Dell™ PowerConnect™ 6024/6024F Systems

CLI Reference Guide

www.dell.com | support.dell.com

Notes, Notices, and Cautions

NOTE: A NOTE indicates important information that helps you make better use of your computer.

NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

⚠ **CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.**

Information in this document is subject to change without notice.

April 2005 Rev. A04

Contents

1 Command Groups

5 Address Table Commands

6 Clock

12 IGMP Snooping Commands

13 IP Routing Protocol-Independent Commands

14 LACP Commands

15 Line Commands

16 Management ACL

17 Multicast Routing Commands

19 PHY Diagnostics Commands

20 Port Channel Commands

21 Port Monitor Commands

22 QoS Commands

24 RIP Commands

25 RMON Commands

26 SNMP Commands

27

28 Spanning-Tree Commands

29 SSH Commands

30 Syslog Commands

33 User Interface

34 VLAN Commands

36 Web Server

37 802.1x Commands

1

Command Groups

Introduction

The Command Language Interface (CLI) is a network management application operated through an ASCII terminal without the use of a Graphic User Interface (GUI) driven software application. By directly entering commands, the user has greater configuration flexibility. The CLI is a basic command-line interpreter similar to the UNIX C shell.

A device can be configured and maintained by entering commands from the CLI, which is based solely on textual input and output with commands being entered by a terminal keyboard and the output displayed as text via a terminal monitor. The CLI can be accessed from a console terminal connected to an EIA/TIA-232 port or through a Telnet session.

This guide describes how the Command Line Interface (CLI) is structured, describes the command syntax, and describes the command functionality.

This guide also provides information for configuring the PowerConnect switch, details the procedures and provides configuration examples. Basic installation configuration is described in the *User's Guide* and must be completed before using this document.

Command Groups

The system commands can be broken down into the functional groups shown below.

Command Group	Description
AAA	Configures connection security including authorization and passwords.
ACL	Configures and displays ACL information.
Address Table	Configures bridging address tables.
Clock	Configures the system clock.
Configuration and Image Files	Manages the device configuration files.
DHCP Relay	Configures DHCP relay on the device.
Ethernet Configuration	Configures all port configuration options for example ports, storm control, port speed and auto-negotiation.
GVRP	Configures and displays GVRP configuration and information.
IGMP Snooping	Configures IGMP snooping and displays IGMP configuration and IGMP information.
IP Addressing	Configures and manages IP addresses on the device.
IP Routing	Configures routing configuration.
LACP	Configures and displays LACP information.

Line	Configures the console and remote Telnet connection.
Management ACL	Configures and displays management access-list information.
Multicast Routing	Configures Multicast routing.
OSPF	Configures and manages OSPF on the device.
PHY Diagnostics	Diagnoses and displays the interface status.
Port Channel	Configures and displays Port channel information.
Port Monitor	Monitors activity on specific target ports.
QoS	Configures and displays QoS information.
RADIUS	Configures and displays RADIUS information.
RIP	Configures RIP.
RMON	Displays RMON statistics.
SNMP	Configures SNMP communities, traps and displays SNMP information.
Spanning Tree	Configures and reports on Spanning Tree protocol.
SSH	Configures SSH authentication.
Syslog Commands	Manages and displays syslog messages.
System Management	Configures the device clock, name and authorized users.
TACACS+	Configures and displays TACACS+ information.
User Interface	Describes user commands used for entering CLI commands.
VLAN	Configures VLANs and displays VLAN information.
VRRP	Configures and manages VRRP on the device.
Web Server	Configures Web based access to the device.
802.1x	Configures commands related to 802.1x security protocol

NOTE: The access mode shown in the following tables is indicated by these abbreviations: UE (User EXEC Mode), PE (Privileged EXEC Mode), GC (Global Configuration Mode), IC (Interface Configuration Mode), LC (Line Configuration) MA (Management Access-level), KC (Key Chain), KE (Key), VC (VLAN Configuration), ML (MAC-List Configuration), MT (MAC-acl), SP (SSH Public Key), SK (SSH Public Key-chain), PM (Policy Map Configuration), OV (OSPF Virtual Link), IP (IP Access List Configuration) and MC (MST Configuration Mode).

AAA Commands

Command Group	Description	Mode
aaa authentication login	Defines login authentication.	GC
aaa authentication enable	Defines authentication method lists for accessing higher privilege levels.	GC
login authentication	Specifies the login authentication method list for a remote telnet or console.	GC
enable authentication	Specifies the authentication method list when accessing a higher privilege level from a remote telnet or console.	LC
ip http authentication	Specifies authentication methods for http.	GC
ip https authentication	Specifies authentication methods for https.	GC
password	Specifies a password on a line.	LC
enable password	Sets a local password to control access to normal and privilege levels.	GC
username	Establishes a username-based authentication system.	GC
passwords min-length	Sets the minimum length for passwords in the local database.	GC
password-aging	Sets the expiration time for line passwords in the local database.	LC
passwords aging	Sets the expiration time for username and enable passwords	GC
passwords history	Sets the number of required password changes before a password in the local database can be reused.	GC
passwords history hold-time	Sets the time period during which a password is relevant for tracking its password history.	GC
passwords history hold-time	Sets the number of failed login attempts before a user account is locked.	GC
aaa login-history file	Enables writing to the login history file.	GC
set username active	Reactivates a locked user account.	PE
set line active	Reactivates a locked user account.	PE
set enable-password active	Reactivates a locked local password.	PE
show authentication methods	Displays information about the authentication methods.	PE
show users accounts	Displays information about the local user database.	PE
show passwords configuration	Displays information about password management.	PE
show users login-history	Displays information about the login history of users.	PE

ACL Commands

Command Group	Description	Mode
ip access-list	Creates IP ACLs, and enters to IP-Access list configuration mode.	GC
permit (IP)	Allows traffic if the conditions defined in the permit statement are matched.	IP
deny (IP)	Denies traffic if the conditions define in the deny statement are matched	IP
mac access-list	Creates Layer 2 MAC ACLs, and enters to MAC-Access list configuration mode.	GC
permit (MAC)	Allows traffic if the conditions defined in the permit statement are matched.	MT
deny (MAC)	Allows traffic if the conditions defined in the permit statement are matched.	MT
service-acl	Applies an access-list to the input of an interface.	IC
show access-lists	Displays access control lists (ACLs) defined on the switch.	PE
show interfaces access-lists	Displays access lists applied on interfaces.	PE

Address Table Commands

Command Group	Description	Mode
bridge address	Adds a static MAC-layer station source address to the bridge table.	VC
bridge multicast filtering	Enables filtering of Multicast addresses.	GC
bridge multicast address	Registers MAC-layer Multicast addresses to the bridge table, and adds static ports to the group.	VC
bridge multicast forbidden address	Forbids adding a specific Multicast address to specific ports.	VC
bridge multicast forward-all	Enables forwarding of all Multicast packets on a port.	VC

bridge multicast forbidden forward-all	Enables forbidding forwarding of all Multicast packets to a port.	VC
bridge aging-time	Sets the address table aging time.	GC
clear bridge	Removes any learned entries from the forwarding database.	PE
port security	Disables new address learning on an interface.	IC
port security routed secure-address	Adds MAC-layer secure addresses to a routed port.	IC
show bridge address-table	Displays dynamically created entries in the bridge-forwarding database.	PE
show bridge address-table static	Displays statically created entries in the bridge-forwarding database.	PE
show bridge multicast address-table	Displays Multicast MAC address table information.	PE
show bridge multicast filtering	Displays the Multicast filtering configuration.	PE
show ports security	Displays the port-lock status.	PE

Clock Commands

Command Group	Description	Mode
clock source	Configures an external time source to maintain the system clock	GC
clock timezone	Defines the time zone for display purposes	GC
clock summer-time	Configures the system clock to automatically switch to Daylight Savings Time	GC
sntp authentication-key	Defines an authentication key for SNTP	GC
sntp authenticate	Set to require authentication for received NTP traffic from servers	GC
sntp trusted-key	Defines the authentication key used to authenticate the SNTP server	GC
sntp client poll timer	Defines polling time for the SNTP client.	GC
sntp broadcast client enable	Enables SNTP Broadcast clients	GC
sntp anycast client enable	Enables SNTP Anycast clients	GC
sntp client enable	Enables SNTP Broadcast and Anycast clients on an interface	IC
sntp unicast client enable	Enables predefined SNTP Broadcast Unicast clients	GC
sntp unicast client poll	Enables polling predefined SNTP Broadcast Unicast clients	GC
sntp server	Configures the device to use SNTP to request and accept NTP traffic from a server	GC
show clock	Displays the time and date of the system clock	UE

show sntp configuration	Displays the SNTP configuration	PE
show sntp status	Displays the SNTP status	PE

Configuration and Image Files Commands

Command Group	**Description**	**Mode**
configure	Enters the global configuration mode.	PE
copy	Copies files from a source to a destination.	PE
delete startup-config	Deletes the startup-config file.	PE
boot system	Specifies the system image that the device loads at startup.	PE
show running-config	Displays the contents of the currently running configuration file.	PE
show startup-config	Displays the startup configuration file contents.	PE
show backup-config	Displays the backup configuration file contents.	PE
show bootvar	Displays the active system image file that the device loads at startup.	PE

DHCP Relay Commands

Command Group	**Description**	**Mode**
ip dhcp relay enable	Enables DHCP relay features on the router.	GC
ip dhcp relay address	Defines the DHCP address available for the DHCP relay.	GC
show ip dhcp relay	Displays the DHCP relay server addresses.	PE

Ethernet Configuration Commands

Command Group	**Description**	**Mode**
interface ethernet	Enters the interface configuration mode to configure an Ethernet type interface.	GC
interface range ethernet	Enters the interface configuration mode to configure multiple Ethernet type interfaces.	GC
interface out-of-band-eth	Configures the out-of-band Ethernet port and enter interface configuration mode.	IC
shutdown	Disables interfaces.	IC
description	Adds a description to an interface.	IC

speed	Configures the speed of a given Ethernet interface when not using auto-negotiation.	IC
duplex	Configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation.	IC
negotiation	Enables auto-negotiation operation for the speed and duplex parameters of a given interface.	IC
flowcontrol	Configures the Flow Control on a given interface.	IC
mdix	Enables automatic crossover on a given interface.	IC
back-pressure	Enables Back Pressure on a given interface.	IC
port jumbo-frame	Enables jumbo frames for the device.	GC
clear counters	Clears statistics on an interface.	UE
set interface active	Reactivates an interface that was suspended by the system.	PE
show interfaces configuration	Displays the configuration for all configured interfaces.	UE
show interfaces status	Displays the status for all configured interfaces.	UE
show interfaces description	Displays the description for all configured interfaces.	UE
show interfaces counters	Displays traffic seen by the physical interface.	UE
show ports jumbo-frame	Displays the jumbo frames configuration.	UE
port storm-control include-multicast	Enables the device to count Multicast packets.	GC
port storm-control broadcast enable	Enables Broadcast storm control.	IC
port storm-control broadcast rate	Configures the maximum Broadcast rate.	IC
show ports storm-control	Displays the storm control configuration.	PE
show interfaces advertise	Displays information about auto negotiation advertisement.	PE

GVRP Commands

Command Group	Description	Mode
gvrp enable (global)	Enables GVRP globally.	GC
gvrp enable (interface)	Enables GVRP on an interface.	IC
garp timer	Adjusts the GARP application join, leave, and leaveall GARP timer values.	IC
gvrp vlan-creation-forbid	Enables or disables dynamic VLAN creation.	IC

gvrp registration-forbid	De-registers all VLANs, and prevents dynamic VLAN registration on the port.	IC
clear gvrp statistics	Clears all the GVRP statistics information.	GC
show gvrp configuration	Displays GVRP configuration information.	PE
show gvrp statistics	Displays GVRP statistics.	PE
show gvrp error-statistics	Displays GVRP error statistics.	UE

IGMP Snooping Commands

Command Group	Description	Mode
ip igmp snooping (Global)	Enables Internet Group Management Protocol (IGMP) snooping.	GC
ip igmp snooping (Interface)	Enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN.	VC
ip igmp snooping mrouter	Enables automatic learning of multicast router ports in the context of a specific VLAN.	VC
ip igmp snooping host-time-out	Configures the host-time-out.	VC
ip igmp snooping mrouter-time-out	Configures the mrouter-time-out.	VC
ip igmp snooping leave-time-out	Configures the leave-time-out.	VC
show ip igmp snooping mrouter	Displays information on dynamically learned Multicast router interfaces.	PE
show ip igmp snooping interface	Displays IGMP snooping configuration.	PE
show ip igmp snooping groups	Displays Multicast groups learned by IGMP snooping.	UE

IP Addressing

Command Group	Description	Mode
ip address	Sets an IP address on the device.	IC
ip address dhcp	Acquires an IP address on an interface from the DHCP server.	IC
show ip interface	Displays the usability status of interfaces configured for IP.	UE
arp	Adds a permanent entry in the ARP cache.	GC
arp timeout	Configures how long an entry remains in the ARP cache	GC
ip proxy-arp	Enables ARP proxy on the device.	GC
clear arp-cache	Deletes all dynamic entries from the ARP cache.	PE
show arp	Displays entries in the ARP table.	PE
directed-broadcast	Enables the translation of a directed Broadcast to physical broadcasts.	IC
broadcast-address	Defines an interface Broadcast address.	IC
helper-address	Enables the device to forward UDP broadcasts, including BOOTP, received on an interface.	IC
show ip helper-address	Displays IP helper address configuration.	PE
ip domain-lookup	Enables IP DNS-based host name-to-address translation.	GC

ip domain-name	Defines a default domain name to complete unqualified host names.	GC
ip name-server	Configures available name servers	GC
ip host	Configures static host name-to-address mapping in the host cache	GC
clear host	Deletes entries from the host name-to-address cache	PE
clear host dhcp	Deletes entries from the DHCP host name-to-address mapping cache	PE
show hosts	Displays the default domain name, a list of name server hosts, static and cached list of host names and addresses.	PE

IP Routing

Command Group	**Description**	**Mode**
interface ip	Configures an IP interface and enters the IP interface configuration mode.	GC
ip route	Establishes static IP routes on the device.	GC
key-chain	Defines authentication key group for routing protocols.	GC
key (key chain)	Defines an authentication key on a key chain.	KC
key (global)	Creates an authentication key on the device.	GC
key-string	Specifies an authentication string for a key.	KE
accept-lifetime	Sets the time period during which the authentication key on a key chain is valid to be received.	KC
send-lifetime	Sets the time period during which an authentication key on a key chain is valid for sending.	KC
ip maximum-paths	Defines the maximum number of parallel routes.	GC
show ip route	Displays the routing table current state.	UE
show ip protocols	Displays the parameters and current state of the active routing protocols.	PE
show key-chains	Displays key-chains information on the device.	PE
show keys	Displays key information.	PE

LACP Commands

Command Group	Description	Mode
lacp system-priority	Configures the system LACP priority.	GC
lacp port-priority	Configures the priority value for physical ports.	IC
lacp timeout	Assigns an administrative LACP timeout.	IC
show lacp ethernet	Displays LACP information for Ethernet ports.	PE
show lacp port-channel	Displays LACP information for a port-channel.	PE

Line Commands

Command Group	Description	Mode
line	Identifies a specific line for configuration and enters the line configuration command mode.	LC
speed	Sets the line baud rate.	LC
exec-timeout	Configures the interval that the system waits until user input is detected.	LC
terminal history	Enables the command history function for the current terminal session.	UE
terminal history size	Defines the command history buffer size for the current terminal session.	UE
show line	Displays line parameters.	UE

Management ACL Commands

Command Group	Description	Mode
management access-list	Defines a management access-list, and enters the access-list for configuration.	GC
permit (management)	Defines a permit rule.	MA
deny (management)	Defines a deny rule.	MA
management access-class	Defines which management access-list is used.	GC
show management access-list	Displays management access-lists.	PE
show management access-class	Displays the active management access-list.	PE

Multicast Routing

Command Group	Description	Mode
ip multicast-routing	Enables IP Multicast routing on the device.	GC
ip dvmrp	Enables DVMRP on an interface.	IC
ip dvmrp metric	Configures the interface metric for DVMRP reports.	IC
ip igmp	Enables IGMP on an interface.	IC
ip igmp query-interval	Configures the frequency at which the software sends IGMP host query messages.	IC
ip igmp last-member-query-interval	Configures the frequency at which the software sends Internet IGMP group-specific host query messages.	IC
ip igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.	IC
ip igmp version	Configures which version of IGMP the router uses.	IC
ip igmp static-group	Configures the router to be a statically connected member of the specified group on the interface.	IC
show ip mroute	Displays the IP Multicast routing table contents.	UE
show ip mroute-next-hop	Displays IP Multicast routing next hop information.	UE
show ip dvmrp interface	Displays DVMRP interface information.	UE
show ip dvmrp neighbor	Displays DVMRP-neighbor information on a per-interface basis.	UE
show ip dvmrp next-hop	Displays DVMRP-next-hop information on a per-interface basis.	UE
show ip dvmrp route	Displays the DVMRP routing table contents.	UE
show ip dvmrp prune	Displays the DVMRP upstream prune state.	UE
show ip igmp interface	Displays IGMP related information about an interface.	UE
show ip igmp groups	Displays the Multicast groups with receivers that are directly connected to the router, and that were learned through IGMP.	UE

OSPF

Command Group	Description	Mode
router ospf enable	Enables OSPF on the device.	GC
router ospf area	Defines an OSPF area on the device.	GC
router ospf redistribute rip	Advertises routes, that are learned by the RIP process, while running OSPF.	GC
router ospf redistribute static	Advertises routes, configured statically, while running OSPF.	GC

router ospf redistribute connected	Enables advertisements of directly connected networks routes, running OSPF.	GC
router ospf area virtual-link	Defines an OSPF virtual link and enters the OSPF Virtual-link Configuration mode.	GC
hello-interval	Specifies the interval between hello packets that the software sends on the OSPF virtual link interface.	OV
dead-interval	Sets the interval at which hello packets must not be seen before its neighbors declare the router down.	OV
retransmit-interval	Specifies the time between LSA retransmissions for adjacencies belonging to the OSPF virtual link interface.	OV
transmit-delay	Sets the estimated time required to send a link-state update packet on the OSPF virtual link interface.	OV
authentication	Enables authentication for OSPF packets and specifies the type of authentication.	OV
router ospf router-id	Configures an OSPF router ID.	GC
router ospf area stub	Defines an area as a stub area.	GC
router ospf area default-cost	Specifies a cost for the default summary route sent into a stub area.	GC
ospf	Creates OSPF routing process on an interface.	IC
ospf enable	Activates OSPF on an interface.	IC
ospf area	Defines an interface area ID.	IC
ospf cost	Specifies the cost of sending a packet on an interface.	IC
ospf priority	Sets the router priority, which determines the designated router for the network.	IC
ospf hello-interval	Specifies the interval between hello packets the software sends on an interface.	IC
ospf dead-interval	Sets the interval at which hello packets must not be seen before neighbors declare the router down.	IC
ospf retransmit-interval	Specifies the time between LSA retransmissions for interface adjacencies.	IC
ospf transmit-delay	Sets the estimated time required to send a link-state update packet on an interface.	IC
ospf authentication	Enables authentication for OSPF packets and specifies the authentication type.	IC
clear ip ospf process	Clears redistribution based on OSPF routing.	PE
show ip ospf	Displays general OSPF routing information.	UE
show ip ospf virtual-links	Displays parameters and the current state of OSPF virtual links.	UE

show ip ospf database	Displays information lists related to the OSPF database.	UE
show ip ospf interface	Displays OSPF-related interface information.	UE
show ip ospf neighbor	Displays OSPF-neighbor information on a per-interface basis.	UE

PHY Diagnostics Commands

Command Group	Description	Mode
test copper-port tdr	Diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.	PE
show copper-ports tdr	Displays the last TDR (Time Domain Reflectometry) tests on specified ports.	PE
show copper-ports cable-length	Displays the estimated copper cable length attached to a port.	PE
show fiber-ports optical-transceiver	Displays the optical transceiver diagnostics.	PE

Port Channel Commands

Command Group	Description	Mode
interface port-channel	Enters the interface configuration mode of a specific port-channel.	GC
interface range port-channel	Enters the interface configuration mode to configure multiple port-channels.	GC
channel-group	Associates a port with a port-channel.	IC
show interfaces port-channel	Displays port-channel information.	PE

Port Monitor Commands

Command Group	Description	Mode
port monitor	Starts a port monitoring session.	IC
port monitor vlan-tagging	Transmits tagged ingress mirrored packets.	IC
show ports monitor	Displays the port monitoring status.	UE

QoS Commands

Command Group	Description	Mode
qos	Enables quality of service (QoS) on the device and enters QoS basic or advance mode.	GC
show qos	Displays the QoS status.	UE
priority-queue out num-of-queues	Enables the egress queues to be expedite queues.	GC
traffic-shape	Sets a shaper on an egress port/queue.	IC
qos wrr-queue threshold	Assigns the tail-drop mechanism on an egress queue and configures the tail-drop thresholds.	GC
wrr-queue bandwidth	Assigns Weighted Round Robin (WRR) weights to egress queues.	IC
wrr-queue	Defines the wrr-queue mechanism on an egress queue.	IC
show qos interface	Displays interface QoS data.	UE
qos map dscp-queue	Modifies the DSCP to CoS map.	GC
qos map tcp-port-queue	Modifies the TCP-Port to DSCP table.	GC
qos map udp-port-queue	Modifies the UDP-Port to DSCP table.	GC
wrr-queue cos-map	Assigns CoS values to select one of the egress queues.	GC
show qos map	Displays all the QoS maps.	PE
qos trust (Global)	Configures the system to basic mode and the "trust" state.	GC
qos trust (Interface)	Enables each port trust state while the system is in basic mode.	IC
qos cos	Configures the default port CoS value.	IC
qos dscp-mutation	Modifies the DSCP to DSCP mutation map.	GC
qos map dscp-mutation	Modifies the DSCP values to the DSCP mutation map values.	GC
qos aggregate-policer	Defines the policer parameters that can be applied to multiple traffic classes within the same policy map.	GC
show qos aggregate-policer	Displays the aggregate policer parameter.	UE
qos map policed-dscp	Modifies the policed-DSCP map for remarking purposes.	GC
class-map	Creates class maps and enters the class-map configuration mode.	GC
show class-map	Displays all the class maps configured on the device.	UE
match	Defines the match criterion to classify traffic.	MT
policy-map	Creates policy maps and enters policy-map configuration mode.	GC
show policy-map	Displays the defined policy maps.	UE

class	Defines the traffic classification and enters the policy-map class configuration mode.	PM
police	Defines a policer for the classified traffic.	PM
police aggregate	Applies an aggregate policer to multiple classes within the same policy map.	PM
trust	Configures the trust state.	PM
set	Sets new values in the IP packet.	PM
service-policy	Applies a policy map to the interface input.	IC

Radius Commands

Command Group	Description	Mode
radius-server host	Specifies a RADIUS server host.	GC
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.	GC
radius-server retransmit	Specifies the number of times the software searches the list of RADIUS server hosts.	GC
radius-server source-ip	Specifies the source IP address used for communication with RADIUS servers.	GC
radius-server timeout	Sets the interval for which a router waits for a server host to reply.	GC
radius-server deadtime	Improves RADIUS response times when servers are unavailable.	GC
show radius-servers	Displays the RADIUS server settings.	UE

RIP Commands

Command Group	Description	Mode
router rip enable	Enables the RIP on the device.	GC
router rip redistribute ospf	Advertises routes learned by OSPF in the RIP process.	GC
router rip redistribute static	Advertises routes statically learned in the RIP process.	GC
rip	Creates a Routing Information Protocol (RIP) process on an interface.	IC
rip passive-interface	Disables the sending of routing updates on an interface.	IC
rip auto-send	Automatically detects if RIP information is required to be sent on the interface.	IC
rip version	Specifies a RIP version.	IC

rip offset	Adds an offset to a metric learned via RIP before adding them to the interface table.	IC
rip default-route offset	Generates a default route into RIP.	IC
rip authentication	Enables authentication for RIP Version 2 packets and specifies the authentication type.	IC
show ip rip	Displays RIP routing information.	PE

RMON Commands

Command Group	Description	Mode
show rmon statistics	Displays RMON Ethernet Statistics.	UE
rmon collection history	Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.	IC
show rmon collection history	Displays the requested history group configuration.	UE
show rmon history	Displays RMON Ethernet Statistics history.	UE
rmon alarm	Configures alarm conditions.	GC
show rmon alarm-table	Displays the alarms summary table.	UE
show rmon alarm	Displays alarm configurations.	UE
rmon event	Configures a RMON event.	GC
show rmon events	Displays the RMON event table.	UE
show rmon log	Displays the RMON logging table.	UE
rmon table-size	Configures the maximum RMON tables sizes.	GC

SNMP Commands

Command Group	Description	Mode
snmp-server community	Sets up the community access string to permit access to SNMP protocol.	GC
snmp-server contact	Sets up a system contact.	GC
snmp-server location	Sets up the information on where the device is located.	GC
snmp-server enable traps	Enables the switch to send SNMP traps or SNMP notifications.	GC
snmp-server trap authentication	Enables the switch to send SNMP traps when authentication failed.	GC
snmp-server host	Specifies the recipient of SNMP notifications.	GC
snmp-server set	Sets SNMP MIB value by the CLI.	GC

snmp-server user	Creates or updates an SNMP server view entry.	GC
snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.	GC
snmp-server user	Configures a new SNMP Version 3 user.	GC
snmp-server v3-host	Specifies the SNMP engine ID on the local device.	GC
snmp-server filter	Creates or updates an SNMP server filter entry.	GC
snmp-server v3-host	Specifies the recipient of SNMPv3 notifications.	GC
show snmp	Displays the SNMP status.	PE
show snmp engineID	Displays the SNMP engine ID.	PE
show snmp users	Displays the configuration of views.	PE
show snmp groups	Displays the configuration of groups.	PE
show snmp filters	Displays the configuration of filters.	PE
show snmp users	Displays the configuration of users.	PE

Spanning Tree Commands

Command Group	**Description**	**Mode**
spanning-tree	Enables spanning tree functionality.	GC
spanning-tree mode	Configures the spanning tree protocol.	GC
spanning-tree forward-time	Configures the spanning tree bridge forward time.	GC
spanning-tree hello-time	Configures the spanning tree bridge Hello Time.	GC
spanning-tree max-age	Configures the spanning tree bridge maximum age.	GC
spanning-tree priority	Configures the spanning tree priority.	GC
spanning-tree disable	Disables spanning tree on a specific port.	IC
spanning-tree cost	Configures the spanning tree path cost for a port.	IC
spanning-tree pathcost method	Configures the spanning tree default pathcost method	GC
spanning-tree port-priority	Configures port priority.	IC
spanning-tree portfast	Enables PortFast mode.	IC
spanning-tree link-type	Overrides the default link-type setting.	IC
spanning-tree bpdu	Defines BPDU handling when spanning tree is disabled on an interface.	GC
clear spanning-tree detected-protocols	Restarts the protocol migration process on all interfaces or on the specified interface.	PE

spanning-tree mst priority	Configures the switch priority for the specified spanning tree instance.	GC
spanning-tree mst max-hops	Configures the number of hops in an MST region before the BDPU is discarded and port information is aged out.	GC
spanning-tree mst port-priority	Configures port priority.	IC
spanning-tree mst cost	configures the path cost for multiple spanning tree (MST) calculations	IC
spanning-tree mst configuration	Enables configuring an MST region by entering the multiple spanning-tree (MST) mode.	GC
instance (mst)	Maps VLANS to an MST instance.	MC
name (mst)	Defines the MST configuration name.	MC
revision (mst)	Defines the configuration revision number..	MC
show (mst)	Displays the current or pending MST region configuration	MC
exit (mst)	Exits the MST configuration mode and applies configuration changes.	MC
abort (mst)	Exits the MST configuration mode without applying configuration changes.	MC
show spanning-tree	Displays spanning tree configuration.	PE

SSH Commands

Command Group	**Description**	**Mode**
ip ssh port	Specifies the port to be used by the SSH server.	GC
ip ssh server	Enables the device to be configured from a SSH server.	GC
crypto key generate dsa	Generates DSA key pairs.	GC
crypto key generate rsa	Generates RSA key pairs.	GC
ip ssh pubkey-auth	Enables public key authentication for incoming SSH sessions.	GC
crypto key pubkey-chain ssh	Enters SSH Public Key-chain configuration mode.	GC
user-key	Specifies which SSH public key is manually configured and enters the SSH public key-string configuration command.	SP
key-string	Manually specifies a SSH public key.	SK
show ip ssh	Displays the SSH server configuration.	PE
show crypto key mypubkey	Displays the SSH public keys stored on the device.	PE
show crypto key pubkey-chain ssh	Displays SSH public keys stored on the device.	PE

Syslog Commands

Command Group	Description	Mode
logging on	Controls error messages logging.	GC
logging	Logs messages to a syslog server.	GC
logging console	Limits messages logged to the console based on severity.	GC
logging buffered	Limits syslog messages displayed from an internal buffer based on severity.	GC
logging buffered size	Changes the number of syslog messages stored in the internal buffer.	GC
clear logging	Clears messages from the internal logging buffer.	PE
logging file	Limits syslog messages sent to the logging file based on severity.	GC
clear logging file	Clears messages from the logging file.	PE
aaa logging	Enables logging AAA login events.	GC
file-system logging	Enables logging file system events.	GC
management logging	Enables logging management access list (ACL) events.	GC
show logging	Displays the state of logging and the syslog messages stored in the internal buffer.	PE
show logging file	Displays the state of logging and the syslog messages stored in the logging file.	PE
show syslog-servers	Displays the syslog servers settings.	PE

System Management Commands

Command Group	Description	Mode
ping	Sends ICMP echo request packets to another node on the network.	UE
reload	Reloads the operating system.	PE
clock set	Manually sets the system clock.	PE
hostname	Specifies or modifies the device host name.	GC
asset-tag	Specifies the device asset-tag.	GC
show users	Displays information about the active users.	UE
show clock	Displays the time and date from the system clock.	UE
show system	Displays system information.	UE
show version	Displays the system version information.	UE
show system id	Displays the service ID information.	PE

traceroute	Discovers the IP routes that packets actually take when travelling to their destinations.	UE
telnet	Logs into a host that supports Telnet.	UE
resume	Switches to another open Telnet session.	UE

TACACS+ Commands

Command Group	Description	Mode
tacacs-server host	Specifies a TACACS+ server host.	GC
tacacs-server key	Sets the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon.	GC
tacacs-server source-ip	Specifies the source IP address used for communication with TACACS+ servers.	GC
tacacs-server timeout	Sets the interval for which the switch waits for a server host to reply.	GC
show tacacs	Displays TACACS+ server settings and statistics.	PE

User Interface Commands

Command Group	Description	Mode
enable	Enters the privileged EXEC mode.	UE
disable	Returns to User EXEC mode.	PE
login	Changes a login username.	UE
exit(configuration)	Exits any configuration mode to the previously highest mode in the CLI mode hierarchy.	(All)
exit(EXEC)	Closes an active terminal session by logging off the device.	UE
end	Ends the current configuration session and returns to the previous command mode.	GC
help	Displays a brief description of the help system.	(All)
history	Enables the command history function.	LC
history size	Changes the command history buffer size for a particular line.	LC
debug-mode	Switches the mode to debug.	PE
show history	Lists the commands entered in the current session.	UE
show privilege	Displays the current privilege level.	UE

VLAN Commands

Command Group	Description	Mode
vlan database	Enters the VLAN database configuration mode.	GC
vlan	Creates a VLAN.	VC
interface vlan	Enters the interface configuration (VLAN) mode.	GC
interface range vlan	Enters the interface configuration mode to configure multiple VLANs.	GC
name	Configures a name to a VLAN.	VC
switchport mode	Configures the VLAN membership mode of a port.	IC
switchport access vlan	Configures the VLAN ID when the interface is in access mode.	IC
switchport trunk allowed vlan	Adds or removes VLANs from a port in general mode.	IC
switchport trunk native vlan	Defines the port as a member of the specified VLAN, and the VLAN ID is the "port default VLAN ID (PVID)".	IC
switchport general allowed vlan	Adds or removes VLANs from a general port.	IC
switchport general pvid	Configures the PVID when the interface is in general mode.	IC
switchport general ingress-filtering disable	Disables port ingress filtering.	IC
switchport general acceptable-frame-type tagged-only	Discards untagged frames at ingress.	IC
switchport forbidden vlan	Forbids adding specific VLANs to a port.	IC
switchport protected	Overrides the FDB decision and sends all Unicast, Multicast and Broadcast traffic to an uplink port.	IC
map protocol protocols-group	Adds a special protocol to a named group of protocols, which may be used for protocol-based VLAN assignment.	VC
switchport general map protocols-group vlan	Sets a protocol-based classification rule.	IC
show vlan	Displays VLAN information.	PE
show vlan internal usage	Displays a list of VLANs being used internally by the switch.	PE
show vlan protocols-groups	Displays protocols-groups information.	PE
show interfaces switchport	Displays switchport configuration.	PE

VRRP Commands

Command Group	Description	Mode
vrrp ip	Defines VRRP for an interface.	IC
vrrp up	Activates VRRP on an interface.	IC
vrrp timer	Configures the time between sending advertisements messages.	IC
vrrp priority	Configures VRRP priority on an interface.	IC
vrrp source-ip	Defines the source IP address used for VRRP messages on an interface.	IC
vrrp authentication	Enables authentication for the VRRP on an interface.	IC
vrrp preempt	Enables the VRRP preemption on an interface.	IC
show vrrp configuration	Displays the VRRP configuration.	PE
show vrrp status	Displays VRRP status.	PE

Web Server Commands

Command Group	Description	Mode
ip http port	Specifies the TCP port for use by a web browser to configure the device.	GC
ip http server	Enables the device to be configured from a browser.	GC
ip https port	Configures a TCP port for use by a secure web browser to configure the device.	GC
ip https server	Enables the device to be configured from a secured browser.	GC
crypto certificate generate	Generates a HTTPS certificate.	GC
crypto certificate request	Generates and displays a certificate request for HTTPS	PE
crypto certificate import	Imports a certificate signed by the Certification Authority for HTTPS	PE
ip https certificate	Configures the active certificate for HTTPS	GC
show ip http	Displays the HTTP server configuration.	PE
show ip https	Displays the HTTPS server configuration.	PE

802.1x Commands

Command Group	Description	Mode
aaa authentication dot1x	Specifies one or more authentication, authorization and accounting (AAA) methods for use on interfaces running IEEE802.1X.	GC
dot1x system-auth-control	Enables 802.1x globally.	GC
dot1x port-control	Enables manual control of the authorization state of the port.	IC
dot1x re-authentication	Enables periodic re-authentication of the client.	IC
dot1x timeout re-authperiod	Sets the number of seconds between re-authentication attempts.	IC
dot1x re-authenticate	Manually initiates a re-authentication of all 802.1x-enabled ports or a specified 802-1x-enabled port.	PE
dot1x timeout quiet-period	Sets the number of seconds the device remains in the quiet state following a failed authentication attempt	IC
dot1x timeout tx-period	Sets the number of seconds the device waits for a response to an EAP-request/identify frame from the client before resending the request.	IC
dot1x max-req	Sets the maximum number of times the device sends an EAP-request frame to the client before restarting the authentication process.	IC
dot1x timeout supp-timeout	Sets the number of seconds the device waits for a response to an EAP-request frame from the client before retransmitting the request.	IC
dot1x timeout server-timeout	Sets the number of seconds the device waits for a response from the authentication server before resending the request.	IC
show dot1x	Displays 802.1x status for the device or the specified interface.	PE
show dot1x users	Displays active 802.1x authenticated users for the device.	PE
show dot1x statistics	Displays 802.1x statistics for the specified interface.	PE
dot1x auth-not-req	Enables unauthorized devices to access that VLAN.	VC
dot1x multiple-hosts	Allows multiple hosts (clients) on an 802.1x-authorized port where the dot1x port-control interface configuration command is set to auto.	IC
dot1x single-host-violation	Configures the action to be taken when a station with a MAC address that is not the supplicant MAC address attempts to access the interface.	IC
show dot1x advanced	Displays 802.1x advanced features for the device or specified interface.	PE

2

Using the CLI

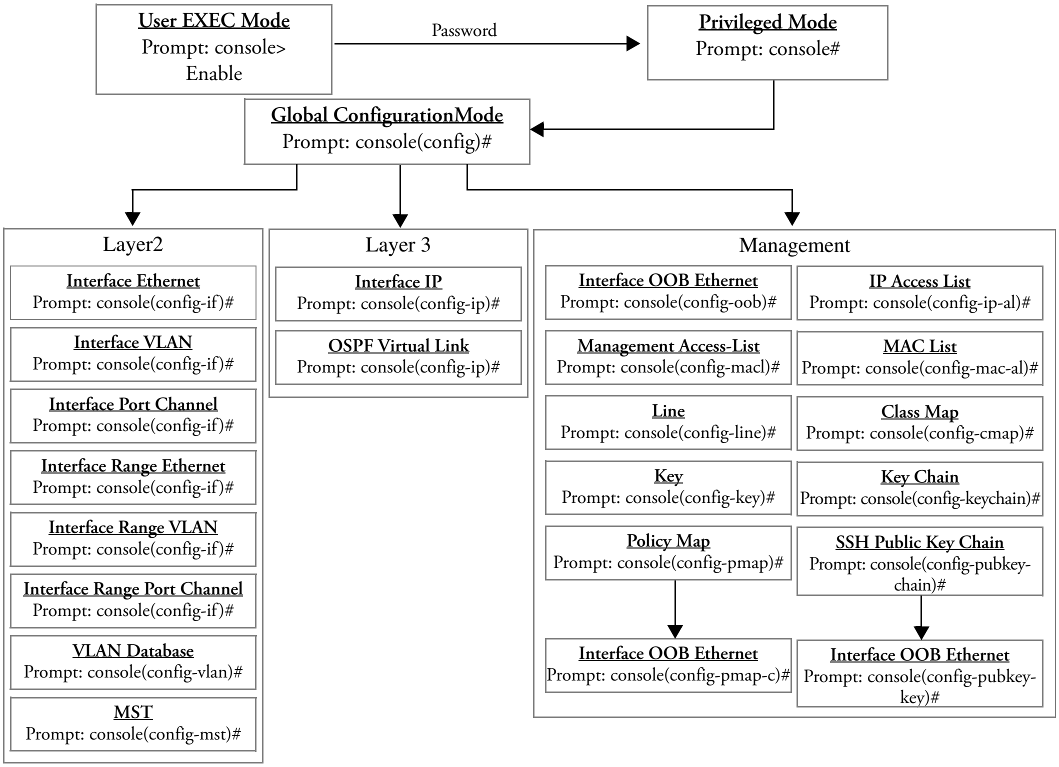
This chapter describes how to start using the CLI and describes implemented command editing features to assist in using the CLI.

CLI Command Modes

Introduction

To assist in configuring devices, the CLI command-line interface is divided into different command modes. Each command mode has its own set of specific commands. Entering a question mark "?" at the system prompt (console prompt) displays a list of commands available for that particular command mode.

From each mode a specific command is used to navigate from one command mode to another. The standard order to access the modes is as follows: User EXEC mode, Privileged EXEC mode, Global Configuration mode, and Interface Configuration mode. The following figure illustrates the command mode access path.


User EXEC Mode
Prompt: console>
Enable
Password
Privileged Mode
Prompt: console#
Global ConfigurationMode
Prompt: console(config)#
Layer2
Interface Ethernet
Prompt: console(config-if)#
Interface VLAN
Prompt: console(config-if)#
Interface Port Channel
Prompt: console(config-if)#
Interface Range Ethernet
Prompt: console(config-if)#
Interface Range VLAN
Prompt: console(config-if)#
Interface Range Port Channel
Prompt: console(config-if)#
VLAN Database
Prompt: console(config-vlan)#
MST
Prompt: console(config-mst)#
Layer 3
Interface IP
Prompt: console(config-ip)#
OSPF Virtual Link
Prompt: console(config-ip)#
Management
Interface OOB Ethernet
Prompt: console(config-oob)#
IP Access List
Prompt: console(config-ip-al)#
Management Access-List
Prompt: console(config-macl)#
MAC List
Prompt: console(config-mac-al)#
Line
Prompt: console(config-line)#
Class Map
Prompt: console(config-cmap)#
Key
Prompt: console(config-key)#
Key Chain
Prompt: console(config-keychain)#
Policy Map
Prompt: console(config-pmap)#
SSH Public Key Chain
Prompt: console(config-pubkey-chain)#
Interface OOB Ethernet
Prompt: console(config-pmap-c)#
Interface OOB Ethernet
Prompt: console(config-pubkey-key)#

When starting a session, the initial mode is the User EXEC mode. Only a limited subset of commands are available in this mode. This level is reserved for tasks that do not change the configuration. To enter the next level, the Privileged EXEC mode, a password is required.

The Privileged EXEC mode provides access to commands that are restricted on the User EXEC mode level and permits access to the device Configuration mode.

The Global Configuration mode manages device configuration on a global level. For specific interface configurations, enter the next level, the Interface Configuration mode.

The Interface Configuration mode configures specific interfaces in the device.

User EXEC Mode

After logging into the device, the user is automatically in the User EXEC command mode unless the user is defined as a privileged user. In general, the User EXEC commands allow the user to perform basic tests, and list system information.

The user-level prompt consists of the device "host name" followed by the angle bracket (>).

```
Console>
```

The default host name is "Console" unless it has been changed using the **hostname** command in the Global Configuration mode.

Privileged EXEC Mode

Because many of the privileged commands set operating parameters, privileged access is password protected to prevent unauthorized use. The password is not displayed on the screen and is case sensitive.

Privileged users enter directly into the Privileged EXEC mode. To enter Privileged EXEC mode commands from the User EXEC mode, perform the following:

1. At the prompt, enter the command **enable** and press <Enter>. A password prompt is displayed.
2. Enter the password and press <Enter>. The password is displayed as "*". The Privileged EXEC mode prompt is displayed. The Privileged EXEC mode prompt consists of the device "host name" followed by "#".

```
Console #
```

To return from the Privileged EXEC mode to the User EXEC mode, use the **disable** command. The following example illustrates how to access the Privileged EXEC mode and return to the User EXEC mode:

```
Console>enable

Enter Password: ******

Console #

Console # disable

Console>
```

Command **Exit** is used to move back from any mode to a previous level mode, except from Privileged EXEC to User EXEC mode, for example from Interface Configuration mode to Global Configuration mode, and from Global Configuration mode to Privileged EXEC mode.

Global Configuration Mode

Global configuration commands apply to features that affect the system as a whole, rather than just a specific interface. The Privileged EXEC mode command **configure** is used to enter the Global Configuration mode.

The Global Configuration mode commands perform the following:

1. At the Privileged EXEC mode prompt, enter the command **configure** and press <Enter>. The Global Configuration mode prompt is displayed. The Global Configuration mode prompt consists of the device "host name" followed by the word "(config)" and "**#**".

```
Console(config)#
```

To return from Global Configuration mode to Privileged EXEC mode, the user can use one of the following commands:

- **exit**
- **end**
- **Ctrl+Z**

The following example illustrates how to access the Global Configuration mode and return to the Privileged EXEC mode:

```
Console#

Console#configure

Console(config)#exit

Console#
```

Interface Configuration Mode and Specific Configuration Modes

Interface configuration modes are used to modify specific interface operations. The following are the Interface Configuration modes:

- **Line Interface**—Contains commands to configure the management connections. These include commands such as line speed, timeout settings, etc. The Global Configuration mode command **line** is used to enter the line configuration command mode.
- **VLAN Database**—Contains commands to create a VLAN as a whole. The Global Configuration mode command **vlan database** is used to enter the VLAN Database Interface Configuration mode.
- **Management Access List**—Contains commands to define management access-lists. The Global Configuration mode command **management access-list** is used to enter the Management Access List Configuration mode.
- **Policy-map Class**—Contains commands to configure QoS packet properties. The overall set of classification rules and their corresponding action (meter, security) are assigned to a specific port. The Global Configuration mode command **policy-map class** is used to enter the Policy-map Class Configuration mode.
- **Ethernet**—Contains commands to manage port configuration. The Global Configuration mode command **interface ethernet** enters the Interface Configuration mode to configure an Ethernet type interface.
- **Port Channel**—Contains commands to configure port-channels, for example, assigning ports to a VLAN or port-channel. Most of these commands are the same as the commands in the Ethernet interface mode, and are used to manage the member ports as a single entity. The Global Configuration mode command **interface port-channel** is used to enter the port-channel Interface Configuration mode.
- **Class-Map**—Contains commands to define a class map. Class maps consists of ACLs which define the matching criteria for determining a frames accessibility to the system. The Global Configuration mode command **class-map** is used to enter the Class-map Configuration mode.
- **SSH Public Key-chain**—Contains commands to manually specify other device SSH public keys. The Global Configuration mode command **crypto key pubkey-chain ssh** is used to enter the SSH Public Key-chain Configuration mode.
- **IP Access-List**—Contains commands to create and manage access lists. The Global Configuration mode command **ip access-list** is used to enter the IP access-list configuration mode.
- **MAC Access-List**—Configures conditions required to allow traffic based on MAC addresses. The Global Configuration mode command **mac access-list** is used to enter the MAC access-list configuration mode.
- **Key**—Identifies a routing protocol authentication key. The Global Configuration mode command key (global) is used to enter the key configuration mode.

- **Key-Chain**—Identifies a group of keys. The Global Configuration mode command **key-chain** is used to enter the key-chain configuration mode.
- Global Configuration mode command **interface ip** is used to enter the Interface IP Configuration mode.

Starting the CLI

The switch can be managed over a direct connection to the switch console port, or via a Telnet connection. The switch can also be managed via an out-of-band (OOB) management port. The switch is managed by entering command keywords and parameters at the prompt. Using the switch command-line interface (CLI) is very similar to entering commands on a UNIX system.

If access is via a Telnet connection, ensure that the device has an IP address defined, that corresponding management access is granted, and that the workstation used to access the device is connected to the device prior to beginning using CLI commands.

NOTE: The following steps are for use on the console line only.

To begin running CLI, perform the following:

1. Start the device and wait until the startup procedure is complete.

   The User EXEC mode is entered into, and the prompt "Console>" is displayed.

2. Configure the device and enter the necessary commands to complete the required tasks.
3. When finished, exit the session with the **quit** or **exit** command.

When a different user is required to log onto the system, in the Privileged EXEC Command mode the **login** command is entered. This effectively logs off the current user and logs on the new user.

Editing Features

Entering Commands

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "**show interfaces status ethernet g5**," **show**, **interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **g5** specifies the port.

When entering commands, the ports are all Giga ports and are referred to with a prefix "g". For example port 5 is referred to as **g5** and port 11 as **g11**.

In the PowerConnect series, all ports are named according to their Ethernet type. Ports in a standalone unit are named (ethernet_type port_number). Ports in stacks are named (unit_number/ethernet_type port_number). The PowerConnect 6024/6024F has only Gigabit Ethernet ports. Therefore, all the ports in the device are called g1..g24. The out-of-band management port is named out-of-band-eth 1.

To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)# username admin password smith
```

When working with the CLI, the command options are not displayed. The command is not selected by a menu but is manually entered. To see what commands are available in each mode or within an Interface Configuration, the CLI does provide a method of displaying the available commands, the command syntax requirements and in some instances parameters required to complete the command. The standard command to request help is the **?**.

There are three instances where the help information can be displayed:

- **Keyword lookup**—The character **?** is entered in place of a command. A list of all valid commands and corresponding help messages are displayed.
- **Partial keyword lookup**—A command is incomplete and the character **?** is entered in place of a parameter. The matched parameters for this command are displayed.

To assist in using the CLI, there is an assortment of editing features. The following features are described:

- Terminal Command Buffer
- Command Completion
- Keyboard Shortcuts

Terminal Command Buffer

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands are stored in the buffer which is maintained on a *First In First Out (FIFO)* basis.These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets.

Keyword	Source or destination
Up-arrow key Ctrl+P	Recalls commands in the history buffer, beginning with the most recent command. Repeats the key sequence to recall successively older commands.
Down-arrow key	Returns to more recent commands in the history buffer after recalling commands with the up-arrow key. Repeating the key sequence will recall successively more recent commands.

By default, the history buffer system is enabled, but it can be disabled at any time. For information about the command syntax to enable or disable the history buffer, see history.

There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 256. By configuring 0, the effect is the same as disabling the history buffer system. For information about the command syntax for configuring the command history buffer, see **history size**.

To display the history buffer, see **show history**.

Negating the Effect of Commands

For many configuration commands, the prefix keyword **no** can be entered to cancel the effect of a command or reset the configuration to the default value. This guide describes the negation effect for all applicable commands.

Command Completion

If a command is entered and it is not complete, if the command is invalid, or if some parameters of the command are invalid or missing, the appropriate error message is displayed. This assists in entering the correct command. By pressing the <Tab> button, an incomplete command is entered. If the characters already entered are not enough for the system to identify a single matching command, press "?" to display the available commands matching the characters already entered.

Incorrect or incomplete commands are automatically re-entered next to the cursor. If a parameter must be added, the parameter can be added to the basic command already displayed next to the cursor. The following example indicated that the command **interface ethernet** requires the parameter **<port-num>**.

```
(config)#interface ethernet

missing mandatory parameter

(config)#interface ethernet
```

Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The following table describes the CLI shortcuts.

Keyboard Key	Description
Up-arrow key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-arrow key	Returns to more recent commands in the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+Z / End	Returns back to the Privileged EXEC mode from all modes.
Backspace key	Moves the cursor back one space.

CLI Command Conventions

When entering commands there are certain command entry standards which apply to all commands. The following table describes the command conventions.

Convention	Description
[ ]	In a command line, square brackets indicates an optional entry.
{ }	In a command line, curly brackets indicates a selection of compulsory parameters separated by the \ character. One option must be selected. For example: **flowcontrol {auto|on|off}** means that for the **flowcontrol** command either **auto**, **on** or **off** must be selected.
Italic font	Indicates a parameter.
<Enter>	Any individual key on the keyboard. For example click **<Enter>**.
Ctrl+F4	Any combination keys pressed simultaneously on the keyboard.
`Screen Display`	Indicates system messages and prompts appearing on the console.
all	When a parameter is required to define a range of ports or parameters and **all** is an option, the default for the command is **all** when no parameters are defined. For example, the command **interface range port-channel** has the option of either entering a range of channels, or selecting **all**. When the command is entered without a parameter, it automatically defaults to **all**.

3

AAA Commands

aaa authentication login

The **aaa authentication login** global configuration command defines login authentication. To return to the default configuration, use the **no** form of this command.

Syntax

aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication login {**default** | *list-name*}

- **default**—Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
- *list-name*—Character string used to name the list of authentication methods activated when a user logs in. (Range: 1-12 characters)
- *method1* [*method2*...]—Specify at least one from the following table:

Keyword	Source or destination
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.
radius	Uses the list of all RADIUS servers for authentication.

Default Configuration

The local user database is checked. This has the same effect as the command **aaa authentication login list-name local**.

NOTE: On the console, login succeeds without any authentication check if the authentication method is not defined.

Command Mode

Global Configuration mode

User Guidelines

The default and optional list names created with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication login** *list-name method* command for a particular protocol, where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. Spaces cannot be used in the string which defines the list-name.

NOTE: Make sure that the given sequence of authentication methods is sensible. For example, a sequence where **Radius** follows **None** is not sensible because **None** requires no authentication and, therefore, the process will never require **Radius** authentication.

Example

The following example configures authentication login.

```
Console (config)# aaa authentication login default radius local
enable none
```

aaa authentication enable

The **aaa authentication enable** global configuration command defines authentication method lists for accessing higher privilege levels. To return to the default configuration use the **no** form of this command.

Syntax

aaa authentication enable {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication enable default

- **default**—Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
- *list-name*—Character string used to name the list of authentication methods activated, when using access higher privilege levels.
- *method1* [*method2*...]—Specify at least one from the following table:

Keyword	Source or destination
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

radius	Uses the list of all RADIUS servers for authentication. Uses username "$enabx$." where x is the privilege level.

Default Configuration

If the **default** list is not set, only the enable password is checked. This has the same effect as the command **aaa authentication enable default enable**.

On the console, the enable password is used if it exists. If no password is set, the process still succeeds. This has the same effect as using the command **aaa authentication enable default enable none**.

Command Mode

Global Configuration mode

User Guidelines

The default and optional list names created with the **aaa authentication enable** command are used with the **enable authentication** command.

Create a list by entering the **aaa authentication enable** *list-name method* command where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. Spaces cannot be used in the string which defines the list-name.

NOTE: Make sure that the given sequence of authentication methods is sensible. For example, a sequence where **Radius** follows **None** is not sensible because **None** requires no authentication and, therefore, the process will never require **Radius** authentication.

All **aaa authentication enable default** requests sent by the router to a RADIUS server include the username "$enabx$.", where x is the requested privilege level.

Example

The following example sets authentication when accessing higher privilege levels.

```
Console (config)# aaa authentication enable default enable
```

login authentication

The **login authentication** line configuration command specifies the login authentication method list for a remote telnet or console. To return to the default specified by the authentication login command, use the **no** form of this command.

Syntax

login authentication {**default** | *list-name*}

no login authentication

- **default**—Uses the default list created with the **authentication login** command.
- *list-name*—Uses the indicated list created with the **authentication login** command.

Default Configuration

Uses the default set with the command **authentication login**.

Command Mode

Line Configuration mode

User Guidelines

Changing login authentication from default to another value may disconnect the telnet session.

Example

The following example specifies the default authentication method for a remote Telnet or console.

```
Console (config)# line console

Console (config-line)# login authentication default
```

enable authentication

The **enable authentication** line configuration command specifies the authentication method list when accessing a higher privilege level from a remote telnet or console. To return to the default specified by the **enable authentication** command, use the **no** form of this command.

Syntax

enable authentication {**default** | *list-name*}

no enable authentication

- **default**—Uses the default list created with the **authentication enable** command.
- *list-name*—Uses the indicated list created with the **authentication enable** command.

Default Configuration

Uses the default set with the command **authentication enable**.

Command Mode

Line Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the default authentication method when accessing a higher privilege level from a remote Telnet or console.

```
Console (config)# line console
Console (config-line)# enable authentication default
```

ip http authentication

The **ip http authentication** global configuration mode command specifies authentication methods for http. To return to the default, use the **no** form of this command.

Syntax

ip http authentication *method1* [*method2*...]

no ip http authentication

- *method1* [*method2*...]—Specify at least one from the following table:

Keyword	Source or destination
local	Uses the local username database for authentication.
none	Uses no authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.
radius	Uses the list of all RADIUS servers for authentication.

Default Configuration

The local user database is checked. This has the same effect as the command **ip http authentication local**.

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

NOTE: Make sure that the given sequence of authentication methods is sensible. For example, a sequence where **Radius** follows **None** is not sensible because **None** requires no authentication and, therefore, the process will never require **Radius** authentication.

Example

The following example configures the http authentication.

```
Console (config)# ip http authentication radius local
```

ip https authentication

The **ip https authentication** global configuration command specifies authentication methods for https servers. To return to the default configuration, use the **no** form of this command.

Syntax

ip https authentication *method1* [*method2*...]

no ip https authentication

- *method1* [*method2*...]—Specify at least one from the following table:

Keyword	Source or destination
local	Uses the local username database for authentication.
none	Uses no authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.
radius	Uses the list of all RADIUS servers for authentication.

Default Configuration

The local user database is checked. This has the same effect as the command **ip https authentication local**.

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

NOTE: Make sure that the given sequence of authentication methods is sensible. For example, a sequence where **Radius** follows **None** is not sensible because **None** requires no authentication and, therefore, the process will never require **Radius** authentication.

Example

The following example configures https authentication.

```
Console (config)# ip https authentication radius local
```

password

The **password** line configuration command specifies a password on a line. To remove the password, use the **no** form of this command.

Syntax

password *password* [**encrypted**]

no password

- *password*—Password for this level. (Range: 1-159 characters)
- **encrypted**—Encrypted password to be entered, copied from another device configuration.

Default Configuration

This command has no default configuration.

Command Mode

Line Configuration mode

User Guidelines

If an encrypted password is specified on a line, the required password length is 32 characters.

Example

The following example specifies a password "dell" on a line.

```
Console (config-line)# password dell
```

enable password

The **enable password** global configuration command sets a local password to control access to normal and privilege levels. To remove the password requirement, use the **no** form of this command.

Syntax

enable password [**level** *level*] *password* [**encrypted**]

no enable password [**level** *level*]

- *password*—Password for this level (Range: 1-159 characters).
- *level*—Level for which the password applies. If not specified ,the level is 15 (Range: 1-15).
- **encrypted**—Encrypted password entered, copied from another device configuration.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

If an encrypted password is specified on a line, the range of the password length changes to 1-32 characters.

Example

The following example defines local level 15 password "dell" to control access to user and privilege levels.

```
Console (config)# enable password level 15 dell
```

username

The **username** global configuration command establishes a username-based authentication system. To remove a user name use the **no** form of this command.

Syntax

username *name* [**password** *password*] [**privilege** *level*] [**encrypted**]

no username

- *name*—The name of the user.
- *password*—The authentication password for the user, from 1 to 159 characters in length.
- *level*—The user level (Range: 1 -15).
- **encrypted**—Encrypted password entered, copied from another device configuration.

Default Configuration

No user name is defined.

The default privilege level is 1.

Command Mode

Global Configuration mode

User Guidelines

If an encrypted password is specified on a line, the range of the password length changes to 1-32 characters.

The password age out time begins from the first time the password is entered. For example, to change a privilege level for a user, the network administrator redefines the same password. Passwords are aged out based on the initial time definitions for the original username/password.

Example

The following example configures user "bob" with password "lee" and user level 15.

```
Console (config)# username bob password lee level 15
```

passwords min-length

The **passwords min-length** global configuration command configures the minimum length required for passwords in the local database. To remove the minimum password length requirement,use the **no** form of this command.

Syntax

passwords min-length *length*

no passwords min-length

- *length*—The mimimum length required for passwords (Range: 8-64).

Default Configuration

No minimum password length.

Command Mode

Global Configuration mode

User Guidelines

Relevant to local user passwords, line passwords and enable passwords.

The software checks the password length when an unencrypted password is defined or a user enters a password when logging in.

NOTE: The length of encrypted passwords is only checked when the user logs in.

Example

The following example configures a minimum length of 8 characters required for passwords in the local database.

```
Console (config)# passwords min-length 8
```

password-aging

The **password-aging** line configuration command configures the expiration time of line passwords in the local database. To return to the default configuration, use the **no** form of this command.

Syntax

password-aging *days*

no password-aging

- *days*—The number of days before a password expires (Range: 1-365).

Default Configuration

No password expiration time.

Command Mode

Line Configuration mode

User Guidelines

The password expiration date is calculated from the day the password is defined, and not from the day aging time is defined.

Ten days before the password expiration date, the user receives a warning to change the password within "n" days. These warnings continue until the password expiration date.

After the password expiration date, the user receives three chances to log in and change the password. If the user still does not change the password, the account is locked.

Example

The following example configures password aging to 120 days.

```
Console (config)# line telnet
Console (config-line)# password-aging 120
```

passwords aging

The **passwords aging** global configuration command configures the expiration time of local username and enable passwords in the local database. To return to the default configuration, use the **no** form of this command.

Syntax

passwords aging username *name days*

no passwords aging username *name*

passwords aging enable-password *level days*

no passwords aging enable-password *level*

- *name*—The name of the user (Range: 1-20 characters).
- *level*—The user level (Range: 1 -15).
- *days*—The number of days before a password expires (Range: 1-365).

·Default Configuration

No password expiration time.

Command Mode

Global Configuration mode

User Guidelines

The password expiration date is calculated from the day the password is defined, and not from the day aging time is defined.

Ten days before the password expiration date, the user receives a Syslog warning to change the password within "n" days. These warnings continue until the password expiration date.

After the password expiration date, the user receives three chances to log in and change the password. If the user still does not change the password, the account is locked.

Example

The following example configures the password expiration time of username "bob" to 120 days.

```
Console (config)# passwords aging username bob 120
```

passwords history

The **passwords history** global configuration command configures the number of required password changes before a password in the local database can be reused. To remove this requirement,use the **no** form of this command.

Syntax

passwords history *number*

no passwords history

- *number*—Indicates the required number of password changes before the password can be reused. (Range: 1-10)

Default Configuration

No required number of password changes before reusing a password.

Command Mode

Global Configuration mode

User Guidelines

Relevant to local user passwords, line passwords and enable passwords.

Password history is not checked during the configuration download.

Password history is saved even if the the feature is disabled.

A user's password history is saved as long as the user is defined.

The password age out time begins from the first time the password is entered. For example, to change a privilege level for a user, the network administrator redefines the same password. Passwords are aged out based on the initial time definitions for the original username/password.

Example

The following example configures the required number of password changes before a password can be reused to 3.

```
Console (config)# passwords history 3
```

passwords history hold-time

The **passwords history hold-time** global configuration command configures the number of days a password is relevant for tracking its password history. To return to the default configuration,use the **no** form of this command.

Syntax

passwords history hold-time *days*

no passwords hold-time

- *days*—Number of days a password is relevant for tracking its password history (Range: 1-365).

Default Configuration

Not enabled.

Command Mode

Global Configuration mode

User Guidelines

Relevant to local user passwords, line passwords and enable passwords.

Passwords are not deleted from the history database when they are no longer relevant for tracking purposes. Increasing the number of days a password is relevant for tracking purposes, may make a password that was no longer relevant for tracking purposes relevant again.

Example

The following example configures the number of days that a password is relevant for tracking its password history to 120.

```
Console (config)# passwords history hold-time 120
```

aaa login-history file

The **aaa login-history file** global configuration command enables writing to the login history file. To disable writing to the file,use the **no** form of this command.

Syntax

aaa login-history file

no aaa login-history file

Default Configuration

Writing to the login history file is enabled.

Command Mode

Global Configuration mode

User Guidelines

The login history is also saved in the internal buffer of the device.

Example

The following example enables writing to the login history file.

```
Console (config)# aaa login-hisory file
```

set username active

The **set username active** privileged EXEC command reactivates a locked user account.

Syntax

set username *name* **active**

- *name*—Name of the user. (Range: 1-20 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example reactivates a suspended user with username "bob".

```
Console # set username bob active
```

set line active

The **set line active** privileged EXEC command reactivates a locked line.

Syntax

set line {**console** | **telnet** | **ssh**} **active**

- **console**—Console terminal line.
- **telnet**—Virtual terminal for remote console access (Telnet).
- **ssh**—Virtual terminal for secured remote console access (SSH).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example reactivates the device as a virtual terminal for remote console access.

```
Console # set line telnet active
```

set enable-password active

The **set enable-password active** privileged EXEC command reactivates a locked local password.

Syntax

set enable-password *level* **active**

- *level*—The user level (Range: 1 -15).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example reactivates a locked local level 15 password.

```
Console # set enable-password 15 active
```

show authentication methods

The **authentication methods** privileged EXEC command displays information about the authentication methods.

Syntax

show authentication methods

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the authentication configuration.

```
Console# show authentication methods


Login Authentication Method Lists
----------------------------------
Console_Default     : None
Network_Default     : Local


Enable  Authentication Method Lists
----------------------------------
Default             : Enable
admin               : Enable



Line           Login Method List         Enable Method List
-------        -----------------         -------------------
Console        Default                   Default
Telnet         Default                   Default
SSH            Default                   Default


http                : None
https               : None
```

show users accounts

The **show users accounts** privileged EXEC command displays information about the local user database.

Syntax

show users accounts

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the local users configured with access to the system.

```
Console# show users accounts


Username  Privilege Password Aging Password Expiry     Lockout
                                   date

--------  --------- -------------- ---------------     -------

Bob       15        -              -                   0

Robert    15        30             Jan 18 2005         1

Smith     15        30             Jan 19 2005         LOCKOUT
```

The following table describes significant fields shown above.

Field	Description
Username	Name of the user.
Privilege	User’s privilege level
Password Aging	User’s password expiration time in days.
Password Expiry Date	Expiration date of the user’s password
Lockout	If lockout control is enabled, specifies the number of failed authentication attempts since the user last logged in successfully. If the user account is locked, specifies LOCKOUT.

show passwords configuration

The **show passwords configuration** privileged EXEC command displays information about password management.

Syntax

show passwords configuration

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information about password management in the local database.

```
Console # show passwords configuration
Minimal length: 8
History: 10
History hold time: 365 days
Lock-out control: Disabled

Enable Passwords
Level            Aging           Expiry date      Lockout
-----            -----           -----------      -------
1                90              Jan 18 2005      1
15               90              Jan 18 2005      0

Line Passwords
Level            Aging           Expiry date      Lockout
-----            -----           -----------      -------
Console          -               -                -
Telnet           90              Jan 18 2005      LOCKOUT
SSH              90              Jan 21 2005      0
```

The following table describes significant fields shown above.

Field	Description
Minimal length	Minimum length required for passwords in the local database.
History	Number of required passwords changes before a password in the local database can be reused.
History hold time	Period of time that a password is relevant for tracking password history.
Lockout control	Control locking a user account after a series of authentication failures.
Enable passwords	Describes the configuration and status of a local password with a specific level.
Aging	Password expiration time in days.
Expiry date	Expiration date of a password
Lockout	If lockout control is enabled, specifies the number of failed authentication attempts since the user last logged in successfully. If the user account is locked, specifies LOCKOUT.
Line Passwords	Describes the configuration and status of a specific line password.

show users login-history

The **show users login-history** privileged EXEC command displays information about the login history of users.

Syntax

show users login-history [**username** *name*]

- *name*—Name of the user. (Range: 1-20 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the login history of users.

```
Console # show users login-history


Login Time            Username          Protocol          Location
--------------        --------          --------          --------
Jan 18 2005  23:58:17 Robert            HTTP              172.16.1.8
Jan 19 2005  07:59:23 Robert            HTTP              172.16.0.8
Jan 19 2005  08:23:48 Bob               Serial
Jan 19 2005  08:29:29 Robert            HTTP              172.16.0.8
Jan 19 2005  08:42:31 John              SSH               172.16.0.1
Jan 19 2005  08:49:52 Betty             Telnet            172.16.1.7
```

4

ACL Commands

ip access-list

The **ip access-list** global configuration command creates IP ACLs, and enters IP Access-list configuration mode. To delete an IP ACL use the **no** form of this command.

Syntax

ip access-list *name*

no ip access-list *name*

- *name*—Enter the IP ACL name consisting of a character string up to 32 characters long.

Default Configuration

All ACLs are deny-all by default.

Command Mode

Global Configuration mode

User Guidelines

ACLs on the system perform both access control and Layer 3 field classification. To define Layer 3 fields access-lists the **ip access-list** command should be used.

ACLs cannot be removed when they are assigned to an interface (using **service-acl** command).

The **ip access-list** command enters the IP-access list configuration mode.

Example

The following example creates an ACL with the name "Dell".

```
Console (config)# ip access-list Dell

Console (config-ip-al)#
```

permit (IP)

The **permit** ip access-list configuration mode command allows traffic if the conditions defined in the permit statement are matched.

Syntax

permit {**any** | protocol-ip} {**any** | **source** source-wildcard } {**any** | **destination** destination-wildcard } [**dscp** dscp-number | **ip-precedence** ip-precedence]

permit-tcp {**any** | **source** source-wildcard } {**any** | source-port} {**any** | **destination** destination-wildcard } {**any** | destination-port} [**dscp** dscp-number | **ip-precedenc**e ip-precedence]

permit-udp {**any** | **source** source-wildcard } {**any** | source-port} {**any** | **destination** destination-wildcard } {**any** | destination-port} [**dscp** dscp-number | **ip-precedence** ip-precedence]

- Source IP address can be one of the following:
  - **any**—Packets received from any IP address.
  - **source** *source-wildcard*—IP address and wildcard for host from which the packet is sent. Specify the IP address as 0.0.0.0 and mask as 255.255.255.255.
- Destination IP address can be one of the following:
  - **any**—Packets sent to any IP address.
  - **destination** *destination-wildcard*—IP address and wildcard for host to which the packet is sent. Specify the IP address as 0.0.0.0 and mask as 255.255.255.255.
- *protocol*—The name or the number of an IP protocol. Use **?** to see list of available protocols (**icmp**, **igmp**, **ip**, **tcp**, **egp**, **igp**, **udp**, **hmp**, **rdp**, **idpr**, **ipv6**, **ipv6-route**, **ipv6-frag**, **idrp**, **rsvp**, **gre**, **esp**, **ah**, **ipv6-icmp**, **eigrp**, **ospf**, **ipip**, **pim**, **l2tp**, **isis**), use **any** for all protocols.
- *destination-port*—Specifies the UDP/TCP destination port. Use **any** for all ports.
- *source-port*—Specifies the UDP/TCP source port. Use **any** for all ports.
- **dscp**—Matches *dscp number* with the packet DSCP value.
- **precedence**—Matches *ip-precedence* with the packet ip-precedence value.

Default Configuration

This command has no default configuration.

Command Mode

IP Access-list Configuration mode

User Guidelines

When an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. If there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

NOTE: Using "any" specifies that all IP protocols are permitted. The permit "any" does not imply that other protocols running over IP (e.g., TCP, UDP, etc.) are "permitted" .

Example

The following example configures an ACE called "Dell" to allow RSVP protocol traffic from IP address 12.1.1.1, mask 0.0.0.0 and DSCP 56.

```
Console (config)# ip access-list Dell

Console (config-ip-al)# permit rsvp 12.1.1.1 0.0.0.0 any dscp 56
```

deny (IP)

The **deny** IP access-list configuration command denies traffic if the conditions defined in the deny statement are matched.

Syntax

deny [**disable-port**] {**any**| *protocol*} {**any** | {**source** *source-wildcard*}} {**any** | {**destination** *destination-wildcard*}} [**dscp** *dscp number* | **ip-precedence** *ip-precedence*]

deny-tcp [**disable-port**] {**any** | {**source** *source-wildcard*}} {**any** |*source-port*} {**any** | {**destination** *destination-wildcard*}} {**any** |*destination-port*} [**dscp** *dscp number* | **ip-precedence** *ip-precedence*]

deny-udp [**disable-port**] {**any** | {**source** *source-mask*}} {**any** | *source-port*} {**any** | {**destination** *destination-mask*}} {**any** | *destination-port*} [**dscp** *dscp number* | **ip-precedence** *ip-precedence*]

- **disable-port**—If the statement is deny, then the port is disabled.
- Source IP address can be one of the following:
  - **any**—Packets received from any IP address.
  - **source** *source-wildcard*—IP address and wildcard for host from which the packet is sent. Specify the IP address as 0.0.0.0 and mask as 255.255.255.255.
- Destination IP address can be one of the following:
  - **any**—Packets sent to any IP address.
  - **destination** *destination-wildcard*—IP address and wildcard for host to which the packet is sent. Specify the IP address as 0.0.0.0 and mask as 255.255.255.255.
- *protocol*—The name or the number of an IP protocol. Use "?" to see list of available protocols (**icmp**, **igmp**, **ip**, **tcp**, **egp**, **igp**, **udp**, **hmp**, **rdp**, **idpr**, **ipv6**, **ipv6-route**, **ipv6-frag**, **idrp**, **rsvp**, **gre**, **esp**, **ah**, **ipv6-icmp**, **eigrp**, **ospf**, **ipip**, **pim**, **l2tp**, **isis**) use **any** for all protocols
- *destination-port*—Specifies the UDP/TCP destination port. Use **any** for all ports.

- *source-port*—Specifies the UDP/TCP source port. Use **any** for all ports.
- **dscp**—Matches *dscp number* with the packet DSCP value.
- **precedence**—Matches *ip-precedence* with the packet ip-precedence value.

Default Configuration

This command has no default configuration.

Command Mode

IP access-list Configuration mode

User Guidelines

When an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. If there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

NOTE: Using "any" specifies that all IP protocols are denied. The deny "any" does not imply that other protocols running over IP (for example, TCP, UDP, etc.) are "denied".

Example

The following example configures an ACL called "Dell" to deny any IP traffic to address 192.1.1.10 and mask 0.0.0.255.

```
Console (config)# ip access-list Dell

Console (config-ip-al)# deny any 192.1.1.10 0.0.0.255 any
```

mac access-list

The **mac access-list** global configuration command creates Layer 2 MAC ACLs, and enters to MAC-Access list configuration mode. To delete a MAC ACL use the **no** form of this command.

Syntax

mac access-list *name*

no mac access-list *name*

- *name*—Enter the MAC ACL name consisting of a character string up to 32 characters long.

Default Configuration

The default for all ACLs is deny.

Command Mode

Global Configuration mode

User Guidelines

ACLs on this system perform both access control and layer 2 field classification. To define Layer 2 access lists, the **mac access-list** command should be used.

ACLs cannot be removed when they are applied to an interface (using **service-acl** command).

MAC named lists are used with VLAN maps and class maps.

Entering the **mac access-list** command enables the MAC-access list configuration mode.

Example

The following example creates a MAC ACL with the name "dell".

```
Console (config)# mac access-list dell

Console (config-mac-al)#
```

permit (MAC)

The **permit** mac-acl configuration mode command allows traffic if the conditions defined in the permit statement are matched.

Syntax

permit {**any** | {**host** *source source-wildcard*}} {**any** | {**destination** *destination-wildcard*}} [**vlan** *vlan-id*]

- Source MAC address can be one of the following:
  - **any**—Packets received from any MAC address.
  - **source** *source-wildcard*—MAC address and wildcard for host from which the packet is sent. Specify the MAC address and wildcard using hexadecimal format (HH:HH:HH:HH:HH:HH) or XXXX.XXXX.XXXX.
- Destination MAC address can be one of the following:
  - **any**—Packets sent to any MAC address.
  - **destination** *destination-wildcard*—MAC address and wildcard for host to which the packet is sent. Specify the MAC address and wildcard using hexadecimal format (HH:HH:HH:HH:HH:HH) or XXXX.XXXX.XXXX.
- **vlan** *vlan-id*—The packet VLAN.

Default Configuration

This command has no default configuration.

Command Mode

Mac-ACL Configuration mode

User Guidelines

When an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. If there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

If **vlan id** is used as a classifier element then it cannot connect a policy map to a VLAN interface.

Example

The following example configures a MAC ACE to allow traffic from MAC address 66:66:66:66:66:66 with any destination on VLAN 4.

```
Console (config-mac-al)# permit 66:66:66:66:66:66
00:00:00:00:00:00 any vlan 4
```

deny (MAC)

The **deny** mac-acl configuration mode command denies traffic if the conditions defined in the permit statement are matched.

Syntax

deny [**disable-port**] {**any** | {**source** *source- wildcard*} *any* | {**destination** *destination-wildcard*}}[**vlan** *vlan-id*]

- **disable-port**—If the statement is deny, then the port is disabled.
- Source MAC address can be one of the following:
  - **any**—Packets received from any MAC address.
  - **source** *source-wildcard*—MAC address and wildcard for host from which the packet is sent. Specify the MAC address and wildcard using hexadecimal format (HH:HH:HH:HH:HH:HH).
- Destination MAC address can be one of the following:
  - **any**—Packets sent to any MAC address.
  - **destination** *destination-wildcard*—MAC address and wildcard for host to which the packet is sent. Specify the MAC address and wildcard using hexadecimal format (HH:HH:HH:HH:HH:HH).
- **vlan** *vlan-id*—The packet VLAN.

Default Configuration

This command has no default configuration.

Command Mode

Mac-ACL Configuration mode

User Guidelines

When an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. If there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

If **vlan id** is used as a classifier element then it cannot connect a policy map to a VLAN interface.

Example

The following example configures a MAC ACE to deny traffic from MAC address 6:6:6:6:6:6.

```
Console (config)# mac access-list dell

Console (config-mac-al)# deny 06:06:06:06:06:06 00:00:FF:FF:FF:FF
any
```

service-acl

The **service-acl** interface configuration command applies an access-list to the interface input. To detach an access-list from an interface use the **no** form of this command.

Syntax

service-acl {**input** *acl-name*}

no service-acl {**input**}

- **input** *acl-name*—Apply the specified ACL to the input interface.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration mode

User Guidelines

Whenever an ACL is assigned to an interface (port, LAG or VLAN), flows (from that ingress interface) that do not match the ACL are matched to the default rule: "drop unmatched packets". If an ACL X is bound to a port and the port becomes a member of the VLAN to which a different ACL Y is bound, then the ACL Y bound to the VLAN overrides the ACL X bound to the port.

Example

The following example attaches the ACL "dell" to the interface input.

```
Console (config-if)# service-acl input dell
```

show access-lists

The **show access-lists** privileged EXEC command displays access control lists (ACLs) defined on the switch.

Syntax

show access-lists [*name*]

- *name*—The ACL name.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays an ACL configured on the device.

```
Console# show access-lists
IP access list one
permit ip host 12.1.1.1 any
permit rsvp host 176.30.40.1 any
```

show interfaces access-lists

The **show interfaces access-lists** privileged EXEC command displays access lists applied on interfaces.

Syntax

show interfaces access-lists [**ethernet** *interface* | **vlan** *vlan-id* | **port-channel** *port-channel-number*]

- *interface*—Port number.
- *vlan-id*—VLAN number.
- *port-channel-number*—port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays an ACL configured on the device.

```
Console# show interfaces access-lists ethernet g1
Interface         Input ACL
---------         ----------
g1                one
```

5

Address Table Commands

bridge address

The **bridge address** VLAN interface configuration command adds a static MAC-layer station source address to the bridge table. To delete the MAC address, use the **no** form of the **bridge address** command (using the **no** form of the command without specifying a MAC address deletes all static MAC addresses belonging to this VLAN).

Syntax

bridge address *mac-address* {**ethernet** *interface* | *port-channel port-channel-number*} [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**]

no bridge address [*mac-address*]

- *mac-address*—A valid MAC address.
- *interface*—A valid Ethernet port.
- *port-channel-number*—A valid port-channel number.
- **permanent—**The address can only deleted by the **no bridge address** command.
- **delete-on-reset**—The address is deleted after reset.
- **delete-on-timeout—**The address is deleted after "age out" time has expired.
- **secure**—The address is deleted after the port changes mode to unlock learning (**no port security** command). This parameter is only available when the port is in learning locked mode.

Default Configuration

No static addresses are defined. The default mode for an added address is **permanent**.

Command Mode

Interface configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example adds a permanent static MAC-layer station source address 3aa2.64b3.a245 on port g8 to the bridge table.

```
Console (config)# interface vlan 2
Console (config-vlan)# bridge address 3aa2.64b3.a245 ethernet g8
permanent
```

bridge multicast filtering

The **bridge multicast filtering** global configuration command enables filtering of Multicast addresses. To disable filtering of Multicast addresses, use the **no** form of the **bridge multicast filtering** command.

Syntax

bridge multicast filtering

no bridge multicast filtering

Default Configuration

Disabled. All Multicast addresses are flooded to all ports of the relevant VLAN.

Command Mode

Global Configuration mode

User Guidelines

If Multicast routers exist on the VLAN and IGMP, snooping is not enabled, the **bridge multicast forward-all** command should be used to enable forwarding all Multicast packets to the Multicast routers.

Example

In this example, bridge Multicast filtering is enabled.

```
Console (config)# bridge multicast filtering
```

bridge multicast address

The **bridge multicast address** interface configuration command registers MAC-layer Multicast addresses to the bridge table, and adds static ports to the group. To unregister the MAC address, use the **no** form of the **bridge multicast address** command.

Syntax

bridge multicast address {*mac-multicast-address* | *ip-multicast-address*}

bridge multicast address {*mac-multicast-address* | *ip-multicast-address*} [**add** | **remove**] {**ethernet** *interface-list* | *port-channel port-channel-number-list*}

no bridge multicast address {*mac-multicast-address* | *ip-multicast-address*}

- **add**—Adds ports to the group. If no option is specified, this is the default option.
- **remove**—Removes ports from the group.
- *mac-multicast-address*—MAC multicast address.
- *ip- multicast-address*—IP multicast address.
- *interface-list*—Separate nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list*—Separate nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of ports.

Default Configuration

No Multicast addresses are defined.

Command Mode

Interface configuration (VLAN) mode

User Guidelines

If the command is executed without **add** or **remove**, the command only registers the group in the bridge database.

Static Multicast addresses can only be defined on static VLANs.

Examples

The following example registers the MAC address:.

```
Console (config)# interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203
```

The following example registers the MAC address and adds ports statically.

```
Console (config)# interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203 add
ethernet g1-9, g2
```

bridge multicast forbidden address

The **bridge multicast forbidden address** interface configuration command forbids adding a specific Multicast address to specific ports.

Syntax

bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*} {**add** | **remove**} {**ethernet** *interface-list* | *port-channel port-channel-number-list*}

no bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*}

- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- *mac-multicast-address*—MAC Multicast address.
- *ip- multicast-address*—IP Multicast address.
- *interface-list*—Separate non consecutive valid Ethernet ports with a comma and no spaces; hyphen is used to designate a range of ports.
- *port-channel-number-list*—Separate non consecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

No forbidden addresses are defined.

Command Modes

Interface Configuration (VLAN) mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.

Examples

In this example the MAC address 0100.5e02.0203 is forbidden on port g9 within VLAN 8.

```
Console (config)# interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203

Console (config-if)# bridge multicast forbidden address
0100.5e02.0203 add ethernet g9
```

bridge multicast forward-all

The **bridge multicast forward-all** interface configuration command enables forwarding of all Multicast packets on a port. To restore the default, use the **no** form of the **bridge multicast forward-all** command.

Syntax

bridge multicast forward-all {**add** | **remove**} {**ethernet** *interface-list* | *port-channel port-channel-number-list*}

no bridge multicast forward-all

- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- *interface-list*—Separate non consecutive valid Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list*—Separate non consecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

Disable forward-all on all ports.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

In this example all Multicast packets on port g8 are forwarded.

```
Console (config)# interface vlan 2

Console (config-if)# bridge multicast forward-all add ethernet g8
```

bridge multicast forbidden forward-all

The **bridge multicast forbidden forward-all** interface configuration command forbids a port to be a forward-all-Multicast port. To restore the default, use the **no** form of the **bridge multicast forward-all** command.

Syntax

bridge multicast forbidden forward-all {**add** | **remove**} {**ethernet** *interface-list* | *port-channel port-channel-number-list*}

no bridge multicast forward-all

- **add**—Forbids forwarding all Multicast packets.
- **remove**—Does not forbid forwarding all Multicast packets.
- *interface-list*—Separates non consecutive valid Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list*—Separates non consecutive valid port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

By default, this setting is disabled (for example, forwarding to the port is not forbidden).

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

IGMP snooping dynamically discovers Multicast router ports. When a Multicast router port is discovered, all the Multicast packets are forwarded to it unconditionally.

This command prevents a port to be a Multicast router port.

Example

In this example, forwarding all Multicast packets to g6 are forbidden.

```
Console (config)# interface vlan 2

Console (config-if)# bridge multicast forbidden forward-all add
ethernet g6
```

bridge aging-time

The **bridge aging-time** global configuration command sets the address table aging time. To restore the default, use the **no** form of the **bridge aging-time** command.

Syntax

bridge aging-time *seconds*

no bridge aging-time

- *seconds*—Time is number of seconds. (Range: 10 - 630 seconds)

Default Configuration

300 seconds

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

In this example the bridge aging time is set to 250.

```
Console (config)# bridge aging-time 250
```

clear bridge

The **clear bridge** privileged EXEC command removes any learned entries from the forwarding database.

Syntax

clear bridge

- This command has no keywords or arguments.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, the bridge tables are cleared.

```
Console# clear bridge
```

port security

The **port security** interface configuration command locks the port. By locking the port, new addresses are not learned on the port. To enable new address learning, use the **no** form of the **port security** command.

Syntax

port security [**forward | discard | discard-shutdown**] [**trap** *seconds*]

no port security

- **forward**—Forwards frames with unlearned source addresses, but does not learn the address.
- **discard**—Discards frames with unlearned source addresses. This is the default if no option is indicated.
- **discard-shutdown**—Discards frames with unlearned source addresses. The port is also shut down.
- **trap** *Seconds*—Sends SNMP traps and defines the minimal amount of time in seconds between two consecutive traps. (Range: 1 - 1,000,000)

Default Configuration

Disabled - No port security

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, frame forwarding is enabled without learning, and with traps sent every 100 seconds on port g1.

```
Console (config)# interface ethernet g1

Console (config-if)# port security forward trap 100
```

port security routed secure-address

The **port security routed secure-address** interface configuration command adds MAC-layer secure addresses to a routed port. Use the **no** form of this command to delete the MAC addresses.

Syntax

port security routed secure-address *mac-address*

no port security routed secure-address *mac-address*

- *mac-address*—Specify a MAC address.

Default Configuration

No addresses are defined.

Command Mode

Interface configuration (Ethernet, port-channel). Cannot be configured for a range of interfaces (range context).

User Guidelines

The command enables adding secure MAC addresses to a routed ports in port security mode. The command is available when the port is a routed port and in port security mode. The address is deleted if the port exits the security mode or is not a routed port.

Example

In this example, the MAC-layer address 66:66:66:66:66:66 is added to port g1.

```
Console (config)# interface ethernet g1

Console (config-if)# port security routed secure-address
66:66:66:66:66:66
```

show bridge address-table

The **show bridge address-table** privileged EXEC command displays all entries in the bridge-forwarding database.

Syntax

show bridge address-table [**vlan** *vlan*] [**ethernet** *interface* **|** **port-channel** *port-channel-number*]

- *vlan*—Specific valid VLAN, such as VLAN 1.
- *interface*—A valid Ethernet port.
- *port-channel-number*—A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, all classes of entries in the bridge-forwarding database are displayed.

```
Console# show bridge address-table


Aging time is 300 sec


vlan  mac address port   type
----   -------------- ----- -----
1 0060.704C.73FF g8 dynamic
1 0060.708C.73FF g8 dynamic
200   0010.0D48.37FF g8 static
```

show bridge address-table static

The **show bridge address-table static** privileged EXEC command displays statically created entries in the bridge-forwarding database.

Syntax

show bridge address-table static [**vlan** *vlan*] [**ethernet** *interface* **|** **port-channel** *port-channel-number*]

- *vlan*—Specific valid VLAN, such as VLAN 1.
- *interface*—A valid Ethernet port.
- *port-channel-number*—A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, all static entries in the bridge-forwarding database are displayed.

```
Console# show bridge address-table static


Aging time is 300 sec


vlan  mac address       port   type
----   --------------    ----- -----
1      00.60.70.4C.73.FF g8    permanent
1      00.60.70.8C.73.FF g8    delete-on-timeout
200    00.10.0D.48.37.FF g9    delete-on-reset
```

show bridge multicast address-table

The **show bridge multicast address-table** privileged EXEC command displays Multicast MAC address table information.

Syntax

show bridge multicast address-table [**vlan** *vlan-id*] [**address** *mac-multicast-address* **|** *ip-multicast-address*] [**format ip | mac**]

- *vlan_id*—A VLAN ID value.
- *mac-multicast-address*—A MAC Multicast address.
- *ip- multicast-address*—An IP Multicast address.
- **format**—Multicast address format. Can be **ip** or **mac**. If format is unspecified, the default is **mac**.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, Multicast MAC address table information is displayed.

```
Console # show bridge multicast address-table


Vlan    MAC address                Type      Ports
------  -----------------------    --------  -------------
1       01.00.5e.02.02.03             staticg1   g2
19      01.00.5e.02.02.08             static     g1-8
19      01.00.5e.02.02.08             dynamicg   9-11


Forbidden ports for multicast addresses:


Vlan    MAC address                Ports
------  -----------------------    -----------------------
1       0100.5e02.0203             g8
19      0100.5e02.0208             g8
```

show bridge multicast filtering

The **show bridge multicast filtering** privileged EXEC command displays the Multicast filtering configuration.

Syntax

show bridge multicast filtering *vlan-id*

- *vlan_id*—A valid VLAN ID value.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, the Multicast configuration for VLAN 1 is displayed.

```
Console # show bridge multicast filtering 1

Filtering: Enabled

VLAN: 1

Port                         Forward-All

                 Static           Status

----             ------           ------

g1               Forbidden        Filter

g2               Forward          Forward(s)

g3               -                Forward(s)
```

show ports security

The **show ports security** privileged EXEC command displays the port-lock status.

Syntax

show ports security [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—A valid Ethernet port.
- *port-channel-number*—A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, all classes of entries in the port-lock status are displayed.

```
Console # show ports security
Port       Status     Action     Trap       Frequency  Counter
----       ------     ------     ----       ---------  -------
g1         Unlocked   -          -          -          -
g2         Unlocked   -          -          -          -
g3         Unlocked   -          -          -          -
g4         Unlocked   -          -          -          -
g5         Unlocked   -          -          -          -
g6         Unlocked   -          -          -          -
g7         Unlocked   -          -          -          -
g8         Unlocked   -          -          -          -
g9         Unlocked   -          -          -          -
...
g22        Unlocked   -          -          -          -
g23        Unlocked   -          -          -          -
g24        Unlocked   -          -          -          -
ch1
ch2        Unlocked   -          -          -          -
ch3        Unlocked   -          -          -          -
ch4        Unlocked   -          -          -          -
ch5        Unlocked   -          -          -          -
ch6        Unlocked   -          -          -          -
ch7        Unlocked   -          -          -          -
```

6

Clock

clock source

The **clock source** global configuration command configures the external time source for the system clock. To disable the external time source and use the hardware internal clock, use the **no** form of this command.

Syntax

clock source sntp

no clock source

Default Configuration

No external clock source.

Command Mode

Global Configuration mode

User Guidelines

Time from the external time source is acquired using the Simple Network Time Protocol (STNP).

Examples

The following example configures an external time source for the system clock.

```
Console(config)# clock source sntp
```

clock timezone

The **clock timezone** global configuration command sets the time zone for display purposes. To set the time to the Coordinated Universal Time (UTC), use the **no** form of this command.

Syntax

clock timezone *hours-offset* [**minutes** *minutes-offset*] [**zone** *acronym*]

no clock timezone

- *hours-offset* — Hours difference from UTC. (Range: -12 – +13)
- *minutes-offset* — Minutes difference from UTC. (Range: 0 – 59)
- *acronym* — The acronym of the time zone. (Range: Up to 4 characters)

Default Configuration

Clock is set to UTC.

Command Mode

Global Configuration mode

User Guidelines

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

Examples

The following example sets the timezone to 6 hours difference from UTC.

```
Console(config)# clock timezone -6 zone CST
```

clock summer-time

The **clock summer-time** global configuration command configures the system to automatically switch to summer time (daylight saving time). To configure the software not to automatically switch to summer time, use the **no** form of this command.

Syntax

clock summer-time recurring {**usa** | **eu** | {*week day month hh:mm week day month hh:mm*}} [**offset** *offset*] [**zone** *acronym*]

clock summer-time date *date month year hh:mm date month year hh:mm* [**offset** *offset*] [**zone** *acronym*]

clock summer-time date *month date year hh:mm month date year hh:mm* [**offset** *offset*] [**zone** *acronym*]

no clock summer-time recurring

- **recurring** — Indicates that summer time should start and end on the corresponding specified days every year.
- **date** — Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.
- **usa** — The summer time rules are the United States rules.
- **eu** — The summer time rules are the European Union rules.
- *week* — Week of the month. (Range: 1 - 5, **first**, **last**)
- *day* — Day of the week (Range: first three letters by name, like **sun**)
- *date* — Date of the month (Range:1 - 31)
- *month* — Month (Range: first three letters by name, like Jan)
- *year* — year - no abbreviation (Range: 2000 - 2097)
- *hh:mm* — Time in military format, in hours and minutes (Range: hh: 0 - 23, mm:0 - 59)

- *offset* — Number of minutes to add during summer time (Range: 1 - 1440).
- *acronym* — The acronym of the time zone to be displayed when summer time is in effect. If unspecified default to the timezone acronym. (Range: Up to 4 characters)

Default Configuration

Summer time is disabled.

Command Mode

Global Configuration mode

User Guidelines

In both the **date** and **recurring** forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

- USA rule for daylight saving time:
  - Start: First Sunday in April
  - End: Last Sunday in October
  - Time: 2 am local time
- EU rule for daylight saving time:
  - Start: Last Sunday in March
  - End: Last Sunday in October
  - Time: 1.00 am (01:00)

Example

The following example sets summer time starting on the first Sunday in April at 2 am and finishing on the last Sunday in October at 2 am.

```
Console(config)# clock summer-time recurring first sun apr 2:00
last sun oct 2:00
```

sntp authentication-key

The **sntp authentication-key** global configuration command defines an authentication key for Simple Network Time Protocol (SNTP). To remove the authentication key for SNTP, use the **no** form of this command.

Syntax

sntp authentication-key *number* **md5** *value*

no sntp authentication-key *number*

- *number* — Key number (Range: 1 - 4294967295)
- *value* — Key value (Range: 1-8 characters)

Default Configuration

No authentication key is defined.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example defines the authentication key for SNTP.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```

sntp authenticate

The **sntp authenticate** global configuration command grants authentication for received Simple Network Time Protocol (SNTP) traffic from servers. To disable the feature, use the **no** form of this command.

Syntax

sntp authenticate

no sntp authenticate

Default Configuration

No authentication.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for both Unicast and Broadcast.

Examples

The following example defines the authentication key for SNTP and grants authentication.

```
Console(config)# sntp authentication-key 8 md5 ClkKey

Console(config)# sntp trusted-key 8

Console(config)# sntp authenticate
```

sntp trusted-key

The **sntp trusted-key** global configuration command authenticates the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize. To disable authentication of the identity of the system, use the **no** form of this command.

Syntax

sntp trusted-key *key-number*

no sntp trusted-key *key-number*

- *key-number* — Key number of authentication key to be trusted. (Range: 1 - 4294967295)

Default Configuration

No keys are trusted.

Command Mode

Global Configuration mode

User Guidelines

This command is relevant for both received Unicast and Broadcast.

Examples

The following example authenticates key 8.

```
Console(config)# sntp authentication-key 8 md5 ClkKey

Console(config)# sntp trusted-key 8
```

sntp client poll timer

The **sntp client poll timer** global configuration command sets the polling time for the Simple Network Time Protocol (SNTP) client. To return to default, use the **no** form of this command.

Syntax

sntp client poll timer *seconds*

no sntp client poll timer

- *seconds* — Polling interval in seconds (Range: 60-86400)

Default Configuration

Polling interval is 1024 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example sets the polling time for the Simple Network Time Protocol (SNTP) client to 120 seconds.

```
Console(config)# sntp client poll timer 120
```

sntp broadcast client enable

The **sntp broadcast client enable** global configuration command enables Simple Network Time Protocol (SNTP) Broadcast clients. To disable SNTP Broadcast clients, use the **no** form of this command.

Syntax

sntp broadcast client enable

no sntp broadcast client enable

Default Configuration

SNTP Broadcast clients are disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **sntp client enable** interface configuration command to enable SNTP clients on a specific interface.

Examples

The following example enables Broadcast clients.

```
Console(config)# sntp broadcast client enable
```

sntp anycast client enable

The **sntp anycast client enable** global configuration command enables Simple Network Time Protocol (SNTP) Anycast clients. To disable SNTP Anycast clients, use the **no** form of this command.

Syntax

sntp anycast client enable

no sntp anycast client enable

Default Configuration

SNTP Anycast clients are disabled.

Command Mode

Global Configuration mode

User Guidelines

Polling time is determined by the **sntp client poll timer** global configuration command.

Use the **sntp client enable** interface configuration command to enable SNTP clients on a specific interface.

Examples

The following example enables Anycast clients.

```
Console(config)# sntp anycast client enable
```

sntp client enable

The **sntp client enable** interface configuration command enables Simple Network Time Protocol (SNTP) Broadcast and Anycast clients on an interface. To disable the SNTP client, use the **no** form of this command.

Syntax

sntp client enable

no sntp client enable

Default Configuration

Client is disabled on an interface.

Command Mode

Interface Configuration (Ethernet, port-channel, VLAN) mode

User Guidelines

Use the **sntp broadcast client enable** global configuration command to enable Broadcast clients globally.

Use the **sntp anycast client enable** global configuration command to enable Anycast clients globally.

Examples

The following example enables SNTP Broadcast and Anycast clients on the interface.

```
Console(config-if)# sntp client enable
```

sntp unicast client enable

The **sntp unicast client enable** global configuration command enables clients to use Simple Network Time Protocol (SNTP) predefined Unicast clients. To disable SNTP Unicast clients, use the **no** form of this command.

Syntax

sntp unicast client enable

no sntp unicast client enable

Default Configuration

The SNTP Unicast clients are disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **sntp server** command to define SNTP servers.

Examples

The following example enables the device to use Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from servers.

```
Console(config)# sntp unicast client enable
```

sntp unicast client poll

The **sntp unicast client poll** global configuration command enables polling for Simple Network Time Protocol (SNTP) predefined Unicast servers. To disable polling for SNTP clients, use the **no** form of this command.

Syntax

sntp unicast client poll

no sntp unicast client poll

Default Configuration

Polling is disabled.

Command Mode

Global Configuration mode

User Guidelines

Polling time is determined by the **sntp client poll timer** global configuration command.

Examples

The following example enables polling for the Simple Network Time Protocol (SNTP) predefined unicast clients:

```
Console(config)# sntp unicast client poll
```

sntp server

The **sntp server** global configuration command configures the device to use Simple Network Time Protocol (SNTP) to request and accept Simple Network Time Protocol (SNTP) traffic from a specified server. To remove a server from the list of SNTP servers, use the **no** form of this command.

Syntax

sntp server {*ip-address* | *hostname*}[**poll**] [**key** *keyid*]

no sntp server *ip-address*

- *ip-address* — IP address of the server. For information about defining a server on an Out-of-Band interface, see the user guidelines.

- *hostname* — Hostname of the server. (Range: 1-158 characters)
- **poll** — Enable polling.
- *keyid* — Authentication key to use when sending packets to this peer. (Range:1-4294967295)

Default Configuration

No servers are defined.

Command Mode

Global Configuration mode

User Guidelines

Up to 8 SNTP servers can be defined.

Use the **sntp unicast client enable** global configuration command to enable Unicast clients globally.

To enable polling globally, you should also use the **sntp unicast client poll** global configuration command.

Polling time is determined by the **sntp client poll timer** global configuration command.

To define an SNTP server on the out-of-band port, use the out-of-band IP address format **oob**/*ip-address*.

Examples

The following example configures the device to accept Simple Network Time Protocol (SNTP) traffic from the server on 192.1.1.1.

```
Console(config)# sntp server 192.1.1.1
```

show clock

The **show clock** user EXEC command displays the time and date from the system clock.

Syntax

show clock [**detail**]

- **detail** — Shows timezone and summertime configuration.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

The symbol that precedes the show clock display indicates the following:

Symbol	Description
*	Time is not authoritative.
(blank)	Time is authoritative.
.	Time is authoritative, but SNTP is not synchronized.

Example

The following example displays the time and date from the system clock.

```
Console> show clock

15:29:03 PDT(UTC-7) Jun 17 2005
Time source is SNTP

Console> show clock detail
15:29:03 PDT(UTC-7) Jun 17 2005
Time source is SNTP

Time zone:
Acronym is PST
Offset is UTC-8

Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.
```

show sntp configuration

The **show sntp configuration** privileged EXEC command shows the configuration of the Simple Network Time Protocol (SNTP).

Syntax

show sntp configuration

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the current SNTP configuration of the device.

```
Console# show sntp configuration
Polling interval: 180 seconds
No MD5 Authentication keys.
Authentication is not required for synchronization.
No trusted keys.

Unicast Clients Polling: Disabled

Server                         Polling         Encryption Key
-----------                    --------        -----------------
42.52.3.123                    Disabled        Disabled
212.12.34.23                   Enabled         Disabled

OOB SNTP servers:

Server                         Polling         Encryption Key
-----------                    --------        -----------------
67.1.1.2                       Disabled        Disabled
```

```
Server                          Polling         Encryption Key
----------                      --------        -----------------
10.1.1.91                       Enabled         9

Broadcast Clients: Enabled
Anycast Clients: Enabled
Broadcast and Anycast Interfaces: g1, g3
```

show sntp status

The **show sntp status** privileged EXEC command shows the status of the Simple Network Time Protocol (SNTP).

Syntax

show sntp status

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

ExamSples

The following example shows the status of the SNTP.

```
Console# show sntp status
Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)

Unicast servers:
Server         Status     Last response                   Offset   Delay
                                                          [mSec]   [mSec]
---------      ------     ---------------                 -----    ------
176.1.1.8      Up         19:58:22.289 PDT Feb 19 2005    7.33     117.79
176.1.8.179    Unknown    12:17.17.987 PDT Feb 19 2005    8.98     189.19
```

```
OOB unicast servers:
Server          Status     Last response                    Offset   Delay
                                                            [mSec]   [mSec]
---------       ------     ---------------                  -----    ------
176.1.1.8       Unknown    19:19:51.198 PDT Feb 19 2005     2.98     129.19


Anycast
server:
Server          Interface  Status  Last response            Offset   Delay
                                                            [mSec]   [mSec]
---------       -------    -----   -------------            ------   -----
176.1.11.8      VLAN 118   Up      9:53:21.789 PDT Feb 19   7.19     119.89
                                   2005


Broadcast:
Server          Interface          Last response
---------       ---------          ------------------------
176.9.1.1       VLAN 119           19:17:59.792 PDT Feb 19 2005
```

7

DHCP Relay Commands

ip dhcp relay enable

The **ip dhcp relay enable** global configuration command enables Dynamic Host Configuration Protocol (DHCP) relay agent features on the router. To disable the relay agent features, use the **no** form of this command.

Syntax

ip dhcp relay enable

no ip dhcp relay enable

Default Configuration

DHCP is disabled on the router.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables DHCP services on the DHCP Server.

```
Console(config)# ip dhcp relay enable
```

ip dhcp relay address

The **ip dhcp relay address** global configuration command defines the DHCP servers available for the DHCP relay. To remove a server from the available DHCP servers list, use the **no** form of this command.

Syntax

ip dhcp relay address *ip-address*

no dhcp relay address [*ip-address*]

- *ip-address*—DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode

Global Configuration mode

User Guidelines

If no IP address is specified when using the **no** form of the command, all configured servers are removed.

Example

The following example defines the DHCP server with the address 172.16.1.1 to be available for DHCP address.

```
Console(config)# ip dhcp relay address 172.16.1.1
```

show ip dhcp relay

The **show ip dhcp relay** privileged EXEC command displays the defined DHCP relay server addresses available for DHCP relay.

Syntax

show ip dhcp relay

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays DHCP relay server addresses.

```
Console# show ip dhcp relay

DHCP relay is enabled.

Servers: 172.16.1.11, 172.16.8.11
```

8

Configuration and Image Files

configure

The **configure** privileged EXEC command enters the global configuration mode.

Syntax

configure

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no default configuration.

Example

In the following example, because no keyword is entered, a prompt is displayed. After the keyword is selected, a message confirming the command entry method is displayed.

```
Console# configure
Console (config)#
```

copy

The **copy** privileged EXEC command copies files from a source to a destination.

Syntax

copy *source-url destination-url*

- *source-url*—The source file location URL or reserved keyword being copied.
- *destination-url*—The destination file URL or reserved keyword.

The following table displays keywords aliases to URL:

Keyword	Source or destination
running-config	Represents the current running configuration file.
startup-config	Represents the startup configuration file.
backup-config	Represents the backup configuration file.
image	The image is executable code which is decompressed during system startup, into the switching and routing software that manages the device. There are always two images stored in the device flash known as "image-1" and "image-2". The images do not necessarily have to contain the same versions of the software. One of these images is always marked as active and the other image serves as a back-up. The "active" image is either the last downloaded image or the image configured as the "active" image. The switch boot code first tries to load and run the active image. However, if the active image is found to be corrupt, the boot code tries to load the back-up image. If the back-up image is also corrupt the boot code prompts the user to initiate the X-modem transfer of a valid image through the serial connection. The image file name is in the format 6024_abcd.dos, where abcd represents the release number.
boot	Boot file. The name of the image is in the format 6024_boot_abcd.rfb, where abcd represents the release number.
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is **tftp:***[[//location]/directory]/filename*.
xmodem:	Source for the file from a serial connection that uses the Xmodem protocol.
null:	Null destination for copies or files. A remote file can be copied to null to determine its size.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The location of a file system dictates the format of the source or destination URL.

The startup-config and the backup-config files cannot be copied to the running-config file.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network. While a configuration file is being copied (downloaded or uploaded), the device ignores the user input sent to the device via CLI. Note that this behavior only applies to the session in the context of which the copying is taking place; all other management sessions may experience a delayed responsiveness but accept CLI commands and process HTTP requests.

Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination exist. Specifically, the following cannot be copied:

- If the source file and destination file are the same file.
- **xmodem** cannot be a destination. Can only be copied to **image**, **boot** and **null**.
- **tftp** cannot be the source and destination on the same copy.
- **startup-config** and **backup-config** cannot be copied to **running-config.**

Copy Character Descriptions

Character	Description
!	For network transfers, an exclamation point indicates that the copy process is taking place. Each "!" indicates that the file download is progressing successfully.
.	For network transfers, a period indicates that the copy process timed out. Many periods in a row typically mean that the copy process may fail.

Copying Image File from a Server to Flash Memory

Use the **copy source-url image** command to copy an image file from a server to Flash memory.

Copying Boot File from a Server to Flash Memory

Use the **copy source-url boot** command to copy a boot file from a server to Flash memory.

Copying a Configuration File from a Server to the Running Configuration

Use the **copy source-url running-config** command to load a "configuration file" from a network server to the device "running configuration". The configuration is added to the "running configuration" as if the commands were typed in the command-line interface (CLI). The resulting configuration file is a combination of the previous "running configuration" and the loaded "configuration file", with the loaded "configuration file" having precedence.

Copying a Configuration File from a Server to the Startup Configuration

Use the **copy source-url startup-config** command to copy a "configuration file" from a network server to the device "startup configuration". These commands replace the startup configuration file with the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the **copy running-config destination-url** command to copy the current configuration file to a network server using TFTP. Use the copy **startup-config destination-url** command to copy the "startup configuration" file to a network server.

The configuration file copy can serve as a backup copy.

Saving the Running Configuration to the Startup Configuration

Use the **copy running-config startup-config** command to copy the "running configuration" to the "startup configuration".

Backup the Running Configuration or Startup Configuration to the Backup Configuration

Use the **copy running-config backup-config** command to backup the "running configuration" to the "backup configuration" file. Use the **copy startup-config backup-config** command to backup the startup configuration to the backup configuration file.

Specifying out-of-band addresses

To copy from/to a server on the out-of-band port, use the out-of-band P address format: **oob/ip-address**.

Example

The following example copies a system image named file1 from the TFTP server with an IP address of 172.16.101.101 to a non active image file.

```
Console# copy tftp://172.16.101.101/file1 image


Accessing file 'file1' on 172.16.101.101...

Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!! [OK]

Copy took 0:01:11 [hh:mm:ss]
```

Example

The following example copies a configuration file named **configfile** from a TFTP server on the out-of-band port with an IP address of 172.16.1.1 to the **startup-config** file.

```
Router# copy tftp://oob/172.16.1.1/file1 startup-config


Accessing file 'configfile' on oob/172.16.1.1...

Loading file1 from oob/172.16.1.1:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!! [OK]

Copy took 0:0:23 [hh:mm:ss]
```

delete startup-config

The **delete startup-config** privileged EXEC command deletes the **startup-config** file.

Syntax

delete startup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example deletes the startup-config file.

```
Console# delete startup-config
```

boot system

The **boot system** privileged EXEC command specifies the system image that the device loads at startup.

Syntax

boot system {**image-1** | **image-2**}

- **image-1**—Specifies image 1 as the system startup image.
- **image-2**—Specifies image 2 as the system startup image.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show bootvar** command to find out which image is the active image.

Examples

The following example loads system image 1 for the next device startup.

```
Console# boot system image-1
```

show running-config

The **show running-config** privileged EXEC command displays the contents of the currently running configuration file.

Syntax

show running-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The print-out is sorted by feature.

Information about the configuration of the Out-of-Band port is shown separately from information about other system configurations. However, information about the Out-of-Band port is displayed with information about the router port.

Examples

The following example displays the contents of the running-config file.

```
Console# show running-config


Router Configuration
---------------------
no spanning-tree
interface ethernet g1
ip address 16.1.1.3 255.0.0.0
exit
radius-server host 16.1.1.200 auth-port 1812    key da
aaa authentication enable 12 radius
aaa authentication login 123 radius
line telnet
login authentication 123
enable authentication 12
exit


OOB host Configuration
-----------------------
Empty configuration
```

show startup-config

The **show startup-config** privileged EXEC command displays the startup configuration file contents.

Syntax

show startup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the contents of the startup-config file.

```
Console# show startup-config


Router Configuration
-----------------------------
Empty configuration


OOB host Configuration
-----------------------------
Empty configuration



_____________________________
Default settings:
_____________________________


Router Configuration
-----------------------------
Service tag: 12345678
SW version 1.3.0.18 (date  27-Dec-2004 time  19:00:32)

```

```
Gigabit Ethernet Ports
-----------------------------
no shutdown
speed 1000
duplex full
negotiation
flow-control off
mdix auto
no back-pressure

interface vlan 1
interface port-channel 1 - 7

no router RIP

no router OSPF enable

spanning-tree
spanning-tree mode STP

qos basic
```

```
OOB host Configuration

------------------------

interface out-of-band-eth

no shutdown

speed 100

duplex full

negotiation

flow-control off

mdix auto

no back-pressure

exit
```

show backup-config

The **show backup-config** privileged EXEC command displays the backup configuration file contents.

Syntax

show backup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the contents of the backup-config file.

```
Console# show backup-config
no spanning-tree
interface ethernet g12
ip address 12.1.1.1 255.0.0.0
exit
```

show bootvar

The **show bootvar** privileged EXEC command displays the active system image file that the device loads at startup.

Syntax

show bootvar

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the active system image file that the device loads at startup.

```
Console# show bootvar
Images currently available on the FLASH
image-1active (selected for next boot)
image-2not active
```

9

Ethernet Configuration Commands

interface ethernet

The **interface ethernet** global configuration command enters the interface configuration mode to configure an Ethernet type interface.

Syntax

interface ethernet *interface*

- *interface*—Valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables ports g18 for configuration.

```
Console(config)# interface ethernet g18
Console(config-if)#
```

interface range ethernet

The **interface range ethernet** global configuration command enters the interface configuration mode to configure multiple Ethernet type interfaces.

Syntax

interface range ethernet {*port-range* | *all*}

- *port-range*—List of valid ports to add. Separate non consecutive ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- **all**—All Ethernet ports.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each active interface in the range. If the command returns an error on one of the active interfaces, it does not stop executing commands on other active interfaces.

Example

The following example shows how ports g18 to g20 and ports g22 to g24 are grouped to receive the same command.

```
Console(config)# interface range ethernet g18-20, g22-24

Console(config-if)#
```

interface out-of-band-eth

The **interface out-of-band-eth** global configuration command configures the Out-of-Band Ethernet port and enter interface configuration mode.

interface out-of-band-eth [*interface*]

- *interface*—Interface number. If unspecified defaults to 1.

Default Configuration

The interface is enabled.

Command Mode

Global Configuration mode

User Guidelines

The following commands are available on interface Out-of-Band-eth mode:

shutdown, **description**, **speed**, **duplex**, **negotiation**, **flowcontrol**, **ip**

Examples

The following example enters Out-of-Band Ethernet interface configuration mode.

```
Console(config)# interface out-of-band-eth

Console(config-oob)#
```

shutdown

The **shutdown** interface configuration command disables interfaces. To restart a disabled interface, use the **no** form of this command.

Syntax

shutdown

no shutdown

Default Configuration

The interface is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel, Out-of-Band Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example disables Ethernet g5.

```
Console(config)# interface ethernet g5
Console(config-if)# shutdown
```

The following example re-enables ethernet port 5.

```
Console(config)# interface ethernet g5
Console(config-if)# no shutdown
```

description

The **description** interface configuration command adds a description to an interface. To remove the description use the **no** form of this command.

Syntax

description *string*

no description

- *string*—Comment or a description of the port up to 64 characters.

Default Configuration

By default, the interface does not have a description.

Command Mode

Interface Configuration (Ethernet, port-channel, Out-of-Band Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example adds a description to the Ethernet g5.

```
Console(config)# interface ethernet g5
Console(config-if)# description RD_SW#3
```

speed

The **speed** interface configuration command configures the speed of a given Ethernet interface when not using auto-negotiation. To restore the default, use the **no** form of this command.

Syntax

speed {10 | 100 | 1000}

no speed

- **10**—Configures the port to 10 Mbps.
- **100**—Configures the port to 100 Mbps.
- **1000**—Configures the port to 1000 Mbps.

Default Configuration

Maximum port capability.

Command Mode

Interface Configuration (Ethernet, port-channel, Out-of-Band Ethernet) mode

User Guidelines

The command "**no speed**" in port-channel context returns each port in the port-channel to its maximum capability.

Before attempting to force a particular duplex mode the port operating at 10/100 Mbps, disable the auto-negotiation on that port.

Example

The following example configures the speed operation of Ethernet g5 to force 100-Mbps operation.

```
Console(config)# interface ethernet g5
Console(config-if)# speed 100
```

duplex

The **duplex** interface configuration command configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation. To restore the default, use the **no** form of this command.

Syntax

duplex {half | full}

no duplex

- **half**—Force half-duplex operation
- **full**—Force full-duplex operation

Default Configuration

The interface is set to full duplex.

Command Mode

Interface Configuration (Ethernet, Out-of-Band Ethernet) mode

User Guidelines

Before attempting to force a particular duplex mode on the port operating at 10/100 Mbps, disable the auto-negotiation on that port.

Half duplex mode can be set only for ports operating at 10 Mbps or 100 Mbps.

Example

The following example configures the duplex operation of Ethernet g5 to force full duplex operation.

```
Console(config)# interface ethernet g5
Console(config-if)# duplex full
```

negotiation

The **negotiation** interface configuration command enables auto-negotiation operation for the speed and duplex parameters of a given interface. To disable negotiation, use the **no** form of this command.

Syntax

negotiation [**capability1** [**capability2…capability5**]]

no negotiation

- **capabilities—**Port capabilities to be advertised.
  (Possible values: 10h, 10f, 100h, 100f and 1000f)

Default Configuration

auto-negotiation with all capabilities

Command Mode

Interface Configuration (Ethernet, port-channel, Out-of-Band Ethernet) mode

User Guidelines

Turning off auto-negotiation on an aggregate link may, under some circumstances, make it non-operational. If the other side has auto-negotiation turned on, it may re-synchronize all members of the aggregated link to half-duplex operation, and may, as per the standards, set them all inactive.

Example

The following example enables autonegotiation with all capabilities on g5.

```
Console(config)# interface ethernet g5

Console(config-if)# negotiation
```

flowcontrol

The **flowcontrol** interface configuration command configures the Flow Control on a given interface. To restore the default, use the **no** form of this command.

Syntax

flowcontrol {**auto** | **on** | **off**}

no flowcontrol

- **auto**—Enables auto-negotiation of Flow Control.
- **on**—Enables Flow Control.

- **off**—Disables Flow Control.

Default Configuration

Flow Control is off.

Command Mode

Interface configuration (Ethernet, port-channel) mode

User Guidelines

Flow Control will operate only if duplex mode is set to FULL. Back Pressure will operate only if duplex mode is set to HALF.

When Flow Control is ON, the head-of-line-blocking mechanism of this port is disabled.

If a link is set to NOT use auto-negotiation, the other side of the link must also be configured to not use auto-negotiation.

To select **auto**, ensure negotiation for Flow Control is enabled.

Example

In the following example, Flow Control is enabled on g5.

```
Console(config)# interface ethernet g5

Console(config-if)# flowcontrol on
```

mdix

The **mdix** interface configuration command enables automatic crossover on a given interface. To disable automatic crossover, use the **no** form of this command.

Syntax

mdix {on | auto}

no mdix

- **on**—Manual mdix
- **auto**—Auto mdi/mdix

Default Configuration

Automatic crossover is enabled

Command Mode

Interface Configuration (Ethernet) mode

Example

In the following example, automatic crossover is enabled on g5.

```
Console(config)# interface ethernet g5
Console(config-if)# mdix auto
```

back-pressure

The **back-pressure** interface configuration command enables Back Pressure on a given interface. To disable Back Pressure, use the **no** form of this command.

Syntax

back-pressure

no back-pressure

Default Configuration

Back Pressure is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

Back Pressure will operate only if duplex mode is set to half.

Example

In the following example Back Pressure is enabled on g5.

```
Console(config)# interface ethernet g5
Console(config-if)# back-pressure
```

port jumbo-frame

The **port jumbo-frame** global configuration command enables jumbo frames for the device. To disable jumbo frames, use the **no** form of this command.

Syntax

port jumbo-frame

no port jumbo-frame

Default Configuration

Jumbo Frames are not enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

In the following example, Jumbo Frames are enabled on the device.

```
Console(config)# port jumbo-frame
```

clear counters

The **clear counters** user EXEC mode command clears statistics on an interface.

Syntax

clear counters [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—Valid Ethernet port.
- *port-channel-number*—Valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In the following example, the counters for interface g1 are cleared.

```
Console> clear counters ethernet g1
```

set interface active

The **set interface active** privileged EXEC mode command reactivates an interface that was suspended by the system.

Syntax

set interface active {**ethernet** *interface* | **port-channel** *port-channel-number*}

- *interface*—Valid Ethernet port.

- *port-channel-number*—Valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

Privilege EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example activates interface g9, which is disabled.

```
Console# set interface active ethernet g9
```

show interfaces configuration

The **show interfaces configuration** Privilege EXEC mode command displays the configuration for all configured interfaces.

Syntax

show interfaces configuration [**ethernet interface** | **port-channel** *port-channel-number* | **oob-eth** *oob-interface*]

- *interface*—Valid Ethernet port.
- *port-channel-number*—Valid port-channel trunk index.
- *oob-interface*—Out-of-Band Ethernet port number.

Default Configuration

This command has no default configuration.

Command Modes

Privilege EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration for all configured interfaces:

```
Console# show interfaces configuration

                                          Flow    Admin    Back   Mdix
     Port    Type       Duplex  Speed  Neg     control  State   Pressure Mode
     ........ ............ ......  .....  ........ .......  .....   ........ ......................................................
     g1     1G-Copper    Full    1000   Enabled  Off     Up      Disabled Auto
     g2     1G-Copper    Full    1000   Enabled  Off     Up      Disabled Auto
     g3     1G-Copper    Full    1000   Enabled  Off     Up      Disabled Auto
     g4     1G-Copper    Full    1000   Enabled  Off     Up      Disabled Auto
     g5     1G-Copper    Full    1000   Enabled  Off     Up      Disabled Auto
     g6     1G-Copper    Full    1000   Enabled  Off     Up      Disabled Auto
     g7     1G-Copper    Full    1000   Enabled  Off     Up      Disabled Auto
     ...
     g22     1G-Combo-C   Full    1000   Enabled  Off     Up      Disabled Auto
     g23     1G-Combo-C   Full    1000   Enabled  Off     Up      Disabled Auto
     g24     1G-Combo-C   Full    1000   Enabled  Off     Up      Disabled Auto


                               Flow    Admin    Back
     Ch      Type    Speed  Neg     control  State   Pressure
     ........ ....... .....  ........ .......  .....   ........
     ch1      --      --     Enabled     Off     Up     Disabled
     ch2      --      --     Enabled     Off     Up     Disabled
     ch3      --      --     Enabled     Off     Up     Disabled
     ch4      --      --     Enabled     Off     Up     Disabled
     ch5      --      --     Enabled     Off     Up     Disabled
     ch6      --      --     Enabled     Off     Up     Disabled
     ch7      --      --     Enabled     Off     Up     Disabled
                                                       Admin
     Oob-eth   Type          Duplex  Speed  Neg       State
     ........  ............ ......  .....  ........ .....
     Oob-eth 1 100M-Copper  Full    100    Enabled  Up
```

The displayed port configuration information includes the following:

- **Port**—The port number.
- **Port Type**—The port designated IEEE shorthand identifier. For example 1000Base-T refers to 1000 Mbps baseband signaling inluding both Tx and Rx transmissions.
- **Duplex**—Displays the port Duplex status.
- **Speed**—Refers to the port speed.
- **Neg**—Describes the Auto-negotiation status.
- **Flow Control**—Displays the Flow Control status.
- **Back Pressure**—Displays the Back Pressure status.
- **MDIX Mode**—Displays the Auto-crossover status.
- **Admin State**—Displays whether the port is enabled or disabled.

show interfaces status

The **show interfaces status** user EXEC command displays the status for all configured interfaces.

Syntax

show interfaces status [**ethernet interface** | **port-channel** *port-channel-number* | **oob-eth** *oob-interface*]

- *interface*—A valid Ethernet port.
- *port-channel-number*—A valid port-channel trunk index.
- *oob-interface*—Out-of-Band Ethernet port number.

Default Configuration

This command has no default configuration.

Command Mode

Privilege EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the status for all configured interfaces.

```
Console# show interfaces status
                                           Flow Link          Back   Mdix
Port     Type          Duplex  Speed Neg      control State       Pressure
Mode
g1       1G-Copper       --      --      --      --  Down           --     --
g2       1G-Copper       --      --      --      --  Down           --     --
g3       1G-Copper       --      --      --      --  Down           --     --
g4       1G-Copper       --      --      --      --  Down           --     --
g5       1G-Copper       --      --      --      --  Down           --     --
g6       1G-Copper       --      --      --      --  Down           --     --
g7       1G-Copper       --      --      --      --  Down           --     --
g8       1G-Copper       --      --      --      --  Down           --     --
...
g22      1G-Combo-C      --      --      --      --  Down           --     --
g23      1G-Combo-C      --      --      --      --  Down           --     --
g24      1G-Combo-C      --      --      --      --  Down           --     --

                                          Flow    Link          Back
Ch       Type    Duplex  Speed  Neg       control  State        Pressure
........ ....... ......  .....  ........ .......  ........... ........
ch1         --      --      --      --       --    Not Present    --
ch2         --      --      --      --       --    Not Present    --
ch3         --      --      --      --       --    Not Present    --
ch4         --      --      --      --       --    Not Present    --
ch5         --      --      --      --       --    Not Present    --
ch6         --      --      --      --       --    Not Present    --
ch7         --      --      --      --       --    Not Present    --

                                              Link
Oob-eth   Type          Duplex  Speed Neg      State
........  ............ ......  ..... ........ ...........
Oob-eth 1 100M-Copper  Full    100   Enabled  Up
```

The displayed port status information includes the following:

- **Port**—The port number.
- **Description**—If the port has a description, the description is displayed.
- **Port Type**—The port designated IEEE shorthand identifier. For example, 1000Base-T refers to 1000 Mbps baseband signaling inluding both Tx and Rx transmissions.
- **Duplex**—Displays the port Duplex status.
- **Speed**—Refers to the port speed.
- **Neg**—Describes the Auto-negotiation status.
- **Flow Control**—Displays the Flow Control status.
- **Back Pressure—**Displays the Back Pressure status.
- **Link State**—Displays the Link Aggregation status.

show interfaces description

The **show interfaces description** user EXEC command displays the description for all configured interfaces.

Syntax

show interfaces description [**ethernet interface | port-channel** *port-channel-number*| **oob-eth** *oob-interface*]

- *interface*—Valid Ethernet port.
- *port-channel-number*—A valid port-channel trunk index.
- *oob-interface*—Out-of-Band Ethernet port number.

Default Configuration

This command has no default configuration.

Command Modes

Privilege EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the description for the interface g1.

```
Console# show interfaces description ethernet g1

Port          Description

.....         ...........

g1            connect_to_server
```

show interfaces counters

The **show interfaces counters** user EXEC command displays traffic seen by the physical interface.

Syntax

show interfaces counters [**ethernet** *interface* **|** **port-channel** *port-channel-number*]

- *interface*—A valid Ethernet port.
- *port-channel-number*—A valid port-channel index.

Default Configuration

This command has no default configuration.

Command Modes

Privilege EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays traffic seen by the physical interface:

```
Console# show interfaces counters
 Port        InOctets  InUcastPkts InMcastPkts InBcastPkts
----------- ---------- ----------- ----------- ------------
 g1            0           0           0           0
 g2            0           0           0           0
 g3            0           0           0           0
 g4            0           0           0           0
 ...
g23            0           0           0           0
g24            0           0           0           0

 Port       OutOctets  OutUcastPkts OutMcastPkts OutBcastPkts
----------- ---------- ------------ ------------ ------------
 g1            0           0            0            0
 g2            0           0            0            0
 g3            0           0            0            0
 g4            0           0            0            0
 ...
g23            0           0            0            0
g24            0           0            0            0

 Ch         InOctets  InUcastPkts InMcastPkts InBcastPkts
----------- --------- ----------- ----------- -----------
 ch1            0           0           0           0
 ch2            0           0           0           0
 ch3            0           0           0           0
 ...
 ch7            0           0           0           0

 Ch        OutOctets  OutUcastPkts OutMcastPkts OutBcastPkts
---------- ---------- ------------ ------------ ------------
 ch1            0           0            0            0
 ch2            0           0            0            0
 ch3            0           0            0            0
 ...
 ch7            0           0            0            0
```

The following example displays counters for port g1.

```
Console# show interfaces counters ethernet g1
 Port        InOctets  InUcastPkts InMcastPkts InBcastPkts
-------- ---------- ----------- ----------- -----------
 g1            0           0           0           0

 Port       OutOctets  OutUcastPkts OutMcastPkts OutBcastPkts
-------- ---------- ------------ ------------ ------------
 g1            0           0            0            0

FCS Errors: 0
Single Collision Frames: 0
Late Collisions: 0
Excessive Collisions: 0
Internal MAC Tx Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

The following table describes the fields shown in the display:

Field	**Description**
InOctets	Counted received octets.
InUcastPkts	Counted received Unicast packets.
InMcastPkts	Counted received Multicast packets.
InBcastPkts	Counted received Broadcast packets.
OutOctets	Counted transmitted octets.
OutUcastPkts	Counted transmitted Unicast packets.
OutMcastPkts	Counted transmitted Multicast packets.
OutBcastPkts	Counted transmitted Broadcast packets.
FCS Errors	Counted frames received that are an integral number of octets in length but do not pass the FCS check.

Single Collision Frames	Counted frames that are involved in a single collision, and are subsequently transmitted successfully.
Late Collisions	Counted times that a collision is detected later than one slotTime into the transmission of a packet.
Excessive Collisions	Counted frames for which transmission fails due to excessive collisions.
Internal MAC Tx Errors	Counted frames for which transmission fails due to an internal MAC sublayer transmit error.
Oversize Packets	Counted frames received that exceed the maximum permitted frame size.
Internal MAC Rx Errors	Counted frames for which reception fails due to an internal MAC sublayer receive error.
Received Pause Frames	Counted MAC Control frames received with an opcode indicating the PAUSE operation.
Transmitted Pause Frames	Counted MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

show ports jumbo-frame

The **show ports jumbo-frame** user EXEC command displays the jumbo frames configuration.

show ports jumbo-frame

Default Configuration

This command has no default configuration.

Command Modes

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the jumbo frames configuration.

```
Console# show ports jumbo-frame

Jumbo frames are disabled

Jumbo frames will be enabled after reset
```

port storm-control include-multicast

The **port storm-control include-multicast** global configuration command enables the device to count Multicast packets together with Broadcast packets. To disable counting of Multicast packets, use the **no** form of this command.

Syntax

port storm-control include-multicast

no port storm-control include-multicast

Default Configuration

Multicast packets are not counted.

Command Modes

Global Configuration mode

User Guidelines

To control multicasts storms use the commands **port storm-control broadcast enable** and **port storm-control broadcast rate**.

Example

The following example enables the counting of Multicast packets.

```
Console# configure
Console(config)# port storm-control include-multicast
```

port storm-control broadcast enable

The **port storm-control broadcast enable** interface configuration command enables Broadcast storm control. To disable Broadcast storm control, use the **no** form of this command.

Syntax

port storm-control broadcast enable

no port storm-control broadcast enable

Default Configuration

Broadcast storm control is disabled.

Command Modes

Interface Configuration (Ethernet) mode

User Guidelines

Use the port **storm-control broadcast rate** interface configuration command, to set the maximum allowable Broadcast rate.

Multicast can be counted as part of the "storm" frames if the **port storm-control include-multicast** global configuration command is already executed.

Example

The following example enables Broadcast storm control on port g5.

```
Console(config)# interface ethernet g5
Console(config-if)# port storm-control broadcast enable
```

port storm-control broadcast rate

The **port storm-control broadcast rate** interface configuration command configures the maximum Broadcast rate. Use the **no** form of this command to configure the default value.

port storm-control broadcast rate *rate*

no port storm-control broadcast rate

- *rate*—Maximum of kilobytes per second of Broadcast and Multicast traffic on a port. (Rate: 0 - 1000000)

Default Configuration

The default storm control Broadcast rate is 12000.

Command Mode

Interface Configuration (Ethernet)

User Guidelines

Use the **port storm-control broadcast enable** interface configuration command to enable Broadcast storm control.

The rate is rounded to the nearest 64 kbytes/sec (except 1 - 63 kbytes/sec, which is rounded to 64 kbytes/sec). Note that if the rate is 0, Broadcast packets are not forwarded.

Example

The following example configures the maximum Broadcast rate 10 kilobytes per second.

```
Console(config)# interface ethernet g2
Console(config-if)# port storm-control broadcast rate 10
```

show ports storm-control

The **show ports storm-control** privileged EXEC command displays the storm control configuration.

Syntax

show ports storm-control [*interface*]

- *interface*—A valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the storm control configuration.

```
Console# show ports storm-control


PortBroadcast Storm control [kbyes/sec]
-------------------------------------------------------
g1      8000
g2 Disabled
g3 Disabled
```

show interfaces advertise

The **show interfaces advertise** privileged EXEC command displays information about auto negotiation advertisement.

Syntax

show interfaces advertise [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—A valid Ethernet port.
- *port-channel-number*—A valid port-channel.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information about auto negoiation advertisement.

```
Console# show interfaces advertise

Port  Type        Neg      Operational Link Advertisement

----  --------    -------  ------------------------------

g1    1G-Copper   Enable   1000f, 100f, 100h, 10f, 10h

g2    1G-Copper   Enable   1000f


Console# show interfaces advertise ethernet g1


Port: Ethernet g1

Type: 1G-Copper

Link state: Up

Auto negotiation: enabled


                           10h     10f     100h    100f    1000f

Admin Local Link           ------  ------  ------  ------  ------
Advertisement

Oper Local Link            yes     yes     yes     yes     yes
Advertisement

Remote Link Advertisement  yes     yes     yes     yes     yes

Priority Resolution        no      no      yes     yes     yes
```

10

GVRP Commands

gvrp enable (global)

GVRP, or GARP VLAN Registration Protocol, is an industry-standard protocol designed to propagate VLAN information from device to device. With GVRP, a single switch is manually configured with all desired VLANs for the network, and all other switches on the network learn these VLANs dynamically.

The **gvrp enable** global configuration command enables GVRP globally. To disable GVRP globally on the switch, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example globally enables GVRP on the device.

```
Console (config)# gvrp enable
```

gvrp enable (interface)

The **gvrp enable** interface configuration command enables GVRP on an interface. To disable GVRP on an interface, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is disabled on all interfaces by default.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

An access port would not dynamically join a VLAN because it is always a member in only one VLAN.

Example

The following example enables GVRP on ethernet g8.

```
Console (config)# interface ethernet g8
Console (config-if)# gvrp enable
```

garp timer

The **garp timer** interface configuration command adjusts the GARP application join, leave, and leaveall GARP timer values. To reset the timer to default values, use the **no** form of this command.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*

no garp timer

- **join**—Indicates the time in milliseconds that PDUs are transmitted. (Range: 10-2147483640)
- **leave**—Indicates the amount of time in milliseconds that the device waits before leaving its GARP state. The Leave Time is activated by a Leave All Time message sent/received, and cancelled by the Join message. (Range: 10-2147483640)
- **leaveall**—Used to confirm the port within the VLAN. The time in milliseconds between messages sent. (Range: 10-2147483640)
- *timer_value*—Timer values in milliseconds.

Default Configuration

The default timer values are as follows:

- Join timer—200 milliseconds
- Leave timer—600 milliseconds
- Leavall timer—10000 milliseconds

Command Mode

Interface configuration (Ethernet, port-channel) mode

User Guidelines

The following *relationship* for the various timer values must be maintained:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on Layer 2-connected devices, GARP application will not operate successfully.

As the number of dynamic VLANs (GVRP) increases, the leave time should be increased from the default value. For example, if the number of dynamic VLANs is 400, it is recommended to increase the leave time.

Example

The following example sets the leave timer for port g8 to 900 milliseconds.

```
Console (config)# interface ethernet g8

Console (config-if)# garp timer leave 900
```

gvrp vlan-creation-forbid

The **gvrp vlan-creation-forbid** interface configuration command enables or disables dynamic VLAN creation. To disable dynamic VLAN creation, use the **no** form of this command.

Syntax

gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid

Default Configuration

By default, dynamic VLAN creation is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command forbids dynamic VLAN creation from the interface. The creation or modification of dynamic VLAN registration entries as a result of the GVRP exchanges on an interface are restricted only to those VLANs for which static VLAN registration exists.

Example

The following example disables dynamic VLAN creation on port g8.

```
Console (config)# interface ethernet g8
Console (config-if)# gvrp vlan-creation-forbid
```

gvrp registration-forbid

The **gvrp registration-forbid** interface configuration command de-registers all dynamic VLANs, and prevents dynamic VLAN registration on the port. To allow dynamic registering for VLANs on a port, use the **no** form of this command.

Syntax

gvrp registration-forbid

no gvrp registration-forbid

Default Configuration

Dynamic registering and deregistering for each VLAN on the port is allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how default dynamic registering and deregistering is forbidden for each VLAN on port g8.

```
Console (config)# interface ethernet g8
Console (config-if)# gvrp registration-forbid
```

clear gvrp statistics

The **clear gvrp statistics** privileged EXEC command clears all the GVRP statistics information.

Syntax

clear gvrp statistics [**ethernet** *interface* **|** **port-channel** *port-channel-number*]

- *interface*—A valid Ethernet interface.
- *port-channel-number*—A valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears all the GVRP statistics information on port g8.

```
Console# clear gvrp statistics ethernet g8
```

show gvrp configuration

The **show gvrp configuration** User EXEC command displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.

Syntax

show gvrp configuration [**ethernet** *interface* **|** **port-channel** *port-channel-number*]

- *interface*—A valid Ethernet interface.
- *port-channel-number*—A valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to display GVRP configuration information:

.

```
Console# show gvrp statistics

GVRP statistics:
----------------
Legend:
rJE  : Join Empty Received    rJIn : Join In Received
rEmp : Empty Received         rLIn : Leave In Received
rLE  : Leave Empty Received   rLA  : Leave All Received
sJE  : Join Empty Sent        sJIn : Join In Sent
sEmp : Empty Sent             sLIn : Leave In Sent
sLE  : Leave Empty Sent       sLA  : Leave All Sent

Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE sLA
---- --- ---- ---- ---- --- --- --- --- --- ---- --- ---
g1   0   0    0    0    0   0   0   0   0   0    0   0
g2   0   0    0    0    0   0   0   0   0   0    0   0
g3   0   0    0    0    0   0   0   0   0   0    0   0
g4   0   0    0    0    0   0   0   0   0   0    0   0
g5   0   0    0    0    0   0   0   0   0   0    0   0
g6   0   0    0    0    0   0   0   0   0   0    0   0
g7   0   0    0    0    0   0   0   0   0   0    0   0
g8   0   0    0    0    0   0   0   0   0   0    0   0
```

```
Console# show gvrp configuration

GVRP Feature is currently enabled on the switch.

Maximum VLANs: 256, Maximum VLANs after reset: 256.

Port   GVRP-   Regist- Dynamic Timers    Crea-   Join  Leave Leave-
       Status  ration  VLAN    (milli-   tion               All
                               seconds)

----   ------  ------  ------- --------  -----   ----  ----- -----

g1     Enabled Normal  Enabled 200       600     10000

g2     Enabled Normal  Enabled 200       600     10000
```

show gvrp statistics

The **show gvrp statistics User** EXEC command displays GVRP statistics.

Syntax

show gvrp statistics [**ethernet** *interface* **|** **port-channel** *port-channel-number*]

- *interface*—A valid Ethernet interface.
- *port-channel-number*—A valid trunk index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

show gvrp error-statistics

The **show gvrp error-statistics** user EXEC command displays GVRP error statistics.

Syntax

show gvrp error-statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—Valid Ethernet interface.
- *port-channel-number*—A valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays GVRP statistics information.

```
Console# show gvrp error-statistics
GVRP Error Statistics:
----------------------
Legend:
  INVPROT  : Invalid Protocol Id
  INVATYP  : Invalid Attribute Type  INVALEN : Invalid Attribute Length
  INVAVAL  : Invalid Attribute Value INVEVENT: Invalid Event

  Port   INVPROT INVATYP INVAVAL INVALEN INVEVENT
-------- ------- ------- ------- ------- --------
```

11

IP Addressing Commands

ip address

The **ip address** interface configuration command sets an IP address. To remove an IP address, use the **no** form of this command.

Syntax

ip address *ip-address* {*mask* | *prefix-length*}

no ip address [*ip-address*]

- *ip-address*—IP address
- *mask*—The IP address network mask
- *prefix-length*—The number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0 -32)

Default Configuration

No IP address is defined for interfaces.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel, out-of-band Ethernet)

User Guidelines

Each part of an IP address must start with a number other than zero. For example, IP address 131.108.1.27 is valid, whereas IP addresses 001.100.192.6 and 192.001.10.3 are invalid.

An IP address cannot be configured for a range of interfaces (range context).

Up to 5 IP addresses may be defined on the out-of-band port.

Example

The following example configures VLAN 1 with the IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
Console (config)# interface vlan 1
Console (config-if)# ip address 131.108.1.27 255.255.255.0
```

ip address dhcp

The **ip address dhcp** interface configuration command acquires an IP address on an interface from the Dynamic Host Configuration Protocol (DHCP) server. To deconfigure any acquired address, use the **no** form of this command.

The **no ip address dhcp** command deconfigures any IP address that was acquired, thus sending a DHCPRELEASE message.

Syntax

ip address dhcp [**hostname** *host-name*]

no ip address dhcp

- *host-name*—Specifies the DHCP host name. This name need not be the same as the host name entered in global configuration mode. (Range: 1-159 characters)

Default Configuration

This command has no default configuration.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel, out-of-band Ethernet)

User Guidelines

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol.

Some DHCP servers require that the DHCPDISCOVER message have a specific host name. The most typical usage of the **ip address dhcp hostname** *host-name* command is when *host-name* is the host name provided by the system administrator.

If a router is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If the **ip address dhcp** command is used with or without the optional keyword, the DHCP option 12 field (host name option) is included in the DISCOVER message. By default, the specified DHCP host name is the device globally configured host name.

The **ip address dhcp** command is not supported on a range of interfaces.

The inband ports of the device are router ports. Therefore, when an interface is defined on the inband ports (or VLAN of which they are members), no default-gateway is configured. After dynamic assignment of the IP interface, manually assign a default route.

Example

The following example acquires an IP address on an Ethernet interface from DHCP.

```
Console (config)# interface ethernet g8
Console (config-if)# ip address dhcp
```

ip default-gateway

The **ip default-gateway global configuration** command defines a default gateway (router). To remove the default gateway use the no form of this command.

Syntax

ip default-gateway *ip-address*

no ip default-gateway

- *ip-address* — Valid IP address that specifies the IP address of the default gateway.

Default Configuration

No default gateway is defined.

Command Mode

Interface Configuration (Out-of-Band Ethernet)

User Guidelines

The setting of the default gateway on the out-of-band port must not precede the assignment of the IP address. Always assign the IP address to the out-of-band port first, and then set the default gateway.

Example

The following example defines ip default gateway 192.6.32.17.

```
Console (config)# interface out-of-band-eth 1
Console (config-oob)# ip address 192.168.1.23
Console (config-oob)# ip default-gateway 192.168.1.1
```

show ip interface

The **show ip interface** user EXEC command displays the usability status of interfaces configured for IP.

Syntax

show ip interface [**ethernet** *interface-number* | vlan *vlan-id* | port-channel *number* | **out-of-band-eth** *oob-interface*]]

- **ethernet** *interface-number*—Ethernet port number.
- **vlan** *vlan-id*—VLAN number.
- **port-channel** *number*—Port-channel number.
- **out-of-band-eth** *oob-interface*—Out-of-band Ethernet port number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays VLAN 1 configuration.

```
Console# show ip interface vlan 1
```

arp

The **arp** global configuration command adds a permanent entry in the Address Resolution Protocol (ARP) cache. To remove an entry from the ARP cache, use the **no** form of this command.

Syntax

arp *ip_addr hw_addr* {**ethernet** *interface-number* | *vlan vlan-id* | *port-channel number*}

no arp *ip_addr* {**ethernet** *interface-number* | *vlan vlan-id* | *port-channel number*}

- *ip_addr*—IP address or IP alias to map to the specified MAC address.
- *hw_addr*—MAC address to map to the specified IP address or IP alias.
- **ethernet** *interface-number*—Ethernet port number.
- **vlan** *vlan-id*—VLAN number.
- **port-channel** *number*—Port-channel number.

Default Configuration

By default, ARP is disabled.

Command Mode

Global Configuration mode

User Guidelines

The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses. Because most hosts support dynamic resolution, static ARP cache entries do not need to be specified.

Example

The following example adds the IP address 198.133.219.232 and MAC address 00-00-0c-40-0f-bc to the ARP table.

```
Console (config)# arp 198.133.219.232 0000.0c40.0fbc ethernet g8
```

arp timeout

The **arp timeout** global configuration command configures how long an entry remains in the ARP cache. To restore the default value, use the **no** form of this command.

Syntax

arp timeout *seconds*

no arp timeout *seconds*

- *seconds*—Time (in seconds) that an entry remains in the ARP cache. (Range: 1 - 40000000)

Default Configuration

The default timeout is 60000 seconds.

Command Mode

Global Configuration mode

User Guidelines

It is recommended not to set the timeout value to less than 3600.

NOTE: The ARP entry is deleted between the period of the "timeout value" and twice the "timeout value". For example, if the timeout value is 20 seconds, the ARP value is deleted during the period of 20 to 40 seconds.

Example

The following example configures ARP timeout to 12000 seconds.

```
Console (config)# arp timeout 12000
```

ip proxy-arp

The **ip proxy-arp** global configuration command enables ARP proxy. To disable ARP, use the **no** form of this command.

Syntax

ip proxy-arp

no ip proxy-arp

Default Configuration

By default ARP proxy is disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures authentication login.

```
Console (config)# ip proxy-arp
```

clear arp-cache

The **clear arp-cache** privileged EXEC command deletes all dynamic entries from the ARP cache.

Syntax

clear arp-cache

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example deletes all dynamic entries from the ARP cache.

```
Console# clear arp-cache
```

show arp

The **show arp** privileged EXEC command displays entries in the ARP table.

Syntax

show arp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

To enter an out-of-band IP interface, use the out-of-band IP address format — **oob/ip-address**. Only the **broadcast-address** command is available on out-of-band IP interfaces.

Example

The following example displays entries in the ARP table.

```
Console# show arp
ARP timeout: 60000 Seconds


   Interface      IP address        HW address          status
--------------- --------------- ------------------- -------------
   Oob-eth 1       10.30.2.1     00:00:0c:07:ac:0a      dynamic
   Oob-eth 1       10.30.2.2     00:07:84:a7:ca:bc      dynamic
```

directed-broadcast

The **directed-broadcast** interface configuration command enables the translation of a directed Broadcast to physical Broadcasts. To disable this function, use the **no** form of this command.

Syntax

directed-broadcast

no directed-broadcast

Default Configuration

Disabled, all IP directed broadcasts are dropped.

Command Mode

IP Interface Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables the translation of directed broadcasts to physical broadcasts on IP interface 1.0.0.1.

```
Console(config)# interface ip 1.0.0.1

Console(config-ip)# directed-broadcast
```

broadcast-address

The **broadcast-address** interface configuration command defines an interface Broadcast address. To restore the default IP Broadcast address, use the **no** form of this command.

Syntax

broadcast-address {**255.255.255.255** | **0.0.0.0**}

no broadcast-address

- **255.255.255.255**—Use 255.255.255.255 as the Broadcast address.
- **0.0.0.0**—Use 0.0.0.0 as the Broadcast address.

Default Configuration

The default is 255.255.255.255 as the Broadcast address.

Command Mode

IP Interface Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines an interface Broadcast address as 0.0.0.0 on IP interface 1.0.0.1.

```
Console(config)# interface ip 1.0.0.1

Console(config-ip)# broadcast-address 0.0.0.0
```

ip helper-address

Use the Global Configuration ip helper-address command to have the device forward User Datagram Protocol (UDP) broadcasts received on an interface. To disable the forwarding of broadcast packets to specific addresses, use the no form of this command.

```
ip helper-address ip-interface address [udp-port-list]
```

```
no ip helper-address ip-interface address
```

Syntax Description

ip-interface- Specify IP interface or all.

address- Destination broadcast or host address to be used when forwarding UDP broadcasts. You can specify **0.0.0.0** to indicate not to forward the UDP packet to any host.

udp-port-list - The broadcast packet destination UDP port number to forward. If not specified, packets for the default services are forwarded to the helper address.

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

The **ip helper-address** command forwards specific UDP broadcast from one interface to another. You can define many helper addresses but the total number of address-port pairs is limited to 128 for the whole device.

The setting of helper address for specific interface has precedence over a setting of helper address for all the interfaces.

You can't enable forwarding of BOOTP/DHCP (ports 67,68) with this command. If you want to relay BOOTP/DHCP packets use the DHCP relay commands.

The **ip helper-address** command specifies a UDP port number for which UDP broadcast packets with that destination port number are forwarded. By default, if no UDP port number is specified, the device forwards UDP broadcast packets for the following six services:

- IEN-116 Name Service (port 42)
- DNS (port 53)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS Server (port 49)
- Time Service (port 37)

Example

```
Console(config)#ip helper address 100.10.1.1
```

helper-address

The **helper-address** interface configuration command enables forwarding User Datagram Protocol (UDP) Broadcast packets received on an interface. To disable forwarding Broadcast packets to specific addresses, use the **no** form of this command.

Syntax

helper-address *address* [*udp-port-list*]

no helper-address *address*

- *address*—Destination Broadcast or host address used when forwarding UDP broadcasts.
- *udp-port-list*—The Broadcast packet destination UDP port number to forward. If not specified, packets for the default services are forwarded to the helper address.

Default Configuration

Broadcast packets forwarding to specific addresses is disabled.

If no UDP port number is specified, the device forwards UDP Broadcast packets for the following six services:

- IEN-116 Name Service (port 42)
- DNS (port 53)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS Server (port 49)
- Time Service (port 37)

Command Mode

IP Interface Configuration mode

User Guidelines

Many helper addresses can be defined. The maximum number of address-port pairs is up to 128 for the whole device.

The **helper-address** interface configuration command forwards a specific UDP Broadcast from one interface to another.

The **helper-address** interface configuration command specifies a UDP port number for which UDP Broadcast packets with that destination port number are forwarded.

The **helper-address** interface configuration command does not enable forwarding packets using BOOTP/DHCP. To forward packets using BOOTP/DHCP, use the **ip dhcp relay enable** and **ip dhcp relay address** global configuration commands and the **show ip dhcp relay** privileged EXEC command.

Example

The following example enables the software to forward UDP broadcasts on interface 1.100.100.0 to IP address 172.16.9.9 to ports 49 and 53.

```
Console(config)# interface ip 1.100.100.0

Console (config-ip)# helper-address 172.16.9.9 49 53
```

show ip helper-address

The **show ip helper-address** privileged EXEC command displays IP helper addresses configuration.

Syntax

show ip helper-address [*interface*]

- *interface*—The IP interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays configured IP helper addresses.

```
Console# show ip helper-address

  Interface    Helper Address          Udp port

--------------- --------------- ------------------------

192.168.1.1   172.16.8.8      37, 49, 53, 67, 68, 137, 138

192.168.2.1   172.16.9.9      37, 49
```

ip domain-lookup

The **ip domain-lookup** global configuration command enables IP Domain Naming System (DNS)-based host name-to-address translation. To disable the DNS, use the **no** form of this command.

Syntax

ip domain-lookup

no ip domain-lookup

Default Configuration

The DNS is enabled.

Command Mode

Global Configuraton mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables the IP Domain Naming System (DNS)-based host name-to-address translation:

```
Console(config)# ip domain-lookup
```

ip domain-name

The **ip domain-name** global configuration command defines a default domain name used to complete unqualified host names. An unqualified host name does not include a dotted-decimal domain name. To delete the default domain name, use the **no** form of this command.

Syntax

ip domain-name *name*

no ip domain-name

- *name*—Default domain name used to complete an unqualified host name. Do not include the initial period that separates the unqualified host name from the domain name (Range: 1-158 characters).

Default Configuration

The default domain name is not defined.

Command Mode

Global Configuraton mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines a default domain name of dell.com:

```
Console(config)# ip domain-name dell.com
```

ip name-server

The **ip name-server** global configuration command defines available name servers. To delete a name server, use the **no** form of this command.

Syntax

ip name-server *server-address1* [*server-address2 … server-address8*]

no ip name-server [*server-address1 … server-address8*]

- *server-address*—IP addresses of the name server. For information about specifying an Out-of-Band IP address, see the user guidelines.

Default Configuration

No name server IP addresses are specified.

Command Mode

Global Configuraton mode

User Guidelines

Server preference is determined by entry order.

Up to 8 servers can be defined in one command or by using multiple commands.

To define a radius server on the out-of-band port, use the out-of-band IP address format: **oob**/ip-address.

Example

The following example sets the available name server:

```
Console(config)# ip name-server 176.16.1.18
```

ip host

The **ip host** global configuration command defines static host name-to-address mapping in the host cache. To delete the name-to-address mapping, use the **no** form of this command.

Syntax

ip host *name address*

no ip host *name*

- *name*—Host name (Range: 1-158 characters).
- *address*—IP address of the host. For information about specifying an out-of-band IP address, see the user guidelines.

Default Configuration

No host is defined.

Command Mode

Global Configuraton mode

User Guidelines

To define an Out-of-Band IP address, use the following format: **oob**/ip-address.

Example

The following example defines a static host name-to-address mapping in the host cache:

```
Console(config)# ip host accounting.dell.com 176.10.23.1
```

clear host

The **clear host** privileged EXEC command deletes entries from the host name-to-address cache.

Syntax

clear host {*name address* | *}

- *name*—Host name to be deleted from the host name-to-address cache (Range: 1-158 characters).
- *—Deletes all entries in the host name-to-address cache.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example deletes all entries from the host name-to-address cache:

```
Console# clear host *
```

clear host dhcp

The **clear host dhcp** privileged EXEC command deletes entries from the DHCP host name-to-address mapping cache.

Syntax

clear host dhcp {*name address* |*}

- *name*—Host name to be deleted from the DHCP host name-to-address mapping cache (Range: 1-158 characters).
- *—Deletes all entries in the DHCP host name-to-address mapping cache.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example deletes all entries from the DHCP host name-to-address mapping cache.

```
Console# clear host dhcp *
```

show hosts

The **show hosts** user EXEC command displays the default domain name, a list of name server hosts and the static and cached list of host names and addresses.

Syntax

show hosts [*name*]

- *name*—Host name (Range: 1-158 characters).

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information about IP hosts.

```
Console> show hosts

Host name: Device
Default domain: gm.com, sales.gm.COM, usa.sales.gm.com(DHCP)
Name/address lookup is enabled
Name servers (Preference order): 176.16.1.18 176.16.1.19

Configured host name-to-address mapping:
Host                         Addresses
--------------------------   ----------------------------
accounting.gm.com            176.16.8.8
                             176.16.8.9(DHCP)

Cache:            TTL
                  (Hours)
Host              Total      Elapsed   Type      Addresses
                  -----      -------   ----      -----------
www.stanford.edu  72         3         IP        171.64.14.203
```

12

IGMP Snooping Commands

ip igmp snooping (Global)

The **ip igmp snooping** global configuration command enables Internet Group Management Protocol (IGMP) snooping. To disable IGMP snooping use the **no** form of this command.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

IGMP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables IGMP snooping.

```
Console (config)# ip igmp snooping
```

ip igmp snooping (Interface)

The **ip igmp snooping** interface configuration command enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN. To disable IGMP snooping on a VLAN interface, use the **no** form of this command.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

IGMP snooping is disabled on all VLANs in the set context.

Command Mode

Interface configuration (VLAN) mode

User Guidelines

IGMP snooping can only be enabled on static VLANs.

Example

The following example enables IGMP snooping on VLAN 2.

```
Console (config)# interface vlan 2
Console (config-if)# ip igmp snooping
```

ip igmp snooping mrouter

The **ip igmp snooping mrouter** interface configuration command enables automatic learning of Multicast router ports in the context of a specific VLAN. To remove automatic learning of Multicast router ports, use the **no** form of this command.

Syntax

ip igmp snooping mrouter learn-pim-dvmrp

no ip igmp snooping mrouter learn-pim-dvmrp

Default Configuration

Automatic learning of mrouter ports is enabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Multicast router ports can be configured statically by the **bridge multicast forward-all** command.

Example

The following example enables automatic learning of Multicast router ports on VLANs.

```
Console (config) # interface vlan 2
Console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp
```

ip igmp snooping host-time-out

The **ip igmp snooping host-time-out** interface configuration command configures the host-time-out. If an IGMP report for a Multicast group was not received for a host-time-out period, from a specific port, this port is deleted from the member list of that Multicast group. To reset to default host-time-out use the **no** form of this command.

Syntax

ip igmp snooping host-time-out *time-out*

no ip igmp snooping host-time-out

- *time-out*—Host timeout in seconds. (Range: 1 - 2147483647)

Default Configuration

The default host-time-out is 260 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The timeout should be at least greater than 2*query_interval+max_response_time of the IGMP router.

Example

The following example configures the host timeout to 300 seconds.

```
Console (config)# interface vlan 2
Console (config-if)# ip igmp snooping host-time-out 300
```

ip igmp snooping mrouter-time-out

The **ip igmp snooping mrouter-time-out** interface configuration command configures the mrouter-time-out. The **mrouter-time-out** command is used for setting the aging-out time after Multicast router ports are automatically learned. To configure the default mrouter-time-out, use the **no** form of this command.

Syntax

ip igmp snooping mrouter-time-out *time-out*

no ip igmp snooping mrouter-time-out

- *time-out*—mrouter timeout in seconds (Range: 1 - 2147483647)

Default Configuration

The default value is 300 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the mrouter timeout to 200 seconds.

```
Console (config)# interface vlan 2
Console (config-if)# ip igmp snooping mrouter-time-out 200
```

ip igmp snooping leave-time-out

The **ip igmp snooping leave-time-out** command configures the leave-time-out. If an IGMP report for a Multicast group is not received within the leave-time-out period after an IGMP leave was received from a specific port, the current port is deleted from the member list of that Multicast group. To configure the default leave-time-out, use the **no** form of this command.

Syntax

ip igmp snooping leave-time-out {*time-out* | *immediate-leave*}

no ip igmp snooping leave-time-out

- *time-out*—leave-time-out in seconds. (Range: 0 - 2147483647)
- *immediate-leave*—Specifies that the port should be immediately removed from the members list after receiving IGMP Leave.

Default Configuration

The default leave-time-out configuration is 10 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The leave timeout should be set greater than the maximum time that a host is allowed to respond to an IGMP Query.

Use **immediate leave** only where there is only one host connected to a port.

The following example configures the host leave-time-out to 60 seconds.

```
Console (config)# interface vlan 2
Console (config-if)# ip igmp snooping leave-time-out 60
```

show ip igmp snooping mrouter

The **show ip igmp snooping mrouter** User EXEC command displays information on dynamically learned Multicast router interfaces.

Syntax

show ip igmp snooping mrouter [**interface** *vlan-id*]

- *vlan_id*—VLAN ID value.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows IGMP snooping mrouter information.

```
Console # show igmp snooping mrouter

VLAN      Ports

-------   -----------------------------------------

2         9
```

show ip igmp snooping interface

The **show ip igmp snooping interface** User EXEC command displays IGMP snooping configuration.

Syntax

show ip igmp snooping interface *vlan-id*

- *vlan_id*—VLAN ID value.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The example displays IGMP snooping information.

```
Console # show ip igmp snooping interface 1
IGMP Snooping is globaly disabled
IGMP Snooping is disabled on VLAN 1
IGMP host timeout is 260 sec
IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec
IGMP mrouter timeout is 300 sec
Automatic learning of multicast router ports is enabled
```

show ip igmp snooping groups

The **show ip igmp snooping groups** user EXEC command displays the Multicast groups learned by IGMP snooping.

Syntax

show ip igmp snooping groups [**vlan** *vlan-id*] [**address** *ip-multicast-address*]

- *vlan_id*—VLAN ID value.
- *ip-multicast-address*—IP Multicast address.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

To see the full Multicast address table (including static addresses) use the **show bridge address-table** command.

Example

The example shows IGMP snooping information on VLAN 1000.

```
Console # show ip igmp snooping groups

Vlan IP Address Querier Ports

---- ------------------ ------- -------------------

1 224-239.130|2.2.3 Yes g1, g2

19 224-239.130|2.2.8 Yes g9-11
```

13

IP Routing Protocol-Independent Commands

interface ip

The **interface ip** global configuration command enters the IP interface configuration mode.

Syntax

interface ip *ip-address*

- *ip-address*—One of the device IP addresses.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures an IP interface and enters the IP interface configuration mode.

```
Console (config)# interface ip 192.168.1.1
Console (config-ip)#
```

ip route

The **ip route** global configuration command establishes static IP routes. To remove static IP routes, use the **no** form of this command.

Syntax

ip route *prefix* {*mask* | *prefix-length*} *gateway* [**metric** *distance*] [**reject-route**]

no ip route *prefix mask* [*gateway*]

- *prefix*—The destination IP route prefix.
- *mask*—The IP address network mask.
- *prefix-length*—The number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0 - 32)
- *gateway*—IP address or IP alias of the next hop that can be used to reach that network.
- **metric** *distance*—An administrative distance .(Range: 1 - 255)

- **reject-route**—Discard all packets matching this route per RFC-2096, and handle them as reject-route. These routes are treated as unreachable networks, and an **ICMP unreachable route** is returned.

Default Configuration

The metric default distance is 1.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example establishes a static route to 172.16.0.0.

```
Console (config)# ip route 172.16.0.0 255.255.0.0  131.16.1.1
```

key-chain

The **key-chain** global configuration command defines authentication key group for routing protocols. To remove the key chain, use the **no** form of this command.

Syntax

key-chain *name-of-chain*

no key-chain *name-of-chain*

- *name-of-chain*—Key chain name.

Default Configuration

No key chain exists.

Command Mode

Global Configuration mode

User Guidelines

To use, an authentication key chain with keys must be configured.

The setting is effective only after reset.

RIP may use only up to two parallel paths.

After specifying the **key-chain** command, the key chain configuration mode is opened.

Example

The following example identifies an authentication keygroup called "M".

```
Console (config)# key-chain M
```

key (key chain)

The **key** key chain configuration command defines an authentication key on a key chain. To remove the key from the key chain, use the **no** form of this command.

Syntax

key *key-id*

no key *key-id*

- *key-id*—An authentication key identification number on a key chain. (Range: 1 - 255)

Default Configuration

No key exists on the key chain.

Command Mode

Key chain configuration mode

User Guidelines

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the **accept-lifetime** and **send-lifetime** key chain key command settings.

Authentication keys and their key strings, which are to be included in the key chain should be defined prior to configuring the key chain. Authentication keys are defined by the **key (global) command**

If the last key expires, authentication stops and an error message is generated.

Example

The following example identifies two authentication keys, number 1 and 2, on a key chain keygroup called "M".

```
Console (config)# key-chain M
Console (config-keychain)# key 1
Console (config-keychain)# key 2
```

key (global)

The **key** global configuration command creates an authentication key. To remove the key, use the **no** form of this command.

Syntax

key *key-id*

no key *key-id*

- *key-id*—An authentication key identification number on a key chain. (Range: 1 - 255)

Default Configuration

No key exists on the key chain.

Command Mode

Global configuration mode

User Guidelines

After entering the key command, the console automatically enters the key chain configuration mode.

Example

The following example creates an authentication key number 3.

```
Console (config)# key 3

Console (config-key)#
```

key-string

The **key-string** SSH public key chain configuration command manually specifies an SSH public key.

Syntax

key-string

key-string row *key-string*

- **row**—Specifies SSH public key row by row.
- *key-string*—UU-encoded DER format is the same format in the **authorized_keys** file used by OpenSSH. Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain from 1 to 16 lowercase alphanumeric characters.

Default Configuration

No key exists.

Command Mode

SSH public key configuration

User Guidelines

Use the **key-string** command to specify which SSH public key to interactively configure next. To complete the interactive command, enter row with no characters.

Use the key-string row command to specify SSH public key row by row. Each row must begin with key-string row command. This command is useful for configuration files.

UU-encoded DER format is the same format in authorized_keys file used by OpenSSH.

Example

The following example automatically specifies an authentication string.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

The following example automatically specifies SSH public row keys "AAAAB3Nza" and "C1yc2".

```
Console(config)# crypto key pubkey-chain ssh

Console(config-pubkey-chain)# user-key bob rsa

Console(config-pubkey-key)# key-string row AAAAB3Nza

Console(config-pubkey-key)# key-string row C1yc2
```

accept-lifetime

The **accept-lifetime** key chain key configuration command sets the time period during which the authentication key is valid for authenticating incoming packets. To reset to the default value, use the **no** form of this command.

Syntax

accept-lifetime infinite *start-time*

accept-lifetime duration *start-time seconds*

accept-lifetime *start-time end-time*

no accept-lifetime [**duration** | **infinite**]

- *start-time*—Beginning time that the key specified by the **key** command is valid to be received. The syntax can be either of the following: *hh:mm:ss month date year* or *hh:mm:ss date month year.*
  - - *hh:mm:ss*—Time in hours, minutes, and seconds (Range: hh 0 - 23:mm 0 - 59: ss 0 - 59)
  - - *day*—Day (by date) in the month (Range: 1 - 31)
  - - *month*—Month (first three letters by name) (Range: Jan, ..., Dec)
  - - *year*—Year (no abbreviation) (Range: 1998 - 2097)
- **infinite**—Key is valid to be received from the *start-time* value with no limit.
- *end-time*—Key is valid from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value.
- *seconds*—Length of time (in seconds) that the key is valid. (Range: 1 - 4294967295)

Default Configuration

There is no time limit, the key is always valid to be received.

Command Mode

Key configuration

User Guidelines

If the last key expires, authentication stops and an error message is generated.

Example

The following example specifies for key 1, an accept-lifetime range from 13:30:00 Jan 25 2005 for 7200 seconds, and for key 2 an accept-lifetime range from 14:30:00 Jan 25 2005 for 7200 seconds.

```
Console (config)# key 1

Console (config-key)# key-string mountain

Console (config-key)# accept-lifetime duration 13:30:00
Jan 25 2005  7200

Console (config)# key 2

Console (config-key)# key-string country

Console (config-key)# accept-lifetime duration 14:30:00
Jan 25 2005  7200
```

send-lifetime

The **send-lifetime** key chain key configuration command sets the time period during which an authentication key is valid to generate MD5 digest for outgoing packets. To revert to the default value, use the **no** form of this command.

Syntax

send-lifetime infinite *start-time*

send-lifetime duration *start-time seconds*

send-lifetime *start-time end-time*

no send-lifetime [duration | infinite]

- *start-time*—Beginning time that the key specified by the **key** command is valid to be sent. The syntax can be either of the following: *hh:mm:ss Month date year* or *hh:mm:ss date Month year.*

  - *hh:mm:ss*—Time in hours, minutes, and seconds (Range: hh 0 - 23:mm 0 - 59: ss 0 - 59)

  - *day*—Day (by date) in the month (Range: 1 - 31)

  - *month*—Month (first three letters by name) (Range: Jan, ...Dec)

  - *year*—Year (no abbreviation) (Range: 1998 - 2097)

- **infinite**—Key is valid to be sent from the *start-time* value with no limit.
- *end-time*—Key is valid to be sent from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value.

- *seconds*—Length of time (in seconds) that the key is valid to be sent. (Range: 1 - 4294967295)

Default Configuration

There is no time limit, the key is always valid to be sent.

Command Mode

Key configuration

User Guidelines

If the last key expires, authentication stops and an error message is generated.

Example

The following example specifies for key 1, a send-lifetime range from 14:00:00 Jan 25 2005 for 3600 seconds, and for key 2 a send-lifetime range from 15:00:00 Jan 25 2005 for 3600 seconds.

```
Console (config)# key 1

Console (config-key)# key-string mountain

Console (config-key)# send-lifetime 14:00:00 Jan 25 2005  duration
3600

Console (config-key)# exit

Console (config)# key 2

Console (config-key)# key-string country

Console (config-key)# send-lifetime 15:00:00 Jan 25 2005  duration
3600
```

ip maximum-paths

The **ip maximum-paths** global configuration command defines the maximum number of parallel routes. To restore the default number of parallel routes, use the **no** form of this command.

Syntax

ip maximum-paths *number-paths*

no ip maximum-paths

- *number-paths*—Maximum number of parallel routes installed in a routing table. (Range: 1 - 4)

Default Configuration

The default number of parallel routes is 4.

Command Mode

Global Configuration mode

User Guidelines

The change to IP maximum-paths takes effect after resetting the device.

Example

The following example defines the maximum number of parallel routes to 2.

```
Console (config)# ip maximum-paths 2
```

show ip route

The **show ip route** user EXEC command displays the routing table current state.

Syntax

show ip route [*protocol*]

show ip route address *address* [*mask* **|** *prefix-length*] [**longer-prefixes**]

- *protocol*—A routing protocol, or the keyword **connected**, **static**. If specifying a routing protocol, use one of the following keywords: **ospf**, **rip**.
- *address*—Address about which routing information should be displayed.
- *mask*—The IP address network mask.
- *prefix-length*—The number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0 - 32)
- **longer-prefixes**—The *address* and *mask* pair becomes a prefix and any routes that match that prefix are displayed.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the whole routing table state.

```
Console> show ip route

Maximum Parallel Paths: 2 (4 after reset)

Codes: C - connected, S - static, R - RIP, O - OSPF, E - OSPF
external

R 10.0.0.0/8 is rejected

C 10.0.1.1/32 is directly connected, Loopback0

C 10.0.1.0/24 is directly connected, Ethernet g1

C 10.0.2.0/24 is directly connected, Ethernet g2

R 10.8.2.0/24 [230/50] via 10.0.2.2, 00:17:19, Ethernet g2

S 10.9.1.0/24 [5/2] via 10.0.1.2, 17:19:18, Ethernet g1

S 10.9.1.0/24 [5/3] via 10.0.2.2, Backup Not Active

O 10.8.1.0/24 [30/2000] via 10.0.1.2, 00:39:08, Ethernet g1

S 172.1.0.0/16 [5/3] via 10.0.1.1, 18:21:58, Ethernet g1

S 172.1.1.0/24 [5/3] via 10.0.2.1, 17:12:19, Ethernet g1

S 172.1.1.1/32 [5/3] via 10.0.3.1, 19:51:18, Ethernet g1
```

The following example displays the routing table for IP address 192.168.1.0 with the address mask 255.255.255.0.

```
Console> show ip route address 192.168.1.0 255.255.255.0

Codes: C - connected, S - static, R - RIP, O - OSPF,
E - OSPF external

S 192.168.1.0/24 [5/3] via 10.0.2.1, 17:12:19, Ethernet g1
```

The following example displays the routing table for IP address 192.168.1.0 with the address mask 255.255.255.0 and matching the prefix created from the IP address and address mask.

```
Console> show ip route address 192.168.1.0 255.255.255.0 longer-
prefixes

Codes: C - connected, S - static, R - RIP, O - OSPF,
E - OSPF external

S 192.168.1.0/24 [5/3] via 10.0.2.1, 17:12:19, Ethernet g1

S 192.168.1.1/32 [5/3] via 10.0.3.1, 19:51:18, Ethernet g1
```

The following table describes the significant fields shown in the display:

Field	Description
O	Indicates protocol that derived the route.
10.8.1.0/24	Indicates the remote network address.
[30/2000]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.0.1.2	Specifies the address of the next router to the remote network.
00:39:08	Specifies the last time the route was updated, in hours:minutes:seconds.
Ethernet 1	Specifies the interface through which the specified network can be reached.

show ip protocols

The **show ip protocols** privileged EXEC command displays the parameters and current state of the active routing protocols.

Syntax

show ip protocols

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the parameters and current state of the active routing protocol process.

```
Console# show ip protocols

Routing Protocol is "rip"
Sending updates every 30 seconds
Invalid after 180 seconds, hold down 120, flushed after 300
Redistributing: RIP, Static, OSPF
Default version control: send version 1, receive version 1
Interfaces:
Interface Send Receive Key-chain
176.1.1.1 1 1 flowers
176.2.1.1 passive 2
Routing Information Sources:
Gateway Last Update
176.1.1.2 0:00:17
Preference: 60
Routing Protocol is "ospf"
Redistributing: OSPF, External direct, Static, RIP
Interfaces:
Interface Metric Key-chain
176.1.1.1 10 flowers
176.2.1.1 1
Routing Information Sources:
Gateway State
176.1.1.2 Full
External Preference: 60
Internal Preference: 20
```

show key-chains

The **show key-chains** privileged EXEC command displays key-chain information.

Syntax

show key-chains [*name-of-chain*]

- *name-of-chain*—Name of a key chain.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays key-chain information.

```
Console# show key-chains
key chain internal
key 1
accept:   13:30:00 Jan 25 2005  duration 7200
send:     14:00:00 Jan 25 2005  duration 3600
key 2
accept:   14:30:00 Jan 25 2005  duration 7200
send:     15:00:00 Jan 25 2005  duration 3600
key chain external
key 1
accept:   13:30:00 Jan 25 2005  until 15:30:00 Jan 25 2005
send:     14:00:00 Jan 25 2005  until 15:00:00 Jan 25 2005
key 2
accept:  14:30:00 Jan 25 2005  until 16:30:00 Jan 25 2005
send:    15:00:00 Jan 25 2005  until 16:00:00 Jan 25 2005
```

show keys

The **show keys** privileged EXEC command displays key information.

Syntax

show keys [*key-id*]

- *key-id*—Identification number of an authentication key on a key chain. (Range: 1 - 255)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays key-chain information.

```
Router# show keys
key 1
accept: 13:30:00 Jan 25 2005  forever
send: 13:30:00 Jan 25 2005  forever
key 2
accept: 13:30:00 Jan 25 2005  until 15:30:00 Jan 25 2005
send: 14:00:00 Jan 25 2005  until 15:00:00 Jan 25 2005
key 3
accept: 14:30:00 Jan 25 2005  until 16:30:00 Jan 25 2005
send: 15:00:00 Jan 25 2005  until 16:00:00 Jan 25 2005
```

14

LACP Commands

lacp system-priority

The **lacp system-priority** global configuration command configures the system priority. To reset to default, use the **no** form of this command.

Syntax

lacp system-priority *value*

no lacp system-priority

- *value*—Value of the priority. (Range: 1 - 65535)

Default Configuration

The default system priority value is 1.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the system priority to 120.

```
Console (config)# lacp system-priority 120
```

lacp port-priority

The **lacp port-priority** interface configuration command configures the priority value for physical ports. To reset to default priority value, use the **no** form of this command.

Syntax

lacp port-priority *value*

no lacp port-priority

- *value*—Port priority value. (Range: 1 - 65535)

Default Configuration

The default port priority value is 1.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the priority value for port g8 to 247.

```
Console (config)# interface ethernet g8

Console (config-if)# lacp port-priority 247
```

lacp timeout

The **lacp timeout** interface configuration command assigns an administrative LACP timeout. To reset the default administrative LACP timeout use the **no** form of this command.

Syntax

lacp timeout {**long** | **short**}

no lacp timeout

- **long**—Specifies a long timeout value.
- **short**—Specifies a short timeout value.

Default Configuration

The default port timeout value is **long**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example assigns an administrative LACP timeout for port g8 to a long timeout value.

```
Console (config)# interface ethernet g8

Console (config-if)# lacp timeout long
```

show lacp ethernet

The **show lacp ethernet** privileged EXEC command displays LACP information for Ethernet ports.

Syntax

show lacp ethernet *interface* [**parameters** | **statistics** | **protocol-state**]

- *Interface*—Ethernet interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to display LACP statistics information.

```
Console# show lacp ethernet g1 statistics

Port 1 LACP Statistics:

LACP PDUs sent:2


LACP PDUs received:2
```

show lacp port-channel

The **show lacp port-channel** privileged EXEC command displays LACP information for a port-channel.

Syntax

show lacp port-channel [*port_channel_number*]

- *port_channel_number*—The port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to display LACP port-channel information.

```
Console# show lacp port-channel 1
Port-Channel ch1
       Port Type Unknown
       Attached Lag id:
       Actor
               System Priority:1
               MAC Address:    0a:d0:0f:f0:eb:ee
               Admin Key:      25
               Oper Key:       25
       Partner
               System Priority:0
               MAC Address:    00:00:00:00:00:00
               Oper Key:       0
```

15

Line Commands

line

The **line** global configuration command identifies a specific line for configuration and enters the line configuration command mode.

Syntax

line {**console** | **telnet** | **ssh**}

- **console**—Console terminal line.
- **telnet**—Virtual terminal for remote console access (Telnet).
- **ssh**—Virtual terminal for secured remote console access (SSH).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example configures the device as a virtual terminal for remote console access.

```
Console(config)# line telnet
Console(config-line)#
```

speed

The **speed** line configuration command sets the line baud rate.

Syntax

speed {*bps*}

- *bps*—Baud rate in bits per second (bps). The options are 2400, 9600, 19200 and 115200.

Default Configuration

This default speed is 115200.

Command Mode

Line Configuration (console) mode

User Guidelines

This command is available only on the console line.

Although not saved to the configuration file, the line baud rate setting is permanently saved until it is explicitly modified.

Examples

The following example configures the line baud rate to 115200.

```
Console (config)# line console

Console(config-line)# speed 115200
```

exec-timeout

The **exec-timeout** line configuration command sets the interval that the system waits until user input is detected. To restore the default setting, use the **no** form of this command.

Syntax

exec-timeout *minutes* [*seconds*]

no exec-timeout

- *minutes*—Integer that specifies the number of minutes. (Range: 0 - 65535)
- *seconds*—Additional time intervals in seconds. (Range: 0 - 59)

Default Configuration

The default configuration is 10 minutes.

Command Mode

Line Configuration mode

User Guidelines

To specify no timeout, enter the **exec-timeout 0** command.

Examples

The following example configures the interval that the system waits until user input is detected to 20 minutes.

```
Console (config)# line console

Console(config-line)# exec-timeout 20
```

show line

The **show line** user EXEC command displays line parameters.

Syntax

show line [**console** | **telnet** | **ssh**]

- **console**—Console terminal line.
- **telnet**—Virtual terminal for remote console access (Telnet).
- **ssh**—Virtual terminal for secured remote console access (SSH).

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the line configuration.

```
Console# show line

Console configuration:
Interactive timeout: 20
History: 10
Baudrate: 9600
Databits: 8
Parity: none
Stopbits: 1


Telnet configuration:
Interactive timeout: 10 minutes 10 seconds
History: 10


SSH configuration:
Interactive timeout: 10 minutes 10 seconds
History: 10
```

terminal history

The **terminal history** user EXEC command enables the command history function for the current terminal session. To disable the command history function, use the **no** form of this command..

Syntax

terminal history

no terminal history

Default Configuration

The default configuration for all terminal sessions is defined by the **history** line configuration command.

Command Mode

User EXEC mode

User Guidelines

The maximum number of commands for all terminal sessions is 256 and for a single terminal session 216. If the maximum of 216 commands is issued in one session, the other sessions operate with a maximum default setting of 10 commands each.

Examples

The following example disables the command history function for the current terminal session.

```
Console# no terminal history
```

terminal history size

The **terminal history size** user EXEC command configures the command history buffer size for the current terminal session. To reset the command history buffer size to the default setting, use the **no** form of this command..

Syntax

terminal history size *number-of-commands*

no terminal history size

- *number-of-commands*—Specifies the number of commands the system may record in its command history buffer. (Range: 10-216)

Default Configuration

The default command history buffer size is 10.

Command Mode

User EXEC mode

User Guidelines

The **terminal history size** user EXEC command configures the size of the command history buffer for the current terminal session. To change the default size of the command history buffer, use the **history size** line configuration command.

The maximum number of commands in all buffers is 256.

Examples

The following example configures the command history buffer size to 20 commands for the current terminal session.

```
Console # terminal history size 20
```

16

Management ACL

management access-list

The **management access-list** configuration command defines an access-list for management, and enters the access-list for configuration. Once in the access-list configuration mode, the denied or permitted access conditions are configured with the **deny** and **permit** commands. To remove an access list, use the **no** form of this command.

Syntax

management access-list *name*

no management access-list *name*

- *name*—The access list name using up to 32 characters.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command enters the access-list configuration mode, where the denied or permitted access conditions with the **deny** and **permit** commands must be defined.

If no match criteria are defined the default is "deny".

If reentering to an access-list context, the new rules are entered at the end of the access-list.

Use the m**anagement access-class** command to select the active access-list.

The active management list cannot be updated or removed.

Examples

The following example shows how to create an access-list called "mlist", configure two management interfaces ethernet g1 and ethernet g9, and make the access-list the active list.

```
Console (config)# management access-list mlist

Console (config-macl)# permit ethernet g1

Console (config-macl)# permit ethernet g9

Console (config-macl)# exit

Console (config)# management access-class mlist
```

The following example shows how to create an access-list called "mlist", configure all interfaces to be management interfaces except interfaces ethernet g1 and ethernet g9, and make the access-list the active list.

```
Console (config)# management access-list mlist
Console (config-macl)# deny ethernet g1
Console (config-macl)# deny ethernet g9
Console (config-macl)# permit
Console (config-macl)# exit
Console (config)# management access-class mlist
```

permit (management)

The **permit** management access-list configuration command defines a permit rule.

Syntax

permit [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number* | **out-of-band-eth** *oob-interface*] [**service** *service*]

permit ip-source *ip-address* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number* | **out-of-band-eth** *oob-interface*] [**service** *service*]

- **ethernet** *interface-number*—A valid Ethernet port number.
- **vlan** *vlan-id*—A valid VLAN number.
- **port-channel** *number*—A valid port channel number.
- *ip-address*—Source IP address.
- **mask** *mask*—Specifies the network mask of the source IP address.
- **mask** *prefix-length*—Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/).
- **service** *service*—Indicates service type. Can be one of the following: **telnet**, **ssh**, **http, https** or **snmp**.
- **out-of-band-eth** *oob-interface*—Out-of-band Ethernet port number.

Default Configuration

This command has no default configuration.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with Ethernet, VLAN and port-channel parameters are valid only if an IP address is defined on the appropriate interface.The system supports up to 256 management access rules.

Example

The following example shows how all ports are permitted in the access-list called "mlist".

```
Console (config)# management access-list mlist

Console (config-macl)# permit
```

deny (management)

The **deny** management access-list configuration command defines a deny rule.

Syntax

deny [**ethernet** *interface-number* **|** **vlan** *vlan-id* **|** **port-channel** *number* **|** **out-of-band-eth** *oob-interface*] [**service** *service*]

deny ip-source *ip-address* [**mask** *mask* **|** *prefix-length*] [**ethernet** *interface-number* **|** **vlan** *vlan-id* **|** **port-channel** *number* **|** **out-of-band-eth** *oob-interface*] [**service** *service*]

- **ethernet** *interface-number*—A valid Ethernet port number.
- **vlan** *vlan-id*—A valid VLAN number.
- **port-channel** *number*—A valid port-channel number.
- *ip-address*—Source IP address.
- **mask** *mask*—Specifies the network mask of the source IP address.
- **mask** *prefix-length*—Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/).
- **service** *service*—Indicates service type. Can be one of the following: **telnet**, **ssh**, **http, https** or **snmp**.
- **out-of-band-eth** *oob-interface*—Out-of-band Ethernet port number.

Default Configuration

This command has no default configuration.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with Ethernet, VLAN and port-channel parameters are valid only if an IP address is defined on the appropriate interface.The system supports up to 256 management access rules.

Example

The following example shows how all ports are denied in the access-list called "mlist".

```
Console (config)# management access-list mlist
Console (config-macl)# deny
```

management access-class

The **management access-class** global configuration command defines which management access-list is used. To disable restriction, use the **no** form of this command.

Syntax

management access-class {**console-only** | *name*}

no management access-class

- *name*—A valid access-list name.
- **console-only**—The device can be managed only from the console.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures an access-list called "mlist" as the management access-list.

```
Console (config)# management access-class mlist
```

show management access-list

The **show management access-list** privileged EXEC command displays management access-lists.

Syntax

show management access-list [*name*]

- *name*—A valid access list name.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the active management access-list.

```
Console# show management access-list

mlist

-----

permit ethernet g1

permit ethernet g9

! (Note: all other access implicitly denied)
```

show management access-class

The **show management access-class** privileged EXEC command displays the active management access-list.

Syntax

show management access-class

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the management access-list information.

```
Console# show management access-class

Management access-class is enabled, using access list mlist
```

17

Multicast Routing Commands

ip multicast-routing

The **ip multicast-routing** command in global configuration mode enables IP Multicast routing and DVMRP. To disable IP Multicast routing, use the **no** form of this command.

Syntax

ip multicast-routing [**dvmrp**]

no ip multicast-routing [**dvmrp**]

Default Configuration

IP Multicast routing is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables IP Multicast routing and DVMRP on a system-wide basis.

DVMRP is the only form of Multicast routing supported by the device and is enabled whether or not DVMRP is specified in the command.

Example

The following example enables IP Multicast routing.

```
Console (config)# ip multicast-routing
```

ip dvmrp

The **ip dvmrp** interface configuration mode enables DVMRP on an interface. To disable DVMRP, use the **no** form of this command.

Syntax

ip dvmrp

no ip dvmrp

Default Configuration

DVMRP is disabled.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

If DVMRP is disabled on an interface, the DVMRP parameters on the interface return to the default values.

Example

The following example enables DVMRP on port g5.

```
Console (config)# interface ethernet g5
Console (config-if)# ip dvmrp
```

ip dvmrp metric

The **ip dvmrp metric** interface configuration mode configures the interface metric for Distance Vector Multicast Routing Protocol (DVMRP) reports. To return to the default, use the **no** form of this command.

Syntax

ip dvmrp metric *metric*

no ip dvmrp metric

- *metric*—Metric for DVMRP reports. (Range: 1 - 31)

Default Configuration

The default metric value is 1.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

If DVMRP is disabled on an interface, the DVMRP parameters on the interface return to default. This command is available only when DVMRP is enabled.

Example

The following example configures the interface metric for DVMRP on port g5 to 15.

```
Console (config)# interface ethernet g5
Console (config-if)# ip dvmrp metric 15
```

ip igmp

The **ip igmp** interface configuration command enables IGMP on an interface. To disable IGMP on an interface, use the **no** form of this command.

Syntax

ip igmp

no ip igmp

Default Configuration

IGMP is by default disabled on interfaces.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

If IGMP is disabled on an interface, the IGMP parameters on the interface return to the default values.

Example

The following example enables IGMP on port g5.

```
Console (config)# interface ethernet g5
Console (config-if)# ip igmp
```

ip igmp query-interval

The **ip igmp query-interval** interface configuration command configures the frequency at which the software sends Internet Group Management Protocol (IGMP) host query messages. To return to the default frequency, use the **no** form of this command.

Syntax

ip igmp query-interval *seconds*

no ip igmp query-interval

- *seconds*—Frequency, in seconds, at which to send IGMP host query messages. (Range: 1 - 65535)

Default Configuration

The default is 125 seconds.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

IGMP must be enabled before setting IGMP parameters.

If IGMP is disabled on an interface, the IGMP parameters on the interface return to the default values.

Example

The following example configures the frequency at which the software sends IGMP host query messages on port g5 to 600 seconds.

```
Console (config)# interface ethernet g5
Console (config-if)# ip igmp query-interval 600
```

ip igmp last-member-query-interval

The **ip igmp last-member-query-interval** interface configuration command configures the frequency at which the software sends Internet Group Management Protocol (IGMP) group-specific host query messages. To set this frequency to the default value, use the **no** form of this command.

Syntax

ip igmp last-member-query-interval *seconds* [*tenths-of-seconds*]

no ip igmp last-member-query-interval

- *seconds*—Frequency, in seconds, at which IGMP group-specific host query messages are sent. (Range: 0 - 25)
- *tenths-of-seconds*—Additional tenths of seconds to add to the defined seconds. (Range: 0 - 9)

Default Configuration

The default frequency is 1 second.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

IGMP must be enabled before setting the frequency.

If IGMP is disabled on an interface, the IGMP parameters on the interface return to the default values.

Example

The following example configures the frequency at which the software sends IGMP group-specific query messages on port g5 to 20 seconds.

```
Console (config)# interface ethernet g5
Console (config-if)# ip igmp last-member-query-interval 20
```

ip igmp query-max-response-time

The **ip igmp query-max-response-time** interface configuration command configures the maximum response time advertised in Internet Group Management Protocol (IGMP) queries. To restore the default response time, use the **no** form of this command.

Default Configuration

The default frequency is 10 seconds.

Syntax

ip igmp query-max-response-time *seconds* [*tenths-of-seconds*]

no ip igmp query-max-response-time

- *seconds*—The maximum response time, in seconds, advertised in Internet Group Management Protocol (IGMP) queries. (Range: 0 - 25)
- *tenths-of-seconds*—Additional tenths of seconds to add to the defined seconds. (Range: 0 - 9)

Default Configuration

This command has no default configuration.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

IGMP must be enabled before setting the response time.

If IGMP is disabled on an interface, the IGMP parameters on the interface return to the default values.

Example

The following example configures the maximum response time advertised in IGMP queries on port g5 to 20 seconds.

```
Console (config)# interface ethernet g5
Console (config-if)# ip igmp query-max-response-time 20
```

ip igmp version

The **ip igmp version** global configuration command configures which version of Internet Group Management Protocol (IGMP) the router uses. To restore the default IGMP version, use the **no** form of this command.

Syntax

ip igmp version {1 | 2}

no ip igmp version

- **1**—IGMP version 1
- **2**—IGMP version 2

Default Configuration

The default is IGMP version 2.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

IGMP must be enabled before setting the IGMP version.

If IGMP is disabled on an interface, the IGMP parameters on the interface return to the default values.

Example

The following example configures the IGMP on port g5 to version 2.

```
Console (config)# interface ethernet g5
Console (config-if)# ip igmp version 2
```

ip igmp static-group

The **ip igmp static-group** interface configuration command configures the router to be a statically connected member of the specified group on the interface. To remove the router as a member of the group, use the **no** form of this command.

Syntax

ip igmp static-group *group-address*

no ip igmp static-group *group-address*

- *group-address*—IP Multicast address of a group to which the router belongs.

Default Configuration

The router is not a member of a group.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the router to be a statically connected member of the specified group on port g5 with IP address 224.0.0.0.

```
Console (config)# interface ethernet g5

Console (config-if)# ip igmp static-group 224.0.0.0
```

show ip mroute

The **show ip mroute** user EXEC command displays the IP Multicast routing table contents.

Syntax

show ip mroute [**group** *group-address*] [**source** *source-address*] [**ethernet** *interface-number* **|** **vlan** *vlan-id* **|** **port-channel** *number*]

- **group** *group-address*—Multicast group IP address.
- **source** *source-address*—The source IP address.
- **ethernet** *interface-number*—Ethernet port number.
- **vlan** *vlan-id*—VLAN number.
- **port-channel** *number*—Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays all ip mroutes.

```
Console# show ip mroute
 Group          Source          Upstream    Interface Up Time   Owner
----------- -----------------    ------------ -----------  --------- --------
224.0.255.1  198.92.37.100/32  10.20.37.33   eth g1   20:20:00   dvmrp
224.0.255.1  199.92.37.100/32  10.20.37.33   eth g1   1d:4h:20m  dvmrp
224.1.255.1  198.92.37.100/32  10.20.37.33   eth g1   21:20:00   dvmrp
224.1.255.1  199.92.37.100/32  10.20.37.33   eth g1   1d:5h:20m  dvmrp
224.8.255.1  179.82.17.200/32  10.20.37.33   vlan127  1w:1d:2h   dvmrp
224.8.255.1  179.82.17.200/32  10.20.37.33   vlan128 3m:2w:2d    dvmrp
224.8.255.1  179.82.17.200/32  10.20.37.33   vlan129 1y:2m:2w    dvmrp
224.9.255.1  179.82.17.200/32  10.20.37.33   p-c 7   1d:5h:20m   dvmrp
```

The following example displays all ip mroutes for source at IP address 192.92.37.100.

```
Console# show ip mroute source 198.92.37.100


  Group          Source          Upstream    Interface Up Time  Expiry Time Owner
---------------------------------------------- --------------------
224.0.255.1  198.92.37.100/32   10.20.37.33   eth g1  20:20:00    0:02:55   dvmrp
224.1.255.1  198.92.37.100/32   10.20.37.33   eth g1  21:20:00    0:02:55   dvmrp
```

The following example displays all ip mroutes for port g1.

```
Console# show ip mroute ethernet g1


  Group          Source         Upstream     Interface  Up Time   Owner
----------- ------------------    ------------   ---------  --------    ------
224.0.255.1  198.92.37.100/32  10.20.37.33   eth g1    20:20:00  dvmrp
224.0.255.1  199.92.37.100/32  10.20.37.33   eth g1    1d:4h:20m dvmrp
224.1.255.1  198.92.37.100/32  10.20.37.33   eth g1    21:20:00  dvmrp
224.1.255.1  199.92.37.100/32  10.20.37.33   eth g1    1d:5h:20m dvmrp
```

The following example displays all ip mroutes for group 224.1.255.1.

```
Console# show ip mroute group 224.1.255.1


  Group          Source         Upstream     Interface  Up Time   Owner
----------- -------------------- -------------- ----------- --------   --------
224.1.255.1  198.92.37.100/32  10.20.37.33  eth g1    21:20:00  dvmrp
224.1.255.1  199.92.37.100/32  10.20.37.33  eth g1    1d:5h:20m dvmrp
```

The following table describes the fields shown in the display:

Field	Description
Group	IP Multicast group address.
Source	The network address that identifies the sources.
Upstream	The upstream neighbor (RPF) address from which IP datagrams from these sources, to this Multicast address are received.
Interface	The IP interface on which IP datagrams sent by these sources to this Multicast address are received.
Up time	The time since the Multicast routing information was learned by the router.
Expiry time	The minimum amount of time remaining before this entry is aged out.
Owner	The Multicast routing protocol via which this Multicast forwarding entry was learned.

show ip mroute-next-hop

The **show ip mroute-next-hop** user EXEC command displays IP Multicast routing next hop information.

Syntax

show ip mroute-next-hop [**group** *group-address*] [**source** *source-address*]

- **group** *group-address*—Multicast group IP address.
- **source** *source-address*—The source IP address.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays Multicast next hop information.

```
Console# show ip mroute-next-hop


  Group          Source          Interface  Up Time    Expiry Time  State   Owner
-------------------------------------------------------------
224.0.255.1    198.92.37.100/32  eth g2    20:20:00   0:02:55    Forward   igmp
224.0.255.1    199.92.37.100/32  eth g2    1:4d:20m   0:02:55    Forward   igmp
224.1.255.1    198.92.37.100/32  eth g2    21:20:00   0:02:55    Forward   dvmrp
224.1.255.1    199.92.37.100/32  eth g2    1:4d:20m   0:02:55    Forward   dvmrp
```

The following table describes the fields shown in the display:

Field	Description
Group	IP Multicast group address.
Source	The network address that identifies the sources.
Interface	The outgoing interface.
Up time	The time since the Multicast routing information was learned by the router.
Expiry time	The minimum amount of time remaining before this entry is aged out. If the state is pruned, the remaining time until the prune expires and the state reverts to forwarding. Otherwise, the remaining time until this entry is removed from the table.
State	An indication of whether the outgoing interface and next-hop represented by this entry is currently being used to forward IP datagrams, or is currently pruned.
Owner	The routing mechanism via which this next-hop was learned.

show ip dvmrp interface

The **show ip dvmrp interface** user EXEC command displays DVMRP interface information.

Syntax

show ip dvmrp interface [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]

- **ethernet** *interface-number*—Ethernet port number.
- **vlan** *vlan-id*—VLAN number.
- **port-channel** *number*—Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays DVMRP interfaces.

```
Console# show ip dvmrp interface

Interface   IP address  Metric   RCV Bad RCV Bad Sent
                                 Packets Routes  Routes
---------   ----------- ------- ------- ------  ------
eth g1      172.16.1.1  10        0       12
```

The following table describes the fields shown in the display:

Field	Description
Interface	Interface type, number.
IP address	The IP address this system uses as a source address on this interface.
Metric	The distance metric for this interface used to calculate distance vectors.
RCV Bad Packets	The number of DVMRP messages received on the interface by the DVMRP process which were subsequently discarded as invalid (for example, invalid packet format, or a route report from an unknown neighbor).
RCV Bad Routes	The number of routes, in valid DVMRP packets, which were ignored because the entry was invalid.
Sent Routes	The number of routes, in DVMRP Report packets, which have been sent on this interface.

show ip dvmrp neighbor

The **show ip dvmrp neighbor** user EXEC command displays DVMRP-neighbor information on a per-interface basis.

Syntax

show ip dvmrp neighbor [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]

- **ethernet** *interface-number*—Ethernet port number.
- **vlan** *vlan-id*—VLAN number.
- **port-channel** *number*—Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays DVMRP neighbor information for port g1.

```
Console# show ip dvmrp neighbor ethernet g1

Inter- Neighbor     Up Time    Expiry   Version Capabilities State
face                           Time

------ ----------- ---------  ------- ------- ----------- -----

eth g1 192.168.1.28 20:20:00  0:02:55 3.255   L,P,G,M     Active

eth g1 192.168.1.10 20:20:00  0:02:55 3.255   L,P,G,M     Active

eth g2 192.168.1.28 20:20:00  0:02:55 3.255   L,P,G,M     Active

eth g2 192.168.1.89 20:20:00  0:02:55 3.255   L,P,G,M     Active
```

The following example displays DVMRP interfaces.

```
Console# show ip dvmrp neighbor

Inter- Neighbor     Up Time    Expiry   Version Capabilities State
face                           Time

------ ----------- ---------  ------- ------- ---------    -----

eth g2 192.168.1.28 20:20:00  0:02:55 3.255   L,P,G,M      Active

eth g2 192.168.1.10 20:20:00  0:02:55 3.255   L,P,G,M      Active
```

The following table describes the fields shown in the display:

Field	Description
Interface	Interface type, number.
Neighbor	The DVMRP neighbor IP address.
Up Time	The time since this DVMRP neighbor became a neighbor of the local router.
Expiry Time	The minimum time remaining before this DVMRP neighbor is aged out.
Version	The neighboring router DVMRP version number.
Capabilities	Describes the neighboring router capabilities. L—Indicates the neighbor has only one interface with neighbors. P—Indicates the neighbor supports pruning. G—Indicates the neighbor sends its generation ID in Probe messages. M—Indicates the neighbor can handle mtrace requests.
State	State of the neighbor adjacency. Can be One way, Active, ignoring or down.

show ip dvmrp next-hop

The **show ip dvmrp next-hop** user EXEC command displays DVMRP-next-hop information on a per-interface basis.

Syntax

show ip dvmrp next-hop [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]

- **ethernet** *interface-number*—Ethernet port number.
- **vlan** *vlan-id*—VLAN number.
- **port-channel** *number*—Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays DVMRP-next-hop information.

```
Console# show ip dvmrp next-hop

Source          Interface   Hop Type

--------------- ---------   --------

198.92.37.100/32  eth g2      Leaf

```

The following table describes the fields shown in the display:

Field	Description
Source	The network address identifying the sources.
Interface	The outgoing interface.
Hop Type	Type is Leaf if no downstream dependent neighbors exist on the outgoing virtual interface. Otherwise, type is Branch.

show ip dvmrp route

The **show ip dvmrp route** user EXEC command displays the Distance Vector Multicast Routing Protocol (DVMRP) routing table contents.

Syntax

show ip dvmrp route [*ip-address*]

- *ip-address*—IP address of an entry in the DVMRP routing table.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the DVMRP routing table contents.

```
Console# show ip dvmrp route

Source         Neighbor    Interface Metric    Expiry   Up
                                                Time    Time

------------- --------------------- -------  -------- --------

171.68.0.0/16 192.168.1.28  eth g1    10      00:02:52 07:55:50
```

The following table describes the fields shown in the display:

Field	Description
Source	The network address that identifies the sources for which this entry contains Multicast routing information.
Neighbor	The upstream neighbor (for example, RPF neighbor) address from which IP datagrams from these sources are received.
Interface	The interface on which IP datagrams sent by these sources are received.
Metric	The distance in hops to the source subnet.
Expiry time	The minimum amount of time remaining before this entry is aged out.
Up time	The time since the route represented by this entry was learned by the router.

show ip dvmrp prune

The **show ip dvmrp prune** user EXEC command displays the Distance Vector Multicast Routing Protocol (DVMRP) upstream prune state.

Syntax

show ip dvmrp prune [**group** *group-address* **source-address** | *source-address*]

- *group-address*—Multicast group IP address
- *source-address*—The source IP address

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the DVMRP upstream prune state.

```
Console# show ip dvmrp prune
Group          Source          Expiry
                                Time
-------------  ------------   --------
224.192.78.88  171.68.0.0/16   00:02:52
224.192.78.89  171.68.0.0/16   00:08:52
```

The following table describes the fields shown in the display:

Field	Description
Group	The group address which has been pruned
Source	The address of the source or source network which has been pruned.
Expiry time	The amount of time remaining before this prune expires at the upstream neighbor. This value should be the minimum of the default prune lifetime and the remaining prune lifetimes of the local router downstream neighbors, if any.

show ip igmp interface

The **show ip igmp interface** user EXEC command displays IGMP related information about an interface.

Syntax

show ip igmp interface [**ethernet** *interface-number* **|** **vlan** *vlan-id* **|** **port-channel** *number*]

- **ethernet** *interface-number*—Ethernet port number.
- **vlan** *vlan-id*—VLAN number.
- **port-channel** *number*—Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays IGMP related information about an interface.

```
Console# show ip igmp interface
Interface    Version    Query     Last     Max       Querier
                      Interval  Member  response    router
                        [sec]    [mSec]   [Sec]
---------    -------   -------   ------  --------  -----------
eth g1          2          60     1000      10      198.92.37.33
eth g2                     60     1000      10      198.92.36.131
```

The following table describes the fields shown in the display:

Field	Description
Interface	Interface type, number.
IP address	Interface IP address.
Version	The version of IGMP running on this interface.
Query interval	The frequency (seconds) at which IGMP Host-Query packets are transmitted.
Last member	The Last Member Query Interval (milliseconds) is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages.
Max response	The maximum query response time (seconds) advertised in IGMPv2 queries.
Querier router	The address of the querier router on the subnet.

show ip igmp groups

The **show ip igmp groups** user EXEC command displays the Multicast groups with receivers that are directly connected to the router, and that were learned through Internet Group Management Protocol (IGMP).

Syntax

show ip igmp groups [**group** *ip-address*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]

- **group** *ip-address*—Multicast group address.
- **ethernet** *interface-number*—Ethernet port number.
- **vlan** *vlan-id*—VLAN number.
- **port-channel** *number*—Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures authentication login.

```
Console# show ip igmp groups


Group Address  Interface  Uptime  Expires     Last Reporter
-------------  ---------  ------  --------    --------------
239.255.255.254  eth g1   1w0d    00:02:19    172.21.200.159
224.0.1.40       eth g1   1w0d    00:02:15    172.21.200.1
224.0.1.40       eth g3   1w0d    00:02:11    static
224.0.1.1        eth g1   1w0d    00:02:11    172.21.200.11
224.9.9.2        eth g1   1w0d    00:02:17    172.21.200.155
232.1.1.1        eth g1   5d21h   00:02:11    172.21.200.206
```

The following table describes the fields shown in the display:

Field	Description
Group Address	Multicast group address.
Interface	Interface through which the group is reachable.
Uptime	How long (in weeks, days, hours, minutes, and seconds) this Multicast group is known.
Expires	How long (in hours, minutes, and seconds) until the entry expires. The word "static" indicates that the entry will not time out, because the entry is defined as static.
Last Reporter	Last host to report being a member of the Multicast group.

18

OSPF Commands

router ospf enable

The **router ospf enable** global configuration command enables the OSPF routing process. To disable the OSPF routing process, use the **no** form of this command.

Syntax

router ospf enable

no router ospf enable

Default Configuration

The OSPF routing process is disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables the OSPF routing process.

```
Console (config)# router ospf enable
```

router ospf area

The **router ospf area** global configuration command defines an OSPF area. To remove the definition, use the **no** form of this command.

Syntax

router ospf area *area-id*

no router ospf area *area-id*

- *area-id*—OSPF area associated with a range of IP addresses.   The **area-id** is specified in a dotted decimal notation similar to an IP address.

Default Configuration

OSPF area 0.0.0.0 is the default, if no area is specified.

Command Mode

Global Configuration mode

User Guidelines

Auto-creation of OSPF areas is supported, so an OSPF area does not have to be defined before assigning it to an interface. To manually define an OSPF area, use the **router ospf area** command. If the auto-creation option is used, the area definition does not appear in the **running configuration** file.

If a question mark is specified at the end of the **router ospf area** command, the same hint is displayed twice at the prompt line.

An OSPF routed network must contain an area 0.   Only one sub-level of area hierarchy is allowed, that is all areas other than 0 must connect to area 0 via an ABR (area border router). An ABR is a router that is connected to two or more OSPF areas.

Small networks usually will only have an area 0.   Larger networks will have multiple OSPF areas to reduce the size of the IP route tables and to reduce the CPU and memory demands on the routers to a manageable level.

It is not necessary to define an OSPF area globally. OSPF areas may also be defined with the interface command.

Example

The following example globally defines an OSPF area with the value of 1.

.

```
Console (config)# router ospf area 0.0.0.1
```

router ospf redistribute rip

The router redistribute rip global configuration command enables incorporating IP routes that have been learned via the RIP routing process into the OSPF routing process.   To disable the redistribution of RIP routes, use the no form of this command.

Syntax

router ospf redistribute rip

no router ospf redistribute rip

Default Configuration

The redistribution of RIP routes is disabled.

Command Mode

Global Configuration mode

User Guidelines

If your network contains other routers that do not run OSPF, but do run RIP routing protocols, the OSPF process can incorporate those routes learned via RIP. When redistribution is enabled, the router becomes an "AS Boundary Router" (ASBR).

OSPF is more robust and converges more rapidly than RIP. Re-distribution of RIP routes should be used with care to avoid network instability. Redistribution should be done only in one direction. If RIP routes are redistributed into OSPF, do not redistribute the same OSPF networks back into RIP.

Example

The following example enables route advertisements learnt by RIP while running OSPF.

```
Console (config)# router ospf redistribute rip
```

router ospf redistribute static

The **router ospf redistribute static** global configuration command enables advertising routes, configured statically, in the OSPF routing process. To disable static route advertising, use the **no** form of this command.

Syntax

router ospf redistribute static

no router ospf redistribute static

Default Configuration

Statically configured route advertising is disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables route advertisements statically configured while running OSPF.

```
Console (config)# router ospf redistribute static
```

router ospf redistribute connected

The **router ospf redistribute connected** global configuration command enables advertising of directly connected networks routes, in the OSPF routing process. To disable advertising, use the **no** form of this command.

Syntax

router ospf redistribute connected

no router ospf redistribute connected

Default Configuration

Advertising of directly connected network routes is disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables advertisements of directly connected networks routes, running OSPF.

```
Console (config)# router ospf redistribute connected
```

router ospf area virtual-link

The **router ospf area virtual-link** global configuration mode command defines an OSPF virtual link and enters the OSPF Virtual-link Configuration mode. To remove a virtual link, use the **no** form of this command.

Syntax

router ospf area *area-id* **virtual-link** *router-id*
no router ospf area *area-id* **virtual-link** *router-id*

- *area-id*—Area associated with the OSPF address range. It is specified as an IP address.
- *router-id*—Router ID associated with the virtual link neighbor.

Default Configuration

No virtual link is defined.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines an OSPF virtual link on neighbor with the address 1.1.1.1.

```
Console (config)# router ospf area 1.1.1.1 virtual-link 1.1.1.1
```

hello-interval

The **hello-interval ospf virtual link** interface configuration command specifies the interval between hello packets that the software sends on the OSPF virtual link interface. To return to the default time, use the **no** form of this command.

Syntax

hello-interval *seconds*

no hello-interval

- *seconds*—Specifies the interval (in seconds). The value must be the same for all nodes on a specific network. (Range: 1 - 65535)

Default Configuration

The default value is 10 seconds.

Command Mode

OSPF virtual link configuration

User Guidelines

This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes are detected, but causes more routing traffic. This value must be the same for all routers and access servers on a specific network.

Example

The following example specifies the interval between hello packets that the software sends on the OSPF virtual link interface as 100.

```
Console (config)# router ospf area 1.1.1.1 virtual-link 1.1.1.1

Console# (config-vlink)# hello-interval 100
```

dead-interval

The **dead-interval ospf** virtual link interface configuration command sets the interval at which hello packets must not be seen before its neighbors declare the router down. To return to the default time, use the **no** form of this command.

Syntax

dead-interval *seconds*

no dead-interval

- *seconds*—Specifies the interval (in seconds). The value must be the same for all nodes on the network. (Range: 0 - 2147483647)

Default Configuration

The default is 60 seconds.

Command Mode

OSPF virtual link configuration

User Guidelines

The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

Example

The following example sets the interval at which hello packets must not be seen before its neighbors declare the router down to 100 seconds.

```
Console (config)# router ospf area 1.1.1.1 virtual-link 1.1.1.1

Console# (config-vlink)# dead-interval 100
```

retransmit-interval

The **retransmit-interval ospf virtual link** interface configuration command specifies the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPF virtual link interface. To return to the default value, use the **no** form of this command.

Syntax

retransmit-interval *seconds*

no retransmit-interval

- *seconds*—Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. (Range: 1- 3600)

Default Configuration

The default value is 5 seconds.

Command Mode

OSPF virtual link configuration

User Guidelines

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it resends the LSA. The setting of this parameter should be conservative to prevent unnecessary retransmissions.

Example

The following example specifies the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPF virtual link interface as 10 seconds.

```
Console (config)# router ospf area 1.1.1.1 virtual-link 1.1.1.1

Console# (config-vlink)# retransmit-interval 10
```

transmit-delay

The **transmit-delay ospf virtual link** interface configuration command sets the estimated time required to send a link-state update packet on the OSPF virtual link interface. To return to the default value, use the **no** form of this command.

Syntax

transmit-delay *seconds*

no transmit-delay

- *seconds*—Time (in seconds) required to send a link-state update. (Range: 1- 3600)

Default Configuration

The default value is 1 second.

Command Mode

OSPF virtual link configuration

User Guidelines

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the seconds argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Example

The following example sets the estimated time required to send a link-state update packet on the OSPF virtual link interface to 10 seconds.

```
Console (config)# router ospf area 1.1.1.1 virtual-link 1.1.1.1
Console# (config-vlink)# transmit-delay 10
```

authentication

The **authentication ospf virtual link** interface configuration command enables authentication for OSPF packets and specifies the type of authentication. To prevent authentication, use the **no** form of this command.

Syntax

authentication {**text** *text* | **md5** *name-of-chain*}

no authentication

- **text** *text*—Clears text authentication. The string can contain from 1 to 8 uppercase and lowercase alphanumeric characters.
- **md5** *name-of-chain*—Keyed Message Digest 5 (MD5) authentication.

Default Configuration

No authentication is provided for OSPF packets.

Command Mode

OSPF virtual link configuration

User Guidelines

There are no user guidelines for this command.

Example

The following example enables authentication for OSPF packets as MD5 with chain name of "hhv".

```
Console (config)# router ospf area 1.1.1.1 virtual-link 1.1.1.1
Console# (config-vlink)# authentication md5 hhv
```

router ospf router-id

The **router ospf router-id global configuration** command configures an OSPF router ID. To return to default, use the **no** form of this command.

Syntax

router ospf router-id *ip-address*

no router ospf router-id

- *ip-address*—Specifies the OSPF router ID as an IP address.

Default Configuration

The default is the first interface IP address.

Command Mode

Global Configuration mode

User Guidelines

An arbitrary value for the ip-address keyword for each router can be configured; however, each router ID must be unique.

Example

The following example configures an OSPF router ID as 196.127.2.1.

```
Console (config)# router ospf router-id 196.127.2.1
```

router ospf area stub

The **router ospf area stub** global configuration command defines an area as a stub area. To disable this function, use the **no** form of this command.

Syntax

router ospf area *area-id* **stub**

no router ospf area *area-id* **stub**

- *area-id*—Area associated with the OSPF address range. It is specified as an IP address.

Default Configuration

No stub area is defined.

Command Mode

Global Configuration mode

User Guidelines

The **router ospf area stub** command must be configured on all routers and access servers in the stub area. Use the **area** router configuration command with the **default-cost** option to specify the default internal router cost sent into a stub area by an ABR.

There are two stub area router configuration commands: the **stub** and **default-cost** options of the **area** router configuration command. In all routers attached to the stub area, the area should be configured as a stub area using the **area** command **stub** option. Use the **default-cost** option only on an ABR attached to the stub area. The **default-cost** option provides the metric for the summary default route generated by the ABR into the stub area.

If a question mark is specified at the end of the **router ospf area stub** command, the same hint is displayed twice at the prompt line.

Example

The following example defines an OSPF stub area 7.7.7.7.

```
Console (config)# router ospf area 7.7.7.7 stub
```

router ospf area default-cost

The **router ospf area default-cost** global configuration command specifies a cost for the default summary route sent into a stub area. To remove the assigned default route cost, use the **no** form of this command.

Syntax

router ospf area *area-id* **default-cost** *cost*

no router ospf area *area-id* **default-cost**

- *area-id*—Area associated with the OSPF address range. It can be specified as either a decimal value or as an IP address.
- *cost*—Cost for the default summary route used for a stub area. (Range: 1 - 16777215)

Default Configuration

A default value is automatically calculated by the router according to RFC 1850.

Command Mode

Global Configuration mode

User Guidelines

A default cost can be defined for an area, only after it has been defined. To define an area, use the **ospf area** command.

A default cost can be defined only for a stub area. To define a stub area, use the **ospf area stub command.**

Example

The following example specifies a cost of 10000 for the default summary route sent into a stub area number 192.168.3.1.

```
Console (config)# router ospf area 192.168.3.1 default-cost 10000
```

ospf

The **ospf** interface configuration command creates the OSPF routing process on an interface. To delete the OSPF routing process, use the **no** form of this command.

Syntax

ospf [area-id]

no ospf

- Area-id is an area associated with the OSPF address range. It can be specified as either a decimal value or as an IP address.

Default Configuration

OSPF is not created on an interface.

Command Mode

IP Interface Configuration mode

User Guidelines

After creating an OSPF process on an interface, the OSPF process must be activated on the interface using the **ospf enable command.**

If the specified area-id has not yet been created, using the **ip interface configuration ospf area** command, then it is auto-created using this command.

- An OSPF area that is auto-created is not displayed in the configuration file.
- An auto-created OSPF area is deleted only after a subsequent reboot, if the OSPF interface is deleted.

If no area is designated, the backbone area is associated with the IP interface. If the backbone has not yet been created, it is auto-created. Note that the negation of the **area** command does not appear in the configuration file, because it is, in fact, the default. However, it does appear when using the **show ospf** command, because it was automatically created.

Example

The following example enables OSPF on IP interface 1.100.100.100.

```
Console(config)# interface ip 1.100.100.100
Console(config-ip)# ospf
```

ospf enable

The **ospf enable** interface configuration command activates OSPF on an interface. To deactivate OSPF on an interface, use the **no** form of this command.

Syntax

ospf enable

no ospf enable

Default Configuration

OSPF is enabled on an interface.

Command Mode

IP Interface Configuration mode

User Guidelines

An OSPF interface must be created before it can be enabled. To enable an OSPF interface, use the **ospf** command.

Example

The following example activates OSPF on IP interface 1.100.100.100.

```
Console(config)# interface ip 1.100.100.100
Console(config-ip)# ospf enable
```

ospf area

The **ospf area** interface configuration command assigns an area to an interface. To remove the definition, use the **no** form of this command.

Syntax

ospf area *area-id*

no ospf area

- *area-id*—Area associated with the OSPF address range. It is specified as an IP address.

Default Configuration

The default is the first area (backbone area - 0.0.0.0).

Command Mode

IP Interface Configuration mode

User Guidelines

An OSPF area must be defined before it can be assigned to an interface. To define an OSPF area, use the **router ospf area** command.

OSPF area auto-creation is supported, so an OSPF area does not have to be defined before assigning it to an interface. To manually define an OSPF area, use the **router ospf area** command. If the auto-creation option is used, the area definition does appear in the running configuration file.

Example

The following example defines an interface area ID of 192.168.2.1 on IP interface 1.100.100.100.

```
Console(config)# interface ip 1.100.100.100

Console(config-ip)# ospf

Console(config-ip)# ospf area 192.168.2.1
```

ospf cost

The **ospf cost** interface configuration command specifies the cost of sending a packet on an interface. To reset the path cost to the default value, use the **no** form of this command.

Syntax

ospf cost *interface-cost*

no ospf cost

- *interface-cost*—Unsigned integer value expressed as the link-state metric. (Range:1 - 65535)

Default Configuration

10^8 divided by the interface speed, but not less than 1. If the value is less than 1, then the default value is 1.

Command Mode

IP Interface Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines a path cost 0f 250 on IP interface 1.100.100.100.

```
Console(config)# interface ip 1.100.100.100
Console(config-ip)# ospf cost 250
```

ospf priority

The **ospf priority** interface configuration command sets the router priority, which is used in electing the designated router for the network. To return to the default value, use the **no** form of this command.

Syntax

ospf priority *number-value*

no ospf priority

- *number-value*—A number value that specifies the router priority. (Range: 0 - 255)

Default Configuration

The default router priority number is 1.

Command Mode

IP Interface Configuration mode

User Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router.

Example

The following example defines a router OSPF priority of 100.

```
Console(config)# interface ip 1.100.100.100
Console(config-ip)# ospf priority 100
```

ospf hello-interval

The **ospf hello-interval** interface configuration command specifies the interval between hello packets the software sends on an interface. To return to the default time, use the **no** form of this command.

Syntax

ospf hello-interval *seconds*

no ospf hello-interval

- *seconds*—Specifies the interval (in seconds). The time value must be the same for all nodes on a specific network. (Range: 1 - 65535)

Default Configuration

The default hello-interval is 10 seconds.

Command Mode

IP Interface Configuration

User Guidelines

This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes are detected, resulting in extra routing traffic. This value must be the same for all routers and access servers on a specific network.

Example

The following example defines the hello-time of 100 seconds on IP interface 1.100.100.100.

```
Console(config)# interface ip 1.100.100.100
Console(config-ip)# ospf hello-interval 100
```

ospf dead-interval

The **ospf dead-interval** interface configuration command sets the interval at which hello packets must not be seen before neighbors declare the router down. To return to the default time, use the **no** form of this command.

Syntax

ospf dead-interval *seconds*

no ospf dead-interval

- *seconds*—Specifies the interval (in seconds). The time value must be the same for all nodes on the network. (Range: 1- 2147483647)

Default Configuration

The default IP Interface dead-interval time is 40 seconds.

Command Mode

IP Interface Configuration

User Guidelines

The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

Example

The following example defines the OSPF dead-interval time of 100 seconds on interface 1.100.100.100.

```
Console(config)# interface ip 1.100.100.100

Console(config-ip)# ospf dead-interval 100
```

ospf retransmit-interval

The **ospf retransmit-interval** interface configuration command specifies the time between link-state advertisement (LSA) retransmissions for interface adjacencies belonging to the interface. To return to the default value, use the **no** form of this command.

Syntax

ospf retransmit-interval *seconds*

no ospf retransmit-interval

- *seconds*—Time (in seconds) between retransmissions. The time must be greater than the expected round-trip delay between any two routers on the attached network. (Range: 1 - 3600)

Default Configuration

The default time is 5 seconds.

Command Mode

IP Interface Configuration

User Guidelines

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it resends the LSA.

Setting this parameter should be conservatively configured, or unnecessary retransmission can result.

Example

The following example specifies 60 seconds between link-state advertisement (LSA) retransmissions for IP interface 1.100.100.100 adjacencies.

```
Console(config)# interface ip 1.100.100.100
Console(config-if)# ospf re-transmit-interval 60
```

ospf transmit-delay

The **ospf transmit-delay** interface configuration command sets the estimated time required to send a link-state update packet on an interface. To return to the default value, use the **no** form of this command.

Syntax

ospf transmit-delay *seconds*

no ospf transmit-delay

- *seconds*—Time (in seconds) required to send a link-state update. (Range: 1 - 3600)

Default Configuration

The default time is 1 second.

Command Mode

IP Interface Configuration

User Guidelines

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Example

The following example sets the estimated time required to send a link-state update packet on IP interface 1.100.100.100 to 60 seconds.

```
Console(config)# interface ip 1.100.100.100
Console(config-if)# ospf transmit-delay 60
```

router ospf compatible rfc1583

To restore the method used to calculate summary route costs per RFC 1583, use the **router ospf compatible rfc1583** command in global configuration mode. To disable RFC 1583 compatibility, use the no form of this command.

Syntax

router ospf compatible rfc1583

no router ospf compatible rfc1583

- This command has no arguments or keywords.

Default Configuration

RFC1583 compatibility mode is supported.

Command Mode

Global Configuration mode

Usage Guidelines

This command enables support of RFC1583 compatibility in products that support later standards.

Example

The following example restores the method of calculation of summary route costs as suggested by RFC 1583:

```
Console (config)# router ospf compatible rfc1583
```

ospf authentication

The **ospf authentication** interface configuration command enables authentication for OSPF packets and specifies the authentication type. To prevent authentication, use the **no** form of this command.

Syntax

ospf authentication {**text** *text* | **md5** *name-of-chain* }

no ospf authentication mode

- **text** *text*—Clear text authentication. The string can contain from 1 to 8 uppercase and lowercase alphanumeric characters.
- **md5** *name-of-chain*—Keyed Message Digest 5 (MD5) authentication.

Default Configuration

No authentication is provided for OSPF packets.

Command Mode

IP Interface Configuration

User Guidelines

There are no user guidelines for this command.

Example

The following example OSPF authentication on IP interface 1.100.100.100 is enabled for MD5 authentication named "mychain".

```
Console(config)# interface ip 1.100.100.100

Console(config-ip)# ospf authentication md5 mychain
```

clear ip ospf process

The **clear ip ospf process** privileged EXEC command clears OSPF database entries learned by the device or by a specific interface.

Syntax

clear ip ospf process [*interface*]

- *interface*—IP interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

OSPF database entries learned by the device or by a specific interface cannot be cleared using the Web user interface

Example

The following example clears OSPF routing redistribution on IP interface 192.168.3.1.

```
Console# clear ip ospf process 192.168.3.1
```

show ip ospf

The **show ip ospf** user EXEC command displays general OSPF routing information.

Syntax

show ip ospf

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures authentication login.

```
Console# show ip ospf
OSPF is enabled
OSPF Router ID 192.42.110.200
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Redistributing External Routes from,
rip with metric mapped to type 2
Number of areas in this router is 3
Area 192.42.110.0
Area is a stub area with default cost 10
Number of interfaces in this area is 1
SPF algorithm executed 6 times
```

The following table describes the fields that display:

Field	Description
OSPF Router ID	OSPF router ID.
Supports...	Number of types of service supported (Type 0 only).

It is...	Possible types are internal, area border, or autonomous system boundary.
Redistributing External Routes from	Lists redistributed routes, by protocol.
Number of areas	Number of areas in router, area addresses, etc.

show ip ospf virtual-links

The **show ip ospf virtual-links** user EXEC command displays parameters and the current state of OSPF virtual links.

Syntax

show ip ospf virtual-links [**area** *area-id*] [**router** *router-id*]

- *area-id*—Area associated with the OSPF address range. It is specified as an IP address.
- *router-id*—Router ID associated with the virtual link neighbor.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays parameters and the current state of OSPF virtual links.

```
Console# show ip ospf virtual-links
Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1
Virtual link has simple password authentication
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Adjacency State FULL
```

The following table describes the fields the display:

Field	Description
Virtual Link to router 192.168.101.2 is up	Specifies the OSPF neighbor, and if the link to that neighbor is up or down.
Transit area 0.0.0.1	The transit area through which the virtual link is formed.
Transmit Delay is 1 sec	The transmit delay (in seconds) on the virtual link.
State POINT_TO_POINT	The state of the OSPF neighbor.
Timer intervals...	The various timer intervals configured for the link.
Adjacency State FULL	The adjacency state between the neighbors.

show ip ospf database

The **show ip ospf database** user EXEC command displays information lists related to the OSPF database. The various forms of this command deliver information about different OSPF link-state advertisements (LSAs).

Syntax

show ip ospf [*area-id*] **database**

show ip ospf [*area-id*] **database** [**adv-router** [*ip-address*]]

show ip ospf [*area-id*] **database** [**asbr-summary**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**database-summary**]

show ip ospf [*area-id*] **database** [**external**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**external**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*area-id*] **database** [**external**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**network**][*link-state-id*]

show ip ospf [*area-id*] **database** [**network**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*area-id*] **database** [**network**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**router**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**router**] [**adv-router** [*ip-address*]]

show ip ospf [*area-id*] **database** [**router**] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**summary**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**summary**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*area-id*] **database** [**summary**] [*link-state-id*] [**self-originate**] [*link-state-id*]

- *area-id*—Area number associated with the OSPF address range defined in the **router ospf area** router configuration command used to define the particular area.
- **adv-router** [*ip-address*]—Displays all the specified router link-state advertisements (LSAs). If no IP address is included, the information is about the local router itself (in this case, the same as the **self-originate keyword**).
- **asbr-summary**—Displays information only about the Autonomous System Boundary Router (ASBR) summary LSAs.

- *link-state-id*—Portion of the Internet environment that is being described by the advertisement. The value entered depends on the type of the LSA. The value must be entered in the form of an IP address.

When the LSA is describing a network, the *link-state-id* argument can take one of two forms:

- The network IP address (as in Type 3 summary link advertisements and in autonomous system external link advertisements).
- A derived address obtained from the link-state ID. (Note that masking a network will link the advertisement link-state ID with the network subnet mask yielding the network IP address.)

When the LSA is describing a router, the link-state ID is always the OSPF router ID of the described router.

When an autonomous system external advertisement (Type 5) is describing a default route, its link-state ID is set to the default destination (0.0.0.0).

- **database-summary**—Displays how many of each type of LSA for each area there are in the database, and the total number of LSA types.
- **external**—Displays information only about the external LSAs.
- **network**—Displays information only about the network LSAs.
- **router**—Displays information only about the router LSAs.
- **self-originate**—Displays only self-originated LSAs (from the local router).
- **summary**—Displays information only about the summary LSAs.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays OSPF database information.

```
Console# show ip ospf database


OSPF Router with ID 200.1.1.11


                 Router Link States(Area 0)


 Link ID         ADV Router      Age         Seq#      Checksum
Link count
 200.1.1.8       200.1.1.8       1381      0x8000010D   0xEF60   2
 200.1.1.11      200.1.1.11      1460      0x800002FE   0xEB3D   4
 200.1.1.12      200.1.1.12      2027      0x80000090   0x875D   3
 200.1.1.27      200.1.1.27      1323      0x800001D6   0x12CC   3


                 Net Link States(Area 0)


 Link ID         ADV Router      Age         Seq#       Checksum
 140.1.1.27      200.1.1.27      1323      0x8000005B    0xA8EE
 141.1.1.11      200.1.1.11      1461      0x8000005B    0x7AC
```

The following table describes the fields shown in the display:

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete the LSA contents.
Link count	Number of interfaces detected for router.

The following example displays OSPF database ASBR information.

```
Console# show ip ospf database asbr-summary


OSPF Router with id 190.20.239.66


Displaying Summary ASB Link States(Area 0.0.0.0)


LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 155.187.245.1 (AS Boundary Router address)
Advertising Router: 155.187.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0 TOS: 0  Metric: 1
```

The following table describes fields shown in the display:

Field	Description
OSPF Router with id	Router ID number.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID (ASBR).
Advertising Router	Advertising router ID.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length in bytes of the LSA.
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link-state metric.

The following example displays external OSPF database information.

```
Console# show ip ospf database external


OSPF Router with id 190.20.239.66


      Displaying AS External Link States


LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 143.105.0.0 (External Network Number)
Advertising Router: 155.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 1
     Forward Address: 0.0.0.0
     External Route Tag: 0
```

The following table describes fields shown in the display:

Field	Description
OSPF Router with id	Router ID number.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID (External Network Number).
Advertising Router	Advertising router ID.
LS Seq Number	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Checksum (Fletcher checksum of the complete contents of the link-state advertisement).
Length	Length in bytes of the LSA.
Network Mask	Network mask implemented.
Metric Type	External type.
TOS	Type of service.
Metric	Link-state metric.
Forward Address	Forwarding address. Data traffic for the advertised destination is forwarded to this address. If the forwarding address is set to 0.0.0.0, data traffic is forwarded to the advertisement originator.
External Route Tag	External route tag, a 32-bit field attached.

The following example displays OSPF database network information.

```
Console# show ip ospf database network


OSPF Router with id 190.20.239.66


                Displaying Net Link States(Area 0.0.0.0)


LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 155.187.1.3 (address of Designated Router)
Advertising Router: 190.20.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
        Attached Router: 190.20.239.66
        Attached Router: 155.187.241.5
        Attached Router: 155.187.1.1
        Attached Router: 155.187.54.5
        Attached Router: 155.187.1.5
```

The following table describes fields shown in the display:

Field	**Description**
OSPF Router with id	Router ID number.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID of designated router.
Advertising Router	Advertising router ID.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Checksum (Fletcher checksum of the link-state advertisement complete contents).
Length	Length in bytes of the link-state advertisement.
Network Mask	Network mask implemented.
Attached Router	List of routers attached to the network, by IP address.

The following example displays OSPF database router information.

```
Console# show ip ospf database router
OSPF Router with id 190.20.239.66
Displaying Router Link States(Area 0.0.0.0)
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 155.187.21.6
Advertising Router: 155.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
 (link ID) Neighboring Router ID: 155.187.21.5
 (Link Data) Router Interface address: 155.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

The following table describes fields shown in the display:

Field	**Description**
OSPF Router with id	Router ID number.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID.
Advertising Router	Advertising router ID.
LS Seq Number	Link-state sequence (detects old or duplicate link-state advertisements).
Checksum	Checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length in LSA bytes.
AS Boundary Router	Router type definition.
Number of Links	Number of active links.
link ID	Link type.
Link Data	Router interface address.
TOS	Type of service metric (Type 0 only).

The following example displays OSPF database router information.

```
Console# show ip ospf database summary


OSPF Router with id 190.20.239.66


Displaying Summary Net Link States(Area 0.0.0.0)


LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 155.187.240.0 (summary Network Number)
Advertising Router: 155.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0   TOS: 0  Metric: 1
```

The following table describes fields shown in the display:

Field	Description
OSPF Router with id	Router ID number.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID (summary network number).
Advertising Router	The ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length in bytes of the link-state advertisement.
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link-state metric.

The following example displays OSPF database summary information.

```
Console# show ip ospf database-summary


OSPF Router with ID (172.19.65.21) (Process ID 1)


Area ID        Router   Network   Sum-Net   Sum-ASBR    Subtotal
1.1.1.1          1         0         0         0           1
AS External      0
Total            1         0         0         0           1
```

The following table describes fields shown in the display:

Field	Description
Area ID	Area ID.
Router	Number of router LSAs in that area.
Network	Number of network LSAs in that area.
Sum-Net	Number of summary LSAs in that area.
Sum-ASBR	Number of summary ASBR LSAs in that area.
Subtotal	Sum of Router, Network, Sum-Net, and Sum-ASBR for that area.
AS External	Number of external LSAs.

show ip ospf interface

The **show ip ospf interface** user EXEC command displays OSPF-related interface information.

Syntax

show ip ospf interface [*interface*]

- *interface*—An OSPF-related IP interface.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays OSPF-related IP interface 192.168.1.1 information.

```
Console# show ip ospf interface 192.168.1.1

IP interface 192.168.1.1/16 is up, OSPF is enabled

Area 0.0.0.0, Router ID 192.77.99.1, Network Type BROADCAST, Cost:
10

Interface has simple password authentication

Transmit Delay is 1 sec, State OTHER, Priority 1

Designated Router id 192.168.1.11, Interface address 192.168.1.11

Backup Designated router id 192.168.1.28, Interface addr
192.168.1.28

Timer intervals configured, Hello 10, Dead 60, Retransmit 5

Neighbor Count is 8, Adjacent neighbor count is 2

Adjacent with neighbor 192.168.1.28 (Backup Designated Router)

Adjacent with neighbor 192.168.1.10 (Designated Router)
```

The following table describes fields shown in the display:

Field	Description
Transmit Delay	Transmit delay, interface state, and router priority.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

show ip ospf neighbor

The **show ip ospf neighbor** user EXEC command displays OSPF-neighbor information on a per-interface basis.

Syntax

show ip ospf neighbor [*interface*]

- *interface*—The IP interface.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

For OSPF routers to become neighbors, they must be directly connected and agree on the following parameters.

- IP prefix and subnet mask
- Area ID
- Authentication (none, text, MD5)
- Options (stub, nssa)
- Hello Interval (default 10 sec.)
- Router Dead Interval (default 40 sec.)

Examples

The following example displays OSPF-neighbor information on interface 192.168.1.1.

```
Console# show ip ospf neighbor 192.168.1.1
Neighbor 192.168.1.11, Address 192.168.1.11
In the area 0.0.0.0
Neighbor priority is 1, State is FULL
Options 2
Neighbor 192.168.1.12, Address 192.168.1.12
In the area 0.0.0.0
Neighbor priority is 2, State is FULL
Options 2
```

The following table describes fields shown in the display:

Field	Description
Neighbor	Neighbor router ID.
Address	IP address of the interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority of the neighbor, neighbor state.
State	OSPF neighbor state (init, two-way, loading, full). On a broadcast media, the roles are Designated Router (DR), Backup Designated Router (BDR), Other (DRother)
Options	Hello packet options field contents. (E-bit only. Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)

19

PHY Diagnostics Commands

test copper-port tdr

The **test copper-port tdr** privileged EXEC command diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.

The device reports only shorts across the cable pairs. The Virtual Cable Test (VCT) analyzes each of the MDI pairs in the cable being tested. Typically, in a CAT5 RJ-45 cable, the positive and negative of each pair are twisted together. The pairs that are twisted together are identifiable: solid orange and striped orange, solid blue and striped blue, solid green and striped green, solid brown and striped brown are twisted together. If, for example, MDI[0]+/- pins are connected to pairs 1,2 of the RJ45, which are connected to the orange pair, then MDI[0]+ will be connected to the solid orange and MDI[0]- will be connected to the striped orange. The short between wires that do not belong to the same pair will not be reported.

Syntax

test copper-port tdr *interface*

- *interface*—A valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The port can only be tested if cable is connected to both sides.

The port under test should be shut down during the test, unless it is a combo port with an active fiber port.

NOTE: The maximum disatance VCT can function is 120 meters.

Examples

The following example results in a report on the cable attached to port g3.

```
Console# test copper-port tdr g3
Cable is open at 100 meters
```

The following example results in a failure to report on the cable attached to port g4.

```
Console# test copper-port tdr g4
Can’t perform the test on fiber ports
```

show copper-ports tdr

The **show copper-ports tdr** privileged EXEC command display the last TDR (Time Domain Reflectometry) tests on specified ports.

Syntax

show copper-ports tdr [*interface*]

- *interface*—A valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the last TDR (Time Domain Reflectometry) tests on all ports.

```
Console# show copper-ports tdr
Port   Result    Length [meters]      Date
----   --------  ---------------  ---------------
g1      OK
g2     Short     50               13:32:00 23 July 1997
g3     Test has not been preformed
g4     Open      128              13:32:08 23 July 1997
g5     Fiber     -                 -
```

show copper-ports cable-length

The **show copper-ports cable-length** privileged EXEC command displays the estimated copper cable length attached to a port.

Syntax

show copper-ports cable-length [*interface*]

- *interface*—A valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This feature works only on 1-Gbps ports.

Example

The following example displays the estimated copper cable length attached to all ports.

```
Console# show copper-ports cable-length
Port     Length [meters]
----     ---------------
g1       < 50
g2       Giga link not active
g3       110-140
g4       Fiber
```

show fiber-ports optical-transceiver

The **show fiber-ports optical-transceiver** privileged EXEC command displays the optical transceiver diagnostics.

Syntax

show fiber-ports optical-transceiver [*interface*] [**detailed**]

Syntax Description

- *interface*—A valid Ethernet port.
- **detailed**—Detailed diagnostics.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

To test optical transceivers ensure a fiber link is present.

Examples

The following example displays the optical transceiver diagnostics.

```
console# show fiber-ports optical-transceiver
Port   Temp    Voltage    Current Output Input   TX     LOS     Data
                          Power   Power          Fault          Ready
----------- ------ -------- -------- ------ -----  -----  ---     -----
g1     N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g2     N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g3     N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g4     N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g5     N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g6     N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g7     N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g8     N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g9     N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g10    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g11    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g12    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g13    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g14    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g15    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g16    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g17    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g18    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g19    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g20    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g21    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g22    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g23    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
g24    N/A     N/A        N/A     N/A    N/A     N/A    N/A     N/A
Temp - Internally measured transceiver temperature
Voltage - Internally measured supply voltage
Current - Measured TX bias current
Output Power - Measured TX output power in milliWatts
Input Power - Measured RX received power in milliWatts
TX Fault - Transmitter fault
LOS - Loss of signal
Data Ready - Indicates transceiver has archived power up and data is
ready
N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

The following example displays detailed optical transceiver diagnostics.

```
Console# show fiber-ports transceiver detailed

                                                Power
Port     Temp    Voltage    Current    Output    Input    TX      LOS    Data
         [C]     [Volt]     [mA]       [dBm]     [dBm]    Fault          Ready
----     -----   -------    -------     ------    ------ -----   ---    -----
g1        48       5.15       50        1.7        1.7      No    No     Yes
g2        43       5.15       10        1.7        1.7      No    No     Yes


g3       Copper


Temp - Internally measured transceiver temperature.
Voltage - Internally measured supply voltage.
Current - Measured TX bias current.
Output Power - Measured TX output power.
Input Power - Measured RX  received power.
Tx Fault - Transmitter fault
LOS - Loss of signal
Data ready - Indicates transceiver has achieved power up and data
is ready.
```

20

Port Channel Commands

interface port-channel

The **interface port-channel** global configuration command enters the interface configuration mode of a specific port-channel.

Syntax

interface port-channel *port-channel-number*

- *port-channel-number*—A valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Seven supported aggregated links are defined, and per port-channel, up to 7 member ports.

Turning off auto-negotiation of an aggregate link may, under some circumstances, make it non-operational. If the other side has auto-negotiation turned on, it may re-synchronize all members of the aggregated link to half-duplex operation, and may, as per the standards, set them all to inactive.

Example

The following example enters the context of port-channel number 1.

```
Console (config)# interface port-channel 1
```

interface range port-channel

The **interface range port-channel** global configuration command enters the interface configuration mode to configure multiple port-channels.

Syntax

interface range port-channel {*port-channel-range* | *all*}

- *port-channel-range*—List of port-channels to configure. Separate non-consecutive port-channels with a comma and no spaces. A hyphen designates a range of port-channels.
- **all**—All the channel-ports.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, it stops the execution of the command on subsequent interfaces.

Example

The following example shows how port-channels 1, 2 and 8 are grouped to receive the same command.

```
Console (config)# interface range port-channel 1-2, 8
Console (config-if)#
```

channel-group

The **channel-group** interface configuration command associates a port with a port-channel. To remove a port from a port channel, use the **no** form of this command.

Syntax

channel-group *port-channel-number* **mode** {**on** | **auto**}

no channel-group

- *port-channel_number*—Specifies the number of the valid port-channel for the current port to join.
- **on**—Forces the port to join a channel.
- **auto**—Allows the port to join a channel as a result of an LACP operation.

Default Configuration

The port is not assigned to any port-channel.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Turning off auto-negotiation on an aggregate link may, under some circumstances make it non operational. If the other side has auto-negotiation turned on, it may re-synchronize all members of the aggregated link to half-duplex operation, and may, as per the standard, set them all to Inactive.

Example

The following example shows how port g5 is configured to port-channel number 1 without LACP.

```
Console (config)# interface ethernet g5
Console (config-if)# channel-group 1 mode on
```

show interfaces port-channel

The **show interfaces port-channel** user EXEC command displays port-channel information (which ports are members of that port-channel, and whether they are currently active or not).

Syntax

show interfaces port-channel [*port-channel-number*]

- *port-channel-number*—Valid port-channel number information to display.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how all port-channel information is displayed.

```
Console (config)# show interfaces port-channel
Channel                         Ports
------------                    ------
Ch 1                  Active    g1, g2   Inactive g3
Ch 2                  Active    g2
Ch 3                  Inactive  g8
```

21

Port Monitor Commands

port monitor

The **port monitor** interface configuration command starts a port monitoring session. To stop a port monitoring session, use the **no** form of this command.

Syntax

port monitor *src-interface* [**rx** | **tx**]

no port monitor *src-interface*

- *src-interface*—Valid Ethernet port number.
- **rx—**Monitors received packets only.
- **tx—**Monitors transmitted packets only.

Default Configuration

No port monitoring sessions are defined.

If no option is specified, monitors both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command enables traffic on one port to be copied to another port, or between the source port (src-interface) and a destination port (the port being configured). Only a single target port can be defined per system.

The port being monitored cannot be set faster than the monitoring port.

The following restrictions apply to ports configured to be destination ports:

- The port cannot be already configured as a source port.
- The port cannot be a member in a port-channel.
- An IP interface is not configured on the port.
- GVRP is not enabled on the port.
- The port is not a member in any VLAN, except for the default VLAN (will automatically be removed from the default VLAN).

The following restrictions apply to ports configured to be source ports:

- Port monitoring Source Ports must be simple ports, and not port-channels.
- The port cannot be already configured as a destination port.

- All the frames are transmitted already tagged from the destination port.

General Restrictions:

- Ports cannot be configured as a group using the **interface range ethernet** command.

NOTE: The Port Mirroring target must be a member of the Ingress VLAN of all Mirroring source ports. Therefore, Multicast and Broadcast frames in these VLANs are seen more than once. (Actually N+1, where N is the number of mirroring source ports). In addition, if there is more than a single VLAN, all frames sent from the mirroring target port are tagged, regardless of the incoming frame state.

Example

The following example shows how traffic on port g8 (source port) is copied to port g1 (destination port).

```
Console(config)# interface ethernet g1
Console(config-if)# port monitor g8
```

port monitor vlan-tagging

The **port monitor vlan-tagging** interface configuration command transmits tagged ingress mirrored packets. To transmit untagged ingress mirrored packets, use the **no** form of this command.

Syntax

port monitor vlan-tagging

no port monitor vlan-tagging

Default Configuration

Ingress mirrored packets are transmitted untagged.

Command Mode

Interface Configuration (Ethernet)

User Guidelines

There are no user guidelines for this command.

Example

The following example configures all ingress mirrored packets from port g9 to be transmitted as tagged packets.

```
Console (config)# interface ethernet g9
Console (config-if)# port monitor vlan-tagging
```

show ports monitor

The **show ports monitor** user EXEC command displays the port monitoring status.

Syntax

show ports monitor

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how the port monitoring status is displayed.

```
Console#  show ports monitor
Source Port  Destination Port  Type   Status    VLAN Tagging
-----------  ----------------  -----  -------   ------------
g1           g8                RX,TX  Active    No
g2           g8                RX,TX  Active    No
g18          g8                RX     Active    No
```

22

QoS Commands

qos

The **qos** global configuration command enables quality of service (QoS) on the device and enters QoS basic or advanced mode. Use the **no** form of this command to disable the QoS features on the device.

Syntax

qos [*advanced*]

no qos

- *advanced*—Enable QoS advanced mode. Advanced mode enables the full QoS configuration.

Default Configuration

By default QoS is enabled in basic mode.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command. However, switching to Basic qos mode sets the trust mode to cos.

Example

The following example shows how QoS is enabled on the device, in basic mode.

```
Console (config)# qos
```

show qos

The **show qos** user EXEC command displays the QoS status.

Syntax

show qos

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays a device where basic mode is supported.

```
Console# show qos

Qos: basic

Basic trust: dscp
```

priority-queue out num-of-queues

The **priority-queue out num-of-queues** global configuration command enables the egress queues to be expedite queues. To disable the expedite queue, which disables all the strict priority queues and returns the queues to strict priority mode, use the **no** form of this command.

Syntax

priority-queue out num-of-queues *number-of-queues*

no priority-queue out num-of-queues

- *number-of-queues*—Assign the number of queues to be expedite queues. The expedite queues would be the queues with higher indexes. The range is 0 – 8.

Default Configuration

All queues are expedite queues.

Command Mode

Global Configuration mode

User Guidelines

When configuring the **priority-queue out num-of-queues** command, the weighted round robin (WRR) weight ratios are affected because there are fewer queues participating in WRR.

Example

The following example sets queue 7, 8 to be an EF queue.

```
Console (config)# priority-queue out num-of-queues 2
```

traffic-shape

The **traffic-shape** interface configuration command sets a shaper on an egress port/queue. To disable the shaper on an interface, use the **no** form of this command.

Syntax

traffic-shape {*committed-rate committed-burst*} [*queue-id*]

no traffic-shape [*queue-id*]

- *committed-rate*—The average traffic rate (CIR) in bits per second (bps).
- *committed-burst*—The excess burst size (CBS) in bytes.
- *queue-id*—Assign shaper to the specified queue.

Default Configuration

No shaper is defined.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

For an egress port, enter the interface configuration mode with the port number, and use the **traffic-shape** command without the *queue-id* option, and the CIR and the CBS are applied on the specified port.

In order to activate shaper for a specific queue, add the queue ID to the line.

Example

The following example sets a shaper on port g5 when the average traffic rate exceeds 124000 bps or the a normal burst size exceeds 96000 bps.

```
Console (config)# interface ethernet g5
Console (config-if) traffic-shape 124000 96000
```

qos wrr-queue threshold

The **qos wrr-queue threshold** global configuration command assigns the tail-drop mechanism on an egress queue and configures the tail-drop thresholds. To assign the default values, use the **no** form of this command.

Syntax

qos wrr-queue threshold *queue-id threshold-percentage*

no qos wrr-queue threshold *queue-id*

- *queue-id*—Specifies the queue ID to assign the tail-drop.

- *threshold-percentage*—Specifies the tail-drop threshold percentage value. (Range: 1 - 100)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

The packet refers to a certain threshold by the conformance level. If threshold 0 is exceeded, packets with the corresponding DP are dropped until the threshold is no longer exceeded. However, packets assigned to threshold 1 and 2 continue to be queued and sent as long as the second or third threshold are not exceeded.

Example

The following example configures the tail-drop thresholds to 80%.

```
Console (config)# qos wrr-queue threshold 1 80
```

wrr-queue bandwidth

The **wrr-queue bandwidth** interface configuration command assigns Weighted Round Robin (WRR) weights to egress queues. The weights ratio determines the frequency in which the packet scheduler dequeues packets from each queue. To return to the default values, use the **no** form of this command.

Syntax

wrr-queue bandwidth *weight1 weight2* ... *weight_n*

no wrr-queue bandwidth

- *weight1...weight_n*—Sets the bandwidth ratio in which the WRR packet scheduler dequeues packets. Separate each value by spaces. (Range: 6 - 255)

Default Configuration

The default WRR weight is 1/8 ratio for all queues (each weight set to 6).

Command Mode

Interface Configuration mode

User Guidelines

The packet refers to a threshold by the conformance level. Weighted round robin queues should be defined on the interface.

A weight between 6 and 255 may be specified. A weight of 0 may also be specified for all queues except queue 8. Note that specifying a weight of 0 is not recommended because it closes the queue.

Example

The following example sets queue weights as follows:

- Queue 1—6
- Queue 2—6
- Queue 3—6
- Queue 4—6
- Queue 5—6
- Queue 6—6
- Queue 7—6
- Queue 8—6

```
Console (config-if)# wrr-queue bandwidth 6 6 6 6 6 6 6 6
```

wrr-queue

The **wrr-queue** interface configuration command defines the wrr-queue mechanism on an egress queue. Use the **no** form of the command to define the default thresholds.

Syntax

wrr-queue {**tail-drop**}

no wrr-queue

- **tail-drop**—Tail-drop mechanism.

Default Configuration

The system default is tail-drop mechanism with 100% for all thresholds.

Command Mode

Interface Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example defines the wrr-queue mechanism on an egress queue to tail-drop.

```
Console (config)# interface ethernet g5
Console (config-if)# wrr-queue tail-drop
```

show qos interface

The **show qos interface** user EXEC command displays interface QoS data.

Syntax

show qos interface [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*] [**buffers** | **queuing** | **policers** | **shapers**]

- **ethernet** *interface-number*—Ethernet port number.
- **vlan** *vlan-id*—VLAN number.
- **port-channel** *number*—Port-channel.
- **buffers**—Displays buffer setting for the interface queues. For gigabit Ethernet interfaces, the queue depth for each of the 8 queues and the thresholds for the WRED/Tail Drop are displayed. For 10/100 interfaces the minimum reserved settings are displayed.
- **queuing**—Displays the queue strategy (WRR or EF), the weight for WRR queues, the CoS to queue map and the EF priority.
- **shapers**—Displays the specified interface shaper and the shaper for the queue on the specified interface.
- **policers**—Displays all the policers configured for this interface, their setting, and the number of policers currently unused.

Default Configuration

For VLAN interface only the **policers** option is relevant.

If no keyword is specified with the **show qos interface** command, the port QoS mode, default CoS value, DSCP-to-DSCP-mutation map (if any) attached to the port, and policy map (if any) attached to the interface are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays output from the **show qos interface ethernet g1 buffers** command.

```
Console# show qos interface ethernet g1 buffers
Ethernet g1
Notify Q depth:
qid-size
1 - 125
2 - 125
3 - 125
4 - 125
5 - 125
6 - 125
7 - 125
8 - 125
qid     WRED     thresh0    thresh1    thresh2
1       disable  100        100        100
2       disable  100        100        100
3       disable  100        100        100
4       disable  100        100        100
5       Enable   N/A        N/A        N/A
6       Enable   N/A        N/A        N/A
7       Enable   N/A        N/A        N/A
8       Enable   N/A        N/A        N/A
qid   MinDP0   MaxDP0   ProbDP0 MinDP1   MaxDP1  ProbDP1 MinDP2  MaxDP2   ProbDP2weight
1     N/A      N/A      N/A     N/A      N/A     N/A     N/A     N/A      N/A     N/A
2     N/A      N/A      N/A     N/A      N/A     N/A     N/A     N/A      N/A     N/A
3     N/A      N/A      N/A     N/A      N/A     N/A     N/A     N/A      N/A     N/A
4     N/A      N/A      N/A     N/A      N/A     N/A     N/A     N/A      N/A     N/A
5     50       60       13      65       80      6       85      95       4       2
6     50       60       13      65       80      6       85      95       4       2
7     50       60       13      65       80      6       85      95       4       2
8 50 60 13 65 80 6 85 95 4 2
```

The following example displays output from the **show qos interface ethernet g1 queueing** command.

```
Console# show qos interface ethernet g1 queueing
Ethernet g1
wrr bandwidth weights and EF priority:
qid-weights Ef - Priority
1 - 125 dis- N/A
2 - 125 dis- N/A
3 - 125 dis- N/A
4 - 125 dis- N/A
5 - N/A ena- 5
6 - 125 dis- N/A
7 - 125 dis- N/A
8 - N/A ena- 8
Cos-queue map:
cos-qid
0 - 3
1 - 1
2 - 2
3 - 4
4 - 5
5 - 6
6 - 7
7 - 8
```

The following example displays output from the **show qos interface g1 shapers** command.

```
Console# show qos interface g1 shapers
Ethernet g1
Port shaper: enable
Committed rate: 192000 bps
Committed burst: 9600 bytes

                Target        Target
qid   Status    Committed     Committed
                Rate [bps]    Burst [bytes]
1     Enable    100000        17000
2     Disable   N/A           N/A
3     Enable    200000        19000
4     Disable   N/A           N/A
5     Disable   N/A           N/A
6     Disable   N/A           N/A
7     Enable    178000        8000
8     Enable    23000         1000
```

The following example displays output from the **show qos interface g1 policers** command.

```
Console# show qos interface ethernet g1 policers
Ethernet g1
Class map: A
Policer type: aggregate
Committed rate: 192000 bps
Committed burst: 9600 bytes
Exceed-action: policed-dscp-transmit

Class map: B
Policer type: single
Committed rate: 192000 bps
Committed burst: 9600 bytes
Exceed-action: drop

Class map: C
Policer type: none
Committed rate: N/A
Committed burst: N/A
Exceed-action: N/A
```

qos map dscp-queue

The **qos map dscp-queue** global configuration command modifies the DSCP to CoS map. To return to the default map, use the **no** form of this command.

Syntax

qos map dscp-queue *dscp-list to queue-id*

no qos map dscp-queue

- *dscp-list*—Specify up to 8 DSCP values, separate each DSCP with a space. (Range: 0 - 63)
- *queue-id*—Enter the queue number to which the DSCP value corresponds.

Default Configuration

The following table describes the default map.

DSCP value	0-7	8-15	16-23	24-31	32-39	40-47	48-56	57-63
Queue-ID	1	2	3	4	5	6	7	8

Command Mode

Global Configuration mode

User Guidelines

Queue settings for 3, 11, 19, ... cannot be modified.

Example

The following example maps DSCP values 33, 40 and 41 to queue 1.

```
Console (config)# qos map dscp-queue 33 40 41 to 1
```

qos map tcp-port-queue

The **qos map tcp-port-queue** global configuration command modifies the TCP-Port to Queue table. To delete table entries use the **no** form of this command. In the case where there are no ports specified and the **no** form of this command is used, the complete table is deleted.

Syntax

qos map tcp-port-queue *port1...port8* to *queue-id*

- **no qos map tcp-port-queue** [*port1...port8*]
- *port1...port8*—Specify up to 8 ports (destination ports) separated by commas that are being mapped. (Range: 1 - 65535)
- *queue-id*—Specify the queue number being mapped.

Default Configuration

The table is empty.

Command Mode

Global Configuration mode

User Guidelines

This command maps the TCP destination port in the ingress packet to a specified queue.

This map is used when the TCP trust mode is enabled and when trust command is enabled.

Example

The following example shows how the mapped TCP ports 2000 and 80 are modified to queue 2.

```
Console (config)# qos map tcp-port-queue 2000 80 to 2
```

qos map udp-port-queue

The **qos map udp-port-queue** global configuration command modifies the UDP-Port to DSCP table. To delete table entries, use the **no** form of this command. In the case where there are no ports specified and the **no** form of this command is used, the complete table is deleted.

Syntax

qos map udp-port-queue *port1...port8 to queue-id*

no qos map udp-port-queue *[port1...port8]*

- *port1...port8*—Specify up to 8 ports (destination ports) separated by commas that are being mapped. (Range: 1 - 65535)
- *queue-id*—Specify the queue number being mapped.

Default Configuration

The table is empty.

Command Mode

Global Configuration mode

User Guidelines

This command maps the UDP destination port in the ingress packet to a specified queue.

This map is used when the UDP trust mode is enabled and when the trust command is enabled.

Example

The following example shows how the mapped UDP ports 2000 and 80 are modified to queue 2.

```
Console (config)# qos map udp-port-queue 2000 80 to 2
```

wrr-queue cos-map

The **wrr-queue cos-map** global configuration command maps assigned CoS values to select one of the egress queues. To return to the default values, use the **no** form of this command.

Syntax

wrr-queue cos-map *queue-id cos1...cos*n

no wrr-queue cos-map [*queue-id*]

- *queue-id*—The queue number to which the following CoS values are mapped.
- *cos1...cos*n—Map to specific queues up to eight CoS values from 0 to 7.

Default Configuration

The map default values are as follows:

- CoS value 1 select queue 1
- CoS value 2 select queue 2
- CoS value 0 select queue 3
- CoS value 3 select queue 4
- CoS value 4 select queue 5
- CoS value 5 select queue 6
- CoS value 6 select queue 7
- CoS value 7 select queue 8

Command Mode

Global Configuration mode

User Guidelines

You can use this command to distribute traffic into different queues, where each queue is configured with different weighted round robin (WRR) and Weighted Random Early Detection (WRED) parameters.

You enable the expedite queues by using the **priority-queue out** interface configuration command **wrr-queue cos-map**.

Example

The following example maps CoS 3 to queue 7.

```
Console (config)# wrr-queue cos-map 7 3
```

show qos map

The show qos map user EXEC command displays all the QoS maps.

Syntax

show qos map [**dscp-queue** | **tcp-port-queue** | **udp-port-queue** | **policed-dscp** | **dscp-mutation**]

- **dscp-queue**—Displays the DSCP to queue map.
- **tcp-port-queue**—Displays the TCP Port to queue map.
- **udp-port-queue**—Displays the UDP Port to queue map.

- **policed-dscp**—Displays the DSCP to DSCP remark table.
- **dscp-mutation**—Displays the DSCP-DSCP mutation table.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC command

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the DSCP port-queue map.

```
Console# show qos map dscp-queue
Dscp-queue map:
d1 : d2 0  1   2  3   4   5   6   7   8   9
------------------------------------------------------
0 :     01  01  01  01  01  01  01  01  02  02
1 :     02  02  02  02  02  02  03  03  03  03
2 :     03  03  03  03  04  04  04  04  04  04
3 :     04  04  05  05  05  05  05  05  05  05
4 :     06  06  06  06  06  06  06  06  07  07
5 :     07  07  07  07  07  07  08  08  08  08
6 : 08 08 08 08
```

The following example displays the TCP port-queue map.

```
Tcp port-queue map:

Port     qid

-----    ------

6000     1

6001     2

6002     3
```

The following example displays the UDP port-queue map.

```
Udp port-queue map:

Port     qid

-----    -----

8000     1

8001     2
```

The following example displays the policed-DSCP map.

```
Policed-dscp map:

d1 : d2 0   1    2    3    4    5    6    7    8    9

--------------------------------------------------------

0 :    00   01   02   03   04   05   06   07   08   09

1 :    10   11   12   13   14   15   16   17   18   19

2 :    20   21   22   23   24   25   26   27   28   29

3 :    30   31   32   33   34   35   36   37   38   39

4 :    40   41   42   43   44   45   46   47   48   49

5 :    50   51   52   53   54   55   56   57   58   59

6 :    60   61   62   63
```

The following example displays the DSCP-mutation map.

```
Dscp-dscp mutation map:
d1 : d2 0    1    2    3    4    5    6    7    8    9
-------------------------------------------------------
0 :     00   01   02   03   04   05   06   07   08   09
1 :     10   11   12   13   14   15   16   17   18   19
2 :     20   21   22   23   24   25   26   27   28   29
3 :     30   31   32   33   34   35   36   37   38   39
4 :     40   41   42   43   44   45   46   47   48   49
5 :     50   51   52   53   54   55   56   57   58   59
6 :     60   61   62   63
```

qos trust (Global)

The **qos trust** global configuration command can be used in basic mode to configure the system to "trust" state. To return to the default state, use the **no** form of this command.

Syntax

qos trust {cos | dscp |tcp-udp-port}

no qos trust

- cos—Classifies ingress packets with the packet CoS values. For untagged packets, the port default CoS is used.
- dscp—Classifies ingress packets with the packet DSCP values.
- tcp-udp-port—Classifies ingress packets with the packet destination port values.

Default Configuration

If the system is in basic mode then CoS is the default trust mode.

Command Mode

Global Configuration mode

User Guidelines

This command can be used only in QoS basic mode.

Packets entering a quality of service (QoS) domain are classified at the edge of the QoS domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain.

Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

For an inter-QoS domain boundary, the port can be configured to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map, if the DSCP values are different between the QoS domains.

To return to the untrusted state, use the **no qos** command to apply best effort service.

Example

The following example configures the system in basic mode to DSCP trust state.

```
Console (config)# qos trust dscp
```

qos trust (Interface)

The **qos trust** interface configuration command enables each port trust state while the system is in basic mode. To disable the trust state on each port, use the **no** form of this command.

Syntax

qos trust

no qos trust

Default Configuration

Each port is enabled while the system is in basic mode.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

Use **no qos trust** to disable the trust mode on each port.

Use **qos trust** to enable trust mode on each port.

Example

The following example configures port g5 in basic mode to default trust state (CoS).

```
Console (config)# interface ethernet g5
Console (config-if) qos trust
```

qos cos

The **qos cos** interface configuration command configures the default port CoS value. To return to the default setting, use the **no** form of this command.

Syntax

qos cos *default-cos*

no qos cos

- *default-cos*—Specifies the default CoS value being assigned to the port. If the port is trusted and the packet is untagged then the default CoS value becomes the CoS value. (Range: 0 - 7)

Default Configuration

Port CoS is 0.

Command Mode

Interface Configuration (Ethernet, port-channel) command

User Guidelines

There are no user guidelines for this command.

Example

The following example configures port g5 default CoS value to 3.

```
Console (config)# interface ethernet g5

Console (config-if) qos cos 3
```

qos dscp-mutation

The **qos dscp-mutation** global configuration command applies the DSCP Mutation map to system DSCP trusted ports. To return to the trust port with no DSCP mutation, use the **no** form of this command.

Syntax

qos dscp-mutation

no qos dscp-mutation

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

The DSCP-to-DSCP-mutation map is applied to a port at the boundary of a quality of service (QoS) administrative domain. If two QoS domains have different DSCP definitions between them, the DSCP-to-DSCP-mutation map is used to translate a set of DSCP values to match the definition of another domain. The map is applied only to ingress and to DSCP-trusted ports. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress ports.

Example

The following example applies the DSCP Mutation map to system DSCP trusted ports.

```
Console (config)# qos dscp-mutation
```

qos map dscp-mutation

The **qos map dscp-mutation** global configuration command modifies the DSCP values to the DSCP mutation map values. To return to the default mutation-map, use the **no** form of this command.

Syntax

qos map dscp-mutation *in-dscp to out-dscp*

no qos map dscp-mutation

- *in-dscp*—Specifies up to 8 DSCP values to be mutated, separate each DSCP with a space. (Range: 0-63)
- *out-dscp*—Specifies up to 8 DSCP values to be mutated, separate each DSCP with a space. (Range: 0-63)

Default Configuration

The default map is "Null" map, which means that each income DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example modifies the DSCP values 1 2 4 5 6 to the DSCP mutation map value 64.

```
Console (config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

qos aggregate-policer

The **qos aggregate-policer** global configuration command defines the policer parameters that can be applied to multiple traffic classes within the same policy map. To remove an existing aggregate policer use the **no** form of this command.

Syntax

qos aggregate-policer *aggregate-policer-name committed-rate-kbps excess-burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]

no qos aggregate-policer

- *aggregate-policer-name*—The aggregate policer name.
- *committed-rate-kbps*—The average traffic rate (CIR) in kilo bits per second (bps).
- *committed-burst-byte*—The normal burst size (CBS) in bytes.
- **exceed-action drop**—Specifies the action to take when rate is exceeded, which is to drop the packet.
- **exceed-action policed-dscp-transmit**—Specifies the action to take when rate is exceeded, which is to remark the packet DSCP according to policed-DCP map.
- **dscp** *dscp*—The value that the DSCP is remarked. Relevant only if **exceed-action** is **policed-dscp-transmit**.

Default Configuration

By default, no aggregate policer is defined.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines the aggregate meter "policer1". When the average traffic rate exceeds 124000 bps, or the normal burst size exceeds 96000 bps, the packet is dropped.

```
Console (config)# qos aggregate-policer policer1 124000 96000
exceed-action drop
```

show qos aggregate-policer

The **show qos aggregate-policer** user EXEC command displays the aggregate policer parameter.

Syntax

show qos aggregate-policer [*aggregate-policer-name*]

- *aggregate-policer-name*—The aggregate policer name being displayed.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the aggregate policer called "policer1".

```
Console# show qos aggregate-policer policer1

aggregate-policer policer1 96000 4800 exceed-action drop

not used by any policy map
```

qos map policed-dscp

The **qos map policed-dscp** global configuration command modifies the policed-DSCP map for remarking purposes. To return to the default map, use the **no** form of this command.

Syntax

qos map policed-dscp *dscp-list to dscp-mark-down*

no qos map policed-dscp

- *dscp- list*—Specifies up to 8 DSCP values separated by spaces. (Range: 0 - 63)
- *dscp-mark-down*—Specifies the DSCP value to mark down. (Range: 0 - 63)

Default Configuration

The default map is the "Null" map, which means that each income DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode

User Guidelines

The DSCP cannot be remapped to 3, 11, 19, ...

Example

The following example maps DSCP values 12 and 58 to value 56 while out of profile.

```
Console (config)# qos map policed-dscp 12 58 to 56
```

class-map

The **class-map** global configuration command creates class maps and enters the class-map configuration mode. To delete a class, use the **no** form of this command.

Syntax

class-map *class-map-name* [**match-all | match-any**]

no class-map *class-map-name*

- *class-map-name*—Specifies the class-map name consisting of a character string 32 characters long.
- **match-all**—Performs a logical AND condition on the IP and MAC ACLs in the class map. All criteria within all the individual ACLs must be matched.
- **match-any**—Performs the logical OR condition, which requires that all the criteria within any ACL in the class does not have to be matched. It is sufficient for one criterion to be matched.

Default Configuration

If neither the **match-all** or **match-any** is specified, the default is **match-all**.

Command Mode

Global Configuration mode

User Guidelines

An error message is generated if there is more than one match statement in a match all class map, and if there is a repetitive classification field in the participation ACL.

In quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **exit**—Exits from QoS class-map configuration mode.
- **match—**Configures classification criteria.
- **no**—Removes a match statement from a class map.

Example

The following example creates a class-map named "class1" which requires all ACE’s to be matched.

```
Console (config)# class-map class1 match-all
Console (config-cmap)#
```

show class-map

The **show class-map** user EXEC command displays all the class-maps configured on the device.

Syntax

show class-map [*class-map-name*]

- *class-map-name*—Specifies the class-map name being displayed.

Default Configuration

If no name is requested all the class-maps are displayed.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the class-map called "class1".

```
Console> show class-map class1
Class Map match-any class1 (id4)
```

match

The **match** class-map configuration command defines the match criterion to classify traffic. To delete the match criterion use **no** form of this command.

Syntax

match access-group *acl-name*

no match access-group *acl-name*

- *acl-name*—Specifies the access list ACL MAC/IP name.

Default Configuration

By default, no match criterion is supported.

Command Mode

Class-map Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines the match criterion as the access-group named "dell". The access-group is in a class map called "class1".

```
Console (config)# class-map class1
Console (config-cmap)# match access-group dell
```

policy-map

The **policy-map** global configuration command creates policy maps and enters policy map configuration mode. To delete a policy map, use the **no** form of this command.

Syntax

policy-map *policy-map-name*

no policy-map *policy-map-name*

- *policy-map-name*—Specifies the policy map name.

Default Configuration

The default behavior of the policy map is to set the DSCP value to 0 for IP packets, and to set the CoS value to 0 if the packet is tagged.

Command Mode

Global Configuration mode

User Guidelines

Before you configure policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified.

Entering the **policy-map** command enables the policy-map configuration mode in which the class policies for that policy map can be configured or modified.

Class policies can be configured in a policy map only if the classes have defined match criteria. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. Only one policy map per interface per direction is supported. The same policy map can be applied to multiple interfaces and directions.

The **service-policy** interface configuration command cannot be used to attach policy maps that contain **set** or **trust** policy-map class configuration commands or that have access control list (ACL) classification to an egress interface. The only match criterion supported is **match ip dscp** *dscp-lis*t. For non-IP packets, the final CoS is converted to DSCP for classification purposes. If there is an attempt to apply a policy map on an egress interface with anything other than the **match ip dscp** class-map configuration command, an error message is generated.

Example

The following example creates policy map called "policy1".

```
Console (config)# policy-map policy1

Console (config-pmap)#
```

show policy-map

The **show policy-map** user EXEC command displays the defined policy maps.

Syntax

show policy-map [*policy-map-name* [**class** *class-name*]]

- *policy-map-name*—The policy map name being displayed.
- **class** *class-name*—Displays the QoS policy action for individual classes.

Default Configuration

If a specific policy-map is not requested, all policy-maps are displayed.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all policy-maps.

```
Console> show policy-map
Policy Map policy1
class class1
set dscp 7
Policy Map policy2
class class2
police 96000 4800 exceed-action drop
class class3
police 124000 96000 exceed-action policed-dscp-transmit
```

class

The **class** policy-map configuration command defines the traffic classification and enters the policy-map class configuration mode. To delete the class map, use the **no** form of this command.

Syntax

class *class-map-name* [**access-group** *acl-name*]

no class *class-map-name*

- *class-map-name*—Specifies a class-map name.
- **access-group**—If a new class is created, the *acl-name* specifies the name of the access IP/MAC list ACL.

Default Configuration

By default, no policy-map class-maps are defined.

Command Mode

Policy-map Configuration mode

User Guidelines

Use the **policy-map** global configuration command to identify the policy-map and to enter Policy-map Configuration mode before using the **class** command. After specifying a policy-map, a policy for new classes can be configured or a policy for any existing classes in that policy-map can be modified. Attach the policy-map to an interface by using the **service-policy** interface configuration command. Use an existing class-map to attach the classification characteristics to the specified policy-map, and to modify the match criteria within the class-map by using the access-group option.

If a new class-map name is used, it is automatically created, but then the access-group must be created.

Example

The following example defines a traffic classification named "class1" with an access-group called "dell". The class is in a policy map called "policy1".

```
Console (config)# policy-map policy1

Console (config-pmap)# class class1 access-group dell
```

police

The **police** policy-map class configuration command defines a policer for classified traffic. To remove an existing policer, use the **no** form of this command.

Syntax

police *committed-rate-kbps committed-burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit** }]

no police

- *committed-rate-kbps*—The average traffic rate (CIR) in kilo bits per second(bps).
- *committed-burst-byte*—The normal burst size (CBS) in bytes.
- **exceed-action drop**—Specifies action taken when the rate is exceed, which is to drop the packet.
- **exceed-action policed-dscp-transmit**—Specifies the action taken when the rate is exceeded, which is to remark the DSCP of the packet according to policed-DSCP map.

Default Configuration

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

User Guidelines

Policing uses a token bucket algorithm. CIR represents how fast the token is removed from the bucket. CBS represents the depth of the bucket.

Example

The following example defines a policer for classified traffic. When the average traffic rate exceeds 124000 bps or the normal burst size exceeds 96000 bps, the packet is dropped. The class is in a policy map called "policy1".

```
Console (config)# policy-map policy1

Console (config-pmap)# class class1

Console (config-pmap-c)# police 124000 9600 exceed-action drop
```

police aggregate

The **police aggregate** policy-map class configuration mode command applies an aggregate policer to multiple classes within the same policy map. To remove an existing aggregate policer from a policy map, use the **no** form of this command.

Syntax

police aggregate *aggregate-policer-name*

no police aggregate

- *aggregate-policer-name*—Specifies the name of an existing aggregate policer defined in the **qos aggregate-policer** command.

Default Configuration

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

User Guidelines

An aggregate policer cannot be used across different policy maps or interfaces.

Example

The following example sets the aggregate meter "policer1" to a class-map. The class is in a policy map called "policy1".

```
Console (config)# policy-map policy1

Console (config-pmap)# class class1

Console (config-pmap-c)# police aggregate policer1
```

trust

The **trust** policy-map class configuration command configures the trust state. The trust state selects the value QoS uses as the source of the internal DSCP value from the packet. To return to the default trust state, use the **no** form of this command.

Syntax

trust [**cos** | **dscp** | **tcp-udp-port**]

no trust

- **cos**—QoS sets the queue according to CoS to Queue Map.
- **dscp**—QoS derives the internal DSCP value by using the DSCP value from the ingress packet.
- **tcp-udp-port**—QoS derives the internal DSCP value by using the destination port value from the ingress packet, and the tcp-udp-port-to-DSCP-map.

Default Configuration

By default, the port is not trusted. If the **trust** keyword is alone then the default value is **dscp**.

Command Mode

Policy-map Class Configuration mode

User Guidelines

This command is used to distinguish the quality of service (QoS) trust behavior for certain traffic from others. For example, incoming traffic with certain DSCP values can be trusted. A class-map can be configured to match and trust the DSCP values in the incoming traffic.

NOTE: Policy-maps that contain set or trust commands, or have ACL classification, cannot be attached to an egress interface by using the service-policy interface configuration command.

Trust values set with this command supersede trust values set on specific interfaces with the **qos trust (Interface)** interface configuration command.

If specifying **trust cos**, QoS maps a packet to a queue using the received or default port CoS value and the CoS-to-queue map.

If specifying **trust dscp**, QoS maps the packet by using the DSCP value from the ingress packet.

If specifying **tcp-udp-port**, QoS maps the packet to a queue by using the TCP\UDP port value from the ingress packet and the tcp-udp-port-to-queue map.

Example

The following example configures the trust state to CoS. The class is in a policy map called "policy1".

```
Console (config)# policy-map policy1
Console (config-pmap)# class class1
Console (config-pmap-c)# trust cos
```

set

The **set** policy-map class configuration command sets new values in the IP packet. To remove the value, use the **no** form of this command.

Syntax

set {**dscp** *new-dscp* | **queue** *queue-id* | **cos** *new-cos*}

no set

- **dscp** *new-dscp*—Enter a new DSCP value for classified traffic. (Range: 0 - 63)
- **queue** *queue-id*—Enter explicit queue ID to set the egress queue.
- **cos** *new-cos*—Enter new user priority for marking in the packet. (Range: 0 - 7)

Default Configuration

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

User Guidelines

NOTE: Policy-maps that contain set or trust commands, or have ACL classification, cannot be attached to an egress interface by using the service-policy interface configuration command.

Example

The following example sets a new DSCP value in the packet to 56. The class is in a policy map called "policy1".

```
Console (config)# policy-map policy1
Console (config-pmap)# set dscp 56
```

service-policy

The **service-policy** interface configuration command applies a policy map to the interface input. To detach the policy map from an interface, use the **no** form of this command.

Syntax

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

- **input** *policy-map-name*—Specifies the policy-map being applied to an input interface.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration mode

User Guidelines

The service-policy interface configuration command cannot be used to attach policy maps that contain set or trust policy-map class configuration commands or that have access control list (ACL) classification to an egress interface. The only match criterion supported on an egress interface is match ip dscp dscp-list. For non-IP Packets, the final CoS is converted to DSCP for classification purposes. If there is an attempt to apply a policy map on an egress interface with anything other than the match ip dscp class-map configuration command, an error message is generated.

NOTE: Only one policy map per interface per direction is supported.

Example

The following example attaches policy map "policy1" to the input interface.

```
Console (config-if)# service-policy input policy1
```

23

Radius Commands

radius-server host

The **radius-server host** global configuration command specifies a RADIUS server host. To delete the specified RADIUS host, use the **no** form of this command.

Syntax

radius-server host *ip-address* [**auth-port** *auth-port-number*] [**timeout** *timeout*] [**retransmit** *retransmit*] [**deadtime** *deadtime*] [**key** *key*] [**source** *source*] [**priority** *priority*] [**usage** *type*]

no radius-server host *ip-address*

- *ip-address*—The RADIUS server host IP address.
- *auth-port-number*—Port number for authentication requests. The host is not used for authentication if set to 0. If unspecified, the port number defaults to 1812. (Range: 0 - 65535)
- *timeout*—Specifies the timeout value in seconds. If no timeout value is specified, the global value is used. (Range: 1 - 30)
- *retransmit*—Specifies the re-transmit value. If no re-transmit value is specified, the global value is used. (Range: 1 -10)
- *deadtime*—Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests. (Range 0 - 2000)
- *key*—Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. If no key value is specified, the global value is used.
- *source*—Specifies the source IP address to use for the communication. If no retransmit value is specified, the global value is used.
- *priority*—Determines the order in which the servers are used, where 0 is the highest priority. (Range: 0 - 65535)
- *type*—Specifies the usage type of the server. Possible values: **login**, **802.1x** and **all**.

Default Configuration

No RADIUS host is specified.

If no usage type is specified, the usage type is **all**.

Command Mode

Global Configuration mode

User Guidelines

To specify multiple hosts, multiple **radius-server host** commands can be used.

If no host-specific timeout, retransmit, deadtime or key values are specified, the global values apply to each host.

To define a radius server on the out-of-band port, use the out-of-band IP address format — **oob/ip-address**.

Example

The following example specifies a RADIUS server host with the following characteristics:

- Server host IP address—192.168.10.1
- Authentication port number—20
- Timeout period—20 seconds

```
Console (config)# radius-server host 192.168.10.1 auth-port 20
timeout 20
```

radius-server key

The **radius-server key** global configuration command sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon. To reset to the default, use the **no** form of this command.

Syntax

radius-server key *[key-string]*

no radius-server key

- *key-string*—Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. The key can be up to 128 characters long.

Default Configuration

The default is an empty string.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon to "dell-server".

```
Console (config)# radius-server key dell-server
```

radius-server retransmit

The **radius-server retransmit** global configuration command specifies the number of times the software searches the list of RADIUS server hosts. To reset the default configuration, use the **no** form of this command.

Syntax

radius-server retransmit *retries*

no radius-server retransmit

- *retries*—Specifies the retransmit value. (Range: 1 - 10)

Default Configuration

The default is 3 attempts.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the number of times the software searches the list of RADIUS server hosts to 5 attempts.

```
Console (config)# radius-server retransmit 5
```

radius-server source-ip

The **radius-server source-ip** global configuration command specifies the source IP address used for communication with RADIUS servers. To return to the default, use the **no** form of this command.

Syntax

radius-server source-ip *source*

no radius-server-ip

- *source*—Specifies the source IP address.

Default Configuration

The default IP address is the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

To define an out-of-band IP address, use the out-of-band IP address format —**oob/ip-address**.

Example

The following example configures the source IP address used for communication with RADIUS servers to 10.1.1.1.

```
Console (config)# radius-server source-ip 10.1.1.1
```

radius-server timeout

The **radius-server timeout** global configuration command sets the interval for which a router waits for a server host to reply. To restore the default, use the **no** form of this command.

Syntax

radius-server timeout *timeout*

no radius-server timeout

- *timeout*—Specifies the timeout value in seconds. (Range: 1 - 30)

Default Configuration

The default value is 3 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the interval for which a router waits for a server host to reply to 5 seconds.

```
Console (config)# radius-server timeout 5
```

radius-server deadtime

The **radius-server deadtime** global configuration command improves RADIUS response times when servers are unavailable. The command is used to cause the unavailable servers to be skipped. To reset the default value, use the **no** form of this command.

Syntax

radius-server deadtime *deadtime*

no radius-server deadtime

- *deadtime*—Length of time in minutes, for which a RADIUS server is skipped over by transaction requests. (Range: 0 - 2000)

Default Configuration

The default dead time is 0 minutes.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets a dead time where a RADIUS server is skipped over by transaction requests for this period, to 10 minutes.

```
Console (config)# radius-server deadtime 10
```

show radius-servers

The show radius-servers user EXEC command displays the RADIUS server settings.

Syntax

show radius-servers

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the RADIUS server settings.

```
Console# show radius-servers
IP address     Auth  Acct   TimeOut   Retransmit  deadtime  source IP  Priority
-------------- ---- ------- --------- ----------- -------- --------   -------
172.16.1.1     1645  1646    3          3           0   172.16.8.1      1
172.16.1.2     1645  1646    1          18          0   172.16.8.1      2


Global values
--------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IP: 172.16.8.1
```

24

RIP Commands

router rip enable

The **router rip** global configuration command enables the Routing Information Protocol (RIP) on the device. To disable the RIP routing process, use the **no** form of this command.

Syntax

router rip enable

no router rip enable

Default Configuration

RIP is disabled on the device.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables RIP on the device.

```
Console (config)# router rip enable
```

router rip redistribute ospf

The **router rip redistribute ospf** global configuration command advertises routes learned by OSPF in the RIP process. To disable advertisements, use the **no** form of this command.

Syntax

router rip redistribute ospf

no router rip redistribute ospf

Default Configuration

Routes learned by OSPF are not advertised in the RIP process (Disabled).

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables routes learned by OSPF in the RIP process to be advertised.

```
Console (config)# router rip redistribute ospf
```

router rip redistribute static

The **router rip redistribute static** global configuration command enables statically configured routes to advertise in the RIP process. To disable advertisements, use the **no** form of this command.

Syntax

router rip redistribute static

no router rip redistribute static

Default Configuration

Routes statically configured are not advertised in the RIP process (Disabled).

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables statically configured routes to advertise in the RIP process.

```
Console(config)# router rip redistribute static
```

rip

The **rip** interface configuration command creates a Routing Information Protocol (RIP) process on an interface. To disable RIP on an interface, use the **no** form of this command.

Syntax

rip

no rip

Default Configuration

RIP is not created.

Command Mode

IP Interface Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables RIP on IP address 100.1.1.1.

```
Console(config)# interface ip 100.1.1.1

Console(config-ip)# rip
```

rip passive-interface

The **rip passive-interface** interface configuration command disables the sending of routing updates on an interface. To re-enable the sending of routing updates, use the **no** form of this command.

Syntax

rip passive-interface

no rip passive-interface

Default Configuration

Routing updates are sent.

Command Mode

IP Interface Configuration mode

User Guidelines

If the sending of routing updates on an interface is disabled, the particular subnet continues to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

Example

The following example disables the sending of routing updates on IP address 100.1.1.1.

```
Console(config)# interface ip 100.1.1.1

Console(config-ip)# rip passive interface
```

rip auto-send

The **rip auto-send** interface configuration command automatically detects if RIP information is required to be sent on the interface. To disable the detection, use the **no** form of this command.

Syntax

rip auto-send

no rip auto-send

Default Configuration

RIP auto-send is enabled.

Command Mode

IP Interface Configuration mode

User Guidelines

If auto-send is enabled on an interface, the router only advertises the default route on the interface, until a RIP message is received. When a RIP message is received, the complete RIP information is sent.

Example

The following example automatically detects whether RIP information is required to be sent on IP address 100.1.1.1.

```
Console(config)# interface ip 100.1.1.1
Console(config-ip)# rip auto-send
```

rip version

The **rip version** interface configuration command specifies a Routing Information Protocol (RIP) version. To return to the default use the **no** form of this command.

Syntax

rip version {1 | 2}

no rip version

- Use RIP Version 1 on the interface.
- Use RIP Version 2 on the interface.

Default Configuration

RIP Version 1 is used on the interface.

Command Mode

IP Interface Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies a RIP version 1 on IP address 100.1.1.1.

```
Console(config)# interface ip 100.1.1.1
Console(config-ip)# rip version 1
```

rip offset

The **rip offset** interface configuration command adds an offset to a metric learned via Routing Information Protocol (RIP) before adding it to the interface table. To return to the default, use the **no** form of this command.

Syntax

rip offset *offset*

no rip offset

- *offset*—Offset being applied. (Range: 1 - 15)

Default Configuration

The default offset value is 1.

Command Mode

IP Interface Configuration mode

User Guidelines

This option is used to make the device prefer RIP routes learned from the specific interfaces less than RIP routes from other interfaces.

Example

The following example applies an offset of 5 to a metric learned via RIP before adding it to the interface table on IP address 100.1.1.1.

```
Console(config)# interface ip 100.1.1.1
Console(config-ip)# rip offset 5
```

rip default-route originate

The rip default-route originate interface configuration command generates a metric for a default route into RIP. To disable this feature, use the no form of this command.

Syntax

rip default-route originate metric

no rip default-route originate

- metric—Metric for a default route. (Range: 1- 15)

Default Configuration

By default, the feature is enabled.

Command Mode

IP Interface Configuration mode

User Guidelines

This command is equivalent to rip default-route offset. Note that this is an origination of a default route with the given metric. Setting the value of the metric to 0 is the same as negating the command. An interface on which this command has been configured does not accept "default route" advertisement, in order to prevent a possible loop on the default route.

Example

The following example applies a metric of 5 to generate a default route to RIP on IP address 100.1.1.1

```
Console(config)# interface ip 100.1.1.1

Console(config-ip)# rip default-route originate 5
```

rip default-route offset

The **rip default-route offset** interface configuration command generates an offset for a default route into RIP. To disable this feature, use the **no** form of this command.

Syntax

rip default-route offset *offset*

no rip default-route offset

- *offset*—Offset being applied. (Range: 0- 15)

Default Configuration

By default, the feature is enabled.

Command Mode

IP Interface Configuration mode

User Guidelines

This command is equivalent to **rip default-route originate**. Note that this is an origination of a default route with the given metric. Setting the value of the metric to 0 is the same as negating the command. An interface on which this command has been configured does not accept **default route** advertisement, in order to prevent a possible loop on the default route.

NOTE: This command will be deprecated in a future version.

Example

The following example applies an offset of 5 to generate a default route to RIP on IP address 100.1.1.1.

```
Console(config)# interface ip 100.1.1.1

Console(config-ip)# rip default-route offset 5
```

rip authentication

The **rip authentication** interface configuration command enables authentication for Routing Information Protocol (RIP) Version 2 packets and specifies the authentication type. To prevent authentication, use the **no** form of this command.

Syntax

rip authentication {**text** *text* | **md5** *name-of-chain* }

no rip authentication

- **text** *text*—Clear text authentication. The string can contain from 1 to 16 uppercase and lowercase alphanumeric characters.
- **md5** *name-of-chain*—Keyed Message Digest 5 (MD5) authentication.

Default Configuration

No authentication is provided for RIP packets.

Command Mode

IP Interface Configuration mode

User Guidelines

It is possible to configure undefined keys for authentication, with the assumption that they will later be defined. In such cases, a message is generated stating that the key does not exist.

Example

The following example enables RIP clear text authentication with the password "dell" on the IP address 100.1.1.1.

```
Console(config)# interface ip 100.1.1.1

Console(config-ip)# rip authetication text dell
```

show ip rip

The **show ip rip** privileged EXEC command displays RIP routing information.

Syntax

show ip rip

show ip rip md5

show ip rip statistics

show ip rip peer

- **md5**—Displays MD5 authentication information.
- **statistics**—Displays statistics information.
- **peer**—Displays peer information.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays IP RIP information.

```
Console# show ip rip

RIP is enabled.

OSPF leaking is enabled.

Static leaking is enabled.

InterfaceVerOffsetDefaultPassiveAutoAuth

RouteSend

--------------------------------------------------

176.16.0.0/1621DisabledNoYesMD5

192.168.0.0/1621DisabledNoNoText
```

The following example displays IP RIP MD5 information.

```
Console# show ip rip md5

Interface       MD5 Authentication key chain

---------       -----------------------------------

176.16.0.0/16   keychain1
```

The following example displays IP RIP statistics.

```
Console# show ip rip statistics

Interface        Received    Received    Sent
                  Bad Packets  Bad Routes   Updates

-----------      -----------    ---------    ----------

176.16.0.0/16     0              1             8

192.168.0.0/16    0              0             7
```

The following table describes the fields shown in the display:

Field	Description
Interface	The interface IP Address.
Received Bad Packets	The number of RIP response packets received by the RIP process which were subsequently discarded for any reason (for example, a version 0 packet, or an unknown command type).
Received Bad Routes	The number of routes, in valid RIP packets, which were ignored for any reason (for example, unknown address family, or invalid metric).
Sent Updates	The number of triggered RIP updates actually sent on this interface. This explicitly does NOT include full updates sent containing new information.

The following example displays IP RIP peer information.

```
Console# show ip rip peer
Address      Route  Last Update Version Received     Received
             Tag                        Bad Packets  Bad Routes
----------   ------ ------------------- ------------ ----------
176.16.1.1           10:00:17           20            1
192.168.1.1          10:00:27           20            0
```

The following table describes the fields shown in the display:

Field	Description
Address	The peer IP Address.
Route Tag	The value in the Routing Domain field in RIP packets received from the peer.
Last Update	Time left since the most recent RIP update was received from this system.
Version	The RIP version number in the header of the last RIP packet received.
Received Bad Packets	The number of RIP response packets from this peer discarded as invalid.
Received Bad Routes	The number of routes from this peer that were ignored because the entry format was invalid.

25

RMON Commands

show rmon statistics

The **show rmon statistics** user EXEC command displays RMON Ethernet Statistics.

Syntax

show rmon statistics {**ethernet interface number** | **port-channel** *port-channel-number*}

- *interface*—Valid Ethernet port.
- *port-channel-number*—Valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays RMON Ethernet Statistics for port g1.

```
Console# show rmon statistics ethernet g1
Port g1
Dropped: 8
Octets: 878128 Packets: 978
Broadcast: 7 Multicast: 1
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 98 65 to 127 Octets: 0
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

The following table describes the significant fields shown in the display:

Field	Description
Dropped	The total number of events in which packets are dropped by the probe due to lack of resources. This number is not always the number of packets dropped; it is the number of times this condition has been detected.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The total number of packets (including bad packets, Broadcast packets, and Multicast packets) received.
Broadcast	The total number of good packets received and directed to the Broadcast address. This does not include Multicast packets.
Multicast	The total number of good packets received and directed to a Multicast address. This number does not include packets directed to the Broadcast address.
CRC Align Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize Pkts	The total number of packets received less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
Oversize Pkts	The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	The total number of packets received less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Jabbers	The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Octets	The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128 to 255 Octets	The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

256 to 511 Octets	The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	The total number of packets (including bad packets) received that are between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to 1518 Octets	The total number of packets (including bad packets) received that are between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

rmon collection history

The **rmon collection history** interface configuration command enables a Remote Monitoring (RMON) MIB history statistics group on an interface. To remove a specified RMON history statistics group, use the **no** form of this command.

Syntax

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history *index*

- *index*—The requested statistics index group. (Range: 1 - 65535)
- **owner** *ownername*—Records the RMON statistics group owner name. If unspecified, the name is an empty string. (Range: 1-159 characters)
- **buckets** *bucket-number*—A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50. (Range: 1 - 65535)
- **interval** *seconds*—The number of seconds in each polling cycle. If unspecified, defaults to 1800. (Range: 1 - 3600)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command cannot be executed on multiple ports using the **interface range ethernet** command.

Example

The following example enables a Remote Monitoring (RMON) MIB history statistics group on port g8 with the index number "1" and a polling interval period of 2400 seconds.

```
Console (config)# interface ethernet g8
Console (config-if)# rmon collection history 1 interval 2400
```

show rmon collection history

The **show rmon collection history** user EXEC command displays the requested history group configuration.

Syntax

show rmon collection history [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface*—Valid Ethernet port.
- *port-channel-number*—Valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all RMON group statistics.

```
Console# show rmon collection history


Index Interface Interval Requested Samples Granted Samples Owner
----- --------- -------- ----------------- --------------- -------
  1       1       1000          50                50            CLI
```

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled Ethernet interface
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry.

show rmon history

The **show rmon history** user EXEC command displays RMON Ethernet Statistics history.

Syntax

show rmon history *index* {**throughput** | **errors** | **other**} [**period** *seconds*]

- *index*—The requested set of samples. (Range: 1 - 65535)
- **throughput**—Displays throughput counters.
- **errors**—Displays error counters.
- **other**—Displays drop and collision counters.
- **period** *seconds*—Specifies the requested period time to display. (Range: 1 - 4294967295)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays RMON Ethernet Statistics history for "throughput" on index number 5.

```
Console# show rmon history 5 throughput

Sample Set: 5                Owner: cli

Interface:  24               interval: 10

Requested samples: 50        Granted samples: 50

Maximum table size: 270

Time                 Octets   Packets    Broadcast   Multicast   %

-------------------- ------- ----------- ----------- ----------- -

09-Mar-2005 18:29:32   0        0          0            0        0

09-Mar-2005  18:29:42  0        0          0            0        0

09-Mar-2005  18:29:52  0        0          0            0        0

09-Mar-2005  18:30:02  0        0          0            0        0

09-Mar-2005  18:30:12   0       0          0            0        0

09-Mar-2005  18:30:22   0       0          0            0        0
```

The following example displays RMON Ethernet Statistics history for "errors" on index number 5.

```
Console# show rmon history 5 errors

Sample Set: 5                      Owner: cli

Interface:  24                     interval: 10

Requested samples: 50              Granted samples: 50

Maximum table size: 270


Time         CRC Align  Undersize  Oversize   Fragments  Jabbers 0

----------   ---------  ---------  ---------  ---------  --------

09-Mar-2005  0          0          0          0          0
18:29:32

09-Mar-2005  0          0          0          0          0
18:29:42
```

The following example displays RMON Ethernet Statistics history for "other" on index number 1.

```
Console# show rmon history 1 other
Sample Set: 1               Owner: CLI
Interface:  1               interval: 10
Requested samples: 50       Granted samples: 50
Maximum table size: 270
Time                    Dropped   Collisions
-------------------- ----------- -----------
10-Mar-2005  22:06:00      0           0
10-Mar-2005  22:06:10      0           0
10-Mar-2005  22:06:20      0           0
```

The following table describes the significant fields shown in the display:

Field	**Description**
Time	Date and Time the entry is recorded.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The number of packets (including bad packets) received during this sampling interval.
Broadcast	The number of good packets received during this sampling interval that were directed to the Broadcast address.
Multicast	The number of good packets received during this sampling interval that were directed to a Multicast address. This number does not include packets addressed to the Broadcast address.
Utilization%	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
Oversize	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.

Fragments	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (AlignmentError). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Dropped	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected.
Collisions	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

rmon alarm

The **rmon alarm** global configuration command configures alarm conditions. To remove an alarm, use the **no** form of this command.

Syntax

rmon alarm *index variable interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup** *direction*] [**owner** *name*]

no rmon alarm *index*

- *index*—The alarm index. (Range: 1 - 65535)
- *variable*—The object identifier of the particular variable to be sampled.
- *interval*—The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. (Range: 1 - 4294967295)
- *rthreshold*—Rising Threshold. (Range: 1 - 4294967295)
- *fthreshold*—Falling Threshold. (Range: 1 - 4294967295)
- *revent*—The Event index used when a rising threshold is crossed .(Range: 1- 65535)
- *fevent*—The Event index used when a falling threshold is crossed. (Range: 1- 65535)
- **type** *type*—The sampling method for the selected variable and calculating the value to be compared against the thresholds. If the method is **absolute**, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the method is **delta**, the selected variable value at the last sample is subtracted from the current value, and the difference compared with the thresholds.

- **startup** *direction*—The alarm that may be sent when this entry is first set to valid. If the first sample (after this entry becomes valid) is greater than or equal to the *rthreshold*, and *direction* is equal to **rising** or **rising-falling**, then a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to the *fthreshold*, and *direction* is equal to **falling** or **rising-falling**, then a single falling alarm is generated.
- **owner** *name*—Enter a name that specifies who configured this alarm. If unspecified, the name is an empty string.

Default Configuration

The following parameters have the following default values:

- **type** *type*—If unspecified, the type is **absolute**.
- **startup** *direction*—If unspecified, the startup direction is **rising-falling**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the following alarm conditions:

- Alarm index—1000
- Variable identifier—dell
- Sample interval—360000 seconds
- Rising threshold—1000000
- Falling threshold—1000000
- Rising threshold event index—10
- Falling threshold event index—20

```
Console (config)# rmon alarm 1000 dell 360000 1000000 1000000 10
20
```

show rmon alarm-table

The **show rmon alarm-table** user EXEC command displays the alarms summary table.

Syntax

show rmon alarm-table

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the alarms summary table.

```
Console# show rmon alarm-table
Index   OID                     Owner
-----   ----------------------- -------
1       1.3.6.1.2.1.2.2.1.10.1  CLI
2       1.3.6.1.2.1.2.2.1.10.1  Manager
3       1.3.6.1.2.1.2.2.1.10.9  CLI
```

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

show rmon alarm

The **show rmon alarm** user EXEC command displays alarm configuration.

Syntax

show rmon alarm *number*

- *number*—Alarm index. (Range: 1 - 65535)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays RMON 1 alarms.

```
Console# show rmon alarm 1

Alarm 1

-------

OID: 1.3.6.1.2.1.2.2.1.10.1

Last sample Value: 878128

Interval: 30

Sample Type: delta

Startup Alarm: rising

Rising Threshold: 8700000

Falling Threshold: 78

Rising Event: 1

Falling Event: 1

Owner: CLI
```

The following table describes the significant fields shown in the display:

Field	Description
OID	Monitored variable OID.
Last Sample Value	The statistic value during the last sampling period. For example, if the sample type is delta, this value is the difference between the samples at the beginning and end of the period. If the sample type is absolute, this value is the sampled value at the end of the period.
Alarm	Alarm index.
Owner	The entity that configured this entry.
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	The method of sampling the variable and calculating the value compared against the thresholds. If the value is **absolute**, the value of the variable is compared directly with the thresholds at the end of the sampling interval. If the value is **delta**, the value of the variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.

Startup Alarm	The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising and falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising and falling, then a single falling alarm is generated.
Rising Threshold	A sampled statistic threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	A sampled statistic threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event	The event index used when a rising threshold is crossed.
Falling Event	The event index used when a falling threshold is crossed.

rmon event

The **rmon event** global configuration command configures an event. To remove an event, use the **no** form of this command.

Syntax

rmon event *index type* [**community** *text*] [**description** *text*] [**owner** *name*]

no rmon event *index*

- *index*—The event index. (Range: 1 - 65535)
- *type*—The type of notification that the device generates about this event. Can have the following values: **none**, **log**, **trap**, **log-trap**. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
- **community** *text*—If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
- **description** *text*—A comment describing this event.
- **owner** *name*—Enter a name that specifies who configured this event. If unspecified, the name is an empty string.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures an event with the trap index of 10.

```
Console (config)# rmon event 10 log
```

show rmon events

The **show rmon events** user EXEC command displays the RMON event table.

Syntax

show rmon events

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the RMON event table.

```
Console# show rmon events
Index  Description      Type      Community Owner    Last time sent
-----  -----------      ----------------------------- --------------------
1      Errors           Log                 CLI      Jan 18 2005  23:58:17
2      High Broadcast   Log-Trap  router    Manager  Jan 18 2005  23:59:48
```

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the event.
Description	A comment describing this event.
Type	The type of notification that the device generates about this event. Can have the following values: **none**, **log**, **trap**, **log-trap**. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

show rmon log

The **show rmon log** user EXEC command displays the RMON logging table.

Syntax

show rmon log [*event*]

- *event*—Event index. (Range: 0 - 65535)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the RMON logging table.

```
Console# show rmon log
Maximum table size: 500
Event  Description      Time
-----  -----------      --------------------
1      Errors           Jan 18 2005  23:48:19
1      Errors           Jan 18 2005  23:58:17
2      High Broadcast   Jan 18 2005  23:59:48
Console# show rmon log
Maximum table size: 500 (800 after reset)
Event  Description      Time
-----  -----------      --------------------
1      Errors           Jan 18 2005  23:48:19
1      Errors           Jan 18 2005  23:58:17
2High BroadcastJan 18 2005  23:59:48
```

The following table describes the significant fields shown in the display:

Field	Description
Event	An index that uniquely identifies the event.
Description	A comment describing this event.
Time	The time this entry created.

rmon table-size

The **rmon table-size** global configuration command configures the maximum RMON tables sizes. To return to the default configuration, use the **no** form of this command.

Syntax

rmon table-size {**history** *entries* | **log** *entries*}

no rmon table-size {**history** | **log**}

- **history** *entries*—Maximum number of history table entries. (Range: 20 - 32767)
- **log** *entries*—Maximum number of log table entries. (Range: 20 - 32767)

Default Configuration

History table size is 270.

Log table size is 100.

Command Mode

Global Configuration mode

User Guidelines

The configured table size is effective after the device is rebooted.

Example

The following example configures the maximum RMON history table sizes to 1000 entries.

```
Console (config)# rmon table-size history 1000
```

26

SNMP Commands

SNMP General Commands

snmp-server contact

The **snmp-server contact** global configuration command sets up a system contact. To remove the system contact information, use the **no** form of the command.

Syntax

snmp-server contact *text*

no snmp-server contact

- *text*—Character string, up to 160 characters, describing the system contact information.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Do not include spaces in the text string.

Example

The following example displays setting up the system contact point as "Dell_Technical_Support".

```
Console (config)# snmp-server contact Dell_Tecnical_Support
```

snmp-server location

The **snmp-server location** global configuration command sets up information on where the device is located. To remove the location string use, the **no** form of this command.

Syntax

snmp-server location *text*

no snmp-server location

- *text*—Character string, up to 160 characters, describing the system location.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Do not include spaces in the text string.

Example

The following example sets the device location as "New_York".

```
Console (config)# snmp-server location New_York
```

snmp-server enable traps

The **snmp-server enable traps** global configuration command enables the switch to send SNMP traps. To disable SNMP traps use the **no** form of the command.

Syntax

snmp-server enable traps

no snmp-server enable traps

Default Configuration

Traps are enabled by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the command to enable SNMP traps.

```
Console (config)# snmp-server enable traps
```

snmp-server trap authentication

The **snmp-server trap authentication** global configuration command enables the switch to send Simple Network Management Protocol traps when authentication fails. To disable SNMP authentication failed traps, use the **no** form of this command.

Syntax

snmp-server trap authentication

no snmp-server trap authentication

Default Configuration

Traps are enabled by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays the command to enable authentication failed SNMP traps.

```
Console (config)# snmp-server trap authentication
```

snmp-server set

The **snmp-server set** global configuration command sets SNMP MIB value by the CLI.

Syntax

snmp-server set *variable-name name1 value1 [name2 value2 …]*

- *variable-name*—MIB variable name.
- *name value...*—List of name and value pairs. In case of scalar MIBs there is only a single pair of name values. In case of entry in a table the first pairs are the indexes, followed by one or more fields.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Although the CLI can set any required configuration, there might be a situation where a SNMP user sets a MIB variable that does not have an equivalent command. In order to generate configuration files that support those situations, the **snmp-server set** command is used.

This command is context sensitive.

Examples

The following example sets the scalar MIB "sysName" to have the value "dell".

```
Console (config)# snmp-server set sysName sysname dell
```

The following example sets the entry MIB "rndCommunityTable" with keys 0.0.0.0 and "public". The field rndCommunityAccess gets the value "super" and the rest of the fields get their default values.

```
Console (config)# snmp-server set rndCommunityTable
rndCommunityMngStationAddr 0.0.0.0 rndCommunityString public
rndCommunityAccess super
```

snmp-server view

The **snmp-server view** global configuration command creates or updates a Simple Network Management Protocol (SNMP) server view entry. To delete a specified SNMP server view entry, use the **no** form of this command.

Syntax

snmp-server view *view-name oid-tree* {**included** | **excluded**}

no snmp-server view *view-name* [*oid-tree*]

- *view-name*—Specifies the label for the view record that is being created or updated. The name is used to reference the record. (Range: 1-30 characters)
- *oid-tree*—Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
- **included**—Indicates that the view type is included.
- **excluded**—Indicates that the view type is excluded.

Default Configuration

All views are included by default.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same view record.

The number of views is limited to 64.

Until the first wildcard, no attempt is made to verify that the MIB node corresponds to the starting portion of the OID.

Examples

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group.

```
Console (config)# snmp-server view user-view system included
Console (config)# snmp-server view user-view system.7 excluded
Console (config)# snmp-server view user-view ifEntry.*.1 included
```

snmp-server group

The **snmp-server group** global configuration command configures a new Simple Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views. To remove a specified SNMP group, use the **no** form of this command.

Syntax

snmp-server group *groupname* {**v1** | **v2** | **v3** {**noauth** | **auth** | **priv**} [**notify** *notifyview*] } [**context** *name*] [**read** *readview*] [**write** *writeview*]

no snmp-server group *groupname* {**v1** | **v2** | **v3** {**noauth** | **auth** | **priv**} [**notify** *notifyview*] } [**context** *name*]

- *groupname*—Specifies the name of the group.
- **v1**—Indicates the SNMP Version 1 security model.
- **v2**—Indicates the SNMP Version 2 security model.
- **v3**—Indicates the SNMP Version 3 security model.
- **noauth**—Indicates no authentication of a packet. Applicable only to the SNMP Version 3 security model.
- **auth**—Indicates authentication of a packet without encrypting it. Applicable only to the SNMP Version 3 security model.
- **priv**—Indicates authentication of a packet with encryption. Applicable only to the SNMP Version 3 security model.
- *name*—Specifies the context of a packet. The following contexts are supported: **router** and **oob**. If the context name is unspecified, all contexts are defined.
- *readview*—Specifies a string that is the name of the view that enables only viewing the contents of the agent. If unspecified, all objects except for the community-table and SNMPv3 user and access tables are available. (Range: 1-30 characters)

- *writeview*—Specifies a string that is the name of the view that enables entering data and configuring the contents of the agent. If unspecified, nothing is defined for the write view. (Range: 1-30 characters)
- *notifyview*—Specifies a string that is the name of the view that enables specifying an inform or a trap. If unspecified, nothing is defined for the notify view. (Range: 1-30 characters)

Default Configuration

No group entry exists.

Command Mode

Global Configuration mode

User Guidelines

The Router context is translated to the “” context in the MIB.

The index of the group name table is comprised of **Group Name**, **Security Model**, and **Security Level**. Different views for the same group can be defined with different security levels. Thus, for example, after having created the appropriate views, a group can be created for which "no authentication" is required, while allowing only notification view for "interfaces". A group of the same name can be created for which "priv" authentication is required. Read views can, for example, be configured for this group for mib2, and write views for interfaces. In this case, users in this group who send "priv" packets can modify all "interfaces" MIBs and view all mib2.

Examples

The following example attaches a group called **user-group** to SNMPv3 and assigns to the group the privacy security level and read access rights to a view called **user-view**.

```
Console (config)# snmp-server group user-group v3 priv read user-
view
```

snmp-server filter

The **snmp-server filter** global configuration command creates or updates a Simple Network Management Protocol (SNMP) server filter entry. To remove the specified SNMP server filter entry, use the **no** form of this command.

Syntax

snmp-server filter *filter-name oid-tree* {**included** | **excluded**}

no snmp-server filter *filter-name* [*oid-tree*]

- *filter-name*—Specifies the label for the filter record that is being updated or created. The name is used to reference the record. (Range: 1-30 characters)

- *oid-tree*—Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
- **included**—Indicates that the filter type is included.
- **excluded**—Indicates that the filter type is excluded.

Default Configuration

No filter entry exists.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same filter record. Later lines take precedence when an object identifier is included in two or more lines.

Examples

The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group.

```
Console(config)# snmp-server filter filter-name system included

Console(config)# snmp-server filter filter-name system.7 excluded

Console(config)# snmp-server filter filter-name ifEntry.*.1
included
```

show snmp

The **show snmp** privileged EXEC command displays the SNMP status.

Syntax

show snmp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the SNMP communications status.

```
Console # show snmp


Community-String               Community-Access  View name     IP address  type
----------------               ----------------  ---------     ----------  ----
public                         read only         user-view     All         Router
private                        read write        Default       172.16.1.1  Router
private-oob                    read write        Default       172.16.1.1  OOB
private                        su                DefaultSuper  172.17.1.1  Router


Community-String               Group name        IP address    type
----------------               ----------------  ----------    ----
public                         user-group        All           Router


OOB management stations
Community-String               Community-Access  View name     IP address  type
----------------               ----------------  ---------     ----------  ----
private                        read write        user-view     176.16.8.9  Router
private-oob                    read write        user-view     176.16.8.9  OOB


Traps are enabled.
Authentication trap is enabled.


Version 1,2 notifications
Target Address Type   Community Version  UDP Port Filter Name   To Sec      Retries
------------- ----    --------- -------  -------- -----------   ------      -------
192.122.173.42 Trap   public    2        162                    15          3
192.122.173.42 Inform public    2        162                    15          3
```

```
OOB trap receivers

Target Address Type   Community Version  UDP Port Filter Name   To Sec       Retries

------------- ----   --------- -------  -------- -----------   ------       -------

176.16.8.9     Trap   public    2        162                    15           3x


Version 3 notifications

Target Address Type   Username  Security UDP Port Filter Name   To Sec       Retries
                                Level

------------- ----   --------- -------  -------- -----------   ------       -------

192.122.173.42 Inform Bob       Priv     162                    15           3


OOB trap receivers

Target Address Type   Username  Security UDP Port Filter Name   To Sec       Retries
                                Level

------------- ----   --------- -------  -------- -----------   ------       -------

176.16.8.9     Inform Bob       Priv     162                    15           3


System Contact: Robert

System Location: Marketing
```

show snmp views

The **show snmp views** privileged EXEC command displays the configuration of views.

Syntax

show snmp views [*viewname*]

- *viewname*—Specifies the name of the view. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of views.

```
Console # show snmp views


Name                 OID Tree          Type
-----------  ----------------------- ---------
user-view    1.3.6.1.2.1.1           Included
user-view    1.3.6.1.2.1.1.7         Excluded
user-view    1.3.6.1.2.1.2.2.1.*.1   Included
```

show snmp groups

The **show snmp groups** privileged EXEC command displays the configuration of groups.

Syntax

show snmp groups [*groupname*]

- *groupname*—Specifies the name of the group. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of views.

```
Console # show snmp groups


Name                Security                       Views
                 Model   Level   Context  Read     Write    Notify
```

```
--------------  -----  -----  -------  -------  -------  -------
user-group       V3     priv   -        Default  ""       ""
managers-group   V3     priv   ""       Default  Default  ""
managers-group   V3     priv   OOB      Default  ""       ""

Console # show snmp groups user-group

Name               Security                       Views
                Model  Level  Context  Read     Write    Notify
--------------  -----  -----  -------  -------  -------  -------
user-group       V3     priv   -        Default  ""       ""
```

show snmp filters

The **show snmp filters** privileged EXEC command displays the configuration of filters.

Syntax

show snmp filters [*filtername*]

- *filtername*—Specifies the name of the filter. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of filters.

```
Console # show snmp filters


Name                    OID Tree            Type

-----------   -----------------------     ---------

user-filter   1.3.6.1.2.1.1               Included

user-filter   1.3.6.1.2.1.1.7             Excluded

user-filter   1.3.6.1.2.1.2.2.1.*.1       Included
```

SNMPv1/v2 Commands

snmp-server community

The **snmp-server community** global configuration command sets up the community access string to permit access to the SNMP protocol. To remove a community or community group, use the **no snmp-server community** command.

Syntax

snmp-server community *community* [**ro** | **rw** | **su**] [*ip-address*][**view** *view-name*][**type** {**router** | **oob**}]

snmp-server community-group *community group-name* [*ip-address*][**type** {**router** | **oob**}]

no snmp-server community *community* [*ip-address*]

- *community*—Community string that acts like a password and permits access to the SNMP protocol. (Range: 1-20 characters)
- **ro**—Indicates read-only access (default).
- **rw**—Indicates read-write access.
- **su**—Indicates SNMP administrator access.
- *ip-address*—Specifies the IP address of the management station. If no IP address is specified, all management stations are permitted. For information on specifying out-of-band IP addresses, see the user guidelines.
- *view-name*—Specifies the name of a previously defined view. For information on views, see the user guidelines. (Range: 1-30 characters)
- group-name—Specifies the name of a previously defined group. For information on groups, see the user guidelines. (Range: 1-30 characters)

- **type router**—Indicates that a community is used for SNMP access to the device only (not to the Out-of-Band port).
- **type oob**—Indicates that a community is used for SNMP access to the Out-of-Band port only.

Default Configuration

No community is defined.

Command Mode

Global Configuration mode

User Guidelines

The **view-name** parameter cannot be specified for **su**, which has access to the whole MIB.

The **view-name** parameter can be used to restrict the access rights of a community string. When it is specified:

- An internal security name is generated.
- The internal security name for SNMPv1 and SNMPv2 security models is mapped to an internal group name.
- The internal group name for SNMPv1 and SNMPv2 security models is mapped to a view-name (read-view and notify-view always, and for **rw** for write-view also)

The **group-name** parameter can also be used to restrict the access rights of a community string. When it is specified:

- An internal security name is generated.
- The internal security name for SNMPv1 and SNMPv2 security models is mapped to the group name.

To define a management station on the out-of-band port, use out-of-band IP address format **oob**/*ip-address*.

For a user to define OOB management port configurations, such as ip address, default gateway, RADIUS, and so forth, two SNMP communities must be defined. A super user can configure OOB management port settings with a single community, by switching between the two communities.

Examples

The following example configures community access string **public** to permit administrative access to SNMP at an administrative station with IP address 192.168.1.20.

```
Console (config)# snmp-server community public su 192.168.1.20
```

The following example configures community access string **public** to permit SNMP read-write access for the Out-of-Band port only.

```
Console (config)# snmp-server community public rw 192.175.1.10
type oob
```

snmp-server host

The **snmp-server host** global configuration command specifies the recipient of Simple Network Management Protocol Version 1 or Version 2 notifications. To remove the specified host, use the **no** form of this command.

Syntax

snmp-server host {*ip-address* | *hostname*} *community-string* [**traps** | **informs**] [**1** | **2**] [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]

no snmp-server host {*ip-address* | *hostname*} [**traps** | **informs**]

- *ip-address*—Specifies the IP address of the host (targeted recipient). For information about specifying an out-of-band IP address, see the user guidelines.
- *hostname*—Specifies the name of the host. (Range:1-158 characters)
- *community-string*—Specifies a password-like community string sent with the notification operation. (Range: 1-20)
- **traps**—Indicates that SNMP traps are sent to this host.
- **informs**—Indicates that SNMP informs are sent to this host. Not applicable to SNMPv1.
- **1**—Indicates that SNMPv1 traps will be used.
- **2**—Indicates that SNMPv2 traps will be used.
- *port*—Specifies the UDP port of the host to use. (Range:1-65535)
- *filtername*—Specifies a string that defines the filter for this host. If unspecified, nothing is filtered. (Range: 1-30 characters)
- *seconds*—Specifies the number of seconds to wait for an acknowledgment before resending informs. (Range: 1-300)
- retries—Specifies the maximum number of times to resend an inform request. (Range: 0-255)

Default Configuration

The default is to send SNMPv2 traps to the host.

The default UDP port of the host to use is 162.

The default timeout period to wait for an acknowedgement before resending informs is 15 seconds.

The default maximum number of times to resend an inform request is 3.

Command Mode

Global Configuration mode

User Guidelines

When configuring an SNMPv1 or SNMPv2 notification recipient, a notification view for that recipient is automatically generated for all the MIB.

When configuring an SNMPv1 notification recipient, the **Inform** option cannot be selected.

If a trap and inform are defined on the same target, and an inform was sent, the trap is not sent.

To define an SNMP recipient on the out-of-band port, use the out-of-band IP address format **oob**/*ip-address*.

Example

The following example enables SNMP traps for host 10.1.1.1 with community string "management" using SNMPv2.

```
Console (config)# snmp-server host 10.1.1.1 management 2
```

SNMPv3 Commands

snmp-server user

The **snmp-server user** global configuration command configures a new SNMP Version 3 user. To delete a user, use the **no** form of this command.

Syntax

snmp-server user *username groupname* [**remote** *engineid-string*] [**auth-md5** *password* **| auth-sha** *password* **| auth-md5-key** *md5-des-keys* **| auth-sha-key** *sha-des-keys*]

no snmp-server user *username* [**remote** *engineid-string*]

- *username*—Specifies the name of the user on the host that connects to the agent. (Range: 1-30 characters)
- *groupname*—Specifies the name of the group to which the user belongs. (Range: 1-30 characters)
- *engineid-string*—Specifies the engine ID of the remote SNMP entity to which the user belongs. The engine ID is a concatenated hexadecimal string. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. If the engine ID is not specified, the local engine ID is used. (Range: 5-32 characters)

- **auth-md5** *password*—Indicates the HMAC-MD5-96 authentication level. The user should enter a password for authentication and generation of a DES key for privacy. (Range: 1-32 characters)
- **auth-sha** *password*—Indicates the HMAC-SHA-96 authentication level. The user should enter a password for authentication and generation of a DES key for privacy. (Range: 1-32 characters)
- **auth-md5-key** *md5-des-keys*—Indicates the HMAC-MD5-96 authentication level. The user should enter a concatenated hexadecimal string of the MD5 key (MSB) and the privacy key (LSB). If authentication is only required, 16 bytes should be entered; if authentication and privacy are required, 32 bytes should be entered. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (16 or 32 bytes)
- **auth-sha-key** *sha-des-keys*—Indicates the HMAC-SHA-96 authentication level. The user should enter a concatenated hexadecimal string of the SHA key (MSB) and the privacy key (LSB). If authentication is only required, 20 bytes should be entered; if authentication and privacy are required, 36 bytes should be entered. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (20 or 36 bytes)

Default Configuration

No group entry exists.

Command Mode

Global Configuration mode

User Guidelines

If auth-md5 or auth-sha is specified, both authentication and privacy are enabled for the user.

The engine ID is a two-digit hexadecimal string. If a single digit number is specified, the device interprets it as a two-digit number by adding a 0 before the number. For example, "1.2.3.3.2.1" is interpreted as "01.02.03.03.02.01.

When a **show running-config** privileged EXEC command is entered, a line for this user will not be displayed. To see if this user has been added to the configuration, type the **show snmp users** privileged EXEC command.

Examples

The following example configures an SNMPv3 user "John" in group "user-group".

```
Console (config)# snmp-server user John user-group
```

snmp-server v3-host

The **snmp-server v3-host** global configuration command specifies the recipient of Simple Network Management Protocol Version 3 notifications. To remove the specified host, use the **no** form of this command.

Syntax

snmp-server v3-host {*ip-address* | *hostname*} *username* [**traps** | **informs**] {**noauth** | **auth** | **priv**} [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]

no snmp-server v3-host {*ip-address* | *hostname*} *username* [**traps** | **informs**]

- *ip-address*—Specifies the IP address of the host (targeted recipient). For information about specifying an out-of-band IP address, see the user guidelines.
- *hostname*—Specifies the name of the host. (Range:1-158 characters)
- *username*—Specifies the name of the user to use to generate the notification. (Range: 1-24)
- **traps**—Indicates that SNMP traps are sent to this host.
- **informs**—Indicates that SNMP informs are sent to this host.
- **noauth**—Indicates no authentication of a packet.
- **auth**—Indicates authentication of a packet without encrypting it.
- **priv**—Indicates authentication of a packet with encryption.
- *port*—Specifies the UDP port of the host to use. (Range: 1-65535)
- *filtername*—Specifies a string that defines the filter for this host. If unspecified, nothing is filtered. (Range: 1-30 characters)
- *seconds*—Specifies the number of seconds to wait for an acknowledgment before resending informs. (Range: 1-300)
- retries—Specifies the maximum number of times to resend an inform request. (Range: 0-255)

Default Configuration

- The default UDP port of the host to use is 162.
- The default timeout period to wait for an acknowedgement before resending informs is 15 seconds.
- The default maximum number of times to resend an inform request is 3.

Command Mode

Global Configuration mode

User Guidelines

A user and notification view are not automatically created. Use the **snmp-server user**, **snmp-server group** and **snmp-server user** global configuration commands to generate a user, group and notify group, respectively.

To define an SNMP recipient on the out-of-band port, use the out-of-band IP address format **oob**/*ip-address*.

NOTE: The type of trap (i.e trap, notification or inform) depends on how the trap receiver has been configured.

Example

The following example configures an SNMPv3 host.

```
Console (config)# snmp-server v3-host 192.168.0.20 john
```

show snmp engineID

The **show snmp engineID** privileged EXEC command displays the ID of the local Simple Network Management Protocol (SNMP) engine.

Syntax

show snmp engineID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the SNMP engine ID.

```
Console # show snmp engineID

Local SNMP engineID: 08009009020C0B099C075878
```

show snmp users

The **show snmp users** privileged EXEC command displays the configuration of users.

Syntax

show snmp users [*username*]

- *username*—Specifies the name of the user. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of users.

```
Console # show snmp users

Name     Group name     Auth Method  Remote
------   -------------  ---------    -------------------------
John     user-group     md5
John     user-group     md5          08009009020C0B099C075879

Console # show snmp users John

Name     Group name     Auth Method  Remote
------   -------------  ---------    -------------------------
John     user-group     md5          08009009020C0B099C075879
```

27

Spanning-Tree Commands

spanning-tree

The **spanning-tree** global configuration command enables spanning-tree functionality. To disable spanning-tree functionality, use the **no** form of this command.

Syntax

spanning-tree

no spanning-tree

Default Configuration

Spanning-tree is enabled.

Command Modes

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables spanning-tree functionality.

```
Console(config)# spanning-tree
```

spanning-tree mode

The **spanning-tree mode** global configuration command configures the spanning-tree protocol. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree mode {stp | rstp}

no spanning-tree mode

- **stp**—STP is supported.
- **rstp**—RSTP is supported.

Default Configuration

Spanning-tree protocol (STP) is supported.

Command Modes

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the spanning-tree protocol to RSTP.

```
Console(config)# spanning-tree mode rstp
```

spanning-tree forward-time

The **spanning-tree forward-time** global configuration command configures the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state.

To reset the default forward time, use the **no** form of this command.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

- *seconds*—Time in seconds .(Range: 4 - 30)

Default Configuration

The default forwarding-time for IEEE Spanning-tree Protocol (STP) is 15 seconds.

Command Modes

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures spanning-tree bridge forward time to 25 seconds.

```
Console(config)# spanning-tree forward-time 25
```

spanning-tree hello-time

The **spanning-tree hello-time** global configuration command configures the spanning-tree bridge hello time, which is how often the switch broadcasts hello messages to other switches.To reset the default hello time, use the **no** form of this command.

Syntax

spanning-tree hello-time *seconds*

no spanning-tree *hello-time*

- *seconds*—Time in seconds. (Range: 1 - 10)

Default Configuration

The default hello time for IEEE Spanning-Tree Protocol (STP) is 2 seconds.

Command Modes

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures spanning-tree bridge hello time to 5 seconds.

```
Console(config)# spanning-tree hello-time 5
```

spanning-tree max-age

The **spanning-tree max-age** global configuration command configures the spanning-tree bridge maximum age. To reset the default maximum age, use the **no** form of this command.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

- *seconds* -Time in seconds. (Range: 6 - 40)

Default Configuration

The default max-age for IEEE STP is 20 seconds.

Command Modes

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the spanning-tree bridge maximum-age to 10 seconds.

```
Console(config)# spanning-tree max-age 10
```

spanning-tree priority

The **spanning-tree priority** global configuration command configures the spanning-tree priority. The priority value is used to determine which bridge is elected as the root bridge. To reset the default spanning-tree priority use the **no** form of this command.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

- *priority*—Priority of the bridge. (Range: 0 - 61440 in steps of 4096)

Default Configuration

The default bridge priority for IEEE STP is 32768.

Command Modes

Global Configuration mode

User Guidelines

The lower the priority, the more likely the bridge is to be the Root Bridge.

Example

The following example configures spanning-tree priority to 12288.

```
Console(config)# spanning-tree priority 12288
```

spanning-tree disable

The **spanning-tree disable** interface configuration command disables spanning-tree on a specific port. To enable spanning-tree on a port use, the **no** form of this command.

Syntax

spanning-tree disable

no spanning-tree disable

Default Configuration

By default, all ports are enabled for spanning-tree.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disables spanning-tree on g5.

```
Console (config)# interface ethernet g5
Console (config-if)# spanning-tree disable
```

spanning-tree cost

The **spanning-tree cost** interface configuration command configures the spanning-tree path cost for a port. To return to the default port path cost, use the **no** form of this command.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

- *cost*—The port path cost. (Range: 1 - 200,000,000)

Default Configuration

The default costs are as follows:

- **Port Channel**—20,000
- **1000 mbps (giga)**—20,000
- **100 mbps**—200,000
- **10 mbps**—2,000,000

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the spanning-tree cost on g5 to 35000.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree cost 35000
```

spanning-tree port-priority

The **spanning-tree port-priority** interface configuration command configures port priority. To reset the default port priority, use the **no** form of this command.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

- *priority*—The port priority. (Range: 0 - 240 in multiples of 16)

Default Configuration

The default port-priority for IEEE STP is 128.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the spanning priority on g5 to 96.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree port-priority 96
```

spanning-tree portfast

The **spanning-tree portfast** interface configuration command enables PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire. To disable PortFast mode, use the **no** form of this command.

Syntax

spanning-tree portfast

no spanning-tree portfast

Default Configuration

PortFast mode is disabled.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This feature should be used only with interfaces connected to end stations. Otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operations.

Example

The following example enables PortFast on g5.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree portfast
```

spanning-tree link-type

The **spanning-tree link-type** interface configuration command overrides the default link-type setting. To reset the default, use the **no** form of this command.

Syntax

spanning-tree link-type {point-to-point | shared}

no spanning-tree spanning-tree link-type

- **point-to-point**—Specifies the port link type as point-to-point.
- **shared**—Specifies that the port link type is shared.

Default Configuration

The switch derives the link type of a port from the duplex mode. A full-duplex port is considered a point-to-point link, and a half-duplex port is considered a shared link.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables shared spanning-tree on g5.

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree link-type shared
```

spanning-tree bpdu

The **spanning-tree bpdu** global configuration command defines BPDU handling when the spanning-tree is disabled on an interface.

Syntax

spanning-tree bpdu {filtering | flooding}

- **filtering**—Filter BPDU packets when spanning-tree is disabled on an interface.

- **flooding**—Flood BPDU packets when spanning-tree is disabled on an interface.

Default Configuration

The default definition is flooding.

Command Modes

Global Configuration mode

User Guidelines

Use this command when STP is disabled on the PowerConnect 6024/6024F.

Example

The following example defines BPDU packet flooding when spanning-tree is disabled on an interface.

```
Console(config)# spanning-tree bpdu flooding
```

clear spanning-tree detected-protocols

The **clear spanning-tree detected-protocols** privileged EXEC command restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.

Syntax

clear spanning-tree detected-protocols [**ethernet interface number | port-channel** *port-channel-number*]

- *interface*—A valid Ethernet port.
- *port-channel-number*—A port-channel index.

Default Configuration

If no interface is specified, the action is applied to all interfaces.

Command Modes

Privileged EXEC mode

User Guidelines

This feature should be used only when working in RSTP mode.

Example

The following example restarts the protocol migration process (forces the renegotiation with neighboring switches) on g1.

```
Console# clear spanning-tree detected-protocols ethernet g1
```

show spanning-tree

The **show spanning-tree** privileged EXEC command displays the spanning-tree configuration.

Syntax

show spanning-tree [**ethernet** *interface-number* | **port-channel** *port-channel-number*] [**instance** *instance-id*]

show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** *instance-id*]

show spanning-tree mst-configuration

- *detail*—Displays detailed information.
- *active*—Displays active ports only.
- *blockedports*—Displays blocked ports only.
- *mst-configuration*—Displays the MST configuration.
- *interface-number*—A valid Ethernet port number.
- *port-channel-number*—A valid port-channel index.
- *instance -id*—ID of the spanning -tree instance (Range: 0-15).

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following examples display spanning-tree information.

```
Console# show spanning-tree


Spanning tree enabled mode RSTP

Default port cost method: long


Root ID    Priority             32768

           Address              00:01:42:97:e0:00

           Path Cost            20000

           Root Port            1 (g1)

           Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 sec


Bridge ID  Priority             36864

           Address              00:02:4b:29:7a:00

           Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 sec


Interfaces

Name       State      Prio.Nbr   Cost       Sts      Role     PortFast   Type

----       -------    --------   -----      ---      ----     --------   ----------

g1         Enabled    128.1      20000      FWD      Root     No         P2p (RSTP)

g2         Enabled    128.2      20000      FWD      Desg     No         Shared (STP)

g3         Disabled   128.3      20000      -        -        -          -

g4         Enabled    128.4      20000      BLK      ALTN     No         Shared (STP)

g5         Enabled    128.5      20000      DIS      -        -          -
```

```
Console# show spanning-tree

Spanning tree enabled mode RSTP
Default port cost method: long

Root ID    Priority             36864
           Address              00:02:4b:29:7a:00
           This switch is the root.
           Hello Time 2 sec     Max Age 20 sec      Forward Delay 15 sec

Interfaces
Name       State      Prio.Nbr   Cost       Sts       Role      PortFast   Type
----       -------    --------   -----      ---       ----      --------   ----------
g1         Enabled    128.1      20000      FWD       Desg      No         P2p (RSTP)
g2         Enabled    128.2      20000      FWD       Desg      No         Shared (STP)
g3         Disabled   128.3      20000      -         -         -          -
g4         Enabled    128.4      20000      FWD       Desg      No         Shared (STP)
g5         Enabled    128.5      20000      DIS       -         -          -

Console# show spanning-tree

Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long

Root ID    Priority             N/A
           Address              N/A
           Path Cost            N/A
           Root Port            N/A
           Hello Time N/A       Max Age N/A         Forward Delay N/A
```

```
Bridge ID Priority            36864
          Address             00:02:4b:29:7a:00
          Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec

Interfaces
Name      State     Prio.Nbr  Cost      Sts      Role     PortFast  Type
----      -------   --------  -----     ---      ----     --------  ----------
g1        Enabled   128.1     20000     -        -        -         -
g2        Enabled   128.2     20000     -        -        -         -
g3        Disabled  128.3     20000     -        -        -         -
g4        Enabled   128.4     20000     -        -        -         -
g5        Enabled   128.5     20000     -        -        -         -

Console# show spanning-tree active

Spanning tree enabled mode RSTP
Default port cost method: long

Root ID   Priority            32768
          Address             00:01:42:97:e0:00
          Path Cost           20000
          Root Port           1 (g1)
          Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec

Bridge ID Priority            36864
          Address             00:02:4b:29:7a:00
          Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec
```

```
Interfaces
Name       State     Prio.Nbr   Cost      Sts      Role     PortFast   Type
----       -------   --------   -----     ---      ----     --------   ----------
g1         Enabled   128.1      20000     FWD      Root     No         P2p (RSTP)
g2         Enabled   128.2      20000     FWD      Desg     No         Shared (STP)
g4         Enabled   128.4      20000     BLK      ALTN     No         Shared (STP)

Console# show spanning-tree blocked ports

Spanning tree enabled mode RSTP
Default port cost method: long

Root ID    Priority             32768
           Address              00:01:42:97:e0:00
           Path Cost            20000
           Root Port            1 (g1)
           Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 sec

Bridge ID  Priority             36864
           Address              00:02:4b:29:7a:00
           Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 sec

Interfaces
Name       State     Prio.Nbr   Cost      Sts      Role     PortFast   Type
----       -------   --------   -----     ---      ----     --------   ----------
g4         Enabled   128.4      20000     BLK      ALTN     No         Shared (STP)
```

```
Console# show spanning-tree detail


Spanning tree enabled mode RSTP
Default port cost method: long


Root ID   Priority             32768
          Address              00:01:42:97:e0:00
          Path Cost            20000
          Root Port            1 (g1)
          Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 sec


Bridge ID Priority  36864
          Address              00:02:4b:29:7a:00
          Hello Time 2 sec     Max Age 20 sec     Forward Delay 15 sec


Number of topology changes 2 last change occurred 2d18h ago
Times:    hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15


Port 1 (g1) enabled
State: Forwarding                         Role: Root
Port id: 128.1                            Port cost: 20000
Type: P2p (configured: auto) RSTP         Port Fast: No (configured:no)
Designated bridge Priority: 32768         Address: 00:01:42:97:e0:00
Designated port id: 128.25                Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638
```

```
Port 2 (g2) enabled
State: Forwarding                         Role: Designated
Port id: 128.2                            Port cost: 20000
Type: Shared (configured: auto) STP       Port Fast: No (configured:no)
Designated bridge Priority: 32768         Address: 00:02:4b:29:7a:00
Designated port id: 128.2                 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (g3) disabled
State: N/A                                Role: N/A
Port id: 128.3                            Port cost: 20000
Type: N/A (configured: auto)              Port Fast: N/A (configured:no)
Designated bridge Priority: N/A           Address: N/A
Designated port id: N/A                   Designated path cost: N/A
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A

Port 4 (g4) enabled
State: Blocking                           Role: Alternate
Port id: 128.4                            Port cost: 20000
Type: Shared (configured:auto) STP        Port Fast: No (configured:no)
Designated bridge Priority: 28672         Address: 00:30:94:41:62:c8
Designated port id: 128.25                Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 5 (g5) enabled
State: Disabled                           Role: N/A
```

```
Port id: 128.5                          Port cost: 20000
Type: N/A (configured: auto)            Port Fast: N/A (configured:no)
Designated bridge Priority: N/A         Address: N/A
Designated port id: N/A                 Designated path cost: N/A
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A

Console# show spanning-tree ethernet g1
Port 1 (g1) enabled
State: Forwarding                       Role: Root
Port id: 128.1                          Port cost: 20000
Type: P2p (configured: auto) RSTP       Port Fast: No (configured:no)
Designated bridge Priority: 32768       Address: 00:01:42:97:e0:00
Designated port id: 128.25              Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Console# show spanning-tree mst-configuration

Name: Region1
Revision: 1
Instance             Vlans mapped        State
--------             ------------        -------
0                    1-9, 21-4094        Enabled
1                    10-20               Enabled
```

```
Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9, 21-4094
CST Root ID          Priority  32768
                     Address   00:01:42:97:e0:00
                     Path Cost 20000
                     Root Port 1 (g1)
                     Hello Time 2 sec     Max Age 20 sec    Forward Delay 15 sec

IST Master ID        Priority  32768
                     Address   00:02:4b:29:7a:00
                     This switch is the IST master.
                     Hello Time 2 sec     Max Age 20 sec    Forward Delay 15 sec
                     Max hops  20

Interfaces
Name       State      Prio.Nbr   Cost       Sts      Role     PortFast   Type
----       -------    --------   -----      ---      ----     --------   ----------
g1         Enabled    128.1      20000      FWD      Root     No         P2p Bound
                                                                         (RSTP)
g2         Enabled    128.2      20000      FWD      Desg     No         Shared Bound
                                                                         (STP)
g3         Enabled    128.3      20000      FWD      Desg     No         P2p
g4         Enabled    128.4      20000      FWD      Desg     No         P2p
```

```
###### MST 1 Vlans Mapped: 10-20

CST Root ID          Priority  24576

                     Address   00:02:4b:29:89:76

                     Path Cost 20000

                     Root Port 4 (g4)

                     Rem hops  19


Bridge ID            Priority  32768

                     Address   00:02:4b:29:7a:00


Interfaces

Name      State      Prio.Nbr  Cost       Sts      Role     PortFast  Type

----      -------    --------  -----      ---      ----     --------  ----------

g1        Enabled    128.1     20000      FWD      Boun     No        P2p Bound
                                                                      (RSTP)

g2        Enabled    128.2     20000      FWD      Boun     No        Shared Bound
                                                                      (STP)

g3        Enabled    128.3     20000      BLK      Altn     No        P2p

g4        Enabled    128.4     20000      FWD      Desg     No        P2p


Console# show spanning-tree detail


Spanning tree enabled mode MSTP

Default port cost method: long


###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID          Priority  32768

                     Address   00:01:42:97:e0:00

                     Path Cost 20000
                     Root Port  1 (g1)
                     Hello Time 2 sec     Max Age 20 sec    Forward Delay 15 sec

IST Master ID        Priority  32768
                     Address   00:02:4b:29:7a:00
                     This switch is the IST master.
                     Hello Time 2 sec     Max Age 20 sec    Forward Delay 15 sec
                     Max hops  20
                     Number of topology changes 2 last change occurred 2d18h ago
                     Times:  hold 1, topology change 35, notification 2
                     hello 2, max age 20, forward delay 15

Port 1 (g1) enabled
State: Forwarding                                  Role: Root
Port id: 128.1                                     Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP         Port Fast: No (configured:no)
Designated bridge Priority: 32768                  Address: 00:01:42:97:e0:00
Designated port id: 128.25                         Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 2 (g2) enabled
State: Forwarding                                  Role: Designated
Port id: 128.2                                     Port cost: 20000
Type: Shared (configured: auto) Boundary STP       Port Fast: No (configured:no)
Designated bridge Priority: 32768                  Address: 00:02:4b:29:7a:00
Designated port id: 128.2                          Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
```

```
Port 3 (g3) enabled
State: Forwarding                                  Role: Designated
Port id: 128.3                                     Port cost: 20000
Type: Shared (configured: auto) Internal           Port Fast: No (configured:no)
Designated bridge Priority: 32768                  Address: 00:02:4b:29:7a:00
Designated port id: 128.3                          Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 4 (g4) enabled
State: Forwarding                                  Role: Designated
Port id: 128.4                                     Port cost: 20000
Type: Shared (configured: auto) Internal           Port Fast: No (configured:no)
Designated bridge Priority: 32768                  Address: 00:02:4b:29:7a:00
Designated port id: 128.2                          Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

###### MST 1 Vlans Mapped: 10-20
Root ID              Priority  24576
                     Address   00:02:4b:29:89:76
                     Path Cost 20000
                     Port Cost 4 (g4)
                     Rem hops  19

Bridge ID            Priority  32768
                     Address   00:02:4b:29:7a:00
                     Number of topology changes 2 last change occurred 1d9h ago
                     Times:  hold 1, topology change 2, notification 2
                     hello 2, max age 20, forward delay 15

Port 1 (g1) enabled
State: Forwarding                                  Role: Boundary
Port id: 128.1                                     Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP         Port Fast: No (configured:no)
Designated bridge Priority: 32768                  Address: 00:02:4b:29:7a:00
Designated port id: 128.1                          Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 2 (g2) enabled
State: Forwarding                                  Role: Designated
Port id: 128.2                                     Port cost: 20000
Type: Shared (configured: auto) Boundary STP       Port Fast: No (configured:no)
Designated bridge Priority: 32768                  Address: 00:02:4b:29:7a:00
Designated port id: 128.2                          Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (g3) disabled
State: Blocking                                    Role: Alternate
Port id: 128.3                                     Port cost: 20000
Type: Shared (configured: auto) Internal           Port Fast: No (configured:no)
Designated bridge Priority: 32768                  Address: 00:02:4b:29:1a:19
Designated port id: 128.78                         Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
```

```
Port 4 (g4) enabled
State: Forwarding                                  Role: Designated
Port id: 128.4                                     Port cost: 20000
Type: Shared (configured: auto) Internal           Port Fast: No (configured:no)
Designated bridge Priority: 32768                  Address: 00:02:4b:29:7a:00
Designated port id: 128.2                          Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9, 21-4094
CST Root ID          Priority  32768
                     Address   00:01:42:97:e0:00
                     Path Cost 20000
                     Root Port 1 (g1)
                     Hello Time 2 sec     Max Age 20 sec    Forward Delay 15 sec

IST Master ID        Priority  32768
                     Address   00:02:4b:19:7a:00
                     Path Cost 10000
                     Rem hops  19

Bridge ID            Priority  32768
                     Address   00:02:4b:29:7a:00
                     Hello Time 2 sec     Max Age 20 sec    Forward Delay 15 sec
                     Max hops   20

Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9, 21-4094
CST Root ID          Priority   32768
                     Address    00:01:42:97:e0:00
                     This switch is root for CST and IST master.
                     Root Port 1 (g1)
                     Hello Time 2 sec     Max Age 20 sec    Forward Delay 15 sec
                     Max hops   20
```

spanning-tree pathcost method

The **spanning-tree pathcost method** global configuration command sets the method by which path cost defaults are determined.. To return to the default setting, use the **no** form of this command.

Syntax

spanning-tree pathcost method {long | short}

no spanning-tree pathcost method

- *long*—Specifies 1 through 200,000,000 range for port path costs.
- *short*—Specifies 1 through 65,535 range for port path costs.

Default Configuration

If the pathcost method is short, the default configuration is:

- Ethernet (10 Mbps) - 100
- Fast Ethernet (100 Mbps) - 19
- Gigabit Ethernet (1000 Mbps) - 4
- Port-Channel - 4

If the pathcost method is long, the default configuration is:

- Ethernet (10 Mbps) - 2,000,000
- Fast Ethernet (100 Mbps) - 200,000
- Gigabit Ethernet (1000 Mbps) - 20,000
- Port-Channel - 20,000

Command Mode

Global Configuration mode

User Guidelines

This command applies to all spanning tree instances on the switch.

If the short method is chosen, the default cost value is in the range of 1 through 65,535.

If the long method is chosen, the default cost value is in the range of 1 through 200,000,000.

Examples

The following example specifies the long pathcost method.

```
Console# spanning-tree pathcost method long
```

spanning-tree mst priority

The **spanning-tree mst priority** global configuration command configures the device priority for the specified spanning-tree instance. To return to the default setting, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

- *instance-id*—ID of the spanning -tree instance (Range: 1-15).
- *priority*—Device priority for the specified spanning-tree instance (Range: 0-61440).

Default Configuration

The default bridge priority for IEEE STP is 32768.

Command Mode

Global Configuration mode

User Guidelines

The priority value must be a multiple of 4096.

The device with the lowest priority is selected as the root of the spanning tree.

Example

The following example configures the spanning tree priority of instance 1 to 4096.

```
Console (config) # spanning-tree mst 1 priority 4096
```

spanning-tree mst max-hops

The **spanning-tree mst priority** global configuration command configures the number of hops in an MST region before the BDPU is discarded and the port information is aged out. To return to the default setting, use the **no** form of this command.

Syntax

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

- *hop-count*—Number of hops in an MST region before the BDPU is discarded . (Range: 1-40)

Default Configuration

The default number of hops is 20.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
Console (config) # spanning-tree mst max-hops 10
```

spanning-tree mst port-priority

The **spanning-tree mst port-priority** interface configuration command configures port priority. To return to the default port priority, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

- *instance-ID*—ID of the spanning -tree instance. (Range: 0-15)
- *priority*—The port priority. (Range: 0 - 240 in multiples of 16)

Default Configuration

The default port-priority for IEEE MSTP is 128.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the port priority of port g1 to 142.

```
Console (config)# interface ethernet g1
Console (config-if)# spanning-tree mst 1 port-priority 142
```

spanning-tree mst cost

The **spanning-tree mst cost** interface configuration command configures the path cost for multiple spanning tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. To return to the default port path cost, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

- *instance-ID*—ID of the spanning -tree instance (Range: 1-15).
- *cost*—The port path cost. (Range: 1 - 200,000,000)

Default Configuration

If the pathcost method is short, the default configuration is:

- Ethernet (10 Mbps) - 100
- Fast Ethernet (100 Mbps) - 19
- Gigabit Ethernet (1000 Mbps) - 4
- Port-Channel - 4

If the pathcost method is long, the default configuration is:

- Ethernet (10 Mbps) - 2,000,000
- Fast Ethernet (100 Mbps) - 200,000
- Gigabit Ethernet (1000 Mbps) - 20,000
- Port-Channel - 20,000

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the MSTP instance 1 path cost for interface g9 to 4.

```
Console (config) # interface ethernet g9

console (config-if) # spanning-tree mst 1 cost 4
```

spanning-tree mst configuration

The **spanning-tree mst configuration** global configuration command enables configuring an MST region by entering the multiple spanning-tree (MST) mode.

Syntax

spanning-tree mst configuration

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

All devices in an MST region must have the same VLAN mapping, configuration revision number and name.

Example

The following example configures an MST region.

```
Console(config)# spanning-tree mst configuration

Console(config-mst) # instance 1 add vlan 10-20

Console(config-mst) # name region1

Console(config-mst) # revision 1
```

instance (mst)

The **instance** MST configuration command maps VLANS to an MST instance.

Syntax

instance *instance-id* {**add** | **remove**} **vlan** *vlan-range*

- *instance-ID*—ID of the MST instance (Range: 1-15).
- *vlan-range*—VLANs to be added to the existing VLANs. To specify a range of VLANs, use a hyphen. To specify a series of VLANS, use a comma. (Range: 1-4093).

Default Configuration

VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Modes

MST Configuration mode

User Guidelines

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps VLANs 10-20 to MST instance 1.

```
Console (config)# spanning-tree mst configuration

Console (config-mst)# instance 1 add vlan 10-20
```

name (mst)

The **name** MST configuration command defines the configuration name. To return to the default setting, use the **no** form of this command.

Syntax

name *string*

- *string*—MST configuration name. Case-sensitive (Range: 1-32).

Default Configuration

Device address.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures sets the configuration name to region1.

```
Console (config) # spanning-tree mst configuration
Console (config-mst) # name "region 1"
```

revision (mst)

The **revision** MST configuration command defines the configuration revision number. To return to the default setting, use the **no** form of this command.

Syntax

revision *value*

no revision

- *value*—Configuration revision number (Range: 0-65535).

Default Configuration

Revision number is 0.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the configuration revision to 1.

```
Console (config) # spanning-tree mst configuration
Console (config-mst) # revision 1
```

show (mst)

The **show** MST configuration command displays the current or pending MST region configuration.

Syntax

show {**current** | **pending**}

Default Configuration

This command has no default configuration.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays a pending MST region configuration.

```
Device(config-mst)# show pending
Pending MST configuration
Name: Region1
Revision: 1
Instance       Vlans Mapped    State
--------       ------------    -----
0              1-9,21-4094     Enabled
1              10-20           Enabled
```

exit (mst)

The **exit** MST configuration command exits the MST configuration mode and applies all configuration changes.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to exit the MST configuration mode and save changes.

```
Console (config) # spanning-tree mst configuration

Console (config-mst) # exit
```

abort (mst)

The **abort** MST configuration command exits the MST configuration mode without applying the configuration changes.

Syntax

abort

Default Configuration

This command has no default configuration.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to exit the MST configuration mode without saving changes.

```
Console (config) # spanning-tree mst configuration
Console (config-mst) # abort
```

28

SSH Commands

ip ssh port

The **ip ssh port** global configuration command specifies the port to be used by the SSH server. To use the default port, use the **no** form of this command.

Syntax

ip ssh port *port-number*

no ip ssh port

- *port-number*—Port number for use by the SSH server (Range: 1 - 65535).

Default Configuration

The default value is 22.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the port to be used by the SSH server as 8080.

```
Console (config)# ip ssh port 8080
```

ip ssh server

The **ip ssh server** global configuration command enables the device to be configured from a SSH server. To disable this function, use the **no** form of this command.

Syntax

ip ssh server

no ip ssh server

Default Configuration

This default is SSH is enabled.

Command Mode

Global Configuration mode

User Guidelines

If encryption keys are not generated, the SSH server is in standby until the keys are generated. To generate SSH server keys, use the commands **crypto key generate rsa**, and **crypto key generate dsa**.

Example

The following example enables the device to be configured from a SSH server.

```
Console (config)# ip ssh server
```

crypto key generate dsa

The **ip ssh server** global configuration command generates DSA key pairs.

Syntax

crypto key generate dsa

Default Configuration

DSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

When upgrading from previous version (00.01.64) of PowerConnect 6024/6024F to the current version, you may need to create a new certificate.
DSA keys are generated in pairs: one public DSA key and one private DSA key. If the device already has DSA keys, a warning and prompt to replace the existing keys with new keys is displayed.

The maximum supported size for the DSA key is 1,024.

This command is not saved in the startup configuration; however, the keys generated by this command are saved in the running configuration, which is never displayed to the user or backed up to another device.

This command may take a considerable period of time to execute.

Example

The following example generates DSA key pairs.

```
Console (config)# crypto key generate dsa
```

crypto key generate rsa

The **crypto key generate rsa** global configuration command generates RSA key pairs.

Syntax

crypto key generate rsa

Default Configuration

RSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

RSA keys are generated in pairs: one public RSA key and one private RSA key. If the device already has RSA keys, a warning and prompt to replace the existing keys with new keys is displayed.

The maximum supported size for the DSA key is 2,048.

This command is not saved in the startup configuration; however, the keys generated by this command are saved in the running configuration, which is never displayed to the user or backed up to another device.

This command may take a considerable period of time to execute.

Example

The following example generates RSA key pairs.

```
Console (config)# crypto key generate rsa
```

ip ssh pubkey-auth

The **ip ssh pubkey-auth** global configuration command enables public key authentication for incoming SSH sessions. To disable this function, use the **no** form of this command.

Syntax

ip ssh pubkey-auth

no ip ssh pubkey-auth

Default Configuration

The function is disabled.

Command Mode

Global Configuration mode

User Guidelines

AAA authentication is independent.

Example

The following example enables public key authentication for incoming SSH sessions.

```
Console (config)# ip ssh pubkey-auth
```

crypto key pubkey-chain ssh

The **crypto key pubkey-chain ssh** global configuration command enters SSH Public Key-chain configuration mode. The mode is used to manually specify other device public keys such as SSH client public keys.

Syntax

crypto key pubkey-chain ssh

Default Configuration

By default, there are no keys.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters the SSH Public Key-chain configuration mode.

```
Console(config)# crypto key pubkey-chain ssh

Console(config-pubkey-chain)#
```

user-key

The **user-key** SSH public key chain configuration command specifies which SSH public key is manually configured and enters the SSH public key-string configuration command. To remove a SSH public key, use the **no** form of this command.

Syntax

user-key *username* {**rsa** | **dsa**}

no user-key *username*

- *username*—Specifies the remote SSH client username, which can be up to 48 characters long.
- **rsa**—RSA key.
- **dsa**—DSA key.

Default Configuration

By default, there are no keys.

Command Mode

SSH Public Key Chain Configuration mode

User Guidelines

Follow this command with the key-string command to specify the key.

Example

The following example enables a SSH public key to be manually configured for the SSH public key chain called "bob".

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)#
```

key-string

To specify the authentication string for a key, use the key-string key configuration command. To remove the authentication string, use the no form of this command.

Syntax

key-string text

no key-string

- text-Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain 1 to 16 characters.

Default Configuration

By default, the key-string is empty.

Command Mode

Key configuration

User Guidelines

There are no user guidelines for this command.

Example

The following example enters public key strings for SSH public key clients called "bob".

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh


Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

show ip ssh

The **show ip ssh** privileged EXEC command displays the SSH server configuration.

Syntax

show ip ssh

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the SSH server configuration.

```
Console# show ip ssh
SSH server enabled. Port: 22
RSA key was generated.
DSA (DSS) key was generated.
SSH Public Key Authentication is enabled.
Active incoming sessions:
IP address SSH username Version Cipher Auth Code
---------- ------------ ------- ------ ---------
172.16.0.1 John Brown   2.0 3   DES     HMAC-SH1
```

The following table describes the significant fields shown in the display:

Field	Description
IP address	Client address
SSH username	User name
Version	SSH version number
Cipher	Encryption type (3DES, Blowfish, RC4)
Auth Code	Authentication Code (HMAC-MD5, HMAC-SHA1)

show crypto key mypubkey

The **show crypto key mypubkey** privileged EXEC command displays the SSH public keys on the device.

Syntax

show crypto key mypubkey [**rsa** | **dsa**]

- **rsa**—RSA key.
- **dsa**—DSA key.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the SSH public keys on the device.

```
Console# show crypto key mypubkey rsa

RSA key data:

005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B
55D6AB22

04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C
73A05DD2

BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301
87685768

Fingerprint(Hex): 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86

Fingerprint(Bubble Babble): yteriuwt jgkljhglk yewiury hdskjfryt
gfhkjglk
```

show crypto key pubkey-chain ssh

The **show crypto key pubkey-chain ssh** privileged EXEC command displays SSH public keys stored on the device.

Syntax

show crypto key pubkey-chain ssh [**username** *username*] [**fingerprint bubble-babble | hex**]

- *username*—Specifies the remote SSH client username.
- **bubble-babble**—Fingerprints in Bubble Babble format.
- **hex**—Fingerprint in Hex format. If fingerprint is unspecified, it defaults to Hex format.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays all SSH public keys stored on the device.

```
Console# show crypto key pubkey-chain ssh

Username Fingerprint

-------- ---------------------------------------------------

bob      9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86

john     98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8
```

The following example displays the SSH public called "bob".

```
Console# show crypto key pubkey-chain ssh username bob

Username: bob

Key: 005C300D 06092A86 4886F70D 01010105 00034B00 30480241
00C5E23B 55D6AB22 04AEF1BA A54028A6 9ACC01C5 129D99E4

Fingerprint: 9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
```

29

Syslog Commands

logging on

The **logging on** global configuration command controls error messages logging. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the process that generated the messages. To disable the logging process, use the **no** form of this command.

Syntax

logging on

no logging on

Default Configuration

Logging is enabled.

Command Mode

Global Configuration mode

User Guidelines

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or syslog server. Logging on and off for these destinations can be individually configured using the **logging buffered**, **logging file**, and **logging** global configuration commands. However, if the **logging on** command is disabled, no messages are sent to these destinations. Only the console receives messages.

Example

The following example shows how logging is enabled.

```
Console (config)# logging on
```

logging

The **logging** global configuration command logs messages to a syslog server. To delete the syslog server with the specified address from the list of syslogs, use the **no** form of this command.

Syntax

logging *ip-address* [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]

no logging *ip-address*

- *ip-address*—Host IP address used as a syslog server or URL of the syslog server.
- *port*—Port number for syslog messages. If unspecified, the port number defaults to 514. (Range: 1 - 65535)

- **severity** *level*—Limits the logging of messages to the syslog servers to a specified level: **emergencies, alerts**, **critical**, **errors, warnings**, **notifications, informational** and **debugging**. If unspecified, the default level is **errors**.
- *facility*—The facility that is indicated in the message. Can be one of the following values: **local0, local1, local2, local3, local4, local5, local 6, local7**. If unspecified, the port number defaults to **local7**.
- *text*—Syslog server description, which can be up to 64 characters.

Default Configuration

As described in the field descriptions.

Command Mode

Global Configuration mode

User Guidelines

Multiple syslog servers can be used.

If no specific severity level is specified, the global values apply to each server.

To define a logging server on the out-of-band port, use the out-of-band IP address format — **oob/ip-address**.

Example

The following example configures messages with a "critical" severity level so that they are logged to a syslog server with an IP address 10.1.1.1.

```
Console (config)# logging 10.1.1.1 severity critical
```

logging console

The **logging console** global configuration command limits messages logged to the console based on severity. To disable logging to the console terminal, use the **no** form of this command.

Syntax

logging console *level*

no logging console

- *level*—Limits the logging of messages displayed on the console to a specified level: **emergencies, alerts**, **critical**, **errors, warnings**, **notifications, informational, debugging.**

Default Configuration

The default is **informational**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example limits messages logged to the console based on severity level "errors".

```
Console (config)# logging console errors
```

logging buffered

The **logging buffered** global configuration command limits syslog messages displayed from an internal buffer based on severity. To cancel the buffer use, use the **no** form of this command.

Syntax

logging buffered *level*

no logging buffered

- *level*—Limits the message logging to a specified level buffer: **emergencies, alerts**, **critical**, **errors, warnings**, **notifications, informational, debugging.**

Default Configuration

The default level is **informational**.

Command Mode

Global Configuration mode

User Guidelines

All the syslog messages are logged to the internal buffer. This command limits the commands displayed to the user.

Example

The following example limits syslog messages displayed from an internal buffer based on the severity level "debugging".

```
Console (config)# logging buffered debugging
```

logging buffered size

The **logging buffered size** global configuration command changes the number of syslog messages stored in the internal buffer. To return the number of messages stored in the internal buffer to the default value, use the **no** form of this command.

Syntax

logging buffered size *number*

no logging buffered size

- *number*—Numeric value indicating the maximum number of messages stored in the history table. (Range: 20 - 400)

Default Configuration

The default number of messages is 200.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example changes the number of syslog messages stored in the internal buffer to 300.

```
Console (config)# logging buffered size 300
```

clear logging

The **clear logging** privileged EXEC command clears messages from the internal logging buffer.

Syntax

clear logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears messages from the internal syslog message logging buffer.

```
Console# clear logging

Clear logging buffer [y/n] y
```

logging file

The **logging file** global configuration command limits syslog messages sent to the logging file based on severity. To cancel the buffer, use the **no** form of this command.

Syntax

logging file *level*

no logging file

- *level*—Limits the logging of messages to the buffer to a specified level: **emergencies, alerts**, **critical**, **errors, warnings**, **notifications, informational** and **debugging.**

Default Configuration

The default severity level is **errors**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example limits syslog messages sent to the logging file based on the severity level "alerts".

```
Console (config)# logging file alerts
```

clear logging file

The **clear logging file** privileged EXEC command clears messages from the logging file.

Syntax

clear logging file

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears messages from the logging file.

```
Console# clear logging file

Clear Logging File [y/n]y
```

aaa logging

The **aaa logging** global configuration command enables logging AAA login events. To disable logging AAA login events, use the **no** form of this command.

Syntax

aaa logging login

no aaa logging login

- **login**—Indicates logging messages related to successful login events, unsuccessful login events and other login-related events.

Default Configuration

Logging AAA login events is enabled.

Command Mode

Global Configuration mode

User Guidelines

Other types of AAA events are not subject to this command.

Example

The following example enables logging messages related to AAA login events.

```
Console(config)# aaa logging login
```

file-system logging

The **file-system logging** global configuration command enables logging file system events. To disable logging file system events, use the **no** form of this command.

Syntax

file-system logging copy

no file-system logging copy

- **copy**—Indicates logging messages related to file copy operations.

Default Configuration

Logging file system events is enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables logging messages related to file copy operations.

```
Console(config)# file-system logging copy
```

management logging

The **management logging** global configuration command enables logging management access list (ACL) events. To disable logging management access list events, use the **no** form of this command.

Syntax

management logging deny

no management logging deny

- **deny**—Indicates logging messages related to deny actions of management ACLs.

Default Configuration

Logging management ACL events is enabled.

Command Mode

Global Configuration mode

User Guidelines

Other types of management ACL events are not subject to this command.

Example

The following example enables logging messages related to deny actions of management ACLs.

```
Console(config)# management logging deny
```

show logging

The **show logging** privileged EXEC command displays the state of logging and the syslog messages stored in the internal buffer.

Syntax

show logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the state of logging and the syslog messages stored in the internal buffer.

```
Console # show logging

Logging is enabled.

Console logging: level debugging. Console Messages: 0 Dropped
(severity).

Buffer logging: level debugging. Buffer Messages: 11 Logged, 200
Max.

File logging: level notifications. File Messages: 0 Dropped
(severity).

Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped
(severity).

Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped
(severity).

OOB Syslog server 176.16.8.9 logging: errors. Messages: 6 Dropped
(severity).

2 messages were not logged (resources)
```

```
Application filtering control
-----------------------------
Application      Event          Status
-----------      -----          ------
AAA              Login          Enabled
File system      Copy           Enabled
Management ACL   Deny           Enabled


Buffer log:
11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface FastEthernet g1,
changed state to up
11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface Ethernet g1,
changed state to up
11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface Ethernet g1,
changed state to up
11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface Ethernet g2,
changed state to up
11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface Ethernet g3,
changed state to up
11-Aug-2005  15:41:43: %SYS-5-CONFIG_I: Configured from memory by
console
11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet g1, changed state to up
11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g1, changed state to down
11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g1, changed state to down
11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g2, changed state to down
11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g3, changed state to down
```

show logging file

The **show logging file** privileged EXEC command displays the state of logging and the syslog messages stored in the logging file.

Syntax

show logging file

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the state of logging and the syslog messages stored in the logging file.

```
Console # show logging file

Logging is enabled.

Console logging: level debugging. Console Messages: 0 Dropped
(severity).

Buffer logging: level debugging. Buffer Messages: 11 Logged, 200
Max.

File logging: level notifications. File Messages: 0 Dropped
(severity).

Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped
(severity).

Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped
(severity).

OOB Syslog server 176.16.8.9 logging: errors. Messages: 6 Dropped
(severity).

2 messages were not logged (resources)
```

```
Application filtering control
-----------------------------
Application           Event                 Status
-----------           -----                 ------
AAA                   Login                 Enabled
File system           Copy                  Enabled
Management ACL        Deny                  Enabled


File log:
11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface FastEthernet g1,
changed state to up
11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface Ethernet g1,
changed state to up
11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface Ethernet g1,
changed state to up
11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface Ethernet g2,
changed state to up
11-Aug-2005  15:41:43: %LINK-3-UPDOWN: Interface Ethernet g3,
changed state to up
11-Aug-2005  15:41:43: %SYS-5-CONFIG_I: Configured from memory by
console
11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet g1, changed state to up
11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g1, changed state to down
11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g1, changed state to down
11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g2, changed state to down
11-Aug-2005  15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g3, changed state to down
```

show syslog-servers

The show syslog-servers privileged EXEC command displays the syslog servers settings.

Syntax

show syslog-servers

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the syslog server settings.

```
Console# show syslog-servers


IP address     Port Severity     Facility   Description
------------- ---- ----------   --------    -----------
192.180.2.275  14  Informational local      7
192.180.2.285  14  Warning       local      7
```

30

System Management

ping

The **ping** user EXEC command sends ICMP echo request packets to another node on the network.

Syntax

ping *host* [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*] st

- *host*—IP address being contacted.
- *packet_size*—Number of bytes in a packet, from 56 to 1,472 bytes. The actual packet size is eight bytes larger than the size specified because the switch adds header information.
- *packet_count*—Number of packets to send, from 1 to 65,535 packets. If 0 is entered it pings until stopped.
- *time_out*—Timeout in milliseconds to wait for each reply, from 1 to 65,535 milliseconds.

Default Configuration

The default packet size is 56 bytes.

The default packet count is 4 packets.

The default time-out is 1,000 milliseconds.

Command Mode

User EXEC mode

User Guidelines

Press **Ctrl-C** to stop pinging. Following are sample results of the **ping** command:

- *Destination does not respond*—If the host does not respond, a "`no answer from host`" message appears in 10 seconds.
- *Destination unreachable*—The gateway for this destination indicates that the destination is unreachable.
- *Network or host unreachable*—The switch found no corresponding entry in the route table.

To ping an out-of-band IP address, use the out-of-band IP address format — **oob/ip-address**.

Examples

The following example displays a ping to IP address 10.1.1.1.

```
Console# ping 10.1.1.1
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
^C
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
Console>
```

The following example displays a ping to out-of-band management port 176.16.1.1.

```
Console# ping oob/176.16.1.1
64 bytes from oob/176.16.1.1: icmp_seq=0. time=5 ms
64 bytes from oob/176.16.1.1: icmp_seq=1. time=5 ms
64 bytes from oob/176.16.1.1: icmp_seq=2. time=5 ms
64 bytes from oob/176.16.1.1: icmp_seq=3. time=5 ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 5/5/5
```

reload

The **reload** privileged EXEC command reloads the operating system.

Syntax

reload

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example reloads the operating system.

```
Console# reload
```

clock set

The **clock set** privileged EXEC command manually sets the system clock.

Syntax

clock set *hh:mm:ss day month year*

or

clock set *hh:mm:ss month day year*

- *hh:mm:ss*—Current time in hours (military format), minutes, and seconds (0 - 23, mm: 0 - 59, ss: 0 - 59).
- *day*—Current day (by date) in the month (1 - 31).
- *month*—Current month using the first three letters by name (Jan, …, Dec).
- *year*—Current year (1998 - 2097).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the system time to 13:32:00 on the 7th March 2005 .

```
Console# clock set 13:32:00 7 Mar 2005
```

hostname

The **hostname** global configuration command specifies or modifies the device host name. To remove the existing host name, use the **no** form of the command.

Syntax

hostname *name*

no hostname

- *name*—The device host name. (Range: 1-159 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the device host name.

```
Console (config)# hostname Dell
```

asset-tag

The **asset-tag** global configuration command specifies the device asset tag. To remove the existing asset tag, use the **no** form of the command.

Syntax

asset-tag *tag*

no asset-tag

- *tag*—The device asset tag.

Default Configuration

This command has no default configuration. No asset tag is defined by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the device asset tag as "1qwepot".

```
Console (config)# asset-tag 1qwepot
```

show users

The **show users** user EXEC command displays information about the active users.

Syntax

show users

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information about the active users.

```
Console# show users
Username    Protocol     Location
----------- ---------    ---------
Bob         Serial
John        SSH          172.16.0.1
Robert      HTTP         172.16.0.8
```

show clock

The **show clock** user EXEC command displays the time and date from the system clock.

Syntax

show clock

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the time and date from the system clock.

```
Console# show clock


15:29:03 Jun 17 2005
```

show system

The **show system** user EXEC command displays system information.

Syntax

show system

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the system information.

```
Console> show system
System Description:                       Ethernet Switch
System Up Time (days,hour:min:sec):       0,00:00:17
System Contact:
System Name:
System Location:
System MAC Address:                       00:00:b0:00:00:00
Sys Object ID:                         1.3.6.1.4.1.674.10895.3006
Type: PowerConnect 3424

         FAN                 Status
--------------------- ---------------------
        Fan 1                  OK
        Fan 2                  OK


    Power supply             Source                Status
--------------------- --------------------- ---------------------
    PowerSupply 1       Internal redundant           OK
    PowerSupply 2       Internal redundant           OK


         Sensor           Temperature (Celsius)            Status
------------------------ ------------------------ ---------------
           1                        38                       ok
           2                        36                       ok
```

show version

The **show version** user EXEC command displays the system version information.

Syntax

show version

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays a system version (this version number is only for demonstration purposes).

```
Console> show version

SW version x.x.x.xx (date xx-xxx-xxxx time 17:34:19)

Boot version x.x.x.xx (date xx-xxx-xxxx time 11:48:21)

HW version x.x.x
```

show system id

The **show system id** user EXEC command displays the ID information.

Syntax

show system id

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

The tag information is on a device by device basis.

Example

The following example displays the system service tag information.

```
Console> show system id
Service Tag: 89788978
Serial number: 8936589782
Asset tag: 7843678957
```

traceroute

The **traceroute** user EXEC command discovers the IP routes that packets actually take when traveling to their destinations.

Syntax

traceroute {*ip-address* |*hostname* }[**size** *packet_size*] [**ttl** *max-ttl*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *ip-address*] [**tos** *tos*]

- *ip-address* — Valid IP address of the destination host. For information on specifying an out-of-band IP address, see the user guidelines.
- *hostname* — Hostname of the destination host. (Range: 1 - 158 characters)
- *packet_size* — Number of bytes in a packet. (Range: 40-1472)
- *max-ttl* — The largest TTL value that can be used. The **traceroute** user EXEC command terminates when the destination is reached or when this value is reached. (Range:1-255)
- *packet_count* — The number of probes to be sent at each TTL level. (Range:1-10)
- *time_out* — The number of seconds to wait for a response to a probe packet. (Range:1-60)
- *ip-address* — One of the interface addresses of the device to use as a source address for the probes. The device will normally pick the valid IP address it considers to be the best source address to use.
- *tos* — The Type-Of-Service byte in the IP Header of the packet. (Range: 0-255)

Default Configuration

packet_size — The default is 40 bytes.

max-ttl — The default is 30.

packet_count — The default count is 3.

time_out — The default is 3 seconds.

Command Mode

User EXEC mode

User Guidelines

The **traceroute** command takes advantage of the error messages generated by a router when a datagram exceeds its time-to-live (TTL) value.

The **traceroute** user EXEC command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The **traceroute** command sends several probes at each TTL level and displays the round-trip time for each.

The **traceroute** user EXEC command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A "time exceeded" error message indicates that an intermediate router has seen and discarded the probe. A "destination unreachable" error message indicates that the destination router has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the **traceroute** user EXEC command prints an asterisk (*).

The **traceroute** user EXEC command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with Esc.

If you want to find the trace to an out-of-band address, use the out-of-band IP address format **oob**/*ip-address*.

Examples

The following example discovers the routes that packets will actually take when traveling to their destination.

```
Console> traceroute umaxp1.physics.lsa.umich.edu
Type Esc to abort.
Tracing the route to umaxp1.physics.lsa.umich.edu (141.211.101.64)
   1 i2-gateway.stanford.edu (192.68.191.83)  0 msec 0 msec 0 msec
   2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
   3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
   4 Abilene--QSV.POS.calren2.net (198.32.249.162)  1 msec 1 msec 1 msec
   5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103)  33 msec 35 msec 35
msec
   6 iplsng-kscyng.abilene.ucaid.edu (198.32.8.80)   47 msec 45 msec 45
msec
   7 so-0-2-0x1.aa1.mich.net (192.122.183.9)  56 msec  53 msec 54 msec
   8 atm1-0x24.michnet8.mich.net (198.108.23.82)  56 msec 56 msec 57 msec
   9 * * *
  10 A-ARB3-LSA-NG.c-SEB.umnet.umich.edu (141.211.5.22) 58 msec 58 msec
58 msec
  11 umaxp1.physics.lsa.umich.edu (141.211.101.64)  62 msec 63 msec 63
msec


Trace completed
```

The following table describes the significant fields shown in the display

Field	Description
1	Indicates the sequence number of the router in the path to the host.
i2-gateway.stanford.edu	Host name of this router.
192.68.191.83	IP address of this router.
1 msec 1 msec 1 msec	Round-trip time for each of the probes that are sent.

The following table describes the characters that can appear in the **traceroute** user EXEC command output.

Field	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
F	Fragmentation is required, and DF is set.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
R	Fragement reassembly time exeeded.
S	Source route failed.
U	Port unreachable.

telnet

The **telnet** user EXEC command logs into a host that supports Telnet.

Syntax

telnet {*ip-address* **|** *hostname*} [*port*] [*keyword1*......]

- *ip-address* — Valid IP address of the destination host. For information on specifying an out-of-band IP address, see the user guidelines.
- *hostname* — Hostname of the destination host. (Range: 1 - 158 characters)
- *port* — A decimal TCP port number, or one of the keywords from the ports table in the user guidelines.
- *keyword* — One or more keywords from the keywords table in the user guidelines.

Default Configuration

port — Telnet port (decimal 23) on the host.

Command Mode

User EXEC mode

User Guidelines

Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, press Esc and then a command character.

The command shows the telnet sessions to remote hosts that were opened by the present telnet session to the local device. It would not show telnet sessions to remote hosts that were opened by other telnet sessions to the local device.

Special Telnet Command Characters

Escape Sequence	Purpose
[Ctrl-Shift-6] b	Break
[Ctrl-Shift-6] c	Interrupt Process (IP)
[Ctrl-Shift-6] h	Erase Character (EC)
[Ctrl-Shift-6] o	Abort Out (AO)
[Ctrl-Shift-6] t	Are You There? (AYT)
[Ctrl-Shift-6] u	Erase Line (EL)

At any time during an active Telnet session, Telnet commands can be listed by pressing the Ctrl-Shift-6 keys followed by a question mark at the system prompt.

Following is a sample of the Telnet command list.

```
Console> ^^?
[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP
^^ H sends telnet EC
^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
^^ x suspends the session (return to system command prompt)
```

Several concurrent Telnet sessions can be opened and switched. To open a subsequent session, the current connection has to be suspended by pressing the escape sequence ‘Ctrl-Shift-6’ and ‘x’ to return to the system command prompt. Then open a new connection using the **telnet** command.

To log into a host on the out-of-band port, use the out-of-band format **oob**/*ip-address*.

Keywords Table

Options	Description
/echo	Enables local echo
/quiet	Prevents onscreen display of all messages from the software.
/source-interface	Specifies the source interface.
/stream	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
Ctrl-shift-6 x	Returns to the system command prompt

Port Table

Keyword	Description	Port Number
bgp	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119

pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

Example

Following is an example of using the **telnet** command to connect to 176.213.10.50.

```
Console> telnet 176.213.10.50

Esc U sends telnet EL
```

resume

The **resume** user EXEC command is used to switch to another open Telnet session.

Syntax

resume [*connection*]

- *connection* — The connection number. (Range: 1 - 4)

Default Configuration

The default is the most recent Telnet connection.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following command switches to another open Telnet session number 1.

```
console> resume 1
```

31

TACACS+ Commands

tacacs-server host

The **tacacs-server host** global configuration command specifies a TACACS+ server host. To delete the specified hostname or IP address, use the **no** form of this command.

Syntax

tacacs-server host {*ip-address* | *hostname*} [**single-connection**] [**port** *port-number*] [**timeout** *timeout*] [**key** *key-string*] [**source** *source*] [**priority** *priority*]

no tacacs-server host {*ip-address* | *hostname*}

- *ip-address*—The IP address of the TACACS+ server.
- *hostname*—The hostname of the TACACS+ server (Range: 1-158 characters).
- **single-connection—**Specify single-connection to maintain a single open connection between the device and the TACACS+ daemon.
- *port-number*—The TACACS+ server port number. If unspecified, the port number defaults to 49 (Range: 0-65535).
- *timeout*—The timeout value in seconds. If no timeout value is specified, the global value is used (Range: 1-30).
- *key-string*—The authentication and encryption key for all TACACS communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. If no key value is specified, the global value is used. Type "" to specify an empty string (Range: 0-128).
- *source*—The source IP address to use for communication. If no source IP value is specified, the global value is used. Specify 0.0.0.0 to use the IP address of the outgoing interface. See the user guidelines for information on specifying an out-of-band IP address.
- *priority*—Determines the order in which the servers are used, where 0 is the highest priority. (Range: 0-65535)

Default Configuration

No TACACS+ host is specified.

Command Mode

Global Configuration mode

User Guidelines

To specify multiple hosts, multiple **tacacs-server host** global configuration commands can be used.

If no host-specific timeout, key or source values are specified, the global values apply to each host.

To define a TACACS+ server on the out-of-band port, use the out-of-band IP address format: **oob**/ip-address.

Example

The following example specifies a TACACS+ host:

```
Console(config)# tacacs-server host 172.16.1.1
```

tacacs-server key

The **tacacs-server key** global configuration command sets the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ daemon. To disable the key, use the **no** form of this command.

Syntax

tacacs-server key [*key-string*]

no tacacs-server key

- *key-string*—The authentication and encryption key for all TACACS communications between the router and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon (Range: 0-128).

Default Configuration

The default is an empty string.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the authentication encryption key:

```
Console(config)# tacacs-server key dell-s
```

tacacs-server source-ip

The **tacacs-server source-ip** global configuration command specifies the source IP address used for communication with TACACS+ servers. To return to the default, use the **no** form of this command.

Syntax

tacacs-server source-ip *source*

no tacacs-server-ip *source*

- *source*—The source IP address.

Default Configuration

The default IP address is the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

To define an out-of-band IP address, use the out-of-band IP address format: **oob**/*ip-address*.

Example

The following example specifies the source IP address:

```
Console(config)# tacacs-server source-ip 172.16.8.1
```

tacacs-server timeout

The **tacacs-server timeout** global configuration command sets the interval during which a router waits for a server host to reply. To restore the default, use the **no** form of this command.

Syntax

tacacs-server timeout *timeout*

no tacacs-server timeout

- *timeout*—The timeout value in seconds. (Range: 1 - 30)

Default Configuration

The default value is 5 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the timeout value as 30:

```
Console(config)# tacacs-server timeout 30
```

show tacacs

The **show tacacs** privileged EXEC command displays the configuration and statistics of a TACACS+ server.

Syntax

show tacacs [*ip-address*]

- *ip-address*—The IP address of the TACACS+ server.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays TACACS+ server settings.

```
Console# show tacacs



IP address   Status      Port  Single      TimeOut Source  Priority
                               Connection          IP

----------   ---------   ----  ----------  ------- ------  --------

172.16.1.1   Connected   49    No          Global  Global  1


OOB TACACS servers

IP address   Status      Port  Single      TimeOut Source  Priority
                               Connection          IP

----------   ---------   ----  ----------  ------- ------  --------

172.16.1.1   Connected   49    No          Global  Global  1
```

```
Global values
-------------
TimeOut: 3
Source IP: 172.16.8.1
OOB Source IP: 172.16.8.1
```

32

User Interface

enable

The **enable** user EXEC command enters the privileged EXEC mode.

Syntax

enable [*privilege-level*]

- *privilege-level*—Privilege level to enter the system. (Range: 1 - 15)

Default Configuration

The default privilege level is 15.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to enter privileged mode:

```
Console> enable
enter password:
Console#
```

disable

The **disable** privileged EXEC command returns to User EXEC mode.

Syntax

disable [*privilege-level*]

- *privilege-level*—Privilege level to enter the system. (Range: 1 - 15)

Default Configuration

The default privilege level is 1.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to return to normal mode.

```
Console# disable

Console>
```

login

The **login** user EXEC command changes a login username.

Syntax

login

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to enter privileged EXEC mode and login.

```
Console> login

User Name:admin

Password:*****


Console#
```

exit(configuration)

The **exit** command exits any configuration mode to the next highest mode in the CLI mode hierarchy.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

All command modes

User Guidelines

There are no user guidelines for this command.

Example

The following example changes the configuration mode from Interface Configuration mode to User EXEC mode.

```
Console(config-if)# exit

Console(config)# exit

Console#
```

exit(EXEC)

The **exit** user EXEC command closes an active terminal session by logging off the device.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

User EXEC command mode

User Guidelines

There are no user guidelines for this command.

Example

The following example closes an active terminal session.

```
Console> exit
```

end

The **end** global configuration command ends the current configuration session and returns to the privileged command mode.

Syntax

end

Default Configuration

This command has no default configuration.

Command Mode

All Command modes

User Guidelines

There are no user guidelines for this command.

Example

The following example ends the current configuration session and returns to the previous command mode.

```
Console (config)# end

Console #
```

help

The **help** command displays a brief description of the help system.

Syntax

help

Default Configuration

This command has no default configuration.

Command Mode

All Command modes

User Guidelines

There are no user guidelines for this command.

history

The **history** line configuration command enables the command history function for a particular line. To disable the command history function, use the **no** form of this command.

Syntax

history

no history

Default Configuration

The history function is enabled.

Command Mode

Line Configuration mode

User Guidelines

This command enables the command history function for a specified line. To enable or disable the command history function for the current terminal session, use the **terminal history** user EXEC command.

Example

The following example enables the command history function for telnet.

```
Console (config)# line telnet

Console (config-line)# history
```

history size

The **history size** line configuration command configures the command history buffer size for a particular line. To reset the command history buffer size to the default, use the **no** form of this command.

Syntax

history size *number-of-commands*

no history size

- *number-of-commands*—Number of commands that the system records in its history buffer. (Range: 10 - 216)

Default Configuration

The default history buffer size is 10.

Command Mode

Line Configuration mode

User Guidelines

This command configures the command history buffer size for a particular line. To configure the command history buffer size for the current terminal session, use the **terminal history size** user EXEC command.

Example

The following example changes the command history buffer size to 100 entries for a particular line.

```
Console (config-line)# history size 100
```

debug-mode

The **debug-mode** privilege EXEC command switches the mode to debug.

Syntax

debug-mode

Default Configuration

This command has no default configuration.

Command Mode

Privilege EXEC command mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables the debug command interface.

```
Console(config)#

Console# debug

>debug

Enter DEBUG Password: *****

DEBUG>
```

show history

The **show history** user EXEC command lists the commands entered in the current session.

Syntax

show history

Default Configuration

This command has no default configuration.

Command Mode

User EXEC command mode

User Guidelines

The commands are listed from the first to the latest command.

The buffer is kept unchanged when entering to configuration mode and returning back.

Example

The following example displays all the commands entered while in the current privileged EXEC mode.

```
Console# show history
Console# show version
Console# show clock
```

show privilege

The **show privilege** user EXEC command displays the current privilege level.

Syntax

show privilege

Default Configuration

This command has no default configuration.

Command Mode

User EXEC command mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the current privilege level.

```
Console# show privilege
Current privilege level is 15
```

33

VLAN Commands

vlan database

The **vlan database** global configuration command enters the VLAN database configuration mode.

Syntax

vlan database

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters the VLAN database mode.

```
Console (config)# vlan database

Console (config-vlan)#
```

vlan

Use the **vlan** interface configuration (VLAN) command to create a VLAN. To delete a VLAN, use the **no** form of this command.

Syntax

vlan {*vlan-range*}

no vlan {*vlan-range*}

- *vlan-range*—A list of valid VLAN IDs to be added. List separate, non-consecutive VLAN IDs separated by commas (without spaces); use a hyphen to designate a range of IDs. (Range: 2 - 4063)

Default Configuration

This command has no default configuration.

Command Mode

VLAN Database mode

User Guidelines

There are no user guidelines for this command.

Example

The following example VLAN number 1972 is created.

```
Console (config)# vlan database
Console (config-vlan)# vlan 1972
```

interface vlan

The **interface vlan** global configuration command enters the interface configuration (VLAN) mode.

Syntax

interface vlan *vlan-id*

- *vlan-id*—The ID of an existing VLAN (excluding GVRP dynamic VLANs).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the VLAN 1 IP address of 131.108.1.27 and subnet mask 255.255.255.0.

```
Console (config)# interface vlan 1
Console (config-if)# ip address 131.108.1.27 255.255.255.0
```

interface range vlan

The **interface range vlan** global configuration command enters the interface configuration mode to configure multiple VLANs.

Syntax

interface range vlan {*vlan-range* | *all*}

- *vlan-range*—A list of valid VLAN IDs to add. Separate non consecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs.
- **all**—All existing static VLANs.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, an error message is displayed and execution continues on other interfaces.

Example

The following example groups VLAN 221 till 228 and VLAN 889 to receive the same command.

```
Console (config)# interface range vlan 221-228,889

Console (config-if)#
```

name

The **name** interface configuration command adds a name to a VLAN. To remove the VLAN name use the **no** form of this command.

Syntax

name *string*

no name

- *string*—Unique name, up to 32 characters in length, to be associated with this VLAN.

Default Configuration

No name is defined.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The VLAN name should be unique.

Example

The following example names VLAN number 19 with the name "Marketing".

```
Console (config)# interface vlan 19
Console (config-if)# name Marketing
```

switchport mode

The **switchport mode** interface configuration command configures the VLAN membership mode of a port. To reset the mode to the appropriate default for the device, use the **no** form of this command.

Syntax

switchport mode {**access** | **trunk** | **general**}

no switchport mode

- **access**—Port belongs to a single, untagged VLAN.
- **trunk**—Port belongs to 1..4063 VLANs, all tagged (except, optionally, for a single native VLAN).
- **general**—Port belongs to 1..4063 VLANs, and each VLAN is explicitly set by the user as tagged or untagged (full 802.1Q mode).

Default Configuration

All port are in access mode, and belong to the default VLAN (whose VID=1).

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures g8 as an untagged layer 2 VLAN interface.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport mode access
```

switchport access vlan

The **switchport access vlan** interface configuration command configures the VLAN ID when the interface is in access mode. To reconfigure the default, use the **no** form of this command.

Syntax

switchport access vlan *vlan-id*

no switchport access vlan

- *vlan-id*—VLAN ID of the VLAN to which the port is configured.

Default Configuration

VLAN ID=1

Command Mode

Interface configuration (Ethernet, port-channel) mode

User Guidelines

The command automatically removes the port from the previous VLAN, and adds it to the new VLAN.

Example

The following example configures a VLAN ID of 23 to the untagged layer 2 VLAN interface number g8.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport access vlan 23
```

switchport trunk allowed vlan

The **switchport trunk allowed vlan** interface configuration command adds or removes VLANs from a trunk port.

Syntax

switchport trunk allowed vlan {**add** *vlan-list* | **remove** *vlan-list*}

- **add** *vlan-list*—List of VLAN IDs to add. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list*—List of VLAN IDs to remove. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designate a range of IDs.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to add VLANs 2 and 5 to 8 to the allowed list of g8.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport trunk allowed vlan add 2,5-8
```

switchport trunk native vlan

The **switchport trunk native vlan** interface configuration command defines the port as a member of the specified VLAN, and the VLAN ID as the "port default VLAN ID (PVID)". To configure the default VLAN ID, use the **no** form of this command.

Syntax

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

- *vlan-id*—Valid VLAN ID of the active VLAN.

Default Configuration

VLAN ID=1

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has the following consequences: incoming untagged frames are assigned to this VLAN and outgoing traffic in this VLAN on this port is sent untagged (despite the normal situation where traffic sent from a trunk-mode port is all tagged).

The command adds the port as a member in the VLAN. If the port is already a member in the VLAN (not as a native), it should be first removed from the VLAN.

Example

The following example g8, in trunk mode, is configured to use VLAN number 123 as the "native" VLAN.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport trunk native vlan 123
```

switchport general allowed vlan

The **switchport general allowed vlan** interface configuration command adds or removes VLANs from a general port.

Syntax

switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]

switchport general allowed vlan remove *vlan-list*

- **add** *vlan-list*—List of VLAN IDs to add. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list*—List of VLAN IDs to remove. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **tagged**—Sets the port to transmit tagged packets for the VLANs. If the port is added to a VLAN without specifying tagged or untagged the default is tagged.
- **untagged**—Sets the port to transmit untagged packets for the VLANs.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to add VLANs 2, 5, and 6 to the allowed list.

```
Console (config)# interface ethernet g8

Console (config-if)# switchport general allowed vlan add 2,5,6
tagged
```

switchport general pvid

The **switchport general pvid** interface configuration command configures the PVID when the interface is in general mode. To configure the default value, use the **no** form of this command.

Syntax

switchport general pvid *vlan-id*

no switchport general pvid

- *vlan-id*—PVID (Port VLAN ID). The vlan-id may belong to a non-existent VLAN.

Default Configuration

VLAN ID=1

Command Mode

Interface configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to configure the PVID for g8, when the interface is in general mode.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport general pvid 234
```

switchport general ingress-filtering disable

The **switchport general ingress-filtering disable** interface configuration command disables port ingress filtering. To enable ingress filtering on a port, use the **no** form of this command.

Syntax

switchport general ingress-filtering disable

no switchport general ingress-filtering disable

Default Configuration

Ingress filtering is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to enables port ingress filtering on g8.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport general ingress-filtering disable
```

switchport general acceptable-frame-type tagged-only

The **switchport general acceptable-frame-type tagged-only** interface configuration command discards untagged frames at ingress. To enable untagged frames at ingress, use the **no** form of this command.

Syntax

switchport general acceptable-frame-type tagged-only

no switchport general acceptable-frame-type tagged-only

Default Configuration

All frame types are accepted at ingress.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures g8 to discard untagged frames at ingress.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport general acceptable-frame-type
tagged-only
```

switchport forbidden vlan

The **switchport forbidden vlan** interface configuration command forbids adding specific VLANs to a port. This may be used to prevent GVRP from automatically making these VLANs active on the selected ports. To revert to allowing the addition of specific VLANs to the port, use the **remove** parameter for this command.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}

- **add** *vlan-list*—List of VLAN IDs to add to the "forbidden" list. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list*—List of VLAN IDs to remove from the "forbidden" list. Separate non consecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Configuration

All VLANs allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example forbids adding VLANs number 234 till 256, to g8.

```
Console (config)# interface ethernet g8
Console (config-if)# switchport forbidden vlan add 234-256
```

switchport protected

The **switchport protected** interface configuration command overrides the FDB decision and sends all Unicast, Multicast and Broadcast traffic to an uplink port. To disable overriding the FDB decision, use the **no** form of this command.

Syntax

switchport protected {**ethernet** *port* **|** **port-channel** *port-channel-number* }

no switchport protected

- *port*—Specifies the uplink port (Ethernet port).
- *port-channel-number*—Specifies the uplink port (port-channel).

Default Configuration

Switchport protected is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel)

User Guidelines

Private VLAN Edge (PVE) supports private communication by isolating PVE-defined ports and ensuring that all Unicast, Broadcast and Multicast traffic from those ports is only forwarded to uplink port(s).

PVE requires only one VLAN on each device but not on every port; this reduces the number of VLANs required by the device. Private VLANs and the default VLAN can function simultaneously in the same device.

Example

The following example configures ethernet port g8 as a protected port, so that all traffic is sent to its uplink (ethernet port g9).

```
Console (config) # interface ethernet g9
Console (config-if) # switchport protected ethernet g8
```

map protocol protocols-group

The **map protocol protocols-group** VLAN database command adds a special protocol to a named group of protocols, which may be used for protocol-based VLAN assignment. To delete a protocol from a group, use the **no** form of this command.

Syntax

map protocol *protocol* [*encapsulation*] **protocols-group** *group*

no map protocol *protocol encapsulation*

- *protocol*—The protocol is a protocol number or one of the reserved names. The format is Hex format.
- *encapsulation*—One of the following values: **ethernet**, **rfc1042**, **llcOther**. If no option is indicated the default is **ethernet**.
- *group*—Group number of group of protocols associated together. (Range: 1 - 2147483647)

Default Configuration

This command has no default configuration.

Command Mode

VLAN Database mode

User Guidelines

The following protocol names are reserved:

- ip-arp
- ipx

Example

The following example maps protocol ip-arp to the group named "213".

```
Console (config)# vlan database
Console (config-vlan)# map protocol ip-arp protocols-group 213
```

switchport general map protocols-group vlan

The **switchport general map protocols-group vlan** interface configuration command sets a protocol-based classification rule. To delete a classification, use the **no** form of this command.

Syntax

switchport general map protocols-group *group* **vlan** *vlan-id*

no switchport general map protocols-group *group*

- *group*—Group number as defined in the **map protocol protocols-group** command. (Range: 1 - 2147483647)
- *vlan-id*—Define the VLAN ID in the classifying rule.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets a protocol-based classification rule of protocol group 1 to VLAN 8.

```
Console (config)# interface ethernet g8

Console (config-if)# switchport general map protocols-group 1 vlan
8
```

show vlan

The **show vlan** privileged EXEC command displays VLAN information.

Syntax

show vlan [**tag** *vlan-id* | **name** *vlan-name*]

- *vlan-id*—A valid VLAN ID
- *vlan-name*—A valid VLAN name string. (Range: 1 - 32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all VLAN information.

```
Console# show vlan
Vlan      Name      Ports                 Type
---- ------------ -------------------- ---------------------------
 1         1         g(1-22),ch(1-7)      other
 2         2         g(1-4)               permanent
 3         3         g(2-3,5,8-9)         permanent
```

show vlan internal usage

The **show vlan internal usage** privileged EXEC command displays a list of VLANs being used internally by the switch.

Syntax

show vlan internal usage

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all VLAN information.

```
Console# show vlan internal usage
VLAN      Usage
--------  ---------------
1008      Eth g21
1009      Eth g22
```

show vlan protocols-groups

The **show vlan protocols-groups** privileged EXEC command displays protocols-groups information.

Syntax

show vlan protocols-groups

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays protocols-groups information.

```
Console# show vlan protocols-groups
Encapsulation          Protocol              Group Id
-------------          --------              --------
ethernet               08 00                 213
ethernet               08 06                 213
ethernet               81 37                 312
ethernet               81 38                 312
rfc1042                08 00                 213
rfc1042                08 06                 213
```

show interfaces switchport

The **show interfaces switchport** privileged EXEC command displays switchport configuration.

Syntax

show interfaces switchport {**ethernet** *interface* | **port-channel** *port-channel-number*}

- *Interface*—Specific interface, such as ethernet g8.
- *port-channel-number*—Valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays switchport configuration individually for g1.

```
Console# show interface switchport ethernet g8

Port : g8

Port Mode: General

Gvrp Status: disabled

Ingress Filtering: true

Acceptable Frame Type: admitAll

Ingress Untagged Vlan ( NATIVE ): 1

Port is member in:

Vlan               Name               Egress rule Port Membership
Type

---- ---------------------------- ----------- ---------------

 1                  1                  Untagged System

 2                  2                  Untagged Static

 3                  3                   Tagged Static
```

```
Forbidden VLANS:
Vlan               Name
---- --------------------------------
 4                vlan4


Classification rules:


Group ID Vlan ID
-------- -------
```

34

VRRP Commands

vrrp ip

The **vrrp ip** interface configuration command defines Virtual Router Redundancy Protocol (VRRP) for an interface. To delete the definition, use the **no** form of this command.

Syntax

vrrp *virtual-router* **ip** *ip-address* [*ip-address2*…*ip-address8*]

no vrrp *virtual-router* **ip**

- *virtual-router*—Virtual router number on the interface for which VRRP is being defined. (Range: 1 - 255)
- *ip-address*—Virtual router IP address. Up to 8 IP addresses can be defined in one command line. One IP address is required.

Default Configuration

No Virtual Router is defined.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

This command cannot be used with a range of ports.

Example

The following example defines VRRP with the IP address 172.16.1.1 and 172.16.2.1 for port g8.

```
Console(config)# interface ethernet g8
Console(config-if)# vrrp 19 ip 172.16.1.1 172.16.2.1
```

vrrp up

The **vrrp up** interface configuration command activates Virtual Router Redundancy Protocol (VRRP) on an interface. To disable VRRP, use the **no** form of this command.

Syntax

vrrp *virtual-router* **up**

no vrrp *virtual-router* **up**

- *virtual-router*—Virtual router number on the interface for which VRRP is being activated. (Range: 1 - 255)

Default Configuration

VRRP is disabled

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

This command cannot be used with a range of ports.

Example

The following example enables VRRP number 45 on port g8.

```
Console(config)# interface ethernet g8

Console(config-if)# vrrp 45 up
```

vrrp timer

The **vrrp timer** interface configuration command configures the time between sending advertisements messages. To restore the timer to its default value, use the **no** form of this command.

Syntax

vrrp *virtual-router* **timer** *seconds*

no vrrp *virtual-router* **timer**

- *virtual-router*—Virtual router number. (Range: 1 - 255)
- *seconds*—The time interval, in seconds, between sending advertisements messages (Range: 1 - 255).

Default Configuration

The default time interval between sending advertisements messages is 1 second.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

This command cannot be used with a range of ports.

Example

The following example configures the time between sending advertisements messages for VRRP as a number from 45 to 100 seconds on g8.

```
Console(config)# interface ethernet g8
Console(config-if)# vrrp 45 timer 100
```

vrrp priority

The **vrrp priority** interface configuration command configures Virtual Router Redundancy Protocol (VRRP) priority on an interface. To restore the default priority value, use the **no** form of this command.

Syntax

vrrp *virtual-router* **priority** *priority*

no vrrp *virtual-router* **priority**

- *virtual-router*—Virtual router number. (Range: 1 - 255)
- *priority*—The priority used for the virtual router master election process. Higher values imply higher priority. (Range: 1 - 255)

Default Configuration

The default VRRP priority values are as follows:

- *Non-owner*—100
- *Owner*—255

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

This command cannot be used with a range of ports.

The owner priority cannot be modified, it is always 255.

Example

The following example configures VRRP number 45 priority to 150 on g8.

```
Console(config)# interface ethernet g8
Console(config-if)# vrrp 45 priority 150
```

vrrp source-ip

The **vrrp source-ip** interface configuration command defines the source IP address used for Virtual Router Redundancy Protocol (VRRP) messages on an interface. To return to default IP address, use the **no** form of this command.

Syntax

vrrp *virtual-router* **source-ip** *ip-address*

no vrrp *virtual-router* **source-ip**

- *virtual-router*—Virtual router number. (Range: 1 - 255)
- *ip-address*—IP address used for VRRP communication.

Default Configuration

The default VRRP message is the VRRP with the lowest IP address.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

This command cannot be used with a range of ports.

Example

The following example defines the source IP address 168.192.1.1 for VRRP messages on g8.

```
Console(config)# interface ethernet g8

Console(config-if)# vrrp 45 source-ip 168.192.1.1
```

vrrp authentication

The **vrrp authentication** interface configuration command enables authentication for the Virtual Router Redundancy Protocol (VRRP) on an interface. To disable authentication, use the **no** form of this command.

Syntax

vrrp *virtual-router* **authentication** *text*

no vrrp *virtual-router* **authentication**

- *virtual-router*—Virtual router number. (Range: 1 - 255)
- *text*—Password up to 8 characters.

Default Configuration

VRRP authentication default is disabled.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

This command cannot be used with a range of ports.

Example

The following example enables authentication for the VRRP number 45 with the password "Dell" on g8.

```
Console(config)# interface ethernet g8
Console(config-if)# vrrp 45 authentication Dell
```

vrrp preempt

The **vrrp preempt** interface configuration command enables the Virtual Router Redundancy Protocol (VRRP) preemption on an interface. To disable preemption, use the **no** form of this command.

Syntax

vrrp *virtual-router* **preempt**

no vrrp *virtual-router* **preempt**

- *virtual-router*—Virtual router number. (Range: 1 - 255)

Default Configuration

VRRP preemption is enabled.

Command Mode

Interface configuration (Ethernet, VLAN, port-channel)

User Guidelines

An exception is that the router that owns the IP address(es) associated with the virtual router always preempts independent of the setting of this command.

Example

The following example enables VRRP preemption on g8.

```
Console(config)# interface ethernet g8
Console(config-if)# vrrp 45 preempt
```

show vrrp configuration

The **show vrrp configuration** privileged EXEC command displays the Virtual Router Redundancy Protocol (VRRP) configuration.

Syntax

show vrrp configuration [**ethernet** *interface-number* **|** **vlan** *vlan-id* **|** **port-channel** *number*]

- **ethernet** *interface-number*—Ethernet port number.
- **vlan** *vlan-id*—VLAN number.
- **port-channel** *number*—Port-channel number.

Default Configuration

There are no user guidelines for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the VRRP configuration.

```
Console# show vrrp configuration

Interface VRID    Address     Priority Timer Auth Preempt    Source-ip
State

--------- ---- --------------- -------- ----- ---- ------- --------------



   g1      10     1.1.1.99       100      1    No    Yes       0.0.0.0
down
```

The following table describes the significant fields shown in the display:

Field	Description
Interface	Interface type and number.
VRID	Virtual Router Identifier.
Address	Virtual Router associated address.
Priority	Priority used for the virtual router master election.
Timer	The time interval, in seconds, between sending advertisement messages.
Auth	Displays if authentication is used.
Preempt	Displays whether a higher priority virtual router preempts a lower priority master.
Source-ip	Source IP address used in the VRRP messages.
State	Displays if the virtual router is up or down.

show vrrp status

The **show vrrp status** privileged EXEC command displays Virtual Router Redundancy Protocol (VRRP) status.

Syntax

show vrrp status [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]

- **ethernet** *interface-number*—Ethernet port number.
- **vlan** *vlan-id*—VLAN number.
- **port-channel** *number*—Port-channel number.

Default Configuration

There are no user guidelines for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures authentication login.

```
Console# show vrrp status
Interface VRID     Address       State         Master          MAC address
--------- ---- --------------- ---------- ---------------- --------------
-----
   g1      10     1.1.1.99     initialize     0.0.0.0
00:00:5e:00:01:0a
```

The following table describes the significant fields shown in the display:

Field	Description
Interface	Interface type and number.
VRID	Virtual Router Identifier.
Address	Virtual Router associated address.
State	The current state of the virtual router. It can be: Initialize, Backup, Master.
Master	The master router IP address.
MAC address	The virtual router, virtual MAC address.

35

Web Server

ip http port

The **ip http port** global configuration command specifies the TCP port for use by a web browser to configure the device. To use the default TCP port, use the **no** form of this command.

Syntax

ip http port *port-number*

no ip http port

- *port-number*—Port number for use by the HTTP server. (Range: 0 - 65535)

Default Configuration

This default port number is 80.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command. However, specifying 0 as the port number will effectively disable HTTP access to the device.

Example

The following example shows how the http port number is configured to 100.

```
Console (config)# ip http port 100
```

ip http server

The **ip http server** global configuration command enables the device to be configured from a browser. To disable this function use the **no** form of this command.

Syntax

ip http server

no ip http server

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables the device to be configured from a browser.

```
Console (config)# ip http server
```

ip https port

The **ip https port** global configuration command configures a TCP port for use by a secure web browser to configure the device. To use the default port, use the **no** form of this command.

Syntax

ip https port *port-number*

no ip https port

- *port-number*—Port number for use by the HTTP server. (Range: 0 - 65535)

Default Configuration

This default port number is 443.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the https port number to 100.

```
Console (config)# ip https port 100
```

ip https server

The **ip https server** global configuration command enables the device to be configured from a secured browser. To disable this function, use the **no** form of this command.

Syntax

ip https server

no ip https server

Default Configuration

The default for the device is disabled.

Command Mode

Global Configuration mode

User Guidelines

You must use the **crypto certificate generate** command to generate the HTTPS certificate.

Example

The following example enables the device to be configured from a browser.

```
Console (config)# ip https server
```

crypto certificate generate

The **crypto certificate generate** global configuration command generates a self-signed HTTPS certificate.

Syntax

crypto certificate [*number*] **generate** [**key-generate** [*length*]] [**passphrase** *string*] [**cn** *common-name*] [**ou** *organization-unit*] [**or** *organization*] [**loc** *location*] [**st** *state*] [**cu** *country*] [**duration** days]

- *number*—Specifies the certificate number. (Range: 2 characters)
- **key-generate**—Regenerates the SSL RSA key.
- *length*—Specifies the SSL RSA key length. (Range: 512 - 2048)
- *string*—Specifies the passphrase used to export the certificate in PKCS12 file format. If unspecified, the certificate cannot be exported. (Range: 8-96 characters)
- *common- name*—Specifies the fully qualified URL or IP address of the device. (Range: 1-64)
- *organization-unit*—Specifies the organizational unit or department name. (Range: 1-64)
- *organization*—Specifies the organization name. (Range: 1-64)
- *location*—Specifies the location or city name. (Range: 1-64)
- *state*—Specifies the state or province name. (Range: 1-64)
- *country*—Specifies the country name. (Range: 1-2)
- *days*—Specifies the number of days a certification is valid. (Range: 30-3650)

Default Configuration

The Certificate and SSL RSA key pairs do not exist.

number—The default value is 1.

length—The default value is 1024.

common- name—The default value is the lowest IP address of the device when the certificate is generated.

days—The default value is 365 days.

Command Mode

Global Configuration mode

User Guidelines

The command is not saved in the router configuration; however, the certificate and keys generated by this command are saved in the private configuration, which is never displayed to the user or backed up to another device.

Example

The following example regenerates a HTTPS certificate.

```
Console (enable)# crypto certificate generate key-generate
```

crypto certificate request

The **crypto certificate request** privileged EXEC command generates and displays a certificate request for HTTPS.

Syntax

crypto certificate *number* **request cn** [*common- name*] [**ou** *organization-unit*] [**or** *organization*] [**loc** *location*] [**st** *state*] [**cu** *country*]

- *number*—Specifies the certificate number. (Range: 2 characters)
- *common- name*—Specifies the fully qualified URL or IP address of the device. (Range: 1-64)
- *organization-unit*—Specifies the organizational unit or department name. (Range: 1-64)
- *organization*—Specifies the organization name. (Range: 1-64)
- *location*—Specifies the location or city name. (Range: 1-64)
- *state*—Specifies the state or province name. (Range: 1-64)
- *country*—Specifies the country name. (Range: 1-2)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request, you must first generate a self-signed certificate using the **crypto certificate generate** global configuration command. Make sure to re-enter values in the certificate fields.

After receiving the certificate from the Certification Authority, use the **crypto certificate import** global configuration command to import the certificate into the device. This certificate replaces the self-signed certificate.

Examples

The following example generates and displays a certificate request for HTTPS.

```
Console# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAxCzAJBgNVBAgTAkNDMQswCQYDVQQH
EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
DgKoZIhvcNAQkBFgFsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ
HdML0831i0fh/F0MV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTDekb2ymCu6K
aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QVl+8Ubx3GyCm
/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH
MRDjEyMwgICCAgICAICAgIMA0GCSqGSIb3DQEBBAUAA4GBAGb8UgIx7rB05m+2
m5ZZPhIwl8ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa
g+uNpyTkDt3ZVU72pjz/fa8TF0n3
-----END CERTIFICATE REQUEST-----
CN= router.gm.com
0= General Motors
C= US
```

crypto certificate import

The **crypto certificate import** global configuration command imports a certificate signed by the Certification Authority for HTTPS.

Syntax

crypto certificate *number* **import**

- *number*—Specifies the certificate number. (Range: 2 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Use this command to enter an external certificate (signed by the Certification Authority) to the device. To end the session, enter a blank line.

The imported certificate must be based on a certificate request created by the **crypto certificate request** privileged EXEC command.

If the public key found in the certificate does not match the device's SSL RSA key, the command fails.

This command is not saved in the router configuration; however, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another device).

Examples

The following example imports a certificate sighed by the Certification Authority for HTTPS.

```
Console(config)# crypto certificate 1 import
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----

Certificate imported successfully.
Issued to: router.gm.com
Issued by: www.verisign.com
Valid from: 8/9/2005  to 8/9/2005
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

ip https certificate

The **ip https certificate** global configuration command configures the active certificate for HTTPS. To return to the default setting, use the **no** form of this command .

Syntax

ip https certificate *number*

no ip https certificate

- *number*—Specifies the certificate number. (Range: 2 characters)

Default Configuration

The default value of the certificate number is 1.

Command Mode

Global Configuration mode

User Guidelines

The HTTPS certificate is generated using the **crypto certificate generate** global configuration command.

Examples

The following example configures the active certificate for HTTPS:

```
Console(config)# ip https certificate 1
```

show ip http

The **show ip http** privileged EXEC command displays the HTTP server configuration.

Syntax

show ip http

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC command

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the HTTP server configuration.

```
Console# show ip http

HTTP server enabled. Port: 80
```

show ip https

The **show ip http** privileged EXEC command displays the HTTPS server configuration.

Syntax

show ip https

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the HTTP server configuration.

```
Console# show ip https
HTTPS server enabled. Port: 443


Certificate 1 is active
Issued by: www.verisign.com
Valid from: 8/9/2005  to 8/9/2005
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788


Certificate 2 is inactive
Issued by: self-signed
Valid from: 8/9/2005  to 8/9/2005
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: 1873B936 88DC3411 BC8932EF 782134BA
```

36

802.1x Commands

aaa authentication dot1x

The **aaa authentication dot1x** global configuration command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1x. To return to the default setting, use the **no** form of this command.

Syntax

aaa authentication dot1x default *method1* [*method2*...]

no aaa authentication dot1x default

- *method1* [*method2*...]— At least one from the following table:

Keyword	Description
Radius	Uses the list of all RADIUS servers for authentication
None	Uses no authentication

Default Configuration

No authentication method is defined.

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

Examples

The following example uses the **aaa authentication dot1x default** command with no authentication:

```
Console(config)# aaa authentication dot1x default none
```

dot1x system-auth-control

The **dot1x system-auth-control** global configuration command enables 802.1x globally. To disable 802.1x globally, use the **no** form of this command.

Syntax

dot1x system-auth-control

no dot1x system-auth-control

Default Configuration

dot1x is disabled.

Command Modes

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example enables 802.1x globally:

```
Console(config)# dot1x system-auth-control
```

dot1x port-control

The **dot1x port-control** interface configuration command enables manual control of the authorization state of the port. To return to the default setting, use the **no** form of this command.

Syntax

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control

- **auto** — Enables 802.1x authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1x authentication exchange between the device and the client.
- **force-authorized** — Disables 802.1x authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port resends and receives normal traffic without 802.1x-based authentication of the client.
- **force-unauthorized** — Denies all access through this interface by forcing the port to transition to the unauthorized state, ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through the interface.

Default Configuration

Port is in the force-authorized mode

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

It is recommended to disable the spanning tree or to enable spanning-tree PortFast mode on 802.1x edge ports (ports in **auto** state that are connected to end stations), in order to go immediately to the forwarding state after successful authentication.

Examples

The following example enables 802.1x authentication on the interface:

```
Console(config)# interface ethernet g16

Console(config-if)# dot1x port-control auto
```

dot1x re-authentication

The **dot1x re-authentication** interface configuration command enables periodic re-authentication of the client. To return to the default setting, use the **no** form of this command.

Syntax

dot1x re-authentication

no dot1x re-authentication

Default Configuration

Periodic re-authentication is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example enables periodic re-authentication of the client:

```
Console(config)# interface ethernet g16

Console(config-if)# dot1x re-authentication
```

dot1x timeout re-authperiod

The **dot1x timeout re-authperiod** interface configuration command sets the number of seconds between re-authentication attempts. To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

- *seconds* — Number of seconds between re-authentication attempts. (Range: 300 - 4294967295)

Default Configuration

Re-authentication period is 3600 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example sets the number of seconds between re-authentication attempts, to 300:

```
Console(config)# interface ethernet g16

Console(config-if)# dot1x timeout re-authperiod 300
```

dot1x re-authenticate

The **dot1x re-authenticate** privileged EXEC mode command enables manually initiating a re-authentication of all 802.1x-enabled ports or the specified 802.1x-enabled port.

dot1x re-authenticate [**ethernet** *interface*]

- *interface* — Valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following command manually initiates a re-authentication of the 802.1x-enabled port:

```
Console# dot1x re-authenticate ethernet g16
```

dot1x timeout quiet-period

The **dot1x timeout quiet-period** interface configuration command sets the number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password). To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

- *seconds* — Time in seconds that the device remains in the quiet state following a failed authentication exchange with the client. (Range: 0 - 65535)

Default Configuration

The device remains in the quiet state for 60 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

During the quiet period, the device does not accept or initiate any authentication requests.

The default value of this command should only be changed to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients authentication servers.

To provide a faster response time to the user, a smaller number than the default should be entered.

Examples

The following example sets the number of seconds that the device remains in the quiet state following a failed authentication exchange to 3600:

```
Console(config)# interface ethernet g16
Console(config-if)# dot1x timeout quiet-period 3600
```

dot1x timeout tx-period

The **dot1x timeout tx-period** interface configuration command sets the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) - request/identity frame from the client before resending the request. To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

- *seconds* — Time in seconds that the device should wait for a response to an EAP - request/identity frame from the client before resending the request. (Range: 1 - 65535)

Default Configuration

The period of time is set to 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should only be changed to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Examples

The following command sets the number of seconds that the device waits for a response to an EAP-request/identity frame to 3600 seconds.

```
Console(config)# interface ethernet g16

Console(config-if)# dot1x timeout tx-period 3600
```

dot1x max-req

The **dot1x max-req** interface configuration command sets the maximum number of times that the device sends an Extensible Authentication Protocol (EAP) - request frame (assuming that no response is received) to the client before restarting the authentication process. To return to the default setting, use the **no** form of this command.

Syntax

dot1x max-req *count*

no dot1x max-req

- *count* — Number of times that the device sends an EAP - request/identity frame before restarting the authentication process. (Range: 1 - 10)

Default Configuration

Number of times is set to 2.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should only be changed to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Examples

The following example sets the number of times that the device sends an EAP-request/identity frame to 6:.

```
Console(config)# interface ethernet g16

Console(config-if)# dot1x max-req 6
```

dot1x timeout supp-timeout

The **dot1x timeout supp-timeout** interface configuration command sets the time that the device waits for a response before retransmitting an Extensible Authentication Protocol (EAP)-request frame to the client. To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

- *seconds* — Time in seconds that the device should wait for a response to an EAP-request frame from the client before resending the request. (Range: 1 - 65535)

Default Configuration

The period of time is set to 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Examples

The following example sets the time for the retransmission of an EAP-request frame to the client to 3600 seconds:

```
Console(config-if)# dot1x timeout supp-timeout 3600
```

dot1x timeout server-timeout

The **dot1x timeout server-timeout** interface configuration mode command sets the time that the device waits for a response from the authentication server before retransmitting packets. To return to the default setting, use the **no** form of this command..

Syntax

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

- *seconds* — Time in seconds that the device waits for a response from the authentication server. (Range: 1 - 65535)

Default Configuration

The period of time is set to 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example sets the time for the retransmission of packets to the authentication server., to 3600 seconds:

```
Console(config-if)# dot1x timeout server-timeout 3600
```

show dot1x

The **show dot1x** privileged EXEC command displays 802.1x status for the device or for the specified interface.

Syntax

show dot1x [**ethernet** *interface*]

- *interface* — Valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays 802.1x port g11 status.

```
Console# show dot1x

802.1x is enabled

Port     Admin Mode   Oper Mode        Reauth       Reauth     Username
                                       Control      Period
g1       Auto         Authorized       Ena          3600       Bob
g2       Auto         Authorized       Ena          3600       John
g3       Auto         Unauthorized     Ena          3600       Clark
g4       Force-Auth   Authorized       Dis          3600       n/a
g5       Force-Auth   Unauthorized*    Dis          3600       n/a

* Port is down or not present


Console# show dot1x ethernet g3

802.1x is enabled

Port     Admin Mode   Oper Mode        Reauth       Reauth     Username
                                       Control      Period
g3       Auto         Unauthorized     Ena          3600       Clark

Quiet period:            60 Seconds
```

```
Tx period:                 30 Seconds
Max req:                   2
Supplicant timeout:        30 Seconds
Server timeout:            30 Seconds
Session Time (HH:MM:SS):  08:19:17
MAC Address:               00:08:78:32:98:78
Authentication Method:     Remote
Termination Cause: Supplicant logoff

Authenticator State Machine
State:                   HELD

Backend State Machine
State:                   IDLE
Authentication success:   9
Authentication fails:     1
```

The following table describes the significant fields shown in the display:

Field	**Description**
Port	The port number.
Admin mode	The port admin mode. Possible values are: Force-auth, Force-unauth, Auto.
Oper mode	The port oper mode. Possible values are: Authorized, Unauthorized or Down.
Reauth Control	Reauthentication control.
Reauth Period	Reauthentication period.
Username	The username representing the identity of the Supplicant. This field shows the username in case the port control is auto. If the port is Authorized, it shows the username of the current user. If the port is unauthorized it shows the last user that was authenticated successfully.
Quiet period	The number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).
Tx period	The number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request.

Max req	The maximum number of times that the device sends an Extensible Authentication Protocol (EAP)-request frame (assuming that no response is received) to the client before restarting the authentication process.
Supplicant timeout	Time in seconds the device waits for a response to an EAP-request frame from the client before resending the request.
Server timeout	Time in seconds the device waits for a response from the authentication server before resending the request.
Session Time	How long the user is logged in.
MAC address	The supplicant MAC address.
Authentication Method	The authentication method used to establish the session.
Termination Cause	The reason for the session termination.
State	The current value of the Authenticator PAE state machine and of the Backend state machine.
Authentication success	Counts the number of times the state machine has received Success message from the Authentication Server.
Authentication fails	Counts the number of times the state machine has received Failure message from the Authentication Server.

show dot1x users

The **show dot1x users** privileged EXEC command displays 802.1x users for the device.

Syntax

show dot1x users [**username** *username*]

- *username* — Supplicant username (Range: 1- 160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays 802.1x users.

```
Console# show dot1x users


Port    Username    Session Time    Auth Method   MAC Address
-----   --------    ------------    -----------   -------------
g1      Bob         1d:03:08:58     Remote        0008:3b79:8787
g2      John        08:19:17        Remote        0008:3b89:3127


Console# show dot1x users username Bob


Port    Username    Session Time    Auth Method   MAC Address
-----   --------    ------------    -----------   -------------
g1      Bob         1d:03:08:58     Remote        0008:3b79:8787
```

The following table describes the significant fields shown in the display:

Field	Description
Port	The interface number.
Username	The username representing the identity of the Supplicant.
Session Time	The period of the the Supplicant is connected to the system.
Auth Method	Supplicant access method.
MAC Address	MAC address from where the Supplicants are connected.

show dot1x statistics

The **show dot1x statistics** privileged EXEC command displays 802.1x statistics for the specified interface.

Syntax

show dot1x statistics ethernet *interface*

- *interface* — Ethernet port name. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays 802.1x statistics for the specified interface.

```
Console# show dot1x statistics ethernet g1


EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource: 00:08:78:32:98:78
```

The following table describes the significant fields shown in the display:

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this Authenticator.
EapolFramesTx	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
EapolStartFramesRx	The number of EAPOL Start frames that have been received by this Authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this Authenticator.
EapolRespIdFramesRx	The number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.

EapolReqIdFramesTx	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolReqFramesTx	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

802.1 Advanced Features

dot1x auth-not-req

The **dot1x auth-not-req** VLAN configuration command enables unauthorized devices access to that VLAN. To disable access, use the **no** form of this command.

Syntax

dot1x auth-not-req

no dot1x auth-not-req

Default Configuration

User should be authorized to access the VLAN.

Command Mode

VLAN Configuration mode

User Guidelines

An access port cannot be a member in an unauthenticated VLAN. The native VLAN of a trunk port cannot be an unauthenticated VLAN. For a general port, the PVID can be the unauthenticated VLAN (although only tagged packets would be accepted in the unauthorized state.)

Examples

The following example enables unauthorized users access to the VLAN:

```
Console (conf) # interface vlan 3
Console(config-if) # dot1x auth-not-req
```

dot1x multiple-hosts

The **dot1x multiple-hosts** interface configuration command allows multiple hosts (clients) on an 802.1x-authorized port where the **dot1x port-control** interface configuration command is set to **auto**. To return to the default setting, use the **no** form of this command.

Syntax

dot1x multiple-hosts

no dot1x multiple-hosts

Default Configuration

Multiple hosts are disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command enables the attachment of multiple clients to a single 802.1x-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized, all attached clients are denied access to the network.

If a port joins a port-channel, its state is multiple hosts as long as the port is a member of the port-channel.

For unauthenticated VLANs, multiple hosts are always enabled.

Examples

The following command allows multiple hosts (clients) on an 802.1x-authorized port:

```
Console(config-if)# dot1x multiple-hosts
```

dot1x single-host-violation

The **dot1x single-host-violation** interface configuration command configures the action to be taken when a station whose MAC address is not the supplicant MAC address attempts to access the interface. To return to the default setting, use the **no** form of this command.

Syntax

dot1x single-host-violation {**forward** | **discard** | **discard-shutdown**} [**trap** *seconds*]

no port dot1x single-host-violation

- **forward** — Forward frames with source addresses that are not the supplicant address, but do not learn the address.
- **discard** — Discard frames with source addresses that are not the supplicant address.

- **discard-shutdown** — Discard frames with source addresses that are not the supplicant address, and shut down the port.
- **trap** — Send SNMP traps
- *seconds* — Minimum time in seconds between consecutive traps. (Range: 1- 1000000)

Default Configuration

Discard frames with source addresses that are not the supplicant address. No traps.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command is relevant when Multiple Hosts is disabled and the user has been successfully authenticated

Examples

The following example uses forward action to forward frames with source addresses that are not the supplicant address:

```
Console(config-if)# dot1x single-host-violation forward trap 100
```

show dot1x advanced

The **show dot1x advanced** privileged EXEC command displays 802.1x advanced features for the device or for the specified interface.

Syntax

show dot1x advanced [**ethernet** *interface*]

- *interface* — Ethernet interface

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays 802.1x advanced features for the device.

```
Console# show dot1x advanced

Unauthenticated VLANs: 91,92

Port          Multiple Hosts
----          --------------
g1            Disabled
g2            Enabled

Console# show dot1x advanced ethernet g1

Port          Multiple Hosts
----          --------------
g1            Disabled

Single host parameters
Violation action: Discard
Trap: Enabled
Trap frequency: 100
Status: Single-host locked
Violations since last trap: 9
```