，从 0 到 1000。                                                                                                                                   |
| 默认     | OS10 交换机在五秒钟后停止发送 RADIUS 身份验证请求。                                                                                                                                                    |
| 命令模式   | CONFIGURATION                                                                                                                                                                       |
| 使用情况信息 | <p>使用此命令可全局配置 RADIUS 服务器上使用的超时值。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p> <p>此命令的 <code>no</code> 版本会将该值重置为默认值。</p> |
| 示例     | <pre>OS10(config)# radius-server timeout 360</pre>                                                                                                                                  |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                    |

## radius-server vrf

为管理或非默认 VRF 实例配置 RADIUS 服务器。

|        |                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>radius-server vrf {management   vrf-name}</code>                                                                                                                                  |
| 参数     | <ul style="list-style-type: none"><li><code>management</code> — 输入关键字以配置管理 VRF 实例的 RADIUS 服务器。</li><li><code>vrf-name</code> — 输入关键字，然后输入 VRF 的名称，以配置该非默认 VRF 实例的 RADIUS 服务器。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                     |
| 命令模式   | CONFIGURATION                                                                                                                                                                           |
| 使用情况信息 | <p>使用此命令可将 RADIUS 服务器与 VRF 关联。如果未在 RADIUS 服务器列表中配置 VRF，则这些服务器将位于默认 VRF 上。RADIUS 的服务器列表和 VRF 具有一对一的映射。</p> <p>此命令的 <code>no</code> 版本将从管理 VRF 实例移除 RADIUS 服务器。</p>                       |
| 示例     | <pre>OS10(config)# radius-server vrf management OS10(config)# radius-server vrf blue</pre>                                                                                              |

支持的版本 10.4.0E(R1) or later

## service obscure-password

在 show 命令输出中隐匿密码。

|        |                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | service obscure-password                                                                                                                                   |
| 参数     | 无                                                                                                                                                          |
| 默认     | 未配置                                                                                                                                                        |
| 命令模式   | CONFIGURATION                                                                                                                                              |
| 使用情况信息 | 使用 service obscure-password 命令，以使密码的文本字符不会显示在 show 命令输出中。命令将隐匿为用户名、NTP、BGP、SNMP、RADIUS 服务器和 TACACS+ 服务器配置的密码。要禁用隐匿密码功能，请使用 no service obscure-password 命令。 |
| 示例     | <pre>OS10(config)# service obscure-password</pre>                                                                                                          |
| 支持的版本  | 10.5.0 or later                                                                                                                                            |

## service simple-password

禁用使用 username password role 和 password-attributes 命令配置的强密码检查。

|        |                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------|
| 语法     | service simple-password                                                                              |
| 参数     | 无                                                                                                    |
| 默认     | 未配置                                                                                                  |
| 命令模式   | CONFIGURATION                                                                                        |
| 使用情况信息 | 使用 service simple-password 命令关闭强密码检查，以便您可以配置不受限制的密码。要恢复到配置更强的密码设置，请使用 no service simple-password 命令。 |
| 示例     | <pre>OS10(config)# service simple-password</pre>                                                     |
| 支持的版本  | 10.5.0 or later                                                                                      |

## show boot protect

显示有权访问引导加载程序保护的已配置用户的当前列表。

|         |                                                                                                    |
|---------|----------------------------------------------------------------------------------------------------|
| 语法      | show boot protect                                                                                  |
| 参数      | 无                                                                                                  |
| 默认      | 未配置                                                                                                |
| 命令模式    | EXEC                                                                                               |
| 使用情况信息  | 显示引导加载程序保护的已授权用户的当前列表，但出于安全原因隐藏其密码。                                                                |
| 示例（已禁用） | <pre>OS10# show boot protect Boot protection disabled</pre>                                        |
| 示例（已启用） | <pre>OS10# show boot protect Boot protection enabled Authorized users: root linuxadmin admin</pre> |

支持的版本 10.4.3.0 或更高版本

show crypto ssh-key

显示 SSH 身份验证中使用的当前主机公钥。

|        |                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show crypto ssh-key {rsa   ecdsa   ed25519}                                                                                                  |
| 参数     | <ul style="list-style-type: none"><li>rsa — 显示 RSA 公钥。</li><li>ecdsa — 显示 ECDSA 公钥。</li><li>ed25519 — 显示 Ed25519 密钥。</li></ul>               |
| 默认     | 未配置                                                                                                                                          |
| 命令模式   | EXEC                                                                                                                                         |
| 使用情况信息 | <p>在使用自定义的位大小重新生成 SSH 服务器密钥后，禁用并重新启用 SSH 服务器以使用新的公钥。要验证更改，请使用 show crypto 命令。</p> <p>如果远程 SSH 客户端使用严格的主机密钥检查，请将新生成的主机密钥复制到客户端设备上的已知主机列表。</p> |

示例

```
OS10# show crypto ssh-key rsa
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACogJtArA0fHJkFpioGaAcp+vrDQFC3l3XFHtd
4lwXY9kM0Ar+37yRsDul8vKodqSDiGLRuPjFTcVjvDdSKWblJRsybkmA6nuHJIyPOScDepLlicM
IOxDhXEE92VRAMGuLI2AoeVYcH+IneWXhwQOkOFLtpxfnsiQY65CfS4aGoHOHWSfX3wI7boEDRD
uvZ8gzRxTuMl6Qr+RxBLJ7/OzkjNIN1/8Ok+8aJtCoJKbcYaduMjmhVNrNUW5TUXoCnp1XNRpkJ
zgS7Lt47yi86rqrTCAQW4eSYJIJs4+4ql9b4MF2D3499Ofn8uS82Mjtj0Nl01lbTbP3gsF4YYdB
WaFqp root@OS10
```

支持的版本 10.4.1.0 or later

show ip ssh

显示 SSH 服务器信息。

|        |                            |
|--------|----------------------------|
| 语法     | show ip ssh                |
| 参数     | 无                          |
| 默认     | 未配置                        |
| 命令模式   | EXEC                       |
| 使用情况信息 | 使用此命令可以查看有关已建立的 SSH 会话的信息。 |
| 示例     |                            |

```
OS10# show ip ssh

SSH Server: Enabled

SSH Server Ciphers: chacha20-poly1305@openssh.com,aes128-ctr,
aes192-ctr,aes256-ctr,
aes128-gcm@openssh.com,aes256-
gcm@openssh.com
SSH Server MACs: umac-64-etm@openssh.com,umac-128-
etm@openssh.com,
hmac-sha2-256-etm@openssh.com,
hmac-sha2-512-etm@openssh.com,
hmac-sha1-
etm@openssh.com,umac-64@openssh.com,
umac-128@openssh.com,hmac-sha2-256,
hmac-sha2-512,hmac-sha1
SSH Server KEX algorithms: curve25519-sha256@libssh.org,ecdh-sha2-
nistp256,
ecdh-sha2-nistp384,ecdh-sha2-nistp521,
diffie-hellman-group-exchange-sha256,
```



|                            |                             |
|----------------------------|-----------------------------|
|                            | diffie-hellman-group14-sha1 |
| Password Authentication:   | Enabled                     |
| Host-Based Authentication: | Disabled                    |
| RSA Authentication:        | Enabled                     |
| Challenge Response Auth:   | Disabled                    |

**支持的版本** 10.3.0E or later

## show mac address-table count

显示 MAC 地址表中的条目数。

|               |                                                                                                                                                                                                                                                                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>show mac address-table count [interface {ethernet <i>slot/port:subport</i>   port-channel <i>number</i>   vlan <i>vlan-id</i>}]</code>                                                                                                                                                                                                                             |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>interface</code> — 显示接口类型： <ul style="list-style-type: none"> <li><code>ethernet <i>node/slot/port[:subport]</i></code> — 显示地址表中的以太网接口配置。</li> <li><code>port-channel <i>channel-number</i></code> — 显示地址表 1 到 128 中的端口通道接口配置。</li> </ul> </li> <li><code>vlan <i>vlan-id</i></code> — 显示特定 VLAN (1 到 4093) 的信息。</li> </ul> |
| <b>默认</b>     | 无                                                                                                                                                                                                                                                                                                                                                                        |
| <b>命令模式</b>   | EXEC                                                                                                                                                                                                                                                                                                                                                                     |
| <b>使用情况信息</b> | 无                                                                                                                                                                                                                                                                                                                                                                        |
| <b>示例</b>     |                                                                                                                                                                                                                                                                                                                                                                          |

```
OS10# show mac address-table count
MAC Entries for all vlans :
Dynamic Address Count : 5
Static Address (User-defined) Count : 0
Total MAC Addresses in Use: 5
OS10#
```

**支持的版本** 10.1.0E 或更高版本

## show logging audit

显示审核日志条目。

|               |                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>show logging audit [reverse] [number]</code>                                                                                                              |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>reverse</code> — 显示从最近事件开始的条目。</li> <li><code>number</code> — 显示指定数量的审核日志条目用户，从 1 到 65535。</li> </ul>              |
| <b>默认</b>     | 从最早的事件开始显示 24 个条目。                                                                                                                                              |
| <b>命令模式</b>   | EXEC                                                                                                                                                            |
| <b>使用情况信息</b> | 只有 <code>sysadmin</code> 和 <code>secadmin</code> 角色可以显示审核日志。输入 <code>reverse</code> 以显示从最近事件开始的条目。您可以更改显示的条目数。审核日志记录发生时，不会显示在控制台上。它们保存在审核日志中，并转发到任何已配置的系统日志服务器。 |

**示例**

```
OS10# show logging audit 4
<14>1 2019-02-14T13:15:06.283337+00:00 OS10 audispd - - - Node.1-Unit.1:PRI [audit],
Dell EMC (OS10) node=OS10 type=USER_END msg=audit(1550150106.277:597): pid=7908 uid=0
auid=4294967295 ses=4294967295 msg='Op=PAM:session_close acct="admin" exe="/bin/su"
hostname=? addr=? terminal=??? res=success'
<110>1 2019-02-14T13:15:16.331515+00:00 OS10 .clish 7412 - - Node.1-Unit.1:PRI [audit],
User admin on console used cmd: 'crypto security-profile mltestprofile' - success
<110>1 2019-02-14T13:15:21.794529+00:00 OS10 .clish 7412 - - Node.1-Unit.1:PRI [audit],
User admin on console used cmd: 'exit' - success
<110>1 2019-02-14T13:16:05.882555+00:00 OS10 .clish 7412 - - Node.1-Unit.1:PRI [audit],
User admin on console used cmd: 'exit' - success
```



```
OS10# show logging audit reverse 4
<110>1 2019-02-14T13:16:05.882555+00:00 OS10 .clish 7412 - - Node.1-Unit.1:PRI [audit],
User admin on console used cmd: 'exit' - success
<110>1 2019-02-14T13:15:21.794529+00:00 OS10 .clish 7412 - - Node.1-Unit.1:PRI [audit],
User admin on console used cmd: 'exit' - success
<110>1 2019-02-14T13:15:16.331515+00:00 OS10 .clish 7412 - - Node.1-Unit.1:PRI [audit],
User admin on console used cmd: 'crypto security-profile mltestprofile' - success
<14>1 2019-02-14T13:15:06.283337+00:00 OS10 audispd - - - Node.1-Unit.1:PRI [audit],
Dell EMC (OS10) node=OS10 type=USER_END msg=audit(1550150106.277:597): pid=7908 uid=0
aid=4294967295 ses=4294967295 msg='Op=PAM:session_close acct="admin" exe="/bin/su"
hostname=? addr=? terminal=??? res=success'OS10# show logging audit reverse 10
```

## 支持的版本

10.4.3.0 or later

# show login-statistics

显示用户登录系统的统计信息。

**语法** `show login-statistics {user user-id | all}`

- 参数**
- `user user-id` — 输入 OS10 用户名。
  - `all` — 显示所有系统用户的登录统计信息。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 只有 `sysadmin` 和 `secadmin` 角色可以访问此命令。`show` 输出将显示系统用户的登录信息，包括成功 and 失败登录的次数、角色更改以及用户上次登录的时间。

## 示例

```
OS10# show login-statistics all
Display statistics upon user login: Enabled
Time-frame in days: 25
```

| User     | Role Change | #Fail since last Login | During last Timeframe | #Success | Last Login Date/Time | Location             |
|----------|-------------|------------------------|-----------------------|----------|----------------------|----------------------|
| admin    | False       | 0                      | 1                     | 13       | 2017-11-02T16:02:44Z | in                   |
| netadmin | False       | 0                      | 0                     | 5        | 2017-11-02T15:59:04Z | (00:00)              |
| mltest   | False       | 0                      | 0                     | 1        | 2017-11-01T15:42:07Z | 1001:10:16:210::4001 |

```
OS10# show login-statistics user mltest
User : mltest
Role changed since last login : False
Failures since last login : 0
Time-frame in days : 25
Failures in time period : 0
Successes in time period : 1
Last Login Time : 2017-11-01T15:42:07Z
Last Login Location : 1001:10:16:210::4001
```

## 支持的版本

10.4.0E(R1) or later

# show privilege

显示当前的权限级别。

**语法** `show privilege`

|       |                                                                |
|-------|----------------------------------------------------------------|
| 参数    | 无                                                              |
| 默认    | 未配置                                                            |
| 命令模式  | EXEC                                                           |
| 示例    | <pre>OS10# show privilege Current privilege level is 15.</pre> |
| 支持的版本 | 10.4.3.0 or later                                              |

## show running-configuration privilege

显示所有用户的已配置权限级别。

|       |                                                                                                                                                                                                                                 |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法    | show running-configuration privilege                                                                                                                                                                                            |
| 参数    | 无                                                                                                                                                                                                                               |
| 默认    | 未配置                                                                                                                                                                                                                             |
| 命令模式  | EXEC                                                                                                                                                                                                                            |
| 示例    | <pre>OS10# show running-configuration privilege privilege exec priv-lvl 3 configure privilege configure priv-lvl 4 "interface ethernet" enable password sha-512 \$6\$Yij02Phe2n6whp7b\$ladskj0HowijIlkajg981 priv- lvl 12</pre> |
| 支持的版本 | 10.4.3.0 or later                                                                                                                                                                                                               |

## show users

显示登录到 OS10 的所有用户的信息。

| 语法        | show users                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |          |             |      |                       |                     |            |          |           |  |  |  |  |  |  |  |   |       |       |          |      |      |                       |                     |   |       |       |          |      |      |                       |                     |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----------|-------------|------|-----------------------|---------------------|------------|----------|-----------|--|--|--|--|--|--|--|---|-------|-------|----------|------|------|-----------------------|---------------------|---|-------|-------|----------|------|------|-----------------------|---------------------|
| 参数        | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |          |             |      |                       |                     |            |          |           |  |  |  |  |  |  |  |   |       |       |          |      |      |                       |                     |   |       |       |          |      |      |                       |                     |
| 默认        | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |          |             |      |                       |                     |            |          |           |  |  |  |  |  |  |  |   |       |       |          |      |      |                       |                     |   |       |       |          |      |      |                       |                     |
| 命令模式      | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |       |          |             |      |                       |                     |            |          |           |  |  |  |  |  |  |  |   |       |       |          |      |      |                       |                     |   |       |       |          |      |      |                       |                     |
| 使用情况信息    | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |          |             |      |                       |                     |            |          |           |  |  |  |  |  |  |  |   |       |       |          |      |      |                       |                     |   |       |       |          |      |      |                       |                     |
| 示例        | <pre>OS10# show users</pre> <table><thead><tr><th>Index</th><th>Line</th><th>User</th><th>Role</th><th>Application</th><th>Idle</th><th>Login-Time</th><th>Location</th></tr><tr><th>Privilege</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></tr></thead><tbody><tr><td>1</td><td>pts/0</td><td>admin</td><td>sysadmin</td><td>bash</td><td>&gt;24h</td><td>2018-09-08 T06:51:37Z</td><td>10.14.1.91 [ssh] 15</td></tr><tr><td>2</td><td>pts/1</td><td>netad</td><td>netadmin</td><td>bash</td><td>&gt;24h</td><td>2018-09-08 T06:54:33Z</td><td>10.14.1.91 [ssh] 10</td></tr></tbody></table> | Index | Line     | User        | Role | Application           | Idle                | Login-Time | Location | Privilege |  |  |  |  |  |  |  | 1 | pts/0 | admin | sysadmin | bash | >24h | 2018-09-08 T06:51:37Z | 10.14.1.91 [ssh] 15 | 2 | pts/1 | netad | netadmin | bash | >24h | 2018-09-08 T06:54:33Z | 10.14.1.91 [ssh] 10 |
| Index     | Line                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | User  | Role     | Application | Idle | Login-Time            | Location            |            |          |           |  |  |  |  |  |  |  |   |       |       |          |      |      |                       |                     |   |       |       |          |      |      |                       |                     |
| Privilege |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |          |             |      |                       |                     |            |          |           |  |  |  |  |  |  |  |   |       |       |          |      |      |                       |                     |   |       |       |          |      |      |                       |                     |
| 1         | pts/0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | admin | sysadmin | bash        | >24h | 2018-09-08 T06:51:37Z | 10.14.1.91 [ssh] 15 |            |          |           |  |  |  |  |  |  |  |   |       |       |          |      |      |                       |                     |   |       |       |          |      |      |                       |                     |
| 2         | pts/1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | netad | netadmin | bash        | >24h | 2018-09-08 T06:54:33Z | 10.14.1.91 [ssh] 10 |            |          |           |  |  |  |  |  |  |  |   |       |       |          |      |      |                       |                     |   |       |       |          |      |      |                       |                     |
| 支持的版本     | 10.2.0E or later 更新了命令以显示 OS10 版本 10.4.3.0 or later 上所有用户的权限级别。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |          |             |      |                       |                     |            |          |           |  |  |  |  |  |  |  |   |       |       |          |      |      |                       |                     |   |       |       |          |      |      |                       |                     |

## system-user linuxadmin disable

禁用 linuxadmin 用户。

|    |                                     |
|----|-------------------------------------|
| 语法 | [no] system-user linuxadmin disable |
| 参数 | 无                                   |
| 默认 | 已启用                                 |

|        |                                                                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 命令模式   | CONFIGURATION                                                                                                                                                               |
| 使用情况信息 | 使用此命令可禁用和锁定 <code>linuxadmin</code> 用户。无命令版本可启用和解锁 <code>linuxadmin</code> 用户。<br>从版本 10.4.3.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。 |
| 示例     | <pre>OS10(config)# system-user linuxadmin disable OS10(config)# no system-user linuxadmin disable</pre>                                                                     |
| 支持的版本  | 10.4.3.0 或更高版本                                                                                                                                                              |

## system-user linuxadmin password

配置 `linuxadmin` 用户的密码。

|        |                                                                                                                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>system-user linuxadmin password {clear-text-password   hashed-password}</code>                                                                                                                                        |
| 参数     | 无                                                                                                                                                                                                                           |
| 默认     | 未配置                                                                                                                                                                                                                         |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                               |
| 使用情况信息 | 使用此命令可设置 <code>linuxadmin</code> 用户的清除文本或哈希密码。<br>从版本 10.4.3.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。                                                                                 |
| 示例     | <pre>OS10(config)# system-user linuxadmin password Dell@Force10!@ OS10(config)# system-user linuxadmin password \$6\$3M55wOYy\$Sw1V9Ok3GE4Hmf6h1ARH.dBHy9gpEFYUvdu15ZpnCYzt.nJjFm0Viz/ rQvvJeX6krRtfYs2ZqBl6TkmLGAwtM</pre> |
| 支持的版本  | 10.4.3.0 或更高版本                                                                                                                                                                                                              |

## tacacs-server host

配置 TACACS+ 服务器和用于对服务器上的交换机进行身份验证的密钥。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>tacacs-server host {hostname   ip-address} key {0 authentication-key   9 authentication-key   authentication-key} [auth-port port-number]</code>                                                                                                                                                                                                                                                                                                                                                                         |
| 参数     | <ul style="list-style-type: none"> <li><code>hostname</code> — 输入 TACACS+ 服务器的主机名称。</li> <li><code>ip-address</code> — 输入 TACACS+ 服务器的 IPv4 (A.B.C.D) 或 IPv6 (x:x:x:x:x) 地址。</li> <li><code>key 0 authentication-key</code> — 以纯文本格式输入身份验证密钥。最多 42 个字符。</li> <li><code>key 9 authentication-key</code> — 以加密格式输入最大包含 128 个字符的身份验证密钥。</li> <li><code>authentication-key</code> — 以纯文本格式输入最多包含 42 个字符的身份验证。不需要在密钥之前输入 0。</li> <li><code>key authentication-key</code> — 输入用于在 TACACS+ 服务器上验证交换机的加密密钥的文本字符串。最多 42 个字符。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 使用情况信息 | <p>身份验证密钥必须与 TACACS+ 服务器上配置的密钥相匹配。您不能在密钥中输入空格。<code>show running-configuration</code> 输出以加密格式显示未加密密钥和加密密钥。使用 <code>tacacs-server timeout</code> 命令配置 TACACS+ 服务器上允许的身份验证请求的全局超时。默认情况下，OS10 在 TACACS+ 服务器上的身份验证尝试在五秒钟后失败。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p>                                                                                                                                                                                              |

此命令的 `no` 版本将移除 TACACS+ 服务器配置。

#### 示例

```
OS10(config)# tacacs-server host 1.5.6.4 key secret1
```

#### 支持的版本

10.4.0E(R2) or later

## tacacs-server timeout

配置用于 TACACS+ 服务器上身份验证尝试的全局超时。

#### 语法

```
tacacs-server timeout seconds
```

#### 参数

*seconds* — 输入用于等待来自 TACACS+ 服务器的身份验证响应的超时期间，从 1 到 1000 秒。

#### 默认

5 秒

#### 命令模式

CONFIGURATION

#### 使用情况信息

从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 `no` 版本会将 TACACS+ 服务器超时重置为默认值。

#### 示例

```
OS10(config)# tacacs-server timeout 360
```

#### 支持的版本

10.4.0E(R2) or later

## tacacs-server vrf

在 TACACS 服务器组与 VRF 和源接口之间创建关联。

#### 语法

```
tacacs-server vrf {management | vrf-name}
```

#### 参数

- `management` — 输入关键字以将 TACACS 服务器关联到管理 VRF 实例。此选项仅将 TACACS 服务器关联限制为管理 VRF。
- `vrf-name` — 输入关键字，然后是 VRF 的名称，以便将 TACACS 服务器与该 VRF 关联。

#### 默认

无。

#### 命令模式

CONFIGURATION

#### 使用情况信息

使用此命令可将 TACACS 服务器与 VRF 实例关联。如果未在 TACACS 服务器列表中配置 VRF，则这些服务器将位于默认 VRF 实例上。TACACS 的服务器列表和 VRF 具有一对一的映射。删除 VRF 实例时，也会自动删除 TACACS 服务器列表。

此命令的 `no` 版本会将该值重置为默认值。

#### 示例

```
[no] tacacs-server management
[no] tacacs-server vrf red
```

#### 支持的版本

10.4.3.0E 或更高版本

## username password role

根据用户名和密码创建身份验证条目，并将角色分配给用户。

#### 语法

```
username username password password role role [priv-lvl privilege-level]
```

#### 参数

- `username username` — 输入文本字符串。最多 32 个字母数字字符；至少一个字符。
- `password password` — 输入文本字符串。最多 32 个字母数字字符；最少 9 个字符。密码前缀 \$1\$、\$5\$ 和 \$6\$ 不支持明文密码。
- `role role` — 输入用户角色：

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <ul style="list-style-type: none"> <li>◦ <code>sysadmin</code> — 对系统中所有命令的完全访问权限、对操作文件系统的命令的独占访问权限，以及对系统 shell 的访问权限。系统管理员可以创建用户 ID 和用户角色。</li> <li>◦ <code>secadmin</code> — 对设置安全策略和系统访问权限的配置命令的完全访问权限，如密码强度、AAA 授权和加密密钥。安全管理员可以显示安全信息，如加密密钥、登录统计信息和日志信息。</li> <li>◦ <code>netadmin</code> — 对管理流经交换机（如路由、接口和 ACL）的流量的配置命令的完全访问权限。网络管理员无法访问安全功能的配置命令或查看安全信息。</li> <li>◦ <code>netoperator</code> — 访问 EXEC 模式以查看当前配置。网络操作员无法修改交换机上的任何配置设置。</li> <li>• <code>priv-lvl privilege-level</code> — 输入权限级别，从 0 到 15。如果未指定 <code>priv-lvl</code> 选项，系统将为 <code>netoperator</code> 角色分配权限级别 1，为 <code>sysadmin</code>、<code>secadmin</code> 和 <code>netadmin</code> 角色分配权限级别 15。</li> </ul> |
| 默认     | <ul style="list-style-type: none"> <li>• 用户名和密码条目以明文形式输入。</li> <li>• 没有默认用户角色。</li> <li>• 对于 <code>netoperator</code>，默认的权限级别为 1，对于 <code>sysadmin</code>、<code>secadmin</code> 和 <code>netadmin</code> 为级别 15。</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | <p>默认情况下，密码必须至少包含 9 个字母数字字符。仅支持以下特殊字符：</p> <pre>! # % &amp; ' ( ) ; &lt; = &gt; [ ] * + - . / : ^ _</pre> <p>以明文形式输入密码。它会转换为正在运行的配置中的 SHA-512 格式。为了向后兼容 OS10 版本 10.3.1E 及更低版本，支持以 MD-5、SHA-256 和 SHA-512 格式输入密码。</p> <p>对于 <code>sysadmin</code>、<code>secadmin</code> 和 <code>netadmin</code> 角色，您不能将高于权限级别 1 的权限级别分配给具有 <code>netoperator</code> 角色且权限级别高于 2 的用户。</p> <p>要增加所需的密码强度，请使用 <code>password-attributes</code> 命令。此命令的 <code>no</code> 版本将删除用户身份验证。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p>                                                                                                              |
| 示例     | <pre>OS10(config)# username user05 password newpwd404 role sysadmin priv-lvl 10</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## username sshkey

使用远程客户端的公钥启用 SSH 免密码登录。远程客户端不会提示输入密码。

|        |                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>username username sshkey sshkey-string</code>                                                                                                                                                                                                                                                                                                                |
| 参数     | <ul style="list-style-type: none"> <li>• <code>username</code> — 输入远程客户端的用户名。此值是使用 <code>username password role</code> 命令配置的用户名。</li> <li>• <code>sshkey-string</code> — 输入远程客户端设备登录到 OS10 交换机要使用的公钥的文本字符串。如果 <code>sshkey-string</code> 包含空格，请用双引号 (") 将字符串括起来。</li> </ul>                                                                                        |
| 默认     | 默认 SSH 服务器密钥是使用 2048 位生成的 RSA 密钥，包含 256 位的 ECDSA 密钥，以及 256 位的 Ed25519 密钥。                                                                                                                                                                                                                                                                                          |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                      |
| 使用情况信息 | <p>要为 SSH 密码配置多个用户名，请使用 <code>username sshkey filename</code> 命令。<code>no username username sshkey</code> 命令将移除指定用户名的 SSH 免密码配置。</p> <p>在 <code>~/.ssh/id_rsa.pub</code> 文件中找到远程客户端上的公钥。使用公钥作为 <code>sshkey-string</code> 或 <code>publickey-string</code> 参数。</p> <p>从版本 10.4.1.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p> |

## 示例

```
OS10(config)# username test sshkey "ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQBqJaD
wgBgQXlPPPPSEyx+F5DVG2RpBH4Zm1YQApE5YJsKlt6RpeOIT1wnJP/o54p1nCemU38i7/zCLWuW
t3XDVVMoSb9Za89hebQ+f6XyNs4aMpyUk5RmuZTXqwnbUUuP3nPw/Y4lKkZJafWx125Ma7Ibw
fUM5wGdBu76j8mvwsWvNxrnkOsweo7Anp67p8Lsg+KBUsx3q8Fpc986qQfdrceFO01WraJR8wzY
lmbQw/C+Hm5Ap6Nr6DoXMWqKdKUr7jfte8ThARYZD8dvZeyzhk3nykYRQ39mqjXnOyEOiDl1e21
QUvI1cjcQPDXgFJUrkcclyPiGUOH5"

OS10(config)# do show running-configuration users
username admin password 6q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD
7/VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIGNs5BKH. role sysadmin

username user10 password 6rounds=656000$G10VRFTJB291ekwo$ITGf0zd4bTUCBBpI
Vsbr6oStnUZMydN5lDs4WE6G3XHETWbcKrGTeAolwEF0cenEgRRPzi3SMmYyzAHCCC8ws0 role
sysadmin

username test sshkey "ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQBqJaDwgBgQXlPPPPSEyx
+F5DVG2RpBH4Zm1YQApE5YJsKlt6RpeOIT1wnJP/o54p1nCemU38i7/zCLWuWt3XDVVMoSb9Za
89hebQ+f6XyNs4aMpyUk5RmuZTXqwnbUUuP3nPw/Y4lKkZJafWx125Ma7IbwfUM5wGdBu76j8m
vwsWvNxrnkOsweo7Anp67p8Lsg+KBUsx3q8Fpc986qQfdrceFO01WraJR8wzYlmbQw/C+Hm5Ap6
Nr6DoXMWqKdKUr7jfte8ThARYZD8dvZeyzhk3nykYRQ39mqjXnOyEOiDl1e21QUvI1cjcQPDXgF
JUrkcclyPiGUOH5"
```

支持的版本 10.4.1.0 or later

## username sshkey filename

为使用多个公钥的远程客户端启用不使用 SSH 密码登录。远程客户端不会提示输入密码。

|        |                                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>username username sshkey filename filepath</code>                                                                                                                                                                   |
| 参数     | <ul style="list-style-type: none"><li><code>username</code> — 输入登录远程客户端的 OS10 用户名。此值是使用 <code>username password role</code> 命令配置的用户名。</li><li><code>filepath</code> — 输入本地文件的绝对路径名称，该名称包含远程设备用于登录到 OS10 交换机的公钥。</li></ul> |
| 默认     | 默认 SSH 服务器密钥是使用 2048 位生成的 RSA 密钥，包含 256 位的 ECDSA 密钥，以及 256 位的 Ed25519 密钥。                                                                                                                                                 |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                             |
| 使用情况信息 |                                                                                                                                                                                                                           |

在使用命令之前，请在 `~/.ssh/id_rsa.pub` 文件中找到远程客户端上的公钥。创建文本文件并将远程客户端上的 SSH 公钥复制到文件中。在单独的行中输入每个公钥。将文件下载到您的主 OS10 目录。

 **注：**当 SSH 密钥文件不存在时输入命令不起作用，并导致静默故障。未启用不使用 SSH 密码登录。

从版本 10.4.1.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

命令的 `no` 版本会针对指定用户名移除不使用 SSH 密码的配置。

## 示例

```
OS10(config)# username user10 sshkey filename /test_file.txt

OS10(config)# do show running-configuration users
username admin password
6q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/30Jc6m5wjF8nnLD
7/VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIGNs5BKH. role sysadmin

username user10 password
6rounds=656000$G10VRFTJB291ekwo$ITGf0zd4bTUCBBpI
Vsbr6oStnUZMydN5lDs4WE6G3XHETWbcKrGTeAolwEF0cenEgRRPzi3SMmYyzAHCCC8ws0
role
sysadmin

username user10 sshkey filename /test_file.txt
```

支持的版本 10.4.1.0 or later

## userrole inherit

重新配置 OS10 默认分配给具有未知用户角色或权限级别的 RADIUS 或 TACACS+ 认证用户的默认 `netoperator` 角色和权限。您还可以配置未知的 RADIUS 或 TACACS+ 用户角色，以继承现有 OS10 角色的权限。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>userrole {default   name} inherit existing-role-name</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 参数     | <ul style="list-style-type: none"><li><code>default inherit</code> — 重新配置分配给已认证用户（具有丢失或未知角色或权限级别）的默认权限。</li><li><code>name inherit</code> — 输入从 OS10 用户角色继承权限的 RADIUS 或 TACACS+ 用户角色的名称；最多 32 个字符。</li><li><code>existing-role-name</code> — 分配与 OS10 用户角色关联的权限：<ul style="list-style-type: none"><li><code>sysadmin</code> — 对系统中所有命令的完全访问权限、对操作文件系统的命令的独占访问权限，以及对系统 shell 的访问权限。系统管理员可以创建用户 ID 和用户角色。</li><li><code>secadmin</code> — 对设置安全策略和系统访问权限的配置命令的完全访问权限，如密码强度、AAA 授权和加密密钥。安全管理员可以显示安全信息，如加密密钥、登录统计信息和日志信息。</li><li><code>netadmin</code> — 对管理流经交换机（如路由、接口和 ACL）的流量的配置命令的完全访问权限。网络管理员无法访问安全功能的配置命令或查看安全信息。</li><li><code>netoperator</code> — 仅访问 EXEC 模式以查看当前配置。网络操作员无法修改交换机上的任何配置设置。</li></ul></li></ul> |
| 默认     | OS10 将 <code>netoperator</code> 角色分配给由 RADIUS 或 TACACS+ 服务器（具有丢失或未知角色或权限级别）认证的用户。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | <p>当 RADIUS 或 TACACS+ 服务器对用户进行认证，并且未返回角色或权限级别，或者返回未知角色或权限级别时，OS10 默认将 <code>netoperator</code> 角色分配给用户。使用此命令可重新配置默认的 <code>netoperator</code> 权限。</p> <p>要将 OS10 用户角色权限分配给未知用户角色，请输入 RADIUS 或 TACACS+ <code>name</code> 及 <code>inherit existing-role-name</code> 值。无命令版本将角色重置为 <code>netoperator</code>。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p>                                                                                                                                                                                                                                                                                                    |
| 示例     | <pre>OS10(config)# userrole default inherit sysadmin</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 支持的版本  | 10.4.0E(R3P3) 或更高版本                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## X.509v3 证书

OS10 支持 X.509v3 证书，以保护交换机与主机（如 RADIUS 服务器）之间的通信安全。交换机和服务器均交换由证书颁发机构 (CA) 颁发的已签名的 X.509v3 证书中的公钥，以便彼此进行身份验证。证书颁发机构使用其私钥来签署交换机和主机证书。

证书中的信息允许两个设备证明所有权和公钥的有效性。假设 CA 受信任，则交换机和身份验证服务器会验证对方的身份并设置安全的加密通信通道。

虽然可以同时使用两种方式，但通常优先使用具有公钥证书的用户身份验证，而不是基于密码的身份验证：

- 避免使用低强度密码的安全风险，并对强力攻击提供更大的阻力。
- 提供受信任并且可证实的标识（使用受信任的 CA 数字签名的证书时）的保证。
- 除了用户身份验证以外，在交换机服务器通信中提供安全保护和机密性。

例如，您可以下载并安装 X.509v3 证书以启用 [RADIUS over TLS 身份验证](#) 的公钥验证（也称为 RadSec）。OS10 支持公钥基础设施 (PKI)，其中包括：

- 生成自签名证书和证书签名请求 (CSR) 及其相应的私钥
- 安装和删除自签名证书和 CA 签名的证书
- 安全删除相应的私钥
- 在系统“trust store”中安装和删除 CA 证书
- 显示证书信息



## X.509v3 概念

|                     |                                                                                                                                                                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>认证</b>           | 将网络设备与公钥关联的文档。在参与的设备之间交换时，将使用证书来验证设备身份以及和设备关联的公钥。PKI 使用以下证书类型： <ul style="list-style-type: none"><li>CA 证书：用于对主机证书进行签名的 CA 证书。CA 证书可由其他 CA 颁发或由其自行签署。自签名 CA 证书称为 <i>根证书</i>。</li><li>主机证书：颁发给网络设备的证书。主机证书可由 CA 或自签名签名。</li><li>自签名证书：与 CA 签名的证书相比的主机签名证书。</li></ul> |
| <b>证书颁发机构 (CA)</b>  | 验证证书内容并对其进行签名的实体，表示证书受信任且正确。中间 CA 在根 CA 和主机之间签署证书。                                                                                                                                                                                                                  |
| <b>证书吊销列表 (CRL)</b> | 包含不再有效的证书的 CA 签名文档，即使尚未过期也是如此。例如，为服务器生成新的证书时，将不再支持旧证书。                                                                                                                                                                                                              |
| <b>证书签发请求 (CSR)</b> | 生成密钥对后，交换机将使用密码私钥来签署获取证书的请求，并将请求发送到证书颁发机构。CSR 包含标识交换机及其公钥的信息。此公钥用于验证 CSR 的私有签名和交换机的可分辨名称 (DN)。CSR 由 CA 签名并返回到主机以用作签名的主机证书。                                                                                                                                          |
| <b>隐私增强邮件 (PEM)</b> | 用于将 X.509v3 数据格式化为安全信息交换的 PKI 标准；如 RFC 1421 中所述。                                                                                                                                                                                                                    |
| <b>公钥基础设施 (PKI)</b> | 管理私有和公有加密密钥生成的应用程序，以及在网络设备上下载、安装和交换 CA 签名的证书。                                                                                                                                                                                                                       |
| <b>X.509v3</b>      | 管理数字证书和公钥加密的公钥基础设施的标准。                                                                                                                                                                                                                                              |

## 公钥基础设施

要在网络中的 OS10 交换机上使用 509v3 证书进行安全通信和用户身份验证，需要具有证书颁发机构 (CA) 的公钥基础设施 (PKI)。CA 签署证书可证明网络设备的可信度。

当组织想要确保客户与网络的连接安全时，它可能会向证书颁发机构（如 VeriSign 或 DigiCert）付款，以便为其域签署证书。但是，要实施 509v3 基础架构，您可以充当您自己的 CA。充当您自己的 CA 时，您可以设置 CA 将证书颁发给同一个受信任域中的主机，以便彼此进行身份验证。

### 509v3 公钥基础设施

要使用 509v3 证书设置 PKI，Dell EMC Networking 建议：

1. 配置用于生成私钥和自签名 CA 证书的根 CA。
2. 配置一个或多个生成私钥和证书签名请求 (CSR) 的中间 CA，并将 CSR 发送到根 CA。
  - 根 CA 使用其私钥来签署中间 CA 的 CSR 并为中间 CA 生成 CA 证书。
  - 中间 CA 将下载并安装 CA 证书。随后，中间 CA 可以为网络中的主机以及 PKI 层次结构中较低的其他中间 CA 签署证书。
  - 根和中间 CA 证书（而不是相应的私钥）将在网络上公开，以用于要下载的网络主机。
  - 只要可能，请将私钥存储为离线或在通用访问受限的位置。
3. 使用 `crypto cert generate request` 命令生成私钥并在 OS10 交换机上创建 CSR。交换机将 CSR 上传到中间 CA。要将私钥存储在本地隐藏位置，Dell EMC Networking 建议将 `key-file private` 参数与命令配合使用。
4. 使用 `crypto ca-cert install` 命令在主机上下载并安装 CA 证书。安装 CA 证书后，主机会信任由 CA 签署并由其他网络设备提供的所有证书。您必须先下载证书到主目录，然后使用 `crypto ca-cert install` 命令安装证书。
5. 从 OS10 交换机上的中间 CA 下载并安装已签名的主机证书和私钥。然后使用 `crypto cert install` 命令进行安装。安装主机证书后，OS10 应用程序将使用证书来保护与网络设备之间的通信。私钥安装在交换机上的内部文件系统中，无法导出或查看。

## 管理 CA 证书

OS10 支持从外部证书颁发机构下载和安装公共 X.509v3 证书。

在数据中心环境中，受信任的 CA 服务器可以创建 CA 证书。主机作为受信任的 CA 服务器运行。网络主机安装使用 CA 私钥进行数字签名的证书，以便在网络中的参与设备之间建立信任。OS10 交换机上的证书用于验证由客户端和服务端（如 Syslog 和 RADIUS 服务器）提供的证书，以与这些设备建立安全连接。

要导入 CA 服务器证书，请执行以下操作：



1. 使用安全方法通过 `copy` 命令下载由 CA 服务器创建的 X.509v3 证书，如 HTTPS、SCP 或 SFTP。将 CA 证书复制到交换机上的本地目录，例如 `home://` 或 `usb://`。
2. 使用 `crypto ca-cert install` 命令安装证书。安装 CA 证书时，请指定存储证书的本地路径。

交换机将验证证书，并将其安装在 PEM 格式的受信任证书的现有目录中。

### 安装 CA 证书

- 在 EXEC 模式下安装 CA 证书。

```
crypto ca-cert install ca-cert-filepath [filename]
```

- `ca-cert-filepath` 指定下载的证书的本地路径；例如，`home://CAcert.pem` 或 `usb://CA-cert.pem`。
- `filename` 指定将证书存储在 OS10 信任存储目录下的可选文件名。以 `filename.crt` 格式输入文件名。

### 示例：下载并安装 CA 证书

```
OS10# copy scp:///tftpuser@10.11.178.103:/tftpboot/certs/Dell_rootCA1.pem home://
Dell_rootCA1.pem
password:

OS10# crypto ca-cert install home://Dell_rootCA1.pem
Processing certificate ...
Installed Root CA certificate
 CommonName = Dell_rootCA1
 IssuerName = Dell_rootCA1
```

### 显示 CA 服务器证书

```
OS10# show crypto ca-certs

Locally installed certificates
Dell_rootCA1.crt
```

```
OS10# show crypto ca-certs Dell_rootCA1.crt
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number:
 95:48:23:17:76:9d:05:e1
 Signature Algorithm: sha256WithRSAEncryption
 Issuer: C = US, ST = California, L = Santa Clara, O = Dell EMC, OU = Networking,
CN = Dell_rootCA1
 Validity
 Not Before: Jul 25 18:21:50 2018 GMT
 Not After : Jul 20 18:21:50 2038 GMT
 Subject: C = US, ST = California, L = Santa Clara, O = Dell EMC, OU =
Networking, CN = Dell_rootCA1
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (4096 bit)
 Modulus:
 00:cd:9d:ca:10:6b:b1:54:81:10:92:42:9f:6a:cb:
 49:51:9d:46:10:cb:67:08:2b:75:2a:62:40:80:a3:
 f5:7d:58:67:f4:cc:c6:70:32:14:4c:f0:4d:cd:7e:
 0d:5c:63:28:5e:6c:ad:9e:13:13:71:6d:9d:10:a9:
 a1:d8:6b:bd:a3:a0:5a:11:19:87:4d:3d:08:6f:10:
 03:df:70:89:5f:b7:56:49:32:57:9c:28:5e:43:7f:
 ca:bc:41:c7:31:51:97:7f:73:b7:b0:c4:13:21:e6:
 2c:4c:19:fd:35:0b:26:16:78:fc:c3:73:21:3a:06:
 f6:ec:87:3f:9f:5e:3a:0c:23:5e:13:4c:9e:5a:70:
 18:d4:ad:cb:cf:47:c1:c6:50:a0:49:df:a0:a6:47:
 1e:13:19:49:9e:67:db:1c:c7:23:9e:37:3b:c7:0c:
 cd:26:46:f6:c1:e1:93:64:29:81:9c:e9:a8:1d:29:
 19:4c:8d:a4:a8:53:66:2b:b2:70:ff:ec:80:d4:87:
 eb:74:e2:11:56:ed:4b:68:fc:53:2e:d4:94:f6:f5:
 e4:77:d9:b6:e8:4a:91:b7:da:46:18:51:bf:e4:b6:
 3e:6a:47:ab:77:f6:93:b7:d0:9a:c8:fa:ba:ae:ed:
 6a:fd:81:54:c8:76:13:1b:57:74:d6:02:78:d7:98:
 38:e6:c5:9b:64:03:b2:76:93:fd:8c:9f:54:c9:a3:
```

```

04:a9:0c:b7:e2:bb:02:50:3f:e0:08:33:32:89:55:
95:9b:30:6c:73:7d:be:63:f1:6c:da:4d:92:41:d0:
f5:d6:bf:e3:c0:da:98:ae:24:37:ed:07:63:86:a1:
cc:da:3b:45:d4:a9:80:e2:d6:ab:c1:ae:2a:99:32:
9d:ba:fe:88:38:f2:02:d1:b3:78:43:17:7e:6e:b1:
a2:17:85:bd:5f:4a:52:90:96:4d:bc:19:85:ed:9d:
49:77:bd:59:44:6c:6c:23:e5:b1:92:af:a0:10:ce:
68:d4:f4:07:9e:ec:ca:c5:95:a2:f4:19:bb:f7:12:
ce:f0:a6:39:df:1a:5b:10:91:d5:77:46:8d:55:9a:
8e:96:e0:70:f6:27:89:43:3d:74:99:b4:7f:4b:38:
71:18:01:64:bb:72:2c:26:6f:6e:e8:06:9a:77:4b:
07:3b:b3:8c:71:ff:61:1b:84:d4:02:46:47:e5:4d:
79:be:22:e9:7a:8c:eb:06:38:38:a6:f7:b7:83:bf:
f2:64:c9:b8:d9:7f:d1:cc:87:ac:80:b0:d0:d3:17:
35:d1:49:44:2e:6e:9f:60:9c:ca:9a:6d:cd:63:79:
7c:6d:33:72:13:74:f1:16:20:50:46:20:e7:c1:ff:
b0:42:95
Exponent: 65537 (0x10001)
X509v3 extensions:
 X509v3 Subject Key Identifier:
 75:22:3F:BE:99:B7:FA:A1:5B:1D:68:0B:E9:5E:21:7D:83:62:AC:DB
 X509v3 Authority Key Identifier:
 keyid:75:22:3F:BE:99:B7:FA:A1:5B:1D:68:0B:E9:5E:21:7D:83:62:AC:DB
 X509v3 Basic Constraints: critical
 CA:TRUE
 X509v3 Key Usage: critical
 Digital Signature, Certificate Sign, CRL Sign
Signature Algorithm: sha256WithRSAEncryption
8e:0c:50:18:5f:db:cc:80:5c:6e:ce:43:29:32:2e:0b:70:96:
db:e8:23:c9:15:a2:99:72:d6:01:c9:61:8e:ed:8d:f8:4d:2f:
99:57:bf:52:1f:4a:5b:7b:ff:24:23:5f:eb:3e:e8:8e:0c:d4:
94:0f:20:a7:e3:3b:18:e9:76:06:5a:ae:65:38:d4:3a:98:d6:
0b:73:5b:b5:8e:4c:b5:74:02:9a:9d:9a:7d:7a:18:2f:32:38:
9e:0e:7b:de:15:3c:f1:33:e8:2d:3f:92:f0:f2:4e:7a:7f:e2:
a5:2e:04:3a:2f:3b:1b:05:71:39:70:6d:a4:6e:8f:25:31:0e:
2c:8a:7e:b4:30:7c:38:2f:48:df:19:56:42:4f:be:5f:d3:02:
70:18:7e:76:66:ca:13:1c:e3:9c:4d:aa:d3:67:96:be:d9:49:
5c:69:10:75:26:53:f7:50:39:06:15:d1:3a:87:47:f6:92:a2:
d4:91:35:29:b7:4b:ea:56:4c:13:5e:32:7f:c7:3f:4c:46:67:
54:8d:67:60:38:98:75:da:24:f2:64:b9:24:a1:e3:5b:42:66:
4c:c7:cb:ee:c3:ca:bd:87:1b:7a:fc:35:53:2d:74:68:db:a7:
47:db:03:a3:30:52:af:67:7f:54:a4:de:60:ca:ae:94:43:f8:
98:85:fc:18:9b:b1:db:81:44:57:0b:be:6a:56:9d:2f:7d:75:
c2:22:a4:7c:d7:ee:f8:de:10:11:26:60:35:1c:4c:87:2e:a2:
fb:1f:5f:30:6c:11:c1:fa:f2:5b:46:02:0a:18:2f:02:a4:99:
f2:43:29:cf:e6:5b:8a:d0:ec:42:bf:49:c6:8a:7e:b4:53:38:
03:1b:fd:a9:49:88:b5:f1:42:93:c7:78:38:6c:2a:1c:be:83:
97:27:b1:26:eb:16:44:ce:34:02:53:45:08:30:c9:3a:76:83:
10:f3:af:c7:6f:0c:74:ec:81:ea:d9:c4:20:a5:1d:72:64:52:
7b:e8:30:1a:9e:3a:05:9c:8a:69:e5:b7:43:b3:36:08:f2:e0:
fb:88:d9:c1:b6:f4:4a:23:27:31:3a:51:b3:68:c9:6f:3e:f5:
dd:98:4d:07:38:ed:f4:d3:ed:06:4c:84:87:3d:cf:f3:2e:e5:
1a:b6:00:71:4c:51:35:c8:95:e4:c6:7e:82:47:d3:25:64:a4:
0b:31:53:d0:e4:6b:97:98:21:4b:fc:e7:12:be:69:01:d8:b5:
74:f5:b6:39:22:8a:8c:39:23:0f:be:4b:0f:9a:01:ac:b8:5b:
12:cb:94:06:30:f5:74:45:20:af:ab:d6:af:21:0c:d8:62:84:
18:c2:cf:4f:be:73:c9:33

```

## 删除 CA 服务器证书

```

OS10# crypto ca-cert delete Dell_rootCA1.crt
Successfully removed certificate

```

## 证书吊销

在交换机和外部设备（如 RADIUS 或 TLS 服务器）设置安全连接之前，它们会分别呈现 CA 签名的证书。证书验证允许对等用户进行身份验证，并随后检查以确保证书尚未被颁发 CA 吊销。

证书包含有关颁发证书的证书分发点 (CDP) 的 URL 和其他信息。通过使用 URL，OS10 访问 CDP 以下载证书吊销列表 (CRL)。如果外部设备的证书在列表中或 CDP 服务器不响应，则不会设置该连接。

证书吊销列表包含所有已吊销证书的列表。颁发证书的 CA 将维护 CRL。CA 将定期发布新的 CRL。OS10 交换机会自动下载新的 CRL 并使用它来验证通过连接设备提供的证书。

当 CA 发布证书时，它通常会在证书中包括 CRL 分发点。OS10 使用 CDP URL 来访问具有当前 CRL 的服务器。在 CRL 吊销检查期间，OS10 支持使用多个 CDP 和 CRL。如果 CRL 检查验证来自外部设备的证书，OS10 将设置安全连接，以执行由应用程序启动的任务。

与 CA 证书相似，CRL 在交换机上的信任存储区中维护，并应用于已启用 PKI 的所有应用程序。要使用 CRL 验证外部设备提供的证书，请执行以下操作：

1. 在 EXEC 模式下配置证书分发点的 URL。

```
crypto cdp add cdp-name cdp-url
```

在 EXEC 模式下验证交换机访问的 CDP。

```
show crypto cdp [cdp-name]
```

要删除已安装的 CDP，请使用 `crypto cdp delete cdp-name` 命令。

2. 在 EXEC 模式下安装从 CDP 下载的 CRL。

```
crypto crl install crl-path [crl-filename]
```

在 EXEC 模式显示交换机上安装的 CRL 的列表。

```
show crypto crl [crl-filename]
```

要删除使用 `crypto crl install` 命令配置的手动安装的 CRL，请使用 `crypto crl delete [crl-filename]` 命令。

要启用交换机上的 CRL 检查，请参阅[安全配置文件](#)。

#### 示例：配置 CDP

```
OS10# crypto cdp add cert1_cdp http://crl.chambersign.org/chambersignroot.crl
Successfully added CDP
```

```
OS10# show crypto cdp
```

```

Manually installed CDPs
cert1_cdp.crl_url

Automatically installed CDPs
```

#### 示例：安装 CRL

```
OS10# crypto crl install home://pki-regression/Network_Solutions_Certificate_
Authority.0.crl.pem
Processing file ...
```

```
issuer=C=US,O=Network Solutions L.L.C.,CN=Network Solutions Certificate
Authority.0.crl.pem
lastUpdate=Jul 7 04:15:08 2019 GMT
nextUpdate=Jul 11 04:15:08 2019 GMT
```

```
OS10# show crypto crl
```

```

Manually installed CRLs
Network_Solutions_Certificate_Authority.0.crl.pem

Downloaded CRLs
```

## 请求并安装主机证书

OS10 还支持交换机获取其自己的 X.509v3 主机证书。在此过程中，您将生成一个证书签名请求 (CSR) 和一个私钥。在本地将私钥保存在安全的位置。将 CSR 文件复制到证书颁发机构。CA 通过对 CSR 中包含的交换机证书进行数字签名，为 OS10 交换机生成主机证书。

然后，管理员将 CA 签名的主机证书复制到交换机上的主目录。由于在生成 CSR 时创建本地私钥，因此无需使用已上传的文件安装私钥。

交换机向需要身份验证的客户端（如 Syslog 和通过 TLS 和 HTTPS 连接的 RADIUS 服务器）呈现自己的主机证书。证书使用 OS10 交换机的私钥进行了数字签名。OS10 支持多个主机证书，以便您可以将不同的证书与不同的应用程序配合使用。有关详细信息，请参阅[安全配置文件](#)。

要从 CA 获取主机证书，请执行以下操作：

1. 创建私钥并生成交换机的证书签名请求。
2. 将 CSR 文件复制到 CA 服务器。
3. 将 CA 签名的证书复制到交换机上的主目录。安装信任的证书。

### 生成证书签名请求和私钥

- 在 EXEC 模式下创建私钥和 CSR。将 CSR 文件存储在主目录或 flash: 中，以便以后可将其复制到 CA 服务器。指定 `keypath` 以将 `device.key` 文件存储在安全的永久位置（如主目录），或使用 `private` 选项将密钥文件存储在不会对用户显示的内部文件系统中的专用隐藏位置。

```
crypto cert generate request [cert-file cert-path key-file {private | keypath}]
[country 2-letter code] [state state] [locality city] [organization organization-name]
[orgunit unit-name] [cname common-name] [email email-address] [validity days]
[length length] [altname alt-name]
```

如果您输入 `cert-file` 选项，则必须输入所有必需的参数，如证书和私钥的存储位置、国家/地区代码、状态、地点和其他值。

如果未指定 `cert-file` 选项，系统会提示您以交互方式填写证书的其他参数值；例如：

```
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value; if you enter '.', the field will be
left blank.
Country Name (2 letter code) [US]:
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Francisco
Organization Name (eg, company) []:Starfleet Command
Organizational Unit Name (eg, section) []:NCC-1701A
Common Name (eg, YOUR name) [hostname]:S4148-001
Email Address []:scotty@starfleet.com
```

交换机使用 SHA-256 作为摘要算法。公钥算法是具有 2048 位模数的 RSA。证书断言 `keyEncipherment`（第 2 位）和 `keyAgreement`（第 4 位）的 `KeyUsage` 位。`keyCertSign` 位（第 5 位）未设置。`ExtendedKeyUsage` 字段表示 `serverAuth` 和 `clientAuth`。

属性 `CA:FALSE` 在证书的“Extensions”部分中设置。证书不用于验证其他证书。

- 如有必要，请重新输入命令，为交换机上的不同应用程序生成多个证书密钥对。您可以在安全配置文件中配置证书密钥对。如果您想要更改指定应用程序的证书密钥对而不中断其他关键服务，则必须使用不同的证书密钥对。例如，RADIUS over TLS 可能使用与 SmartFabric 服务不同的证书密钥对。

### 注：

如果使用 `crypto fips enable` 命令的系统处于 FIPS 模式，则将使用 FIPS 验证和法规合规性算法生成 CSR 和私钥。您可以管理是否在 FIPS 模式下生成密钥。

### 将 CSR 复制到 CA 服务器

您可以使用 TFTP、FTP 或 SCP 将 CSR 从闪存复制到目标，如 USB 闪存盘。

```
OS10# copy home:///DellHost.pem scp:///tftpuser@10.11.178.103:/tftpboot/certs/
DellHost.pem
password:
```

CA 服务器使用其私钥对 CSR 进行签名。然后 CA 服务器使签名的证书可供 OS10 交换机下载和安装。

## 安装主机证书

1. 使用 `copy` 命令通过安全的方法将 CA 服务器签名的 X.509v3 证书下载到本地主目录，如 HTTPS、SCP 或 SFTP。
  2. 使用 `crypto cert install` 命令安装证书和使用 CSR 生成的私钥。
- 在 EXEC 模式下安装受信任证书和密钥文件。

```
crypto cert install cert-file home://cert-filepath key-file {key-path | private}
[password passphrase] [fips]
```

- o `cert-file cert-filepath` 指定已下载证书的源位置；例如，`home://s4048-001-cert.pem` 或 `usb://s4048-001-cert.pem`。
  - o `key-file {key-path | private}` 指定用于检索下载或本地生成的私钥的本地路径。输入 `private` 以从本地隐藏位置安装密钥，然后使用证书名称重命名密钥文件。
  - o `password passphrase` 指定在使用密码生成私钥时用于解密私钥的密码。
  - o `fips` 将以与 FIPS 兼容的方式安装证书密钥对。输入 `fips` 以安装 FIPS 感知应用程序（如 RADIUS over TLS）使用的证书密钥对。如果不输入 `fips`，则证书密钥对将存储为与 FIPS 不兼容的对。
- 注：**您可以决定证书密钥对是否以与 FIPS 兼容的方式生成。请勿在 FIPS 模式以外使用 FIPS 兼容的证书密钥对。启用 FIPS 模式后，仍可为非 FIPS 证书生成 CSRs，以便与非 FIPS 应用程序配合使用。请确保使用 `crypto cert install` 命令将这些证书作为非 FIPS 安装。
- o 如果在 `crypto cert generate request` 命令中使用 `key-file private` 选项后输入 `fips`，则 FIPS 兼容的私钥将存储在内部文件系统中不会对用户显示的隐藏位置。

如果证书安装成功，将显示主机证书及其公用名的文件名。使用文件名在安全配置文件中 `crypto security-profile` 命令配置证书。

## 示例：生成 CSR 并上传到服务器

```
OS10# crypto cert generate request cert-file home://DellHost.pem key-file home://
DellHost.key email admin@dell.com length 1024 altname DNS:dell.domain.com
Processing certificate ...
Successfully created CSR file /home/admin/DellHost.pem and key

OS10# copy home://DellHost.pem scp:///tftpuser@10.11.178.103:/tftpboot/certs/
DellHost.pem
password:
```

## 主机证书提示

当管理大量交换机时，您可以选择不为所有交换机生成大量 CSR。在每个交换机上安装主机证书的另一种方法是同时生成私钥文件和 CSR；例如，在 CA 服务器上。CSR 由 CA 签名，后者会生成证书和密钥文件。然后，您可以使用 `copy` 命令将受信任证书和密钥文件复制到交换机，并使用 `crypto cert install cert-file home://cert-filename key-file home://key-filename` 命令进行安装。

**注：**出于安全原因，私钥文件将复制到内部安全位置并从可访问的文件系统中删除。

## 示例：下载并安装受信任证书和私钥

```
OS10# copy scp:///tftpuser@10.11.178.103:/tftpboot/certs/Dell_host1_CA1.pem home://
Dell_host1_CA1.pem
password:

OS10# copy scp:///tftpuser@10.11.178.103:/tftpboot/certs/Dell_host1_CA1.key home://
Dell_host1_CA1.key
password:

OS10# crypto cert install cert-file home://Dell_host1_CA1.pem key-file home://
Dell_host1_CA1.key
Processing certificate ...
Certificate and keys were successfully installed as "Dell_host1_CA1.pem" that may be
used in a
security profile. CN = Dell_host1_CA1
```

## 显示受信任证书

```
OS10# show crypto cert

```

```
Installed non-FIPS certificates
Dell_host1_CA1.pem
Installed FIPS certificates
```

```
OS10# show crypto cert Dell_host1_CA1.pem
----- Non FIPS certificate -----
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 4096 (0x1000)
 Signature Algorithm: sha256WithRSAEncryption
 Issuer: C = US, ST = California, O = Dell EMC, OU = Networking, CN =
Dell_interCA1
 Validity
 Not Before: Jul 25 19:11:19 2018 GMT
 Not After : Jul 22 19:11:19 2028 GMT
 Subject: C = US, ST = California, L = Santa Clara, O = Dell EMC, OU =
Networking, CN = Dell_host1_CA1
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (2048 bit)
 Modulus:
 00:e7:81:4b:4a:12:8d:ce:88:e6:73:3f:da:19:03:
 c6:56:01:19:b2:02:61:3f:5b:1e:33:28:a1:ed:e3:
 85:bc:56:fb:18:d5:16:2e:a0:e7:3a:f9:34:b4:df:
 37:97:93:a9:b9:94:b2:9f:69:af:fa:31:77:68:06:
 89:7b:6d:fc:91:14:4a:c8:7b:23:93:f5:44:5a:0a:
 3f:ce:9b:af:a6:9b:49:29:fd:fd:cb:34:40:c4:02:
 30:95:37:28:50:d8:81:fb:1f:83:88:d9:1f:a3:0e:
 49:a1:b3:df:90:15:d4:98:2b:b2:38:98:6e:04:aa:
 bd:92:1b:98:48:4d:08:49:69:41:4e:6a:ee:63:d8:
 2a:9f:e6:15:e2:1d:c3:89:f5:f0:d0:fb:c1:9c:46:
 92:a9:37:b9:2f:a0:73:cf:e7:d1:88:96:b8:4a:84:
 91:83:8c:f0:9a:e0:8c:6e:7a:fa:6e:7e:99:3a:c3:
 2c:04:f9:06:8e:05:21:5f:aa:6e:9f:b7:10:37:29:
 0c:03:14:a0:9d:73:1f:95:41:39:9b:96:30:9d:0a:
 cb:d0:65:c3:59:23:01:f7:f5:3a:33:b9:e9:95:11:
 0c:51:f4:e9:1e:a5:9d:f7:95:84:9c:25:74:0c:21:
 4f:8b:07:29:2f:e3:47:14:50:8b:03:c1:fb:83:85:
 dc:bb
 Exponent: 65537 (0x10001)
 X509v3 extensions:
 X509v3 Basic Constraints:
 CA:FALSE
 Netscape Cert Type:
 SSL Client, S/MIME
 Netscape Comment:
 OpenSSL Generated Client Certificate
 X509v3 Subject Key Identifier:
 4A:20:AA:E1:69:BF:BE:C5:66:2E:22:71:70:B4:7E:32:6F:E0:05:28
 X509v3 Authority Key Identifier:
 keyid:A3:39:CB:C7:76:86:3B:05:44:34:C2:6F:90:73:1F:5F:64:55:5C:76
 X509v3 Key Usage: critical
```

## 删除受信任证书

```
OS10# OS10# crypto cert delete Dell_host1_CA1.pem
Certificate and keys were successfully deleted. CN = Dell_host1_CA1
```

## 自签名证书

管理员可能倾向于不要设置证书颁发机构，并在网络中实施证书信任模式，但仍要使用传输层安全 (TLS) 协议提供的私有功能。在这种情况下，可以使用自签名证书。

自签名证书未由 CA 签名。交换机在其证书中将自己呈现为受信任的设备。连接客户端可能会提示用户信任证书（例如，当网页浏览器警告站点不安全时）或拒绝证书，具体取决于配置。自签名证书不提供针对中间人攻击的保护。

要生成并安装自签名证书，请执行以下操作：

1. 在本地目录中创建自签名证书和密钥，或 USB 闪存盘。
2. 安装自签名证书。

## 生成自签名证书

- 在 EXEC 模式下创建自签名证书。将 `device.key` 文件保存在安全的永久位置，如 NVRAM。

```
crypto cert generate self-signed [cert-file cert-path key-file {private | keypath}]
[country 2-letter code] [state state] [locality city] [organization organization-name]
[orgunit unit-name] [cname common-name] [email email-address] [validity days]
[length length] [altname alt-name]
```

如果输入 `cert-file` 选项，则必须输入所有必需的参数，包括存储证书和私钥的本地路径。

如果您指定 `cert-file` 选项，系统会提示您以交互方式输入证书的其他参数值；例如：

```
You are about to be asked to enter information that will be incorporated in your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value; if you enter '.', the field will be
left blank.
Country Name (2 letter code) [US]:
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Francisco
Organization Name (eg, company) []:Starfleet Command
Organizational Unit Name (eg, section) []:NCC-1701A
Common Name (eg, YOUR name) [hostname]:S4148-001
Email Address []:scotty@starfleet.com
```

交换机使用 SHA-256 作为摘要算法。公钥算法是具有 2048 位模数的 RSA。

**注：**将自签名 509v3 证书与 Syslog 和 RADIUS 服务器配合使用，将服务器配置为接受自签名证书。 syslog 日志和 RADIUS 服务器需要相互身份验证，这意味着客户端和服务端必须彼此验证。 Dell EMC Networking 建议将 CA 服务器配置为网络中的所有受信证书。

## 安装自签名证书

- 在 EXEC 模式下安装自签名证书和密钥文件。

```
crypto cert install cert-file home://cert-filename key-file {key-path | private}
[password passphrase] [fips]
```

- `cert-file cert-path` 指定已下载证书的源位置；例如，`home://s4048-001-cert.pem` 或 `usb://s4048-001-cert.pem`。
- `key-file {key-path | private}` 指定用于检索下载或本地生成的私钥的本地路径。输入 `private` 以从本地隐藏位置安装密钥，然后使用证书名称重命名密钥文件。
- `password passphrase` 指定在使用密码生成私钥时用于解密私钥的密码。
- `fips` 将以与 FIPS 兼容的方式安装证书密钥对。输入 `fips` 以安装 FIPS 感知应用程序（如 RADIUS over TLS）使用的证书密钥对。如果不输入 `fips`，则证书密钥对将存储为非 FIPS 兼容的对。

**注：**您可以决定证书密钥对是否以与 FIPS 兼容的方式生成。请勿在 FIPS 模式以外使用 FIPS 兼容的证书密钥对。

- 如果在 `crypto cert generate request` 命令中使用 `key-file private` 选项后输入 `fips`，则 FIPS 兼容的私钥将存储在内部文件系统中不会对用户显示的隐藏位置。

如果证书安装成功，将显示自签名证书及其公用名的文件名。使用文件名在安全配置文件中使用 `crypto security-profile` 命令配置证书。

## 示例：生成并安装自签名证书和密钥

```
OS10# crypto cert generate self-signed cert-file home://DellHost.pem key-file home://
DellHost.key email admin@dell.com length 1024 altname DNS:dell.domain.com validity 365
Processing certificate ...
Successfully created certificate file /home/admin/DellHost.pem and key

OS10# crypto cert install cert-file home://DellHost.pem key-file home://DellHost.key
Processing certificate ...
```



```
Certificate and keys were successfully installed as "DellHost.pem" that may be used in a security profile. CN = DellHost.
```

## 显示自签名证书

```
OS10# show crypto cert
```

```

Installed non-FIPS certificates
DellHost.pem

Installed FIPS certificates
```

```
OS10# show crypto cert DellHost.pem
```

```
----- Non FIPS certificate -----
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 245 (0xf5)
 Signature Algorithm: sha256WithRSAEncryption
 Issuer: emailAddress = admin@dell.com
 Validity
 Not Before: Feb 11 20:10:12 2019 GMT
 Not After : Feb 11 20:10:12 2020 GMT
 Subject: emailAddress = admin@dell.com
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (1024 bit)
 Modulus:
 00:c7:12:ca:a8:d6:d2:1c:ab:66:9a:d1:db:50:5a:
 b5:8a:e4:53:9d:f6:b4:fc:cd:f4:b9:46:8a:03:86:
 be:0b:50:51:c7:25:76:9f:ff:b4:f9:f8:d9:6f:5d:
 53:52:0c:4d:05:ed:31:23:79:44:5c:d7:62:01:9d:
 41:e8:ff:3a:b0:35:0c:22:d7:ef:df:05:9a:28:6b:
 95:10:8e:bc:c6:62:3a:82:30:0f:4f:4e:19:17:48:
 f1:bd:1e:0c:4f:54:03:42:f3:a7:de:22:40:3d:5e:
 6b:b2:8e:23:17:53:ef:10:d9:ae:1d:1f:d6:e4:ae:
 25:9f:d9:39:60:5c:49:b0:ad
 Exponent: 65537 (0x10001)
 X509v3 extensions:
 X509v3 Subject Key Identifier:
 DA:39:A3:EE:5E:6B:4B:0D:32:55:BF:EF:95:60:18:90:AF:D8:07:09
 X509v3 Subject Alternative Name:
 DNS:dell.domain.com
 Signature Algorithm: sha256WithRSAEncryption
 b8:83:ae:34:bb:84:e6:b4:a3:fd:77:20:67:15:3f:02:76:ca:
 f6:74:d4:d2:36:0e:58:8c:96:13:c2:85:8a:df:ba:c0:d9:c8:
```

## 安全配置文件

要为不同的 OS10 应用程序使用独立的安全凭据集，您可以配置多个安全配置文件并将其分配给 OS10 应用程序。安全配置文件包含证书和私钥对。

例如，您可以针对 RADIUS over TLS 身份验证和 SmartFabric 服务维护不同的安全配置文件。通过使用不同的安全配置文件，您可以升级一个应用程序，而不会中断另一个应用程序的操作。配置配置文件时，将安全配置文件分配给应用程序。

安装证书密钥对时，两者都采用证书的名称。例如，如果您使用以下命令安装证书：

```
OS10# crypto cert install cert-file home://Dell_host1.pem key-file home://abcd.key
```

证书密钥对安装为 Dell\_host1.pem 和 Dell\_host1.key。在配置命令中，请参阅配对 Dell\_host1。配置安全配置文件时，您可以在 `certificate certificate-name` 命令中输入 Dell\_host1。

### 配置安全配置文件

1. 在 CONFIGURATION 模式下创建特定于应用程序的安全配置文件。

```
crypto security-profile profile-name
```



2. 在安全配置文件模式下将证书和私钥对分配到安全配置文件。对于 `certificate-name`，输入与不带 `.pem` 扩展名的 `show crypto certs` 输出中显示的证书密钥对的名称。

```
certificate certificate-name
exit
```

3. (可选) 为从 SECURITY-PROFILE 模式中的外部设备接收的证书启用 CRL 检查。CRL 检查使用交换机上安装的 CRL 验证证书的有效性。

```
revocation-check
```

4. (可选) 对安全配置文件模式中的外部设备所提供的证书启用对等名称检查。对等名称检查可确保证书与对等设备的名称匹配，例如远程服务器名称。

```
peer-name-check
```

5. 使用安全配置文件以配置基于 X.509v3 的服务；例如，要使用 X.509v3 证书配置 RADIUS over TLS 身份验证，请输入以下 `radius-server host tls` 命令：

```
radius-server host {hostname | ip-address} tls security-profile profile-name
[auth-port port-number] key {0 authentication-key | 9 authentication-key |
authentication-key}
```

### 示例：RADIUS over TLS 身份验证中的安全配置文件

```
OS10# show crypto cert

Installed non-FIPS certificates
dv-fedgov-s6010-1.pem

Installed FIPS certificates
OS10#
OS10(config)#
OS10(config)# crypto security-profile radius-prof
OS10(config-sec-profile)# certificate dv-fedgov-s6010-1
OS10(config-sec-profile)# revocation-check
OS10(config-sec-profile)# peer-name-check
OS10(config-sec-profile)# exit
OS10(config)#
OS10(config)# radius-server host radius-server-2.test.com tls security-profile radius-
prof key radsec
OS10(config)# end
OS10# show running-configuration crypto security-profile
!
crypto security-profile radius-prof
 certificate dv-fedgov-s6010-1

OS10# show running-configuration radius-server
radius-server host radius-server-2.test.com tls security-profile radius-prof key 9
2b9799adc767c0efe8987a694969b1384c541414ba18a44cd9b25fc00ff180e9
```

## 群集安全

当您启用 VLT 或结构自动化应用程序时，加入群集的交换机将使用安全通道彼此通信。只有当您在交换机上启用了 VLT 或结构群集配置时，才会启用安全通道。OS10 安装默认的 X.509v3 证书密钥对，以在群集中的对等设备之间建立安全通道。

替换用于群集应用程序的默认证书密钥对：

- 在不受信任设备访问管理或 OS10 交换机上的数据端口的部署中。
- 默认情况下，X.509v3 证书将于 2021 年 7 月 27 日到期。如果默认证书密钥对到期，则对等交换机上的 VLT 域不会出现。

**❗ 注：**运行 10.5.0.0 版本的交换机上的 OS10 安装的默认证书密钥对的到期日期为 2021 年 7 月 27 日。要确保在到期日期之前群集中的安全通信，请安装最新的 X.509v3 证书密钥对。

通过使用 `cluster security-profile` 命令配置特定于应用程序的安全配置文件，从而创建自定义 X.509v3 证书密钥对。在 VLT 域或结构应用程序群集中的对等设备之间使用的默认或自定义 X.509v3 证书密钥对到期时，请按照以下项目中的步骤安装有效的 CA 证书：

- [管理 CA 证书](#)。
- [请求并安装主机证书](#)。

在为群集应用程序替换默认的证书密钥对时，请确保群集中的所有设备都使用相同的自定义证书密钥对或同一 CA 颁发的唯一证书密钥对。

 **小心:** 当您替换默认的证书密钥对时，群集设备将暂时丢失其安全通道连接。Dell EMC Networking 建议您在维护时间内更改群集安全配置。

本示例显示如何为群集应用程序安装 X.509v3 CA 和主机证书密钥对。有关详情，请参阅：

- 导入和安装 CA 证书 — 请参阅[管理 CA 证书](#)。
- 生成 CSR 并安装主机证书 — 请参阅[请求和安装主机证书](#)。

#### 1. 安装受信任的 CA 证书。

```
OS10# copy tftp://CAadmin:secret@172.11.222.1/GeoTrust_Universal_CA.crt
home:// GeoTrust_Universal_CA.crt

OS10# crypto ca-cert install home://GeoTrust_Universal_CA.crt
Processing certificate ...
Installed Root CA certificate

CommonName = GeoTrust Universal CA
IssuerName = GeoTrust Universal CA
```

#### 2. 生成 CSR，将 CSR 复制到 CA 服务器、下载签名的证书，并安装主机证书。

```
OS10# crypto cert generate request cert-file home://s4048-001.csr key-file home://
tsr6.key cname "Top of Rack 6" altname "IP:10.0.0.6 DNS:tor6.dell.com" email
admin@dell.com organization "Dell EMC" orgunit Networking locality "Santa Clara" state
California country US length 1024
Processing certificate ...
Successfully created CSR file /home/admin/tor6.csr and key

OS10# copy home://tor6.csr scp://CAadmin:secret@172.11.222.1/s4048-001-csr.pem

OS10# copy scp://CAadmin:secret@172.11.222.1/s4048-001.crt usb://s4048-001.crt

OS10# crypto cert install crt-file usb://s4048-001.crt key-file usb://s4048-001.key
This will replace the already installed host certificate.
Do you want to proceed ? [yes/no(default)]:yes
Processing certificate ...
Host certificate installed successfully.
```

#### 3. 配置 X.509v3 安全配置文件。

```
OS10# show crypto cert

Installed non-FIPS certificates
s4048-001

Installed FIPS certificates
OS10# config terminal
OS10(config)# crypto security-profile secure-cluster
OS10(config-sec-profile)# certificate s4048-001
OS10(config-sec-profile)# exit
```

#### 4. 配置群集安全配置文件

```
OS10(config)# cluster security-profile secure-cluster
OS10(config)# exit
```

## X.509v3 命令

### certificate

在特定于应用程序的安全配置文件中配置证书和私钥对。

|        |                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>certificate certificate-name</code>                                                                                                                                                                                                                       |
| 参数     | <i>certificate-name</i> — 输入在不带 .pem 扩展名的 <code>show crypto certs</code> 输出中显示的证书密钥对名称。                                                                                                                                                                         |
| 默认     | 未配置                                                                                                                                                                                                                                                             |
| 命令模式   | SEC-PROFILE                                                                                                                                                                                                                                                     |
| 使用情况信息 | <p>使用 <code>certificate</code> 命令将证书和私钥与安全配置文件相关联。通过特定于应用程序的安全配置文件，您可以更改 OS10 应用程序（如 SmartFabric 服务）使用的证书密钥对，而不会中断其他任务关键型应用程序的服务。</p> <p>安装证书密钥对时，两者都采用证书的名称。输入不带扩展名的证书密钥对名称作为 <i>certificate-name</i> 值。要从配置文件中移除证书密钥对，请输入 <code>no certificate</code> 命令。</p> |

#### 示例

```
OS10# crypto security-profile secure-radius-profile
OS10(config-sec-profile)# certificate Dell_host1
```

支持的版本 10.4.3.0 or later

### cluster security-profile

为群集应用程序创建安全配置文件。

|        |                                                                                                                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>cluster security-profile profile-name</code>                                                                                                                                                                                                                                |
| 参数     | <i>profile-name</i> — 输入安全配置文件的名称；最多 32 个字符。                                                                                                                                                                                                                                      |
| 默认     | 未配置                                                                                                                                                                                                                                                                               |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                     |
| 使用情况信息 | <p>当您启用 VLT 或结构自动化应用程序时，加入群集的交换机将使用安全通道彼此通信。OS10 安装默认的 X.509v3 证书密钥对，以在群集中的对等设备之间建立安全通道。如果不受信任的设备访问交换机上的管理或数据端口，请使用 <code>cluster security-profile</code> 命令将默认的证书密钥对替换为自定义的 X.509v3 证书密钥对。安全配置文件使用 <code>certificate</code> 命令将证书和私钥对关联起来。命令的 <code>no</code> 形式将删除群集安全配置文件。</p> |

#### 示例

```
OS10(config)# cluster security-profile secure-cluster
OS10(config)#
```

支持的版本 10.4.3.0 or later

### crypto ca-cert delete

删除 CA 证书。

|      |                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | <code>crypto ca-cert delete {ca-cert-filepath   all}</code>                                                                                                                                             |
| 参数   | <ul style="list-style-type: none"><li><i>ca-cert-filepath</i> — 输入存储下载的 CA 证书的本地路径；例如，<code>home://CAcert.pem</code> 或 <code>usb://CA-cert.pem</code>。</li><li><code>all</code> — 删除所有 CA 证书。</li></ul> |
| 默认   | 未配置                                                                                                                                                                                                     |
| 命令模式 | EXEC                                                                                                                                                                                                    |

## 使用情况信息

要显示当前安装的 CA 证书，请使用 `show crypto ca-certs` 命令。

## 示例

```
OS10# crypto ca-cert delete Amazon_Root_CA.crt
Successfully removed certificate

OS10# crypto ca-cert delete all
Proceed to delete all installed CA certificates? [confirm yes/
no(default)]:yes
```

## 支持的版本

10.4.3.0 or later

# crypto ca-cert install

从复制到交换机的证书颁发机构安装证书。

## 语法

`crypto ca-cert install ca-cet-filepath [filename]`

## 参数

- `ca-cert-filepath` — 输入存储下载的 CA 证书的本地路径；例如，`home://CAcert.pem` 或 `usb://CA-cert.pem`。
- `filename` — （可选）输入将 CA 证书存储在 OS10 信任存储目录下的文件名。以 `filename.crt` 格式输入文件名。

## 默认

未配置

## 命令模式

EXEC

## 使用情况信息

在使用 `crypto ca-cert install` 命令之前，请使用安全连接将证书复制到交换机上的主目录，如 HTTPS、SCP 或 SFTP。成功安装后，将显示 CA 证书的主题和颁发者。要删除受信任的证书，请使用 `crypto ca-cert delete` 命令。

## 示例

```
OS10# crypto ca-cert install home://GeoTrust_Universal_CA.crt
Processing certificate ...
Installed Root CA certificate
CommonName = GeoTrust Universal CA
IssuerName = GeoTrust Universal CA
```

## 支持的版本

10.4.3.0 or later

# crypto cdp add

在交换机上安装证书分发点 (CDP)。

## 语法

`crypto cdp add cdp-name cdp-url`

## 参数

- `cdp-name` — 输入 CDP 名称。
- `cdp-name` — 输入用于访问 CDP 的 HTTP URL。

## 默认

未配置

## 命令模式

EXEC

## 使用情况信息

使用 `show crypto cdp` 命令显示交换机上已安装的 CDP

## 示例

```
OS10# crypto cdp add Comsign http://fedir.comsign.co.il/crl/ComSignCA.crl
```

## 支持的版本

10.5.0 or later

# crypto cdp delete

从交换机上的信任存储区中删除证书分发点。

## 语法

`crypto cdp delete crl-filename`

|        |                                                                                      |
|--------|--------------------------------------------------------------------------------------|
| 参数     | <ul style="list-style-type: none"> <li><code>cdp-name</code> — 输入 CDP 名称。</li> </ul> |
| 默认     | 未配置                                                                                  |
| 命令模式   | EXEC                                                                                 |
| 使用情况信息 | 删除 CRL 之前, 请使用 <code>show crypto cdp</code> 命令显示交换机上安装的所有 CDP 的列表。                   |

**示例**

```
OS10# crypto cdp delete Comsign
```

**支持的版本** 10.5.0 or later

## crypto cert delete

删除已安装的主机证书和使用它创建的私钥。

|        |                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>crypto cert delete filename [fips]</code>                                                                                                                                                                                                 |
| 参数     | <ul style="list-style-type: none"> <li><code>filename</code> — 输入在 <code>show crypto cert</code> 命令中显示的主机证书的文件名。</li> <li><code>fips</code> — (可选) 删除与 FIPS 兼容的证书密钥对。要验证证书是否不与 FIPS 或 FIPS 兼容, 请使用 <code>show crypto cert</code> 命令。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                             |
| 命令模式   | EXEC                                                                                                                                                                                                                                            |
| 使用情况信息 | <p>删除系统的证书时, 也会删除私钥。请勿删除在安全配置文件中使用的主机证书。要显示当前安装的主机证书和关联的密钥, 请使用 <code>show crypto cert</code> 命令。</p> <p><b>注:</b> 与 FIPS 兼容和不兼容的证书可以具有相同的文件名。要删除与 FIPS 兼容的证书, 您必须在命令中输入参数 <code>fips</code>。</p>                                               |

**示例**

```
OS10# crypto cert delete Dell_host1_CA1.pem
Certificate and keys were successfully deleted. CN = Dell_host1_CA1
```

**支持的版本** 10.4.3.0 or later

## crypto cert generate

创建证书签名请求 (CSR) 或自签名证书。

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>crypto cert generate {request   self-signed} [cert-file cert-path key-file {private   keypath}] [country 2-letter code] [state state] [locality city] [organization organization-name] [orgunit unit-name] [cname common-name] [email email-address] [validity days] [length length] [altname alt-name]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 参数 | <ul style="list-style-type: none"> <li><code>request</code> — 创建要复制到 CA 的证书签名请求。</li> <li><code>self-signed</code> — 创建自签名证书。</li> <li><code>cert-file cert-path</code> — (可选) 输入用于存储自签名证书或 CSR 的本地路径。您可以输入完整路径或相对路径; 例如, <code>flash://certs/s4810-001-request.csr</code> 或 <code>usb://s4810-001.crt</code>。如果不输入 <code>cert-file</code> 选项, 系统将以交互方式提示您填写证书签名请求的剩余字段。使用 <code>copy</code> 命令将 CSR 导出到 CA。</li> <li><code>key-file {key-path   private}</code> — 输入存储下载或本地生成的私钥的本地路径。如果密钥已下载到远程服务器, 请使用安全方法输入服务器路径, 如 HTTPS、SCP 或 SFTP。输入 <code>private</code> 以将密钥存储在本地隐藏位置。</li> <li><code>country 2-letter-code</code> — (可选) 输入标识国家/地区的两字母代码。</li> <li><code>state state</code> — 输入省/自治区/直辖市的名称。</li> <li><code>locality city</code> — 输入城市的名称。</li> </ul> |

- `organization organization-name` — 输入组织的名称。
- `orgunit unit-name` — 输入设备的名称。
- `cname common-name` — 输入分配给证书的通用名称。通用名称是呈现给连接设备的主要身份。默认情况下，交换机的主机名称为通用名称。您可以为交换机配置不同的通用名称；例如，IP 地址。如果 `common-name` 值与设备的呈现的标识不匹配，则表示签名的证书未验证。
- `email email-address` — 输入用于与组织通信的有效电子邮件地址。
- `validity days` — 输入证书的有效天数。对于 CSR，有效性不起作用。对于自签名证书，默认值为 3650 天或 10 年。
- `length bit-length` — 输入关键字长度的位值。对于 FIPS 模式，范围从 2048 到 4096；对于非 FIPS 模式，范围从 1024 到 4096。FIPS 和非 FIPS 模式的默认密钥长度为 2048 位。FIPS 模式的最小密钥长度值为 2048 位。非 FIPS 模式的最小密钥长度值为 1024 位。
- `altname altname` — 为组织输入备用名称；例如，使用 IP 地址 `altname IP:192.168.1.100`。

## 默认

未配置

## 命令模式

EXEC

## 使用情况信息

当您想要 CA 签署主机证书时，请生成 CSR。如果您不设置 CA 并在网络中实施证书信任模型，则生成自签名证书。

如果输入 `cert-file` 选项，则必须输入所有必需的参数，包括存储证书和私钥的本地路径。

如果未指定 `cert-file` 选项，系统会提示您以交互方式填写证书的其他参数值；例如：

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value; if you enter '.', the
field will be left blank.
Country Name (2 letter code) [US]:
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Francisco
Organization Name (eg, company) []:Starfleet Command
Organizational Unit Name (eg, section) []:NCC-1701A
Common Name (eg, YOUR name) [hostname]:S4148-001
Email Address []:scotty@starfleet.com
```

如果系统处于 FIPS 模式 (`crypto fips enable` 命令)，则使用已根据 FIPS 140-2 标准验证的加密库中的认可算法生成 CSR 和私钥。您可以使用 `crypto cert install` 命令和 `fips` 选项，安装符合 FIPS 的证书密钥对。

## 示例

```
OS10# crypto cert generate request cert-file home://cert1.pem key-file
home://cee OS10-VM email admin@dell.com length 1024 altname DNS.dell.com
Processing certificate ...
```

```
Successfully created CSR file /home/admin/cert1.pem and key
```

```
OS10# crypto cert generate self-signed cert-file home://cert2.pem key-
file home:e OS10-VM email admin@dell.com length 1024 altname.dell.com
validity 365
Processing certificate ...
```

```
Successfully created certificate file /home/admin/cert2.pem and key
```

## 支持的版本

10.4.3.0 or later

## crypto cert install

在交换机上安装主机证书和私钥。主机证书可以来自 CA 或自签名。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>crypto cert install cert-file cert-path key-file {key-path   private} [password passphrase] [fips]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"><li><code>cert-file cert-path</code> — 输入存储下载的证书的本地路径。您可以输入完整路径或相对路径；例如，<code>home://s4048-001-cert.pem</code> 或 <code>usb://s4048-001-cert.pem</code> 或 <code>flash://certs/s4810-001-request.crt</code>。</li><li><code>key-file {key-path   private}</code> — 输入用于检索下载或本地生成的私钥的本地路径。指定 <code>key-path</code> 以从本地目录安装密钥。输入 <code>private</code> 以安装本地隐藏位置的密钥。成功安装证书后，将从指定的 <code>key-path</code> 位置删除私钥并将其复制到隐藏位置。</li><li><code>password passphrase</code> — （可选）如果密钥是使用密码生成的，则输入用来解密私钥的密码。</li><li><code>fips</code> — （可选）将证书密钥对安装为与 FIPS 兼容。输入 <code>fips</code> 以安装 FIPS 感知应用程序（如 RADIUS over TLS）使用的证书密钥对。如果不输入 <code>fips</code>，则证书密钥对将存储为非 FIPS 兼容的对。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | <p>在使用 <code>crypto cert install</code> 命令之前，请使用安全连接将 CA 签名的证书复制到交换机上的主目录，如 HTTPS、SCP、SFTP 和私钥（可选）。要删除受信任的证书，请使用 <code>crypto cert delete</code> 命令。</p> <p>成功安装受信任证书需要：</p> <ul style="list-style-type: none"><li>下载的证书已正确格式化。</li><li>下载的证书公钥与私钥对应。</li></ul> <p>您可以通过输入不带扩展名的证书的文件名，将已安装的证书密钥对分配到安全配置文件。</p> <p>可以使用 <code>crypto cert install</code> 命令和可选的 <code>fips</code> 选项，在交换机上以 FIPS 模式或非 FIPS 模式存储证书，但同时在这两种模式下不可行。您必须确保在 FIPS 模式下安装的证书符合 FIPS 140-2 标准。</p>                                                                                                                                                                                                                                    |
| 示例     | <pre>OS10# crypto cert install cert-file home://Dell_host1_CA1.pem key-file home://Dell_host1_CA1.key Processing Certificate ... Certificate and keys were successfully installed as "Dell_host1_CA1.pem" that may be used in a security profile. CN = Dell_host1_CA1.</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 支持的版本  | 10.4.3.0 or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## crypto crl delete

删除交换机上的信任存储中的证书吊销列表文件。

|        |                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>crypto crl delete crl-filename</code>                                                                                                                                       |
| 参数     | <ul style="list-style-type: none"><li><code>crl-filename</code> — 输入带有 <code>.pem</code> 扩展名的 CRL 文件名，如 <code>show crypto crl</code> 输出中的 Manually installed CRLs 下所显示。</li></ul> |
| 默认     | 未配置                                                                                                                                                                               |
| 命令模式   | EXEC                                                                                                                                                                              |
| 使用情况信息 | <p><code>crypto crl delete</code> 命令仅删除手动安装的 CRL。删除 CRL 之前，请使用 <code>show crypto crl</code> 命令显示交换机上安装的所有 CRL 的列表。</p>                                                            |
| 示例     | <pre>OS10# crypto crl delete COMODO_Certification_Authority.0.crl.pem</pre>                                                                                                       |
| 支持的版本  | 10.5.0 or later                                                                                                                                                                   |

## crypto crl install

安装复制到交换机的证书吊销列表文件。

|        |                                                                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>crypto crl install <i>crl-path</i> [<i>crl-filename</i>]</code>                                                                                                                                                                                                                                       |
| 参数     | <ul style="list-style-type: none"><li><i>crl-path</i> — 输入要在其中下载 CRL 的目录的路径。</li><li><i>crl-filename</i> — (可选) 输入您复制到交换机的 CRL 文件名。</li></ul>                                                                                                                                                               |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                         |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                        |
| 使用情况信息 | 在使用 <code>crypto crl install</code> 命令之前, 请将 CRL 拷贝到 <code>home://</code> 或 <code>usb://</code> 目录。如果未在命令中输入 CRL 文件名, 则可以在出现提示时复制并粘贴。使用 <code>show crypto crl</code> 命令可查看交换机上已安装的 CRL。在 <code>show</code> 输出中, 将安装显示在 <code>Manually installed CRLs</code> 下的 CRL — 使用 <code>crypto crl install</code> 命令。 |

|    |                                                                                                                                                                                                                                                                                                                                                                                  |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# copy scp:///tftpuser@10.11.178.103:/crl_example_file.pem home:// password:  OS10# crypto crl install home:// Network_Solutions_Certificate_Authority.0.crl.pem  OS10# show crypto crl -----             Manually installed CRLs             ----- Network_Solutions_Certificate_Authority.0.crl.pem -----             Downloaded CRLs                     -----</pre> |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

支持的版本 10.5.0 or later

## crypto fips enable

启用 FIPS 模式。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>crypto fips enable</code>                                                                                                                                                                                                                                                                                                                                                                                       |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 使用情况信息 | <p>您可以在 FIPS 140-2 兼容模式下使用 OS10。在此模式下, 应用程序将加密算法限制为 NIST FIPS 140-2 标准和认证进程支持的密码。启用 FIPS 模式时:</p> <ul style="list-style-type: none"><li>SSH 服务将重新启动。现有 SSH 会话不会受到影响。只有新的 SSH 会话在已启用 FIPS 模式下运行。</li><li>重新生成 SSH 主机密钥。</li><li>如果 SNMPv3 配置了隐私设置, 它将以 FIPS 模式运行。</li></ul> <p>如果您使用 <code>crypto fips enable</code> 命令启用 FIPS, RADIUS over TLS 在 FIPS 模式下运行。在 FIPS 模式中, RADIUS over TLS 需要在交换机上安装符合 FIPS 的证书和密钥对。</p> |

|    |                                     |
|----|-------------------------------------|
| 示例 | <pre>OS10# crypto fips enable</pre> |
|----|-------------------------------------|

支持的版本 10.4.3.0 or later



## crypto security-profile

创建特定于应用程序的安全配置文件。

|        |                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>crypto security-profile profile-name</code>                                                                        |
| 参数     | <i>profile-name</i> — 输入安全配置文件的名称；最多 32 个字符。                                                                             |
| 默认     | 未配置                                                                                                                      |
| 命令模式   | CONFIGURATION                                                                                                            |
| 使用情况信息 | 为交换机上的特定应用程序创建安全配置文件，例如 RADIUS over TLS。安全配置文件使用 <code>certificate</code> 命令将证书和私钥对关联起来。命令的 <code>no</code> 形式将删除安全配置文件。 |

### 示例

```
OS10# crypto security-profile secure-radius-profile
OS10(config-sec-profile)#
```

支持的版本 10.4.3.0 or later

## peer-name-check

在安全配置文件中为外部设备提供的证书启用对等名称检查。

|        |                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------|
| 语法     | <code>peer-name-check</code>                                                                                 |
| 参数     | 无                                                                                                            |
| 默认     | 未配置                                                                                                          |
| 命令模式   | SEC-PROFILE                                                                                                  |
| 使用情况信息 | 使用 <code>peer-name-check</code> 命令启用 OS10 应用程序，以验证用于连接到该交换机的证书是否与对等设备的名称（如远程服务器名称）匹配。无命令版本会在安全配置文件中禁用对等名称检查。 |

### 示例

```
OS10(config)# crypto security-profile profile-1
OS10(config-sec-profile)# peer-name-check

OS10(config)# crypto security-profile profile-1
OS10(config-sec-profile)# no peer-name-check
```

支持的版本 10.5.0 or later

## revocation-check

启用安全配置文件中的 CRL 检查。

|        |                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>revocation-check</code>                                                                                                                                           |
| 参数     | 无                                                                                                                                                                       |
| 默认     | 未配置                                                                                                                                                                     |
| 命令模式   | SEC-PROFILE                                                                                                                                                             |
| 使用情况信息 | 使用 <code>revocation-check</code> 命令可为交换机上已启用 PKI 的应用程序启用对外部设备所提供的证书的验证。使用 <code>show crypto crl</code> 命令可显示交换机上安装的 CRL，并用于确保来自外部设备的证书的有效性和可信性。无命令版本会在安全配置文件中禁用 CRL 检查。 |

### 示例

```
OS10(config)# crypto security-profile profile-1
OS10(config-sec-profile)# revocation-check

OS10(config)# crypto security-profile profile-1
OS10(config-sec-profile)# no revocation-check
```

**支持的版本** 10.5.0 or later

## show crypto ca-certs

显示交换机上安装的所有 CA 证书。

|               |                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------|
| <b>语法</b>     | show crypto ca-certs [ <i>filename</i> ]                                                            |
| <b>参数</b>     | <i>filename</i> — (可选) 输入 CA 证书的文本文件名 (如 show crypto ca-certs 输出中所示)。以格式 <i>filename.crt</i> 输入文件名。 |
| <b>默认</b>     | 显示所有已安装的 CA 证书。                                                                                     |
| <b>命令模式</b>   | EXEC                                                                                                |
| <b>使用情况信息</b> | 要删除 CA 证书, 请使用 crypto ca-cert delete 命令。输入在 show crypto ca-certs 输出中显示的文件名。                         |

### 示例

```
OS10# show crypto ca-certs

Locally installed certificates
Dell_interCA1.crt
Dell_rootCA1.crt

OS10# show crypto ca-certs Dell_interCA1.crt
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 4096 (0x1000)
 Signature Algorithm: sha256WithRSAEncryption
 Issuer: C = US, ST = California, L = Santa Clara, O = Dell EMC,
OU = Networking, CN = Dell_rootCA1
 Validity
 Not Before: Jul 25 18:49:22 2018 GMT
 Not After : Jul 22 18:49:22 2028 GMT
 Subject: C = US, ST = California, O = Dell EMC, OU = Networking,
CN = Dell_interCA1
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (4096 bit)
 Modulus:
 00:b8:46:93:86:27:af:3e:fb:a7:bd:c1:25:76:fd:
 50:87:02:de:98:2b:95:2e:b0:49:e4:5c:7c:db:83:
 b9:e7:3d:e3:61:63:e9:e1:e9:6f:a4:eb:b8:06:bf:
 57:b7:bb:17:d1:50:ee:7c:ad:d1:09:fe:c3:2c:ea:
 79:bf:b9:fa:92:52:22:0e:49:62:0b:97:b8:92:c2:
 59:43:2e:53:e0:c6:d4:ea:d5:ec:35:79:4f:c2:95:
 82:91:43:ee:3e:3d:ae:e3:a9:ba:37:94:79:27:b3:
 0d:f9:5a:cc:1b:fd:6d:24:d6:00:ce:1d:3d:4a:fa:
 95:94:c8:a5:1c:65:cc:f0:08:4a:7f:79:c7:68:4e:
 c2:3a:b5:b9:21:82:1c:25:45:f4:7e:84:f9:d3:af:
 28:06:0b:8d:da:72:c1:41:1a:ca:c1:63:de:d6:25:
 ef:f8:ec:a7:93:88:e0:a0:4f:93:14:81:a6:e8:90:
 31:7a:b8:53:4c:52:44:e1:5c:6a:aa:94:b6:0d:eb:
 73:b8:18:21:d5:9c:a4:73:a4:54:16:5b:af:b0:35:
 0d:36:ff:cb:72:04:63:d1:df:48:59:d3:e9:51:e1:
 cb:2a:61:20:ee:31:25:51:68:0e:be:98:c3:22:98:
 29:f9:13:03:c4:2d:bb:4a:d2:cf:7d:00:f9:4c:2e:
 46:70:e3:ab:e7:3c:91:b0:c9:f7:48:89:ea:e7:df:
 4f:f4:f5:fc:3a:17:dc:f8:8c:48:e5:aa:03:84:d7:
 20:7b:55:2e:73:63:85:1c:97:a1:bb:96:95:a1:d3:
 ae:0c:7a:ae:02:3c:2c:07:b6:9b:c5:97:69:fa:88:
 bd:ec:8b:88:b3:90:e3:dc:aa:98:15:c6:91:99:a4:
```

**支持的版本** 10.4.3.0 or later

## show crypto cdp

显示已配置的证书分发点 (CDP) 的列表。

|        |                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show crypto cdp [cdp-name]</code>                                                                                                                                                                                                                                                                                                                               |
| 参数     | <ul style="list-style-type: none"><li><code>cdp-name</code> — (可选) 通过输入在 <code>show crypto cdp</code> 输出中显示的 CDP 名称, 可显示更多详细信息。</li></ul>                                                                                                                                                                                                                             |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                   |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                  |
| 使用情况信息 | <p>使用 <code>show crypto cdp</code> 命令以验证交换机上安装的 CDP 并显示连接到 CDP 的 URL。OS10 使用 URL 访问 CDP 和下载新的 CRL。在 <code>show</code> 输出中:</p> <ul style="list-style-type: none"><li>使用 <code>crypto cdp add</code> 命令可手动安装 CDP。</li><li>当您安装具有指定 CDP 的 CA 证书时, 自动安装的 CDP 将自动进行配置。</li></ul> <p>使用 <code>crypto cdp install</code> 和 <code>crypto cdp delete</code> 命令可添加或删除 CDP。</p> |

### 示例

```
OS10# show crypto cdp

Manually installed CDPs
Comsign

Automatically installed CDPs
COMODO_Certification_Authority

OS10# show crypto cdp Comsign
http://fedir.comsign.co.il/crl/ComSignCA.crl
```

支持的版本 10.5.0 or later

## show crypto cert

显示有关指定的证书或所有已安装的证书的信息。

|        |                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show crypto cert [filename]</code>                                                                            |
| 参数     | <code>filename</code> — (可选) 输入在 <code>show crypto certs</code> 输出中显示的证书的文本文件名。以格式 <code>filename.crt</code> 输入文件名。 |
| 默认     | 显示所有已安装的主机证书。                                                                                                       |
| 命令模式   | EXEC                                                                                                                |
| 使用情况信息 | 要删除证书, 请使用 <code>crypto cert delete filename</code> 命令。                                                             |

### 示例

```
OS10# show crypto cert

Installed non-FIPS certificates
Dell_host1_CA1.pem

Installed FIPS certificates

OS10# show crypto cert Dell_host1_CA1.pem
----- Non FIPS certificate -----
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 4096 (0x1000)
 Signature Algorithm: sha256WithRSAEncryption
 Issuer: C = US, ST = California, O = Dell EMC, OU = Networking,
```

```

CN = Dell_interCA1
 Validity
 Not Before: Jul 25 19:11:19 2018 GMT
 Not After : Jul 22 19:11:19 2028 GMT
 Subject: C = US, ST = California, L = Santa Clara, O = Dell EMC,
OU = Networking, CN = Dell_host1_CA1
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (2048 bit)
 Modulus:
 00:e7:81:4b:4a:12:8d:ce:88:e6:73:3f:da:19:03:
 c6:56:01:19:b2:02:61:3f:5b:1e:33:28:a1:ed:e3:
 85:bc:56:fb:18:d5:16:2e:a0:e7:3a:f9:34:b4:df:
 37:97:93:a9:b9:94:b2:9f:69:af:fa:31:77:68:06:
 89:7b:6d:fc:91:14:4a:c8:7b:23:93:f5:44:5a:0a:
 3f:ce:9b:af:a6:9b:49:29:fd:fd:cb:34:40:c4:02:
 30:95:37:28:50:d8:81:fb:1f:83:88:d9:1f:a3:0e:
 49:a1:b3:df:90:15:d4:98:2b:b2:38:98:6e:04:aa:
 bd:92:1b:98:48:4d:08:49:69:41:4e:6a:ee:63:d8:
 2a:9f:e6:15:e2:1d:c3:89:f5:f0:d0:fb:c1:9c:46:
 92:a9:37:b9:2f:a0:73:cf:e7:d1:88:96:b8:4a:84:
 91:83:8c:f0:9a:e0:8c:6e:7a:fa:6e:7e:99:3a:c3:
 2c:04:f9:06:8e:05:21:5f:aa:6e:9f:b7:10:37:29:
 0c:03:14:a0:9d:73:1f:95:41:39:9b:96:30:9d:0a:
 cb:d0:65:c3:59:23:01:f7:f5:3a:33:b9:e9:95:11:
 0c:51:f4:e9:1e:a5:9d:f7:95:84:9c:25:74:0c:21:
 4f:8b:07:29:2f:e3:47:14:50:8b:03:c1:fb:83:85:
 dc:bb
 Exponent: 65537 (0x10001)
 X509v3 extensions:
 X509v3 Basic Constraints:
 CA:FALSE
 Netscape Cert Type:
 SSL Client, S/MIME
 Netscape Comment:
 OpenSSL Generated Client Certificate
 X509v3 Subject Key Identifier:

4A:20:AA:E1:69:BF:BE:C5:66:2E:22:71:70:B4:7E:32:6F:E0:05:28
 X509v3 Authority Key Identifier:

keyid:A3:39:CB:C7:76:86:3B:05:44:34:C2:6F:90:73:1F:5F:64:55:5C:76
 X509v3 Key Usage: critical

```

**支持的版本** 10.4.3.0 or later

## show crypto crl

显示已安装的证书吊销列表文件的列表。

- |               |                                                                                                                                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>show crypto crl [crl-filename]</code>                                                                                                                                                                                                     |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>crl-filename</code> — (可选) 输入具有 .pem 扩展名的 CRL 文件名。</li> </ul>                                                                                                                                      |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                             |
| <b>命令模式</b>   | EXEC                                                                                                                                                                                                                                            |
| <b>使用情况信息</b> | <p>使用 <code>show crypto crl</code> 命令可验证交换机上安装的 CRL。在 <code>show</code> 输出中：</p> <ul style="list-style-type: none"> <li>手动安装的 CRL 是使用 <code>crypto crl install</code> 命令安装的。</li> <li>下载的 CRL 会从配置的 CDP 或者在您安装具有指定 CDP 的 CA 证书时自动安装。</li> </ul> |

### 示例

```

OS10# show crypto crl

Manually installed CRLs
COMODO_Certification_Authority.0.crl.pem

```

| Downloaded CRLs |

```
OS10# show crypto crt COMODO_Certification_Authority.0.crl.pem
Certificate Revocation List (CRL):
Version 2 (0x1)
Signature Algorithm: sha1WithRSAEncryption
Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/
CN=COMODO Certification
Authority
Last Update: May 8 20:34:21 2019 GMT
Next Update: May 12 20:34:21 2019 GMT
CRL extensions:
X509v3 Authority Key Identifier:
keyid:0B:58:E5:8B:C6:4C:15:37:A4:40:A9:30:A9:21:BE:47:36:5A:56:FF
X509v3 CRL Number:
2904
No Revoked Certificates.
Signature Algorithm: sha1WithRSAEncryption
5b:77:52:c0:a0:4e:77:be:4a:c4:6a:7e:92:98:2e:a1:6b:3c:
ad:2d:ac:db:0a:19:1d:a3:56:98:7f:d6:93:f3:1d:4b:61:40:
c3:e0:40:45:0b:41:4b:66:87:35:2b:3a:4c:f3:f1:7e:44:7e:
fe:7f:51:5d:17:ee:b3:4c:15:75:a6:a0:7b:2e:b1:92:3e:b6:
71:a8:01:8d:78:ac:80:3b:16:f2:f1:a8:fd:09:68:9f:7e:09:
55:c6:80:2c:2f:e7:f3:54:51:94:3a:d8:b4:d6:00:3f:63:b1:
19:f3:42:2a:d2:c4:3b:de:c4:4d:ad:f0:72:c5:b4:25:51:e5:
3c:76:8b:97:3c:db:fe:3f:7f:41:d2:d9:aa:7f:98:90:6b:cf:
27:53:0e:66:83:8e:cc:81:ef:6a:e5:cd:c2:f1:e2:ea:84:4f:
73:bb:90:5a:b3:19:a3:50:6a:c7:b3:99:e4:09:fd:56:99:83:
3a:15:93:b0:4a:49:28:78:69:85:de:fc:06:cc:b9:a5:5b:d9:
4a:b0:46:90:ce:94:3a:9c:f3:04:e4:d7:98:36:29:a8:8b:fe:
72:26:b0:fd:39:5e:14:f5:00:6d:0e:4f:ec:d4:a5:ca:4f:e1:
d9:4f:5a:37:21:e3:a2:fb:80:db:cd:68:0b:a0:fa:58:0d:5e:
40:e1:e4:1c
```

支持的版本

10.5.0 or later

## 示例：使用 X.509v3 证书配置 RADIUS over TLS

本示例显示如何安装支持 RADIUS over TLS 身份验证的受信任 X.509v3 CA 和主机证书密钥对。

### 1. 安装受信任的 CA 证书。

```
OS10# copy tftp://CAadmin:secret@172.11.222.1/GeoTrust_Universal_CA.crt home://
GeoTrust_Universal_CA.crt
OS10# crypto ca-cert install home://GeoTrust_Universal_CA.crt
Processing certificate ...
Installed Root CA certificate
CommonName = GeoTrust Universal CA
IssuerName = GeoTrust Universal CA
```

### 2. 生成 CSR，将 CSR 复制到 CA 服务器、下载签名的证书，并安装主机证书。

```
OS10# crypto cert generate request cert-file home://s4048-001-csr.pem
key-file home://tsr6-key.pem cname "Top of Rack 6" altname "IP:10.0.0.6
DNS:tor6.dell.com"
email admin@dell.com organization "Dell EMC" orgunit Networking locality "santa Clara"
state California country US length 1024
Processing certificate ...
Successfully created CSR file /home/admin/tor6-csr.pem and key

OS10# copy home://tor6-csr.pem scp://CAadmin:secret@172.11.222.1/s4048-001-csr.pem

OS10# copy scp://CAadmin:secret@172.11.222.1/s4048-001.crt usb://s4048-001-crt.pem

OS10# crypto cert install crt-file usb://s4048-001-crt.pem key-file usb://s4048-001-
crt.key
```

```
This will replace the already installed host certificate.
Do you want to proceed ? [yes/no(default)]:yes
Processing certificate ...
Host certificate installed successfully.
```

### 3. 配置 X.509v3 安全配置文件。

```
OS10# show crypto cert

Installed non-FIPS certificates
s4048-001-csr.pem

Installed FIPS certificates

OS10# config terminal
OS10(config)# crypto security-profile radius-admin
OS10(config-sec-profile)# certificate s4048-001-csr
OS10(config-sec-profile)# exit
```

### 4. 配置 RADIUS over TLS 服务器。

```
OS10# radius-server host 10.0.0.1 tls security-profile radius-admin key radsec
```

### 5. 配置基于 RADIUS 的用户身份验证。

```
OS10# aaa authentication login default group radius local
```

## OpenFlow

交换机在同一硬件中实施控制平面和数据平面。软件定义的网络 (SDN) 将软件 (控制平面) 与硬件 (数据平面) 分离。集中式 SDN 控制器将处理控制面流量以及数据平面流的硬件配置。

SDN 控制器是 SDN 的“大脑”。SDN 控制器使用北向应用程序编程接口 (API) 与业务逻辑应用程序和南向 API 通信，以设置受控制的网络设备，例如 OS10 交换机。

OpenFlow 是 SDN 的实施。OpenFlow 将启用可编程网络。您可以使用表述性状态转移 (REST) 或 JAVA API (北向 API)，以便为业务逻辑应用程序开发 SDN 控制器网络应用程序。SDN 控制器使用 OpenFlow 南向 API 与交换机进行通信，并从业务逻辑应用程序中中继信息。

SDN 的优势包括自定义、加快新功能的开发、更低的操作成本，并促进开放的多供应商环境。

OS10 支持 OpenFlow 协议版本 1.0 和 1.3。

OS10 支持仅 OpenFlow 模式。在此模式下，SDN 控制器将控制交换机的数据路径。OpenFlow 通道将处理所有数据包。

**注：**当交换机处于 OpenFlow 模式时，将禁用所有第二层 (L2) 和第 3 层 (L3) 协议。此外，链路层查找协议 (LLDP)、Dot1x 和虚拟链路中继 (VLT) 等链路级别协议也将被禁用。

**注：**不支持 OpenFlow 混合模式。

### 支持的平台

- S4048-ON
- S4048T-ON
- S4100-ON
- S4248FB-ON
- S4248FBL-ON
- S6010-ON
- Z9100-ON
- Z9264F-ON

**注：**S3048-ON 不受支持。

OS10 OpenFlow 实施将保留 VLAN 1 和 4095。

以下是 OS10 中的已知 OpenFlow 限制：

将交换机从 OpenFlow 模式转换回正常模式将移除所有 OpenFlow 配置。交换机将恢复到 Openflow 前的状态。在正常模式下指定的管理、接口 (最大传输单元 [MTU] 和 LLDP) 和身份验证、授权和核算 (AAA) 设置将被保留。

要在出厂默认模式下启动交换机，必须执行以下操作：

1. 使用 `delete startup-configuration` 命令删除启动配置。

2. 输入 `reload` 命令。

**注：**请勿使用 `no openflow` 或 `no mode openflow-only` 命令。

```
OS10# delete startup-configuration
OS10# reload
```

## OpenFlow 逻辑交换机实例

在仅 OpenFlow 模式下，您只能配置一个逻辑交换机实例。启用 OpenFlow 模式后，创建逻辑交换机实例。默认情况下，逻辑交换机实例处于禁用状态。启用逻辑交换机实例时，OpenFlow 应用程序将启动与配置的连接器的连接。

创建 OpenFlow 逻辑交换机实例时，所有物理接口都会自动添加到其中。

# OpenFlow 控制器

OS10 符合以下 SDN 控制器：

- RYU
- 开放式网络操作系统 (ONOS)

要与控制器建立连接，请在 OpenFlow 逻辑交换机实例中配置控制器和端口 ID 的 IPv4 地址。默认端口是 6653。您可以在 OOB 连接模式将控制器连接到交换机。但是，您可以使用 `in-band` 命令将任何前面板端口用作管理接口。带内端口将从 OpenFlow 交换机实例中移除，并且不受控制器控制。

管理端口 MTU 为 1532，带内端口 MTU 为 9216。

OpenFlow 使用传输控制协议 (TCP) 和传输层安全 (TLS) 协议进行通信。

如果 OpenFlow 交换机失去与控制器的连接，则交换机将立即进入故障安全模式。控制器安装的所有流程都会保留在交换机上。将根据您配置的硬或空闲超时来移除流条目。

## OpenFlow 版本 1.3

本部分提供了有关适用于 OS10 的 OpenFlow 版本 1.3 规格的信息。

### 端口

OpenFlow 交换机支持以下 OpenFlow 端口：

表. 58: 支持的端口类型

| 端口类型      | 支持  |
|-----------|-----|
| 物理端口      | 支持  |
| 逻辑端口      | 不支持 |
| 保留的端口     |     |
| (必需) 所有   | 支持  |
| (必需) 控制器  | 支持  |
| (必需) 表    | 不支持 |
| (必需) 输入端口 | 不支持 |
| (必需) 任何   | 支持  |
| (可选) 本地   | 不支持 |
| (可选) 正常   | 不支持 |
| (可选) 泛洪   | 不支持 |

### 流表

OpenFlow 流表包含流条目。每个流表条目均包含以下字段：

表. 59: 支持的字段

| 字段           | 支持 |
|--------------|----|
| match_fields | 支持 |
| priority     | 支持 |
| counters     | 支持 |
| instructions | 支持 |



表. 59: 支持的字段 （续）

| 字段       | 支持  |
|----------|-----|
| timeouts | 支持  |
| cookie   | 不支持 |

组表

不支持

计量表

不支持

指令

每个流条目都包含一组在数据包与条目匹配时执行的指令。

表. 60: 支持的指令

| 指令                            | 支持  |
|-------------------------------|-----|
| (可选) Meter 计量器 id             | 不支持 |
| (可选) Apply-Actions 操作         | 支持  |
| (可选) Clear-Actions            | 不支持 |
| (必需) Write-Actions 操作         | 支持  |
| (可选) 写入元数据/掩码                 | 不支持 |
| (可选) Goto-table next-table-id | 不支持 |

操作集

操作集将与每个数据包关联。

表. 61: 支持的操作集

| 操作集       | 支持       |
|-----------|----------|
| 向内复制 TTL  | 不支持      |
| pop       | 不支持      |
| push-MPLS | 不支持      |
| push-VLAN | 不支持      |
| 向外复制 TTL  | 不支持      |
| 减量 TTL    | 不支持      |
| set       | 支持（可选字段） |
| qos       | 不支持      |
| 组         | 不支持      |
| output    | 支持       |

# 操作类型

一种操作类型将与每个数据包关联。

表. 62: 支持的操作类型

| 操作类型      | 支持                                                                                                                                                  |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 输出        | 支持                                                                                                                                                  |
| 设置队列      | 不支持                                                                                                                                                 |
| 丢弃        | 支持                                                                                                                                                  |
| 组         | 不支持                                                                                                                                                 |
| 推送标签/弹出标签 | 不支持                                                                                                                                                 |
| 设置字段      | 部分支持 <ul style="list-style-type: none"><li>源 MAC — 支持</li><li>目标 MAC — 支持</li><li>VLAN ID — 支持</li><li>VLAN PCP — 支持</li><li>IP DSCP — 支持</li></ul> |
| 更改 — TTL  | 不支持                                                                                                                                                 |

# 计数器

计数器用于统计目的。

表. 63: 支持的计数器

| 必需/可选         | 计数器         | 位  | 支持  |
|---------------|-------------|----|-----|
| 每个流表          |             |    |     |
| Required (必需) | 引用计数 (活动条目) | 32 | 支持  |
| 可选            | 数据包查找       | 64 | 支持  |
| 可选            | 数据包匹配       | 64 | 支持  |
| 每个流条目         |             |    |     |
| 可选            | 接收的数据包      | 64 | 支持  |
| 可选            | 接收的字节数      | 64 | 支持  |
| Required (必需) | 持续时间 (秒)    | 32 | 支持  |
| 可选            | 持续时间 (毫微秒)  | 32 | 支持  |
| 每个端口          |             |    |     |
| Required (必需) | 接收的数据包      | 64 | 支持  |
| Required (必需) | 传输的数据包      | 64 | 支持  |
| 可选            | 接收的字节数      | 64 | 支持  |
| 可选            | 传输的字节数      | 64 | 支持  |
| 可选            | 接收丢弃        | 64 | 不支持 |
| 可选            | 发送丢弃        | 64 | 不支持 |
| 可选            | 接收错误        | 64 | 支持  |
| 可选            | 传输错误        | 64 | 支持  |

表. 63: 支持的计数器 (续)

| 必需/可选         | 计数器        | 位  | 支持  |
|---------------|------------|----|-----|
| 可选            | 接收帧对齐错误    | 64 | 不支持 |
| 可选            | 接收超限错误     | 64 | 不支持 |
| 可选            | 接收 CRC 错误  | 64 | 支持  |
| 可选            | 冲突         | 64 | 支持  |
| Required (必需) | 持续时间 (秒)   | 32 | 不支持 |
| 可选            | 持续时间 (毫微秒) | 32 | 不支持 |
| <b>每个队列</b>   |            |    |     |
| Required (必需) | 传输数据包      | 64 | 不支持 |
| 可选            | 传输字节数      | 64 | 不支持 |
| 可选            | 传输超限错误     | 64 | 不支持 |
| Required (必需) | 持续时间 (秒)   | 32 | 不支持 |
| 可选            | 持续时间 (毫微秒) | 32 | 不支持 |
| <b>每组</b>     |            |    |     |
| 可选            | 引用计数 (流条目) | 32 | 不支持 |
| 可选            | 数据包计数      | 64 | 不支持 |
| 可选            | 字节计数       | 64 | 不支持 |
| Required (必需) | 持续时间 (秒)   | 32 | 不支持 |
| 可选            | 持续时间 (毫微秒) | 32 | 不支持 |
| <b>每组存储区</b>  |            |    |     |
| 可选            | 数据包计数      | 64 | 不支持 |
| 可选            | 字节计数       | 64 | 不支持 |
| <b>每个计量器</b>  |            |    |     |
| 可选            | 流计数        | 32 | 不支持 |
| 可选            | 输入数据包计数    | 64 | 不支持 |
| 可选            | 输入字节计数     | 64 | 不支持 |
| Required (必需) | 持续时间 (秒)   | 32 | 不支持 |
| 可选            | 持续时间 (毫微秒) | 32 | 不支持 |
| <b>每个仪表频带</b> |            |    |     |
| 可选            | 带内数据包计数    | 64 | 不支持 |
| 可选            | 带内字节计数     | 64 | 不支持 |

## OpenFlow 协议

OpenFlow 协议支持三种消息类型，每种类型都有多个子类型：

- 控制器到交换机
- 异步
- 对称

### 控制器到交换机

**表. 64: 支持的控制器到交换机类型**

| 控制器到交换机的类型 | 支持/不支持 |
|------------|--------|
| 功能请求       | 支持     |
| 配置 get     | 支持     |
| 配置 set     | 支持     |
| 修改状态       | 支持     |
| 读取状态       | 支持     |
| 数据包输出      | 支持     |
| 界线         | 支持     |
| 角色-请求      | 支持     |

## 异步

**表. 65: 支持的异步类型**

| 异步类型  | 支持/不支持 |
|-------|--------|
| 数据包输入 | 支持     |
| 流已移除  | 支持     |
| 端口状态  | 支持     |
| 错误    | 支持     |

## 对称

**表. 66: 支持的对称类型**

| 对称类型 | 支持/不支持 |
|------|--------|
| 问候   | 支持     |
| 回音   | 支持     |
| 试验者  | 不支持    |

## 连接设置 TCP

**表. 67: 支持的模式**

| 模式      | 支持/不支持                                                                                  |
|---------|-----------------------------------------------------------------------------------------|
| 连接中断    | <ul style="list-style-type: none"> <li>故障-安全-模式 — 支持</li> <li>故障—独立-模式 — 不支持</li> </ul> |
| TLS 加密  | 支持                                                                                      |
| 多个控制器   | 不支持                                                                                     |
| 辅助连接    | 不支持                                                                                     |
| 逻辑交换机数量 | 一声                                                                                      |

## 支持的控制器

REST APIs on

- RYU
- ONOS

## 流表修改消息

表. 68: 支持的消息

| 流表修改消息                | 支持/不支持 |
|-----------------------|--------|
| OFPPC_ADD=0           | 支持     |
| OFPPC_MODIFY=1        | 支持     |
| OFPPC_MODIFY_STRICT=2 | 支持     |
| OFPPC_DELETE=3        | 支持     |
| OFPPC_DELETE_STRICT=4 | 支持     |

## 消息类型

表. 69: 支持的消息类型

| 消息类型        | 信息                               | 支持  |
|-------------|----------------------------------|-----|
| 不可变消息       | OFPT_HELLO=0                     | 支持  |
|             | OFPT_ERROR=1                     | 支持  |
|             | OFPT_ECHO_REQUEST=2              | 支持  |
|             | OFPT_ECHO_REPLY=3                | 支持  |
| 交换机配置消息     | OFPT_FEATURES_REQUEST=5          | 支持  |
|             | OFPT_FEATURES_REPLY=6            | 支持  |
|             | OFPT_GET_CONFIG_REQUEST=7        | 支持  |
|             | OFPT_GET_CONFIG_REPLY=8          | 支持  |
|             | OFPT_SET_CONFIG=9                | 支持  |
| 异步消息        | OFPT_PACKET_IN=10                | 支持  |
|             | OFPT_FLOW_REMOVED=11             | 支持  |
|             | OFPT_PORT_STATUS=12              | 支持  |
| 控制器命令消息     | OFPT_PACKET_OUT=13               | 支持  |
|             | OFPT_FLOW_MOD=14                 | 支持  |
|             | OFPT_GROUP_MOD=15                | 不支持 |
|             | OFPT_PORT_MOD=16                 | 支持  |
|             | OFPT_TABLE_MOD=17                | 不支持 |
| 多部分消息       | OFPT_MULTIPART_REQUEST=18        | 支持  |
|             | OFPT_MULTIPART_REPLY=19          | 支持  |
| 屏障消息        | OFPT_BARRIER_REQUEST=20          | 支持  |
|             | OFPT_BARRIER_REPLY=21            | 支持  |
| 队列配置消息      | OFPT_QUEUE_GET_CONFIG_REQUEST=22 | 不支持 |
|             | OFPT_QUEUE_GET_CONFIG_REPLY=23   | 不支持 |
| 控制器角色更改请求消息 | OFPT_ROLE_REQUEST=24             | 不支持 |

表. 69: 支持的消息类型 (续)

| 消息类型          | 信息                        | 支持  |
|---------------|---------------------------|-----|
|               | OFPT_ROLE_REPLY=25        | 不支持 |
| 异步消息配置        | OFPT_GET_ASYNC_REQUEST=26 | 不支持 |
|               | OFPT_GET_ASYNC_REPLY=27   | 不支持 |
|               | OFPT_SET_ASYNC=28         | 不支持 |
| 计量器和速率限值器配置消息 | OFPT_METER_MOD=29         | 不支持 |

## 流匹配字段

表. 70: 支持的字段

| 流匹配字段                       | 支持/不支持 |
|-----------------------------|--------|
| OFPXMT_OFB_IN_PORT = 0      | 支持     |
| OFPXMT_OFB_IN_PHY_PORT = 1  | 不支持    |
| OFPXMT_OFB_METADATA = 2     | 不支持    |
| OFPXMT_OFB_ETH_DST = 3      | 支持     |
| OFPXMT_OFB_ETH_SRC = 4      | 支持     |
| OFPXMT_OFB_ETH_TYPE = 5     | 支持     |
| OFPXMT_OFB_VLAN_VID = 6     | 支持     |
| OFPXMT_OFB_VLAN_PCP = 7     | 支持     |
| OFPXMT_OFB_IP_DSCP = 8      | 支持     |
| OFPXMT_OFB_IP_ECN = 9       | 支持     |
| OFPXMT_OFB_IP_PROTO = 10    | 支持     |
| OFPXMT_OFB_IPV4_SRC = 11    | 支持     |
| OFPXMT_OFB_IPV4_DST = 12    | 支持     |
| OFPXMT_OFB_TCP_SRC = 13     | 支持     |
| OFPXMT_OFB_TCP_DST = 14     | 支持     |
| OFPXMT_OFB_UDP_SRC = 15     | 支持     |
| OFPXMT_OFB_UDP_DST = 16     | 支持     |
| OFPXMT_OFB_SCTP_SRC = 17    | 不支持    |
| OFPXMT_OFB_SCTP_DST = 18    | 不支持    |
| OFPXMT_OFB_ICMPV4_TYPE = 19 | 支持     |
| OFPXMT_OFB_ICMPV4_CODE = 20 | 支持     |

**表. 70: 支持的字段 (续)**

| 流匹配字段                          | 支持/不支持 |
|--------------------------------|--------|
| OFPXMT_OFB_ARP_OP = 21         | 不支持    |
| OFPXMT_OFB_ARP_SPA = 22        | 不支持    |
| OFPXMT_OFB_ARP_TPA = 23        | 不支持    |
| OFPXMT_OFB_ARP_SHA = 24        | 不支持    |
| OFPXMT_OFB_ARP_THA = 25        | 不支持    |
| OFPXMT_OFB_IPV6_SRC = 26       | 不支持    |
| OFPXMT_OFB_IPV6_DST = 27       | 不支持    |
| OFPXMT_OFB_IPV6_FLABEL = 28    | 不支持    |
| OFPXMT_OFB_ICMPV6_TYPE = 29    | 不支持    |
| OFPXMT_OFB_ICMPV6_CODE = 30    | 不支持    |
| OFPXMT_OFB_IPV6_ND_TARGET = 31 | 不支持    |
| OFPXMT_OFB_IPV6_ND_SLL = 32    | 不支持    |
| OFPXMT_OFB_IPV6_ND_TLL = 33    | 不支持    |
| OFPXMT_OFB_MPLS_LABEL = 34     | 不支持    |
| OFPXMT_OFB_MPLS_TC = 35        | 不支持    |
| OFPXMT_OFB_MPLS_BOS = 36       | 不支持    |
| OFPXMT_OFB_PBB_ISID = 37       | 不支持    |
| OFPXMT_OFB_TUNNEL_ID = 38      | 不支持    |
| OFPXMT_OFB_IPV6_EXTHDR = 39    | 不支持    |

## 操作结构

**表. 71: 支持的操作结构**

| 操作结构                    | 支持/不支持 |
|-------------------------|--------|
| OFPAT_OUTPUT = 0        | 支持     |
| OFPAT_COPY_TTL_OUT = 11 | 不支持    |
| OFPAT_COPY_TTL_IN = 12  | 不支持    |
| OFPAT_SET_MPLS_TTL = 15 | 不支持    |
| OFPAT_DEC_MPLS_TTL = 16 | 不支持    |
| OFPAT_PUSH_VLAN = 17    | 不支持    |
| OFPAT_POP_VLAN = 18     | 不支持    |

表. 71: 支持的操作结构 (续)

| 操作结构                  | 支持/不支持 |
|-----------------------|--------|
| OFPAT_PUSH_MPLS = 19  | 不支持    |
| OFPAT_POP_MPLS = 20   | 不支持    |
| OFPAT_SET_QUEUE = 21  | 不支持    |
| OFPAT_GROUP = 22      | 不支持    |
| OFPAT_SET_NW_TTL = 23 | 不支持    |
| OFPAT_DEC_NW_TTL = 24 | 不支持    |
| OFPAT_SET_FIELD = 25  | 支持     |
| OFPAT_PUSH_PBB = 26   | 不支持    |
| OFPAT_POP_PBB = 27    | 不支持    |

## 数据路径支持的功能

表. 72: 支持的功能

| 功能                         | 支持/不支持 |
|----------------------------|--------|
| OFPC_FLOW_STATS = 1 << 0   | 支持     |
| OFPC_TABLE_STATS = 1 << 1  | 不支持    |
| OFPC_PORT_STATS = 1 << 2   | 支持     |
| OFPC_GROUP_STATS = 1 << 3  | 不支持    |
| OFPC_IP_REASM = 1 << 5     | 不支持    |
| OFPC_QUEUE_STATS = 1 << 6  | 不支持    |
| OFPC_PORT_BLOCKED = 1 << 8 | 不支持    |

## 多部分消息类型

表. 73: 支持的消息类型

| 消息类型说明            | 请求/回复正文                                                                                                                        | 信息                   | 支持 |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------|----------------------|----|
| 此 OpenFlow 交换机的说明 | <ul style="list-style-type: none"> <li>请求正文为空</li> <li>回复正文是 struct ofp_desc</li> </ul>                                        | OFPMPP_DESC = 0      | 支持 |
| 单个流统计信息           | <ul style="list-style-type: none"> <li>请求正文是 struct ofp_flow_stats_request</li> <li>回复正文是 struct ofp_flow_stats 的阵列</li> </ul> | OFPMPP_FLOW = 1      | 支持 |
| 聚合流统计信息           | <ul style="list-style-type: none"> <li>请求正文是 struct ofp_aggregate_stats_request</li> </ul>                                     | OFPMPP_AGGREGATE = 2 | 支持 |



表. 73: 支持的消息类型 (续)

| 消息类型说明                  | 请求/回复正文                                                                                                                                                                            | 信息                        | 支持  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-----|
|                         | <ul style="list-style-type: none"> <li>回复正文是 struct ofp_aggregate_stats_reply</li> </ul>                                                                                           |                           |     |
| 流表统计信息                  | <ul style="list-style-type: none"> <li>请求正文为空</li> <li>回复正文是 struct ofp_table_stats 的阵列</li> </ul>                                                                                 | OFPMP_TABLE = 3           | 支持  |
| 端口统计信息                  | <ul style="list-style-type: none"> <li>请求正文是 struct ofp_port_stats_request</li> <li>回复正文是 struct ofp_port_stats 的阵列</li> </ul>                                                     | OFPMP_PORT_STATS = 4      | 支持  |
| 端口的队列统计信息               | <ul style="list-style-type: none"> <li>请求正文是 struct ofp_queue_stats_request</li> <li>回复正文是 struct ofp_queue_stats 的阵列</li> </ul>                                                   | OFPMP_QUEUE = 5           | 不支持 |
| 组计数器统计信息                | <ul style="list-style-type: none"> <li>请求正文是 struct ofp_group_stats_request</li> <li>回复是 struct ofp_group_stats 的阵列</li> </ul>                                                     | OFPMP_GROUP = 6           | 不支持 |
| 组说明                     | <ul style="list-style-type: none"> <li>请求正文为空</li> <li>回复正文是 struct ofp_group_desc_stats 的阵列</li> </ul>                                                                            | OFPMP_GROUP_DESC = 7      | 不支持 |
| 组功能                     | <ul style="list-style-type: none"> <li>请求正文为空</li> <li>回复正文是 struct ofp_group_features</li> </ul>                                                                                  | OFPMP_GROUP_FEATURES = 8  | 不支持 |
| 计量器统计信息                 | <ul style="list-style-type: none"> <li>请求正文是 struct ofp_meter_multipart_requests</li> <li>回复正文是 struct ofp_meter_stats 的阵列</li> </ul>                                              | OFPMP_METER = 9           | 不支持 |
| 计量器配置                   | <ul style="list-style-type: none"> <li>请求正文是 struct ofp_meter_multipart_requests</li> <li>回复正文是 struct ofp_meter_config 的阵列</li> </ul>                                             | OFPMP_METER_CONFIG = 10   | 不支持 |
| 计量器功能                   | <ul style="list-style-type: none"> <li>请求正文为空</li> <li>回复正文是 struct ofp_meter_features</li> </ul>                                                                                  | OFPMP_METER_FEATURES = 11 | 不支持 |
| 表功能                     | <ul style="list-style-type: none"> <li>请求正文为空或包含 struct ofp_table_features 的阵列, 其中包括控制器所需的交换机视图。<br/>如果交换机无法设置指定的视图, 将返回错误</li> <li>回复正文是 struct ofp_table_features 的阵列</li> </ul> | OFPMP_TABLE_FEATURES = 12 | 支持  |
| Port description (端口说明) | <ul style="list-style-type: none"> <li>请求正文为空</li> <li>回复正文是 struct ofp_port 的阵列</li> </ul>                                                                                        | OFPMP_PORT_DESC = 13      | 支持  |

## 交换机说明

OFPMPL\_DESC 多部分请求类型包括有关交换机制造商、硬件版本、软件版本、序列号和说明的信息。

表. 74: 支持的说明

| 交换机说明                           | 支持/不支持 |
|---------------------------------|--------|
| char mfr_desc[DESC_STR_LEN]     | 支持     |
| char hw_desc[DESC_STR_LEN]      | 支持     |
| char sw_desc[DESC_STR_LEN]      | 支持     |
| char serial_num[SERIAL_NUM_LEN] | 支持     |
| char dp_desc[DESC_STR_LEN]      | 支持     |

## 属性类型

表. 75: 支持的属性

| 属性类型                             | 支持/不支持 |
|----------------------------------|--------|
| OFPTFPT_INSTRUCTIONS = 0         | 支持     |
| OFPTFPT_INSTRUCTIONS_MISS = 1    | 不支持    |
| OFPTFPT_NEXT_TABLES = 2          | 不支持    |
| OFPTFPT_NEXT_TABLES_MISS = 3     | 不支持    |
| OFPTFPT_WRITE_ACTIONS = 4        | 支持     |
| OFPTFPT_WRITE_ACTIONS_MISS = 5   | 不支持    |
| OFPTFPT_APPLY_ACTIONS = 6        | 支持     |
| OFPTFPT_APPLY_ACTIONS_MISS = 7   | 不支持    |
| OFPTFPT_MATCH = 8                | 支持     |
| OFPTFPT_WILDCARDS = 10           | 支持     |
| OFPTFPT_WRITE_SETFIELD = 12      | 支持     |
| OFPTFPT_WRITE_SETFIELD_MISS = 13 | 不支持    |
| OFPTFPT_APPLY_SETFIELD = 14      | 支持     |
| OFPTFPT_APPLY_SETFIELD_MISS = 15 | 不支持    |

## 组配置

表. 76: 支持的配置

| 组配置                             | 支持/不支持 |
|---------------------------------|--------|
| OFPGFC_SELECT_WEIGHT = 1 << 0   | 不支持    |
| OFPGFC_SELECT_LIVENESS = 1 << 1 | 不支持    |
| OFPGFC_CHAINING = 1 << 2        | 不支持    |
| OFPGFC_CHAINING_CHECKS = 1 << 3 | 不支持    |

## 控制器角色

表. 77: 支持的控制器角色

| 控制器角色                   | 支持/不支持 |
|-------------------------|--------|
| OFPCR_ROLE_NOCHANGE = 0 | 不支持    |
| OFPCR_ROLE_EQUAL = 1    | 支持     |
| OFPCR_ROLE_MASTER = 2   | 支持     |
| OFPCR_ROLE_SLAVE = 3    | 不支持    |

## 数据包内原因

表. 78: 支持的原因

| 数据包内原因               | 支持/不支持 |
|----------------------|--------|
| OFPR_NO_MATCH = 0    | 支持     |
| OFPR_ACTION = 1      | 支持     |
| OFPR_INVALID_TTL = 2 | 不支持    |

## 流移除原因

表. 79: 支持的原因

| 流移除原因                  | 支持/不支持 |
|------------------------|--------|
| OFPRR_IDLE_TIMEOUT = 0 | 支持     |
| OFPRR_HARD_TIMEOUT = 1 | 支持     |
| OFPRR_DELETE = 2       | 支持     |
| OFPRR_GROUP_DELETE = 3 | 不支持    |

## 从交换机到控制器的错误类型

表. 80: 支持的错误类型

| 错误类型                       | 支持/不支持 |
|----------------------------|--------|
| OFPET_HELLO_FAILED = 0     | 支持     |
| OFPET_BAD_REQUEST = 1      | 支持     |
| OFPET_BAD_ACTION = 2       | 支持     |
| OFPET_BAD_INSTRUCTION = 3  | 支持     |
| OFPET_BAD_MATCH = 4        | 支持     |
| OFPET_FLOW_MOD_FAILED = 5  | 支持     |
| OFPET_GROUP_MOD_FAILED = 6 | 不支持    |

**表. 80: 支持的错误类型 (续)**

| 错误类型                                  | 支持/不支持 |
|---------------------------------------|--------|
| OFFPET_PORT_MOD_FAILED = 7            | 支持     |
| OFFPET_TABLE_MOD_FAILED = 8           | 不支持    |
| OFFPET_QUEUE_OP_FAILED = 9            | 不支持    |
| OFFPET_SWITCH_CONFIG_FAILED = 10      | 不支持    |
| OFFPET_ROLE_REQUEST_FAILED = 11       | 不支持    |
| OFFPET_METER_MOD_FAILED = 12          | 不支持    |
| OFFPET_TABLE_FEATURES_FAILED = 13     | 不支持    |
| <b>错误的请求代码</b>                        |        |
| OFFBRC_BAD_VERSION = 0                | 支持     |
| OFFBRC_BAD_TYPE = 1                   | 支持     |
| OFFBRC_BAD_MULTIPART = 2              | 不支持    |
| OFFBRC_BAD_EXPERIMENTER = 3           | 不支持    |
| OFFBRC_BAD_EXP_TYPE = 4               | 不支持    |
| OFFBRC_EPERM = 5                      | 不支持    |
| OFFBRC_BAD_LEN = 6                    | 支持     |
| OFFBRC_BUFFER_EMPTY = 7               | 不支持    |
| OFFBRC_BUFFER_UNKNOWN = 8             | 不支持    |
| OFFBRC_BAD_TABLE_ID = 9               | 支持     |
| OFFBRC_IS_SLAVE = 10                  | 不支持    |
| OFFBRC_BAD_PORT = 11                  | 支持     |
| OFFBRC_BAD_PACKET = 12                | 不支持    |
| OFFBRC_MULTIPART_BUFFER_OVERFLOW = 13 | 不支持    |
| <b>错误的操作代码</b>                        |        |
| OFFBAC_BAD_TYPE = 0                   | 支持     |
| OFFBAC_BAD_LEN = 1                    | 支持     |
| OFFBAC_BAD_EXPERIMENTER = 2           | 不支持    |
| OFFBAC_BAD_EXP_TYPE = 3               | 不支持    |
| OFFBAC_BAD_OUT_PORT = 4               | 支持     |
| OFFBAC_BAD_ARGUMENT = 5               | 支持     |

**表. 80: 支持的错误类型 (续)**

| 错误类型                           | 支持/不支持 |
|--------------------------------|--------|
| OFPBAC_EPERM = 6               | 不支持    |
| OFPBAC_TOO_MANY = 7            | 支持     |
| OFPBAC_BAD_QUEUE = 8           | 不支持    |
| OFPBAC_BAD_OUT_GROUP = 9       | 不支持    |
| OFPBAC_MATCH_INCONSISTENT = 10 | 不支持    |
| OFPBAC_UNSUPPORTED_ORDER = 11  | 不支持    |
| OFPBAC_BAD_TAG = 12            | 不支持    |
| OFPBAC_BAD_SET_TYPE = 13       | 不支持    |
| OFPBAC_BAD_SET_LEN = 14        | 不支持    |
| OFPBAC_BAD_SET_ARGUMENT = 15   | 支持     |
| <b>错误的指令代码</b>                 |        |
| OFPBIC_UNKNOWN_INST = 0        | 不支持    |
| OFPBIC_UNSUP_INST = 1          | 不支持    |
| OFPBIC_BAD_TABLE_ID = 2        | 不支持    |
| OFPBIC_UNSUP_METADATA = 3      | 不支持    |
| OFPBIC_UNSUP_METADATA_MASK = 4 | 不支持    |
| OFPBIC_BAD_EXPERIMENTER = 5    | 不支持    |
| OFPBIC_BAD_EXP_TYPE = 6        | 不支持    |
| OFPBIC_BAD_LEN = 7             | 不支持    |
| OFPBIC_EPERM = 8               | 不支持    |
| <b>错误的匹配代码</b>                 |        |
| OFPBMC_BAD_TYPE = 0            | 不支持    |
| OFPBMC_BAD_LEN = 1             | 不支持    |
| OFPBMC_BAD_TAG = 2             | 不支持    |
| OFPBMC_BAD_DL_ADDR_MASK = 3    | 不支持    |
| OFPBMC_BAD_NW_ADDR_MASK = 4    | 不支持    |
| OFPBMC_BAD_WILDCARDS = 5       | 不支持    |
| OFPBMC_BAD_FIELD = 6           | 不支持    |
| OFPBMC_BAD_VALUE = 7           | 不支持    |

**表. 80: 支持的错误类型 (续)**

| 错误类型                             | 支持/不支持 |
|----------------------------------|--------|
| OFPBMC_BAD_MASK = 8              | 不支持    |
| OFPBMC_BAD_PREREQ = 9            | 不支持    |
| OFPBMC_DUP_FIELD = 10            | 不支持    |
| OFPBMC_EPERM = 11                | 不支持    |
| <b>流修改失败的代码</b>                  |        |
| OFPFMFC_UNKNOWN = 0              | 支持     |
| OFPFMFC_TABLE_FULL = 1           | 支持     |
| OFPFMFC_BAD_TABLE_ID = 2         | 支持     |
| OFPFMFC_OVERLAP = 3              | 支持     |
| OFPFMFC_EPERM = 4                | 不支持    |
| OFPFMFC_BAD_TIMEOUT = 5          | 不支持    |
| OFPFMFC_BAD_COMMAND = 6          | 支持     |
| OFPFMFC_BAD_FLAGS = 7            | 不支持    |
| <b>组修改失败的代码</b>                  |        |
| OFPGMFC_GROUP_EXISTS = 0         | 不支持    |
| OFPGMFC_INVALID_GROUP = 1        | 不支持    |
| OFPGMFC_WEIGHT_UNSUPPORTED = 2   | 不支持    |
| OFPGMFC_OUT_OF_GROUPS = 3        | 不支持    |
| OFPGMFC_OUT_OF_BUCKETS = 4       | 不支持    |
| OFPGMFC_CHAINING_UNSUPPORTED = 5 | 不支持    |
| OFPGMFC_WATCH_UNSUPPORTED = 6    | 不支持    |
| OFPGMFC_LOOP = 7                 | 不支持    |
| OFPGMFC_UNKNOWN_GROUP = 8        | 不支持    |
| OFPGMFC_CHAINED_GROUP = 9        | 不支持    |
| OFPGMFC_BAD_TYPE = 10            | 不支持    |
| OFPGMFC_BAD_COMMAND = 11         | 不支持    |
| OFPGMFC_BAD_BUCKET = 12          | 不支持    |
| OFPGMFC_BAD_WATCH = 13           | 不支持    |
| OFPGMFC_EPERM = 14               | 不支持    |

表. 80: 支持的错误类型 (续)

| 错误类型                      | 支持/不支持 |
|---------------------------|--------|
| <b>端口修改失败的代码</b>          |        |
| OFPPMFC_BAD_PORT = 0      | 支持     |
| OFPPMFC_BAD_HW_ADDR = 1   | 支持     |
| OFPPMFC_BAD_CONFIG = 2    | 不支持    |
| OFPPMFC_BAD_ADVERTISE = 3 | 不支持    |
| OFPPMFC_EPERM = 4         | 不支持    |
| <b>表修改失败的代码</b>           |        |
| OFPTMFC_BAD_TABLE = 0     | 支持     |
| OFPTMFC_BAD_CONFIG = 1    | 不支持    |
| OFPTMFC_EPERM = 2         | 不支持    |
| <b>队列操作失败的代码</b>          |        |
| OFPQOFC_BAD_PORT = 0      | 支持     |
| OFPQOFC_BAD_QUEUE = 1     | 不支持    |
| OFPQOFC_EPERM = 2         | 不支持    |
| <b>交换机配置失败的代码</b>         |        |
| OFPSCFC_BAD_FLAGS = 0     | 不支持    |
| OFPSCFC_BAD_LEN = 1       | 不支持    |
| OFPSCFC_EPERM = 2         | 不支持    |
| <b>角色请求失败的代码</b>          |        |
| OFPRRFC_STALE = 0         | 不支持    |
| OFPRRFC_UNSUP = 1         | 不支持    |
| OFPRRFC_BAD_ROLE = 2      | 不支持    |
| <b>表功能失败的代码</b>           |        |
| OFPTFFC_BAD_TABLE = 0     | 支持     |
| OFPTFFC_BAD_METADATA = 1  | 不支持    |
| OFPTFFC_BAD_TYPE = 2      | 不支持    |
| OFPTFFC_BAD_LEN = 3       | 不支持    |

表. 80: 支持的错误类型 (续)

| 错误类型                     | 支持/不支持 |
|--------------------------|--------|
| OFPTFFC_BAD_ARGUMENT = 4 | 不支持    |
| OFPTFFC_EPERM = 5        | 不支持    |

## OpenFlow 使用案例

通过 OS10 OpenFlow 协议支持，可以灵活地使用供应商中立的应用程序和使用您创建的应用程序。例如，OS10 OpenFlow 实施支持类似于以下 web 站点中所示的 L2 应用程序：

- <https://github.com/osrg/ryu/tree/master/ryu/app> (仅支持 L2 应用程序)
- <https://github.com/osrg/ryu/tree/master/ryu/app>

**注：**OS10 支持基于 OpenFlow 版本 1.0 和 1.3 的应用程序。

- **卸下环路交换**

请考虑单个广播域的情况，其中的环路交换很常见。发生此问题的原因是 L2 网络中的冗余路径。

环路交换会创建具有广播的广播风暴，并将多播从每个交换机端口转发出去。网络中的每个交换机重复重新广播邮件，并充斥整个网络。

为了解决 OpenFlow 网络中的广播风暴，集中式控制器可做出所有控制平面决策并管理交换机。控制器拥有拓扑的完整视图。MAC 地址学习是集中式的。OpenFlow 将标识正确的路径并将数据包转发到相关的交换机，从而避免环路交换。

- **反应性流安装**

对于双向流量，请考虑动态学习流的情况。当数据包到达时，流将学习。

通过在 OpenFlow 网络中进行动态学习，OpenFlow 交换机将接收与流表条目不匹配的数据包，并将数据包发送到 SDN 控制器以进行处理。控制器将标识数据包必须遍历的路径，并使用新条目更新流表。控制器还将确定流表条目的缓存时间。

## 配置 OpenFlow

当您将交换机从正常模式转换为 OpenFlow 模式时，交换机将保留管理、接口和 AAA 设置。

**注：**确保交换机和控制器之间的 IP 连接。

下面列出了在 OpenFlow 控制器和逻辑交换机实例之间建立连接所需的最低配置：

1. 进入 OPENFLOW 配置模式。

```
OS10# configure terminal
OS10 (config)# openflow
OS10 (config-openflow)#
```

2. 启用仅 OpenFlow 模式。

```
OS10 (config-openflow)# mode openflow-only
```

重新加载交换机。输入 yes 以启用仅 OpenFlow 模式。

**注：**在 OpenFlow 模式下启动交换机时，它会禁用所有第 2 层 (L2) 和第 3 层 (L3) 协议。许多 CLI 命令在仅 OpenFlow 模式下不可用。有关仅 OpenFlow 模式的可用命令的列表，请参阅[仅 OpenFlow 模式命令](#)。

3. 配置逻辑交换机实例。

a. 选项 1；对于带外 (OOB) 管理：

- i. 配置管理端口的 IP 地址。确保交换机和控制器之间存在 IP 连接。

```
OS10# configure terminal
OS10 (config)# interface management 1/1/1
OS10 (conf-if-ma-1/1/1)# ip address 11.1.1.1/24
```



```
OS10 (conf-if-ma-1/1/1)# no shutdown
OS10 (conf-if-ma-1/1/1)# exit
```

ii. 配置逻辑交换机实例 *of-switch-1*。

```
OS10# configure terminal
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
```

b. 选项 2; 对于带内管理:

i. 将其中一个前面板端口配置为管理端口。

```
OS10# configure terminal
OS10 (config)# openflow
OS10 (config-openflow)# in-band-mgmt interface ethernet 1/1/1
OS10 (config-openflow)#
```

ii. 配置前面板管理端口上的 IPv4 地址。

```
OS10# configure terminal
OS10 (config)# interface ethernet 1/1/1
OS10 (conf-if-eth1/1/1)# ip address 11.1.1.1/24
OS10 (conf-if-eth1/1/1)# no shutdown
```

iii. 配置逻辑交换机实例 *of-switch-1*。

```
OS10# configure terminal
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
```

4. 使用 IPv4 或 IPv6 地址配置一个或多个 OpenFlow 控制器，以与逻辑交换机实例建立连接。您可以配置最多八个 OpenFlow 控制器。

```
OS10 (config-openflow-switch)# controller ipv4 ip-address port port-id
OS10 (config-openflow-switch)# controller ipv6 ipv6-address port port-id
```

```
OS10 (config-openflow-switch)# controller ipv4 10.1.1.1 port 6633
OS10 (config-openflow-switch)# controller ipv4 10.1.1.8 port 6633
OS10 (config-openflow-switch)# controller ipv4 10.1.1.12 port 6633
OS10 (config-openflow-switch)# controller ipv4 10.1.2.17 port 6633
OS10 (config-openflow-switch)# controller ipv4 10.1.23.12 port 6633
OS10 (config-openflow-switch)# controller ipv4 10.1.99.121 port 6633
OS10 (config-openflow-switch)# controller ipv6 2025::1 port 6633
OS10 (config-openflow-switch)# controller ipv6 2025::12 port 6633
```

IP 或 IPv6 地址用于控制器，端口 6633 用于 OpenFlow 通信。

5. 输入 `no shutdown` 命令以启用逻辑交换机实例。

```
OS10 (config-openflow-switch) no shutdown
```

## 建立 TLS 连接

- 从支持公钥基础设施 (PKI) 的服务器生成交换机和控制器证书。您需要以下证书：
  - 控制器证书
  - 交换机证书
  - 用于验证交换机证书的私钥文件
- 证书和私钥文件必须采用隐私增强邮件 (PEM) 格式。

对于基于证书的身份验证，您必须先在交换机和控制器之间建立 TLS 连接，然后才能在交换机上配置 OpenFlow。以下步骤说明了如何在 OS10 交换机上安装控制器和交换机证书。请参阅控制器说明文件以了解有关如何在控制器上安装证书的信息。

**① 注：**此步骤是可选的。如果您想要在交换机和控制器之间配置基于证书的身份验证，请使用此过程。

1. 使用管理员凭据登录到 OS10 交换机。
2. 输入以下命令以将证书复制到 OS10 交换机。

在以下命令中，OS10 交换机上的目标路径和目标文件名（例如 `config://../openflow/cacert.pem`）在部署中保持不变。确保输入以下示例中指定的目标路径和目标文件名称：

```
OS10# copy scp://username:password@server-ip/full-path-to-the-certificates/controller-
cert.pem config://../openflow/cacert.pem
OS10# copy scp://username:password@server-ip/full-path-to-the-certificates/switch-
cert.pem config://../openflow/sc-cert.pem
OS10# copy scp://username:password@server-ip/full-path-to-the-certificates/switch-
privkey.pem config://../openflow/sc-privkey.pem
```

其中，`server-ip` 指存储证书的服务器，`username` 和 `password` 指通过证书访问服务器所需的凭据。

3. 执行在[交换机上配置 OpenFlow 协议](#)主题中所述的步骤，以配置 OpenFlow。

## OpenFlow 命令

### controller

配置逻辑交换机实例连接到的 OpenFlow 控制器。

|        |                                                                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>controller {ipv4 ipv4-address  ipv6 ipv6-address [port port-number]<br/>[security {none tls}]}</code>                                                                                                                                                                                                                                                                    |
| 参数     | <ul style="list-style-type: none"><li><code>ipv4 ipv4-address</code>— 输入 <code>ipv4</code>，然后输入控制器的 IP 地址。</li><li><code>ipv6 ipv6-address</code>— 输入 <code>ipv6</code>，然后输入控制器的 IPv6 地址。</li><li><code>port port-number</code>— 输入关键字，然后输入端口号，从 1 到 65535。默认端口是 6653。</li><li><code>security {none tls}</code> — 指定连接的类型。默认值为 <code>security none</code>。使用 TCP 连接。</li></ul> |
| 默认     | TCP。默认端口号为 6653。                                                                                                                                                                                                                                                                                                                                                               |
| 命令模式   | OPENFLOW SWITCH CONFIGURATION                                                                                                                                                                                                                                                                                                                                                  |
| 使用情况信息 | 您可以配置最多八个 OpenFlow 控制器。<br><br>如果指定 <code>security tls</code> 选项，则 OpenFlow 应用程序会在为基于证书的身份验证指定的以下位置查找以下证书和私钥。有关获取证书以及将其安装在交换机和控制器上的信息，请参阅 <a href="#">在交换机和控制器之间建立 TLS 连接</a> 。                                                                                                                                                                                                |

|                               |                                                                |
|-------------------------------|----------------------------------------------------------------|
| <b>ca_cert</b> (将控制器标识为可信的证书) | <code>/config/etc/opt/dell/os10/openflow/cacert.pem</code>     |
| <b>证书</b> (将交换机标识为可信的证书)      | <code>/config/etc/opt/dell/os10/openflow/sc-cert.pem</code>    |
| <b>私钥</b> (与交换机证书对应的私钥)       | <code>/config/etc/opt/dell/os10/openflow/sc-privkey.pem</code> |

**示例** 以下示例将在端口 6633 上针对逻辑交换机实例 `of-switch-1` 配置具有 IP 地址 10.11.63.56 的 OpenFlow 控制器：

```
OS10# configure terminal
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# controller ipv4 10.11.63.56 port 6633
OS10 (config-openflow-switch)#
```

以下示例将在端口 6633 上针对逻辑交换机实例 `of-switch-1` 配置多个 OpenFlow 控制器：

```
OS10# configure terminal
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# controller ipv4 10.1.1.1 port 6633
OS10 (config-openflow-switch)# controller ipv4 10.1.1.8 port 6633
```

```

OS10 (config-openflow-switch)# controller ipv4 10.1.1.12 port 6633
OS10 (config-openflow-switch)# controller ipv4 10.1.2.17 port 6633
OS10 (config-openflow-switch)# controller ipv4 10.1.23.12 port 6633
OS10 (config-openflow-switch)# controller ipv4 10.1.99.121 port 6633
OS10 (config-openflow-switch)# controller ipv6 2025::1 port 6633
OS10 (config-openflow-switch)# controller ipv6 2025::12 port 6633

```

**支持的版本** 10.4.1.0 or later

## dpid-mac-address

指定逻辑交换机实例的数据路径 ID (DPID) 的 MAC 地址位。

**语法** `dpid-mac-address MAC-address`

**参数** `MAC-address`— 采用十六进制表示法的 48 位 MAC 地址, nn:nn:nn:nn:nn:nn

**默认** MAC 地址

**命令模式** OPENFLOW SWITCH CONFIGURATION

**使用情况信息** 控制器使用 DPID 来标识逻辑交换机实例。DPID 是在 `features_reply` 消息中发送至控制器的 64 位数字。DPID 从实例 ID 进行构建, 这是最显著的 16 位 (默认值为 0) 和 DPID MAC 地址, 这是最不显著的 48 位。OS10 目前仅支持一个逻辑交换机实例, 并且实例 ID 自动设置为 0。此值不可配置。

您可以使用此命令来修改 DPID 的 MAC 地址位。

**示例** DPID MAC 地址为 00:00:00:00:00:0a。

```

OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# dpid-mac-address 00:00:00:00:00:0a
OS10 (config-openflow-switch)#

```

**支持的版本** 10.4.1.0 or later

## in-band-mgmt

将前面板端口配置为 SDN 控制器连接到的管理接口。

**语法** `in-band-mgmt interface ethernet node/slot/port[:subport]`

**参数** `node/slot/port[:subport]`— 输入物理端口信息。

**默认** 无

**命令模式** OPENFLOW CONFIGURATION

**使用情况信息** 使用此命令可将任意一个前面板端口转换为管理接口。此端口不是 OpenFlow 逻辑交换机实例的一部分。默认情况下, 所有端口均为 L2 端口。如果将前面板端口之一配置为管理接口, 则该端口将成为 L3 端口。您只能将 L3 IPv4 地址配置为在此命令中指定的前面板端口。确保指定的端口和控制器之间具有 IP 连接。

此命令的 `no` 形式将移除此配置, 并且前面板端口将成为 OpenFlow 逻辑交换机实例的一部分。

**示例**

```

OS10# configure terminal
OS10(config)# openflow
OS10 (config-openflow)# in-band-mgmt interface ethernet 1/1/1
OS10 (config-openflow)# no shutdown

```

**支持的版本** 10.4.1.0 or later

# max-backoff

配置在使用 OpenFlow 控制器请求连接后逻辑交换机实例等待的时间间隔（以秒为单位）。

|        |                                                                                   |
|--------|-----------------------------------------------------------------------------------|
| 语法     | <code>max-backoff interval</code>                                                 |
| 参数     | <code>interval</code> — 输入在尝试与 OpenFlow 控制器建立连接后逻辑交换机实例等待的时间量（以秒为单位），从 1 到 65535。 |
| 默认     | 8 秒                                                                               |
| 命令模式   | OPENFLOW SWITCH CONFIGURATION                                                     |
| 使用情况信息 | 如果间隔时间已过，则逻辑交换机实例将重新尝试与 OpenFlow 控制器建立连接。                                         |
| 示例     |                                                                                   |

```
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# max-backoff 25
OS10 (config-openflow-switch)#
```

支持的版本 10.4.1.0 or later

# mode openflow-only

在交换机上启用仅限 OpenFlow 模式。

|        |                                                                                               |
|--------|-----------------------------------------------------------------------------------------------|
| 语法     | <code>mode openflow-only</code>                                                               |
| 参数     | 无                                                                                             |
| 默认     | 无                                                                                             |
| 命令模式   | OPENFLOW CONFIGURATION                                                                        |
| 使用情况信息 | 使用此命令可以启用仅限 OpenFlow 模式。此命令将重新加载交换机并引导至仅限 OpenFlow 模式。此命令将删除所有 L2 和 L3 配置。但是，系统管理和 AAA 配置会保留。 |

此命令的 `no` 形式会提示您重新加载交换机。如果您输入 `yes`，交换机将删除所有 OpenFlow 配置，包括控制器 IP、端口、证书和重新加载，然后返回到正常模式。

 **注:** 有关当交换机处于仅限 OpenFlow 模式时可用命令的列表，请参阅[仅限 OpenFlow 模式中可用的 CLI 命令](#)。

|    |  |
|----|--|
| 示例 |  |
|----|--|

```
OS10 (config-openflow)# mode openflow-only
OS10 (config-openflow)#
```

支持的版本 10.4.1.0 or later

# openflow

进入 OPENFLOW 配置模式。

|        |                          |
|--------|--------------------------|
| 语法     | <code>openflow</code>    |
| 参数     | 无                        |
| 默认     | 无                        |
| 命令模式   | CONFIGURATION            |
| 使用情况信息 | 在此模式下，将执行所有 OpenFlow 配置。 |

此命令的 `no` 形式会提示交换机重新加载。如果您输入 `yes`，系统将删除所有 OpenFlow 配置，并且在重新加载后，交换机将恢复到正常模式。

## 示例

```
OS10# configure terminal
OS10(config)# openflow
OS10 (config-openflow)#
```

**支持的版本** 10.4.1.0 or later

## probe-interval

配置使用逻辑交换机实例配置的控制器的回显请求间隔（以秒为单位）。

**语法** `probe-interval interval`

**参数** `interval`— 输入 keepalive 消息之间的时间量（以秒为单位），也称为回显请求，从 1 到 65535。

**默认** 5 秒

**命令模式** OPENFLOW SWITCH CONFIGURATION

**使用情况信息** 无

## 示例

```
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# probe-interval 20
OS10 (config-openflow-switch)#
```

**支持的版本** 10.4.1.0 or later

## protocol-version

指定逻辑交换机接口使用的协议版本。

**语法** `protocol-version version`

**参数** `version`— 选择以下操作之一：

- `negotiate` — 输入关键字以与控制器协商版本 1.0 或 1.3。已选择受支持的最高版本。
- `1.0` — 将逻辑交换机实例 OpenFlow 协议版本指定为 1.0。
- `1.3` — 将逻辑交换机实例 OpenFlow 协议版本指定为 1.3。

**默认** `negotiate`

**命令模式** OPENFLOW SWITCH CONFIGURATION

**使用情况信息** ⓘ **注：**只有在禁用了逻辑交换机实例时才应运行此命令。使用 `shutdown` 命令可禁用逻辑交换机实例。运行此命令后，输入 `no shutdown` 命令以再次启用逻辑交换机实例。

- 指定 `negotiate` 时，交换机会协商版本 1.0 和 1.3，并选择控制器支持的最高版本。协商基于 OpenFlow 规格 1.3 中所述的手握握手。
- 指定 `1.0` 时，交换机将建立与仅支持版本 1.0 的控制器连接。
- 指定 `1.3` 时，交换机将建立与仅支持版本 1.3 的控制器连接。

## 示例

以下示例显示了已配置为与支持 OpenFlow 协议版本 1.3 的控制器进行交互的逻辑交换机实例 `of-switch-1`。

```
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# shutdown
OS10 (config-openflow-switch)# protocol-version 1.3
OS10 (config-openflow-switch)# no shutdown
OS10 (config-openflow-switch)#
```

**支持的版本** 10.4.1.0 or later

# rate-limit packet\_in

配置控制器连接的最大数据包速率，以及在一秒内发送至控制器的突发流量中允许的最大数据包数。

|        |                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>rate-limit packet_in controller-packet-rate [burst maximum-packets-to-controller]</code>                                                                                                                                                                                                                                                                     |
| 参数     | <ul style="list-style-type: none"><li><code>controller-packet-rate</code>— 控制器 OpenFlow 通道连接的速率（以每秒数据包数为单位），从 100 到 268000000 秒。默认值为 0 秒（已禁用）。</li><li><code>maximum-packets-to-controller</code>— 控制器 OpenFlow 通道连接的数据包中的突发，从 25 到 1073000。默认值为 0 秒（已禁用）。此参数是可选的。如果未配置，则将其设置为配置的速率值的 25%。</li></ul>                                                               |
| 默认     | 已禁用                                                                                                                                                                                                                                                                                                                                                                |
| 命令模式   | OPENFLOW SWITCH CONFIGURATION                                                                                                                                                                                                                                                                                                                                      |
| 使用情况信息 | <p>OpenFlow 设置控制器与逻辑交换机实例的连接的指定速率和突发。控制器上的实际速率和脉冲的最大数量为配置的值的两倍。例如，当您配置的速率为 1000 PPS 和每秒突发 300 个数据包时，数据包可以每秒高达 2000 PPS 和 600 个数据包突发在连接上传出。</p> <p>此命令的 <code>no</code> 形式将禁用控制器连接上的速率限制。</p> <p> <b>注：</b>此命令是一个软件速率限制命令，仅适用于控制器与逻辑交换机实例之间的 OpenFlow 通道连接。此命令与交换机的数据平面速率限制无关。</p> |

**示例** 以下示例将使用 OpenFlow 控制器配置一个逻辑交换机实例（交换机 1），其速率为 1000 PPS 和 300 个数据包的数据包突发。

```
OS10 (config)# openflow
OS10 (config-openflow)# switch of-switch-1
OS10 (config-openflow-switch)# controller ipv4 10.11.63.56 port 6633
OS10 (config-openflow-switch)# rate-limit packet_in 1000 burst 300
OS10 (config-openflow-switch)#
```

**支持的版本** 10.4.1.0 or later

# show openflow

显示常规 OpenFlow 交换机和逻辑交换机实例信息。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show openflow</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 示例     | <pre>OS10# show openflow  Manufacturer           : DELL Hardware Description    : Software Description    : Dell Networking OS10-Premium, Dell Networking Application Software Version: 10.4.9999EX Serial Number           : Capabilities             : port, table, flow Switch mode             : openflow-only Match fields            :     Layer-1 : in-port     Layer-2 : eth-src, eth-dst, eth-type, vlan-id, vlan-pcp     Layer-3 : ipv4-src, ipv4-dst, ip-protocol, ip-dscp, ip-ecn     Layer-4 : tcp-src, tcp-dst, udp-src, udp-dst, icmpv4-type, icmpv4-</pre> |

```

code
Instructions : apply-actions, write-actions
Actions : output, set-field
Set field actions : eth-src, eth-dst, vlan-id, vlan-pcp, ip-
dscp
TLS parameters :
 certificate identifying trustworthy controller : /config/etc/opt/
dell/osl0/openflow/cacert.pem
 certificate identifying trustworthy switch : /config/etc/opt/
dell/osl0/openflow/sc-cert.pem
 private key : /config/etc/opt/
dell/osl0/openflow/sc-privkey.pem

```

**支持的版本** 10.4.1.0 or later

## show openflow flows

显示特定逻辑交换机实例的 OpenFlow 流。

**语法** `show openflow switch logical-switch-name flows`

**参数** `logical-switch-name` — 输入逻辑交换机实例名称以查看流信息。

**默认** 无

**命令模式** EXEC

**使用情况信息** 无

**示例**

```

OSl0# show openflow switch of-switch-1 flows
Logical switch name: of-switch-1
Total flows: 1
 Flow: 0
 Table ID: 0, Table: Ingress ACL TCAM table
 Flow ID: 0
 Priority: 32768, Cookie: 0
 Hard Timeout: 0, Idle Timeout: 0
 Packets: 0, Bytes: 0
 Match Parameters:
 In Port: ethernet1/1/1
 EType: 0x800
 SMAC: 00:0b:c4:a8:22:b0/ff:ff:ff:ff:ff:ff
 DMAC: 00:0b:c4:a8:22:b1/ff:ff:ff:ff:ff:ff
 VLAN id: 2/4095
 VLAN PCP: 1
 IP DSCP: 4
 IP ECN: 1
 IP Proto: 1
 Src Ip: 10.0.0.1/255.255.255.255
 Dst Ip: 20.0.0.1/255.255.255.255
 ICMPv4 Type: 1
 ICMPv4 Code: 10
 L4 Src Port: *
 L4 Dst Port: *
 Apply-Actions: Output= ethernet1/1/2, ethernet1/1/3:1
 Write-Actions: Drop

```

**支持的版本** 10.4.1.0 or later

## show openflow ports

显示特定逻辑交换机实例的 OpenFlow 端口。

**语法** `show openflow switch logical-switch-name ports`

**参数** `logical-switch-name` — 输入逻辑交换机实例的名称以查看端口信息。

默认 无

命令模式 EXEC

使用情况信息 无

示例

```
OS10# show openflow switch of-switch-1 ports
Logical switch name: of-switch-1
Interface Name of-port ID Config-State Link-State SPEED DUPLEX
AUTONEG TYPE
ethernet1/1/1 1 PORT_UP(CLI) LINK_UP 40GB FD
YES COPPER
ethernet1/1/2 5 PORT_UP(CLI) LINK_UP 40GB FD
YES COPPER
ethernet1/1/3:1 9 PORT_UP(CLI) LINK_UP 10GB FD
NO FIBER
ethernet1/1/3:2 10 PORT_UP(CLI) LINK_DOWN 0MB FD
NO FIBER
ethernet1/1/3:3 11 PORT_UP(CLI) LINK_DOWN 0MB FD
NO FIBER
ethernet1/1/3:4 12 PORT_UP(CLI) LINK_DOWN 0MB FD
NO FIBER
ethernet1/1/4 13 PORT_UP(CLI) LINK_UP 40GB FD
YES COPPER
ethernet1/1/5:1 17 PORT_UP(CLI) LINK_UP 10GB FD
NO FIBER
ethernet1/1/5:2 18 PORT_UP(CLI) LINK_DOWN 0MB FD
NO FIBER
ethernet1/1/5:3 19 PORT_UP(CLI) LINK_DOWN 0MB FD
NO FIBER
ethernet1/1/5:4 20 PORT_UP(CLI) LINK_DOWN 0MB FD
NO FIBER
ethernet1/1/6 21 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/7 25 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/8 29 PORT_UP(CLI) LINK_DOWN 0MB FD
YES COPPER
ethernet1/1/9 33 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/10 37 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/11 41 PORT_UP(CLI) LINK_UP 40GB FD
YES COPPER
ethernet1/1/12 45 PORT_UP(CLI) LINK_UP 40GB FD
YES COPPER
ethernet1/1/13 49 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/14 53 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/15 57 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/16 61 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/17 65 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/18 69 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/19 73 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/20 77 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/21 81 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/22 85 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/23 89 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/24 93 PORT_UP(CLI) LINK_DOWN 0MB FD
NO NONE
ethernet1/1/25 97 PORT_UP(CLI) LINK_DOWN 0MB FD
```



|                |        |     |               |           |     |    |
|----------------|--------|-----|---------------|-----------|-----|----|
| NO             | COPPER |     |               |           |     |    |
| ethernet1/1/26 |        | 101 | PORT_UP (CLI) | LINK_DOWN | 0MB | FD |
| NO             | COPPER |     |               |           |     |    |
| ethernet1/1/27 |        | 105 | PORT_UP (CLI) | LINK_DOWN | 0MB | FD |
| NO             | NONE   |     |               |           |     |    |
| ethernet1/1/28 |        | 109 | PORT_UP (CLI) | LINK_DOWN | 0MB | FD |
| NO             | NONE   |     |               |           |     |    |
| ethernet1/1/29 |        | 113 | PORT_UP (CLI) | LINK_DOWN | 0MB | FD |
| NO             | NONE   |     |               |           |     |    |
| ethernet1/1/30 |        | 117 | PORT_UP (CLI) | LINK_DOWN | 0MB | FD |
| NO             | NONE   |     |               |           |     |    |
| ethernet1/1/31 |        | 121 | PORT_UP (CLI) | LINK_DOWN | 0MB | FD |
| NO             | NONE   |     |               |           |     |    |
| ethernet1/1/32 |        | 125 | PORT_UP (CLI) | LINK_DOWN | 0MB | FD |
| NO             | NONE   |     |               |           |     |    |

支持的版本10.4.1.0 or later

show openflow switch

显示交换机实例的 OpenFlow 参数。

|        |                      |
|--------|----------------------|
| 语法     | show openflow switch |
| 参数     | 无                    |
| 默认     | 无                    |
| 命令模式   | EXEC                 |
| 使用情况信息 | 无                    |
| 示例     |                      |

```

OS10# show openflow switch
Logical switch name: of-switch-1
 Internal switch instance ID: 0
 Config state: true
 Signal Version: negotiate
 Data plane: secure
 Max backoff (sec): 8
 Probe Interval (sec): 5
 DPID: 90:b1:1c:f4:a5:23
 Switch Name : of-switch-1
 Number of buffers: 0
 Number of tables: 1
 Table ID: 0
 Table name: Ingress ACL TCAM table
 Max entries: 1000
 Active entries: 0
 Lookup count: 0
 Matched count: 0
 Controllers:
 10.16.208.150:6633, Protocol: none,
 packet-in Rate limit (packet per second): 0
 packet-in Burst limit: 0

```

支持的版本10.4.1.0 or later

show openflow switch controllers

显示特定逻辑交换机实例的 OpenFlow 控制器。

|    |                                                             |
|----|-------------------------------------------------------------|
| 语法 | show openflow switch <i>logical-switch-name</i> controllers |
| 参数 | <i>logical-switch-name</i> — 输入要查询的逻辑交换机实例的名称。              |

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | 此命令将显示所有活动的 OpenFlow 控制器的信息。                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 示例     | <pre>OS10# show openflow switch ice controllers Logical switch name: ice Total Controllers: 2   Controller: 1     Target: 10.16.132.59:6653     Protocol: TCP     Connected: YES     Role: Master     Last_error: Connection timed out     State: ACTIVE     sec_since_disconnect: 0   Controller: 2     Target: [2001::2]:6653     Protocol: TCP     Connected: YES     Role: Equal     Last_error: Connection timed out     State: ACTIVE     sec_since_disconnect: 0</pre> |
| 支持的版本  | 10.4.1.0 or later                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## switch

创建逻辑交换机实例或修改现有逻辑交换机实例。

|        |                                                                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>switch logical-switch-name</code>                                                                                                                                                                                                                                                         |
| 参数     | <code>logical-switch-name</code> — 输入要创建或修改的逻辑交换机实例的名称，最多包含 15 个字符。OS10 仅支持逻辑交换机的一个实例。                                                                                                                                                                                                          |
| 默认     | 无                                                                                                                                                                                                                                                                                               |
| 命令模式   | OPENFLOW CONFIGURATION                                                                                                                                                                                                                                                                          |
| 使用情况信息 | <p>您必须为逻辑交换机实例配置控制器。默认情况下，逻辑交换机实例处于禁用状态。要与控制器建立连接，请使用 <code>no shutdown</code> 命令启用逻辑交换机实例。交换机中的所有物理和逻辑接口都分配给配置的逻辑交换机。</p> <p>此命令的 <code>no</code> 形式将移除逻辑交换机实例。</p> <p><b>注：</b> OS10 仅支持逻辑交换机的一个实例。如果您尝试创建第二个逻辑交换机实例，将显示以下消息：</p> <pre>% Warning: Only one Switch instance is supported</pre> |

|       |                                                                                                                                                |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例    | <pre>OS10# config terminal OS10 (config)# openflow OS10 (config-openflow)# switch of-switch-1 OS10 (config-openflow-switch)# no shutdown</pre> |
| 支持的版本 | 10.4.1.0 or later                                                                                                                              |

## 仅限 OpenFlow 模式的命令

将交换机配置为仅限 OpenFlow 模式时，仅提供以下命令；所有其他命令将被禁用。

**注：**

- 当交换机处于 OpenFlow 模式时，interface 命令下的 ntp 子命令不适用。
- 当使用 in-band-mgmt 命令将接口配置为管理端口时，interface 命令下的 ip 和 ipv6 子命令才适用。
- ip 和 ipv6 命令必须仅在带内模式下使用（使用 in-band-mgmt 命令）。

表. 81: 模式和 CLI 命令

| 模式            | 可用的 CLI 命令                                                                                                                       |
|---------------|----------------------------------------------------------------------------------------------------------------------------------|
| CONFIGURATION | aaa                                                                                                                              |
|               | alias                                                                                                                            |
|               | banner                                                                                                                           |
|               | class-map                                                                                                                        |
|               | clock                                                                                                                            |
|               | control-plane                                                                                                                    |
|               | crypto                                                                                                                           |
|               | end                                                                                                                              |
|               | eula-consent                                                                                                                     |
|               | exec-timeout                                                                                                                     |
|               | exit                                                                                                                             |
|               | feature                                                                                                                          |
|               | help                                                                                                                             |
|               | host-description                                                                                                                 |
|               | hostname                                                                                                                         |
|               | interface                                                                                                                        |
|               | ip <ul style="list-style-type: none"> <li>• ip access-list</li> <li>• ip route</li> <li>• ip ssh</li> <li>• ip telnet</li> </ul> |
|               | ipv6 <ul style="list-style-type: none"> <li>• ip access-list</li> </ul>                                                          |
|               | line                                                                                                                             |
|               | logging                                                                                                                          |
|               | login                                                                                                                            |
|               | management                                                                                                                       |
|               | no                                                                                                                               |
|               | ntp                                                                                                                              |
|               | openflow                                                                                                                         |
|               | password-attributes                                                                                                              |
|               | policy-map                                                                                                                       |
|               | radius-server                                                                                                                    |
|               | rest                                                                                                                             |
|               | scale-profile                                                                                                                    |
|               | support-assist                                                                                                                   |

表. 81: 模式和 CLI 命令 (续)

| 模式                               | 可用的 CLI 命令                                                                                                                                     |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
|                                  | system                                                                                                                                         |
|                                  | tacacs-server                                                                                                                                  |
|                                  | trust                                                                                                                                          |
|                                  | username                                                                                                                                       |
|                                  | userrole                                                                                                                                       |
| EXEC                             | <p>所有命令</p> <p>以下调试命令不可用:</p> <ul style="list-style-type: none"> <li>• debug iscsi</li> <li>• debug radius</li> <li>• debug tacacs+</li> </ul> |
| LAG INTERFACE CONFIGURATION      | 不支持 LAG。                                                                                                                                       |
| LOOPBACK INTERFACE CONFIGURATION | 环回接口不受支持。                                                                                                                                      |
| INTERFACE CONFIGURATION          | description                                                                                                                                    |
|                                  | end                                                                                                                                            |
|                                  | exit                                                                                                                                           |
|                                  | ip                                                                                                                                             |
|                                  | mtu                                                                                                                                            |
|                                  | negotiation                                                                                                                                    |
|                                  | ntp                                                                                                                                            |
|                                  | show                                                                                                                                           |
|                                  | shutdown                                                                                                                                       |
| VLAN INTERFACE CONFIGURATION     | 不支持 VLAN。                                                                                                                                      |

## 访问控制列表

OS10 使用两种类型的访问策略：基于硬件的 ACL 和基于软件的路由映射。使用 ACL 筛选流量并丢弃或转发匹配的数据包。要重新分发与配置的条件匹配的路由，请使用路由映射。

### ACL

ACL 是包含匹配条件的筛选器；例如，检查互联网协议 (IP)、传输控制协议 (TCP) 或用户数据报协议 (UDP) 数据包，以及在 NPU 上转发或丢弃数据包等操作。ACL 允许或拒绝基于 MAC 和/或 IP 地址的流量。ACL 条目的数量与硬件相关。

ACL 只有两个操作 — 转发或丢弃。路由 — 映射不仅允许或阻止重新分发的路由，还可以在将路由重新分配到另一个协议时修改与其关联的信息。当数据包与筛选器匹配时，设备将根据筛选器的指定操作丢弃或转发数据包。如果数据包与 ACL 中的任何筛选器均不匹配，则数据包将丢弃隐式拒绝。在将 ACL 应用到接口之前，ACL 规则不会消耗硬件资源。

ACL 进程按顺序进行。如果数据包与第一个筛选器中的条件不匹配，则应用第二个筛选器。如果您配置了多个基于硬件的 ACL，筛选规则将根据优先级数字处理单元 (NPU) 规则应用于数据包内容。

### 路由映射

路由映射是基于软件的协议筛选重新分发路由（从一个协议到另一个协议），并在路由通告的决策条件中使用。路由映射定义了从指定路由协议重新分配到目标路由进程的路由，请参阅[路由映射](#)。

具有多个匹配条件的路由映射、同一路由映射序列中的两个或更多匹配项，具有不同的匹配命令。将数据包与此条件匹配是 AND 操作。如果在路由映射序列中找不到匹配项，该进程将移至下一个路由映射序列，直至找到匹配项，或直至不再有序列。找到匹配项后，数据包将转发，无需其他路由映射序列。如果在路由映射序列中包含 continue 子句，则在找到匹配项后，下一个路由映射序列也将进行处理。

## IP ACL

ACL 根据以下条件筛选数据包：

- IP 协议号
- 源和目标 IP 地址
- 源和目标 TCP 端口号
- 源和目标 UDP 端口号

对于 ACL、TCP 和 UDP 筛选器，匹配特定 TCP 或 UDP 端口上的条件。对于 ACL TCP 筛选器，您还可以匹配已建立 TCP 会话上的条件。

创建 ACL 时，筛选器顺序非常重要。您可以在输入时为筛选器分配序列号，或者 OS10 可以按创建筛选器的顺序分配编号。序列号显示在 show running-configuration 和 show ip access-lists [in | out] 命令输出中。

入口和出口热锁 ACL 允许您在不中断流量流的情况下将新规则附加到现有的 ACL 或删除。内容可寻址内存 (CAM) 中的现有条目无序显示新条目。默认情况下，热锁 ACL 处于启用状态，并且支持所有平台上的 ACL。

 **注：** 并非所有 ACL 都支持入口 ACL。

## MAC ACL

MAC ACL 会筛选数据包标头上的流量。此流量筛选基于：

|                     |                                                         |
|---------------------|---------------------------------------------------------|
| <b>源 MAC 数据包地址</b>  | MAC 地址范围 — 以 3x4 点分隔的十六进制表示法表示的地址掩码，而 any 表示规则匹配所有源地址。  |
| <b>目标 MAC 数据包地址</b> | MAC 地址范围 — 以 3x4 点分隔的十六进制表示法表示的地址掩码，而 any 表示规则匹配所有目标地址。 |
| <b>数据包协议</b>        | 通过 EtherType 字段内容设置并为所有协议分配协议号。                         |
| <b>VLAN ID</b>      | 在数据包标头中设置                                               |

**服务类别**                      显示在数据包标头中

IPv4/IPv6 和 MAC ACL 分别适用于入站和出站数据包。您可以为多个 ACL 分配接口，每个 ACL 类型的每个数据包方向限制为一个 ACL。

## 控制平面 ACL

OS10 提供了控制平面 ACL 以选择性地限制发往 CPU 端口的数据包，从而提供更高的安全性。控制平面 ACL 提供：

- 用于保护 CPU 拒绝服务 (DoS) 攻击的选项。
- 精细控制以允许或阻止进入 CPU 的流量。

控制平面 ACL 适用于前面板和管理端口。控制平面 ACL 是以下类型之一：

- IP ACL
- IPv6 ACL
- MAC ACL

 **注：** MAC ACL 仅应用于通过前面板端口输入的数据包。

没有隐式拒绝规则。如果配置的条件均不匹配，则默认行为将允许。如果您需要拒绝与任何配置的条件不匹配的流量，请明确配置拒绝语句。

控制平面 ACL 与 VTY ACL（管理 ACL）相互排斥。VTY ACL 为会话连接协议（如 SSH 或 TELNET）提供安全访问权限；但是，控制平面 ACL 允许或拒绝任何 TCP 或 UDP，包括从特定主机和网络进行 SSH 和 TELNET 会话，同时还会同时筛选 IPv4 和 IPv6 流量。

### 配置控制平面 ACL

要配置控制平面 ACL，请使用现有的 ACL 模板，并根据需要创建适当的规则以允许或拒绝流量，类似于为 VTY ACL 创建访问列表。但是，当您应用此控制平面 ACL 时，您必须将其应用于控制平面模式而不是 VTY 模式。例如：

```
OS10# configure terminal
OS10(config)# control-plane
OS10(config-control-plane)# ip access-group acl_name in
```

其中 *acl\_name* 是控制平面 ACL 的名称，最多为 140 个字符。

 **注：** 在入口流量上用控制平面 ACL。

## 控制平面 ACL 限定符

本部分列出了支持的控制平面 ACL 规则限定符。

 **注：** OS10 仅支持下面列出的限定符。确保在 ACL 规则中仅使用这些限定符。

- IPv4 限定符：
  - DST\_IP — 目标 IP 地址
  - SRC\_IP — 源 IP 地址
  - IP\_TYPE — IP 类型
  - IP\_PROTOCOL — TCP、UDP 等协议
  - L4\_DST\_PORT — 目标端口号
- IPv6 限定符：
  - DST\_IPv6 — 目标地址
  - SRC\_IPv6 — 源地址
  - IP\_TYPE — IP 类型；例如，IPv4 或 IPv6
  - IP\_PROTOCOL — TCP、UDP 等
  - L4\_DST\_PORT — 目标端口
- MAC 限定符：
  - OUT\_PORT — 出口 CPU 端口
  - SRC\_MAC — 源 MAC 地址
  - DST\_MAC — 目标 MAC 地址
  - ETHER\_TYPE — 以太网类型

- OUTER\_VLAN\_ID — VLAN ID
- IP\_TYPE — IP 类型
- OUTER\_VLAN\_PRI — DOT1P 值

## IP 片段处理

OS10 支持一个可配置的选项，用于明确拒绝 IP 片段数据包，尤其适用于第二个及后续的数据包。此选项将现有的 ACL 命令语法与所有 L3 规则的 `fragments` 关键字进行扩展：

- 允许使用第二个和后续片段，因为您不能将 L3 规则应用到这些片段。如果最终拒绝数据包，则必须拒绝第一个片段，并且不能重新组装作为一个整体的数据包。
- 系统在隐式拒绝之前为第二个和后续片段应用隐式准许。
- 如果配置显式拒绝，则第二个和后续的片段不会命中针对片段的隐式允许规则。

## IP 片段 ACL

当数据包超过最大数据包大小时，数据包会分成大量较小的数据包，其中包含原始数据包的部分内容。此数据包流从初始数据包开头，其中包含原始数据包中包含的所有 L3 和第 4 层 (L4) 标头信息，并且后跟多个仅包含 L3 标头信息的数据包。

此数据包流包含来自原始数据包的所有信息，该数据包足够小，以避免最大数据包大小限制。这为 ACL 处理提供了一个特殊问题。

如果 ACL 筛选器基于 L4 信息，零碎数据包流中的非初始数据包将与 L4 信息不匹配，即使原始数据包与筛选器相匹配也是如此。由于这种筛选，将不会由 ACL 处理数据包。

示例显示了拒绝第二个和后续的片段，并允许接口上的所有数据包。这些 ACL 将拒绝目标 IP 10.1.1.1 的所有第二个和后续片段，但允许使用目标 IP 10.1.1.1 的第一个片段和非零碎数据包。第二个示例显示了允许所有数据包（分散且非零碎）的 ACL，目标 IP 为 10.1.1.1。

### 拒绝第二个和后续片段

```
OS10(config)# ip access-list ABC
OS10(conf-ipv4-acl)# deny ip any 10.1.1.1/32 fragments
OS10(conf-ipv4-acl)# permit ip any 10.1.1.1/32
```

### 允许接口上的所有数据包

```
OS10(config)# ip access-list ABC
OS10(conf-ipv4-acl)# permit ip any 10.1.1.1/32
OS10(conf-ipv4-acl)# deny ip any 10.1.1.1/32 fragments
```

## L3 ACL 规则

使用 ACL 命令进行 L3 数据包过滤。在 TCP 目标端口等于 24 的情况下，将允许来自主机 10.1.1.1 的 TCP 数据包，并且所有其他都被拒绝。

在 TCP 目标端口等于 24 的情况下，将允许来自主机 10.1.1.1 的第一个片段或非零散的 TCP 数据包，并且允许来自主机 10.1.1.1 的所有 TCP 的非第一个片段。所有其他不是第一个片段的 IP 数据包都将被拒绝。

## 仅允许具有 L3 信息的 ACL

如果数据包的 L3 信息与 ACL 中的信息匹配，则会检查数据包的片段偏移量 (FO)：

- 如果数据包的  $FO > 0$ ，则允许数据包
- 如果数据包的  $FO = 0$ ，则下一个 ACL 条目进程

## 仅拒绝具有 L3 信息的 ACL

如果数据包的 L3 信息与 ACL 中的 L3 信息不匹配，则会检查数据包的 FO：

- 如果数据包的  $FO > 0$ ，则将拒绝数据包

- 如果数据包的 FO = 0，则下一个 ACL 行进程

## 允许来自主机的所有数据包

```
OS10(config)# ip access-list ABC
OS10(conf-ipv4-acl)# permit tcp host 10.1.1.1 any eq 24
OS10(conf-ipv4-acl)# deny ip any any fragment
```

## 仅允许来自主机的第一个片段和非零碎数据包

```
OS10(config)# ip access-list ABC
OS10(conf-ipv4-acl)# permit tcp host 10.1.1.1 any eq 24
OS10(conf-ipv4-acl)# permit tcp host 10.1.1.1 any fragment
OS10(conf-ipv4-acl)# deny ip any any fragment
```

要记录拒绝的所有数据包并覆盖隐式拒绝规则和 TCP/UDP 片段的隐式允许规则，请使用类似的配置。当 ACL 筛选数据包时，它会查看 FO 以确定它是否是一个片段：

- FO = 0 表示它是第一个片段，否则该数据包是非片段
- FO > 0 表示它是原始数据包的片段

## 为筛选器分配序列号

IP ACL 可筛选源和目标 IP 地址、IP 主机地址、TCP 地址、TCP 主机地址、UDP 地址以及 UDP 主机地址。流量按筛选顺序通过筛选器传递。通过首先输入 IP ACCESS-LIST 模式，然后为筛选器分配序列号来配置 IP ACL。

## 用户提供的序列号

- 通过在 CONFIGURATION 模式下创建 IP ACL 来输入 IP ACCESS LIST 模式。

```
ip access-list access-list-name
```

- 在 IPV4-ACL 模式下配置丢弃或转发筛选器。

```
seq sequence-number {deny | permit | remark} {ip-protocol-number | icmp | ip |
protocol | tcp | udp} {source prefix | source mask | any | host} {destination mask |
any | host ip-address} [count [byte]] [fragments]
```

## 自动生成的序列号

如果您创建的 ACL 仅包含一个或两个筛选器，您可以让系统根据您的配置筛选器的顺序分配序列号。系统使用 10 个值的倍数为筛选器分配序列号。

- 配置拒绝或允许筛选器可检查 IPV4 ACL 模式下的 IP 数据包。

```
{deny | permit} {source mask | any | host ip-address} [count [byte]] [fragments]
```

- 配置拒绝或允许筛选器可检查 IPV4 ACL 模式下的 TCP 数据包。

```
{deny | permit} tcp {source mask | any | host ip-address}} [count [byte]] [fragments]
```

- 配置拒绝或允许筛选器可检查 IPV4 ACL 模式下的 UDP 数据包。

```
{deny | permit} udp {source mask | any | host ip-address}} [count [byte]] [fragments]
```



为筛选器分配序列号

```
OS10(config)# ip access-list acl1
OS10(conf-ip4-acl)# seq 5 deny tcp any any capture session 1 count
```

通过 ACL 查看处理的 ACL 和数据包

```
OS10# show ip access-lists in
Ingress IP access-list acl1
Active on interfaces :
 ethernet1/1/5
seq 5 permit ip any any count (10000 packets)
```

## 删除 ACL 规则

在低于 10.4.2 的版本中，删除 ACL 规则需要序列号。  
在 10.4.2 版本或更高版本后，您也可以使用 CLI 命令的 `no` 形式删除 ACL 规则，而无需使用序列号。  
删除 ACL 规则时，将应用以下条件：

- 输入 CLI 命令的准确 `no` 形式。每个 ACL 规则都是一个独立的实体。例如，规则 `deny ip any any` 不同于 `deny ip any any count`。  
例如，如果您已配置以下规则：

```
deny ip 1.1.1.1/24 2.2.2.2/24
deny ip any any
```

使用命令 `no deny ip any any` 将仅删除 `deny ip any any` 规则。  
要删除 `deny ip 1.1.1.1/24 2.2.2.2/24` 规则，必须明确使用 `no deny ip 1.1.1.1/24 2.2.2.2/24` 命令。

**注：**通配符选项不受支持。

- 您不能再使用不同的序列号多次配置相同的 ACL 规则。此选项可防止在系统中输入重复的规则并占用内存空间。
- 当您从以前的版本升级到版本 10.4.2 或更高版本时，升级过程会删除所有重复的 ACL 规则，并且系统中仅存在 ACL 规则的一个实例。

## L2 和 L3 ACL

在 L2 模式下，在接口上配置 L2 和 L3 ACL。如果在接口上同时使用 L2 和 L3 ACL，则规则将适用。

- L3 ACL 将筛选数据包，然后 L2 ACL 将筛选数据包
- 出口 L3 ACL 将筛选数据包

规则按顺序应用：

- 入口 L3 ACL
- 入口 L2 ACL
- 出口 L3 ACL
- 出口 L2 ACL

**注：**在入口 ACL 中，L2 的优先级高于 L3，在出口 ACL 中，L3 的优先级高于 L2。

表. 82: L2 和 L3 目标流量

| L2 ACL/L3 ACL | 目标流量      |
|---------------|-----------|
| 拒绝/拒绝         | L3 ACL 拒绝 |
| 拒绝/允许         | L3 ACL 允许 |
| 允许/拒绝         | L3 ACL 拒绝 |
| 允许/允许         | L3 ACL 允许 |

# 分配和应用 ACL 筛选器

要筛选以太网接口、端口通道接口或 VLAN，请将 IP ACL 筛选器分配给相应的接口。IP ACL 适用于进入物理、端口通道或 VLAN 接口的所有流量。流量可以随 ACL 筛选器中配置的条件和操作进行转发或丢弃。

要更改 ACL 筛选器功能，请将相同的 ACL 筛选器应用到不同的接口。例如，获取 ACL“ABCD”并使用 `in` 关键字进行应用，它将成为入口 ACL。如果使用 `out` 关键字应用相同的 ACL 筛选器，则它将成为出口 ACL。

您可以将 IP ACL 筛选器应用到物理、端口通道或 VLAN 接口。允许的 ACL 筛选器数量与硬件相关。

1. 在 CONFIGURATION 模式下输入接口信息。

```
interface ethernet node/slot/port
```

2. 在 INTERFACE 模式下配置接口的 IP 地址，将其置于 L3 模式。

```
ip address ip-address
```

3. 在 INTERFACE 模式下，将 IP ACL 筛选器应用于进入或退出接口的流量。

```
ip access-group access-list-name {in | out}
```

## 配置 IP ACL

```
OS10(config)# interface ethernet 1/1/28
OS10(conf-if-eth1/1/28)# ip address 10.1.2.0/24
OS10(conf-if-eth1/1/28)# ip access-group abcd in
```

## 查看应用到接口的 ACL 筛选器

```
OS10# show ip access-lists in
Ingress IP access-list acl1
Active on interfaces :
 ethernet1/1/28
seq 10 permit ip host 10.1.1.1 host 100.1.1.1 count (0 packets)
seq 20 deny ip host 20.1.1.1 host 200.1.1.1 count (0 packets)
seq 30 permit ip 10.1.2.0/24 100.1.2.0/24 count (0 packets)
seq 40 deny ip 20.1.2.0/24 200.1.2.0/24 count (0 packets)
seq 50 permit ip 10.0.3.0 255.0.255.0 any count (0 packets)
seq 60 deny ip 20.0.3.0 255.0.255.0 any count (0 packets)
seq 70 permit tcp any eq 1000 100.1.4.0/24 eq 1001 count (0 packets)
seq 80 deny tcp any eq 2100 200.1.4.0/24 eq 2200 count (0 packets)
seq 90 permit udp 10.1.5.0/28 eq 10000 any eq 10100 count (0 packets)
seq 100 deny tcp host 20.1.5.1 any rst psh count (0 packets)
seq 110 permit tcp any any fin syn rst psh ack urg count (0 packets)
seq 120 deny icmp 20.1.6.0/24 any fragment count (0 packets)
seq 130 permit 150 any any dscp 63 count (0 packets)
```

要查看与 ACL 匹配的数据包数，请在创建 ACL 条目时使用 `count` 选项。

- 将规则与计数选项配合使用以创建 ACL，请参阅[为筛选器分配序列号](#)。
- 将 ACL 应用为 CONFIGURATION 模式下的接口上的入站或出站 ACL，并查看与 ACL 匹配的数据包数量。

```
show ip access-list {in | out}
```

# 入口 ACL 筛选器

要创建入口 ACL 筛选器，请在 EXEC 模式下使用 `ip access-group` 命令。要配置入口，请使用 `in` 关键字。使用 `ip access-list acl-name` 命令将规则应用于 ACL。要查看访问列表，请使用 `show access-lists` 命令。

1. 在 INTERFACE 模式下，在接口上应用入口访问列表。

```
ip access-group access-group-name in
```

2. 返回 CONFIGURATION 模式。

```
exit
```

3. 在 CONFIGURATION 模式下创建访问列表。

```
ip access-list access-list-name
```

4. 在 ACCESS-LIST 模式下为访问列表创建规则。

```
permit ip host ip-address host ip-address count
```

#### 将 ACL 规则应用到访问组和查看访问列表

```
OS10(config)# interface ethernet 1/1/28
OS10(conf-if-eth1/1/28)# ip access-group abcd in
OS10(conf-if-eth1/1/28)# exit
OS10(config)# ip access-list acl1
OS10(conf-ip4-acl)# permit ip host 10.1.1.1 host 100.1.1.1 count
```

## 出口 ACL 筛选器

出口 ACL 筛选器会影响离开网络的流量。在物理接口上配置出口 ACL 筛选器可通过明确仅允许授权流量来保护系统基础架构免遭恶意和故意的攻击。这些系统范围的 ACL 筛选器无需在每个接口上应用 ACL 筛选器。

您可以使用出口 ACL 筛选器来限制出口流量。例如，当您将拒绝服务 (DoS) 攻击流量隔离到特定接口并应用出口 ACL 筛选器以阻止 DoS 流退出网络时，您可以保护下游设备。

1. 在 INTERFACE 模式下，在接口上应用出口访问列表。

```
ip access-group access-group-name out
```

2. 返回 CONFIGURATION 模式。

```
exit
```

3. 在 CONFIGURATION 模式下创建访问列表。

```
ip access-list access-list-name
```

4. 在 ACCESS-LIST 模式下为访问列表创建规则。

```
seq 10 deny ip any any count fragment
```

#### 将规则应用于 ACL 筛选器

```
OS10(config)# interface ethernet 1/1/29
OS10(conf-if-eth1/1/29)# ip access-group egress out
OS10(conf-if-eth1/1/29)# exit
OS10(config)# ip access-list egress
OS10(conf-ip4-acl)# seq 10 deny ip any any count fragment
```

#### 查看 IP ACL 筛选器配置

```
OS10# show ip access-lists out
Egress IP access-list abcd
Active on interfaces :
 ethernet1/1/29
seq 10 deny ip any any fragment count (100 packets)
```

## VTY ACL

要限制 Telnet 和 SSH 到交换机的连接，请在虚拟终端线路上应用访问列表 (VTY)。有关详细信息，请参阅[虚拟终端线路 ACL](#)。

# SNMP ACL

要筛选交换机上的 SNMP 请求，请将访问列表分配给 SNMP 社区。支持 IPv4 和 IPv6 访问列表以限制 IP 源地址。有关详细信息，请参阅[限制 SNMP 访问权限](#)。

## 清除访问列表计数器

清除特定访问列表或所有列表的 IPv4、IPv6 或 MAC 访问列表计数器。计数器将计算匹配访问列表中的每个允许或拒绝语句的数据包数。要获取与访问列表匹配的更新数据包数，请清除要从零开始的计数器。如果不配置访问列表名称，则所有 IP 访问列表计数器都将清除。

要查看访问列表信息，请使用 `show access-lists` 命令。

- 在 EXEC 模式下清除 IPv4 访问列表计数器。

```
clear ip access-list counters access-list-name
```

- 在 EXEC 模式下清除 IPv6 访问列表计数器。

```
clear ipv6 access-list counters access-list-name
```

- 在 EXEC 模式下清除 MAC 访问列表计数器。

```
clear mac access-list counters access-list-name
```

## IP 前缀列表

IP 前缀列表可控制路由策略。IP 前缀列表是一系列顺序筛选器，其中包含匹配条件和用于处理路由的允许或拒绝操作。按顺序筛选进程，以便当路由前缀与第一个筛选器中的条件不匹配时，第二个筛选器将应用，依此类推。

路由前缀是与 IP 地址中的位匹配的 IP 地址模式。路由前缀的格式为 A.B.C.D/x，其中 A.B.C.D 是以点分隔的十进制地址，/x 是与点分十进制地址匹配的位的数量。

当路由前缀与筛选器匹配时，系统将根据筛选器的指定操作丢弃或转发数据包。如果路由前缀与前缀列表中的任何筛选器都不匹配，路由将丢弃，隐式拒绝。

例如，在 112.24.0.0/16 中，地址 112.24.0.0 的前 16 位与 112.24.0.0 和 112.24.255.255 之间的所有地址匹配。对于具有 `le`（小于或等于）和 `ge`（大于或等于）参数的特定路由使用允许或拒绝筛选器，其中 x.x.x.x/x 表示路由前缀：

- 要仅拒绝 /8 前缀，请输入 `deny x.x.x.x/x ge 8 le 8`
- 要允许掩码大于 /8 但小于 /12 的路由，请输入 `permit x.x.x.x/x ge 8 le 12`
- 要拒绝掩码小于 /24 的路由，请输入 `deny x.x.x.x/x le 24`
- 要允许具有大于的 /20 掩码的路由，请输入 `permit x.x.x.x/x ge 20`

以下规则适用于前缀列表：

- 无允许或拒绝筛选器的前缀列表允许所有路由
- 假定 *implicit deny* — 路由将丢弃与允许或拒绝筛选器不匹配的所有路由前缀
- 当路由与筛选器匹配后，筛选器的操作将应用，并且不会对该路由应用其他筛选器

使用前缀列表处理适用于开放最短路径优先 (OSPF)、路由表管理器 (RTM) 和边界网关协议等路由协议 (BGP) 的路由。

要配置前缀列表，请在 PREFIX-LIST 和 ROUTER-BGP 模式下使用命令。在 PREFIX-LIST 模式下创建前缀列表，并在 ROUTER-BGP 模式中将该列表分配给命令。

## 路由映射

路由映射是一系列包含匹配条件和操作的命令。它们可以更改满足匹配条件的数据包。ACL 和前缀列表只能在路由映射处理路由时丢弃或转发数据包或流量。例如，使用路由映射仅筛选特定路由并添加指标。

- 路由映射也有**隐式拒绝**。与数据包或流量丢弃的 ACL 和前缀列表不同，如果路由与路由映射条件不匹配，则不会重新分发该路由。

- 路由映射将处理路由重新分布的路由。例如，要添加指标，路由映射只能筛选特定的路由。如果路由与条件不匹配，路由映射将决定数据包或流量的丢弃位置。如果该路由不匹配，则不会重新分发。
- 路由映射使用命令来确定如何处理流量。要删除路由映射中的匹配条件，请使用 `no match` 命令。
- 在 BGP 路由映射中，如果重复相同的匹配语句；例如，如果匹配指标在同一序列号中具有不同的值，则只考虑最后一个匹配项和设置值。

### 配置匹配指标

```
OS10(config)# route-map hello
OS10(conf-route-map)# match metric 20
```

### 查看路由映射

```
OS10(conf-route-map)# do show route-map
route-map hello, permit, sequence 10
 Match clauses:
 metric 20
```

### 更改匹配

```
OS10(conf-route-map)# match metric 30
```

### 查看更新的路由映射

```
OS10(conf-route-map)# do show route-map
route-map hello, permit, sequence 10
 Match clauses:
 metric 30
```

要筛选重新分发的路由，请合并路由映射和 IP 前缀列表。如果路由或数据包匹配配置的条件，则 OS10 将根据前缀列表的 `permit` 或 `deny` 配置来处理路由。

当路由映射和前缀列表合并时：

- 对于具有 `permit` 操作的路由映射：
  - 如果路由与前缀列表设置为 `deny`，则会拒绝路由
  - 如果路由与前缀列表设置为 `permit`，则允许该路由，并应用任何一组操作
- 对于具有 `deny` 操作的路由映射：
  - 如果路由与前缀列表设置为 `deny`，则会拒绝路由
  - 如果路由与前缀列表设置为 `permit`，则允许该路由，并应用任何一组操作

### 查看 IP 前缀列表和路由映射配置

```
OS10(conf-router-bgp-neighbor-af)# do show ip prefix-list
ip prefix-list p1:
seq 1 deny 10.1.1.0/24
seq 10 permit 0.0.0.0/0 le 32
ip prefix-list p2:
seq 1 permit 10.1.1.0/24
seq 10 permit 0.0.0.0/0 le 32
```

### 查看路由映射配置

```
OS10(conf-router-bgp-neighbor-af)# do show route-map
route-map test1, deny, sequence 10
Match clauses:
ip address prefix-list p1
Set clauses:
route-map test2, permit, sequence 10
Match clauses:
ip address prefix-list p1
Set clauses:
route-map test3, deny, sequence 10
Match clauses:
ip address prefix-list p2
Set clauses:
route-map test4, permit, sequence 10
Match clauses:
```

```
ip address prefix-list p2
Set clauses:
```

## 匹配路由

配置路由映射的匹配条件。对于每个路由映射的 `match` 命令数没有限制，但应将匹配筛选器数减少到低于路由映射。`set` 命令不需要相应的 `match` 命令。

- 将具有特定指标值的路由与 ROUTE-MAP 模式匹配，从 0 到 4294967295。

```
match metric metric-value
```

- 将具有特定标签的路由与 ROUTE-MAP 模式匹配，从 0 到 4294967295。

```
match tag tag-value
```

- 匹配其下一跳是 ROUTE-MAP 模式下特定接口的路由。

```
match interface interface
```

- `ethernet` — 输入以太网接口信息。
- `port-channel` — 输入端口通道号。
- `vlan` — 输入 VLAN ID 号。

### 检查匹配路由

```
OS10(config)# route-map test permit 1
OS10(conf-route-map)# match tag 250000
OS10(conf-route-map)# set weight 100
```

## 设置条件

对于每个路由映射的 `set` 命令数没有限制，但应将集筛选器数减少到低于路由映射。`set` 命令不需要相应的 `match` 命令。

- 在 ROUTE-MAP 模式下，针对 BGP 路由更新输入下一跳的 IP 地址（格式为 A.B.C.D）。

```
set ip next-hop address
```

- 在 ROUTE-MAP 模式下，针对 BGP 路由更新输入下一跳的 IPv6 地址（格式为 A::B）。

```
set ipv6 next-hop address
```

- 在 ROUTE-MAP 模式下，输入 BGP 路由的 LOCAL\_PREF 属性的范围值，从 0 到 4294967295。

```
set local-preference range-value
```

- 在 ROUTE-MAP 模式下，输入重新分布的路由的度量值，从 0 到 4294967295。

```
set metric {+ | - | metric-value}
```

- 在 ROUTE-MAP 模式下，输入分布式路由的 OSPF 类型。

```
set metric-type {type-1 | type-2 | external | internal}
```

- 在 ROUTE-MAP 模式下，输入 ORIGIN 属性。

```
set origin {egp | igp | incomplete}
```

- 在 ROUTE-MAP 模式下，输入重新分布的路由的标记值，从 0 到 4294967295。

```
set tag tag-value
```

- 在 ROUTE-MAP 模式下，输入路由权重的值，从 0 到 65535。

```
set weight value
```

检查设置条件

```
OS10(config)# route-map ip permit 1
OS10(conf-route-map)# match metric 2567
```

## Continue 子句

只有 BGP 路由-映射支持 continue 子句。找到匹配项时，set 子句将运行并转发数据包 — 不会进行路由映射处理。如果您在不配置模块的情况下配置 continue 子句，则下一个顺序模块将继续。

如果您在模块的末尾配置 continue 命令，则在找到匹配项后，下一个模块仍会继续。该示例显示了路由映射模块末尾的 continue 子句 — 如果在路由映射中找到匹配项，则 test 模块 10、模块 30 将继续。

Route-map continue 子句

```
OS10(config)# route-map test permit 10
OS10(conf-route-map)# continue 30
```

## 基于 ACL 流的监控

基于流的监控可通过仅选择要镜像的所需流来节省带宽，而不是从接口镜像整个数据包。此功能可用于 L2 和 L3 入口流量。使用 ACL 规则指定基于流的监控。基于流的监控可复制传入的数据包，可与在入口端口上应用的 ACL 规则匹配并转发，或将其镜像到另一个端口。源端口为受监控的端口 (MD)，目标端口为监控端口 (MG)。

当数据包到达受监控的端口时，数据包将根据配置的 ACL 规则进行验证。如果数据包与某个 ACL 规则匹配，系统会检查相应的流处理器并执行为该端口指定的操作。如果在流处理器条目中设置了镜像操作，则会将端口详细信息发送到目标端口。

## 基于流的镜像

基于流的镜像是一种镜像会话，其中流量与镜像到目标端口的指定策略匹配。基于端口的镜像可以维护一个包含所有监控会话的数据库，包括端口监控会话。数据库包含有关针对基于流的监控已启用或未启用的会话的信息。基于流的镜像也称为基于策略的镜像。

要启用基于流的镜像，请使用 flow-based enable 命令。将检查包含穿过入口接口的特定流的流量。适当的 ACL 规则会在入口方向应用。默认情况下，未启用基于流的镜像。

要启用穿过目标端口的流量的评估和复制，请使用适用于为分配到源或受监控端口 (MD) 的 permit、deny 或 seq 命令配置监控选项。为 ACL 规则输入关键 capture session session-id 和 seq、permit 或 deny 命令，以允许或丢弃 IPv4、IPv6、ARP、UDP、EtherType、ICMP 和 TCP 数据包。

IPV4-ACL 模式

```
seq sequence-number {deny | permit} {source [mask] | any | host ip-address} [count [byte]]
[fragments] [threshold-in-msgs count] [capture session session-id]
```

如果配置了 flow-based enable 命令，但未在源端口或受监控端口上应用 ACL，则基于流的监控和端口镜像都无法正常工作。只有入口流量支持基于流的监控。

命令 show monitor session session-id 将显示输出，指示是否已启用特定会话进行流监控。

查看基于流的监控

```
OS10# show monitor session 1
S.Id Source Destination Dir SrcIP DstIP DSCP TTL State Reason

1 ethernet1/1/1 ethernet1/1/4 both N/A N/A N/A N/A true Is UP
```

## 与 ACL 规则匹配的流量

```
OS10# show ip access-lists in
Ingress IP access-list testflow
Active on interfaces :
 ethernet1/1/1
seq 5 permit icmp any any capture session 1 count (0 packets)
seq 10 permit ip 102.1.1.0/24 any capture session 1 count bytes (0 bytes)
seq 15 deny udp any any capture session 2 count bytes (0 bytes)
seq 20 deny tcp any any capture session 3 count bytes (0 bytes)
```

## 启用基于流的监控

基于流的监控通过仅镜像指定的流量（而不是所有接口流量）来节省带宽。它可用于 L2 和 L3 入口和出口流量。使用 ACL 筛选器配置要监控的流量。

1. 在监控会话模式下创建监控会话。

```
monitor session session-number type {local | rspan-source}
```

2. 在 MONITOR-SESSION 模式下，为镜像会话启用基于流的监控。

```
flow-based enable
```

3. 在 CONFIGURATION 模式下定义包含关键字 `capture session session-id` 的 ACL 规则。系统仅考虑将规则与关键字 `capture session` 相匹配的端口监控流量。

```
ip access-list
```

4. 在 INTERFACE 模式下将 ACL 应用于受监控的端口。

```
ip access-group access-list
```

### 启用基于流的监控

```
OS10(config)# monitor session 1 type local
OS10(conf-mon-local-1)# flow-based enable
OS10(config)# ip access-list testflow
OS10(conf-ipv4-acl)# seq 5 permit icmp any any capture session 1
OS10(conf-ipv4-acl)# seq 10 permit ip 102.1.1.0/24 any capture session 1 count byte
OS10(conf-ipv4-acl)# seq 15 deny udp any any capture session 2 count byte
OS10(conf-ipv4-acl)# seq 20 deny tcp any any capture session 3 count byte
OS10(conf-ipv4-acl)# exit
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip access-group testflow in
OS10(conf-if-eth1/1/1)# no shutdown
```

### 查看访问列表配置

```
OS10# show ip access-lists in
Ingress IP access-list testflow
Active on interfaces :
 ethernet1/1/1
seq 5 permit icmp any any capture session 1 count (0 packets)
seq 10 permit ip 102.1.1.0/24 any capture session 1 count bytes (0 bytes)
seq 15 deny udp any any capture session 2 count bytes (0 bytes)
seq 20 deny tcp any any capture session 3 count bytes (0 bytes)
```

### 查看监控会话

```
OS10(conf-if-eth1/1/1)# show monitor session all
S.Id Source Destination Dir SrcIP DstIP DSCP TTL State Reason

1 ethernet1/1/1 ethernet1/1/4 both N/A N/A N/A N/A true Is UP
```



# 查看 ACL 表利用率报告

show acl-table-usage detail 命令将显示各种功能及其利用率的入口和出口 ACL 表。

硬件池区域显示入口应用程序组（池）、映射到每个组的功能，以及每个池中的已用和可用空间量。在池中存储单个 ACL 规则所需的空間量取决于 TCAM 片的主要宽度。

服务池显示每个功能的已用和可用空间量。为某个功能配置的 ACL 规则数将显示在已配置的规则列中。已用行的数量取决于已配置规则应用到的端口的数量。在已分配的池下，如果您尚未单独为每个功能保留空间，对于为应用程序组分配的总池数，您可以查看为特定功能保留的专用空间的百分比或共享的短语。在下面的示例中，SYSTEM\_FLOW 功能在入口应用程序组 1 中保留 15% 的空间，池计数为 1，表示为 15:1。

|                                   |                |                 |           |                  |           |      |
|-----------------------------------|----------------|-----------------|-----------|------------------|-----------|------|
| OS10# show acl-table-usage detail |                |                 |           |                  |           |      |
| Ingress ACL utilization           |                |                 |           |                  |           |      |
| Hardware Pools                    |                |                 |           |                  |           |      |
| -----                             |                |                 |           |                  |           |      |
| Pool ID                           | App(s)         |                 |           |                  | Used rows | Free |
| rows                              | Max rows       |                 |           |                  |           |      |
| -----                             |                |                 |           |                  |           |      |
| 0                                 | SYSTEM_FLOW    |                 |           |                  | 49        |      |
| 975                               | 1024           |                 |           |                  |           |      |
| 1                                 | SYSTEM_FLOW    |                 |           |                  | 49        |      |
| 975                               | 1024           |                 |           |                  |           |      |
| 2                                 | USER_IPV4_ACL  |                 |           |                  | 3         |      |
| 1021                              | 1024           |                 |           |                  |           |      |
| 3                                 | USER_L2_ACL    |                 |           |                  | 2         |      |
| 1022                              | 1024           |                 |           |                  |           |      |
| 4                                 | USER_IPV6_ACL  |                 |           |                  | 2         |      |
| 510                               | 512            |                 |           |                  |           |      |
| 5                                 | USER_IPV6_ACL  |                 |           |                  | 2         |      |
| 510                               | 512            |                 |           |                  |           |      |
| 6                                 | FCOE           |                 |           |                  | 55        |      |
| 457                               | 512            |                 |           |                  |           |      |
| 7                                 | FCOE           |                 |           |                  | 55        |      |
| 457                               | 512            |                 |           |                  |           |      |
| 8                                 | ISCSI_SNOOPING |                 |           |                  | 12        |      |
| 500                               | 512            |                 |           |                  |           |      |
| 9                                 | FREE           |                 |           |                  | 0         |      |
| 512                               | 512            |                 |           |                  |           |      |
| 10                                | PBR_V6         |                 |           |                  | 1         |      |
| 511                               | 512            |                 |           |                  |           |      |
| 11                                | PBR_V6         |                 |           |                  | 1         |      |
| 511                               | 512            |                 |           |                  |           |      |
| -----                             |                |                 |           |                  |           |      |
| Service Pools                     |                |                 |           |                  |           |      |
| -----                             |                |                 |           |                  |           |      |
| App                               |                | Allocated pools | App group | Configured rules | Used rows | Free |
| rows                              | Max rows       |                 |           |                  |           |      |
| -----                             |                |                 |           |                  |           |      |
| USER_L2_ACL                       |                | Shared:1        | G3        | 1                | 2         |      |
| 1022                              | 1024           |                 |           |                  |           |      |
| USER_IPV4_ACL                     |                | Shared:1        | G2        | 2                | 3         |      |
| 1021                              | 1024           |                 |           |                  |           |      |
| USER_IPV6_ACL                     |                | Shared:2        | G4        | 1                | 2         |      |
| 510                               | 512            |                 |           |                  |           |      |
| PBR_V6                            |                | Shared:2        | G10       | 1                | 1         |      |
| 511                               | 512            |                 |           |                  |           |      |
| SYSTEM_FLOW                       |                | Shared:2        | G0        | 49               | 49        |      |
| 975                               | 1024           |                 |           |                  |           |      |
| ISCSI_SNOOPING                    |                | Shared:1        | G8        | 12               | 12        |      |
| 500                               | 512            |                 |           |                  |           |      |
| FCOE                              |                | Shared:2        | G6        | 55               | 55        |      |
| 457                               | 512            |                 |           |                  |           |      |
| -----                             |                |                 |           |                  |           |      |
| Egress ACL utilization            |                |                 |           |                  |           |      |

| Hardware Pools     |                    |           |                  |           |           |      |
|--------------------|--------------------|-----------|------------------|-----------|-----------|------|
| Pool ID            | App(s)             |           |                  |           | Used rows | Free |
| rows               | Max rows           |           |                  |           |           |      |
| 0                  | USER_IPV4_EGRESS   |           |                  |           | 2         |      |
| 254                | 256                |           |                  |           |           |      |
| 1                  | USER_L2_ACL_EGRESS |           |                  |           | 2         |      |
| 254                | 256                |           |                  |           |           |      |
| 2                  | USER_IPV6_EGRESS   |           |                  |           | 2         |      |
| 254                | 256                |           |                  |           |           |      |
| 3                  | USER_IPV6_EGRESS   |           |                  |           | 2         |      |
| 254                | 256                |           |                  |           |           |      |
| Service Pools      |                    |           |                  |           |           |      |
| App                | Allocated pools    | App group | Configured rules | Used rows | Free      |      |
| rows               | Max rows           |           |                  |           |           |      |
| USER_L2_ACL_EGRESS | Shared:1           | G1        | 1                | 2         |           |      |
| 254                | 256                |           |                  |           |           |      |
| USER_IPV4_EGRESS   | Shared:1           | G0        | 1                | 2         |           |      |
| 254                | 256                |           |                  |           |           |      |
| USER_IPV6_EGRESS   | Shared:2           | G2        | 1                | 2         |           |      |
| 254                | 256                |           |                  |           |           |      |

## 已知行为

- 在 S4200-ON 平台上，show acl-table-usage detail 命令输出将列出多个可用的硬件池 (FREE)，但当系统创建新的服务池时，您将看到“ACL CAM 表已满”警告日志。系统将无法创建任何新的服务池。但是，现有组可以继续增长到最大可用池空间。
- 在 S4200-ON 平台上，show acl-table usage detail 命令输出将列出入口 ACL 利用率表下的所有可用硬件池，并在出口 ACL 利用率表下显示无。只有在配置出口 ACL 时，系统才会为出口 ACL 表分配池空间。您可以再次运行 show acl-table-usage detail 命令，以查看在出口 ACL 利用率表下分配的池空间。
- 在 S52xx-ON、Z91xx-ON、Z92xx-ON 平台上，在每个功能的服务池下列出的已配置规则数是 ACL 数乘以应用它们的端口数。此数字是累积的。您可以查看已用行和可用行，以指示硬件中已使用和可用的实际空间量。

## ACL 日志记录

您可以配置 ACL 以筛选流量、丢弃或转发与特定条件匹配的数据包。ACL 日志记录功能允许您获取与在入站方向上接口上应用的访问控制列表条目 (ACE) 匹配的数据包的附加信息。

当匹配的数据包命中已启用日志的 ACL 条目时，OS10 将创建一条日志消息，其中包含有关数据包的附加信息。

ACL 日志记录有助于管理穿过网络的流量，并且对网络监管和维护活动非常有用。

大容量网络流量可能会导致大量日志，这可能会对系统性能和效率造成负面影响。

您可以指定创建日志的阈值以及必须创建日志的时间间隔。

阈值定义初始数据包匹配后创建日志消息的频率。默认值为 10 条消息。此值可配置，范围为 1 到 100。

默认情况下，时间间隔设置为 5 分钟，日志每 5 分钟创建一次。在此间隔期间，系统将继续对照配置的 ACL 规则检查数据包，并允许或拒绝流量，但日志记录会暂时暂停。此值可配置，范围为 1 至 10 分钟。

例如，如果您将阈值配置为 20，而间隔为 10 分钟，则在初始数据包匹配后，将记录与该 ACL 条目匹配的第 20 个数据包。系统将等待 10 分钟的时间间隔，在此期间不会进行日志记录。间隔时间过后，将再次记录与 ACL 条目匹配的 20 个数据包。

## 重要事项

ACL 日志记录功能是：

- 仅适用于 IPv4 和 IPv6 用户 ACL。不会记录 MAC ACL。
- 仅适用于在入站方向的接口上应用的用户 ACL。即使无法为出站 ACL 启用 ACL 日志记录，也会应用 ACL 配置。

如果已启用 ACL 日志记录，则从版本 10.4.3.0 降级到以前的版本将失败，并且不应用相应的 ACL 规则。在降级之前，请确保禁用 ACL 日志记录或删除启动配置。

Dell EMC 建议您不要启用控制平面协议相同用户 ACL 条目的日志记录。

DELL EMC 建议启用 128 日志的 ACL 条目的最大比例。如果无法在未来的 ACL 条目上启用日志记录，则会显示 syslog 错误消息，指示无法启用日志记录。但是，将应用 ACL 条目。

## ACL 命令

### clear ip access-list counters

清除特定访问列表的 ACL 计数器。

|        |                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>clear ip access-list counters [access-list-name]</code>                                                                                 |
| 参数     | <code>access-list-name</code> — (可选) 输入要清除计数器的 IP 访问列表的名称。最多 140 个字符。                                                                         |
| 默认     | 未配置                                                                                                                                           |
| 命令模式   | EXEC                                                                                                                                          |
| 使用情况信息 | 如果不输入访问列表名称，则所有 IPv6 访问列表计数器都将清除。计数器将计算匹配访问列表中的每个允许或拒绝语句的数据包数。要获取与访问列表匹配的最新数据包数，请清除要从零开始的计数器。要查看访问列表信息，请使用 <code>show access-lists</code> 命令。 |
| 示例     | <pre>OS10# clear ip access-list counters</pre>                                                                                                |
| 支持的版本  | 10.2.0E or later                                                                                                                              |

### clear ipv6 access-list counters

清除特定访问列表的 IPv6 访问列表计数器。

|        |                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>clear ipv6 access-list counters [access-list-name]</code>                                                                               |
| 参数     | <code>access-list-name</code> — (可选) 输入要清除计数器的 IPv6 访问列表的名称。最多 140 个字符。                                                                       |
| 默认     | 未配置                                                                                                                                           |
| 命令模式   | EXEC                                                                                                                                          |
| 使用情况信息 | 如果不输入访问列表名称，则所有 IPv6 访问列表计数器都将清除。计数器将计算匹配访问列表中的每个允许或拒绝语句的数据包数。要获取与访问列表匹配的最新数据包数，请清除要从零开始的计数器。要查看访问列表信息，请使用 <code>show access-lists</code> 命令。 |
| 示例     | <pre>OS10# clear ipv6 access-list counters</pre>                                                                                              |
| 支持的版本  | 10.2.0E or later                                                                                                                              |

## clear mac access-list counters

清除特定或所有 MAC 访问列表的计数器。

|               |                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>clear mac access-list counters [access-list-name]</code>                                                                               |
| <b>参数</b>     | <code>access-list-name</code> — (可选) 输入要清除计数器的 MAC 访问列表的名称。最多 140 个字符。                                                                       |
| <b>默认</b>     | 未配置                                                                                                                                          |
| <b>命令模式</b>   | EXEC                                                                                                                                         |
| <b>使用情况信息</b> | 如果不输入访问列表名称，则所有 MAC 访问列表计数器都将清除。计数器将计算匹配访问列表中的每个允许或拒绝语句的数据包数。要获取与访问列表匹配的最近数据包数，请清除要从零开始的计数器。要查看访问列表信息，请使用 <code>show access-lists</code> 命令。 |
| <b>示例</b>     | <pre>OS10# clear mac access-list counters</pre>                                                                                              |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                             |

## deny

配置筛选器以丢弃具有特定 IP 地址的数据包。

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>deny [protocol-number   icmp   ip   tcp   udp] [A.B.C.D   A.B.C.D/x   any   host ip-address] [A.B.C.D   A.B.C.D/x   any   host ip-address] [capture   count   dscp value   fragment   log]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>参数</b>     | <ul style="list-style-type: none"><li>• <code>protocol-number</code> — (可选) 输入 IP 标头中标识的协议号，从 0 到 255。</li><li>• <code>icmp</code> — (可选) 输入要拒绝的 ICMP 地址。</li><li>• <code>ip</code> — (可选) 输入要拒绝的 IP 地址。</li><li>• <code>tcp</code> — (可选) 输入要拒绝的 TCP 地址。</li><li>• <code>udp</code> — (可选) 输入要拒绝的 UDP 地址。</li><li>• <code>A.B.C.D</code> — 以点分隔的十进制格式输入 IP 地址。</li><li>• <code>A.B.C.D/x</code> — 输入与点分十进制地址匹配的位数。</li><li>• <code>any</code> — (可选) 输入关键字 <code>any</code> 以指定任何源或目标 IP 地址。</li><li>• <code>host ip-address</code> — (可选) 输入关键字和 IP 地址，以仅使用主机地址。</li><li>• <code>capture</code> — (可选) 捕获筛选器处理的数据包。</li><li>• <code>count</code> — (可选) 计算筛选器处理的数据包数。</li><li>• <code>byte</code> — (可选) 计算筛选器处理的字节数。</li><li>• <code>dscp value</code> — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。</li><li>• <code>fragment</code> — (可选) 使用 ACL 控制数据包片段。</li><li>• <code>log</code> — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li></ul> |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>命令模式</b>   | IPv4-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>使用情况信息</b> | OS10 不能同时计算数据包和字节数；使用 <code>count byte</code> 选项时，仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>示例</b>     | <pre>OS10(config)# ip access-list testflow OS10(conf-ip4-acl)# deny udp any any</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## deny (IPv6)

配置筛选器以丢弃具有特定 IPv6 地址的数据包。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>deny [protocol-number   icmp   ipv6   tcp   udp] [A::B   A::B/x   any   host ipv6-address] [A::B   A::B/x   any   host ipv6-address] [capture   count   dscp value   fragment   log]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 参数     | <ul style="list-style-type: none"><li>• <code>protocol-number</code> — (可选) 输入 IP 标头中标识的协议号, 从 0 到 255。</li><li>• <code>icmp</code> — (可选) 输入要拒绝的 ICMP 地址。</li><li>• <code>ipv6</code> — (可选) 输入要拒绝的 IPv6 地址。</li><li>• <code>tcp</code> — (可选) 输入要拒绝的 TCP 地址。</li><li>• <code>udp</code> — (可选) 输入要拒绝的 UDP 地址。</li><li>• <code>A::B</code> — 以点分隔的十进制格式输入 IPv6 地址。</li><li>• <code>A::B/x</code> — 输入与 IPv6 地址匹配的位数。</li><li>• <code>any</code> — (可选) 输入关键字 <code>any</code> 以指定任何源或目标 IP 地址。</li><li>• <code>host ipv6-address</code> — (可选) 输入关键字和 IPv6 地址, 以仅使用主机地址。</li><li>• <code>capture</code> — (可选) 捕获筛选器处理的数据包。</li><li>• <code>count</code> — (可选) 计算筛选器处理的数据包数。</li><li>• <code>byte</code> — (可选) 计算筛选器处理的字节数。</li><li>• <code>dscp value</code> — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。</li><li>• <code>fragment</code> — (可选) 使用 ACL 控制数据包片段。</li><li>• <code>log</code> — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 命令模式   | IPV6-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 使用情况信息 | OS10 不能同时计算数据包和字节数; 使用 <code>count byte</code> 选项时, 仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 示例     | <pre>OS10(config)# ipv6 access-list ipv6test OS10(conf-ipv6-acl)# deny ipv6 any any capture session 1</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## deny (MAC)

配置筛选器以丢弃具有特定 MAC 地址的数据包。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>deny {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00]   any} {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00]   any} [protocol-number   capture   cos   count   vlan]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 参数     | <ul style="list-style-type: none"><li>• <code>nn:nn:nn:nn:nn:nn</code> — 输入要发送或发送到的数据包的网络的 MAC 地址。</li><li>• <code>00:00:00:00:00:00</code> — (可选) 输入 MAC 地址中的哪些位必须匹配。如果不输入掩码, 则将应用 <code>00:00:00:00:00:00</code> 掩码。</li><li>• <code>any</code> — (可选) 根据筛选器设置路由。<ul style="list-style-type: none"><li>◦ <code>protocol-number</code> — (可选) 在标头中标识的 MAC 协议编号, 从 600 到 ffff。</li><li>◦ <code>capture</code> — (可选) 捕获筛选器处理的数据包。</li><li>◦ <code>cos</code> — (可选) CoS 值, 从 0 到 7。</li><li>◦ <code>count</code> — (可选) 计算筛选器处理的数据包数。</li><li>◦ <code>vlan</code> — (可选) VLAN ID 号, 从 1 到 4093。</li></ul></li></ul> |
| 默认     | 已禁用                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 命令模式   | MAC-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 使用情况信息 | OS10 不能同时计算数据包和字节数; 使用 <code>count byte</code> 选项时, 仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## 示例

```
OS10(config)# mac access-list macacl
OS10(conf-mac-acl)# deny any any cos 7
OS10(conf-mac-acl)# deny any any vlan 2
```

## 支持的版本

10.2.0E or later

# deny icmp

配置筛选器以丢弃所有或特定的互联网控制消息协议 (ICMP) 消息。

## 语法

```
deny icmp [A.B.C.D | A.B.C.D/x | any | host ip-address] [[A.B.C.D |
A.B.C.D/x | any | host ip-address] [capture | count | dscp value | fragment
| log]
```

## 参数

- A.B.C.D — 以十六进制格式输入采用冒号分隔的 IP 地址。
- A.B.C.D/x — 输入要与 IP 地址匹配的位数。
- any — (可选) 输入关键字 any 以指定任何源或目标 IP 地址。
- host ip-address — (可选) 输入 IP 地址以仅使用主机地址。
- capture — (可选) 捕获筛选器处理的数据包。
- count — (可选) 计算筛选器处理的数据包数。
- byte — (可选) 计算筛选器处理的字节数。
- dscp value — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
- fragment — (可选) 使用 ACL 控制数据包片段。
- log — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

## 默认

未配置

## 命令模式

IPV4-ACL

## 使用情况信息

OS10 不能同时计算数据包和字节数; 使用 count byte 选项时, 仅增加字节数。此命令的 no 版本将移除筛选器。

## 示例

```
OS10(config)# ip access-list egress
OS10(conf-ipv4-acl)# deny icmp any any capture session 1
```

## 支持的版本

10.2.0E or later

# deny icmp (IPv6)

配置筛选器以丢弃所有或特定 ICMP 消息。

## 语法

```
deny icmp [A::B | A::B/x | any | host ipv6-address] [A::B | A::B/x | any |
host ipv6-address] [capture | count | dscp value | fragment | log]
```

## 参数

- A::B — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
- A::B/x — 输入与 IPv6 地址匹配的位数。
- any — (可选) 输入关键字 any 以指定任何源或目标 IP 地址。
- host ipv6-address — (可选) 输入 IPv6 地址, 以仅使用主机地址。
- capture — (可选) 捕获筛选器处理的数据包。
- count — (可选) 计算筛选器处理的数据包数。
- byte — (可选) 计算筛选器处理的字节数。
- dscp value — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
- fragment — (可选) 使用 ACL 控制数据包片段。
- log — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

## 默认

未配置

## 命令模式

IPV6-ACL

## 使用情况信息

OS10 不能同时计算数据包和字节数; 使用 count byte 选项时, 仅增加字节数。此命令的 no 版本将移除筛选器。

## 示例

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# deny icmp any any capture session 1
```

## 支持的版本

10.2.0E or later

# deny ip

配置筛选器以从 IPv4 地址中丢弃所有或特定数据包。

## 语法

```
deny ip [A.B.C.D | A.B.C.D/x | any | host ip-address] [[A.B.C.D | A.B.C.D/x | any | host ip-address] [capture | count [byte] | dscp value | fragment]
```

## 参数

- A.B.C.D — 以点分隔的十进制格式输入 IPv4 地址。
- A.B.C.D/x — 输入与点分十进制地址匹配的位数。
- any — (可选) 设置受筛选器约束的所有路由：
  - capture — (可选) 捕获筛选器处理的数据包。
  - count — (可选) 计算筛选器处理的数据包数。
  - byte — (可选) 计算筛选器处理的字节数。
  - dscp value — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
  - fragment — (可选) 使用 ACL 控制数据包片段。
- host ip-address — (可选) 输入 IPv4 地址, 以仅使用主机地址。

## 默认

未配置

## 命令模式

IPV4-ACL

## 使用情况信息

OS10 不能同时计算数据包和字节数; 使用 count byte 选项时, 仅增加字节数。此命令的 no 版本将移除筛选器。

## 示例

```
OS10(config)# ip access-list testflow
OS10(conf-ipv4-acl)# deny ip any any capture session 1 count
```

## 支持的版本

10.2.0E or later

# deny ipv6

配置筛选器以从 IPv6 地址丢弃所有或特定数据包。

## 语法

```
deny ipv6 [A::B | A::B/x | any | host ipv6-address] [A::B | A::B/x | any | host ipv6-address] [capture | count [byte] | dscp | fragment]
```

## 参数

- A::B — (可选) 输入从中发送数据包的源 IPv6 地址和目标地址。
- A::B/x — (可选) 以 /前缀格式 (/x) 和目标掩码输入源网络掩码。
- any — (可选) 设置受筛选器约束的所有路由：
  - capture — (可选) 捕获筛选器处理的数据包。
  - count — (可选) 计算筛选器处理的数据包数。
  - byte — (可选) 计算筛选器处理的字节数。
  - dscp value — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
  - fragment — (可选) 使用 ACL 控制数据包片段。
- host ipv6-address — (可选) 输入 IPv6 地址, 以仅使用主机地址。

## 默认

未配置

## 命令模式

IPV6-ACL

## 使用情况信息

OS10 不能同时计算数据包和字节数; 使用 count byte 选项时, 仅增加字节数。此命令的 no 版本将移除筛选器。

## 示例

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# deny ipv6 any any capture session 1
```



支持的版本 10.2.0E or later

## deny tcp

配置筛选器以丢弃符合筛选条件的传输控制协议 (TCP) 数据包。

**语法** `deny tcp [A.B.C.D | A.B.C.D/x | any | host ip-address [operator]] [[A.B.C.D | A.B.C.D/x | any | host ip-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | count | dscp value | fragment | log]`

- 参数**
- A.B.C.D — 以 A.B.C.D 格式输入 IPv4 地址。
  - A.B.C.D/x — 以 A.B.C.D/x 格式输入匹配的位数。
  - any — (可选) 输入关键字 any 以指定任何源或目标 IP 地址。
  - host ip-address — (可选) 输入关键字和 IPv4 地址, 以仅使用主机地址。
  - ack — (可选) 将“位”设置为“确认”。
  - fin — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。
  - psh — (可选) 将“位”设置为“推送”。
  - rst — (可选) 将“位”设置为“重置”。
  - syn — (可选) 将“位”设置为“同步”。
  - urg — (可选) 将“位”设置为“紧急”。
  - capture — (可选) 捕获筛选器处理的数据包。
  - count — (可选) 计算筛选器处理的数据包数。
  - byte — (可选) 计算筛选器处理的字节数。
  - dscp value — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
  - fragment — (可选) 使用 ACL 控制数据包片段。
  - log — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。
  - operator — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用:
    - eq — 等于
    - gt — 大于
    - lt — 小于
    - neq — 不等于
    - range — 端口范围, 包括指定的端口号。

**默认** 未配置

**命令模式** IPV4-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数; 使用 count byte 选项时, 仅增加字节数。此命令的 no 版本将移除筛选器。

**示例**

```
OS10(config)# ip access-list testflow
OS10(conf-ip4-acl)# deny tcp any any capture session 1
```

支持的版本 10.2.0E or later

## deny tcp (IPv6)

配置将丢弃符合筛选条件的 TCP IPv6 数据包的筛选器。

**语法** `deny tcp [A::B | A::B/x | any | host ipv6-address [operator]] [A::B | A:B/x | any | host ipv6-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | count | dscp value | fragment | log]`

- 参数**
- A::B — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
  - A::B/x — 输入与 IPv6 地址匹配的位数。
  - any — (可选) 输入关键字 any 以指定任何源或目标 IP 地址。
  - host ipv6-address — (可选) 输入 IPv6 地址, 以仅使用主机地址。
  - capture — (可选) 捕获筛选器处理的数据包。
  - count — (可选) 计算筛选器处理的数据包数。



- `byte` — (可选) 计算筛选器处理的字节数。
- `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
- `fragment` — (可选) 使用 ACL 控制数据包片段。
- `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。
- `operator` — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用：
  - `eq` — 等于
  - `gt` — 大于
  - `lt` — 小于
  - `neq` — 不等于
  - `range` — 端口范围, 包括指定的端口号。

**默认** 未配置

**命令模式** IPV6-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数; 使用 `count byte` 选项时, 仅增加字节数。此命令的 `no` 版本将移除筛选器。

**示例**

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# deny tcp any any capture session 1
```

**支持的版本** 10.2.0E or later

## deny udp

配置筛选器以丢弃符合筛选条件的用户数据报协议 (UDP) 数据包。

**语法** `deny udp [A.B.C.D | A.B.C.D/x | any | host ip-address [operator]] [A.B.C.D | A.B.C.D/x | any | host ip-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | count | dscp value | fragment | log]`

**参数**

- `A.B.C.D` — 以点分隔的十进制格式输入 IPv4 地址。
- `A.B.C.D/x` — 输入与点分十进制地址匹配的位数。
- `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
- `host ip-address` — (可选) 输入 IPv4 地址, 以仅使用主机地址。
- `ack` — (可选) 将“位”设置为“确认”。
- `fin` — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。
- `psh` — (可选) 将“位”设置为“推送”。
- `rst` — (可选) 将“位”设置为“重置”。
- `syn` — (可选) 将“位”设置为“同步”。
- `urg` — (可选) 将“位”设置为“紧急”。
- `capture` — (可选) 捕获筛选器处理的数据包。
- `count` — (可选) 计算筛选器处理的数据包数。
- `byte` — (可选) 计算筛选器处理的字节数。
- `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
- `fragment` — (可选) 使用 ACL 控制数据包片段。
- `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。
- `operator` — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用：
  - `eq` — 等于
  - `gt` — 大于
  - `lt` — 小于
  - `neq` — 不等于
  - `range` — 端口范围, 包括指定的端口号。

**默认** 未配置

**命令模式** IPV4-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数; 使用 `count byte` 选项时, 仅增加字节数。此命令的 `no` 版本将移除筛选器。

## 示例

```
OS10(config)# ip access-list testflow
OS10(conf-ip4-acl)# deny udp any any capture session 1
```

支持的版本 10.2.0E or later

## deny udp (IPv6)

配置筛选器以丢弃与筛选条件匹配的 UDP IPv6 数据包。

**语法** deny udp [A::B | A::B/x | any | host ipv6-address [operator]] [A::B | A::B/x | any | host ipv6-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | count | dscp value | fragment | log]

- 参数**
- A::B — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
  - A::B/x — 输入与 IPv6 地址匹配的位数。
  - any — (可选) 输入关键字 any 以指定任何源或目标 IP 地址。
  - host ipv6-address — (可选) 输入关键字和 IPv6 地址，以仅使用主机地址。
  - ack — (可选) 将“位”设置为“确认”。
  - fin — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。
  - psh — (可选) 将“位”设置为“推送”。
  - rst — (可选) 将“位”设置为“重置”。
  - syn — (可选) 将“位”设置为“同步”。
  - urg — (可选) 将“位”设置为“紧急”。
  - capture — (可选) 捕获筛选器处理的数据包。
  - count — (可选) 计算筛选器处理的数据包数。
  - byte — (可选) 计算筛选器处理的字节数。
  - dscp value — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
  - fragment — (可选) 使用 ACL 控制数据包片段。
  - log — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。
  - operator — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用：
    - eq — 等于
    - gt — 大于
    - lt — 小于
    - neq — 不等于
    - range — 端口范围，包括指定的端口号。

**默认** 未配置

**命令模式** IPV6-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数；使用 count byte 选项时，仅增加字节数。此命令的 no 版本将移除筛选器。

## 示例

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# deny udp any any capture session 1
```

支持的版本 10.2.0E or later

## description

配置 ACL 说明。

**语法** description text

**参数** text — 输入说明文本字符串。最多 80 个字符。

**默认** 已禁用

**命令模式** IPV4-ACL、IPV6-ACL、MAC-ACL

**使用情况信息** 此命令的 `no` 版本将删除 ACL 说明。

**示例**

```
OS10(conf-ipv4-acl)# description ipacltest
```

**支持的版本** 10.2.0E or later

## ip access-group

配置 IPv4 访问组。

**语法** `ip access-group access-list-name {in | out}`

**参数**

- `access-list-name` — 输入 IPv4 访问列表的名称。最多 140 个字符。
- `in` — 将 ACL 应用于传入流量。
- `out` — 将 ACL 应用于传出流量。

**默认** 未配置

**命令模式** INTERFACE  
CONTROL-PLANE

**使用情况信息** 在 CONTROL-PLANE 模式下使用此命令可应用控制平面 ACL。控制平面 ACL 仅应用于入口流量。默认情况下，控制平面 ACL 应用于前面板端口和管理端口。此命令的 `no` 版本将删除 IPv4 ACL 配置。

**示例**

```
OS10(conf-if-eth1/1/8)# ip access-group testgroup in
```

**示例（控制平面 ACL）**

```
OS10# configure terminal
OS10(config)# control-plane
OS10(config-control-plane)# ip access-group aaa-cp-acl in
```

**支持的版本** 10.2.0E or later; 10.4.1 或更高版本（控制平面 ACL）

## ip access-list

创建要根据 IP 地址筛选的 IP 访问列表。

**语法** `ip access-list access-list-name`

**参数** `access-list-name` — 输入 IPv4 访问列表的名称。最多 140 个字符。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 无

**示例**

```
OS10(config)# ip access-list acl1
```

**支持的版本** 10.2.0E or later

## ip as-path access-list

使用正则表达式为 BGP 路由创建 AS 路径 ACL 筛选器。

**语法** `ip as-path access-list name {deny | permit} regexp-string`

**参数**

- `name` — 输入访问列表名称。
- `deny | permit` — 拒绝或接受匹配的路由。
- `regexp-string` — 输入正则表达式字符串以匹配 AS 路径路由属性。

|        |                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                               |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                     |
| 使用情况信息 | <p>您可以在入站和出站 BGP 路由上指定访问列表筛选器。ACL 筛选器由正则表达式组成。如果正则表达式与 BGP 路由中的 AS 路径属性匹配，则该路由将被拒绝或接受。AS 路径不包含本地 AS 编号。如果指定 <code>deny</code> 和 <code>regex</code>，此命令的 <code>no</code> 版本将移除单个访问列表条目。否则，将移除整个访问列表。</p> <p>正则表达式中不支持 question mark (?) 字符。所有其他特殊字符均受支持。当在正则表达式中使用 backslash (\) 或 double quotes (") 时，请在这些字符前面加上 backslash (\)。例如，输入 \\ 或 \"。</p> |
| 示例     | <pre>OS10(config)# ip as-path access-list abc deny 123</pre>                                                                                                                                                                                                                                                                                      |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                  |

## ip community-list standard deny

为 BGP 创建用于拒绝访问的标准社区列表。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip community-list standard name deny {aa:nn   no-advertise   local-AS   no-export   internet}</code>                                                                                                                                                                                                                                                                                                                |
| 参数     | <ul style="list-style-type: none"> <li><b>name</b> — 输入用于识别一个或多个拒绝社区组的标准社区列表的名称。</li> <li><b>aa:nn</b> — 以 <code>aa:nn</code> 格式输入社区编号，其中 <code>aa</code> 是标识自治系统的编号，<code>nn</code> 是标识自治系统中的社区的数字。</li> <li><b>no-advertise</b> — BGP 不会将此路由通告给任何内部或外部对等。</li> <li><b>local-AS</b> — BGP 不会将此路由通告给外部对等方。</li> <li><b>no-export</b> — BGP 不会在 BGP 联合边界外部通告此路由。</li> <li><b>internet</b> — BGP 不会将此路由通告给互联网社区。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                             |
| 使用情况信息 | 此命令的 <code>no</code> 版本将移除社区列表。                                                                                                                                                                                                                                                                                                                                                                                           |
| 示例     | <pre>OS10(config)# ip community-list standard STD_LIST deny local-AS</pre>                                                                                                                                                                                                                                                                                                                                                |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                                                                                          |

## ip community-list standard permit

创建 BGP 的标准社区列表以允许访问。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ip community-list standard name permit {aa:nn   no-advertise   local-as   no-export   internet}</code>                                                                                                                                                                                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"> <li><b>name</b> — 输入用于识别一个或多个拒绝社区组的标准社区列表的名称。</li> <li><b>aa:nn</b> — 以 <code>aa:nn</code> 格式输入社区编号，其中 <code>aa</code> 是标识自治系统的编号，<code>nn</code> 是标识自治系统中的社区的数字。</li> <li><b>no-advertise</b> — BGP 不会将此路由通告给任何内部或外部对等。</li> <li><b>local-as</b> — BGP 不会将此路由通告给外部对等方。</li> <li><b>no-export</b> — BGP 不会在 BGP 联合边界外部通告此路由。</li> <li><b>internet</b> — BGP 不会将此路由通告给互联网社区。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                             |
| 使用情况信息 | 此命令的 <code>no</code> 版本将移除社区列表。                                                                                                                                                                                                                                                                                                                                                                                           |

## 示例

```
OS10(config)# ip community-list standard STD_LIST permit local-AS
```

## 支持的版本

10.3.0E or later

# ip extcommunity-list standard deny

为 BGP 创建扩展社区列表以拒绝访问。

## 语法

```
ip extcommunity-list standard name deny {4byteas-generic | rt | soo}
```

## 参数

- *name* — 输入用于标识一个或多个扩展社区的拒绝组的社区列表的名称。
- *4byteas-generic* — 输入通用扩展社区，然后是关键字 *transitive* 或 *non-transitive*。
- *rt* — 输入路由目标。
- *soo* — 输入路由来源或站点原件。

## 默认

未配置

## 命令模式

CONFIGURATION

## 使用情况信息

此命令的 *no* 版本将移除扩展社区列表。

## 示例

```
OS10(config)# ip extcommunity-list standard STD_LIST deny 4byteas-generic transitive 1.65534:40
```

## 支持的版本

10.3.0E or later

# ip extcommunity-list standard permit

为 BGP 创建扩展社区列表以允许访问。

## 语法

```
ip extcommunity-list standard name permit {4byteas-generic | rt | soo}
```

## 参数

- *name* — 输入用于标识一个或多个扩展社区的允许组的社区列表的名称。
- *rt* — 输入路由目标。
- *soo* — 输入路由来源或站点原件。

## 默认

未配置

## 命令模式

CONFIGURATION

## 使用情况信息

此命令的 *no* 版本将移除扩展社区列表。

## 示例

```
OS10(config)# ip extcommunity-list standard STD_LIST permit 4byteas-generic transitive 1.65412:60
```

## 支持的版本

10.3.0E or later

# ip prefix-list description

配置 IP 前缀列表的说明。

## 语法

```
ip prefix-list name description
```

## 参数

- *name* — 输入前缀列表的名称。
- *description* — 输入命名的前缀列表的说明。

## 默认

未配置

## 命令模式

CONFIGURATION

## 使用情况信息

此命令的 *no* 版本会移除指定的前缀列表。

## 示例

```
OS10(config)# ip prefix-list TEST description TEST_LIST
```

## 支持的版本

10.3.0E or later

# ip prefix-list deny

创建前缀列表以拒绝来自指定网络地址的路由筛选。

## 语法

```
ip prefix-list name deny [A.B.C.D/x [ge | le]] prefix-len
```

## 参数

- *name* — 输入前缀列表的名称。
- *A.B.C.D/x* — (可选) 以 /前缀格式 (/x) 输入源网络地址和掩码。
- *ge* — 输入以指示大于或等于指定范围的网络地址。
- *le* — 输入以指示小于或等于指定范围的网络地址。
- *prefix-len* — 输入前缀长度。

## 默认

未配置

## 命令模式

CONFIGURATION

## 使用情况信息

此命令的 *no* 版本将移除指定的前缀-列表。

## 示例

```
OS10(config)# ip prefix-list denyprefix deny 10.10.10.2/16 le 30
```

## 支持的版本

10.3.0E or later

# ip prefix-list permit

创建前缀列表以允许来自指定网络地址的路由筛选。

## 语法

```
ip prefix-list name permit [A.B.C.D/x [ge | le]] prefix-len
```

## 参数

- *name* — 输入前缀列表的名称。
- *A.B.C.D/x* — (可选) 以 /前缀格式 (/x) 输入源网络地址和掩码。
- *ge* — 输入以指示大于或等于指定范围的网络地址。
- *le* — 输入以指示小于或等于指定范围的网络地址。
- *prefix-len* — 输入前缀长度。

## 默认

未配置

## 命令模式

CONFIGURATION

## 使用情况信息

此命令的 *no* 版本将移除指定的前缀-列表。

## 示例

```
OS10(config)# ip prefix-list allowprefix permit 10.10.10.1/16 ge 10
```

## 支持的版本

10.3.0E or later

# ip prefix-list seq deny

配置筛选器以拒绝从指定前缀列表进行路由筛选。

## 语法

```
ip prefix-list name seq num deny {A.B.C.D/x [ge | le] prefix-len}
```

## 参数

- *name* — 输入前缀列表的名称。
- *num* — 输入序列列表编号。
- *A.B.C.D/x* — 以 /前缀格式 (/x) 输入源网络地址和掩码。
- *ge* — 输入以指示大于或等于指定范围的网络地址。
- *le* — 输入以指示小于或等于指定范围的网络地址。

|        |                                                                                               |
|--------|-----------------------------------------------------------------------------------------------|
| 默认     | <ul style="list-style-type: none"> <li><code>prefix-len</code> — 输入前缀长度。</li> </ul>           |
| 命令模式   | 未配置                                                                                           |
| 使用情况信息 | CONFIGURATION                                                                                 |
| 示例     | 此命令的 <code>no</code> 版本会移除指定的前缀列表。                                                            |
| 支持的版本  | OS10(config)# ip prefix-list seqprefix seq 65535 deny 10.10.10.1/16 ge 10<br>10.3.0E or later |

## ip prefix-list seq permit

配置筛选器以允许从指定前缀列表进行路由筛选。

|        |                                                                                                                                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ipv6 prefix-list [name] seq num permit A::B/x [ge   le] prefix-len</code>                                                                                                                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"> <li><code>name</code> — 输入前缀列表的名称。</li> <li><code>num</code> — 输入序列列表编号。</li> <li><code>A.B.C.D/x</code> — 以 /前缀格式 (/x) 输入源网络地址和掩码。</li> <li><code>ge</code> — 输入以指示大于或等于指定范围的网络地址。</li> <li><code>le</code> — 输入以指示小于或等于指定范围的网络地址。</li> <li><code>prefix-len</code> — 输入前缀长度。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                          |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                |
| 使用情况信息 | 此命令的 <code>no</code> 版本会移除指定的前缀列表。                                                                                                                                                                                                                                                                                           |
| 示例     | OS10(config)# ip prefix-list seqprefix seq 65535 permit 10.10.10.1/16 le 30                                                                                                                                                                                                                                                  |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                             |

## ipv6 access-group

配置 IPv6 访问组。

|              |                                                                                                                                                                                                    |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法           | <code>ipv6 access-group access-list-name {in   out}</code>                                                                                                                                         |
| 参数           | <ul style="list-style-type: none"> <li><code>access-list-name</code> — 输入 IPv6 ACL 的名称。最多 140 个字符。</li> <li><code>in</code> — 将 ACL 应用于传入流量。</li> <li><code>out</code> — 将 ACL 应用于传出流量。</li> </ul> |
| 默认           | 未配置                                                                                                                                                                                                |
| 命令模式         | INTERFACE<br>CONTROL-PLANE                                                                                                                                                                         |
| 使用情况信息       | 在 CONTROL-PLANE 模式下使用此命令可应用控制平面 ACL。控制平面 ACL 仅应用于入口流量。默认情况下，控制平面 ACL 应用于前面板端口和管理端口。此命令的 <code>no</code> 版本将移除 IPv6 ACL 配置。                                                                         |
| 示例           | OS10(conf-if-eth1/1/8)# ipv6 access-group test6 in                                                                                                                                                 |
| 示例（控制平面 ACL） | OS10# configure terminal<br>OS10(config)# control-plane<br>OS10(config-control-plane)# ipv6 access-group aaa-cp-acl in                                                                             |
| 支持的版本        | 10.2.0E or later; 10.4.1 或更高版本（控制平面 ACL）                                                                                                                                                           |

## ipv6 access-list

基于 IPv6 地址创建要筛选的 IP 访问列表。

|        |                                                             |
|--------|-------------------------------------------------------------|
| 语法     | <code>ipv6 access-list access-list-name</code>              |
| 参数     | <code>access-list-name</code> — 输入 IPv6 访问列表的名称。最多 140 个字符。 |
| 默认     | 未配置                                                         |
| 命令模式   | CONFIGURATION                                               |
| 使用情况信息 | 无                                                           |
| 示例     | <pre>OS10(config)# ipv6 access-list acl6</pre>              |
| 支持的版本  | 10.2.0E or later                                            |

## ipv6 prefix-list deny

创建前缀列表以拒绝来自指定 IPv6 网络地址的路由筛选。

|        |                                                                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ipv6 prefix-list prefix-list-name deny {A::B/x [ge   le] prefix-len}</code>                                                                                                                                                                                                               |
| 参数     | <ul style="list-style-type: none"><li>• <code>prefix-list-name</code> — 输入 IPv6 前缀列表名称。</li><li>• <code>A::B/x</code> — 输入要拒绝的 IPv6 地址。</li><li>• <code>ge</code> — 输入以指示大于或等于指定范围的网络地址。</li><li>• <code>le</code> — 输入以指示小于或等于指定范围的网络地址。</li><li>• <code>prefix-len</code> — 输入前缀长度。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                             |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                   |
| 使用情况信息 | 此命令的 <code>no</code> 版本会移除指定的前缀列表。                                                                                                                                                                                                                                                              |
| 示例     | <pre>OS10(config)# ipv6 prefix-list TEST deny AB10::1/128 ge 10 le 30</pre>                                                                                                                                                                                                                     |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                |

## ipv6 prefix-list description

配置 IPv6 前缀列表的说明。

|        |                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>ipv6 prefix-list name description</code>                                                                                            |
| 参数     | <ul style="list-style-type: none"><li>• <code>name</code> — 输入 IPv6 前缀列表的名称。</li><li>• <code>description</code> — 输入命名的前缀列表的说明。</li></ul> |
| 默认     | 未配置                                                                                                                                       |
| 命令模式   | CONFIGURATION                                                                                                                             |
| 使用情况信息 | 此命令的 <code>no</code> 版本会移除指定的前缀列表。                                                                                                        |
| 示例     | <pre>OS10(config)# ipv6 prefix-list TEST description TEST_LIST</pre>                                                                      |
| 支持的版本  | 10.3.0E or later                                                                                                                          |



## ipv6 prefix-list permit

创建前缀列表以允许来自指定 IPv6 网络地址的路由筛选。

**语法** `ipv6 prefix-list prefix-list-name permit {A::B/x [ge | le] prefix-len}`

- 参数**
- `prefix-list-name` — 输入 IPv6 前缀列表名称。
  - `A::B/x` — 输入要允许的 IPv6 地址。
  - `ge` — 输入以指示大于或等于指定范围的网络地址。
  - `le` — 输入以指示小于或等于指定范围的网络地址。
  - `prefix-len` — 输入前缀长度。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本将移除指定的前缀-列表。

**示例**

```
OS10(config)# ipv6 prefix-list TEST permit AB20::1/128 ge 10 le 30
```

**支持的版本** 10.3.0E or later

## ipv6 prefix-list seq deny

配置筛选器以拒绝从指定前缀列表进行路由筛选。

**语法** `ipv6 prefix-list [name] seq num deny {A::B/x [ge | le] prefix-len}`

- 参数**
- `name` — (可选) 输入 IPv6 前缀列表的名称。
  - `num` — 输入指定 IPv6 前缀列表的序号。
  - `A::B/x` — 以 /前缀格式 (/x) 输入 IPv6 地址和掩码。
  - `ge` — 输入以指示大于或等于指定范围的网络地址。
  - `le` — 输入以指示小于或等于指定范围的网络地址。
  - `prefix-len` — 输入前缀长度。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本将移除指定的前缀-列表。

**示例**

```
OS10(config)# ipv6 prefix-list TEST seq 65535 deny AB20::1/128 ge 10
```

**支持的版本** 10.3.0E or later

## ipv6 prefix-list seq permit

配置筛选器以允许从指定前缀列表进行路由筛选。

**语法** `ipv6 prefix-list [name] seq num permit A::B/x [ge | le] prefix-len`

- 参数**
- `name` — (可选) 输入 IPv6 前缀列表的名称。
  - `num` — 输入指定 IPv6 前缀列表的序号。
  - `A::B/x` — 以 /前缀格式 (/x) 输入 IPv6 地址和掩码。
  - `ge` — 输入以指示大于或等于指定范围的网络地址。
  - `le` — 输入以指示小于或等于指定范围的网络地址。
  - `prefix-len` — 输入前缀长度。

**默认** 未配置

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本将移除指定的前缀-列表。

|       |                                                                        |
|-------|------------------------------------------------------------------------|
| 示例    | OS10(config)# ipv6 prefix-list TEST seq 65535 permit AB10::1/128 ge 30 |
| 支持的版本 | 10.3.0E or later                                                       |

## mac access-group

配置 MAC 访问组。

|              |                                                                                                                                                                   |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法           | mac access-group <i>access-list-name</i> {in   out}                                                                                                               |
| 参数           | <ul style="list-style-type: none"> <li><i>access-list-name</i> — 输入 MAC 访问列表的名称。最多 140 个字符。</li> <li>in — 将 ACL 应用于传入流量。</li> <li>out — 将 ACL 应用于传出流量。</li> </ul> |
| 默认           | 未配置                                                                                                                                                               |
| 命令模式         | CONFIGURATION<br>CONTROL-PLANE                                                                                                                                    |
| 使用情况信息       | 在 CONTROL-PLANE 模式下使用此命令可应用控制平面 ACL。控制平面 ACL 仅应用于入口流量。默认情况下，控制平面 ACL 应用于前面板端口。此命令的 no 版本会将该值重置为默认值。                                                               |
| 示例           | <pre>OS10(config)# mac access-group maclist in OS10(conf-mac-acl)#</pre>                                                                                          |
| 示例（控制平面 ACL） | <pre>OS10# configure terminal OS10(config)# control-plane OS10(config-control-plane)# mac access-group maclist in</pre>                                           |
| 支持的版本        | 10.2.0E or later; 10.4.1 或更高版本（控制平面 ACL）                                                                                                                          |

## mac access-list

根据 MAC 地址创建要筛选的 MAC 访问列表。

|        |                                                      |
|--------|------------------------------------------------------|
| 语法     | mac access-list <i>access-list-name</i>              |
| 参数     | <i>access-list-name</i> — 输入 MAC 访问列表的名称。最多 140 个字符。 |
| 默认     | 未配置                                                  |
| 命令模式   | CONFIGURATION                                        |
| 使用情况信息 | 无                                                    |
| 示例     | <pre>OS10(config)# mac access-list maclist</pre>     |
| 支持的版本  | 10.2.0E or later                                     |

## permit

配置筛选器以允许具有特定 IPv4 地址的数据包。

|    |                                                                                                                                                                                                                             |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | permit [ <i>protocol-number</i>   icmp   ip   tcp   udp] [A.B.C.D   A.B.C.D/x   any   host <i>ip-address</i> ] [A.B.C.D   A.B.C.D/x   any   host <i>ip-address</i> ] [capture   count   dscp <i>value</i>   fragment   log] |
| 参数 | <ul style="list-style-type: none"> <li><i>protocol-number</i> — （可选）输入 IP 标头中标识的协议号，从 0 到 255。</li> <li>icmp — （可选）输入允许的 ICMP 地址。</li> </ul>                                                                                |

- `ip` — (可选) 输入允许的 IPv4 地址。
- `tcp` — (可选) 输入允许的 TCP 地址。
- `udp` — (可选) 输入允许的 UDP 地址。
- `A.B.C.D` — 以点分隔的十进制格式输入 IPv4 地址。
- `A.B.C.D/x` — 输入必须与点分十进制地址匹配的位数。
- `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
- `host ip-address` — (可选) 输入 IPv4 地址，以仅使用主机地址。
- `capture` — (可选) 捕获筛选器处理的数据包。
- `count` — (可选) 计算筛选器处理的数据包数。
- `byte` — (可选) 计算筛选器处理的字节数。
- `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。
- `fragment` — (可选) 使用 ACL 控制数据包片段。
- `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

**默认** 未配置

**命令模式** IPV4-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数；当您输入 `count byte` 选项时，仅增加字节数。此命令的 `no` 版本将移除筛选器。

**示例**

```
OS10(config)# ip access-list testflow
OS10(conf-ipv4-acl)# permit udp any any capture session 1
```

**支持的版本** 10.2.0E or later

## permit (IPv6)

配置筛选器以允许具有特定 IPv6 地址的数据包。

**语法** `permit [protocol-number | icmp | ipv6 | tcp | udp] [A::B | A::B/x | any | host ipv6-address] [A::B | A::B/x | any | host ipv6-address] [capture | count | dscp value | fragment | log]`

- 参数**
- `protocol-number` — (可选) 输入 IPv6 标头中标识的协议号，从 0 到 255。
  - `icmp` — (可选) 输入允许的 ICMP 地址。
  - `ipv6` — (可选) 输入允许的 IPv6 地址。
  - `tcp` — (可选) 输入允许的 TCP 地址。
  - `udp` — (可选) 输入允许的 UDP 地址。
  - `A::B` — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
  - `A::B/x` — 输入必须与 IPv6 地址匹配的位数。
  - `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
  - `host ip-address` — (可选) 输入 IPv6 地址，以仅使用主机地址。
  - `capture` — (可选) 捕获筛选器处理的数据包。
  - `count` — (可选) 计算筛选器处理的数据包数。
  - `byte` — (可选) 计算筛选器处理的字节数。
  - `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。
  - `fragment` — (可选) 使用 ACL 控制数据包片段。
  - `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

**默认** 未配置

**命令模式** IPV6-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数；当您输入 `count byte` 选项时，仅增加字节数。此命令的 `no` 版本将移除筛选器。

**示例**

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# permit udp any any capture session 1
```

**支持的版本** 10.2.0E or later

# permit (MAC)

配置筛选器以允许具有特定 MAC 地址的数据包。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>permit {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00]   any} {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00]   any} [protocol-number   capture   count [byte]   cos   vlan]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 参数     | <ul style="list-style-type: none"><li>• <code>nn:nn:nn:nn:nn:nn</code> — 输入 MAC 地址。</li><li>• <code>00:00:00:00:00:00</code> — (可选) 输入 MAC 地址中的哪些位必须匹配。如果不输入掩码, 则将应用 <code>00:00:00:00:00:00</code> 掩码。</li><li>• <code>any</code> — (可选) 设置哪些路由受筛选器约束:<ul style="list-style-type: none"><li>◦ <code>protocol-number</code> — 输入 MAC 标头中标识的 MAC 协议编号, 从 600 到 ffff。</li><li>◦ <code>capture</code> — (可选) 输入筛选器处理的捕获数据包。</li><li>◦ <code>count</code> — (可选) 输入筛选器处理的数据包计数。</li><li>◦ <code>byte</code> — (可选) 输入筛选器处理的字节计数。</li><li>◦ <code>cos</code> — (可选) 输入 CoS 值, 从 0 到 7。</li><li>◦ <code>vlan</code> — (可选) 输入 VLAN 编号, 从 1 到 4093。</li></ul></li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 命令模式   | MAC-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | OS10 不能同时计算数据包和字节数; 当您输入 <code>count byte</code> 选项时, 仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 示例     | <pre>OS10(config)# mac access-list macacl OS10(conf-mac-acl)# permit 00:00:00:00:11:11 00:00:11:11:11:11 any cos 7 OS10(conf-mac-acl)# permit 00:00:00:00:11:11 00:00:11:11:11:11 any vlan 2</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

# permit icmp

配置筛选器以允许所有或特定 ICMP 消息。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>permit icmp [A.B.C.D   A.B.C.D/x   any   host ip-address] [[A.B.C.D   A.B.C.D/x   any   host ip-address] [capture   count   dscp value   fragment   log]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 参数     | <ul style="list-style-type: none"><li>• <code>A.B.C.D</code> — 以点分隔的十进制格式输入 IPv4 地址。</li><li>• <code>A.B.C.D/x</code> — 输入必须与点分十进制地址匹配的位数。</li><li>• <code>any</code> — (可选) 输入关键字 <code>any</code> 以指定任何源或目标 IP 地址。</li><li>• <code>host ip-address</code> — (可选) 输入 IPv4 地址, 以仅使用主机地址。</li><li>• <code>capture</code> — (可选) 捕获筛选器处理的数据包。</li><li>• <code>count</code> — (可选) 计算筛选器处理的数据包数。</li><li>• <code>byte</code> — (可选) 计算筛选器处理的字节数。</li><li>• <code>dscp value</code> — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。</li><li>• <code>fragment</code> — (可选) 使用 ACL 控制数据包片段。</li><li>• <code>log</code> — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 命令模式   | IPV4-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 使用情况信息 | OS10 不能同时计算数据包和字节数; 当您输入 <code>count byte</code> 选项时, 仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 示例     | <pre>OS10(config)# ip access-list testflow OS10(conf-ipv4-acl)# permit icmp any any capture session 1</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## permit icmp (IPv6)

配置筛选器以允许所有或特定 ICMP 消息。

**语法** `permit icmp [A::B | A::B/x | any | host ipv6-address] [A::B | A:B/x | any | host ipv6-address] [capture | count | dscp value | fragment | log]`

- 参数**
- A::B — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
  - A::B/x — 输入必须与 IPv6 地址匹配的位数。
  - any — (可选) 输入关键字 any 以指定任何源或目标 IP 地址。
  - host ipv6-address — (可选) 输入 IPv6 地址，以仅使用主机地址。
  - capture — (可选) 捕获筛选器处理的数据包。
  - count — (可选) 计算筛选器处理的数据包数。
  - byte — (可选) 计算筛选器处理的字节数。
  - dscp value — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。
  - fragment — (可选) 使用 ACL 控制数据包片段。
  - log — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

**默认** 未配置

**命令模式** IPV6-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数；当您输入 count byte 选项时，仅增加字节数。此命令的 no 版本将移除筛选器。

**示例**

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# permit icmp any any capture session 1
```

**支持的版本** 10.2.0E or later

## permit ip

配置筛选器以允许来自 IPv4 地址的所有或特定数据包。

**语法** `permit ip [A.B.C.D | A.B.C.D/x | any | host ip-address] [[A.B.C.D | A.B.C.D/x | any | host ip-address] [capture | count | dscp value | fragment | log]`

- 参数**
- A.B.C.D — 以点分隔的十进制格式输入 IPv4 地址。
  - A.B.C.D/x — 输入与点分十进制地址匹配的位数。
  - any — (可选) 输入关键字 any 以指定任何源或目标 IP 地址。
  - host ip-address — (可选) 输入 IPv4 地址，以仅使用主机地址。
  - capture — (可选) 捕获筛选器处理的数据包。
  - count — (可选) 计算筛选器处理的数据包数。
  - byte — (可选) 计算筛选器处理的字节数。
  - dscp value — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。
  - fragments — (可选) 使用 ACL 控制数据包片段。
  - log — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

**默认** 未配置

**命令模式** IPV4-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数；当您输入 count byte 选项时，仅增加字节数。此命令的 no 版本将移除筛选器。

**示例**

```
OS10(conf-ipv4-acl)# permit ip any any capture session 1
```

**支持的版本** 10.2.0E or later

# permit ipv6

配置筛选器以允许来自 IPv6 地址的所有或特定数据包。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>permit ipv6 [A::B   A::B/x   any   host ipv6-address] [A::B   A:B/x   any   host ipv6-address] [capture   count   dscp value   fragment   log]</code>                                                                                                                                                                                                                                                                                                                                                                          |
| 参数     | <ul style="list-style-type: none"><li>• A::B — (可选) 输入从中发送数据包的源 IPv6 地址和目标地址。</li><li>• A::B/x — (可选) 以 /前缀格式 (/x) 和目标掩码输入源网络掩码。</li><li>• any — (可选) 输入关键字 any 以指定任何源或目标 IP 地址。</li><li>• host ipv6-address — 输入 IPv6 地址, 以仅使用主机地址。</li><li>• capture — (可选) 输入以捕获筛选器处理的数据包。</li><li>• count — (可选) 输入以计算筛选器处理的数据包数。</li><li>• byte — (可选) 输入以计算筛选器处理的字节数。</li><li>• dscp value — (可选) 输入以根据 DSCP 值 (从 0 到 63) 拒绝数据包。</li><li>• fragment — (可选) 输入以使用 ACL 来控制数据包片段。</li><li>• log — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 命令模式   | IPv6-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 使用情况信息 | OS10 不能同时计算数据包和字节数; 当您输入 count byte 选项时, 仅增加字节数。此命令的 no 版本将移除筛选器。                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 示例     | <pre>OS10(conf-ipv6-acl)# permit ipv6 any any count capture session 1</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

# permit tcp

配置筛选器以允许符合筛选条件的 TCP 数据包。

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>permit tcp [A.B.C.D   A.B.C.D/x   any   host ip-address [operator]] [[A.B.C.D   A.B.C.D/x   any   host ip-address [operator] ] [ack   fin   psh   rst   syn   urg] [capture   count   dscp value   fragment   log]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 参数 | <ul style="list-style-type: none"><li>• A.B.C.D — 以点分隔的十进制格式输入 IPv4 地址。</li><li>• A.B.C.D/x — 输入必须与点分十进制地址匹配的位数。</li><li>• any — (可选) 输入关键字 any 以指定任何源或目标 IP 地址。<br/> 注: 控制平面 ACL 不支持 any 参数。</li><li>• host ip-address — (可选) 输入 IPv4 地址, 以仅使用主机地址。</li><li>• ack — (可选) 将“位”设置为“确认”。</li><li>• fin — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。</li><li>• psh — (可选) 将“位”设置为“推送”。</li><li>• rst — (可选) 将“位”设置为“重置”。</li><li>• syn — (可选) 将“位”设置为“同步”。</li><li>• urg — (可选) 将“位”设置为“紧急”。</li><li>• capture — (可选) 捕获筛选器处理的数据包。</li><li>• count — (可选) 计算筛选器处理的数据包数。</li><li>• byte — (可选) 计算筛选器处理的字节数。</li><li>• dscp value — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。</li><li>• fragment — (可选) 使用 ACL 控制数据包片段。</li><li>• log — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li><li>• operator — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用:<ul style="list-style-type: none"><li>◦ eq — 等于</li><li>◦ gt — 大于</li><li>◦ lt — 小于</li></ul></li></ul> |

- neq — 不等于
- range — 端口范围，包括指定的端口号。

 **注：**控制平面 ACL 仅支持 eq 运算符。

|        |                                                                      |
|--------|----------------------------------------------------------------------|
| 默认     | 未配置                                                                  |
| 命令模式   | IPV4-ACL                                                             |
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 count byte 选项时，仅增加字节数。此命令的 no 版本将移除筛选器。      |
| 示例     | <pre>OS10(conf-ipv4-acl)# permit tcp any any capture session 1</pre> |
| 支持的版本  | 10.2.0E or later                                                     |

## permit tcp (IPv6)

配置筛选器以允许符合筛选条件的 TCP 数据包。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <pre>permit tcp [A::B   A::B/x   any   host ipv6-address [eq   lt   gt   neq   range]] [A::B   A:B/x   any   host ipv6-address [eq   lt   gt   neq   range]] [ack   fin   psh   rst   syn   urg] [capture   count   dscp value   fragment   log]</pre>                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 参数     | <ul style="list-style-type: none"> <li>• A::B — 以十六进制格式输入采用冒号分隔的 IPv6 地址。</li> <li>• A::B/x — 输入必须与 IPv6 地址匹配的位数。</li> <li>• any — (可选) 输入关键字 any 以指定任何源或目标 IP 地址。</li> </ul> <p> <b>注：</b>控制平面 ACL 不支持 any 参数。</p> <ul style="list-style-type: none"> <li>• host ipv6-address — (可选) 输入 IPv6 地址，以仅使用主机地址。</li> <li>• capture — (可选) 捕获筛选器处理的数据包。</li> <li>• count — (可选) 计算筛选器处理的数据包数。</li> <li>• byte — (可选) 计算筛选器处理的字节数。</li> <li>• dscp value — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。</li> <li>• fragment — (可选) 使用 ACL 控制数据包片段。</li> <li>• log — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 命令模式   | IPV6-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 count byte 选项时，仅增加字节数。此命令的 no 版本将移除筛选器。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 示例     | <pre>OS10(config)# ipv6 access-list ipv6test OS10(conf-ipv6-acl)# permit tcp any any capture session 1</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## permit udp

配置筛选器，以允许符合筛选条件的 UDP 数据包。

|    |                                                                                                                                                                                                                                                                  |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <pre>permit udp [A.B.C.D   A.B.C.D/x   any   host ip-address [eq   lt   gt   neq   range]] [[A.B.C.D   A.B.C.D/x   any   host ip-address [eq   lt   gt   neq   range]] [ack   fin   psh   rst   syn   urg] [capture   count   dscp value   fragment   log]</pre> |
| 参数 | <ul style="list-style-type: none"> <li>• A.B.C.D — 以点分隔的十进制格式输入 IPv4 地址。</li> <li>• A.B.C.D/x — 输入必须与点分十进制地址匹配的位数。</li> <li>• any — (可选) 输入关键字 any 以指定任何源或目标 IP 地址。</li> </ul>                                                                                   |



- `host ip-address` — (可选) 输入 IPv4 地址, 以仅使用主机地址。
- `ack` — (可选) 将“位”设置为“确认”。
- `fin` — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。
- `psh` — (可选) 将“位”设置为“推送”。
- `rst` — (可选) 将“位”设置为“重置”。
- `syn` — (可选) 将“位”设置为“同步”。
- `urg` — (可选) 将“位”设置为“紧急”。
- `capture` — (可选) 捕获筛选器处理的数据包。
- `count` — (可选) 计算筛选器处理的数据包数。
- `byte` — (可选) 计算筛选器处理的字节数。
- `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。
- `fragment` — (可选) 使用 ACL 控制数据包片段。
- `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。
- `operator` — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用:
  - `eq` — (可选) 允许相同的数据包。
  - `lt` — (可选) 允许少于的数据包。
  - `gt` — (可选) 允许大于的数据包。
  - `neq` — (可选) 允许不等于的数据包。
  - `range` — (可选) 允许具有特定源和目标地址的数据包。

 **注:** 控制平面 ACL 仅支持 `eq` 运算符。

#### 默认

未配置

#### 命令模式

IPV4-ACL

#### 使用情况信息

OS10 不能同时计算数据包和字节数; 当您输入 `count byte` 选项时, 仅增加字节数。此命令的 `no` 版本将移除筛选器。

#### 示例

```
OS10(config)# ip access-list testflow
OS10(conf-ipv4-acl)# permit udp any any capture session 1
```

#### 支持的版本

10.2.0E or later

## permit udp (IPv6)

配置筛选器以允许符合筛选条件的 UDP 数据包。

#### 语法

```
permit udp [A::B | A::B/x | any | host ipv6-address [operator]] [A::B |
A::B/x | any | host ipv6-address [operator]] [ack | fin | psh | rst | syn |
urg] [capture | count | dscp value | fragment | log]
```

#### 参数

- `A::B` — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
- `A::B/x` — 输入必须与 IPv6 地址匹配的位数。
- `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
-  **注:** 控制平面 ACL 仅支持 `eq` 运算符。
- `host ipv6-address` — (可选) 输入关键字和 IPv6 地址, 以仅使用主机地址。
- `ack` — (可选) 将“位”设置为“确认”。
- `fin` — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。
- `psh` — (可选) 将“位”设置为“推送”。
- `rst` — (可选) 将“位”设置为“重置”。
- `syn` — (可选) 将“位”设置为“同步”。
- `urg` — (可选) 将“位”设置为“紧急”。
- `capture` — (可选) 捕获筛选器处理的数据包。
- `count` — (可选) 计算筛选器处理的数据包数。
- `byte` — (可选) 计算筛选器处理的字节数。
- `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。
- `fragment` — (可选) 使用 ACL 控制数据包片段。



- `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。
- `operator` — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用：
  - `eq` — 等于
  - `gt` — 大于
  - `lt` — 小于
  - `neq` — 不等于
  - `range` — 端口范围，包括指定的端口号。

|        |                                                                                           |
|--------|-------------------------------------------------------------------------------------------|
| 默认     | 未配置                                                                                       |
| 命令模式   | IPV6-ACL                                                                                  |
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 <code>count byte</code> 选项时，仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器。 |
| 示例     | <pre>OS10(conf-ipv6-acl)# permit udp any any capture session 1 count</pre>                |
| 支持的版本  | 10.2.0E or later                                                                          |

## remark

指定 ACL 条目说明。

|        |                                                                            |
|--------|----------------------------------------------------------------------------|
| 语法     | <code>remark description</code>                                            |
| 参数     | <code>description</code> — 输入说明。最多 80 个字符。                                 |
| 默认     | 未配置                                                                        |
| 命令模式   | IPV4-ACL                                                                   |
| 使用情况信息 | 为给定的 IPv4、IPv6 或 MAC 配置最多 16777214 条注释。命令的 <code>no</code> 版本将移除 ACL 条目说明。 |
| 支持的版本  | 10.2.0E or later                                                           |

## seq deny

在创建筛选器时分配一个序列号以拒绝 IPv4 地址。

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>seq sequence-number deny [protocol-number   icmp   ip   tcp   udp] [A.B.C.D   A.B.C.D/x   any   host ip-address] [A.B.C.D   A.B.C.D/x   any   host ip-address] [capture   count   dscp value   fragment   log]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 参数 | <ul style="list-style-type: none"> <li>• <code>sequence-number</code> — 输入序列号，以标识用于编辑和排序编号的 ACL，从 1 到 16777214。</li> <li>• <code>protocol-number</code> — (可选) 输入协议号，从 0 到 255。</li> <li>• <code>icmp</code> — (可选) 输入要拒绝的 ICMP 地址。</li> <li>• <code>ip</code> — (可选) 输入要拒绝的 IPv4 地址。</li> <li>• <code>tcp</code> — (可选) 输入要拒绝的 TCP 地址。</li> <li>• <code>udp</code> — (可选) 输入要拒绝的 UDP 地址。</li> <li>• <code>A.B.C.D</code> — (可选) 以点分十进制格式输入 IPv4 地址。</li> <li>• <code>A.B.C.D/x</code> — (可选) 输入必须与点分十进制地址匹配的位数。</li> <li>• <code>any</code> — (可选) 输入关键字 <code>any</code> 以指定任何源或目标 IP 地址。</li> <li>• <code>host ip-address</code> — (可选) 输入 IPv4 地址，以仅使用主机地址。</li> <li>• <code>capture</code> — (可选) 捕获筛选器处理的数据包。</li> <li>• <code>count</code> — (可选) 计算筛选器处理的数据包数。</li> <li>• <code>byte</code> — (可选) 计算筛选器处理的字节数。</li> <li>• <code>dscp value</code> — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。</li> <li>• <code>fragment</code> — (可选) 使用 ACL 控制数据包片段。</li> <li>• <code>log</code> — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li> </ul> |
| 默认 | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|        |                                                                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 命令模式   | IPv4-ACL                                                                                                                                             |
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 <code>count byte</code> 选项时，仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 <code>no seq sequence-number</code> 命令。 |
| 示例     | <pre>OS10(config)# ip access-list testflow OS10(conf-ipv4-acl)# seq 10 deny tcp any any capture session 1 log</pre>                                  |
| 支持的版本  | 10.2.0E or later                                                                                                                                     |

## seq deny (IPv6)

在创建筛选器时分配一个序列号以拒绝 IPv6 地址。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>seq sequence-number deny [protocol-number icmp   ip   tcp   udp] [A::B   A::B/x   any   host ipv6-address] [A::B   A::B/x   any   host ipv6-address] [capture   count   dscp value   fragment   log]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 参数     | <ul style="list-style-type: none"> <li><code>sequence-number</code> — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。</li> <li><code>protocol-number</code> — (可选) 输入协议号，从 0 到 255。</li> <li><code>icmp</code> — (可选) 输入要拒绝的 ICMP 地址。</li> <li><code>ip</code> — (可选) 输入要拒绝的 IPv6 地址。</li> <li><code>tcp</code> — (可选) 输入要拒绝的 TCP 地址。</li> <li><code>udp</code> — (可选) 输入要拒绝的 UDP 地址。</li> <li><code>A::B</code> — 以十六进制格式输入采用冒号分隔的 IPv6 地址。</li> <li><code>A::B/x</code> — 输入必须与 IPv6 地址匹配的位数。</li> <li><code>any</code> — (可选) 输入关键字 <code>any</code> 以指定任何源或目标 IP 地址。</li> <li><code>host ipv6-address</code> — (可选) 输入以仅使用 IPv6 主机地址。</li> <li><code>capture</code> — (可选) 输入以捕获筛选器处理的数据包。</li> <li><code>count</code> — (可选) 输入以计算筛选器处理的数据包数。</li> <li><code>byte</code> — (可选) 输入以计算筛选器处理的字节数。</li> <li><code>dscp value</code> — (可选) 输入以根据 DSCP 值 (从 0 到 63) 拒绝数据包。</li> <li><code>fragment</code> — (可选) 输入以使用 ACL 来控制数据包片段。</li> <li><code>log</code> — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 命令模式   | IPv6-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 <code>count byte</code> 选项时，仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 <code>no seq sequence-number</code> 命令。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 示例     | <pre>OS10(config)# ipv6 access-list ipv6test OS10(conf-ipv6-acl)# seq 5 deny ipv6 any any capture session 1 count log</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## seq deny (MAC)

在创建筛选器时，将序列号分配给 MAC 访问列表中的拒绝筛选器。

|    |                                                                                                                                                                                                                                                                                                  |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>seq sequence-number deny {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00]   any} {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00]   any} [protocol-number   capture   cos   count [byte]   vlan]</code>                                                                                                        |
| 参数 | <ul style="list-style-type: none"> <li><code>sequence-number</code> — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。</li> <li><code>nn:nn:nn:nn:nn:nn</code> — 输入源 MAC 地址。</li> <li><code>00:00:00:00:00:00</code> — (可选) 输入 MAC 地址中的哪些位必须匹配。如果不输入掩码，则将应用 <code>00:00:00:00:00:00</code> 掩码。</li> </ul> |

- any — (可选) 设置受筛选器约束的所有路由：
  - *protocol-number* — 在 MAC 标头中标识的协议编号，从 600 到 ffff。
  - *capture* — (可选) 捕获筛选器处理的数据包。
  - *cos* — (可选) CoS 值，从 0 到 7。
  - *count* — (可选) 计算筛选器处理的数据包数。
  - *byte* — (可选) 计算筛选器处理的字节数。
  - *vlan* — (可选) VLAN ID 号，从 1 到 4093。

|        |                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | 未配置                                                                                                                                                                                                          |
| 命令模式   | CONFIG-MAC-ACL                                                                                                                                                                                               |
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 <i>count byte</i> 选项时，仅增加字节数。此命令的 <i>no</i> 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 <i>no seq sequence-number</i> 命令。                                                                           |
| 示例     | <pre>OS10(config)# mac access-list macacl OS10(conf-mac-acl)# seq 10 deny 00:00:00:00:11:11 00:00:11:11:11:11 any cos 7 OS10(conf-mac-acl)# seq 20 deny 00:00:00:00:11:11 00:00:11:11:11:11 any vlan 2</pre> |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                             |

## seq deny icmp

指定筛选器，以便在创建筛选器时拒绝 ICMP 消息。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <i>seq sequence-number deny icmp</i> [ <i>A.B.C.D</i>   <i>A.B.C.D/x</i>   <i>any</i>   <i>host ip-address</i> ] [ <i>A.B.C.D</i>   <i>A.B.C.D/x</i>   <i>any</i>   <i>host ip-address</i> ] [ <i>capture</i>   <i>count</i>   <i>dscp value</i>   <i>fragment</i>   <i>log</i> ]                                                                                                                                                                                                                                                                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"> <li>• <i>sequence-number</i> — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。</li> <li>• <i>A.B.C.D</i> — 以点分隔的十进制格式输入 IPv4 地址。</li> <li>• <i>A.B.C.D/x</i> — 输入必须与点分十进制地址匹配的位数。</li> <li>• <i>any</i> — (可选) 输入关键字 <i>any</i> 以指定任何源或目标 IP 地址。</li> <li>• <i>host ip-address</i> — (可选) 输入 IPv4 地址，以仅使用主机 IP 地址。</li> <li>• <i>capture</i> — (可选) 捕获筛选器处理的数据包。</li> <li>• <i>count</i> — (可选) 计算筛选器处理的数据包数。</li> <li>• <i>byte</i> — (可选) 计算筛选器处理的字节数。</li> <li>• <i>dscp value</i> — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。</li> <li>• <i>fragment</i> — (可选) 使用 ACL 控制数据包片段。</li> <li>• <i>log</i> — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 命令模式   | IPV4-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 <i>count byte</i> 选项时，仅增加字节数。此命令的 <i>no</i> 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 <i>no seq sequence-number</i> 命令。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 示例     | <pre>OS10(config)# ip access-list egress OS10(conf-ipv4-acl)# seq 5 deny icmp any any capture session 1 log</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## seq deny icmp (IPv6)

指定在创建筛选器时拒绝 ICMP 消息的序列号。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>seq sequence-number deny icmp [A::B   A::B/x   any   host ipv6-address] [A::B   A::B/x   any   host ipv6-address] [capture   count   dscp value   fragment   log]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 参数     | <ul style="list-style-type: none"><li><code>sequence-number</code> — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。</li><li><code>A::B</code> — 以十六进制格式输入采用冒号分隔的 IPv6 地址。</li><li><code>A::B/x</code> — 输入必须与 IPv6 地址匹配的位数。</li><li><code>any</code> — (可选) 输入关键字 <code>any</code> 以指定任何源或目标 IP 地址。</li><li><code>host ipv6-address</code> — (可选) 输入 IPv6 地址，以仅使用主机地址。</li><li><code>capture</code> — (可选) 捕获筛选器处理的数据包。</li><li><code>count</code> — (可选) 计算筛选器处理的数据包数。</li><li><code>byte</code> — (可选) 计算筛选器处理的字节数。</li><li><code>dscp value</code> — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。</li><li><code>fragment</code> — (可选) 使用 ACL 控制数据包片段。</li><li><code>log</code> — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 命令模式   | IPv6-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 <code>count byte</code> 选项时，仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 <code>no seq sequence-number</code> 命令。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 示例     | <pre>OS10(config)# ipv6 access-list ipv6test OS10(conf-ipv6-acl)# seq 10 deny icmp any any capture session 1 log</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## seq deny ip

在创建筛选器时分配一个序列号以拒绝 IPv4 地址。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>seq sequence-number deny ip [A.B.C.D   A.B.C.D/x   any   host ip-address] [A.B.C.D   A.B.C.D/x   any   host ip-address] [capture   count   dscp value   fragment   log]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 参数     | <ul style="list-style-type: none"><li><code>sequence-number</code> — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。</li><li><code>A.B.C.D</code> — 以点分隔的十进制格式输入 IPv4 地址。</li><li><code>A.B.C.D/x</code> — 输入必须与点分十进制地址匹配的位数。</li><li><code>any</code> — (可选) 输入关键字 <code>any</code> 以指定任何源或目标 IP 地址。</li><li><code>host ip-address</code> — (可选) 输入 IPv4 地址，以仅使用主机地址。</li><li><code>capture</code> — (可选) 捕获筛选器处理的数据包。</li><li><code>count</code> — (可选) 计算筛选器处理的数据包数。</li><li><code>byte</code> — (可选) 计算筛选器处理的字节数。</li><li><code>dscp value</code> — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。</li><li><code>fragment</code> — (可选) 使用 ACL 控制数据包片段。</li><li><code>log</code> — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 命令模式   | IPv4-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 <code>count byte</code> 选项时，仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 <code>no seq sequence-number</code> 命令。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## 示例

```
OS10(config)# ip access-list egress
OS10(config-ipv4-acl)# seq 10 deny ip any any capture session 1 log
```

支持的版本 10.2.0E or later

## seq deny ipv6

在创建筛选器时分配筛选器以拒绝 IPv6 地址。

**语法** `seq sequence-number deny ip [A::B | A::B/x | any | host ipv6-address] [A::B | A:B/x | any | host ipv6-address] [capture | count | dscp value | fragment | log]`

- 参数**
- *sequence-number* — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。
  - *A::B* — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
  - *A::B/x* — 输入必须与 IPv6 地址匹配的位数。
  - *any* — (可选) 输入关键字 *any* 以指定任何源或目标地址。
  - *host ip-address* — (可选) 输入 IPv6 地址，以仅使用主机地址。
  - *capture* — (可选) 捕获筛选器处理的数据包。
  - *count* — (可选) 计算筛选器处理的数据包数。
  - *byte* — (可选) 计算筛选器处理的字节数。
  - *dscp value* — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
  - *fragment* — (可选) 使用 ACL 控制数据包片段。
  - *log* — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

**默认** 未配置

**命令模式** IPV6-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数；当您输入 *count byte* 选项时，仅增加字节数。此命令的 *no* 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 *no seq sequence-number* 命令。

## 示例

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# seq 10 deny ipv6 any any capture session 1 log
```

支持的版本 10.2.0E or later

## seq deny tcp

在创建筛选器时分配筛选器以拒绝 TCP 数据包。

**语法** `seq sequence-number deny tcp [A.B.C.D | A.B.C.D/x | any | host ip-address [operator]] [[A.B.C.D | A.B.C.D/x | any | host ip-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | count | dscp value | fragment | log]`

- 参数**
- *sequence-number* — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。
  - *A.B.C.D* — 以点分隔的十进制格式输入 IPv4 地址。
  - *A.B.C.D/x* — 输入必须与点分十进制地址匹配的位数。
  - *any* — (可选) 输入关键字 *any* 以指定任何源或目标 IP 地址。
  - *host ip-address* — (可选) 输入 IPv4 地址，以仅使用主机地址。
  - *ack* — (可选) 将“位”设置为“确认”。
  - *fin* — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。
  - *psh* — (可选) 将“位”设置为“推送”。
  - *rst* — (可选) 将“位”设置为“重置”。
  - *syn* — (可选) 将“位”设置为“同步”。
  - *urg* — (可选) 将“位”设置为“紧急”。
  - *capture* — (可选) 捕获筛选器处理的数据包。

- `count` — (可选) 计算筛选器处理的数据包数。
- `byte` — (可选) 计算筛选器处理的字节数。
- `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
- `fragment` — (可选) 使用 ACL 控制数据包片段。
- `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。
- `operator` — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用：
  - `eq` — 等于
  - `gt` — 大于
  - `lt` — 小于
  - `neq` — 不等于
  - `range` — 端口范围, 包括指定的端口号。

**默认** 未配置

**命令模式** IPV4-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数; 当您输入 `count byte` 选项时, 仅增加字节数。此命令的 `no` 版本将移除筛选器, 或者如果您知道筛选器的顺序编号, 则使用 `no seq sequence-number` 命令。

**示例**

```
OS10(config)# ip access-list egress
OS10(conf-ip4-acl)# seq 10 deny tcp any any capture session 1 log
```

**支持的版本** 10.2.0E or later

## seq deny tcp (IPv6)

在创建筛选器时分配筛选器以拒绝 TCP 数据包。

**语法** `seq sequence-number deny tcp [A::B | A::B/x | any | host ipv6-address [operator]] [A::B | A::B/x | any | host ipv6-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | count | dscp value | fragment | log]`

- 参数**
- `sequence-number` — 输入序列号, 以标识用于编辑的路由映射和顺序编号, 从 1 到 16777214。
  - `A::B` — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
  - `A::B/x` — 输入必须与 IPv6 地址匹配的位数。
  - `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
  - `host ip-address` — (可选) 输入 IPv6 地址, 以仅使用主机地址。
  - `ack` — (可选) 将“位”设置为“确认”。
  - `fin` — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。
  - `psh` — (可选) 将“位”设置为“推送”。
  - `rst` — (可选) 将“位”设置为“重置”。
  - `syn` — (可选) 将“位”设置为“同步”。
  - `urg` — (可选) 将“位”设置为“紧急”。
  - `capture` — (可选) 捕获筛选器处理的数据包。
  - `count` — (可选) 计算筛选器处理的数据包数。
  - `byte` — (可选) 计算筛选器处理的字节数。
  - `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
  - `fragment` — (可选) 使用 ACL 控制数据包片段。
  - `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。
  - `operator` — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用：
    - `eq` — 等于
    - `gt` — 大于
    - `lt` — 小于
    - `neq` — 不等于
    - `range` — 端口范围, 包括指定的端口号。

**默认** 未配置

**命令模式** IPV6-ACL

## 使用情况信息

OS10 不能同时计算数据包和字节数；当您输入 `count byte` 选项时，仅增加字节数。此命令的 `no` 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 `no seq sequence-number` 命令。

## 示例

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# seq 10 deny tcp any any capture session 1 log
```

## 支持的版本

10.2.0E or later

# seq deny udp

在创建筛选器时分配筛选器以拒绝 UDP 数据包。

## 语法

```
seq sequence-number deny udp [A.B.C.D | A.B.C.D/x | any | host ip-address
[operator]] [[A.B.C.D | A.B.C.D/x | any | host ip-address [operator]] [ack
| fin | psh | rst | syn | urg] [capture | count | dscp value | fragment |
log]
```

## 参数

- `sequence-number` — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。
- `A.B.C.D` — 以点分隔的十进制格式输入 IPv4 地址。
- `A.B.C.D/x` — 输入必须与点分十进制地址匹配的位数。
- `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
- `host ip-address` — (可选) 输入 IPv4 地址，以仅使用主机地址。
- `ack` — (可选) 将“位”设置为“确认”。
- `fin` — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。
- `psh` — (可选) 将“位”设置为“推送”。
- `rst` — (可选) 将“位”设置为“重置”。
- `syn` — (可选) 将“位”设置为“同步”。
- `urg` — (可选) 将“位”设置为“紧急”。
- `capture` — (可选) 捕获筛选器处理的数据包。
- `count` — (可选) 计算筛选器处理的数据包数。
- `byte` — (可选) 计算筛选器处理的字节数。
- `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
- `fragment` — (可选) 使用 ACL 控制数据包片段。
- `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。
- `operator` — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用：
  - `eq` — 等于
  - `gt` — 大于
  - `lt` — 小于
  - `neq` — 不等于
  - `range` — 端口范围，包括指定的端口号。

## 默认

未配置

## 命令模式

IPV4-ACL

## 使用情况信息

OS10 不能同时计算数据包和字节数；当您输入 `count byte` 选项时，仅增加字节数。此命令的 `no` 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 `no seq sequence-number` 命令。

## 示例

```
OS10(config)# ip access-list egress
OS10(conf-ipv4-acl)# seq 10 deny udp any any capture session 1 log
```

## 支持的版本

10.2.0E or later



## seq deny udp (IPv6)

在创建筛选器时分配筛选器以拒绝 UDP 数据包。

**语法** `seq sequence-number deny udp [A::B | A::B/x | any | host ipv6-address [operator]] [A::B | A::B/x | any | host ipv6-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | count | dscp value | fragment | log]`

- 参数**
- `sequence-number` — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。
  - `A::B` — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
  - `A::B/x` — 输入必须与 IPv6 地址匹配的位数。
  - `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
  - `host ipv6-address` — (可选) 输入 IPv6 地址，以仅使用主机地址。
  - `ack` — (可选) 将“位”设置为“确认”。
  - `fin` — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。
  - `psh` — (可选) 将“位”设置为“推送”。
  - `rst` — (可选) 将“位”设置为“重置”。
  - `syn` — (可选) 将“位”设置为“同步”。
  - `urg` — (可选) 将“位”设置为“紧急”。
  - `capture` — (可选) 捕获筛选器处理的数据包。
  - `count` — (可选) 计算筛选器处理的数据包数。
  - `byte` — (可选) 计算筛选器处理的字节数。
  - `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 拒绝数据包。
  - `fragment` — (可选) 使用 ACL 控制数据包片段。
  - `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。
  - `operator` — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用：
    - `eq` — 等于
    - `gt` — 大于
    - `lt` — 小于
    - `neq` — 不等于
    - `range` — 端口范围，包括指定的端口号。

**默认** 未配置

**命令模式** IPV6-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数；当您输入 `count byte` 选项时，仅增加字节数。此命令的 `no` 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 `no seq sequence-number` 命令。

**示例**

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# seq 10 deny udp any any capture session 1 log
```

**支持的版本** 10.2.0E or later

## seq permit

在创建筛选器时分配序列号以允许数据包。

**语法** `seq sequence-number permit [protocol-number A.B.C.D | A.B.C.D/x | any | host ip-address] [A.B.C.D | A.B.C.D/x | any | host ip-address] [capture | count | dscp value | fragment | log]`

- 参数**
- `sequence-number` — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。
  - `protocol-number` — (可选) 输入协议号，从 0 到 255。
  - `A.B.C.D` — 以点分隔的十进制格式输入 IPv4 地址。
  - `A.B.C.D/x` — 输入必须与点分十进制地址匹配的位数。
  - `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
  - `host ip-address` — (可选) 输入 IPv4 地址，以仅使用主机地址。
  - `capture` — (可选) 捕获筛选器处理的数据包。



- `count` — (可选) 计算筛选器处理的数据包数。
- `byte` — (可选) 计算筛选器处理的字节数。
- `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。
- `fragment` — (可选) 使用 ACL 控制数据包片段。
- `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

**默认** 未配置

**命令模式** IPV4-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数; 当您输入 `count byte` 选项时, 仅增加字节数。此命令的 `no` 版本将移除筛选器, 或者如果您知道筛选器的顺序编号, 则使用 `no seq sequence-number` 命令。

**示例**

```
OS10(config)# ip access-list testflow
OS10(conf-ipv4-acl)# seq 10 permit ip any any capture session 1 log
```

**支持的版本** 10.2.0E or later

## seq permit (IPv6)

在创建筛选器时分配序列号以允许 IPv6 数据包。

**语法** `seq sequence-number permit protocol-number [A::B | A::B/x | any | host ipv6-address] [A::B | A::B/x | any | host ipv6-address] [capture | count | dscp value | fragment | log]`

- 参数**
- `sequence-number` — 输入序列号, 以标识用于编辑的路由映射和顺序编号, 从 1 到 16777214。
  - `protocol-number` — (可选) 输入协议号, 从 0 到 255。
  - `A::B` — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
  - `A::B/x` — 输入必须与 IPv6 地址匹配的位数。
  - `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
  - `host ipv6-address` — (可选) 输入 IPv6 地址, 以仅用作主机地址。
  - `capture` — (可选) 输入以捕获筛选器处理的数据包。
  - `count` — (可选) 输入以计算筛选器处理的数据包数。
  - `byte` — (可选) 输入以计算筛选器处理的字节数。
  - `dscp value` — (可选) 输入 DSCP 值以允许数据包, 从 0 到 63。
  - `fragment` — (可选) 输入以使用 ACL 来控制数据包片段。
  - `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

**默认** 未配置

**命令模式** IPV6-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数; 当您输入 `count byte` 选项时, 仅增加字节数。此命令的 `no` 版本将移除筛选器, 或者如果您知道筛选器的顺序编号, 则使用 `no seq sequence-number` 命令。

**示例**

```
OS10(config)# ipv6 access-list ipv6test
OS10(conf-ipv6-acl)# seq 10 permit ipv6 any any capture session 1 log
```

**支持的版本** 10.2.0E or later

## seq permit (MAC)

在创建筛选器时分配序列号以允许 MAC 地址。

**语法** `seq sequence-number permit {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00] | any} {nn:nn:nn:nn:nn:nn [00:00:00:00:00:00] | any} [protocol-number | capture | cos | count [byte] | vlan]`

- 参数**
- `sequence-number` — 输入序列号, 以标识用于编辑的路由映射和顺序, 从 1 到 16777214。

- *nn:nn:nn:nn:nn:nn* — 输入要发送或发送到的数据包的网络的 MAC 地址。
- *00:00:00:00:00:00* — (可选) 输入 MAC 地址中的哪些位必须匹配。如果不输入掩码, 则将应用 *00:00:00:00:00:00* 掩码。
- *any* — (可选) 将所有路由设置为符合筛选器的条件:
  - *protocol-number* — (可选) 输入 MAC 标头中标识的协议号, 从 600 到 ffff。
  - *capture* — (可选) 输入筛选器处理的捕获数据包。
  - *cos* — (可选) 输入 CoS 值, 从 0 到 7。
  - *count* — (可选) 输入筛选器处理的数据包计数。
  - *byte* — (可选) 输入筛选器处理的字节计数。
  - *vlan* — (可选) 输入 VLAN 编号, 从 1 到 4093。

**默认** 未配置

**命令模式** MAC-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数; 当您输入 *count byte* 选项时, 仅增加字节数。此命令的 *no* 版本将移除筛选器, 或者如果您知道筛选器的顺序编号, 则使用 *no seq sequence-number* 命令。

**示例**

```
OS10(config)# mac access-list macacl
OS10(conf-mac-acl)# seq 10 permit 00:00:00:00:11:11 00:00:11:11:11:11
any cos 7
OS10(conf-mac-acl)# seq 20 permit 00:00:00:00:11:11 00:00:11:11:11:11
any vlan 2
```

**支持的版本** 10.2.0E or later

## seq permit icmp

在创建筛选器时分配一个序列号以允许 ICMP 消息

**语法** *seq sequence-number permit icmp* [*A.B.C.D* | *A.B.C.D/x* | *any* | *host ip-address*] [*A.B.C.D* | *A.B.C.D/x* | *any* | *host ip-address*] [*capture* | *count* | *dscp value* | *fragment* | *log*]

- 参数**
- *sequence-number* — 输入序列号, 以标识用于编辑的路由映射和顺序编号, 从 1 到 16777214。
  - *A.B.C.D* — 以点分隔的十进制格式输入 IPv4 地址。
  - *A.B.C.D/x* — 输入必须与点分十进制地址匹配的位数。
  - *any* — (可选) 输入关键字 *any* 以指定任何源或目标 IP 地址。
  - *host ip-address* — (可选) 输入 IPv4 地址, 以仅使用主机地址。
  - *capture* — (可选) 捕获筛选器处理的数据包。
  - *count* — (可选) 计算筛选器处理的数据包数。
  - *byte* — (可选) 计算筛选器处理的字节数。
  - *dscp value* — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。
  - *fragment* — (可选) 使用 ACL 控制数据包片段。
  - *log* — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

**默认** 未配置

**命令模式** IPV4-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数; 当您输入 *count byte* 选项时, 仅增加字节数。此命令的 *no* 版本将移除筛选器, 或者如果您知道筛选器的顺序编号, 则使用 *no seq sequence-number* 命令。

**示例**

```
OS10(config)# ip access-list egress
OS10(conf-ipv4-acl)# seq 5 permit icmp any any capture session 1 log
```

**支持的版本** 10.2.0E or later

## seq permit icmp (IPv6)

在创建筛选器时分配一个序列号以允许 ICMP 消息。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>seq sequence-number permit icmp [A::B   A::B/x   any   host ipv6-address] [A::B   A:B/x   any   host ipv6-address] [capture   count   dscp value   fragment   log]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 参数     | <ul style="list-style-type: none"><li><code>sequence-number</code> — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。</li><li><code>A::B</code> — 以十六进制格式输入采用冒号分隔的 IPv6 地址。</li><li><code>A::B/x</code> — 输入必须与 IPv6 地址匹配的位数。</li><li><code>any</code> — (可选) 输入关键字 <code>any</code> 以指定任何源或目标 IP 地址。</li><li><code>host ipv6-address</code> — (可选) 输入 IPv6 地址，以仅使用主机地址。</li><li><code>capture</code> — (可选) 捕获筛选器处理的数据包。</li><li><code>count</code> — (可选) 计算筛选器处理的数据包数。</li><li><code>byte</code> — (可选) 计算筛选器处理的字节数。</li><li><code>dscp value</code> — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。</li><li><code>fragment</code> — (可选) 使用 ACL 控制数据包片段。</li><li><code>log</code> — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 命令模式   | IPv6-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 <code>count byte</code> 选项时，仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 <code>no seq sequence-number</code> 命令。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 示例     | <pre>OS10(config)# ipv6 access-list ipv6test OS10(conf-ipv6-acl)# seq 5 permit icmp any any capture session 1 log</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## seq permit ip

在创建筛选器时分配序列号以允许数据包。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>seq sequence-number permit ip [A.B.C.D   A.B.C.D/x   any   host ip-address] [A.B.C.D   A.B.C.D/x   any   host ip-address] [capture   count   dscp value   fragment   log]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 参数     | <ul style="list-style-type: none"><li><code>sequence-number</code> — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。</li><li><code>A.B.C.D</code> — 以点分隔的十进制格式输入 IPv4 地址。</li><li><code>A.B.C.D/x</code> — 输入必须与点分十进制地址匹配的位数。</li><li><code>any</code> — (可选) 输入关键字 <code>any</code> 以指定任何源或目标 IP 地址。</li><li><code>host ip-address</code> — (可选) 输入 IPv4 地址，以仅使用主机地址。</li><li><code>capture</code> — (可选) 捕获筛选器处理的数据包。</li><li><code>count</code> — (可选) 计算筛选器处理的数据包数。</li><li><code>byte</code> — (可选) 计算筛选器处理的字节数。</li><li><code>dscp value</code> — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。</li><li><code>fragment</code> — (可选) 使用 ACL 控制数据包片段。</li><li><code>log</code> — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 命令模式   | IPv4-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 <code>count byte</code> 选项时，仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 <code>no seq sequence-number</code> 命令。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## 示例

```
OS10(config)# ip access-list egress
OS10(conf-ip4-acl)# seq 5 permit ip any any capture session 1 log
```

支持的版本 10.2.0E or later

## seq permit ipv6

在创建筛选器时分配序列号以允许数据包。

**语法** `seq sequence-number permit ipv6 [A::B | A::B/x | any | host ipv6-address] [A::B | A::B/x | any | host ipv6-address] [capture | count | dscp value | fragment | log]`

- 参数**
- `sequence-number` — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。
  - `A::B` — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
  - `A::B/x` — 输入必须与 IPv6 地址匹配的位数。
  - `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
  - `host ipv6-address` — (可选) 输入 IPv6 地址，以仅使用主机地址。
  - `capture` — (可选) 捕获筛选器处理的数据包。
  - `count` — (可选) 计算筛选器处理的数据包数。
  - `byte` — (可选) 计算筛选器处理的字节数。
  - `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。
  - `fragment` — (可选) 使用 ACL 控制数据包片段。
  - `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

**默认** 未配置

**命令模式** IPV6-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数；当您输入 `count byte` 选项时，仅增加字节数。此命令的 `no` 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 `no seq sequence-number` 命令。

## 示例

```
OS10(config)# ipv6 access-list egress
OS10(conf-ipv6-acl)# seq 5 permit ipv6 any any capture session 1 log
```

支持的版本 10.2.0E or later

## seq permit tcp

在创建筛选器时分配序列号以允许 TCP 数据包。

**语法** `seq sequence-number permit tcp [A.B.C.D | A.B.C.D/x | any | host ip-address [operator]] [[A.B.C.D | A.B.C.D/x | any | host ip-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | count | dscp value | fragment | log]`

- 参数**
- `sequence-number` — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。
  - `A.B.C.D` — 以点分隔的十进制格式输入 IPv4 地址。
  - `A.B.C.D/x` — 输入必须与点分十进制地址匹配的位数。
  - `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
  - `host ip-address` — (可选) 输入 IPv4 地址，以仅使用主机地址。
  - `operator` — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用：
    - `eq` — 等于
    - `gt` — 大于
    - `lt` — 小于
    - `neq` — 不等于
    - `range` — 端口范围，包括指定的端口号。
  - `ack` — (可选) 将“位”设置为“确认”。

- `fin` — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。
- `psh` — (可选) 将“位”设置为“推送”。
- `rst` — (可选) 将“位”设置为“重置”。
- `syn` — (可选) 将“位”设置为“同步”。
- `urg` — (可选) 将“位”设置为“紧急”。
- `capture` — (可选) 捕获筛选器处理的数据包。
- `count` — (可选) 计算筛选器处理的数据包数。
- `byte` — (可选) 计算筛选器处理的字节数。
- `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。
- `fragment` — (可选) 使用 ACL 控制数据包片段。
- `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

**默认** 未配置

**命令模式** IPV4-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数；当您输入 `count byte` 选项时，仅增加字节数。此命令的 `no` 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 `no seq sequence-number` 命令。

**示例**

```
OS10(config)# ip access-list egress
OS10(conf-ip4-acl)# seq 5 permit tcp any any capture session 1 log
```

**支持的版本** 10.2.0E or later

## seq permit tcp (IPv6)

在创建筛选器时分配序列号以允许 TCP IPv6 数据包。

**语法** `seq sequence-number permit tcp [A::B | A::B/x | any | host ipv6-address [operator]] [A::B | A::B/x | any | host ipv6-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | count | dscp value | fragment | log]`

**参数**

- `sequence-number` — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。
- `A::B` — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
- `A::B/x` — 输入必须与 IPv6 地址匹配的位数。
- `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
- `host ipv6-address` — (可选) 输入 IPv6 地址，以仅使用主机地址。
- `operator` — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用：
  - `eq` — 等于
  - `gt` — 大于
  - `lt` — 小于
  - `neq` — 不等于
  - `range` — 端口范围，包括指定的端口号。
- `ack` — (可选) 将“位”设置为“确认”。
- `fin` — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。
- `psh` — (可选) 将“位”设置为“推送”。
- `rst` — (可选) 将“位”设置为“重置”。
- `syn` — (可选) 将“位”设置为“同步”。
- `urg` — (可选) 将“位”设置为“紧急”。
- `capture` — (可选) 捕获筛选器处理的数据包。
- `count` — (可选) 计算筛选器处理的数据包数。
- `byte` — (可选) 计算筛选器处理的字节数。
- `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。
- `fragment` — (可选) 使用 ACL 控制数据包片段。
- `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

**默认** 未配置

**命令模式** IPV6-ACL

|        |                                                                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 <code>count byte</code> 选项时，仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 <code>no seq sequence-number</code> 命令。 |
| 示例     | <pre>OS10(config)# ipv6 access-list egress OS10(conf-ipv6-acl)# seq 5 permit tcp any any capture session 1 log</pre>                                 |
| 支持的版本  | 10.2.0E or later                                                                                                                                     |

## seq permit udp

在创建筛选器时分配序列号以允许 UDP 数据包。

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | <code>seq sequence-number permit udp [A.B.C.D   A.B.C.D/x   any   host ip-address [operator]] [[A.B.C.D   A.B.C.D/x   any   host ip-address [operator] ] [ack   fin   psh   rst   syn   urg] [capture   count   dscp value   fragment   log]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 参数   | <ul style="list-style-type: none"><li>• <code>sequence-number</code> — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。</li><li>• <code>A.B.C.D</code> — 以点分隔的十进制格式输入 IPv4 地址。</li><li>• <code>A.B.C.D/x</code> — 输入必须与点分十进制地址匹配的位数。</li><li>• <code>any</code> — （可选）输入关键字 <code>any</code> 以指定任何源或目标 IP 地址。</li><li>• <code>host ip-address</code> — （可选）输入 IPv4 地址，以仅使用主机地址。</li><li>• <code>operator</code> — （可选）输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用：<ul style="list-style-type: none"><li>◦ <code>eq</code> — 等于</li><li>◦ <code>gt</code> — 大于</li><li>◦ <code>lt</code> — 小于</li><li>◦ <code>neq</code> — 不等于</li><li>◦ <code>range</code> — 端口范围，包括指定的端口号。</li></ul></li><li>• <code>ack</code> — （可选）将“位”设置为“确认”。</li><li>• <code>fin</code> — （可选）将“位”设置为“完成” — 不能从发件人获得更多数据。</li><li>• <code>psh</code> — （可选）将“位”设置为“推送”。</li><li>• <code>rst</code> — （可选）将“位”设置为“重置”。</li><li>• <code>syn</code> — （可选）将“位”设置为“同步”。</li><li>• <code>urg</code> — （可选）将“位”设置为“紧急”。</li><li>• <code>capture</code> — （可选）捕获筛选器处理的数据包。</li><li>• <code>count</code> — （可选）计算筛选器处理的数据包数。</li><li>• <code>byte</code> — （可选）计算筛选器处理的字节数。</li><li>• <code>dscp value</code> — （可选）根据 DSCP 值（从 0 到 63）拒绝数据包。</li><li>• <code>fragment</code> — （可选）使用 ACL 控制数据包片段。</li><li>• <code>log</code> — （可选）启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。</li></ul> |
| 默认   | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 命令模式 | IPv4-ACL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|        |                                                                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 使用情况信息 | OS10 不能同时计算数据包和字节数；当您输入 <code>count byte</code> 选项时，仅增加字节数。此命令的 <code>no</code> 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 <code>no seq sequence-number</code> 命令。 |
| 示例     | <pre>OS10(config)# ip access-list egress OS10(conf-ipv4-acl)# seq 5 permit udp any any capture session 1 log</pre>                                   |
| 支持的版本  | 10.2.0E or later                                                                                                                                     |



## seq permit udp (IPv6)

在创建筛选器时分配序列号以允许 UDP IPv6 数据包。

**语法** `seq sequence-number permit udp [A::B | A::B/x | any | host ipv6-address [operator]] [A::B | A::B/x | any | host ipv6-address [operator]] [ack | fin | psh | rst | syn | urg] [capture | count | dscp value | fragment | log]`

- 参数**
- `sequence-number` — 输入序列号，以标识用于编辑的路由映射和顺序编号，从 1 到 16777214。
  - `A::B` — 以十六进制格式输入采用冒号分隔的 IPv6 地址。
  - `A::B/x` — 输入必须与 IPv6 地址匹配的位数。
  - `any` — (可选) 输入关键字 `any` 以指定任何源或目标 IP 地址。
  - `host ipv6-address` — (可选) 输入 IPv6 地址，以仅使用主机地址。
  - `operator` — (可选) 输入逻辑运算符以匹配指定端口号上的数据包。下列选项可用：
    - `eq` — 等于
    - `gt` — 大于
    - `lt` — 小于
    - `neq` — 不等于
    - `range` — 端口范围，包括指定的端口号。
  - `ack` — (可选) 将“位”设置为“确认”。
  - `fin` — (可选) 将“位”设置为“完成” — 不能从发件人获得更多数据。
  - `psh` — (可选) 将“位”设置为“推送”。
  - `rst` — (可选) 将“位”设置为“重置”。
  - `syn` — (可选) 将“位”设置为“同步”。
  - `urg` — (可选) 将“位”设置为“紧急”。
  - `capture` — (可选) 捕获筛选器处理的数据包。
  - `count` — (可选) 计算筛选器处理的数据包数。
  - `byte` — (可选) 计算筛选器处理的字节数。
  - `dscp value` — (可选) 根据 DSCP 值 (从 0 到 63) 允许数据包。
  - `fragment` — (可选) 使用 ACL 控制数据包片段。
  - `log` — (可选) 启用 ACL 日志记录。记录与 ACL 规则匹配的数据包的信息。

**默认** 未配置

**命令模式** IPV6-ACL

**使用情况信息** OS10 不能同时计算数据包和字节数；当您输入 `count byte` 选项时，仅增加字节数。此命令的 `no` 版本将移除筛选器，或者如果您知道筛选器的顺序编号，则使用 `no seq sequence-number` 命令。

**示例**

```
OS10(config)# ipv6 access-list egress
OS10(conf-ipv6-acl)# seq 5 permit udp any any capture session 1 log
```

**支持的版本** 10.2.0E or later

## show access-group

显示 IP、MAC 或 IPv6 访问组信息。

**语法** `show {ip | mac | ipv6} access-group name`

- 参数**
- `ip` — 查看 IP 访问组信息。
  - `mac` — 查看 MAC 访问组信息。
  - `ipv6` — 查看 IPv6 访问组信息。
  - `access-group name` — 输入访问组的名称。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

### 示例 (IP)

```
OS10# show ip access-group aaa
Ingress IP access list aaa on ethernet1/1/1
Ingress IP access list aaa on ethernet1/1/2
Egress IP access list aaa on ethernet1/1/2
```

### 示例 (MAC)

```
OS10# show mac access-group bbb
Ingress MAC access list aaa on ethernet1/1/1
Ingress MAC access list aaa on ethernet1/1/2
Egress MAC access list aaa on ethernet1/1/2
```

### 示例 (IPv6)

```
OS10# show ipv6 access-group ccc
Ingress IPV6 access list aaa on ethernet1/1/1
Ingress IPV6 access list aaa on ethernet1/1/2
Egress IPV6 access list aaa on ethernet1/1/2
```

### 示例 (控制平面 ACL - IP)

```
OS10# show ip access-group aaa-cp-acl
Ingress IP access-list aaa-cp-acl on control-plane data mgmt
```

### 示例 (控制平面 ACL - MAC)

```
OS10# show mac access-group aaa-cp-acl
Ingress MAC access-list aaa-cp-acl on control-plane data
```

### 示例 (控制平面 ACL - IPv6)

```
OS10# show ipv6 access-group aaa-cp-acl
Ingress IPV6 access-list aaa-cp-acl on control-plane data mgmt
```

### 支持的版本

10.2.0E or later; 10.4.1 或更高版本 (控制平面 ACL)

## show access-lists

显示 IP、MAC 或 IPv6 访问列表信息。

#### 语法

```
show {ip | mac | ipv6} access-lists {in | out} access-list-name
```

#### 参数

- ip — 查看 IP 访问列表信息。
- mac — 查看 MAC 访问列表信息。
- ipv6 — 查看 IPv6 访问列表信息。
- access-lists in | out — 输入 access lists in 或 access lists out。
- access-list-name — 输入访问列表的名称。

#### 默认

未配置

#### 命令模式

EXEC

#### 使用情况信息

无

### 示例 (MAC 输入)

```
OS10# show mac access-lists in
Ingress MAC access list aaa
Active on interfaces :
 ethernet1/1/1
 ethernet1/1/2
seq 10 permit any any
seq 20 permit 11:11:11:11:11:11 22:22:22:22:22:22 any monitor count
bytes (0 bytes)
```

### 示例 (MAC 输出)

```
OS10# show mac access-lists out
Egress MAC access list aaa
Active on interfaces :
 ethernet1/1/1
 ethernet1/1/2
seq 10 permit any any
```



```
seq 20 permit 11:11:11:11:11:11 22:22:22:22:22:22 any monitor count
bytes (0 bytes)
```

#### 示例 (IP 输入)

```
OS10# show ip access-lists in
Ingress IP access list aaaa
Active on interfaces :
 ethernet1/1/1
 ethernet1/1/2
seq 10 permit ip any any log
seq 20 permit tcp any any count (0 packets)
seq 30 permit udp any any count bytes (0 bytes)
```

#### 示例 (IP 输出)

```
OS10# show ip access-lists out
Egress IP access list aaaa
Active on interfaces :
 ethernet1/1/1
 ethernet1/1/2
seq 10 permit ip any any
seq 20 permit tcp any any count (0 packets)
seq 30 permit udp any any count bytes (0 bytes)
```

#### 示例 (IPv6 输入)

```
OS10# show ipv6 access-lists in
Ingress IPV6 access list bbb
Active on interfaces :
 ethernet1/1/1
 ethernet1/1/2
seq 10 permit any any
Ingress IPV6 access list ggg
Active on interfaces :
 ethernet 1/1/3
seq 5 permit ipv6 11::/32 any log count (0 packets)
```

#### 示例 (IPv6 输出)

```
OS10# show ipv6 access-lists out
Egress IPV6 access list bbb
Active on interfaces :
 ethernet1/1/1
 ethernet1/1/2
seq 10 permit any any
Egress IPV6 access list ggg
Active on interfaces :
 ethernet 1/1/1
seq 5 permit ipv6 11::/32 any count (0 packets)
```

#### 示例 (IP 输入 — 控制平面 ACL)

```
OS10# show ip access-lists in
Ingress IP access-list aaa-cp-acl
Active on interfaces :
 control-plane data
seq 10 permit ip any any
 control-plane mgmt
seq 10 permit ip any any
```

#### 示例 (IPv6 输入 — 控制平面 ACL)

```
OS10# show ipv6 access-lists in
Ingress IPV6 access-list aaa-cp-acl
Active on interfaces :
 control-plane data
seq 10 permit ipv6 any any
 control-plane mgmt
seq 10 permit ipv6 any any
```

#### 示例 (MAC 输入 — 控制平面 ACL)

```
OS10# show mac access-lists in
Ingress MAC access-list mac-cp1
Active on interfaces :
```

```
control-plane data
seq 10 deny any any count (159 packets)
```

**支持的版本** 10.2.0E or later; 10.4.1 或更高版本 (控制平面 ACL)

## show acl-table-usage detail

显示入口和出口 ACL 表、使用的功能及其空间利用率。

**语法** show acl-table-usage detail

**参数** 无

**默认** 无

**命令模式** EXEC

**使用情况信息** 硬件池显示入口应用程序组（池）、映射到每个组的功能，以及每个池中的已用和可用空间量。在池中存储单个 ACL 规则的主要宽度。

服务池显示每个功能的已用和可用空间量。为某个功能配置的 ACL 规则数将显示在已配置的规则列中。已用行的数量显示为已用行的数量。

**示例** Z9100-ON 平台

```
OS10# show acl-table-usage detail
```

```
Ingress ACL utilization - Pipe 0
Hardware Pools
```

| Pool ID | App(s)        | Used rows | Free rows | Max rows |
|---------|---------------|-----------|-----------|----------|
| 0       | SYSTEM_FLOW   | 98        | 414       | 512      |
| 1       | SYSTEM_FLOW   | 98        | 414       | 512      |
| 2       | SYSTEM_FLOW   | 98        | 414       | 512      |
| 3       | USER_IPV4_ACL | 4         | 508       | 512      |
| 4       | USER_IPV4_ACL | 4         | 508       | 512      |
| 5       | FREE          | 0         | 512       | 512      |
| 6       | USER_IPV6_ACL | 4         | 508       | 512      |
| 7       | USER_IPV6_ACL | 4         | 508       | 512      |
| 8       | USER_IPV6_ACL | 4         | 508       | 512      |
| 9       | USER_L2_ACL   | 4         | 508       | 512      |
| 10      | USER_L2_ACL   | 4         | 508       | 512      |
| 11      | FREE          | 0         | 512       | 512      |

```
Service Pools
```

| App                  | Allocated pools | App group | Configured rules | Used rows |
|----------------------|-----------------|-----------|------------------|-----------|
| USER_L2_ACL<br>256   | Shared:2        | G9        | 1                | 2         |
| USER_IPV4_ACL<br>256 | Shared:2        | G3        | 1                | 2         |
| USER_IPV6_ACL<br>256 | Shared:3        | G6        | 1                | 2         |
| SYSTEM_FLOW<br>256   | Shared:3        | G0        | 49               | 49        |

```
Ingress ACL utilization - Pipe 1
Hardware Pools
```

| Pool ID | App(s)        | Used rows | Free rows | Max rows |
|---------|---------------|-----------|-----------|----------|
| 0       | SYSTEM_FLOW   | 98        | 414       | 512      |
| 1       | SYSTEM_FLOW   | 98        | 414       | 512      |
| 2       | SYSTEM_FLOW   | 98        | 414       | 512      |
| 3       | USER_IPV4_ACL | 0         | 512       | 512      |
| 4       | USER_IPV4_ACL | 0         | 512       | 512      |
| 5       | FREE          | 0         | 512       | 512      |

|                                  |                 |           |                  |           |
|----------------------------------|-----------------|-----------|------------------|-----------|
| 6                                | USER_IPV6_ACL   | 0         | 512              | 512       |
| 7                                | USER_IPV6_ACL   | 0         | 512              | 512       |
| 8                                | USER_IPV6_ACL   | 0         | 512              | 512       |
| 9                                | USER_L2_ACL     | 0         | 512              | 512       |
| 10                               | USER_L2_ACL     | 0         | 512              | 512       |
| 11                               | FREE            | 0         | 512              | 512       |
| -----                            |                 |           |                  |           |
| Service Pools                    |                 |           |                  |           |
| -----                            |                 |           |                  |           |
| App                              | Allocated pools | App group | Configured rules | Used rows |
| -----                            |                 |           |                  |           |
| SYSTEM_FLOW                      | Shared:3        | G0        | 49               | 49        |
| 256                              |                 |           |                  |           |
| -----                            |                 |           |                  |           |
| Ingress ACL utilization - Pipe 2 |                 |           |                  |           |
| Hardware Pools                   |                 |           |                  |           |
| -----                            |                 |           |                  |           |
| Pool ID                          | App(s)          | Used rows | Free rows        | Max rows  |
| -----                            |                 |           |                  |           |
| 0                                | SYSTEM_FLOW     | 98        | 414              | 512       |
| 1                                | SYSTEM_FLOW     | 98        | 414              | 512       |
| 2                                | SYSTEM_FLOW     | 98        | 414              | 512       |
| 3                                | USER_IPV4_ACL   | 0         | 512              | 512       |
| 4                                | USER_IPV4_ACL   | 0         | 512              | 512       |
| 5                                | FREE            | 0         | 512              | 512       |
| 6                                | USER_IPV6_ACL   | 0         | 512              | 512       |
| 7                                | USER_IPV6_ACL   | 0         | 512              | 512       |
| 8                                | USER_IPV6_ACL   | 0         | 512              | 512       |
| 9                                | USER_L2_ACL     | 0         | 512              | 512       |
| 10                               | USER_L2_ACL     | 0         | 512              | 512       |
| 11                               | FREE            | 0         | 512              | 512       |
| -----                            |                 |           |                  |           |
| Service Pools                    |                 |           |                  |           |
| -----                            |                 |           |                  |           |
| App                              | Allocated pools | App group | Configured rules | Used rows |
| -----                            |                 |           |                  |           |
| SYSTEM_FLOW                      | Shared:3        | G0        | 49               | 49        |
| 256                              |                 |           |                  |           |
| -----                            |                 |           |                  |           |
| Ingress ACL utilization - Pipe 3 |                 |           |                  |           |
| Hardware Pools                   |                 |           |                  |           |
| -----                            |                 |           |                  |           |
| Pool ID                          | App(s)          | Used rows | Free rows        | Max rows  |
| -----                            |                 |           |                  |           |
| 0                                | SYSTEM_FLOW     | 98        | 414              | 512       |
| 1                                | SYSTEM_FLOW     | 98        | 414              | 512       |
| 2                                | SYSTEM_FLOW     | 98        | 414              | 512       |
| 3                                | USER_IPV4_ACL   | 0         | 512              | 512       |
| 4                                | USER_IPV4_ACL   | 0         | 512              | 512       |
| 5                                | FREE            | 0         | 512              | 512       |
| 6                                | USER_IPV6_ACL   | 0         | 512              | 512       |
| 7                                | USER_IPV6_ACL   | 0         | 512              | 512       |
| 8                                | USER_IPV6_ACL   | 0         | 512              | 512       |
| 9                                | USER_L2_ACL     | 0         | 512              | 512       |
| 10                               | USER_L2_ACL     | 0         | 512              | 512       |
| 11                               | FREE            | 0         | 512              | 512       |
| -----                            |                 |           |                  |           |
| Service Pools                    |                 |           |                  |           |
| -----                            |                 |           |                  |           |
| App                              | Allocated pools | App group | Configured rules | Used rows |
| -----                            |                 |           |                  |           |
| SYSTEM_FLOW                      | Shared:3        | G0        | 49               | 49        |
| 256                              |                 |           |                  |           |
| -----                            |                 |           |                  |           |
| Egress ACL utilization           |                 |           |                  |           |
| Hardware Pools                   |                 |           |                  |           |
| -----                            |                 |           |                  |           |
| Pool ID                          | App(s)          | Used rows |                  |           |
| -----                            |                 |           |                  |           |
| 0                                | FREE            | 0         |                  |           |
| 256                              |                 |           |                  |           |
| 1                                | FREE            | 0         |                  |           |

|               |                 |           |                  |           |
|---------------|-----------------|-----------|------------------|-----------|
| 256           |                 |           |                  |           |
| 2             | FREE            |           |                  | 0         |
| 256           |                 |           |                  |           |
| 3             | FREE            |           |                  | 0         |
| 256           |                 |           |                  |           |
| -----         |                 |           |                  |           |
| Service Pools |                 |           |                  |           |
| -----         |                 |           |                  |           |
| App           | Allocated pools | App group | Configured rules | Used rows |
| -----         |                 |           |                  |           |
| -----         |                 |           |                  |           |

S6010-ON 平台

|                                   |                    |           |                  |           |
|-----------------------------------|--------------------|-----------|------------------|-----------|
| OS10# show acl-table-usage detail |                    |           |                  |           |
| Ingress ACL utilization           |                    |           |                  |           |
| Hardware Pools                    |                    |           |                  |           |
| -----                             |                    |           |                  |           |
| Pool ID                           | App(s)             | Used rows | Free rows        | Max rows  |
| -----                             |                    |           |                  |           |
| 0                                 | SYSTEM_FLOW        | 49        | 975              | 1024      |
| 1                                 | SYSTEM_FLOW        | 49        | 975              | 1024      |
| 2                                 | USER_IPV4_ACL      | 3         | 1021             | 1024      |
| 3                                 | USER_L2_ACL        | 2         | 1022             | 1024      |
| 4                                 | USER_IPV6_ACL      | 2         | 510              | 512       |
| 5                                 | USER_IPV6_ACL      | 2         | 510              | 512       |
| 6                                 | FCOE               | 55        | 457              | 512       |
| 7                                 | FCOE               | 55        | 457              | 512       |
| 8                                 | ISCSI_SNOOPING     | 12        | 500              | 512       |
| 9                                 | FREE               | 0         | 512              | 512       |
| 10                                | PBR_V6             | 1         | 511              | 512       |
| 11                                | PBR_V6             | 1         | 511              | 512       |
| -----                             |                    |           |                  |           |
| Service Pools                     |                    |           |                  |           |
| -----                             |                    |           |                  |           |
| App                               | Allocated pools    | App group | Configured rules | Used rows |
| -----                             |                    |           |                  |           |
| USER_L2_ACL                       | Shared:1           | G3        | 1                | 2         |
| 1024                              |                    |           |                  |           |
| USER_IPV4_ACL                     | Shared:1           | G2        | 2                | 3         |
| 1024                              |                    |           |                  |           |
| USER_IPV6_ACL                     | Shared:2           | G4        | 1                | 2         |
| 512                               |                    |           |                  |           |
| PBR_V6                            | Shared:2           | G10       | 1                | 1         |
| 512                               |                    |           |                  |           |
| SYSTEM_FLOW                       | Shared:2           | G0        | 49               | 49        |
| 1024                              |                    |           |                  |           |
| ISCSI_SNOOPING                    | Shared:1           | G8        | 12               | 12        |
| 512                               |                    |           |                  |           |
| FCOE                              | Shared:2           | G6        | 55               | 55        |
| 512                               |                    |           |                  |           |
| -----                             |                    |           |                  |           |
| Egress ACL utilization            |                    |           |                  |           |
| Hardware Pools                    |                    |           |                  |           |
| -----                             |                    |           |                  |           |
| Pool ID                           | App(s)             | Used rows | Free rows        | Max rows  |
| -----                             |                    |           |                  |           |
| 0                                 | USER_IPV4_EGRESS   | 2         | 254              | 256       |
| 1                                 | USER_L2_ACL_EGRESS | 2         | 254              | 256       |
| 2                                 | USER_IPV6_EGRESS   | 2         | 254              | 256       |
| 3                                 | USER_IPV6_EGRESS   | 2         | 254              | 256       |
| -----                             |                    |           |                  |           |
| Service Pools                     |                    |           |                  |           |
| -----                             |                    |           |                  |           |
| App                               | Allocated pools    | App group | Configured rules | Used rows |
| -----                             |                    |           |                  |           |
| USER_L2_ACL_EGRESS                | Shared:1           | G1        | 1                | 2         |
| 256                               |                    |           |                  |           |
| USER_IPV4_EGRESS                  | Shared:1           | G0        | 1                | 2         |
| 256                               |                    |           |                  |           |

|                  |          |    |   |   |
|------------------|----------|----|---|---|
| USER_IPV6_EGRESS | Shared:2 | G2 | 1 | 2 |
|------------------|----------|----|---|---|

**支持的版本** 10.4.2 和更高版本

## show ip as-path-access-list

显示配置的 AS 路径访问列表。

- 语法** show ip as-path-access-list [*name*]
- 参数** *name* — (可选) 指定 AS 路径访问列表的名称。
- 默认** 无
- 命令模式** EXEC
- 使用情况信息** 无
- 示例**

```
OS10# show ip as-path-access-list
ip as-path access-list hello
 permit 123
 deny 35
```

**支持的版本** 10.3.0E or later

## show ip community-list

按字母顺序显示已配置的 IP 社区列表。

- 语法** show ip community-list [*name*]
- 参数** *name* — (可选) 输入标准 IP 社区列表的名称。最多 140 个字符。
- 默认** 无
- 命令模式** EXEC
- 使用情况信息** 无
- 示例**

```
OS10# show ip community-list
Standard Community List hello
 deny local-AS
 permit no-export
 deny 1:1
```

**支持的版本** 10.3.0E or later

## show ip extcommunity-list

按字母顺序显示配置的 IP 外部社区列表。

- 语法** show ip extcommunity-list [*name*]
- 参数** *name* — (可选) 输入扩展 IP 外部社区列表的名称。最多 140 个字符。
- 默认** 无
- 命令模式** EXEC
- 使用情况信息** 无
- 示例**

```
OS10# show ip extcommunity-list
Standard Extended Community List hello
```

```
permit RT:1:1
deny SOO:1:4
```

支持的版本 10.3.0E or later

## show ip prefix-list

显示配置的 IPv4 或 IPv6 前缀列表信息。

|        |                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show {ip   ipv6} prefix-list [prefix-name]                                                                                                 |
| 参数     | <ul style="list-style-type: none"><li>ip   ipv6 — (可选) 显示与 IPv4 或 IPv6 相关的信息。</li><li>prefix-name — 为前缀列表名称输入一个文本字符串。最多 140 个字符。</li></ul> |
| 默认     | 无                                                                                                                                          |
| 命令模式   | EXEC                                                                                                                                       |
| 使用情况信息 | 无                                                                                                                                          |
| 示例     |                                                                                                                                            |

```
OS10# show ip prefix-list
ip prefix-list hello:
seq 10 deny 1.2.3.4/24
seq 20 permit 3.4.4.5/32
```

### 示例 (IPv6)

```
OS10# show ipv6 prefix-list
ipv6 prefix-list hello:
seq 10 permit 1::1/64
seq 20 deny 2::2/64
```

支持的版本 10.3.0E or later

## 显示日志记录访问列表

显示 ACL 日志记录阈值和时间间隔配置。

|        |                          |
|--------|--------------------------|
| 语法     | show logging access-list |
| 参数     | 无                        |
| 默认     | 无                        |
| 命令模式   | EXEC                     |
| 使用情况信息 | 无                        |
| 示例     |                          |

```
OS10# show logging access-list
ACL Logging
Threshold : 10
Interval : 5
```

支持的版本 10.4.3.0 or later

## 路由映射命令

### continue

配置路由映射的下一个序列。

|    |                     |
|----|---------------------|
| 语法 | continue seq-number |
|----|---------------------|

|        |                                           |
|--------|-------------------------------------------|
| 参数     | <i>seq-number</i> — 输入下一个序列号，从 1 到 65535。 |
| 默认     | 未配置                                       |
| 命令模式   | ROUTE-MAP                                 |
| 使用情况信息 | 此命令的 <code>no</code> 版本将删除匹配。             |
| 示例     |                                           |

```
OS10(config)# route-map bgp
OS10(conf-route-map)# continue 65535
```

支持的版本 10.3.0E or later

## match as-path

配置筛选器以匹配其 BGP 路径中具有特定 AS 路径的路由。

|        |                                                          |
|--------|----------------------------------------------------------|
| 语法     | <code>match as-path as-path-name</code>                  |
| 参数     | <i>as-path-name</i> — 输入已建立的 AS-PATH ACL 的名称。最多 140 个字符。 |
| 默认     | 未配置                                                      |
| 命令模式   | ROUTE-MAP                                                |
| 使用情况信息 | 此命令的 <code>no</code> 版本将删除匹配 AS 路径筛选器。                   |
| 示例     |                                                          |

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match as-path pathtest1
```

支持的版本 10.3.0E or later

## match community

配置筛选器以匹配其 BGP 路径中具有特定 COMMUNITY 属性的路由。

|        |                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>match community community-list-name [exact-match]</code>                                                                                             |
| 参数     | <ul style="list-style-type: none"> <li><i>community-list-name</i> — 输入已配置的社区列表的名称。</li> <li><code>exact-match</code> — (可选) 仅选择具有指定社区列表名称的那些路由。</li> </ul> |
| 默认     | 未配置                                                                                                                                                        |
| 命令模式   | ROUTE-MAP                                                                                                                                                  |
| 使用情况信息 | 此命令的 <code>no</code> 版本将删除社区匹配筛选器。                                                                                                                         |
| 示例     |                                                                                                                                                            |

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match community commlist1 exact-match
```

支持的版本 10.3.0E or later

## match extcommunity

配置筛选器以匹配其 BGP 路径中具有特定 EXTCOMMUNITY 属性的路由。

|      |                                                                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | <code>match extcommunity extcommunity-list-name [exact-match]</code>                                                                                              |
| 参数   | <ul style="list-style-type: none"> <li><i>extcommunity-list-name</i> — 输入已配置的扩展社区列表的名称。</li> <li><code>exact-match</code> — (可选) 仅选择具有指定扩展社区列表名称的那些路由。</li> </ul> |
| 默认   | 未配置                                                                                                                                                               |
| 命令模式 | ROUTE-MAP                                                                                                                                                         |

**使用情况信息** 此命令的 `no` 版本将删除扩展社区匹配筛选器。

**示例**

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match extcommunity extcommlist1 exact-match
```

**支持的版本** 10.3.0E or later

## match interface

配置筛选器以匹配下一中继站配置的接口的路由。

**语法** `match interface interface`

**参数** `interface` — 接口类型:

- `ethernet node/slot/port[:subport]` — 输入下一跳接口的以太网接口信息。
- `port-channel id-number` — 输入端口通道号作为下一跳接口, 从 1 到 128。
- `vlan vlan-id` — 输入 VLAN 号作为下一跳接口, 从 1 到 4093。

**默认** 未配置

**命令模式** ROUTE-MAP

**使用情况信息** 此命令的 `no` 版本将删除匹配。

**示例**

```
OS10(conf-route-map)# match interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)#
```

**支持的版本** 10.2.0E or later

## match ip address

配置筛选器以根据 IP 前缀列表中指定的 IP 地址匹配路由。

**语法** `match ip address {prefix-list prefix-list-name | access-list-name}`

**参数**

- `prefix-list-name` — 输入已配置的前缀列表的名称。最多 140 个字符。
- `access-list-name` — 输入已配置的访问列表的名称。

**默认** 未配置

**命令模式** ROUTE-MAP

**使用情况信息** 此命令的 `no` 版本将删除匹配。

**示例**

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match ip address prefix-list test10
```

**支持的版本** 10.3.0E or later

## match ip next-hop

根据在 IP 前缀列表中指定的下一跳 IP 地址配置筛选器以进行匹配。

**语法** `match ip next-hop prefix-list prefix-list`

**参数**

`prefix-list` — 输入已配置的前缀列表的名称。最多 140 个字符。

**默认** 未配置

**命令模式** ROUTE-MAP

**使用情况信息** 此命令的 `no` 版本将删除匹配。



## 示例

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match ip next-hop prefix-list test100
```

支持的版本 10.3.0E or later

## match ipv6 address

配置筛选器以根据 IP 前缀列表中指定的 IPv6 地址匹配路由。

**语法** `match ipv6 address {prefix-list prefix-list | access-list}`

- 参数**
- *prefix-list* — 输入已配置的前缀列表的名称。最多 140 个字符。
  - *access-list* — 输入访问组或列表的名称。

**默认** 未配置

**命令模式** ROUTE-MAP

**使用情况信息** 此命令的 `no` 版本将删除匹配。

## 示例

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match ipv6 address test100
```

支持的版本 10.3.0E or later

## match ipv6 next-hop

根据在 IP 前缀列表中指定的下一跳 IPv6 地址配置筛选器以进行匹配。

**语法** `match ipv6 next-hop prefix-list prefix-list`

**参数** *prefix-list* — 输入已配置的前缀列表的名称。最多 140 个字符。

**默认** 未配置

**命令模式** ROUTE-MAP

**使用情况信息** 此命令的 `no` 版本将删除匹配。

## 示例

```
OS10(config)# route-map bgp
OS10(conf-route-map)# match ipv6 next-hop prefix-list test100
```

支持的版本 10.3.0E or later

## match metric

配置筛选器以匹配特定值。

**语法** `match metric metric-value`

**参数** *metric-value* — 输入与路由指标匹配的值，从 0 到 4294967295。

**默认** 未配置

**命令模式** ROUTE-MAP

**使用情况信息** 此命令的 `no` 版本将删除匹配。

## 示例

```
OS10(conf-route-map)# match metric 429132
```

支持的版本 10.2.0E or later

## match origin

配置筛选器以匹配基于 BGP 的源属性的路由。

|        |                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>match origin {egp   igp   incomplete}</code>                                                                                                                                      |
| 参数     | <ul style="list-style-type: none"><li>• <code>egp</code> — 仅与远程 EGP 路由匹配。</li><li>• <code>igp</code> — 仅在本本地 IGP 路由上匹配。</li><li>• <code>incomplete</code> — 与通过其他方式获知的未知路由匹配。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                     |
| 命令模式   | ROUTE-MAP                                                                                                                                                                               |
| 使用情况信息 | 此命令的 <code>no</code> 版本将删除匹配。                                                                                                                                                           |
| 示例     | <pre>OS10(config)# route-map bgp OS10(conf-route-map)# match origin egp</pre>                                                                                                           |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                        |

## match route-type

根据定义路由的方式配置筛选器以匹配路由。

|        |                                                                                                                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>match route-type {{external {type-1   type-2}   internal   local }}</code>                                                                                                                                                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"><li>• <code>external</code> — 仅在外部 OSPF 路由上匹配。输入关键字，然后输入以下内容之一：<ul style="list-style-type: none"><li>◦ <code>type-1</code> — 仅在 OSPF 类型 1 路由上匹配。</li><li>◦ <code>type-2</code> — 仅在 OSPF 类型 2 路由上匹配。</li></ul></li><li>• <code>internal</code> — 仅匹配 OSPF 区域内生成的路由。</li><li>• <code>local</code> — 仅在本本地生成的路由上匹配。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                           |
| 命令模式   | ROUTE-MAP                                                                                                                                                                                                                                                                                                                                                     |
| 使用情况信息 | 此命令的 <code>no</code> 版本将删除匹配。                                                                                                                                                                                                                                                                                                                                 |
| 示例     | <pre>OS10(config)# route-map bgp OS10(conf-route-map)# match route-type external type-1</pre>                                                                                                                                                                                                                                                                 |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                              |

## match tag

配置筛选器以仅重新发布与特定标记值匹配的路由。

|        |                                                          |
|--------|----------------------------------------------------------|
| 语法     | <code>match tag tag-value</code>                         |
| 参数     | <code>tag-value</code> — 输入与标签编号匹配的标签值，从 0 到 4294967295。 |
| 默认     | 未配置                                                      |
| 命令模式   | ROUTE-MAP                                                |
| 使用情况信息 | 此命令的 <code>no</code> 版本将删除匹配。                            |
| 示例     | <pre>OS10(conf-route-map)# match tag 656442</pre>        |
| 支持的版本  | 10.2.0E or later                                         |

## route-map

启用路由映射语句并配置其操作和序列号。

|        |                                                                                                                                                                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>route-map map-name [permit   deny   sequence-number]</code>                                                                                                                                                                                                                      |
| 参数     | <ul style="list-style-type: none"><li><code>map-name</code> — 输入路由映射的名称。最多 140 个字符。</li><li><code>sequence-number</code> — (可选) 输入数字, 以标识用于编辑的路由映射和顺序编号, 从 1 到 65535。默认值为 10。</li><li><code>permit</code> — (可选) 将路由映射默认值设置为允许。</li><li><code>deny</code> — (可选) 将路由默认设置为拒绝。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                    |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                          |
| 使用情况信息 |  <b>注:</b> 删除路由映射时要格外小心 — 如果不输入序列号, 则将删除所有具有相同映射名称的路由映射。<br>此命令的 <code>no</code> 版本将移除路由映射。                                                                                                           |
| 示例     | <pre>OS10(config)# route-map route1 permit 100 OS10(config-route-map)#</pre>                                                                                                                                                                                                           |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                       |

## set comm-list add

从匹配的入站或出站 BGP 路由中将列表中的社区添加到 COMMUNITY 属性。

|        |                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>set comm-list {community-list-name} add</code>                                                                                         |
| 参数     | <code>community-list-name</code> — 输入已建立社区列表的名称。最多 140 个字符。                                                                                  |
| 默认     | 无                                                                                                                                            |
| 命令模式   | ROUTE-MAP                                                                                                                                    |
| 使用情况信息 | 在路由映射中, 使用此 <code>set</code> 命令可将社区的列表 (将允许语句传递到从 BGP 对等节点发送或接收的 BGP 路由的 COMMUNITY 属性)。使用 <code>set comm-list delete</code> 命令从匹配的路由中删除社区列表。 |
| 示例     | <pre>OS10(config)# route-map bgp OS10(conf-route-map)# set comm-list comlist1 add</pre>                                                      |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                         |

## set comm-list delete

从匹配的入站或出站 BGP 路由中的 COMMUNITY 属性中删除指定列表中的社区。

|        |                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>set comm-list {community-list-name} delete</code>                                                                                                                                                                                                                                                                                                                               |
| 参数     | <code>community-list-name</code> — 输入已建立社区列表的名称。最多 140 个字符。                                                                                                                                                                                                                                                                                                                           |
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                                                     |
| 命令模式   | ROUTE-MAP                                                                                                                                                                                                                                                                                                                                                                             |
| 使用情况信息 | 配置在 <code>set comm-list delete</code> 命令中使用的社区列表, 以便每个筛选器仅包含一个社区。例如, 筛选器 <code>deny 100:12</code> 可接受, 但筛选器 <code>deny 120:13 140:33</code> 会导致错误。如果在同一路由图序列中配置 <code>set comm-list delete</code> 命令和 <code>set community</code> 命令, 则在插入 <code>set community</code> 命令之前处理删除 <code>set comm-list delete</code> 命令。要将社区列表中的社区添加到 BGP 路由中的社区属性, 请使用 <code>set comm-list add</code> 命令。 |

## 示例

```
OS10(config)# route-map bgp
OS10(conf-route-map)# set comm-list comlist1 delete
```

支持的版本 10.3.0E or later

## set community

设置 BGP 更新中的社区属性。

**语法** `set community {none | community-number}`

**参数**

- `none` — 输入以从符合路由映射条件的路由中移除社区属性。
- `community-number` — 以 `aa:nn` 格式输入社区编号，其中 `aa` 是 AS 编号，2 字节，`nn` 是特定于 AS 的值。

**默认** 未配置

**命令模式** ROUTE-MAP

**使用情况信息** 此命令的 `no` 版本 JIAGN 删除 BGP COMMUNITY 属性分配。

## 示例

```
OS10(config)# route-map bgp
OS10(conf-route-map)# set community none
```

支持的版本 10.3.0E or later

## set extcomm-list add

从匹配的入站或出站 BGP 路由中将指定列表中的社区添加到 EXTCOMMUNITY 属性。

**语法** `set extcomm-list extcommunity-list-name add`

**参数** `extcommunity-list-name` — 输入已建立的扩展社区列表的名称。最多 140 个字符。

**默认** 无

**命令模式** ROUTE-MAP

**使用情况信息** 在路由映射中，使用此 `set` 命令可将社区的扩展列表（将允许语句传递到从 BGP 对等节点发送或接收的 BGP 路由的 EXTCOMMUNITY 属性）。使用 `set extcomm-list delete` 命令从匹配的路由中删除扩展社区列表。

## 示例

```
OS10(config)# route-map bgp
OS10(conf-route-map)# set extcomm-list TestList add
```

支持的版本 10.4.0E(R1) or later

## set extcomm-list delete

从匹配的入站或出站 BGP 路由中的 EXTCOMMUNITY 属性中删除指定列表中的社区。

**语法** `set extcomm-list extcommunity-list-name delete`

**参数** `extcommunity-list-name` — 输入已建立的扩展社区列表的名称。最多 140 个字符。

**默认** 无

**命令模式** ROUTE-MAP

**使用情况信息** 要将 `extcommunity` 列表中的社区添加到 BGP 路由中的 EXTCOMMUNITY 属性，请使用 `set extcomm-list add` 命令。

## 示例

```
OS10(config)# route-map bgp
OS10(conf-route-map)# set extcomm-list TestList delete
```

支持的版本 10.3.0E or later

## set extcommunity

为 BGP 更新设置路由映射中的扩展社区属性。

**语法** `set extcommunity rt {asn2:nn | asn4:nnnn | ip-addr:nn}`

**参数**

- `asn2:nn` — 以 2 字节为格式输入数字；例如，1-65535:1-4294967295。
- `asn4:nnnn` — 以 4 字节格式输入数字；例如，1-4294967295:1-65535 或 1-65535:1-65535。
- `ip-addr:nn` — 以点分隔格式输入，从 1 到 65535。

**默认** 未配置

**命令模式** ROUTE-MAP

**使用情况信息** 此命令的 `no` 版本将从路由映射中删除 `set` 子句。

## 示例

```
OS10(config)# route-map bgp
OS10(conf-route-map)# set extcommunity rt 10.10.10.2:325
```

支持的版本 10.3.0E or later

## set local-preference

设置 AS 路径的首选项值。

**语法** `set local-preference value`

**参数** `value` — 输入数字作为 LOCAL\_PREF 属性值，从 0 到 4294967295。

**默认** 未配置

**命令模式** ROUTE-MAP

**使用情况信息** 此命令将更改用于满足路由映射条件的路由的 LOCAL\_PREF 属性。要更改所有路由的 LOCAL\_PREF，请使用 `bgp default local-preference` 命令。此命令的 `no` 版本将移除 LOCAL\_PREF 属性。

## 示例

```
OS10(conf-route-map)# set local-preference 200
```

支持的版本 10.2.0E or later

## set metric

设置路由协议的指标值。

**语法** `set metric [+ | -] metric-value`

**参数**

- `+` — (可选) 将指标值添加到重新分发的路由。
- `-` — (可选) 从重新分发的路由中减去指标值。
- `metric-value` — 输入新的指标值，从 0 到 4294967295。

**默认** 未配置

**命令模式** ROUTE-MAP

|               |                                                                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>使用情况信息</b> | 要建立绝对指标，请勿在指标值之前输入加号或减号。要建立相对指标，请在度量值之前输入一个加号或减号。该值将添加到与路由映射匹配的任何路由的指标。您不能在同一路由映射序列中同时使用绝对指标和相对指标。设置任一指标都会覆盖先前配置的任何值。此命令的 <code>no</code> 版本将移除筛选器。 |
| <b>示例（绝对）</b> | <pre>OS10(conf-route-map)# set metric 10</pre>                                                                                                      |
| <b>示例（相对）</b> | <pre>OS10(conf-route-map)# set metric -25</pre>                                                                                                     |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                                    |

## set metric-type

为重新分发的 `route` 设置指标类型。

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>set metric-type {type-1   type-2   external}</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>type-1</code> — 将路由添加到现有社区。</li> <li><code>type-2</code> — 在本地 AS 发送路由。</li> <li><code>external</code> — 禁止向对等节点通告。</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>命令模式</b>   | ROUTE-MAP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>使用情况信息</b> | <ul style="list-style-type: none"> <li><b>BGP</b> <p>仅影响出站路由映射中的 BGP 行为，并且对其他类型的路由映射不起作用。如果路由映射同时包含 <code>set metric-type</code> 和 <code>set metric</code> 子句，则该 <code>set metric</code> 子句优先。如果您在 BGP 出站路由映射中输入 <code>internal</code> 指标类型，则 BGP 会将通告路由的 MED 设置为通告路由下一跳的 IGP 成本。如果下一跳的成本发生变化，则不强制 BGP 重新通告该路由。</p> <ul style="list-style-type: none"> <li><code>external</code> — 恢复为用于传播 MED 的正常 BGP 规则（默认值）。</li> <li><code>internal</code> — 设置要传播到外部对等节点的已接收路由的 MED，使其等于间接下一跳的 IGP 成本。</li> </ul> </li> <li><b>OSPF</b> <ul style="list-style-type: none"> <li><code>external</code> — 设置外部路由的成本，使其等于所有内部成本和外部成本的总和。</li> <li><code>internal</code> — 设置外部路由的成本，使其等于外部成本（默认值）。</li> </ul> </li> </ul> <p>此命令的 <code>no</code> 版本将从路由映射中移除 <code>set</code> 子句。</p> |
| <b>示例</b>     | <pre>OS10(conf-route-map)# set metric-type internal</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## set next-hop

将 IPv4 或 IPv6 地址设置为下一跳。

|               |                                                                                                                                                                                                                                                                                                                     |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>set {ip   ipv6} next-hop ip-address</code>                                                                                                                                                                                                                                                                    |
| <b>参数</b>     | <code>ip-address</code> — 输入下一跳的 IPv4 或 IPv6 地址。                                                                                                                                                                                                                                                                    |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                                 |
| <b>命令模式</b>   | ROUTE-MAP                                                                                                                                                                                                                                                                                                           |
| <b>使用情况信息</b> | <p>如果在 ROUTER-BGP 模式下使用 <code>set next-hop</code> 命令应用路由映射，则它优先于在 ROUTER-NEIGHBOR 模式下使用的 <code>next-hop-self</code> 命令。在路由映射配置中，要配置多个下一跳条目，请使用多个 <code>set {ip   ipv6} next-hop</code> 命令。当您在 ROUTER-BGP 模式下应用路由映射以进行重新分发或路由更新时，仅配置一个下一跳。仅在用于其他功能的路由映射（如基于策略的路由 [PBR]）中配置多个下一跳条目。此命令的 <code>no</code> 版本将删除该设置。</p> |

|                  |                                                                 |
|------------------|-----------------------------------------------------------------|
| <b>示例</b>        | <pre>OS10(conf-route-map)# set ip next-hop 10.10.10.2</pre>     |
| <b>示例 (IPv6)</b> | <pre>OS10(conf-route-map)# set ipv6 next-hop 11AA:22CC::9</pre> |
| <b>支持的版本</b>     | 10.2.0E or later                                                |

## set origin

设置通告路由的来源。

|               |                                                                                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>set origin {egp   igp   incomplete}</code>                                                                                                                              |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>egp</code> — 输入以添加到现有社区。</li> <li><code>igp</code> — 输入以在本地 AS 进行发送。</li> <li><code>incomplete</code> — 输入以便不通告给对等节点。</li> </ul> |
| <b>默认</b>     | 未配置                                                                                                                                                                           |
| <b>命令模式</b>   | ROUTE-MAP                                                                                                                                                                     |
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本将从路由映射中删除 <code>set</code> 子句。                                                                                                                         |
| <b>示例</b>     | <pre>OS10(conf-route-map)# set origin egp</pre>                                                                                                                               |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                                                              |

## set tag

为重新分配的路由设置一个标签。

|               |                                                             |
|---------------|-------------------------------------------------------------|
| <b>语法</b>     | <code>set tag tag-value</code>                              |
| <b>参数</b>     | <code>tag-value</code> — 为要重新分配的路由输入一个标签号，从 0 到 4294967295。 |
| <b>默认</b>     | 未配置                                                         |
| <b>命令模式</b>   | CONFIGURATION                                               |
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本将从路由映射中删除 <code>set</code> 子句。       |
| <b>示例</b>     | <pre>OS10(conf-route-map)# set tag 23</pre>                 |
| <b>支持的版本</b>  | 10.2.0E or later                                            |

## set weight

为路由表设置 BGP 权重。

|               |                                                           |
|---------------|-----------------------------------------------------------|
| <b>语法</b>     | <code>set weight weight</code>                            |
| <b>参数</b>     | <code>weight</code> — 输入编号作为权重，由路由用来满足路由映射规格，从 0 到 65535。 |
| <b>默认</b>     | 默认路由器起源为 32768 — 所有其他路由为 0。                               |
| <b>命令模式</b>   | ROUTE-MAP                                                 |
| <b>使用情况信息</b> | 命令的 <code>no</code> 版本从路由映射中删除 <code>set</code> 子句。       |
| <b>示例</b>     | <pre>OS10(conf-route-map)# set weight 200</pre>           |
| <b>支持的版本</b>  | 10.2.0E or later                                          |

## show route-map

显示当前的路由映射配置。

|               |                                                  |
|---------------|--------------------------------------------------|
| <b>语法</b>     | <code>show route-map [map-name]</code>           |
| <b>参数</b>     | <i>map-name</i> — (可选) 指定已配置的路由映射的名称。最多 140 个字符。 |
| <b>默认</b>     | 无                                                |
| <b>命令模式</b>   | EXEC                                             |
| <b>使用情况信息</b> | 无                                                |
| <b>示例</b>     |                                                  |

```
OS10# show route-map
route-map abc, permit, sequence 10
 Match clauses:
 ip address (access-lists): hello
 as-path abc
 community hello
 metric 2
 origin egp
 route-type external type-1
 tag 10
 Set clauses:
 metric-type type-1
 origin igp
 tag 100
```

|              |                  |
|--------------|------------------|
| <b>支持的版本</b> | 10.3.0E or later |
|--------------|------------------|



## 服务质量

服务质量 (QoS) 会通过优先级高于关键应用程序流量来保留高度关键应用程序流量的网络资源。QoS 划分不同类型的流量，并确保服务质量。

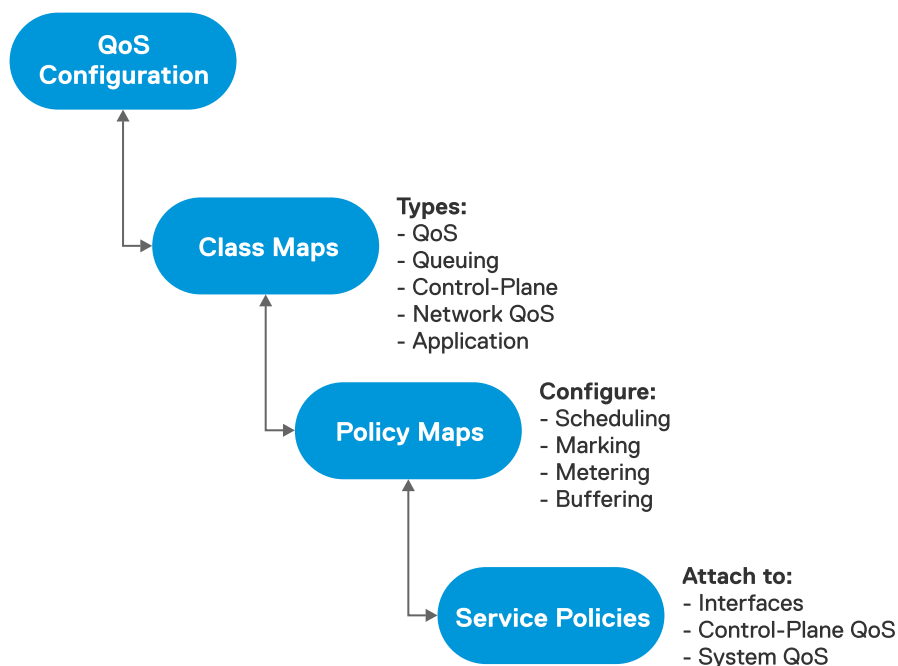
您可以控制以下流量流参数：延迟、带宽、抖动和丢弃。

不同的 QoS 功能可控制流量流的参数，因为流量会将网络设备从入口传输到出口接口。



## 配置服务质量

基于适用于流量的分类和策略的网络流量进程。



配置 QoS 流程包含三个步骤：

1. 创建类别映射以分类流量流。下面是不同类型的类别映射：

- qos（默认值）— 对入口数据流量进行分类。
- 排队 — 对出口队列进行分类。
- 控制平面 — 对控制平面流量进行分类。
- 网络 qos — 将流量类别 ID 归类为入口缓冲区配置。
- 应用程序 — 对应用程序类型流量进行分类。保留的策略映射 **policy-iscsi** 定义了 **class-iscsi** 流量的操作。

2. 创建策略映射以定义分类的流量流的策略。以下是不同类型的策略映射：

- Qos（默认值）— 对基于 **qos** 类别映射分类的对流量定义进行以下操作：
  - 监察
  - 使用流量类别 ID 进行标记
  - 修改 CoS 和 DSCP 等数据包字段
- 排队 — 对基于 **queuing** 类别映射分类的出口队列定义以下操作：
  - 塑形
  - 为队列分配带宽
  - 为队列分配严格优先级
  - 为队列配置缓冲
  - 队列上的加权随机早期检测 (WRED)/显式拥塞通知 (ECN) 配置
- 控制平面 — 定义控制队列的监察，以对 CPU 队列上的 **control-plane** 流量进行速率限制。
- 网络 qos — 基于 **network-qos** 类别映射为匹配的所选流量类别定义入口缓冲区配置。
- 应用程序 — 定义 **application** 分类流量的以下操作：
  - 修改 CoS 和 DSCP 等数据包字段。
  - 标记流量类别 ID。

3. 将策略映射应用到端口接口、所有接口的系统或控制平面流量，如下所示：

- 在控制平面模式下应用控制平面策略。
- 在物理接口的输入方向或系统 QoS 模式下应用 QoS 和网络 QoS 策略。
- 在物理接口的输出方向或系统 QoS 模式下应用队列策略。
- 在系统 QoS 模式下应用应用程序类型策略映射。

当您在系统级别（系统 QoS 模式）应用策略时，该策略在系统中的所有端口上有效。但是，接口级别策略优先于系统级别策略。

# 入口流量类别

入口流量可以是数据，也可以是控制流量。

OS10 根据各种参数将网络流量分组到不同的流量类别中，从类别 0 到 7。将流量分组到不同的类别可在通过交换机进行通信时帮助标识流量并确定其优先级。

 **注：**流量类别也称 QoS。

默认情况下，OS10 不会对数据流量进行分类。OS10 将默认流量类别 ID 0 分配给所有数据流量。

OS10 隐式地对所有控制流量（例如 STP、OSPF、ICMP 等）进行分类，然后将流量转发到控制平面应用程序。有关详细信息，请参阅[控制平面监察](#)。

## 数据流量类别

您可以根据 ACL 或信任对数据流量进行分类。

基于 ACL 的分类占用大量的网络处理器资源。基于信任的分类通过预定义的方式分类流量，而无需使用网络处理器资源。

## 基于信任的类别

OS10 支持基于 802.1p CoS 字段 (L2) 或 DSCP 字段 (L3) 的分类。

### 802.1p CoS 信任映射：

信任 802.1p CoS 字段，以使用流量类 ID 以及 CoS 流的颜色进行标记。加权随机检测 (WRED) 使用颜色来定义出口流量的丢弃概率和阈值。请参阅[颜色流量](#)了解更多信息。默认情况下，802.1p 优先级级别 0 分配有流量类别 (TC) ID 1，而 802.1p 优先级 1 分配有 TC 0。其余的 802.1p 优先级级别（2 到 7）将分配相应的 TC ID。

**表. 83: 默认的 802.1p CoS 信任映射**

| CoS | 流量类别 ID | Color (颜色) |
|-----|---------|------------|
| 0   | 1       | G          |
| 1   | 0       | G          |
| 2   | 2       | G          |
| 3   | 3       | G          |
| 4   | 4       | G          |
| 5   | 5       | G          |
| 6   | 6       | G          |
| 7   | 7       | G          |

 **注：**您不能修改默认 CoS 信任映射。

### 用户定义的 802.1p CoS 信任映射

您可以通过创建 dot1p 信任映射来覆盖默认映射。所有未指定的 dot1p 条目均映射到默认流量类别 ID 0。

#### 配置用户定义的 802.1p CoS 信任映射

1. 创建 dot1p 信任映射。

```
OS10(config)# trust dot1p-map example-dot1p-trustmap-name
OS10(config-tmap-dot1p-map)#
```

2. 定义映射到流量类别 (qos 组 ID) 的 dot1p 值集。

```
OS10(config-tmap-dot1p-map)# qos-group 3 dot1p 0-4
OS10(config-tmap-dot1p-map)# qos-group 5 dot1p 5-7
```

3. 验证映射条目。

```
OS10# show qos maps type trust-map-dot1p example-dot1p-trustmap-name

DOT1P Priority to Traffic-Class Map : example-dot1p-trustmap-name
Traffic-Class DOT1P Priority

3 0-4
5 5-7
```

4. 在特定接口或系统 qos 全局级别上应用映射。

- 接口级别

```
OS10(conf-if-eth1/1/1)# trust-map dot1p example-dot1p-trustmap-name
```

**注:** 在接口级别中, 命令的 no 版本会将配置返回到系统-qos 级别。如果在系统-qos 级别没有可用的配置, 则配置将恢复为默认映射。

- 系统-qos 级别

```
OS10(config-sys-qos)# trust-map dot1p example-dot1p-trustmap-name
```

应用 CoS 信任映射

创建信任映射后, 必须在接口或系统-qos 级别应用信任映射。要在特定接口或系统-qos (全局) 级别应用信任映射, 请执行以下操作:

- 接口级别

```
OS10(conf-if-eth1/1/1)# trust-map dot1p example-dot1p-trustmap-name
```

**注:** 在接口级别中, 命令的 no 版本会将配置返回到系统 qos 级别。如果在系统-qos 级别没有可用的配置, 则配置将恢复为默认映射。

- 系统-qos 级别

```
OS10(config-sys-qos)# trust-map dot1p example-dot1p-trustmap-name
```

DSCP 信任映射:

在策略映射中为 DSCP 流分配预定义和保留的信任分类。加权随机检测 (WRED) 使用分配给特定流量的颜色来确定丢弃概率和阈值。

表. 84: 默认的 DSCP 信任映射

| DSCP 值 | 流量类别 ID | Color (颜色) |
|--------|---------|------------|
| 0-3    | 0       | G          |
| 4-7    | 0       | Y          |
| 8-11   | 1       | G          |
| 12-15  | 1       | Y          |
| 16-19  | 2       | G          |
| 20-23  | 2       | Y          |
| 24-27  | 3       | G          |
| 28-31  | 3       | Y          |
| 32-35  | 4       | G          |
| 36-39  | 4       | Y          |

表. 84: 默认的 DSCP 信任映射 (续)

| DSCP 值 | 流量类别 ID | Color (颜色) |
|--------|---------|------------|
| 40-43  | 5       | G          |
| 44-47  | 5       | Y          |
| 48-51  | 6       | G          |
| 52-55  | 6       | Y          |
| 56-59  | 7       | G          |
| 60-62  | 7       | Y          |
| 63     | 7       | R          |

 注: 您不能修改默认的 DSCP 信任映射。

用户定义的 DCSP 信任映射

您可以通过创建用户定义的 DSCP 信任映射来覆盖默认映射。所有未指定的 DSCP 条目均映射到默认流量类别 ID 0 和颜色 G。

配置用户定义的 DSCP 信任映射

- 1. 创建 DSCP 信任映射。

```
OS10(config)# trust dscp-map example-dscp-trustmap-name
OS10(config-tmap-dscp-map)#
```

- 2. 定义映射到流量类别 (qos 组 ID) 的 dscp 值集。

```
OS10(config-tmap-dscp-map)# qos-group 3 dscp 0-15
OS10(config-tmap-dscp-map)# qos-group 5 dscp 16-30
```

- 3. 验证映射条目。

```
OS10# show qos maps type trust-map-dscp example-dscp-trustmap-name

DSCP Priority to Traffic-Class Map : example-dscp-trustmap-name
Traffic-Class DSCP Priority

3 0-15
5 16-30
```

- 4. 在特定接口或系统-qos 全局级别上应用映射。

- 接口级别

```
OS10(conf-if-eth1/1/1)# trust-map dscp example-dscp-trustmap-name
```

- 系统-qos 级别

```
OS10(config-sys-qos)# trust-map dscp example-dscp-trustmap-name
```

应用 DSCP 信任映射

您必须在接口或系统-qos 级别应用信任映射。要在特定接口或系统-qos (全局) 级别应用信任映射, 请执行以下操作:

- 接口级别

```
OS10(conf-if-eth1/1/1)# trust-map dscp example-dscp-trustmap-name
```

- 系统-qos 级别

```
OS10(config-sys-qos)# trust-map dscp example-dscp-trustmap-name
```

## 基于 ACL 的分类

通过使用 ACL 条目匹配数据包字段来划分入口流量。

使用 IP 或 MAC ACL 以根据特定于 QoS 的字段或通用字段对流量流进行分类。创建类别映射模板以匹配字段。

OS10 允许根据在类别映射中配置的匹配类型来匹配 *any* 字段或 *all*。

使用访问组匹配筛选器以匹配 MAC 或 IP ACL。在类别映射中最多可以配置四个访问组筛选器：

- 802.1p CoS
- VLAN ID (802.1Q)
- DSCP + ECN
- IP 优先级

OS10 支持配置匹配筛选器的范围或逗号分隔值（VLAN ID 除外）。当您应用与新值相同的匹配筛选器时，系统将使用新值覆盖之前的值。

### 配置基于 ACL 的分类

1. 创建 *qos* 类型的类别映射。

```
OS10(config)# class-map type qos example-cmap-cos
```

2. 定义要匹配的字段：

```
OS10(config-cmap-qos)# match cos 3
```

3. 创建 *qos* 类型的策略-映射以引用类别。

```
OS10(config)# policy-map type qos example-pmap-cos
```

4. 请参阅策略映射中的类别映射，并定义流的所需操作。

```
OS10# configure terminal
OS10(config)# class-map type qos example-cmap-cos
OS10(config-cmap-qos)# match cos 3
OS10(config-cmap-qos)# exit
OS10(config)# policy-map type qos example-pmap-cos
OS10(config-pmap-qos)# class example-cmap-cos
OS10(config-pmap-c-qos)# set qos-group 3
```

5. 将 *qos* 类型策略-映射全局应用或应用到接口。在此示例中，策略-映射将应用到接口。

```
OS10# configure terminal
OS10(config)# interface ethernet 1/1/14
OS10(conf-if-eth1/1/14)# service-policy input type qos example-pmap-cos
```

如果到达接口的流量与您已配置的 802.1p 条件匹配，则会将其分配给 TC 3 或 *qos* 组 3。

## 基于 ACL 的分类和信任

本部分介绍如何在配置基于信任的分类时配置基于 ACL 的分类。

如果在特定端口上针对一组 DSCP/COS 值和基于信任的分类配置基于 ACL 的分类，基于 ACL 的分类优先于基于信任的分类。

1. 创建用户定义的 *dscp* 或 *dot1p* 信任映射。

```
OS10(config)# trust dscp-map userdef-dscp
OS10(config-tmap-dscp-map)# qos-group 3 dscp 15
OS10(config-tmap-dscp-map)# qos-group 5 dscp 30
```

2. 将用户定义的信任映射应用到接口或系统 QoS。

```
OS10(conf-if-eth1/1/1)# trust-map dscp userdef-dscp

or

OS10(config)# system qos
OS10(config-sys-qos)# trust-map dscp userdef-dscp
```

3. 创建类别映射并将其连接到已配置信任的策略。本示例使用 802.1p cos 来定义匹配条件。您可以使用 dscp 或其他访问组匹配筛选器。如果 802.1p 流量与定义的条件匹配，则 set qos-group 1 命令会将流量分配给 TC 1。

```
OS10(config)# class-map type qos example-class-map
OS10(config-cmap-qos)# match cos 1
OS10(config-cmap-qos)# exit

OS10(config)# policy-map type qos example-policy-map
OS10(config-pmap-qos)# class example-class-map
OS10(config-pmap-c-qos)# set qos-group 1
```

4. 将策略映射连接到接口或系统 QoS 模式。

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# service-policy input type qos example-policy-map

or

OS10(config)# system qos
OS10(config-sys-qos)# service-policy input type qos example-policy-map
```

在此示例中，DSCP 15 流映射到流量类别 3 或 qos 组 3，DSCP 30 流映射到 TC 5 或 qos 组 5。其余的 DSCP 流将根据配置的信任进行映射。

## 控制平面监察

控制平面监察 (CoPP) 通过保护路由处理器不必要的流量并为重要的控制平面和管理流量提供优先级，提高系统的安全性。CoPP 通过 QoS CLI 使用专用的控制平面配置来设置用于控制平面数据包的速率限制功能。

如果发往 CPU 的控制数据包的速率高于 CPU 可以处理的数据包的速率，CoPP 将提供一种方法来选择性地丢弃某些控制流量，以便 CPU 可以处理高优先级控制流量。您可以使用 CoPP 通过网络处理器 (NPU) 的每个 CPU 端口队列对流量进行速率限制。

CoPP 对所有控制平面流量应用策略操作。控制平面类别映射不使用任何匹配条件。要对控制平面流量强制实施速率限制或速率监察，请创建策略映射。您可以使用 control-plane 命令将 CoPP 服务策略直接连接到控制平面。

从版本 10.4.2 开始，默认的速率限制已从 12 个 CPU 队列进行更改，并且映射到每个 CPU 队列的协议会发生更改。

**注：** 当您从以前的版本升级到版本 10.4.2，并且在先前版本中配置了具有速率限制的 CoPP 策略，将根据队列的新 CoPP 映射重新映射 CoPP 策略。例如：

- 您在版本 10.4.1 中为队列 5 配置了 CoPP 策略，适用于 ARP 请求、ICMPv6-RS-NS、iSCSI 侦听和 iSCSI COS。
- 升级到版本 10.4.2 后，队列 5 的 CoPP 策略将根据新 CoPP 协议映射重新映射至队列，如下所示：
  - ARP 请求已映射到队列 6
  - ICMPv6-RS-NS 已映射到队列 5
  - iSCSI 已映射到队列 0

在升级之前，CoPP 策略中的速率限制配置会在升级后分别自动重新映射至队列 6、5 和 0。

例如，在版本 10.4.1 中，队列 5 上应用了以下策略配置（在 10.4.1 中映射到 ARP\_REQ、ICMPV6\_RS、ICMPV6\_NS 和 iSCSI 协议）：

```
policy-map type control-plane test
!
class test
 set qos-group 5
 police cir 300 pir 300
```

升级到版本 10.4.2 后，策略配置显示如下：

```
policy-map type control-plane test
!
class test_Remapped_0
 set qos-group 0
 police cir 300 pir 300
!
class test_Remapped_5
```

```

set qos-group 5
police cir 300 pir 300
!
class test_Remapped_6
set qos-group 6
police cir 300 pir 300

```

在版本 10.4.2 中，ARP\_REQ 映射到队列 6，ICMPV6\_RS 和 ICMPV6\_NS 映射到队列 5，并且 ISCSI 映射到队列 0。

默认情况下，发往 CPU 的 CoPP 流量归类为不同的队列，如下所示。

**表. 85: CoPP: 协议与队列之间的映射 — 低于版本 10.4.2**

| 队列 | 协议                                     |
|----|----------------------------------------|
| 0  | IPv6                                   |
| 1  | —                                      |
| 2  | IGMP                                   |
| 3  | VLT、NDS                                |
| 4  | ICMPv6、ICMPv4                          |
| 5  | ARP 请求、ICMPV6-RS-NS、ISCSI 侦听、ISCSI-COS |
| 6  | ICMPv6-RA-NA、SSH、TELNET、TACACS、NTP、FTP |
| 7  | RSTP、PVST、MSTP、LACP                    |
| 8  | Dot1X、LLDP、FCOE-FPORT                  |
| 9  | BGPv4、OSPFv6                           |
| 10 | DHCPv6、DHCPv4、VRRP                     |
| 11 | OSPF Hello、OpenFlow                    |

下表列出了 CoPP 协议与队列之间的映射，以及 S4148FE-ON 平台上的默认速率限制和缓冲区大小。控制平面队列的数量取决于硬件平台。

**表. 86: CoPP: 协议与队列之间的映射，以及默认速率限制和缓冲区大小 — 从版本 10.4.2 和更高版本**

| 队列 | 协议                  | 最小速率限制<br>(以 pps 为单<br>位) | 最大速率限制<br>(以 pps 为单<br>位) | 最小保证缓冲区<br>(以字节为单<br>位) | 静态共享限制<br>(以字节为单<br>位) |
|----|---------------------|---------------------------|---------------------------|-------------------------|------------------------|
| 0  | 未解析、iSCSI、IPv6      | 600                       | 600                       | 1664                    | 20800                  |
| 1  | SFlow               | 1000                      | 1000                      | 1664                    | 20800                  |
| 2  | IGMP、MLD、PIM 控制     | 400                       | 400                       | 1664                    | 48880                  |
| 3  | VLT、NDS             | 600                       | 1000                      | 1664                    | 48880                  |
| 4  | IPv6 ICMP、IPv4 ICMP | 500                       | 500                       | 1664                    | 20800                  |
| 5  | ICMPv6 RS、RA、NS、NA  | 500                       | 500                       | 1664                    | 48880                  |
| 6  | ARP 请求              | 500                       | 1000                      | 1664                    | 48880                  |
| 7  | ARP 响应              | 500                       | 1000                      | 1664                    | 48880                  |



表. 86: CoPP: 协议与队列之间的映射, 以及默认速率限制和缓冲区大小 — 从版本 10.4.2 和更高版本 (续)

| 队列 | 协议                            | 最小速率限制<br>(以 pps 为单<br>位) | 最大速率限制<br>(以 pps 为单<br>位) | 最小保证缓冲区<br>(以字节为单<br>位) | 静态共享限制<br>(以字节为单<br>位) |
|----|-------------------------------|---------------------------|---------------------------|-------------------------|------------------------|
| 8  | SSH、TELNET、NTP、<br>FTP、TACACS | 500                       | 500                       | 1664                    | 20800                  |
| 9  | FCoE                          | 600                       | 600                       | 1664                    | 48880                  |
| 10 | LACP                          | 600                       | 1000                      | 1664                    | 48880                  |
| 11 | STP、RSTP、MSTP                 | 400                       | 400                       | 1664                    | 48880                  |
| 12 | DOT1X、LLDP                    | 500                       | 500                       | 1664                    | 48880                  |
| 13 | IPv6 OSPF                     | 600                       | 1000                      | 1664                    | 48880                  |
| 14 | IPv4 OSPF                     | 600                       | 1000                      | 1664                    | 48880                  |
| 15 | BGP                           | 600                       | 1000                      | 1664                    | 48880                  |
| 16 | IPv4 DHCP、IPv6 DHCP           | 500                       | 500                       | 1664                    | 48880                  |
| 17 | VRRP                          | 600                       | 1000                      | 1664                    | 48880                  |
| 18 | BFD                           | 700                       | 700                       | 1664                    | 48880                  |
| 19 | 远程 CPS                        | 700                       | 1000                      | 1664                    | 48880                  |
| 20 | MCAST 数据                      | 300                       | 300                       | 1664                    | 20800                  |
| 21 | ACL 日志记录                      | 100                       | 100                       | 1664                    | 20800                  |
| 22 | MCAST 已知数据                    | 300                       | 300                       | 1664                    | 20800                  |

有关当前协议到队列映射的信息和每个队列配置的速率限制, 请参阅 [show control-plane info](#)。

## 配置控制平面监察

速率限制协议 CPU 队列需要配置控制平面类型 QoS 策略。

- 为所需的 CPU 绑定队列创建 QoS 策略、类别映射和策略映射。
- 将 QoS 策略与特定速率限制关联。
- 将 QoS 服务策略分配给控制平面队列。

默认情况下, 峰值信息率 (pir) 和已提交信息率 (cir) 值以控制平面的每秒数据包数 (pps) 为单位。CoPP for CPU 队列将输入速率从 kb/秒 (kbps) 转换为数据表/秒 (pps), 假设 64 字节是平均数据包大小, 并且将该速率应用到相应的队列 — 1 kbps 大致相当于 2 pps。

1. 在 CONFIGURATION 模式下创建 control-plane 类型类别映射并配置类别映射的名称。

```
class-map type control-plane example-copp-class-map-name
```

2. 返回 CONFIGURATION 模式。

```
exit
```

3. 在 CONFIGURATION 模式下创建输入策略映射以将 QoS 策略分配给所需的服务队列。

```
policy-map type control-plane example-copp-policy-map-name
```

- 在 POLICY-MAP 模式下将策略映射与类别映射关联。

```
class example-copp-class-map-name
```

- 在 POLICY-MAP-CLASS-MAP 模式下配置特定队列编号的标记。使用 `show control-plane info` 命令可查看控制平面队列的列表。

```
set qos-group queue-number
```

- 在 POLICY-MAP-CLASS-MAP 模式下配置传入流量的速率监察。

```
police {cir committed-rate | pir peak-rate}
```

- `cir committed-rate`— 以 pps 为单位输入承诺速率值，从 0 到 4000000。
- `pir peak rate` — 以 pps 为单位输入峰值速率值，从 0 到 4000000。

## 为 CoPP 创建 QoS 策略

```
OS10(config)# class-map type control-plane example-copp-class-map-name
OS10(config-cmap-control-plane)# exit
OS10(config)# policy-map type control-plane example-copp-policy-map-name
OS10(config-pmap-control-plane)# class example-copp-class-map-name
OS10(config-pmap-c)# set qos-group 2
OS10(config-pmap-c)# police cir 100 pir 100
```

## 查看策略-映射

```
OS10(config)# do show policy-map
Service-policy (control-plane) input: example-copp-policy-map-name
Class-map (control-plane): example-copp-class-map-name
 set qos-group 2
 police cir 100 bc 100 pir 100 be 100
```

## 分配服务策略

针对发往 CPU 的流量控制率需要配置 **control-plane** 类型策略。要启用 CoPP，请将定义的策略映射应用到控制平面模式。

- 从 CONFIGURATION 模式进入 CONTROL-PLANE 模式。

```
control-plane
```

- 在 CONTROL-PLANE 模式下，定义 input 类型服务策略并配置服务策略的名称。

```
service-policy input example-copp-policy-map-name
```

## 分配控制平面服务策略

```
OS10(config)# control-plane
OS10(conf-control-plane)# service-policy input example-copp-policy-map-name
```

## 查看控制平面服务策略

```
OS10(conf-control-plane)# do show qos control-plane
Service-policy (input): example-copp-policy-map-name
```

## 查看配置

使用 `show` 命令可显示分配给每个控制板队列的协议流量以及应用到每个队列的当前速率限制。使用 `show` 命令可输出验证 CoPP 配置。

## 查看 CoPP 配置

```
OS10# show qos control-plane
Service-policy (input): example-copp-policy-map-name
```

查看 CMAP1 配置

```
OS10# show class-map type control-plane example-copp-class-map-name
Class-map (control-plane): example-copp-class-map-name (match-any)
```

查看 CoPP 服务策略

```
OS10# show policy-map type control-plane
Service-policy(control-plane) input: example-copp-policy-map-name
Class-map (control-plane): example-copp-class-map-name
set qos-group 2
police cir 100 bc 100 pir 100 be 100
```

查看 CoPP 信息

```
OS10# show control-plane info
Queue Min Rate Limit(in pps) Max Rate Limit(in pps)
Protocols
0 600 600 ISCSI UNKNOWN UNICAST
1 1000 1000 SFLOW
2 400 400 IGMP MLD PIM
3 600 1000 VLT NDS
4 500 1000 IPV6_ICMP IPV4_ICMP
5 500 1000 ICMPV6_RS ICMPV6_NS ICMPV6_RA
ICMPV6_NA
6 500 1000 ARP_REQ SERVICEABILITY
7 500 1000 ARP_RESP
8 500 500 SSH TELNET TACACS NTP FTP
9 600 600 FCOE
10 600 1000 LACP
11 400 400 RSTP PVST MSTP
12 500 500 DOT1X LLDP
13 600 1000 IPV6_OSPF IPV4_OSPF
14 600 1000 OSPF_HELLO
15 600 1000 BGP
16 500 500 IPV6_DHCP IPV4_DHCP
17 600 1000 VRRP
18 700 700 BFD
19 700 1000 OPEN_FLOW REMOTE CPS
20 300 300 MCAST DATA
21 100 100 ACL LOGGING
22 300 300 MCAST KNOWN DATA
```

查看 CoPP 统计信息

```
OS10# show control-plane statistics
Queue Dropped Bytes Packets Bytes Dropped Packets
0 0 26 1768 0 0
1 0 0 0 0 0
2 0 0 0 0 0
3 0 0 0 0 0
4 0 36 3816 0 0
5 0 36 3096 0 0
6 0 919 58816 0 0
7 0 67 4288 0 0
8 0 0 0 0 0
9 0 0 0 0 0
10 0 0 0 0 0
11 0 80662 5539376 0 0
12 0 2779 462189 0 0
13 0 0 0 0 0
14 0 1265 108790 0 0
15 0 422 36075 0 0
16 0 0 0 0 0
17 0 0 0 0 0
18 0 0 0 0 0
19 0 0 0 0 0
```

# 出口流量类别

出口流量根据流量流上标记的流量类别 ID 分类到不同的队列中。

通过启用信任或对入口流量进行分类来设置流的流量类别 ID，并通过策略映射使用流量类别 ID 对其进行标记。默认情况下，所有流量的流量类别 ID 的值为 0。

Qos-映射的优先级顺序为：

- 1. 接口级别映射
- 2. 系统 qos 级别映射
- 3. 默认映射

表. 87: 流量类别 ID 至队列的默认映射

| 流量类别 ID | 队列 ID |
|---------|-------|
| 0       | 0     |
| 1       | 1     |
| 2       | 2     |
| 3       | 3     |
| 4       | 4     |
| 5       | 5     |
| 6       | 6     |
| 7       | 7     |

## 用户定义的 QoS 映射

您可以通过创建 QoS 映射来覆盖默认映射。

### 配置用户定义的 QoS 映射

- 1. 创建 QoS 映射。

```
OS10(config)# qos-map traffic-class tc-q-map
```

- 2. 定义映射到队列的流量类别值的集。

```
OS10(config-qos-map)# queue 3 qos-group 0-3
```

- 3. 验证映射条目。

```
OS10# show qos maps type tc-queue
Traffic-Class to Queue Map: tc-q-map
Queue Traffic-Class

3 0-3
```

- 4. 在特定接口或系统 QoS 的全局级别上应用映射。

- 接口级别

```
OS10(conf-if-eth1/1/1)# qos-map traffic-class tc-q-map
```

- 系统-qos 级别

```
OS10(config-sys-qos)# qos-map traffic-class tc-q-map
```

## 选择针对队列分类的所有流量

1. 创建队列类型类别映射以匹配队列 5。

```
OS10(config)# class-map type queuing q5
```

2. 定义要匹配的队列。

```
OS10(config-cmap-queuing)# match queue 5
```

## 监察流量

使用监察来限制入口流量流的速率。流可以是端口上的所有入口流量或使用 QoS 类别映射定义的特定流。

此外，还可以使用监察颜色来对流量进行着色：

- 当流量以小于承诺速率的速率到达时，颜色为绿色。
- 当流量以高于或等于承诺速率以及低于峰值速率的平均速率传播时，颜色为黄色。
- 当流量速率高于配置的峰值速率时，流量将丢弃，以保证进入流量流的带宽限制。

峰值速率是在正常流量条件下到达或离开接口的流量的最大速率。峰值脉冲大小表示聚合的未使用峰值带宽的最大大小。此聚合带宽可实现突发流量（超出峰值速率）的短暂持续时间。

接口速率监察可限制在接口上接收的流量的速率。

### 配置接口速率监察

1. 创建 QoS 类型空类别映射以匹配所有流量。

```
OS10(config)# class-map example-cmap-all-traffic
```

2. 创建 QoS 类型策略-映射以定义限速器。

```
OS10(config)# policy-map example-interface-policer
OS10(config-pmap-qos)# class example-cmap-all-traffic
OS10(config-pmap-c-qos)# police cir 4000 pir 6000
```

3. 将 QoS 类型策略映射应用到接口。

```
OS10(config)# interface ethernet 1/1/14
OS10(conf-if-eth1/1/14)# service-policy input type qos example-interface-policer
```

流速率监察可以控制流量流的速率。

### 配置流速率监察

1. 创建 QoS 类型的类别映射以匹配流量流。

```
OS10(config)# class-map example-cmap-cos3
OS10(config-cmap-qos)# match cos 3
```

2. 创建 QoS 类型策略映射以定义限速器，并（可选）为 CoS 流分配流量类别 ID，以将监察流量重定向到非默认队列。

```
OS10(config)# policy-map example-flow-policer
OS10(config-pmap-qos)# class example-cmap-cos3
OS10(config-pmap-c-qos)# set qos-group 3
OS10(config-pmap-c-qos)# police cir 4000 pir 6000
```

3. 将 QoS 类型策略映射应用到接口。

```
OS10(config)# interface ethernet 1/1/15
OS10(conf-if-eth1/1/15)# service-policy input type qos example-flow-policer
```

## 标记流量

您可以选择流并使用流量类别 ID 进行标记。流量类别 ID 用于标识流量到达队列计划的出口时的流量流。

### 标记流量

1. 创建 QoS 类型的类别映射以匹配流量流。

```
OS10(config)# class-map cmap-cos3
OS10(config-cmap-qos)# match cos 3
```

2. 创建 QoS 类型策略映射以将其标记为流量类别 ID，并将其分配给 CoS 流。

```
OS10(config)# policy-map cos3-TC3
OS10(config-pmap-qos)# class cmap-cos3
OS10(config-pmap-c-qos)# set qos-group 3
```

## 颜色流量

您可以选择流量流并使用颜色进行标记。根据以下内容对流量流进行着色：

- 测定。请参阅[监察流量](#)。
- 默认信任。请参阅[基于信任的分类](#)。
- DSCP、支持 ECN 的流量 (ECT) 或不支持 ECT 的流量。使用 `set color` 命令以根据 DSCP、支持 ECN 的功能或不支持 ECN 的功能的流量对流量进行着色。

使用 DSCP 值的流量监察和流量颜色相互排斥。您不能同时进行配置。使用 DSCP 值进行监察和标记优先于基于信任的类别。基于信任的类别具有最低优先级。

### 基于 DSCP、ECT 或非 ECT 的颜色流量

1. 创建 QoS 类型的类别映射以匹配流量流。

```
OS10(config)# class-map type qos example-cmap-dscp-3-ect
OS10(config-cmap-qos)# match ip dscp 3
```

2. 创建 QoS 类型策略-映射以对流量流进行着色。

```
OS10(config)# policy-map type qos example-pmap-ect-color
OS10(config-pmap-qos)# class example-cmap-dscp-3-ect
OS10(config-pmap-c-qos)# set qos-group 3
OS10(config-pmap-c-qos)# set color yellow
```

## 修改数据包字段

您可以修改 CoS 或 DSCP 字段的值。

1. 创建 QoS 类型类别映射，以匹配流量流。

```
OS10(config)# class-map cmap-dscp-3
OS10(config-cmap-qos)# match ip dscp 3
```

2. 修改策略-映射以更新 DSCP 字段。

```
OS10(config)# policy-map modify-dscp
OS10(config-pmap-qos)# class cmap-dscp-3
OS10(config-pmap-c-qos)# set qos-group 3
OS10(config-pmap-c-qos)# set dscp 10
```

## 整形流量

您可以整形出口流量的速率。启用速率整形后，系统会将超出指定速率的所有流量都进行缓冲，直至缓冲区内存耗尽。速率整形使用为某个接口或队列保留的所有缓冲区并共享缓冲区内存，直至达到配置的阈值。

### 配置流量整形

1. 在 CONFIGURATION 模式下输入 `queuing` 类型策略-映射并配置策略映射名称。

```
policy-map type queuing policy-map-name
```

2. 在 POLICY-MAP-QUEUEING 模式下输入要应用于速率整形的类别名称。最多 32 个字符。

```
class class-name
```

3. (可选) 通过匹配类别映射中相应的 qos 组, 在特定队列上配置速率整形。如果未配置该 match qos-group 命令, 则速率整形将应用于所有队列。

```
match qos-group queue-number
```

4. 在 POLICY-MAP-QUEUEING-CLASS 模式下, 输入最小和最大速率整形值。

```
shape {min {kbps | mbps | pps}min-value} {max {kbps | mbps | pps}max-value}
```

- 0 至 400000000 — Kb/秒 — kbps
- 0 至 40000 — Mb/秒 — mbps
- 1 至 268000000 — 每秒数据包数 (pps)

## 带宽分配

您可以分配相对带宽来限制大型流, 并划分较小流的优先级。当优先级队列消耗最大链路带宽时, 相对的带宽量将分配给非优先队列。

加权赤字轮循 (WDRR) 是一种计划方法, 它使用赤字计数器为流量流分配带宽。

按加权赤字循环 (WDRR) 或严格优先级 (SP) 为某个接口安排相互排斥的各个出口队列。如果存在 bandwidth percent 命令, 则无法配置 priority 命令。

1. 在 CONFIGURATION 模式下创建 queuing 类型类别映射并配置类别映射的名称。

```
class-map type queuing example-que-cmap-name
```

2. 在 CLASS-MAP 模式下为队列应用匹配条件。

```
match queue queue-number
```

3. 返回 CONFIGURATION 模式。

```
exit
```

4. 在 CONFIGURATION 模式下创建 queuing 类型策略-映射并配置策略映射名称。

```
policy-map type queuing example-que-pmap-name
```

5. 在 POLICY-MAP 模式下配置队列类别。

```
class example-que-cmap-name
```

6. 在 POLICY-MAP-CLASS-MAP 模式下, 为非优先队列分配带宽百分比, 从 1 到 100。

```
bandwidth percent value
```

### 配置带宽分配

```
OS10(config)# class-map type queuing example-que-cmap-name
OS10(config-cmap-queuing)# match queue 5
OS10(config-cmap-queuing)# exit
OS10(config)# policy-map type queuing example-que-pmap-name
OS10(config-pmap-queuing)# class example-que-cmap-name
OS10(config-pmap-c-que)# bandwidth percent 80
```

### 查看类别映射

```
OS10(conf-cmap-queuing)# do show class-map
Class-map (queuing): example-que-cmap-name
Match: queue 5
```

## 查看策略-映射

```
OS10(config-pmap-c-que)# do show policy-map
Service-policy (queuing) output: example-que-pmap-name
Class-map (queuing): example-que-cmap-name
bandwidth percent 80
```

# 严格优先级队列

OS10 将队列用于出口 QoS 策略类型。在处理任何其他队列之前，启用严格优先级以使来自分配队列的所有数据包出列。分配多个队列严格优先级时，最高编号队列将获得最高优先级。您可以为任意数量的队列配置严格优先级。默认情况下，所有队列都会计划每个 WDRR 流量。

使用 `priority` 命令将优先级分配给单个单播队列 — 此配置将取代 `bandwidth percent` 配置。已启用优先级的队列可以挤掉相同出口接口的其他队列。

## 创建类别映射

1. 在 CONFIGURATION 模式下创建类别映射并配置类别映射的名称。

```
class-map type queuing class-map-name
```

2. 在 CLASS-MAP 模式下配置匹配条件。

```
match queue queue-id
```

## 定义策略映射

1. 定义策略映射并创建策略映射名称 CONFIGURATION 模式。

```
policy-map type queuing policy-map-name
```

2. 在 POLICY-MAP 模式下创建队列类并为策略映射配置名称。

```
class class-map-name
```

3. 在 POLICY-MAP-CLASS-MAP 模式下将计划程序设置为严格优先级。

```
priority
```

## 应用策略映射

1. 将策略映射应用到 INTERFACE 模式下的接口或 SYSTEM-QOS 模式下的所有接口。

```
system qos
```

或

```
interface ethernet node/slot/port[:subport]
```

2. 在 SYSTEM-QOS 模式或 INTERFACE 模式下输入输出服务策略。

```
service-policy {output} type {queuing} policy-map-name
```

## 在类别映射上启用严格优先级，并全局应用策略映射

```
OS10(config)# class-map type queuing example-cmap-strictpriority
OS10(config-cmap-queuing)# match queue 7
OS10(config-cmap-queuing)# exit
OS10(config)# policy-map type queuing example-pmap-strictpriority
OS10(config-pmap-queuing)# class example-cmap-strictpriority
OS10(config-pmap-c-que)# priority
OS10(config-pmap-c-que)# exit
OS10(config-pmap-queuing)# exit
OS10(config)# system qos
OS10(config-sys-qos)# service-policy output type queuing example-pmap-strictpriority
```

## 在接口上启用严格优先级



**注：**您可以在 SYSTEM-QOS 模式下全局应用策略映射，也可将其应用到接口上。OS10 不支持在 SYSTEM-QOS 模式下和接口级别应用相同的策略映射。

但是，您可以在 SYSTEM-QOS 模式或接口级别应用不同的队列策略映射。在这种情况下，在接口上应用的策略映射优先于全局应用的策略映射。

```
OS10(config)# interface ethernet 1/1/5
OS10(conf-if-eth1/1/5)# service-policy output type queuing example-pmap-strictpriority
```

### 查看策略-映射

```
OS10(conf-if-eth1/1/5)# do show policy-map
Service-policy(queuing) output: example-pmap-strictpriority
Class-map (queuing): example-cmap-strictpriority
priority
```

## 速率调整

监察和塑形等 QoS 功能不包括额外开支字段，例如引言、智能帧分隔符 (SFD)、框架间间隙 (IFG) 等。对于速率计算，这些功能仅包括目标 MAC 地址 (DMAC) 和 CRC 字段之间的帧长度。

通过启用速率调整，可以选择在速率计算中包含以下额外开支字段：

- 引言 — 7 个字节
- 开始帧分隔符 — 1 个字节
- 目标 MAC 地址 — 6 个字节
- 源 MAC 地址 — 6 个字节
- 以太网类型/长度 — 2 个字节
- 有效负载 — 变量
- 循环冗余检查 — 4 个字节
- 框架间间隙 — 变量

默认情况下，速率调整功能处于禁用状态。要启用速率调整，请使用 `qos-rate-adjust value_of_rate_adjust` 命令。例如：

```
qos-rate-adjust 8
```

如果您已在特定队列上配置 WDRR 并进行塑形，队列可能会变得拥塞。您应在配置 QoS 速率调整值时考虑额外开支字段大小，以避免非拥塞队列上的流量丢弃。

如果队列中有多个流，则必须找到不同流的额外开支大小，并且 QoS 速率调整值应为该队列内各种流中的最大额外开支大小。

请考虑在具有两个不同流量流 (TS1 和 TS2) 的队列上配置 WDRR 和塑形的示例，其中使用引言、SFD 和 IFG 额外开支字段：

- 如果 TS1 中的 IFG 使用 16 个字节，则 QoS 速率调整值应为 24 (引言 + SFD 需要 8 个字节，IFG 为 16 个字节)。
- 如果 TS2 中的 IFG 使用 12 个字节，则 QoS 速率调整值应为 20 (引言 + SFD 需要 8 个字节，IFG 为 12 个字节)。

在这种情况下，两个数据流的最高 QoS 速率调整值为 24 个字节。因此，您必须将 QoS 速率调整值配置为 24。

**注：**S4200-ON 系列平台上不支持此功能。

## 缓冲区管理

OS10 设备将总可用缓冲区资源分布到两个缓冲池中，并以入口方向和三个缓冲池为所有物理端口的出口方向。

您可以将单个流量类别或一组流量类别映射到一个优先级组。系统中的所有端口根据每个优先级组或队列的配置状态，从相应的池中分配特定数量的缓冲区。池中的剩余缓冲区在所有配置相似的端口上共享。

以下缓冲池可用：

- 入口缓冲池：
  - 有损池（默认）
  - 无损池

- PFC — 适用于所有平台
  - LLFC — 适用于除 S4200-ON 系列交换机以外的所有平台
- 出口缓冲池：
  - 有损池（默认）
  - 无损池
    - PFC — 适用于所有平台
    - LLFC — 适用于除 S4200-ON 系列交换机以外的所有平台
  - CPU 池（CPU 控制流量）

此部分中使用以下术语：

- 默认缓冲区 — 默认情况下，系统会将特定数量的默认缓冲区分配给所有端口。
- 保留缓冲区 — 系统会在端口或优先级组（入口）和端口或队列（出口）上保留专用的缓冲区大小。
- 共享缓冲区 — 是总可用缓冲区空间减去保留缓冲区空间。共享缓冲区用于 CPU 控制流量，并在需要内存空间时动态分配给这些端口。
- Alpha 值 —
- Xoff 阈值（传输关闭） — 当系统达到 Xoff 阈值时，为防止流量丢失，系统将暂停，并且不接受任何进一步的数据包。
- Xon 阈值（传输开启） — 当系统达到 Xon 阈值时，系统将恢复并接受数据包。

例如，将所有端口分配为有损（默认）池的保留缓冲区时，有损池中的剩余缓冲区将在所有端口（除 CPU 端口以外）间共享。在端口上启用优先级流控制（PFC）时，所有已启用 PFC 的队列和优先级组都将使用无损池中的缓冲区。

您必须使用网络 QoS 策略类型来配置端口上的 PFC。

OS10 将专门为 CPU 流量提供单独的缓冲池。CPU 端口队列的所有默认保留缓冲区均来自 CPU 池。其余的缓冲区在所有 CPU 队列中共享。您可以修改 CPU 队列的缓冲区设置。

您可以使用 `control-plane-buffer-size` 命令配置 CPU 池的大小。

OS10 允许为每个端口的每个优先级组和队列配置缓冲区。

针对入口池上的入口数据包和出口池中的出口数据包将进行缓冲区使用情况核算。您可以按每个队列级别的优先级组和出口数据包缓冲区核算配置入口数据包缓冲区。

## 配置入口缓冲区

默认情况下，所有流量类别映射到入口缓冲区的默认优先级组（PG）7。缓冲区保留基于默认优先级组 ID 7。所有缓冲区均属于默认池的一部分，并且所有端口都从默认池中共享缓冲区。当您配置网络 qos 策略映射时，将创建一个新的优先级组，以从无损池为其分配缓冲区。其余未映射到任何 PFC 相关 PG 的流量类别，请使用默认缓冲区。

对于 10G、25G、40G、50G 和 100G 的速度，保留缓冲区大小为 9360 字节。对于不同的平台，支持的速度会有所不同。

表. 88: 最大缓冲区大小

| 平台                | 最大缓冲区大小 |
|-------------------|---------|
| S4000             | 12 MB   |
| S6010-ON、S4048-ON | 16 MB   |
| S4100-ON 系列       | 12 MB   |
| S4200-ON 系列       | 6 GB    |
| S5200-ON 系列       | 32 MB   |
| Z9100-ON          | 16 MB   |
| Z9264F-ON         | 42 MB   |

下表列出了为 S4100-ON 系列平台上的默认入口缓冲区分配的值。对于不同的平台和速度，这些值可能会有所不同。使用 `show qos ingress buffers` 命令查看交换机上的默认入口缓冲区。

表. 89: S4100-ON 系列平台上的默认入口缓冲区

| 速度               | 10G | 25G | 40G | 50G | 100G |
|------------------|-----|-----|-----|-----|------|
| PG 7 的保留缓冲区（默认值） | 9KB | 9KB | 9KB | 9KB | 9KB  |

下表列出了默认优先级组 7 的链路级流控制 (LLFC) 缓冲区设置：

表. 90: LLFC 的默认设置

| 速度                    | 10G  | 25G  | 40G  | 50G  | 100G  |
|-----------------------|------|------|------|------|-------|
| 默认保留缓冲区               | 9KB  | 9KB  | 18KB | 18KB | 36KB  |
| 默认 Xon 阈值             | 36KB | 45KB | 75KB | 91KB | 142KB |
| 默认 Xoff 阈值            | 9KB  | 9KB  | 9KB  | 9KB  | 9KB   |
| 默认动态共享缓冲区阈值 (alpha 值) | 9KB  | 9KB  | 9KB  | 9KB  | 9KB   |

**注：**□于不同的平台，支持的速度会有所不同。使用保留□缓冲区后，每个 LLFC 都会开始从无□池中使用共享□缓冲区，其 alpha □用于确定□□，但 S4200-ON 系列平台除外。

下表列出了每个 PFC 优先级组的优先级流控制 (PFC) 缓冲区设置：

表. 91: PFC 的默认设置

| 速度                               | 10G  | 25G  | 40G  | 50G  | 100G  |
|----------------------------------|------|------|------|------|-------|
| S4000、S4048-ON、S6010-ON 的默认保留缓冲区 | 9KB  | 不适用  | 9KB  | 不适用  | 不适用   |
| S41xx、Z9100-ON 的默认保留缓冲区          | 9KB  | 9KB  | 18KB | 18KB | 36KB  |
| 默认 Xoff 阈值                       | 36KB | 45KB | 75KB | 91KB | 142KB |
| 默认 Xon 阈值                        | 9KB  | 9KB  | 9KB  | 9KB  | 9KB   |
| 默认动态共享缓冲区阈值 (alpha 值)            | 9KB  | 9KB  | 9KB  | 9KB  | 9KB   |

**注：**□于不同的平台，支持的速度会有所不同。使用保留□缓冲区后，每个 PFC 均会从无□池中使用共享□缓冲区，并且 alpha □用于确定□□。

启用 LLFC 或 PFC 时，您可以覆盖默认优先级组设置。

1. 创建网络 qos 类型类别映射以匹配流量类别。对于 LLFC，将所有流量类别匹配为 0 至 7。对于 PFC，匹配所需的流量类别。

```
OS10(config)# class-map type network-qos example-cmap-in-buffer
OS10 (config-cmap-nqos)# match qos-group 0-7
```

2. 创建网络 qos 类型策略映射以定义流量类别的操作，如缓冲区配置和阈值。

```
OS10(config)# policy-map type network-qos example-pmap-in-buffer
OS10(config-pmap-network-qos)# class example-cmap-in-buffer
OS10 (config-pmap-c-nqos)# pause buffer-size 300 pause-threshold 200 resume-threshold 100
OS10 (config-pmap-c-nqos)# queue-limit thresh-mode dynamic 5
```

## 配置出口缓冲区

所有端口队列均使用保留缓冲区进行分配。当使用保留缓冲区时，每个队列都会从使用默认池中的共享缓冲区开始。

下表列出了为 S4100-ON 系列平台上的默认出口缓冲区分配的值。对于不同的平台和速度，这些值可能会有所不同。使用 show qos egress buffers 命令可查看交换机上的默认出口缓冲区。

表. 92: S4100-ON 系列平台上的默认出口缓冲区

| 速度                 | 10G     | 25G     | 40G     | 50G     | 100G    |
|--------------------|---------|---------|---------|---------|---------|
| 为每个端口的队列保留的缓冲区（默认） | 1664 字节 | 1664 字节 | 1664 字节 | 1664 字节 | 1664 字节 |

默认动态共享缓冲区阈值为 8。

1. 创建队列类型类别映射以匹配队列。

```
OS10(config)# class-map type queuing example-cmap-eg-buffer
OS10(config-cmap-queuing)# match queue 1
```

2. 创建队列类型策略映射以定义队列的操作，如缓冲区配置和阈值。

```
OS10(config)# policy-map type queuing example-pmap-eg-buffer
OS10(config-pmap-queuing)# class example-cmap-eg-buffer
OS10(config-pmap-c-que)# queue-limit queue-len 200 thresh-mode dynamic 5
```

## 深度缓冲区模式

**注：**在 S4200-ON 系列上支持功能。

OS10 可让您根据系统要求灵活配置缓冲区模式。系统内存包含数据包缓冲区列表和每个数据包信息 (PPI)，用于为每个多播流量启用统计标记、入口塑形、PFC 和输出逻辑接口时间戳。

S4200-ON 系列交换机附带默认的 4.63 GB 深度缓冲区。您可以使用 `hardware deep-buffer-mode` 命令将此深度缓冲区提升至 6.24 GB。有关如何配置深度缓冲区模式的信息，请参阅[配置深度缓冲区模式](#)。下表列出了不同模式下的总缓冲区可用性：

表. 93: 不同模式下的缓冲区可用性

| 平台          | 默认深度缓冲区 | 增强的深度缓冲区 |
|-------------|---------|----------|
| S4200-ON 系列 | 4.63 GB | 6.24 GB  |

深度缓冲区模式仅在将其保存在启动配置中并重新加载交换机后才会生效。

**注：**不支持在运行禁用深度缓冲区模式配置。

## 限制

深度缓冲区模式和网络 QoS 配置不能共存。仅在网络 QoS 配置时启用深度缓冲区模式；例如，LLFC 和 PFC 处于禁用状态。要配置深度缓冲区模式，请禁用所有网络 QoS 相关配置。

## 配置深度缓冲区模式

在配置深度缓冲区模式之前，您必须禁用所有网络 QoS 配置；例如，PFC 和 LLFC。默认情况下，深度缓冲区模式处于禁用状态。

1. 在 CONFIGURATION 模式下启用深度缓冲区模式。

```
OS10# configure terminal
OS10(config)# hardware deep-buffer-mode
```

**注：**要禁用深度缓冲区模式，请使用命令的 `no` 格式。禁用深度缓冲区模式仅在将其保存在启动配置中并重新加载交换机后才会生效。

配置深度缓冲区模式后，系统将显示一条警告消息，说明仅在将配置保存到启动配置中并重新加载交换机后才会生效。

```
% Warning: Deep buffer mode configuration will be applied only after a save and reload.
```

2. 在 CONFIGURATION 模式下的启动配置中保存深度缓冲区模式。

```
OS10(config)# do write memory
```

3. 在 CONFIGURATION 模式下重新加载交换机。

```
OS10(config)# do reload
Proceed to reboot the system? [confirm yes/no]:yes
```

要查看深度缓冲区模式状态，请使用 `show hardware deep-buffer-mode` 命令。show 命令输出将显示当前引导和下一次引导中的深度缓冲区模式的状态。

在启用深度缓冲区模式状态之前将显示以下默认设置：

```
OS10# show hardware deep-buffer-mode
Deep Buffer Mode Configuration Status

Current-boot Settings : Disabled

Next-boot Settings : Disabled
```

以下是在启动配置中保存配置后的深度缓冲区模式状态：

```
OS10# show hardware deep-buffer-mode
Deep Buffer Mode Configuration Status

Current-boot Settings : Disabled

Next-boot Settings : Enabled
```

以下是交换机重新加载后的深度缓冲区模式状态：

```
OS10# show hardware deep-buffer-mode
Deep Buffer Mode Configuration Status

Current-boot Settings : Enabled

Next-boot Settings : Enabled
```

## 拥塞规避

拥塞规避可预见并采取必要的措施来避免拥塞。以下机制可规避拥塞：

- **尾部丢弃** — 数据包在流量队列中进行缓冲。当缓冲区耗尽或达到配置的阈值时，将丢弃多余的数据包。默认情况下，OS10 使用尾部丢弃进行拥塞规避。
- **随机早期检测 (RED)** — 在尾部丢弃的情况下，不会在缓冲区利用率中考虑不同的流。当多个主机启动重新传输时，尾部丢弃会导致 TCP 全局重新同步。如果平均队列长度超过配置的最小阈值，RED 不会等待队列完全填充，而是开始使用特定丢弃概率丢弃额外的数据包。较早的丢弃可确保只有部分 TCP 源速度减慢，从而规避全局 TCP 重新同步。
- **加权随机早期检测 (WRED)** — 这可以为每种颜色（红色、黄色、绿色）流量提供不同的丢弃概率和阈值。您可以通过将颜色分配给流来配置三种不同流的丢弃特性。使用各种方法将颜色分配给特定流或流量，如入口监察、qos 输入策略-映射等。
- **显式拥塞通知 (ECN)** — 这是 WRED 的扩展。ECN 将数据包中 ECN 字段的拥塞 (CE) 位标记为支持 ECN 的流量 (ECT)，而不是在平均队列长度超过最小阈值时丢弃数据包。

1. 在 CONFIGURATION 模式下配置 WRED 配置文件。

```
OS10(config)# wred example-wred-prof
```

2. 在 WRED CONFIGURATION 模式下，为不同颜色配置 WRED 阈值参数。

```
OS10(config-wred)# random-detect color yellow minimum-threshold 100 maximum-threshold 300 drop-probability 40
```

3. 在 WRED CONFIGURATION 模式下配置 WRED 配置文件的指数权重值。

```
OS10(config-wred)# random-detect weight 4
```

4. 启用 ECN。

```
OS10(config-wred)# random-detect ecn
```

5. 启用队列上的 WRED/ECN。

```
OS10(config)# class-map type queuing example-cmap-wred
OS10(config-cmap-queuing)# match queue 2
OS10(config-cmap-queuing)# exit
OS10(config)# policy-map type queuing example-pmap-wred
```

```
OS10(config-pmap-queuing)# class example-cmap-wred
OS10(config-pmap-c-queue)# random-detect example-wred-prof
```

6. 启用端口上的 WRED/ECN。

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# random-detect example-wred-prof
```

7. 启用服务池上的 WRED/ECN。

```
OS10(config)# system qos
OS10(config-sys-qos)# random-detect pool 0 example-wred-prof
```

**注：**在 S4200-ON 系列平台上，仅全局启用 ECN。此外，仅在队列级别应用 ECN 配置。您不能在接口或服务池级别配置 ECN。如果您尝试在接口或服务池级别应用 ECN 配置，则不接受配置。

1. 在 CONFIGURATION 模式下配置 WRED 配置文件。

```
OS10(config)# wred example-wred-prof-1
```

2. 在 WRED CONFIGURATION 模式下，为不同颜色配置 WRED 阈值参数。

```
OS10(config-wred)# random-detect color yellow minimum-threshold 100 maximum-threshold 300 drop-probability 40
```

3. 在 WRED CONFIGURATION 模式下配置 WRED 配置文件的指数权重值。

```
OS10(config-wred)# random-detect weight 4
```

4. 在 WRED CONFIGURATION 模式下配置 ECN 阈值参数。

```
OS10(config-wred)# random-detect ecn minimum-threshold 100 maximum-threshold 300 drop-probability 40
```

5. 退出 WRED CONFIGURATION 模式。

```
OS10(config-wred)#exit
```

6. 创建 QoS 类别映射。

```
OS10(config)# class-map type queuing example-cmap-wred-1
OS10(config-cmap-queuing)# match queue 2
```

7. 进入 QOS POLICY-MAP 模式并创建队列策略类型。

```
OS10(config)# policy-map type queuing example-pmap-wred-1
OS10(config-pmap-queuing)# class example-cmap-wred-1
```

8. 将 WRED 配置文件分配给指定队列。

```
OS10(config-pmap-c-queue)# random-detect example-wred-prof-1
```

9. 退出 CLASS MAP 和 POLICY MAP 模式。

```
OS10(config-pmap-c-queue)#exit
OS10(config-pmap-queuing)#exit
```

10. 进入 SYSTEM QOS 模式。

```
OS10(config)#configure system-qos
```

11. 全局启用 ECN。

```
OS10(config-sys-qos)#random-detect ecn
```

全局启用 ECN 后，ECN 会将数据包中 ECN 字段的 CE 位标记为 ECT。

在 S4200-ON 系列平台中，为支持 ECN 的流量 (ECT) 配置单独的阈值。如果启用 ECN，根据所配置的 ECN 阈值标记，将标记 ECT；而根据 WRED 阈值，非 ECT 将丢弃。



# 风暴控制

由数据包泛洪或其他原因形成的流量风暴可能会降低网络性能。风暴控制功能允许您控制 L2 和 L3 物理接口上的未知单播、多播和广播流量。

OS10 设备会按固定的时间间隔监控当前流量速率级别，将流量速率与配置的级别进行比较，并丢弃剩余流量。

默认情况下，在所有接口上禁用风暴控制。在 INTERFACE 模式下使用 `storm-control { broadcast | multicast | unknown-unicast } rate-in-pps` 命令启用风暴控制。

 **注：**此功能在 Z9332F-ON 平台上不受支持。

- 在以太网 1/1/1 上以每秒 1000 个数据包数 (pps) 为速率启用广播风暴控制。

```
OS10(config-if-eth1/1/1)# storm-control broadcast 1000
```

## RoCE 实现更快的访问和无损连接

远程直接内存访问 (RDMA) 在网络中的两台计算机之间启用内存传输，而不涉及任何一台计算机的 CPU。

RDMA 网络可提供高带宽和低延迟，而无需可评估的 CPU 开销，从而提高应用程序性能、存储和数据中心利用率，并简化网络管理。传统上，仅在 InfiniBand 环境中支持 RDMA。目前，在使用以太网或混合协议环境的数据中心中也实施了 RDMA over Converged Ethernet (RoCE)。

OS10 设备支持 RoCE v1 和 RoCE v2 协议。

- RoCE v1 — 允许在同一以太网广播域中的两个主机之间进行通信的以太网层协议。
- RoCE v2 — 一种互联网层协议，允许路由 RoCE v2 数据包，称为可路由 RoCE (RRoCE)。

要启用 RRoCE，请在交换机的所有接口上的入口和出口方向上配置 QoS 服务策略。有关此配置的详细信息，请参阅[在交换机上配置 RoCE](#)。

## 在交换机上配置 RoCE

以下示例介绍了在交换机上配置 RoCE 的步骤。此配置示例使用适用于 RoCE 的优先级 3。

1. 进入 CONFIGURATION 模式。

```
OS10# configure terminal
OS10 (config)#
```

2. 启用数据中心桥接交换协议 (DCBX)。

```
OS10 (config)# dcbx enable
```

3. 创建 VLAN。在此示例中，VLAN 55 将交换 RoCE 流量。您可以配置从 1 到 4093 的任何值。

```
OS10 (config)# interface vlan 55
```

4. 创建适用于优先级流控制 (PFC) 的网络 qos 类型的类别映射。

```
OS10 (config)# class-map type network-qos pfcdot1p3
OS10 (config-cmap-nqos)# match qos-group 3
```

5. 创建适用于增强的传输选择 (ETS) 的队列类型的类别映射。

```
OS10 (config)# class-map type queuing Q0
OS10 (config-cmap-queuing)# match queue 0
OS10 (config)# class-map type queuing Q3
OS10 (config-cmap-queuing)# match queue 3
```

6. 创建适用于 ETS 的 QoS 映射。

```
OS10 (config)# qos-map traffic-class 2Q
OS10(config-qos-map)# queue 0 qos-group 0-2, 4-7
OS10(config-qos-map)# queue 3 qos-group 3
```

7. 创建适用于 PFC 的策略映射。

```
OS10 (config)# policy-map type network-qos policy_pfcdot1p3
OS10(config-pmap-network-qos)# class pfcdot1p3
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 3
```

8. 创建出口策略映射。

```
OS10 (config)# policy-map type queuing policy_2Q
OS10 (config-pmap-queuing)# class Q0
OS10 (config-pmap-c-que)# bandwidth percent 30
OS10 (config-pmap-c-que)# exit
OS10 (config-pmap-queuing)# class Q3
OS10 (config-pmap-c-que)# bandwidth percent 70
```

9. 全局或在接口级别应用 dot1p 信任。在此示例中，dot1p 信任已全局应用。

```
OS10 (config)# system qos
OS10 (config-sys-qos)# trust-map dot1p default
```

10. 在要支持 RoCE 的所有交换机接口上执行以下配置：

a. 进入 INTERFACE 模式，然后输入 no shutdown 命令。

```
OS10# configure terminal
OS10 (config)# interface ethernet 1/1/1
OS10 (conf-if-eth1/1/1)# no shutdown
```

b. 将交换机端口模式更改为中继模式。

```
OS10 (conf-if-eth1/1/1)# switchport mode trunk
```

c. 指定在中继端口上允许的 VLAN。

```
OS10 (conf-if-eth1/1/1)# switchport trunk allowed vlan 55
```

d. 将网络 qos 类型的策略-映射应用到接口。

```
OS10 (conf-if-eth1/1/1)# service-policy input type network-qos policy_pfcdot1p3
```

e. 将队列策略应用到接口上的出口流量。

```
OS10 (conf-if-eth1/1/1)# service-policy output type queuing policy_2Q
```

f. 在接口上启用 ETS。

```
OS10 (conf-if-eth1/1/1)# ets mode on
```

g. 在接口上应用适用于 ETS 配置的 qos 映射。

```
OS10 (conf-if-eth1/1/1)# qos-map traffic-class 2Q
```

h. 在接口上启用 PFC。

```
OS10 (conf-if-eth1/1/1)# priority-flow-control mode on
```

## RoCE for VXLAN over VLT

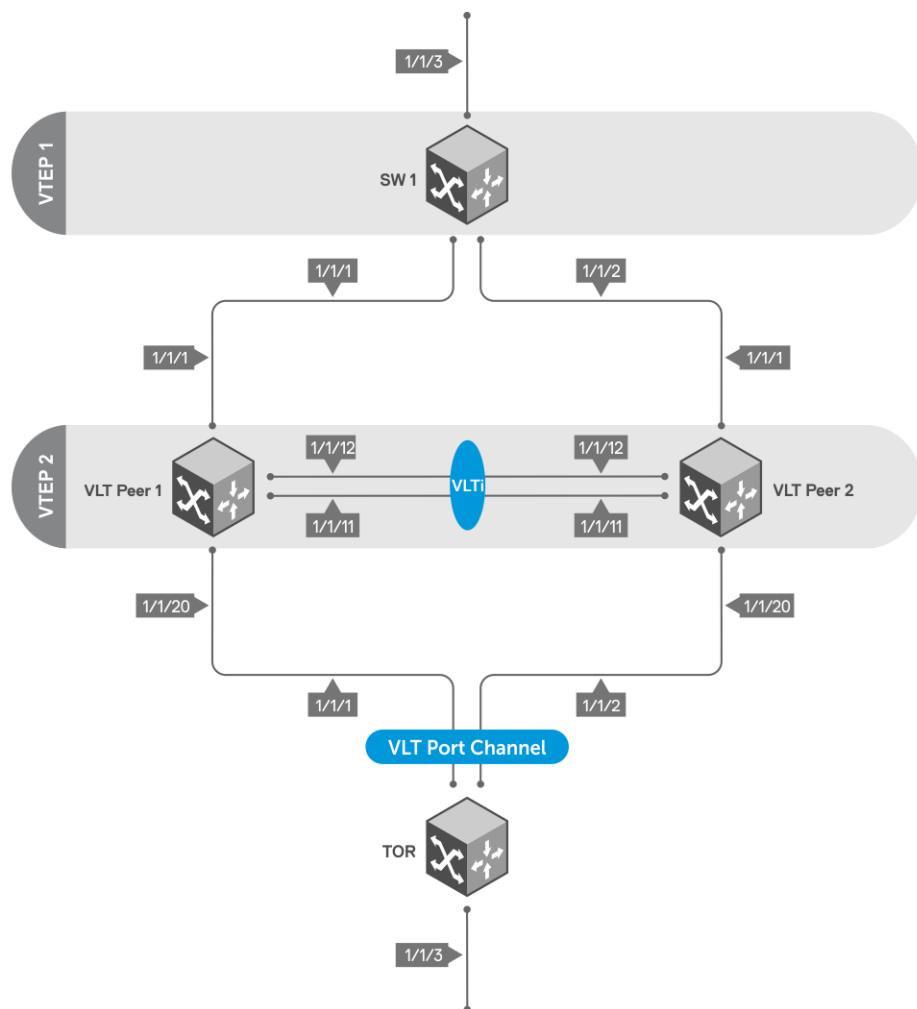
OS10 在 VLT 设置中支持 RoCE for VXLAN。使用 VXLAN 配置 RoCE 类似于在没有 VXLAN 的情况下配置 RoCE。当您配置 VXLAN 并跨 VLT 拓扑时，在您想要支持 RoCE 的 VLT 拓扑中的所有接口上应用配置。

有关如何配置 RoCE 的详细信息，请参阅[“在交换机上配置 RoCE”](#)部分。



## RoCE for VXLAN over VLT 的示例配置

下面介绍了已通过 VXLAN over VLT 启用了 VXLAN 的拓扑。SW1 配置为 VTEP1，并且是连接到外部网络的上游交换机。VLT 对等节点 1 和 VLT 对等节点 2 形成 VLT 拓扑，并且也配置为 VTEP 2。架顶式 (ToR) 交换机通过 VLT 端口通道连接至 VLT 对等节点。ToR 是适用于终端设备（如虚拟机）的下游交换机。



以下示例显示了此网络中的每个设备及其各自的配置：

### SW1 配置

#### VXLAN 配置 — SW1

```
OS10# configure terminal
OS10(config)# interface vlan 3000
OS10(conf-if-vl-3000)# exit
OS10(config)# interface vlan 200
OS10(conf-if-vl-200)# exit
OS10(config)# interface loopback 1
OS10(conf-if-lo-1)# ip address 1.1.1.1/32
OS10(conf-if-lo-1)# exit
OS10(config)# router ospf 1
OS10(config-router-ospf-1)# router-id 8.8.8.8
OS10(config-router-ospf-1)# exit
OS10(config)# interface vlan 3000
OS10(conf-if-vl-3000)# ip ospf 1 area 0
OS10(conf-if-vl-3000)# exit
OS10(config)# interface loopback 1
OS10(conf-if-lo-1)# ip ospf 1 area 0
OS10(conf-if-lo-1)# exit
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# switchport mode trunk
```

```

OS10(config-if-eth1/1/1)# switchport trunk allowed vlan 3000
OS10(config-if-eth1/1/1)# exit
OS10(config)# interface ethernet 1/1/2
OS10(config-if-eth1/1/2)# switchport mode trunk
OS10(config-if-eth1/1/2)# switchport trunk allowed vlan 3000
OS10(config-if-eth1/1/2)# exit
OS10(config)# configure terminal
OS10(config)# nve
OS10(config-nve)# source-interface loopback 1
OS10(config-nve)# exit
OS10(config)# virtual-network 5
OS10(config-vn-5)# vxlan-vni 1000
OS10(config-vn-vxlan-vni)# remote-vtep 2.2.2.2
OS10(config-vn-vxlan-vni-remote-vtep)# exit
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-5)# exit
OS10(config)# interface vlan 200
OS10(config-if-vl-200)# virtual-network 5
OS10(config-if-vl-200)# end
OS10#
OS10# configure terminal
OS10(config)# interface ethernet 1/1/3
OS10(config-if-eth1/1/3)# switchport mode trunk
OS10(config-if-eth1/1/3)# switchport trunk allowed vlan 200
OS10(config-if-eth1/1/3)# end

```

## PFC 配置 — SW1

```

OS10# configure terminal
OS10(config)# trust dot1p-map t1
OS10(config-tmap-dot1p-map)# qos-group 0 dot1p 0
OS10(config-tmap-dot1p-map)# qos-group 1 dot1p 1
OS10(config-tmap-dot1p-map)# qos-group 2 dot1p 2
OS10(config-tmap-dot1p-map)# qos-group 3 dot1p 3
OS10(config-tmap-dot1p-map)# qos-group 4 dot1p 4
OS10(config-tmap-dot1p-map)# qos-group 5 dot1p 5
OS10(config-tmap-dot1p-map)# qos-group 6 dot1p 6
OS10(config-tmap-dot1p-map)# qos-group 7 dot1p 7
OS10(config-tmap-dot1p-map)# end
OS10# configure terminal
OS10(config)# class-map type network-qos c5
OS10(config-cmap-nqos)# match qos-group 5
OS10(config-cmap-nqos)# exit
OS10(config)# policy-map type network-qos p5
OS10(config-pmap-network-qos)# class c5
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 5
OS10(config-pmap-c-nqos)# end
OS10# configure terminal
OS10(config)# interface range ethernet 1/1/3,1/1/1,1/1/2
OS10(config-range-eth1/1/3,1/1/1,1/1/2)# flowcontrol receive off
OS10(config-range-eth1/1/3,1/1/1,1/1/2)# priority-flow-control mode on
OS10(config-range-eth1/1/3,1/1/1,1/1/2)# ets mode on
OS10(config-range-eth1/1/3,1/1/1,1/1/2)# service-policy input type network-qos p5
OS10(config-range-eth1/1/3,1/1/1,1/1/2)# trust-map dot1p t1

```

## LLFC 配置 — SW1

您可以按如下所示配置 LLFC，而不是 PFC：

```

OS10(config)# configure terminal
OS10(config)# class-map type network-qos llfc
OS10(config-cmap-nqos)# match qos-group 0-7
OS10(config-cmap-nqos)# exit
OS10(config)# policy-map type network-qos llfc
OS10(config-pmap-network-qos)# class llfc
OS10(config-pmap-c-nqos)# pause buffer-size 100 pause-threshold 50 resume-threshold 10
OS10(config-pmap-c-nqos)# end
OS10#
OS10# configure terminal
OS10(config)# interface range ethernet 1/1/1,1/1/2,1/1/3
OS10(config-range-eth1/1/1,1/1/2,1/1/3)# flowcontrol transmit on

```

```
OS10(config-range-eth1/1/1,1/1/2,1/1/3)# flowcontrol receive on
OS10(config-range-eth1/1/1,1/1/2,1/1/3)# service-policy input type network-qos llfc
OS10(config-range-eth1/1/1,1/1/2,1/1/3)# end
```

## WRED 和 ECN 配置 — SW1

```
OS10# configure terminal
OS10(config)# wred w1
OS10(config-wred)# random-detect ecn
OS10(config-wred)# random-detect color green minimum-threshold 100 maximum-threshold 500
drop-probability 100
OS10(config-wred)# random-detect color yellow minimum-threshold 100 maximum-threshold
500 drop-probability 100
OS10(config-wred)# random-detect color red minimum-threshold 100 maximum-threshold 500
drop-probability 100
OS10(config-wred)# exit
OS10(config)# class-map type queuing cq
OS10(config-cmap-queuing)# match queue 5
OS10(config-cmap-queuing)# exit
OS10(config)# policy-map type queuing pq
OS10(config-pmap-queuing)# class cq
OS10(config-pmap-c-que)# random-detect w1
OS10(config-pmap-c-que)# end
OS10# configure terminal
OS10(config)# interface range ethernet 1/1/3,1/1/1,1/1/2
OS10(config-range-eth1/1/3,1/1/1,1/1/2)# flowcontrol receive off
OS10(config-range-eth1/1/3,1/1/1,1/1/2)# priority-flow-control mode on
OS10(config-range-eth1/1/3,1/1/1,1/1/2)# ets mode on
OS10(config-range-eth1/1/3,1/1/1,1/1/2)# service-policy input type network-qos p5
OS10(config-range-eth1/1/3,1/1/1,1/1/2)# service-policy output type queuing pq
OS10(config-range-eth1/1/3,1/1/1,1/1/2)# trust-map dot1p t1
OS10(config-range-eth1/1/3,1/1/1,1/1/2)# end
```

## 启用 DCBx — SW1

```
OS10# configure terminal
OS10(config)# dcbx enable
```

## VLT 对等节点 1 上的配置

### VLT 配置 — VLT 对等节点 1

```
OS10# configure terminal
OS10(config)# interface range ethernet 1/1/12,1/1/11
OS10(config-range-eth1/1/12,1/1/11)# no switchport mode
OS10(config-range-eth1/1/12,1/1/11)# no switchport
OS10(config-range-eth1/1/12,1/1/11)# no negotiation
OS10(config-range-eth1/1/12,1/1/11)# exit
OS10(config)# vlt-domain 1
OS10(config-vlt-1)# discovery-interface ethernet 1/1/12
OS10(config-vlt-1)# discovery-interface ethernet 1/1/11
OS10(config-vlt-1)# vlt-mac aa:bb:cc:dd:ee:ff
OS10(config-vlt-1)# end
OS10#
OS10# configure terminal
OS10(config)# interface port-channel 2
OS10(config-if-po-2)# vlt-port-channel 20
OS10(config-if-po-2)# no shutdown
OS10(config-if-po-2)# exit
OS10(config)# interface range ethernet 1/1/20
OS10(config-range-eth1/1/20)# channel-group 2 mode active
OS10(config-range-eth1/1/20)# exit
```

## VXLAN 配置 — VLT 对等节点 1

```
OS10(config)# configure terminal
OS10(config)# interface vlan 3000
OS10(config-if-vl-3000)# ip address 5.5.5.2/24
OS10(config-if-vl-3000)# exit
OS10(config)# interface vlan 200
OS10(config-if-vl-200)# exit
```

```

OS10(config)# interface loopback1
OS10(config-if-lo-1)# no shutdown
OS10(config-if-lo-1)# ip address 2.2.2.2/11
OS10(config-if-lo-1)# exit
OS10(config)# router ospf 1
OS10(config-router-ospf-1)# router-id 9.9.9.9
OS10(config-router-ospf-1)# exit
OS10(config)# interface loopback 1
OS10(config-if-lo-1)# ip ospf 1 area 0
OS10(config-if-lo-1)#
OS10(config-if-lo-1)# configure terminal
OS10(config)# interface vlan 3000
OS10(config-if-vl-3000)# ip ospf 1 area 0
OS10(config-if-vl-3000)# end
OS10# configure terminal
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# switchport mode trunk
OS10(config-if-eth1/1/1)# switchport trunk allowed vlan 3000
OS10(config-if-eth1/1/1)# exit
OS10(config)# nve
OS10(config-nve)# source-interface loopback 1
OS10(config-nve)# exit
OS10(config)# virtual-network 5
OS10(config-vn-5)# vxlan-vni 1200
OS10(config-vn-vxlan-vni)# remote-vtep 1.1.1.1
OS10(config-vn-vxlan-vni-remote-vtep)# exit
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-5)# exit
OS10(config)# interface vlan 200
OS10(config-if-vl-200)# virtual-network 5
OS10(config-if-vl-200)# end
OS10#
OS10# configure terminal
OS10(config)# interface port-channel 2
OS10(config-if-po-2)# switchport mode trunk
OS10(config-if-po-2)# switchport trunk allowed vlan 200
OS10(config-if-po-2)# end

```

## PFC 配置 — VLT 对等节点 1

```

OS10# configure terminal
OS10(config)# trust dot1p-map t1
OS10(config-tmap-dot1p-map)# qos-group 0 dot1p 0
OS10(config-tmap-dot1p-map)# qos-group 1 dot1p 1
OS10(config-tmap-dot1p-map)# qos-group 2 dot1p 2
OS10(config-tmap-dot1p-map)# qos-group 3 dot1p 3
OS10(config-tmap-dot1p-map)# qos-group 4 dot1p 4
OS10(config-tmap-dot1p-map)# qos-group 5 dot1p 5
OS10(config-tmap-dot1p-map)# qos-group 6 dot1p 6
OS10(config-tmap-dot1p-map)# qos-group 7 dot1p 7
OS10(config-tmap-dot1p-map)# end
OS10# configure terminal
OS10(config)# class-map type network-qos c5
OS10(config-cmap-nqos)# match qos-group 5
OS10(config-cmap-nqos)# exit
OS10(config)# policy-map type network-qos p5
OS10(config-pmap-network-qos)# class c5
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 5
OS10(config-pmap-c-nqos)# end
OS10# configure terminal
OS10(config)# interface range ethernet 1/1/1,1/1/20,1/1/31,1/1/32
OS10(config-range-eth1/1/1,1/1/20,1/1/31,1/1/32)# flowcontrol receive off
OS10(config-range-eth1/1/1,1/1/20,1/1/31,1/1/32)# priority-flow-control mode on
OS10(config-range-eth1/1/1,1/1/20,1/1/31,1/1/32)# ets mode on
OS10(config-range-eth1/1/1,1/1/20,1/1/31,1/1/32)# service-policy input type network-qos p5
OS10(config-range-eth1/1/1,1/1/20,1/1/31,1/1/32)# trust-map dot1p t1
OS10(config-range-eth1/1/1,1/1/20,1/1/31,1/1/32)# end

```

## LLFC 配置 — VLT 对等节点 1

您可以按如下所示配置 LLFC，而不是 PFC：

```
OS10# configure terminal
OS10(config)# class-map type network-qos llfc
OS10(config-cmap-nqos)# match qos-group 0-7
OS10(config-cmap-nqos)# exit
OS10(config)# policy-map type network-qos llfc
OS10(config-pmap-network-qos)# class llfc
OS10(config-pmap-c-nqos)# pause buffer-size 120 pause-threshold 50 resume-threshold 12
OS10(config-pmap-c-nqos)# end
OS10# configure terminal
OS10(config)# interface range ethernet 1/1/1,1/1/20,1/1/31,1/1/32
OS10(conf-range-eth1/1/1,1/1/20,1/1/31,1/1/32)# flowcontrol transmit on
OS10(conf-range-eth1/1/1,1/1/20,1/1/31,1/1/32)# flowcontrol receive on
OS10(conf-range-eth1/1/1,1/1/20,1/1/31,1/1/32)# service-policy input type network-qos llfc
OS10(conf-range-eth1/1/1,1/1/20,1/1/31,1/1/32)# end
```

## WRED/ECN 配置 — VLT 对等节点 1

```
OS10# configure terminal
OS10(config)# wred w1
OS10(config-wred)# random-detect ecn
OS10(config-wred)# random-detect color green minimum-threshold 120 maximum-threshold 500 drop-probability 100
OS10(config-wred)# random-detect color yellow minimum-threshold 120 maximum-threshold 500 drop-probability 100
OS10(config-wred)# random-detect color red minimum-threshold 120 maximum-threshold 500 drop-probability 100
OS10(config-wred)# exit
OS10(config)# class-map type queuing cq
OS10(config-cmap-queuing)# match queue 5
OS10(config-cmap-queuing)# exit
OS10(config)# policy-map type queuing pq
OS10(config-pmap-queuing)# class cq
OS10(config-pmap-c-que)# random-detect w1
OS10(config-pmap-c-que)# end
OS10# configure terminal
OS10(config)# interface range ethernet 1/1/1,1/1/20,1/1/12,1/1/11
OS10(conf-range-eth1/1/1,1/1/20,1/1/12,1/1/11)# service-policy input type network-qos p5
OS10(conf-range-eth1/1/1,1/1/20,1/1/12,1/1/11)# service-policy output type queuing pq
OS10(conf-range-eth1/1/1,1/1/20,1/1/12,1/1/11)# trust-map dot1p t1
OS10(conf-range-eth1/1/1,1/1/20,1/1/12,1/1/11)# flowcontrol receive off
OS10(conf-range-eth1/1/1,1/1/20,1/1/12,1/1/11)# priority-flow-control mode on
OS10(conf-range-eth1/1/1,1/1/20,1/1/12,1/1/11)# ets mode on
OS10(conf-range-eth1/1/1,1/1/20,1/1/12,1/1/11)# end
```

## 启用 DCBx — VLT 对等节点 1

```
OS10# configure terminal
OS10(config)# dcbx enable
```

## VLT 对等节点 2 上的配置

### VLT 配置 — VLT 对等节点 2

```
OS10# configure terminal
OS10(config)# interface range ethernet 1/1/11,1/1/12
OS10(conf-range-eth1/1/11,1/1/12)# no switchport mode
OS10(conf-range-eth1/1/11,1/1/12)# no switchport
OS10(conf-range-eth1/1/11,1/1/12)# no negotiation
OS10(conf-range-eth1/1/11,1/1/12)# exit
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# discovery-interface ethernet 1/1/11
OS10(conf-vlt-1)# discovery-interface ethernet 1/1/12
OS10(conf-vlt-1)# vlt-mac aa:bb:cc:dd:ee:ff
OS10(conf-vlt-1)# end
OS10#
OS10# configure terminal
OS10(config)# interface port-channel 2
OS10(conf-if-po-2)# vlt-port-channel 20
```

```
OS10(config-if-po-2)# no shutdown
OS10(config-if-po-2)# exit
```

## VXLAN 配置 — VLT 对等节点 2

```
OS10(config)# configure terminal
OS10(config)# interface vlan 3000
OS10(config-if-vl-3000)# ip address 5.5.5.3/24
OS10(config-if-vl-3000)# exit
OS10(config)# interface vlan 200
OS10(config-if-vl-200)# exit
OS10(config)# interface loopback 1
OS10(config-if-lo-1)# no shutdown
OS10(config-if-lo-1)# ip address 2.2.2.2/32
OS10(config-if-lo-1)# exit
OS10(config)# router ospf 1
OS10(config-router-ospf-1)# router-id 10.10.10.10
OS10(config-router-ospf-1)# exit
OS10(config)# interface loopback 1
OS10(config-if-lo-1)# ip ospf 1 area 0
OS10(config-if-lo-1)# configure terminal
OS10(config)# interface vlan 3000
OS10(config-if-vl-3000)# ip ospf 1 area 0
OS10(config-if-vl-3000)# end
OS10# configure terminal
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# switchport mode trunk
OS10(config-if-eth1/1/1)# switchport trunk allowed vlan 3000
OS10(config-if-eth1/1/1)# exit
OS10(config)# nve
OS10(config-nve)# source-interface loopback 1
OS10(config-nve)# exit
OS10(config)# virtual-network 5
OS10(config-vn-5)# vxlan-vni 1000
OS10(config-vn-vxlan-vni)# remote-vtep 1.1.1.1
OS10(config-vn-vxlan-vni-remote-vtep)# exit
OS10(config-vn-vxlan-vni)# exit
OS10(config-vn-5)# exit
OS10(config)# interface vlan 200
OS10(config-if-vl-200)# virtual-network 5
OS10(config-if-vl-200)# end
OS10#
OS10# configure terminal
OS10(config)# interface port-channel 2
OS10(config-if-po-2)# switchport mode trunk
OS10(config-if-po-2)# switchport trunk allowed vlan 200
OS10(config-if-po-2)# end
```

## PFC 配置 — VLT 对等节点 2

```
OS10# configure terminal
OS10(config)# trust dot1p-map t1
OS10(config-tmap-dot1p-map)# qos-group 0 dot1p 0
OS10(config-tmap-dot1p-map)# qos-group 1 dot1p 1
OS10(config-tmap-dot1p-map)# qos-group 2 dot1p 2
OS10(config-tmap-dot1p-map)# qos-group 3 dot1p 3
OS10(config-tmap-dot1p-map)# qos-group 4 dot1p 4
OS10(config-tmap-dot1p-map)# qos-group 5 dot1p 5
OS10(config-tmap-dot1p-map)# qos-group 6 dot1p 6
OS10(config-tmap-dot1p-map)# qos-group 7 dot1p 7
OS10(config-tmap-dot1p-map)# end
OS10# configure terminal
OS10(config)# class-map type network-qos c5
OS10(config-cmap-nqos)# match qos-group 5
OS10(config-cmap-nqos)# exit
OS10(config)# policy-map type network-qos p5
OS10(config-pmap-network-qos)# class c5
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 5
OS10(config-pmap-c-nqos)# end
OS10# configure terminal
OS10(config)# interface range ethernet 1/1/1,1/1/20,1/1/11,1/1/12
```

```

OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# flowcontrol receive off
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# priority-flow-control mode on
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# ets mode on
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# service-policy input type network-qos p5
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# trust-map dot1p t1
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# end

```

## LLFC 配置 — VLT 对等节点 2

您可以按如下所示配置 LLFC，而不是 PFC：

```

OS10# configure terminal
OS10(config)# class-map type network-qos llfc
OS10(config-cmap-nqos)# match qos-group 0-7
OS10(config-cmap-nqos)# exit
OS10(config)# policy-map type network-qos llfc
OS10(config-pmap-network-qos)# class llfc
OS10(config-pmap-c-nqos)# pause buffer-size 50 pause-threshold 30 resume-threshold 10
OS10(config-pmap-c-nqos)# end
OS10# configure terminal
OS10(config)# interface range ethernet 1/1/1,1/1/20,1/1/11,1/1/12
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# flowcontrol transmit on
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# flowcontrol receive on
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# service-policy input type network-qos llfc
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# end

```

## WRED/ECN 配置 — VLT 对等节点 2

```

OS10# configure terminal
OS10(config)# wred w1
OS10(config-wred)# random-detect ecn
OS10(config-wred)# random-detect color green minimum-threshold 100 maximum-threshold 500 drop-probability 100
OS10(config-wred)# random-detect color yellow minimum-threshold 100 maximum-threshold 500 drop-probability 100
OS10(config-wred)# random-detect color red minimum-threshold 100 maximum-threshold 500 drop-probability 100
OS10(config-wred)# exit
OS10(config)# class-map type queuing cq
OS10(config-cmap-queuing)# match queue 5
OS10(config-cmap-queuing)# exit
OS10(config)# policy-map type queuing pq
OS10(config-pmap-queuing)# class cq
OS10(config-pmap-c-que)# random-detect w1
OS10(config-pmap-c-que)# end
OS10# configure terminal
OS10(config)# interface range ethernet 1/1/1,1/1/20,1/1/11,1/1/12
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# flowcontrol receive off
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# priority-flow-control mode on
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# ets mode on
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# service-policy input type network-qos p5
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# service-policy output type queuing pq
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# trust-map dot1p t1
OS10(conf-range-eth1/1/1,1/1/20,1/1/11,1/1/12)# end

```

## 启用 DCBx — VLT 对等节点 2

```

OS10# configure terminal
OS10(config)# dcbx enable

```

## ToR 设备上的配置

### 系统配置 — ToR 设备

```

NOS# configure terminal
NOS(config)# interface vlan 200
NOS(conf-if-vl-200)# no shutdown
NOS(conf-if-vl-200)# exit
NOS(config)# interface port-channel 2
NOS(conf-if-po-2)# no shutdown
NOS(conf-if-po-2)# exit

```

```

NOS(config)# interface range ethernet 1/1/1,1/1/2
NOS(conf-range-eth1/1/1,1/1/2)# channel-group 2 mode active
NOS(conf-range-eth1/1/1,1/1/2)# end
NOS#
NOS# configure terminal
NOS(config)# interface ethernet 1/1/3
NOS(conf-if-eth1/1/3)# switchport mode trunk
NOS(conf-if-eth1/1/3)# switchport trunk allowed vlan 200
NOS(conf-if-eth1/1/3)# end
NOS#
NOS# configure terminal
NOS(config)# interface port-channel 2
NOS(conf-if-po-2)# switchport mode trunk
NOS(conf-if-po-2)# switchport trunk allowed vlan 200
NOS(conf-if-po-2)# end

```

## PFC 配置 — ToR 设备

```

NOS# configure terminal
NOS(config)# trust dot1p-map t1
NOS(config-tmap-dot1p-map)# qos-group 0 dot1p 0
NOS(config-tmap-dot1p-map)# qos-group 1 dot1p 1
NOS(config-tmap-dot1p-map)# qos-group 2 dot1p 2
NOS(config-tmap-dot1p-map)# qos-group 3 dot1p 3
NOS(config-tmap-dot1p-map)# qos-group 4 dot1p 4
NOS(config-tmap-dot1p-map)# qos-group 5 dot1p 5
NOS(config-tmap-dot1p-map)# qos-group 6 dot1p 6
NOS(config-tmap-dot1p-map)# qos-group 7 dot1p 7
NOS(config-tmap-dot1p-map)# configure terminal
NOS(config)# class-map type network-qos pfc5
NOS(config-cmap-nqos)# match qos-group 5
NOS(config-cmap-nqos)# exit
NOS(config)# policy-map type network-qos policy5
NOS(config-pmap-network-qos)# class pfc5
NOS(config-pmap-c-nqos)# pause
NOS(config-pmap-c-nqos)# pfc-cos 5
NOS(config-pmap-c-nqos)# end
NOS#
NOS# configure terminal
NOS(config)# interface range ethernet 1/1/1,1/1/2,1/1/3
NOS(conf-range-eth1/1/1,1/1/2,1/1/3)# flowcontrol receive off
NOS(conf-range-eth1/1/1,1/1/2,1/1/3)# service-policy input type network-qos policy5
NOS(conf-range-eth1/1/1,1/1/2,1/1/3)# trust-map dot1p t1
NOS(conf-range-eth1/1/1,1/1/2,1/1/3)# priority-flow-control mode on
NOS(conf-range-eth1/1/1,1/1/2,1/1/3)# ets mode on
NOS(conf-range-eth1/1/1,1/1/2,1/1/3)# end

```

## LLFC 配置 — ToR 设备

您可以按如下所示配置 LLFC，而不是 PFC：

```

NOS# configure terminal
NOS(config)# class-map type network-qos llfc
NOS(config-cmap-nqos)# match qos-group 0-7
NOS(config-cmap-nqos)# exit
NOS(config)# policy-map type network-qos llfc
NOS(config-pmap-network-qos)# class llfc
NOS(config-pmap-c-nqos)# pause buffer-size 100 pause-threshold 50 resume-threshold 10
NOS(config-pmap-c-nqos)# end
NOS# configure terminal
NOS(config)# interface range ethernet 1/1/1,1/1/2,1/1/3
NOS(conf-range-eth1/1/1,1/1/2,1/1/3)# flowcontrol transmit on
NOS(conf-range-eth1/1/1,1/1/2,1/1/3)# flowcontrol receive on
NOS(conf-range-eth1/1/1,1/1/2,1/1/3)# service-policy input type network-qos llfc
NOS(conf-range-eth1/1/1,1/1/2,1/1/3)# end

```

## WRED/ECN 配置 — ToR 设备

```

NOS# configure terminal
NOS(config)# wred w1
NOS(config-wred)# random-detect ecn
NOS(config-wred)# random-detect color green minimum-threshold 100 maximum-threshold 500

```



```

drop-probability 100
NOS(config-wred)# random-detect color yellow minimum-threshold 100 maximum-threshold 500
drop-probability 100
NOS(config-wred)# random-detect color red minimum-threshold 100 maximum-threshold 500
drop-probability 100
NOS(config-wred)# exit
NOS(config)# class-map type queuing cq
NOS(config-cmap-queuing)# match queue 5
NOS(config-cmap-queuing)# exit
NOS(config)# policy-map type queuing pq
NOS(config-pmap-queuing)# class cq
NOS(config-pmap-c-que)# random-detect w1
NOS(config-pmap-c-que)# end
NOS# configure terminal
NOS(config)# interface range ethernet 1/1/1,1/1/2,1/1/3
NOS(config-range-eth1/1/1,1/1/2,1/1/3)# flowcontrol receive off
NOS(config-range-eth1/1/1,1/1/2,1/1/3)# priority-flow-control mode on
NOS(config-range-eth1/1/1,1/1/2,1/1/3)# ets mode on
NOS(config-range-eth1/1/1,1/1/2,1/1/3)# service-policy input type network-qos policy5
NOS(config-range-eth1/1/1,1/1/2,1/1/3)# service-policy output type queuing pq
NOS(config-range-eth1/1/1,1/1/2,1/1/3)# trust-map dot1p t1
NOS(config-range-eth1/1/1,1/1/2,1/1/3)# end

```

## 启用 DCBx — ToR 设备

```

OS10# configure terminal
OS10(config)# dcbx enable

```

## 缓冲区统计信息跟踪

OS10 提供了缓冲区统计信息跟踪 (BST) 功能，可观察交换机上的缓冲区使用情况，而不会影响性能。此功能将维护单独的计数器集以用于缓冲区使用情况核算：

- 入口优先级组
- 入口服务池
- 入口共享空间池
- 出口队列
- 出口服务池

您可以获取不同缓冲区对象的缓冲区统计信息的快照，例如与某个端口关联的所有入口优先级组的快照、绑定到某个端口的所有出口单播队列等。

您可以在全局级别启用 BST。OS10 将跟踪缓冲区利用率，并在一段时间内提供最大峰值统计信息值和受监控 BST 计数器的当前值。

在 SYSTEM-QOS 模式下使用 `buffer-statistics-tracking` 命令来启用 BST：

```

OS10# configure terminal
OS10(config)# configure system-qos
OS10(config-sys-qos)# buffer-statistics-tracking

```

## 清除计数器

您可以选择重置峰值缓冲区利用率值并确定新的峰值缓冲区利用率值。使用 `clear qos statistics type buffer-statistics-tracking` 命令可清除跟踪的值并刷新此计数器。

BST 会跟踪一段时间内的峰值缓冲区利用率。在任何给定的时间点，都会显示过去的峰值缓冲区使用情况。

例如，如果您在 BST 处启用了 T0 并使用 `show` 命令查看在时间 T1 的峰值缓冲区利用率值，则会显示 T0 和 T1 之间的峰值使用率。如果您在时间 T2 再次查看峰值缓冲区利用率，则会显示 T0 和 T2 之间的峰值使用率。但是，如果您在时间 T3 时使用 `clear qos statistics type buffer-statistics-tracking` 命令清除了该计数器并在时间 T4 时查看峰值缓冲区利用率，则会显示 T3 和 T4 之间的峰值使用率。

**注：**当 BST 处于启用状态时，如果您影响先或先映射配置的任何配置行更改（例如，移除类映射、将类映射添加到策略映射 [nqos]），请确保使用 `clear qos statistics type buffer-statistics-tracking` 命令清除缓冲区信息，以查看当前配置的峰值缓冲区利用率。

BST 的优势包括：

- 检测微爆发拥塞
- 监控缓冲区利用率和历史趋势
- 根据实时数据确定特定端口或队列上的入口或出口共享缓冲区以及余量的最佳大小和阈值

 **注:** S4248F-ON 平台上不支持 BST。

禁用 BST 后，请确保使用 `clear qos statistics type buffer-statistics-tracking` 命令清除计数器。

## 端口到端口管道和 MMU 映射

端口管道处理与一组前端 I/O 端口之间的网络流量。在 Z9100-ON, Z9264F-ON 和 MX9116n 平台上，接口在端口通道之间共享，端口通道在内存管理单元 (MMU) 之间共享。

由于接口跨端口通道，Dell EMC Networking 建议使用来自入口和出口的相同端口通道的接口，以实现最佳性能。要查找端口到端口通道和 MMU 映射，请使用 `show qos port-map details` 命令。

**Z9100-ON 输出示例：**

OS10# show qos port-map details

| Interface  | Port Pipe | Ingress MMU | Egress MMU | Oper Status |
|------------|-----------|-------------|------------|-------------|
| Eth 1/1/1  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/2  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/3  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/4  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/5  | 2         | 2, 3        | 1, 3       | up          |
| Eth 1/1/6  | 2         | 2, 3        | 1, 3       | up          |
| Eth 1/1/7  | 2         | 2, 3        | 1, 3       | up          |
| Eth 1/1/8  | 2         | 2, 3        | 1, 3       | up          |
| Eth 1/1/9  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/10 | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/11 | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/12 | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/13 | 2         | 2, 3        | 1, 3       | down        |
| Eth 1/1/14 | 2         | 2, 3        | 1, 3       | down        |
| Eth 1/1/15 | 2         | 2, 3        | 1, 3       | down        |
| Eth 1/1/16 | 2         | 2, 3        | 1, 3       | down        |
| Eth 1/1/17 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/18 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/19 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/20 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/21 | 0         | 0, 1        | 0, 2       | down        |
| Eth 1/1/22 | 0         | 0, 1        | 0, 2       | down        |

|            |   |      |      |      |
|------------|---|------|------|------|
| Eth 1/1/23 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/24 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/25 | 3 | 0, 1 | 1, 3 | up   |
| Eth 1/1/26 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/27 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/28 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/29 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/30 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/31 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/32 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/33 | 1 | 2, 3 | 0, 2 | up   |
| Eth 1/1/34 | 2 | 2, 3 | 1, 3 | up   |

查看单一接口的信息：

```
OS10# show qos port-map details interface ethernet 1/1/1
```

| Interface | Port Pipe | Ingress MMU | Egress MMU | Oper Status |
|-----------|-----------|-------------|------------|-------------|
| Eth 1/1/1 | 1         | 2, 3        | 0, 2       | up          |

**Z9264F-ON 输出示例：**

```
OS10# show qos port-map details
```

| Interface    | Port Pipe | Ingress MMU | Egress MMU | Oper Status |
|--------------|-----------|-------------|------------|-------------|
| Eth 1/1/1:1  | 0         | 0, 1        | 0, 2       | up          |
| Eth 1/1/3:1  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/3:2  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/3:3  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/3:4  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/5:1  | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/5:2  | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/5:3  | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/5:4  | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/7:1  | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/7:2  | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/7:3  | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/7:4  | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/9:1  | 0         | 0, 1        | 0, 2       | down        |
| Eth 1/1/9:2  | 0         | 0, 1        | 0, 2       | down        |
| Eth 1/1/9:3  | 0         | 0, 1        | 0, 2       | down        |
| Eth 1/1/9:4  | 0         | 0, 1        | 0, 2       | down        |
| Eth 1/1/11:1 | 0         | 0, 1        | 0, 2       | up          |
| Eth 1/1/11:2 | 0         | 0, 1        | 0, 2       | up          |
| Eth 1/1/11:3 | 0         | 0, 1        | 0, 2       | up          |
| Eth 1/1/11:4 | 0         | 0, 1        | 0, 2       | up          |
| Eth 1/1/13:1 | 0         | 0, 1        | 0, 2       | up          |
| Eth 1/1/13:2 | 0         | 0, 1        | 0, 2       | up          |
| Eth 1/1/13:3 | 0         | 0, 1        | 0, 2       | up          |
| Eth 1/1/13:4 | 0         | 0, 1        | 0, 2       | up          |
| Eth 1/1/15   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/16   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/17:1 | 2         | 2, 3        | 1, 3       | up          |
| Eth 1/1/19:1 | 3         | 0, 1        | 1, 3       | down        |

|              |   |      |      |      |
|--------------|---|------|------|------|
| Eth 1/1/19:2 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/19:3 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/19:4 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/21:1 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/21:2 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/21:3 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/21:4 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/23   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/24   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/25:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/25:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/25:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/25:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/27:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/27:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/27:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/27:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/29:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/29:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/29:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/29:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/31   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/32   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/33   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/34   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/35:1 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/35:2 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/35:3 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/35:4 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/37:1 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/37:2 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/37:3 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/37:4 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/39:1 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/39:2 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/39:3 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/39:4 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/41:1 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/41:2 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/41:3 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/41:4 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/43   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/44   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/45   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/46   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/47   | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/48   | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/49   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/50   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/51:1 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/51:2 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/51:3 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/51:4 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/53   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/54   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/55   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/56   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/57:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/57:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/57:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/57:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/59   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/60   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/61   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/62   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/63   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/64   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/65   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/66   | 1 | 2, 3 | 0, 2 | down |

查看单一接口的信息：

```
OS10# show qos port-map details interface ethernet 1/1/1
```

| Interface   | Port Pipe | Ingress MMU | Egress MMU | Oper Status |
|-------------|-----------|-------------|------------|-------------|
| Eth 1/1/1:1 | 0         | 0, 1        | 0, 2       | up          |

**MX9116n 输出示例：**

```
OS10# show qos port-map details
```

| Interface    | Port Pipe | Ingress MMU | Egress MMU | Oper Status |
|--------------|-----------|-------------|------------|-------------|
| Eth 1/1/1    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/2    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/3    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/4    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/5    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/6    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/7    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/8    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/9    | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/10   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/11   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/12   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/13   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/14   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/15   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/16   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/17:1 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/17:2 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/17:3 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/17:4 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/18:1 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/18:2 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/18:3 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/18:4 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/19:1 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/19:2 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/19:3 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/19:4 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/20:1 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/20:2 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/20:3 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/20:4 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/21:1 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/21:2 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/21:3 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/21:4 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/22:1 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/22:2 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/22:3 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/22:4 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/23:1 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/23:2 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/23:3 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/23:4 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/24:1 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/24:2 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/24:3 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/24:4 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/25:1 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/25:2 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/25:3 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/25:4 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/26:1 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/26:2 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/26:3 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/26:4 | 1         | 2, 3        | 0, 2       | down        |

|              |   |      |      |      |
|--------------|---|------|------|------|
| Eth 1/1/27:1 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/27:2 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/27:3 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/27:4 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/28:1 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/28:2 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/28:3 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/28:4 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/29:1 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/29:2 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/29:3 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/29:4 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/30:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/30:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/30:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/30:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/31:1 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/31:2 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/31:3 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/31:4 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/32:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/32:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/32:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/32:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/33:1 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/33:2 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/33:3 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/33:4 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/34:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/34:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/34:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/34:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/35   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/36   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/37   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/38   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/39   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/40   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/41:1 | 2 | 2, 3 | 1, 3 | up   |
| Eth 1/1/41:2 | 2 | 2, 3 | 1, 3 | up   |
| Eth 1/1/41:3 | 2 | 2, 3 | 1, 3 | up   |
| Eth 1/1/41:4 | 2 | 2, 3 | 1, 3 | up   |
| Eth 1/1/42:1 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/42:2 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/42:3 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/42:4 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/43:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/43:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/43:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/43:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/44:1 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/44:2 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/44:3 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/44:4 | 0 | 0, 1 | 0, 2 | up   |

查看单一接口的信息：

| OS10# show qos port-map details interface ethernet 1/1/1 |           |             |            |             |
|----------------------------------------------------------|-----------|-------------|------------|-------------|
| Interface                                                | Port Pipe | Ingress MMU | Egress MMU | Oper Status |
| Eth 1/1/1                                                | 3         | 0, 1        | 1, 3       | down        |

# QoS 命令

## bandwidth

为队列分配权重百分比。

|        |                                                       |
|--------|-------------------------------------------------------|
| 语法     | <code>bandwidth percent value</code>                  |
| 参数     | <code>percent value</code> — 输入到队列的带宽分配百分比，从 1 到 100。 |
| 默认     | 未配置                                                   |
| 命令模式   | POLICY-MAP CLASS-MAP                                  |
| 使用情况信息 | 如果配置此命令，则不能将 <code>priority</code> 命令用于类。             |

示例

```
OS10(config-pmap-c-que)# bandwidth percent 70
```

支持的版本 10.2.0E or later

## buffer-statistics-tracking

全局启用或禁用缓冲区统计信息跟踪功能。

|        |                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>buffer-statistics-tracking</code>                                                                                          |
| 参数     | 无                                                                                                                                |
| 默认     | 已禁用                                                                                                                              |
| 命令模式   | SYSTEM-QOS                                                                                                                       |
| 使用情况信息 | 命令的 <code>no</code> 形式将全局禁用缓冲区统计信息跟踪功能。禁用 BST 后，请确保使用 <code>clear qos statistics type buffer-statistics-tracking</code> 命令清除计数器。 |

示例

```
OS10# configure terminal
OS10(config)# system qos
OS10(config-sys-qos)# buffer-statistics-tracking
```

支持的版本 10.4.3.0 or later

## class

为策略映射类型创建 QoS 类别。

|        |                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>class class-name</code>                                                                                                                                                |
| 参数     | <code>class-name</code> — 输入类别映射的名称。最多 32 个字符。                                                                                                                               |
| 默认     | 未配置                                                                                                                                                                          |
| 命令模式   | POLICY-MAP-QUEUEING<br>POLICY-MAP-QOS<br>POLICY-MAP-NQOS<br>POLICY-MAP-CP<br>POLICY-MAP-APPLICATION                                                                          |
| 使用情况信息 | 如果在策略映射下定义了类别映射，则 <code>qos</code> 、 <code>queuing</code> 或 <code>control-plane</code> 类型与策略映射相同。您必须提前创建此映射。唯一的例外情况是策略映射类型为 <code>trust</code> ，其中的类类型必须为 <code>qos</code> 。 |

|       |                                           |
|-------|-------------------------------------------|
| 示例    | <pre>OS10 (conf-pmap-qos)# class c1</pre> |
| 支持的版本 | 10.2.0E or later                          |

## class-map

创建筛选流量的 QoS 类别映射，以匹配数据包与为网络创建的相应策略。

|        |                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <pre>class-map [type {qos   queuing   control-plane}] [{match-any   match-all}]<br/>class-map-name</pre>                                                                                                                                                                                                                                                                         |
| 参数     | <ul style="list-style-type: none"><li>type — 输入类别映射类型。</li><li>qos — 输入 qos 类型类别映射。</li><li>queuing — 输入 queueing 类型类别映射。</li><li>control-plane — 输入 control-plane 类型类别映射。</li><li>match-all — 确定当存在多个匹配条件时如何评估数据包。输入关键字以确定所有数据包都必须符合要分配给类别的匹配条件。</li><li>match-any — 确定当存在多个匹配条件时如何评估数据包。输入关键字以确定数据包必须满足至少一个要分配给类别的匹配条件。</li><li>class-map-name — 输入类别映射名称。最多 32 个字符。</li></ul> |
| 默认     | <ul style="list-style-type: none"><li>qos — 类别映射类型</li><li>match-any — 类别映射筛选器</li></ul>                                                                                                                                                                                                                                                                                         |
| 命令模式   | CLASS-MAP-QOS                                                                                                                                                                                                                                                                                                                                                                    |
| 使用情况信息 | 向 control-plane、qos 和 queuing 类型类别映射应用 match-any 或 match-all                                                                                                                                                                                                                                                                                                                     |
| 示例     | <pre>OS10 (config)# class-map type qos match-all c1<br/>OS10 (conf-cmap-qos)#</pre>                                                                                                                                                                                                                                                                                              |
| 命令历史记录 | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                 |

## clear qos statistics

清除系统中的所有 QoS 相关统计信息，包括 PFC 计数器。

|        |                                       |
|--------|---------------------------------------|
| 语法     | <pre>clear qos statistics</pre>       |
| 参数     | 无                                     |
| 默认     | 未配置                                   |
| 命令模式   | EXEC                                  |
| 使用情况信息 | 无                                     |
| 示例     | <pre>OS10# clear qos statistics</pre> |
| 支持的版本  | 10.2.0E or later                      |

## clear qos statistics type

清除所有队列计数器，包括 PFC，用于控制平面、qos 和队列。

|    |                                                                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <pre>clear qos statistics type {{qos   queuing   control-plane   buffer-<br/>statistics-tracking} [interface ethernet node/slot/port[:subport]]}</pre> |
| 参数 | <ul style="list-style-type: none"><li>qos — 清除 qos 类型统计信息。</li><li>queuing — 清除 queueing 类型统计信息。</li></ul>                                             |



- `control-plane` — 清除 `control-plane` 类型统计信息。
- `buffer-statistics-tracking` — 清除所有接口和服务池上的峰值缓冲区使用情况计数统计信息。  
 **注:** 此命令不会清除 Z9100-ON 平台上的入口服务池统计信息。
- `interface ethernet node-id/slot/port-id [:subport]` — 清除为 `qos`、`queuing` 或 `control-plane` 配置的以太网接口的 QoS 统计信息。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# clear qos statistics type qos interface ethernet 1/1/5
```

**示例（控制平面）**

```
OS10# clear qos statistics type control-plane interface ethernet 1/1/7
```

**示例（队列）**

```
OS10# clear qos statistics type queuing interface ethernet 1/1/2
```

**示例（BST）**

```
OS10# clear qos statistics type buffer-statistics-tracking
```

**支持的版本** 10.2.0E or later

## control-plane

进入 CONTROL-PLANE 模式。

**语法** `control-plane`

**参数** 无

**默认** 未配置

**命令模式** CONTROL-PLANE

**使用情况信息** 如果将访问列表附加到控制板的 `class-map` 类型，则访问列表会忽略 `permit` 和 `deny` 关键字。

**示例（类别映射）**

```
OS10(config)# class-map type control-plane c1
OS10(config-cmap-control-plane)#
```

**示例（策略映射）**

```
OS10(config)# policy-map type control-plane p1
OS10(config-pmap-control-plane)#
```

**支持的版本** 10.2.0E or later

## control-plane-buffer-size

配置 CPU 池的缓冲区大小。

**语法** `control-plane-buffer-size size-of-buffer-pool`

**参数** `size-of-buffer-pool`— 输入缓冲区大小（以 KB 为单位），从 620 KB 到 900 KB。

**默认** 无

**命令模式** SYSTEM-QOS

**使用情况信息** 此命令将配置 CPU 池的缓冲区大小。系统将从总系统缓冲区分配 CPU 池的缓冲区大小。将为每个 CPU 队列分配最小保证缓冲区，其余部分可用于共享用途。缓冲池的大小因每个队列的 CPU 队列和缓冲区使

用情况而异，但不能少于为每个 CPU 队列分配的最小保证缓冲区数。此命令的 `no` 版本将移除为 CPU 池配置的缓冲区大小，并将缓冲区大小恢复为默认值 620 KB。

#### 示例

```
OS10(config-sys-qos)# control-plane-buffer-size 900
```

#### 支持的版本

10.4.2.0 和更高版本

## flowcontrol

启用或禁用接口上的链路级流控制。

#### 语法

```
flowcontrol [receive | transmit] [on | off]
```

#### 参数

- `receive` — (可选) 指示端口可从远程设备接收流控制数据包。
- `transmit` — (可选) 指示本地端口可将流控制数据包发送到远程设备。
- `on` — (可选) 与 `receive` 配合使用时，允许本地端口接收流控制流量。与 `transmit` 配合使用时，允许本地端口向远程设备发送流控制流量。
- `off` — (可选) 与 `receive` 配合使用时，将禁止远程设备将流控制流量发送到本地端口。与 `transmit` 配合使用时，将禁止本地端口将流控制流量发送到远程设备。

#### 默认

已禁用 (`off`)

#### 命令模式

INTERFACE

#### 使用情况信息

此命令的 `no` 版本将值恢复为默认值。

#### 示例

```
OS10(conf-if-eth1/1/2)# flowcontrol transmit on
```

#### 支持的版本

10.3.0E or later

## hardware deep-buffer-mode

配置深度缓冲区模式。

#### 语法

```
hardware deep-buffer-mode
```

#### 参数

无

#### 默认

已禁用

#### 命令模式

CONFIGURATION

#### 使用情况信息

仅适用于 S4200-ON 系列交换机。深度缓冲区模式配置仅在将其保存在启动配置中并重新引导交换机后才会生效。此命令的 `no` 版本将禁用深度缓冲区模式。

#### 示例

```
OS10(config)# hardware deep-buffer-mode
```

#### 支持的版本

10.4.3.0 or later

## match

配置 QoS 策略的匹配条件。

#### 语法

```
match {cos cos-number | ip [access-group name name | dscp dscp-value [ecn ecn-value] | precedence value] | ip-any [dscp dscp-value [ecn ecn-value] | precedence value] | ipv6 [access-group name name | dscp dscp-value [ecn ecn-value] | precedence value] | mac access-group acl-name | not [cos | ip | ip-any | ipv6] | vlan vlan-id |}
```

#### 参数

- `cos cos-number` — 为 CoS 匹配条件输入队列编号，从 0 到 7。
- `ip` — 输入 IPv4 匹配条件。

- `access-group name name` — (可选) 输入 IPv4 访问组名称。
- `dscp dscp-value` — (可选) 输入适用于 L3 DSCP 匹配条件的 DSCP 值, 0 到 63。
- `ecn ecn-value` — (可选) 输入 ECN 位匹配条件的 ECN 值, 从 0 到 3。
- `precedence value` — (可选) 输入 L3 优先级匹配条件的优先级值, 从 0 到 7。
- `ip-any` — 输入 IPv4 或 IPv6 匹配条件。
- `dscp dscp-value` — (可选) 输入适用于 L3 DSCP 匹配条件的 DSCP 值, 0 到 63。
- `ecn ecn-value` — (可选) 输入 ECN 位匹配条件的 ECN 值, 从 0 到 3。
- `precedence value` — (可选) 输入 L3 优先级匹配条件的优先级值, 从 0 到 7。
- `ipv6` — 输入 IPv6 匹配条件。
- `access-group name name` — (可选) 输入 IPv6 访问组名称。
- `dscp dscp-value` — (可选) 为 L3 DSCP 匹配条件配置 DSCP 值, 从 0 到 63。
- `ecn ecn-value` — (可选) 输入 ECN 位匹配条件的 ECN 值, 从 0 到 3。
- `mac access-group name name` — 输入 MAC 访问列表匹配条件的访问组名称。最多 140 个字符。
- `dscp dscp-value` — 输入用于标记 DSCP 数据包的 DSCP 值, 从 0 到 63。
- `not` — 输入要否定匹配条件的 IP 或 CoS。
- `vlan vlan-id` — 为 VLAN 匹配条件输入 VLAN 数量, 从 1 到 4093。

**默认** 未配置

**命令模式** CLASS-MAP

**使用情况信息** 在 `match-any` 类别中, 您可以输入多个匹配条件。在 `match-all` 类别中, 如果匹配案例为 `access-group`, 则不允许使用其他匹配条件。如果将访问列表附加到 `class-map type control-plane` 或 `qos`, 则访问列表 (IPv4、IPv6) 会忽略 `permit` 和 `deny` 关键字。

**示例 1**

```
OS10(conf-cmap-qos)# match ip access-group name ag1
OS10(config-cmap-qos)# match ipv6 access-group name ACLv6
```

**支持的版本** 10.2.0E or later

## match cos

将服务成本 (CoS) 值与 L2 dot1p 数据包相匹配。

**语法** `match [not] cos cos-value`

**参数**

- `cos-value` — 输入一个 CoS 值, 从 0 到 7。
- `not` — 输入 `not` 以取消匹配条件。

**默认** 未配置

**命令模式** CLASS-MAP

**使用情况信息** 您不能具有使用相同的筛选器类型的两个匹配语句。如果输入两个匹配语句的筛选器类型相同, 则第二个语句将覆盖第一个语句。

**示例**

```
OS10(conf-cmap-qos)# match cos 3
```

**支持的版本** 10.2.0E or later

## match dscp

将 DSCP 值配置为类别映射的匹配条件。

**语法** `match [not] {ip | ipv6 | ip-any } dscp [dscp-value] [ecn ecn-value]`

**参数**

- `not` — (可选) 输入以取消之前应用的匹配条件。
- `ip` — 输入以使用 IPv4 作为匹配协议。
- `ipv6` — 输入以使用 IPv6 作为匹配协议。

- `ip-any` — 输入以同时使用 IPv4 和 IPv6 作为匹配协议。
- `dscp dscp-value` — 以单个数字、逗号分隔或带连字符的范围输入 DSCP 值，从 0 到 63。
- `ecn ecn-value` — (可选) 输入 ECN 位匹配条件的 ECN 值，从 0 到 3。

|        |                                                                                                                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | 未配置                                                                                                                                                                                                                                                     |
| 命令模式   | CLASS-MAP                                                                                                                                                                                                                                               |
| 使用情况信息 | 您不能使用相同的筛选器类型输入两个匹配语句。如果输入两个匹配语句的筛选器类型相同，则第二个语句将覆盖第一个语句。类别映射中的 <code>match-all</code> 选项不支持 <code>ip-any</code> 。选择 <code>ip</code> 或 <code>IPv6</code> 用于 <code>match-all</code> 条件。如果您选择了 <code>ip-any</code> ，则不能选择 <code>ip ipv6</code> 用于相同的筛选器类型。 |
| 示例     | <pre>OS10(conf-cmap-qos)# match ip-any dscp 17-20</pre>                                                                                                                                                                                                 |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                        |

## match precedence

将 IP 优先级值配置为匹配条件。

|        |                                                                                                                                                                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>match [not] {ip   ipv6   ip-any} precedence precedence-list</code>                                                                                                                                                                                                                                                                 |
| 参数     | <ul style="list-style-type: none"> <li>• <code>not</code> — 输入以取消之前应用的匹配优先级规则。</li> <li>• <code>ip</code> — 输入以使用 IPv4 作为匹配优先级规则。</li> <li>• <code>ipv6</code> — 输入以使用 IPv6 作为匹配优先级规则。</li> <li>• <code>ip-any</code> — 输入以同时使用 IPv4 和 IPv6 作为匹配优先级规则。</li> <li>• <code>precedence precedence-list</code> — 输入优先级列表值，从 0 到 7。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                      |
| 命令模式   | CLASS-MAP                                                                                                                                                                                                                                                                                                                                |
| 使用情况信息 | 您不能使用相同的筛选器类型输入两个匹配语句。如果输入两个匹配语句的筛选器类型相同，则第二个语句将覆盖第一个语句。                                                                                                                                                                                                                                                                                 |
| 示例     | <pre>OS10(conf-cmap-qos)# match not ipv6 precedence 3</pre>                                                                                                                                                                                                                                                                              |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                         |

## 匹配队列

为队列配置匹配条件。

|        |                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------|
| 语法     | <code>match queue queue-number</code>                                                              |
| 参数     | <code>queue-number</code> — 输入队列编号，从 0 到 7。                                                        |
| 默认     | 未配置                                                                                                |
| 命令模式   | CLASS-MAP                                                                                          |
| 使用情况信息 | 只有当类别映射类型为 <code>queuing</code> 时，才能配置此命令。您不能使用相同的筛选器类型输入两个匹配语句。如果输入两个匹配语句的筛选器类型相同，则第二个语句将覆盖第一个语句。 |
| 示例     | <pre>OS10(conf-cmap-queuing)# match queue 1</pre>                                                  |
| 支持的版本  | 10.2.0E or later                                                                                   |

## match vlan

根据 VLAN ID 号配置匹配条件。

|        |                                                          |
|--------|----------------------------------------------------------|
| 语法     | <code>match vlan <i>vlan-id</i></code>                   |
| 参数     | <i>vlan-id</i> — 输入 VLAN ID 号，从 1 到 4093。                |
| 默认     | 未配置                                                      |
| 命令模式   | CLASS-MAP                                                |
| 使用情况信息 | 您不能使用相同的筛选器类型输入两个匹配语句。如果输入两个匹配语句的筛选器类型相同，则第二个语句将覆盖第一个语句。 |
| 示例     | <pre>OS10(conf-cmap-qos)# match vlan 100</pre>           |
| 支持的版本  | 10.2.0E or later                                         |

## mtu

计算匹配流的缓冲区大小分配。

|        |                                             |
|--------|---------------------------------------------|
| 语法     | <code>mtu <i>size</i></code>                |
| 参数     | <i>size</i> — 输入缓冲区的大小（1500 到 9216）。        |
| 默认     | 9216                                        |
| 命令模式   | POLICY-MAP-CLASS-MAP                        |
| 使用情况信息 | 此命令的 <code>no</code> 版本将值恢复为默认值。            |
| 示例     | <pre>OS10(conf-pmap-nqos-c)# mtu 2500</pre> |
| 支持的版本  | 10.3.0E or later                            |

## pause

启用基于端口的缓冲区限制的暂停，以启动或停止与对等节点的通信。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>pause [buffer-size <i>size</i> pause-threshold <i>xoff-size</i> resume-threshold <i>xon-size</i>]</code>                                                                                                                                                                                                                                                                                                         |
| 参数     | <ul style="list-style-type: none"><li><code>buffer-size <i>size</i></code> — （可选）输入用作保证缓冲区的入口缓冲区大小（以 KB 为单位）默认值：10G-45KB、40G-93KB。</li><li><code>pause-threshold <i>xoff-size</i></code> — （可选）输入端口向对等节点启动或发起 <code>pause</code> 的缓冲区限制（以 KB 为单位），默认值：10G-9KB、40G-18KB。</li><li><code>resume-threshold <i>xon-size</i></code> — （可选）输入端口向对等节点停止或取消 <code>pause</code> 的缓冲区限制（以 KB 为单位）（默认值 10G-9KB、40G-9KB）。</li></ul> |
| 默认     | 请参阅参数值                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 命令模式   | POLICY-MAP-CLASS-MAP                                                                                                                                                                                                                                                                                                                                                                                                   |
| 使用情况信息 | 仅在 <code>network-qos</code> 策略类型下使用此命令。缓冲区大小、暂停阈值和恢复阈值因平台而异。将具有 <code>pause</code> 的策略映射添加到系统 <code>qos</code> 以服务要在所有端口上启用 <code>pause</code> 的输入，具体取决于按端口链路级别流控制或优先级流控制启用模式。链路级别流控制的 <code>xoff</code> 和 <code>xon</code> 阈值设置适用于所有流量类别都必须映射到单个 PG 的端口。特定于平台的默认值基于 9216 的 MTU 大小和 100 米的线缆长度。此命令的 <code>no</code> 版本将值恢复为默认值。                                                                                        |
| 示例     | <pre>OS10(conf-pmap-c-nqos)# pause buffer-size 45 pause-threshold 25 resume-threshold 10</pre>                                                                                                                                                                                                                                                                                                                         |

### 示例（全局和共享缓冲区）

```
OS10(config)# policy-map type network-qos nqGlobalpolicy1
OS10(conf-cmap-nqos)# class CLASS-NAME
OS10(conf-cmap-nqos-c)# pause buffer-size 45 pause-threshold 30 resume-threshold 30
```

```
OS10(config)# policy-map type network-qos nqGlobalpolicy1
OS10(conf-cmap-nqos)# class type network-qos nqclass1
OS10(conf-cmap-nqos-c)# pause buffer-size 45 pause-threshold 30 resume-threshold 10
```

**支持的版本** 10.3.0E or later

## pfc-cos

为服务成本 (CoS) 配置优先级流控制。

**语法** `pfc-cos cos-value`

**参数** `cos-value` — 为要启用的优先级流控制输入一个逗号分隔或带字符的 CoS 值范围，从 0 到 7。

 **注：**范围 0-7 无效。所有其他范围（包括 0-6 和 1-7）均有效。

**默认** 未配置

**命令模式** POLICY-MAP-CLASS-MAP

**使用情况信息** 要配置链路级别流控制，请不要为此策略的匹配类配置 `pfc-cos`。将具有 `pfc-cos` 配置的策略映射添加到 `system-qos`，以在输入时提供服务，以在所有端口上启用优先级流控制行为，具体取决于每个端口的优先级流控制启用模式。将具有 `pfc-cos` 配置的策略映射添加到接口配置，以在输入时提供服务，并根据端口的优先级流控制启用模式在该特定端口上启用优先级流控制。如果在接口上将 40G 配置为 10G 模式并且在 `system-qos` 上已启用 `pause`（无丢弃），则所有队列可能或不会根据缓冲区的可用性丢弃流量。此命令的 `no` 版本将值恢复为默认值。

### 示例

```
OS10(conf-pmap-c-nqos)# pfc-cos 0-2
```

### 示例（全局缓冲区/共享缓冲区）

```
OS10(config)# policy-map type network-qos nqGlobalpolicy1
OS10(conf-cmap-nqos)# class CLASS-NAME
OS10(conf-cmap-nqos-c)# pause buffer-size 45 pause-threshold 25 resume-threshold 10
OS10(conf-cmap-nqos-c)# pfc-cos 0-2
OS10(conf-cmap-nqos-c)# queue-limit 140
```

**支持的版本** 10.3.0E or later

## pfc-max-buffer-size

配置启用了优先级流控制的流的最大缓冲区大小。

**语法** `pfc-max-buffer-size max-buffer-size`

**参数** `max-buffer-size` — 输入最大缓冲区大小（以 KB 为单位）。

**默认** 无

**命令模式** SYSTEM-QOS

**使用情况信息** 此命令可配置无损缓冲池的最大大小。此命令的 `no` 版本将移除最大缓冲区大小限制。

### 示例

```
OS10(config-sys-qos)# pfc-max-buffer-size 2000
```

**支持的版本** 10.4.0E(R1) or later

## pfc-shared-buffer-size

更改已启用优先级流控制的流的共享缓冲区大小限制。

|        |                                                                 |
|--------|-----------------------------------------------------------------|
| 语法     | <code>pfc-shared-buffer-size buffer-size</code>                 |
| 参数     | <code>buffer-size</code> — 输入优先级流控制缓冲区的大小（以 KB 为单位），从 0 到 8911。 |
| 默认     | 832 KB                                                          |
| 命令模式   | SYSTEM-QOS                                                      |
| 使用情况信息 | 此命令的 <code>no</code> 版本将值恢复为默认值。                                |
| 示例     | <pre>OS10(conf-sys-qos)# pfc-shared-buffer-size 2000</pre>      |
| 支持的版本  | 10.3.0E or later                                                |

## pfc-shared-headroom-buffer-size

在暂停帧生成后为减震数据包配置共享的余量大小。

 **注：** 此命令仅在以下平台上可用：

- S5212F-ON、S5224F-ON、S5232F-ON、S5248F-ON、S5296F-ON
- Z9100-ON
- Z9264F-ON

|        |                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>pfc-shared-headroom-buffer-size headroom-buffer-size</code>                                                                            |
| 参数     | <code>headroom-buffer-size</code> — 输入优先级流控制余量缓冲区的大小（以 KB 为单位），从 1 到 3399。                                                                   |
| 默认     | 1024 KB                                                                                                                                      |
| 命令模式   | SYSTEM-QOS                                                                                                                                   |
| 使用情况信息 | 所有已启用 PFC 的优先级组都可以使用共享的余量空间。余量是在 PFC 帧到达发送方之后可传入数据包的缓冲区空间。达到阈值后，PFC 帧将向发送方生成。在 PFC 帧生成后发送者发送的数据包将被吸收到余量缓冲区中。此命令的 <code>no</code> 版本将值恢复为默认值。 |
| 示例     | <pre>OS10(conf-sys-qos)# pfc-shared-headroom-buffer-size 2000</pre>                                                                          |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                         |

## police

配置针对传入流量的流量监察。

|      |                                                                                                                                                                                                                                                                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | <code>police {cir committed-rate [bc committed-burst-size]} {pir peak-rate [be peak-burst-size]}</code>                                                                                                                                                                                                                                                                                     |
| 参数   | <ul style="list-style-type: none"><li>• <code>cir committed-rate</code> — 输入提交的速率值（以 kb/秒为单位），从 0 到 4000000。</li><li>• <code>bc committed-burst-size</code> — （可选）在用于控制平面监察的数据包中输入提交的脉冲大小（对于数据包以 KB 为单位），从 16 到 200000。</li><li>• <code>pir peak-rate</code> — 输入峰值速率值（以每秒千位为单位），从 0 到 40000000。</li><li>• <code>be peak-burst-size</code> — （可选）输入峰值脉冲大小（以千字节为单位），从 16 到 200000。</li></ul> |
| 默认   | <ul style="list-style-type: none"><li>• <code>bc committed-burst-size</code> 对于 control plane，值为 200 KB；对于所有其他类别映射类型，值为 100 KB</li><li>• <code>be peak-burst-size</code> 对于 control plane，值为 200 KB；对于所有其他类别映射类型，值为 100 KB</li></ul>                                                                                                                                                        |
| 命令模式 | POLICY-MAP-CLASS-MAP                                                                                                                                                                                                                                                                                                                                                                        |

|        |                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------|
| 使用情况信息 | 如果不提供峰值速率 <code>pir</code> 值，则提交的速率 <code>cir</code> 值将作为 <code>pir</code> 值。只有入口 QoS 策略类型支持此命令。对于控制平面监察，速率值以 pps 为单位。 |
| 示例     | <pre>OS10(config-pmap-c-qos)# police cir 5 bc 30 pir 20 be 40</pre>                                                    |
| 支持的版本  | 10.2.0E or later                                                                                                       |

## policy-map

进入 QoS POLICY-MAP 模式，并创建或修改 QoS 策略映射。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>policy-map policy-map-name [type {qos   queuing   control-plane   application   network-qos }]</code>                                                                                                                                                                                                                                                                                                                                                        |
| 参数     | <ul style="list-style-type: none"><li><code>policy-map-name</code> — 输入策略映射的类别名称。最多 32 个字符。</li><li><code>type</code> — 输入策略-映射类型。<ul style="list-style-type: none"><li><code>qos</code> — 创建 qos 策略映射类型。</li><li><code>queuing</code> — 创建 queueing 策略映射类型。</li><li><code>control-plane</code> — 创建 control-plane 策略映射类型。</li><li><code>application</code> — 创建 application 策略映射类型。</li><li><code>network-qos</code> — 创建 network-qos 策略映射类型。</li></ul></li></ul> |
| 默认     | <code>qos = class-map type and match-any = class-map filter</code>                                                                                                                                                                                                                                                                                                                                                                                                 |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 使用情况信息 | 此命令的 <code>no</code> 版本将删除策略映射。                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 示例     | <pre>OS10(config)# policy-map p1</pre>                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 示例（队列） | <pre>OS10(config)# policy-map type queuing p1</pre>                                                                                                                                                                                                                                                                                                                                                                                                                |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## priority

将计划程序设置为严格优先级。

|        |                                              |
|--------|----------------------------------------------|
| 语法     | <code>priority</code>                        |
| 参数     | 无                                            |
| 默认     | WDRR — 当提到优先级时，它会移动到具有默认级别 1 的 SP。           |
| 命令模式   | POLICY-MAP-CLASS-MAP                         |
| 使用情况信息 | 如果使用此命令，则不允许带宽。只有出口 QoS 策略类型支持此命令。           |
| 示例     | <pre>OS10(config-pmap-c-que)# priority</pre> |
| 支持的版本  | 10.2.0E or later                             |

## priority-flow-control mode

启用或禁用接口上的优先级流控制模式。

|    |                                                                                   |
|----|-----------------------------------------------------------------------------------|
| 语法 | <code>priority-flow-control mode [on]</code>                                      |
| 参数 | <ul style="list-style-type: none"><li><code>on</code> — （可选）启用优先级流控制模式。</li></ul> |



|        |                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | 已禁用                                                                                                                                                                        |
| 命令模式   | INTERFACE                                                                                                                                                                  |
| 使用情况信息 | 在接口上启用优先级流控制之前，请验证匹配 <code>network-qos</code> 的类型策略是否已为接口配置 <code>pfc-cos</code> 值。如果不使用接口的 <code>network-qos</code> 类型策略，则使用此命令可禁用优先级流控制。此命令的 <code>no</code> 版本将值恢复为默认值。 |
| 示例     | <pre>OS10(conf-if-eth1/1/2)# priority-flow-control mode on</pre>                                                                                                           |
| 支持的版本  | 10.3.0E or later                                                                                                                                                           |

## qos-group dot1p

配置 dot1p 信任映射到流量类别。

|        |                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>qos-group tc-list [dot1p values]</code>                                                                                                                                           |
| 参数     | <ul style="list-style-type: none"> <li><code>qos-group tc-list</code> — 输入流量单值类别 ID，从 0 到 7。</li> <li><code>dot1p values</code> — (可选) 输入单个、逗号分隔的或者带有连字符的 dot1p 值范围，从 0 到 7。</li> </ul> |
| 默认     | 0                                                                                                                                                                                       |
| 命令模式   | TRUST-MAP                                                                                                                                                                               |
| 使用情况信息 | 如果信任映射未将 dot1p 值定义给任何流量类别，这些流将映射到默认流量类别 0。如果某些 dot1p 值已映射到现有流量类别，您将看到错误。对于启用了 PFC 的 CoS 值，您必须具有 1:1 的 dot1p 到流量类别映射。您还必须具有使用 DCB 的所有接口的通用 dot1p 信任映射。此命令的 <code>no</code> 版本将值恢复为默认值。   |
| 示例     | <pre>OS10(conf-tmap-dot1p-qos)# qos-group 5 dot1p 5</pre>                                                                                                                               |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                        |

## qos-group dscp

配置到流量类别的 DSCP 信任映射。

|        |                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>qos-group tc-list [dscp values]</code>                                                                                                                                          |
| 参数     | <ul style="list-style-type: none"> <li><code>qos-group tc-list</code> — 输入流量单值类别 ID，从 0 到 7。</li> <li><code>dscp values</code> — (可选) 输入单个、逗号分隔或者带有连字符的 DSCP 值范围，从 0 到 63。</li> </ul> |
| 默认     | 0                                                                                                                                                                                     |
| 命令模式   | TRUST-MAP                                                                                                                                                                             |
| 使用情况信息 | 如果信任映射未将 DSCP 值定义给任何流量类别，这些流将映射到默认流量类别 0。如果某些 DSCP 值已映射到现有流量类别，您将看到错误。此命令的 <code>no</code> 版本将值恢复为默认值。                                                                                |
| 示例     | <pre>OS10(conf-tmap-dscp-qos)# qos-group 5 dscp 42</pre>                                                                                                                              |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                      |

## qos-map traffic-class

为队列映射创建用户定义的信任映射。

|    |                                                |
|----|------------------------------------------------|
| 语法 | <code>qos-map traffic-class map-name</code>    |
| 参数 | <code>map-name</code> — 输入队列信任映射的名称。最多 32 个字符。 |
| 默认 | 未配置                                            |

|        |                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 命令模式   | CONFIGURATION                                                                                                                                                                                                   |
| 使用情况信息 | 如果应用于接口或系统级别，则流量类别会将所有流量路由到映射队列。此命令的 <code>no</code> 版本将值恢复为默认值。                                                                                                                                                |
| 示例     | <pre> OS10(config)# qos-map traffic-class queue-map1 OS10(config-qos-map)# queue 1 qos-group 5 OS10(config-qos-map)# queue 2 qos-group 6 OS10(config-qos-map)# queue 3 qos-group 7 OS10(config-qos-map)# </pre> |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                |

## qos-rate-adjust

配置要添加到每个帧的额外字段的数据字节数以用于速率计算。

|        |                                                                             |
|--------|-----------------------------------------------------------------------------|
| 语法     | <code>qos-rate-adjust [value-of-adjust]</code>                              |
| 参数     | <code>value-of-adjust</code> — 要添加到每个帧中的额外字段的字节数，从 1 到 31。                  |
| 默认     | 0                                                                           |
| 命令模式   | CONFIGURATION                                                               |
| 使用情况信息 | 此命令的 <code>no</code> 形式将移除速率调整配置，并且与使用 <code>qos-rate-adjust 0</code> 命令相同。 |
| 示例     | <pre> OS10(config)# qos-rate-adjust 10 </pre>                               |
| 支持的版本  | 10.4.3.0 or later                                                           |

## queue-limit

配置静态或动态共享缓冲区阈值。

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>queue-limit {queue-len value   thresh-mode [dynamic threshold-alpha-value   static threshold-value]}</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 参数 | <ul style="list-style-type: none"> <li><code>queue-len value</code> — 为队列输入可保证的大小（从 0 到 8911）。 <ul style="list-style-type: none"> <li>45 KB (10G)/111 KB (40G) — 如果队列已启用优先级流控制</li> <li>2 KB (10G)/8 KB (40G) — 如果队列是有损/链路级别流控制</li> <li>如果这是一个优先级流控制队列，则此配置无效</li> <li>仅支持 POLICY-MAP-CLASS-MAP (<code>pmap-c-queue</code>) 模式</li> </ul> </li> <li><code>thresh-mode</code> — （可选）缓冲区阈值模式。</li> <li><code>dynamic thresh-alpha-value</code> — （可选）输入值索引可将共享阈值计算为启用的动态共享缓冲区阈值，从 0 到 10。默认值： <ul style="list-style-type: none"> <li>0 = 1/128</li> <li>1 = 1/64</li> <li>2 = 1/32</li> <li>3 = 1/16</li> <li>4 = 1/8</li> <li>5 = 1/4</li> <li>6 = 1/2</li> <li>7 = 1</li> <li>8 = 2</li> <li>9 = 4</li> <li>10 = 8</li> </ul> </li> <li><code>static thresh-value</code> — （可选）输入静态共享缓冲区阈值（以字节为单位），从 1 到 65535。</li> </ul> |
| 默认 | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|            |                                                                                                                                                                                                                                                                |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 命令模式       | POLICY-MAP-CLASS-MAP                                                                                                                                                                                                                                           |
| 使用情况信息     | 使用 <code>queue-len value</code> 参数设置队列的最小保证队列长度。此命令的 <code>no</code> 版本将值恢复为默认值。                                                                                                                                                                               |
| 示例         | <pre> OS10(config)# policy-map type network-qos nqGlobalpolicy1 OS10(config-cmap-nqos)# class type network-qos nqclass1 OS10(config-cmap-nqos-c)# pause buffer-size 45 pause-threshold 30 resume-threshold 10 OS10(config-cmap-nqos-c)# queue-limit 150 </pre> |
| 示例 (queue) | <pre> OS10(config)# policy-map type queuing pmap1 OS10(config-pmap-queuing)# class cmap1 OS10(config-pmap-c-que)# queue-limit queue-len 100 OS10(config-pmap-c-que)# queue-limit thresh-mode static 50 </pre>                                                  |
| 支持的版本      | 10.3.0E or later                                                                                                                                                                                                                                               |

## queue bandwidth

配置接口上给定队列的带宽。

|        |                                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>queue queue-number bandwidth bandwidth-percentage</code>                                                                              |
| 参数     | <ul style="list-style-type: none"> <li><code>queue-number</code> — 输入队列号。</li> <li><code>bandwidth-percentage</code> — 输入带宽的百分比。</li> </ul> |
| 默认     | 未配置                                                                                                                                         |
| 命令模式   | POLICY-MAP-CLASS-MAP                                                                                                                        |
| 使用情况信息 | 此命令的 <code>no</code> 版本将从队列移除带宽。                                                                                                            |
| 示例     | 无                                                                                                                                           |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                        |

## queue qos-group

将 dot1p 流量类别配置到队列。

|        |                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>queue number [qos-group dot1p-values]</code>                                                                                                                                           |
| 参数     | <ul style="list-style-type: none"> <li><code>queue number</code> — 输入流量单值队列 ID，从 0 到 7。</li> <li><code>qos-group dot1p-values</code> — (可选) 输入单个、逗号分隔的或者带有连字符的 dot1p 值范围，从 0 到 7。</li> </ul> |
| 默认     | 0                                                                                                                                                                                            |
| 命令模式   | TRUST-MAP                                                                                                                                                                                    |
| 使用情况信息 | 如果信任映射未定义队列的流量类别值，这些流将映射到默认队列 0。如果某些流量类别值已映射到现有的队列，您将看到错误。此命令的 <code>no</code> 版本将值恢复为默认值。                                                                                                   |
| 示例     | <pre> OS10(config-tmap-tc-queue-qos)# queue 2 qos-group 5 </pre>                                                                                                                             |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                             |

## queue qos-group (Z9332F-ON)

配置不同队列的不同流量类别类型的映射。

|    |                                                                                    |
|----|------------------------------------------------------------------------------------|
| 语法 | <code>queue number qos-group traffic-class-numbertype {unicast   multicast}</code> |
|----|------------------------------------------------------------------------------------|

|        |                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 参数     | <ul style="list-style-type: none"> <li><code>queue number</code> — 输入流量单值队列 ID，从 0 到 7。多播队列的范围从 0 到 2。</li> <li><code>qos-group traffic-class-number</code> — 输入流量类别号，可以是单个、逗号分隔或连字符范围</li> <li><code>typeunicast   multicast</code> — 选择单播或多播队列类型</li> </ul> |
| 默认     | 不适用                                                                                                                                                                                                                                                           |
| 命令模式   | CONFIGURATION (config-qos-map)                                                                                                                                                                                                                                |
| 使用情况信息 | 此命令适用于 Z9332F-ON。此命令的 <code>no</code> 版本将值恢复为默认值。                                                                                                                                                                                                             |
| 示例     | <pre>OS10(config-qos-map)# queue 2 qos-group 2-5 type unicast</pre>                                                                                                                                                                                           |
| 支持的版本  | 10.5.0 或更高版本                                                                                                                                                                                                                                                  |

## random-detect (interface)

为指定接口分配 WRED 配置文件。

|        |                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------|
| 语法     | <code>random-detect wred-profile</code>                                                           |
| 参数     | <code>wred-profile</code> — 输入现有 WRED 配置文件的名称。                                                    |
| 默认     | 未配置                                                                                               |
| 命令模式   | INTERFACE                                                                                         |
| 使用情况信息 | 此命令的 <code>no</code> 版本会从接口移除 WRED 配置文件。                                                          |
| 示例     | <pre>OS10(config)# interface ethernet 1/1/1 OS10(conf-if-eth1/1/1)# random-detect test_wred</pre> |
| 支持的版本  | 10.4.0E(R1) or later                                                                              |

## random-detect (queue)

将 WRED 配置文件分配给指定队列。

|        |                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>random-detect wred-profile-name</code>                                                                                             |
| 参数     | <code>wred-profile-name</code> — 输入现有 WRED 配置文件的名称。                                                                                      |
| 默认     | 未配置                                                                                                                                      |
| 命令模式   | PMAP-C-QUE                                                                                                                               |
| 使用情况信息 | 此命令的 <code>no</code> 版本将从队列中移除 WRED 配置文件。                                                                                                |
| 示例     | <pre>OS10(config)# policy-map type queuing p1 OS10(config-pmap-queuing)# class c1 OS10(config-pmap-c-que)# random-detect test_wred</pre> |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                     |

## random-detect color

配置可用颜色的 WRED 配置文件的阈值。

|    |                                                                                                                                                                                                                                               |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>random-detect color color-name minimum-threshold minimum-value maximum-threshold maximum-value drop-probability drop-rate</code>                                                                                                        |
| 参数 | <ul style="list-style-type: none"> <li><code>color-name</code> — 输入 WRED 配置文件的丢弃优先级颜色。可用选项为绿色、黄色和红色。</li> <li><code>minimum-value</code> — 输入指定颜色的最小阈值，从 1 到 12480。</li> <li><code>maximum-value</code> — 输入指定颜色的最大阈值，从 1 到 12480。</li> </ul> |

|        |                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | <ul style="list-style-type: none"> <li><code>drop-rate</code> — 输入丢弃优先级的速率（以百分比表示），从 0 到 100。</li> </ul>                                               |
| 命令模式   | 未配置                                                                                                                                                    |
| 使用情况信息 | WRED CONFIGURATION                                                                                                                                     |
| 示例     | 此命令的 <code>no</code> 版本将移除 WRED 配置文件。                                                                                                                  |
| 支持的版本  | <pre> OS10(config)# wred test_wred OS10(config-wred)# random-detect color green minimum-threshold 100 maximum-threshold 300 drop-probability 40 </pre> |

random-detect ecn

为 WRED 配置文件启用显式拥塞通知 (ECN)。

|        |                                                                                |
|--------|--------------------------------------------------------------------------------|
| 语法     | <code>random-detect ecn</code>                                                 |
| 参数     | 无                                                                              |
| 默认     | 未配置                                                                            |
| 命令模式   | WRED CONFIGURATION                                                             |
| 使用情况信息 | 此命令的 <code>no</code> 版本将禁用 ECN。                                                |
| 示例     | <pre> OS10(config)# wred test_wred OS10(config-wred)# random-detect ecn </pre> |
| 支持的版本  | 10.4.0E(R1) or later                                                           |

random-detect ecn

针对系统全局启用 ECN。

|        |                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>random-detect ecn</code>                                                                                                                                                           |
| 默认     | 未配置                                                                                                                                                                                      |
| 命令模式   | SYSTEM QOS                                                                                                                                                                               |
| 使用情况信息 | <p>此命令的 <code>no</code> 版本会在全局范围内禁用 ECN。</p> <p><b>注:</b> 此命令可在全局范围内启用 ECN，并且仅在 S4200-ON 系列平台上受支持。在 SYSTEM QOS 模式下，此命令在其他平台上不可用。此外，您只能为每个队列配置 ECN；您不能在 S4200-ON 系列平台上的接口或服务池上配置 ECN。</p> |
| 示例     | <pre> applicableOS10(config)# system-qos OS10(config-sys-qos)# random-detect ecn </pre>                                                                                                  |
| 支持的版本  | 10.4.1.0 or later                                                                                                                                                                        |

random-detect pool

将 WRED 配置文件分配给指定的全局缓冲池。

|    |                                                                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>random-detect pool pool-value wred-profile-name</code>                                                                                           |
| 参数 | <ul style="list-style-type: none"> <li><code>pool-value</code> — 输入池值，从 0 到 1。</li> <li><code>wred-profile-name</code> — 输入现有 WRED 配置文件的名称。</li> </ul> |
| 默认 | 未配置                                                                                                                                                    |

|        |                                                                                          |
|--------|------------------------------------------------------------------------------------------|
| 命令模式   | SYSTEM-QOS                                                                               |
| 使用情况信息 | 此命令的 <code>no</code> 版本会从接口移除 WRED 配置文件。                                                 |
| 示例     | <pre>OS10(config)# system qos OS10(config-sys-qos)# random-detect pool 0 test_wred</pre> |
| 支持的版本  | 10.4.0E(R1) or later                                                                     |

## random-detect weight

配置用于计算 WRED 配置文件的平均队列深度的指数权重值。

|        |                                                                                    |
|--------|------------------------------------------------------------------------------------|
| 语法     | <code>random-detect weight weight-value</code>                                     |
| 参数     | <code>weight-value</code> — 输入权重的值，从 1 到 15。                                       |
| 默认     | 未配置                                                                                |
| 命令模式   | WRED CONFIGURATION                                                                 |
| 使用情况信息 | 此命令的 <code>no</code> 版本将从 WRED 配置文件中移除权重系数。                                        |
| 示例     | <pre>OS10(config)# wred test_wred OS10(config-wred)# random-detect weight 10</pre> |
| 支持的版本  | 10.4.0E(R1) or later                                                               |

## service-policy

配置输入和输出服务策略。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>service-policy {input   output} [type {qos   queuing   network-qos}] policy-map-name</code>                                                                                                                                                                                                                                                                                                                    |
| 参数     | <ul style="list-style-type: none"> <li><code>input</code> — 输入以将 QoS 策略分配到接口输入。</li> <li><code>output</code> — 输入以将 QoS 策略分配到接口输出。</li> <li><code>qos</code> — 输入以分配 <code>qos</code> 类型策略映射。</li> <li><code>queuing</code> — 输入以分配 <code>queuing</code> 类型策略-映射。</li> <li><code>network-qos</code> — 输入以分配 <code>network-qos</code> 类型策略-映射。</li> <li><code>policy-map-name</code> — 输入策略映射名称。最多 32 个字符。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 命令模式   | INTERFACE                                                                                                                                                                                                                                                                                                                                                                                                            |
| 使用情况信息 | 仅将一个策略映射连接到每个 <code>qos</code> 和 <code>queuing</code> 策略映射类型的接口输入和输出。您可以将四个服务策略连接到系统 QoS — 分别对应于 <code>qos</code> 、 <code>queuing</code> 和 <code>network-qos</code> 类型策略映射。当您配置接口级别策略和系统级策略时，接口级别策略优先于系统级策略。                                                                                                                                                                                                         |
| 示例     | <pre>OS10(conf-if-eth1/1/7)# service-policy input type qos pl</pre>                                                                                                                                                                                                                                                                                                                                                  |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                     |

## set cos

设置服务成本 (CoS) 值以标记 L2 802.1p (dot1p) 数据包。

|    |                                              |
|----|----------------------------------------------|
| 语法 | <code>set cos cos-value</code>               |
| 参数 | <code>cos-value</code> — 输入一个 CoS 值，从 0 到 7。 |

|        |                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | 未配置                                                                                                                                                   |
| 命令模式   | POLICY-MAP-CLASS-MAP                                                                                                                                  |
| 使用情况信息 | 您不能使用相同的操作类型输入两个 <code>set</code> 语句。如果输入两个具有相同操作类型的 <code>set</code> 语句，则第二个语句会覆盖第一个。当类别映射类型为 <code>qos</code> 时， <code>qos</code> 组与数据队列 0 至 7 相对应。 |
| 示例     | <pre>OS10(conf-pmap-c-qos)# set cos 6</pre>                                                                                                           |
| 支持的版本  | 10.2.0E or later                                                                                                                                      |

## set dscp

根据其 DSCP 值和颜色映射配置文件设置传入数据包的丢弃优先级。

|        |                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>set dscp dscp-value [color {red   yellow}]</code>                                                                                                                                                                                                     |
| 参数     | <ul style="list-style-type: none"> <li><code>dscp-value</code> — 输入一个 DSCP 值，从 0 到 63。</li> <li><code>color</code> — (可选) — 输入以应用颜色映射配置文件。</li> <li><code>red</code> — (可选) 输入以标记要丢弃的数据包。</li> <li><code>yellow</code> — (可选) 输入以标记要传送到出口队列的数据包。</li> </ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                         |
| 命令模式   | POLICY-MAP-CLASS-MAP                                                                                                                                                                                                                                        |
| 使用情况信息 | 此命令仅支持 QoS 入口策略类型。标记为 <code>color yellow</code> 的数据包将发送到出口队列，然后出口队列将传输具有可用带宽的数据包。如果带宽不可用，则丢弃数据包。所有数据包都标记为 <code>color red</code> 丢弃。当类别映射类型为 <code>qos</code> 时， <code>qos</code> 组与数据队列 0 至 7 相对应。                                                         |
| 示例     | <pre>OS10(conf-pmap-c-qos)# set dscp 10</pre>                                                                                                                                                                                                               |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                            |

## set qos-group

为 QoS 组队列配置标记。

|        |                                                                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>set qos-group queue-number</code>                                                                                                                                                                |
| 参数     | <code>queue-number</code> — 输入队列编号，从 0 到 7。                                                                                                                                                            |
| 默认     | 未配置                                                                                                                                                                                                    |
| 命令模式   | POLICY-MAP-CLASS-MAP                                                                                                                                                                                   |
| 使用情况信息 | 此命令仅支持 <code>qos</code> 或 <code>control-plane</code> 入口策略类型。当类别映射类型为 <code>control-plane</code> 时， <code>qos</code> 组与 CPU 队列 0 到 11 对应。当类别映射类型为 <code>qos</code> 时， <code>qos</code> 组与数据队列 0 到 7 对应。 |
| 示例     | <pre>OS10(conf-pmap-c-qos)# set qos-group 7</pre>                                                                                                                                                      |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                       |

## shape

塑造传出流量速率。

|    |                                                                                                                                                                  |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | <code>shape {min {kbps   mbps   pps} min-value [burst-size]} {max {kbps   mbps   pps} max-value [max-burst-size]}</code>                                         |
| 参数 | <ul style="list-style-type: none"> <li><code>min</code> — 以 kbps、mbps 或 pps 为单位输入最小提交速率。</li> <li><code>kbps</code> — 以 kb/秒为单位输入提交速率，从 0 到 40000000。</li> </ul> |

- `mbps` — 以 mb/秒为单位输入提交速率，从 0 到 40000。
- `pps` — 以每秒数据包数输入提交速率，从 1 到 268000000。
- `burst-size` — 以每数据包 kb 为单位输入脉冲大小，从 0 到 10000 或从 1 到 1073000。
- `max` — 以 kbps、mbps 或 pps 为单位输入最大峰值速率。
- `max-burst-size` — 以每数据包 kb 为单位输入脉冲大小，从 0 到 10000 或从 1 到 1073000。

**默认** 最大脉冲大小为 50 kb 或 200 个数据包

**命令模式** POLICY-MAP-CLASS-MAP

**使用情况信息** 此命令仅支持入口 QoS 策略类型。您必须输入最小值和最大值。如果您以 pps 为单位输入速率值，则会在数据包中提供突发。如果输入的速率以 kbps 或 mbps 为单位，则以 kb 为单位提供脉冲值。如果您以 pps 为单位输入最小速率，则还必须以 pps 为单位输入最大速率。

**示例**

```
OS10(conf-pmap-c-que)# shape min kbps 11 max kbps 44
```

**支持的版本** 10.2.0E or later

## show class-map

显示所有现有类别映射的配置详细信息。

**语法** `show class-map [type {control-plane | qos | queuing | network-qos} class-map-name]`

- 参数**
- `type` — 输入策略-映射类型 — qos、queuing 或 control-plane。
  - `qos` — 显示所有 qos 类型的映射策略。
  - `queuing` — 显示所有 queuing 类型的映射策略。
  - `network-qos` — 显示所有 network-qos 类型的映射策略。
  - `control-plane` — 显示所有 control-plane 类型的映射策略。
  - `class-map-name` — 显示 QoS 类别映射名称。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 此命令将显示 qos、queuing、network-qos 或 control-plane 类型的所有类别映射。`class-map-name` 参数将显示已配置的类别映射名称的所有详细信息。

**示例**

```
OS10# show class-map type qos cl
Class-map (qos): cl (match-all)
Match(not): ip-any dscp 10
```

**支持的版本** 10.2.0E or later

## show control-plane buffers

显示每个 CPU 队列的池类型、保留缓冲区大小和最大阈值。

**语法** `show control-plane buffers`

**参数** 无

**默认** 无

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# show control-plane buffers
queue-number pool-type rsvd-buf-size threshold-mode threshold-value

0 lossy 1664 static
```



|       |       |      |        |
|-------|-------|------|--------|
| 20800 |       |      |        |
| 1     | lossy | 1664 | static |
| 20800 |       |      |        |
| 2     | lossy | 1664 | static |
| 48880 |       |      |        |
| 3     | lossy | 9216 | static |
| 48880 |       |      |        |
| 4     | lossy | 1664 | static |
| 20800 |       |      |        |
| 5     | lossy | 1664 | static |
| 48880 |       |      |        |
| 6     | lossy | 1664 | static |
| 48880 |       |      |        |
| 7     | lossy | 1664 | static |
| 48880 |       |      |        |
| 8     | lossy | 1664 | static |
| 48880 |       |      |        |
| 9     | lossy | 9216 | static |
| 48880 |       |      |        |
| 10    | lossy | 1664 | static |
| 48880 |       |      |        |
| 11    | lossy | 1664 | static |
| 48880 |       |      |        |
| 12    | lossy | 1664 | static |
| 48880 |       |      |        |
| 13    | lossy | 9216 | static |
| 48880 |       |      |        |
| 14    | lossy | 1664 | static |
| 48880 |       |      |        |
| 15    | lossy | 9216 | static |
| 48880 |       |      |        |
| 16    | lossy | 1664 | static |
| 48880 |       |      |        |
| 17    | lossy | 1664 | static |
| 48880 |       |      |        |
| 18    | lossy | 1664 | static |
| 48880 |       |      |        |
| 19    | lossy | 1664 | static |
| 48880 |       |      |        |
| 20    | lossy | 1664 | static |
| 20800 |       |      |        |
| 21    | lossy | 1664 | static |
| 20800 |       |      |        |
| 22    | lossy | 1664 | static |
| 20800 |       |      |        |

支持的版本10.4.2 和更高版本

show control-plane buffer-stats

显示每个 CPU 队列的控制平面缓冲区统计信息。

|        |                                 |
|--------|---------------------------------|
| 语法     | show control-plane buffer-stats |
| 参数     | 无                               |
| 默认     | 存在预定义的默认配置文件。                   |
| 命令模式   | EXEC                            |
| 使用情况信息 | 无                               |
| 示例     |                                 |

| OS10# show control-plane buffer-stats |       |       |               |      |
|---------------------------------------|-------|-------|---------------|------|
| Queue                                 | TX    | TX    | Used reserved | Used |
| shared                                | pckts | bytes | buffers       |      |
| -----                                 |       |       |               |      |
| 0                                     | 0     | 0     | 0             |      |

|    |   |     |   |
|----|---|-----|---|
| 0  |   |     |   |
| 1  | 0 | 0   | 0 |
| 0  |   |     |   |
| 2  | 0 | 0   | 0 |
| 0  |   |     |   |
| 3  | 0 | 0   | 0 |
| 0  |   |     |   |
| 4  | 0 | 0   | 0 |
| 0  |   |     |   |
| 5  | 0 | 0   | 0 |
| 0  |   |     |   |
| 6  | 3 | 204 | 0 |
| 0  |   |     |   |
| 7  | 6 | 408 | 0 |
| 0  |   |     |   |
| 8  | 0 | 0   | 0 |
| 0  |   |     |   |
| 9  | 0 | 0   | 0 |
| 0  |   |     |   |
| 10 | 0 | 0   | 0 |
| 0  |   |     |   |
| 11 | 0 | 0   | 0 |
| 0  |   |     |   |
| 12 | 0 | 0   | 0 |
| 0  |   |     |   |
| 13 | 0 | 0   | 0 |
| 0  |   |     |   |
| 14 | 0 | 0   | 0 |
| 0  |   |     |   |
| 15 | 0 | 0   | 0 |
| 0  |   |     |   |
| 16 | 0 | 0   | 0 |
| 0  |   |     |   |
| 17 | 0 | 0   | 0 |
| 0  |   |     |   |
| 18 | 0 | 0   | 0 |
| 0  |   |     |   |
| 19 | 0 | 0   | 0 |
| 0  |   |     |   |
| 20 | 0 | 0   | 0 |
| 0  |   |     |   |
| 21 | 0 | 0   | 0 |
| 0  |   |     |   |
| 22 | 0 | 0   | 0 |
| 0  |   |     |   |

支持的版本10.4.2 和更高版本

show control-plane info

显示控制平面队列映射和速率限制。

语法show control-plane info

参数无

默认未配置

命令模式EXEC

使用情况信息监控控制平面的统计信息并对 CoPP 进行故障处理。

示例

|         |                         |                        |               |  |
|---------|-------------------------|------------------------|---------------|--|
| OS10#   | show control-plane info |                        |               |  |
| Queue   | Min Rate Limit(in pps)  | Max Rate Limit(in pps) | Protocols     |  |
| 0       | 600                     | 600                    | ISCSI UNKNOWN |  |
| UNICAST |                         |                        |               |  |
| 1       | 1000                    | 1000                   | SFLOW         |  |
| 2       | 400                     | 400                    | IGMP MLD PIM  |  |
| 3       | 600                     | 1000                   | VLT NDS       |  |

|                               |     |      |                     |
|-------------------------------|-----|------|---------------------|
| 4                             | 500 | 1000 | IPV6_ICMP IPV4_ICMP |
| 5                             | 500 | 1000 | ICMPV6_RS           |
| ICMPV6_NS ICMPV6_RA ICMPV6_NA |     |      |                     |
| 6                             | 500 | 1000 | ARP_REQ             |
| SERVICEABILITY                |     |      |                     |
| 7                             | 500 | 1000 | ARP_RESP            |
| 8                             | 500 | 500  | SSH_TELNET TACACS   |
| NTP FTP                       |     |      |                     |
| 9                             | 600 | 600  | FCOE                |
| 10                            | 600 | 1000 | LACP                |
| 11                            | 400 | 400  | RSTP PVST MSTP      |
| 12                            | 500 | 500  | DOT1X LLDP          |
| 13                            | 600 | 1000 | IPV6_OSPF IPV4_OSPF |
| 14                            | 600 | 1000 | OSPF_HELLO          |
| 15                            | 600 | 1000 | BGP                 |
| 16                            | 500 | 500  | IPV6_DHCP IPV4_DHCP |
| 17                            | 600 | 1000 | VRRP                |
| 18                            | 700 | 700  | BFD                 |
| 19                            | 700 | 1000 | OPEN_FLOW REMOTE    |
| CPS                           |     |      |                     |
| 20                            | 300 | 300  | MCAST DATA          |
| 21                            | 100 | 100  | ACL LOGGING         |
| 22                            | 300 | 300  | MCAST KNOWN DATA    |

支持的版本10.2.0E or later

show control-plane statistics

显示所有 CPU 队列统计信息的计数器。

- 语法 show control-plane statistics
- 参数 无
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 无
- 示例

|                                     |         |       |         |         |               |
|-------------------------------------|---------|-------|---------|---------|---------------|
| OS10# show control-plane statistics |         |       |         |         |               |
| Queue                               | Packets | Bytes | Dropped | Packets | Dropped Bytes |
| 0                                   | 0       | 0     | 0       |         | 0             |
| 1                                   | 0       | 0     | 0       |         | 0             |
| 2                                   | 0       | 0     | 0       |         | 0             |
| 3                                   | 0       | 0     | 0       |         | 0             |
| 4                                   | 0       | 0     | 0       |         | 0             |
| 5                                   | 0       | 0     | 0       |         | 0             |
| 6                                   | 3       | 204   | 0       |         | 0             |
| 7                                   | 6       | 408   | 0       |         | 0             |
| 8                                   | 0       | 0     | 0       |         | 0             |
| 9                                   | 0       | 0     | 0       |         | 0             |
| 10                                  | 0       | 0     | 0       |         | 0             |
| 11                                  | 0       | 0     | 0       |         | 0             |
| 12                                  | 0       | 0     | 0       |         | 0             |
| 13                                  | 0       | 0     | 0       |         | 0             |
| 14                                  | 0       | 0     | 0       |         | 0             |
| 15                                  | 0       | 0     | 0       |         | 0             |
| 16                                  | 0       | 0     | 0       |         | 0             |
| 17                                  | 0       | 0     | 0       |         | 0             |
| 18                                  | 0       | 0     | 0       |         | 0             |
| 19                                  | 0       | 0     | 0       |         | 0             |
| 20                                  | 0       | 0     | 0       |         | 0             |
| 21                                  | 0       | 0     | 0       |         | 0             |
| 22                                  | 0       | 0     | 0       |         | 0             |
| OS10#                               |         |       |         |         |               |

支持的版本10.2.0E or later

# show hardware deep-buffer-mode

显示交换机当前和下一次引导时的深度缓冲区模式的状态。

|        |                                |
|--------|--------------------------------|
| 语法     | show hardware deep-buffer-mode |
| 参数     | 无                              |
| 默认     | 未配置                            |
| 命令模式   | EXEC                           |
| 使用情况信息 | 仅适用于 S4200-ON 系列交换机。           |
| 示例     | 示例：默认设置                        |

```
OS10# show hardware deep-buffer-mode
Deep Buffer Mode Configuration Status

Current-boot Settings : Disabled

Next-boot Settings : Disabled
```

示例：保存到启动配置

```
OS10# show hardware deep-buffer-mode
Deep Buffer Mode Configuration Status

Current-boot Settings : Disabled

Next-boot Settings : Enabled
```

示例：重新加载交换机

```
OS10# show hardware deep-buffer-mode
Deep Buffer Mode Configuration Status

Current-boot Settings : Enabled

Next-boot Settings : Enabled
```

|       |                   |
|-------|-------------------|
| 支持的版本 | 10.4.3.0 or later |
|-------|-------------------|

# show interface priority-flow-control

显示优先级流控制、运行状态、CoS 位图和每个端口的统计信息。

|           |                                                                                         |
|-----------|-----------------------------------------------------------------------------------------|
| 语法        | show interface ethernet <i>node/slot/port[:subport]</i> priority-flow-control [details] |
| 参数        | details — (可选) 显示接口的所有优先级流控制信息。                                                         |
| 默认        | 未配置                                                                                     |
| 命令模式      | EXEC                                                                                    |
| 使用情况信息    | 无                                                                                       |
| 示例 (详细信息) |                                                                                         |

```
OS10# show interface ethernet 1/1/14 priority-flow-control details

ethernet1/1/14
Admin Mode: On
Operstatus: On
PFC Priorities: 0,4,7
Total Rx PFC Frames: 300
Total Tx PFC Frames: 200
Cos Rx Tx

```

|   |     |     |
|---|-----|-----|
| 0 | 0   | 0   |
| 1 | 0   | 0   |
| 2 | 0   | 0   |
| 3 | 300 | 200 |
| 4 | 0   | 0   |
| 5 | 0   | 0   |
| 6 | 0   | 0   |
| 7 | 0   | 0   |

**支持的版本** 10.3.0E or later

## show qos interface

显示应用于特定接口的 QoS 配置。

|               |                                                                   |
|---------------|-------------------------------------------------------------------|
| <b>语法</b>     | <code>show qos interface ethernet node/slot/port[:subport]</code> |
| <b>参数</b>     | <code>node/slot/port[:subport]</code> — 输入以太网接口信息。                |
| <b>默认</b>     | 未配置                                                               |
| <b>命令模式</b>   | EXEC                                                              |
| <b>使用情况信息</b> | 无                                                                 |
| <b>示例</b>     |                                                                   |

```
OS10# show qos interface ethernet 1/1/10
Ethernet 1/1/10
 unknown-unicast-storm-control : 100 pps
 multicast-storm-control : 200 pps
 broadcast-storm-control : Disabled
 flow-control-rx: Enabled
 flow-control-tx: Disabled
 Service-policy (Input) (qos): p1
```

**支持的版本** 10.2.0E or later

## show policy-map

显示有关所有现有策略映射的信息。

|               |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>show policy-map type {control-plane   qos   queuing   network-qos} [policy-map-name]</code>                                                                                                                                                                                                                                                                                                                    |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>type</code> — 输入策略-映射类型 — qos、queuing 或 control-plane。</li> <li><code>qos</code> — 显示所有 qos 类型的映射策略。</li> <li><code>queuing</code> — 显示所有已配置 queuing 类型的策略映射。</li> <li><code>network-qos</code> — 显示所有已配置 network-qos 类型的策略映射。</li> <li><code>control-plane</code> — 显示所有 control-plane 类型的映射策略。</li> <li><code>policy-map-name</code> — 显示 QoS 策略映射名称的详细信息。</li> </ul> |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>命令模式</b>   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>使用情况信息</b> | 无                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>示例</b>     |                                                                                                                                                                                                                                                                                                                                                                                                                      |

```
OS10# show policy-map
Service-policy(qos) input: p1
 Class-map (qos): c1
 set qos-group 1
Service-policy(qos) input: p2
 Class-map (qos): c2
 set qos-group 2
```

**支持的版本** 10.2.0E or later

## show qos control-plane

显示应用于控制平面的 QoS 配置。

|        |                                                                    |
|--------|--------------------------------------------------------------------|
| 语法     | show qos control-plane                                             |
| 参数     | 无                                                                  |
| 默认     | 未配置                                                                |
| 命令模式   | EXEC                                                               |
| 使用情况信息 | 监控控制平面的统计信息并对 CoPP 进行故障处理。                                         |
| 示例     | <pre>OS10# show qos control-plane Service-policy (Input): p1</pre> |
| 支持的版本  | 10.2.0E or later                                                   |

## show qos egress buffers interface

显示出口缓冲区配置。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show qos egress buffers interface [interface node/slot/port[:subport]]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 参数     | <ul style="list-style-type: none"><li>interface — (可选) 输入接口类型。</li><li>node/slot/port[:subport] — (可选) 输入端口信息。</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 示例     | <pre>OS10# show qos egress buffers interface ethernet 1/1/1 Interface : ethernet1/1/1 Speed : 0 queue-number  pool-type    rsvd-buf-size  threshold-mode  threshold-value ----- 0               lossy        1664           dynamic         8 1               lossy        1664           dynamic         8 2               lossy        1664           dynamic         8 3               lossless     0              static          12479488 4               lossy        1664           dynamic         8 5               lossy        1664           dynamic         8 6               lossy        1664           dynamic         8 7               lossy        1664           dynamic         8</pre> |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## show qos egress buffer-statistics-tracking

显示给定接口上的队列的出口队列级别峰值缓冲区使用计数（以字节为单位）。

|        |                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show qos egress buffer-statistics-tracking interface ethernet [node/slot/port] [[mcast   ucast] queue {all   [0-7]}] [detail]                                                                                                                                                                    |
| 参数     | <ul style="list-style-type: none"><li>node/slot/port — 输入端口信息。</li><li>[[mcast   ucast] queue {all   [0-7]}] — 输入 mcast 或 ucast 关键字以分别查看多播或单播队列的出口队列峰值缓冲区利用率。输入 all 关键字以指定所有队列，或输入队列编号。</li><li>detail — (可选) 显示支持多个 MMU 实例的平台（例如 Z9100-ON 系列、Z9200-ON 系列 和 MX9116n）中的每个 MMU 实例级别统计信息。</li></ul> |
| 默认     | 不适用                                                                                                                                                                                                                                                                                              |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                             |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                |

示例

```
OS10# show qos egress buffer-statistics-tracking interface ethernet 1/1/1
Interface : ethernet1/1/1
Speed : 0
QType Queue Total buffers
 peak count

Unicast 0 0
Unicast 1 0
Unicast 2 0
Unicast 3 0
Unicast 4 0
Unicast 5 0
Unicast 6 0
Unicast 7 0
Multicast 0 0
Multicast 1 0
Multicast 2 0
Multicast 3 0
Multicast 4 0
Multicast 5 0
Multicast 6 0
Multicast 7 0
```

支持的版本 10.4.3.0 or later

show qos egress buffer-stats interface

显示出口接口的缓冲区统计信息。

语法 show qos egress buffer-stats interface [interface node/slot/port[:subport]] [detail]

- 参数
- interface — (可选) 输入接口类型。
  - node/slot/port[:subport] — (可选) 输入端口信息。
  - detail — 显示支持多个 MMU 实例的平台中的每个 MMU 出口缓冲区统计信息，例如 Z9100-ON、Z9264F-ON 和 MX9116n。

默认 未配置

命令模式 EXEC

使用情况信息 无

示例

```
OS10# show qos egress buffer-stats interface ethernet 1/1/1
Interface : ethernet1/1/1
Speed : 0
Queue TX TX Used reserved Used shared
 pkts bytes buffers

0 0 0 0
1 0 0 0
2 0 0 0
3 0 0 0
4 0 0 0
5 0 0 0
6 0 0 0
7 0 0 0
OS10#
```

支持的版本 10.3.0E or later

## show qos headroom-pool buffer-statistics-tracking

显示余量池级别的峰值缓冲区使用计数（以字节为单位）。

|        |                                                                                      |
|--------|--------------------------------------------------------------------------------------|
| 语法     | show qos headroom-pool buffer-statistics-tracking [detail]                           |
| 参数     | 详细信息 — 显示具有多个 MMU 实例（例如 Z9100-ON、Z9264F-ON 和 MX9116n）的平台中的每个内存管理单元 (MMU) 实例的余量池统计信息。 |
| 默认     | 未配置                                                                                  |
| 命令模式   | EXEC                                                                                 |
| 使用情况信息 | 受支持的平台包括 Z9100-ON 系列、Z9200-ON 系列、 S5200-ON 系列 和 MX9116n。                             |
| 示例     |                                                                                      |

```
OS10# show qos headroom-pool buffer-statistics-tracking
Headroom Pool Buffers-Usage

0 0
1 0
2 0
3 0
```

支持的版本 10.4.3.0 or later

## show qos ingress buffers interface

显示接口缓冲区配置。

|        |                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------|
| 语法     | show qos ingress buffers interface [interface node/slot/port[:subport]]                                                |
| 参数     | <ul style="list-style-type: none"><li>interface — （可选）输入接口类型。</li><li>node/slot/port[:subport] — （可选）输入端口信息。</li></ul> |
| 默认     | 未配置                                                                                                                    |
| 命令模式   | EXEC                                                                                                                   |
| 使用情况信息 | 无                                                                                                                      |
| 示例     |                                                                                                                        |

```
OS10(config)# show qos ingress buffer interface ethernet 1/1/1
Interface ethernet 1/1/1
Speed 40G

PG# PRIORITIES qos group Reserved Shared buffer ALLOTTED (Kb)
shared buffer id buffers MODE XOFF XON
threshold threshold

0 4 4 35 DYNAMIC 9
9 8
1 3 3 35 DYNAMIC 9
9 8
2 - - 0 STATIC 0
0 0
3 - - 0 STATIC 0
0 0
4 - - 0 STATIC 0
0 0
5 - - 0 STATIC 0
0 0
6 - - 0 STATIC 0
0 0
7 - 0-2, 5-7 8 STATIC 0
0 0
```

支持的版本 10.3.0E or later



## show qos ingress buffer-statistics-tracking

显示给定接口上给定优先级组的入口优先级组级别峰值缓冲区使用次数（以字节为单位）。

|        |                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show qos ingress buffer-statistics-tracking interface ethernet [node/slot/port] [priority-group {0-7}] [detail]                                                                                                                                                                                                                                                                                          |
| 参数     | <ul style="list-style-type: none"><li>node/slot/port — 输入端口信息。</li><li>[priority-group {0-7}] — 输入 priority-group 关键字，后跟组编号。</li><li>detail — （可选）显示支持多个 MMU 实例的平台（例如 Z9100-ON 系列、Z9200-ON 系列 和 MX9116n）中的每个 MMU 实例级别统计信息。</li></ul>                                                                                                                                                                     |
| 默认     | 不适用                                                                                                                                                                                                                                                                                                                                                                                                      |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                     |
| 使用情况信息 | 当 BST 处于启用状态时，如果您对影响优先级组或优先级映射配置的任何配置进行更改（例如，移除类映射、将类映射添加到策略映射 [nqos]），请确保使用 clear qos statistics type buffer-statistics-tracking 命令清除缓冲区统计信息，以查看当前配置的实际峰值缓冲区利用率。                                                                                                                                                                                                                                        |
| 示例     | <pre>OS10# show qos ingress buffer-statistics-tracking interface ethernet 1/1/1 Interface : ethernet1/1/1 Speed : 0 Priority Peak shared   Peak HDRM Group   buffers         buffers ----- 0        0             0 1        0             0 2        0             0 3        0             0 4        0             0 5        0             0 6        0             0 7        0             0</pre> |

支持的版本 10.4.3.0 or later

## show qos ingress buffer-stats interface

显示入口接口的缓冲区统计信息。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show qos ingress buffer-stats interface [interface node/slot/port[:subport]] [detail]                                                                                                                                                                                                                                                                                                                                                                 |
| 参数     | <ul style="list-style-type: none"><li>interface — （可选）输入接口类型。</li><li>node/slot/port[:subport] — （可选）输入端口信息。</li><li>detail — 显示支持多个 MMU 实例的平台（例如 Z9100-ON 系列、Z9200-ON 系列 和 MX9116n）中的每个 MMU 实例级别统计信息。</li></ul>                                                                                                                                                                                                                                      |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 示例     | <pre>OS10(config)# show qos ingress buffer-stats interface ethernet 1/1/15 Interface : ethernet1/1/15 Speed : 10G Priority Used reserved   Used shared   Used HDRM Group   buffers         buffers         buffers ----- 0        9360             681824         35984 1         0              0              0 2         0              0              0 3         0              0              0 4         0              0              0</pre> |

|   |   |   |   |
|---|---|---|---|
| 5 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 |

支持的版本10.3.0E or later

show qos maps

显示活动的系统信任图。

**语法** show qos maps type {tc-queue | trust-map-dot1p | trust-map dscp} trust-map-name

- 参数**
- dot1p — 输入以查看 dot1p 信任图。
  - dscp — 输入以查看 DSCP 信任图。
  - tc-queue — 输入以查看到队列映射的流量类别。
  - trust-map — 输入信任映射的名称。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例 (dot1p)**

```
OS10# show qos maps type tc-queue queue-map1
Traffic-Class to Queue Map: queue-map1
Queue Traffic-Class

1 5
2 6
3 7
OS10# show qos maps type trust-map-dot1p dot1p-trustmap1
DOT1P Priority to Traffic-Class Map : dot1p-trustmap1
Traffic-Class DOT1P Priority

0 2
1 3
2 4
3 5
4 6
5 7
6 1
OS10# show qos maps type trust-map-dscp dscp-trustmap1
DSCP Priority to Traffic-Class Map : dscp-trustmap1
Traffic-Class DSCP Priority

0 8-15
2 16-23
1 0-7
OS10# show qos maps
Traffic-Class to Queue Map: queue-map1
Queue Traffic-Class

1 5
2 6
3 7
DOT1P Priority to Traffic-Class Map : map1
Traffic-Class DOT1P Priority

DOT1P Priority to Traffic-Class Map : dot1p-trustmap1
Traffic-Class DOT1P Priority

0 2
1 3
2 4
3 5
4 6
5 7
```

```

6 1
DSCP Priority to Traffic-Class Map : dscp-trustmap1
Traffic-Class DSCP Priority

0 8-15
2 16-23
1 0-7
Default Dot1p Priority to Traffic-Class Map
Traffic-Class DOT1P Priority

0 1
1 0
2 2
3 3
4 4
5 5
6 6
7 7
Default Dscp Priority to Traffic-Class Map
Traffic-Class DSCP Priority

0 0-7
1 8-15
2 16-23
3 24-31
4 32-39
5 40-47
6 48-55
7 56-63
Default Traffic-Class to Queue Map
Traffic-Class Queue number

0 0
1 1
2 2
3 3
4 4
5 5
6 6
7 7
OS10#

```

**示例 (dscp)**

```

OS10# show qos trust-map dscp new-dscp-map

new-dscp-map
qos-group Dscp
 Id

0 0-7
1 8-15
2 16-23
3 24-31
4 32-39
5 40-47
6 48-55
7 56-63

```

**支持的版本** 10.3.0E or later

# show qos maps (Z9332F-ON)

显示 dot1p 到流量类别、DSCP 到流量类别以及流量类别到设备中的队列映射的 QoS 映射配置。

**语法** show qos maps type tc-queue

- 参数**
- qos — 输入以查看入口或出口 QoS 配置
  - maps — 输入以查看 QoS 映射信息

- type — (可选) 输入以查看 Qos 映射类型
- tc-queue — 输入以查看流量类别到队列映射

**默认** 不适用

**命令模式** EXEC

**使用情况信息** 该命令仅适用于 Z9332F-ON。该命令提供优先级到流量类别和流量类别到队列映射，包含默认值和用户配置的值。Type 列显示了与流量类别到队列映射条目对应的队列类型。对于除 Z9332F-ON 以外的其他平台，Both 将显示在 Type 列中，指示该映射同时适用于单播和多播队列。

**示例**

```
show qos maps type tc-queue
Traffic-Class to Queue Map: sundar
Queue Traffic-Class Type

2 2-5 Unicast
0-2 0 Multicast
```

**支持的版本** 10.5.0 or later

## show qos port-map details

将端口显示为端口通道和 MMU 映射。

**语法** show qos port-map details [interface interface-type]

**参数** interface interface-type — (可选) 输入关键字 interface 和接口类型。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 在 Z9100-ON, Z9264F-ON 和 MX9116n 平台上，接口在端口通道之间共享，端口通道在内存管理单元 (MMU) 之间共享。由于接口跨端口通道，Dell EMC Networking 建议使用来自入口和出口的相同端口通道的接口，以实现最佳性能。要查找端口到端口通道和 MMU 映射，请使用 show qos port-map details 命令。

**示例** Z9100-ON 交换机:

```
OS10# show qos port-map details
```

| Interface  | Port Pipe | Ingress MMU | Egress MMU | Oper Status |
|------------|-----------|-------------|------------|-------------|
| Eth 1/1/1  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/2  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/3  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/4  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/5  | 2         | 2, 3        | 1, 3       | up          |
| Eth 1/1/6  | 2         | 2, 3        | 1, 3       | up          |
| Eth 1/1/7  | 2         | 2, 3        | 1, 3       | up          |
| Eth 1/1/8  | 2         | 2, 3        | 1, 3       | up          |
| Eth 1/1/9  | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/10 | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/11 | 1         | 2, 3        | 0, 2       | up          |

|            |   |      |      |      |
|------------|---|------|------|------|
| Eth 1/1/12 | 1 | 2, 3 | 0, 2 | up   |
| Eth 1/1/13 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/14 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/15 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/16 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/17 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/18 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/19 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/20 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/21 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/22 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/23 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/24 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/25 | 3 | 0, 1 | 1, 3 | up   |
| Eth 1/1/26 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/27 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/28 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/29 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/30 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/31 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/32 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/33 | 1 | 2, 3 | 0, 2 | up   |
| Eth 1/1/34 | 2 | 2, 3 | 1, 3 | up   |

查看单一接口的信息：

```
OS10# show qos port-map details interface ethernet 1/1/1
```

| Interface | Port Pipe | Ingress MMU | Egress MMU | Oper Status |
|-----------|-----------|-------------|------------|-------------|
| Eth 1/1/1 | 1         | 2, 3        | 0, 2       | up          |

Z9264F-ON 交换机：

```
OS10# show qos port-map details
```

| Interface   | Port Pipe | Ingress MMU | Egress MMU | Oper Status |
|-------------|-----------|-------------|------------|-------------|
| Eth 1/1/1:1 | 0         | 0, 1        | 0, 2       | up          |
| Eth 1/1/3:1 | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/3:2 | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/3:3 | 1         | 2, 3        | 0, 2       | up          |
| Eth 1/1/3:4 | 1         | 2, 3        | 0, 2       | up          |

|              |   |      |      |      |
|--------------|---|------|------|------|
| Eth 1/1/5:1  | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/5:2  | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/5:3  | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/5:4  | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/7:1  | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/7:2  | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/7:3  | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/7:4  | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/9:1  | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/9:2  | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/9:3  | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/9:4  | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/11:1 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/11:2 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/11:3 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/11:4 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/13:1 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/13:2 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/13:3 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/13:4 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/15   | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/16   | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/17:1 | 2 | 2, 3 | 1, 3 | up   |
| Eth 1/1/19:1 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/19:2 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/19:3 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/19:4 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/21:1 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/21:2 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/21:3 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/21:4 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/23   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/24   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/25:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/25:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/25:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/25:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/27:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/27:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/27:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/27:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/29:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/29:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/29:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/29:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/31   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/32   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/33   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/34   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/35:1 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/35:2 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/35:3 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/35:4 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/37:1 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/37:2 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/37:3 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/37:4 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/39:1 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/39:2 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/39:3 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/39:4 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/41:1 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/41:2 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/41:3 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/41:4 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/43   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/44   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/45   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/46   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/47   | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/48   | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/49   | 2 | 2, 3 | 1, 3 | down |

|              |   |      |      |      |
|--------------|---|------|------|------|
| Eth 1/1/50   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/51:1 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/51:2 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/51:3 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/51:4 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/53   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/54   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/55   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/56   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/57:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/57:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/57:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/57:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/59   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/60   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/61   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/62   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/63   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/64   | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/65   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/66   | 1 | 2, 3 | 0, 2 | down |

查看单一接口的信息：

```
OS10# show qos port-map details interface ethernet 1/1/1
```

| Interface   | Port Pipe | Ingress MMU | Egress MMU | Oper Status |
|-------------|-----------|-------------|------------|-------------|
| Eth 1/1/1:1 | 0         | 0, 1        | 0, 2       | up          |

MX9116n 结构引擎：

```
OS10# show qos port-map details
```

| Interface    | Port Pipe | Ingress MMU | Egress MMU | Oper Status |
|--------------|-----------|-------------|------------|-------------|
| Eth 1/1/1    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/2    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/3    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/4    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/5    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/6    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/7    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/8    | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/9    | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/10   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/11   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/12   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/13   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/14   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/15   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/16   | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/17:1 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/17:2 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/17:3 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/17:4 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/18:1 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/18:2 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/18:3 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/18:4 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/19:1 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/19:2 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/19:3 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/19:4 | 3         | 0, 1        | 1, 3       | down        |
| Eth 1/1/20:1 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/20:2 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/20:3 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/20:4 | 1         | 2, 3        | 0, 2       | down        |
| Eth 1/1/21:1 | 3         | 0, 1        | 1, 3       | down        |

|              |   |      |      |      |
|--------------|---|------|------|------|
| Eth 1/1/21:2 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/21:3 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/21:4 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/22:1 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/22:2 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/22:3 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/22:4 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/23:1 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/23:2 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/23:3 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/23:4 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/24:1 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/24:2 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/24:3 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/24:4 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/25:1 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/25:2 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/25:3 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/25:4 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/26:1 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/26:2 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/26:3 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/26:4 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/27:1 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/27:2 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/27:3 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/27:4 | 3 | 0, 1 | 1, 3 | down |
| Eth 1/1/28:1 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/28:2 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/28:3 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/28:4 | 1 | 2, 3 | 0, 2 | down |
| Eth 1/1/29:1 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/29:2 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/29:3 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/29:4 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/30:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/30:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/30:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/30:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/31:1 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/31:2 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/31:3 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/31:4 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/32:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/32:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/32:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/32:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/33:1 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/33:2 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/33:3 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/33:4 | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/34:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/34:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/34:3 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/34:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/35   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/36   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/37   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/38   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/39   | 0 | 0, 1 | 0, 2 | down |
| Eth 1/1/40   | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/41:1 | 2 | 2, 3 | 1, 3 | up   |
| Eth 1/1/41:2 | 2 | 2, 3 | 1, 3 | up   |
| Eth 1/1/41:3 | 2 | 2, 3 | 1, 3 | up   |
| Eth 1/1/41:4 | 2 | 2, 3 | 1, 3 | up   |
| Eth 1/1/42:1 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/42:2 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/42:3 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/42:4 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/43:1 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/43:2 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/43:3 | 2 | 2, 3 | 1, 3 | down |



|              |   |      |      |      |
|--------------|---|------|------|------|
| Eth 1/1/43:4 | 2 | 2, 3 | 1, 3 | down |
| Eth 1/1/44:1 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/44:2 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/44:3 | 0 | 0, 1 | 0, 2 | up   |
| Eth 1/1/44:4 | 0 | 0, 1 | 0, 2 | up   |

查看单一接口的信息：

```
OS10# show qos port-map details interface ethernet 1/1/1
```

| Interface | Port Pipe | Ingress MMU | Egress MMU | Oper Status |
|-----------|-----------|-------------|------------|-------------|
| Eth 1/1/1 | 3         | 0, 1        | 1, 3       | down        |

**支持的版本** 10.5.0 or later

## show qos-rate-adjust

显示流量监管和塑形的速率调整限制的状态。

**语法** show qos-rate-adjust

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 不适用于 S4200-ON 系列交换机。

**示例**

```
OS10# show qos-rate-adjust
```

QoS Rate adjust configured for Policer and Shaper (in bytes) : 10

**支持的版本** 10.4.3.0 or later

## show qos service-pool buffer-statistics-tracking

显示服务池级别的峰值缓冲区使用计数（以字节为单位）。

**语法** show qos service-pool buffer-statistics-tracking [detail]

**参数** 详细信息 — 显示具有多个 MMU 实例（例如 Z9100-ON、Z9264F-ON 和 MX9116n）的平台中的每个内存管理单元 (MMU) 实例的服务池级别峰值缓冲区利用率。

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```
OS10# show qos service-pool buffer-statistics-tracking
```

| Service Pool | Ingress Buffers | Egress Buffers |
|--------------|-----------------|----------------|
| 0            | 0               | 0              |
| 1            | 0               | 0              |
| 2            | 0               | 0              |
| 3            | 0               | 0              |

**支持的版本** 10.4.3.0 or later

# show qos system

显示应用到系统的 QoS 配置。

|        |                   |
|--------|-------------------|
| 语法     | show qos system   |
| 参数     | 无                 |
| 默认     | 未配置               |
| 命令模式   | EXEC              |
| 使用情况信息 | 查看并验证系统级服务策略配置信息。 |
| 示例     |                   |

```
show qos system
ETS Mode : off
ECN Mode : off
buffer-statistics-tracking : off
```

支持的版本 10.4.1.0 or later

# show qos system buffers

显示系统缓冲区配置和利用率。

|        |                                                                             |
|--------|-----------------------------------------------------------------------------|
| 语法     | show qos system {ingress   egress} buffers [detail]                         |
| 参数     | detail — 显示支持多个 MMU 实例的平台中的每个 MMU 级别的系统缓冲区，例如 Z9100-ON、Z9264F-ON 和 MX9116n。 |
| 默认     | 未配置                                                                         |
| 命令模式   | EXEC                                                                        |
| 使用情况信息 | 无                                                                           |
| 示例     |                                                                             |

```
OS10# show qos system ingress buffer
All values are in kb
Total buffers - 12187
 Total lossless buffers - 0
 Maximum lossless buffers - 5512
 Total shared lossless buffers - 0
 Total used shared lossless buffers -
 Total lossy buffers - 11567
 Total shared lossy buffers - 11192
 Total used shared lossy buffers - 0
```

在 Z9100-ON、Z9264F-ON 和 MX9116n 等平台上支持以下命令：

```
OS10# show qos system ingress buffer detail
All values are in kb
Total buffers - 43008
 Total lossless buffers - 0
 Maximum lossless buffers - 23312
 Total shared lossless buffers - 0
 Total used shared lossless buffers -
 Total lossy buffers - 42388
 Total shared lossy buffers - 39974
 Total used shared lossy buffers - 0
 MMU 0
 Total lossy buffers - 10597
 Total shared lossy buffers - 10012
 Total used shared lossy buffers - 0
 MMU 1
 Total lossy buffers - 10597
 Total shared lossy buffers - 10012
 Total used shared lossy buffers - 0
 MMU 2
```

```
Total lossy buffers - 10597
Total shared lossy buffers - 9993
Total used shared lossy buffers - 0
MMU 3
Total lossy buffers - 10597
Total shared lossy buffers - 9993
Total used shared lossy buffers - 0

OS10# show qos system egress buffer
All values are in kb
Total buffers - 12187
Total lossless buffers - 0
Total shared lossless buffers - 0
Total used shared lossless buffers - 0
Total lossy buffers - 11567
Total shared lossy buffers - 9812
Total used shared lossy buffers - 0
Total CPU buffers - 620
Total shared CPU buffers - 558
Total used shared CPU buffers - 0
```

在 Z9100-ON、Z9264F-ON 和 MX9116n 等平台上支持以下命令：

```
OS10# show qos system egress buffer detail
All values are in kb
Total buffers - 43008
Total lossless buffers - 0
Total shared lossless buffers - 0
Total used shared lossless buffers - 0
Total lossy buffers - 42388
Total shared lossy buffers - 33938
Total used shared lossy buffers - 0
MMU 0
Total lossy buffers - 10597
Total shared lossy buffers - 8484
Total used shared lossy buffers - 0
MMU 1
Total lossy buffers - 10597
Total shared lossy buffers - 8484
Total used shared lossy buffers - 0
MMU 2
Total lossy buffers - 10597
Total shared lossy buffers - 8484
Total used shared lossy buffers - 0
MMU 3
Total lossy buffers - 10597
Total shared lossy buffers - 8484
Total used shared lossy buffers - 0
```

支持的版本 10.3.0E or later

show qos wred-profile

显示 WRED 配置文件配置的详细信息。

- 语法 show qos wred-profile [wred-profile-name]
- 参数 wred-profile-name — (可选) 输入以太网接口信息。
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 无
- 示例

```
OS10# show qos wred-profile
Profile Name | Green | Yellow | Rec
| MIN MAX DROP-RATE | MIN MAX DROP-RATE | MIN MAX
```

示例 (S4200) — 在全局启用 ECN 时。

|           | KB  | KB   | %   | KB | KB  | %   | KB | KB  |
|-----------|-----|------|-----|----|-----|-----|----|-----|
| wred_prof | 100 | 1000 | 100 | 50 | 100 | 100 | 50 | 100 |

```
OS10#show qos wred-profile wred_prof1
Wred-profile-name gmin-thd gmax-thd gmax-drop-rate ymin-thd ymax-thd ymax-drop-rate rmin-thd rmax-thd
wred_prof1 0 0 0 1 10 40 0 0 0

S4200 o/p

OS10# show qos wred-profile
Profile Name	Green	Yellow	Red
MIN	MAX	DROP-RATE	MIN	MAX	DROP-RATE	MIN	MAX	DROP-RATE	WEIGHT	ECN
KB	KB	%	KB	KB	%	KB	KB	%		
-----|-----|-----|-----|
profile1 | 10 | 100 | 100 | | | | | | | | Off |
-----|-----|-----|-----|
profile2 | | | | | | | | | | | On |
-----|-----|-----|-----|
Color Blind ECN Thd| 100 1000 | 100 | | | | | | | |
-----|-----|-----|-----|
```

支持的版本

## show queuing statistics

显示 QoS 队列统计信息。

语法

show queuing statistics interface ethernet *node/slot/port[:subport]* [wred | queue *number*]

参数

- node/slot/port[:subport]* — 输入以太网接口信息。
- queue number* — 输入 QoS 队列号，从 0 到 7。

默认

未配置

命令模式

EXEC

使用情况信息

使用此命令可以查看所有队列计数器。WRED 计数器仅在端口级别可用。

示例

```
OS10# show queuing statistics interface ethernet 1/1/1
Interface ethernet1/1/1
Queue Packets Dropped-Bytes Bytes Dropped-
Packets
0 0 0 0
0 0 0
1 0 0 0
0 0 0
2 0 0 0
0 0 0
3 0 0 0
0 0 0
4 0 0 0
0 0 0
5 0 0 0
0 0 0
6 0 0 0
0 0 0
7 0 0 0
0 0 0
```

示例 (wred)

```
OS10# show queuing statistics interface ethernet 1/1/1 wred
Interface ethernet1/1/1 (All queues)
Description Packets
Bytes
Output 0
0
Dropped 0
0
Green Drop 0
0
Yellow Drop 0
0
Red Drop 0
0
ECN marked count 0 0
```

示例 (queue)

```
OS10# show queuing statistics interface ethernet 1/1/1 queue 3
Interface ethernet1/1/1
Queue Packets Bytes Dropped-
Packets Dropped-Bytes
3 0 0
0 0 0
```

支持的版本 10.2.0E or later

system qos

进入 SYSTEM-QOS 模式以配置系统级 QoS 配置。

|        |               |
|--------|---------------|
| 语法     | system qos    |
| 参数     | 无             |
| 默认     | 未配置           |
| 命令模式   | CONFIGURATION |
| 使用情况信息 | 无             |

示例

```
OS10(config)# system qos
OS10(config-sys-qos)#
```

支持的版本 10.2.0E or later

trust dot1p-map

为 dot1p 流创建用户定义的信任映射。

|        |                                                                          |
|--------|--------------------------------------------------------------------------|
| 语法     | trust dot1p-map map-name                                                 |
| 参数     | map-name — 输入 dot1p 信任映射的名称。最多 32 个字符。                                   |
| 默认     | 未配置                                                                      |
| 命令模式   | CONFIGURATION                                                            |
| 使用情况信息 | 如果启用信任，流量将符合 dot1p 映射。default-dot1p-trust 是保留的信任映射名称。此命令的 no 版本将值恢复为默认值。 |

示例

```
OS10(config)# trust dot1p-map map1
OS10(config-tmap-dot1p-map)# qos-group 4 dot1p 5
```

支持的版本 10.3.0E or later

## trust dscp-map

为 DSCP 流创建用户定义的信任映射。

|        |                                                                                                |
|--------|------------------------------------------------------------------------------------------------|
| 语法     | <code>trust dscp-map map-name</code>                                                           |
| 参数     | <code>map-name</code> — 输入 DSCP 信任映射的名称。最多 32 个字符。                                             |
| 默认     | 未配置                                                                                            |
| 命令模式   | CONFIGURATION                                                                                  |
| 使用情况信息 | 如果启用信任，流量将遵守此信任映射。 <code>default-dscp-trust</code> 是保留的信任映射名称。此命令的 <code>no</code> 版本将值恢复为默认值。 |
| 示例     | <pre>OS10(config)# trust dscp-map dscp-trust1</pre>                                            |
| 支持的版本  | 10.3.0E or later                                                                               |

## trust-map

在接口或系统 QoS 上配置信任映射。

|        |                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>trust-map {dot1p   dscp} {default   trust-map-name}</code>                                                                                                                                                                                                                                                                                                                                 |
| 参数     | <ul style="list-style-type: none"><li><code>dot1p</code> — 应用 dot1p 信任映射。</li><li><code>dscp</code> — 应用 dscp 信任映射。</li><li><code>default</code> — 应用默认 dot1p 或 dscp 信任映射。</li><li><code>trust-map-name</code> — 输入信任映射的名称。</li></ul>                                                                                                                                                            |
| 默认     | 已禁用                                                                                                                                                                                                                                                                                                                                                                                              |
| 命令模式   | INTERFACE<br>SYSTEM-QoS                                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | 使用 <code>show qos maps type [tc-queue   trust-map-dot1p   trust-map-dscp] [trust-map-name]</code> 命令查看当前的信任映射。只有在没有流量流的情况下，才能更改信任映射。验证是否应用了正确的策略映射。此命令的 <code>no</code> 版本将值恢复为默认值。此命令的 <code>no</code> 版本会从接口或系统 QoS 中删除应用的信任映射。                                                                                                                                                                |
| 示例     | <pre>OS10(config)# interface ethernet 1/1/10 OS10(conf-if-eth1/1/10)# trust-map dot1p default OS10(conf-if-eth1/1/10)# trust-map dot1p d1  OS10(config)# interface ethernet 1/1/2 OS10(conf-if-eth1/1/2)# trust-map dscp default OS10(conf-if-eth1/1/2)# trust-map dscp d2  OS10(config)# system qos OS10(config-sys-qos)# trust-map dot1p default OS10(config-sys-qos)# trust-map dscp d2</pre> |
| 支持的版本  | 10.4.1.0 or later                                                                                                                                                                                                                                                                                                                                                                                |

## wred

配置加权随机早期检测 (WRED) 配置文件。

|    |                                                   |
|----|---------------------------------------------------|
| 语法 | <code>wred wred-profile-name</code>               |
| 参数 | <code>wred-profile-name</code> — 输入 WRED 配置文件的名称。 |
| 默认 | 未配置                                               |

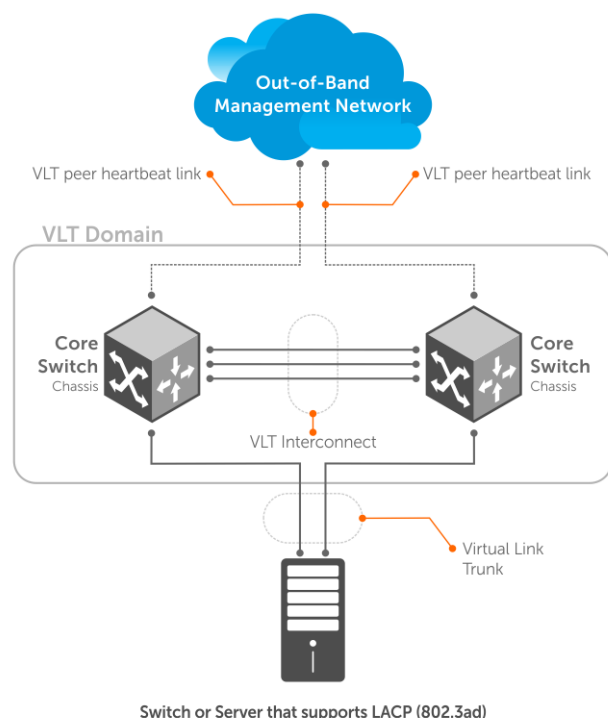
|        |                                                            |
|--------|------------------------------------------------------------|
| 命令模式   | CONFIGURATION                                              |
| 使用情况信息 | 此命令的 <code>no</code> 版本将移除 WRED 配置文件。                      |
| 示例     | <pre>OS10(config)# wred test_wred OS10(config-wred)#</pre> |
| 支持的版本  | 10.4.0E(R1) or later                                       |

## 虚拟链路中继

虚拟链路中继 (VLT) 是在终端设备（如服务器和两个或更多连接的网络设备）之间使用的第 2 层聚合协议。VLT 有助于聚合在多个交换机上端接的端口。OS10 当前在两个不同的交换机上支持 VLT 端口通道终端。

VLT:

- 通过使用在多个上游节点上端接的相同端口通道，提供节点级冗余。
- 提供无循环拓扑
- 消除 STP 阻止的端口
- 通过使用所有可用的上行链路带宽，优化带宽利用率
- 在链路或设备发生故障时保证快速聚合
- 使用虚拟路由器冗余协议 (VRRP)，增强优化转发
- 使用第 3 层 VLAN 的 VLT 对等路由，优化路由
- 提供链路级弹性
- 确保高可用性



从连接设备的角度来看，VLT 呈现了单个逻辑 L2 域，该设备具有在 VLT 域中不同节点上端接的虚拟链路中继。这两个 VLT 节点对于上游网络中的设备具有独立的第二层/第三层 (L2/L3) 交换机。L2/L3 控制平面协议和系统管理功能在两个 VLT 节点中正常工作。

支持 LACP 的外部交换机或服务器将两个 VLT 交换机视作单个虚拟交换机。因此，VLT 域中两个交换机上的 VLT 配置必须相同。

### VLT 物理端口

VLT 物理端口上支持 802.1p、802.1q、LLDP、流控制、端口监控和巨型帧。

### 系统管理协议

VLT 端口 (SNMP、AAA、ACL、DNS、FTP、SSH、系统日志、NTP、RADIUS、SCP 和 LLDP) 上支持所有系统管理协议。

### L3 VLAN 连接

通过为两个设备上的同一 VLAN 配置 VLAN 接口，在 VLT 对上启用 L3 VLAN 连接（这些 VLAN 分配有 IP VLT 地址）。



|                       |                                                                                                                                                            |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>使用 VRRP 进行优化转发</b> | 要确保 VLT 节点两端的行为相同，VRRP 需要状态信息协调。VRRP 主动-主动模式可优化 VLT 上的 L3 转发。默认情况下，在所有 VLAN 接口上启用 VRRP 主动-主动模式。VRRP 主动-主动模式允许每个对等节点在本地转发 L3 数据包，从而减少了对等节点之间通过 VLTi 链路的流量流。 |
| <b>生成树协议</b>          | VLT 端口支持 RSTP、RPVST+ 和 MSTP。                                                                                                                               |
| <b>多播</b>             | 在 VLT 端口上支持 IGMP 侦听和 MLD 侦听。                                                                                                                               |

**注:** 在 VLT 端口上不支持 802.1x 和 DHCP 侦听。

## 术语

|                      |                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------|
| <b>VLT 域</b>         | 域包括 VLT 对等节点设备、VLT 互连和连接到所连接设备的 VLT 中的所有端口通道。它也是您必须用来分配 VLT 全局参数的配置模式。                                  |
| <b>VLT 互连 (VLTi)</b> | 用于同步操作状态的 VLT 对等节点交换机之间的链路。                                                                             |
| <b>VLT 对等节点设备</b>    | 使用专用端口通道连接的一对设备 — VLTi。您必须单独配置 VLT 对等节点。                                                                |
| <b>查找接口</b>          | VLT 互连 (VLTi) 链路中 VLT 对等节点上的接口。                                                                         |
| <b>VLT MAC 地址</b>    | 分配给 VLT 域的唯一 MAC 地址。VLT MAC 地址是两个 VLT 对等节点中的通用地址。如果未配置 VLT MAC 地址，则主要对等节点的 MAC 地址将用作两个对等节点的 VLT MAC 地址。 |
| <b>VLT 节点优先级</b>     | 优先级基于确定的主要和辅助 VLT 节点。如果未配置优先级，则 MAC 地址最低的 VLT 节点将选择为主 VLT 节点。                                           |
| <b>VLT 端口通道</b>      | 连接的设备与 VLT 对等节点交换机之间的组合端口通道。                                                                            |
| <b>VLT 端口通道 ID</b>   | 将 VLT 对等节点上的端口通道接口分组为连接到所连接设备的单个虚拟链路中继。为您捆绑在一起的两个节点上的端口通道接口分配统一端口通道 ID。                                 |
| <b>孤立端口</b>          | 不属于 VLT 端口通道但属于跨区 VLAN 的成员的端口。术语“跨区 VLAN”指在两个 VLT 对等节点上配置的 VLAN。                                        |

## VLT 域

VLT 域包括 VLT 对等设备、VLTi 和所有连接到所连接设备的 VLT 端口通道。它也是您必须用来分配 VLT 全局参数的配置模式。

- 每个 VLT 域必须具有您创建的唯一 MAC 地址或 VLT 自动创建。
  - VLAN ID 4094 作为 VLT 域的内部控制 VLAN 保留。在此控制 VLAN 上使用 IPv6 寻址来 VLT 对等通信。
  - ARP、IPv6 邻居和 MAC 表在 VLT 对等节点之间同步。
  - VLT 对等设备作为单独的节点运行，并为连接到非 VLT 端口的设备提供独立的控制 and 数据平面。
  - VLT 域中的一个节点采用主角色，而另一个节点承担辅助角色。在具有两个节点的 VLT 域中，默认情况下，VLT 将主节点角色分配给具有最低 MAC 地址的节点。您可以通过使用 `primary-priority` 命令为每个节点分配优先级来覆盖默认的主选举机制。
  - 如果主要对等主机发生故障，次要对等主机会承担主角色。如果主对等主机（优先级较低）后来恢复联机状态，则会为其分配次要角色（没有抢占）。
  - 在 VLT 域中，对等网络设备必须运行相同的 OS10 软件版本。
- 注:** 在升级过程中允许临时例外。有关详细信息，请参阅 *Dell EMC SmartFabric OS 10.5.0.x Release Notes*。
- 在对等设备上配置相同的 VLT 域 ID。如果 VLT 对等主机上发生 VLT 域 ID 不匹配，VLTi 将不会激活。
  - 在 VLT 域中，VLT 对等控制器支持连接到仅连接到一个对等节点的网络设备。
  - 配置 VLT 域时，系统将生成 VLT 的单元 ID。您不能更改 VLT 单元 ID。要识别 VLT 域中的 VLT 节点，请使用 `show vlt` 命令。

## VLT 互连

VLT 互连 (VLTi) 会同步 VLT 对等节点之间的状态。OS10 会自动将 VLTi 端口添加到跨 VLT 对等节点上的 VLAN，但不会将 VLTi 端口添加到仅一个对等上配置的 VLAN。

- VLAN ID 4094 保留为 VLT 域的内部控制 VLAN，并且用户不可配置。
- 端口通道 1000 是为 VLTi 链路保留的，用户不可配置。
- VLTi 将跨两个节点同步 L2 和 L3 控制平面信息。仅当存在需要 VLTi 到达最终目标的链路故障时，才能将 VLTi 用于数据流量。
- 具有未知目标 MAC 地址、多播或广播流量的流量可能会导致跨 VLTi 泛洪。
- MAC、ARP IPv6 在 VLT 对等节点上通过 VLAN 进行学习的邻居使用 VLTi 进行同步。
- VLTi 支持 LLDP、流控制、端口监控和巨型帧功能。默认情况下，VLTi 端口设置为支持的最大 MTU 值。

## 正常 LACP 和 VLT

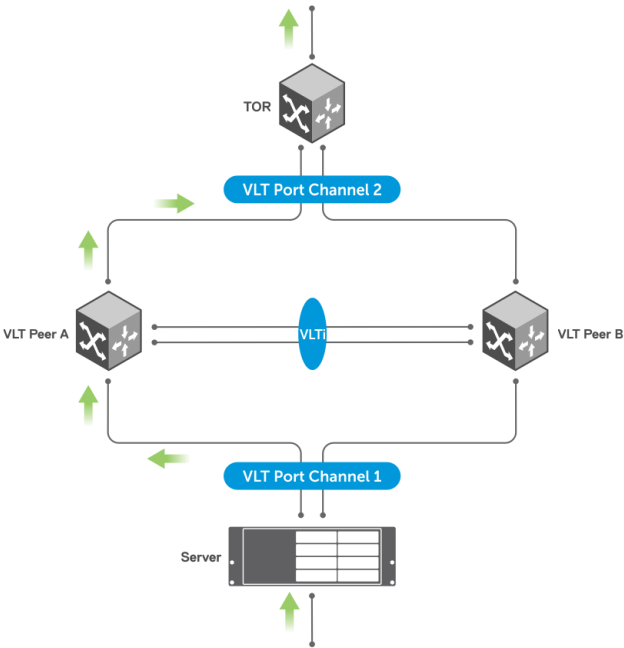
重新加载 VLT 节点时，包括 VLT 端口通道接口在内的所有接口都会停止。在 VLT 端口通道接口的另一端连接的架顶式 (ToR) 设备可能需要很长时间来检测接口状态更改并将流量切换到另一个活动 VLT 节点。通过使用 LACP PDU，正常的 LACP 功能使 VLT 节点可在接管 VLT 端口通道接口的成员端口之前通知 ToR 设备。因此，正常 LACP 功能使 ToR 设备可以将流量切换到另一个活动 VLT 节点。

在以下情况下支持正常 LACP：

- 重新加载 VLT 节点时
- 当辅助 VLT 节点检测到 VLTi 链路停止运行，但心跳信号正常工作时

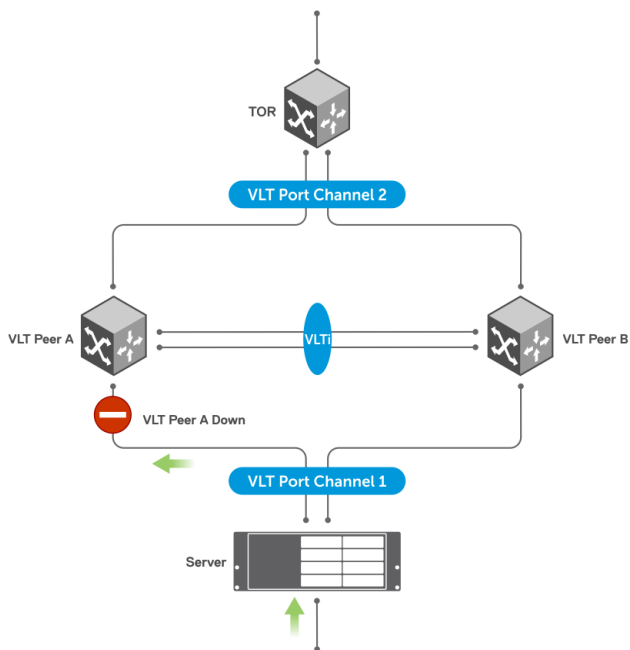
默认情况下，正常 LACP 处于启用状态，并且您无法将其禁用。

下面显示了 VLT 设置的正常行为，其中的数据流过到目标的最佳路径：

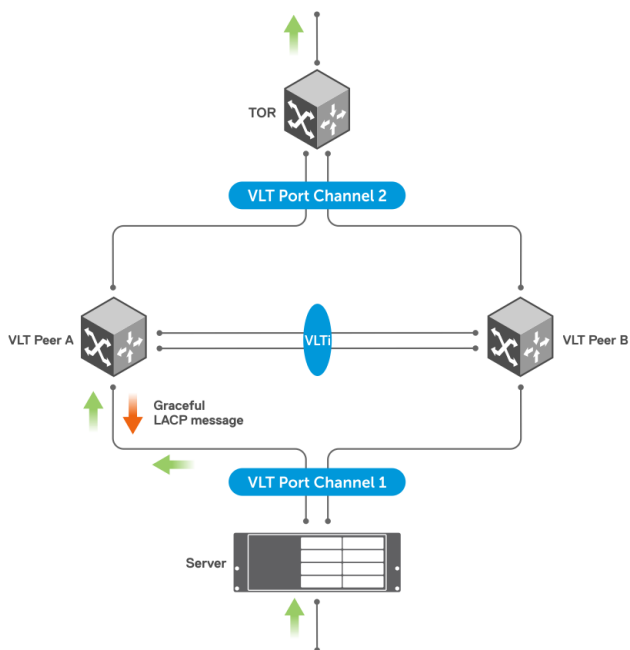


下图显示了正在重新加载或即将停止 VLT 对等节点 A 的情况：

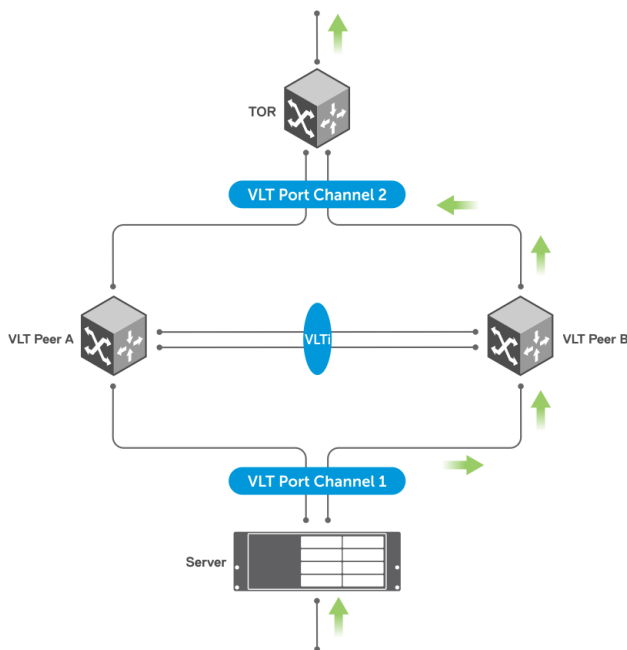
在 LACP 会合之前，服务器会继续将流量转发到 VLT 对等节点，从而导致流量丢失，从而延长时间间隔。



通过正常 LACP，VLT 对等节点将正常 LACP PDU 发送至所有 VLT 成员端口，如下所示：



这些 PDU 将通知服务器移将流量定向到 VLT 对等节点 B，从而更大限度地降低流量损失。



## 配置 VLT

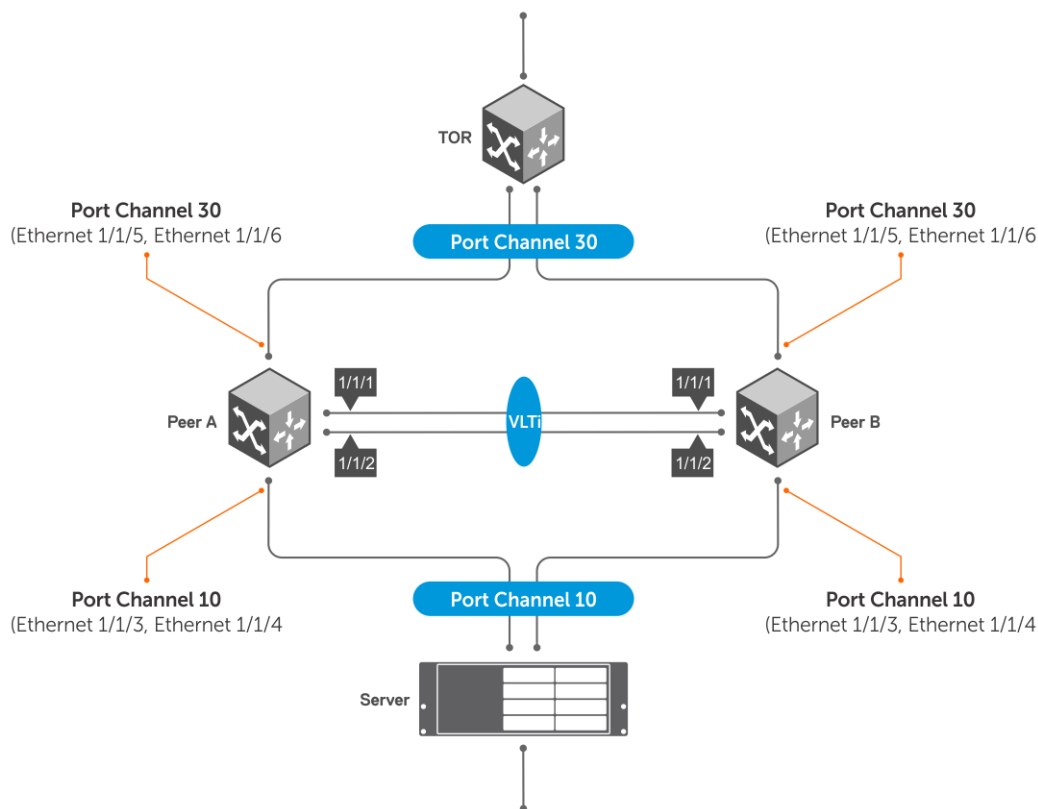
验证两个 VLT 对等设备是否运行相同的操作系统版本。对于 VRRP 操作，请在每个 VLT 对等上配置 VRRP 组和 L3 路由。

分别在每个 VLT 对等设备上配置以下设置：

1. 为防止 VLT 域中的循环，Dell EMC Networking 建议使用 `spanning-tree mode` 命令在全局范围内启用 STP。启用 STP 可防止故障布线导致的意外回路。
2. 通过在每个对等主机上使用 `vlt-domain` 命令配置相同的域 ID 来创建 VLT 域。
3. （可选）要基于 VLT 节点的系统 MAC 地址覆盖默认 VLT 主选举机制，请使用 `primary-priority` 命令为每个 VLT 节点配置 VLT 节点优先级。为所需的主 VLT 对等节点输入较低的优先级值，并为所需的从属 VLT 对等节点提供更高优先级值。

**注：**如果重新加载了 VLT 对等节点，则它将自动成为辅助对等节点，而不考虑 VLT 的主要优先级设置。

4. 使用 `no switchport` 命令可配置 VLTi 接口。
5. 使用 `discovery-interface` 命令可配置每个对等节点上的 VLTi 接口。在配置 VLTi 的两端后，如果未配置主优先级，将自动分配 VLT 域中的主要和辅助角色。
6. （可选）手动重新配置默认的 VLT MAC 地址。在两个 VLT 对等节点中配置相同的 VLT MAC 地址。手动配置可更大程度地减少当一个对等交换机重新引导时，在两个对等设备上同步 VLT 域的默认 MAC 地址所需的时间。
7. （可选）配置非默认时间间隔，以延迟在重新加载后或在关闭或失败后 VLTi 出现故障时，延迟在辅助 VLT 对等节点中启动 VLT 端口。默认时间间隔为 90 秒。
8. 使用 `backup destination {ip-address | ipv6 ipv6-address} [vrf management] [interval interval-time]` 命令配置 VLT 心跳备份链路。
9. 使用 `vlt-port-channel` 命令配置 VLT 对等节点与连接的设备之间的 VLT 端口通道。从 1 到 128 将同一 VLT 端口通道 ID 分配给您捆绑在一起的不同对等节点上的接口。对等接口显示为到下游设备的单个 VLT 端口通道。
10. 将 VLT 域中的对等设备连接到已连接的访问设备或服务器。



## 配置生成树协议

Dell EMC Networking 建议在两个 VLT 对等节点上配置一种受支持的生成树协议（MSTP、RSTP 或 RPVST+）。

在 VLT 启动阶段和孤立端口的情况下，使用生成树协议进行初始环回预防。在对等交换机上配置 VLT 之前，在网络中配置生成树协议。

**注：**RPVST+ 默认已启用。

## RPVST+ 配置

在两个 VLT 对等节点上配置 RPVST+。这会为系统中配置的每个 VLAN 创建 RPVST+ 实例。在两个 VLT 节点上配置了 RPVST+ 时，OS10 支持最多 60 个 VLAN。主 VLT 对等节点中的 RPVST+ 实例控制主要和次要对等主机上的 VLT 端口通道。

**注：**RPVST+ 是交换机上运行的默认 STP 模式。仅当您在交换机上运行 STP 的另一种变体时，才能使用以下命令。

- 在 CONFIGURATION 模式下的每个对等节点上启用 RPVST+。

```
spanning-tree mode rapid-pvst
```

### 配置 RPVST+ — 对等节点 1

```
OS10(config)# spanning-tree mode rapid-pvst
```

### 配置 RPVST+ — 对等节点 2

```
OS10(config)# spanning-tree mode rapid-pvst
```

### 查看 VLTi 上的 RPVST+ 信息

```
OS10# show spanning-tree virtual-interface
```

```
VFP(VirtualFabricPort) of vlan 100 is Designated Blocking
```

```

Edge port: No (default)
Link type: point-to-point (auto)
Boundary: No, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-
violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 7, Received: 9
Interface
Name PortID Prio Cost Sts Cost Designated
ID PortID

VFP(VirtualFabricPort) 0.1 0 1 BLK 0 4196
90b1.1cf4.a602 0.1

```

**i** 注: 要查看所有其他端口, 请使用 `show spanning-tree active` 命令。

## 详细查看 VLTi 上的 RPVST+ 信息

```

OS10# show spanning-tree virtual-interface detail
Port 1 (VFP(VirtualFabricPort)) of vlan1 is designated Forwarding
Port path cost 1, Port priority 0, Port Identifier 0.1
Designated root priority: 4097, address: 90:b1:1c:f4:a6:02
Designated bridge priority: 4097, address: 90:b1:1c:f4:a6:02
Designated port ID: 0.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 202, Received: 42
Port 1 (VFP(VirtualFabricPort)) of vlan100 is designated Forwarding
Port path cost 1, Port priority 0, Port Identifier 0.1
Designated root priority: 4196, address: 90:b1:1c:f4:a6:02
Designated bridge priority: 4196, address: 90:b1:1c:f4:a6:02
Designated port ID: 0.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 101, Received: 21

```

## RSTP 配置

- 在 CONFIGURATION 模式下的每个对等节点上启用 RSTP。

```
spanning-tree mode rstp
```

### 配置 RSTP - 对等 1

```
OS10(config)# spanning-tree mode rstp
```

### 配置 RSTP - 对等 2

```
OS10(config)# spanning-tree mode rstp
```

## 查看 VLTi 特定的 STP 信息

```

OS10# show spanning-tree virtual-interface
VFP(VirtualFabricPort) of RSTP 1 is Designated Forwarding
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: No, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-
violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 11, Received: 7
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated
ID PortID

VFP(VirtualFabricPort) 0.1 0 1 FWD 0 32768 0078.7614.6062 0.1

```

 **注:** 要查看所有其他端口, 请使用 `show spanning-tree active` 命令。

### 查看 STP 虚拟接口详细信息

```
OS10# show spanning-tree virtual-interface detail
Port 1 (VFP(VirtualFabricPort)) of RSTP 1 is designated Forwarding
Port path cost 1, Port priority 0, Port Identifier 0.1
Designated root priority: 32768, address: 00:78:76:14:60:62
Designated bridge priority: 32768, address: 00:78:76:14:60:62
Designated port ID: 0.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 15, Received: 5
```

## MSTP 配置

在 VLT 节点上启用多个生成树协议 (MSTP) 时, 在同一个 MST 区域中配置两个 VLT 对等节点, 以避免网络循环。确保两个 VLT 对等节点上的 VLAN 到实例映射、地区名称和版本 ID 相同。

 **注:** OS10 最多支持 64 个 MST 实例。

要配置 MSTP over VLT, 请在两个 VLT 对等节点上执行以下步骤:

1. 启用 MSTP。  
CONFIGURATION 模式  
`spanning-tree mode mst`
2. 进入 MST 配置模式。  
CONFIGURATION 模式  
`spanning tree mst configuration`
3. 创建 MST 实例并根据需要添加多个 VLAN。  
MULTIPLE-SPANNING-TREE  
`instance instance-number vlan from-vlan-id - to-vlan-id`
4. 配置 MST 版本号, 从 0 到 65535。  
MULTIPLE-SPANNING-TREE  
`revision revision-number`
5. 配置 MST 区域名称。  
MULTIPLE-SPANNING-TREE  
`name name-string`

以下示例显示了两个 VLT 节点均配置了同一个 MST VLAN 到实例映射。

#### VLT Peer 1 configuration

```
OS10(config)# spanning-tree mode mst
OS10(config)# spanning-tree mst configuration
OS10(conf-mst)# instance 1 vlan 2-10
OS10(conf-mst)# revision 10
OS10(conf-mst)# name ExampleMSTregion
```

#### VLT Peer 2 configuration

```
OS10(config)# spanning-tree mode mst
OS10(config)# spanning-tree mst configuration
OS10(conf-mst)# instance 1 vlan 2-10
OS10(conf-mst)# revision 10
OS10(conf-mst)# name ExampleMSTregion
```

以下示例显示了有关 VLTi 的 MSTP 信息:

 **注:** 要查看所有其他端口, 请使用 `show spanning-tree active` 或 `show spanning-tree msti` 命令。

```
OS10# show spanning-tree virtual-interface
VFP(VirtualFabricPort) of MSTI 0 is Designated Forwarding
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: Yes, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 387, Received: 16
Interface
Name PortID Prio Cost Sts Cost Designated
PortID

-VFP(VirtualFabricPort) 0.1 0 1 FWD 0 32768
3417.ebf2.a8c4 0.1

VLT-LAG -1(vlt-portid-1) of MSTI 0 is in Designated Forwarding
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: No, Bpdu-filter: Disable, Bpdu-Guard: Disable,
Shutdown-on-Bpdu-Guard-violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 1234, Received: 123

Virtual
Interface
Name PortID Prio Cost Sts Cost Designated
PortID

-
VLT-LAG -1(vlt-portid1) 128.2001 128 2000000 FWD 0 32768
90b1.1cf4.a523 128.2001
```

 **注:** 要查看所有其他端口, 请使用 `show spanning-tree active` 命令。

以下示例详细显示了有关 VLTi 的 MSTP 信息:

```
OS10# show spanning-tree virtual-interface detail
Port 1 (VFP(VirtualFabricPort)) of MSTI 0 is designated Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.1
Designated root priority: 32768, address: 34:17:44:55:66:7f
Designated bridge priority: 32768, address: 90:b1:1c:f4:a5:23
Designated port ID: 128.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 2714, Received: 1234

Port 2001 (VLT-LAG -1(vlt-portid-1)) of MSTI 0 is designated Forwarding
Port path cost 200000, Port priority 128, Port Identifier 128.2001
Designated root priority: 32768, address: 34:17:44:55:66:7f
Designated bridge priority: 32768, address: 90:b1:1c:f4:a5:23
Designated port ID: 128.2001, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 2714, Received: 1234
```

## 创建 VLT 域

VLT 域需要 ID 编号。在两个对等节点上配置相同的 VLT 域 ID。有关详情, 请参阅 [VLT 域](#) 一节。no vlt-domain 命令将禁用 VLT。禁用 VLT 可能会导致网络中的循环。因此, 请慎重使用命令的 no 格式。

1. 配置 VLT 域并进入 VLT-DOMAIN 模式。在每个对等节点上配置相同的 VLT 域 ID, 从 1 到 255。

```
vlt-domain domain-id
```

2. 在 VLT 对等节点上重复步骤以创建 VLT 域。



## 对等节点 1

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)#
```

## 对等节点 2

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)#
```

# 配置 VLTi

在对等接口上配置 VLTi 之前，请使用 `no switchport` 命令从 L2 模式中移除每个接口。有关详情，请参阅 [VLT 互连](#) 部分。

1. 输入要从 CONFIGURATION 模式进入的 VLT 域 ID。

```
vlt-domain domain-id
```

2. 配置一个或连字符分隔的 VLT 对等接口的范围，以便在 INTERFACE 模式下成为 VLTi 的成员。

```
discovery-interface {ethernet node/slot/port[:subport] | ethernet node/slot/
port[:subport] -node/slot/port[:subport]}
```

3. 在 VLT 对等节点上重复步骤。

## 对等节点 1

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# exit
OS10(config)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# exit
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# discovery-interface ethernet1/1/1
OS10(conf-vlt-1)# discovery-interface ethernet1/1/2
```

## 对等节点 2

```
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# no switchport
OS10(conf-if-eth1/1/1)# exit
OS10(config)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# no switchport
OS10(conf-if-eth1/1/2)# exit
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# discovery-interface ethernet1/1/1-1/1/2
```

# 配置 VLT MAC 地址

您可以手动配置 VLT MAC 地址。

在两个 VLT 对等交换机上配置相同的 VLT MAC 地址，以避免在 VLT 故障切换期间出现任何不可预知的行为。例如，当某个设备停机或 VLTi 重置时。如果未配置 VLT MAC 地址，则主要对等节点的 MAC 地址将用作所有对等节点的 VLT MAC 地址。

使用 `vlt-mac mac-address` 以在两个 VLT 对等节点中配置 MAC 地址。

## 配置示例：

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# vlt-mac 00:00:00:00:00:02
```

 **注：** Dell EMC Networking 建议在 VLT 对等交换机上手动配置 VLT MAC 地址。在两个对等节点上使用相同的 MAC 地址。

## 配置延迟还原计时器

当辅助 VLT 节点引导时，它会等待预配置的时间量（延迟还原），以还原 VLT 端口状态。此延迟允许 VLT 对等节点完成控制数据信息交换。

如果在 VLTi 链路发生故障时对等 VLT 设备正常运行，则在 VLT 对等交换机之间进行重新加载或对等链路还原后系统会延迟启动 VLT 端口。

当两个 VLT 对等节点启动并运行时，如果 VLTi 出现故障并且显示 VLT 心跳信号，则辅助对等节点将关闭 VLT 端口。当 VLTi 启动时，从属对等节点不会立即启动其 VLT 端口。只有在 VLT 端口还原计时器过期后，VLT 端口才会启动。延迟还原计时器允许两 VLT 个对等节点将控制信息相互同步。

默认计时器为 90 秒。您可以使用 `delay-restore seconds` 命令来修改计时器的持续时间。

**示例：**

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# delay-restore 100
```

## 配置 VLT 对等节点存活检查

VLT 对等节点存活机制检查对等节点是否可用。系统将发送定期存活活动消息，以检测对等节点的存活。对于对等节点存活检查，您必须使用不同于 VLTi 的链路。此链路称为 VLT 备份链路。

**注：** Dell EMC Networking 建议使用 VLT 备份链路的 OOB 管理网口连接。

如果 VLTi 停机，备份链路可帮助区分对等节点故障的 VLTi 链路故障。如果 VLTi 中的所有链路均出现故障，VLT 节点将通过备份链路交换节点存活信息。

基于节点存活信息：

- 如果只有 VLTi 链路失败，但对等节点处于活动状态，则辅助 VLT 对等节点将关闭其 VLT 端口。
- 如果主 VLT 节点发生故障，则 VLTi 和心跳信号都会失败，并且当前辅助对等节点将接管主角色。

使用 `backup destination {ip-address | ipv6 ipv6-address} [vrf management] [interval interval-time]` 配置 VLT 备份链路。interval 范围从 1 至 30 秒。默认间隔为 30 秒。无论配置的时间间隔如何，当 VLTi 链路失败时，系统会检查心跳信号连接，而不等待计时间隔，从而允许更快的融合。

**注：** 在 SmartFabric 服务模式下，从版本 10.5.0 开始配置 VLT 域和备份参数。

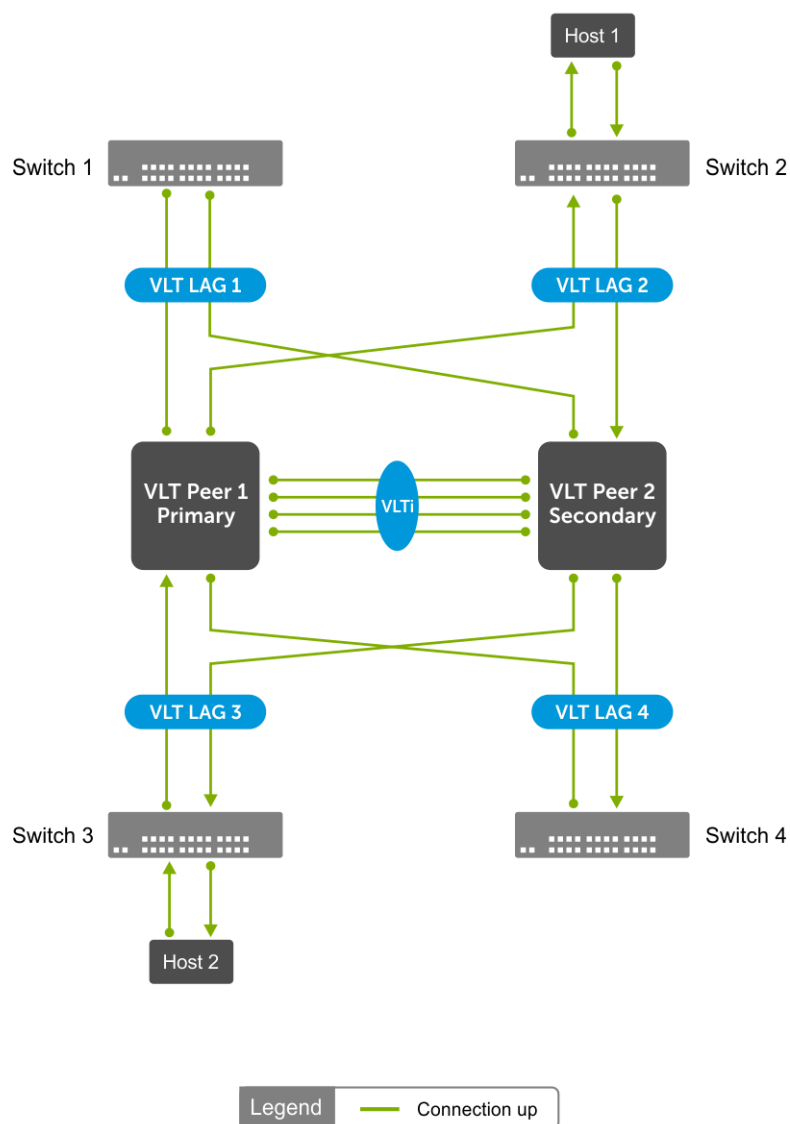
**配置示例：**

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination 10.16.151.110 vrf management interval 20

OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# backup destination ipv6 1::1 vrf management interval 20
```

以下示例描述了使用 VLT 备份链路的不同案例：

在下图中，未配置备份链路：



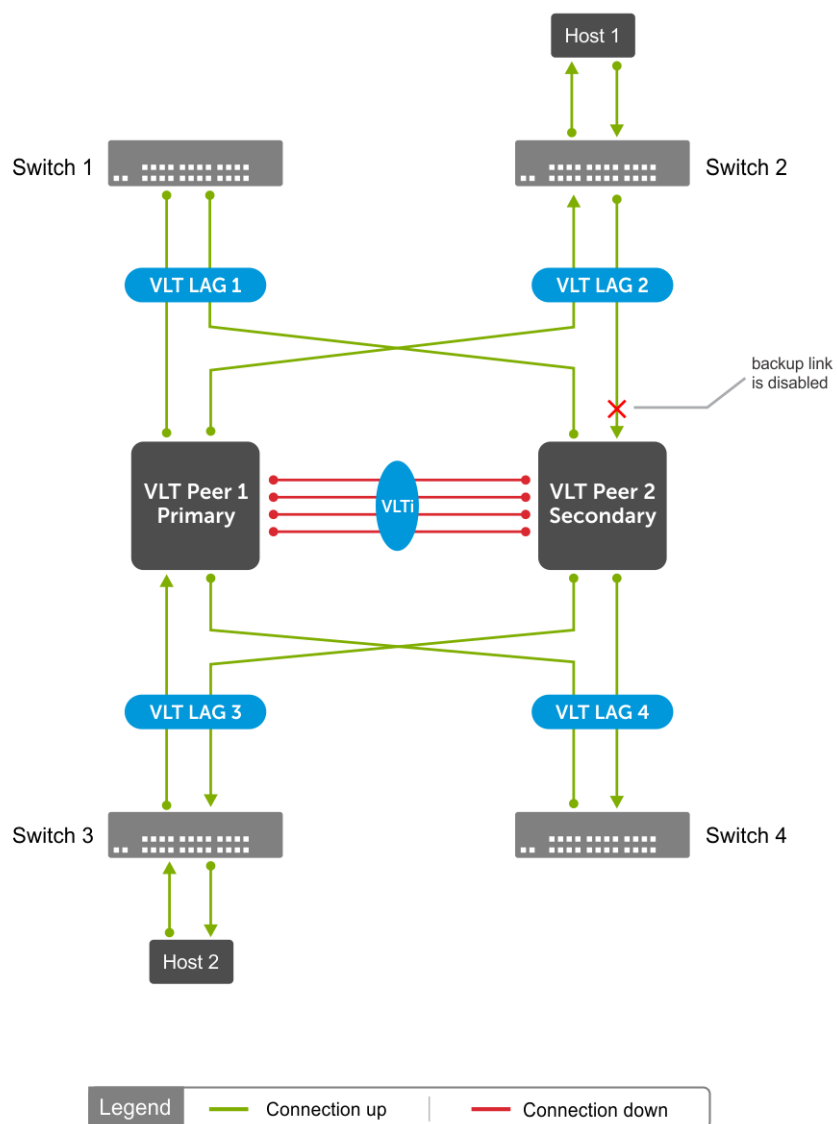
### 在 VLTi 故障期间支持新流

如果 VLTi 失败，在故障后学习的 MAC 地址不会与 VLT 对等节点同步。因此，VLTi 失败会导致流量持续泛洪，而不是单播。

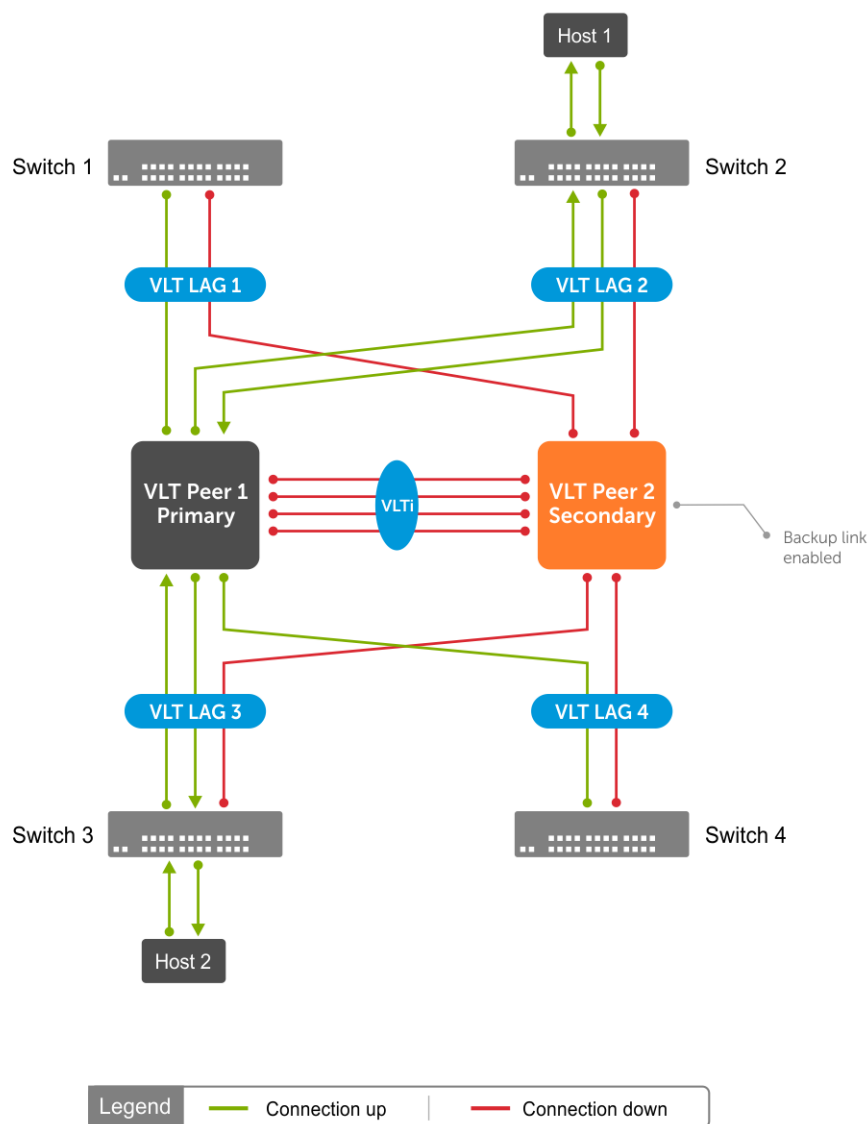
如果 VLTi 链路失败，则不会发生 MAC 和 ARP 同步。因此，系统会泛洪 L2 数据包并丢弃 L3 数据包。

例如，在下图中，当 VLTi 关闭后，VLT 对等节点 1 会学习主机 2 的 MAC 地址：

由于 VLTi 链路停止，VLT 对等节点 2 未与主机 2 的 MAC 地址同步。如果从主机 1 的流量发送到 VLT 对等节点 2，则 VLT 对等节点 2 会使流量泛洪。



启用 VLT 备份链路后，辅助 VLT 对等节点 2 通过备份链路标识节点存活。如果主要节点正常运行，则辅助对等存活将关闭 VLT 的端口通道。现在，来自主机 1 的流量达到 VLT 对等节点 1，然后到达目标主机 2。在这种情况下，流量是单播，而非泛洪，如下图所示：

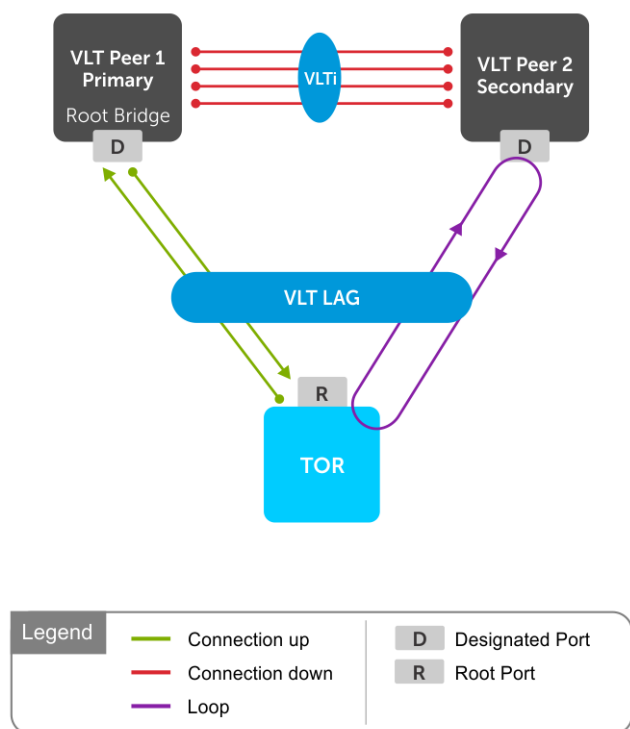


### 在 VLTi 发生故障期间防止循环 VLT 备份链路的角色

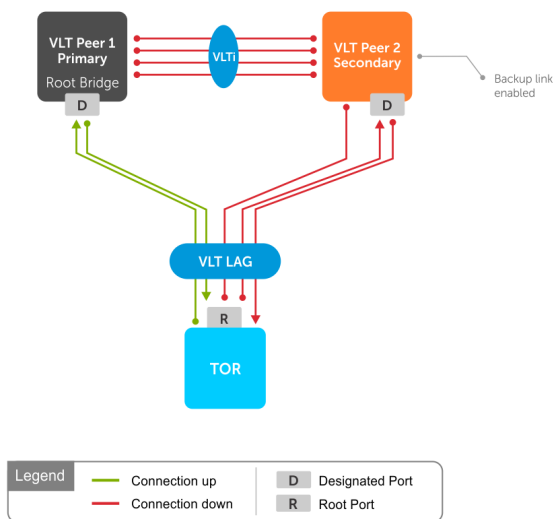
当 VLTi 停止时，STP 可能无法检测到系统中的任何循环，这会在 L2 网络中创建数据环。

在下图中，STP 在所有三个交换机中运行：

在稳定状态下，VLT 对等节点 1 被选作根桥。当 VLTi 停止时，两个 VLT 节点都会成为主要节点。在此状态下，VLT 对等节点 2 将 STP BPDU 发送到 TOR 时，假定 TOR 将 BPDU 发送到 VLT 对等节点 1。因此，VLT 对等节点 2 不会接收 VLT 端口上的 BPDU，但会从孤立端口接收 TOR BPDU。VLT 对等节点 2 中的 STP 假定系统中没有循环，并且同时打开了 VLT 和孤立端口。打开 VLT 和孤立端口会在系统中创建一个数据环，从而导致系统中断。



启用 VLT 备份链路后，辅助 VLT 对等主机通过备份链路标识主节点存活。如果主 VLT 对等节点正常运行，则辅助 VLT 对等节点将关闭 VLT 端口通道。在这种情况下，STP 将打开孤立端口，在系统中不存在任何循环，如下图所示：



## 配置 VLT 端口通道

VLT 端口通道（也称为虚拟链路中继）会关联连接的设备和 VLT 对等交换机。OS10 的每个节点最多支持 128 个 VLT 端口通道。

1. 在 INTERFACE 模式下输入端口通道 ID VLT 编号（从 1 到 128）。

```
interface port-channel id-number
```

2. 将同一 ID 分配给每个 VLT 对等上的 VLT 端口通道。对等是指到下游设备的单个交换机。

```
vlt-port-channel vlt-port-channel-id
```

3. 在 VLT 对等节点上重复步骤。

## 配置 VLT 端口通道 — 对等节点 1

```
OS10(config)# interface port-channel 20
OS10(conf-if-po-20)# vlt-port-channel 20
```

## 配置 VLT 端口通道 — 对等节点 2

```
OS10(config)# interface port-channel 20
OS10(conf-if-po-20)# vlt-port-channel 20
```

# 配置 VLT 对等路由

VLT 对等路由可启用优化的路由，其中为 VLT 对等方的 L3 端点发送的数据包在本地进行路由。VLT 支持对 IPv4 和 IPv6 流量进行单播路由。

要启用 VLT 单播路由，两个 VLT 对等都必须处于 L3 模式。在两个对等主机上的 VLAN 配置必须对称。您不能将同一 VLAN 配置为一个节点上的 L2 和另一个节点上的 L3。

1. 在 CONFIGURATION 模式下输入 VLT 域 ID，从 1 到 255。

```
vlt-domain domain-id
```

2. 在 VLT 域模式下启用对等路由。

```
peer-routing
```

3. 在 VLT 对等节点上重复步骤。

## 配置单播路由 - 对等 1

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# peer-routing
```

## 配置单播路由 - 对等 2

```
OS10(config)# vlt-domain 1
OS10(conf-vlt-1)# peer-routing
```

# 配置 VRRP 主动-主动模式

要启用通过 VLT 转发优化 L3，请使用 VRRP 主动-主动模式。默认情况下，在 VLAN 接口上已启用 VRRP 主动-主动模式。在这种模式下，每个对等节点会在本地转发 L3 流量，从而消除 VLTi 链路中的流量流。在每个对等主机上配置相同的静态和动态 L3 路由，以确保两个对等控制器上的 L3 可访问性和路由表相同。

1. 在 VLAN-INTERFACE 模式下启用 VRRP 主动-主动模式。

```
vrrp mode active-active
```

2. 在横跨两个对等节点的 L3 VLAN 上配置 VRRP。
3. 在 VLT 对等节点上重复步骤。

## 配置 VRRP 主动-主动模式 — 对等节点 1

```
OS10(conf-if-vl-10)# vrrp mode active-active
```

 **注：** VRRP 主动-主动是默认模式。

## 配置 VRRP 主动-主动模式 — 对等节点 2

```
OS10(conf-if-vl-10)# vrrp mode active-active
```

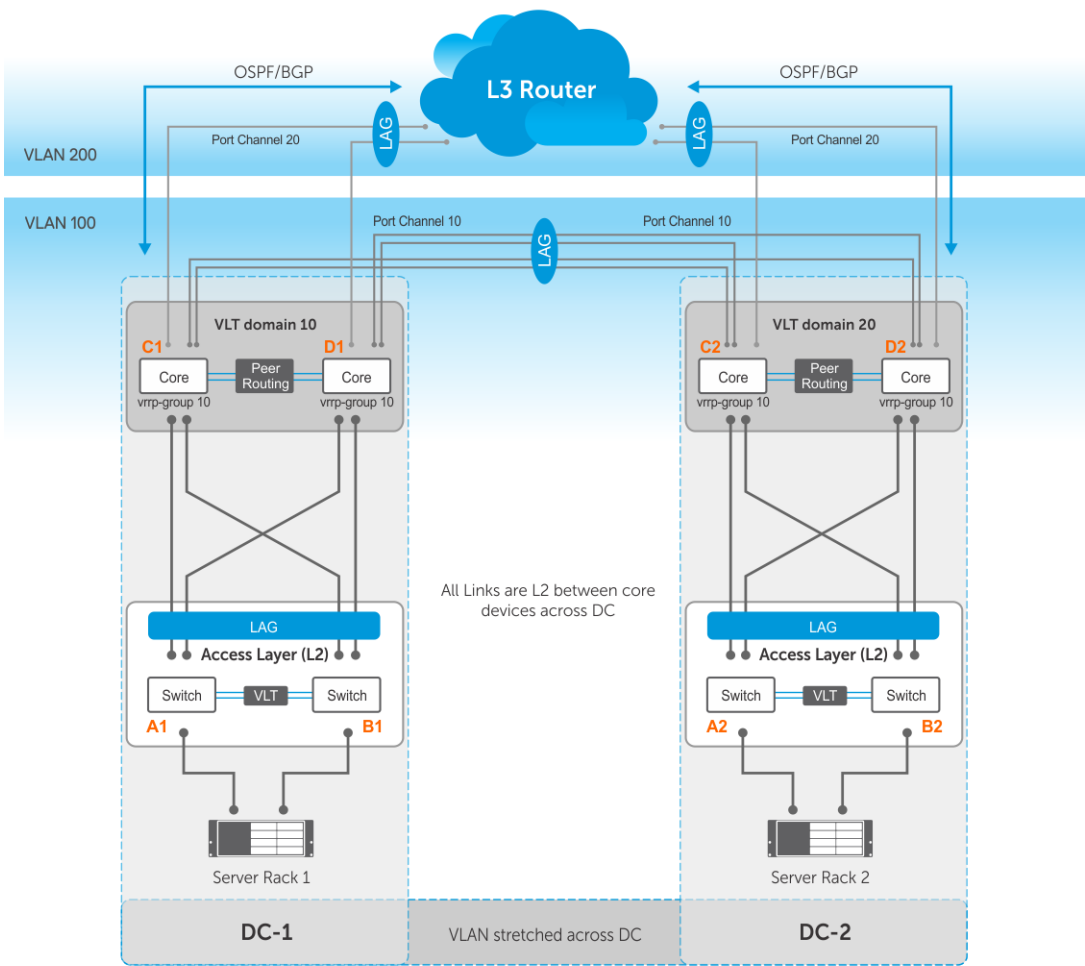
# 通过 eVLT 在数据中心之间迁移虚拟机

OS10 交换机支持使用 VRRP 主动-主动模式在数据中心之间移动虚拟机 (VM)。

在跨数据中心扩展或跨区的 VLAN 中配置具有相同 VRRP 组 ID 和虚拟 IP 的对称 VRRP。虚拟机使用 VLAN 的 VRRP 虚拟 IP 地址作为网关 IP。由于 VLAN 配置在数据中心内对称，因此您可以将虚拟机从一个数据中心移到另一个。

您必须在三级模式下为 VLAN 分配相同的 VRRP 组 ID，并且 VRRP 处于主动-主动模式。

下图显示了具有两个数据中心的配置示例：



- 服务器机架、机架 1 和机架 2 分别是数据中心 DC1 和 DC2 的一部分。
  - 机架 1 连接到 L2 网络段中的设备 A1 和 B1。
  - 机架 2 连接到 L2 网络段中的设备 A2 和 B2。
  - A1 和 B1 之间存在 VLT 端口通道，以及 A2 和 B2。
  - A1 和 B1 连接到核心路由器 C1 和 D1（已启用 VLT 路由）。
  - A2 和 B2 连接到核心路由器 C2 和 D2（已启用 VLT 路由）。
  - 数据中心通过直接链接或 eVLT 连接。
  - 本地 VLT 域中的核心路由器 C1 和 D1 使用 VLT 链路连接到远程 VLT 域中的核心路由器 C2 和 D2。
  - 本地 VLT 域中的核心路由器 C1 和 D1 以及远程 VLT 域中的 C2 和 D2 是 L3 云的一部分。
  - 核心路由器 C1、D1、C2、D2 位于具有相同 VRRP 组 ID 的 VRRP 组中。
- 当在服务器机架 1 中运行的虚拟机迁移到服务器机架 2 时，将在不中断的情况下路由该虚拟机的 L3 数据包。

### C1 配置示例：

- 在核心路由器之间配置 L2 链路上的 VRRP：

```
C1(config)# interface vlan 100
C1(conf-if-vl-100)# ip address 10.10.100.1/24
C1(conf-if-vl-100)# vrrp-group 10
```



```
C1(conf-vlan100-vrid-10)# priority 250
C1(conf-vlan100-vrid-10)# virtual-address 10.10.100.5
```

- **为 VLAN 100 配置 VLT 端口通道:**

```
C1(config)# interface port-channel 10
C1(conf-if-po-10)# vlt-port-channel 10
C1(conf-if-po-10)# switchport mode trunk
C1(conf-if-po-10)# switchport trunk allowed vlan 100
C1(conf-if-po-10)# exit
```

- **将成员添加到端口通道 10:**

```
C1(config)# interface ethernet 1/1/3
C1(conf-if-eth1/1/3)# channel-group 10
C1(conf-if-eth1/1/3)# exit
C1(config)# interface ethernet 1/1/4
C1(conf-if-eth1/1/4)# channel-group 10
C1(conf-if-eth1/1/4)# exit
```

- **在核心路由器的 L3 端配置 OSPF:**

```
C1(config)# router ospf 100
C1(config-router-ospf-100)# redistribute connected
C1(config-router-ospf-100)# exit
C1(config)# interface vlan 200
C1(conf-if-vl-200)# ip ospf 100 area 0.0.0.0
```

- **为 VLAN 200 配置 VLT 端口通道:**

```
C1(config)# interface port-channel 20
C1(conf-if-po-20)# vlt-port-channel 20
C1(conf-if-po-20)# switchport mode trunk
C1(conf-if-po-20)# switchport trunk allowed vlan 200
C1(conf-if-po-20)# exit
```

- **将成员添加到端口通道 20:**

```
C1(config)# interface ethernet 1/1/5
C1(conf-if-eth1/1/5)# channel-group 20
C1(conf-if-eth1/1/5)# exit
C1(config)# interface ethernet 1/1/6
C1(conf-if-eth1/1/6)# channel-group 20
C1(conf-if-eth1/1/6)# exit
```

## D1 配置示例:

- **在核心路由器之间配置 L2 链路上的 VRRP:**

```
D1(config)# interface vlan 100
D1(conf-if-vl-100)# ip address 10.10.100.2/24
D1(conf-if-vl-100)# vrrp-group 10
D1(conf-vlan100-vrid-10)# virtual-address 10.10.100.5
```

- **为 VLAN 100 配置 VLT 端口通道:**

```
D1(config)# interface port-channel 10
D1(conf-if-po-10)# vlt-port-channel 10
D1(conf-if-po-10)# switchport mode trunk
D1(conf-if-po-10)# switchport trunk allowed vlan 100
D1(conf-if-po-10)# exit
```

- **将成员添加到端口通道 10:**

```
D1(config)# interface ethernet 1/1/3
D1(conf-if-eth1/1/3)# channel-group 10
D1(conf-if-eth1/1/3)# exit
D1(config)# interface ethernet 1/1/4
D1(conf-if-eth1/1/4)# channel-group 10
D1(conf-if-eth1/1/4)# exit
```

- 在核心路由器的 L3 端配置 OSPF:

```
D1(config)# router ospf 100
D1(config-router-ospf-100)# redistribute connected
D1(config-router-ospf-100)# exit
D1(config)# interface vlan 200
D1(config-if-vl-200)# ip ospf 100 area 0.0.0.0
```

- 为 VLAN 200 配置 VLT 端口通道:

```
D1(config)# interface port-channel 20
D1(config-if-po-20)# vlt-port-channel 20
D1(config-if-po-20)# switchport mode trunk
D1(config-if-po-20)# switchport trunk allowed vlan 200
D1(config-if-po-20)# exit
```

- 将成员添加到端口通道 20:

```
D1(config)# interface ethernet 1/1/5
D1(config-if-eth1/1/5)# channel-group 20
D1(config-if-eth1/1/5)# exit
D1(config)# interface ethernet 1/1/6
D1(config-if-eth1/1/6)# channel-group 20
D1(config-if-eth1/1/6)# exit
```

## C2 配置示例:

- 在核心路由器之间配置 L2 链路上的 VRRP:

```
C2(config)# interface vlan 100
C2(config-if-vl-100)# ip address 10.10.100.3/24
C2(config-if-vl-100)# vrrp-group 10
C2(config-vlan100-vrid-10)# virtual-address 10.10.100.5
```

- 为 VLAN 100 配置 VLT 端口通道:

```
C2(config)# interface port-channel 10
C2(config-if-po-10)# vlt-port-channel 10
C2(config-if-po-10)# switchport mode trunk
C2(config-if-po-10)# switchport trunk allowed vlan 100
C2(config-if-po-10)# exit
```

- 将成员添加到端口通道 10:

```
C2(config)# interface ethernet 1/1/3
C2(config-if-eth1/1/3)# channel-group 10
C2(config-if-eth1/1/3)# exit
C2(config)# interface ethernet 1/1/4
C2(config-if-eth1/1/4)# channel-group 10
C2(config-if-eth1/1/4)# exit
```

- 在核心路由器的 L3 端配置 OSPF:

```
C2(config)# router ospf 100
C2(config-router-ospf-100)# redistribute connected
C2(config-router-ospf-100)# exit
C2(config)# interface vlan 200
C2(config-if-vl-200)# ip ospf 100 area 0.0.0.0
```

- 为 VLAN 200 配置 VLT 端口通道:

```
C2(config)# interface port-channel 20
C2(config-if-po-20)# vlt-port-channel 20
C2(config-if-po-20)# switchport mode trunk
C2(config-if-po-20)# switchport trunk allowed vlan 200
C2(config-if-po-20)# exit
```

- 将成员添加到端口通道 20:

```
C2(config)# interface ethernet 1/1/5
C2(config-if-eth1/1/5)# channel-group 20
C2(config-if-eth1/1/5)# exit
```

```
C2(config)# interface ethernet 1/1/6
C2(config-if-eth1/1/6)# channel-group 20
C2(config-if-eth1/1/6)# exit
```

#### D2 配置示例：

- 在核心路由器之间配置 L2 链路上的 VRRP：

```
D2(config)# interface vlan 100
D2(config-if-vl-100)# ip address 10.10.100.4/24
D2(config-if-vl-100)# vrrp-group 10
D2(config-vlan100-vrid-10)# virtual-address 10.10.100.5
```

- 为 VLAN 100 配置 VLT 端口通道：

```
D2(config)# interface port-channel 10
D2(config-if-po-10)# vlt-port-channel 10
D2(config-if-po-10)# switchport mode trunk
D2(config-if-po-10)# switchport trunk allowed vlan 100
D2(config-if-po-10)# exit
```

- 将成员添加到端口通道 10：

```
D2(config)# interface ethernet 1/1/3
D2(config-if-eth1/1/3)# channel-group 10
D2(config-if-eth1/1/3)# exit
D2(config)# interface ethernet 1/1/4
D2(config-if-eth1/1/4)# channel-group 10
D2(config-if-eth1/1/4)# exit
```

- 在核心路由器的 L3 端配置 OSPF：

```
D2(config)# router ospf 100
D2(config-router-ospf-100)# redistribute connected
D2(config-router-ospf-100)# exit
D2(config)# interface vlan 200
D2(config-if-vl-200)# ip ospf 100 area 0.0.0.0
```

- 为 VLAN 200 配置 VLT 端口通道：

```
D2(config)# interface port-channel 20
D2(config-if-po-20)# vlt-port-channel 20
D2(config-if-po-20)# switchport mode trunk
D2(config-if-po-20)# switchport trunk allowed vlan 200
D2(config-if-po-20)# exit
```

- 将成员添加到端口通道 20：

```
D2(config)# interface ethernet 1/1/5
D2(config-if-eth1/1/5)# channel-group 20
D2(config-if-eth1/1/5)# exit
D2(config)# interface ethernet 1/1/6
D2(config-if-eth1/1/6)# channel-group 20
D2(config-if-eth1/1/6)# exit
```

## 查看 VLT 信息

要监控操作或验证 VLT 域的配置，请在主要和次要对上使用 VLT show 命令。

- 在 EXEC 模式下查看有关 VLT 域配置的详细信息，包括 VLTi 状态、本地和对等 MAC 地址、对等节点的路由状态以及 VLT 对等参数。

```
show vlt domain-id
```

- 在 EXEC 模式下查看本地和远程 VLT 对等节点的角色。

```
show vlt domain-id role
```

- 在 EXEC 模式下查看 VLT 配置中的任何不匹配。

```
show vlt domain-id mismatch
```

- 在 EXEC 模式下查看有关 VLT 端口的详细信息。

```
show vlt domain-id vlt-port-detail
```

- 在 EXEC 模式下查看所有 VLT 域的当前配置。

```
show running-configuration vlt
```

## VLT 命令

### backup destination

配置心跳信号计时器的 VLT 备份链路。

|               |                                                                                                                                                                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>backup destination {ip-address   ipv6 ipv6-address} [vrf management] [interval interval-time]</code>                                                                                                                                                                                            |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>ip-address</code> — 输入备份链路的 IPv4 地址。</li> <li><code>ipv6-address</code> — 输入备份链路的 IPv6 地址。</li> <li><code>vrf management</code> — (可选) 为备份 IPv4 或 IPv6 地址配置管理 VRF 实例。</li> <li><code>interval interval-time</code> — (可选) 以秒为单位输入配置心跳时间间隔的时间。</li> </ul> |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                                                                   |
| <b>命令模式</b>   | VLT-DOMAIN                                                                                                                                                                                                                                                                                            |
| <b>使用情况信息</b> | 此命令的 <code>no</code> 版本将从备份链路移除 IP 地址。                                                                                                                                                                                                                                                                |
| <b>示例</b>     | <pre>OS10(config)# vlt-domain 1 OS10(conf-vlt-1)# backup destination 10.16.151.110 vrf management interval 30</pre> <pre>OS10(config)# vlt-domain 1 OS10(conf-vlt-1)# backup destination ipv6 1::1 vrf management interval 30</pre>                                                                   |
| <b>支持的版本</b>  | 10.3.1E or later                                                                                                                                                                                                                                                                                      |

### delay-restore

配置在 VLT 对等交换机之间进行重新加载或对等链路还原后延迟显示 VLT 端口的时间间隔。

|               |                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>delay-restore seconds</code>                                                                                                                   |
| <b>参数</b>     | <code>seconds</code> — 输入在检测到 VLTi 链路后延迟显示 VLT 端口的延迟时间（以秒为单位），从 1 到 1200。                                                                            |
| <b>默认</b>     | 90 秒                                                                                                                                                 |
| <b>命令模式</b>   | VLT-DOMAIN                                                                                                                                           |
| <b>使用情况信息</b> | 使用此命令可以让系统延迟一个短暂的时间段显示 VLT 端口，以便在 VLT 对等节点之间交换控制信息（如 MAC 和 ARP 表）。如果对等 VLT 设备在 VLTi 链路失败时运行，请在重新加载 VLT 设备后使用此命令。此命令的 <code>no</code> 版本会将延迟时间重置为默认值。 |
| <b>示例</b>     | <pre>OS10(conf-vlt-1)# delay-restore 100</pre>                                                                                                       |
| <b>支持的版本</b>  | 10.3.0E or later                                                                                                                                     |

## discovery-interface

配置接口，以在 VLT 对等体之间查找和连接 VLT 互连 (VLTi) 链路中的 VLT 对等体。

|        |                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------|
| 语法     | <code>discovery-interface {ethernet node/slot/port[:subport]}</code>                              |
| 参数     | <code>ethernet</code> — 输入 VLT 对等体上的端口的以太网接口信息。您还可以输入由连字符和逗号分隔的一系列接口。                             |
| 默认     | 无                                                                                                 |
| 命令模式   | VLT-DOMAIN                                                                                        |
| 使用情况信息 | VLT 节点查找服务会自动将查找端口连接到其对等节点端口，并创建 VLTi 接口。此命令的 <code>no</code> 版本将禁用查找接口配置。                        |
| 示例     | <pre>OS10(config)# vlt-domain 1 OS10(conf-vlt-1)# discovery-interface ethernet 1/1/15</pre>       |
| 示例（范围） | <pre>OS10(config)# vlt-domain 2 OS10(conf-vlt-2)# discovery-interface ethernet 1/1/1-1/1/12</pre> |
| 支持的版本  | 10.2.0E or later                                                                                  |

## peer-routing

启用优化的路由，其中为 VLT 对等方的 L3 端点发送的数据包在本地进行路由。

|        |                                           |
|--------|-------------------------------------------|
| 语法     | <code>peer-routing</code>                 |
| 参数     | 无                                         |
| 默认     | 已禁用                                       |
| 命令模式   | VLT-DOMAIN                                |
| 使用情况信息 | 此命令的 <code>no</code> 版本将禁用对等路由。           |
| 示例     | <pre>OS10(conf-vlt-1)# peer-routing</pre> |
| 支持的版本  | 10.2.0E or later                          |

## peer-routing-timeout

配置在对等节点不可用时系统禁用对等路由的延迟时间。此命令同时支持 IPv6 和 IPv4 路由。

|        |                                                                                          |
|--------|------------------------------------------------------------------------------------------|
| 语法     | <code>peer-routing-timeout value</code>                                                  |
| 参数     | <code>value</code> — 输入超时值（以秒为单位），从 0 到 65535。                                           |
| 默认     | 0                                                                                        |
| 命令模式   | VLT-DOMAIN                                                                               |
| 使用情况信息 | 当计时器过期时，系统会检查是否有可用的 VLT 对等。如果 VLT 对等不可用，则系统将在对等上禁用对等路由。如果未配置计时器，系统将不会禁用对等路由，即使对等不可用也是如此。 |
| 示例     | <pre>OS10(conf-vlt-1)# peer-routing-timeout 120</pre>                                    |
| 支持的版本  | 10.3.0E or later                                                                         |

# primary-priority

在选择期间选择主要和辅助 VLT 对等设备时配置优先级。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>primary-priority value</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 参数     | <code>value</code> — 输入比远程对等设备的优先级值更低的值。范围是从 1 到 65535。默认值为 32768。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 默认     | 32768。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 命令模式   | VLT-DOMAIN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 使用情况信息 | <ul style="list-style-type: none"><li>在每个对等交换机上配置 VLT 域并在 VLT 互连的每一端连接两个 VLT 对等设备后，系统将会选择主要和辅助 VLT 对等设备。要在选择进程之前配置主要和辅助角色，请使用 <code>primary-priority</code> 命令。在主要对等节点上输入较低的值，并在辅助对等节点上输入更高的值。如果主要对等节点发生故障，辅助对等节点（优先级较高）将获得主要角色。如果主要对等节点（优先级较低）再次恢复联机，则将其分配辅助角色；没有抢占。</li><li>如果在两个 VLT 对等节点上配置的优先级值相等，VLT 将根据两个节点的系统 MAC 地址的值使用默认的主要选择机制。具有最低系统 MAC 地址的 VLT 对等节点将承担主要角色。</li><li>如果心跳信号正常，并且在 VLT 对等节点之间 VLTi 链路中断，则 VLT 对等节点都将保留其主要角色和辅助角色。但是，辅助 VLT 对等节点上的 VLT 端口通道关闭。</li></ul> <div> <b>注：</b>使用此命令为 VLT 对等节点配置优先级时，配置不会立即生效。主要优先级配置将在下次触发选择时生效。</div> |

|       |                                                  |
|-------|--------------------------------------------------|
| 示例    | <pre>OS10 (conf-vlt-1) #primary-priority 2</pre> |
| 支持的版本 | 10.4.1.0 or later                                |

# show running-configuration vlt

显示所有 VLT 域的当前配置。

|        |                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show running-configuration vlt</code>                                                                                                                                                                                                                     |
| 参数     | 无                                                                                                                                                                                                                                                               |
| 默认     | 未配置                                                                                                                                                                                                                                                             |
| 命令模式   | EXEC                                                                                                                                                                                                                                                            |
| 使用情况信息 | 无                                                                                                                                                                                                                                                               |
| 示例     | <pre>OS10# show running-configuration vlt ! vlt domain 1   peer-routing   discovery-interface ethernet1/1/17 ! interface port-channel1   vlt-port-channel 1 ! interface port-channel2   vlt-port-channel 2 ! interface port-channel3   vlt-port-channel 3</pre> |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                |

# show spanning-tree virtual-interface

显示特定于 VLTi 的 STP、RPVST+ 和 MSTP 信息。

|    |                                                            |
|----|------------------------------------------------------------|
| 语法 | <code>show spanning-tree virtual-interface [detail]</code> |
|----|------------------------------------------------------------|

参数  
默认  
命令模式  
使用情况信息  
示例

detail — (可选) 显示详细的输出。  
未配置  
EXEC  
无

```
OS10# show spanning-tree virtual-interface
VFP(VirtualFabricPort) of RSTP 1 is Designated Forwarding
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: No, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 11, Received: 7
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated

VFP(VirtualFabricPort) 0.1 0 1 FWD 0 32768 0078.7614.6062 0.1
```

```
OS10# show spanning-tree virtual-interface

VFP(VirtualFabricPort) of vlan 100 is Designated Blocking
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: No, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 7, Received: 9
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated

VFP(VirtualFabricPort) 0.1 0 1 BLK 0 4196 90b1.1cf4.a602 0.1
```

示例 (详细信息)

```
OS10# show spanning-tree virtual-interface detail
Port 1 (VFP(VirtualFabricPort)) of RSTP 1 is designated Forwarding
Port path cost 1, Port priority 0, Port Identifier 0.1
Designated root priority: 32768, address: 00:78:76:14:60:62
Designated bridge priority: 32768, address: 00:78:76:14:60:62
Designated port ID: 0.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 15, Received: 5
```

```
OS10# show spanning-tree virtual-interface detail
Port 1 (VFP(VirtualFabricPort)) of vlan1 is designated Forwarding
Port path cost 1, Port priority 0, Port Identifier 0.1
Designated root priority: 4097, address: 90:b1:1c:f4:a6:02
Designated bridge priority: 4097, address: 90:b1:1c:f4:a6:02
Designated port ID: 0.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 202, Received: 42
Port 1 (VFP(VirtualFabricPort)) of vlan100 is designated Forwarding
Port path cost 1, Port priority 0, Port Identifier 0.1
Designated root priority: 4196, address: 90:b1:1c:f4:a6:02
Designated bridge priority: 4196, address: 90:b1:1c:f4:a6:02
Designated port ID: 0.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 101, Received: 21
```

示例 (MSTP 信息)

```
OS10# show spanning-tree virtual-interface
VFP(VirtualFabricPort) of MSTI 0 is Designated Forwarding
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: Yes, Bpdu-filter: Disable, Bpdu-Guard: Disable, Shutdown-on-Bpdu-Guard-violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 387, Received: 16
Interface
Name PortID Prio Cost Sts Cost Bridge ID Designated

VFP(VirtualFabricPort) 0.1 0 1 FWD 0 32768 3417.ebf2.a8c4 0.1

VLT-LAG -1(vlt-portid-1) of MSTI 0 is in Designated Forwarding
```

```
Edge port: No (default)
Link type: point-to-point (auto)
Boundary: No, Bpdu-filter: Disable, Bpdu-Guard: Disable,
Shutdown-on-Bpdu-Guard-violation: No
Root-Guard: Disable, Loop-Guard: Disable
Bpdus (MRecords) Sent: 1234, Received: 123

Virtual
Interface
Name PortID Prio Cost Sts Cost Designated
 Bridge ID

VLT-LAG -1(vlt-portid1) 128.2001 128 2000000 FWD 0 32768 90b1.1cf4.a523 128.2001
```

示例（VLT 上的 MSTP 信息）

```
OS10# show spanning-tree virtual-interface detail
Port 1 (VFP(VirtualFabricPort)) of MSTI 0 is designated Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.1
Designated root priority: 32768, address: 34:17:44:55:66:7f
Designated bridge priority: 32768, address: 90:b1:1c:f4:a5:23
Designated port ID: 128.1, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 2714, Received: 1234

Port 2001 (VLT-LAG -1(vlt-portid-1)) of MSTI 0 is designated Forwarding
Port path cost 200000, Port priority 128, Port Identifier 128.2001
Designated root priority: 32768, address: 34:17:44:55:66:7f
Designated bridge priority: 32768, address: 90:b1:1c:f4:a5:23
Designated port ID: 128.2001, designated path cost: 0
Number of transitions to forwarding state: 1
Edge port: No (default)
Link Type: Point-to-Point
BPDU Sent: 2714, Received: 1234
```

支持的版本 10.3.0E or later

show vlt

显示有关 VLT 域的信息。

|        |                                                                                        |
|--------|----------------------------------------------------------------------------------------|
| 语法     | show vlt domain-id                                                                     |
| 参数     | domain-id — 输入 VLT 域 ID，从 1 到 255。                                                     |
| 默认     | 未配置                                                                                    |
| 命令模式   | EXEC                                                                                   |
| 使用情况信息 | 在下面的示例中，VLT 节点的 status 是 up。如果您看到此 VLT 节点的 role 列为 primary，则对等节点上的 role 会列为 secondary。 |

示例

```
OS10# show vlt 255
Domain ID : 255
Unit ID : 1
Role : primary
Version : 2.0
Local System MAC address : 34:17:eb:3a:bd:80
Role priority : 1
VLT MAC address : aa:bb:cc:dd:ee:ff
IP address : fda5:74c8:b79e:1::1
Delay-Restore timer : 100 seconds
Peer-Routing : Enabled
Peer-Routing-Timeout timer : 9999 seconds
VLTi Link Status
port-channell1000 : up

VLT Peer Unit ID System MAC Address Status IP Address Version

2 34:17:eb:3a:c2:80 up fda5:74c8:b79e:1::2 2.0
```

支持的版本 10.2.0E or later



## show vlt backup-link

显示心跳的详细状态。

|        |                                |
|--------|--------------------------------|
| 语法     | show vlt domain-id backup-link |
| 参数     | domain-id — 输入 VLT 域 ID。       |
| 默认     | 未配置                            |
| 命令模式   | EXEC                           |
| 使用情况信息 | 无                              |
| 示例     |                                |

```
OS10# show vlt 255 backup-link
VLT Backup Link

Destination : 10.16.208.164
Peer Heartbeat status : Up
Heartbeat interval : 1
Heartbeat timeout : 3
```

支持的版本 10.3.1E or later

## show vlt mac-inconsistency

显示在跨多个 VLAN VLT 对等方之间学习的动态 MAC 地址的不一致。

|        |                                                                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show vlt mac-inconsistency                                                                                                                               |
| 参数     | 无                                                                                                                                                        |
| 默认     | 未配置                                                                                                                                                      |
| 命令模式   | EXEC                                                                                                                                                     |
| 使用情况信息 | 使用此命令可以检查 VLT 对等节点之间的 MAC 地址表条目是否存在不匹配。仅当您观察到网络融合问题时，才能使用此命令。要验证对等交换机上的 VLT 配置不匹配问题，请使用 show vlt domain-name mismatch command。<br><br>如果存在流量融合问题，请使用此命令。 |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show vlt-mac-inconsistency Checking Vlan 228 .. Found 7 inconsistencies .. Progress 100% VLAN 128 ----- MAC 00:00:00:00:00:02 is missing from Node(s) 2 VLAN 1 ----- MAC 00:a0:c9:00:00:18 is missing from Node(s) 2 MAC 00:a0:c9:00:00:20 is missing from Node(s) 2 VLAN 131 ----- MAC 00:00:00:00:00:02 is missing from Node(s) 2 VLAN 132 ----- MAC 00:00:00:00:00:02 is missing from Node(s) 2 VLAN 135 ----- MAC 00:00:00:00:00:02 is missing from Node(s) 2 VLAN 137 ----- MAC 00:00:00:00:00:02 is missing from Node(s) 2  Run "show vlt mismatch ..." commands to identify configuration issues</pre> |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

支持的版本 10.2.0E or later

# show vlt mismatch

显示 VLT 域配置中的不匹配项。

|           |                                                                                                                                                                                                                                                                                                                                                                            |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法        | show vlt <i>id</i> mismatch [ <i>dhcp-snooping</i>   <i>peer-routing</i>   <i>vlan</i>   <i>vlt-vlan vlt-port-id</i>   <i>virtual-network</i> ]                                                                                                                                                                                                                            |
| 参数        | <ul style="list-style-type: none"><li><i>id</i> — 输入 VLT 域 ID, 从 1 到 255。</li><li><i>dhcp-snooping</i> — 显示 VLT 域中 DHCP 侦听配置中的不匹配项。</li><li><i>peer-routing</i> — 显示对等路由配置中的不匹配项。</li><li><i>vlan</i> — 显示 VLT 域中 VLAN 配置中的不匹配项。</li><li><i>vlt-vlan vlt-port-id</i> — 显示 VLT 端口配置中的不匹配项, 从 1 到 4095。</li><li><i>virtual-network</i> — 显示 VLT 对等节点之间的虚拟网络配置不匹配项。</li></ul> |
| 默认        | 未配置                                                                                                                                                                                                                                                                                                                                                                        |
| 命令模式      | EXEC                                                                                                                                                                                                                                                                                                                                                                       |
| 使用情况信息    | 不匹配输出中的 * 指示本地节点条目。                                                                                                                                                                                                                                                                                                                                                        |
| 示例 (无不匹配) |                                                                                                                                                                                                                                                                                                                                                                            |

```
OS10# show vlt 1 mismatch
Peer-routing mismatch:
No mismatch

VLAN mismatch:
No mismatch

VLT VLAN mismatch:
No mismatch
```

## 示例 (不匹配)

```
OS10# show vlt 1 mismatch
Peer-routing mismatch:
VLT Unit ID Peer-routing

* 1 Enabled
 2 Disabled

VLAN mismatch:
No mismatch

VLT VLAN mismatch:
VLT ID : 1
VLT Unit ID Mismatch VLAN List

* 1 1
 2 2
VLT ID : 2
VLT Unit ID Mismatch VLAN List

* 1 1
 2 2
```

## 示例 (不匹配的对等路由)

```
OS10# show vlt 1 mismatch peer-routing
Peer-routing mismatch:
VLT Unit ID Peer-routing

* 1 Enabled
 2 Disabled
```

## 示例 (不匹配的 VLAN)

```
OS10# show vlt 1 mismatch vlan
VLT Unit ID Mismatch VLAN List

* 1 -
 2 4
```

示例（不匹配的 VLT VLAN）

```
OS10# show vlt 1 mismatch vlt-vlan
VLT ID : 1
VLT Unit ID Mismatch VLAN List

* 1 1
 2 2
VLT ID : 2
VLT Unit ID Mismatch VLAN List

* 1 1
 2 2
```

示例（不匹配一虚拟网络（VN）名称在对等中不可用）

```
OS10# show vlt all mismatch virtual-network
Virtual Network Name Mismatch:
VLT Unit ID Mismatch Virtual Network List

 1 10,104
* 2 -
```

示例（VLTi 和 VLAN 不匹配）

```
OS10# show vlt all mismatch virtual-network
Virtual Network: 100
VLT Unit ID Configured VLTi-Vlans

 1 101
* 2 100
```

示例（VN 模式不匹配）

```
OS10# show vlt all mismatch virtual-network
Virtual Network: 102
VLT Unit ID Configured Virtual Network Mode

 1 PV
* 2 Attached
```

示例（端口与 VLAN 列表不匹配）

```
OS10# show vlt all mismatch virtual-network
Virtual Network: 102
VLT Unit ID Mismatch (VLT Port,Vlan) List

 1 -
* 2 (vlt-port-channel10,vlan99)

Virtual Network: 103
VLT Unit ID Mismatch (VLT Port,Vlan) List

 1 (vlt-port-channel10,vlan103)
* 2 (vlt-port-channel10,vlan104)
```

示例（未标记的接口不匹配）

```
OS10# show vlt all mismatch virtual-network
Virtual Network: 104
VLT Unit ID Mismatch Untagged VLT Port-channel List

 1 10
* 2 -
```

示例（任意广播 MAC 地址）

```
show vlt 1 mismatch virtual-network

Interface virtual-network Anycast-mac mismatch:
VLT Unit ID Anycast-MAC

 1 00:01:02:03:04:051
* 2 00:01:02:03:04:055
```

示例（任意广播 MAC 地址在其中一个对等不可用）

```
show vlt 1 mismatch virtual-network

Interface virtual-network Anycast-mac mismatch:
VLT Unit ID Anycast-MAC

 1 00:01:02:03:04:051
* 2 -
```

示例（虚拟网络接口任意广播 IP 地址）

```
show vlt 1 mismatch virtual-network

Interface virtual-network Anycast-IP mismatch:

Virtual-network: 10

VLT Unit ID Anycast-IP

 1 10.16.128.25
* 2 10.16.128.20

Virtual-network: 20

VLT Unit ID Anycast-IP

 1 10.16.128.26
* 2 10.16.128.30
```

示例（两个对等上的一个虚拟网络上未配置的任意广播 IP 地址）

```
show vlt 1 mismatch virtual-network
Interface virtual-network Anycast-IP mismatch:

Virtual-network: 10

VLT Unit ID Anycast-IP

 1 10.16.128.25
* 2 ABSENT

Virtual-network: 20

VLT Unit ID Anycast-IP

 1 ABSENT
* 2 10.16.128.30
```

示例（虚拟网络不匹配和任意广播 IP 地址不匹配）

```
Interface virtual-network Anycast-IP mismatch:

Virtual-network: 10

VLT Unit ID Anycast-IP

 1 10.16.128.25
* 2 10.16.128.20

Virtual-network: 20

VLT Unit ID Anycast-IP

 1 10.16.128.26
* 2 ABSENT

Virtual-network: 30

VLT Unit ID Anycast-IP

 1 ABSENT
* 2 10.16.128.30
```

示例（显示多播路由不匹配）

```
OS10# show vlt mismatch

Multicast routing mismatches:

PIM spanned status

Vlan status V4 V6
VlanId Local Peer Local Peer
Vlan 5 Inactive Active Inactive Inactive
Vlan 25 Active Inactive Inactive Active
```

支持的版本 10.2.0E or later

show vlt role

显示本地对等体的 VLT 角色。

- 语法 show vlt id role
- 参数 id — 输入 VLT 域 ID, 从 1 到 255。
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 不匹配输出中的 \* 指示本地不匹配。
- 示例

```
OS10# show vlt 1 role
VLT Unit ID Role

* 1 primary
 2 secondary
```

支持的版本 10.2.0E or later

show vlt vlt-port-detail

显示有关 VLT 端口的详细状态信息。

- 语法 show vlt id vlt-port-detail
- 参数 id — 输入 VLT 域 ID, 从 1 到 255。
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 不匹配输出中的 \* 指示本地不匹配。
- 示例

```
OS10# show vlt 1 vlt-port-detail
Vlt-port-channel ID : 1
VLT Unit ID Port-Channel Status Configured ports Active ports

* 1 port-channel1 down 2 0
 2 port-channel1 down 2 0
VLT ID : 2
VLT Unit ID Port-Channel Status Configured ports Active ports

* 1 port-channel2 down 1 0
 2 port-channel2 down 1 0
VLT ID : 3
VLT Unit ID Port-Channel Status Configured ports Active ports

 2 port-channel3 down 1 0
```

支持的版本 10.2.0E or later

## vlt-domain

创建 VLT 域。

|        |                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------|
| 语法     | <code>vlt-domain domain-id</code>                                                                      |
| 参数     | <code>domain-id</code> — 在每个对等主机上输入 VLT 域 ID，从 1 到 255。                                                |
| 默认     | 无                                                                                                      |
| 命令模式   | CONFIGURATION                                                                                          |
| 使用情况信息 | 在每个对等方上配置相同的 VLT 域 ID。如果 VLT 对等主机上发生的 VLT 域 ID 不匹配，则对等方之间的 VLTi 链路不会激活。此命令的 <code>no</code> 版本将禁用 VLT。 |
| 示例     | <pre>OS10(config)# vlt-domain 1</pre>                                                                  |
| 支持的版本  | 10.2.0E or later                                                                                       |

## vlt-port-channel

配置用于将 VLT 对等接口上的接口映射到单个 VLT 端口通道的 ID。

|          |                                                                                        |
|----------|----------------------------------------------------------------------------------------|
| 语法       | <code>vlt-port-channel vlt-port-channel-id</code>                                      |
| 参数       | <code>vlt-port-channel-id</code> — 输入 VLT 端口通道 ID，从 1 到 128。                           |
| 默认       | 未配置                                                                                    |
| 命令模式     | PORT-CHANNEL INTERFACE                                                                 |
| 使用情况信息   | 为 VLT 对等体上的接口分配相同的 VLT 端口通道 ID，以创建 VLT 端口通道。此命令的 <code>no</code> 版本将移除 VLT 端口通道 ID 配置。 |
| 示例（对等 1） | <pre>OS10(conf-if-po-10)# vlt-port-channel 1</pre>                                     |
| 示例（对等 2） | <pre>OS10(conf-if-po-20)# vlt-port-channel 1</pre>                                     |
| 支持的版本    | 10.2.0E or later                                                                       |

## vlt-mac

为 VLT 域中的所有对等交换机配置 MAC 地址。

|        |                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>vlt-mac mac-address</code>                                                                                                                                                                                                                                                                                                                                                   |
| 参数     | <code>mac-address</code> — 以 <code>nn:nn:nn:nn:nn:nn</code> 格式输入拓扑的 MAC 地址。                                                                                                                                                                                                                                                                                                        |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                |
| 命令模式   | VLT-DOMAIN                                                                                                                                                                                                                                                                                                                                                                         |
| 使用情况信息 | <p>使用此命令可更大程度地减少当一个对等交换机重新引导时，在两个对等设备上同步 VLT 域的默认 MAC 地址所需的时间。如果未配置 VLT MAC 地址，则主要对等节点的 MAC 地址将用作所有对等节点的 VLT MAC 地址。在所有对等交换机中，此配置必须对称，以避免任何不可预知的行为。例如，设备停止或 VLTi 重置。此命令的 <code>no</code> 版本将禁用 VLT MAC 地址配置。</p> <p> <b>注：</b>在所有 VLT 对等交换机中将 VLT MAC 地址配置为对称，以避免任何设备停机或 VLTi 重置时出现不可预测的行为。</p> |
| 示例     | <pre>OS10(conf-vlt-1)# vlt-mac 00:00:00:00:00:02</pre>                                                                                                                                                                                                                                                                                                                             |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                   |

## vrrp mode active-active

使 VRRP 对等主机在 VLAN 接口中以本地方式转发到 L3 流量。

|        |                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | vrrp mode active-active                                                                                                                                      |
| 参数     | 无                                                                                                                                                            |
| 默认     | 已启用                                                                                                                                                          |
| 命令模式   | VLAN INTERFACE                                                                                                                                               |
| 使用情况信息 | <p>此命令仅适用于 VLAN 接口。</p> <p>在非 VLT 网络中，备份 VRRP 网关将转发 L3 流量。如果您想要在不具有 VLT 拓扑的 VLAN 上使用 VRRP 组，请禁用主动-主动功能，以确保只有活动的 VRRP 网关转发 L3 流量。</p> <p>此命令的 no 版本将禁用配置。</p> |
| 示例     | <pre>OS10(conf-if-vl-10)# vrrp mode active-active</pre>                                                                                                      |
| 支持的版本  | 10.2.0E or later                                                                                                                                             |

## 上行链路故障检测

上行链路故障检测 (UFD) 指示与连接到交换机的服务器的上游连接丢失。

交换机为设备（如服务器）提供上游连接。如果交换机丢失上游连接，下游设备也会丢失连接。但是，下游设备通常不会收到表明上游连接丢失的指示，因为与交换机的连接仍在运行。要解决此问题，请使用 UFD。

UFD 将下游接口与上游接口关联。当上游连接失败时，交换机将通过操作禁用其下游链路。下游链路上的故障允许下游设备识别上游连接丢失。这允许下游服务器选择备用路径（如果有），以将流量发送至上游设备。

UFD 在上游和下游接口之间创建关联（称为 *uplink-state group*）。上行链路状态组中的接口可以是物理以太网或光纤通道接口或端口通道。

已启用的上行链路状态组将跟踪所有已分配的上游接口的状态。上游接口失败会导致自动禁用上行链路状态组中的下游接口，如下图所示。如果上行链路状态组中只有一个上游接口发生故障，则同一上行链路状态组中的特定数量的下游接口将会发生故障。您可以根据从服务器到上游接口的流量条件来配置发生故障的下游接口的数量。这可避免上游端口上的过载流量。

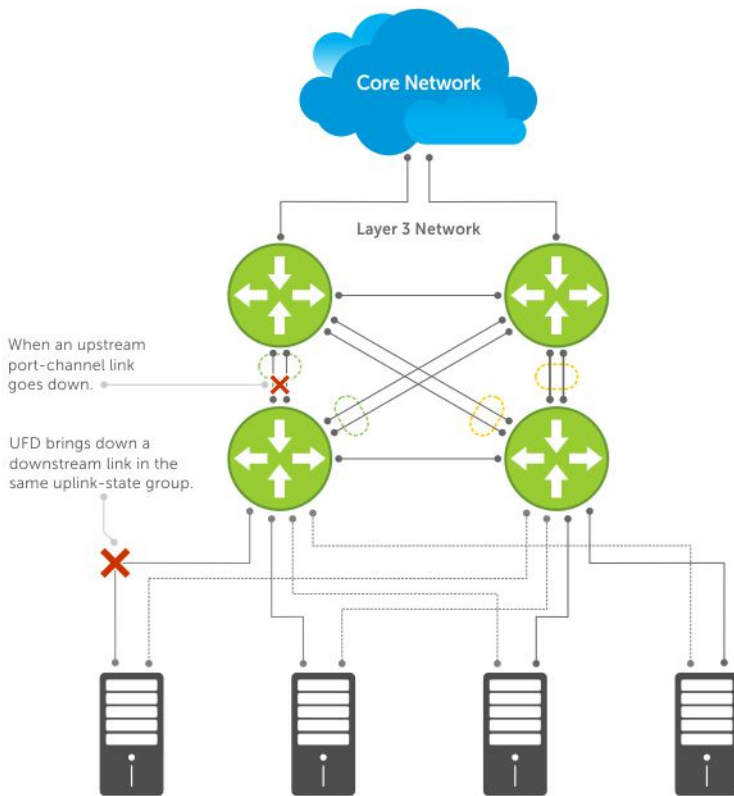
默认情况下，如果上行链路状态组中的所有上游接口发生故障，则同一上行链路状态组中的所有下游接口将设置为链路关闭状态。

此外，在上行链路状态组中，当上行链路接口的链路状态发生变化时，您可以配置下游端口的自动恢复。

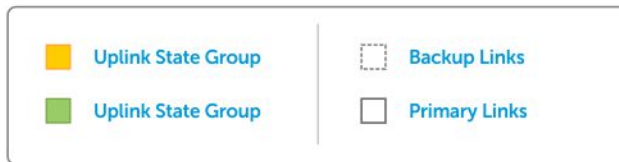
您还可以手动显示处于 UFD 禁用错误状态的下游接口。

### UFD 拓扑





Server traffic is diverted over a backup link to upstream devices.



## 配置上行链路故障检测

在配置上行链路状态组之前，请考虑以下事项：

- 您可以将物理端口或端口通道分配给上行链路状态组。
- 一次只能将一个接口分配给一个上行链路状态组。
- 您可以将上行链路状态组指定为上游或下游接口，但不能同时指定二者。
- 您可以配置多个上行链路状态组并且并发运行它们。
- 您不能将端口通道及其成员分配给上行链路状态组，这会使组处于非活动状态。不属于任何端口通道的端口通道和单个端口可以作为上行链路状态组的成员共存。
- 如果上行链路状态组中的其中一个上游接口发生故障，您可以设置处于停止状态的下游端口，并且状态为 *UFD Disabled error*。您可以将系统配置为禁用用户可配置的下游端口集或组中的所有下游端口。
- 下游端口将按从编号最低的端口开始到编号最高的端口的顺序被禁用。
- 当上行链路状态组中的上游接口出现故障时，将显示由于特定上游接口导致停止的已禁用 UFD 的下游端口集，并且这些下游端口中的 *UFD Disabled error* 会被清除。
- 如果禁用上行链路状态组，则不会禁用下游接口，而不考虑上游接口的状态。
- 如果未将上游接口分配给上行链路状态组，则不会禁用下游接口。

配置：

1. 在 CONFIGURATION 模式下创建上行链路状态组。

```
uplink-state-group group-id
```

2. 在 UPLINK-STATE-GROUP 模式下配置上游和下游接口。

```
upstream {interface-type | interface-range[track-vlt-status] | VLTi}
downstream {interface-type | interface-range}
```

3. (可选) 在 UPLINK-STATE-GROUP 模式下禁用上行链路状态组跟踪。

```
no enable
```

4. (可选) 在 UPLINK-STATE-GROUP 模式下提供上行链路状态组的描述性名称。

```
name string
```

5. 在 UPLINK-STATE-GROUP 模式下, 当上游接口停机时, 配置要禁用的下游接口的数量。

```
downstream disable links{number | all}
```

6. (可选) 在 UPLINK-STATE-GROUP 模式下, 启用已禁用的下游接口的自动恢复。

```
downstream auto-recover
```

7. (可选) 在 UPLINK-STATE-GROUP 模式下, 配置计时器以延迟下游端口上的 UFD 操作。当您配置为在 VLT 网络中跟踪 VLT 状态时, 如果 VLT 端口通道是上行链路状态组的上游成员, 则延迟计时器会在 VLT 状态为正在运行而不是对等端口通道运行状态时触发。

```
defer-time timer
```

8. (可选) 在 EXEC 模式下清除下游接口的 UFD 错误禁用状态。

```
clear ufd-disable
```

## 配置上行链路状态组

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# upstream ethernet 1/1/7:1
OS10(conf-uplink-state-group-1)# downstream ethernet 1/1/1-1/1/5
OS10(conf-uplink-state-group-1)# downstream ethernet 1/1/9:2-1/1/9:3
OS10(conf-uplink-state-group-1)# enable
OS10(conf-uplink-state-group-1)# name UFDGROUP1
OS10(conf-uplink-state-group-1)# defer-time 10
OS10(conf-uplink-state-group-1)# no downstream auto-recover
OS10(conf-uplink-state-group-1)# downstream disable links 2
```

## 查看上行链路状态组配置

```
OS10#show uplink-state-group 1
```

```
Uplink State Group: 1 Status: Enabled,down
```

```
OS10# show uplink-state-group 1 detail
```

```
(Up): Interface up (Dwn): Interface down (Dis): Interface disabled

Uplink State Group : 1 Status : Enabled,up Name : UFDGROUP1
Defer Time : 10 second(s)
Upstream Interfaces : Eth 1/1/7:1(Up)
Downstream Interfaces: Eth 1/1/1(Dwn) Eth 1/1/2(Dwn) Eth 1/1/3(Dwn) Eth 1/1/4(Dwn)
 Eth 1/1/5(Dwn) Eth 1/1/9:2(Dwn) Eth 1/1/9:3(Dwn)
```

```
OS10#show uplink-state-group 1 detail
```

```
(Up): Interface up (Dwn): Interface down (Dis): Interface disabled (NA): Not Available
*: VLT port-channel, V: VLT status, P: Peer Operational status ^: Tracking status
```

```
Uplink State Group : 1 Name: iscsi_group, Status: Enabled, Up
Upstream Interfaces : eth1/1/35(Up) *po10(V:Up, ^P:Dwn) VLTi(NA)
Downstream Interfaces : eth1/1/2(Up) *po20(V: Up,P: Up)

OS10#show uplink-state-group 2 detail

(Up): Interface up (Dwn): Interface down (Dis): Interface disabled (NA): Not Available

*: VLT port-channel, V: VLT status, P: Peer Operational status ^: Tracking status

Uplink State Group : 1 Name: iscsi_group, Status: Enabled, Up
Upstream Interfaces : eth1/1/36(Up) *po30(^V:Up, P:Dwn) VLTi(Up)
Downstream Interfaces : eth1/1/4(Up) *po20(V: Up,P: Up)

OS10(conf-uplink-state-group-1)# show configuration
!
uplink-state-group 1
 downstream ethernet1/1/1-1/1/5
 downstream ethernet1/1/9:2-1/1/9:3
 upstream ethernet1/1/7:1
```

## VLT 上的上行链路故障检测

在 VLT 模式下的交换机中创建上行链路状态组时，请确保 VLT 设置中的所有节点都具有相同的上行链路状态组配置和 VLT 端口通道作为成员。如果两个 VLT 对等的 UFD 配置不同，UFD 将无法正常工作。

当您在上行链路状态组中配置 VLT 端口通道作为上游成员并配置为跟踪 VLT 状态时，系统将跟踪 VLT 的结构状态。当结构状态停机时，每个 VLT 节点中的上行链路状态组将禁用该节点的下游 VLT 端口通道。

当您配置为跟踪 VLT 状态时，系统会将上行链路状态组的下游成员置于错误已禁用状态，或者根据 VLT 端口通道的运行状态从错误已禁用状态中清除。

如果不跟踪 VLT 状态，系统会跟踪端口通道的运行状态。

在 UPLINK-STATE-GROUP 模式下使用 `upstream interface-type track-vlt-status` 命令跟踪 VLT 状态。

要将 VLTi 链路配置为上行链路状态组的成员，请在 UPLINK-STATE-GROUP 模式下使用 `upstream VLTi` 命令。您不能将 VLTi 链路配置为上行链路状态组中的下游成员，因为 UFD 可能会在上游成员停止运行时禁用 VLTi 链路。您不能跟踪上游 VLTi 成员的 VLT 状态。

下表介绍了在 VLT 网络上应用 UFD 时的各种情况：

表. 94: VLT 网络上的 UFD

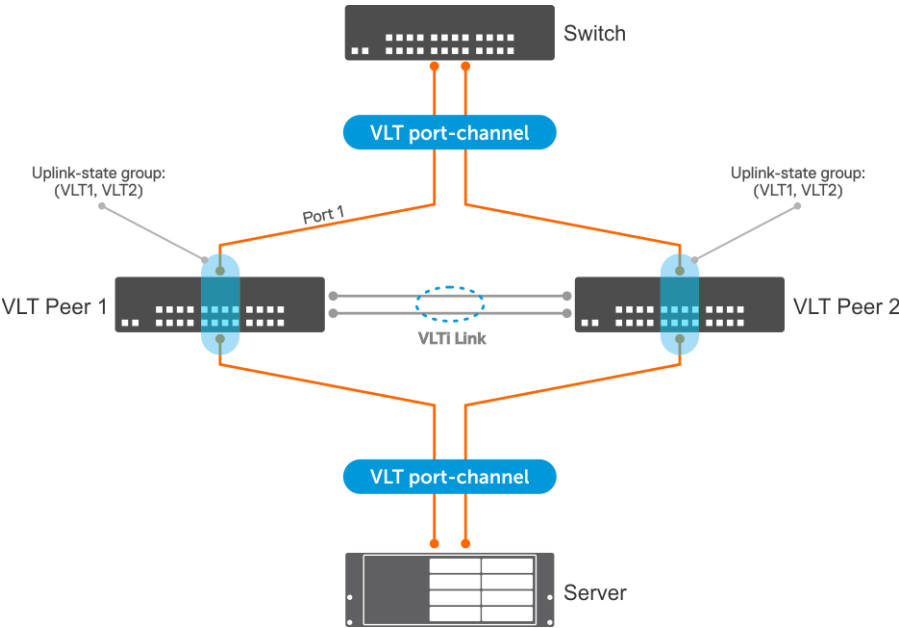
| 事件                 | 主要节点上的 VLT 操作 | 次要节点上的 VLT 操作                                  | UFD 操作                                                                                                                                                  |
|--------------------|---------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLTi 链路停止运行但心跳正常   | 无操作           | VLT 模块会将 VLT 端口通道禁用请求发送到上行链路和下行链路的接口管理器 (IFM)。 | UFD 会接收上游 VLT 端口通道的停止运行状态，并将下游 VLT 端口通道的错误禁用状态发送到 IFM。                                                                                                  |
| VLTi 链路正在运行，并且心跳正常 | 无操作           | VLT 模块会将 VLT 端口通道启用请求发送到上行链路和下行链路的接口管理器 (IFM)。 | UFD 会接收上游 VLT 端口通道的正常运行状态，并将下游 VLT 端口通道的清除错误禁用状态发送到 IFM。                                                                                                |
| 重新引导 VLT 次要对等节点    | 无操作           | 重新引导后，运行延迟恢复计时器。上游和下游 VLT 端口通道在计时器过期之前仍保持禁用状态。 | 作为上游 VLT 端口通道的 UFD <code>error-disables</code> 下游 VLT 端口通道停止运行。计时器过期后，UFD 将在上游 VLT 端口通道的正常运行状态，并将下游 VLT 端口通道的 <code>clear error-disable</code> 发送到 IFM。 |

表. 94: VLT 网络上的 UFD （续）

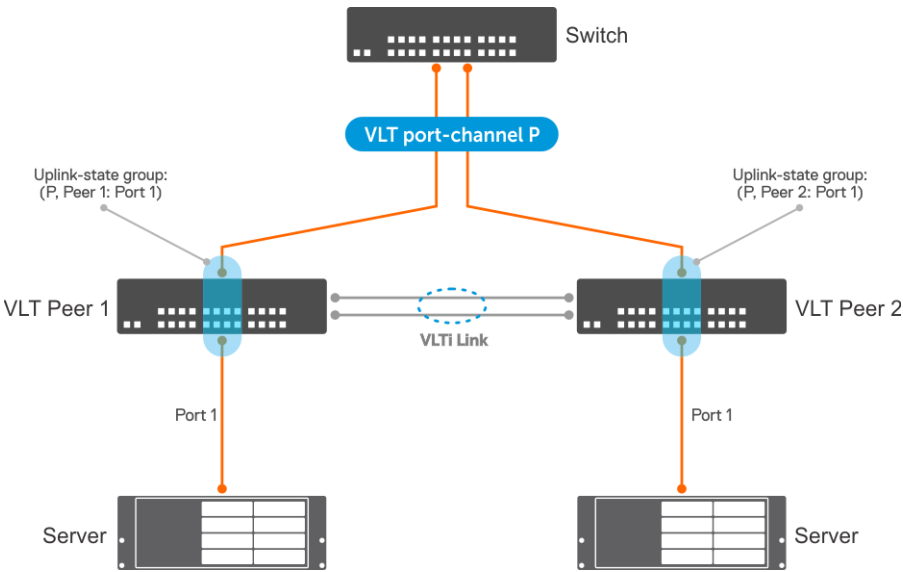
| 事件                                  | 主要节点上的 VLT 操作       | 次要节点上的 VLT 操作 | UFD 操作                                                                                                                        |
|-------------------------------------|---------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| 重新引导 VLT 主要对等节点                     | 主要成为次要对等，并运行延迟恢复计时器 | 次要变为主要        | 作为上游 VLT 端口通道的 UFD error-disables 下游 VLT 端口通道停止运行。计时器过期后，UFD 将在上游 VLT 端口通道的正常运行状态，并将下游 VLT 端口通道的 clear error-disable 发送到 IFM。 |
| 添加到 UFD 组的查找接口                      | 无效配置                | 无效配置          | 无效配置                                                                                                                          |
| 配置为查找接口的 UFD 组成员                    | 无效配置                | 无效配置          | 无效配置                                                                                                                          |
| UFD 组成员作为 VLT 端口通道                  | 无操作                 | 无操作           | UFD 使用结构状态来跟踪 UFD 组状态。                                                                                                        |
| VLT 端口通道作为 UFD 组的成员添加               | 无操作                 | 无操作           | UFD 使用结构状态来跟踪 UFD 组状态。                                                                                                        |
| 从属于 UFD 组的上游成员的端口通道接口中移除 VLT 端口通道配置 | 无操作                 | 无操作           | 停止跟踪 UFD 组的结构状态。开始跟踪本地端口通道运行状态，这是 UFD 组的上游成员。                                                                                 |
| 结构状态为正常运行                           | 无操作                 | 无操作           | 启用下游成员，即清除错误禁用状态。                                                                                                             |
| 结构状态为停止运行                           | 无操作                 | 无操作           | 禁用下游成员，即设置错误禁用状态。                                                                                                             |

UFD VLT 的示例配置

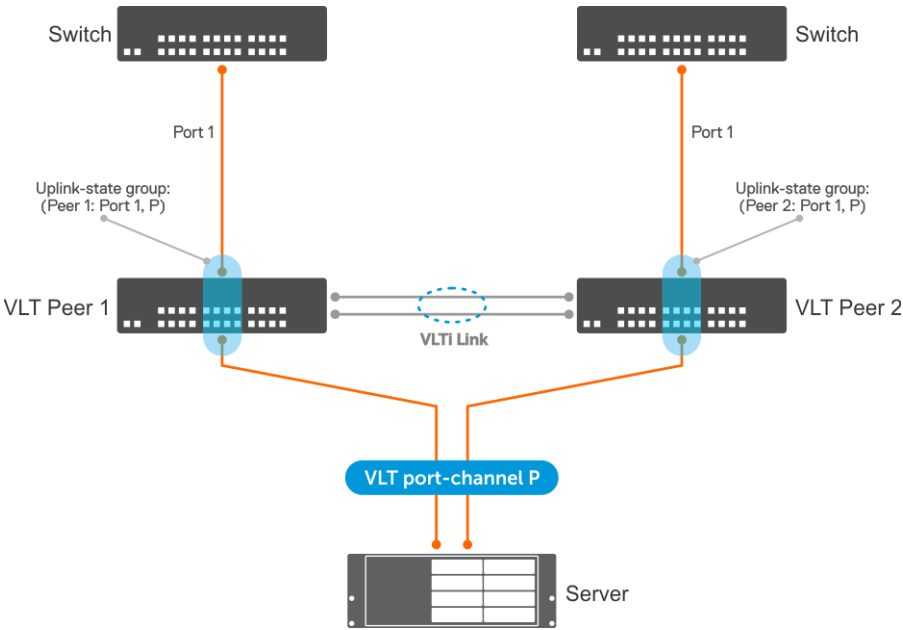
以下示例显示了 VLT 上的一些上行链路状态组。  
在下图中，上游和下游成员均为 VLT 端口通道的一部分。上行链路状态组包括 VLT 端口通道作为成员。



在下面的示例中，上游成员是 VLT 端口通道的一部分，下游成员是孤立端口。上行链路状态组包括 VLT 端口通道、VLT 节点和下游端口。这两个 VLT 节点上的配置是对称的。



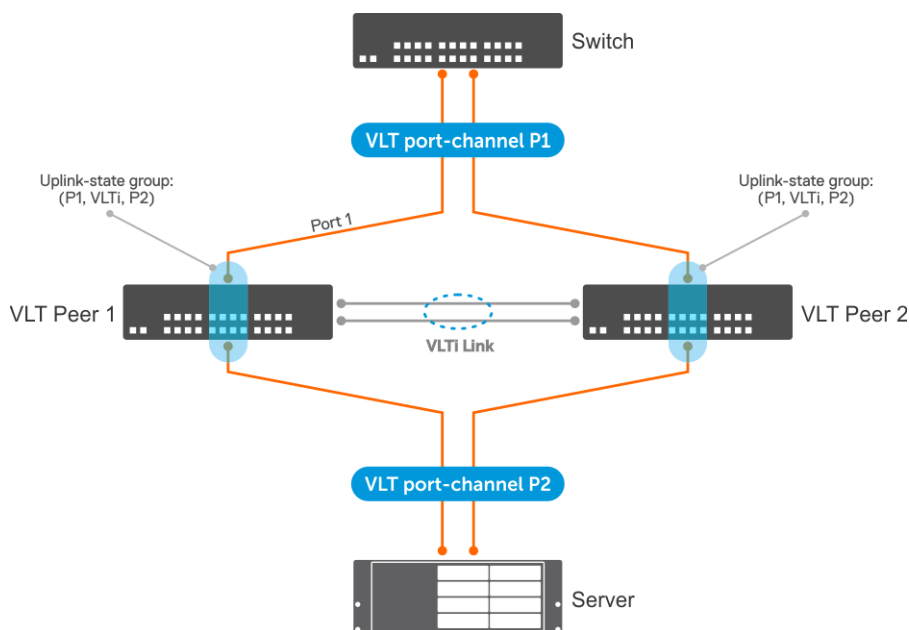
在下面的示例中，下游成员是 VLT 端口通道的一部分，而上游成员是孤立端口。上行链路状态组包括 VLT 端口通道、VLT 节点和上游端口。这两个 VLT 节点上的配置是对称的。



OS10 不支持向上行链路状态组添加 VLTi 链路成员。您可以使用 `upstream VLTi` 命令将 VLTi 链路作为上游成员添加到上行链路状态组。如果系统中未提供 VLTi 链路，OS10 允许添加 VLTi 链路作为上游成员。在这种情况下，当链路可用时，UFD 将开始跟踪 VLTi 链路的运行状态。在 VLTi 链路可用之前，`show uplink-state-group details` 命令会将链路的状态显示为 NA。

在下面的示例中，连接到交换机的 VLT 端口信道和 VLTi 链路均为上游成员。连接到服务器的 VLT 端口通道是一个下游成员。UFD 会跟踪对等端口通道的运行状态。

**注：**您不能将 VLTi 链路配置为上行链路状态组中的下游成员。如果配置，UFD 在上游成员运行时会禁用 VLTi 链路，这会影响 VLT 功能。



## UFD 命令

### clear ufd-disable

覆盖上行链路状态组配置并打开下游接口。

**语法** `clear ufd-disable {interface interface-type | uplink-state-group group-id}`

**参数**

- `interface-type` — 输入接口类型。
- `group-id` — 输入上行链路状态组 ID，从 1 到 32。

**默认** 无

**命令模式** EXEC

**使用情况信息** 此命令会手动打开处于 UFD 禁用错误状态的已禁用下游接口。下游接口开启后将不会禁用，直到在上游接口中有任何更改。此命令不会影响已启动的下游接口或不属于 UFD 组的接口。

**示例**

```
OS10# clear ufd-disable interface ethernet 1/1/2
OS10# clear ufd-disable uplink-state-group 1
```

**支持的版本** 10.4.0E(R3) or later

### defer-time

配置计时器以延迟下游端口上的 UFD 操作。

**语法** `defer-time timer`

**参数** `timer` — 输入定时器值（以秒为单位），范围从 1 到 120。

**默认** 已禁用

**命令模式** UPLINK-STATE-GROUP

**使用情况信息** 您可以使用 `show uplink-state-group [group-id] detail` 命令查看配置的计时器详细信息。此命令的 `no` 版本将禁用计时器。

### 示例

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# defer-time 120
```

**支持的版本** 10.4.1.0 or later

## downstream

将接口或接口范围添加为上行链路状态组的下游接口。

**语法** downstream {*interface-type* | *interface-range*}

- 参数**
- *interface-type* — 将接口类型输入为以太网或端口通道。
  - *interface-range* — 输入接口范围。

**默认** 无

**命令模式** UPLINK-STATE-GROUP

**使用情况信息** 您不能将已经是上行链路状态组成员的接口分配给另一个组。此命令的 `no` 版本将从上行链路状态组中移除接口。

### 示例

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# downstream ethernet 1/1/1
```

**支持的版本** 10.4.0E(R3) or later

## downstream auto-recover

启用已禁用的下游接口的自动恢复。

**语法** downstream auto-recover

**参数** 无

**默认** 已启用

**命令模式** UPLINK-STATE-GROUP

**使用情况信息** 此命令的 `no` 版本将禁用下游接口的自动恢复。

### 示例

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# no downstream auto-recover
```

**支持的版本** 10.4.1.0 or later

## downstream disable links

配置在上行链路状态组中的上游接口发生故障时要禁用的下游接口数量。

**语法** downstream disable links{*number* | all}

- 参数**
- *number* — 输入要禁用的下游接口数，从 1 到 1024。
  - all — 输入 all 以禁用所有下游接口。

**默认** 未配置

**命令模式** UPLINK-STATE-GROUP

**使用情况信息** 此命令的 `no` 版本会将设置恢复为默认状态。

### 示例

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# downstream disable links 2
```

支持的版本 10.4.1.0 or later

enable

启用跟踪上行链路状态组。

- 语法 enable
- 参数 无
- 默认 已禁用
- 命令模式 UPLINK-STATE-GROUP
- 使用情况信息 此命令的 no 版本将禁用上行链路状态组跟踪。
- 示例

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# enable
```

支持的版本 10.4.0E(R3) or later

name

配置上行链路状态组的描述性名称。

- 语法 name string
- 参数 string 输入上行链路状态组的说明。最多 32 个字符。
- 默认 未配置
- 命令模式 UPLINK-STATE-GROUP
- 使用情况信息 此命令的 no 版本将移除描述性名称。
- 示例

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# name test_ufd_group
```

支持的版本 10.4.0E(R3) or later

show running-configuration uplink-state-group

显示特定于上行链路状态组的运行配置。

- 语法 show running-configuration uplink-state-group [group-id]
- 参数 group-id — 输入上行链路组 ID。此时将显示指定组 ID 的运行配置。
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 无
- 示例

```
OS10# show running-configuration uplink-state-group
!
uplink-state-group 1
 downstream ethernet1/1/8:1-1/1/8:4
 upstream ethernet1/1/9:1-1/1/9:4
 upstream port-channel1-3
```

支持的版本 10.4.0E(R3) or later



# show uplink-state-group

显示已配置的上行链路状态。

|        |                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------|
| 语法     | show uplink-state-group [group-id] [detail]                                                                               |
| 参数     | <ul style="list-style-type: none"><li>group-id — 输入上行链路组 ID。此时将显示指定组 ID 的状态。</li><li>detail — 显示上行链路状态组状态的详细信息。</li></ul> |
| 默认     | 未配置                                                                                                                       |
| 命令模式   | EXEC                                                                                                                      |
| 使用情况信息 | 无                                                                                                                         |
| 示例     |                                                                                                                           |

```
OS10# show uplink-state-group

Uplink State Group: 9, Status: Enabled,down
```

```
OS10# show uplink-state-group 9

Uplink State Group: 9, Status: Enabled,down
OS10#
```

## 示例（详细信息）

```
OS10# show uplink-state-group detail

(Up): Interface up (Dwn): Interface down (Dis): Interface disabled

Uplink State Group : 1 Status : Enabled,up Name : UFDGROUP1
Defer Time : 10 second(s)
Upstream Interfaces : Eth 1/1/7:1(Up)
Downstream Interfaces: Eth 1/1/1(Dwn) Eth 1/1/2(Dwn) Eth
1/1/3(Dwn) Eth 1/1/4(Dwn)
 Eth 1/1/5(Dwn) Eth 1/1/9:2(Dwn) Eth
1/1/9:3(Dwn)
```

```
OS10# show uplink-state-group 2 detail

(Up): Interface up (Dwn): Interface down (Dis): Interface disabled

Uplink State Group : 2 Status : Enabled,down Name: UFDGROUP
Upstream Interfaces : Eth 1/1/6(Dwn) Eth 1/1/10(Dwn) Eth
1/1/11(Dwn) Eth 1/1/12(Dwn)
 Eth 1/1/13(Dwn) Eth 1/1/14(Dwn) Eth 1/1/15(Dwn)
Downstream Interfaces: Eth 1/1/16(Dis) Eth 1/1/17(Dis) Eth
1/1/18(Dis) Eth 1/1/19(Dis)
 Eth 1/1/20(Dis)
```

## 示例（已跟踪 VLTi 和 VLT 状态的详细信息）

```
OS10#show uplink-state-group 1 detail

(Up): Interface up (Dwn): Interface down (Dis): Interface disabled (NA):
Not Available

*: VLT port-channel, V: VLT status, P: Peer Operational status ^:
Tracking status

Uplink State Group : 1 Name: iscsi_group, Status: Enabled, Up
Upstream Interfaces : eth1/1/35(Up) *po10(V:Up, ^P:Dwn) VLTi(NA)
Downstream Interfaces : eth1/1/2(Up) *po20(V: Up,P: Up)
```

```
OS10#show uplink-state-group 2 detail

(Up): Interface up (Dwn): Interface down (Dis): Interface disabled (NA):
Not Available
```

```
*: VLT port-channel, V: VLT status, P: Peer Operational status ^:
Tracking status

Uplink State Group : 1 Name: iscsi_group, Status: Enabled, Up
Upstream Interfaces : eth1/1/36(Up) *po30(^V:Up, P:Dwn) VLTi(Up)
Downstream Interfaces : eth1/1/4(Up) *po20(V: Up,P: Up)
```

**支持的版本** 10.4.0E(R3) or later

## uplink-state-group

创建一个上行链路状态组并启用上游链路跟踪。

**语法** `uplink-state-group group-id`

**参数** `group-id` — 输入上行链路状态组的唯一 ID，从 1 到 32。

**默认** 无

**命令模式** CONFIGURATION

**使用情况信息** 此命令的 `no` 版本会删除上行链路状态组。

**示例**

```
OS10(config)# uplink-state-group 1
```

**支持的版本** 10.4.0E(R3) or later

## upstream

将一个接口或一系列接口作为上游接口添加到上行链路状态组。

**语法** `upstream {interface-type | interface-range [ track-vlt-status ] | VLTi}`

**参数**

- `interface-type` — 将接口类型输入为以太网或端口通道。
- `interface-range` — 输入接口范围。
- `VLTi` — 将 VLTi 链路配置为上行链路状态组的成员。
- `track-vlt-status` — (可选) 跟踪上游成员的 VLT 状态。此选项仅适用于端口通道接口。

**默认** 当您在不使用 `track-vlt-status` 选项的情况下添加上游成员时，将默认跟踪操作状态。

**命令模式** UPLINK-STATE-GROUP

**使用情况信息** 您不能将已经是上行链路状态组成员的接口分配给另一个组。此命令的 `no` 版本将从上行链路状态组中移除接口。

**示例**

```
OS10(config)# uplink-state-group 1
OS10(conf-uplink-state-group-1)# upstream ethernet 1/1/45-1/1/48
```

```
OS10(conf-uplink-state-group-1)# upstream VLTi
```

```
OS10(conf-uplink-state-group-1)# upstream port-channel 10 track-vlt-
status
```

**支持的版本** 10.4.0E(R3) or later

## 聚合数据中心服务

OS10 支持聚合数据中心服务，包括 IEEE 802.1 数据中心桥接 (DCB) 扩展到传统以太网。DCB 在数据中心网络中提供 I/O 整合。每个网络设备都有多个流量类别，同时确保在局域网 (LAN) 流量和对延迟敏感的服务计划流量之间进行无损耗的存储流量交付。

- 802.1Qbb — 优先级流控制
- 802.1Qaz — 增强的传输选择
- 数据中心桥接交换 (DCBX) 协议

DCB 支持将 LAN 和存储区域网络 (SAN) 流量与服务器上的端到端链路中的共享物理网络 (SAN) 流量结合到存储设备。在聚合网络中，所有服务器、存储设备和网络设备均已启用 DCB。DCB 支持通过以太网光纤通道 (FCoE) 和 iSCSI 存储数据传输。在启用了链路级别流控制 (LLFC) 的接口上不支持 DCB。

|                             |                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------|
| <b>优先级流控制 (PFC)</b>         | 使用基于优先级的流控制来确保无损耗地传输存储流量，同时传输在没有流控制的情况下更好地执行的其他流量类别，请参阅 <a href="#">优先级流控制</a> 。          |
| <b>增强的传输选择 (ETS)</b>        | 为基于 802.1p 服务类别 (CoS) 的流量类别分配带宽。使用 ETS 提高网络拥塞期间的首选流量类别吞吐量，请参阅 <a href="#">增强的传输选择</a> 。   |
| <b>数据中心桥接交换协议 (DCBX)。</b>   | 配置 DCBX 协议 DCB 邻居使用来查找和交换即插即用功能的配置信息，请参阅 <a href="#">数据中心桥接交换</a> 。                       |
| <b>互联网小型计算机系统接口 (iSCSI)</b> | 使用 iSCSI 自动配置和检测存储设备，监控 iSCSI 会话，并在 iSCSI 流量上应用 QoS 策略，请参阅 <a href="#">互联网小型计算机系统接口</a> 。 |

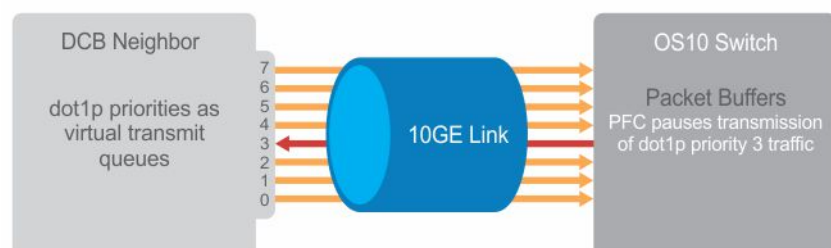
## 优先级流控制

在聚合数据中心网络中，为确保由于拥塞而丢失任何帧，请使用 PFC。PFC 使用以太网标头中的 802.1p 优先级来暂停从传输设备发送的优先级特定流量。802.1p 优先级也称为服务类别 (CoS) 或 dot1p 优先级值。

当 PFC 检测到 dot1p 流量类别的拥塞时，它会将优先级流量的暂停帧发送到传输设备。通过这种方式，PFC 可确保交换机不会丢弃指定的优先级流量。

PFC 增强了现有的 802.3x 暂停功能，以基于 802.1p 优先级启用流控制。PFC 将暂停 802.1p 流量类型的流量，而不是停止链路上的所有流量（由 802.3x 暂停机制执行）。例如，当接口上出现 LAN 流量拥塞时，PFC 可确保存储和服务器流量的无损流，同时允许对其他流量进行有损的最大努力传输。

PFC 通过暂停入口接口上的优先级 dot1p 流量来处理流量拥塞，并允许更大的 dot1p 流量（也称为有损的数据传输）。



## PFC 配置说明

- PFC 受 802.1p 支持，dot1p 优先级流量从 0 到 7。FCoE 流量通常使用 dot1p 优先级 3 — iSCSI 存储流量使用 dot1p 优先级 4。

- 通过使用网络 qos 级别和策略映射来配置用于入口流量的 PFC。有关详细信息，请参阅[服务质量](#)。已启用 PFC 的流量队列被视为无损队列。在所有已启用 PFC 的端口上配置相同的网络 qos 策略映射。使用出口接口上的 ETS 队列（输出）策略为无损流量配置所需的带宽。
- 在网络 qos 策略类映射中，使用命令为匹配类映射优先级生成 PFC 暂停帧：
  - 使用 `pause` 命令发送在拥塞期间匹配类映射流量的暂停帧。
  - （可选）为 PFC 类映射流量的保留入口缓冲区大小输入用户定义的值，以及使用 `pause [buffer-size kilobytes pause-threshold kilobytes resume-threshold kilobytes]` 命令发送 XOFF 和 XON 暂停帧的阈值。
  - 配置用于使用 `pfc-cos` 命令发送暂停帧的匹配 dot1p 值。
  - （可选）设置静态和动态阈值，用于确定可用于使用 `queue-limit thresh-mode` 命令 PFC 类别映射流量队列的共享缓冲区。
- 默认情况下，有损的入口缓冲区将处理所有入口流量。启用 PFC 时，dot1p 入口流量将在无损池中（而不是共享的有损池）中争用共享缓冲区。在某个接口上支持的无损队列数取决于有损的可用内存量。
- 使用 `priority-flow-control mode on` 命令为 FCoE 和 iSCSI 流量启用 PFC；例如，优先级 3 和 4。
- 在接口上启用 DCBX，以检测和自动配置对等体的 PFC/ETS 参数。
- 默认情况下，在接口上已禁用 PFC 和 802.3x LLFC。您不能同时启用 PFC 和 LLFC。LLFC 可确保在最大努力传输中的有损流量。启用 PFC 可保证无损 FCoE 和 iSCSI 流量。PFC 通过暂停指定的入口 dot1p 流量来管理缓冲区拥塞；LLFC 可暂停接口上的所有数据传输。要启用 LLFC，请使用 `flowcontrol [receive | transmit] [on | off]` 命令。
- SYSTEM-QOS 模式在所有接口上全局应用服务策略：
  - 在 INTERFACE 或 SYSTEM-QOS 模式下，在接口或所有接口上创建并应用一对一 802.1p 优先级到流量类别映射。
  - 在 INTERFACE 或 SYSTEM-QOS 模式下，在接口或所有接口上创建并应用一对一流量类别到队列映射。

### 为流量类别映射配置 dot1p 优先级

决定是否要使用默认的 802.1p 优先级到流量类别 (qos-group) 映射或配置新映射。下面显示了 OS10 中流量类别映射的默认 dot1p。

|                  |   |   |   |   |   |   |   |   |
|------------------|---|---|---|---|---|---|---|---|
| Dot1p Priority : | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Traffic Class :  | 1 | 0 | 2 | 3 | 4 | 5 | 6 | 7 |

- 应用默认信任映射可以指定 dot1p 值在 SYSTEM-QOS 或 INTERFACE 模式下受信任。

```
trust-map dot1p default
```

### 配置非默认 dot1p 优先级到流量类别映射

1. 在 CONFIGURATION 模式下配置 dot1p 流量类别的信任映射。信任映射不会修改输出流中的入口 dot1p 值。  
使用一对一映射在 TRUST 模式下将 qos-group 分配到受信任的 dot1p 值。Dot1p 优先级为 0 到 7。对于 PFC 流量类别，仅将一个 dot1p 值映射到 qos-group 数字；对于基于 Broadcom 的 NPU 平台，qos-group 数字和 dot1p 值必须相同。只有内部使用 qos-group 数值以将入口流量类别进行分类。

```
trust dot1p-map dot1p-map-name
 qos-group {0-7} dot1p {0-7}
exit
```

2. 将 trust dot1p-map 策略应用于在 SYSTEM-QOS 或 INTERFACE 模式下的入口流量。

```
trust-map dot1p trust-policy-map-name
```

### 配置流量类别队列映射

 **注：** Z9332F-ON 在队列映射上具有不同的配置。有关详细信息，请参阅为 Z9332F-ON [配置流量类别到队列映射](#)。

确定您是要使用默认流量类别队列映射，还是配置非默认流量类别到队列映射。

|                 |   |   |   |   |   |   |   |   |
|-----------------|---|---|---|---|---|---|---|---|
| Traffic Class : | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Queue :         | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

如果您使用的是默认流量类别到队列映射，则无需执行其他配置步骤。

1. 在 CONFIGURATION 模式下创建流量类别到队列映射。使用一对一映射在 QOS-MAP 模式下将流量类别 qos-group 分配到队列。对于 PFC 流量类别，仅将一个 qos-group 值映射到 queue 数值。qos-group 数值仅在内部使用，以对入口流量进行分类。

```
qos-map traffic-class tc-queue-map-name
 queue {0-7} qos-group {0-7}
exit
```

2. 在 SYSTEM-QOS 或 INTERFACE 模式下应用流量类别队列映射。

```
qos-map traffic-class tc-queue-map-name
```

**为 Z9332F-ON 配置流量类别到队列映射**

Z9332F-ON 在前面板端口上支持每个 Ingress Traffic Manager 的 12 个队列。12 个队列划分为八个单播 (UC) 和四个多播 (MC) 组合。对于多播队列，MCQ 索引 0 至 2 用于 MC 流。MCQ 索引 3 从 CPU 发送控制数据包。

默认情况下，按以下顺序映射多播流量：

TC0-TC2: Q0

TC3-TC5: Q1

TC6-TC7: Q2

您可以根据要求将 UC 和 MC 流量的不同流量类别映射到不同的队列。

**配置 TC 到队列映射**

```
OS10# show qos maps
Traffic-Class to Queue Map: sundar

Queue Traffic Class Type

3 1-3 Unicast
4 4,6,0 Unicast
```

**默认的 TC 到队列映射格式**

以下是 Z9332F-ON 的格式：

```
Default Traffic-Class to Queue Map

Traffic Class Queue Number Type

0 0 Unicast
0-2 0 Multicast
1 1 Unicast
3-5 1 Multicast
2 2 Unicast
6-7 2 Multicast
3 3 Unicast
4 4 Unicast
5 5 Unicast
6 6 Unicast
7 7 Unicast
```

以下是默认的 TC 到队列映射格式：

```
Default Traffic-Class to Queue Map

Traffic-Class Queue number Type

0 0 Both
1 1 Both
2 2 Both
3 3 Both
4 4 Both
5 5 Both
6 6 Both
7 7 Both
```

查看接口 PFC 配置

```
OS10# show interface ethernet 1/1/1 priority-flow-control details
ethernet1/1/1
Admin Mode : true
Operstatus: true
PFC Priorities: 4
Total Rx PFC Frames: 0
Total Tx PFC frames: 0
Cos Rx Tx

0 0 0
1 0 0
2 0 0
3 0 0
4 0 0
5 0 0
6 0 0
7 0 0
```

配置 PFC

PFC 提供了一种基于入口流量中的 802.1p 优先级的暂停机制。PFC 将防止因网络拥塞而丢失帧。配置 PFC 无损缓冲区，并为每个接口启用 dot1p 流量的暂停帧。在每个已启用 PFC 的接口上重复 PFC 配置。默认情况下，PFC 处于禁用状态。确定您是要使用默认 dot1p 优先级到流量类别映射，还是配置非默认流量类别到队列映射。要更改默认设置，请参阅 [PFC 配置说明](#)。

- 配置步骤：
- 1. 创建 PFC dot1p 流量类别。
  - 2. 为 PFC 流量配置入口缓冲区。
  - 3. 应用服务策略并启用 PFC。
  - 4. （可选）为无损流量配置 PFC 共享缓冲区。

创建 PFC dot1p 流量类别

- 1. 在 CONFIGURATION 模式下创建 network-qos 类别映射以对 PFC 流量类别进行分类，从 1 到 7。使用 match qos-group 命令指定流量类别。QoS 组将映射 1:1 到流量类别 1 至 7；例如，qos-group 1 对应于流量类别 1。在 CLASS-MAP 模式下输入单个值、连字符分隔的范围或用逗号分隔的多个 qos-group 值。

```
class-map type network-qos class-map-name
 match qos-group {1-7}
exit
```

- 2. （可选）重复步骤 1 以配置其他 PFC 流量类别类别映射。

为 PFC 流量配置暂停和入口缓冲区

有关默认入口队列设置和默认 dot1p 优先级队列映射，请参阅 [PFC 配置说明](#)。

- 1. 在 CONFIGURATION 模式下创建 network-qos 策略映射。

```
policy-map type network-qos policy-map-name
```

- 2. 在 POLICY-MAP 模式下将策略映射与 network-qos 类别映射关联。

```
class class-map-name
```

- 3. 在 POLICY-CLASS-MAP 模式下为用于 network-qos 类别映射的入口缓冲区配置默认值。

```
pause
```

（可选）更改为 network-qos 类别映射流量保留的入口缓冲区大小的默认值，以及用于发送 XOFF 和 XON 暂停帧的阈值（以 kb 为单位）。

```
pause [buffer-size kilobytes {pause-threshold kilobytes | resume-threshold kilobytes}]
```

- 在 POLICY-CLASS-MAP 模式下启用 dot1p 流量的 PFC 暂停功能。Dot1p 值必须与步骤 2 中类别映射中的 qos-group 流量类别编号相同。输入单个 dot1p 值（从 1 到 7）、连字符分隔的范围或多个 dot1p 值（用逗号分隔）。

```
pfc-cos dot1p-priority
```

- （可选）设置用于限制分配给 PFC 流量类别队列的共享缓冲区的静态和动态阈值。根据可用的 PFC 共享缓冲区配置静态或固定队列限制（以 kb 为单位）或动态阈值（权重 1-10；默认值为 9）。

```
queue-limit thresh-mode {static kilobytes | dynamic weight}
```

- （可选）重复步骤 2 至 4 以在其他流量类别上配置 PFC。

### 应用服务策略并启用 PFC

- 在 INTERFACE 模式下，在入口接口或接口范围上应用 PFC 服务策略。

```
interface ethernet node/slot/port:[subport]
 service-policy input type network-qos policy-map-name
```

```
interface range ethernet node/slot/port:[subport]-node/slot/port[:subport]
 service-policy input type network-qos policy-map-name
```

- 在 INTERFACE 模式下启用 PFC（不带 DCBX for FCoE）和 iSCSI 流量。

```
priority-flow-control mode on
```

### 配置 PFC

在具有 dot1p 3 和 4 流量的流量类别上已启用 PFC。这两个流量类别需要不同的入口队列处理。在 network-qos ppl 策略映射中，类别 cc1 使用自定义 PFC 缓冲区大小和暂停帧设置；类别 cc2 使用默认设置。

```
OS10(config)# system qos
OS10(config-sys-qos)# trust-map dot1p default

OS10(config)# system qos
OS10(config-sys-qos)# exit

OS10(config)# class-map type network-qos cc1
OS10(config-cmap-nqos)# match qos-group 3
OS10(config-cmap-nqos)# exit

OS10(config)# class-map type network-qos cc2
OS10(config-cmap-nqos)# match qos-group 4
OS10(config-cmap-nqos)# exit

OS10(config)# policy-map type network-qos ppl
OS10(config-pmap-network-qos)# class cc1
OS10(config-pmap-c-nqos)# pause buffer-size 30 pause-threshold 20 resume-threshold 10
OS10(config-pmap-c-nqos)#pfc-cos 3
OS10(config-pmap-c-nqos)#exit
OS10(config-pmap-network-qos)# class cc2
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)#pfc-cos 4
OS10(config-pmap-c-nqos)#exit

OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# service-policy input type network-qos ppl

OS10(conf-if-eth1/1/1)# priority-flow-control mode on
OS10(conf-if-eth1/1/1)# no shutdown
```

### 查看 PFC 配置和运行状态

```
OS10(conf-if-eth1/1/1)# do show interface ethernet 1/1/1 priority-flow-control details
ethernet1/1/1
Admin Mode : true
Operstatus: true
PFC Priorities: 3,4
Total Rx PFC Frames: 300
Total Tx PFC frames: 200
Cos Rx Tx
```

|       |     |     |
|-------|-----|-----|
| ----- |     |     |
| 0     | 0   | 0   |
| 1     | 0   | 0   |
| 2     | 0   | 0   |
| 3     | 300 | 200 |
| 4     | 0   | 0   |
| 5     | 0   | 0   |
| 6     | 0   | 0   |
| 7     | 0   | 0   |

查看 PFC 入口缓冲区配置

|                                                         |             |               |               |  |
|---------------------------------------------------------|-------------|---------------|---------------|--|
| OS10# show qos ingress buffers interface ethernet 1/1/1 |             |               |               |  |
| Interface : ethernet1/1/1                               |             |               |               |  |
| Speed : 0                                               |             |               |               |  |
| Priority-grp                                            | Reserved    | Shared-buffer | Shared-buffer |  |
| XOFF                                                    |             |               |               |  |
| XON                                                     |             |               |               |  |
| no                                                      | buffer-size | mode          | threshold     |  |
| threshold                                               |             |               |               |  |
| d                                                       | threshold   |               |               |  |
| -----                                                   |             |               |               |  |
| -----                                                   |             |               |               |  |
| 0                                                       | -           | -             | -             |  |
| -                                                       |             |               |               |  |
| 1                                                       | -           | -             | -             |  |
| -                                                       |             |               |               |  |
| 2                                                       | -           | -             | -             |  |
| -                                                       |             |               |               |  |
| 3                                                       | -           | -             | -             |  |
| -                                                       |             |               |               |  |
| 4                                                       | -           | -             | -             |  |
| -                                                       |             |               |               |  |
| 5                                                       | -           | -             | -             |  |
| -                                                       |             |               |               |  |
| 6                                                       | -           | -             | -             |  |
| -                                                       |             |               |               |  |
| 7                                                       | 9360        | static        | 12779520      |  |
| -                                                       |             |               |               |  |
| -                                                       |             |               |               |  |

查看 PFC 系统缓冲区配置

|                                      |   |       |
|--------------------------------------|---|-------|
| OS10# show qos system ingress buffer |   |       |
| All values are in kb                 |   |       |
| Total buffers                        | - | 12187 |
| Total lossless buffers               | - | 0     |
| Maximum lossless buffers             | - | 5512  |
| Total shared lossless buffers        | - | 0     |
| Total used shared lossless buffers   | - |       |
| Total lossy buffers                  | - | 11567 |
| Total shared lossy buffers           | - | 11192 |
| Total used shared lossy buffers      | - | 0     |
|                                      |   |       |
| OS10# show qos system egress buffer  |   |       |
| All values are in kb                 |   |       |
| Total buffers                        | - | 12187 |
| Total lossless buffers               | - | 0     |
| Total shared lossless buffers        | - | 0     |
| Total used shared lossless buffers   | - |       |
| Total lossy buffers                  | - | 11567 |
| Total shared lossy buffers           | - | 9812  |
| Total used shared lossy buffers      | - | 0     |



```
Total CPU buffers - 620
Total shared CPU buffers - 558
Total used shared CPU buffers - 0
```

## 查看 PFC 入口缓冲区统计信息

```
OS10(config)# show qos ingress buffer-stats interface ethernet 1/1/15
Interface : ethernet1/1/15
Speed : 10G
Priority Used reserved Used shared Used HDRM
Group buffers buffers buffers

0 9360 681824 35984
1 0 0 0
2 0 0 0
3 0 0 0
4 0 0 0
5 0 0 0
6 0 0 0
7 0 0 0
```

## PFC 命令

### pause

配置用于 PFC 流量类别的入口缓冲区和暂停帧设置。

- 语法** `pause [buffer-size kilobytes pause-threshold kilobytes resume-threshold kilobytes]`
- 参数**
- `buffer-size kilobytes` — 以 kb 为单位输入 PFC dot1p 流量的保留（保证）入口缓冲区大小，从 0 到 7787。
  - `pause-threshold kilobytes` — 输入用于将暂停帧以 kb 发送到传输设备的阈值，从 0 到 7787。
  - `resume-threshold kilobytes` — 输入用于请求传输设备或恢复发送流量的阈值（以 kb 为单位），从 0 到 7787。

**默认** 为 PFC 流量类别保留的默认入口缓冲区大小以及暂停和恢复阈值因接口类型而异。为 PFC 流量类别保留的默认出口缓冲区对于所有接口类型都是 0。

**表. 95: 端口默认值**

| 端口速度        | 10G 端口 | 25G 端口 | 40G 端口 | 50G 端口 | 100G 端口 |
|-------------|--------|--------|--------|--------|---------|
| PFC 保留入口缓冲区 | 45 KB  | 54 KB  | 93 KB  | 111 KB | 178 KB  |
| PFC 暂停阈值    | 9 KB   | 9 KB   | 18 KB  | 18 KB  | 36 KB   |
| PFC 恢复阈值    | 9 KB   | 9 KB   | 9 KB   | 9 KB   | 9 KB    |

**命令模式** POLICY-CLASS NETWORK-QOS

**使用情况信息** 使用不带可选参数的 `pause` 命令以应用默认的入口缓冲区大小以及暂停 (XON) 和恢复 (XOFF) 阈值。`pause-threshold`、`resume-threshold` 和 `buffer-size` 参数的默认值在接口类型和端口速度上有所不同。默认值基于大小为 9216 字节的默认 MTU。使用可选的 `queue-limit thresh-mode` 命令可在策略类映射中更改 PFC 流量类别队列可用的共享缓冲区数。

**示例**

```
OS10(config)# policy-map type network-qos pp1
OS10(conf-pmap-network-qos)# class cc1
OS10(conf-pmap-c-nqos)# pause buffer-size 30 pause-threshold 20 resume-threshold 10
```

**支持的版本** 10.3.0E or later

## pfc-cos

配置用于发送 PFC 暂停帧的匹配 dot1p 值。

|          |                                                                                                                                                                                                                                                                                                                                            |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法       | <code>pfc-cos dot1p-priority</code>                                                                                                                                                                                                                                                                                                        |
| 参数       | <code>dot1p-priority</code> — 输入 PFC 流量类别的单个 dot1p 值（从 1 到 7）、连字符分隔的范围或多个 dot1p 值（用逗号分隔）。                                                                                                                                                                                                                                                  |
| 默认       | 未配置                                                                                                                                                                                                                                                                                                                                        |
| 命令模式     | POLICY-CLASS NETWORK-QOS                                                                                                                                                                                                                                                                                                                   |
| 使用情况信息   | 当您输入已启用 PFC 的 dot1p 优先级与 <code>pfc-cos</code> 时，dot1p 值必须与用于定义 PFC 流量类别的网络 qos 类别映射中的相同 <code>match qos-group</code> （流量类别）编号，请参阅 <a href="#">配置 PFC 示例</a> 。只有内部使用 <code>qos-group</code> 数值以将入口流量类别进行分类。有关默认的 dot1p 优先级到流量类别映射以及如何配置非默认映射，请参阅 <a href="#">PFC 配置说明</a> 。PFC 流量类别需要 1 到 1 映射 — 只有一个 dot1p 值映射到 <code>qos-group</code> 编号。 |
| 示例       | <pre>OS10(config)# class-map type network-qos cc1 OS10(conf-cmap-nqos)# match qos-group 3 OS10(conf-cmap-nqos)# exit</pre>                                                                                                                                                                                                                 |
| 示例（策略映射） | <pre>OS10(config)# policy-map type network-qos ppl OS10(conf-pmap-network-qos)# class cc1 OS10(conf-pmap-c-nqos)# pfc-cos 3</pre>                                                                                                                                                                                                          |
| 支持的版本    | 10.3.0E or later                                                                                                                                                                                                                                                                                                                           |

## pfc-shared-buffer-size

为交换机上已启用 PFC 的流量配置可用的共享缓冲区数。

|        |                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>pfc-shared-buffer-size kilobytes</code>                                                                                                                                             |
| 参数     | <code>kilobytes</code> — 输入可用于已启用 PFC 的 dot1p 流量的共享缓冲区总量（以 kb 为单位），从 0 到 7787。                                                                                                            |
| 默认     | 832KB                                                                                                                                                                                     |
| 命令模式   | SYSTEM-QOS                                                                                                                                                                                |
| 使用情况信息 | 默认情况下，有损的入口缓冲区将处理所有入口流量。启用 PFC 时，dot1p 入口流量将在无损池中（而不是共享的有损池）中争用共享缓冲区。使用此命令可增大或减小允许 PFC 启用的流的共享缓冲区。只有在使用 <code>priority-flow-control mode on</code> 命令启用接口上的 PFC 之后，才会为 PFC 流保留已配置的共享缓冲区数。 |
| 示例     | <pre>OS10(config)# system qos OS10(conf-sys-qos)# pause-shared-buffer-size 1024</pre>                                                                                                     |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                          |

## priority-flow-control

在入口接口上启用 PFC。

|      |                                                                   |
|------|-------------------------------------------------------------------|
| 语法   | <code>priority-flow-control {mode on}</code>                      |
| 参数   | <code>mode on</code> — 在不启用 DCBX 的情况下在接口上为 FCoE 和 iSCSI 流量启用 PFC。 |
| 默认   | 已禁用                                                               |
| 命令模式 | INTERFACE                                                         |

**使用情况信息** 在启用 PFC 之前，请将网络 qos 策略类别映射应用到接口的特定 PFC dot1p 优先级值。在 PFC 网络 qos 策略类映射中，如果您不确定要使用的 `pause-threshold` 和 `resume-threshold` 设置，请使用默认的 `buffer-size` 值。您不能在接口上同时启用 PFC 和 LLFC。此命令的 `no` 版本将禁用接口上的 PFC。禁用 PFC 时，删除应用到接口的 PFC `network-qos` 策略类别映射。

**示例**

```
OS10(conf-if-eth1/1/1)# priority-flow-control mode on
```

**支持的版本** 10.3.0E or later

queue-limit

设置用于限制 PFC 流量类别队列的共享缓冲区大小的静态和动态阈值。

**语法** `queue-limit {thresh-mode [static kilobytes | dynamic weight]}`

**参数**

- `thresh-mode` — 缓冲区阈值模式。
- `static kilobytes` — 输入可用于 PFC 流量类别队列的固定共享缓冲区限制（以千字节为单位），从 0 到 7787；通过 `pfc-shared-buffer-size` 命令调整的最大数量。
- `dynamic weight` — 输入用于动态确定 PFC 流量类别队列可用的共享缓冲区限制的权重值，从 1 到 10。

**默认** 动态权重 9 和静态共享缓冲区限制为 12,479,488。

**命令模式** POLICY-CLASS NETWORK-QOS

**使用情况信息** 要调整可用于在交换机上的 PFC 流量类别队列的静态限制的可用共享缓冲区量，请使用 `pfc-shared-buffer-size` 命令。可用共享缓冲区的当前数量决定了动态队列限制。

**示例**

```
OS10(config)# policy-map type network-qos ppl
OS10(conf-pmap-network-qos)# class ccl
OS10(conf-pmap-c-nqos)# queue-limit thresh-mode static 1024
```

**支持的版本** 10.3.0E or later

show interface priority-flow-control

显示接口上的 PFC 操作状态、配置和统计信息。

**语法** `show interface [ethernet node/slot/port[:subport]] priority-flow-control [details]`

**参数** `ethernet node/slot/port[:subport]`

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 使用 `details` 选项针对每个 dot1p CoS 值显示已接收/已传输帧上的 PFC 统计信息。使用 `clear qos statistics interface ethernet 1/1/1` 命令删除 PFC 统计信息并重新启动计数器。

**示例（详细信息）**

```
OS10(config)# show interface ethernet 1/1/15 priority-flow-control
details

ethernet1/1/15
Admin Mode : true
Operstatus: true
PFC Priorities: 3
Total Rx PFC Frames: 0
Total Tx PFC frames: 587236
Cos Rx Tx

0 0 0
1 0 0
2 0 0
3 0 587236
```

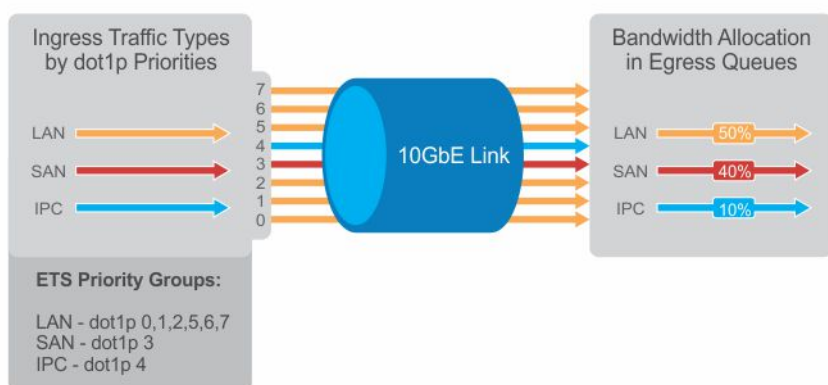
|   |   |   |
|---|---|---|
| 4 | 0 | 0 |
| 5 | 0 | 0 |
| 6 | 0 | 0 |
| 7 | 0 | 0 |

支持的版本 10.3.0E or later

## 增强的传输选择

ETS 提供了自定义的带宽分配给 802.1p 类别流量。在网络拥塞期间，为需要不同带宽、延迟和尽力处理的以太网、FCoE 或 iSCSI 流量类别分配不同数量的带宽。

ETS 使用其 802.1p 优先级值将流量划分为不同的优先级组。为确保每个流量类别均进行了正确的划分，并获得所需的带宽，请为每个优先级组配置带宽和队列计划。要为低延迟存储和服务器群集流量设置优先级，请为优先级组分配更多带宽。要对 LAN 流量进行评级限制，请将较少的带宽分配给不同的优先级组。



## ETS 配置说明

- ETS 在第二层 (L2) 802.1p 优先级 (dot1p 0 - 7) 和第三层 (L3) DSCP (0 - 63) 流量上受支持。FCoE 流量使用 dot1p 优先级 3 — iSCSI 存储流量使用 dot1p 优先级 4。
- 在接口上应用这些映射和策略：
  - 信任映射 — 默认情况下，OS10 接口不接受入口流量中的 L2 和 L3 优先级字段。创建信任映射，以提供无损流量的 dot1p 和 DSCP 类别。信任映射不会更改出口流中的入口 dot1p 和 DSCP 值。在信任映射中，将 qos-group 流量类别分配给信任 DOT1P/DSCP 值。Qos 组编号仅在内部使用，用于计划入口流量的类别。
  - QoS 映射 — 创建 QoS 映射，以将信任 dot1p 和 DSCP 流量类别分配给无损队列。
  - 入口信任策略 — 将服务策略配置为入口流量中的信任 dot1p 值。
  - 出口队列策略 — 通过分配带宽来匹配 queuing 类别和策略映射中的无损队列，以为出口流量配置 ETS。
- 在接口上应用 PFC 网络 qos (输入) 和 ETS 队列 (输出) 策略，以确保无损传输。
- 已启用 ETS 的接口可使用动态加权循环调度 (DWRR) 或严格优先级计划运行。
- OS10 控制流量将发送到控制队列，这些队列具有高于数据流量队列的严格优先级。在严格优先级队列上不支持 ETS 分配的带宽。严格优先级队列仅从 DCBX 类型、长度、值 (TLV) 接收带宽。
- 支持 ETS TLV 的 CEE/IEEE 2.5 版本。在 TLV 中从对等接收 ETS 配置。

## 配置 ETS

ETS 为同一链路上的无损存储、延迟敏感和尽力的数据流量提供流量优先级。

- 配置 dot1p 和 DSCP 流量类别，并将其分配给无损队列。
- 为每个无损队列分配有保证的带宽。如果另一个队列不使用其共享，ETS 队列可能会超过分配的带宽量。

默认情况下，ETS 在所有接口上处于禁用状态。

1. 在 CONFIGURATION 模式下配置 dot1p 和 DSCP 值的信任映射。信任映射不会修改输出流中的入口值。在 TRUST 模式下，将 qos-group（流量类别从 0 到 7）分配到信任 dot1p/DSCP 值 qos-group 数字仅限内部使用，用于计划入口流量的类别。以连字符范围或用逗号分隔方式输入多个 dot1p 和 dscp 值。

```
trust dot1p-map dot1p-map-name
 qos-group {0-7} dot1p {0-7}
 exit
trust dscp-map dscp-map-name
 qos-group {0-7} dscp {0-63}
 exit
```

2. 在 CONFIGURATION 模式下，将具有可信流量类别 (qos-group) 的 QoS 映射配置为信任流量类别。在 QOS-MAP 模式下，将一个或多个 qos 组（从 0 到 7）分配到指定队列。以连字符范围或用逗号分隔方式输入多个 qos-group 值。如有必要，输入多个 queue qos-group 条目。

```
qos-map traffic-class queue-map-name
 queue {0-7} qos-group {0-7}
 exit
```

3. 应用默认的信任映射，指定在 SYSTEM-QOS 或 INTERFACE 模式下信任 dot1p 和 dscp 值。

```
trust-map {dot1p | dscp} default
```

4. 在 CONFIGURATION 模式下为每个 ETS 队列创建 queuing 类别映射。在 CLASS-MAP 模式中输入 match queue 条件。

```
class-map type queuing class-map-name
 match queue {0-7}
 exit
```

5. 在 CONFIGURATION 模式下创建 queuing 策略映射。进入 POLICY-CLASS-MAP 模式，并配置分配到每个流量类别队列映射的带宽百分比。跨 ETS 队列的所有 DWRR 分配带宽的总和必须为 100%，不包括严格优先级队列。否则，QoS 会自动调整带宽百分比，以便 ETS 队列始终获得 100% 的带宽。剩余的非 ETS 队列会分别接收 1% 的带宽。

```
policy-map type queuing policy-map-name
 class class-map-name
 bandwidth percent {1-100}
```

（可选）要将队列配置为严格优先级，请使用 priority 命令。安排到严格优先级队列的数据包将在非优先级队列中的数据之前进行传输。

```
policy-map type queuing policy-map-name
 class class-map-name
 priority
```

6. 应用 dot1p 和 DSCP 值的信任映射，并且在 SYSTEM-QOS 模式下在交换机上全局应用或者在 INTERFACE 模式下在接口或接口范围上应用流量类别队列映射。

```
system qos
 trust-map dot1p dot1p-map-name
 trust-map dscp dscp-map-name
 qos-map traffic-class queue-map-name
```

或

```
interface {ethernet node/slot/port[:subport] | range ethernet node/slot/
port[:subport]-node/slot/port[:subport]}
 trust-map dot1p dot1p-map-name
 trust-map dscp dscp-map-name
 qos-map traffic-class queue-map-name
```

7. 将 qos 信任策略应用于在系统 QOS 或接口模式下的入口流量。

```
service-policy input type qos trust-policy-map-name
```

8. 将 queuing 策略应用于在系统 QoS 或接口模式下的出口流量。

```
service-policy output type queuing policy-map-name
```

9. 在 SYSTEM-QOS 模式下全局启用 ETS, 或者在 INTERFACE 模式下在接口/接口范围启用 ETS。

```
ets mode on
```

## 配置 ETS

```
OS10(config)# trust dot1p-map dot1p_map1
OS10(config-trust-dot1pmap)# qos-group 0 dot1p 0-3
OS10(config-trust-dot1pmap)# qos-group 1 dot1p 4-7
OS10(config-trust-dot1pmap)# exit

OS10(config)# trust dscp-map dscp_map1
OS10(config-trust-dscpmap)# qos-group 0 dscp 0-31
OS10(config-trust-dscpmap)# qos-group 1 dscp 32-63
OS10(config-trust-dscpmap)# exit

OS10(config)# qos-map traffic-class tc-q-map1
OS10(config-qos-tcmap)# queue 0 qos-group 0
OS10(config-qos-tcmap)# queue 1 qos-group 1
OS10(config-qos-tcmap)# exit

OS10(config)# system qos
OS10(config-sys-qos)# trust-map dot1p default

OS10(config)# class-map type queuing c1
OS10(config-cmap-queuing)# match queue 0
OS10(config-cmap-queuing)# exit
OS10(config)# class-map type queuing c2
OS10(config-cmap-queuing)# match queue 1
OS10(config-cmap-queuing)# exit

OS10(config)# policy-map type queuing p1
OS10(config-pmap-queuing)# class c1
OS10(config-pmap-queuing)# bandwidth percent 30
OS10(config-pmap-queuing)# exit
OS10(config)# policy-map type queuing p2
OS10(config-pmap-queuing)# class c2
OS10(config-pmap-queuing)# bandwidth percent 70
OS10(config-pmap-queuing)# exit

OS10(config)# system qos
OS10(config-sys-qos)# trust-map dot1p dot1p_map1
OS10(config-sys-qos)# trust-map dscp dscp_map1
OS10(config-sys-qos)# qos-map traffic-class tc-q-map1
OS10(config-sys-qos)# ets mode on
OS10(config-sys-qos)# service-policy output type queuing p1
```

## 查看 ETS 配置

```
OS10# show qos interface ethernet 1/1/1
Interface
unknown-unicast-storm-control : Disabled
multicast-storm-control : Disabled
broadcast-storm-control : Disabled
flow-control-rx : Disabled
flow-control-tx : Disabled
ets mode : Disabled
Dot1p-tc-mapping : dot1p_map1
Dscp-tc-mapping : dscp_map1
tc-queue-mapping : tc-q-map1
```

## 查看 QoS 映射: 流量类别到队列映射

```
OS10# show qos maps
Traffic-Class to Queue Map: tc-q-map1
queue 0 qos-group 0
```

```

queue 1 qos-group 1
Traffic-Class to Queue Map: dot1p_map1
qos-group 0 dot1p 0-3
qos-group 1 dot1p 4-7
DSCP Priority to Traffic-Class Map : dscp_map1
qos-group 0 dscp 0-31
qos-group 1 dscp 32-63

```

## ETS 命令

### ets mode on

在接口上启用 ETS。

**语法** ets mode on

**参数** 无

**默认** 已禁用

**命令模式** INTERFACE

**使用情况信息** 在 SYSTEM-QOS 模式下启用所有交换机接口的 ETS 或在 INTERFACE 模式下启用接口或接口范围的 ETS。此命令的 no 版本将禁用 ETS。

**示例**

```
OS10(config-sys-qos)# ets mode on
```

**支持的版本** 10.3.0E or later

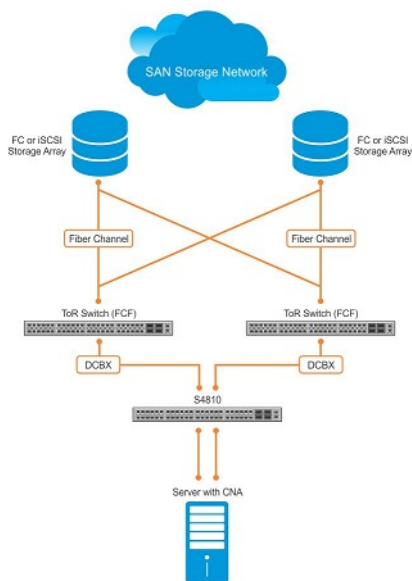
## 数据中心桥接交换

DCBX 允许交换机自动查找和设置配置了兼容设置器且已启用 DCBX 的对等节点。在聚合数据中心网络中，DCBX 在端到端解决方案中提供服务器、存储和网络设备的即插即用功能。

DCBX 使用链路层查找协议 (LLDP) 来协调自动协商和设备设置交换，例如 PFC 和 ETS。DCBX 使用 LLDP TLV 来执行 DCB 参数交换：

- PFC 配置和应用程序优先级配置
- ETS 配置和 ETS 建议

此示例 DCBX 拓扑在交换机上显示两个 40 GbE 端口，这些端口配置为 DCBX 自动上游端口，并用作到架顶式 (ToR) 交换机的上行链路。ToR 交换机属于光纤通道存储网络。



## DCBX 配置说明

- 要在聚合网络中交换链路级别配置，DCBX 是使用 DCB 功能的前提条件，例如 PFC 和 ETS。DCBX 还部署在支持 FCoE 或 iSCSI 流量的无损操作的拓扑中。在这些情况下，所有网络设备都必须启用 DCBX，以便 DCBX 启用端到端。
- DCBX 使用 LLDP 来通告并自动与直接连接的 DCB 对等主机协商管理状态和 PFC/ETS 配置。如果禁用某个接口上的 LLDP，DCBX 将无法运行。在所有 DCBX 端口上启用 LLDP，
- 默认情况下，DCBX 在全局级别处于禁用状态。在交换机上全局启用 DCBX，以使用 PFC、ETS 和 iSCSI 配置激活 DCBX TLV 消息的交换。
- 默认情况下，DCBX 在 OS10 接口上处于启用状态。您可以按每个接口手动重新配置 DCBX 设置。例如，您可以使用 `no lldp tlv-select dcbxp` 命令禁用接口上的 DCBX，或使用 `dcbx version` 命令更改 DCBX 版本。
- 要使 DCBX 正常运行，必须在全局和接口级别启用 DCBX。如果 `show lldp dcbx interface` 命令返回消息 `DCBX feature not enabled`，则不会在两个级别启用 DCBX。
- OS10 支持 DCBX 版本 CEE 和 IEEE 2.5。
- 默认情况下，DCBX 公布所有 TLV — PFC、ETS 建议、ETS 配置、DCBXP 和基本 TLV。
- 默认情况下，启用 DCBX 的端口以手动角色运行。此端口只能使用用户配置的设置来操作，并且不会与从 DCBX 对等方收到 DCB 设置进行自动配置。当您启用 DCBX 时，该端口会将其 PFC 和 ETS 端口通告给对等设备，但不接受外部或传播内部 DCB 配置。
- 当不使用本地交换机配置 DCB 功能时，DCBX 会检测对等设备上的配置错误。配置错误检查是特定于功能的，因为某些 DCB 功能支持非对称（非相同）配置。

## 配置 DCBX

通过 DCBX，数据中心设备可以向使用 LLDP 直接连接的对等节点通告和交换配置设置。LLDP 默认已启用。

为确保聚合数据中心网络的一致且高效的操作，DCBX 会检测到对等配置错误。

默认情况下，在全局级别禁用并在接口级别启用 DCBX。要使 DCBX 正常运行，必须在全局和接口级别启用 DCBX。您可以按每个接口手动重新配置 DCBX 设置或禁用 DCBX。

- 在 INTERFACE 模式下配置端口上使用的 DCBX 版本。

```
dcbx version {auto | cee | ieee}
```

- `auto` — 根据对等响应自动选择 DCBX 版本（默认值）。
- `cee` — 将 DCBX 版本设置为 CEE。
- `ieee` — 将 DCBX 版本设置为 IEEE 802.1Qaz。



2. (可选) 默认情况下, 已启用 DCBX 的端口将通告所有 TLV。如果 PFC 或 ETS TLV 处于禁用状态, 请在 INTERFACE 模式下输入命令以重新启用 PFC 或 ETS TLV 通告。

```
dcbx tlv-select {ets-conf | ets-reco | pfc}
```

- ets-conf — 启用 ETS 配置 TLV。
- ets-reco — 启用 ETS 建议 TLV。
- pfc — 启用 PFC TLV。

3. (可选) 默认情况下, 在端口上启用 DCBX。如果 DCBX 已禁用, 请在 INTERFACE 模式下启用它。

```
lldp tlv-select dcbxp
```

4. 返回 CONFIGURATION 模式。

```
exit
```

5. 在 CONFIGURATION 模式下全局启用交换机上的 DCBX, 以使用 PFC、ETS 和 iSCSI 配置激活 DCBX TLV 消息的交换。

```
dcbx enable
```

## 配置 DCBX

### 查看 DCBX 配置

```
OS10# show lldp dcbx interface ethernet 1/1/15
```

|                                          |                                           |
|------------------------------------------|-------------------------------------------|
| E-ETS Configuration TLV enabled          | e-ETS Configuration TLV disabled          |
| R-ETS Recommendation TLV enabled         | r-ETS Recommendation TLV disabled         |
| P-PFC Configuration TLV enabled          | p-PFC Configuration TLV disabled          |
| F-Application priority for FCOE enabled  | f-Application Priority for FCOE disabled  |
| I-Application priority for iSCSI enabled | i-Application Priority for iSCSI disabled |

-

```
Interface ethernet1/1/15
 Port Role is Manual
 DCBX Operational Status is Enabled
 Is Configuration Source? FALSE
 Local DCBX Compatibility mode is CEE
 Local DCBX Configured mode is CEE
 Peer Operating version is CEE
 Local DCBX TLVs Transmitted: ErPFI
```

#### Local DCBX Status

```

DCBX Operational Version is 0
DCBX Max Version Supported is 0
Sequence Number: 14
Acknowledgment Number: 5
Protocol State: In-Sync
```

#### Peer DCBX Status

```

DCBX Operational Version is 0
DCBX Max Version Supported is 255
Sequence Number: 5
Acknowledgment Number: 14
 220 Input PFC TLV pkts, 350 Output PFC TLV pkts, 0 Error PFC pkts
 220 Input PG TLV Pkts, 396 Output PG TLV Pkts, 0 Error PG TLV Pkts
 71 Input Appln Priority TLV pkts, 80 Output Appln Priority TLV pkts, 0 Error Appln
Priority TLV Pkts
```

```
Total DCBX Frames transmitted 538
Total DCBX Frames received 220
Total DCBX Frame errors 0
Total DCBX Frames unrecognized 0
```

查看 DCBX PFC TLV 状态

```
OS10# show lldp dcbx interface ethernet 1/1/15 pfc detail

Interface ethernet1/1/15
 Admin mode is on
 Admin is enabled, Priority list is 4,5,6,7
 Remote is enabled, Priority list is 4,5,6,7
 Remote Willing Status is disabled
 Local is enabled, Priority list is 4,5,6,7
 Oper status is init
 PFC DCBX Oper status is Up
 State Machine Type is Feature
 PFC TLV Tx Status is enabled
 Application Priority TLV Parameters :

 ISCSI TLV Tx Status is enabled
 Local ISCSI PriorityMap is 0x10
 Remote ISCSI PriorityMap is 0x10

 220 Input TLV pkts, 350 Output TLV pkts, 0 Error pkts
 71 Input Appln Priority TLV pkts, 80 Output Appln Priority TLV pkts, 0 Error Appln
 Priority TLV Pkts
```

查看 DCBX ETS TLV 状态

```
OS10# show lldp dcbx interface ethernet 1/1/15 ets detail

Interface ethernet1/1/15
Max Supported PG is 8
Number of Traffic Classes is 8
Admin mode is on

Admin Parameters :

Admin is enabled

PG-grp Priority# Bandwidth TSA

0 0,1,2,3 70% ETS
1 4,5,6,7 30% ETS
2 0% 0% SP
3 0% 0% SP
4 0% 0% SP
5 0% 0% SP
6 0% 0% SP
7 0% 0% SP
15 0% 0% SP

Remote Parameters :

Remote is enabled
PG-grp Priority# Bandwidth TSA

0 0,1,2,3 70% ETS
1 4,5,6,7 30% ETS
2 0% 0% SP
3 0% 0% SP
4 0% 0% SP
5 0% 0% SP
6 0% 0% SP
7 0% 0% SP
15 0% 0% SP

Remote Willing Status is disabled
Local Parameters :

Local is enabled

PG-grp Priority# Bandwidth TSA

0 0,1,2,3 70% ETS
```

|    |            |     |     |
|----|------------|-----|-----|
| 1  | 4, 5, 6, 7 | 30% | ETS |
| 2  |            | 0%  | SP  |
| 3  |            | 0%  | SP  |
| 4  |            | 0%  | SP  |
| 5  |            | 0%  | SP  |
| 6  |            | 0%  | SP  |
| 7  |            | 0%  | SP  |
| 15 |            | 0%  | SP  |

Oper status is init  
ETS DCBX Oper status is Up  
State Machine Type is Feature  
Conf TLV Tx Status is enabled  
Reco TLV Tx Status is disabled

220 Input Conf TLV Pkts, 396 Output Conf TLV Pkts, 0 Error Conf TLV Pkts

DCBX 命令

dcbx enable

在所有端口接口上全局启用 DCBX。

|        |                                                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | dcbx enable                                                                                                                                                                                                                                                                     |
| 参数     | 无                                                                                                                                                                                                                                                                               |
| 默认     | 已禁用                                                                                                                                                                                                                                                                             |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                   |
| 使用情况信息 | 默认情况下，在全局级别禁用并在接口级别启用 DCBX。要使 DCBX 正常运行，必须在全局和接口级别启用 DCBX。使用 dcbx enable 命令，以使用 PFC、ETS 和 iSCSI 配置激活 DCBX TLV 消息的交换。要配置已启用 DCBX 的端口通告的 TLV，请更改 DCBX 版本；要禁用接口上的 DCBX，请使用 DCBX 接口级别命令。DCBX 允许对等体使用 LLDP 通告 DCB 配置，并通过兼容的设置进行自我配置。如果在交换机上全局禁用 DCBX，您可以重新启用它，以确保对聚合数据中心网络中对等体的一致操作。 |
| 示例     | OS10(config)# dcbx enable                                                                                                                                                                                                                                                       |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                |

dcbx tlv-select

配置由启用 DCBX 的端口通告的 DCB TLV。

|        |                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | dcbx tlv-select {[ets-conf] [ets-reco] [pfc]}                                                                                                 |
| 参数     | <ul style="list-style-type: none"> <li>ets-conf — 通告 ETS 配置 TLV。</li> <li>ets-reco — 通告 ETS 建议 TLV。</li> <li>pfc — 通告 PFC TLV。</li> </ul>     |
| 默认     | DCBX 将通告 PFC、ETS 建议和 ETS 配置 TLV。                                                                                                              |
| 命令模式   | INTERFACE                                                                                                                                     |
| 使用情况信息 | 默认情况下，启用 DCBX 的端口会将所有 TLV 通告到 DCBX 对等节点。如果 PFC 或 ETS TLV 处于禁用状态，请输入命令以重新启用 PFC 或 ETS TLV 通告。您可以使用相同的命令启用多个 TLV 选项，例如 ets-conf、ets、reco 和 pfc。 |
| 示例     | OS10(config-if-eth1/1/2)# dcbx tlv-select ets-conf pfc                                                                                        |
| 支持的版本  | 10.3.0E or later                                                                                                                              |

## dcbx version

配置在端口接口上使用的 DCBX 版本。

|        |                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>dcbx version {auto   cee   ieee}</code>                                                                                                                                                |
| 参数     | <ul style="list-style-type: none"><li><code>auto</code> — 根据对等响应自动选择 DCBX 版本。</li><li><code>cee</code> — 将 DCBX 版本设置为 CEE。</li><li><code>ieee</code> — 将 DCBX 版本设置为 IEEE 802.1Qaz。</li></ul> |
| 默认     | 自动                                                                                                                                                                                           |
| 命令模式   | INTERFACE                                                                                                                                                                                    |
| 使用情况信息 | 在自动模式下，已启用 DCBX 的端口检测到对等设备端口上存在不兼容的 DCBX 版本，并会自动重新配置本地端口上的兼容版本。此命令的 <code>no</code> 版本将禁用 DCBX 版本。                                                                                           |
| 示例     | <pre>OS10(config-if-eth1/1/2)# dcbx version cee</pre>                                                                                                                                        |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                             |

## lldp tlv-select dcbxp

启用和禁用端口接口上的 DCBX。

|        |                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>lldp tlv-select dcbxp</code>                                                                                                                                                           |
| 参数     | 无                                                                                                                                                                                            |
| 默认     | 启用的接口级别；禁用的全局级别                                                                                                                                                                              |
| 命令模式   | INTERFACE                                                                                                                                                                                    |
| 使用情况信息 | 必须在全局和接口级别启用 DCBX。使用 <code>dcbx enable</code> 命令，以使用 PFC、ETS 和 iSCSI 配置激活 DCBX TLV 消息的交换。要配置已启用 DCBX 的端口通告的 TLV，请更改 DCBX 版本；要禁用接口上的 DCBX，请使用 DCBX 接口级别命令。此命令的 <code>no</code> 版本将禁用接口上 DHCP。 |
| 示例     | <pre>OS10(config-if-eth1/1/1)# lldp tlv-select dcbxp</pre>                                                                                                                                   |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                             |

## show lldp dcbx interface

显示 DCBX 配置和接口上的 PFC 或 ETS TLV 状态。

|        |                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show lldp dcbx interface ethernet node/slot/port[:subport] [ets detail   pfc detail]</code>                                                                                                                                                                                                                       |
| 参数     | <ul style="list-style-type: none"><li><code>interface ethernet node/slot/port[:subport]</code> — 输入接口信息。</li><li><code>ets detail</code> — 显示使用 DCBX 对等体的 ETS TLV 状态和操作。</li><li><code>pfc detail</code> — 显示使用 DCBX 对等体的 PFC TLV 状态和操作。</li></ul>                                                                      |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                     |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                    |
| 使用情况信息 | 请先启用 DCBX，然后再使用此命令。DCBX 通告所有 TLV — PFC、ETS 建议、ETS 配置、DCBXP 和基本 TLV。要在多个端口上显示 DCBX 配置和 TLV 操作的端口范围。<br><div> <b>注：</b>在命令输出中，<code>Is configuration source</code> 参数将始终显示 <code>False</code>。Configuration source 是不支持的端口角色的类型。</div> |
| 示例（接口） | <pre>OS10# show lldp dcbx interface ethernet 1/1/15 E-ETS Configuration TLV enabled          e-ETS Configuration TLV disabled R-ETS Recommendation TLV enabled         r-ETS Recommendation TLV disabled</pre>                                                                                                          |

```

P-PFC Configuration TLV enabled p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled i-Application Priority for iSCSI disabled

Interface ethernet1/1/15
 Port Role is Manual
 DCBX Operational Status is Enabled
 Is Configuration Source? FALSE
 Local DCBX Compatibility mode is IEEEv2.5
 Local DCBX Configured mode is IEEEv2.5
 Peer Operating version is IEEEv2.5
 Local DCBX TLVs Transmitted: ERPF1
 5 Input PFC TLV pkts, 2 Output PFC TLV pkts, 0 Error PFC pkts
 5 Input ETS Conf TLV Pkts, 2 Output ETS Conf TLV Pkts, 0 Error ETS Conf TLV
Pkts
 5 Input ETS Reco TLV pkts, 2 Output ETS Reco TLV pkts, 0 Error ETS Reco TLV
Pkts
 5 Input Appln Priority TLV pkts, 2 Output Appln Priority TLV pkts, 0 Error
Appln Priority TLV Pkts

Total DCBX Frames transmitted 8
Total DCBX Frames received 20
Total DCBX Frame errors 0
Total DCBX Frames unrecognized 0

```

### 示例 (ETS 详细信息)

```

OS10# show lldp dcbx interface ethernet 1/1/15 ets detail
Interface ethernet1/1/15
Max Supported PG is 8
Number of Traffic Classes is 8
Admin mode is on

Admin Parameters :

Admin is enabled

PG-grp Priority# Bandwidth TSA

0 0,1,2,3 70% ETS
1 4,5,6,7 30% ETS
2 0% SP
3 0% SP
4 0% SP
5 0% SP
6 0% SP
7 0% SP

Remote Parameters :

Remote is enabled
PG-grp Priority# Bandwidth TSA

0 0,1,2,3 70% ETS
1 4,5,6,7 30% ETS
2 0% SP
3 0% SP
4 0% SP
5 0% SP
6 0% SP
7 0% SP

Remote Willing Status is disabled
Local Parameters :

Local is enabled

PG-grp Priority# Bandwidth TSA

0 0,1,2,3 70% ETS
1 4,5,6,7 30% ETS

```

```

2 0% SP
3 0% SP
4 0% SP
5 0% SP
6 0% SP
7 0% SP

Oper status is init
ETS DCBX Oper status is Up
State Machine Type is Asymmetric
Conf TLV Tx Status is enabled
Reco TLV Tx Status is enabled

5 Input Conf TLV Pkts, 2 Output Conf TLV Pkts, 0 Error Conf TLV Pkts
5 Input Reco TLV Pkts, 2 Output Reco TLV Pkts, 0 Error Reco TLV Pkts

```

### 示例 (PFC 详细信息)

```

OS10# show lldp dcbx interface ethernet 1/1/15 pfc detail
Interface ethernet1/1/15
 Admin mode is on
 Admin is enabled, Priority list is 4,5,6,7
 Remote is enabled, Priority list is 4,5,6,7
 Remote Willing Status is disabled
 Local is enabled, Priority list is 4,5,6,7
 Oper status is init
 PFC DCBX Oper status is Up
 State Machine Type is Symmetric
 PFC TLV Tx Status is enabled
 Application Priority TLV Parameters :

 ISCSI TLV Tx Status is enabled
 Local ISCSI PriorityMap is 0x10
 Remote ISCSI PriorityMap is 0x10

 5 Input TLV pkts, 2 Output TLV pkts, 0 Error pkts
 5 Input Appln Priority TLV pkts, 2 Output Appln Priority TLV pkts, 0 Error
 Appln Priority TLV Pkts

```

### 支持的版本

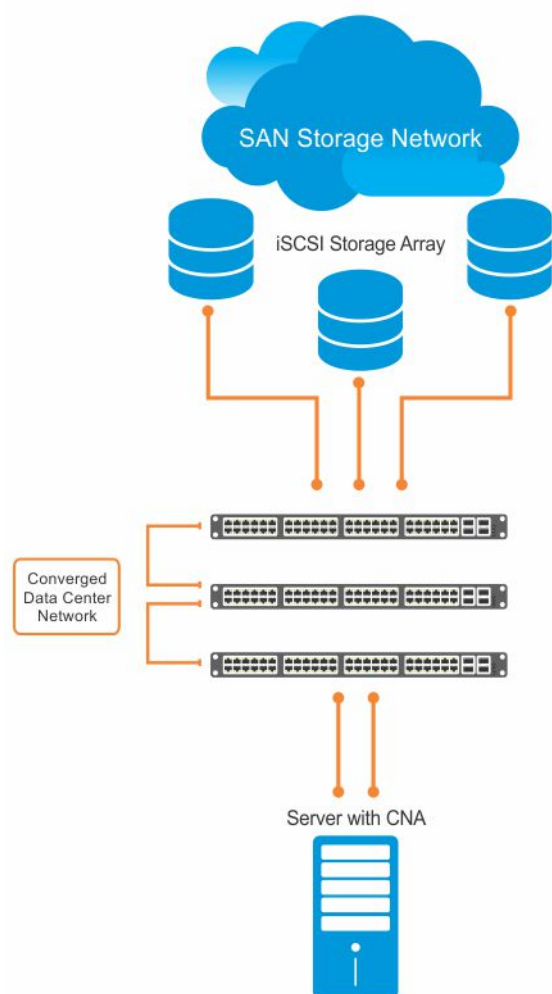
10.3.0E or later

## 互联网小型计算机系统接口

iSCSI 是一种基于 TCP/IP 的协议，可在数据中心网络中的服务器与存储设备之间建立和管理连接。启用 iSCSI 后，iSCSI 优化功能会自动检测直接连接到交换机端口的 Dell EMC EqualLogic 存储阵列。要支持不支持自动检测的存储阵列，请使用 `iscsi profile-storage name` 命令手动配置 iSCSI 优化。

iSCSI 优化使交换机能够自动检测 Dell EMC iSCSI 存储阵列和自动配置交换机端口，以提高存储流量吞吐量。交换机监控 iSCSI 会话并对 iSCSI 流量应用 QoS 策略。iSCSI 优化通过以太网网络运行或不使用 DCBX。

- 默认情况下，iSCSI 使用当前流控制配置。如果不配置流控制，iSCSI 可自动配置流控制设置，以便仅接收处于启用状态并且仅传输处于禁用状态。
- 交换机将监控和跟踪活动 iSCSI 会话，包括端口信息和 iSCSI 会话信息。
- 用户配置的 iSCSI CoS 配置文件适用于所有 iSCSI 流量。使用分类器规则可将 iSCSI 数据流量定向到优先将 QoS 处理排入队列，而不是通过交换机传递的其他数据。优先处理可帮助避免在拥塞期间的会话中断，否则可能会导致 iSCSI 数据包丢失。



在 iSCSI 会话中，交换机将 CNA 服务器（iSCSI 启动器）连接到 SAN 或 TCP/IP 网络中的存储阵列（iSCSI 目标）。交换机上运行 iSCSI 优化使用 dot1p 优先级队列分配来确保 iSCSI 流量获得优先级处理。

## iSCSI 配置说明

- 启用 iSCSI 优化，以便交换机自动检测和自动配置直接连接到接口的 Dell EMC EqualLogic 存储阵列。在验证与存储设备的连接后，iSCSI 会自动配置交换机参数。启用接口以支持直接连接到端口但不是由 iSCSI 自动检测的存储设备。
- 启用 iSCSI 会话监控和 iSCSI 会话的老化时间。默认情况下，iSCSI 监控会话将侦听 TCP 端口 860 和 3260。
- 配置应用到入口 iSCSI 流的 CoS/DSCP 值 — 在 POLICY-CLASS-MAP 模式下创建 `class-iscsi` 类别映射。
- 启用 LLDP 以使用 iSCSI。DCBX 应用程序 TLV 将承载发送 iSCSI 流量时使用的 dot1p 优先级的相关信息。此信息 TLV 封装在 LLDP PDU 中。您可以重新配置在 TLV 中通告的 802.1p 优先级位。

## 配置 iSCSI 优化

iSCSI 协议使用 iSCSI 命令在网络中的服务器和存储阵列之间提供存储流量 TCP/IP 传输。

1. 配置接口或接口范围以检测已连接的存储设备。

```
interface ethernet node/slot/port:[subport]

interface range ethernet node/slot/port:[subport]-node/slot/port[:subport]
```

2. 启用接口以支持直接连接到端口但不是由 iSCSI 自动检测的存储设备。对于不支持 LLDP 的存储设备，请使用此命令。当您启用 iSCSI 优化时，交换机将自动检测和自动配置直接连接到接口的 Dell EMC EqualLogic 存储阵列。

```
iscsi profile-storage storage-device-name
```

3. 在 INTERFACE 模式下配置 DCBX 以使用 LLDP 将 iSCSI 应用程序 TLV 和 dot1p 优先级一起发送到 iSCSI 流量。

```
lldp tlv-select dcbxp-appln iscsi
```

4. 返回 CONFIGURATION 模式。

```
exit
```

5. (可选) 如有必要，在 CONFIGURATION 模式下重新配置目标存储设备的 iSCSI TCP 端口和 IP 地址。使用逗号分隔 TCP 端口号，从 0 到 65535；默认值为 860 和 3260。

```
iscsi target port tcp-port1 [tcp-port2, ..., tcp-port16] [ip-address ip-address]
```

6. 配置应用于入口 iSCSI 流的 QoS 策略。在 CONFIGURATION 模式下将服务策略应用于入口接口。

(可选) 重设默认的 CoS dot1p 优先级 (默认值为 4) 和/或用于 iSCSI 流量的受信任 DSCP 值。在 POLICY-CLASS-MAP 模式下分配内部 qos-group 队列 (从 0 到 7)，dot1p (从 0 到 7)，以及 DSCP (从 0 到 63) 的值。

```
class-map type application class-iscsi
policy-map type application policy-iscsi
 class class-iscsi
 set qos-group traffic-class-number
 set cos dot1p-priority
 set dscp dscp-value
 end
service-policy type application policy-iscsi
```

7. 在 CONFIGURATION 模式下启用 TCP 端口上的 iSCSI 监控会话。

```
iscsi session-monitoring enable
```

8. (可选) 在 CONFIGURATION 模式下设置 iSCSI 监控会话长度的帐龄时间，5 至 43200 分钟；默认值为 10。

```
iscsi aging time [minutes]
```

9. (可选) 在 CONFIGURATION 模式下重新配置 iSCSI 应用程序 TLV 中通告的 dot1p 优先级位。默认位图为 0x10 (dot1p 4)。只有在使用 pfc-cos dot1p-priority 命令为 dot1p 4 流量启用 PFC 暂停时，才会在 iSCSI 应用程序 TLV 中发送默认的 dot1p 4 值。

如果未配置 iscsi priority-bits dot1p 值，并且在步骤 6 中配置了一个 set cos 值，则 set cos 值将在 iSCSI 应用程序 TLV 中发送。如果未配置 iscsi priority-bits 或 set cos 值，将通告默认的 dot1p 4。

```
iscsi priority-bits dot1p-bitmap
```

10. 在 CONFIGURATION 模式下启用交换机上 iSCSI 自动检测和自动配置。

```
iscsi enable
```

## 配置 iSCSI 优化

```
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# iscsi profile-storage compellent
OS10(config-if-eth1/1/1)# lldp tlv-select dcbxp-appln iscsi
OS10(config-if-eth1/1/1)# exit

OS10(config)# iscsi target port 3261 ip-address 10.1.1.1
OS10(config)# policy-map type application policy-iscsi
OS10(config-pmap-application)# class class-iscsi
OS10 (config-pmap-c-app)# set qos-group 4
OS10 (config-pmap-c-app)# set cos 4
OS10 (config-pmap-c-app)# exit
OS10(config-pmap-application)# exit

OS10(config)# system qos
OS10(config-sys-qos)# service-policy type application policy-iscsi
OS10(config-sys-qos)# exit
```



```
OS10(config)# iscsi session-monitoring enable
OS10(config)# iscsi aging time 15
OS10(config)# iscsi priority-bits 0x20
OS10(config)# iscsi enable
```

## 查看 iSCSI 优化

```
OS10# show iscsi
iSCSI Auto configuration is Enabled
iSCSI session monitoring is Enabled
iSCSI COS qos-group 4 remark dot1p 4
Session aging time 15
Maximum number of connections is 100
Port IP Address

3260
860
3261 10.1.1.1
```

```
OS10# show iscsi session detailed
Session 1

Target:iqn.2001-05.com.equallogic:0-8a0906-00851a00c-98326939fba510a1-517
Initiator:iqn.1991-05.com.microsoft:win-rlkpjo4jun2
Up Time:00:00:18:12(DD:HH:MM:SS)
Time for aging out:29:23:59:35(DD:HH:MM:SS)
ISID:400001370000
Initiator Initiator Target Target Connection
IP Address TCP Port IP Address TCP Port ID

10.10.10.210 54748 10.10.10.40 3260 1

Session 2

Target:iqn.2001-05.com.equallogic:0-8a0906-01251a00c-8ab26939fbd510a1-518
Initiator:iqn.1991-05.com.microsoft:win-rlkpjo4jun2
Up Time:00:00:16:02(DD:HH:MM:SS)
Time for aging out:29:23:59:35(DD:HH:MM:SS)
ISID:400001370000
Initiator Initiator Target Target Connection
IP Address TCP Port IP Address TCP Port ID

10.10.10.210 54835 10.10.10.40 3260 1
```

```
OS10# show iscsi storage-devices
Interface Name Storage Device Name Auto Detected Status

ethernet1/1/23 EQL-MEM true
```

## VLT 上的 iSCSI 同步

在以下情况下，在 VLT LAG 上学习 iSCSI 会话：

- 如果 iSCSI 会话会在 VLT LAG 上接收到控制数据包（作为登录请求或登录响应）。
- 如果 iSCSI 会话未接收控制数据包，但会接收 VLT LAG 上的数据包。当您在 iSCSI 会话启动后启用 iSCSI 会话监控时，会发生这种情况。

VLT LAG 上的 iSCSI 会话的相关信息与 VLT 对等节点同步。

基于多种方案进行 iSCSI 会话同步：

- 如果在属于 VLT LAG 的接口上收到 iSCSI 登录请求，则该信息将与 VLT 对等节点同步，并与该接口关联。
- 对于连接的任何更新，包括在 VLT LAG 成员上学习的时效更新将与 VLT 对等节点同步。
- 如果在非 VLT 接口上收到了 iSCSI 登录请求，后跟来自 VLT 接口的响应，该连接将与 VLT LAG 接口关联，并且与该会话相关的信息将与 VLT 对等节点同步。
- 当 VLT 互连出现时，有关在 VLT 对等节点之间的 VLT LAG 交换上学习的 iSCSI 会话的信息。

## iSCSI 命令

### iscsi aging

设置监控 iSCSI 会话的帐龄时间。

|        |                                                                        |
|--------|------------------------------------------------------------------------|
| 语法     | <code>iscsi aging [time minutes]</code>                                |
| 参数     | <code>time minutes</code> — 输入 iSCSI 会话监控允许的帐龄时间（以分钟为单位），从 5 到 43,200。 |
| 默认     | 10 分钟                                                                  |
| 命令模式   | CONFIGURATION                                                          |
| 使用情况信息 | 配置在关闭会话之前允许在 TCP 端口上监控 iSCSI 会话的帐龄时间。此命令的 <code>no</code> 版本将禁用帐龄时间。   |
| 示例     | <pre>OS10(config)# iscsi aging time 30</pre>                           |
| 支持的版本  | 10.3.0E or later                                                       |

### iscsi enable

支持对连接的存储阵列和交换机自动配置进行 iSCSI 自动检测。

|        |                                                                                                                                                                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>iscsi enable</code>                                                                                                                                                                                                                                |
| 参数     | 无                                                                                                                                                                                                                                                        |
| 默认     | 无                                                                                                                                                                                                                                                        |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                            |
| 使用情况信息 | <p>iSCSI 优化功能会自动检测存储阵列和自动配置交换机端口，并使用从已连接的设备收到的 iSCSI 参数。此命令的 <code>no</code> 版本将禁用 iSCSI 自动检测。</p> <p>从版本 10.4.1.1 开始，在执行 OS10 的全新安装时，iSCSI 自动配置已启用并且流控制接收设置为开。但是，当您从较早的版本升级到版本 10.4.1.1 或更高版本时，将保留现有的 iSCSI 配置，并且流控制接收可以设置为开或关，具体取决于升级之前的 iSCSI 配置。</p> |
| 示例     | <pre>OS10(config)# iscsi enable</pre>                                                                                                                                                                                                                    |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                         |

### iscsi priority-bits

重置在 iSCSI 应用程序 TLV 中通告的优先级位图。

|        |                                                                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>iscsi priority-bits {priority-bitmap}</code>                                                                                                                                                                                       |
| 参数     | <code>priority-bitmap</code> — 为 iSCSI 应用程序 TLV (0x1 至 0xff) 中的 iSCSI 流量输入 dot1p 优先级通告的位图值。                                                                                                                                              |
| 默认     | 0x10 (dot1p 4)                                                                                                                                                                                                                           |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                            |
| 使用情况信息 | <p>默认情况下，iSCSI 流量在帧标题中使用 dot1p 优先级 4。使用此命令可重新配置 iSCSI 应用程序 TLV 中通告的 dot1p 优先级位。仅输入一个 dot1p 位图值 — 不支持使用此命令设置多个位图值。仅在您使用 <code>pfc-cos dot1p-priority</code> 命令为 dot1p 4 流量启用了 PFC 暂停帧时默认 dot1p 4 值才通告。此命令的 <code>no</code> 版本将重置为默认值。</p> |
| 示例     | <pre>OS10(config)# iscsi priority-bits 0x20</pre>                                                                                                                                                                                        |

支持的版本 10.3.0E or later

## iscsi profile-storage

配置用于直接连接到未通过 iSCSI 自动检测到的存储设备的端口。

**语法** `iscsi profile-storage storage-device-name`

**参数** `storage-device-name` — 输入不会自动检测 iSCSI 的存储阵列的用户定义名称。

**默认** 未配置

**命令模式** INTERFACE

**使用情况信息** 配置 iSCSI 支持的直接连接的存储阵列（如果不会自动检测到）。对于不支持 LLDP 的存储设备，此命令是必需的。此命令的 `no` 版本将禁用连接。

**示例**

```
OS10(config-if-eth1/1/2)# iscsi profile-storage compellant
```

支持的版本 10.3.0E or later

## iscsi session-monitoring enable

启用 iSCSI 会话监控。

**语法** `iscsi session-monitoring enable`

**参数** 无

**默认** 已禁用

**命令模式** CONFIGURATION

**使用情况信息** 要在 iSCSI 监控会话中配置帐龄超时，请使用 `iscsi aging time` 命令。要在 iSCSI 监控会话中配置侦听连接的存储设备的 TCP 端口，请使用 `iscsi target port` 命令。此命令的 `no` 版本将禁用 iSCSI 会话监控。

**示例**

```
OS10(config)# iscsi session-monitoring enable
```

支持的版本 10.3.0E or later

## iscsi target port

配置用于监控与目标存储设备的 iSCSI 会话的 TCP 端口。

**语法** `iscsi target port tcp-port1 [tcp-port2, ..., tcp-port16] [ip-address ip-address]`

**参数**

- `tcp-port` — 输入一个或多个 TCP 端口号，从 0 到 65535。使用逗号分隔 TCP 端口号。
- `ip-address ip-address` — （可选）在 TCP 端口上为其 iSCSI 流量监控的存储阵列输入采用 A.B.C.D 格式的 IP 地址。

**默认** 3260,860

**命令模式** CONFIGURATION

**使用情况信息** 您可以配置最多 16 个 TCP 端口，以监控来自目标存储设备的 iSCSI 流量。此命令的 `no` 版本（包括 IP 地址）会从 iSCSI 监控中删除 TCP 端口。

**示例**

```
OS10(config)# iscsi target port 26,40
```

支持的版本 10.3.0E or later

## lldp tlv-select dcbxp-appln iscsi

使端口能够向 DCBX 对等节点通告 iSCSI 应用程序 TLV。

|        |                                                                                                                                                                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | lldp tlv-select dcbxp-appln iscsi                                                                                                                                                                                                                                                                     |
| 参数     | 无                                                                                                                                                                                                                                                                                                     |
| 默认     | iSCSI 应用程序 TLV 将通告至 DCBX 对等节点。                                                                                                                                                                                                                                                                        |
| 命令模式   | INTERFACE                                                                                                                                                                                                                                                                                             |
| 使用情况信息 | DCB 设备使用 DCBX 与对等节点交换 iSCSI 配置信息并自行配置。iSCSI 参数交换时间、长度和值 (TLV) 消息。DCBX 需要启用 LLDP 才能通告 iSCSI 应用程序 TLV。iSCSI 应用程序 TLV 将向 DCBX 对等节点通告使用 iscsi priority-bits 命令配置的 PFC dot1p 优先级位图。如果您未配置 iSCSI dot1p 位图值，则仅当使用 pfc-cos 命令将 dot1p 4 配置为 PFC 优先级时，iSCSI 应用程序 TLV 才会默认通告 dot1p 4。此命令的 no 版本将禁用 iSCSI TLV 传输。 |
| 示例     | <pre>OS10(conf-if-eth1/1/1)# lldp tlv-select dcbxp-appln iscsi</pre>                                                                                                                                                                                                                                  |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                                                                      |

## show iscsi

显示当前配置的 iSCSI 设置。

|        |                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show iscsi                                                                                                                                                                                                                                       |
| 参数     | 无                                                                                                                                                                                                                                                |
| 命令模式   | EXEC                                                                                                                                                                                                                                             |
| 使用情况信息 | 此命令输出将显示全局 iSCSI 配置设置。要查看目标和启动器信息，请使用 show iscsi session 命令。                                                                                                                                                                                     |
| 示例     | <pre>OS10# show iscsi iSCSI Auto configuration is Enabled iSCSI session monitoring is Enabled iSCSI COS qos-group 4 remark dot1p 4 Session aging time 15 Maximum number of connections is 256 Port IP Address ----- 3260 860 3261 10.1.1.1</pre> |
| 支持的版本  | 10.3.0E or later                                                                                                                                                                                                                                 |

## show iscsi session

显示有关活动 iSCSI 会话的信息。

|        |                                                  |
|--------|--------------------------------------------------|
| 语法     | show iscsi session [detailed]                    |
| 参数     | detailed — 显示活动 iSCSI 会话的详细版本。                   |
| 命令模式   | EXEC                                             |
| 使用情况信息 | 在 iSCSI 会话中，Target 是存储设备，Initiator 是连接到存储设备的服务器。 |
| 示例     | <pre>OS10# show iscsi session</pre>              |

示例（详细）

```
OS10# show iscsi session detailed
Session 1

Target:iqn.2001-05.com.equallogic:0-8a0906-00851a00c-98326939fba510a1-517
Initiator:iqn.1991-05.com.microsoft:win-rlkpjo4jun2
Up Time:00:00:18:12 (DD:HH:MM:SS)
Time for aging out:29:23:59:35 (DD:HH:MM:SS)
ISID:400001370000
Initiator Initiator Target Target Connection
IP Address TCP Port IP Address TCP Port ID

10.10.10.210 54748 10.10.10.40 3260 1

Session 2

Target:iqn.2001-05.com.equallogic:0-8a0906-01251a00c-8ab26939fbd510a1-518
Initiator:iqn.1991-05.com.microsoft:win-rlkpjo4jun2
Up Time:00:00:16:02 (DD:HH:MM:SS)
Time for aging out:29:23:59:35 (DD:HH:MM:SS)
ISID:400001370000
Initiator Initiator Target Target Connection
IP Address TCP Port IP Address TCP Port ID

10.10.10.210 54835 10.10.10.40 3260 1
```

支持的版本 10.3.0E or later

show iscsi storage-devices

显示直接连接到 OS10 端口的存储阵列的相关信息。

语法 show iscsi storage-devices

参数 无

命令模式 EXEC

使用情况信息 命令输出将显示连接到每个交换机端口的存储设备以及 iSCSI 是否自动检测它。

示例

```
OS10# show iscsi storage-devices
Interface Name Storage Device Name Auto Detected Status

ethernet1/1/23 EQL-MEM true
```

支持的版本 10.3.0E or later

聚合网络 DCB 示例

聚合数据中心网络具有多个 SAN、服务器和 LAN 流量类型，对数据传输的不同方面敏感。例如，存储流量对数据包丢失敏感，而服务器流量对延迟敏感。在单个融合链路中，所有流量类型均会共存，而不会对其他性能施加限制。DCB 允许 iSCSI 和 FCoE SAN 流量与同一网络上的服务器和 LAN 流量共存。DCB 功能将减少或避免丢弃帧、重新传输和网络拥塞。

- DCB 使用以下内容提供 FCoE 和 iSCSI 存储流量的无损传输：
- 为网络应用程序的不同服务需求单独提供流量类别。
  - PFC 流控制以暂停数据传输，并避免在拥塞期间丢弃数据包。
  - ETS 带宽分配可保证突发流量的共享带宽百分比，同时允许每个流量类别在另一个流量类别不使用其共享时超过其分配的带宽。
  - DCBX 发现对等，包括 PFC、ETS 和其他 DCB 设置参数交换、不匹配检测以及 DCB 参数的远程配置。
  - DCBX 中的 iSCSI 应用程序协议 TLV 信息将通告以向对等端口传达 iSCSI 支持。

- 本示例显示如何配置 DCB 融合网络，其中：
- DCBx 已全局启用，以确保在启用 DCBx 的设备之间交换 DCBx、PFC、ETS 和 iSCSI 配置。
  - PFC 配置为确保 dot1p 优先级 4、5、6 和 7 流量的无损流量。
  - 对于优先级为 4、5、6 和 7 的流量，ETS 为 dot1p 优先级 0、1、2 和 3 流量分配 30% 的带宽和 70% 的带宽。

- iSCSI 配置为将 dot1p 优先级 6 用于 iSCSI 流量，并在 iSCSI 应用程序 TLV 中通告优先级 6。

## 1. DCBX 配置 (全局)

在交换机上全局配置 DCBX，以使用 PFC、ETS 和 iSCSI 配置来启用 DCBX TLV 消息的交换。

```
OS10# configure terminal
OS10(config)# dcbx enable
```

## 2. PFC 配置 (全局)

在具有 dot1p 4、5、6 和 7 流量的流量类别上已启用 PFC。所有流量类别均使用默认 PFC 暂停共享缓冲区大小的设置，以及在网络 qos 策略映射中的入口队列处理中暂停帧。trust-map dot1p default 接收 (信任) 所有 dot1p 入口流量。

```
OS10(config)# class-map type network-qos test4
OS10(config-cmap-nqos)# match qos-group 4
OS10(config-cmap-nqos)# exit
OS10(config)# class-map type network-qos test5
OS10(config-cmap-nqos)# match qos-group 5
OS10(config-cmap-nqos)# exit
OS10(config)# class-map type network-qos test6
OS10(config-cmap-nqos)# match qos-group 6
OS10(config-cmap-nqos)# exit
OS10(config)# class-map type network-qos test7
OS10(config-cmap-nqos)# match qos-group 7
OS10(config-cmap-nqos)# exit

OS10(config)# policy-map type network-qos test
OS10(config-pmap-network-qos)# class test4
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 4
OS10(config-pmap-c-nqos)# exit
OS10(config-pmap-network-qos)# class test5
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 5
OS10(config-pmap-c-nqos)# exit
OS10(config-pmap-network-qos)# class test6
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 6
OS10(config-pmap-c-nqos)# exit
OS10(config-pmap-network-qos)# class test7
OS10(config-pmap-c-nqos)# pause
OS10(config-pmap-c-nqos)# pfc-cos 7
OS10(config-pmap-c-nqos)# exit
OS10(config-pmap-network-qos)# exit

OS10(config)# system qos
OS10(config-sys-qos)# trust-map dscp default
```

## 3. PFC 配置 (接口)

将带 dot1p 信任的服务策略和 PFC 配置应用到接口。

```
OS10(config)# interface ethernet 1/1/53
OS10(conf-if-eth1/1/53)# no shutdown
OS10(conf-if-eth1/1/53)# service-policy input type network-qos test
OS10(conf-if-eth1/1/53)# trust-map dot1p default
OS10(conf-if-eth1/1/53)# priority-flow-control mode on
OS10(conf-if-eth1/1/53)# end
```

## 4. ETS 配置 (全局)

信任 dot1p-map 将 dot1p 0、1、2 和 3 流量分配给 qos 组 0，将 dot1p 4、5、6 和 7 流量分配给 qos 组 1。qos-map traffic 类别映射将 qos 组 0 中的流量类别分配给队列 0，将 qos 组 1 流量分配给队列 1。队列策略映射将 30% 的接口带宽分配给队列 0，将 70% 的带宽分配给队列 1。

```
OS10(config)# trust dot1p-map tmap1
OS10(config-tmap-dot1p-map)# qos-group 0 dot1p 0-3
OS10(config-tmap-dot1p-map)# qos-group 1 dot1p 4-7
OS10(config-tmap-dot1p-map)# exit

OS10(config)# qos-map traffic-class tmap2
```

```

OS10(config-qos-map)# queue 0 qos-group 0
OS10(config-qos-map)# queue 1 qos-group 1
OS10(config-qos-map)# exit

OS10(config)# class-map type queuing cmap1
OS10(config-cmap-queuing)# match queue 0
OS10(config-cmap-queuing)# exit
OS10(config)# class-map type queuing cmap2
OS10(config-cmap-queuing)# match queue 1
OS10(config-cmap-queuing)# exit

OS10(config)# policy-map type queuing pmap1
OS10(config-pmap-queuing)# class cmap1
OS10(config-pmap-c-que)# bandwidth percent 30
OS10(config-pmap-c-que)# exit
OS10(config-pmap-queuing)# class cmap2
OS10(config-pmap-c-que)# bandwidth percent 70
OS10(config-pmap-c-que)# end

OS10(config)# system qos
OS10(config-sys-qos)# trust-map dot1p default

```

## 5. ETS 配置 (接口和全局)

将服务策略与 dot1p 信任和 ETS 配置应用到接口或所有交换机接口上。交换机上只支持一个 qos-map traffic-class 映射。

```

OS10(config)# interface ethernet 1/1/53
OS10(conf-if-eth1/1/53)# trust-map dot1p tmap1
OS10(conf-if-eth1/1/53)# qos-map traffic-class tmap2
OS10(conf-if-eth1/1/53)# trust-map dot1p default
OS10(conf-if-eth1/1/53)# service-policy output type queuing pmap1
OS10(conf-if-eth1/1/53)# ets mode on
OS10(conf-if-eth1/1/53)# end

```

```

OS10(config)# system qos
OS10(config-sys-qos)# trust-map dot1p tmap1
OS10(config-sys-qos)# qos-map traffic-class tmap2
OS10(config-sys-qos)# trust-map dot1p default
OS10(config-sys-qos)# service-policy output type queuing pmap1
OS10(config-sys-qos)# ets mode on

```

## 6. 验证 DCB 配置

```

OS10(conf-if-eth1/1/53)# show configuration
!
interface ethernet1/1/53
 switchport access vlan 1
 no shutdown
 service-policy input type network-qos test
 trust-map dot1p default
 service-policy output type queuing pmap1
 ets mode on
 qos-map traffic-class tmap2
 trust-map dot1p tmap1
 priority-flow-control mode on

```

## 7. 验证 DCBX 运行状态

```

OS10(conf-if-eth1/1/53)# do show lldp dcbx interface ethernet 1/1/53
E-ETS Configuration TLV enabled e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled i-Application Priority for iSCSI disabled

Interface ethernet1/1/53
Port Role is Manual
DCBX Operational Status is Enabled
Is Configuration Source? FALSE

```

```

Local DCBX Compatibility mode is IEEEv2.5
Local DCBX Configured mode is AUTO
Peer Operating version is IEEEv2.5
Local DCBX TLVs Transmitted: ERPfI
4 Input PFC TLV pkts, 3 Output PFC TLV pkts, 0 Error PFC pkts
2 Input ETS Conf TLV Pkts, 27 Output ETS Conf TLV Pkts, 0 Error ETS Conf TLV Pkts
2 Input ETS Reco TLV pkts, 27 Output ETS Reco TLV pkts, 0 Error ETS Reco TLV Pkts

Total DCBX Frames transmitted 0
Total DCBX Frames received 0
Total DCBX Frame errors 0
Total DCBX Frames unrecognized 0

```

## 8. 验证 PFC 配置和操作

```

OS10(conf-if-eth1/1/53)# do show lldp dcbx interface ethernet 1/1/53 pfc detail

Interface ethernet1/1/53
Admin mode is on
Admin is enabled, Priority list is 4,5,6,7
Remote is enabled, Priority list is 4,5,6,7
Remote Willing Status is disabled
Local is enabled, Priority list is 4,5,6,7
Oper status is init
PFC DCBX Oper status is Up
State Machine Type is Symmetric
PFC TLV Tx Status is enabled
Application Priority TLV Parameters :

ISCSI TLV Tx Status is enabled
Local ISCSI PriorityMap is 0x10
Remote ISCSI PriorityMap is 0x10

4 Input TLV pkts, 3 Output TLV pkts, 0 Error pkts
4 Input Appln Priority TLV pkts, 3 Output Appln Priority TLV pkts,
0 Error Appln Priority TLV Pkts

```

## 9. 验证 ETS 配置和操作

```

OS10(conf-if-eth1/1/53)# do show lldp dcbx interface ethernet 1/1/53 ets detail

Interface ethernet1/1/53
Max Supported PG is 8
Number of Traffic Classes is 8
Admin mode is on

Admin Parameters :

Admin is enabled

PG-grp Priority# Bandwidth TSA

0 0,1,2,3, 30% ETS
1 4,5,6,7 70% ETS
2 0% ETS
3 0% ETS
4 0% ETS
5 0% ETS
6 0% ETS
7 0% ETS

Remote Parameters :

Remote is enabled
PG-grp Priority# Bandwidth TSA

0 0,1,2,3, 30% ETS
1 4,5,6,7 70% ETS
2 0% SP
3 0% SP
4 0% SP
5 0% SP

```



```

6 0% SP
7 0% SP

Remote Willing Status is disabled
Local Parameters :

Local is enabled

PG-grp Priority# Bandwidth TSA

0 0,1,2,3, 30% ETS
1 4,5,6,7 70% ETS
2 0% ETS
3 0% ETS
4 0% ETS
5 0% ETS
6 0% ETS
7 0% ETS

Oper status is init
ETS DCBX Oper status is Up
State Machine Type is Asymmetric
Conf TLV Tx Status is enabled
Reco TLV Tx Status is enabled

2 Input Conf TLV Pkts, 27 Output Conf TLV Pkts, 0 Error Conf TLV Pkts
2 Input Reco TLV Pkts, 27 Output Reco TLV Pkts, 0 Error Reco TLV Pkts

```

## 10. iSCSI 优化配置 (全局)

本示例接受在受监控的 iSCSI 会话中使用老化时间和 TCP 端口的默认设置。Compellent 存储阵列连接到该端口。策略 iSCSI 策略映射设置会在交换机上全局设置用于 iSCSI 流量的 6 CoS dot1p 优先级。默认情况下，iSCSI 流量使用优先级 4。`iscsi priority-bits 0x40` 命令可将应用程序 TLV 中 iSCSI 流量使用的通告 dot1p 优先级设置为 6。0x40 二进制 0 1 0 0 0 0 0 0。

```

OS10(conf-if-eth1/1/53)# iscsi profile-storage compellent
OS10(conf-if-eth1/1/53)# lldp tlv-select dcbxp-appln iscsi
OS10(conf-if-eth1/1/53)# exit

OS10(config)# iscsi target port 3261 ip-address 10.1.1.1
OS10(config)# policy-map type application policy-iscsi
OS10(config-pmap-application)# class class-iscsi
OS10(config-pmap-c-app)# set qos-group 6
OS10(config-pmap-c-app)# set cos 6
OS10(config-pmap-c-app)# exit
OS10(config-pmap-application)# exit

OS10(config)# system qos
OS10(config-sys-qos)# service-policy type application policy-iscsi
OS10(config-sys-qos)# exit

OS10(config)# iscsi session-monitoring enable
OS10(config)# iscsi priority-bits 0x40
OS10(config)# iscsi enable

```

## 11. 验证 iSCSI 优化 (全局)

启用 iSCSI 优化后，将在 `show` 命令输出中添加 iSCSI 应用程序优先级 TLV 参数，以验证 PFC 配置。

```

OS10(conf-if-eth1/1/53)# do show lldp dcbx interface ethernet 1/1/53 pfc detail

Interface ethernet1/1/53
 Admin mode is on
 Admin is enabled, Priority list is 4,5,6,7
 Remote is enabled, Priority list is 4,5,6,7
 Remote Willing Status is disabled
 Local is enabled, Priority list is 4,5,6,7
 Oper status is init
 PFC DCBX Oper status is Up
 State Machine Type is Symmetric
 PFC TLV Tx Status is enabled
 Application Priority TLV Parameters :

```

```

ISCSI TLV Tx Status is enabled
Local ISCSI PriorityMap is 0x40
Remote ISCSI PriorityMap is 0x10

4 Input TLV pkts, 3 Output TLV pkts, 0 Error pkts
4 Input Appln Priority TLV pkts, 3 Output Appln Priority TLV pkts, 0 Error Appln
Priority TLV Pkts

```

## 12. DCBX 配置 (接口)

本示例显示如何配置和验证不同的 DCBX 版本。

```

OS10(conf-if-eth1/1/53)# dcbx version cee
OS10(conf-if-eth1/1/53)# show configuration
!
interface ethernet1/1/53
 switchport access vlan 1
 no shutdown
 dcbx version cee
 service-policy input type network-qos test
 trust-map dot1p default
 service-policy output type queuing pmap1
 ets mode on
 qos-map traffic-class tmap2
 trust-map dot1p tmap1
 priority-flow-control mode on

OS10(conf-if-eth1/1/53)# do show lldp dcbx interface ethernet 1/1/53
E-ETS Configuration TLV enabled e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled i-Application Priority for iSCSI disabled

Interface ethernet1/1/53
Port Role is Manual
DCBX Operational Status is Enabled
Is Configuration Source? FALSE
Local DCBX Compatibility mode is CEE
Local DCBX Configured mode is CEE
Peer Operating version is CEE
Local DCBX TLVs Transmitted: ErPfi

Local DCBX Status

DCBX Operational Version is 0
DCBX Max Version Supported is 0
Sequence Number: 2
Acknowledgment Number: 1
Protocol State: In-Sync

Peer DCBX Status

DCBX Operational Version is 0
DCBX Max Version Supported is 0
Sequence Number: 1
Acknowledgment Number: 2
3 Input PFC TLV pkts, 3 Output PFC TLV pkts, 0 Error PFC pkts
3 Input PG TLV Pkts, 3 Output PG TLV Pkts, 0 Error PG TLV Pkts
3 Input Appln Priority TLV pkts, 3 Output Appln Priority TLV pkts,
0 Error Appln Priority TLV Pkts

Total DCBX Frames transmitted 3
Total DCBX Frames received 3
Total DCBX Frame errors 0
Total DCBX Frames unrecognized

```

```

OS10(conf-if-eth1/1/53)# dcbx version cee
OS10(conf-if-eth1/1/53)# show configuration
!
interface ethernet1/1/53
 switchport access vlan 1
 no shutdown
 dcbx version ieee
 service-policy input type network-qos test
 trust-map dot1p default
 service-policy output type queuing pmap1
 ets mode on
 qos-map traffic-class tmap2
 trust-map dot1p tmap1
 priority-flow-control mode on

OS10(conf-if-eth1/1/53)# do show lldp dcbx interface ethernet 1/1/53
E-ETS Configuration TLV enabled e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled i-Application Priority for iSCSI disabled

Interface ethernet1/1/53
 Port Role is Manual
 DCBX Operational Status is Enabled
 Is Configuration Source? FALSE
 Local DCBX Compatibility mode is IEEEv2.5
 Local DCBX Configured mode is IEEEv2.5
 Peer Operating version is IEEEv2.5
 Local DCBX TLVs Transmitted: ERPfI
 13 Input PFC TLV pkts, 4 Output PFC TLV pkts, 0 Error PFC pkts
 3 Input ETS Conf TLV Pkts, 26 Output ETS Conf TLV Pkts, 0 Error ETS Conf TLV Pkts
 3 Input ETS Reco TLV pkts, 26 Output ETS Reco TLV pkts, 0 Error ETS Reco TLV Pkts

Total DCBX Frames transmitted 0
Total DCBX Frames received 0
Total DCBX Frame errors 0
Total DCBX Frames unrecognized 0

```

sFlow 是一种基于标准的采样技术，嵌入在用于监控网络流量的交换机和路由器中。它为具有多个交换机和路由器的高速网络提供流量监控。

- OS10 支持 sFlow 版本 5
- 只有数据端口支持 sFlow 收集器
- OS10 最多支持两个 sFlow 收集器
- OS10 不支持 SNMP、VLAN、隧道接口、扩展的 sFlow、回退机制和出口采样上的 sFlow

sFlow 使用两种类型的采样：

- 交换或路由数据包流的基于数据包的统计采样
- 接口计数器的基于时间的采样

**注：**在 S4248FB-ON 和 S4248FBL-ON 平台上，根据已启用 sFlow 的所有端口中的累积数据包计数来执行采样。

sFlow 监控由嵌入在设备和 sFlow 收集器中的 sFlow 代理组成：

- SFlow 代理驻留在数据包路径中的任意位置。代理将流量样本和接口计数器合并为 sFlow 数据报，并定期将它们转发到 sFlow 收集器。数据报包含有关的信息，但不限于数据包包头、入口和出口接口、采样参数和接口计数器。特定于应用程序的集成电路 (ASIC) 处理数据包采样。
- SFlow 收集器分析从不同设备接收的数据报，并生成流量流的网络范围视图。

## 启用 sFlow

您可以在所有接口上全局启用 sFlow 或在一组特定的接口上启用 sFlow。如果您尝试同时在这两种模式上启用 sFlow，系统将显示一条错误消息。

如果仅在一组接口上配置 sFlow，则对已启用 sFlow 的端口的任何进一步更改都会触发 sFlow 代理重新启动。这会导致轮询计数器统计信息的间隔时间为 30 秒，并且在所有已启用 sFlow 的端口上重置 sFlow 计数器。

在端口通道上启用 sFlow 时：

- 在基于接口模式下，当您添加新成员端口或从任何已启用 sFlow 的端口通道组移除现有成员端口时，已启用 sFlow 的端口的计数器统计信息将重置为零。
- 为端口通道数据源的端口成员单独报告的 sFlow 计数器统计信息是准确的。为端口通道报告的计数器统计信息可能不准确。要计算端口通道数据源的正确计数器，请将单个端口成员的计数器统计信息相加。

### 全局启用或禁用 sFlow

默认情况下，sFlow 处于全局禁用状态。

- 在 CONFIGURATION 模式下全局启用所有接口上的 sFlow。

```
sflow enable all-interfaces
```

- 在 CONFIGURATION 模式下禁用 sFlow。

```
no sflow
```

### 在特定接口上启用或禁用 sFlow

- 在 CONFIGURATION 模式下启用 sFlow。

```
sflow enable
```

- 在 CONFIGURATION 模式下禁用 sFlow。

```
no sflow enable
```

### 在特定接口上启用 sFlow

```
OS10(config)# sflow enable
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# sflow enable
```

### 在一系列接口上启用 sFlow

```
OS10(config)# sflow enable
OS10(config)# interface range ethernet 1/1/1-1/1/10
OS10(conf-range-eth1/1/1-1/1/10)# sflow enable
```

### 在端口通道上启用 sFlow

```
OS10(config)# sflow enable
OS10(config)# interface range port-channel 1-10
OS10(conf-range-po-1-10)# sflow enable
```

## 最大标头大小配置

- 在 CONFIGURATION 模式下将数据包的最大大小设置为 64 至 256。默认值为 128 字节。

```
max-header-size header-size
```

- 在 CONFIGURATION 模式下禁用标头大小。

```
no sflow max-header-size
```

- 在 EXEC 模式下查看最大数据包标头大小。

```
show sflow
```

### 配置 sFlow 最大标头大小

```
OS10(config)# sflow max-header-size 80
```

### 查看 sFlow 信息

```
OS10# show sflow
sFlow services are enabled
Management Interface sFlow services are disabled
Global default sampling rate: 32768
Global default counter polling interval: 20
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
1 collector(s) configured
Collector IP addr:10.16.151.245 Agent IP addr:10.16.132.181 UDP port:6343 VRF:Default
31722 UDP packets exported
0 UDP packets dropped
34026 sFlow samples collected
```

### 查看 sFlow 运行的配置

```
OS10# show running-configuration sflow
sflow enable
sflow max-header-size 80
sflow polling-interval 30
sflow sample-rate 4096
sflow collector 10.16.150.1 agent-addr 10.16.132.67 6767 max-datagram-size 800
sflow collector 10.16.153.176 agent-addr 3.3.3.3 6666
!
interface ethernet1/1/1
sflow enable
!
```

# 收集器配置

配置 sFlow 收集器的 IPv4 或 IPv6 地址。配置收集器时，输入有效且可访问的 IPv4 或 IPv6 地址。您可以配置最多两个 sFlow 收集器。如果指定两个收集器，则示例将同时发送到。两个收集器的代理 IP 地址必须相同。

## 默认 VRF 的收集器配置

- 在配置模式中输入 sFlow 收集器的 IPv4 或 IPv6 地址、IPv4 或 IPv6 地址、UDP 收集器端口号和最大数据报大小。

```
sflow collector {ip-address | ipv6-address} agent-addr {ip-address | ipv6-address}
[collector-port-number] [max-datagram-size datagram-size-number]
```

命令的 `no` 形式在 CONFIGURATION 模式下禁用 sFlow 收集器。

## 非默认 VRF 的收集器配置

如果为非默认 VRF 配置收集器，请先创建 VRF。如果未指定 VRF 实例，系统将为默认 VRF 实例配置收集器。

以下是使用非默认 VRF 配置 sFlow 收集器的步骤：

1. 创建非默认 VRF 实例。

```
OS10(config)# ip vrf RED
```

2. 启用 sFlow 功能。

```
OS10(config)# sflow enable
```

3. 将 IP 地址分配给可用作 sFlow 代理的接口，并将其添加到 VRF 实例中。

```
OS10(conf-if-eth1/1/1)# sflow enable
OS10(conf-if-eth1/1/1)# ip vrf forwarding RED
OS10(conf-if-eth1/1/1)# ip address 1.1.1.1/24
OS10(conf-if-eth1/1/1)# no shutdown
```

4. 将 IP 地址分配给可访问 sFlow 收集器并将其添加到 VRF 实例的接口。

```
OS10(conf-if-eth1/1/1)# interface ethernet 1/1/2
OS10(conf-if-eth1/1/2)# sflow enable
OS10(conf-if-eth1/1/2)# ip vrf forwarding RED
OS10(conf-if-eth1/1/2)# ip address 4.4.4.4/24
OS10(conf-if-eth1/1/2)# no shutdown
```

5. 输入 sFlow 收集器和代理的 IP 地址，并将其分配给 VRF 实例。

```
OS10(config)# sflow collector 4.4.4.1 agent-addr 1.1.1.1 vrf RED
```

### 查看 sFlow 信息

```
OS10# show sflow
sFlow services are enabled
Management Interface sFlow services are disabled
Global default sampling rate: 32768
Global default counter polling interval: 10
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
1 collector(s) configured
Collector IP addr:4.4.4.1 Agent IP addr:1.1.1.1 UDP port:6343 VRF:RED
0 UDP packets exported
0 UDP packets dropped
0 sFlow samples collected
```

# 轮询间隔配置

接口的轮询间隔是发送至收集器的计数器连续样本之间的秒数。您可以配置轮询接口统计信息的持续时间。除非有特定部署需要配置较低轮询间隔值，否则将轮询间隔配置为最大值。

- 在 CONFIGURATION 模式下将默认计数器轮询间隔从 10 更改为 300。默认值为 20。

```
sflow polling-interval interval-size
```

- 在 CONFIGURATION 模式下禁用轮询间隔。

```
no sflow polling-interval
```

- 以 EXEC 模式查看轮询间隔。

```
show sflow
```

## 配置 sFlow 轮询间隔

```
OS10(config)# sflow polling-interval 200
```

## 查看 sFlow 信息

```
OS10# show sflow
sFlow services are enabled
Management Interface sFlow services are disabled
Global default sampling rate: 32768
Global default counter polling interval: 200
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
1 collector(s) configured
Collector IP addr:10.16.151.245 Agent IP addr:10.16.132.181 UDP port:6343 VRF:Default
31722 UDP packets exported
0 UDP packets dropped
34026 sFlow samples collected
```

## 查看 sFlow 运行的配置

```
OS10# show running-configuration sflow
sflow enable
sflow max-header-size 80
sflow polling-interval 200
sflow sample-rate 4096
sflow collector 10.16.150.1 agent-addr 10.16.132.67 6767 max-datagram-size 800
sflow collector 10.16.153.176 agent-addr 3.3.3.3 6666
!
interface ethernet1/1/1
sflow enable
!
```

# 采样率配置

采样率是指在采集样本之前跳过的数据包数。如果采样率为 4096，则会为观察到的 4096 个数据包各生成一个样本。

- 在 CONFIGURATION 模式下设置采样率，从 4096 到 65535。默认值为 32768。

```
sflow sample-rate sampling-size
```

- 在 CONFIGURATION 模式下禁用数据包采样。

```
no sflow sample-rate
```

- 以 EXEC 模式查看采样率。

```
show sflow
```

## 配置 sFlow 采样率

```
OS10(config)# sflow sample-rate 4096
```

## 查看 sFlow 数据包标头大小

```
OS10# show sflow
sFlow services are enabled
Management Interface sFlow services are disabled
Global default sampling rate: 4096
Global default counter polling interval: 20
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
1 collector(s) configured
Collector IP addr:10.16.151.245 Agent IP addr:10.16.132.181 UDP port:6343 VRF:Default
31722 UDP packets exported
0 UDP packets dropped
34026 sFlow samples collected
```

## 查看 sFlow 运行的配置

```
OS10# show running-configuration sflow
sflow enable
sflow max-header-size 80
sflow polling-interval 20
sflow sample-rate 4096
sflow collector 10.16.150.1 agent-addr 10.16.132.67 6767 max-datagram-size 800
sflow collector 10.16.153.176 agent-addr 3.3.3.3 6666
!
interface ethernet1/1/1
sflow enable
!
```

# 源接口配置

您可以将接口配置为 sFlow 的源。sFlow 代理使用配置的源接口的 IP 地址作为代理 IP 地址。

- 在 CONFIGURATION 模式下配置源接口。

```
sflow source-interface {ethernet node/slot/port[:subport] | loopback loopback-ID |
port-channel port-channel-ID | vlan vlan-ID}
```

- 查看接口详情。

```
show running-configuration sflow
```

```
show sflow
```

## 配置 sFlow 源接口

```
OS10(config)# sflow source-interface ethernet 1/1/1
OS10(config)# sflow source-interface port-channel 1
OS10(config)# sflow source-interface loopback 1
OS10(config)# sflow source-interface vlan 10
```

## 查看 sFlow 运行的配置

```
OS10# show running-configuration sflow
sflow enable all-interfaces
sflow source-interface vlan10
sflow collector 5.1.1.1 agent-addr 4.1.1.1 6343
sflow collector 6.1.1.1 agent-addr 4.1.1.1 6343
```



```
OS10(config)#show running-configuration interface vlan
!
interface vlan1
no shutdown
!
interface vlan10
no shutdown
ip address 10.1.1.1/24
```

## 查看 sFlow 详情

```
OS10# show sflow
sFlow services are enabled
Management Interface sFlow services are disabled
Global default sampling rate: 32768
Global default counter polling interval: 30
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
2 collector(s) configured
Collector IP addr:5.1.1.1 Agent IP addr:10.1.1.1 UDP port:6343 VRF:Default → It shows
active agent-ip
Collector IP addr:6.1.1.1 Agent IP addr:10.1.1.1 UDP port:6343 VRF:Default → It shows
active agent-ip
2 UDP packets exported
0 UDP packets dropped
2 sFlow samples collected
```

## 查看 sFlow 信息

OS10 不支持丢弃的 UDP 数据包和从硬件收到的样本的统计信息。

- 以 EXEC 模式查看 sFlow 配置详细信息和统计信息。

```
OS10# show sflow
sFlow services are enabled
Management Interface sFlow services are disabled
Global default sampling rate: 32768
Global default counter polling interval: 30
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
1 collector(s) configured
Collector IP addr:10.16.151.245 Agent IP addr:10.16.132.181 UDP port:6343 VRF:Default
31722 UDP packets exported
0 UDP packets dropped
34026 sFlow samples collected
```

- 在 EXEC 模式下查看特定接口上的 sFlow 配置详细信息。

```
OS10# show sflow interface port-channel 1
port-channel1
sFlow is enabled on port-channel1
Samples rcvd from h/w: 0
```

- 在 EXEC 模式下查看 sFlow 运行配置。

```
OS10# show running-configuration sflow
sflow enable
sflow max-header-size 80
sflow polling-interval 30
sflow sample-rate 4096
sflow collector 10.16.150.1 agent-addr 10.16.132.67 6767 max-datagram-size 800
sflow collector 10.16.153.176 agent-addr 3.3.3.3 6666
!
interface ethernet1/1/1
sflow enable
!
```

# sFlow 命令

## sflow collector

配置将 sFlow 数据报转发到的 sFlow 收集器 IP 地址。您可以配置最多两个收集器。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>sflow collector {ipv4-address   ipv6-address} agent-addr {ipv4-address   ipv6-address} [collector-port-number] [max-datagram-size datagram-size-number] [vrf vrf-name]</code>                                                                                                                                                                                                                                                                                                                                                                                |
| 参数     | <ul style="list-style-type: none"><li>• <code>ipv4-address   ipv6-address</code> — 输入 IPv4 或 IPv6 地址，采用 A.B.C.D/A::B 格式。</li><li>• <code>agent-addr ipv4-address   ipv6-address</code> — 输入 sFlow 代理 IP 地址。如果配置两个收集器，则两个收集器的代理 IP 地址必须相同。</li><li>• <code>collector-port-number</code> — (可选) 输入 UDP 端口号，从 1 到 65535。默认值为 6343。</li><li>• <code>max-datagram-size datagram-size-number</code> — (可选) 输入 max-datagram-size 和大数字 (以字节为单位)，从 400 到 1500。默认值为 1400。</li><li>• <code>vrf</code> — (可选) 输入 VRF 实例以将 VRF 上下文设置为收集器 IP 地址。如果未指定 VRF，系统将使用默认 VRF。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 使用情况信息 | <p>您必须输入有效且可访问的 IPv4 或 IPv6 地址。如果配置两个收集器，流量样本将同时发送至两者。SFlow 代理地址是用于将代理标识到收集器的 IPv4 或 IPv6 地址。此命令的 <code>no</code> 版本将移除已配置的 sFlow 收集器。</p> <p>如果指定非默认 VRF，请先创建 VRF。</p>                                                                                                                                                                                                                                                                                                                                                                                            |

### 示例

```
OS10(config)# sflow collector 10.1.1.1 agent-addr 2.2.2.2 6343 max-datagram-size 1500 vrf default
```

```
OS10(config)# sflow collector 10.1.1.1 agent-addr 2.2.2.2 6343 max-datagram-size 1500 vrf vrf-core
```

**支持的版本** 10.3.0E or later。在 OS10 版本 10.4.3.0 or later 上更新了命令以指定非默认 VRF

## sflow enable

在特定接口上或在所有接口上全局启用 sFlow。

|        |                                                   |
|--------|---------------------------------------------------|
| 语法     | <code>sflow enable [all-interfaces]</code>        |
| 参数     | <code>all-interfaces</code> — (可选) 输入以全局启用 sFlow。 |
| 默认     | 已禁用                                               |
| 命令模式   | CONFIGURATION                                     |
| 使用情况信息 | 此命令的 <code>no</code> 版本可禁用 sFlow。                 |

### 示例 (接口)

```
OS10(config)# sflow enable
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# sflow enable
```

### 示例 (接口范围)

```
OS10(config)# sflow enable
OS10(config)# interface range ethernet 1/1/1-1/1/10
OS10(config-range-eth1/1/1-1/1/10)# sflow enable
```

### 示例（端口通道）

```
OS10(config)# sflow enable
OS10(config)# interface range port-channel 1-10
OS10(config-range-po-1-10)# sflow enable
```

**支持的版本** 10.3.0E or later

## sflow max-header-size

设置数据包的最大标头大小。

**语法** `sflow max-header-size header-size`

**参数** `header-size` — 输入从 64 到 256 的标头大小（以字节为单位）。默认值为 128。

**默认** 128 字节

**命令模式** CONFIGURATION

**使用情况信息** 使用命令的 `no` 版本将标头大小重置为默认值。

**示例**

```
OS10(config)# sflow max-header-size 256
```

**支持的版本** 10.3.0E or later

## sflow polling-interval

设置 sFlow 轮询间隔。

**语法** `sflow polling-interval interval-value`

**参数** `interval-value` — 在各部分输入间隔值，从 10 到 300。默认值为 30。

**默认** 30

**命令模式** CONFIGURATION

**使用情况信息** 接口的轮询间隔是发送至收集器的计数器连续样本之间的秒数。您可以配置轮询接口统计信息的持续时间。命令的 `no` 版本将间隔时间重置为默认值。

**示例**

```
OS10(config)# sflow polling-interval 200
```

**支持的版本** 10.3.0E or later

## sflow sample-rate

配置采样率。

**语法** `sflow sample-rate value`

**参数** `value` — 输入数据包采样率，从 4096 到 65535。默认值为 32768。

**默认** 32768

**命令模式** CONFIGURATION

**使用情况信息** 采样率是指在采集样本之前跳过的数据包数。例如，如果采样率为 4096，则会为观察到的 4096 个数据包各生成一个样本。命令的 `no` 版本会将采样率重置为默认值。

**示例**

```
OS10(config)# sflow sample-rate 4096
```

**支持的版本** 10.3.0E or later

## sflow source-interface

配置作为 sFlow 源的接口。SFlow 代理使用配置的源接口的 IP 地址作为代理 IP 地址。

|           |                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法        | <code>sflow source-interface {ethernet <i>node/slot/port[:subport]</i>   loopback <i>loopback-ID</i>   port-channel <i>port-channel-ID</i>   vlan <i>vlan-ID</i>}</code>                                                                                                                                                                                                                       |
| 参数        | <ul style="list-style-type: none"><li>• <code>ethernet <i>node/slot/port[:subport]</i></code>— 输入物理接口类型的详细信息。</li><li>• <code>loopback <i>loopback-ID</i></code>— 输入环回接口的详细信息。环回 ID 的范围从 0 到 16383。</li><li>• <code>port-channel <i>port-channel-ID</i></code>— 输入端口通道的详细信息。端口通道 ID 的范围从 1 到 128。</li><li>• <code>vlan <i>vlan-ID</i></code>— 输入 VLAN 的详细信息。VLAN ID 编号的范围从 1 到 4093。</li></ul> |
| 默认        | 已禁用                                                                                                                                                                                                                                                                                                                                                                                            |
| 命令模式      | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                  |
| 使用情况信息    | 此命令的 <code>no</code> 版本会从接口中删除配置。                                                                                                                                                                                                                                                                                                                                                              |
| 示例 (以太网)  | <pre>OS10(config)# sflow source-interface ethernet 1/1/1</pre>                                                                                                                                                                                                                                                                                                                                 |
| 示例 (环回)   | <pre>OS10(config)# sflow source-interface loopback 1</pre>                                                                                                                                                                                                                                                                                                                                     |
| 示例 (端口通道) | <pre>OS10(config)# sflow source-interface port-channel 1</pre>                                                                                                                                                                                                                                                                                                                                 |
| 示例 (VLAN) | <pre>OS10(config)# sflow source-interface vlan 10</pre>                                                                                                                                                                                                                                                                                                                                        |
| 支持的版本     | 10.4.1.0 or later                                                                                                                                                                                                                                                                                                                                                                              |

## show sflow

显示所有接口或特定接口类型的当前 sFlow 配置。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show sflow [interface type]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 参数     | <code>interface type</code> — (可选) 输入 <code>ethernet</code> 或 <code>port-channel</code> 用于接口类型。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 使用情况信息 | OS10 不支持丢弃的 UDP 数据包和从硬件收到的样本的统计信息。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 示例     | <pre>OS10# show sflow sFlow services are enabled Management Interface sFlow services are disabled Global default sampling rate: 32768 Global default counter polling interval: 30 Global default extended maximum header size: 128 bytes Global extended information enabled: none 1 collector(s) configured Collector IP addr:10.16.151.245 Agent IP addr:10.16.132.181 UDP port:6343 VRF:Default 31722 UDP packets exported 0 UDP packets dropped 34026 sFlow samples collected</pre> <pre>OS10# show sflow sFlow services are enabled Management Interface sFlow services are disabled Global default sampling rate: 32768 Global default counter polling interval: 30 Global default extended maximum header size: 128 bytes Global extended information enabled: none</pre> |

```
1 collector(s) configured
Collector IP addr:10.16.151.145 Agent IP addr:10.16.132.160 UDP
port:6343 VRF:RED
0 UDP packets exported
0 UDP packets dropped
0 sFlow samples collected
```

#### 示例（端口通道）

```
OS10# show sflow interface port-channel 1
port-channell
sFlow is enabled on port-channell
Samples rcvd from h/w: 0
```

#### 支持的版本

10.3.0E or later

## 遥测

网络运行状况依赖于性能监控和数据收集进行分析和故障处理。网络数据通常使用提取模式收集 SNMP 和 CLI 命令。在提取模式中，管理设备发送 `get` 请求并从客户端提取数据。随着网络对象数量和指标的增长，传统方法将限制网络规模和效率。使用多个管理系统进一步限制网络扩展。提取模式通过收集所有数据来增加交换机上的处理负载，即使没有发生更改也是如此。

流式遥测提供了一种备选方法，其中数据通过高效的增量更新从网络设备连续传输。操作员使用定义明确的传感器标识符订阅所需的特定数据。

虽然 SNMP 管理系统即使未更改也对数据进行轮询，但流式遥测允许访问近实时、模型驱动和分析就绪数据。它支持更高效的网络自动化、流量优化和预防性故障处理。

例如，流式遥测会实时报告链路的数据包丢弃或高利用率。网络自动化应用程序可以使用此信息来调配新路径并优化网络间的流量传输。数据使用 Google Protocol 缓冲器 (GPB) 进行编码，并使用 Google 协议 RPC (gRPC) 传输进行流式处理。

您可以使用 OS10 遥测将数据传输到：

- 戴尔实施的外部收集器，例如 VMware vRNI 或 Wavefront
- 您实施的专有网络收集器

## 遥测术语

|               |                                                                                                                                      |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>拔出模式</b>   | 交换机将根据订阅中的传感器路径和目标启动一个或多个设备的会话。                                                                                                      |
| <b>传感器路径</b>  | 用于收集流式遥测数据的路径。                                                                                                                       |
| <b>传感器组</b>   | 多个传感器路径和排除筛选器的可重复使用组。                                                                                                                |
| <b>目标组</b>    | 要将遥测数据流式传输到的目标服务器上的 IP 地址和传输端口。您可以配置多个目标，并在订阅配置文件中重复使用目标组。                                                                           |
| <b>订阅配置文件</b> | 与传感器路径关联的数据收集器目标和流属性。订阅将传感器路径和目标组与传输协议、编码格式和流式间隔结合使用。<br>交换机中的遥测代理尝试与订阅配置文件中的每个收集器建立会话，并将数据传输到收集器。如果收集器不可访问，则遥测代理会持续尝试以一分钟的时间间隔建立连接。 |

## YANG 塑形的遥测数据

本部分介绍可以通过建议的最小采样间隔将遥测数据流式传输到目标的 YANG 容器。

## BGP

表. 96: BGP

| YANG 容器                       | 最小采样间隔 (毫秒) |
|-------------------------------|-------------|
| bgp/bgp-oper/bgpPeerCount     | 15000       |
| bgp/bgp-oper/bgpPrfxCntsEntry | 15000       |

## BGP 对等

表. 97: BGP 对等

| YANG 容器                          | 最小采样间隔 (毫秒) |
|----------------------------------|-------------|
| infra-bgp/peer-state/peer-status | 0           |

## 缓冲区统计信息

表. 98: 缓冲区统计信息

| YANG 容器                      | 最小采样间隔 (毫秒) |
|------------------------------|-------------|
| base-qos/queue-stat          | 15000       |
| base-qos/priority-group-stat | 15000       |
| base-qos/buffer-pool-stat    | 15000       |
| base-qos/buffer-pool         | 15000       |

## 设备信息

表. 99: 设备信息

| YANG 容器                                     | 最小采样间隔 (毫秒) |
|---------------------------------------------|-------------|
| base-pas/chassis                            | 15000       |
| base-pas/card                               | 15000       |
| base-switch/switching-entities/switch-stats | 15000       |

## 环境统计信息

表. 100: 环境统计信息

| YANG 容器                 | 最小采样间隔 (毫秒) |
|-------------------------|-------------|
| base-pas/entity         | 15000       |
| base-pas/psu            | 15000       |
| base-pas/fan-try        | 15000       |
| base-pas/fan            | 15000       |
| base-pas/led            | 15000       |
| base-pas/temperature    | 15000       |
| base-pas/temp_threshold | 15000       |
| base-pas/media          | 15000       |
| base-pas/media-channel  | 15000       |

## 接口统计信息

表. 101: 接口统计信息

| YANG 容器                                        | 最小采样间隔 (毫秒) |
|------------------------------------------------|-------------|
| if/interfaces-state/interface/statistics       | 15000       |
| dell-base-if-cmn/if/interfaces-state/interface | 15000       |

## 端口通道 (lag) 成员端口

表. 102: 端口通道 (lag) 成员端口

| YANG 容器                        | 最小采样间隔 (毫秒) |
|--------------------------------|-------------|
| dell-base-if-cmn/if/interfaces | 0           |

## 系统统计信息

表. 103: 系统统计信息

| YANG 容器                      | 最小采样间隔 (毫秒) |
|------------------------------|-------------|
| system-status/current-status | 15000       |

# 配置遥测

**注:** 要配置流式遥测收集器，从 Dell EMC 支持站点下载并使用 OS10 遥测 .proto 文件。

要启用将遥测数据流式传输到订阅配置文件中的目标，请执行以下操作：

- 1. 在交换机上启用遥测。
  - 2. 配置目标组。
  - 3. 通过关联一个或多个目标组和预配置的传感器组来配置订阅配置文件。
- 完成步骤 3 后，遥测代理会开始将数据传输到目标设备。

## 配置说明

- 遥测代理从 OS10 应用程序和交换机硬件收集数据。当您配置的采样速率为 0 时，如果接近实时，遥测会在发生事件时立即收集数据。如果配置采样率，遥测将执行定期数据收集。在配置传感器组中介绍了建议的最小采样间隔。
- OS10 遥测支持：
  - 只有一个配置的目标组，并且组中只有一个目标地址。
  - 仅一个订阅配置文件。

## 启用遥测

- 1. 从 CONFIGURATION 模式进入 TELEMETRY 模式。

```
OS10(config)# telemetry
```

- 2. 在 TELEMETRY 模式下启用流式遥测。

```
OS10(conf-telemetry)# enable
```

## 配置传感器组

传感器组定义收集并流传输到目标的数据。使用任何预配置的传感器组来监控系统资源。要显示每个组的传感器路径，请使用 show telemetry sensor-group 命令。

表. 104: 预配置的传感器组

| 预配置的传感器组  | 最小采样间隔（毫秒） |
|-----------|------------|
| BGP       | 15000      |
| BGP-peer  | 0          |
| 缓冲区       | 15000      |
| 设备        | 15000      |
| 环境        | 15000      |
| 接口        | 15000      |
| LAG（端口通道） | 0          |
| 系统        | 15000      |

## 配置目标组

目标组定义将流式遥测数据发送到的目标服务器。

- 1. 在 TELEMETRY 模式下输入目标组名称。最多 32 个字符。

```
OS10(conf-telemetry)# destination-group group-name
```

- 2. 在 DESTINATION-GROUP 模式下输入 IPv4 或 IPv6 地址和传输服务端口号。10.4.3.0 版本中仅支持一个目标。您可以输入 ip-address 的完全限定域名 (FQDN)。目标域名解析为 IP 地址 — 请参阅[系统域名和列表](#)。

```
OS10(conf-telemetry-dg-dest)# destination ip-address port-number
```

- 3. 返回 TELEMETRY 模式。

```
OS10(conf-telemetry-dg-dest)# exit
```



## 配置订阅配置文件

订阅配置文件将目标组与传感器组关联，并指定数据编码格式和传输协议。

1. 在 TELEMETRY 模式下输入订阅配置文件名称。最多 32 个字符。

```
OS10(conf-telemetry)# subscription-profile profile-name
```

2. 在 SUBSCRIPTION-PROFILE 模式下输入预配置的传感器组的名称和采样间隔。有效的传感器组名称为：bgp、bgp-peer、buffer、device、environment、interface、lag 和 system。要查看预配置的传感器组的数据内容，请使用 show telemetry sensor-group 命令。interface 传感器组仅支持物理和端口通道接口。

采样间隔（以毫秒为单位），从 0（无论何时发生事件；近时间）到 4294967295。默认值为 15000。重复此步骤以将传感器组添加到订阅配置文件。

```
OS10(conf-telemetry-sp-subscription)# sensor-group group-name sampling-interval
```

3. 在 SUBSCRIPTION-PROFILE 模式下输入目标组的名称。遥测数据将发送到目标组中指定的 IP 地址和端口。重复此步骤以将目标组添加到订阅配置文件。

```
OS10(conf-telemetry-sp-subscription)# destination-group name
```

4. 在 SUBSCRIPTION-PROFILE 模式下输入源接口。系统使用源接口派生用于与目标设备进行通信的 VRF 实例和 IP 地址。对于 gRPC 传输，源接口配置是可选的。

```
OS10(conf-telemetry-sp-subscription)# source interface
```

其中 *interface* 是以下值之一：

- ethernet *node/slot/port[:subport]* — 输入物理以太网接口。
- loopback *number* — 输入环回接口，从 0 到 16383。
- management 1/1/1 — 输入管理接口。
- port-channel *channel-id* — 输入端口通道 ID，从 1 到 28。
- vlan *vlan-id* — 输入 VLAN ID，从 1 到 4093。

5. 在 SUBSCRIPTION-PROFILE 模式下配置传输遥测数据的 gpb 编码格式。

```
OS10(conf-telemetry-sp-subscription)# encoding format
```

6. 在 SUBSCRIPTION-PROFILE 模式下配置用于将数据流式传输到目标的 gRPC 传输协议。启用传输安全层 (TLS) 证书的 gRPC 是默认传输协议。要禁用 TLS 证书交换，请使用 transport grpc no-tls 命令。

```
OS10(conf-telemetry-sp-subscription)# transport protocol [no-tls]
```

配置订阅配置文件后，遥测代理开始收集数据并将其流式传输至目标设备。

## 查看遥测配置

使用以下 show 命令显示遥测配置。

```
OS10# show telemetry

Telemetry Status : enabled

-- Telemetry Destination Groups --
Group : dest1
 Destination : 10.11.56.204 Port : 40001

-- Telemetry Sensor Groups --
Group : bgp
 Sensor Path : bgp/bgp-oper/bgpPrfxCntersEntry
 Sensor Path : bgp/bgp-oper/bgpPeerCount
Group : bgp-peer
 Sensor Path : infra-bgp/peer-state/peer-status
Group : buffer
 Sensor Path : base-qos/queue-stat
 Sensor Path : base-qos/priority-group-stat
 Sensor Path : base-qos/buffer-pool-stat
```

```

 Sensor Path : base-qos/buffer-pool
Group : device
 Sensor Path : base-pas/chassis
 Sensor Path : base-pas/card
 Sensor Path : base-switch/switching-entities/switch-stats
Group : environment
 Sensor Path : base-pas/entity
 Sensor Path : base-pas/psu
 Sensor Path : base-pas/fan-tray
 Sensor Path : base-pas/fan
 Sensor Path : base-pas/led
 Sensor Path : base-pas/temperature
 Sensor Path : base-pas/temp_threshold
 Sensor Path : base-pas/media
 Sensor Path : base-pas/media-channel
Group : interface
 Sensor Path : if/interfaces-state/interface/statistics
 Sensor Path : dell-base-if-cmn/if/interfaces-state/interface
Group : lag
 Sensor Path : dell-base-if-cmn/if/interfaces
Group : system
 Sensor Path : system-status/current-status

-- Telemetry Subscription Profiles --
Name : subscription-1

 Destination Groups(s) : dest1

 Sensor-group Sample-interval

 bgp 300000
 bgp-peer 0
 buffer 15000
 device 300000
 environment 300000
 interface 180000
 lag 0
 system 300000

 Encoding : gpb
 Transport : grpc TLS : disabled
 Source Interface : ethernet1/1/1
 Active : true
 Reason : Connection summary: One or more active connections
 The connection 10.11.56.204:40001 is in connected state

```

## 查看目标组

```

OS10# show telemetry destination-group

Telemetry Status : enabled

-- Telemetry Destination Groups --
Group : dest1
 Destination : 10.11.56.204 Port : 40001

```

## 查看传感器组

```

OS10# show telemetry sensor-group

Telemetry Status : enabled

-- Telemetry Sensor Groups --
Group : bgp
 Sensor Path : bgp/bgp-oper/bgpPrfxCntersEntry
 Sensor Path : bgp/bgp-oper/bgpPeerCount
Group : bgp-peer
 Sensor Path : infra-bgp/peer-state/peer-status
Group : buffer
 Sensor Path : base-qos/queue-stat
 Sensor Path : base-qos/priority-group-stat
 Sensor Path : base-qos/buffer-pool-stat

```

```

 Sensor Path : base-qos/buffer-pool
Group : device
 Sensor Path : base-pas/chassis
 Sensor Path : base-pas/card
 Sensor Path : base-switch/switching-entities/switch-stats
Group : environment
 Sensor Path : base-pas/entity
 Sensor Path : base-pas/psu
 Sensor Path : base-pas/fan-tray
 Sensor Path : base-pas/fan
 Sensor Path : base-pas/led
 Sensor Path : base-pas/temperature
 Sensor Path : base-pas/temp_threshold
 Sensor Path : base-pas/media
 Sensor Path : base-pas/media-channel
Group : interface
 Sensor Path : if/interfaces-state/interface/statistics
 Sensor Path : dell-base-if-cmn/if/interfaces-state/interface
Group : lag
 Sensor Path : dell-base-if-cmn/if/interfaces
Group : system
 Sensor Path : system-status/current-status

```

## 查看订阅配置文件

```

OS10# show telemetry subscription-profile

Telemetry Status : enabled

-- Telemetry Subscription Profile --

Name : subscription-1

 Destination Groups(s) : dest1

 Sensor-group Sample-interval

 bgp 300000
 bgp-peer 0
 buffer 15000
 device 300000
 environment 300000
 interface 180000
 lag 0
 system 300000

Encoding : gpb
Transport : grpc TLS : disabled
Source Interface : ethernet1/1/1
Active : true
Reason : Connection summary: One or more active connections
 The connection 10.11.56.204:40001 is in connected state

```

## 验证正在运行的配置中的遥测

```

OS10# show running-configuration telemetry
!
telemetry
enable
!
destination-group dest1
 destination 10.11.56.204 40001
!
subscription-profile subscription-1
 destination-group dest1
 sensor-group bgp 300000
 sensor-group bgp-peer 0
 sensor-group buffer 15000
 sensor-group device 300000
 sensor-group environment 300000
 sensor-group interface 180000
 sensor-group lag 0

```

```
sensor-group system 300000
encoding gpb
transport grpc no-tls
source-interface ethernet1/1/1
```

## 遥测命令

### debug telemetry

启动数据收集以处理遥测操作故障。

|        |                                                                                   |
|--------|-----------------------------------------------------------------------------------|
| 语法     | debug telemetry                                                                   |
| 参数     | 无                                                                                 |
| 默认     | 未配置                                                                               |
| 命令模式   | EXEC                                                                              |
| 使用情况信息 | 发生错误情况时，使用 debug telemetry 命令可将遥测数据存储在调试文件中。遥测调试文件存储在 /var/log/grpc_server.log 中。 |
| 示例     | <pre>OS10# debug telemetry</pre>                                                  |
| 支持的版本  | 10.4.3.0 or later                                                                 |

### destination

配置接收流式遥测的目标管理设备。

|        |                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | destination {ip-address   domain-name} port-number                                                                                                                                                                                               |
| 参数     | <ul style="list-style-type: none"><li>ip-address — 输入目标设备的 IPv4 或 IPv6 地址。您可以输入完全限定域名 (FQDN)。目标域名解析为 IP 地址 — 请参阅<a href="#">系统域名和列表</a>。</li><li>domain-name — 输入目标设备的完全限定域名。最多 32 个字符。</li><li>port-number — 输入要在目标设备上发送遥测数据的传输服务端口号。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                              |
| 命令模式   | DESTINATION-GROUP                                                                                                                                                                                                                                |
| 使用情况信息 | 将目标组与订阅关联时，遥测数据将发送到 destination 命令指定的 IP 地址和端口。在 10.4.3.0 版本中，仅支持一个目标。此命令的 no 版本将移除配置的目标。                                                                                                                                                        |
| 示例     | <pre>OS10(conf-telemetry)# destination-group dest1 OS10(conf-telemetry-dg-dest1)# destination 10.11.56.204 40001 OS10(conf-telemetry-dg-dest1)#</pre>                                                                                            |
| 支持的版本  | 10.4.3.0 or later                                                                                                                                                                                                                                |

### destination-group (subscription-profile)

将目标组分配给流式遥测的订阅配置文件。

|      |                                  |
|------|----------------------------------|
| 语法   | destination-group group-name     |
| 参数   | group-name — 输入目标组的名称。最多 32 个字符。 |
| 默认   | 未配置                              |
| 命令模式 | SUBSCRIPTION-PROFILE             |

**使用情况信息** 订阅配置文件会关联目标组和传感器组。目标组定义将流式遥测数据发送到的目标服务器。此命令的 `no` 版本将从订阅配置文件中移除已配置的组。

**示例**

```
OS10(conf-telemetry)# subscription-profile subscription-1
OS10(conf-telemetry-sp-subscription-1)# destination-group dest1
```

**支持的版本** 10.4.3.0 or later

## destination-group (telemetry)

配置流式遥测的目标组。

**语法** `destination-group group-name`

**参数** `group-name` — 输入目标组的名称。最多 32 个字符。

**默认** 未配置

**命令模式** TELEMETRY

**使用情况信息** 目标组定义将流式遥测数据发送到的目标服务器。此命令的 `no` 版本将移除已配置的组。

**示例**

```
OS10(conf-telemetry)# destination-group dest1
OS10(conf-telemetry-dg-dest1)#
```

**支持的版本** 10.4.3.0 or later

## enable

在交换机上启用遥测。

**语法** `enable`

**参数** 无

**默认** 遥测已禁用。

**命令模式** TELEMETRY

**使用情况信息** 输入 `no enable` 命令以禁用遥测。

**示例**

```
OS10(conf-telemetry)# enable
```

**支持的版本** 10.4.3.0 or later

## encoding

配置用于将流式遥测数据传输到目标设备的编码格式。

**语法** `encoding format`

**参数** `format` — 输入流式传输数据的 gpb (Google 协议缓冲区) 编码格式。

**默认** 无

**命令模式** SUBSCRIPTION-PROFILE

**使用情况信息** 命令 `no` 的版本将从订阅配置文件中移除配置的编码格式。

**示例**

```
OS10(conf-telemetry)# subscription-profile subscription-1
OS10(conf-telemetry-sp-subscription-1)# encoding gpb
```

**支持的版本** 10.4.3.0 or later

# sensor-group (subscription-profile)

将具有采样间隔的传感器组分配到流式遥测的订阅配置文件。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>sensor-group {bgp   bgp-peer   buffer   device   environment   interface   lag   system   oc-bfd} group-name sampling-interval</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 参数     | <ul style="list-style-type: none"><li><code>bgp</code> — 输入 <code>bgp</code> 以将 BGP 统计信息传感器组分配给订阅配置文件。</li><li><code>bgp-peer</code> — 输入 <code>bgp-peer</code> 以将 BGP 对等统计信息传感器组分配给订阅配置文件。</li><li><code>buffer</code> — 输入 <code>buffer</code> 以将缓冲区统计信息分配给订阅配置文件。</li><li><code>device</code> — 输入 <code>device</code> 以将设备统计信息传感器组分配给订阅配置文件。</li><li><code>environment</code> — 输入 <code>environmnet</code> 以将环境统计信息传感器组分配给订阅配置文件。</li><li><code>interface</code> — 输入 <code>interface</code> 以将接口统计信息传感器组分配给订阅配置文件。</li><li><code>lag</code> — 输入 <code>lag</code> 以将 LAG 统计信息传感器组分配给订阅配置文件。</li><li><code>system</code> — 输入 <code>system</code> 以将系统统计信息传感器组分配给订阅配置文件。</li><li><code>group-name</code> — 输入传感器组的名称。</li><li><code>sampling-interval</code> — 输入用于收集数据样本的时间间隔（以毫秒为单位）。范围为 0 到 4294967295。默认值为 15000。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 命令模式   | SUBSCRIPTION-PROFILE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 使用情况信息 | 此命令会将从中针对流式遥测收集数据的传感器分配给订阅配置文件，并指定采样率。要将传感器组添加到订阅配置文件，请重新输入命令。 <code>interface</code> 传感器组仅支持物理和端口通道接口。此命令的 <code>no</code> 版本将从订阅配置文件中删除传感器组。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

示例

```
OS10(conf-telemetry)# subscription-profile sp01
OS10(conf-telemetry-sp-sp01)#
OS10(conf-telemetry-sp-sp01)# sensor-group
 bgp BGP statistics sensor
group
 bgp-peer BGP Peer statistics sensor group
 buffer QOS Buffer statistics sensor group
 device Device statistics sensor group
 environment Switch peripheral statistics sensor group
 interface Interface statistics sensor group
 lag Lag statistics sensor group
 system System statistics sensor group
```

```
OS10(conf-telemetry)# subscription-profile subscription-1
OS10(conf-telemetry-sp-subscription-1)# sensor-group bgp 30000
OS10(conf-telemetry-sp-subscription-1)# sensor-group environment 415000
```

支持的版本 10.4.3.0 or later

# sensor-group (telemetry)

配置流式遥测的传感器组。

 **注:** 此命令在版本 10.4.3.0 上不受支持。

|      |                                                                                                                                                                                                                                                               |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法   | <code>sensor-group group-name</code>                                                                                                                                                                                                                          |
| 参数   | <code>group-name</code> — 输入传感器组的名称。最多 32 个字符。您可以输入预配置的传感器组配置文件的名称。有效值包括： <code>bgp</code> 、 <code>bgp-peer</code> 、 <code>buffer</code> 、 <code>device</code> 、 <code>environment</code> 、 <code>interface</code> 、 <code>system</code> 和 <code>lag</code> 。 |
| 默认   | 未配置                                                                                                                                                                                                                                                           |
| 命令模式 | TELEMETRY                                                                                                                                                                                                                                                     |

|               |                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>使用情况信息</b> | 传感器组将定义收集并流式传输到目标的 YANG 模式。您也可以使用预配置的传感器组配置文件，而无需指定 YANG 容器路径。在版本 10.4.3.0 中，遥测仅支持预配置的传感器组。interface 传感器组仅支持物理和端口通道接口。要查看预配置的传感器组中的 YANG 路径，请使用 <code>show telemetry sensor-group</code> 命令。 |
| <b>示例</b>     | <pre>OS10(conf-telemetry)# sensor-group bgp OS10(conf-telemetry-sg-bgp)#</pre>                                                                                                               |
| <b>支持的版本</b>  | 10.4.3.0 or later                                                                                                                                                                            |

## sensor-path

配置传输数据的 YANG 容器的路径。

 **注:** 此命令在版本 10.4.3.0 上不受支持。

|               |                                                                                                                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>sensor-path yang-path</code>                                                                                                                                                                                                                             |
| <b>参数</b>     | <code>yang-path</code> — 输入 YANG 路径。请参阅针对遥测数据收集的阳路径的 <a href="#">YANG 模型遥测数据</a> 。                                                                                                                                                                             |
| <b>默认</b>     | 未配置                                                                                                                                                                                                                                                            |
| <b>命令模式</b>   | SENSOR-GROUP                                                                                                                                                                                                                                                   |
| <b>使用情况信息</b> | 指定的 YANG 路径中的数据将按指定的时间间隔或在发生事件时以接近实时的顺序传输到配置的目标。您可以在容器层次结构中的任意级别输入传感器路径。此路径下的层次结构中所有容器的数据将流式传输到目标设备。要配置传感器组中的多个传感器路径，请重新输入命令。                                                                                                                                  |
| <b>示例</b>     | <pre>OS10(conf-telemetry)# sensor-group interfaces OS10(conf-telemetry-sg-interfaces)# sensor-group dell-base-if-cmn/if/ interfaces-state/interface OS10(conf-telemetry-sg-interfaces)# sensor-group dell-base-cmn/if/ interfaces/interface/member-ports</pre> |
| <b>支持的版本</b>  | 10.4.3.0 or later                                                                                                                                                                                                                                              |

## show telemetry

显示流式遥测的已配置目标组、传感器组和订阅配置文件。

|               |                                                                                                                                                                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>show telemetry [destination-group [group-name]   sensor-group [group-name]   subscription-profile [profile-name]]</code>                                                                                                                                                                                 |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>destination-group</code> — 仅显示目标组或指定组。</li> <li><code>sensor-group</code> — 仅显示传感器组或指定组。</li> <li><code>subscription-profile</code> — 仅显示订阅配置文件或指定的配置文件。</li> </ul>                                                                                               |
| <b>默认</b>     | 显示所有目标组、传感器组和订阅配置。                                                                                                                                                                                                                                                                                             |
| <b>命令模式</b>   | EXEC                                                                                                                                                                                                                                                                                                           |
| <b>使用情况信息</b> | 使用 <code>show telemetry</code> 命令验证配置的目标设备、传感器数据源和订阅配置文件。                                                                                                                                                                                                                                                      |
| <b>示例</b>     | <pre>OS10# show telemetry  Telemetry Status           : disabled -- Telemetry Destination Groups -- -- Telemetry Sensor Groups -- Group : bgp   Sensor Path : bgp/bgp-oper/bgpPrfxCntrsEntry   Sensor Path : bgp/bgp-oper/bgpPeerCount Group : bgp-peer   Sensor Path : infra-bgp/peer-state/peer-status</pre> |

```

Group : buffer
 Sensor Path : base-qos/queue-stat
 Sensor Path : base-qos/priority-group-stat
 Sensor Path : base-qos/buffer-pool-stat
 Sensor Path : base-qos/buffer-pool
Group : device
 Sensor Path : base-pas/chassis
 Sensor Path : base-pas/card
 Sensor Path : base-switch/switching-entities/switch-stats
Group : environment
 Sensor Path : base-pas/entity
 Sensor Path : base-pas/psu
 Sensor Path : base-pas/fan-tray
 Sensor Path : base-pas/fan
 Sensor Path : base-pas/led
 Sensor Path : base-pas/temperature
 Sensor Path : base-pas/temp_threshold
 Sensor Path : base-pas/media
 Sensor Path : base-pas/media-channel
Group : interface
 Sensor Path : if/interfaces-state/interface/statistics
 Sensor Path : dell-base-if-cmn/if/interfaces-state/interface
Group : lag
 Sensor Path : dell-base-if-cmn/if/interfaces
Group : system
 Sensor Path : system-status/current-status
Group : oc-bfd
 Sensor Path : openconfig-bfd/bfd
Group : oc-bgp
 Sensor Path : openconfig-bgp/bgp/neighbors/neighbor
 Sensor Path : openconfig-bgp/bgp/rib/afi-safis/afi-safi
Group : oc-buffer
 Sensor Path : openconfig-qos/qos/interfaces/interface
Group : oc-device
 Sensor Path : openconfig-platform/components/component
 Sensor Path : openconfig-network-instance/network-instances/network-
instance
Group : oc-environment
 Sensor Path : openconfig-platform/components/component
Group : oc-interface
 Sensor Path : openconfig-interfaces/interfaces/interface
Group : oc-lacp
 Sensor Path : openconfig-lacp/lacp
Group : oc-lag
 Sensor Path : openconfig-interfaces/interfaces/interface
Group : oc-lldp
 Sensor Path : openconfig-lldp/lldp
Group : oc-stp
 Sensor Path : openconfig-spanning-tree/stp
Group : oc-system
 Sensor Path : openconfig-system/system
 Sensor Path : openconfig-platform/components/component
Group : oc-vendor-ufd
 Sensor Path : ufd/uplink-state-group-stats/ufd-groups
Group : oc-vendor-vxlan
 Sensor Path : vxlan/vxlan-state/remote-endpoint/stats
Group : oc-vlan
 Sensor Path : openconfig-interfaces/interfaces/interface
Group : oc-vrrp
 Sensor Path : openconfig-interfaces/interfaces/interface/subinterfaces/
subinterface
-- Telemetry Subscription Profiles --

```

```

OS10# show telemetry destination-group

Telemetry Status : enabled

-- Telemetry Destination Groups --

```



```
Group : dest1
Destination : 10.11.56.204 Port : 40001
```

```
OS10# show telemetry sensor-group
```

```
Telemetry Status : enabled

-- Telemetry Sensor Groups --
Group : bgp
 Sensor Path : bgp/bgp-oper/bgpPrfxCntrsEntry
 Sensor Path : bgp/bgp-oper/bgpPeerCount
Group : bgp-peer
 Sensor Path : infra-bgp/peer-state/peer-status
Group : buffer
 Sensor Path : base-qos/queue-stat
 Sensor Path : base-qos/priority-group-stat
 Sensor Path : base-qos/buffer-pool-stat
 Sensor Path : base-qos/buffer-pool
Group : device
 Sensor Path : base-pas/chassis
 Sensor Path : base-pas/card
 Sensor Path : base-switch/switching-entities/switch-stats
Group : environment
 Sensor Path : base-pas/entity
 Sensor Path : base-pas/psu
 Sensor Path : base-pas/fan-tray
 Sensor Path : base-pas/fan
 Sensor Path : base-pas/led
 Sensor Path : base-pas/temperature
 Sensor Path : base-pas/temp_threshold
 Sensor Path : base-pas/media
 Sensor Path : base-pas/media-channel
Group : interface
 Sensor Path : if/interfaces-state/interface/statistics
 Sensor Path : dell-base-if-cmn/if/interfaces-state/interface
Group : lag
 Sensor Path : dell-base-if-cmn/if/interfaces
Group : system
 Sensor Path : system-status/current-status
```

```
OS10# show telemetry subscription-profile
```

```
Telemetry Status : enabled

-- Telemetry Subscription Profile --

Name : subscription-1

Destination Groups(s) : dest1

Sensor-group Sample-interval

bgp 300000
bgp-peer 0
buffer 15000
device 300000
environment 300000
interface 180000
lag 0
system 300000

Encoding : gpb
Transport : grpc TLS : disabled
Source Interface : ethernet1/1/1
Active : true
Reason : Connection summary: One or more active connections
 The connection 10.11.56.204:40001 is in connected state
```

## 支持的版本

10.4.3.0 or later

# source interface

配置用于将遥测数据传输到目标设备的源接口。

|        |                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>source interface interface</code>                                                                                                                                                                                                                                                                                                                                              |
| 参数     | <code>interface</code> — 以下值之一： <ul style="list-style-type: none"><li><code>ethernet node/slot/port[:subport]</code> — 输入物理以太网接口。</li><li><code>loopback number</code> — 输入环回接口，从 0 到 16383。</li><li><code>management 1/1/1</code> — 输入管理接口。</li><li><code>port-channel channel-id</code> — 输入端口通道 ID，从 1 到 28。</li><li><code>vlan vlan-id</code> — 输入 VLAN ID，从 1 到 4093。</li></ul> |
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                                                    |
| 命令模式   | SUBSCRIPTION-PROFILE                                                                                                                                                                                                                                                                                                                                                                 |
| 使用情况信息 | 遥测代理使用源接口派生用于与目标设备进行通信的 VRF 实例和 IP 地址。对于 gRPC 传输，源接口配置是可选的。命令的 <code>no</code> 版本将从订阅配置文件中移除配置的源接口。                                                                                                                                                                                                                                                                                  |
| 示例     | <pre>OS10(conf-telemetry)# subscription-profile subscription-1 OS10(conf-telemetry-sp-subscription-1)# source-interface ethernet 1/1/1</pre>                                                                                                                                                                                                                                         |
| 支持的版本  | 10.4.3.0 or later                                                                                                                                                                                                                                                                                                                                                                    |

# subscription-profile

配置流式遥测数据的订阅配置文件。

|        |                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------|
| 语法     | <code>subscription-profile profile-name</code>                                                               |
| 参数     | <code>profile-name</code> — 输入配置文件名称。最多 32 个字符。                                                              |
| 默认     | 未配置                                                                                                          |
| 命令模式   | TELEMETRY                                                                                                    |
| 使用情况信息 | 订阅配置文件将目标组与传感器组关联，并指定数据编码格式和传输协议。遥测数据将发送到目标组中指定的 IP 地址和端口。                                                   |
| 示例     | <pre>OS10(conf-telemetry)# subscription-profile subscription-1 OS10(conf-telemetry-sp-subscription-1)#</pre> |
| 支持的版本  | 10.4.3.0 or later                                                                                            |

# telemetry

进入遥测配置模式以配置流式遥测。

|        |                                                          |
|--------|----------------------------------------------------------|
| 语法     | <code>telemetry</code>                                   |
| 参数     | 无                                                        |
| 默认     | 在交换机上禁用遥测。                                               |
| 命令模式   | CONFIGURATION                                            |
| 使用情况信息 | 启用和禁用遥测模式下的流式遥测。                                         |
| 示例     | <pre>OS10(config)# telemetry OS10(conf-telemetry)#</pre> |
| 支持的版本  | 10.4.3.0 or later                                        |

## transport

配置用于将遥测数据流式传输到远程管理设备的传输协议。

|        |                                                                                                                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>transport protocol [no-tls]</code>                                                                                                                                                                                                                                                                                                                    |
| 参数     | <ul style="list-style-type: none"><li><code>protocol</code> — 输入用于遥测会话的 gRPC (Google 远程过程调用) 传输协议。</li><li><code>no-tls</code> — (可选) 通过 gRPC 传输禁用传输安全层 (TLS) 证书交换。</li></ul>                                                                                                                                                                               |
| 默认     | OS10 遥测在启用了 TLS 证书的情况下使用 gRPC 协议进行传输。                                                                                                                                                                                                                                                                                                                       |
| 命令模式   | SUBSCRIPTION-PROFILE                                                                                                                                                                                                                                                                                                                                        |
| 使用情况信息 | <p>默认情况下, gRPC with TLS 传输默认已启用。要使用 gRPC over TLS, 您必须在交换机上安装 X.509v3 证书。要禁用 TLS 证书交换, 请使用 <code>transport grpc no-tls</code> 命令。</p> <p> <b>注:</b> gRPC with TLS 传输不支持主机证书。要使用 CA 证书, 请参阅<a href="#">请求和安装主机证书</a>。</p> <p>命令的 <code>no</code> 版本将从订阅配置文件中删除已配置的传输协议。</p> |
| 示例     | <pre>OS10(config-telemetry)# subscription-profile subscription-1 OS10(config-telemetry-sp-subscription-1)# transport grpc</pre>                                                                                                                                                                                                                             |
| 支持的版本  | 10.4.3.0 or later                                                                                                                                                                                                                                                                                                                                           |

## 示例：配置流式遥测

```
OS10(config)# telemetry
OS10(config-telemetry)# enable
OS10(config-telemetry)# destination-group dest1
OS10(config-telemetry-dg-dest1)# destination 10.11.56.204 40001
OS10(config-telemetry-dg-dest1)# exit
OS10(config-telemetry)# subscription-profile subscription-1
OS10(config-telemetry-sp-subscription-1)# sensor-group bgp 300000
OS10(config-telemetry-sp-subscription-1)# sensor-group bgp-peer 0
OS10(config-telemetry-sp-subscription-1)# sensor-group buffer 15000
OS10(config-telemetry-sp-subscription-1)# sensor-group device 300000
OS10(config-telemetry-sp-subscription-1)# sensor-group environment 300000
OS10(config-telemetry-sp-subscription-1)# sensor-group interface 180000
OS10(config-telemetry-sp-subscription-1)# sensor-group lag 0
OS10(config-telemetry-sp-subscription-1)# sensor-group system 300000
OS10(config-telemetry-sp-subscription-1)# destination-group dest1
OS10(config-telemetry-sp-subscription-1)# encoding gpb
OS10(config-telemetry-sp-subscription-1)# transport grpc no-tls
OS10(config-telemetry-sp-subscription-1)# source-interface ethernet 1/1/1
OS10(config-telemetry-sp-subscription-1)# end
```

```
OS10# show telemetry

Telemetry Status : enabled

-- Telemetry Destination Groups --
Group : dest1
 Destination : 10.11.56.204 Port : 40001

-- Telemetry Sensor Groups --
Group : bgp
 Sensor Path : bgp/bgp-oper/bgpPrfxCntersEntry
 Sensor Path : bgp/bgp-oper/bgpPeerCount
Group : bgp-peer
 Sensor Path : infra-bgp/peer-state/peer-status
Group : buffer
 Sensor Path : base-qos/queue-stat
 Sensor Path : base-qos/priority-group-stat
 Sensor Path : base-qos/buffer-pool-stat
 Sensor Path : base-qos/buffer-pool
Group : device
```

```

Sensor Path : base-pas/chassis
Sensor Path : base-pas/card
Sensor Path : base-switch/switching-entities/switch-stats
Group : environment
Sensor Path : base-pas/entity
Sensor Path : base-pas/psu
Sensor Path : base-pas/fan-tray
Sensor Path : base-pas/fan
Sensor Path : base-pas/led
Sensor Path : base-pas/temperature
Sensor Path : base-pas/temp_threshold
Sensor Path : base-pas/media
Sensor Path : base-pas/media-channel
Group : interface
Sensor Path : if/interfaces-state/interface/statistics
Sensor Path : dell-base-if-cmn/if/interfaces-state/interface
Group : lag
Sensor Path : dell-base-if-cmn/if/interfaces
Group : system
Sensor Path : system-status/current-status

-- Telemetry Subscription Profiles --
Name : subscription-1

Destination Groups(s) : dest1

Sensor-group Sample-interval

bgp 300000
bgp-peer 0
buffer 15000
device 300000
environment 300000
interface 180000
lag 0
system 300000

Encoding : gpb
Transport : grpc TLS : disabled
Source Interface : ethernet1/1/1
Active : true
Reason : Connection summary: One or more active connections
 The connection 10.11.56.204:40001 is in connected state

```

## RESTCONF API

RESTCONF 是使用 HTTPS 连接的表述性状态传输 (REST)。通过 OS10 RESTCONF API 在 OS10 交换机上使用 JavaScript Object Notation (JSON) 结构化消息来设置配置参数。使用任何编程语言创建并发送 JSON 消息。本章中的示例使用 curl。

OS10 RESTCONF 实施符合 RFC 8040。您可以使用 RESTCONF API 来配置和监控 OS10 交换机。

OS10 RESTCONF API 将 HTTP 与端口 443 上的传输层安全 (TLS) 协议配合使用。OS10 支持 RFC 7230 中定义的 HTTP/1.1 传输。RESTCONF API 使用基于可插拔身份验证模块 (PAM) 的身份验证。

在受支持的平台上，默认情况下，OS10 RESTCONF API 处于禁用状态。要配置和启用 RESTCONF API，请参阅 [配置 RESTCONF API 部分](#)。

要配置和监控 OS10 交换机，请使用 REST API 客户端工具（如 Postman 或 Swagger）来执行 web 请求。REST API 请求（例如 GET、PUT、POST、DELETE 和 PATCH）在 OS10 RESTCONF 资源上运行，例如：

**表. 105: OS10 RESTCONF 资源**

| 资源 | 说明                         | URL                  |
|----|----------------------------|----------------------|
| 数据 | RESTCONF API 客户端访问的配置和操作数据 | /restconf/data       |
| 操作 | 协议特定数据模型操作的容器 OS10 通告      | /restconf/operations |

要浏览 OS10 RESTCONF API 端点和操作，请参阅 [Dell EMC 支持站点](#) 的 OS10 Enterprise Edition 软件页面上提供的 OpenAPI JSON 文件。下载 JSON 文件并将其导入到 REST API 客户端工具；例如，Swagger 或 Postman，以生成代码、文档和测试案例。有关 OpenAPI 规格的信息，请转至 <https://swagger.io/docs/specification/about/>。

## 配置 RESTCONF API

要在 OS10 接口上使用 RESTCONF API，必须使用 `rest api restconf` 命令启用 RESTCONF API 服务。您还可以配置 HTTPS 访问，包括：

- 安全套接字层 (SSL) 自签名服务器证书中需要的主机名称
- HTTPS 连接超时
- 用于加密 HTTPS 连接中的数据的加密套件

启用 RESTCONF API 之后，您可以从远程设备发送 HTTPS 请求。

1. （可选）使用最多 30 个字母数字字符，在 CONFIGURATION 模式下的 RESTCONF HTTPS 连接中配置 SSL 自签名服务器证书所需的主机名称。输入 OS10 交换机的 IP 地址或域名。默认情况下，OS10 交换机的域名用作主机名称。

```
rest https server-certificate name hostname
```

2. （可选）配置 RESTCONF HTTPS 会话在 CONFIGURATION 模式下使用的超时时间为 30 至 65535 秒；默认值为 30。

```
rest https session timeout seconds
```

3. （可选）限制交换机在 RESTCONF HTTPS 会话中使用的密码，以在 CONFIGURATION 模式中对数据进行加密和解密。默认情况下，支持 OS10 上安装的所有加密套件。用空格分隔多个条目。有效的密码套件值为：

- `dhe-rsa-with-aes-128-gcm-SHA256`
- `dhe-rsa-with-aes-256-gcm-SHA384`
- `ecdhe-rsa-with-aes-128-gcm-SHA256`
- `ecdhe-rsa-with-aes-256-gcm-SHA384`

```
rest https cipher-suite
```

4. 在 CONFIGURATION 模式下启用 RESTCONF API。

```
rest api restconf
```

## RESTCONF API 配置

```
OS10(config)# rest https server-certificate name OS10.dell.com
OS10(config)# rest https session timeout 60
OS10(config)# rest https cipher-suite dhe-rsa-with-aes-128-gcm-SHA256
dhe-rsa-with-aes-256-gcm-SHA384 ecdhe-rsa-with-aes-256-gcm-SHA384
OS10(config)# rest api restconf
```

# RESTCONF API 的 CLI 命令

## rest api restconf

在交换机上启用 RESTCONF API 服务。

|        |                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>rest api restconf</code>                                                                                                                                |
| 参数     | 无                                                                                                                                                             |
| 默认     | RESTCONF API 处于禁用状态。                                                                                                                                          |
| 命令模式   | CONFIGURATION                                                                                                                                                 |
| 使用情况信息 | <ul style="list-style-type: none"><li>启用 RESTCONF API 之后，您可以从远程设备的 HTTPS 请求发送 <code>curl</code> 命令。</li><li>命令的 <code>no</code> 版本将禁用 RESTCONF API。</li></ul> |

**示例**

```
OS10(config)# rest api restconf
```

**支持的版本** 10.4.1.0 or later

## rest https cipher-suite

限制加密和解密 REST HTTPS 数据的密码。

|        |                                                                                                                                                                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>rest https cipher-suite <i>cipher-list</i></code>                                                                                                                                                                                                                          |
| 参数     | <i>cipher-list</i> — 输入 REST API HTTPS 会话中支持的密码。用空格分隔多个条目。有效的加密套件包括： <ul style="list-style-type: none"><li>dhe-rsa-with-aes-128-gcm-SHA256</li><li>dhe-rsa-with-aes-256-gcm-SHA384</li><li>ecdhe-rsa-with-aes-128-gcm-SHA256</li><li>ecdhe-rsa-with-aes-256-gcm-SHA384</li></ul> |
| 默认     | 支持使用 OS10 安装的所有加密套件。                                                                                                                                                                                                                                                             |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                    |
| 使用情况信息 | <ul style="list-style-type: none"><li>使用 <code>rest https cipher-suite</code> 命令限制 RESTCONF HTTPS 会话使用的密码。</li><li>命令的 <code>no</code> 版本将移除加密列表并恢复默认值。</li></ul>                                                                                                                |

**示例**

```
OS10(config)# rest https cipher-suite dhe-rsa-with-aes-128-gcm-SHA256
dhe-rsa-with-aes-256-gcm-SHA384 ecdhe-rsa-with-aes-256-gcm-SHA384
```

**支持的版本** 10.4.1.0 or later

## rest https server-certificate

创建 RESTCONF HTTPS 连接使用的 SSL 自签名服务器证书。

**语法** `rest https server-certificate name hostname`

**参数** `name hostname` — 输入 OS10 交换机的 IP 地址或域名。

**默认** OS10 交换机域名用作 `hostname`。

**命令模式** CONFIGURATION

**使用情况信息** 命令的 `no` 版本将从 SSL 服务器证书移除主机名称。

**示例**

```
OS10(config)# rest https server-certificate name 10.10.10.10
```

**支持的版本** 10.4.1.0 or later

## rest https session timeout

配置 RESTCONF HTTPS 连接使用的超时。

**语法** `rest https session timeout seconds`

**参数** `seconds` — 输入来自 RESTCONF 客户端的 HTTPS 请求的交换机超时时间，从 30 到 65535 秒。

**默认** 30 秒

**命令模式** CONFIGURATION

**使用情况信息**

- 如果在配置的时间内未收到 HTTPS 请求，交换机将关闭 RESTCONF HTTPS 会话。
- 命令的 `no` 版本将移除已配置的 RESTCONF HTTPS 会话超时。

**示例**

```
OS10# rest https session timeout 60
```

**支持的版本** 10.4.1.0 or later

## RESTCONF API 任务

使用 RESTCONF API，您可以使用 HTTPS 请求调配 OS10 交换机。此部分中的示例显示如何使用 `curl` 命令访问 OS10 RESTCONF API。`curl` 是 Linux shell 命令，可生成 HTTPS 请求并在外部服务器上执行。



### curl 命令

`curl` 命令选项包括：

- `-X` 可指定 HTTPS 请求类型；例如，`POST`、`PATCH` 或 `GET`。
- `-u` 可指定用户名和密码以用于服务器身份验证。
- `-k` 可指定文本文件以读取 `curl` 参数。文本文件中的命令行参数将以似乎在命令行中提供的方式使用。从远程编排系统访问 OS10 RESTCONF API 时，将使用 OS10 交换机的 IP 地址或 URL。
- 将 HTTPS 发送到服务器时，`-H` 可指定额外的标头以包括在请求中。您可以输入多个额外的标头。
- `-d` 将在 HTTPS 请求中发送指定的数据。

在 `curl` 命令中，使用 `%2F` 以代表反斜杠 (/)；例如，输入 `ethernet1/2/3` 作为 `ethernet1%2F1%2F3`。

有关详细信息，请参阅 [curl Man 页面](#)。

## 使用情况信息

使用 `curl` 命令访问 OS10 RESTCONF API 时，请考虑以下情况：

- Dell EMC 建议使用目标资源的指定 UR，以用于扩展系统中的 GET 查询。例如，`curl -X GET -k -u admin:admin -H "accept:application/json" https://$TARGET/restconf/data/interfaces/interface/port-channel10`
- OS10 在 RESTCONF 数据库的根资源上不支持 REST 查询。例如，GET 查询 `curl -X GET -k -u admin:admin https://$TARGET/restconf/data` 将返回错误。
- 当 RESTCONF 查询正在进行时，您无法配置任何 CLI 命令，直到 RESTCONF 查询完成。
- 建议使用 POST 请求，而不是 PUT，以替换目标数据资源。

## 查看 CLI 命令的 XML 结构

要使用 RESTCONF API 配置和监控 OS10 交换机，请使用 JSON 格式的数据参数创建 HTTPS 请求。JSON 数据参数与 OS10 命令的 XML 结构中的参数相同。

要在 OS10 命令的 XML 代码中显示参数值作为参考，请在 EXEC 模式下使用 `debug cli netconf` 命令。在 CONFIGURATION 模式中，使用 `do debug cli netconf` 命令。

此命令可启用 CLI 到 XML 显示。在提示符下，输入 XML 请求的 OS10 命令和所需的回复。要退出 CLI 到 XML 显示，请使用 `no debug cli netconf` 命令。

找到适用于相同 JSON 数据参数的 XML 参数值。例如，要在 OS10 交换机上配置 VLAN 20，请在卷曲命令中输入 RESTCONF 端点和 JSON 内容。请注意，JSON `type` 和 `name` 参数显示在 `interface vlan` 命令的 XML 结构中。

- RESTCONF 端点: `/restconf/data/interfaces`
- JSON 数据内容:

```
{
 "interface": [{
 "type": "iana-if-type:l2vlan",
 "enabled": true,
 "description": "vlan20",
 "name": "vlan20"
 }]
}
```

- 卷曲命令:

```
curl -X POST -u admin:admin -k "https://10.11.86.113/restconf/data/interfaces"
-H "accept: application/json" -H "Content-Type: application/json"
-d '{ "interface": [{ "type": "iana-if-type:l2vlan", "enabled": true,
"description":"vlan20", "name":"vlan20"}]}'
```

要显示卷曲命令中 `type` 和 `name` 参数的值，请显示 `interface vlan 20` 配置命令的 XML 结构:

```
OS10(config)# do debug cli netconf
OS10(config)# interface vlan 10

Request:
<?xml version="1.0" encoding="UTF-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <edit-config>
 <target>
 <candidate/>
 </target>
 <default-operation>merge</default-operation>
 <error-option>stop-on-error</error-option>
 <test-option>set</test-option>
 <config>
 <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces"
xmlns:ianaift="urn:ietf:params:xml:ns:yang:iana-if-type" xmlns:dell-if="http://
www.dellemc.com/networking/os10/dell-interface" xmlns:dell-eth="http://www.dellemc.com/
networking/os10/dell-ethernet" xmlns:dell-lag="http://www.dellemc.com/networking/os10/
dell-lag">
 <interface>
 <type>ianaift:l2vlan</type>
 <name>vlan10</name>
 </interface>
 </interfaces>
```



```

 </config>
 </edit-config>
</rpc>

Reply:
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="10">
 <ok/>
</rpc-reply>
OS10(config)# do no debug cli netconf

```

## RESTCONF API 示例

一些常见的 RESTCONF API 操作包括配置系统主机名称和环回接口等接口。本部分中的示例使用 `curl` 命令发送 HTTPS 请求。

### 系统

#### 配置系统主机名称

**RESTCONF 端点** `/restconf/data/dell-system:system/hostname`

#### JSON 内容

```
{
 "hostname": "MyHost"
}
```

#### 参数

- `hostname string` — 输入系统的主机名称。默认值为 OS10。

#### 示例

```
curl -X PATCH -k -u admin:admin -H "Content-Type: application/json"
https://10.11.86.113/restconf/data/dell-system:system/hostname
-d '{"hostname": "MyHost"}'
```

### 接口

#### 配置环回接口

**RESTCONF 端点** `/restconf/data/interfaces`

#### JSON 内容

```
{
 "interface": [{
 "type": "iana-if-type:softwareLoopback",
 "enabled": true,
 "description": "loopback interface",
 "name": "loopback1"}]
}
```

#### 参数

- `type string` — 为环回接口输入 `iana-if-type:softwareLoopback`。
- `enabled bool` — 输入 `true` 以启用接口；输入 `false` 以禁用。
- `description string` — 输入用于说明接口的文本字符串。最多 80 个字母数字字符。
- `name string` — 输入接口的 `loopback loopback-id`，其中 `loopback-id` 是从 0 到 16383。

#### 示例

```
curl -X POST -k -u admin:admin "https://10.11.86.113/restconf/data/
interfaces"
-H "accept: application/json" -H "Content-Type: application/json"
-d '{"interface": [{"type": "iana-if-type:softwareLoopback", "enabled":
```

```
true,
"description":"loopback interface", "name":"loopback1"]}]}'
```

## 配置环回接口 IP 地址

**RESTCONF 端点** /restconf/data/interfaces/interface/loopback1

### JSON 内容

```
{
 "dell-ip:ipv4":{
 "address": {
 "primary-addr":"6.6.6.6/24"
 }
 }
}
```

### 参数

- `primary-addr` *ip-address/prefix-length* — 以点分隔的十进制 A.B.C.D/x 格式输入环回 IP 地址。

### 示例

```
curl -X POST -k -u admin:admin "https://10.11.86.113/restconf/data/
interfaces/interface/loopback1"
-H "accept: application/json" -H "Content-Type: application/json"
-d '{"dell-ip:ipv4":{"address": {"primary-addr":"6.6.6.6/24"}}}'
```

## OS10 故障处理

关键工作负载和应用程序需要持续的可用性。Dell EMC Networking 提供了工具，可帮助您监控问题并进行故障处理。

|                |                     |
|----------------|---------------------|
| <b>数据包和流捕获</b> | 管理数据包和流量            |
| <b>指标度量</b>    | Ping、往返时间、抖动、响应时间等  |
| <b>分析和报告</b>   | 指标和数据包捕获            |
| <b>提醒</b>      | 触发问题报告              |
| <b>日志记录</b>    | 捕获系统历史记录            |
| <b>性能监控</b>    | 建立基线并定义用于检测性能问题的触发器 |
| <b>映射和表示</b>   | 定义设备位置和状态           |

Dell EMC 建议以下妥善做法：

- 从应用程序的视点查看端到端流量。
- 在需要时，随时随地按需快速部署网络管理基础架构。
- 将分析扩展到网络之外，并观察与主机之间的来往流量。
- 重点关注实时评估，并使用趋势分析来备份您的结论。
- 强调有效而非绝对 — 利用管理解决方案快速解决最常见、最昂贵的问题。
- 解决网络性能问题，然后再关注应用程序性能。
- 使用适合您的网络和需求的方法和技术。
- 持续监控性能和可用性，作为系统性能和系统正常运行时间的基准，以便快速将网络问题与应用程序问题分开。

## 诊断工具

本节包含有关对网络设备进行调试、监控和故障处理的高级软件和硬件命令的信息。

**注：**输出示例仅用于参考目的，可能不适用于您的特定系统。

### 查看资源清册

使用 `show inventory` 命令可以查看设备的模块 ID。

```
OS10# show inventory
Product : S4148F-ON
Description : S4148F-ON 48x10GbE, 2x40GbE QSFP+, 4x100GbE QSFP28 Interface
Module
Software version : 10.5.0.0
Product Base :
Product Serial Number :
Product Part Number :

Unit Type Part Number Rev Piece Part ID Svc Tag Exprs
Svc Code

* 1 S4148F-ON 09H9MN X01 TW-09H9MN-28298-713-0026 9531XC2 198
985 006 10
 1 S4148F-ON-PWR-1-AC 06FKHH A00 CN-06FKHH-28298-6B5-03NY
 1 S4148F-ON-FANTRAY-1 0N7MH8 X01 TW-0N7MH8-28298-713-0101
 1 S4148F-ON-FANTRAY-2 0N7MH8 X01 TW-0N7MH8-28298-713-0102
 1 S4148F-ON-FANTRAY-3 0N7MH8 X01 TW-0N7MH8-28298-713-0103
 1 S4148F-ON-FANTRAY-4 0N7MH8 X01 TW-0N7MH8-28298-713-0104
```

## 引导分区和映像

显示系统引导分区和映像信息。

- 在 EXEC 模式下查看所有引导信息。

```
show boot
```

- 在 EXEC 模式下查看引导详细信息。

```
show boot detail
```

### 查看引导信息

```
OS10# show boot
Current system image information:
=====
Type Boot Type Active Standby Next-Boot

Node-id 1 Flash Boot [B] 10.5.0.0 [A] 10.5.0.0 [B] active
```

### 查看引导详细信息

```
OS10# show boot detail
Current system image information detail:
=====
Type: Node-id 1
Boot Type: Flash Boot
Active Partition: B
Active SW Version: 10.5.0.0
Active SW Build Version: 10.5.0.270
Active Kernel Version: Linux 4.9.168
Active Build Date/Time: 2019-07-29T23:35:01Z
Standby Partition: A
Standby SW Version: 10.5.0EX
Standby SW Build Version: 10.5.0EX.252
Standby Build Date/Time: 2019-07-27T17:31:55Z
Next-Boot: active[B]
```

## 监控进程

显示 CPU 进程信息。

- 在 EXEC 模式下查看进程 CPU 利用率信息。

- `show processes node-id node-id-number [pid process-id]`

### 查看 CPU 利用率

```
OS10# show processes node-id 1
top - 09:19:32 up 5 days, 6 min, 2 users, load average: 0.45, 0.39, 0.34
Tasks: 208 total, 2 running, 204 sleeping, 0 stopped, 2 zombie
%Cpu(s): 9.7 us, 3.9 sy, 0.3 ni, 85.8 id, 0.0 wa, 0.0 hi, 0.3 si, 0.0 st
KiB Mem: 3998588 total, 2089416 used, 1909172 free, 143772 buffers
KiB Swap: 399856 total, 0 used, 399856 free. 483276 cached Mem

 PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
 9 root 20 0 0 0 0 S 6.1 0.0 5:22.41 rcuos/1
 819 snmp 20 0 52736 6696 4132 S 6.1 0.2 2:44.18 snmpd
 30452 admin 20 0 22076 2524 2100 R 6.1 0.1 0:00.02 top
 1 root 20 0 112100 5840 3032 S 0.0 0.1 0:12.32 systemd
 2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd
 3 root 20 0 0 0 0 S 0.0 0.0 0:25.37 ksoftirqd/0
 5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:
 7 root 20 0 0 0 0 R 0.0 0.0 5:15.27 rcu_sched
 8 root 20 0 0 0 0 S 0.0 0.0 2:43.64 rcuos/0
 10 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_bh
 11 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/0
 12 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcuob/1
```

```

13 root rt 0 0 0 0 S 0.0 0.0 0:07.30 migration/0
14 root rt 0 0 0 0 S 0.0 0.0 0:02.18 watchdog/0
15 root rt 0 0 0 0 S 0.0 0.0 0:02.12 watchdog/1
16 root rt 0 0 0 0 S 0.0 0.0 0:04.98 migration/1
17 root 20 0 0 0 0 S 0.0 0.0 0:03.92 ksoftirqd/1
19 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/1:+
20 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 khelper
21 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kdevtmpfs
22 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 netns
23 root 20 0 0 0 0 S 0.0 0.0 0:00.41 khungtaskd
24 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 writeback
25 root 25 5 0 0 0 S 0.0 0.0 0:00.00 ksmd
--more--

```

```

OS10# show processes node-id 1 pid 1019
top - 09:21:58 up 5 days, 8 min, 2 users, load average: 0.18, 0.30, 0.31
Tasks: 1 total, 0 running, 1 sleeping, 0 stopped, 0 zombie
%Cpu(s): 9.7 us, 3.9 sy, 0.3 ni, 85.8 id, 0.0 wa, 0.0 hi, 0.3 si, 0.0 st
KiB Mem: 3998588 total, 2089040 used, 1909548 free, 143772 buffers
KiB Swap: 399856 total, 0 used, 399856 free. 483276 cached Mem
 PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
 1019 root 20 0 1829416 256080 73508 S 6.6 6.4 1212:36 base_nas
OS10#

```

## LED 设置

信标 LED 标识端口的位置和系统状态（闪烁或稳定的 LED）。

 **注：**此功能在 Z9332F-ON 平台上不受支持。

使用以下命令更改系统或接口的定位 LED 的当前状态：

```
location-led system {node-id | node-id/unit-id} {on | off}
```

```
location-led interface ethernet {chassis/slot/port[:subport]} {on | off}
```

### 更改系统定位 LED 的状态

```

OS10# location-led system 1 on
OS10# location-led system 1 off

```

### 更改接口定位 LED 的状态

```

OS10# location-led interface ethernet 1/1/1 on
OS10# location-led interface ethernet 1/1/1 off

```

## 数据包分析

使用 Linux `tcpdump` 命令来分析网络数据包。使用筛选器来限制数据包收集和输出。您必须登录 Linux shell 才能使用此命令。有关详细信息，请参阅[登录 OS10 设备](#)。

使用不带 `tcpdump` 参数的 Linux 命令可查看流过所有接口的数据包。要将捕获的数据包写入文件，请使用 `-w` 参数。要使捕获的文件输出脱机，您可以使用开放源代码软件包（例如 `wireshark`）。

### 从以太网接口捕获数据包

```

$ tcpdump -i e101-003-0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on e101-003-0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:39:22.457185 IP 3.3.3.1 > 3.3.3.4: ICMP echo request, id 5320, seq 26, length 64
01:39:22.457281 IP 3.3.3.1 > 3.3.3.4: ICMP echo reply, id 5320, seq 26, length 64

```

## 从接口捕获两个数据包

```
$ tcpdump -c 2 -i e101-003-0
listening on e101-003-0, link-type EN10MB (Ethernet), capture size 96 bytes
01:39:22.457185 IP 3.3.3.1 > 3.3.3.4: ICMP echo request, id 5320, seq 26, length 64
01:39:22.457281 IP 3.3.3.1 > 3.3.3.4: ICMP echo reply, id 5320, seq 26, length 64
2 packets captured
13 packets received by filter
0 packets dropped by kernel
```

## 捕获数据包并写入文件

```
$ tcpdump -w 06102016.pcap -i e101-003-0
listening on e101-003-0, link-type EN10MB (Ethernet), capture size 96 bytes
32 packets captured
32 packets received by filter
0 packets dropped by kernel
```

## 端口适配器和模块

使用 `show diag` 命令可查看 OS10 端口适配器和硬件模块的诊断信息。

### 查看诊断硬件信息

```
OS10# show diag
00:00.0 Host bridge: Intel Corporation Atom Processor S1200 Internal (rev 02)
00:01.0 PCI bridge: Intel Corporation Atom Processor S1200 PCI Express Root Port 1 (rev 02)
00:02.0 PCI bridge: Intel Corporation Atom Processor S1200 PCI Express Root Port 2 (rev 02)
00:03.0 PCI bridge: Intel Corporation Atom Processor S1200 PCI Express Root Port 3 (rev 02)
00:04.0 PCI bridge: Intel Corporation Atom Processor S1200 PCI Express Root Port 4 (rev 02)
00:0e.0 IOMMU: Intel Corporation Atom Processor S1200 Internal (rev 02)
00:13.0 System peripheral: Intel Corporation Atom Processor S1200 SMBus 2.0 Controller 0 (rev 02)
00:13.1 System peripheral: Intel Corporation Atom Processor S1200 SMBus 2.0 Controller 1 (rev 02)
00:14.0 Serial controller: Intel Corporation Atom Processor S1200 UART (rev 02)
00:1f.0 ISA bridge: Intel Corporation Atom Processor S1200 Integrated Legacy Bus (rev 02)
01:00.0 Ethernet controller: Broadcom Corporation Device b850 (rev 03)
02:00.0 SATA controller: Marvell Technology Group Ltd. Device 9170 (rev 12)
03:00.0 PCI bridge: Pericom Semiconductor PI7C9X442SL PCI Express Bridge Port (rev 02)
04:01.0 PCI bridge: Pericom Semiconductor PI7C9X442SL PCI Express Bridge Port (rev 02)
04:02.0 PCI bridge: Pericom Semiconductor PI7C9X442SL PCI Express Bridge Port (rev 02)
04:03.0 PCI bridge: Pericom Semiconductor PI7C9X442SL PCI Express Bridge Port (rev 02)
07:00.0 USB controller: Pericom Semiconductor PI7C9X442SL USB OHCI Controller (rev 01)
07:00.1 USB controller: Pericom Semiconductor PI7C9X442SL USB OHCI Controller (rev 01)
07:00.2 USB controller: Pericom Semiconductor PI7C9X442SL USB EHCI Controller (rev 01)
08:00.0 Ethernet controller: Intel Corporation 82574L Gigabit Network Connection
```

## 测试网络连接

使用 `ping` 和 `traceroute` 命令测试网络连接。当您对 IP 地址执行 `ping` 操作时，您会将数据包发送到目标并等待响应。如果没有响应，则目标不处于活动状态。在配置过程中，如果无法连接到 HOSTNAME 或 IP 地址，则 `ping` 命令将非常有用。

当您执行 `traceroute` 时，输出会显示从您的设备到目标 IP 地址的数据包采用的路径。它还列出了数据包遍历以到达其目标的所有中间跳（路由器），包括遍历的总跳数。

### 检查 IPv4 连接

```
OS10# ping 172.31.1.255

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 172.31.1.255, timeout is 2 seconds:
```

```
Reply to request 1 from 172.31.1.208 0 ms
Reply to request 1 from 172.31.1.216 0 ms
Reply to request 1 from 172.31.1.205 16 ms
::
Reply to request 5 from 172.31.1.209 0 ms
Reply to request 5 from 172.31.1.66 0 ms
Reply to request 5 from 172.31.1.87 0 ms
```

## 检查 IPv6 连接

```
OS10# ping 100::1

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 100::1, timeout is 2 seconds:
!!!!!!
Success rate is 100.0 percent (5/5), round-trip min/avg/max = 0/0/0 (ms)
```

## 跟踪 IPv4 网络路由

```
OS10# traceroute www.Dell Networking.com

Translating "www.Dell Networking.com"...domain server (10.11.0.1) [OK]
Type Ctrl-C to abort.

Tracing the route to www.Dell Networking.com (10.11.84.18),
30 hops max, 40 byte packets

TTL Hostname Probe1 Probe2 Probe3
 1 10.11.199.190 001.000 ms 001.000 ms 002.000 ms
 2 gwegress-sjc-02.Dell Networking.com (10.11.30.126) 005.000 ms 001.000 ms 001.000 ms
 3 fw-sjc-01.Dell Networking.com (10.11.127.254) 000.000 ms 000.000 ms 000.000 ms
 4 www.Dell Networking.com (10.11.84.18) 000.000 ms 000.000 ms 000.000 ms
```

## 跟踪 IPv6 网络路由

```
OS10# traceroute 100::1

Type Ctrl-C to abort.

Tracing the route to 100::1, 64 hops max, 60 byte packets

Hops Hostname Probe1 Probe2 Probe3
 1 100::1 000.000 ms 000.000 ms 000.000 ms

OS10# traceroute 3ffe:501:ffff:100:201:e8ff:fe00:4c8b

Type Ctrl-C to abort.

Tracing the route to 3ffe:501:ffff:100:201:e8ff:fe00:4c8b,
64 hops max, 60 byte packets

Hops Hostname Probe1 Probe2 Probe3
 1 3ffe:501:ffff:100:201:e8ff:fe00:4c8b
 000.000 ms 000.000 ms 000.000 ms
```

## 查看解决方案 ID

作为较大解决方案一部分的 Dell EMC Networking 交换机需要解决方案标识符 (ID)。

要查看解决方案 ID (包括产品基础、产品序列号和产品部件编号)，请使用以下 `show` 命令：

### 查看资源清册

```
OS10# show inventory
```

```

Product : S6000-ON
Description : S6000-ON 32x40GbE QSFP+ Interface Module
Software version : 10.4.9999EX
Product Base : ECS Gen3
Product Serial Number : APM001123456789
Product Part Number : 900-590-001

Unit Type Part Number Rev Piece Part ID Svc Tag Exprs Svc Code

* 1 S4248FB-ON CN-0W1K08-77931-647-0017 OS11SIM 539 375 922 22
 1 S4248FB-ON-PWR-2-AC 02RPHX A00 CN-02RPHX-17972-5BH-00RE
 1 S4248FB-ON-FANTRAY-1 03CH15 A00 CN-03CH15-77931-62T-0039
 1 S4248FB-ON-FANTRAY-2 03CH15 A00 CN-03CH15-77931-62T-0133
 1 S4248FB-ON-FANTRAY-3 03CH15 A00 CN-03CH15-77931-62T-0067
 1 S4248FB-ON-FANTRAY-4 03CH15 A00 CN-03CH15-77931-62T-0034
 1 S4248FB-ON-FANTRAY-5 03CH15 A00 CN-03CH15-77931-62T-0041

```

## 查看许可证状态

```

OS10# show license status
System Information

Vendor Name : Dell EMC
Product Name : S6000-VM
Hardware Version:
Platform Name : x86_64-dell_s6000_vm
PPID : VM0S6000000674000ABCD
Service Tag : OS11SIM
Product Base : ECS Gen3
Product Serial Number : APM001123
Product Part Number : 900-590-0

```

## 查看技术支持详细信息

```

OS10# show tech-support

-----show inventory-----

Product : S6000-ON
Description : S6000-ON 32x40GbE QSFP+ Interface Module
Software version : 10.4.9999EX
Product Base : ECS Gen3
Product Serial Number : APM001123456789
Product Part Number : 900-590-001

<<Output Truncated>>

```



# 查看诊断

使用 show 命令查看系统诊断信息。使用 show hash-algorithm 命令可查看为链路聚合组 (LAG) 和同等成本多路径 (ECMP) 协议配置的当前散列算法。

## 查看环境

```
OS10# show environment
```

| Unit | State | Temperature |
|------|-------|-------------|
| 1    | up    | 43          |

| Thermal sensors |           |                                    |             |
|-----------------|-----------|------------------------------------|-------------|
| Unit            | Sensor-Id | Sensor-name                        | Temperature |
| 1               | 1         | CPU On-Board temp sensor           | 32          |
| 1               | 2         | Switch board temp sensor           | 28          |
| 1               | 3         | System Inlet Ambient-1 temp sensor | 27          |
| 1               | 4         | System Inlet Ambient-2 temp sensor | 25          |
| 1               | 5         | System Inlet Ambient-3 temp sensor | 26          |
| 1               | 6         | Switch board 2 temp sensor         | 31          |
| 1               | 7         | Switch board 3 temp sensor         | 41          |
| 1               | 8         | NPU temp sensor                    | 43          |

## 查看哈希算法

```
OS10# show hash-algorithm
LagAlgo - CRC
EcmpAlgo - CRC
```

## 查看资源清册

```
OS10# show inventory
Product : S4148F-ON
Description : S4148F-ON 48x10GbE, 2x40GbE QSFP+, 4x100GbE QSFP28 Interface
Module
Software version : 10.5.0.0
Product Base
Product Serial Number :
Product Part Number :
```

| Unit | Type                | Part Number | Rev | Piece                    | Part ID | Svc Tag | Exprs |
|------|---------------------|-------------|-----|--------------------------|---------|---------|-------|
| 985  | 006 10              |             |     |                          |         |         |       |
| * 1  | S4148F-ON           | 09H9MN      | X01 | TW-09H9MN-28298-713-0026 | 9531XC2 | 198     |       |
| 1    | S4148F-ON-PWR-1-AC  | 06FKHH      | A00 | CN-06FKHH-28298-6B5-03NY |         |         |       |
| 1    | S4148F-ON-FANTRAY-1 | 0N7MH8      | X01 | TW-0N7MH8-28298-713-0101 |         |         |       |
| 1    | S4148F-ON-FANTRAY-2 | 0N7MH8      | X01 | TW-0N7MH8-28298-713-0102 |         |         |       |
| 1    | S4148F-ON-FANTRAY-3 | 0N7MH8      | X01 | TW-0N7MH8-28298-713-0103 |         |         |       |
| 1    | S4148F-ON-FANTRAY-4 | 0N7MH8      | X01 | TW-0N7MH8-28298-713-0104 |         |         |       |

## 查看系统信息

```
OS10# show system
```

|                |                     |
|----------------|---------------------|
| Node Id        | : 1                 |
| MAC            | : 14:18:77:15:c3:e8 |
| Number of MACs | : 256               |
| Up Time        | : 1 day 00:48:58    |

|                            |           |
|----------------------------|-----------|
| -- Unit 1 --               |           |
| Status                     | : up      |
| System Identifier          | : 1       |
| Down Reason                | : unknown |
| Digital Optical Monitoring | : disable |
| System Location LED        | : off     |
| Required Type              | : S4148F  |
| Current Type               | : S4148F  |

```

Hardware Revision : X01
Software Version : 10.5.0.0
Physical Ports : 48x10GbE, 2x40GbE, 4x100GbE
BIOS : 3.33.0.0-3
System CPLD : 0.4
Master CPLD : 0.10
Slave CPLD : 0.7

-- Power Supplies --
PSU-ID Status Type AirFlow Fan Speed(rpm) Status

1 up AC NORMAL 1 13312 up
2 fail

-- Fan Status --
FanTray Status AirFlow Fan Speed(rpm) Status

1 up NORMAL 1 13195 up
2 up NORMAL 1 13151 up
3 up NORMAL 1 13239 up
4 up NORMAL 1 13239 up

```

## 诊断命令

### location-led interface

更改接口的位置 LED。

|               |                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>location-led interface ethernet {chassis/slot/port[:subport]} {on   off}</code>                                                                      |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>chassis/slot/port[:subport]</code> — 输入以太网接口编号。</li> <li><code>on   off</code> — 将接口 LED 设置为打开或关闭。</li> </ul> |
| <b>默认</b>     | 未配置                                                                                                                                                        |
| <b>命令模式</b>   | EXEC                                                                                                                                                       |
| <b>使用情况信息</b> | 使用此命令可以更改指定接口的位置 LED。                                                                                                                                      |
| <b>示例</b>     | <pre>OS10# location-led interface ethernet 1/1/1 on OS10# location-led interface ethernet 1/1/1 off</pre>                                                  |
| <b>支持的版本</b>  | 10.3.0E or later                                                                                                                                           |

### location-led system

显示系统的定位 LED。

|               |                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>location-led system {node-id   node-id/unit-id} {on   off}</code>                                                                                |
| <b>参数</b>     | <ul style="list-style-type: none"> <li><code>node-id   node-id/unit-id</code> — 输入系统 ID。</li> <li><code>on   off</code> — 将系统 LED 设置为打开或关闭。</li> </ul> |
| <b>默认</b>     | 未配置                                                                                                                                                    |
| <b>命令模式</b>   | EXEC                                                                                                                                                   |
| <b>使用情况信息</b> | 使用此命令可以更改指定系统 ID 的定位 LED。                                                                                                                              |
| <b>示例</b>     | <pre>OS10# location-led system 1 on OS10# location-led system 1 off</pre>                                                                              |

支持的版本 10.3.0E or later

show boot

显示引导分区相关的信息。

- 语法 show boot [detail]
- 参数 detail — (可选) 输入以显示详细信息。
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 使用 boot system 命令为下一次重新引导设置引导分区。
- 示例

```
OS10# show boot
Current system image information:
=====
Type Boot Type Active Standby Next-Boot

Node-id 1 Flash Boot [B] 10.5.0.0 [A] 10.5.0.0 [B] active
```

示例 (详细信息)

```
OS10# show boot detail
Current system image information detail:
=====
Type: Node-id 1
Boot Type: Flash Boot
Active Partition: B
Active SW Version: 10.5.0.0
Active SW Build Version: 10.5.0.270
Active Kernel Version: Linux 4.9.168
Active Build Date/Time: 2019-07-29T23:35:01Z
Standby Partition: A
Standby SW Version: 10.5.0EX
Standby SW Build Version: 10.5.0EX.252
Standby Build Date/Time: 2019-07-27T17:31:55Z
Next-Boot: active[B]
```

支持的版本 10.2.0E or later

show diag

显示端口适配器和模块的诊断信息。

- 语法 show diag
- 参数 无
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 无
- 示例

```
OS10# show diag
00:00.0 Host bridge: Intel Corporation Atom processor C2000 SoC
Transaction Router (rev 02)
00:01.0 PCI bridge: Intel Corporation Atom processor C2000 PCIe Root
Port 1 (rev 02)
00:02.0 PCI bridge: Intel Corporation Atom processor C2000 PCIe Root
Port 2 (rev 02)
00:03.0 PCI bridge: Intel Corporation Atom processor C2000 PCIe Root
Port 3 (rev 02)
00:04.0 PCI bridge: Intel Corporation Atom processor C2000 PCIe Root
Port 4 (rev 02)
```

```

00:0e.0 Host bridge: Intel Corporation Atom processor C2000 RAS (rev 02)
00:0f.0 IOMMU: Intel Corporation Atom processor C2000 RCEC (rev 02)
00:13.0 System peripheral: Intel Corporation Atom processor C2000 SMBus
2.0 (rev 02)
00:14.0 Ethernet controller: Intel Corporation Ethernet Connection I354
(rev 03)
00:14.1 Ethernet controller: Intel Corporation Ethernet Connection I354
(rev 03)
00:16.0 USB controller: Intel Corporation Atom processor C2000 USB
Enhanced Host Controller (rev 02)
00:17.0 SATA controller: Intel Corporation Atom processor C2000 AHCI
SATA2 Controller (rev 02)
00:18.0 SATA controller: Intel Corporation Atom processor C2000 AHCI
SATA3 Controller (rev 02)
00:1f.0 ISA bridge: Intel Corporation Atom processor C2000 PCU (rev 02)
00:1f.3 SMBus: Intel Corporation Atom processor C2000 PCU SMBus (rev 02)
01:00.0 Ethernet controller: Broadcom Corporation Device b340 (rev 01)
01:00.1 Ethernet controller: Broadcom Corporation Device b340 (rev 01)

```

**支持的版本** 10.2.0E or later

## show environment

显示有关环境系统组件的信息，例如温度、风扇和电压。

**语法** show environment

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

**示例**

```

OS10# show environment

Unit State Temperature

1 up 43

Thermal sensors
Unit Sensor-Id Sensor-name Temperature

1 1 CPU On-Board temp sensor 32
1 2 Switch board temp sensor 28
1 3 System Inlet Ambient-1 temp sensor 27
1 4 System Inlet Ambient-2 temp sensor 25
1 5 System Inlet Ambient-3 temp sensor 26
1 6 Switch board 2 temp sensor 31
1 7 Switch board 3 temp sensor 41
1 8 NPU temp sensor 43

```

**支持的版本** 10.2.0E or later

## show hash-algorithm

显示哈希算法信息。

**语法** show hash-algorithm

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

示例

```
OS10# show hash-algorithm
LagAlgo - CRC EcmpAlgo - CRC
```

支持的版本 10.2.0E or later

show inventory

显示系统清单信息。

- 语法 show inventory
- 参数 无
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 无
- 示例

```
OS10# show inventory
Product : S4148F-ON
Description : S4148F-ON 48x10GbE, 2x40GbE QSFP+, 4x100GbE QSFP28 Interfa
Software version : 10.5.0.0
Product Base :
Product Serial Number :
Product Part Number :

Unit Type Part Number Rev Piece Part ID Svc Tag

* 1 S4148F-ON 09H9MN X01 TW-09H9MN-28298-713-0026 9531XC2
 1 S4148F-ON-PWR-1-AC 06FKHH A00 CN-06FKHH-28298-6B5-03NY
 1 S4148F-ON-FANTRAY-1 0N7MH8 X01 TW-0N7MH8-28298-713-0101
 1 S4148F-ON-FANTRAY-2 0N7MH8 X01 TW-0N7MH8-28298-713-0102
 1 S4148F-ON-FANTRAY-3 0N7MH8 X01 TW-0N7MH8-28298-713-0103
 1 S4148F-ON-FANTRAY-4 0N7MH8 X01 TW-0N7MH8-28298-713-0104
```

支持的版本 10.2.0E or later

show processes

查看进程 CPU 利用率信息。

- 语法 show processes node-id node-id-number [pid process-id]
- 参数
  - node-id-number — 将节点 ID 编号输入为 1。
  - process-id — (可选) 输入进程 ID 号, 从 1 到 2147483647。
- 默认 未配置
- 命令模式 EXEC
- 使用情况信息 无
- 示例

```
OS10# show processes node-id 1
top - 09:19:32 up 5 days, 6 min, 2 users, load average: 0.45, 0.39,
0.34
Tasks: 208 total, 2 running, 204 sleeping, 0 stopped, 2 zombie
%Cpu(s): 9.7 us, 3.9 sy, 0.3 ni, 85.8 id, 0.0 wa, 0.0 hi, 0.3 si,
0.0 st
KiB Mem: 3998588 total, 2089416 used, 1909172 free, 143772 buffers
KiB Swap: 399856 total, 0 used, 399856 free. 483276 cached
Mem
 PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+
COMMAND
 9 root 20 0 0 0 0 S 6.1 0.0 5:22.41
rcuos/1
```

|             |       |    |     |        |      |      |   |     |     |         |       |
|-------------|-------|----|-----|--------|------|------|---|-----|-----|---------|-------|
| 819         | snmp  | 20 | 0   | 52736  | 6696 | 4132 | S | 6.1 | 0.2 | 2:44.18 | snmpd |
| 30452       | admin | 20 | 0   | 22076  | 2524 | 2100 | R | 6.1 | 0.1 | 0:00.02 | top   |
| 1           | root  | 20 | 0   | 112100 | 5840 | 3032 | S | 0.0 | 0.1 | 0:12.32 |       |
| systemd     |       |    |     |        |      |      |   |     |     |         |       |
| 2           | root  | 20 | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:00.00 |       |
| kthreadd    |       |    |     |        |      |      |   |     |     |         |       |
| 3           | root  | 20 | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:25.37 |       |
| ksoftirqd/0 |       |    |     |        |      |      |   |     |     |         |       |
| 5           | root  | 0  | -20 | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:00.00 |       |
| kworker/0:+ |       |    |     |        |      |      |   |     |     |         |       |
| 7           | root  | 20 | 0   | 0      | 0    | 0    | R | 0.0 | 0.0 | 5:15.27 |       |
| rcu_sched   |       |    |     |        |      |      |   |     |     |         |       |
| 8           | root  | 20 | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 2:43.64 |       |
| rcuos/0     |       |    |     |        |      |      |   |     |     |         |       |
| 10          | root  | 20 | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:00.00 |       |
| rcu_bh      |       |    |     |        |      |      |   |     |     |         |       |
| 11          | root  | 20 | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:00.00 |       |
| rcuob/0     |       |    |     |        |      |      |   |     |     |         |       |
| 12          | root  | 20 | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:00.00 |       |
| rcuob/1     |       |    |     |        |      |      |   |     |     |         |       |
| 13          | root  | rt | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:07.30 |       |
| migration/0 |       |    |     |        |      |      |   |     |     |         |       |
| 14          | root  | rt | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:02.18 |       |
| watchdog/0  |       |    |     |        |      |      |   |     |     |         |       |
| 15          | root  | rt | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:02.12 |       |
| watchdog/1  |       |    |     |        |      |      |   |     |     |         |       |
| 16          | root  | rt | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:04.98 |       |
| migration/1 |       |    |     |        |      |      |   |     |     |         |       |
| 17          | root  | 20 | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:03.92 |       |
| ksoftirqd/1 |       |    |     |        |      |      |   |     |     |         |       |
| 19          | root  | 0  | -20 | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:00.00 |       |
| kworker/1:+ |       |    |     |        |      |      |   |     |     |         |       |
| 20          | root  | 0  | -20 | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:00.00 |       |
| khelper     |       |    |     |        |      |      |   |     |     |         |       |
| 21          | root  | 20 | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:00.00 |       |
| kdevtmpfs   |       |    |     |        |      |      |   |     |     |         |       |
| 22          | root  | 0  | -20 | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:00.00 | netns |
| 23          | root  | 20 | 0   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:00.41 |       |
| khungtaskd  |       |    |     |        |      |      |   |     |     |         |       |
| 24          | root  | 0  | -20 | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:00.00 |       |
| writeback   |       |    |     |        |      |      |   |     |     |         |       |
| 25          | root  | 25 | 5   | 0      | 0    | 0    | S | 0.0 | 0.0 | 0:00.00 | ksmd  |
| --more--    |       |    |     |        |      |      |   |     |     |         |       |

```

OS10# show processes node-id 1 pid 1019
top - 09:21:58 up 5 days, 8 min, 2 users, load average: 0.18, 0.30, 0.31
Tasks: 1 total, 0 running, 1 sleeping, 0 stopped, 0 zombie
%Cpu(s): 9.7 us, 3.9 sy, 0.3 ni, 85.8 id, 0.0 wa, 0.0 hi, 0.3 si, 0.0 st
KiB Mem: 3998588 total, 2089040 used, 1909548 free, 143772 buffers
KiB Swap: 399856 total, 0 used, 399856 free. 483276 cached
Mem
 PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+
COMMAND
 1019 root 20 0 1829416 256080 73508 S 6.6 6.4 1212:36
base_nas
OS10#

```

**支持的版本** 10.3.0E or later

## show system

显示系统信息。

**语法** show system [brief | node-id]

- 参数**
- brief — 查看系统信息的缩写列表。
  - node-id — 查看节点 ID 号。

默认  
命令模式  
使用情况信息  
示例

未配置  
EXEC  
无

```
OS10# show system

Node Id : 1
MAC : 14:18:77:15:c3:e8
Number of MACs : 256
Up Time : 1 day 00:48:58

-- Unit 1 --
Status : up
System Identifier : 1
Down Reason : unknown
Digital Optical Monitoring : disable
System Location LED : off
Required Type : S4148F
Current Type : S4148F
Hardware Revision : X01
Software Version : 10.5.0.0
Physical Ports : 48x10GbE, 2x40GbE, 4x100GbE
BIOS : 3.33.0.0-3
System CPLD : 0.4
Master CPLD : 0.10
Slave CPLD : 0.7

-- Power Supplies --
PSU-ID Status Type AirFlow Fan Speed(rpm) Status

1 up AC NORMAL 1 13312 up
2 fail

-- Fan Status --
FanTray Status AirFlow Fan Speed(rpm) Status

1 up NORMAL 1 13195 up
2 up NORMAL 1 13151 up
3 up NORMAL 1 13239 up
4 up NORMAL 1 13239 up
```

示例 (node-id)

```
OS10# show system node-id 1 fanout-configured

Interface Breakout capable Breakout state

Eth 1/1/5 No BREAKOUT_1x1
Eth 1/1/6 No BREAKOUT_1x1
Eth 1/1/7 No BREAKOUT_1x1
Eth 1/1/8 No BREAKOUT_1x1
Eth 1/1/9 No BREAKOUT_1x1
Eth 1/1/10 No BREAKOUT_1x1
Eth 1/1/11 No BREAKOUT_1x1
Eth 1/1/12 No BREAKOUT_1x1
Eth 1/1/13 No BREAKOUT_1x1
Eth 1/1/14 No BREAKOUT_1x1
Eth 1/1/15 No BREAKOUT_1x1
Eth 1/1/16 No BREAKOUT_1x1
Eth 1/1/17 No BREAKOUT_1x1
Eth 1/1/18 No BREAKOUT_1x1
Eth 1/1/19 No BREAKOUT_1x1
Eth 1/1/20 No BREAKOUT_1x1
Eth 1/1/21 No BREAKOUT_1x1
Eth 1/1/22 No BREAKOUT_1x1
Eth 1/1/23 No BREAKOUT_1x1
```

|            |     |              |
|------------|-----|--------------|
| Eth 1/1/24 | No  | BREAKOUT_1x1 |
| Eth 1/1/25 | Yes | BREAKOUT_1x1 |

### 示例 (brief)

```
OS10# show system brief

Node Id : 1
MAC : 14:18:77:15:c3:e8

-- Unit --
Unit Status ReqType CurType Version

1 up S4148F S4148F 10.5.0EX

-- Power Supplies --
PSU-ID Status Type AirFlow Fan Speed(rpm) Status

1 up AC NORMAL 1 13312 up
2 fail

-- Fan Status --
FanTray Status AirFlow Fan Speed(rpm) Status

1 up NORMAL 1 13195 up
2 up NORMAL 1 13151 up
3 up NORMAL 1 13239 up
4 up NORMAL 1 13239 up
```

**支持的版本** 10.2.0E or later

## traceroute

显示数据包传输到 IP 地址所用的路由。

**语法**

```
traceroute [vrf {management | vrf-name}] host [-46dFITnreAUDV] [-f first_ttl] [-g gate,...] [-i device] [-m max_ttl] [-N squeries] [-p port] [-t tos] [-l flow_label] [-w waittime] [-q nqueries] [-s src_addr] [-z sendwait] [--fwmark=num] host [packetlen]
```

- 参数**
- `vrf management` — (可选) 将路由跟踪到管理 VRF 实例中的 IP 地址。
  - `vrf vrf-name` — (可选) 将路由跟踪到指定 VRF 实例中的 IP 地址。
  - `host` — 输入用于跟踪数据包的主机。
  - `-i interface` — (可选) 输入用于跟踪路由发送数据包的接口的 IP 地址。默认情况下，根据路由表选择接口。
  - `-m max_ttl` — (可选) 输入跟踪路由探测的最大生存时间值的最大跳数。默认值为 30。
  - `-p port` — (可选) 输入目标端口：
    - 对于 UDP 跟踪，请输入跟踪路由使用的目标端口基座。每个探测都会增加目标端口号。
    - 对于 ICMP 跟踪，请输入初始 ICMP 顺序值，每次探测进行增量。
    - 对于 TCP 跟踪，输入要连接的常数目标端口。
    - `-P protocol` — (可选) 使用指定协议的原始数据包进行跟踪路由。默认协议为 253 (RFC 3692)。
    - `-s source_address` — (可选) 输入其中一个接口的备用源地址。默认情况下，使用传出接口的地址。
    - `-q nqueries` — (可选) 输入每跳的探测数据包数。默认值为 3。
    - `-N squeries` — (可选) 输入同时发送出去以加速跟踪路由的探测数据包数量。默认值为 16。
    - `-t tos` — (可选) 对于 IPv4，输入要使用的服务类型 (ToS) 和优先级值。16 可设置低延迟；8 可设置高吞吐量。
    - `-UL` — (可选) 将 UDPLITE 用于跟踪路由。默认端口是 53。
    - `-w waittime` — (可选) 输入等待探测响应的的时间 (以秒为单位)。默认值为 5 秒。



- `-z sendwait` — (可选) 输入两次探测之间等待的最短时间间隔。默认值为 0。大于 10 的值指定的值以毫秒为单位, 否则指定的值以秒为单位。当路由器速率限制 ICMP 消息时, 此选项非常有用。
- `--mtu` — (可选) 从正在跟踪的路径中查找最大传输单元 (MTU)。
- `--back` — (可选) 根据转发方向, 打印反向跳转的数量。
- `host` — (必填) 输入目标设备的名称或 IP 地址。
- `packet_len` — (可选) 输入探测数据包的总大小。对于 IPv4, 默认值为 60 字节, IPv6 为 80。

|        |      |
|--------|------|
| 默认     | 未配置  |
| 命令模式   | EXEC |
| 使用情况信息 | 无    |
| 示例     |      |

```
OS10# traceroute www.dell.com
traceroute to www.dell.com (23.73.112.54), 30 hops max, 60 byte packets
 1 10.11.97.254 (10.11.97.254) 4.298 ms 4.417 ms 4.398 ms
 2 10.11.3.254 (10.11.3.254) 2.121 ms 2.326 ms 2.550 ms
 3 10.11.27.254 (10.11.27.254) 2.233 ms 2.207 ms 2.391 ms
 4 Host65.hbms.com (63.80.56.65) 3.583 ms 3.776 ms 3.757 ms
 5 host33.30.198.65 (65.198.30.33) 3.758 ms 4.286 ms 4.221 ms
 6 3.GigabitEthernet3-3.GW3.SCL2.ALTER.NET (152.179.99.173) 4.428 ms
 2.593 ms 3.243 ms
 7 0.xe-7-0-1.XL3.SJC7.ALTER.NET (152.63.48.254) 3.915 ms 3.603 ms
 3.790 ms
 8 TenGigE0-4-0-5.GW6.SJC7.ALTER.NET (152.63.49.254) 11.781 ms 10.600
ms 9.402 ms
 9 23.73.112.54 (23.73.112.54) 3.606 ms 3.542 ms 3.773 ms
```

### 示例 (IPv6)

```
OS10# traceroute 20::1
traceroute to 20::1 (20::1), 30 hops max, 80 byte packets
 1 20::1 (20::1) 2.622 ms 2.649 ms 2.964 ms
```

支持的版本 10.2.0E or later

## 恢复 Linux 密码

如果丢失或忘记了 Linux 管理员密码, 您可以在 CONFIGURATION 模式下使用 `system-user linuxadmin password {clear-text-password | hashed-password}` 命令以从 CLI 进行重新配置。使用 `write memory` 命令保存密码。例如:

```
OS10(config)# system-user linuxadmin password Dell@Force10!@
OS10(config)# exit
OS10# write memory
```

有关详情, 请参阅 [Linux 管理员用户配置](#)。

如果同时丢失 OS10 用户和 Linux 管理员密码, 使您无法登录到 CLI, 则必须从 GRUB 恢复 linuxadmin 密码:

1. 连接到串行控制台端口。串行设置为 115200 波特、8 数据位和无奇偶校验。
2. 重新引导或开启系统。
3. 在 Grub 提示符中按 **ESC** 键可查看引导菜单。默认情况下 OS10-A 分区已选择。

```
+-----+
| *OS10-A |
| OS10-B |
| ONIE |
+-----+
```

4. 按 **e** 键以打开 OS10 GRUB 编辑器。
5. 使用箭头键导航到以 `linux` 开头的行的末尾。在行末尾添加 `init=/bin/bash`。

```
+-----+
|-----|
```

```
|setparams 'OS10-
A'
|
|
| set
root='(hd0,gpt7)'
|
| echo 'Loading
OS10 ...'
| linux (hd0,gpt7)/boot/os10.linux console=ttyS0,115200 root=/dev/sda7 \rw init=/
bin/bash |
| initrd (hd0,gpt7)/boot/
os10.initrd
+-----+
+-----+
```

- 按 **Ctrl + x** 以重新引导系统。如果 **Ctrl + x** 不会导致系统重新引导，请按 **Alt + 0**。系统将在没有密码的情况下引导至根 shell。

- 在根提示符处，输入 `usermod -s /bin/bash linuxadmin` 以启用 `linuxadmin` 用户。

```
root@OS10: /# usermod -s /bin/bash linuxadmin
```

- 通过输入 `passwd -s linuxadmin` 命令来验证 `linuxadmin` 密码状态。

如果密码处于锁定状态，在命令输出中将显示 `linuxadmin` 后跟 `L`。通过输入 `passwd -u linuxadmin` 命令来解锁密码。

```
root@OS10:~# passwd -S linuxadmin
linuxadmin L 10/01/2018 0 99999 7 -1

root@OS10:~# passwd -u linuxadmin
passwd: password expiry information changed.
```

- 在根提示符处，输入 `linuxadmin` 作为用户名。

```
root@OS10: /# linuxadmin
```

- 使用 `/opt/dell/os10/bin/recover_linuxadmin_password.sh plain-password` 命令配置密码。以纯文本形式输入 `linuxadmin` 密码。

```
root@OS10: /# /opt/dell/os10/bin/recover_linuxadmin_password.sh Dell@admin0!@
```

- 输入 `sync` 命令以保存新密码。

```
root@OS10: /# sync
```

- 重新引导系统，然后输入新密码。

```
root@OS10: /# reboot -f
Rebooting.[822.327073] sd 0:0:0:0: [sda] Synchronizing SCSI cache

[822.340656] reboot: Restarting system

[822.344339] reboot: machine restart
BIOS (Dell Inc) Boot Selector
S6010-ON (SI) 3.20.0.3 (32-port TE/FG)
```

## 恢复 OS10 用户名密码

如果丢失或忘记了 OS10 的用户名密码（包括 `admin` 密码），则可以通过执行以下步骤来恢复它。

- 连接到串行控制台端口。串行设置为 115200 波特、8 数据位和无奇偶校验。
- 重新引导或开启系统。



```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```

* Dell EMC Network Operating System (OS10) *-
* *-
*- Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved. *-
* *-

```

This product is protected by U.S. and international copyright and intellectual property laws. Dell EMC and the Dell EMC logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

```
s4048t-1# configure terminal
s4048t-1(config)#
```

9. 在 CONFIGURATION 模式下使用 `username password role` 命令配置用户名称的已恢复密码；例如：

```
s4048t-1(config)# username admin password admin12345 role sysadmin
```

## 还原出厂默认设置

要还原系统出厂默认设置，请将系统重新引导至 ONIE: Uninstall OS 模式。

 **小心：**恢复出厂默认设置会擦除所有已安装的操作系统，并且需要很长时间来擦除存储。

如果无法恢复已安装操作系统的出厂默认设置，请从 Grub 菜单重新引导系统，然后选择 ONIE: Rescue。ONIE Rescue 会绕过已安装的操作系统，并将系统引导至 ONIE，直至您重新引导系统。ONIE Rescue 完成后，系统将重置并引导至 ONIE 控制台。

1. 使用 ONIE: Uninstall OS 命令从 Grub 菜单恢复系统上的出厂默认设置。要选择突出显示的条目，请使用向上和向下箭头键。

```
+-----+
| ONIE: Install OS |
| ONIE: Rescue |
| *ONIE: Uninstall OS |
| ONIE: Update ONIE |
| ONIE: Embed ONIE |
| ONIE: Diag ONIE |
+-----+
```

2. 按 **Enter** 键以激活控制台。  
3. 使用 `onie-uninstaller` 命令返回默认 ONIE 设置。

```
ONIE:/ # onie-uninstaller
uninstallerErasing internal mass storage device: /dev/sda4 (32MB)
 Percent complete: 100%
Erase complete.
Deleting partition 4 from /dev/sda
Erasing internal mass storage device: /dev/sda5 (300MB)
 Percent complete: 100%
Erase complete.
Deleting partition 5 from /dev/sda
Erasing internal mass storage device: /dev/sda6 (300MB)
 Percent complete: 100%
Erase complete.
Deleting partition 6 from /dev/sda
Erasing internal mass storage device: /dev/sda7 (12461MB)
 Percent complete: 100%
Erase complete.
Deleting partition 7 from /dev/sda
```

```
Installing for i386-pc platform.
Installation finished. No error reported.
Uninstall complete. Rebooting...
ONIE:/ # discover: Rescue mode detected. No discover stopped.
Stopping: dropbear ssh daemon... done.
Stopping: telnetd... done.
Stopping: syslogd... done.
Info: Unmounting kernel filesystems
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL tosd 4:0:0:0: [sda] Synchronizing SCSI cache
Restarting system.
machine restart
```

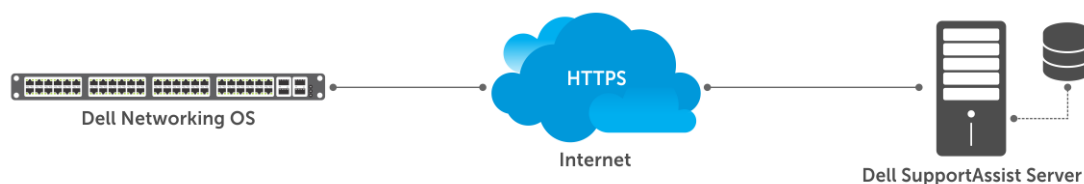
## SupportAssist

SupportAssist 功能可监控网络中运行 Dell EMC Networking 操作系统的设备。此功能通过以下方式为您的 IT 支持功能提供额外的服务层：

- 识别问题并帮助您快速解决问题。
- 主动监控网络并更大限度减少停机风险。

SupportAssist 会定期从网络设备收集有关配置、清单、日志等的信息。它会将这些信息安全地发送到集中式 Dell EMC SupportAssist 基础架构服务器，在此部分中称为 SupportAssist 服务器。Dell EMC SupportAssist 基础架构服务将指定收集数据的结构化格式。如果失败，SupportAssist 会自动创建支持案例。您可以通过电子邮件收到有关案例详细信息的通知。

SupportAssist 通过互联网与 SupportAssist 服务器通信，并按安排的时间间隔上传故障处理信息。



**注：**当您从旧版本（低于版本 10.5.0.0）升级，交换机不会保留 SupportAssist 配置。升级完成后，再次启用并配置 SupportAssist。您必须重新配置 SupportAssist，因为 OS10 交换机（从版本 10.5.0.0 开始）连接到其他 Dell EMC 服务器，您必须接受 EULA 并再次重新配置服务器。

但是，如果您使用的是内部网关（SupportAssist Enterprise 或 SAE），则不需要重新配置 SupportAssist。SAE 不需要 OS10 交换机上的任何 SupportAssist 配置。

## 重要事项

- Dell EMC 为大规模部署提供 SupportAssist Enterprise。
  - SupportAssist Enterprise 要求您部署 SupportAssist Enterprise 网关服务器。请参阅 [SupportAssist Enterprise 说明文件](#) 以了解更多信息。
  - 如果您不想部署 SupportAssist Enterprise 网关服务器，则可以在 OS10 交换机上配置 SupportAssist。有关详细信息，请参阅 [配置 SupportAssist](#) 部分。
- 在 OS10 交换机上配置 SupportAssist 需要与 SupportAssist 服务器建立互联网连接。如果网络中断，SupportAssist 会忽略在停机期间收集的信息。当互联网连接恢复后，SupportAssist 会生成警报。
- 在配置 SupportAssist 之前，您必须接受 SupportAssist 终端用户许可协议 (EULA)。
- 如果 SupportAssist 服务器使用域名配置，请确保该网络设备有权访问域名服务器 (DNS)。此版本只支持 IPv4 寻址。
- 此功能使用 show 命令收集调试信息。使用 show 命令可能会影响 CPU 的使用情况。
- 系统将 show 命令输出存储在 .zip 文件中。.zip 文件的大小取决于 show 命令输出。

## 配置 SupportAssist

如果 OS10 交换机驻留在防火墙后面，请打开防火墙上的端口 443，以获得以下 SupportAssist 服务器的出站连接：

- <https://esrs3.emc.com>

- <https://esrs3-dr.emc.com>

1. 进入配置模式。

```
OS10# configure terminal
OS10(config)#
```

2. 接受 EULA。

```
OS10(config)# eula-consent support-assist accept
```

3. 从 CONFIGURATION 模式进入 SupportAssist 模式。

```
OS10(config)# support-assist
OS10(conf-support-assist)#
```

4. (必需) 在 SUPPORT-ASSIST 模式下指定 SupportAssist 服务器 URL 或 IP 地址, 并指定 Dell Digital Locker (DDL) 凭据以访问 SupportAssist 服务器。此帐户必须有权访问 DDL 中的 OS10 交换机。您可以输入 `default` 来指定 SUPPORTASSIST 服务器 URL (<https://esrs3.emc.com>)。

```
OS10(conf-support-assist)# server url default username example-username password
example-password
```

或

```
OS10(conf-support-assist)# server url https://domain username example-username
password example-password
```

5. (必需) 在 SUPPORT-ASSIST 模式下将接口配置为连接到 SupportAssist 服务器。

```
OS10(conf-support-assist)# source-interface interface
```

6. (必需) 在 SUPPORT-ASSIST 模式下配置贵公司的联系信息。

```
OS10(conf-support-assist)# contact-company name ExampleCompanyName
OS10(conf-support-assist-ExampleCompanyName)#
```

7. 在 EXEC 模式下立即或在安排的时间触发活动。

```
OS10# support-assist-activity full-transfer {start-now | schedule [hourly | daily |
weekly | monthly | yearly]}
```

## 移除 SupportAssist 安排

```
OS10# no support-assist-activity full-transfer schedule
```

## 设置公司名称

配置名称、地址和区域信息。Dell EMC 技术支持将使用此信息来确定哪个公司拥有该设备。

1. (必需) 在 SUPPORT-ASSIST 模式下配置联系信息。

```
OS10(conf-support-assist)# contact-company name example-company-name
```

2. (必需) 在 SUPPORT-ASSIST 模式下配置地址信息。使用双引号在城市或省/自治区名称中添加空格。使用 `no address` 命令可移除配置。输入 ? 可查看受支持的国家/地区名称和代码的列表。您还可以在以下位置找到此信息: [国家/地区名称和代码](#)。

```
OS10(conf-support-assist-example-company-name)# address city city-name state state-
name country country-code zipcode number
```

3. (必需) 在 SUPPORT-ASSIST 模式下配置街道地址信息。使用双引号在地址中添加空格。使用 `no street-address` 命令可移除配置。

```
OS10(conf-support-assist-example-company-name)# street-address {address-line-1}
[address-line-2 address-line-3]
```

4. (可选) 在 SUPPORT-ASSIST 模式下配置区域。使用 `no territory` 命令可移除配置。

```
OS10(conf-support-assist-example-company-name)# territory company-territory
```

### 配置 SupportAssist 公司

```
OS10(conf-support-assist)# contact-company name ExampleCompanyName
OS10(conf-support-assist-ExampleCompanyName)# address city San Jose state California
country USA zipcode 95125
OS10(conf-support-assist-ExampleCompanyName)# street-address "123 Example Street" "Bldg
999"
OS10(conf-support-assist-ExampleCompanyName)# territory Sales
```

## 设置联系信息

在 SUPPORT-ASSIST 模式下配置联系详细信息。您可以设置名称、电子邮件地址、电话和首选联系方式。

1. 需要在 SUPPORT-ASSIST 模式下输入联系人姓名。

```
OS10(config)# support-assist
OS10(conf-support-assist)# contact-company name ExampleCompanyName
OS10(conf-support-assist-ExampleCompanyName)# contact-person first firstname last
lastname
```

2. 需要在 SUPPORT-ASSIST 模式中输入电子邮件地址。

```
OS10(conf-support-assist-ExampleCompanyName)# email-address primary email-address
[alternate alternate-email-address]
```

您可以选择配置备用电子邮件地址。

3. (可选) 在 SUPPORT-ASSIST 模式下输入首选的联系方法。

```
OS10(conf-support-assist-ExampleCompanyName-firstnamelastname)# preferred-method
{email | phone | no-contact}
```

4. (必需) 在 SUPPORT-ASSIST 模式下输入联系人电话号码。电话号码的最小长度为九位数字。

```
OS10(conf-support-assist-ExampleCompanyName)# phone primary number [alternate number]
```

您可以选择配置备用电话号码。

### 配置联系人详细信息

```
OS10(config)# support-assist
OS10(conf-support-assist)# contact-company name ExampleCompanyName
OS10(conf-support-assist-ExampleCompanyName)# contact-person first Firstname last
Lastname
OS10(conf-support-assist-ExampleCompanyName)# email-address primary
youremail@example.com alternate alternate_email@example.com
OS10(conf-support-assist-ExampleCompanyName-FirstnameLastname)# preferred-method email
OS10(conf-support-assist-ExampleCompanyName)# phone primary 000-123-4567 alternate
123-456-7890
```

## 安排活动

为完整数据传输安排时间。

- ① **注：**当开始完全数据传输时，SupportAssist 将与用户 `mgmt_evt_user` 一起打开 SSH 会话以收集数据。运行 `show sessions` 命令以查看活动用户会话的列表时，系统也会显示 `mgmt_evt_user` 会话。SupportAssist 需要激活此会话才能收集数据。中止此会话会停止数据收集。

- 在 EXEC 模式下配置完全传输或日志传输活动。

```
OS10# support-assist-activity {full-transfer} schedule {hourly | daily | weekly |
monthly | yearly}
```

- hourly min number— 输入安排每小时任务的时间，从 0 到 59。
- daily hour number min number— 输入安排每天任务的时间，从 0 到 23 小时以及 0 到 59 分钟。
- weekly day-of-week number hour number min number— 输入安排每周任务的时间，从 0 到 6 天、0 到 23 小时以及 0 到 59 分钟。
- monthly day number hour number min number— 输入安排每月任务的时间，从 1 到 31 天、0 到 23 小时以及 0 到 59 分钟。
- yearly month number day number hour number min number— 输入安排每年任务的时间，从 1 到 12 个月、1 到 31 天、0 到 23 小时以及 0 到 59 分钟。

为完整传输配置活动安排

```
OS10# support-assist-activity full-transfer schedule daily hour 22 min 50
OS10# support-assist-activity full-transfer schedule weekly day-of-week 6 hour 22 min 30
OS10# support-assist-activity full-transfer schedule monthly day 15 hour 12 min 30
```

设置默认活动计划

```
OS10(conf-support-assist)# no support-assist-activity full-transfer schedule
```

查看状态

使用以下 show 命令查看 SupportAssist 配置状态、详细信息和 EULA 信息：

- 在 EXEC 模式下查看 SupportAssist 活动。

```
show support-assist status
```

- 在 EXEC 模式下查看 EULA 许可协议。

```
show support-assist eula
```

查看 SupportAssist 状态

```
OS10# show support-assist status
EULA support-assist : Accepted
Service : Enabled
Contact-Company : ExampleCompanyName
Street Address : Olympia
City : SanJose
State : California
Country : USA
Zipcode : 95123
Territory : West
Contact-person : Firstname Lastname
Primary email : youremail@example.com
Alternate email : emailid@example.com
Primary phone : 000-123-4567
Alternate phone : 777777777
Contact method : email
Server(configured) : default

Activity Enable State :
 Activity State

 full-transfer Enabled
 event-notification Enabled

Scheduled Activity List :
 Activity Schedule Schedule created on

 full-transfer None Never
```



| Activity Status :<br>Activity                      | Status  | last start          | last success |
|----------------------------------------------------|---------|---------------------|--------------|
| -----                                              | -----   | -----               | -----        |
| full-transfer<br>16:15:19                          | Success | 2019-06-13 16:08:51 | 2019-06-13   |
| event-notification<br>16:04:39                     | Success | 2019-06-13 16:04:35 | 2019-06-13   |
| keep-alive<br>17:30:03                             | Success | 2019-06-13 18:00:00 | 2019-06-13   |
| Server Status :                                    |         |                     |              |
| Last KeepAlive Status : Failed                     |         |                     |              |
| Last KeepAlive Successful at : 2019-06-13 17:30:03 |         |                     |              |
| Last KeepAlive Failed at : 2019-06-13 18:00:03     |         |                     |              |
| Last MFT Status : Success                          |         |                     |              |
| Last MFT Successful at : 2019-06-13 16:15:19       |         |                     |              |
| Last MFT Failed at : Never                         |         |                     |              |

## 查看 EULA 许可证

```
OS10# show support-assist eula
SUPPORTASSIST ENTERPRISE - SOFTWARE TERMS
*** IMPORTANT INFORMATION - PLEASE READ CAREFULLY ***
This SupportAssist Software ("Software") contains computer programs and other
proprietary material and information, the
use of which is governed by and expressly conditioned upon acceptance of this
SupportAssist Enterprise Software
Terms ("Agreement"). This Agreement is a legally binding agreement between the entity
that has obtained the
Software ("You" or "Customer") and Provider (which may be a Dell Inc. Affiliate or an
authorized reseller ("Reseller")),
as explained below). If you are acting on behalf of a U.S. Federal Government agency,
please stop installing the
Software and contact your sales account representative.
.
.
.
<<Output Truncated>>
```

## 国家/地区名称和代码的列表

本部分提供了您必须在 `address` 命令中使用的国家/地区代码列表。

**表. 106: 国家/地区名称和代码**

| 国家/地区名称 | 国家/地区代码 |
|---------|---------|
| 阿富汗     | AFG     |
| 奥兰群岛    | ALA     |
| 阿尔巴尼亚   | ALB     |
| 阿尔及利亚   | DZA     |
| 美属萨摩亚群岛 | ASM     |
| 安道尔     | AND     |
| 安哥拉     | AGO     |
| 安圭拉     | AIA     |
| 南极洲     | ATA     |
| 安提瓜和巴布达 | ATG     |
| 阿根廷     | ARG     |
| 亚美尼亚    | ARM     |

表. 106: 国家/地区名称和代码 (续)

| 国家/地区名称        | 国家/地区代码 |
|----------------|---------|
| 阿鲁巴            | ABW     |
| 澳大利亚           | AUS     |
| 奥地利            | AUT     |
| 阿塞拜疆           | AZE     |
| 巴哈马            | BHS     |
| 巴林             | BHR     |
| 孟加拉国           | BGD     |
| 巴巴多斯           | BRB     |
| 白俄罗斯           | BLR     |
| 比利时            | BEL     |
| 伯利兹            | BLZ     |
| 贝宁             | BEN     |
| 百慕大            | BMU     |
| 不丹             | BTN     |
| 多民族玻利维亚国       | BOL     |
| 博内尔岛、圣尤斯特歇斯和塞巴 | BES     |
| 波斯尼亚和黑塞哥维那     | BIH     |
| 博茨瓦纳           | BWA     |
| 布韦岛            | BVT     |
| 巴西             | BRA     |
| 英属印度洋领地        | IOT     |
| 文莱达鲁萨兰国        | BRN     |
| 保加利亚           | BGR     |
| 布基纳法索          | BFA     |
| 布隆迪            | BDI     |
| 柬埔寨            | KHM     |
| 喀麦隆            | CMR     |
| 加拿大            | CAN     |
| 佛得角            | CPV     |
| 开曼群岛           | CYM     |
| 中非共和国          | CAF     |
| 乍得             | TCD     |
| 智利             | CHL     |
| 中国             | CHN     |
| 圣诞岛            | CXR     |
| 科科斯（基林）群岛      | CCK     |
| 哥伦比亚           | COL     |

表. 106: 国家/地区名称和代码 (续)

| 国家/地区名称         | 国家/地区代码 |
|-----------------|---------|
| Comoros         | COM     |
| 刚果              | COGCG   |
| 刚果民主共和国         | COD     |
| 库克群岛            | COK     |
| 哥斯达黎加           | CRI     |
| Côte d'Ivoire   | CIV     |
| 克罗地亚            | HRV     |
| 古巴              | CUB     |
| Curaçao         | CUW     |
| 塞浦路斯            | CYP     |
| 捷克共和国           | CZE     |
| 丹麦              | DNK     |
| 吉布提             | DJI     |
| 多米尼加            | DMA     |
| 多米尼加共和国         | DOM     |
| 厄瓜多尔            | ECU     |
| 埃及              | EGY     |
| 萨尔瓦多            | SLV     |
| 赤道几内亚           | GNQ     |
| 厄立特里亚           | ERI     |
| 爱沙尼亚            | EST     |
| 埃塞俄比亚           | ETH     |
| 福克兰群岛 (马尔维纳斯群岛) | FLK     |
| 法罗群岛            | FRO     |
| 斐济              | FJI     |
| 芬兰              | FIN     |
| 法国              | FRA     |
| 法属圭亚那           | GUF     |
| 法属波利尼西亚         | PYF     |
| 法属南部和南极领地       | ATF     |
| 加蓬              | GAB     |
| 冈比亚             | GMB     |
| 格鲁吉亚            | GEO     |
| 德国              | DEU     |
| 加纳              | GHA     |
| 直布罗陀            | GIB     |
| 希腊              | GRC     |

表. 106: 国家/地区名称和代码 (续)

| 国家/地区名称     | 国家/地区代码 |
|-------------|---------|
| 格陵兰         | GRL     |
| 格林纳达        | GRD     |
| 瓜德罗普        | GLP     |
| 关岛          | GUM     |
| 危地马拉        | GTM     |
| 根西岛         | GGY     |
| 几内亚         | GIN     |
| 几内亚比绍       | GNB     |
| 圭亚那         | GUY     |
| 海地          | HTI     |
| 赫德和麦克唐纳群岛   | HMD     |
| 梵蒂冈 (梵蒂冈城国) | VAT     |
| 洪都拉斯        | HND     |
| 香港          | HKG     |
| 匈牙利         | HUN     |
| 冰岛          | ISL     |
| 印度          | IND     |
| 印度尼西亚       | IDN     |
| 伊朗伊斯兰共和国    | IRN     |
| 伊拉克         | IRQ     |
| 爱尔兰         | IRL     |
| 马恩岛         | IMN     |
| 以色列         | ISR     |
| 意大利         | ITA     |
| 牙买加         | JAM     |
| 日本          | JPN     |
| 泽西          | JEY     |
| 约旦          | JOR     |
| 哈萨克斯坦       | KAZ     |
| 肯尼亚         | KEN     |
| 基里巴斯        | KIR     |
| 韩国民主人民共和国   | PRK     |
| 韩国          | KOR     |
| 科威特         | KWT     |
| 吉尔吉斯斯坦      | KGZ     |
| 老挝人民民主共和国   | LAO     |
| 拉脱维亚        | LVA     |

表. 106: 国家/地区名称和代码 (续)

| 国家/地区名称      | 国家/地区代码 |
|--------------|---------|
| 黎巴嫩          | LBN     |
| 莱索托          | LSO     |
| 利比里亚         | LBR     |
| 利比亚          | LBY     |
| 列支敦士登        | LIE     |
| 立陶宛          | LTU     |
| 卢森堡          | LUX     |
| (中国) 澳门特别行政区 | MAC     |
| 马其顿共和国       | MKD     |
| 马达加斯加        | MDG     |
| 马拉维          | MWI     |
| 马来西亚         | MYS     |
| 马尔代夫         | MDV     |
| 马里           | MLI     |
| 马耳他          | MLT     |
| 马绍尔群岛        | MHL     |
| 马提尼克         | MTQ     |
| 毛里塔尼亚        | MRT     |
| 毛里求斯         | MUS     |
| 马约特          | MYT     |
| 墨西哥          | MEX     |
| 密克罗尼西亚联邦     | FSM     |
| 摩尔多瓦         | MDA     |
| 摩纳哥          | MCO     |
| 蒙古国          | MNG     |
| 黑山共和国        | MNE     |
| 蒙特塞拉特        | MSR     |
| 摩洛哥          | MAR     |
| 莫桑比克         | MOZ     |
| 缅甸           | MMR     |
| 纳米比亚         | NAM     |
| 瑙鲁           | NRU     |
| 尼泊尔          | NPL     |
| 荷兰           | NLD     |
| 新喀里多尼亚       | NCL     |
| 新西兰          | NZL     |
| 尼加拉瓜         | NIC     |

表. 106: 国家/地区名称和代码 (续)

| 国家/地区名称           | 国家/地区代码 |
|-------------------|---------|
| 尼日尔               | NER     |
| 尼日利亚              | NGA     |
| 纽埃岛               | NIU     |
| 诺福克岛              | NFK     |
| 北马里亚纳群岛           | MNP     |
| 挪威                | NOR     |
| 阿曼                | OMN     |
| 巴基斯坦              | PAK     |
| 帕劳                | PLW     |
| 巴勒斯坦国             | PSE     |
| 巴拿马               | PAN     |
| 巴布亚新几内亚           | PNG     |
| 巴拉圭               | PRY     |
| 秘鲁                | PER     |
| 菲律宾               | PHL     |
| 皮特凯恩群岛            | PCN     |
| 波兰                | POL     |
| 葡萄牙               | PRT     |
| 波多黎各              | PRI     |
| 卡塔尔               | QAT     |
| RÄ©union          | REU     |
| 罗马尼亚              | ROU     |
| 俄罗斯               | RUS     |
| 卢旺达               | RWA     |
| Saint BarthÄ©lemy | BLM     |
| 圣赫勒拿、阿森松和特里斯坦达库尼亚 | SHN     |
| 圣基茨和尼维斯           | KNA     |
| 圣卢西亚              | LCA     |
| 法属圣马丁             | MAF     |
| 圣皮埃尔和密克隆          | SPM     |
| 圣文森特和格林纳丁斯        | VCT     |
| 萨摩亚               | WSM     |
| 圣马力诺              | SMR     |
| 圣多美和普林西比          | STP     |
| 沙特阿拉伯             | SAU     |
| 塞内加尔              | SEN     |
| 塞尔维亚              | SRB     |

表. 106: 国家/地区名称和代码 (续)

| 国家/地区名称     | 国家/地区代码 |
|-------------|---------|
| 塞舌尔         | SYC     |
| 塞拉利昂        | SLE     |
| 新加坡         | SGP     |
| 荷兰属圣马丁      | SXM     |
| 斯洛伐克        | SVK     |
| 斯洛文尼亚       | SVN     |
| 所罗门群岛       | SLB     |
| 索马里         | SOM     |
| 南非          | ZAF     |
| 南乔治亚和南桑威奇群岛 | SGS     |
| 南苏丹         | SSD     |
| 西班牙         | ESP     |
| 斯里兰卡        | LKA     |
| 苏丹          | SDN     |
| 苏里南         | SUR     |
| 斯瓦巴和扬马延     | SJM     |
| 斯威士兰        | SWZ     |
| 瑞典          | SWE     |
| 瑞士          | CHE     |
| 阿拉伯叙利亚共和国   | SYR     |
| (中国) 台湾地区   | TWN     |
| 塔吉克斯坦       | TJK     |
| 坦桑尼亚        | TZA     |
| 泰国          | THA     |
| 东帝汶落地       | TLS     |
| 多哥          | TGO     |
| 托克劳         | TKL     |
| 汤加          | TON     |
| 特立尼达和多巴哥    | TTO     |
| 突尼斯         | TUN     |
| 土耳其         | TUR     |
| 土库曼斯坦       | TKM     |
| 特克斯和凯科斯群岛   | TCA     |
| 图瓦卢         | TUV     |
| 乌干达         | UGA     |
| 乌克兰         | UKR     |
| 阿拉伯联合酋长国    | ARE     |

表. 106: 国家/地区名称和代码 (续)

| 国家/地区名称     | 国家/地区代码 |
|-------------|---------|
| 英国          | GBR     |
| 美国          | USA     |
| 美国本土外小岛屿    | UMI     |
| 乌拉圭         | URY     |
| 乌兹别克斯坦      | UZB     |
| 瓦努阿图        | SATT    |
| 委内瑞拉玻利瓦尔共和国 | VEN     |
| 越南          | VNM     |
| 英属维尔京群岛     | VGB     |
| 美属维尔京群岛     | VIR     |
| 瓦利斯和富图纳群岛   | WLF     |
| 西撒哈拉        | ESH     |
| 也门          | YEM     |
| 赞比亚         | ZMB     |
| 津巴布韦        | ZWE     |

## SupportAssist 命令

### eula-consent

接受或拒绝 SupportAssist 终端用户许可协议 (EULA)。

|         |                                                                                                                                                                                           |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法      | <code>eula-consent {support-assist} {accept   reject}</code>                                                                                                                              |
| 参数      | <ul style="list-style-type: none"><li><code>support-assist</code> — 输入以接受或拒绝服务的 EULA。</li><li><code>accept</code> — 输入以接受 EULA 同意。</li><li><code>reject</code> — 输入以拒绝 EULA 同意。</li></ul> |
| 默认      | 未配置                                                                                                                                                                                       |
| 命令模式    | CONFIGURATION                                                                                                                                                                             |
| 使用情况信息  | <p>如果拒绝终端用户许可协议，则无法访问 SupportAssist 配置子模式。如果存在现有 SupportAssist 配置，将移除配置并禁用该功能。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持</p>    |
| 示例 (接受) | <pre>OS10(config)# eula-consent support-assist accept</pre>                                                                                                                               |
| 示例 (拒绝) | <pre>OS10(config)# eula-consent support-assist reject  This action will disable Support Assist and erase all configured data.Do you want to proceed ? [Y/N]:Y</pre>                       |
| 支持的版本   | 10.2.0E or later                                                                                                                                                                          |



## show eula-consent support-assist

显示 SupportAssist 终端用户许可协议的状态（无论是接受还是拒绝）。

|        |                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show eula-consent support-assist                                                                                                 |
| 参数     | 无                                                                                                                                |
| 默认     | 拒绝                                                                                                                               |
| 命令模式   | EXEC                                                                                                                             |
| 使用情况信息 | 使用此命令可查看 SupportAssist EULA 的状态。<br>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持 |
| 示例     | <pre>OS10# show eula-consent support-assist EULA support-assist : Accepted</pre>                                                 |
| 支持的版本  | 10.2.0E or later                                                                                                                 |

## support-assist

进入 SupportAssist 子配置模式。

|        |                                                                                              |
|--------|----------------------------------------------------------------------------------------------|
| 语法     | support-assist                                                                               |
| 参数     | 无                                                                                            |
| 默认     | 不适用                                                                                          |
| 命令模式   | CONFIGURATION                                                                                |
| 使用情况信息 | 从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持 |
| 示例     | <pre>OS10(config)# support-assist OS10(conf-support-assist)#</pre>                           |
| 支持的版本  | 10.2.0E or later                                                                             |

## support-assist-activity

为数据收集和传输活动安排时间，或执行按需数据收集和托管文件传输。

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法 | support-assist-activity full-transfer {start-now   [schedule {hourly <i>minute</i>   daily hour <i>number</i> min <i>number</i>   weekly day-of-week <i>number</i> hour <i>number</i> min <i>number</i>   monthly day <i>number</i> hour <i>number</i> min <i>number</i>   yearly month <i>number</i> day <i>number</i> hour <i>number</i> min <i>number</i> }]}                                                                                                                                                                                                                                                                                |
| 参数 | <ul style="list-style-type: none"><li>start-now — 将传输安排为立即启动。</li><li>hourly <i>minute</i>— 输入关键字并指定哪分钟安排任务，0-59。</li><li>daily — 安排日常任务：<ul style="list-style-type: none"><li>hour <i>number</i>— 输入关键字并指定几点安排任务，0-23。</li><li>min <i>number</i>— 输入关键字并指定哪分钟安排任务，0-59。</li></ul></li><li>weekly — 安排每周执行任务：<ul style="list-style-type: none"><li>day-of-week <i>number</i>— 输入每周的关键字并指定星期几安排任务，0-6。</li><li>hour <i>number</i>— 输入关键字并指定几点安排任务，0-23。</li><li>min <i>number</i>— 输入关键字并指定哪分钟安排任务，0-59。</li></ul></li><li>monthly — 安排月度任务：<ul style="list-style-type: none"><li>day <i>number</i>— 输入关键字并指定该月安排任务的日期，1-31。</li></ul></li></ul> |

- *hour number*— 输入关键字并指定几点安排任务，0-23。
  - *min number*— 输入关键字并指定哪分钟安排任务，0-59。
- *yearly* — 安排年度任务：
  - *month number*— 输入关键字并指定哪个月安排任务，1-12。
  - *day number*— 输入关键字并指定该月安排任务的日期，1-31。
  - *hour number*— 输入关键字并指定几点安排任务，0-23。
  - *min number*— 输入关键字并指定哪分钟安排任务，0-59。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 使用情况信息 | 从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持<br>此命令的 <i>no</i> 版本将移除配置。                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 示例     | <pre>OS10# support-assist-activity full-transfer start-now</pre> <pre>OS10# support-assist-activity full-transfer schedule hourly min 59</pre> <pre>OS10# support-assist-activity full-transfer schedule daily hour 23 min 59</pre> <pre>OS10# support-assist-activity full-transfer schedule weekly day-of-week 1 hour 23 min 59</pre> <pre>OS10# support-assist-activity full-transfer schedule monthly day 30 hour 23 min 59</pre> <pre>OS10# support-assist-activity full-transfer schedule yearly month 12 day 31 hour 23 min 59</pre> |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## SupportAssist 配置命令

### activity

为完整传输或事件通知启用数据收集活动。

|        |                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>activity {event-notification   full-transfer}</code>                                                                                                  |
| 参数     | 无                                                                                                                                                           |
| 默认     | 已启用                                                                                                                                                         |
| 命令模式   | SUPPORT-ASSIST                                                                                                                                              |
| 使用情况信息 | <p>此命令可为指定的活动启用数据收集。</p> <p>从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。</p> <p>此命令的 <i>no</i> 版本将禁用该活动。</p> |
| 示例     | <pre>OS10(conf-support-assist)# activity event-notification enable</pre> <pre>OS10(conf-support-assist)# activity full-transfer enable</pre>                |
| 支持的版本  | 10.2.0E or later                                                                                                                                            |

## contact-company

配置公司联系信息。

|        |                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>contact-company name <i>company-name</i></code>                                                                                                                                     |
| 参数     | <i>company-name</i> — 输入联系人公司名称。                                                                                                                                                          |
| 默认     | 未配置                                                                                                                                                                                       |
| 命令模式   | SUPPORT-ASSIST                                                                                                                                                                            |
| 使用情况信息 | <p>您只能输入一个联系人公司。此命令会将您带到子模式，您可以在其中提供更多公司联系信息。</p> <p>从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。</p> <p>此命令的 <code>no</code> 版本将移除配置。</p> |
| 示例     | <pre>OS10(conf-support-assist)# contact-company name ExampleCompanyName OS10(conf-support-assist-ExampleCompanyName)#</pre>                                                               |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                          |

## server url

配置 SupportAssist 服务器的 URL 和端口，并指定 SupportAssist 服务器授权所需的用户名和密码。

|        |                                                                                                                                                                                                                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>server url {default   <i>server-url-string</i>} username <i>username</i> password <i>password</i></code>                                                                                                                                                                                                                                        |
| 参数     | <ul style="list-style-type: none"><li><code>default</code> — 输入用于连接到 SupportAssist 服务器 (<a href="https://esrs3.emc.com">https://esrs3.emc.com</a>) 的默认值。</li><li><i>server-url-string</i>— 输入 SupportAssist 服务器的域名或 IP 地址。</li><li><i>username</i>— 输入用于与 SupportAssist 服务器建立连接的用户名。</li><li><i>password</i>— 输入与 SupportAssist 服务器建立连接的密码。</li></ul> |
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                     |
| 命令模式   | SUPPORT-ASSIST                                                                                                                                                                                                                                                                                                                                        |
| 使用情况信息 | <p>输入您的 Dell Digital Locker (DDL) 凭据。此帐户必须有权访问 DDL 中的 OS10 交换机。要查看服务器配置。此命令的 <code>no</code> 版本将移除配置，仅配置一个 SupportAssist 服务器时，请使用 <code>show support-assist status</code> 命令。</p> <p>从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。</p>                                                                  |
| 示例     | <pre>OS10(conf-support-assist)# server url default username youremailid@example.com password Password1</pre>                                                                                                                                                                                                                                          |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                      |

## show configuration

显示设备上当前运行的 SupportAssist 配置。

|        |                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------|
| 语法     | <code>show configuration</code>                                                                    |
| 参数     | 无                                                                                                  |
| 默认     | 未配置                                                                                                |
| 命令模式   | SUPPORT-ASSIST                                                                                     |
| 使用情况信息 | <p>从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。</p> |

## 示例

```
OS10(conf-support-assist)# show configuration
!
support-assist
server url https://esrs3stg.emc.com username example-username password
9
76dbcf6c

ce4bd298375e15bb989a9a6e6ee51d130d446ce3c25ade72a6f99fc6
source-interface mgmt1/1/1
!
contact-company name "Example Company Name"
street-address No:123 Example Street Bldg 999
address city San Jose state California country USA zipcode 95125
territory Global
!
contact-person first Firstname last Lastname
email-address primary youremail@example.com alternate
alternate_email@example.com
phone primary 0001234567 alternate 1234567890
preferred-method email
```

## 支持的版本

10.2.0E or later

## show running-configuration support-assist

显示设备上当前运行的 SupportAssist 配置。

### 语法

show running-configuration support-assist

### 参数

无

### 默认

未配置

### 命令模式

EXEC

### 使用情况信息

从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。

## 示例

```
OS10# show running-configuration support-assist
!
support-assist
server url https://esrs3stg.emc.com username example-username password
9
76dbcf6c

ce4bd298375e15bb989a9a6e6ee51d130d446ce3c25ade72a6f99fc6
source-interface mgmt1/1/1
!
contact-company name "Example Company Name"
street-address No:123 Example Street Bldg 999
address city San Jose state California country USA zipcode 95125
territory Global
!
contact-person first Firstname last Lastname
email-address primary youremail@example.com alternate
alternate_email@example.com
phone primary 0001234567 alternate 1234567890
preferred-method email
```

## 支持的版本

10.2.0E or later

## show support-assist eula

显示 SupportAssist 的 EULA。

### 语法

show support-assist eula

|        |                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------|
| 参数     | 无                                                                                                                              |
| 默认     | 无                                                                                                                              |
| 命令模式   | EXEC                                                                                                                           |
| 使用情况信息 | 使用此命令可以查看 SupportAssist 的 EULA。<br>从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。 |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show support-assist eula SUPPORTASSIST ENTERPRISE - SOFTWARE TERMS *** IMPORTANT INFORMATION - PLEASE READ CAREFULLY *** This SupportAssist Software ("Software") contains computer programs and other proprietary material and information, the use of which is governed by and expressly conditioned upon acceptance of this SupportAssist Enterprise Software Terms ("Agreement"). This Agreement is a legally binding agreement between the entity that has obtained the Software ("You" or "Customer") and Provider (which may be a Dell Inc. Affiliate or an authorized reseller ("Reseller"), as explained below). If you are acting on behalf of a U.S. Federal Government agency, please stop installing the Software and contact your sales account representative. . . . &lt;&lt;Output Truncated&gt;&gt;</pre> |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|

show support-assist status

显示 SupportAssist 状态信息，包括活动和事件。

|        |                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------|
| 语法     | show support-assist status                                                                                                 |
| 参数     | 无                                                                                                                          |
| 默认     | 未配置                                                                                                                        |
| 命令模式   | EXEC                                                                                                                       |
| 使用情况信息 | 使用此命令可以查看 SupportAssist 状态。<br>从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。 |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10# show support-assist status EULA support-assist : Accepted Service             : Enabled Contact-Company      : ExampleCompanyName Street Address       : Olympia City                 : SanJose State                : California Country              : USA Zipcode              : 95123 Territory             : West Contact-person        : Firstname Lastname Primary email         : youremail@example.com Alternate email       : emailid@example.com Primary phone         : 000-123-4567 Alternate phone       : 777777777 Contact method        : email Server(configured)   : default  Activity Enable State :   Activity             State -----</pre> |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                    |          |                     |                     |
|----------------------------------------------------|----------|---------------------|---------------------|
| full-transfer                                      | Enabled  |                     |                     |
| event-notification                                 | Enabled  |                     |                     |
| Scheduled Activity List :                          |          |                     |                     |
| Activity                                           | Schedule |                     | Schedule created on |
| -----                                              | -----    |                     | -----               |
| full-transfer                                      | None     |                     | Never               |
| Activity Status :                                  |          |                     |                     |
| Activity                                           | Status   | last start          | last success        |
| -----                                              | -----    | -----               | -----               |
| full-transfer                                      | Success  | 2019-06-13 16:08:51 | 2019-06-13 16:1     |
| event-notification                                 | Success  | 2019-06-13 16:04:35 | 2019-06-13 16:0     |
| keep-alive                                         | Success  | 2019-06-13 18:00:00 | 2019-06-13 17:3     |
| Server Status :                                    |          |                     |                     |
| Last KeepAlive Status : Failed                     |          |                     |                     |
| Last KeepAlive Successful at : 2019-06-13 17:30:03 |          |                     |                     |
| Last KeepAlive Failed at : 2019-06-13 18:00:03     |          |                     |                     |
| Last MFT Status : Success                          |          |                     |                     |
| Last MFT Successful at : 2019-06-13 16:15:19       |          |                     |                     |
| Last MFT Failed at : Never                         |          |                     |                     |

支持的版本10.2.0E or later

source-interface

配置源接口以建立与 SupportAssist 服务器的传出连接。

|        |                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | source-interface interface                                                                                                                                                                                                                                                                                                                       |
| 参数     | <div>interface:</div> <ul style="list-style-type: none"> <li>• ethernet node/slot/port[:subport]— 输入物理以太网接口。</li> <li>• loopback number— 输入环回接口，从 0 到 16383。</li> <li>• management 1/1/1 — 输入管理接口。</li> <li>• port-channel channel-id— 输入端口通道接口，从 1 到 128。</li> <li>• vlan vlan-id— 输入 VLAN ID，从 1 到 4093。</li> </ul>                            |
| 默认     | 未配置。                                                                                                                                                                                                                                                                                                                                             |
| 命令模式   | SUPPORT-ASSIST                                                                                                                                                                                                                                                                                                                                   |
| 使用情况信息 | <p>从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。</p> <p>此命令的 no 版本将移除配置。</p>                                                                                                                                                                                                                       |
| 示例     | <div>OS10(conf-support-assist)# source-interface ethernet 1/1/4</div> <div>OS10(conf-support-assist)# source-interface loopback 1</div> <div>OS10(conf-support-assist)# source-interface mgmt 1/1/1</div> <div>OS10(conf-support-assist)# source-interface port-channel 10</div> <div>OS10(conf-support-assist)# source-interface vlan 100</div> |
| 支持的版本  | 10.4.0E(R1) or later                                                                                                                                                                                                                                                                                                                             |

## SupportAssist 公司命令

### address

配置公司地址。

|        |                                                                                                                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>address city name state name country name zipcode number</code>                                                                                                                                                                              |
| 参数     | <ul style="list-style-type: none"><li>• <code>city name</code>— 输入关键字和城市名称。</li><li>• <code>state name</code>— 输入关键字和省/自治区/直辖市名称。</li><li>• <code>country name</code>— 输入关键字和国家/地区代码。</li><li>• <code>zipcode number</code>— 输入关键字和邮政编码。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                                |
| 命令模式   | SUPPORT-ASSIST 联系公司子模式                                                                                                                                                                                                                             |
| 使用情况信息 | <p>输入 ? 可查看受支持的国家/地区名称和代码的列表。您还可以在以下位置找到此信息：<a href="#">国家/地区名称和代码</a>。</p> <p>从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。</p> <p>此命令的 <code>no</code> 版本将移除配置。</p>                                |

|    |                                                                                                                          |
|----|--------------------------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10(conf-support-assist-ExampleCompanyName)# address city SanJose state California country USA zipcode 95123</pre> |
|----|--------------------------------------------------------------------------------------------------------------------------|

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|

### contact-person

配置个人的联系人姓名。

|        |                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>contact-person {first <i>firstname</i> last <i>lastname</i>}</code>                                                                                                    |
| 参数     | <ul style="list-style-type: none"><li>• <code>first <i>firstname</i></code> — 输入联系人的关键字和名字。为多个名字使用双引号。</li><li>• <code>last <i>lastname</i></code> — 输入联系人的关键字和姓氏。</li></ul> |
| 默认     | 未配置                                                                                                                                                                          |
| 命令模式   | SUPPORT-ASSIST                                                                                                                                                               |
| 使用情况信息 | <p>从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。</p> <p>此命令的 <code>no</code> 版本将移除配置。</p>                                      |

|    |                                                                                                       |
|----|-------------------------------------------------------------------------------------------------------|
| 示例 | <pre>OS10(conf-support-assist-ExampleCompanyName)# contact-person first Firstname last Lastname</pre> |
|----|-------------------------------------------------------------------------------------------------------|

|       |                  |
|-------|------------------|
| 支持的版本 | 10.2.0E or later |
|-------|------------------|

### street-address

配置公司的街道地址。

|      |                                                                              |
|------|------------------------------------------------------------------------------|
| 语法   | <code>street-address {<i>line-1</i>} [<i>line-2</i>] [<i>line-3</i>]</code>  |
| 参数   | <code>line-1 line-2 line-3</code> — 输入公司的地址，从 1 行到 3 行。将文本括在双引号内。在每行文本后插入空格。 |
| 默认   | 未配置                                                                          |
| 命令模式 | <ul style="list-style-type: none"><li>• SUPPORT-ASSIST</li></ul>             |

|               |                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>使用情况信息</b> | 从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。<br>此命令的 <code>no</code> 版本将移除配置。 |
| <b>示例</b>     | <pre>OS10 (conf-support-assist-ExampleCompanyName) # street-address "One Dell Way" "Suite 100" "Santa Clara"</pre>           |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                             |

## territory

配置公司所在的位置。

|               |                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>territory territory-name</code>                                                                                                          |
| <b>参数</b>     | <code>territory-name</code> — 输入公司所在的区域。                                                                                                       |
| <b>默认</b>     | 未配置                                                                                                                                            |
| <b>命令模式</b>   | CONF-SUPPORT-ASSIST                                                                                                                            |
| <b>使用情况信息</b> | 从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。<br>此命令的 <code>no</code> 版本将移除配置。                   |
| <b>示例</b>     | <pre>OS10 (conf-support-assist) # contact-company name ExampleCompanyName OS10 (conf-support-assist-ExampleCompanyName) # territory West</pre> |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                               |

## SupportAssist 人员命令

### email-address

配置联系人的电子邮件地址。

|               |                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>语法</b>     | <code>email-address primary email-id [alternate email-id]</code>                                                                                       |
| <b>参数</b>     | <code>email-id</code> — 输入联系人的电子邮件地址。                                                                                                                  |
| <b>默认</b>     | 未配置                                                                                                                                                    |
| <b>命令模式</b>   | SUPPORT-ASSIST                                                                                                                                         |
| <b>使用情况信息</b> | 从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。<br>此命令的 <code>no</code> 版本将移除配置。                           |
| <b>示例</b>     | <pre>OS10 (conf-support-assist-ExampleCompanyName-FirstnameLastname) # email-address primary youremail@example.com alternate emailid@example.com</pre> |
| <b>支持的版本</b>  | 10.2.0E or later                                                                                                                                       |

### phone

配置联系人的电话号码。

|           |                                                      |
|-----------|------------------------------------------------------|
| <b>语法</b> | <code>phone primary string [alternate string]</code> |
| <b>参数</b> | <code>string</code> — 输入联系人的电话号码。电话号码的最小长度为九位数字。     |



|        |                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------|
| 默认     | 无                                                                                                               |
| 命令模式   | SUPPORT-ASSIST                                                                                                  |
| 使用情况信息 | 从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。<br>此命令的 no 版本将移除配置。 |
| 示例     | <pre>OS10 (conf-support-assist-ExampleCompanyName-FirstnameLastname) # phone primary 000-123-4567</pre>         |
| 支持的版本  | 10.2.0E or later                                                                                                |

preferred-method

配置用于联系个人的首选方法。

|        |                                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | preferred-method {email   phone   no-contact}                                                                                                                                                                                                                                                |
| 参数     | <ul style="list-style-type: none"><li>email — 输入以选择电子邮件作为首选的联系方法。</li><li>phone — 输入以选择手机作为首选联系方法。</li><li>no-contact — 输入以指定不希望通过电子邮件或电话联系到个人。</li></ul>                                                                                                                                    |
| 默认     | No-contact                                                                                                                                                                                                                                                                                   |
| 命令模式   | SUPPORT-ASSIST                                                                                                                                                                                                                                                                               |
| 使用情况信息 | 从版本 10.4.0 (R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0 开始，在 SmartFabric 模式下也受支持。<br>此命令的 no 版本将移除配置。                                                                                                                                                                              |
| 示例     | <pre>OS10 (conf-support-assist-ExampleCompanyName-FirstnameLastname) # preferred-method email  OS10 (conf-support-assist-ExampleCompanyName-FirstnameLastname) # preferred-method phone  OS10 (conf-support-assist-ExampleCompanyName-FirstnameLastname) # preferred-method no-contact</pre> |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                             |

支持套装

支持套装基于 sosreport 工具。使用支持套装生成 sosreport tar 文件来收集 Linux 系统配置和诊断信息，以及 show 命令输出以发送至 Dell EMC 技术支持。

要发送有关 Linux 系统配置和 OS10 诊断的 Dell EMC 技术支持故障处理详细信息，请生成 sosreport tar 文件。

1. 在 EXEC 模式下生成 tar 文件。

```
generate support-bundle
```

2. 在 EXEC 模式下验证生成的文件。

```
dir supportbundle
```

3. 在 EXEC 模式下使用 FTP/SFTP/SCP/TFTP 发送支持套装。

```
copy supportbundle://sosreport-filename.tar.gz tftp://server-address/path
```

使用 delete supportbundle://sosreport-filename.tar.gz 命令以删除生成的支持套装。

# 事件通知

generate support-bundle 命令的事件通知在所支持的套装开始和结束时进行处理，并报告成功或失败。

## 支持套装生成开始事件

```
Apr 19 16:57:55: %Node.1-Unit.1:PRI:OS10 %log-notice:SUPPORT_BUNDLE_STARTED: generate support-bundle execution has started successfully:All Plugin options disabled
Apr 19 16:57:55: %Node.1-Unit.1:PRI:OS10 %log-notice:SUPPORT_BUNDLE_STARTED: generate support-bundle execution has started successfully:All Plugin options enabled
```

## sosreport 生成开始事件

```
May 11 22:9:43: %Node.1-Unit.1:PRI:OS10 %log-notice:SOSREPORT_GEN_STARTED: CLI output collection task completed; sosreport execution task started:All Plugin options disabled
May 11 22:9:43: %Node.1-Unit.1:PRI:OS10 %log-notice:SOSREPORT_GEN_STARTED: CLI output collection task completed; sosreport execution task started:All Plugin options enabled
```

## 支持套装生成成功事件

```
Apr 19 17:0:9: %Node.1-Unit.1:PRI:OS10 %log-notice:SUPPORT_BUNDLE_COMPLETED: generate support-bundle execution has completed successfully:All Plugin options disabled
Apr 19 17:0:9: %Node.1-Unit.1:PRI:OS10 %log-notice:SUPPORT_BUNDLE_COMPLETED: generate support-bundle execution has completed successfully:All Plugin options enabled
```

## 支持套装生成失败

```
Apr 19 17:0:14: %Node.1-Unit.1:PRI:OS10 %log-notice:SUPPORT_BUNDLE_FAILURE: Failure in generate support-bundle execution:All Plugin options disabled
Apr 19 17:0:14: %Node.1-Unit.1:PRI:OS10 %log-notice:SUPPORT_BUNDLE_FAILURE: Failure in generate support-bundle execution:All Plugin options enabled
```

# generate support-bundle

生成 sosreport tar 文件，收集有关 Linux 系统的配置和诊断信息。

|          |                                                                                                                                          |
|----------|------------------------------------------------------------------------------------------------------------------------------------------|
| 语法       | generate support-bundle [enable-all-plugin-options]                                                                                      |
| 参数       | enable-all-plugin-options —（可选）在启用所有插件选项的情况下生成完整支持套装。                                                                                    |
| 默认       | 无                                                                                                                                        |
| 命令模式     | EXEC                                                                                                                                     |
| 使用情况信息   | 要将 tar 文件发送给 Dell EMC 技术支持，请使用 dir supportbundle 和 copy supportbundle://sosreport-OS10-file-number.tar.gz tftp://server-address/path 命令。 |
| 示例       | <pre>OS10# generate support-bundle</pre>                                                                                                 |
| 示例（启用选项） | <pre>OS10# generate support-bundle enable-all-plugin-options</pre>                                                                       |
| 支持的版本    | 10.2.0E or later                                                                                                                         |

# 系统监控

使用系统警报和日志信息监控 OS10。

## 系统事件和警报

事件会通知您系统中您可能感兴趣的更改或情况。警报指示系统进入了异常状态，并且可能需要立即采取措施。

事件划分为：

- **无状态事件** — 有关系统状况的一次性通知，例如 ACL 更新、防火墙策略更新等。
- **有状态事件** — 发生异常情况时引发的事件，并在情况恢复正常时清除。这些类型的事件称为警报。

事件可以具有以下严重级别之一：

- **严重** — 存在严重情况，需要立即采取措施。如果一个或多个硬件组件发生故障或者一个或多个硬件组件超出温度阈值，则可能会触发严重事件。
- **重要** — 发生了重大错误，需要上报或通知。例如，如果发生接口故障（如端口通道关闭），则可能会触发重大警报。
- **次要** — 发生次要错误或非严重情况，如果未选中此复选框，则可能会导致系统服务中断或性能下降。次要警报需要监控或维护。
- **警告** — 观察到警告条件，但可能会导致错误状况。
- **通知** — 出现通知事件，但不会影响性能。

当系统触发警报时，发生内存不足、温度超出关键点等情况。系统从条件中恢复后，警报将被清除。

严重性级别为的所有有状态事件为严重、重要、次要或警告触发警报。但是，您可以自定义事件严重性或使用[严重性配置文件](#)关闭事件通知。

触发的警报处于以下状态之一：

- **活动** — 发出警报并且当前处于活动状态。
- **已确认** — 发出警报；用户了解情况并确认警报。此警报不会影响系统或系统 LED 的整体运行状况。

某些警报直接进入活动和已清除状态，并且需要少量的管理工作。您必须确认或调查具有高严重性的警报。

OS10 将所有活动和已确认警报存储在当前警报列表 (CAL) 中，并在事件历史记录列表 (EHL) 中归档所有过去的事件。

重新加载后，将清除 CAL 中的警报。

EHL 是持久的，并且在重新加载、重新启动或升级后保留已归档的事件。EHL 可以存储最多 86,000 个事件或 30 天的事件（以较早者为准）。

指示交换机状态的系统 LED 取决于 CAL 中的警报严重性，并且将呈现：

- 红色 — 针对严重或重要警报
- 琥珀色 — 针对次要或警告警报
- 绿色 — 无警报

## 严重性配置文件

OS10 允许您使用严重性配置文件更改事件的严重性。严重性配置文件是一个 .xml 文件，它可以定义事件的有效严重性或禁用事件通知。

OS10 附带默认的严重性配置文件。您不能修改或删除默认配置文件。但是，OS10 允许您定义自定义的严重性配置文件。

- **默认严重性配置文件** — 所有事件均在默认配置文件中定义。默认配置文件将事件归类为严重、警告或通知。
- **自定义严重性配置文件** — 包含您修改的事件。您可以将事件的严重性归类为严重、主要、次要、警告或通知。

在自定义配置文件中定义的事件及其特性优先于默认配置文件。

要创建自定义的严重性配置文件，请将默认的严重性配置文件复制到远程主机并对其进行修改。创建自定义配置文件后，将其从远程主机复制到 OS10 交换机并应用它。自定义配置文件会在系统重新启动后生效。

### 注：

- 要自定义严重性配置文件，您的用户帐户必须具有以下权限之一：System admin (sysadmin)、security admin (secadmin) 或 network admin (netadmin)。

- 您不能编辑活动的自定义配置文件。要编辑活动的自定义严重性配置文件，请选择另一个严重性配置文件并对其进行应用。

`severity-profile://` 分区包含所有已定义的严重性配置文件。要查看严重性配置文件列表，请使用 `dir severity-profile` 命令。

要删除严重性配置文件，请使用 `delete` 命令。您可以删除除默认和活动配置文件以外的所有严重性配置文件。

## 配置自定义严重性配置文件

要修改事件严重性或禁用事件通知，请执行以下操作：

您的用户帐户必须具有以下权限之一：System admin (sysadmin)、security admin (secadmin) 或 network admin (netadmin)。

1. 使用 `dir` 命令可查看 `severity-profile://` 分区中的可用严重性配置文件的列表。

```
OS10# dir severity-profile
Date (modified) Size (bytes) Name

2019-03-27T15:24:06Z 46741 default.xml
2019-04-01T11:22:33Z 456 custom.xml
```

2. 将一个可用的严重性配置文件复制到远程主机。

```
OS10# copy severity-profile://default.xml scp://username:password@a.b.c.d/dir-path/
mySevProf.xml
```

3. 修改包含所需更改的 .xml 文件。

**注：**修改 xml 文件时，必须选择以下严重级别之一：

- 严重
- 重要
- 次要
- 警告
- 通知

如果您希望 OS10 生成事件，请将启用标记设置为 `true`。要关闭事件通知，请将启用标记设置为 `false`。

如果您输入的值无效，则 `event severity-profile` 命令将失败。

4. 将自定义配置文件复制到 OS10 交换机。

```
OS10# copy scp://username:password@a.b.c.d/dir-path/mySevProf.xml severity-profile://
mySevProf_1.xml
```

复制自定义配置文件时，必须更新自定义配置文件的名称。您不能使用与默认配置文件相同的名称 (`default.xml`) 或活动配置文件 (`mySevProf.xml`)。

5. 在交换机上应用自定义严重性配置文件。

```
OS10# event severity-profile mySevProf_1.xml
```

**注：**必须重新启动交换机才能使更改生效。

6. 重新启动交换机。

```
OS10# reload
```

7. 使用 `show event severity-profile` 命令可查看处于活动状态的自定义配置文件。

```
OS10# show event severity-profile
Severity Profile Details

Currently Active : default
Active after restart : mySevProf_1.xml
```

## 删除自定义严重性配置文件

您可以删除不再需要的自定义严重性配置文件。但是，您不能删除默认或活动的严重性配置文件。

要删除自定义严重性配置文件，请使用 `delete severity-profile://profile-name` 命令。例如：

```
OS10# delete severity-profile://mySevProf_1.xml
```

## 系统日志记录

您可以使用严重性级别更改系统日志记录的默认设置，以控制记录的系统消息的类型。日志记录严重性的范围如下：

- `log-emerg` — 系统不稳定。
- `log-alert` — 需要立即采取措施。
- `log-crit` — 严重情况
- `log-err` — 错误情况
- `log-warning` — 警告条件
- `log-notice` — 正常但重要的条件（默认）
- `log-info` — 通知消息
- `log-debug` — 调试消息
- 在 CONFIGURATION 模式下输入记录到控制台的最低严重性级别。

```
logging console severity
```

- 在 CONFIGURATION 模式下输入记录到系统日志文件的最低严重性级别。

```
logging log-file severity
```

- 在 CONFIGURATION 模式下输入记录到终端行的最低严重性级别。

```
logging monitor severity
```

- 在 CONFIGURATION 模式下配置远程 syslog 服务器。

```
logging server {ipv4-address | ipv6-address} [tcp | udp | tls] [port-number]
[severity severity-level] [vrf {management | vrf-name}]
```

## 禁用系统日志记录

您可以使用任何日志记录命令的 `no` 版本来禁用系统日志记录。

- 禁用控制台日志记录，并将最低日志记录严重性重置为 CONFIGURATION 模式下的默认值。

```
no logging console severity
```

- 禁用日志文件日志记录，并将最低日志记录严重性重置为 CONFIGURATION 模式下的默认值。

```
no logging log-file severity
```

- 禁用监控日志记录，并将最低日志记录严重性重置为 CONFIGURATION 模式下的默认值。

```
no logging monitor severity
```

- 禁用服务器日志记录，并将最低日志记录严重性重置为 CONFIGURATION 模式下的默认值。

```
no logging server severity
```

- 在 CONFIGURATION 模式下重新启用任何日志记录命令。

```
no logging enable
```

## 为日志通知启用服务器日志记录

```
OS10(config)# logging server 10.11.86.139 severity log-notice
```

## 通过 TLS 的系统日志记录

要在发送到 syslog 服务器的已记录系统消息中提供增强的安全性和隐私，您可以使用传输层安全 (TLS) 协议。系统通过 TLS 进行日志记录会对 OS10 交换机与配置的远程日志记录服务器之间的通信进行加密，包括：

- 使用公钥基础设施 (PKI) 证书可以执行客户端和服务器的相互身份验证
- 加密整个身份验证交换，以便用户 ID 和密码都不易发现，并且在传输期间不会修改数据。

### 配置说明

通过 TLS 进行系统日志记录需要：

- 在证书颁发机构 (CA) 上配置 X.509v3 PKI 证书，并在交换机上安装。交换机和 syslog 服务器均交换签名的 X.509v3 证书中的公钥，以便彼此进行身份验证。有关详细信息，请参阅 [X.509v3 证书](#)。
- 您可以根据[安全配置文件](#)中的说明，配置用于系统日志记录的安全配置文件。

### 配置通过 TLS 的系统日志记录

1. 按照[管理 CA 证书](#)中所述，使用安全的方法（如 SCP 或 HTTPS）复制 CA 服务器创建的 X.509v3 证书。然后在 EXEC 模式下安装受信任的 CA 证书。

```
crypto ca-cert install ca-cert-filepath [filename]
```

- *ca-cert-filepath* 指定下载的证书的本地路径；例如，`home://CAcert.pem` 或 `usb://CA-cert.pem`。
  - *filename* 指定将证书存储在 OS10 信任存储目录下的可选文件名。以 *filename.crt* 格式输入文件名。
2. 如[请求和安装主机证书](#)中所述，从 CA 服务器获取 X.509v3 主机证书：
    - a. 创建私钥并生成交换机的证书签名请求。
    - b. 将 CSR 文件复制到 CA 服务器以进行签名。
    - c. 将 CA 签名的证书复制到交换机上的主目录。
    - d. 安装主机证书：

```
crypto cert install cert-file home://cert-filepath key-file {key-path | private}
[password passphrase] [fips]
```

当您安装 X.509v3 证书密钥对时：

- 两者均采用证书的名称。例如，如果您使用以下命令安装证书：

```
OS10# crypto cert install cert-file home://Dell_host1.pem key-file home://abcd.key
```

证书密钥对安装为 `Dell_host1.pem` 和 `Dell_host1.key`。在配置命令中，请参阅配对 `Dell_host1`。配置安全配置文件时，您可以在 `certificate certificate-name` 命令中输入 `Dell_host1`。

- 出于安全原因，由于密钥文件包含私钥信息，因此将其复制到 OS10 文件系统的安全位置，并将其从 `key-file key-path` 参数中指定的原始位置删除。

**i 注：** `fips` 将以与 FIPS 兼容的方式安装证书密钥对。输入 `fips` 以安装由 FIPS 感知应用程序使用的证书密钥对，例如 Syslog over TLS。如果不输入 `fips`，则证书密钥对将存储为与 FIPS 不兼容的对。

您可以决定证书密钥对是否以与 FIPS 兼容的方式生成。请勿在 FIPS 模式以外使用 FIPS 兼容的证书密钥对。启用 FIPS 模式后，仍可为非 FIPS 证书生成 CSRs，以便与非 FIPS 应用程序配合使用。请确保使用 `crypto cert install` 命令将这些证书作为非 FIPS 安装。

3. 使用 X.509v3 证书为通过 TLS 的系统日志记录配置安全配置文件。
  - a. 在 CONFIGURATION 模式下创建系统日志安全配置文件。请参阅[安全配置文件](#)了解更多信息。

```
crypto security-profile profile-name
```

- b. 在 SECURITY-PROFILE 模式下将 X.509v3 证书和私钥对分配到安全配置文件。对于 *certificate-name*，输入与不带 `.pem` 扩展名的 `show crypto certs` 输出中显示的证书密钥对的名称。

```
certificate certificate-name
exit
```

- c. 在 CONFIGURATION 模式下创建特定于系统日志记录的配置文件。

```
logging security-profile profile-name
```

其中 *profile-name* 是在步骤 2a 中通过 `crypto security-profile profile-name` 命令创建的 Syslog 安全配置文件。您不能删除为日志记录服务器配置的加密服务器配置文件。

如果重新配置加密安全 *profile-name*，配置的系统日志 TLS 服务器将自动更新为使用新配置文件所用的新证书密钥对。

如果您重新配置分配给加密安全配置文件的证书，Syslog TLS 服务器将自动更新为使用新的证书密钥对。

如果从已配置的加密安全配置文件中删除证书，则通过 TLS 进行的系统日志记录将失败。与外部设备进行协议交换需要主机证书。

4. 在 CONFIGURATION 模式下配置远程 TLS 服务器以接收系统消息。

```
logging server {ipv4-address | ipv6-address} tls [port-number]
[severity severity-level] [vrf {management | vrf-name}]
```

#### 示例：配置 Syslog over TLS

```
OS10# copy tftp://CAadmin:secret@172.11.222.1/cacert.pem home://cacert.pem

OS10# crypto ca-cert install home://cacert.pem
Processing certificate ...
Installed Root CA certificate
CommonName = Certificate Authority CA
IssuerName = Certificate Authority CA

OS10# show crypto ca-certs

Locally installed certificates
cacert.crt

OS10# crypto cert generate request cert-file home://clientreq.pem key-file home://
clientkey.pem cname "Top of Rack 6" altname "IP:10.0.0.6 DNS:tor6.dell.com" email
admin@dell.com organization "Dell EMC" orgunit Networking locality "Santa Clara" state
California country US length 2048
Processing certificate ...
Successfully created CSR file /home/admin/clientreq.pem and key

OS10# copy home://clientreq.pem scp://CAadmin:secret@172.11.222.1/clientreq.pem

OS10# copy scp://CAadmin:secret@172.11.222.1/clientcert.pem home://clientcert.pem
OS10# copy scp://CAadmin:secret@172.11.222.1/clientkey.pem home://clientkey.pem

OS10# crypto cert install cert-file home://clientcert.pem key-file home://clientkey.pem
Processing certificate ...
Certificate and keys were successfully installed as "clientcert.crt" that may be used in
a security profile. CN = 10.0.0.6

OS10# show crypto cert

Installed non-FIPS certificates
clientcert.crt

Installed FIPS certificates

OS10(config)# crypto security-profile dellprofile
OS10(config-sec-profile)# certificate clientcert
OS10(config-sec-profile)# exit
OS10(config)# logging security-profile dellprofile
OS10(config)# logging server 10.11.86.139 tls
OS10(config)# do show running-configuration logging
!
logging security-profile dellprofile
logging server 10.11.86.139 tls 514
```



## 查看系统日志

系统日志文件包含系统事件和警报日志。

使用 `show trace` 命令以查看当前 syslog 文件。所有事件和警报信息都会发送至 syslog 服务器（如果已配置）。

`show logging` 命令接受以下参数：

- `log-file` — 提供详细的日志，包括保存到文件的软件和硬件。
- `process-names` — 提供当前运行的所有进程的列表（可根据进程名称进行筛选）。

### 查看日志记录日志-文件

```
OS10# show logging log-file
Jun 1 05:01:46 %Node.1-Unit.1:PRI:OS10 %log-notice:ETL_SERVICE_UP: ETL service
is up
Jun 1 05:02:06 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_UNIT_DETECTED: Unit pres
ent:Unit 1#003
Jun 1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_PSU_DETECTED: Power Supp
ly Unit present:PSU 1#003
Jun 1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_PSU_DETECTED: Power Supp
ly Unit present:PSU 2#003
Jun 1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_FAN_TRAY_DETECTED: Fan t
ray present:Fan tray 1#003
Jun 1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_FAN_TRAY_DETECTED: Fan t
ray present:Fan tray 2#003
Jun 1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_FAN_TRAY_DETECTED: Fan t
ray present:Fan tray 3#003
Jun 1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-crit:EQM_FAN_AIRFLOW MISMATCH: MAJO
R ALARM: FAN AIRFLOW MISMATCH: SET: One or more fans have mismatching or unknown
airflow directions#003
Jun 1 05:02:10 %Node.1-Unit.1:PRI:OS10 %log-notice:NDM_SERVICE_UP: NDM Service
Ready!
Jun 1 05:02:10 %Node.1-Unit.1:PRI:OS10 %log-notice:SU_SERVICE_UP: Software upgr
ade service is up:software upgrade service up
--More--
```

### 查看日志记录进程名称

```
OS10# show logging process-names
dn_alm
dn_app_vlt
dn_app_vrrp
dn_bgp
dn_dot1x
dn_eqa
dn_eqm
dn_eth_drv
dn_etl
dn_i3
dn_ifm
dn_infra_afs
dn_issu
dn_l2_services
dn_l2_services_
dn_l2_services_
dn_l2_services_
dn_l2_services_
dn_l3_core_serv
dn_l3_service
dn_lacp
dn_lldp
dn_mgmt_entity_
--More--
```

## 环境监控

监控硬件环境以检测温度、CPU 和内存利用率。



查看环境

```
OS10# show environment

Unit State Temperature Voltage

1 up 42

Thermal sensors
Unit Sensor-Id Sensor-name Temperature

1 1 T2 temp sensor 28
1 2 system-NIC temp sensor 25
1 3 Ambient temp sensor 24
1 4 NPU temp sensor 40

```

链路套装监控

监控链路聚合组 (LAG) 套装允许链路中的流量分配量在任何给定时间查找不均匀分布。阈值为 60% 是可接受的成员链路上的流量的数量。

对于三个连续的实例，链路以 15 秒的间隔监控。在该时间内的任何偏差都会发送 syslog，并生成警报事件。当偏差清除时，将发送另一个 syslog，并生成清除警报事件。

链路套装利用率将计算所有链路的总带宽除以所有链路的总字节数。如果启用监控，则在链路套装（不是套装内的链路）的利用率超过 60% 时，将执行利用率计算。

配置用于链路套装监控的阈值级别

```
OS10(config)# link-bundle-trigger-threshold 10
```

查看链路套装监控阈值配置

```
OS10(config)# do show running-configuration
link-bundle-trigger-threshold 10
!
...
```

显示链路套装利用率

```
OS10(config)# do show link-bundle-utilization

Link-bundle trigger threshold - 10
```

警报命令

alarm acknowledge

确认活动警报。

**语法**

**参数**

**默认**

**命令模式**

**使用情况信息**

**示例**

**支持的版本**

`alarm acknowledge sequence-number`

- `sequence-number` — 确认与序列号对应的警报。

未配置

EXEC

使用 `show alarm` 命令查看所有活动警报。使用活动警报序列号确认特定警报。

```
OS10# alarm acknowledge 1
```

10.4.3 或更高版本

## event severity-profile

配置严重性配置文件以更改事件的严重性，或关闭事件通知。

|        |                                                                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | event severity-profile {default   profile-name}                                                                                                                                        |
| 参数     | profile-name— 自定义严重性配置文件的名称，最多 64 个字符。文件扩展名 .xml 是可选的。                                                                                                                                 |
| 默认     | Default.xml                                                                                                                                                                            |
| 命令模式   | EXEC                                                                                                                                                                                   |
| 使用情况信息 | 配置严重性配置文件以更改事件的特征。如果配置自定义配置文件，该配置文件将应用于默认配置文件之上。重新启动系统以使更改生效。系统重新启动可确保根据新应用的严重性配置文件相应地标记现有的状态事件。严重性配置文件存储在 severity-profile:// 分区中。此分区包含出厂默认严重性配置文件 default.xml。您不能编辑或删除默认和活动的严重性配置文件。 |
| 示例     | <pre>OS10# event severity-profile MySevPro_1 %Notice: Severity profile will be active after system restart</pre>                                                                       |
| 支持的版本  | 10.5.0 or later                                                                                                                                                                        |

## show alarms

显示系统中的所有当前活动警报。

|        |                                                                                                                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show alarms                                                                                                                                                                                                                                                                                                                                                   |
| 参数     | 无                                                                                                                                                                                                                                                                                                                                                             |
| 默认     | 无                                                                                                                                                                                                                                                                                                                                                             |
| 命令模式   | EXEC                                                                                                                                                                                                                                                                                                                                                          |
| 使用情况信息 | 无                                                                                                                                                                                                                                                                                                                                                             |
| 示例     | <pre>OS10# show alarms  Sq No      Severity      Name Timestamp  ----- -----     7563    critical      EQM_MORE_PSU_FAULT      Fri Jul 26 19:26:16 2019      /pus/1     7566    warning      EQM_TML_MINOR_CROSSED   Fri Jul 26 19:30:22 2019      /pus/1     7569    information  L2_SERV_LACP_CMS_CPS_SEND_FAIL  Fri Jul 26 19:55:40 2019      /pus/1</pre> |
| 支持的版本  | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                              |

## show alarms acknowledged

显示所有已确认的警报。

|        |                          |
|--------|--------------------------|
| 语法     | show alarms acknowledged |
| 参数     | 无                        |
| 默认     | 无                        |
| 命令模式   | EXEC                     |
| 使用情况信息 | 无                        |

## 示例

```
show alarms acknowledged

Sq No Severity Name
Timestamp -----

100071 warning EQM_FAN_FAULT_MINOR Tue Jul 23 13:53:47
2019 /psu/1/fan/1
100072 critical EQM_FAN_FAULT_MAJOR Tue Jul 23 13:53:47
2019 /psu/1
```

支持的版本 10.2.0E or later

## show alarms details

显示有关活动警报的详细信息。

语法 show alarms details

参数 无

默认 无

命令模式 EXEC

使用情况信息 show alarms details 命令的输出指示警报是否已确认。如果未确认警报，则 Acknowledged 字段将设置为 false，并且 Ack-time 值为空。如果警报已确认，则 Acknowledged 字段设置为 true，并且系统将显示确认警报的时间。

## 示例

### 警报未确认：

```
OS10# show alarms details

Active-alarm details - 732

Sequence Number: 732
Severity: critical
Source: /psu/2
Name: EQM_MORE_PSU_FAULT
Description: psu 2 is not working correctly
Raise-time: Mon Jul 29 06:12:30 2019
Ack-time:
New: true
Acknowledged: false

```

### 警报已确认：

```
OS10# show alarms details

Active-alarm details - 732

Sequence Number: 732
Severity: critical
Source: /psu/2
Name: EQM_MORE_PSU_FAULT
Description: psu 2 is not working correctly
Raise-time: Mon Jul 29 06:12:30 2019
Ack-time: Mon Jul 29 06:16:35 2019
New: true
Acknowledged: true

```

支持的版本 10.2.0E or later

## show alarms sequence

根据指定的序列号显示与活动警报对应的信息。

|        |                                                                                               |
|--------|-----------------------------------------------------------------------------------------------|
| 语法     | <code>show alarms sequence sequence-number</code>                                             |
| 参数     | <ul style="list-style-type: none"><li><code>sequence-number</code> — 输入与活动警报对应的序列号。</li></ul> |
| 默认     | 无                                                                                             |
| 命令模式   | EXEC                                                                                          |
| 使用情况信息 | 使用显示警报命令查看所有活动警报。使用活动警报序列号可查看有关该警报的详细信息。                                                      |
| 示例     |                                                                                               |

```
NOS# show alarms sequence 3
Active-alarm details - 1

Sequence Number: 3
Severity: major
Type: 1081375
Source: /psu/2
Name: EQM_MORE_PSU_FAULT
Description: psu 2 is not working correctly
Raise-time: Sun 10-07-2018 18:39:47
Ack-time:
State: raised

```

支持的版本 10.4.3E 或更高版本

## show alarms severity

显示与特定严重性级别相对应的所有活动警报。

|        |                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>show alarms severity severity</code>                                                                                                                                                                                            |
| 参数     | <code>severity</code> — 设置警报严重性: <ul style="list-style-type: none"><li><code>critical</code> — 严重警报严重性。</li><li><code>major</code> — 重要警报严重性。</li><li><code>minor</code> — 次要警报严重性。</li><li><code>warning</code> — 警告警报严重性。</li></ul> |
| 默认     | 未配置                                                                                                                                                                                                                                   |
| 命令模式   | EXEC                                                                                                                                                                                                                                  |
| 使用情况信息 | 无                                                                                                                                                                                                                                     |
| 示例（警告） |                                                                                                                                                                                                                                       |

```
OS10# show alarms severity warning

Active-alarm details - 1

Sequence Number: 5
Severity: warning
Type: 1081364
Source: Node.1-Unit.1
Name: EQM_THERMAL_WARN_CROSSED
Description:
Raise-time: Sat 10-06-2018 0:1:5
Ack-time: Sun 10-07-2018 20:39:47
New: true
State: raised
```

示例（重要）

```
OS10# show alarms severity critical

Active-alarm details - 0

```

```
Sequence Number: 1
Severity: critical
Type: 1081367
Source: Node.1-Unit.1
Name: EQM_THERMAL_CRIT_CROSSED
Description:
Raise-time: Sat 10-06-2018 0:1:5
Ack-time: Sun 10-07-2018 20:39:47
New: true
State: raised
```

#### 示例（次要）

```
NOS# show alarms severity minor
Active-alarm details - 1

Sequence Number: 4
Severity: minor
Type: 1081375
Source: /psu/1
Name: EQM_MORE_PSU_FAULT
Description: psu 2 is not working correctly
Raise-time: Sun 10-07-2018 18:39:47
Ack-time: Sun 10-07-2018 20:39:47
New: true
State: acknowledged

```

#### 支持的版本

10.4.3 或更高版本

## show alarms summary

显示所有活动警报的摘要。

**语法** `show alarms summary`

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 无

#### 示例

```
OS10# show alarms summary
Active-alarm Summary

Total-count: 2
Critical-count: 0
Major-count: 1
Minor-count: 1
Warning-count: 0

```

#### 支持的版本

10.2.0E or later

## show event history

显示输出顶部最新的所有事件的历史记录。

**语法** `show event history [summary] [reverse] [severity severity-name] [details] [sequence sequence-number]`

- 参数**
- `summary` — 显示事件历史记录摘要。
  - `reverse` — 显示起始事件历史记录摘要，并在输出顶部列出最旧的事件。
  - `severity` — 显示给定严重性的事件历史记录：严重、主要、次要、警告、信息。
  - `details` — 在详细信息中显示事件历史记录。

- `sequence sequence-number`— 显示给定序列号的事件详细信息。

默认

无

命令模式

EXEC

使用情况信息

在 OS10 交换机中显示事件日志。

示例

```
OS10# show event history
Sq No State Name Timestamp Source

6 Cleared EQM_FANTRAY_FAULT Sun 10-07-2018 22:39:50 /fantray/3
5 Ack EQM_MORE_PSU_FAULT Sun 10-07-2018 20:39:49 /psu/1
4 Raised EQM_MORE_PSU_FAULT Sun 10-07-2018 18:39:47 /psu/1
3 Raised EQM_MORE_PSU_FAULT Sun 10-07-2018 18:39:44 /psu/2
2 Raised EQM_FANTRAY_FAULT Sun 10-07-2018 16:39:42 /fantray/3
1 Stateless SYSTEM_REBOOT Sun 10-07-2018 15:39:41 -
```

示例 (严重性)

```
OS10# show event history severity critical
Sq No State Name Timestamp Source

4 Raised EQM_MORE_PSU_FAULT Sun 10-07-2018 18:39:47 /psu/1
3 Raised EQM_MORE_PSU_FAULT Sun 10-07-2018 18:39:44 /psu/2
2 Raised EQM_FANTRAY_FAULT Sun 10-07-2018 16:39:42 /fantray/3
```

示例 (反向)

```
OS10# show event history reverse
Sq No State Name Timestamp Source

1 Stateless SYSTEM_REBOOT Sun 10-07-2018 15:39:41 -
2 Raised EQM_FANTRAY_FAULT Sun 10-07-2018 16:39:42 /fantray/3
3 Raised EQM_MORE_PSU_FAULT Sun 10-07-2018 18:39:44 /psu/2
4 Raised EQM_MORE_PSU_FAULT Sun 10-07-2018 18:39:47 /psu/1
5 Ack EQM_MORE_PSU_FAULT Sun 10-07-2018 20:39:49 /psu/1
6 Cleared EQM_FANTRAY_FAULT Sun 10-07-2018 22:39:50 /fantray/3
```

示例 (顺序)

```
OS10# show event history sequence 2
Event History Details - 2

Sequence Number: 2
Severity: informational
Name: IFM_ASTATE_UP
Description: Dummy Event
Timestamp: Fri May 03 18:13:07 2019
Source: -
State: stateless

```

示例 (详细信息)

```
OS10# show event history details
Event History Details - 2

Sequence Number: 2
Severity: informational
Name: IFM_ASTATE_UP
Description: Dummy Event
Timestamp: Fri May 03 18:13:07 2019
Source: -
State: stateless

Event History Details - 1

Sequence Number: 1
Severity: informational
Name: IFM_ASTATE_UP
Description: Dummy Event
Timestamp: Fri May 03 18:13:05 2019
Source: -
```

```
State: stateless

```

#### 示例（摘要）

如果序列号计数器未进行回滚，则最后一个翻转时间值为空。

```
OS10# show event history summary

Event History Summary

Total-count: 583
Raised-count: 4
Ack-count: 0
Cleared-count: 0
Stateless-count: 579
Next Sequence Number: 584
Last Rollover Time:

```

#### 支持的版本

10.5.0 or later

## show event severity-profile

显示在系统重新启动后变为活动状态的活动严重性配置文件和配置文件。

**语法** show event severity-profile

**参数** 无

**默认** 无

**命令模式** EXEC

**使用情况信息** 无

#### 示例

```
OS10# show event severity-profile
Severity Profile Details

Currently Active : default
Active after restart : mySevProf.xml
```

#### 支持的版本

10.5.0 or later

## 日志记录命令

### clear logging

清除日志记录缓冲区中的消息。

**语法** clear logging log-file

**参数** 无

**默认** 未配置

**命令模式** EXEC

**使用情况信息** 从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

#### 示例

```
OS10# clear logging log-file

Proceed to clear the log file [confirm yes/no(default)]:
```

支持的版本 10.2.0E or later

## logging console

禁用、启用或配置登录控制台的最低严重性级别。

|         |                                                                                                                                                                                                                                                                                                                                                    |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法      | logging console {disable   enable   severity}                                                                                                                                                                                                                                                                                                      |
| 参数      | <p>severity — 设置最低日志记录严重性级别：</p> <ul style="list-style-type: none"><li>• log-emerg — 设置为不可用。</li><li>• log-alert — 需要设置为立即操作。</li><li>• log-crit — 设置为“严重条件”。</li><li>• log-err — 设置为“错误条件”。</li><li>• log-warning — 设置为“警告条件”。</li><li>• log-notice — 设置为“正常”，但“重要”条件为默认值。</li><li>• log-info — 设置为通知消息。</li><li>• log-debug — 设置为调试消息。</li></ul> |
| 默认      | Log-notice                                                                                                                                                                                                                                                                                                                                         |
| 命令模式    | CONFIGURATION                                                                                                                                                                                                                                                                                                                                      |
| 使用情况信息  | <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p> <p>要将严重性设置为默认级别，请使用 no logging console severity 命令。默认严重性级别为 log-notice。</p>                                                                                                                                                                   |
| 示例      | <pre>OS10(config)# logging console disable</pre>                                                                                                                                                                                                                                                                                                   |
| 示例（启用）  | <pre>OS10(config)# logging console enable</pre>                                                                                                                                                                                                                                                                                                    |
| 示例（严重性） | <pre>OS10(config)# logging console severity log-warning</pre>                                                                                                                                                                                                                                                                                      |
| 支持的版本   | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                   |

## logging enable

启用系统日志记录。

|        |                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------|
| 语法     | logging enable                                                                                                                   |
| 参数     | 无                                                                                                                                |
| 默认     | 已启用                                                                                                                              |
| 命令模式   | CONFIGURATION                                                                                                                    |
| 使用情况信息 | <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p> <p>此命令的 no 版本将禁用所有日志记录。</p> |
| 示例     | <pre>OS10(config)# logging enable</pre>                                                                                          |
| 支持的版本  | 10.2.0E or later                                                                                                                 |



## logging log-file

禁用、启用或设置记录到日志文件的最低严重性级别。

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法      | <code>logging log-file {disable   enable   severity}</code>                                                                                                                                                                                                                                                                                                                                                                                                         |
| 参数      | <code>severity</code> — 设置最低日志记录严重性级别： <ul style="list-style-type: none"><li>• <code>log-emerg</code> — 将系统设置为不可用。</li><li>• <code>log-alert</code> — 需要设置为立即操作。</li><li>• <code>log-crit</code> — 设置为“严重条件”。</li><li>• <code>log-err</code> — 设置为“错误条件”。</li><li>• <code>log-warning</code> — 设置为“警告条件”。</li><li>• <code>log-notice</code> — 设置为“正常”，但“重要”条件为默认值。</li><li>• <code>log-info</code> — 设置为通知消息。</li><li>• <code>log-debug</code> — 设置为调试消息。</li></ul> |
| 默认      | Log-notice                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 命令模式    | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 使用情况信息  | <p>要将日志文件严重性重置为默认级别，请使用 <code>no logging log-file severity</code> 命令。默认严重性级别为 <code>log-notice</code>。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p>                                                                                                                                                                                                                                                     |
| 示例      | <pre>OS10(config)# logging log-file disable</pre>                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 示例（启用）  | <pre>OS10(config)# logging log-file enable</pre>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 示例（严重性） | <pre>OS10(config)# logging log-file severity log-notice</pre>                                                                                                                                                                                                                                                                                                                                                                                                       |
| 支持的版本   | 10.2.0E or later                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## logging monitor

设置日志记录到终端行的最低严重性级别。

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | <code>logging monitor severity severity-level</code>                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 参数     | <code>severity-level</code> — 设置最低日志记录严重性级别： <ul style="list-style-type: none"><li>• <code>log-emerg</code> — 将系统设置为不可用。</li><li>• <code>log-alert</code> — 需要设置为立即操作。</li><li>• <code>log-crit</code> — 设置为“严重条件”。</li><li>• <code>log-err</code> — 设置为“错误条件”。</li><li>• <code>log-warning</code> — 设置为“警告条件”。</li><li>• <code>log-notice</code> — 设置为“正常”，但“重要”条件为默认值。</li><li>• <code>log-info</code> — 设置为通知消息。</li><li>• <code>log-debug</code> — 设置为调试消息。</li></ul> |
| 默认     | Log-notice                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 命令模式   | CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 使用情况信息 | <p>要将显示器严重性重置为默认级别，请使用 <code>no logging monitor severity</code> 命令。默认严重性级别为 <code>log-notice</code>。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p>                                                                                                                                                                                                                                                             |

## 示例

```
OS10(config)# logging monitor severity log-info
```

## 支持的版本

10.2.0E or later

# logging security-profile

创建用于系统日志记录的 TLS 安全配置文件。

## 语法

```
logging security-profile profile-name
```

## 参数

*profile-name* — 输入使用 `crypto security-profile profile-name` 命令创建的 Syslog over TLS 安全配置文件的名称；最多 32 个字符。

## 默认

未配置

## 命令模式

CONFIGURATION

## 使用情况信息

使用此命令可以指定已配置的加密安全配置文件，以用于通过 TLS 将系统消息发送到远程服务器。TLS 需要在交换机上安装 X.509v3 证书密钥对。

## 示例

```
OS10(config)# logging security-profile prof1
```

## 支持的版本

10.5.0 or later

# logging server

配置远程 syslog 服务器。

## 语法

```
logging server {ipv4-address | ipv6-address} [tcp | udp | tls] [port-number] [severity severity-level] [vrf {management | vrf-name}]
```

## 参数

- *ipv4-address | ipv6-address* — (可选) 输入日志服务器的 IPv4 或 IPv6 地址。
- *tcp | udp | tls port-number* — (可选) 使用 TCP、UDP 或 TLS 传输将 syslog 消息发送到远程日志记录服务器上的指定端口，从 1 到 65535。
- *severity-level* — (可选) 设置日志记录阈值严重性：
  - *log-emerg* — 系统不可用。
  - *log-alert* — 需要立即采取措施。
  - *log-crit* — 严重情况
  - *log-err* — 错误情况
  - *log-warning* — 警告条件
  - *log-notice* — 正常但重要的条件 (默认)
  - *log-info* — 通知消息
  - *log-debug* — 调试消息
- *vrf {management | vrf-name}* — (可选) 为管理或指定的 VRF 实例配置日志服务器。

## 默认

未配置系统日志记录到远程服务器。配置后，默认情况下，系统消息会通过 UDP 发送到远程日志记录服务器上的端口 514。发送严重级别 *log-notice* 和更低级别的系统消息。

## 命令模式

CONFIGURATION

## 使用情况信息

使用 `logging server` 命令可将日志消息转发到 syslog 服务器进行存储。

*tls* 选项要求已使用 `logging security-profile` 命令配置了有效的安全配置文件。如果删除日志记录安全配置文件，系统消息将使用 UDP (默认) 发送到远程 syslog 服务器。

从版本 10.5.0.0 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。

此命令的 *no* 版本会删除 syslog 服务器。

|    |                                                                             |
|----|-----------------------------------------------------------------------------|
| 示例 | OS10(config)# logging server 10.11.86.139 severity log-info                 |
|    | OS10(config)# logging server fda8:6c3:ce53:a890::2 tcp 1468                 |
|    | OS10(config)# logging server 10.11.86.139 vrf management severity log-debug |

支持的版本 10.5.0 or later

## show logging

按日志文件、进程名称或摘要显示系统日志记录消息。

|        |                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 语法     | show logging {log-file [ <i>process-name</i>   <i>line-numbers</i> ]   process-names}                                                                                     |
| 参数     | <ul style="list-style-type: none"> <li><i>process-name</i> — (可选) 输入要用作 syslog 消息中的筛选器的进程名称。</li> <li><i>line-numbers</i> — (可选) 输入要包括在日志记录消息中的行数，从 1 到 65535。</li> </ul> |
| 默认     | 无                                                                                                                                                                         |
| 命令模式   | EXEC                                                                                                                                                                      |
| 使用情况信息 | <p>此命令的输出为 <code>/var/log/eventlog</code> 文件。</p> <p>从版本 10.4.0E(R3S) 开始，在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始，在 SmartFabric 模式下也受支持。</p>                    |

|          |                                                 |
|----------|-------------------------------------------------|
| 示例（日志文件） | OS10# show logging log-file process-name dn_qos |
|----------|-------------------------------------------------|

|          |                                                                                                                                                                                                                                                                                                 |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 示例（进程名称） | <pre>OS10# show logging process-names dn_pas_svc dn_system_mgmt_ dn_env_tmpctl_ dn_pm dn_eth_drv dn_etl dn_eqa dn_alm dn_eqm dn_issu dn_swupgrade dn_ifm dn_ppm dn_l2_services dn_dotlx dn_l3_core_serv dn_policy dn_qos dn_switch_res_m dn_ospfv3 dn_lacp dn_i3 dn_supportassis --More--</pre> |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

支持的版本 10.2.0E or later

## show trace

显示跟踪消息。

|    |                                    |
|----|------------------------------------|
| 语法 | show trace [ <i>number-lines</i> ] |
|----|------------------------------------|

|        |                                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|
| 参数     | <code>number-lines</code> — (可选) 输入要包括在日志消息中的行数, 从 1 到 65535。                                                                               |
| 默认     | 已启用                                                                                                                                         |
| 命令模式   | EXEC                                                                                                                                        |
| 使用情况信息 | 此命令的输出为 <code>/var/log/syslog</code> 文件。<br>从版本 10.4.0E(R3S) 开始, 在全交换模式下的 MX9116n 和 MX5108n 交换机上受支持。从版本 10.5.0.1 开始, 在 SmartFabric 模式下也受支持。 |

## 示例

```
OS10# show trace
May 23 17:10:03 OS10 base_nas: [NETLINK:NH-
EVENT]:ds_api_linux_neigh.c:nl_to_nei
gh_info:109, Operation:Add-NH family:IPv4(2) flags:0x0 state:Failed(32)
if_idx:4
May 23 17:10:03 OS10 base_nas: [NETLINK:NH-
EVENT]:ds_api_linux_neigh.c:nl_to_nei
gh_info:120, NextHop IP:192.168.10.1
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Values are invalid - can't
be conv
erted to SAI types (func:2359304)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Hash value - 20 can't be
converted
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Values are invalid - can't
be conv
erted to SAI types (func:2359305)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Values are invalid - can't
be conv
erted to SAI types (func:2359311)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Hash value - 20 can't be
converted
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Values are invalid - can't
be conv
erted to SAI types (func:2359312)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Invalid operation type for
NDI (23
59344)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Invalid operation type for
NDI (23
59345)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Invalid operation type for
NDI (23
59346)
May 23 17:10:04 OS10 base_nas: [NDI:NDI-SAI], Invalid operation type for
NDI (23
59319)
May 23 17:10:08 OS10 base_nas: [NETLINK:NH-
EVENT]:ds_api_linux_neigh.c:nl_to_nei
--More--
```

支持的版本 10.2.0E or later

## 登录 OS10 设备

Linux shell 访问仅用于故障处理和诊断目的。linuxadmin 同时用于默认用户名和密码。出于安全原因, 您必须使用 `system-user` 命令从命令行界面更改 linuxadmin 默认密码。

如果您在从 CLI 更改密码之前登录 Linux shell, 系统会提示您更改 Linux shell 中的密码。如果在 Linux shell 中更改密码, 请从 CLI 配置相同的密码, 以避免行为不一致。要保存新密码以供将来登录, 请输入 `write memory` 命令。

 **小心:** 从 Linux shell 更改系统状态可能会导致意外且不可预知的系统行为。请仅使用 Linux shell 命令来显示系统状态和变量, 或 Dell EMC 支持的指示。

```
OS10 login: linuxadmin
Password: linuxadmin >> only for first-time login
You are required to change your password immediately (root enforced)
Changing password for linuxadmin.
(current) UNIX password: linuxadmin
```

```
Enter new UNIX password: enter a new password
Retype new UNIX password: re-enter the new password
Linux OS10 3.16.7-ckt20 #1 SMP Debian 3.16.7-ckt20-1+deb8u4 (2017-05-01) x86_64
```

The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/\*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.

```

-* Dell EMC Network Operating System (OS10) *-
-* *-
-* Copyright (c) 1999-2017 by Dell Inc. All Rights Reserved. *-
-* *-

```

This product is protected by U.S. and international copyright and  
intellectual property laws. Dell EMC and the Dell EMC logo are  
trademarks of Dell Inc. in the United States and/or other  
jurisdictions. All other marks and names mentioned herein may be  
trademarks of their respective companies.

**linuxadmin@OS10:~\$**

要登录 OS10 并访问命令行界面，请在 Linux shell 提示符处输入 `su - admin`，然后输入 admin 密码。

```
linuxadmin@OS10:~$ su - admin
Password: admin
OS10#
```

## 常见问题

本部分包含已启用 ONIE 的设备的常见问题解答。

- **安装**包含有关如何进入 ONIE 的信息：重新引导后的安装模式、查找有关特定交换机的信息、如何登录 OS10 shell 等。
- **硬件**包含有关如何查看默认控制台设置、如何查看硬件警报和事件、如何查看 LED 状态等信息。
- **配置**包含有关如何进入 CONFIGURATION 模式、如何修改候选配置等信息。
- **安全**包含有关如何添加用户、对 RADIUS 进行故障处理、如何查看当前 DHCP 信息等信息。
- **第 2 层**包含有关如何配置 802.1x、LACP、LLDP、MAC 等路由信息的信息。
- **第 3 层**包含有关如何对 BCP、ECMP、OSPF 等进行故障处理的信息。
- **系统管理**包含有关如何查看当前接口配置信息、如何查看所有系统设备的列表、如何查看软件版本等信息。
- **服务质量**包含有关服务质量的信息：分类和标记、拥塞管理、监察和整形等。
- **监控**包含有关如何查看警报、事件、日志等信息。

## 安装

### 如何配置默认管理路由？

虽然在安装期间配置了默认管理路由，但您可以使用 Linux shell 中的 `route add default gw` 命令来配置路由的默认管理 IP 地址。SupportAssist 需要将默认管理路由配置为正常工作，以及 DNS 配置和代理服务器的路由。

### 如何以系统管理方式登录 OS10 shell？

linuxadmin 用作在根级别进入 OS10 的用户名和密码。

### 在哪里可以找到特定设备的其他安装信息？

请参阅您的设备随附的 *安装指南* 或 Dell EMC 支持页面上特定于平台的 *安装指南*，网址为 [dell.com/support](http://dell.com/support)。

## 硬件

**用于 ON-Series 设备的默认控制台设置是什么？**

- 将数据速率设置为 115200 波特。
- 将数据格式设置为 8 位，停止位为 1，无奇偶校验
- 将流控制设置为无

**如何查看硬件资源清单？**

使用 `show inventory` 命令可查看完整的系统资源清单。

**如何查看与进程相关的信息？**

使用 `show processes node-id node-id-number [pid process-id]` 命令可查看进程 CPU 利用率信息。

## 配置

**如何进入 CONFIGURATION 模式？**

使用 `configure terminal` 命令可从 EXEC 模式更改为 CONFIGURATION 模式。

**我对正在运行的配置文件进行了更改，但未显示更新。如何查看更改？**

使用 `show running-configuration` 命令可查看对正在运行的配置文件所做的更改。以下是可用配置文件之间的差异：

- 启动配置中包含在设备启动时应用的配置
- 正在运行的配置中包含设备的当前配置
- 候选配置是一个中间临时缓冲区，在将配置更改应用到正在运行的配置之前将其进行存储

## 安全性

**如何添加新用户？**

使用 `username` 命令可添加新用户。使用 `show users` 命令可查看当前用户的列表。

**如何查看 RADIUS 的事务以解决问题？**

使用 `debug radius` 命令。

**如何查看当前 DHCP 绑定信息？**

使用 `show ip dhcp binding` 命令。

## 第 2 层

**如何查看 VLAN 运行的配置？**

使用 `show vlan` 命令可查看所有已配置的 VLAN。

## 第 3 层

**如何查看 IPv6 接口信息？**

使用 `show ipv6 route summary` 命令。

**如何查看所有 IP 路由的摘要信息？**

使用 `show running-configuration` 命令。

**如何查看 OSPF 数据库的摘要信息？**

使用 `show ip ospf database` 命令。

**如何查看连接到本地路由器的 OSPF 邻居的配置？**

使用 `show ip ospf neighbor` 命令。

## 系统管理

### 如何查看当前接口配置？

使用 `show running-configuration` 命令可以查看当前配置的所有接口。

### 如何查看所有系统设备的列表？

使用 `show inventory` 命令可以查看完整列表。

### 如何查看软件版本？

使用 `show version` 命令可以查看当前运行的软件版本。

## 访问控制列表

### 如何设置筛选器以拒绝或允许来自 IPv4 或 IPv6 地址的数据包？

使用 `deny` 或 `permit` 命令创建 ACL 筛选器。

### 如何清除访问列表计数器？

使用 `clear ip access-list counters`、`clear ipv6 access-list counters` 或 `clear mac access-list counters` 命令。

### 如何设置筛选器以自动分配特定地址的定序器编号？

将 `seq deny` 或 `seq permit` 命令用于特定数据包过滤。

### 如何查看访问列表和访问组信息？

使用 `show {ip | mac | ipv6} access-group` 和 `show {ip | mac | ipv6} access-list` 命令。

## 服务质量

### QoS 错误消息是什么？

流控制错误消息：

- `Error: priority-flow-control mode is on, disable pfc mode to enable LLFC`
- `% Warning: Make sure all qos-groups are matched in a single class in attached policy-map`

优先级流控制模式错误消息：

`% Error: LLFC flowcontrol is on, disable LLFC to enable PFC`

PFC 共享缓冲区大小错误消息：

`% Error: Hardware update failed.`

暂停错误消息：

`% Error: Buffer-size should be greater than Pause threshold and Pause threshold should be greater than equal to Resume threshold.`

服务错误消息的 PFC 成本：

- `% Error: Not enough buffers are available, to enable system-qos wide pause for all pfc-cos values in the policymap`
- `% Error: Not enough buffers are available, to enable system-qos wide pause for the pfc-cos values in the policymap`
- `% Error: Not enough buffers are available, to enable pause for all pfc-cos values in the policymap for this interface`
- `% Warning: Not enough buffers are available, for lossy traffic. Expect lossy traffic drops, else reconfigure the pause buffers`

## 监控

### 如何检查 SupportAssist 是否已启用？

使用 `show support-assist status` 命令可查看当前的配置信息。

### **如何查看警报列表？**

使用 `show alarms details` 可查看所有系统警报的列表。

### **如何启用或禁用系统日志记录？**

使用 `logging enable` 命令或 `logging disable` 命令。

### **如何查看系统日志记录消息？**

使用 `show logging` 命令可按日志文件或进程名称查看消息。



## 支持资源

Dell EMC 支持站点提供了一系列说明文件和工具，帮助您有效地使用 Dell EMC 设备。通过支持网站，您可以获得有关 Dell EMC Networking 产品的技术信息、获取软件升级和增补软件、下载可用的管理软件并管理打开的案例。Dell EMC 支持站点提供面向这些服务的安全的集成访问。

要访问 Dell EMC 支持站点，请转到 [www.dell.com/support/](http://www.dell.com/support/)。要以您的语言显示信息，请向下滚动到页面的底部，然后从下拉菜单中选择您所在的国家或地区。

- 要获取特定于产品的信息，请输入交换机的 7 字符服务编号或 11 位快速服务代码，然后单击**提交**。

要查看服务编号或快速服务代码，请拉出机箱上的标签或从 CLI 输入 `show chassis` 命令。

- 要接收更多种类的技术支持，请单击**联系我们**，或者单击**技术支持**。

要访问系统文档，请参阅 [www.dell.com/manuals/](http://www.dell.com/manuals/)。

要搜索驱动程序和下载，请参阅 [www.dell.com/drivers/](http://www.dell.com/drivers/)。

要参加 Dell EMC 社区博客和论坛，请参阅 [www.dell.com/community](http://www.dell.com/community)。