

# Dell™ PowerConnect™ 6200 系列用户指南

[简介](#)

[硬件说明](#)

[使用 Dell™ OpenManage™ Switch Administrator](#)

[电缆和端口信息](#)

[配置 Dell™ PowerConnect™](#)

[配置系统信息](#)

[配置 IP 电话和访问点支持功能](#)

[配置交换信息](#)

[查看统计数据/RMON](#)

[配置路由](#)




[配置 IPv6](#)

[配置服务质量](#)

[配置 IP 多点传送](#)

[获得帮助](#)

## 注、注意和警告

-  **注：**注表示可以帮助您更好地使用计算机的重要信息。
-  **注意：**注意表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。
-  **警告：**警告表示可能会造成财产损失、人身伤害甚至死亡。

型号 PC6224、PC6248、PC6224P、PC6248P 和 PC6224F

本说明文件中的信息如有更改，恕不另行通知。

© 2007 Dell Inc.。版权所有，翻印必究。

未经 Dell Inc. 书面许可，严禁以任何形式进行复制。

本文中使用的商标：*Dell*、*Dell OpenManage*、*DELL* 徽标、*Inspiron*、*Dell*

*Precision*、*Dimension*、*OptiPlex*、*PowerConnect*、*PowerApp*、*PowerVault*、*Axim*、*DellNet* 和 *Latitude* 是 Dell Inc. 的商标。*Microsoft*、*Windows* 和 *Windows Vista* 是 Microsoft Corporation 在美国和/或其它国家或地区的商标或注册商标。*Procomm Plus* 是 Symantec Corporation 或其子公司在美国和其它国家或地区的商标。

本文件中提及的其它商标和产品名称是指拥有相应商标和名称的公司或其制造的产品。Dell Inc. 对本公司的商标和产品名称之外的其它商标和产品名称不拥有任何专有权。

型号 PC6224、PC6248、PC6224P、PC6248P 和 PC6224F

2007 年 9 月 修订版 A00

[返回目录页面](#)

# 简介

## Dell™ PowerConnect™ 6200 系列用户指南

- [功能](#)
- [CLI 说明文件](#)

👉 **注意：**在继续之前，请阅读本产品的版本注释。您可以从 Dell 支持网站 [support.dell.com](http://support.dell.com) 下载版本注释。

Dell™ PowerConnect™ 6200 系列是独立式或堆栈式第 2 层和第 3 层交换机，它们扩展了 Dell PowerConnect LAN 交换产品的范围。这些交换机包括以下特性：

- 1U 型机架可安装机箱设计。
- 支持多层交换机的所有数据通信要求，包括第 2 层交换、IPv4 路由、IPv6 路由、IP 多点传送、服务质量、安全和系统管理功能。
- 具有可热交换的附属交换机，实现了高可用性。

---

## 功能

本节介绍了交换机的用户可配置功能。有关功能列表，请参阅此软件版本的版本注释。

### 基于端口的功能

#### 超长帧支持

超长帧能够以较少的帧数传输相同的数据，从而减少了开销、处理时间和中断次数。

#### 自动 MDI/MDIX 支持

本交换机支持自动检测绞接电缆和直通电缆的功能。

终端站点的标准布线为介质相关接口 (MDI)，集线器和交换机的标准布线则称为带有绞接电缆的介质相关接口 (MDIX)。

有关为端口或 LAG 配置 MDI/MDIX 的信息，请参阅[端口配置](#)或[LAG 配置](#)。

#### 自适应

自适应功能使交换机可以公布运行模式。它提供了在共用点对点链路网段的两台交换机之间交换信息的方法，以及自动将这两台交换机配置为可以最大程度地利用其传输能力的方法。

PowerConnect 6200 系列通过提供端口公布来增强自适应功能。系统管理员可以通过端口公布来配置公布的端口速率。

有关自适应的信息，请参阅[端口配置](#)或[LAG 配置](#)。

#### 流控制支持 (IEEE 802.3x)

流控制通过请求高速交换机抑制发送信息包，从而使低速交换机能够与高速交换机进行通信。传输会暂时停止，以防止缓冲区溢出。

有关为端口或 LAG 配置流控制的信息，请参阅[端口配置](#)或[LAG 配置](#)。

## 防队列头阻塞

防队列头 (HOL) 阻塞功能可防止由于通信竞争同一出口端口资源而导致通信延迟和帧丢失。HOL 阻塞会对信息包进行排队，先转发队列头的信息包，然后再转发队列尾的信息包。

## 背压支持

在半双工链路中，接收器可通过占用链路使其不能用于其它通信来防止缓冲区溢出。

## 备用存储和转发 (ASF)

备用存储和转发 (ASF) 功能可以缩短大型信息包的等待时间。当启用了 ASF 时，内存管理单元 (MMU) 可以在信息包整个到达单元缓冲池 (CBP) 内存之前将其转发到出口端口。ASF 也称为穿透模式，可以通过命令行界面进行配置。有关如何配置 ASF 功能的信息，请参阅《CLI 参考指南》。

## 支持 MAC 地址的功能

### MAC 地址支持

交换机最多可支持 8 K MAC 地址，并且保留两个 MAC 地址以供系统使用。

### 自动记忆 MAC 地址

交换机能够使传入信息包自动记忆 MAC 地址。

### 自动管理 MAC 地址的存在时间

在给定时间段内尚未接收到任何通信的 MAC 地址将会过期，这样便可以防止桥接表溢出。

有关配置 MAC 地址过期时间段的信息，请参阅[动态地址表](#)。

### 静态 MAC 输入项

用户定义的 MAC 输入项存储在桥接表中，地址为自动记忆的地址。

有关配置静态 MAC 地址的信息，请参阅[静态地址表](#)。

### 可识别 VLAN 的基于 MAC 的交换

来自未知源地址的信息包将发送到 CPU 并添加到硬件表中。这样，以后发送到此地址或从其发出的信息包将会得以更有效的转发。

### MAC 多点传送支持

多点传送服务是一种受限制的广播服务，它允许采用一对多和多对多的连接形式。在第 2 层多点传送服务中，将会接收发送到特定多点传送地址的单个帧，并且创建要在每个相关端口上传输的该帧的副本。

有关配置 MAC 多点传送支持的信息，请参阅[管理多点传送支持](#)。

## 第 2 层功能

### IGMP 监测

IGMP 监测用于在交换机将 IGMP 帧内容从工作站点转发至上游多点传送路由器时对这些内容进行检查。该监测使交换机能够识别与多点传送会话相关的工作站点，并确定哪些多点传送路由器正在发送多点传送帧。

### 端口镜像

通过将传入和传出信息包的副本从多达 4 个源端口转发至监测端口，端口镜像可以监测和镜像网络通信。

### 广播风暴控制

转发第 2 层帧时，广播帧、未知单点传送帧和多点传送帧将一起传输至相关虚拟局域网 (VLAN) 中的所有端口。这会占用带宽并载入所有端口上连接的全部节点。风暴控制可限制交换机接受和转发的广播帧、未知单点传送帧和多点传送帧的数量。

## 虚拟局域网支持的功能

### VLAN 支持

VLAN 是组成单个广播域的一组交换端口。根据 VLAN 标记或根据入口端口和信息包内容的组合，信息包被分类为属于不同的 VLAN。具有通用属性的信息包可以属于同一 VLAN。

有关配置 VLAN 的信息，请参阅[配置 VLAN](#)。

### 基于端口的 VLAN

基于端口的 VLAN 根据传入信息包的入口端口将其分类至不同的 VLAN。

有关配置 VLAN 的信息，请参阅[配置 VLAN](#)。

### 基于 IEEE 802.1v 协议的 VLAN

数据链路层（第 2 层）协议标识中定义了 VLAN 分类规则。基于协议的 VLAN 用来将第 2 层通信隔离以区别于第 3 层协议。

有关定义基于协议的 VLAN 的信息，请参阅[协议组](#)。

### 完全兼容 802.1Q VLAN 标记

IEEE 802.1Q 定义了虚拟桥接 LAN 的体系结构、VLAN 中提供的服务以及提供这些服务所涉及的协议和算法。



## GVRP 支持

GARP VLAN 注册协议 (GVRP) 支持在 802.1Q 主干端口上删减 IEEE 802.1Q 兼容 VLAN 和创建动态 VLAN。启用 GVRP 后，交换机将在处于活动状态的基础生成树协议拓扑所属的所有端口上注册和传播 VLAN 成员关系。

有关配置 GVRP 的信息，请参阅 [GVRP 参数](#)。

## 受保护的端口（专用 VLAN 边缘）

专用 VLAN 边缘 (PVE) 端口是第 2 层安全保护功能，它们在同一 VLAN 的成员端口之间提供基于端口的安全保护功能。这种端口是通用 VLAN 的扩展。受保护端口上的通信仅发送到上行链路端口，而不能发送到 VLAN 内的其它端口。

## 基于子网的 VLAN

利用此功能，可以根据信息包的源 IP 地址将传入的未标记信息包分配给 VLAN 和通信级别。

有关配置基于子网的 VLAN 的信息，请参阅[将 IP 子网捆绑到 VLAN](#)。

## 基于 MAC 的 VLAN

利用此功能，可以根据信息包的源 MAC 地址将传入的未标记信息包分配给 VLAN 和通信级别。

有关配置基于 MAC 的 VLAN 的信息，请参阅[将 MAC 捆绑到 VLAN](#)。

## 生成树协议功能

### 每台交换机的生成树协议 (STP)

802.1d STP 是第 2 层交换机的标准要求，使得网桥能够自动防止和解决 L2 转发环路。交换机使用经过专门格式化的帧并在端口上有选择地转发，从而交换配置信息。

有关配置生成树协议的信息，请参阅[配置生成树协议](#)。

### IEEE 802.1w 快速生成树

快速生成树协议 (RSTP) 检测并使用网络拓扑，以实现更快速的聚合，并且不会产生转发环路。

有关配置快速生成树协议的信息，请参阅[快速生成树](#)。

### 多生成树

多生成树 (MSTP) 操作用于将 VLAN 映射到生成树实例。MSTP 提供了一种不同的负载平衡方案。分配给不同 VLAN 的信息包是沿 MSTP 域 (MST 域) 内不同的路径传输的。域是指具有相同 MSTP 设置的一个或多个互连的 MSTP 网桥。管理员根据此标准将 VLAN 通信分配给唯一路径。

有关配置多生成树的信息，请参阅 [MSTP 设置](#)。

### 生成树根保护

生成树根保护功能用于防止生成树实例的根发生意外变化。一个网桥 ID 的优先级可设置为零，而另一个 MAC 地址较小的网桥 ID 也可以将优先级设置为零且优先于根网桥。

## 网桥协议数据单元保护

生成树 BPDU 保护用于在新设备试图进入已经存在的 STP 拓扑时禁用该端口。这样，原来不属于 STP 的设备不允许影响 STP 拓扑。

## 链路聚合功能

### 链路聚合

最多可以合并 8 个端口来形成一个链路聚合组 (LAG)。这样即可在物理链路中断时进行容错保护、实现更高的带宽连接速度以及提高带宽粒度。

一个 LAG 由具有相同速率的端口组成，并被设置为全双工运行模式。

有关配置 LAG 的信息，请参阅 [LAG 配置](#)。

### 链路聚合和 LACP

链路聚合控制协议 (LACP) 在链路中持续使用对等交换以确定不同链路的聚合功能，并不断地在给定的配对系统之间提供可以获得的最高级别的聚合功能。LACP 自动确定、配置、捆绑和监测系统内端口与聚合器的捆绑情况。

有关 LACP 的信息，请参阅 [LACP 参数](#)。

## IP 电话和访问点支持功能

### 以太网供电 (PoE) 配置

PowerConnect 6200 支持功率阈值、SNMP 陷阱和 PoE 旧有设备支持这三种 PoE 配置。

有关配置 PoE 的信息，请参阅[以太网供电配置](#)。

### 用于介质端点设备的链路层发现协议 (LLDP)

用于介质端点设备的链路层发现协议 (LLDP-MED) 扩展了 LLDP 标准，支持网络配置和策略、设备定位、以太网供电管理以及详细目录管理。

有关配置 LLDP-MED 的信息，请参阅[配置用于介质端点设备的链路层发现协议 \(LLDP\)](#)。

### 语音 VLAN

语音 VLAN 功能使交换机端口能够按指定的优先级传送语音通信。优先级能够分离端口收到的语音通信和数据通信。

有关配置 LLDP-MED 的信息，请参阅[为语音 VLAN 配置端口](#)。

## IPv4 路由功能

## 地址解析协议

PowerConnect 6200 使用 ARP 协议将第 2 层 MAC 地址与第 3 层 IPv4 地址相关联。此外，管理员可以通过静态方式向 ARP 表添加输入项。

## 开放最短路径优先

OSPF 路由协议定义两种区域类型：常规 OSPF 区域和 OSPF 末节区域。OSPF 内部和外部路由信息可以在整个常规 OSPF 区域中传播；它能够支持跨域通信和虚拟链路。OSPF 末节区域不接收外部路由信息；配置末节区域的动机是针对那些资源有限的路由器来限制区域数据库的大小。

## BOOTP/DHCP 中继代理

BootP 协议允许设备从适当的服务器请求和接收配置数据及参数。DHCP 是 BootP 的扩展，它允许系统启动时从网络服务器接收附加的设置参数。值得注意的是，BootP 在获取 IP 地址后停止运行，而 DHCP 服务则是一个不中断过程。例如，分配给系统的 IP 地址有一个“租用时间”，这个时间可能过期，这个时间可能过期，但系统的 IP 地址可以动态更新。

## 路由信息协议

在一个 Internet 自治系统中使用的路由协议称之为内部网关协议 (IGP)。RIP 是一种根据中等规模的网络应用而设计的 IGP。

## 虚拟路由冗余协议

虚拟路由冗余协议 (VRRP) 用于在网络拓扑中向主机提供冗余路由器，主机无需重新配置或了解网络中存在多个路由器。

## IPv6 路由功能

### DHCPv6

DHCPv6 合并了“无状态”服务器的概念，其中 DHCPv6 不是用于向客户端分配 IP 地址，而只是提供其它网络信息，例如 DNS、网络时间协议 (NTP) 和/或会话初始化协议 (SIP) 信息。

### OSPFv3

OSPFv3 为 IPv6 网络提供路由协议。OSPFv3 是一个基于 OSPF 版本 2 组件的新路由组件。在双栈 IPv6 中，可以同时配置和使用 OSPF 和 OSPFv3 组件。

### IPv6 路由

由于 IP4 和 IPV6 可以共存于网络中，因此此类网络上的路由器需要转发这两种类型的通信。假设存在这种共存现象，PowerConnect 6200 将维护两个路径选择表 rto 和 rto6，这两个表都能在同一组接口上进行转发。IPV6 接口的管理方式与 IPV4 接口的管理方式相似。

## 服务质量功能

### 服务质量 (QoS) 支持

为克服无法预料的网络通信以及优化性能，可以在整个网络中应用服务质量 (QoS)，以确保根据特定标准划分网络通信的优先级。交换机支持两种类型的 QoS：差别服务和 Service Level。Service Level。

## 差别服务

QoS 功能包括差别服务 (DiffServ) 支持，这种支持可以根据定义的逐跳行为 (per-hop behavior) 将通信量分类为数据流及进行某些 QoS 处理。

## Service Level

借助 Service Level (CoS) 队列功能，可以直接配置交换机排队功能的某些方面。当不需要差别服务的复杂度时，Service Level 便能为不同类型的网络通信提供所需的 QoS 保障。

## IPv4 多点传送功能

### 距离向量多点传送路由协议

DVMRP 与所有启用 DVMRP 的路由器交换信息查询包，同时建立双向邻居关系并创建邻居列表。它还交换报告信息包并创建单点传送拓扑表，该表用于构建多点传送路径选择表。而后，该多点传送路径选择表将用于路由多点传送信息包。

### Internet 组管理协议

Internet 组管理协议 (IGMP) 由 IPv4 系统（主机和路由器）用于将它们的 IP 多点传送组成员关系报告给任何邻近的多点传送路由器。PowerConnect 6200 执行 IGMP 协议的“多点传送路由器部分”，这意味着它将收集进行有效的多点传送路由所需的成员关系信息。

### 协议无关的多点传送密集模式

协议无关的多点传送 (PIM) 是一个标准的多点传送路由协议，在 Internet 中提供可伸缩的域间多点传送路由选择功能，与任何特定单点传送路由协议所提供的机制无关。PIM-DM 协议使用现有的单点传送路由选择表和加入/剪除/嫁接机制来构建树。PIM-DM 使用逆向路径转发 (RPF) 创建基于源的最短路径分布树。

### 协议无关的多点传送稀疏模式

PIM-SM 用于有效地将多点传送通信路由到多点传送组，该组可以跨越广域网，并且组内带宽是一个约束条件。PIM-SM 默认使用共享树并实施基于源的树，以此提高效率。此数据阈值速率用于在树之间切换。

## 交换机管理功能

### SNMP 警报和陷阱日志

系统用严重性代码和时间戳来记录事件。事件将作为 SNMP 陷阱被发送至陷阱接收列表。

有关 SNMP 警报和陷阱的信息，请参阅[定义 SNTP 全局参数](#)。

## 基于 Web 的管理

您可以通过任何 Web 浏览器来管理系统。交换机包含一个支持 HTML 页面的嵌入式 Web 服务器，通过这些页面可以监测和配置系统。

## 配置文件下载

交换机的配置文件包含整个系统范围和特定端口的设备配置数据。您可以通过命令行界面 (CLI) 命令显示配置文件。

有关下载配置文件的信息，请参阅[下载文件](#)。

## 软件下载

通过软件下载可以存储备份固件映像文件。有关下载软件的信息，请参阅[软件下载和重新引导](#)。

## 小型文件传输协议 (TFTP)

PowerConnect 6200 系列支持通过 TFTP 上载/下载引导映像文件、固件和配置文件。

## 远程监测 (RMON)

RMON 是一种标准的 MIB，它定义了当前和历史 MAC 层统计数据和控制对象，使系统可以跨整个网络实时捕获信息。

## 简单网络管理协议 (SNMP) 版本 1、2 和 3

可以使用管理信息库 (MIB) 变量组合对系统进行全面管理，这些变量的组合值表示系统状态的所有方面，并且 SNMP 协议可检查这些值，还可能修改这些值。UDP/IP 传输协议支持 SNMP v1/v2c/v3。

## 命令行界面

命令行界面 (CLI) 的语法和语义尽可能地符合业界惯例。CLI 由必要元素和可选元素组成。上下文帮助提供当前命令所允许的格式和取值范围，CLI 解释器则提供命令和关键字自动完成功能。

## 系统日志

系统日志是一种允许向一组所需的远程服务器发送事件通知的协议，在这些远程服务器中可以存储、检查和处理事件通知。

有关系统日志的信息，请参阅[管理日志](#)。

## SNTP

简单网络时间协议 (SNTP) 可以确保将网络交换机的时钟时间同步精确到毫秒。时间同步由网络 SNTP 服务器来执行。

有关 SNTP 的详细信息，请参阅[配置 SNTP 设置](#)。

## 安全保护功能

## 访问控制列表 (ACL)

访问控制列表 (ACL) 确保只有授权用户才可以访问特定资源，同时阻止任何非授权试图访问网络资源的行为。ACL 可用于提供流量控制，限制路由更新的内容，决定转发或阻止的通信类型，除此之外还提供网络安全保护。

有关定义 ACL 的信息，请参阅 [IP ACL 配置](#)和 [MAC ACL 配置](#)。

## 基于端口的验证 (802.1x)

基于端口的验证启用通过外部服务器针对各个端口验证系统用户。只有经验证和经批准的系统用户才可以传输和接收数据。使用可扩展验证协议 (EAP)，通过远程验证拨入用户服务 (RADIUS) 服务器来验证端口。另外还支持 PEAP、EAP-TTL、EAP-TTLS 和 EAP-TLS。

## 锁定端口支持

锁定端口功能用于限制拥有特定 MAC 地址的用户对某个端口的访问。可以在该端口上手动定义或记忆这些地址。当一个数据帧经过锁定端口并且该帧的源 MAC 地址与该端口无绑定关系时，保护机制将被启动。

有关启用锁定端口安全保护的信息，请访问[端口安全保护](#)。

## 密码管理安全保护

密码管理可提高网络安全性，还可改进密码控制。分配的 SSH、Telnet、HTTP、HTTPS 和 SNMP 访问密码均提供安全保护功能。

有关密码管理的详细信息，请参阅[密码管理](#)。

## TACACS+

TACACS+ 为验证访问交换机的用户提供了集中式安全保护。TACACS+ 提供了集中式用户管理系统，同时还保持了与 RADIUS 和其它验证过程的一致性。

## RADIUS 客户端

RADIUS 是一个基于客户端/服务器的协议，RADIUS 服务器维护用户数据库，数据库中包含每个用户的验证信息（例如用户名、密码和帐户信息）。

## SSH/SSL

安全命令解释程序 (SSH) 是一个提供到设备的安全远程连接的协议。此连接所提供的功能类似于入站的远程登录连接。

安全套接层 (SSL) 协议提供了一种使两个站点间的加密连接抽象化的方法。一旦建立，此类连接与无安全保护连接的用法几乎无任何差异。

---

## CLI 说明文件

Dell PowerConnect 6200 系列的另一个资源是《[CLI 参考指南](#)》。该指南提供有关用于配置和管理交换机和堆栈的 CLI 命令的信息。说明文件提供详细的 CLI 说明、语法、默认值和示例。

---

[返回目录页面](#)

[返回目录页面](#)

# 硬件说明

## Dell™ PowerConnect™ 6200 系列用户指南

- [端口说明](#)
- [其它特性](#)
- [LED 定义](#)

本节包含有关设备特性和模块硬件配置的信息。包括以下主题：

- [Dell™ PowerConnect™ 6200 系列前面板](#)
- [PowerConnect 6200 系列背面板](#)
- [控制台 \(RS-232\) 端口](#)
- [物理尺寸](#)
- [电源设备](#)
- [通风系统](#)
- [堆栈](#)
- [LED 定义](#)

---

## 端口说明

### Dell™ PowerConnect™ 6200 系列前面板

PowerConnect 6224 交换机前面板提供 24 个 10/100/1000 Base-T RJ-45 端口以及 4 个 SFP 组合端口，这些端口具有自动感测模式，可自动感测速率、流控制和双工模式。SFP 收发器单独出售。PowerConnect 6248 前面板提供 48 个 10/100/1000 Base-T RJ-45 端口和 4 个 SFP 组合端口。

图 2-1. 具有 24 个 10/100/1000 Base-T 端口的 PowerConnect 6224



图 2-2. 具有 48 个 10/100/1000 Base-T 端口的 PowerConnect 6248



图 2-3. 具有 24 个 SFP 端口的 PowerConnect 6224F



图 2-4. 具有 24 个 10/100/1000 Base-T 端口的 PowerConnect 6224P



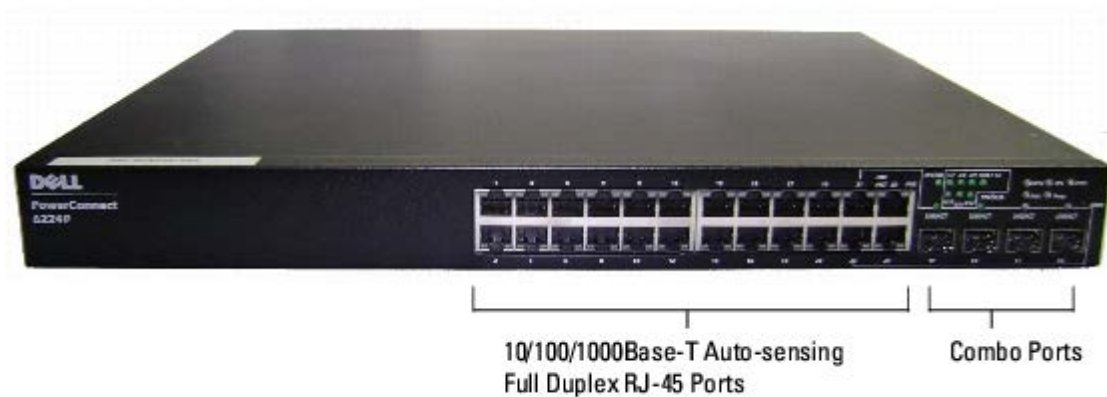


图 2-5. 具有 48 个 10/100/1000 Base-T 端口的 PowerConnect 6248P



- 交换机可自动检测 RJ-45 端口上绞接电缆和直通电缆之间的差别。
- SFP 端口同时支持 SX 模块和 LX 模块。
- RJ-45 端口支持速率为 10/100/1000 Mbps 的半双工和全双工模式。
- 针孔状重置按钮位于前面板上。

## PowerConnect 6200 系列背面板

每个 PowerConnect 6200 系列交换机在背面板上都提供一个 RS-232 维护端口。这种串行连接可用于管理整个堆栈。

双 10Gbps 扩充槽也位于交换机的背面板上。右边的槽可以支持插入式双 10GbE XFP 模块或 CX4 模块。左边的槽可以支持插入式双 10GbE XFP 模块、CX4 模块或堆栈模块。

图 2-6. PowerConnect 6200 系列背面板



## 控制台 (RS-232) 端口

控制台 (RS-232) 端口仅用于通过串行接口进行管理。可以借助此端口直接连接到交换机，还可以使用此端口通过连接到 EIA/TIA-232 端口的控制台终端访问 CLI。

控制台端口支持八个数据位、一个停止位、无奇偶校验位、无流控制的异步数据。默认波特率为 9600 bps。

**注：**如果安装的是交换机堆栈，则在通电及配置之前，需要组装该堆栈并进行布线。交换机堆栈首次通电时，这些交换机将选出主交换机，这一主交换机可能位于堆栈中的任何位置。该交换机将亮起主交换机 LED，即前面板上的一组 LED 中最左侧的 LED。将终端连接至主交换机。如果将终端连接至附属交换机，将无法使用 CLI。

## 其它特性

### 物理尺寸

6200 系列交换机的物理尺寸如下所示：

- 440 x 460 x 44 毫米 (宽 x 厚 x 高)
- 17.32 x 18.11 x 1.73 英寸 (宽 x 厚 x 高)

### 电源设备

6200 系列交换机拥有一个需要标准交流电的内部电源设备。对于非 PoE 交换机，您也可以配备冗余直流电源设备，例如 PowerConnect RPS-600。对于 PoE 交换机，您可以配备 PowerConnect EPS-470。通过观察 LED 可以验证操作是否正常。有关信息，请参阅[系统 LED](#)。

### 通风系统

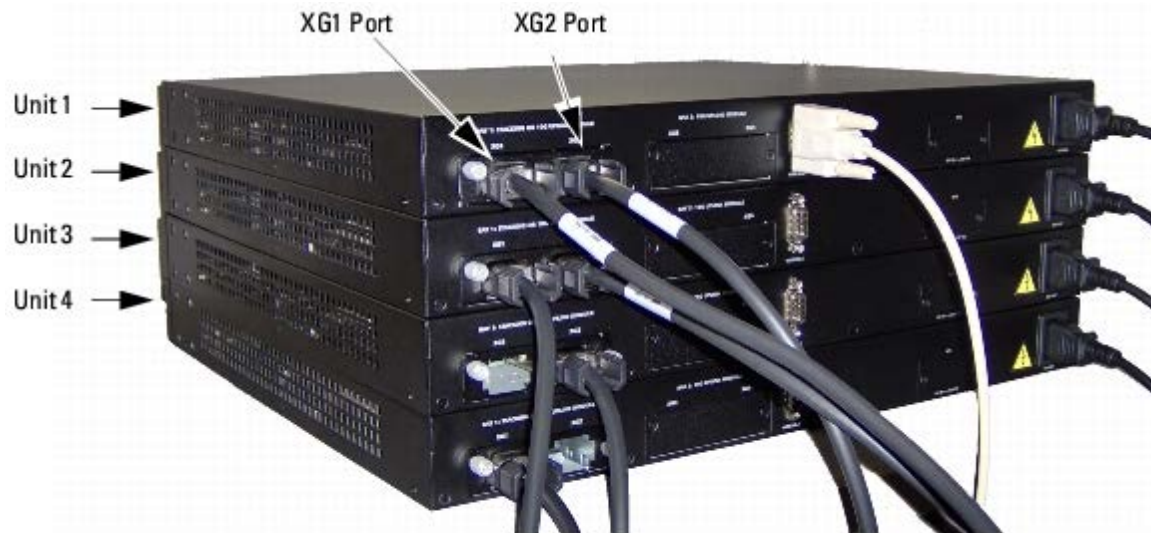
PowerConnect 6224 通过三个风扇来实现冷却。而 PowerConnect 6248 有四个风扇。可以通过观察 LED 来验证操作是否正常。有关 LED 的信息，请参阅[系统 LED](#)。

### 堆栈

以堆栈方式最多可以安装 12 台 PowerConnect 6224 和/或 6248 交换机，且支持多达 576 个前面板端口。要以堆栈方式安装，请使用交换机背面左侧的堆栈端口来连接相邻的单元。请参阅[图 2-7](#)。

- 使用一根短的堆栈电缆，将最顶部的交换机的堆栈端口与直接位于其下方的交换机的堆栈端口相连。在堆栈中的每台交换机的背面“托架 1”中安装一个单独购买的堆栈模块。
- 如果需要，请使用单独购买的长（3 米）堆栈电缆连接到交换机。重复此过程，直至所有设备连接完成。
- 使用剩下的堆栈电缆连接其它空闲端口，一端连接顶部的交换机，一端连接底部的交换机。

图 2-7. 连接交换机堆栈



在图 2-7 中，交换机堆栈间的物理连接如下所示：

- 单元 1 和单元 2 通过每台交换机上的 XG1 端口相连接。
- 单元 2 和单元 3 通过每台交换机上的 XG2 端口相连接。
- 单元 1 和单元 4 通过单元 1 上的 XG2 端口和单元 4 上的 XG1 端口相连接。

## 堆栈备用单元

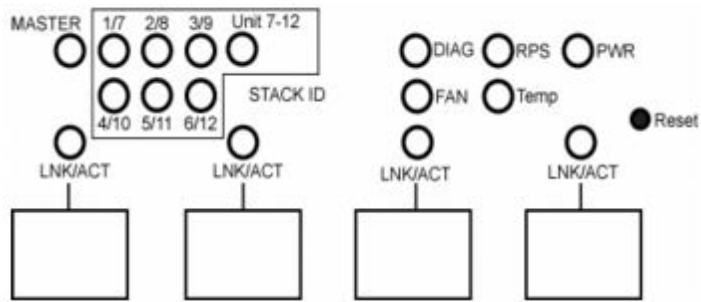
堆栈功能支持“备用”或后援单元，当堆栈中的主单元出现故障时，备用单元将发挥主单元的作用。一旦发现堆栈中的主单元出现故障，备用单元就会使用当前的配置初始化控制层面并启用其它的所有堆栈单元。备用单元会同步备份堆栈的当前配置。在切换过程中会关闭并打开所有端口以避免出现循环，同时将新的主软件应用程序置于一致的状态。

堆栈中预配置了备用单元，但您也可以使用 CLI 选择其它的堆栈成员作为备用单元。有关详情，请参阅《CLI 参考指南》。

## LED 定义

前面板上包含若干个发光二极管 (LED)，用于指示链路、电源设备、风扇、系统诊断程序和堆栈的状态。

图 2-8. 前面板 LED



## SFP 端口 LED

图 2-9 所示为每个 SFP 端口上方的 SFP 端口 LED。

图 2-9. SFP 端口 LED

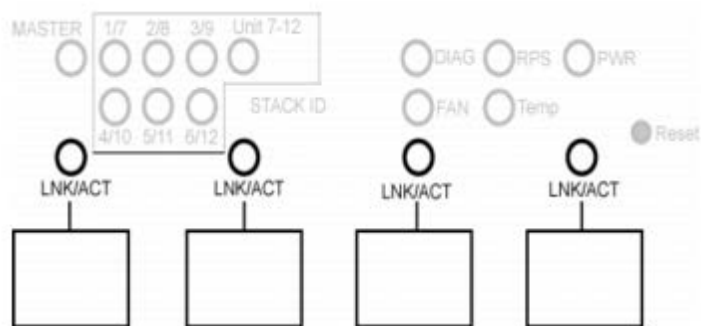


表 2-1 包含 SFP 端口 LED 的定义。

表 2-1. SFP 端口 LED 定义

LED	颜色	定义
LNK/ACT	呈绿色稳定亮起	端口链路当前已连通。
	呈绿色闪烁	端口当前正在发送和/或接收网络通信。
	熄灭	端口链路当前未连通。

## XFP 模块端口 LED

当 XFP 模块插入背面板时，XFP 连接器位于该模块上。表 2-2 包含 XFP 端口 LED 的定义：

表 2-2. XFP 端口 LED 定义

LED	颜色	定义
XFP	绿色	端口链路当前已连通。
	呈绿色闪烁	端口当前正在发送和/或接收网络通信。
	熄灭	端口链路当前未连通。

## 10/100/1000 Base-T 端口 LED

每个 10/100/1000 Base-T 端口均具有两个 LED。下图所示为 10/100/100 Base-T 端口 LED。

图 2-10. 10/100/1000 Base-T 端口 LED

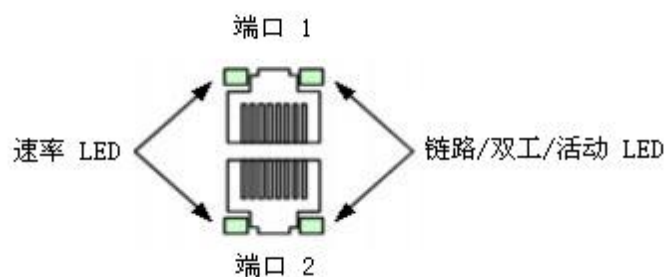


表 2-3 包含 PowerConnect 6224、6248 和 6224F 的 10/100/1000 Base-T 端口 LED 定义。

表 2-3. 10/100/1000 Base-T 端口定义 (6224、6248 和 6224F)

LED	颜色	定义
Speed (速度)	绿色	端口的运行速率为 1000 Mbps。
	琥珀色	端口的运行速率为 10/100 Mbps。
	稳定亮起	链路连通但链路上没有活动。
	闪烁	链路连通且链路上存在活动。
Link (链路)	熄灭	链路未连通。
	绿色	全双工模式。
	熄灭	半双工模式。

表 2-4 包含 PowerConnect 6224P 和 6248P 的 10/100/1000 Base-T 端口 LED 定义。

表 2-4. 10/100/1000 Base-T 端口定义 (6224P 和 6248P)

LED	颜色	定义
Speed/Link/Act (速度/链路/工作)	呈绿色稳定亮起	端口的运行速率为 1000 Mbps。
	呈绿色闪烁	端口的运行速率为 10/100 Mbps。
	熄灭	链路未连通。
FDX (全双工)	呈绿色稳定亮起	检测到 PoE 用电设备，且其正在正常负载下工作。
	呈绿色闪烁	端口当前处于过渡模式。正在检测 PoE 用电设备或者该设备出现了故障。
	呈琥珀色稳定亮起	用电设备过载或电量不足。
	呈琥珀色闪烁	用电设备的能耗超过了预定义的电量配额。
	熄灭	没有检测到任何用电设备。

## 系统 LED

系统 LED 位于前面板的右侧，提供有关电源设备、风扇、温度条件和诊断程序的信息。图 2-11 所示为系统 LED。

图 2-11. 系统 LED

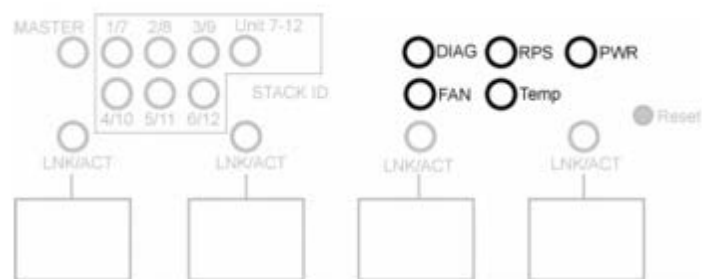


表 2-5 包含系统 LED 的定义。

表 2-5. 系统 LED 定义

LED	颜色	定义
DIAG	呈绿色闪烁	诊断测试正在进行中。
	绿色	诊断测试已成功完成。
	红色	诊断测试失败。
RPS	绿色	冗余电源设备 (RPS) 存在且工作正常。
	红色	冗余电源设备存在，但出现故障。
	熄灭	无冗余电源设备。
PWR	绿色	电源设备工作正常。
	红色	电源设备出现故障。
FAN	绿色	风扇工作正常。
	红色	一个或多个风扇出现故障。
Temp	绿色	系统温度低于阈值限制。
	红色	系统温度高于阈值限制。

## 堆栈 LED

堆栈 LED 位于前面板的右侧，提供有关堆栈中交换机的位置和状态的信息。图 2-12 所示为堆栈 LED。表 2-6 包含堆栈 LED 的定义。

图 2-12. 堆栈 LED

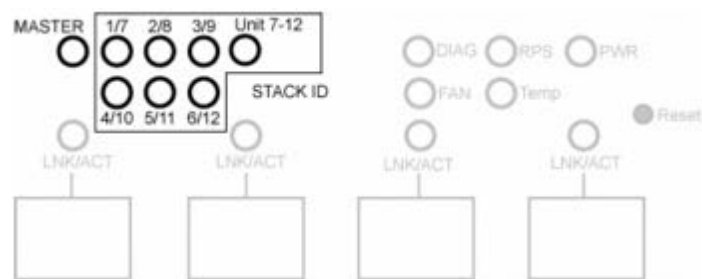


表 2-6. 堆栈 LED 定义

LED	颜色	定义
-----	----	----

所有 LED 熄灭		该单元作为独立式交换机运行。
MASTER	绿色	该单元当前是堆栈中的主交换机。
	熄灭	该单元不是堆栈中的主交换机。
单元 7–12	绿色	堆栈 ID 介于 7 至 12 之间。
	熄灭	堆栈 ID 介于 1 至 6 之间。
1/7	绿色	该单元是堆栈中的第 1 台或第 7 台交换机。
	熄灭	该单元不是堆栈中的第 1 台或第 7 台交换机。
2/8	绿色	该单元是堆栈中的第 2 台或第 8 台交换机。
	熄灭	该单元不是堆栈中的第 2 台或第 8 台交换机。
3/9	绿色	该单元是堆栈中的第 3 台或第 9 台交换机。
	熄灭	该单元不是堆栈中的第 3 台或第 9 台交换机。
4/10	绿色	该单元是堆栈中的第 4 台或第 10 台交换机。
	熄灭	该单元不是堆栈中的第 4 台或第 10 台交换机。
5/11	绿色	该单元是堆栈中的第 5 台或第 11 台交换机。
	熄灭	该单元不是堆栈中的第 5 台或第 11 台交换机。
6/12	绿色	该单元是堆栈中的第 6 台或第 12 台交换机。
	熄灭	该单元不是堆栈中的第 6 台或第 12 台交换机。

---

[返回目录页面](#)

[返回目录页面](#)

# 使用 Dell™ OpenManage™ Switch Administrator

Dell™ PowerConnect™ 6200 系列用户指南

- [设置交换机的 IP 地址](#)
- [启动应用程序](#)
- [了解界面](#)
- [使用 Switch Administrator 按钮](#)
- [定义字段](#)
- [通过 CLI 访问交换机](#)
- [使用 CLI](#)

---

## 设置交换机的 IP 地址

设置 IP 地址的方法有两种：使用 DHCP 或静态地分配地址。要启动 CLI，请参阅标题为[通过 CLI 访问交换机](#)的小节。

### 使用 DHCP 设置 IP 地址

- 在 console> 提示符下键入 enable，然后按 <Enter> 键。
- 在 console# 提示符下键入 config，然后按 <Enter> 键。
- 键入 ip address dhcp，然后按 <Enter> 键。
- 键入 exit。
- 在 console# 提示符下键入 show ip interface management。

### 设置静态地址

- 在 console> 提示符下键入 enable，然后按 <Enter> 键。
- 在 console# 提示符下键入 config，然后按 <Enter> 键。
- 键入 ip address none。
- 要配置 IP 地址 10.256.24.64，其网络掩码为 255.255.248.0，网关为 10.256.24.1，请键入下列信息：  
ip address 10.256.24.64 255.255.248.0  
ip default-gateway 10.256.24.1
- 键入 exit。
- 键入 show ip interface management。

---

## 启动应用程序

- 打开 Web 浏览器。



□□□ 在地址栏中输入交换机的 IP 地址（如 CLI 中所定义）并按 <Enter> 键。

有关为交换机分配 IP 地址的信息，请参阅[配置概览](#)。

□□□ 当显示 **Login**（登录）窗口时，请输入用户名和密码。

 **注：**交换机未配置默认密码，可以在通过控制台端口连接到 CLI 时在不输入密码的情况下对其进行配置。密码区分大小写，并且只能为字母数字。有关恢复丢失密码的信息，请参阅[密码恢复程序](#)。

□□□ 单击 **OK**（确定）。

□□□ 系统将显示 **Dell OpenManage Switch Administrator** 主页。

## 了解界面

主页（请参阅[图 3-1](#)）包含以下视图：

- 树视图 — 树视图位于主页左侧，提供了功能及其组件的可展开视图。
- 设备视图 — 设备视图位于主页右侧，用于显示设备的视图、信息或表区域和/或配置说明。

图 3-1. Switch Administrator 组件

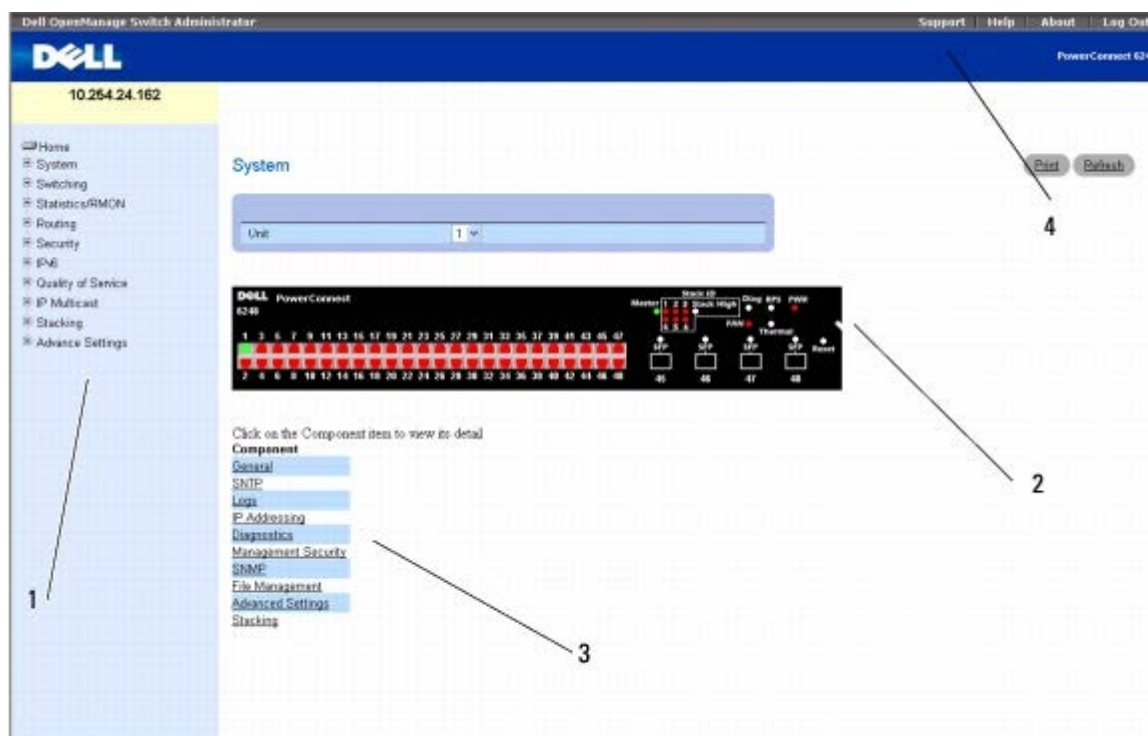


表 3-1 列出了界面组件及其对应的编号。

表 3-1. 接口组件

组件	说明
1	树视图包含各种设备功能的列表。可以展开树视图中的分支以查看特定功能下的所有组件，也可以折叠分支以隐藏功能组件。向右拖动垂直条，可以扩展树区域以显示组件的全名。

2	<p>设备视图提供了有关设备端口、当前配置和状态、表信息以及功能组件的信息。</p> <p>端口颜色表明端口当前是否处于活动状态。绿色表示端口已启用，红色表示端口发生了错误，蓝色表示链路禁用。</p> <p><b>注：</b>在设备视图中不显示 LED 状态。只需查看实际交换机，即可确定 LED 状态。有关 LED 的信息，请参阅 <a href="#">LED 定义</a>。</p> <p>根据所选的选项，设备视图底部的区域将显示其他设备信息和/或对话框，以供配置参数。</p>
3	组件列表包含功能组件的列表。但也可以通过在树视图中展开某个功能来查看组件。
4	信息按钮使您可以访问有关交换机的信息和 Dell 支持。有关详情，请参阅 <a href="#">信息按钮</a> 。

## 使用 Switch Administrator 按钮

### 信息按钮

表 3-2. 信息按钮

按钮	说明
<b>Support</b> (支持)	打开位于 <a href="http://support.dell.com">support.dell.com</a> 的 Dell 支持页面
<b>Help</b> (帮助)	联机帮助，包含可帮助您配置和管理交换机的信息。联机帮助页面上下文相关。例如，如果打开的是 <b>IP Addressing (IP 寻址)</b> 页面，则单击 <b>Help</b> (帮助) 将打开该页面的帮助主题。
<b>About</b> (关于)	包含版本号和 Dell 版权信息。
<b>Log Out</b> (注销)	退出应用程序。

### 设备管理按钮

表 3-3. 设备管理按钮

按钮	说明
<b>Apply Changes</b> (应用更改)	将设置更改应用于设备。
<b>Add</b> (添加)	将信息添加至表或对话框。
<b>Telnet</b>	启动 Telnet 会话。
<b>Query</b> (查询)	查询表。
<b>Show All</b> (全部显示)	显示设备表。
左箭头/右箭头	在列表之间移动信息。
<b>Refresh</b> (刷新)	刷新设备信息。
<b>Reset All Counters</b> (重置所有计数器)	清除统计计数器。
<b>Print</b> (打印)	打印 <b>Network Management System</b> (网络管理系统) 页面和/或表信息。
<b>Draw</b> (绘图)	迅速创建统计图表。

## 复选框

表 3-4. 复选框

复选框类型	说明
<b>Add</b> (添加)	转至配置页面的超链接。
<b>Remove</b> (删除)	删除选定项。
<b>General selection</b> (一般选择)	要启用配置项 (即调整记录文件的灵敏度) , 请选择 <code>diffserv</code> 的匹配标准和 <code>ACL</code> 规则参数。

## 定义字段


用户定义的字段可以包含 1 至 159 个字符, 除非 Dell OpenManage Switch Administrator Web 页面上另有说明。

除以下字符之外, 可以使用其他任何字符:

- \
- /
- :
- \*
- ?
- <
- >
- |

## 通过 CLI 访问交换机

可以通过与控制台端口的直接连接或通过 Telnet 连接来管理交换机。


 **注:** 如果管理的是堆栈, 请确保串行接口电缆连接到堆栈的主交换机。

使用 CLI 类似于在 Linux 系统中输入命令。如果是通过 Telnet 连接进行访问, 请确保在使用 CLI 命令之前设备具有已定义的 IP 地址, 并且用于访问设备的工作站已连接至设备。


有关配置初始 IP 地址的信息, 请参阅[配置概览](#)。

## 控制台连接

□□□ 接通交换机 (或堆栈) 的电源并等待, 直至启动完成。

 **注:** 如果安装的是交换机堆栈, 请将终端连接至主交换机。该交换机将亮起主交换机 LED。交换机堆栈首次通电时, 这些交换机将选出主交换机, 这一主交换机可能位于堆栈中的任何位置。如果将终端连接到附属交换机, 则无法通过附属交换机的串行接口使用 CLI。

□□□ 如果管理员尚未配置登录验证方法, 则交换机启动时将显示 `console>` 提示符。否则, 用户看到的是 `User: login` 提示。

 **注：** 以下步骤假定系统中配置了管理员用户和密码。

□□□ 在提示符下键入 `admin`，然后按 `<Enter>` 键。

系统现在将显示 `Password:` 提示符。

□□□ 输入密码，密码将显示为星号 (\*)。

系统现在将显示 `console#` 提示符。

□□□ 配置设备并输入必要的命令以完成所需的任务。

□□□ 任务完成后，使用 `quit` 或 `exit` 命令退出会话。

## Telnet 连接

Telnet 为终端仿真 TCP/IP 协议。通过 TCP/IP 协议网络可以将 ASCII 终端虚拟连接至本地设备。需要远程登录时，可选择 Telnet 作为本地登录终端。

交换机同时最多支持四个 Telnet 会话。可以通过 Telnet 会话使用所有 CLI 命令。

## 使用 CLI

### 命令模式概览

CLI 分为几种命令模式。每种命令模式都有其特定的命令集。在控制台提示符后输入问号将显示特定命令模式的可用命令列表。

每种模式均有一个特定的命令，用于从一种命令模式切换到另一种命令模式。

在 CLI 会话初始化过程中，CLI 模式为用户执行模式。在用户执行模式中只能使用有限的命令子集。此模式级别专用于不更改交换机配置的任务，还可用于访问配置子系统。如果配置启用密码，优先执行模式可能需要密码。有关设置启用密码的详情，请参阅[安全保护管理和密码配置](#)。

优先执行模式可提供对设备全局配置的访问。要在设备内进行特定的全局配置，请进入下一个级别，即全局配置模式。此时不需要密码。


全局配置模式以全局级别管理设备配置。

接口配置模式以物理接口级别配置设备。需要子命令的接口命令具有另一种级别，称为子接口配置模式。

### 用户执行模式

用户执行级提示符由主机名后跟尖括号 (>) 组成。例如：

```
console>
```

 **注：** 如果未在初始配置过程中修改主机名，则默认的主机名为 `console`。

用户执行命令用于连接至远程设备、临时更改终端设置、执行基本检测以及列出系统信息。

要列出用户执行命令，请在命令提示符后输入问号。

### 优先执行模式

保护优先访问可以防止未经授权的访问并确保运行参数。密码区分大小写，密码的每个字符在屏幕上都显示为星号。

要查看并列出的优先执行模式命令，请：

□□□ 在提示符下键入 **enable**，然后按 <Enter> 键。

□□□ 当系统显示输入密码提示时，输入密码并按 <Enter> 键。

优先执行模式提示符显示为设备主机名后跟 #。例如：

```
console#
```

□□□ 要列出优先执行命令，请在命令提示符下键入问号。

□□□ 要从优先执行模式返回到用户执行模式，请键入 **exit** 命令或按 <Ctrl><Z> 组合键。

以下示例说明了如何访问优先执行模式，然后再返回用户执行模式：

```
console>enable  
Enter Password: *****  
console#  
console#exit  
console>
```

使用 **exit** 命令可以返回到上一个模式。例如，可以从接口配置模式返回全局配置模式，以及从全局配置模式返回优先执行模式。

## 全局配置模式

全局配置命令适用于系统配置，而不是特定的协议或接口。

要访问全局配置模式：

□□□ 在优先执行模式提示符后键入 **configure** 并按 <Enter> 键。全局配置模式提示符显示为设备主机名后跟 (config) 和数字符号 #。

```
console(config)#
```

□□□ 要列出全局配置命令，请在命令提示符后输入问号。

□□□ 要从全局配置模式返回到优先执行模式，请键入 **exit** 命令或使用 <Ctrl><Z> 命令。

以下示例说明了如何访问全局配置模式并返回到优先执行模式：

```
console#  
console#configure  
console(config)#exit  
console#
```

## 接口配置模式

使用接口配置命令可以修改特定的 IP 接口设置（包括网桥组和说明等）。接口配置模式包括：

- **VLAN** — 包含创建 VLAN 并将其配置为一个整体的命令，例如创建一个 VLAN 并将 IP 地址应用于该 VLAN。
- **Port Channel**（端口信道）— 包含配置链路聚合组 (LAG) 的命令。
- **Ethernet**（以太网）— 包含管理以太网端口配置的命令。

- **Loopback** (回送) — 包含用于管理回送接口配置的命令。
- **Tunnel** (通道) — 包含用于管理通道接口配置的命令。

---

[返回目录页面](#)

[返回目录页面](#)

## 电缆和端口信息

Dell™ PowerConnect™ 6200 系列用户指南

- [10/100/1000 以太网接口](#)
- [SFP 接口](#)
- [双 10G 插槽接口](#)
- [串行电缆连接](#)
- [直流电和交流电连接](#)

本节介绍了交换机的物理接口，并提供了有关电缆连接的信息。

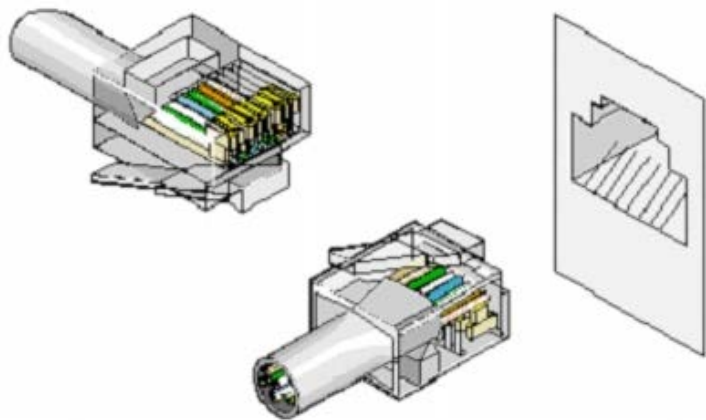
站点是通过前面板上的物理接口连接至交换机的。对于每个站点，将设置相应的模式（半/全双工和自动）。

---

### 10/100/1000 以太网接口

使用直通电缆可以将交换端口连接至以标准 RJ-45 以太网站点模式布线的站点。传输设备使用绞接电缆相互连接。[图 4-1](#) 所示为 RJ-45 连接器。

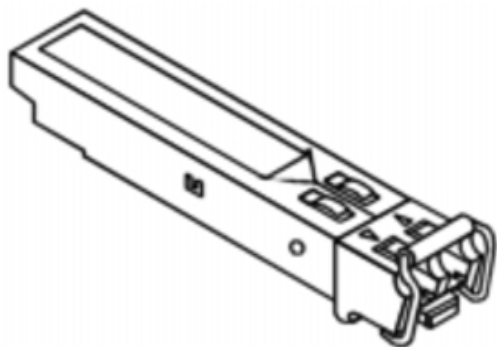
图 4-1. RJ-45 连接器



### SFP 接口

SFP 接口位于控制台前面。 [图 4-2](#) 所示为 SFP 连接器。

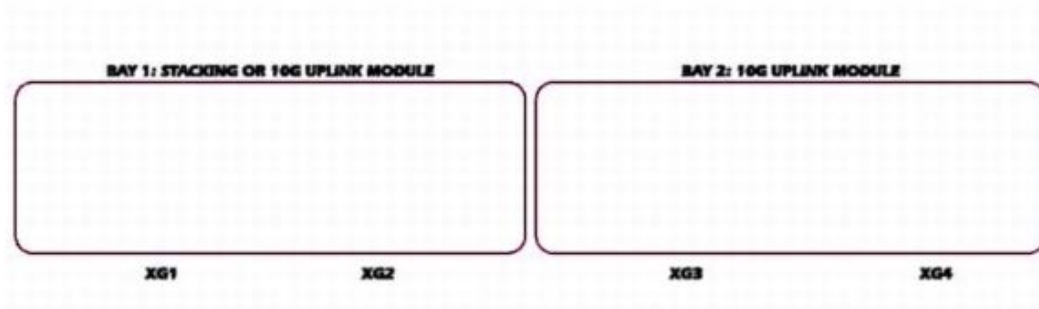
图 4-2. SFP 连接器



## 双 10G 插槽接口

6200 系列交换机背面的插槽支持双 XAU1 接口。当这些接口支持 XFP 模块时，可以在 10 Gbps 速率下运行；当支持堆栈模块时，其运行速率为 12 Gbps（仅左边的插槽，可从背面看到）。图 4-3 所示为 XAU1 插槽。

图 4-3. XAU1 插槽



## 串行电缆连接

可以使用串行电缆（虚拟调制解调器）将交换机连接到终端进行初始设置和配置（此外，还可以使用运行终端仿真软件的计算机）。交换机的串行电缆是一种内孔对内孔的 DB-9 绞接电缆（请参阅图 4-4）。

图 4-4. 串行连接器



## 将交换机连接至终端

- 将串行电缆连接至终端（控制台）ASCII DTE RS-232。
- 将接口电缆连接到交换机的串行端口（请参阅图 4-5）。
- 如果配置的是堆栈，则将接口电缆连接到主交换机的串行端口。

图 4-5. 交换机的串行连接



## 直流电和交流电连接

- 使用已安全接地的 5 英尺（1.5 米）标准电源电缆，将电源电缆连接到背面板上的交流电源主插槽（请参阅图 4-6）。
- 将电源电缆连接至接地的交流电源插座。



□□□ 如果使用的是冗余直流电源设备（例如 RPS600 或 EPS470），则将直流电源电缆连接到背面板上的直流电源插槽（请参阅图 4-6）。

□□□ 通过检查前面板上的 LED 来确定设备已正确连接并且运行正常。

有关 LED 的完整说明，请参阅 [LED 定义](#)。

图 4-6. 交换机的交流和直流电源连接



[返回目录页面](#)

[返回目录页面](#)

# 配置 Dell™ PowerConnect™


## Dell™ PowerConnect™ 6200 系列用户指南

- [启动 CLI](#)
- [一般配置信息](#)
- [引导交换机](#)
- [配置概览](#)
- [高级配置](#)
- [软件下载和重新引导](#)
- [引导菜单功能](#)
- [实例配置过程](#)


本章介绍交换机初始配置。包括以下主题：

- [启动 CLI](#)
- [一般配置信息](#)
- [引导交换机](#)
- [配置概览](#)
- [高级配置](#)
- [软件下载和重新引导](#)
- [引导菜单功能](#)
- [实例配置过程](#)

完成所有外部连接后, 请将某个终端与交换机相连以监测引导和其它过程。


 **注：**如果安装的是交换机堆栈, 请将终端连接至主交换机。交换机堆栈首次通电时, 这些交换机将选出主交换机, 这一主交换机可能位于堆栈中的任何位置。该交换机将亮起主交换机 LED。如果将终端连接至附属交换机, 将无法使用 CLI。

然后, 按照[图 5-1](#) 中所示的安装和配置过程的顺序执行操作。对于初始配置, 请执行标准交换机配置。本节稍后将对执行其它功能进行说明。

 **注意：**在继续之前, 请阅读本产品的版本注释。您可以从 Dell 支持网站 [support.dell.com](http://support.dell.com) 下载版本注释。

## 启动 CLI

要开始运行 CLI, 请按以下步骤进行：

 **注：**以下步骤仅适用于控制台线路。

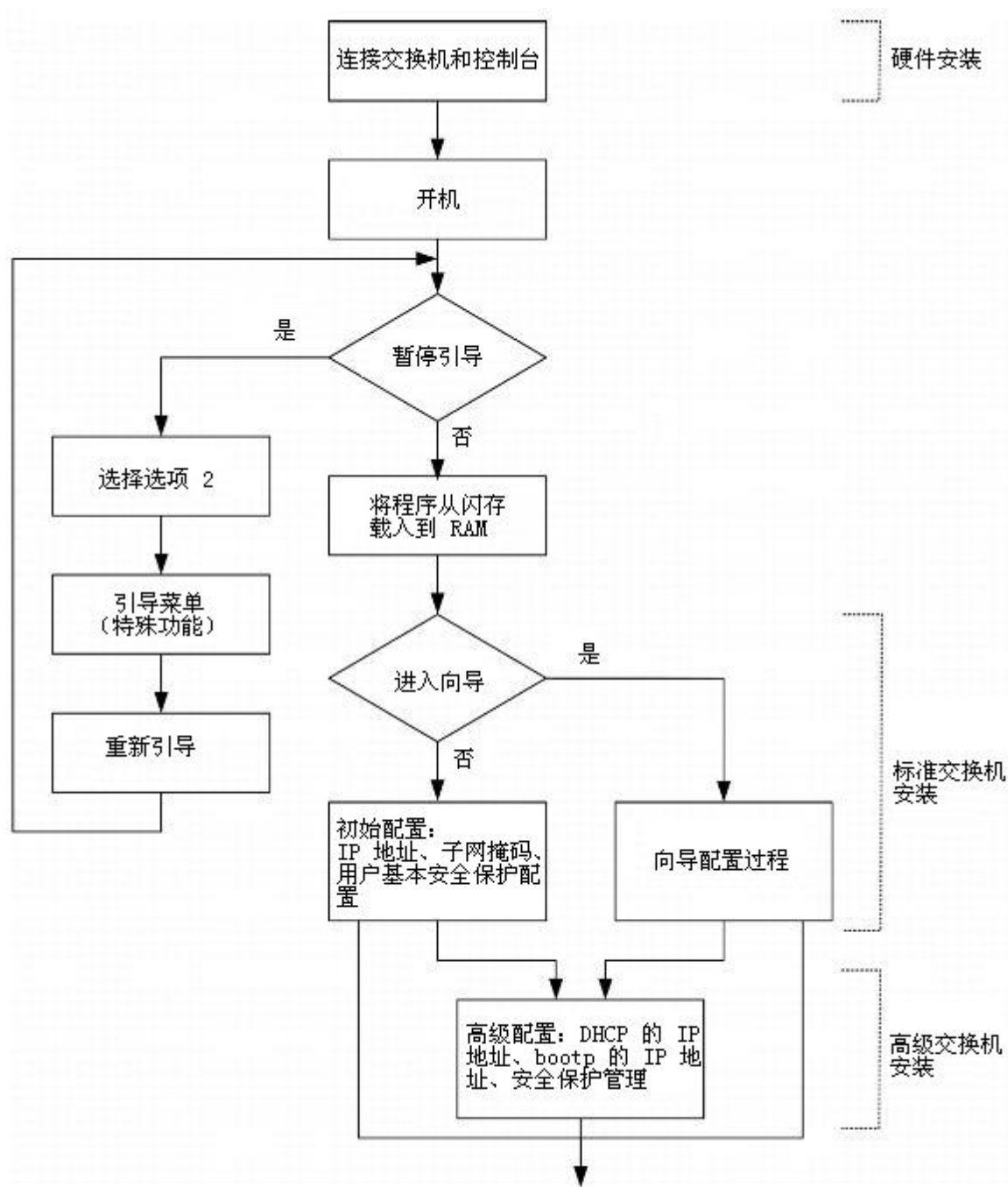
□□□ 启动交换机并等待, 直至系统完成启动过程。这时将显示 **Easy Setup Wizard** (简易安装向导) 欢迎消息。

□□□ 使用 **Easy Setup Wizard** (简易安装向导) 配置交换机并输入必要的命令以完成所需的任务。

□□□ 任务完成后, 使用 **quit** 或 **exit** 命令退出会话。

可以通过与交换机控制台端口的直接连接或 Telnet 连接来管理交换机 (或堆栈)。如果直接连接到交换机, 则无需用户帐户即可访问交换机。然而, 如要通过 Telnet 访问交换机, 则必须至少定义一个用户帐户。另外, 如果是通过 Telnet 连接进行访问, 服务器必须具有已定义的 IP 地址, 已被授予相应的管理访问权限, 并且在使用 CLI 命令之前工作站已连接至交换机。

图 5-1.



安装和配置流程图

## 一般配置信息


6200 系列交换机在交付时提供含有交换机操作系统的二进制文件，以及用于定义交换机与其网络环境的关系的 ASCII 配置文件。配置过程包括调整 ASCII 配置文件，以便每个交换机都适合其唯一的网络拓扑。

## 自适应


自适应允许交换机（或堆栈，作为一个单元进行操作）公布操作模式，并与另一个共享点对点链路网段的交换机共享信息。这样可以自动配置这两个交换机，以最大程度地利用其能力。

自适应完全在链路初始化过程中的物理层内执行，而不会引发 MAC 或更高协议层的任何额外开销。自适应允许端口执行以下操作：

- 公布其能力
- 确认接收和理解两个交换机共享的共同操作模式
- 拒绝使用两个交换机没有共享的操作模式
- 为每个端口配置两个端口均支持的最高级操作模式

 **注:** 确保总是尽可能地在链路两端使用自适应, 以避免潜在的问题。

如果交换机的一个端口将要连接到的工作站或服务器网络接口卡 (NIC) 不支持自适应, 或没有设置为自适应, 则需要执行更多的步骤。交换端口和 NIC 均必须手动设置为相同的速率和双工模式。使用 **Web** 浏览器界面或 **CLI** 命令可以完成此设置。

 **注意:** 如果链路另一端的站点尝试与手动配置为全双工的端口自适应, 则自适应将导致此站点尝试以半双工运行。产生的不匹配可能会导致严重的帧丢失。这是自适应标准所固有的。

## 终端连接配置

交换机需要配置以下终端连接参数:

- 无奇偶校验
- 1 个停止位
- 8 个数据位
- 无流控制


## 波特率

可以将波特率手动更改为以下任一值:

- 2400
- 4800
- 9600 (默认波特率)
- 19200
- 38400
- 57600
- 115200

以下是使用 **CLI** 命令更改默认波特率的配置示例:

```
console#configure
console(config)#line console
console(config-line)#speed 115200
```

 **注:** 切记在工作站的终端仿真软件上设置波特率, 使之与交换机速率相符。

## 其它配置要求

以下是下载嵌入式软件和配置交换机的要求:

- ASCII 终端 (或仿真) 连接到单元后部的串行端口 (绞接电缆)
- 为交换机分配以用于交换机远程控制的 IP 地址可以与 Telnet、SSH 等配合使用

## 引导交换机

打开电源并连接本地终端后, 交换机将进行开机自测 (POST)。POST 在每次初始化交换机时进行, 用于检查硬件组件, 以确定交换机在完全引导之前是否完全正常运转。

如果检测到严重问题, 程序流程就会停止。如果 POST 成功通过, 将载入一个有效的可执行映像到 RAM 中。

POST 信息显示在终端上, 用于指出自测是否成功。

要引导交换机, 请执行以下步骤:

□□□ 确保串行电缆连接至终端。

□□□ 将电源设备连接至交换机。

□□□ 打开交换机电源。

在交换机引导时, 引导检测会首先计算交换机内存可用性, 然后再继续引导。

□□□ 在引导过程中, 如有必要运行特殊过程, 可以使用 **Boot** (引导) 菜单。要进入 **Boot** (引导) 菜单, 请在以下消息显示之后的前十秒钟内按 **2**。

选择一个选项。如果 10 秒钟内未选择, 则

操作码将启动。

1 - 启动操作码。

2 - 启动 Boot (引导) 菜单。

选择 (1, 2):2

有关 **Boot** (引导) 菜单的信息, 请参阅[引导菜单功能](#)。以下文本是整个 POST 的显示示例:

```
CPU Card ID: (CPU 卡 ID: ) 0x508541
volume descriptor ptr (pVolDesc): (卷描述符指针 [pVolDesc]: ) 0xffefd0
cache block I/O descriptor ptr (cbio): (高速缓存块 I/O 描述符指针 [cbio]: ) 0xffefde0
auto disk check on mount: (自动磁盘安装检查: ) NOT ENABLED (未启用)
max # of simultaneously open files: (同时打开文件的最大个数: ) 22
file descriptors in use: (使用中的文件描述符: ) 0
# of different files in use: (使用中的不同文件数: ) 0
# of descriptors for deleted files: (已删除文件的描述符数: ) 0
# of obsolete descriptors: (废弃的描述符数: ) 0
current volume configuration: (当前卷配置: )
- volume label: (卷标签: ) NO LABEL; (in boot sector: ) (无标签; [在引导扇区]: )
- volume Id: (卷 ID: ) 0x0
- total number of sectors: (扇区总数: ) 60,716
- bytes per sector: (每扇区字节数: ) 512
- # of sectors per cluster: (每群集扇区数: ) 4
- # of reserved sectors: (保留的扇区数: ) 1
```

```

- FAT entry size: (FAT 输入项大小: ) FAT16
- # of sectors per FAT copy: (每 FAT 副本的扇区数: ) 60
- # of FAT table copies: (FAT 表副本数: ) 2
- # of hidden sectors: (隐藏的扇区数: ) 4
- first cluster is in sector # 136 (第一个群集位于扇区 136 中)
- Update last access date for open-read-close = FALSE (更新上次打开-读取-关闭的访问日期 = FALSE)
- directory structure: (目录结构: ) VFAT
- root dir start sector: (根目录起始扇区: ) 121
- # of sectors per root: (每根目录扇区数: ) 15
- max # of entries in root: (根目录中的最大输入项数: ) 240
FAT handler information: (FAT 处理程序信息: )
-----

```

```

- allocation group size: (分配组大小: ) 2 clusters (2 个群集)
- free space on volume: (卷上的可用空间: ) 15,335,424 bytes (15,335,424 字节)

```

```

Boot Menu Version: (引导菜单版本: ) 22 Dec 2006 (2006 年 12 月 22 日)

```

```

Select an option. (选择一个选项。) If no selection in 10 seconds then (如果 10 秒钟内未选择, 则)
operational code will start. (操作码将启动。)

```

```

1 - Start operational code. (1 - 启动操作码。)
2 - Start Boot Menu. (2 - 启动引导菜单。)

```

```

Select (1, 2):2 (选择 (1, 2):2)

```

```

Boot Menu Version: (引导菜单版本: ) 22 Dec 2006 (2006 年 12 月 22 日)

```

```

Options available (可用选项)

```

```

1 - Start operational code (1 - 启动操作码)
2 - Change baud rate (2 - 更改波特率)
3 - Retrieve event log using XMODEM (3 - 使用 XMODEM 检索事件日志)
4 - Load new operational code using XMODEM (4 - 使用 XMODEM 载入新操作码)
5 - Display operational code vital product data (5 - 显示操作码重要产品数据)
6 - Run flash diagnostics (6 - 运行 flash 诊断)
7 - Update boot code (7 - 更新引导代码)
8 - Delete backup image (8 - 删除备份映像)
9 - Reset the system (9 - 重置系统)
10 - Restore configuration to factory defaults (delete config files) (10 - 将配置恢复为出厂默认值 [删除配置文件])
11 - Activate Backup Image (11 - 激活备份映像)
12 - Password Recovery Procedure (12 - 密码恢复程序)

```

```

[Boot Menu] ([引导菜单])

```

引导过程大约运行 60 秒钟。

自动引导消息在 POST 末尾显示 (请参见最后的行) 表示, 引导过程中没有遇到任何问题。要从 [Boot Menu] ([引导菜单]) 提示符返回操作码, 请按 **1**。



**注:** 以下输出显示的是一个配置示例。每个交换机所显示的项目 (例如地址、版本和日期) 可能会有所不同。

```

Operational Code Date: (操作码日期: ) Fri May 4 07:44:08 2007 (2007 年 5 月 4 日, 星期五, 07:44:08)

```

```

Uncompressing (正在解压缩) .....

```

50% 100%

|||||

Attaching interface lo0...done (正在连接接口 lo0...完成)

Adding 36263 symbols for standalone. (正在为独立式交换机添加 36263 个符号。)

volume descriptor ptr (pVolDesc): (卷描述符指针 [pVolDesc]:) 0xffc0650

cache block I/O descriptor ptr (cbio): (高速缓存块 I/O 描述符指针 [cbio]:) 0xffc0730

auto disk check on mount: (自动磁盘安装检查:) NOT ENABLED (未启用)

max # of simultaneously open files: (同时打开文件的最大个数:) 22

file descriptors in use: (使用中的文件描述符:) 0

# of different files in use: (使用中的不同文件数:) 0

# of descriptors for deleted files: (已删除文件的描述符数:) 0

# of obsolete descriptors: (废弃的描述符数:) 0

current volume configuration: (当前卷配置:)

- volume label: (卷标签:) NO LABEL; (in boot sector:) (无标签; [在引导扇区]:)

- volume Id: (卷 Id:) 0x0

- total number of sectors: (扇区总数:) 60,716

- bytes per sector: (每扇区字节数:) 512

- # of sectors per cluster: (每群集扇区数:) 4

- # of reserved sectors: (保留的扇区数:) 1

- FAT entry size: (FAT 输入项大小:) FAT16

- # of sectors per FAT copy: (每 FAT 副本的扇区数:) 60

- # of FAT table copies: (FAT 表副本数:) 2

- # of hidden sectors: (隐藏的扇区数:) 4

- first cluster is in sector # 136 (第一个群集位于扇区 136 中)

- Update last access date for open-read-close = FALSE (更新上次打开-读取-关闭的访问日期 = FALSE)

- directory structure: (目录结构:) VFAT

- root dir start sector: (根目录起始扇区:) 121

- # of sectors per root: (每根目录扇区数:) 15

- max # of entries in root: (根目录中的最大输入项数:) 240

FAT handler information: (FAT 处理程序信息:)

-----

- allocation group size: (分配组大小:) 2 clusters (2 个群集)

- free space on volume: (卷上的可用空间:) 15,337,472 bytes (15,337,472 字节)

Timebase: (时基:) 66.666666 MHz, MEM:266.666664 MHz, PCI:66.666666 MHz, CPU: 533.333328 MHz

SOC unit 0 attached to PCI device BCM56314\_A0 (SOC 单元 0 连接至 PCI 设备 BCM56314\_A0)

SOC unit 1 attached to PCI device BCM56314\_A0 (SOC 单元 1 连接至 PCI 设备 BCM56314\_A0)

Adding BCM transport pointers (正在添加 BCM 传输指针)

Configuring CPUTRANS TX (正在配置 CPUTRANS TX)

Configuring CPUTRANS RX (正在配置 CPUTRANS RX)

hpc - No stack ports. Starting in stand-alone mode. (hpc - 无堆栈端口。在独立模式下启动。)

(Unit 1 - Waiting to select management unit)> (单元 1 - 正在等待选择管理单元) >

```
<188> JAN 01 00:00:08 0.0.0.0-1 POE[254746256]:broad_poe.c(286) 4 % Unable to set POE Power bank
73 (broad_poe.c(286) 4 % 无法设置 POE 充电器 73)
```

Applying configuration, please wait ... (正在应用配置, 请稍候...)

No Potential unit to configure as Standby when unit 1 joined (当单元 1 加入时, 无法将任何潜在单元配置为备用交换机)

```
<187> JAN 01 00:00:13 192.168.2.1-1 UNITMGR[244207968]:unitmgr.c(4490) 15 %
```

No Potential unit to configure as Standby when unit 1 joined (当单元 1 加入时, 无法将任何潜在单元配置为备用交换机)

....

console>

交换机成功引导后, 将出现一个提示符, 并可以使用本地终端开始配置交换机。但是, 在配置交换机之前, 请确保交换机上已安装了最新的软件版本。如果此版本不是最新的版本, 请下载并安装最新的版本。请参阅[软件下载和重新引导](#)。


## 配置概览

在配置交换机之前, 从网络管理员处获得以下信息:

- 网络 IP 子网掩码
- 用于配置默认路由的默认网关 (下一个跃点路由器) IP 地址

有以下两种配置类型:

- 初始配置包括具有基本安全保护措施的配置功能。
- 高级配置包括动态 IP 配置和更高级的安全保护措施。

 **注意:** 更改任何配置之后, 必须先保存新配置, 然后再重新引导。要保存配置, 请输入:

```
console#copy running-config startup-config
```

简易安装向导

如果系统引导时没有进行任何配置或只保留出厂默认设置, 则会显示一个 **Easy Setup Wizard** (简易安装向导)。**Easy Setup Wizard** (简易安装向导) 用于指导您完成某些初始步骤, 以设置基本系统配置和安全性, 并使交换机具有可管理性。**Easy Setup Wizard** (简易安装向导) 要求在试运行交换机时设置初始管理员帐户。向导设置的这一管理帐户具有最高权限 (15 级)。

**Easy Setup Wizard** (简易安装向导) 将指导您对新安装的交换机进行基本的初始配置, 以便通过 Web、CLI 和远程 Dell Network Manager 立即部署交换机, 并使其发挥作用和完全具有可管理性。初始安装之后, 可以进入系统设置更高级的配置。

默认情况下, 交换机出厂时的 IP 地址为 192.168.2.1, 子网掩码为 255.255.255.0。系统采用默认管理 VLAN ID=1 进行设置。初始试运行必须通过串行接口进行, 如果没有 IP 地址, 则无法访问其它管理界面。

该向导设置交换机的以下配置:

- 建立拥有权限的初始用户帐户以及有效的密码。在安装过程中, 该向导将配置一个具有权限的用户帐户。初始帐户具有最高权限 (15 级)。
- 启用 CLI 登录和 HTTP/HTTPS 访问, 以便仅使用本地验证设置。您可以稍后返回并配置 Radius 或 TACACS+。
- 设置管理 VLAN 的 IP 地址。
- 设置 SNMP 管理器要使用的 SNMP 团体字符串 (给定了 IP 地址)。如果该交换机不使用 SNMP 管理, 则可以选择跳过这一步。如果已配置, 默认访问级别将设置为用于访问 SNMP 管理界面的最高权限级别。最初仅激活 SNMPv1/2c。SNMPv3 将禁用, 直至返回而为 SNMPv3 配置安全访问 (例如引擎 ID, 查看等)。SNMP 团体字符串可以包含空格。当您要输入团体字符串时, 向导要求使用引号。尽管团体字符串中可以包含空格, 但并不鼓励使用。默认团体字符串不包含空格。
- 允许指定管理服务器 IP, 或允许从所有 IP 地址中进行 SNMP 访问。
- 设置默认网关 IP 地址。



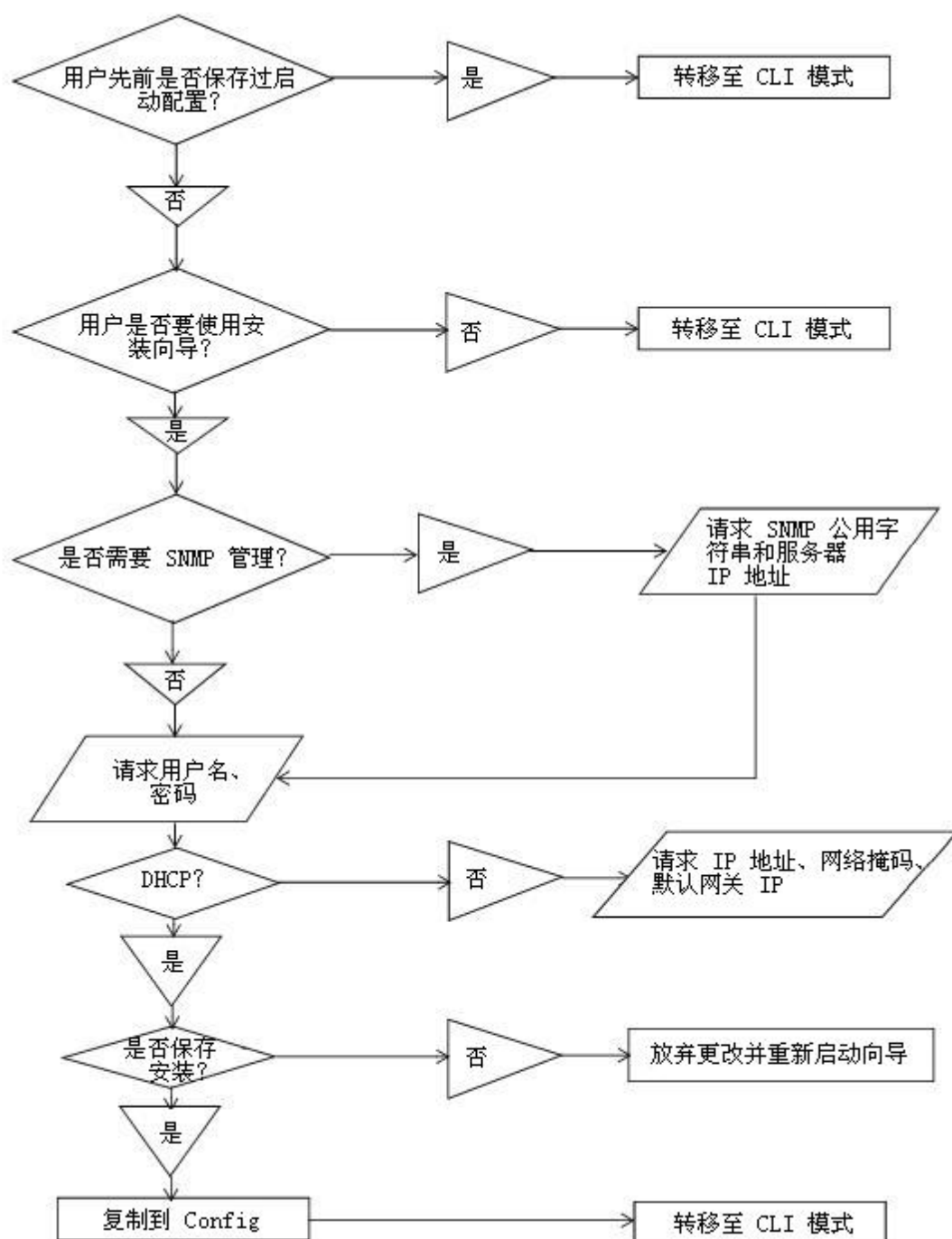
如果最初没有使用向导，会话将默认采用 CLI 模式。安装向导在每次登录时都会继续显示，直至保存一个配置。一旦保存后，向导选项仅在交换机复位为出厂默认设置时才再次显示。

由于交换机会在没有串行连接的字段中开机，因此如果交换机尚未配置，交换机则会等待 60 秒钟，以便对设置提示作出响应。如果没有作出任何响应，交换机将使用出厂默认配置继续正常运行。系统下次重新引导时会提供运行安装向导的机会。

## 功能流程

以下功能流程图显示了 **Easy Setup Wizard**（简易安装向导）的过程。

图 5-2. 安装向导流程图




## 简易安装向导示例会话

本节介绍了一个 **Easy Setup Wizard** (简易安装向导) 会话。请参阅上一节中的状态图以了解一般流程。以下会话所用的值仅为示例: 请要求网络管理员提供实际的值:

- 管理 VLAN 的 IP 地址为 192.168.1.1:255.255.255.0。
- 用户名为 *admin*, 密码为 *admin123*。
- 网络管理系统 IP 地址为 192.168.1.10。
- 默认网关为 192.168.1.100。
- 要使用的 SNMP 团体字符串为 *Dell\_Network\_Manager*。

安装向导根据上述定义的方式配置初始值。向导完成后, 按照以下方式配置系统:

- 启用 SNMPv1/2c, 并按上述定义的方式设置团体字符串。SNMPv3 处于禁用状态。
- 根据定义的方式设置 *admin* 用户帐户。
- 配置网络管理系统。从该管理站, 可以访问 SNMP、HTTP 及 CLI 界面。通过选择 (0.0.0.0) IP 地址, 还可以选择允许所有 IP 地址访问这些管理界面。
- 为默认管理 VLAN (1) 配置 IP 地址。
- 配置默认网关地址。

 **注:** 在以下示例中, 可能的用户选项包括在 [ ] 中。另外, 可能时, { } 将提供默认值。如果未定义选项, 输入 <Return> 将接受默认值。帮助文本在括号中。

以下示例包含与使用上面列出的输入值运行 **Dell Easy Setup Wizard** (简易安装向导) 示例会话相关的提示序列和响应。

Welcome to Dell Easy Setup Wizard (欢迎使用 Dell 简易安装向导)

该安装向导将指导您完成初始交换机配置, 并尽快使您开机并运行。您可以跳过安装向导, 并进行 CLI 模式以手动方式配置交换机。您必须在 60 秒之内答复下一个问题才能运行安装向导, 否则系统将使用默认的系统配置继续正常运行。注: 可以随时通过输入 [ctrl+z] 键退出安装向导。

Would you like to run the set up wizard (you must answer this question within 60 seconds)? (是否要运行安装向导 [必须在 60 秒内回答该问题]? ) [Y/N] (是/否) **y** (是)

### Step 1: (步骤 1: )

The system is not set up for SNMP management by default. To manage the switch using SNMP (required for Dell Network Manager) you can (默认情况下, 系统未设置为使用 SNMP 管理。要使用 SNMP 管理交换机 [Dell Network Manager 要求], 您可以: )

o Set up the initial SNMP version 2 account now. (立即设置初始 SNMP 版本 2 帐户。)

o Return later and set up other SNMP accounts. (For more information on setting up an SNMP version 1 or 3 account, see the user documentation). (稍后返回, 然后设置其它 SNMP 帐户。有关设置 SNMP 版本 3 帐户的详情, 请参阅用户说明文件)。

Would you like to set up the SNMP management interface now? (是否立即设置 SNMP 管理界面?) [Y/N] (是/否) **y** (是)

To set up the SNMP management account you must specify the management system IP address and the "community string" or password that the particular management system uses to access the switch. The wizard automatically assigns the highest access level [Privilege Level 15] to this account. You can use Dell Network Manager or other management interfaces to change this setting and to add additional management system later. For more information on adding management systems, see the user documentation. (要设置 SNMP 管理帐户, 必须指定管理系统 IP 地址, 以及“团体字符串”或特定管理系统用于访问交换机的密码。该向导将自动为此帐户分配最高级别的访问权限 [权限级别 15]。可以使用 Dell Open Manage Network Manager 或其它管理界面更改这一设置, 并且稍后添加其它管理系统。有关添加管理系统的详细信息, 请参阅《用户指南》。)

To add a management station: (要添加管理站: )

Please enter the SNMP community string to be used {public}: (请输入要使用的 SNMP 团体字符串 {public}: )

>> **Dell\_Network\_Manager**<Return>

Please enter the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from any

Management Station {0.0.0.0}: (请输入管理系统的 IP 地址 [A.B.C.D] 或通配符 [0.0.0.0] 以便从任何管理站 {0.0.0.0} 进行管理:)

>> 192.168.1.10<Return>

## Step 2: (步骤 2:)


Now we need to set up your initial privilege (Level 15) user account. This account is used to login to the CLI and Web interface. You may set up other accounts and change privilege levels later. For more information on setting up user accounts and changing privilege levels, see the user documentation. (现在, 需要设置初始权限 [级别 15] 用户帐户。该帐户用于登录到 CLI 界面及 Web 界面。稍后, 可以设置其它帐户并更改权限级别。有关设置用户帐户和更改权限级别的详情, 请参阅《用户指南》。)

To set up a user account: (要设置用户帐户:)

Please enter the user name {admin}: (请输入用户名 {admin}:) **admin**<Return>

Please enter the user password: (请输入用户密码:) **\*\*\*\*\***<Return>

Please reenter the user password: (请重新输入用户密码:) **\*\*\*\*\***<Return>

 **注:** 如果第一次和第二次输入的密码不相同, 系统将提示用户直至密码相同为止。

## Step 3: (步骤 3:)

Next, an IP address is set up. The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch. Optionally you may request that the system automatically retrieve an IP address from the network via DHCP (this requires that you have a DHCP server running on the network). (接下来, 设置 IP 地址。在默认 VLAN (VLAN #1) 上定义 IP 地址, 其中的所有端口均是成员。对于交换机, 这是用于访问 CLI 界面、Web 界面或 SNMP 界面的 IP 地址。另外, 您还可以请求系统通过 DHCP 从网络自动检索 IP 地址, 而这要求网络上运行有一个 DHCP 服务器。)


To set up an IP address: (要设置 IP 地址:)

Please enter the IP address of the device (A.B.C.D) or enter "DHCP" (without the quotes) to automatically request an IP address from the network DHCP server: (请输入设备的 IP 地址 [A.B.C.D] 或输入 "DHCP" [不带引号] 以自动从网络 DHCP 服务器请求 IP 地址 (192.168.2.1):)

>> 192.168.2.1<Return>


Please enter the IP subnet mask (A.B.C.D or /nn){255.255.255.0}: (请输入 IP 子网掩码 [(A.B.C.D 或 /nn){255.255.255.0}]:)

>> 255.255.255.0<Return>

 **注:** 如果您在上面的步骤中选择了 DHCP, 则系统不会要求提供 IP 子网掩码, 因为此信息由 DHCP 服务器提供。

## Step 4: (步骤 4:)

Finally, set up the default gateway. Please enter the IP address of the gateway from which this network is reachable (for example 0.0.0.0): (最后, 设置默认网关。请输入通过它可访问网络的网关的 IP 地址 [例如 0.0.0.0]:) >> 192.168.2.100<Return>

 **注:** 如果您在上面的步骤中选择了 DHCP, 则系统不会要求提供默认网关, 因为此信息由 DHCP 服务器提供。

This is the configuration information that has been collected: (以下是已收集的配置信息:)

SNMP Interface = "Dell\_Network\_Manager"@192.168.1.10 (SNMP 界面 = "Dell\_Network\_Manager"@192.168.1.10)

User Account set up = admin (用户帐户设置 = admin)

Password = \*\*\*\*\* (密码 = \*\*\*\*\*)

Management IP address = 192.168.2.1 255.255.255.0 (管理 IP 地址 = 192.168.2.1 255.255.255.0)

Default Gateway = 192.168.2.100 (默认网关 = 192.168.2.100)

## Step 5: (步骤 5:)

If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file. If the information is incorrect, select (N) to discard configuration and restart the wizard: (如果信息正确, 请选择 (Y) 保存配置, 并将其复制到启动配置文件。如果信息不正确, 请选择 (N) 丢弃配置, 然后重新启动向导: ) [Y/N] (是/否) **y** (是)

Thank you for using Dell Easy Set up Wizard. You will now enter CLI mode. (感谢您使用 Dell 简易安装向导。现在您将进入 CLI 模式。)

## 高级配置

### CLI 基础知识

“用户执行”模式和“优先执行”模式下的 **help** 命令可以显示键盘快捷方式。以下是帮助命令的显示实例：

```

Console>help
HELP: (帮助: )
Special keys: (特殊键: )
DEL, BS .... delete previous character (删除上一个字符)
Ctrl-A .... go to beginning of line (转至行开头)
Ctrl-E .... go to end of line (转至行末尾)
Ctrl-F .... go forward one character (前进一个字符)
Ctrl-B .... go backward one character (后退一个字符)
Ctrl-D .... delete current character (删除当前字符)
Ctrl-U, X .. delete to beginning of line (删除行开头)
Ctrl-K .... delete to end of line (删除行末尾)
Ctrl-W .... delete previous word (删除上一个字)
Ctrl-T .... transpose previous character (转置上一个字符)
Ctrl-P .... go to previous line in history buffer (转至历史缓冲区中的上一行)
Ctrl-R .... rewrites or pastes the line (重写或粘贴行)
Ctrl-N .... go to next line in history buffer (转至历史缓冲区中的下一行)
Ctrl-Y .... print last deleted character (打印上次删除的字符)
Ctrl-Z .... return to root command prompt (返回引导命令提示符)
Ctrl-Q .... enables serial flow (启用串行流)
Ctrl-S .... disables serial flow (禁用串行流)
    Tab, <SPACE> command-line completion (命令行完成)
Exit .... go to next lower command prompt (转至下一个较低的命令提示符)
? .... list choices (列出选项)

```

### 上下文相关帮助

**?** 命令用于获取 CLI 中的上下文相关帮助。该命令可用于获取可能的子命令列表或列出以部分输入的命令开头的可能命令。在空行指定后，**?** 命令可提供命令树中给定级别所需的命令列表。**?** 还可用于命令输入，以返回完全命令所需的参数的列表。用户已提供的参数不列于命令列表中，以便仅列出丢失的参数。

### 接口命名惯例

在工业标准的 CLI 实施中，存在可接受的 CLI 接口命名惯例。Dell 设备接口命名惯例如下：

- 单元编号/接口 **ID** — 每个接口的标识方法均为：单元编号后跟一个 / 符号，然后紧跟接口 **ID**（如下所示）。例如，**2/g10** 表示堆栈的第二个单元内的千兆位端口 **10**。
- 单元编号 — 单元编号仅用于许多交换机堆栈以形成虚拟设备的堆栈解决方案。在此情况下，单元编号表示堆栈内的物理设备标识符。

- 接口 **ID** — 由接口类型后跟接口编号构成。当前有预定义的接口类型列表（如下所示）。如果要定义额外的接口类型，则必须向 Dell 注册。例如，**2/g10** 表示第二个单元上的千兆位端口 10。
- 接口类型 — 以下接口类型在 6200 系列交换机中定义：
  - **g** — 千兆位以太网端口（例如 **1/g2** 为千兆位以太网端口 2）。
  - **xg** — 10 千兆位以太网端口（例如 **1/xg2** 为 10 千兆位以太网端口 2）。

## PowerConnect 6200 系统的《CLI 参考指南》

有关所有用于 6200 系列交换机的 CLI 命令的详细信息，请参阅《CLI 参考指南》。

本节提供有关以下常见任务的摘要信息：

- [修改交换端口默认设置](#)
- [从 DHCP 服务器检索 IP 地址](#)
- [配置初始控制台密码](#)
- [配置初始 Telnet 密码](#)
- [配置初始 HTTP 密码](#)
- [配置初始 HTTPS 密码](#)

### 修改交换端口默认设置

通过 DHCP 和 BOOTP 配置/获取 IP 地址时，从这些服务器获取的配置包括 IP 地址，还可能包括子网掩码和默认网关。

首次登录时，CLI 会进入命令结构的根目录。要转至其它级别的命令结构，请输入诸如 **configure** 的命令，可使 CLI 进入 *config* 子目录树。要返回命令结构中的上一级别，请使用 **exit** 命令。

```
SwitchA#configure
SwitchA(config)#exit
SwitchA#
```

以下示例显示了 6200 系列交换机所用的系统提示符：

- **SwitchA>** 表示设备名称为 *SwitchA*，CLI 当前处于顶级命令结构。CLI 同时也处于用户执行模式。
- **SwitchA#** — 该提示符与上面的提示符类似，但不同之处在于 **#** 表示 CLI 处于优先执行模式（而不是处于用户执行模式）。
- **SwitchA(config)#** — 表示 CLI 当前处于命令结构的全局配置模式。在顶级键入 **configure** 即可进入该模式。
- **SwitchA(config-if)#** — 该提示符表示 CLI 当前处于接口配置模式。从配置模式键入 **interface range ethernet**、**interface range port-channel** 或 **interface range vlan** 即可进入该模式。在此情况下，由于没有接口的特定参考，因此系统在通用接口集中运行。
- **SwitchA(config-if-1/g1)#** — 表示 CLI 当前在千兆位以太网接口 1 上运行。

### 交换端口默认设置

下表说明了交换机端口的默认设置。

表 5-1. 端口默认设置

--	--

功能	默认设置
端口速率和模式	1000M 自适应
端口转发状态	已启用
防队列阻塞	打开 (已启用)
流控制	熄灭
背压	熄灭

以下是使用 CLI 命令更改端口 1/ g1 的端口速率的示例:

```
console(config)#interface ethernet 1/g1
console(config-if-1/g1)#speed 100
```

## 从 DHCP 服务器检索 IP 地址

使用 DHCP 协议检索 IP 地址时, 该交换机用作 DHCP 客户端。

要从 DHCP 服务器检索 IP 地址, 请执行以下步骤:

选择任何一个端口并将其连接至 DHCP 服务器或具有 DHCP 服务器的子网, 以便检索 IP 地址。

 **注:** 要从 DHCP 服务器检索 IP 地址, 没有必要删除交换机配置。

□□□ 输入以下命令, 以使用选定的端口来获取 IP 地址。

- 分配动态 IP 地址:

```
console#config
console(config)#ip address dhcp
```

接口将自动获取 IP 地址。

□□□ 要验证 IP 地址, 请在系统提示符后输入 **show ip interface** 命令, 如下例所示:

```
console#show ip interface
Management Interface: (管理接口: )
IP Address (IP 地址) ..... 10.240.4.125
Subnet Mask (子网掩码) ..... 255.255.255.0
Default Gateway (默认网关) ..... 10.240.4.1
Burned In MAC Address (固化 MAC 地址) ..... 00:10:18:82:04:35
Network Configuration Protocol Current (当前网络配置协议) .....DHCP
Management VLAN ID (管理 VLAN ID) ..... 1
Routing Interfaces: (路由接口: )

                                Netdir Multi
Interface (接口)  IP Address (IP 地址)  IP Mask (IP 掩码)  Bcast (广播)  CastFwd (传送转发)
-----
vlan1            192.168.10.10 255.255.255.0 Disable (禁用)  Disable (禁用)
vlan2            0.0.0.0 0.0.0.0 Enable (启用)  Disable (禁用)
loopback2       0.0.0.0 0.0.0.0 Disable (禁用)  Disable (禁用)
```

## 安全保护管理和密码配置

系统安全保护是通过 AAA（验证、授权和计费）机制进行处理的，它可以管理用户访问权限、特权和管理方法。AAA 使用本地和远程用户数据库。数据加密是通过 SSH 机制进行处理的。

系统在出厂时未配置默认密码；所有密码均由用户定义。如果用户定义的密码丢失，则可以从 **Boot**（引导）菜单中调用密码恢复程序。该程序仅适用于本地终端，并允许在不输入密码的情况下从本地终端一次性访问交换机。

### 配置安全保护密码

您可以为以下服务配置安全保护密码：

- 控制台
- Telnet
- SSH
- HTTP
- HTTPS



**注：**创建用户名时，默认的优先级为 "1"，即允许访问权限但不允许配置权限。必须将优先级设置为 "15" 才能启用对交换机的访问权限和配置权限。

### 配置初始控制台密码

要配置初始控制台密码，请输入以下命令：

```
console(config)#aaa authentication login default line
console(config)#aaa authentication enable default line
console(config)#line console
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password secret123
```

- 通过控制台会话首次登录交换机时，请在密码提示符后输入 **secret123**。
- 将交换机的模式更改为启用时，请在密码提示符后输入 **secret123**。

### 配置初始 Telnet 密码

要配置初始 Telnet 密码，请输入以下命令：

```
console(config)#aaa authentication login default line
console(config)#aaa authentication enable default line
console(config)#line telnet
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password pass1234
```

- 通过 Telnet 会话首次登录交换机时，请在密码提示符后输入 **pass1234**。



- 将交换机的模式更改为启用时，请输入 **pass1234**。

## 配置初始 HTTP 密码

要配置初始 HTTP 密码，请输入以下命令：

```
console(config)#ip http authentication local
console(config)#username admin password user1234 level 15
```

## 配置初始 HTTPS 密码

要配置初始 HTTPS 密码，请输入以下命令：


```
console(config)#ip https authentication local
```

 **注：** 您应在每次升级交换机上的控制软件应用程序（安装新版本）时生成新的 **crypto** 证书。

配置为通过控制台、Telnet 或 SSH 会话使用 HTTPS 会话时，只需输入一次以下命令。

 **注：** 在 Web 浏览器中，只有启用 SSL 2.0 或更高版本才能显示页面内容。


```
console(config)#crypto certificate 1 generate
console(config)#ip https server
```

 **注：** HTTP 和 HTTPS 服务需要的访问级别为 15，并直接连接至配置级别的访问。

## 软件下载和重新引导

### 通过 XModem 下载软件

本节包含使用 XModem 下载交换机软件（系统和引导映像）的说明，而 XModem 是用于更新备份配置文件的数据传输协议。

 **注：** 由于 XModem 下载不能在其它地方工作，因此在执行此操作时，您必须连接至串行控制台接口。

要使用 XModem 下载软件映像文件：

指定开始传输过程的源文件路径。

以下是一个信息显示示例：

```
console#copy xmodem image
Mode (模式) .....XMODEM
Data Type (数据类型) .....Code
Destination Filename (目的地文件名) ..... image2
管理访问功能将在传输期间被禁用
Are you sure you want to start? (确实要开始吗?) (y/n) (是/否) y (是)
console#boot system image2
```



## 通过 TFTP 服务器下载软件

本节包含通过 TFTP 服务器下载交换机软件（系统和引导映像）的说明。开始下载软件之前，必须先在网络上安装 TFTP 服务器。

从存储系统映像副本的闪存区解压缩系统映像时，交换机将引导并运行。

 **注意：**您必须运行 **boot system** 命令才能激活最新下载的映像。

除非选择其它映像，否则，下次引导时，交换机将解压缩并运行当前活动的系统映像。

要通过 TFTP 服务器下载映像：

□□□ 确保已在其中一个交换机端口上配置了 IP 地址，并且可以将 ping 发送至 TFTP 服务器。

□□□ 确保要下载的文件已保存在 TFTP 服务器上（.stk 文件）。

□□□ 输入 **show version** 命令以验证交换机上当前运行的是哪个软件版本。

以下是一个信息显示示例：

```
console>show version
Image Descriptions (图像说明)
image1:default image (默认图像)
image2:
Images currently available on Flash (当前闪存中可用的图像)
-----
unit (单元)  image1      image2    current-active (当前活动)  next-active (下一个活动)
-----
1   0.15.0.0   0.15.0.0   image1          image1
```

□□□ 输入 **show bootvar** 命令以验证哪个系统映像当前处于活动状态。以下是一个信息显示示例：

```
console>show bootvar
Image Descriptions (图像说明)
image1:default image (默认图像)
image2:
Images currently available on Flash (当前闪存中可用的图像)
-----
unit (单元)  image1      image2    current-active (当前活动)  next-active (下一个活动)
-----
1   0.15.0.0   0.15.0.0   image1          image1
```

□□□ 输入命令 **copy tftp://{ tftp 地址}/{ 文件名} image2** 将新的系统映像复制到交换机。

下载新的映像之后，该映像将被保存在分配给另一个系统映像副本的区域中（image2，如示例中所示）。以下是一个信息显示示例：

```
console#copy tftp://10.254.24.64/pc62xxr0v34.stk image2
Mode (模式) .....TFTP
Set TFTP Server IP (设置 TFTP 服务器 IP) ..... 10.254.24.64
TFTP Path (TFTP 路径) ..... ./
TFTP Filename (TFTP 文件名) ..... pc62xxr0v34.stk
Data Type (数据类型) .....Code
```

Destination Filename (目的地文件名) ..... image2

管理访问功能将在传输期间被禁用

Are you sure you want to start? (确实要开始吗?) (y/n) (是/否) **y** (是)

感叹号表示复制过程正在进行。句号表示复制过程已超时。如果一行中有多个句号，则表示复制过程失败。

- 通过输入 **boot system** 命令来为下一次引导选择映像。运行此命令之后，输入 **show bootvar** 命令，以确保为下一次引导选择了作为 **boot system** 命令的一个参数的副本。

以下是一个信息显示示例：

```
console#boot system image2
```

```
Activating image image2 (正在激活图像 image2) ..
```

```
console>show bootvar
```

```
Image Descriptions (图像说明)
```

```
image1:default image (默认图像)
```

```
image2:
```

```
Images currently available on Flash (当前闪存中可用的图像)
```

```
-----
unit (单元)   image1   image2   current-active (当前活动)   next-active (下一个活动)
-----
```

```
1    0.15.0.0  0.15.0.0   image1       image2
```

如果未通过输入 **boot system** 命令选择下一次引导的映像，系统将从当前活动的映像进行引导 (image1，如示例中所示)。

- 输入 **reload** 命令。系统将显示以下信息：

```
console#reload
```

```
Management switch has unsaved changes. (管理服务器仍未保存更改。)
```

```
Are you sure you want to continue? (确实要继续吗?) (y/n) (是/否)
```

- 输入 **y** (是)。然后将显示以下信息。

```
Configuration Not Saved! (配置未保存!)
```

```
Are you sure you want to reload the stack? (是否确定要重新载入堆栈?) (y/n) (是/否)
```

- 输入 **y** (是) 以重新引导交换机。

## 更新引导代码

**update bootcode** 命令用于更新所有交换机上的引导代码。对于每个交换机，引导代码从活动映像中抽取并被编程到闪存。要更新某交换机的引导代码，请在命令中指定单元 (如以下示例所示)。

要显示交换机上的引导代码，请重新引导该交换机。在引导过程中将显示建立日期。

- 输入以下命令 (其中 2 为单元编号)：

```
console# update bootcode 2
```

```
Updating boot code (正在更新引导代码) ...
```

```
Boot code update completed successfully. (已成功更新引导代码。)
```

- 输入 **reload** 命令。

```
console#reload
```

```
Are you sure you want to reload the stack? (是否确定要重新载入堆栈?) (y/n) (是/否)
```

输入 **y** (是) 以重新引导交换机。

---

## 引导菜单功能

您可以通过 **Boot** (引导) 菜单执行许多配置任务, 该菜单可在完成第一部分的 POST 后调用。

要显示 **Boot** (引导) 菜单:

在引导过程中, 在以下消息显示之后十秒钟内按 **2**:

```
Boot Menu Version: (引导菜单版本: ) Oct 20 2004 (2004 年 10 月 20 日)
```

```
Select an option. (选择一个选项。) If no selection in 10 seconds then (如果 10 秒钟内未选择, 则) operational code will start. (操作码将启动。)
```

```
1 - Start operational code. (1 - 启动操作码。)
```

```
2 - Start Boot Menu. (2 - 启动引导菜单。)
```

选择 (1, 2):

**Boot** (引导) 菜单将显示, 并包含以下配置功能:

```
1 - Start operational code (1 - 启动操作码)
```

```
2 - Change baud rate (2 - 更改波特率)
```

```
3 - Retrieve event log using XMODEM (3 - 使用 XMODEM 检索事件日志)
```

```
4 - Load new operational code using XMODEM (4 - 使用 XMODEM 载入新操作码)
```

```
5 - Display operational code vital product data (5 - 显示操作码重要产品数据)
```

```
6 - Run flash diagnostics (6 - 运行 flash 诊断)
```

```
7 - Update boot code (7 - 更新引导代码)
```

```
8 - Delete backup image (8 - 删除备份映像)
```

```
9 - Reset the system (9 - 重置系统)
```

```
10 - Restore configuration to factory defaults (delete config files) (10 - 将配置恢复为出厂默认值 [删除配置文件])
```

```
11 - Activate Backup Image (11 - 激活备份映像)
```

```
12 - Password Recovery Procedure (12 - 密码恢复程序)
```

以下各节将介绍 **Boot** (引导) 菜单选项。

## 启动操作码

选项 **1** 用于恢复载入操作码。

要从 **Boot** (引导) 菜单重新启动引导过程:

在 **Boot** (引导) 菜单中, 选择 **1** 并按 <Enter>。

系统将显示以下提示:

```
Operational Code Date: (操作码日期: ) Thu Jun 8 12:51:44 2006 (2006 年 6 月 8 日, 星期四, 12:51:44)
```

```
Uncompressing (正在解压缩) .....
50% 100%
||||||||||||||||||||||||||||||||||||||||||||||||||||||||
1 File: (1 个文件: ) bootos.c Line (线) :462 Task (任务) :ffffe00 EC:2863311530 (0xaaaaaaaa)
(0 d 0 hrs 0 min 13 sec)(0 天 0 小时 0 分 13 秒)
Timebase: (时基: ) 24.750275 MHz, MEM:99.001100 MHz, PCI:33.000366 MHz, CPU:198.002200 MHz
PCI device BCM5675_A0 attached as unit 0. (PCI 设备 BCM5675_A0 已连接为单元 0。)
PCI device BCM5695_B0 attached as unit 1. (PCI 设备 BCM5695_B0 已连接为单元 2。)
PCI device BCM5695_B0 attached as unit 2. (PCI 设备 BCM5695_B0 已连接为单元 2。)
PCI device BCM5673_A1 attached as unit 3. (PCI 设备 BCM5673_A1 已连接为单元 4。)
PCI device BCM5673_A1 attached as unit 4. (PCI 设备 BCM5673_A1 已连接为单元 4。)
Adding BCM transport pointers (正在添加 BCM 传输指针)
Configuring CPUTRANS TX (正在配置 CPUTRANS TX)
Configuring CPUTRANS RX (正在配置 CPUTRANS RX)
st_state(0) = 0x0
st_state(1) = 0x3
st_state(2) = 0x2
```

## 更改波特率

选项 **2** 用于更改串行接口的波特率。

要从 **Boot** (引导) 菜单更改波特率:

在 **Boot** (引导) 菜单中, 选择 **2** 并按 <Enter>。

系统将显示以下提示:

```
[Boot Menu] ([引导菜单]) 2
```

选择波特率:

- 1 - 1200
- 2 - 2400
- 3 - 4800
- 4 - 9600
- 5 - 19200
- 6 - 38400
- 7 - 57600
- 8 - 115200
- 0 - no change (无更改)



**注:** 所选的波特率会立即生效。

启动过程将会继续。

## 使用 **XMODEM** 检索事件日志

选项 3 用于检索事件日志并将其下载到 ASCII 终端。

要从 **Boot** (引导) 菜单检索事件日志:

在 **Boot** (引导) 菜单中, 选择 **3** 并按 <Enter>。

系统将显示以下提示:

```
[引导菜单]3
```

```
Sending event log, start XMODEM receive (正在发送事件记录, 开始 XMODEM 接收) .....
```

```
File asciilog.bin Ready to SEND in binary mode (文件 asciilog.bin 准备在二进制模式中发送)
```

```
Estimated File Size 169K, 1345 Sectors, 172032 Bytes (预计文件大小 169K, 1345 个扇区, 172032 字节)
```

```
Estimated transmission time 3 minutes 20 seconds (预计传输时间 3 分 20 秒)
```

```
Send several Control-X characters to cancel before transfer starts. (发送若干 Control-X 字符以在传输开始前取消。)
```

启动过程将会继续。

## 使用 XMODEM 载入新操作码

当必须下载新的软件版本以替换损坏的文件、更新或升级系统软件时, 请使用选项 4。

要从 **Boot** (引导) 菜单下载软件:

在 **Boot** (引导) 菜单中, 选择 **4** 并按 <Enter>。

系统将显示以下提示:

```
[Boot Menu] ([引导菜单]) 4
```

```
Ready to receive the file with XMODEM/CRC (准备使用 XMODEM/CRC 接收文件) ....
```

```
Ready to RECEIVE File xcode.bin in binary mode (准备在二进制模式中接收文件 xcode.bin)
```

```
Send several Control-X characters to cancel before transfer starts. (发送若干 Control-X 字符以在传输开始前取消。)
```

使用超级终端时, 单击 **HyperTerminal** (超级终端) 菜单栏上的 **Transfer** (传输)。

在 **Transfer** (传输) 菜单中, 单击 **Send File** (发送文件)。

系统将显示 **Send File** (发送文件) 窗口。

输入要下载文件的文件路径。

确保协议定义为 Xmodem。

单击 **Send** (发送)。

软件将被下载。软件下载需要几分钟时间, 终端仿真应用程序 (例如超级终端) 可能会显示下载过程进度。

## 显示操作码重要产品数据

选项 5 用于查看引导映像信息。

要从 **Boot** (引导) 菜单显示引导映像信息:

在 **Boot** (引导) 菜单中, 选择 **5** 并按 <Enter>。

系统将显示以下提示:

[Boot Menu] ([引导菜单]) **5**

以下映像位于 Flash 系统文件中:

```
File Name (文件名).....image1
CRC.....0xb017 (45079)
Target Device (目标设备) .....0x00508541
Size (大小) .....0x8ec50c (9356556)
Number of Components (组件数) .....2
Operational Code Size (操作码大小) .....0x7ec048 (8306760)
Operational Code Offset (操作码偏移) .....0x74 (116)
Operational Code FLASH flag (操作码闪存标记) .....1
Operational Code CRC (操作码循环冗余检查) .....0x9B4D
Boot Code Version (引导代码版本) .....1
Boot Code Size (引导代码大小) .....0x100000 (1048576)
Boot Code Offset (引导代码偏移) .....0x7ec0bc (8306876)
Boot Code FLASH flag (引导代码闪存标记) .....0
Boot Code CRC (引导代码循环冗余检查) .....0x1CB8
VPD - rel 0 ver 31 maint_lvl 0
Timestamp - Thu Jun 8 12:51:44 2006 (时间戳 - 2006 年 6 月 8 日, 星期四, 12:51:44)
File (文件) - pc62xxr0v31.stk
```

启动过程将会继续。

## 运行 Flash 诊断程序

选项 **6** 用于运行 FLASH 诊断。用户操作先通过 Y/N (是/否) 问题进行确认, 然后才执行命令。

要从 **Boot** (引导) 菜单执行完整的 Flash 内存测试:

在 **Boot** (引导) 菜单中, 选择 **6** 并按 <Enter>。

系统将显示以下提示:

[Boot Menu] ([引导菜单]) **6**

Do you wish to run flash diagnostics? (是否要运行 flash 诊断?) (Boot code region will not be tested.) (引导代码区域将不会进行测试。) (y/n): (是/否: ) **y**

Input number of diagnostic iterations (输入诊断反复次数) -> **1**

Testing 2 x 28F128J3 base: (正在测试 2 x 28F128J3 基础) 0xfe000000

Iterations remaining = 1 (反复剩余次数 = 1)

Erasing sector 0 (正在擦除扇区 6)


Verify sector 0 erased (验证扇区 6 是否被擦除)

Writing sector 0 (正在写入扇区 6)

Erasing sector 1 (正在擦除扇区 6)

Verify sector 1 erased (验证扇区 6 是否被擦除)

```
Writing sector 1 (正在写入扇区 6)
Erasing sector 2 (正在擦除扇区 6)
Verify sector 2 erased (验证扇区 6 是否被擦除)
Writing sector 2 (正在写入扇区 6)
Erasing sector 3 (正在擦除扇区 6)
Verify sector 3 erased (验证扇区 6 是否被擦除)
Writing sector 3 (正在写入扇区 6)
Erasing sector 4 (正在擦除扇区 6)
Verify sector 4 erased (验证扇区 6 是否被擦除)
Writing sector 4 (正在写入扇区 6)
Erasing sector 5 (正在擦除扇区 6)
Verify sector 5 erased (验证扇区 6 是否被擦除)
Writing sector 5 (正在写入扇区 6)
Erasing sector 6 (正在擦除扇区 6)
Verify sector 6 erased (验证扇区 6 是否被擦除)
Writing sector 6 (正在写入扇区 6)
```

 **注:** 此过程将运行, 直至所有分区被清除、已确认清除和写入。

```
Flash Diagnostics passed (Flash 诊断已通过)
[Boot Menu] ([引导菜单])
```

□□□ 启动过程将会继续。

## 更新引导代码

选项 **7** 用于更新 FLASH 内存中的引导代码。此选项仅在使用“引导菜单”选项 **4** 下载新的引导代码后才有效。用户操作先通过 Y/N (是/否) 问题进行确认, 然后才执行命令。

要从 **Boot** (引导) 菜单下载软件:

□□□ 在 **Boot** (引导) 菜单中, 选择 **7** 并按 <Enter>。

系统将显示以下提示:

```
Do you wish to update Boot Code? (是否要更新引导代码?) (y/n) (是/否) y (是)
Erasing Boot Flash.....Done. (正在擦除引导闪存.....完成。)
Wrote 0x10000 bytes. (已写入 0x10000 字节。)
Wrote 0x20000 bytes. (已写入 0x20000 字节。)
Wrote 0x30000 bytes. (已写入 0x30000 字节。)
Wrote 0x40000 bytes. (已写入 0x40000 字节。)
Wrote 0x50000 bytes. (已写入 0x50000 字节。)
Wrote 0x60000 bytes. (已写入 0x60000 字节。)
Boot code updated (引导代码已更新)
```

□□□ 启动过程将会继续。

## 删除备份映像

选项 8 用于删除 FLASH 内存中的备份映像。用户操作先通过 Y/N (是/否) 问题进行确认, 然后才执行命令。

要从 **Boot** (引导) 菜单删除备份映像:

□□□ 在 **Boot** (引导) 菜单中, 选择 **8** 并按 <Enter>。

系统将显示以下提示:

```
Are you SURE you want to delete backup image : image2 ? (是否确定要删除备份图  
像: image2?) (y/n) (是/否) :y (是)
```

```
Backup image deleted (备份图像已删除) ...
```

```
[Boot Menu] ([引导菜单])
```

□□□ 启动过程将会继续。

## 重置系统

选项 9 用于清除所有 FLASH 并将系统重置为其默认设置。用户操作先通过 Y/N (是/否) 问题进行确认, 然后才执行命令。

要从 **Boot** (引导) 菜单重置系统:

□□□ 在 **Boot** (引导) 菜单中, 选择 **9** 并按 <Enter>。

系统将显示以下提示:

```
[引导菜单]9
```

```
Are you SURE you want to reset the system? (是否确定要重置系统?) (y/n) (是/否) :y (是)
```

□□□ 启动过程将会重新启动。

## 将配置恢复为出厂默认值 (删除配置文件)

选项 10 用于进行加载 (需要使用系统默认配置) 和引导 (无需使用当前启动配置)。从 **Boot** (引导) 菜单中选择 **10** 可以恢复系统默认值。然后, 可通过从 **Boot** (引导) 菜单中选择 **1** 来启动引导序列。

要从 **Boot** (引导) 菜单下载软件:

□□□ 在 **Boot** (引导) 菜单中, 选择 **10** 并按 <Enter>。

系统将显示以下提示:

```
Are you SURE you want to delete the configuration? (是否确定要删除配置?) (y/n) (是/否) :y (是)
```

□□□ 启动过程将会继续。

## 激活备份映像

选项 11 用于激活备份映像。选择此选项后, 活动映像将成为备份映像。

要激活备份映像:

□□□ 在 **Boot** (引导) 菜单中, 选择 **11** 并按 <Enter>。



系统将显示以下信息:

```
Backup image - image2 activated. (备份图像 - image2 已激活)
```

□□□ 启动过程将会继续。

## 密码恢复程序

如果密码丢失, 可使用选项 **12**。此选项允许交换机引导一次, 而不会提示输入控制台密码。注意, 此模式不会提示输入 *enable* 密码。

要仅为本地终端恢复丢失的密码:

□□□ 在 **Boot** (引导) 菜单中, 选择 **12** 并按 <Enter>。

密码被删除。

□□□ 启动过程将会继续。

□□□ 为确保交换机的安全, 请重新为适用的管理方法配置密码。

---

## 实例配置过程

本节将介绍建立交换机的远程网络管理连接所需的基本步骤。但本节对交换机上的各种配置或相关命令不作介绍。

本节还将介绍使用默认配置和定义首次访问交换机时的情况。如果之前输入的配置产生问题, 则启动配置文件 (接通电源时的交换机配置) 应被清除且应重新引导交换机。请参阅[设备默认设置](#)。

## 交换机设置要求

本示例需要以下组件:

- PowerConnect 6200 系列交换机
- 安装了以下组件的工作站:
  - 网络适配卡
  - ASCII 终端应用程序 (例如 Microsoft® Windows® HyperTerminal 或 Procomm Plus™ Terminal)
  - 浏览器应用程序
- 一条虚拟调制解调器 F2F 电缆
- 直通或绞接 UTP (5 类) 电缆

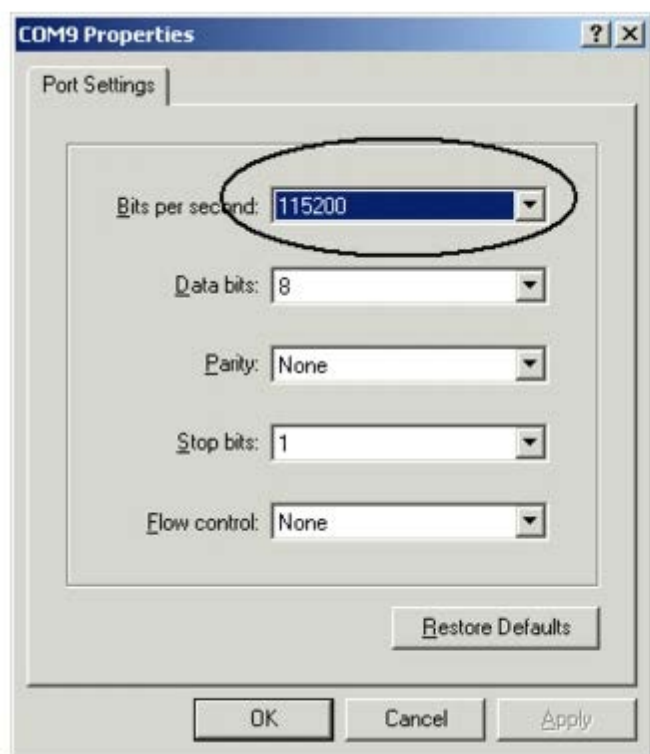
## 初始连接


□□□ 通过 **RS-232** 端口连接交换机和工作站。

□□□ 使用以下设置来设置 **ASCII** 终端并选择适当的 **COM** 端口。


示例屏幕使用的是 **HyperTerminal**。

图 5-3. HyperTerminal 属性窗口



 **注：**新交换机的默认波特率为 9600。该交换机可能具有其它波特率。如果使用默认波特率无法查看交换机终端，请尝试其它波特率。

□□□ 使用 F2F 虚拟调制解调器电缆将工作站连接至交换机。

 **注：**如果配置的是堆栈，请将工作站连接至主交换机。

□□□ 连接交换机电源线，然后打开交换机电源。系统将开始引导过程。显示以下内容时，可根据需要通过选择 **2** 进入 **Boot**（引导）菜单，以运行特殊过程。


选择一个选项。如果 10 秒钟内未选择，则将启动操作码。

1 - Start operational code. (1 - 启动操作码。)

2 - Start Boot Menu. (2 - 启动引导菜单。)

Select (1, 2) (选择 [1, 2]) : **2**

如果没有进入 **Boot**（引导）菜单，系统会将代码解压缩到 **RAM** 并继续操作。代码将从 **RAM** 开始运行，并且系统将显示端口编号及其状态（良好或断开）的列表。

 **注：**以下屏幕信息是一个配置示例。每个交换机所显示的项目（例如地址、版本和日期）可能会有所不同。

current volume configuration: (当前卷配置: )

- volume Id: (卷 ID: ) NO LABEL; (in boot sector: ) (无标签; [在引导扇区]: )

- volume Id: (卷 ID: ) 0x0

- total number of sectors: (扇区总数: ) 60,716

- bytes per sector: (每扇区字节数: ) 512

- # of sectors per cluster: (每群集扇区数: ) 4

- # of reserved sectors: (保留的扇区数: ) 1

- FAT entry size: (FAT 输入项大小: ) FAT16
- # of sectors per FAT copy: (每 FAT 副本的扇区数: ) 60
- # of FAT table copies: (FAT 表副本数: ) 2
- # of hidden sectors: (隐藏的扇区数: ) 4
- first cluster is in sector # 136 (第一个群集位于扇区 136 中)
- Update last access date for open-read-close = FALSE (更新上次打开-读取-关闭的访问日期 = FALSE)
- directory structure: (目录结构: ) VFAT
- root dir start sector: (根目录起始扇区: ) 121
- # of sectors per root: (每根目录扇区数: ) 15
- max # of entries in root: (根目录中的最大输入项数: ) 240

FAT handler information: (FAT 处理程序信息: )

-----

- allocation group size: (分配组大小: ) 2 clusters (2 个群集)
- free space on volume: (卷上的可用空间: ) 21,348,352 bytes (15,335,424 字节)

Boot Menu Version: (引导菜单版本: ) 27 Apr 2006 (2006 年 4 月 27 日)

Select an option. (选择一个选项。) If no selection in 10 seconds then (如果 10 秒钟内未选择, 则) operational code will start. (操作码将启动。)

- 1 - Start operational code. (1 - 启动操作码。)
- 2 - Start Boot Menu. (2 - 启动引导菜单。)

Select (1, 2):1 (选择 (1, 2):2)

Operational Code Date: (操作码日期: ) Wed May 17 10:54:19 2006 (2006 年 5 月 17 日, 星期三, 10:54:19)

Uncompressing (正在解压缩) .....

50% 100%

||||||||||||||||||||||||||||||||||||||||||||||||||||||||

volume descriptor ptr (pVolDesc): (卷描述符指针 [pVolDesc]: ) 0xfd7e6c0

cache block I/O descriptor ptr (cbio): (高速缓存块 I/O 描述符指针 [cbio]: ) 0xfd7fe40

auto disk check on mount: (自动磁盘安装检查: ) NOT ENABLED (未启用)

max # of simultaneously open files: (同时打开文件的最大个数: ) 22

file descriptors in use: (使用中的文件描述符: ) 0

# of different files in use: (使用中的不同文件数: ) 0

# of descriptors for deleted files: (已删除文件的描述符数: ) 0

# of obsolete descriptors: (废弃的描述符数: ) 0

current volume configuration: (当前卷配置: )

- volume Id: (卷 ID: ) NO LABEL; (in boot sector: ) (无标签; [在引导扇区]: )
- volume Id: (卷 ID: ) 0x0
- total number of sectors: (扇区总数: ) 60,716
- bytes per sector: (每扇区字节数: ) 512
- # of sectors per cluster: (每群集扇区数: ) 4
- # of reserved sectors: (保留的扇区数: ) 1
- FAT entry size: (FAT 输入项大小: ) FAT16
- # of sectors per FAT copy: (每 FAT 副本的扇区数: ) 60
- # of FAT table copies: (FAT 表副本数: ) 2

```

- # of hidden sectors: (隐藏的扇区数: ) 4
- first cluster is in sector # 136 (第一个群集位于扇区 136 中)
- Update last access date for open-read-close = FALSE (更新上次打开-读取-关闭的访问日期 = FALSE)
- directory structure: (目录结构: ) VFAT
- root dir start sector: (根目录起始扇区: ) 121
- # of sectors per root: (每根目录扇区数: ) 15
- max # of entries in root: (根目录中的最大输入项数: ) 240
FAT handler information: (FAT 处理程序信息: )
-----
- allocation group size: (分配组大小: ) 2 clusters (2 个群集)
- free space on volume: (卷上的可用空间: ) 21,350,400 bytes (15,335,424 字节)
File (文件) :unitmgr.c, Line (线) :3419, Error (错误) 0 (0x0)
Timebase: (时基: ) 66.666666 MHz, MEM:266.666664 MHz, PCI:66.666666 MHz, CPU:533.333328 MHz
SOC unit 1 attached to PCI device BCM56304_B0 (SOC 单元 0 连接至 PCI 设备 BCM56304_B0)
SOC unit 1 attached to PCI device BCM56304_B0 (SOC 单元 1 连接至 PCI 设备 BCM56304_B0)
Adding BCM transport pointers (正在添加 BCM 传输指针)
Configuring CPUTRANS TX (正在配置 CPUTRANS TX)
Configuring CPUTRANS RX (正在配置 CPUTRANS RX)
hpc - No stack ports. Starting in stand-alone mode. (hpc - 无堆栈端口。在独立模式下启动。)
(Unit 1 - Waiting to select management unit)> (单元 1 - 正在等待选择管理单元) >

```

## 设备默认设置

要返回设备默认设置，请在出现特权模式提示符 (#) 时使用 `delete startup-config` 命令，然后重新引导设备。设备一旦重新载入，将采用默认设置进行设置。

```

console>
console>enable
console#delete startup-config
Startup file was deleted (启动文件已删除)
console#reload
Management switch has unsaved changes. (管理服务器仍未保存更改。)
Are you sure you want to continue? (确实要继续吗?) (y/n) (是/否) y (是)
Configuration Not Saved! (配置未保存!)
Are you sure you want to reload the stack? (是否确定要重新载入堆栈?) (y/n) (是/否) y (是)
Reloading all switches.. (正在重新载入所有交换机..)

```

## 启用远程管理

在控制台输入 `enable` 命令，以进入如下优先执行屏幕：

```

console>enable
console#

```

使用 CAT5 电缆通过一个以太网端口或与交换机相连的网络将管理站连接至交换机。

本示例使用的是端口 **1/g1**。

□□□ (在 ASCII 终端上) 确保接口状态已更改为 **up** (良好) 且 **STP** 状态为转发 (30 秒钟后), 如下所示:

```
console#
01-Jan-2000 01:43:03 %LINK-I-Up:Vlan 1
01-Jan-2000 01:43:03 %LINK-I-Up:1/g1
01-Jan-2000 01:43:34 %STP-I-PORTSTATUS:Port 1/g1: (端口 1/g1: ) STP status Forwarding (STP 状态为正在转发)
```

□□□ 在控制台输入 **config** 命令, 以进入如下配置屏幕模式:

```
console#config
```

□□□ 使用以下命令将 IP 地址设置为 DHCP:

```
console(config)#ip address dhcp
```

□□□ 使用以下命令设置默认网关:

```
console(config)#ip default-gateway 10.254.24.162
```

□□□ 如果管理站是远程网络的成员且未直接连接至接口, 请配置静态路由。

所配置的 IP 地址必须与其中一个交换机 IP 接口属于同一子网。本示例中的静态地址为 **192.168.20.100**。

```
console(config)#ip route 192.168.10.10 255.255.255.0 192.168.20.1 200
```

□□□ 请从交换机对管理站执行 **Ping** 命令, 以确保实现连接。

等待 30 秒钟以使端口处于 **STP** 转发状态, 然后再对管理站执行 **Ping** 命令。本示例中管理站 IP 为 **50.1.1.2**。

```
console>ping 50.1.1.2
64 bytes from 50.1.1.2:icmp_seq=1. time=0 ms
64 bytes from 50.1.1.2:icmp_seq=2. time=0 ms
64 bytes from 50.1.1.2:icmp_seq=3. time=0 ms
64 bytes from 50.1.1.2:icmp_seq=4. time=0 ms
----50.1.1.2 PING Statistics (PING 统计) ----
4 packets transmitted, 4 packets received, 0% packet loss (4 个信息包已发送, 4 个信息包已接收, 0% 信息包丢失)
round-trip (ms) min/avg/max = 0/0/0
```

□□□ 定义用户名和密码, 以便对远程用户 (HTTP 和 HTTPS) 具有 15 级交换机优先访问权限。

在本示例中, 用户名为 **Dell**, 密码为 **Dell1234**, 权限级别为 15。权限级别范围为 1–15, 15 为最高级别。15 级访问权限是用于 Web 界面的唯一访问级别。

```
console#config
console(config)#username Dell password Dell1234 level 15
console(config)#ip http authentication local
console(config)#ip https authentication local
console(config)#crypto certificate generate key_generate
Generating RSA private key, 1024 bit long modulus (正在生成 RSA 私钥, 1024 位长的模块)
```

```
console(config)#ip https server
```

□□□□ 定义用户名和密码以允许访问本地用户，例如控制台、Telnet 或 Web Server 等。

在本示例中，用户名和密码分别为 **Dell** 和 **Dell1234**，权限级别为 15。

```
console(config)#username Dell password Dell1234 level 15
```

```
console(config)#aaa authentication login default line
```

```
console(config)#aaa authentication enable default line
```

```
console(config)#line console
```

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

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

```
console(config-line)#password tommy123
```

```
console(config-line)#exit
```

```
console(config)#line telnet
```

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

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

```
console(config-line)#password bobby123
```

```
console(config-line)#exit
```

```
console(config)#line ssh
```

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

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

```
console(config-line)#password jones123
```

```
console(config-line)#exit
```

□□□□ 将 **running-config** 文件保存为 **startup-config** 文件。

这可确保刚刚完成的配置在交换机重新引导后保持不变。

```
console(config)#exit
```

```
console#copy running-config startup-config
```

此时交换机完成配置，并可通过不同的选项（例如，Telnet、Web 浏览器界面和其它选项）对其进行管理。

## 配置安全管理访问 (HTTPS)

通过标准 Web 浏览器对交换机进行安全管理时，将使用 SSL（安全套接层）安全协议。

要通过标准 Web 浏览器对交换机进行安全管理，请执行以下操作：

□□□ 为了配置交换机以允许 HTTPS 服务器并创建安全密钥，请使用命令 **ip https server** 和 **crypto certificate 1 generate**：

```
console#configure
```

```
console(config)#crypto certificate 1 generate
```

```
Generating RSA private key, 1024 bit long modulus (正在生成 RSA 私钥, 1024 位长的模块)
```

```
console(config)#ip https server
```

```
console(config)#
```

将管理站配置为与常规 HTTP 连接相同的配置。

在浏览器窗口输入地址 `https://设备 IP 地址` (必须输入 `https`) 以通过 HTTPS 连接至交换机。

系统将显示 **Security Alert** (安全警报) 窗口。

单击 **Yes** (是) 确认接受安全认证 (如果未经第三方认证)。

系统将显示 **Login Screen** (登录屏幕)。

输入分配的用户名和密码。

系统将显示交换机 Dell OpenManage™ Switch Administrator。

---

[返回目录页面](#)

[返回目录页面](#)

## 配置系统信息

Dell™ PowerConnect™ 6200 系列用户指南

- [打开 System（系统）页面](#)
- [定义一般设备信息](#)
- [配置 SNMP 设置](#)
- [管理日志](#)
- [定义 IP 寻址](#)
- [运行电缆诊断程序](#)
- [管理设备安全保护](#)
- [定义 SNMP 参数](#)
- [管理文件](#)
- [定义高级设置](#)
- [定义堆栈](#)

---

## 打开 System（系统）页面

使用 **System（系统）** 页面上列出的菜单定义交换机与其环境的关系。要显示 **System（系统）** 页面，请在树视图中单击 **System（系统）**。**System（系统）** 菜单页面包含以下功能的链接：

- [定义一般设备信息](#)
- [配置 SNMP 设置](#)
- [管理日志](#)
- [定义 IP 寻址](#)
- [运行电缆诊断程序](#)
- [管理设备安全保护](#)
- [定义 SNMP 参数](#)
- [管理文件](#)
- [定义高级设置](#)
- [定义堆栈](#)

---

## 定义一般设备信息

**General（一般）** 菜单页面包含指向可以配置设备参数的页面的链接。此页面用于访问以下功能：

- [资产](#)
- [系统健康状况](#)
- [版本](#)
- [系统资源](#)
- [时区配置](#)
- [夏令时配置](#)
- [时钟详情](#)



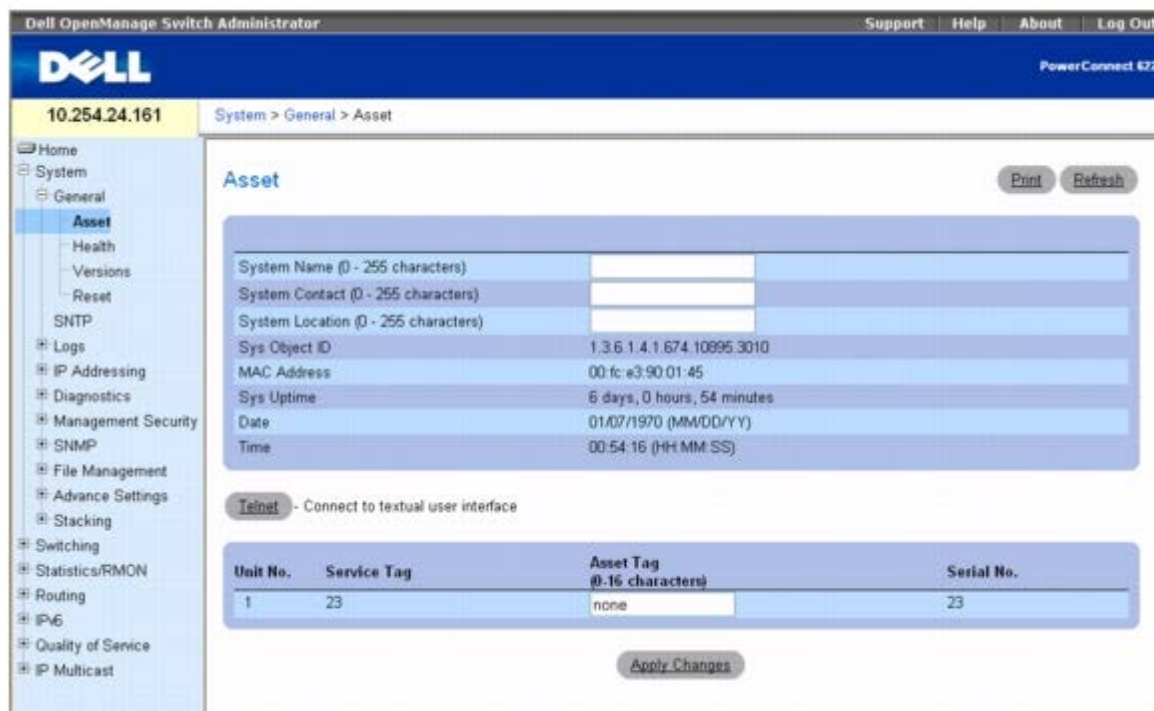
- [重置](#)

## 资产

**Asset** (资产) 页面用于配置和查看一般设备信息。

要显示 **Asset** (资产) 页面，请在树视图中单击 **System** (系统) ® **General** (一般) ® **Asset** (资产)。

图 6-1. 资产



**Asset** (资产) 页面包含以下字段：

**System Name (0 –255 characters)** (系统名称 [0 至 255 个字符]) — 用于分配设备系统名称。

**System Contact (0–255 characters)** (系统联系人 [0 至 255 个字符]) — 用于分配联系人的姓名。

**System Location (0 –255 characters)** (系统位置 [0 至 255 个字符]) — 用于指定系统位置。

**Sys Object ID** (系统对象 ID) — 分配的系统对象 ID。

**MAC Address** (MAC 地址) — 显示交换机的 MAC 地址。

**Sys Uptime** (系统运行时间) — 显示自上次系统重新启动后经过的天数、小时数和分钟数。

**Date** (日期) — 显示当前系统日期。其格式为月、日、年 (MM/DD/YY)。例如，11/01/05 为 2005 年 11 月 1 日。

**Time** (时间) — 显示当前系统时间。其格式为时、分、秒 (HH:MM:SS)。例如，20:12:03 为 8:12:03 PM。

**Unit No.** (单元编号) — 显示交换机在堆栈中的位置。

**Service Tag** (服务标签) — 显示维修设备时使用的服务参考号码。

**Asset Tag (0 –16 characters)** (资产标签 [0 至 16 个字符]) — 显示用户定义的设备参考。

**Serial No.** (序列号) — 显示设备的序列号。

## 定义系统信息

□□□ 打开 **Asset**（资产）页面。


□□□ 定义以下字段：**System Name**（系统名称）、**System Contact**（系统联系人）、**System Location**（系统位置）和 **Asset Tag**（资产标签）。

□□□ 单击 **Apply Changes**（应用更改）。

系统将应用系统参数并更新设备。

## 启动 Telnet 会话

□□□ 打开 **Asset**（资产）页面。

 **注：**需要在启动 Telnet 会话之前设置适当的 Telnet 参数。有关信息，请参阅“[配置初始 Telnet 密码](#)”。如果客户端使用的是 Microsoft® Windows® 环境，则必须针对 Telnet 配置程序。如果客户端使用的是 Unix 环境，则 Telnet 程序必须存在于路径中。

□□□ 单击 **Telnet**。

将显示提示符，表示系统已准备好接受输入。

## 使用 CLI 命令配置设备信息

有关执行此功能的 CLI 命令的信息，请参阅《[CLI 参考指南](#)》的以下章节：

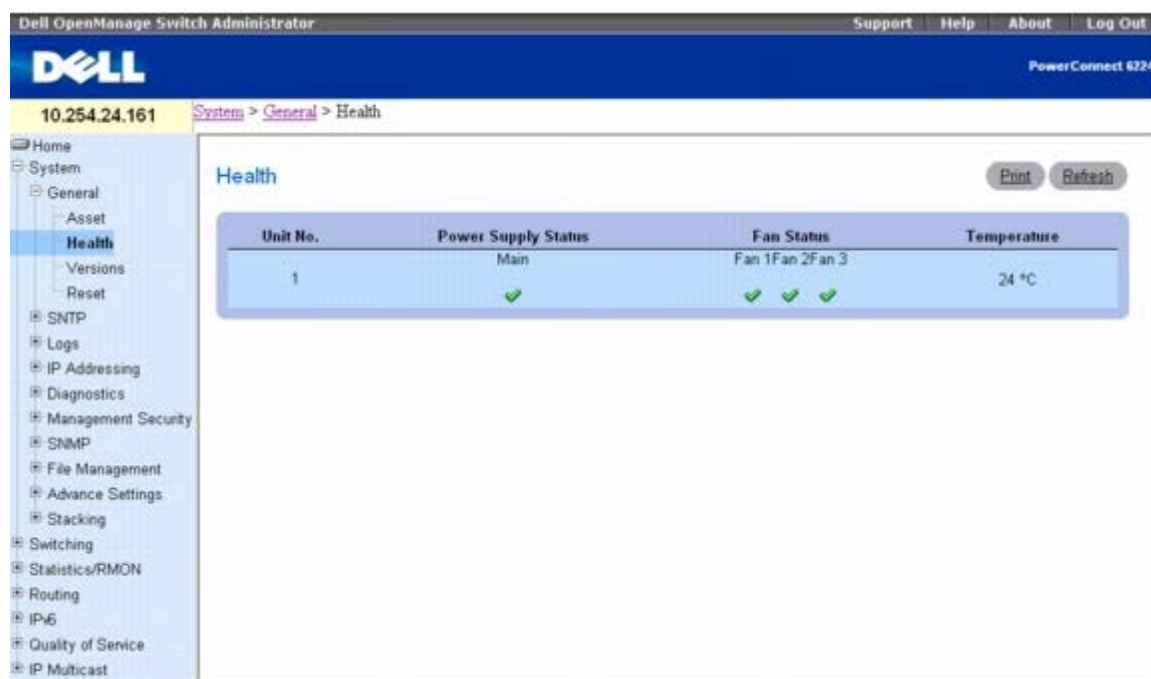
- 系统管理命令
- SNMP 命令
- 时钟命令

## 系统健康状况

**Health**（健康状况）页面用于查看物理设备信息，包括有关交换机的电源和通风条件的信息。

要显示 **Health**（健康状况）页面，请在树视图中单击 **System**（系统）® **General**（一般）® **Health**（健康状况）。

图 6-2. 健康状况



**Health**（健康状况）页面包含以下字段：

**Unit No.**（单元编号）— 显示单元在堆栈中的位置。

**Power Supply Status**（电源设备状态）— 显示电源设备状态。

✓ — 电源设备工作正常。

✗ — 电源设备工作不正常。

**Not Present**（不存在）— 电源设备当前不存在。

**Fan Status**（风扇状态）— 表示风扇状态。PowerConnect 6224 有三个风扇，6248 则有四个。

✓ — 风扇工作正常。

✗ — 风扇工作不正常。

**Not Present**（不存在）— 风扇当前不存在。

**Temperature**（温度）— 显示设备当前的运行温度。

## 使用 CLI 命令查看系统健康状况信息

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

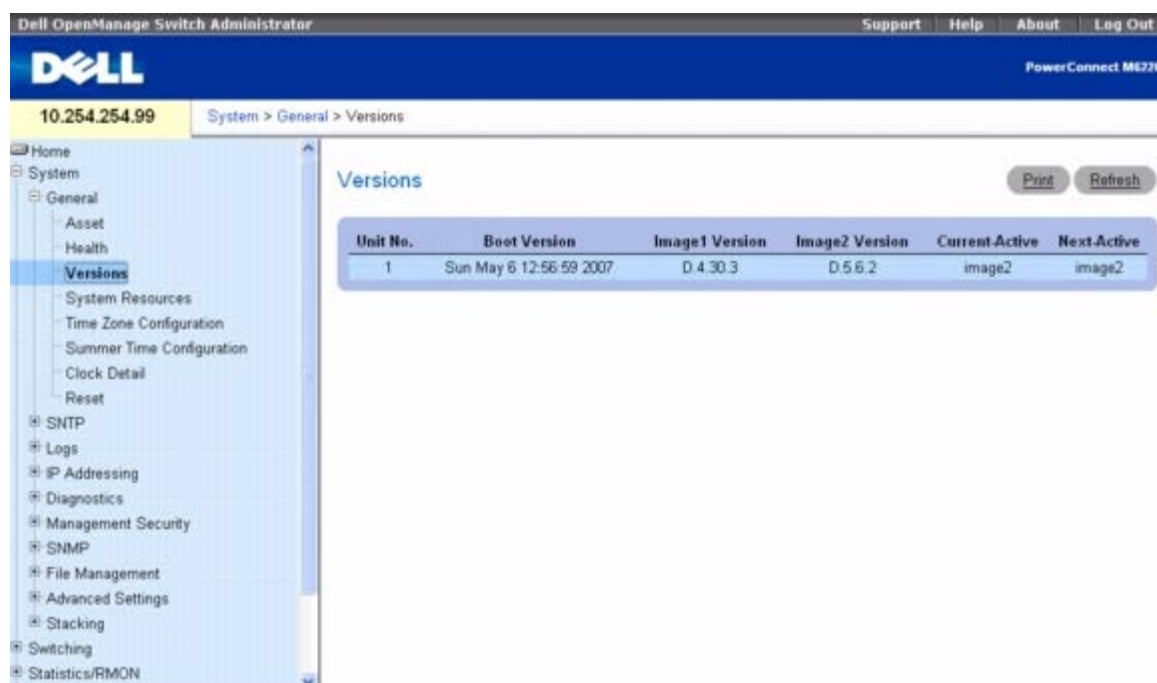
- 系统管理命令

## 版本

**Versions**（版本）页面用于查看当前运行的软件版本信息。

要显示 **Versions**（版本）页面，请在树视图中单击 **System**（系统）® **General**（一般）® **Versions**（版本）。

图 6-3. 版本



**Versions** (版本) 页面包含以下字段：

**Unit No.** (单元编号) — 显示单元在堆栈中的位置。

**Boot Version** (引导版本) — 显示活动映像的引导映像版本。

**Image1 Version** (映像 1 版本) — 显示两个可用软件映像中的第一个软件映像的版本号。

**Image2 Version** (映像 2 版本) — 显示两个可用软件映像中的另一个软件映像的版本号。

**Current-Active** (当前活动) — 显示设备上运行的当前软件版本。

**Next-Active** (下一个活动) — 显示要在当前版本崩溃时载入的软件版本。

## 使用 CLI 显示设备版本

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 系统管理命令

## 系统资源

**System Resources** (系统资源) 页面用于查看有关内存和任务使用情况的信息。

要显示 **System Resources** (系统资源) 页面，请在树视图中单击 **System** (系统) ® **General** (一般) ® **System Resources** (系统资源)。

图 6-4. 系统资源

The screenshot shows the Dell OpenManage Switch Administrator interface. The top navigation bar includes 'Support', 'Help', 'About', and 'Log Out'. The main header displays the Dell logo and 'PowerConnect M6720'. The breadcrumb path is 'System > General > System Resources'. The left sidebar shows a tree view with 'System Resources' selected. The main content area is titled 'System Resources' and contains two sections: 'Memory Usage' and 'Task Utilization Report'.

**Memory Usage**

Total Memory	262144 KBytes
Available Memory	32637 KBytes

**Task Utilization Report**

Task Name	Utilization (%)
osapiTimer	1.05%
bcmLZX.D	0.60%
bcmCNTR.D	0.20%
bcmLNK.D	0.10%
bcmRX	0.25%
ipMapForwardingTask	0.05%
Kernel/Interrupt/Idle	97.75%
<b>TOTAL</b>	<b>100.00%</b>

**System Resources**（系统资源）页面包含以下字段：

**Total Memory**（总计内存）— 显示交换机上的总计内存空间。

**Available Memory**（可用内存）— 显示交换机上可用（可分配）的内存空间。

**Task Name**（任务名称）— 交换机上正在运行的任务的名称。

**Utilization (%)**（利用率百分比）— 相应的任务所使用的 CPU 时间百分比。该值是针对 2 秒钟的持续时间计算得出的。

## 使用 CLI 显示系统资源

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

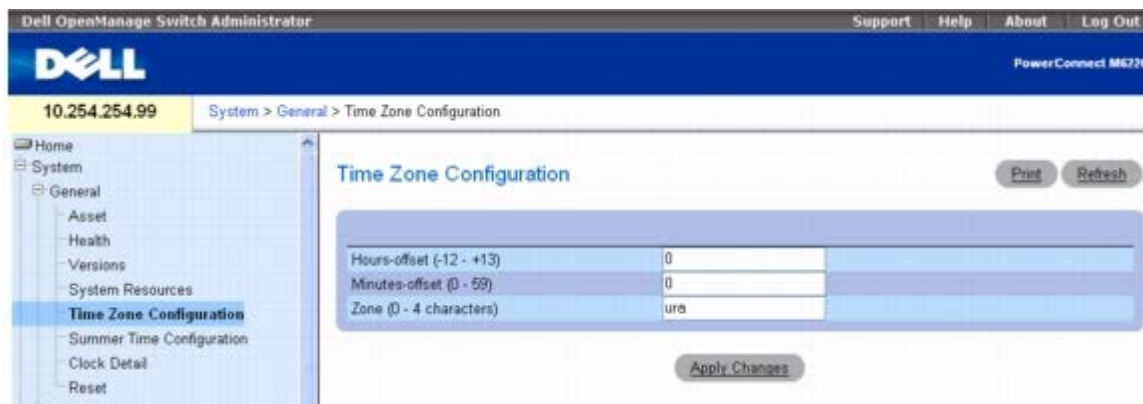
- 系统管理命令

## 时区配置

**Time Zone Configuration**（时区配置）用于配置与协调世界时 (UTC) 之间的时区差。

要显示 **Time Zone Configuration**（时区配置）页面，请在树视图中单击 **System**（系统）® **General**（一般）® **Time Zone Configuration**（时区配置）。

图 6-5. 时区配置



**Time Zone Configuration** (时区配置) 页面包含以下字段：

**Hours-offset** (小时偏移量) — 设置与 UTC 之间的小时偏移量。（范围：-12 至 +13）

**Minutes-offset** (分钟偏移量) — 设置与 UTC 之间的分钟偏移量。（范围：0–59）

**Zone** (区域) — 设置时区的缩写。（范围：0至 4 个字符）

## 定义时区参数

□□□ 打开 **Time Zone Configuration** (时区配置) 页面。

□□□ 根据需要定义各个字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改时区设置并更新设备。

## 使用 CLI 配置时区设置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

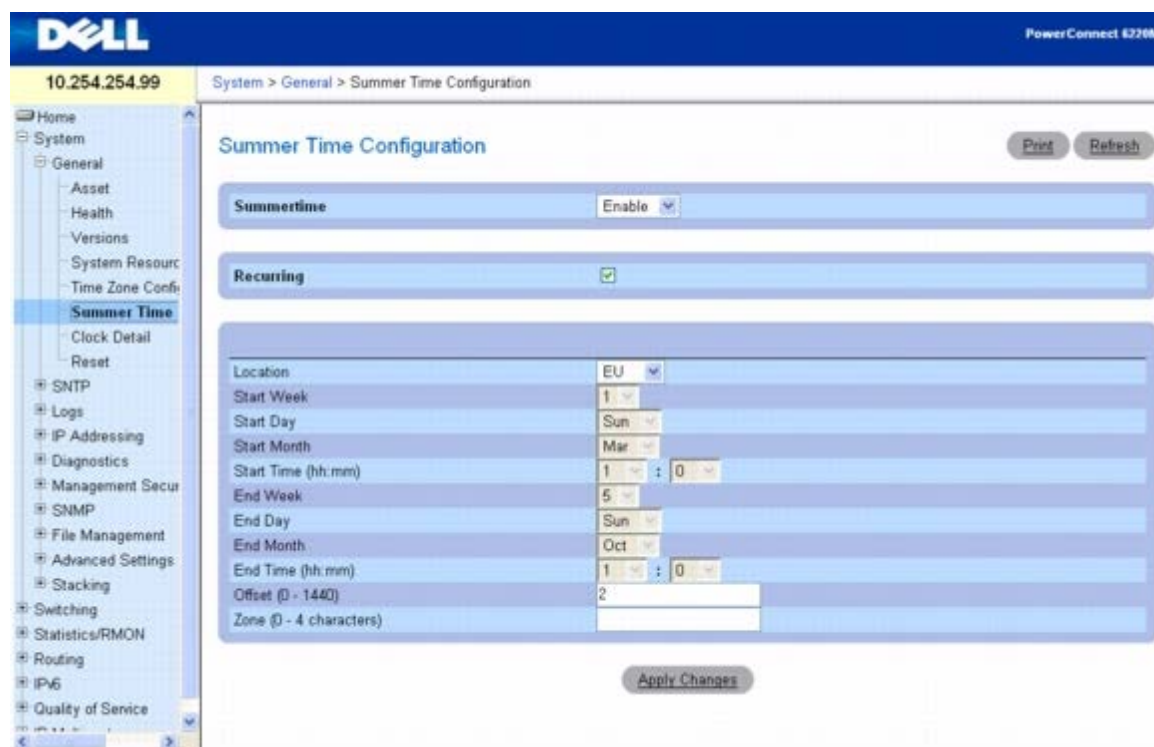
- 时钟命令

## 夏令时配置

**Summer Time Configuration** (夏令时配置) 页面用于指定规定的夏令时时长和偏移量。

要显示 **Summer Time Configuration** (夏令时配置) 页面，请在树视图中单击 **System** (系统) ® **General** (一般) ® **Summer Time Configuration** (夏令时配置)。

图 6-6. 夏令时配置



当选择或清除 **Recurring**（周期性）复选框时，**Summer Time Configuration**（夏令时配置）页面上的字段会发生变化。**Summer Time Configuration**（夏令时配置）页面包含以下字段：

**Recurring**（周期性）— 选择此复选框表示每年都会重复此配置。

**Location**（位置）— 只有当选择了 **Recurring**（周期性）复选框时，此字段才会显示。本软件为美国和欧盟预定义了夏令时配置。要为美国或欧盟以外的地区设置夏令时，请选择 **None**（无）。

**Start Week**（起始周）— 选择起始周编号。只有当选择了 **Recurring**（周期性）复选框时，此字段才会显示。

**Start Day**（起始日）— 选择起始日编号。只有当选择了 **Recurring**（周期性）复选框时，此字段才会显示。

**Start Month**（起始月）— 选择起始月份。

**Start Time**（起始时间）— 选择 hh:mm 格式的起始时间。

**Start Date**（起始日期）— 选择起始日期。只有当清除了 **Recurring**（周期性）复选框时，此字段才会显示。

**Start Year**（起始年）— 选择起始年份。只有当清除了 **Recurring**（周期性）复选框时，此字段才会显示。

**End Week**（结束周）— 选择结束周编号。只有当选择了 **Recurring**（周期性）复选框时，此字段才会显示。

**End Day**（结束日）— 选择结束日编号。只有当选择了 **Recurring**（周期性）复选框时，此字段才会显示。

**End Month**（结束月）— 选择结束月份。

**End Time**（结束时间）— 选择 hh:mm 格式的结束时间。

**End Date**（结束日期）— 选择结束日期。只有当清除了 **Recurring**（周期性）复选框时，此字段才会显示。

**End Year**（结束年）— 选择结束年份。只有当清除了 **Recurring**（周期性）复选框时，此字段才会显示。

**Offset**（偏移量）— 设置要在夏令时期间增加的分钟数（0 至 1440 分钟）。

**Zone**（区域）— 设置要在夏令时生效时显示的时区缩写。

## 定义夏令时参数

□□□ 打开 **Summer Time Configuration**（夏令时配置）页面。



□□□ 根据需要定义各个字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将修改夏令时设置并更新设备。

## 使用 CLI 配置夏令时参数

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 时钟命令

## 时钟详情

**Clock Detail**（时钟详情）页面用于查看当前时间、时区和夏令时设置的相关信息。

要显示 **Clock Detail**（时钟详情）页面，请在树视图中单击 **System**（系统）® **General**（一般）® **Clock Detail**（时钟详情）。

图 6-7. 时钟详情

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb navigation is System > General > Clock Detail. The left sidebar shows the navigation tree with 'Clock Detail' selected. The main content area displays the following information:

Current Time	
Time (hh:mm)	11:01:19
Zone	ura (UTC +0:00)
Date	1 Jan 1970
Time Source	No time source

Time Zone	
Zone	ura
Offset	UTC +0:00

Summertime	
Recurring	No
Start Date	1 Jan 2000
Start Time (hh:mm)	00:00
End Date	2 Jan 2000
End Time (hh:mm)	00:00
Offset	0
Zone	Acronym not configured

**Clock Detail**（时钟详情）页面提供了以下时钟功能的相关信息：

**Current Time**（当前时间）— 这部分显示当前时间。

**Time Zone**（时区）— 这部分显示时区设置。

**Summertime**（夏令时）— 这部分显示夏令时设置。

## 使用 CLI 显示时钟详情

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：



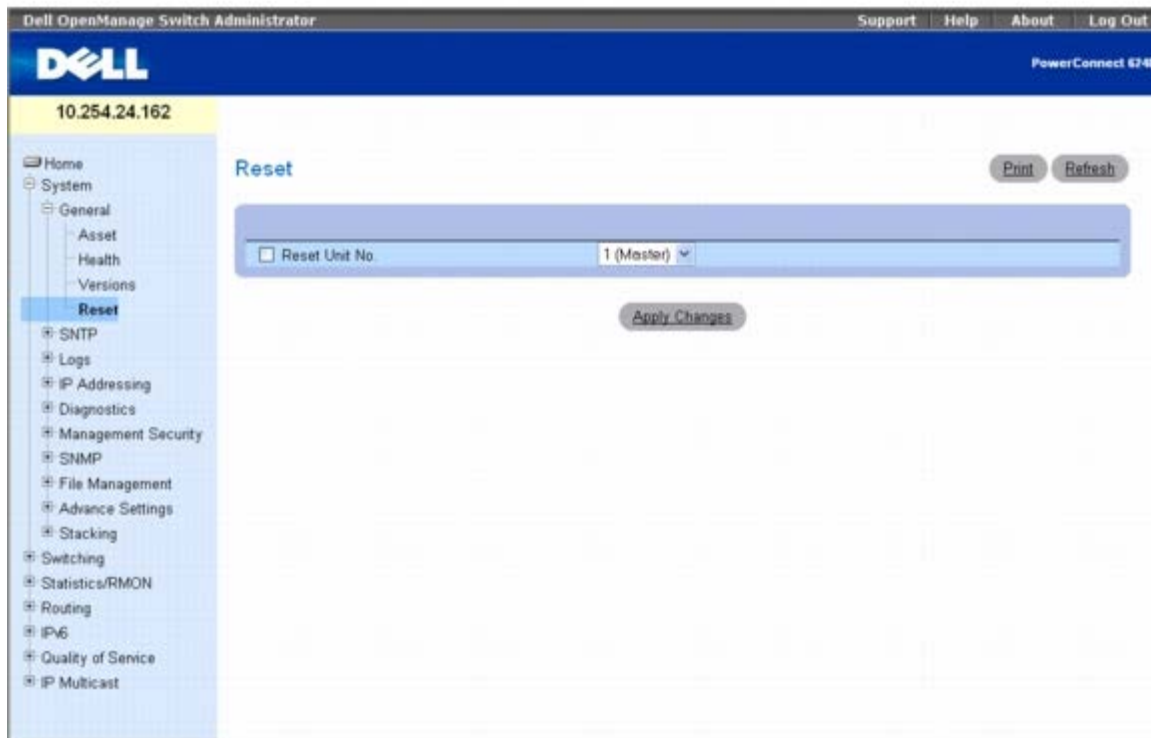
- 时钟命令

## 重置

**Reset** (重置) 页面用于重置设备。

要显示 **Reset** (重置) 页面，请在树视图中单击 **System** (系统) ® **General** (一般) ® **Reset** (重置)。

图 6-8. 重置



**Reset** (重置) 页面包含以下字段：

**Reset Unit No.** (重置单元编号) — 用于选择堆栈中要重置的设备。

## 重置设备

- 打开 **Reset** (重置) 页面。
- 单击 **Reset Unit No.** (重置单元编号)。
- 选择 **Individual Unit** (单个单元) 或 **All** (全部)。
- 单击 **Apply Changes** (应用更改) 按钮。
- 当显示确认信息时，单击 **OK** (确定)。

所选设备将重置。设备重置后，输入用户名和密码。

## 配置 SNTP 设置

本设备支持简单网络时间协议 (SNTP)。SNTP 确保网络设备时钟时间同步准确，最多可准确到毫秒。时间同步由网络 SNTP 服务器来执行。本设

备仅作为 **SNTP** 客户端运行，无法为其它系统提供时间服务。

时间源通过层来建立。层定义参考时钟的精度。层越高（最高为零），时钟越准确。本设备为 2 层设备，可从 1 层和更高层接收时间。

以下是层的示例：

- **0 层** — 实时时钟用作时间源，例如 *GPS* 系统。
- **1 层** — 使用直接链接至 0 层时间源的服务器。1 层时间服务器提供主要网络时间标准。
- **2 层** — 时间源在网络路径中远离 1 层。例如，2 层服务器通过网络链路并使用 *NTP* 从 1 层服务器接收时间。

系统将根据时间级别和服务器类型对从 **SNTP** 服务器接收到的信息进行评估。

通过以下时间级别来评定和确定 **SNTP** 时间定义：

- **T1** — 客户端发送原始请求的时间。
- **T2** — 服务器接收到原始请求的时间。
- **T3** — 服务器向客户端发送答复的时间。
- **T4** — 客户端接收到服务器答复的时间。

设备可以轮询服务器类型为单点传送和广播的服务器的服务器时间。

轮询单点传送信息用于轮询 IP 地址已知的服务器。为获取同步信息，设备仅轮询在设备上配置的 **SNTP** 服务器。T1 至 T4 用于确定服务器时间。这一方法由于最为安全，因而是最常用的设备时间同步方法。如果选择了此方法，设备仅接受来自 **SNTP Servers (SNTP 服务器)** 页面上为设备定义的 **SNTP** 服务器的 **SNTP** 信息。

服务器 IP 地址未知时，可以使用广播信息。**SNTP** 服务器发送广播信息时，**SNTP** 客户端侦听该信息。如果启用广播轮询，则即使设备未请求同步信息，也会接受该信息。这是最不安全的方法。

设备可主动请求信息或每经过一个轮询间隔检索一次同步信息。如果启用单点传送和广播轮询，信息检索的顺序为：

- 首先使用来自设备上定义的服务器的信息。如果没有启用单点传送轮询，或者设备上没有定义服务器，设备将接受任一响应的 **SNTP** 服务器的时间信息。
- 如果有多个单点传送设备作出响应，将优先使用具有较低层的设备的同步信息。
- 如果服务器具有相同的层，则接受首先响应的 **SNTP** 服务器的同步信息。

**MD5** (报文摘要 5) 验证可以维护到 **SNTP** 服务器的设备同步路径的安全。**MD5** 是一种生成 128 位散列的算法。**MD5** 是 **MD4** 的一种变体，它增强了 **MD4** 的安全性。**MD5** 验证通信的完整性并验证通信的起点。

**SNTP** 菜单页面包含指向可以配置 **SNTP** 参数的页面的链接。

要显示 **SNTP** 页面，请在树视图中单击 **System (系统) ® SNTP**。

此页面用于访问以下功能：

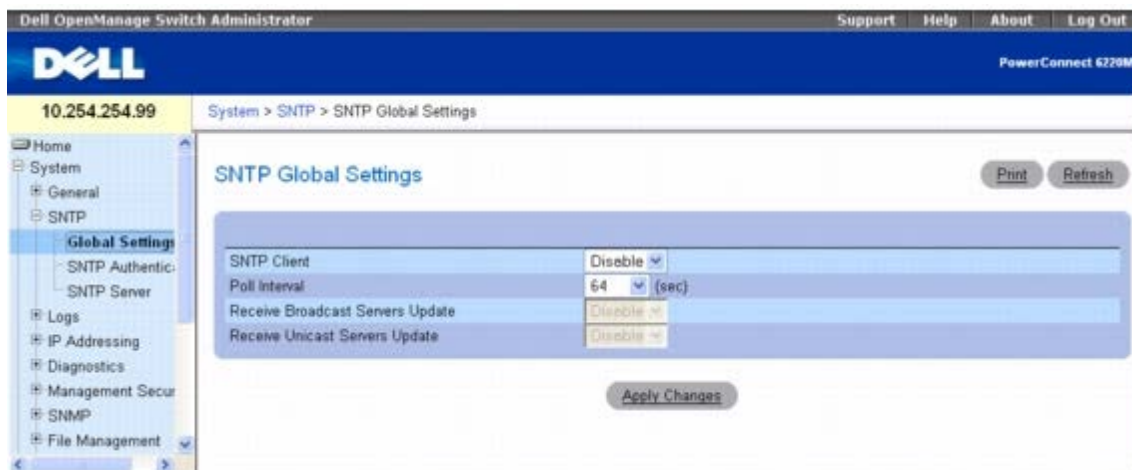
- [SNTP 全局设置](#)
- [SNTP 验证](#)
- [SNTP 服务器](#)

## SNTP 全局设置

*SNTP Global Settings (SNTP 全局设置)* 页面用于查看和调整 **SNTP** 参数。

要显示 *SNTP Global Settings (SNTP 全局设置)* 页面，请在树视图中单击 **System (系统) ® SNTP ® Global Settings (全局设置)**。

图 6-9. SNTP 全局设置



**SNTP Global Settings** (SNTP 全局设置) 页面包含以下字段：

**SNTP Client** (SNTP 客户端) — 使用下拉式列表启用或禁用客户端。当禁用了客户端时，也会禁用下面的某些字段。

**Poll Interval** (轮询间隔) — 定义轮询 SNTP 服务器以获得单点传送信息的时间间隔 (以秒为单位)。范围是 60 至 1024 秒。

**Receive Broadcast Servers Updates** (接收广播服务器更新) — 如果启用该选项，将在选定的接口上侦听 SNTP 服务器以获得广播服务器时间信息。只要接收到 SNTP 数据包，即使并未请求同步，都会同步该设备。

**Receive Unicast Servers Update** (接收单点传送服务器更新) — 如果启用该选项，将轮询在设备上定义的 SNTP 服务器以获得单点传送服务器时间信息。

## 定义 SNTP 全局参数

□□□ 打开 **SNTP Global Settings** (SNTP 全局设置) 页面。

□□□ 根据需要定义各个字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 SNTP 全局设置并更新设备。

## 使用 CLI 命令定义 SNTP 全局参数

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

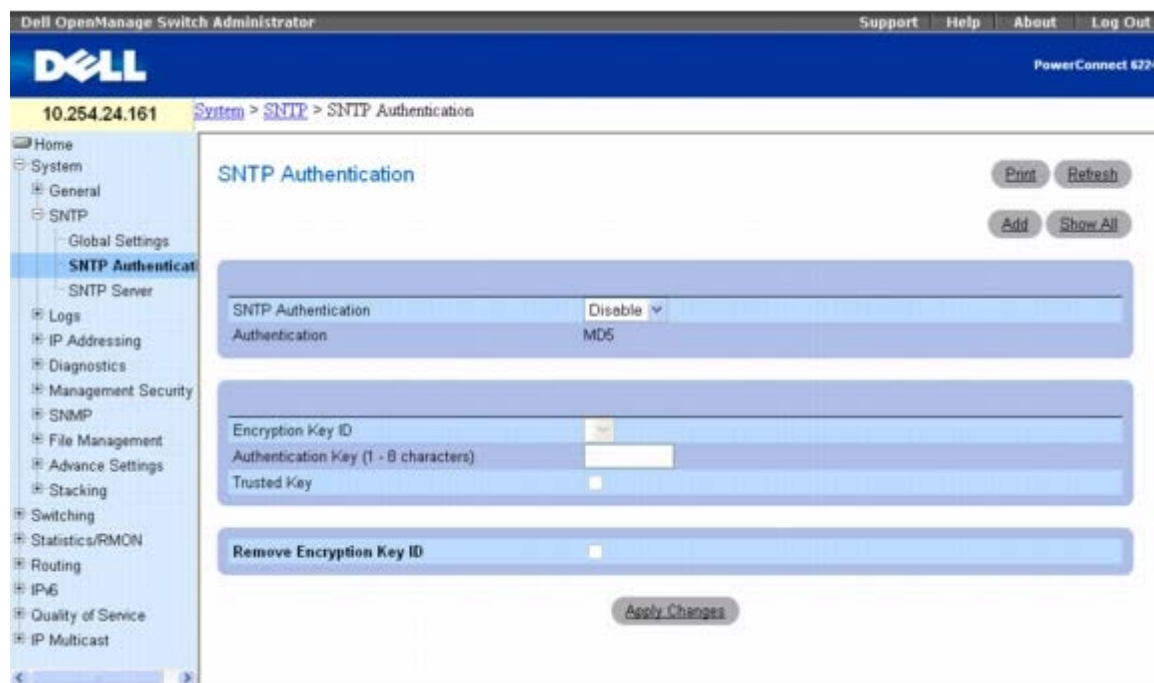
- 时钟命令。

## SNTP 验证

**SNTP Authentication** (SNTP 验证) 页面用于启用设备和 SNTP 服务器之间的 SNTP 验证，并选择所需的 SNTP 服务器。使用 **SNTP Authentication** (SNTP 验证) 页面可启用或禁用 SNTP 验证、修改所选加密密钥 ID 的验证密钥、将所选验证密钥指定为信任的密钥以及删除所选的加密密钥 ID。

在树视图中单击 **System** (系统) ® **SNTP** ® **Authentication** (验证) 以显示 **SNTP Authentication** (SNTP 验证) 页面。

图 6-10. SNTP 验证



**SNTP Authentication (SNTP 验证)** 页面包含以下字段：

**SNTP Authentication (SNTP 验证)** — 如果启用该选项，要求验证设备和 SNTP 服务器之间的 SNTP 会话。

**Authentication (验证)** — 验证的类型。系统仅支持 MD5。

**Encryption Key ID (加密密钥 ID)** — 含有用户定义的密钥 ID 列表，这些密钥 ID 用来验证 SNTP 服务器和设备。可能的字段值为 1 至 4294767295。

**Authentication Key (1–8 Characters) (验证密钥 [1 至 8 个字符])** — 显示验证时使用的密钥。

**Trusted Key (受信任的密钥)** — 选择以指定使用的加密密钥（单点传送），或取消选择以验证 SNTP 服务器（广播）。

**Remove Encryption Key ID (删除加密密钥 ID)** — 选择以删除所选的验证密钥。

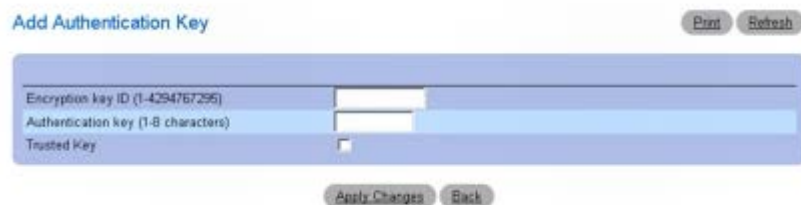
## 添加 SNTP 验证密钥

□□□ 打开 **SNTP Authentication (SNTP 验证)** 页面。

□□□ 单击 **Add** (添加)。

系统将显示 **Add Authentication Key** (添加验证密钥) 页面：

图 6-11. 添加验证密钥



□□□ 根据需要定义各个字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将添加 SNTP 验证密钥并更新设备。

## 显示验证密钥表

□□□ 打开 **SNTP Authentication** (**SNTP 验证**) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Authentication Key Table** (验证密钥表) 页面：

图 6-12. 验证密钥表

Encryption Key ID	Authentication Key	Trusted Key	Remove
4545	xsgdw	Yes	<input type="checkbox"/> Edit

## 删除验证密钥

□□□ 打开 **SNTP Authentication** (**SNTP 验证**) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Authentication Key Table** (验证密钥表) 页面。

□□□ 选择 **Authentication Key Table** (验证密钥表) 条目的 **Remove** (删除) 复选框。

□□□ 单击 **Apply Changes** (应用更改)。

系统将删除条目并更新设备。

## 使用 CLI 命令定义 SNTP 验证设置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 时钟命令。

## SNTP 服务器

**SNTP Server** (**SNTP 服务器**) 页面用于查看和修改用于启用 SNTP 服务器的信息以及添加新的 SNTP 服务器。

要显示 **SNTP Server** (**SNTP 服务器**) 页面，请在树视图中单击 **System** (系统) ® **SNTP** ® **SNTP Server** (**SNTP 服务器**)。

图 6-13. SNTP 服务器



**SNTP Servers (SNTP 服务器)** 页面包含以下字段：

**SNTP Server (SNTP 服务器)** — 从下拉式菜单中选择用户定义的 SNTP 服务器 IP 地址。通过使用 **Add (添加)** 按钮，可以最多添加八个 SNTP 服务器。

**Encryption Key ID (加密密钥 ID)** — 指定 SNTP 服务器和设备之间通信所使用的用户定义密钥 ID。加密密钥 ID 在 **SNTP Authentication (SNTP 验证)** 页面中定义。

**Priority (1–8) (优先级 [1-8])** — 指定向服务器发送 SNTP 请求时服务器条目的优先级。取值范围为 1 至 8，默认值为 1。将优先使用具有最低数值的服务器。

**Status (状态)** — 显示运行中的 SNTP 服务器的状态。可能的字段值包括：

**Up (运行)** — SNTP 服务器当前运行正常。

**Down (关闭)** — 表示 SNTP 服务器当前不可用。例如，SNTP 服务器当前未连接或已关机。

**In progress (进行中)** — SNTP 服务器当前正在发送或接收 SNTP 信息。

**Unknown (未知)** — 当前正在发送的 SNTP 信息的进程为未知。例如，设备当前正在寻找接口。

**Last Response (上一响应)** — 显示上一次接收到 SNTP 服务器响应的的时间。

**Remove SNTP Server (删除 SNTP 服务器)** — 如果选择该选项，将从 **SNTP Servers (SNTP 服务器)** 列表中删除指定的 SNTP 服务器。

## 添加 SNTP 服务器

□□□ 打开 **SNTP Servers (SNTP 服务器)** 页面。

□□□ 单击 **Add (添加)** 。

系统将显示 **Add SNTP Server (添加 SNTP 服务器)** 页面。

图 6-14. 添加 SNTP 服务器

□□□ 根据需要定义各个字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将添加 SNTP 服务器并更新设备。

## 显示 SNTP 服务器表

□□□ 打开 **SNTP Servers**（SNTP 服务器）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **SNTP Servers Table**（SNTP 服务器表）页面。

图 6-15. SNTP 服务器表

## 修改 SNTP 服务器

□□□ 打开 **SNTP Servers**（SNTP 服务器）页面。

□□□ 单击 **Show All**（全部显示）。

系统将打开 **SNTP Servers Table**（SNTP 服务器表）。

□□□ 单击要修改的 **SNTP Server**（SNTP 服务器）条目旁边的 **Edit**（编辑）。

□□□ 修改相关的字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将更新 SNTP 服务器信息。

## 删除 SNTP 服务器

□□□ 打开 **SNTP Servers**（SNTP 服务器）页面。

□□□ 单击 **Show All**（全部显示）。

### SNTP Servers Table SNTP



系统将打开 ( 服务器表)。

□□□ 选择一个 **SNTP Server** (SNTP 服务器) 条目。

□□□ 选中 **Remove** (删除) 复选框。

□□□ 单击 **Apply Changes** (应用更改)。

系统将删除条目并更新设备。

## 使用 CLI 命令定义 SNTP 服务器

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 时钟命令。

---

## 管理日志

交换机在响应事件和错误时，或者如果在平台、配置或其它方面产生了错误，交换机都会生成信息。这些信息将存储于本地平台上，同时转发到为监控而设的一个或多个中央收集点以及长期性存档装置。本地和远程记录功能配置包括根据信息严重性和生成信息的组件，对记录或转发的信息进行筛选。

内存中的日志根据信息组件和严重性设置在内存中存储信息。在堆栈式系统中，该日志仅存在于堆栈平台的顶层。堆栈中的其它平台则将信息转发至堆栈顶层的日志。而不能对非堆栈顶层平台的内存中的日志进行存取。

永久性日志存储于永久性存储设备中。可以配置两种类型的永久性日志。

- 第一种日志类型是系统启动日志。系统启动日志存储了系统重新引导后的前 N 条信息。该日志的日志已满操作属性始终设为满时停止，并可最多存储 32 条信息。
- 第二种日志类型是系统操作日志。系统操作日志存储了系统操作期间的最后 N 条信息。该日志的日志已满操作属性始终设为覆盖。此日志最多可以存储 1000 条信息。

日志子系统收到符合存储标准的信息后，会将该信息存储于系统启动日志或系统操作日志中，但不会同时存储于两者中。换言之，系统启动时，如果配置了启动日志，信息将存储于启动日志中，直至达到其容量限制。然后，如果配置了操作日志，则其它信息将开始使用操作日志进行存储。

系统最多会保留三个版本的永久性日志，它们分别名为 <FILE>0.txt、<FILE>1.txt 和 <FILE>2.txt。系统启动时，<FILE>2.txt 会被删除，<FILE>1.txt 将重命名为 <FILE>2.txt、<FILE>0.txt 将重命名为 <FILE>1.txt，同时创建 <FILE>0.txt，并开始在 <FILE>0.txt 中存储日志。（对于操作日志，上例中的 <FILE> 应替换为 olog，对于启动日志，则替换为 slog。）

本地永久性日志可以通过 CLI、与本地串行电缆连接的 xmodem 和 TFTP 检索。

要显示 **Logs** (日志) 菜单页面，请在树视图中单击 **System** (系统) ® **Logs** (日志)。此页面用于访问以下功能：

- [全局设置](#)
- [RAM 日志表](#)
- [日志文件](#)
- [远程日志服务器设置](#)

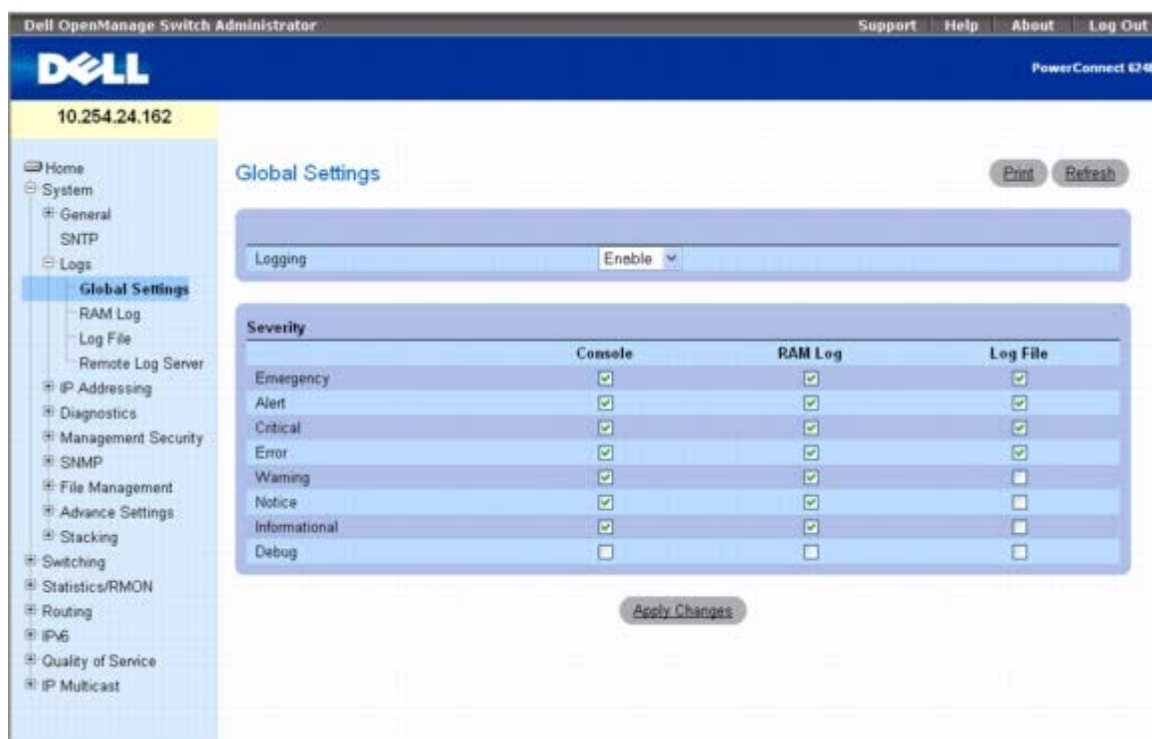
## 全局设置

**Global Settings** (全局设置) 页面用于启动全局日志并定义日志参数。**Severity** (严重性) 日志信息按照严重性从高到低的顺序列出。

要显示 **Global Settings** (全局设置) 页面，请在树视图中单击 **System** (系统) ® **Logs** (日志) ® **Global Settings** (全局设置)。



图 6-16. 全局设置



**Global Settings** (全局设置) 页面包含以下字段：

**Logging** (记录) — 为高速缓存、文件和服务器日志启用设备全局日志。所有打印至控制台的日志都保存于日志文件中。可能的字段值包括：

**Enable** (启用) — 允许在高速缓存 (RAM)、文件 (快擦写存储器) 和外部服务器中保存日志。

**Disable** (禁用) — 禁止保存日志。无法禁止记录打印至控制台的日志。

## Severity (严重性)

使用此区域中的复选框调整控制台、永久性内存和日志文件的严重性。

选择某个级别后，在此级别以上的级别都将自动选中。例如，如果选择“Error (错误)”，系统将自动选中“Error (错误)”、“Critical (严重)”、“Alert (警报)”和“Emergency (紧急)”。如果取消选择“Error (错误)”，则所有其下的级别，例如“Error (错误)”、“Warning (警告)”、“Notice (通告)”、“Informational (信息)”、“Debug (调试)”等都没有选中。

**Emergency** (紧急) — 最高的警告级别。如果设备停机或运行不正常，将在设备上保存紧急日志。

**Alert** (警报) — 第二级别的警告。如果设备出现严重故障，将保存警报日志；例如，如果所有设备功能停止运行。

**Critical** (严重) — 第三级别的警告。如果设备出现严重故障，将保存严重日志；例如，其中两个设备端口无法运行，而其余设备端口可以运行。

**Error** (错误) — 发生了设备错误，例如某个端口脱机。

**Warning** (警告) — 最低级别的设备警告。

**Notice** (通告) — 为网络管理员提供设备信息。

**Informational** (信息) — 提供设备信息。

**Debug** (调试) — 提供有关日志的详细信息。调试仅应由具有资格的支持人员输入。

复选框显示于以下三栏中：

**Console** (控制台) — 发送至控制台的日志。

**RAM Logs** (RAM 日志) — 发送至 (高速缓存) RAM 的日志。


**Log File**（日志文件）— 发送至文件（快擦写存储器）的日志。

## 启用日志

□□□ 打开 **Global Settings**（全局设置）页面。

□□□ 在 **Logging**（记录）下拉式菜单中选择 **Enable**（启用）。

□□□ 使用复选框选择日志类型和严重性。

 **注：**如果您选择一个严重性级别，则所有更高的严重性级别都将自动选中。

□□□ 单击 **Apply Changes**（应用更改）。

系统将保存日志设置并更新设备。

## 通过 CLI 启用全局日志

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

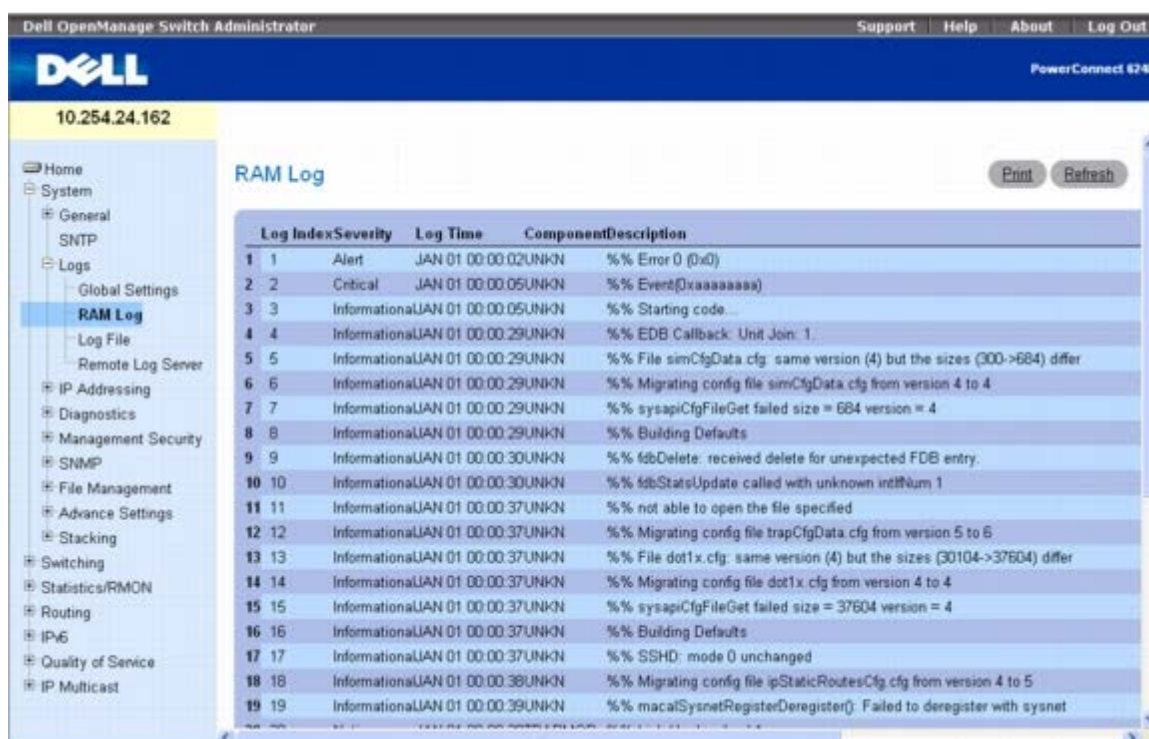
- 系统日志命令。

## RAM 日志表

**RAM Log Table**（RAM 日志表）页面用于查看有关特定 RAM（高速缓存）日志条目的信息，包括日志输入时间、日志严重性以及日志说明。

要显示 **RAM Log Table**（RAM 日志表），请在树视图中单击 **System**（系统）® **Logs**（日志）® **RAM Log**（RAM 日志）。

图 6-17. RAM 日志表



Log Index	Severity	Log Time	Component	Description
1	Alert	JAN 01 00:00:02	UNKN	%% Error 0 (0x0)
2	Critical	JAN 01 00:00:05	UNKN	%% Event[0xaaaaaaaa]
3	Informational	UN 01 00:00:05	UNKN	%% Starting code...
4	Informational	UN 01 00:00:29	UNKN	%% EDB Callback: Unit Join: 1
5	Informational	UN 01 00:00:29	UNKN	%% File simCfgData.cfg: same version (4) but the sizes (300->684) differ
6	Informational	UN 01 00:00:29	UNKN	%% Migrating config file simCfgData.cfg from version 4 to 4
7	Informational	UN 01 00:00:29	UNKN	%% sysapiCfgFileGet failed size = 684 version = 4
8	Informational	UN 01 00:00:29	UNKN	%% Building Defaults
9	Informational	UN 01 00:00:30	UNKN	%% %bDelete: received delete for unexpected FDB entry.
10	Informational	UN 01 00:00:30	UNKN	%% %bStatsUpdate called with unknown int#num 1
11	Informational	UN 01 00:00:37	UNKN	%% not able to open the file specified
12	Informational	UN 01 00:00:37	UNKN	%% Migrating config file trapCfgData.cfg from version 5 to 6
13	Informational	UN 01 00:00:37	UNKN	%% File dot1x.cfg: same version (4) but the sizes (30104->37604) differ
14	Informational	UN 01 00:00:37	UNKN	%% Migrating config file dot1x.cfg from version 4 to 4
15	Informational	UN 01 00:00:37	UNKN	%% sysapiCfgFileGet failed size = 37604 version = 4
16	Informational	UN 01 00:00:37	UNKN	%% Building Defaults
17	Informational	UN 01 00:00:37	UNKN	%% SSHD: mode 0 unchanged
18	Informational	UN 01 00:00:39	UNKN	%% Migrating config file ipStaticRoutesCfg.cfg from version 4 to 5
19	Informational	UN 01 00:00:39	UNKN	%% maca(SysnetRegisterDeregister): Failed to deregister with sysnet

**RAM Log Table** (RAM 日志表) 包含以下字段：

**Log Index** (日志索引) — 表示 RAM 日志表内的日志编号。

**Severity** (严重性) — 日志严重性。

**Log Time** (日志时间) — 日志输入到 RAM 日志表时的时间。

**Component** (组件) — 记录的组件。

**Description** (说明) — 日志说明。

## 删除日志信息

□□□ 打开 **RAM Log Table** (RAM 日志表) 页面。

□□□ 单击 **Clear Log** (清除日志)。

系统将从日志文件表中删除日志信息并更新设备模块。

## 使用 CLI 删除日志信息

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

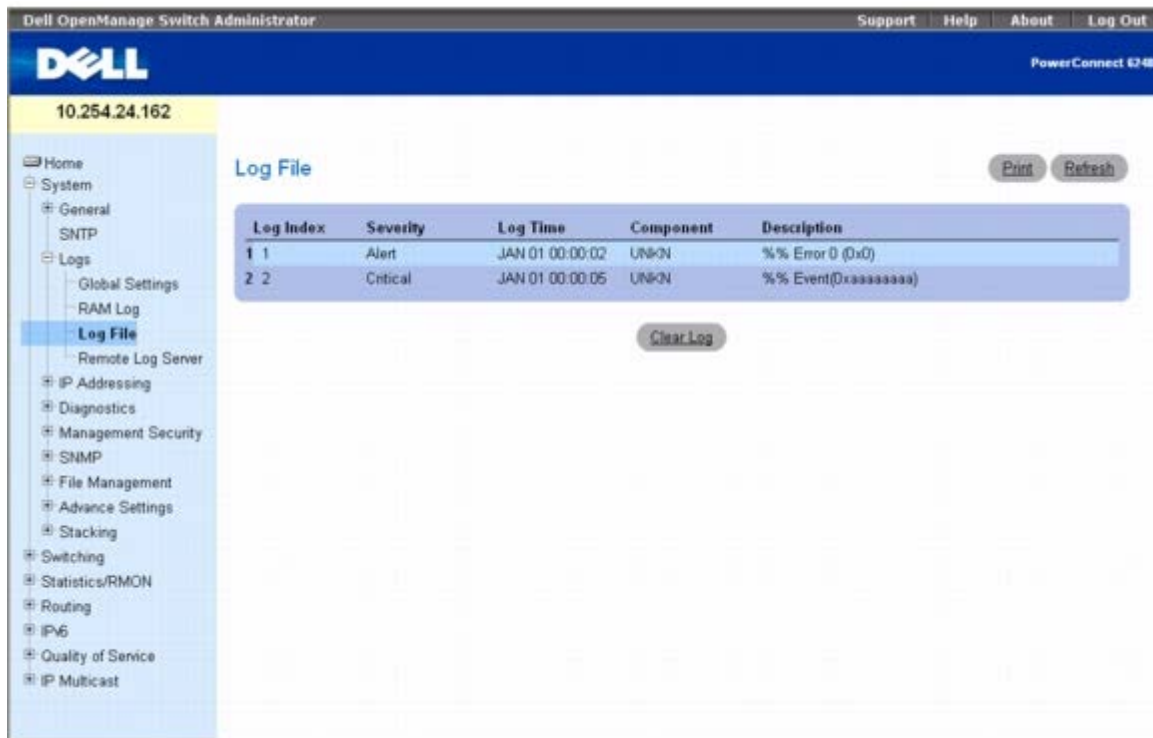
- 系统日志命令。

## 日志文件

**Log File** (日志文件) 包含有关特定日志条目的信息，包括日志输入时间、日志严重性以及日志说明。

要显示 **Log File** (日志文件)，请在树视图中单击 **System** (系统) ® **Logs** (日志) ® **Log File** (日志文件)。

图 6-18. 日志文件



**Log File Table** (日志文件表) 页面包含以下字段：

- **Log Index** (日志索引) — **Log File Table** (日志文件表) 中的日志编号。
- **Severity** (严重性) — 日志严重性。
- **Log Time** (日志时间) — 日志输入到 **Log File Table** (日志文件表) 时的时间。
- **Component** (组件) — 记录的组件。
- **Description** (说明) — 日志说明。

## 删除日志信息

□□□ 打开 **Log File Table** (日志文件表) 页面。

□□□ 单击 **Clear Log** (清除日志) 。

系统将从日志文件中删除日志信息并更新设备模块。

## 使用 CLI 删除日志信息

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

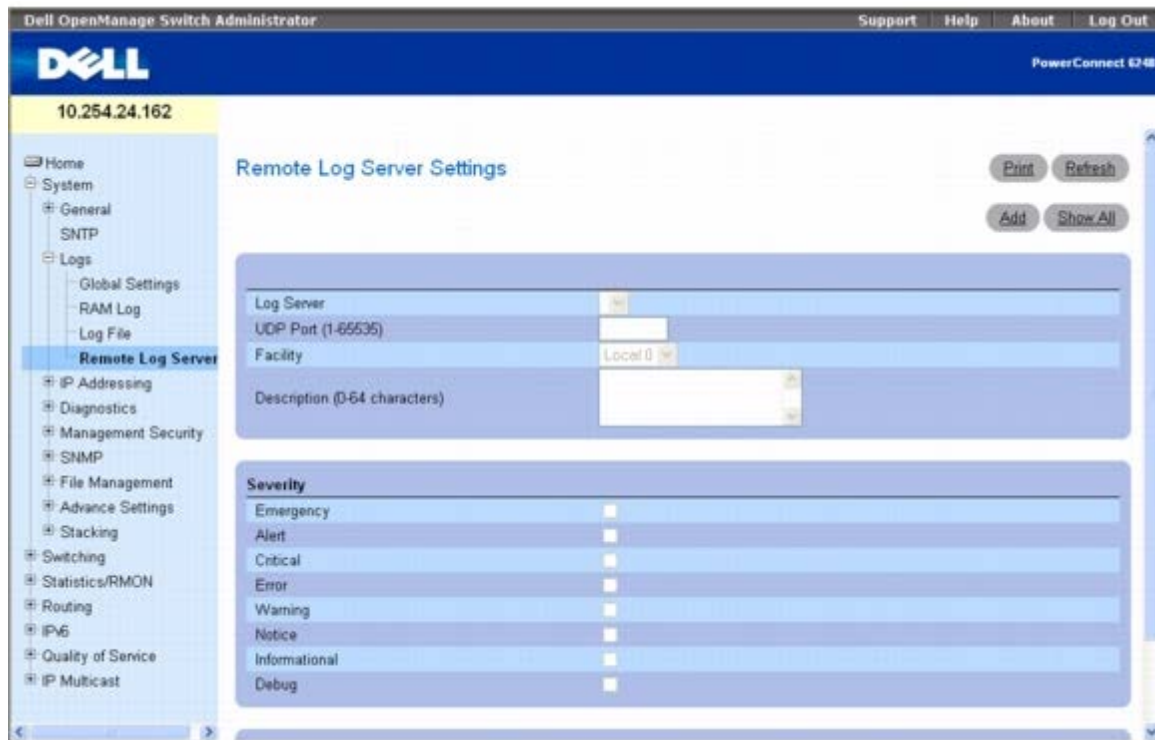
- 系统日志命令。

## 远程日志服务器设置

**Remote Log Server Settings** (远程日志服务器设置) 页面用于查看可用的日志服务器、定义新的日志服务器以及设置发送至服务器的日志事件的严重性。

要显示 **Remote Log Server Settings**（远程日志服务器设置）页面，请单击 **System**（系统）® **Logs**（日志）® **Remote Log Server**（远程日志服务器）。

图 6-19. 远程日志服务器设置



**Remote Logs Server Settings**（远程日志服务器设置）页面包含以下字段：

**Log Server**（日志服务器）— 可以将日志发送到的服务器。

**UDP Port (1-65535)**（UDP 端口 [1-65535]）— 设置发送日志的 UDP 端口。默认值为 514。

**Facility**（设备）— 用于向远程服务器发送系统日志的用户定义的应用程序。只能为一个服务器分配一个设备。如果分配了第二个设备，则第一个设备将被代替。为机器定义的所有应用程序在服务器上都使用同一设备。可能的字段值为 **Local 0** 至 **Local 7**。

**Description**（说明）— 设置服务器说明。最大长度为 64 个字符。

**Severity**（严重性）— 选择日志严重性。选择严重性级别后，所有更高的级别都将自动选中。

**Remove Log Server**（删除日志服务器）— 从 **Log Server**（日志服务器）列表中删除某个服务器。选择复选框可将服务器从列表中删除。将复选框留空则会在服务器列表中保留该服务器。


**Remote Log Server Settings**（远程日志服务器设置）页面还包含严重性列表。其中的严重性定义与 **RAM Log Table**（RAM 日志表）页面中的严重性定义相同。

## 将日志发送至服务器

□□□ 打开 **Remote Log Server Settings**（远程日志服务器设置）页面。

□□□ 定义 **UDP Port**（UDP 端口）、**Facility**（设备）和 **Description**（说明）字段。

□□□ 在 **Log Parameters**（日志参数）复选框中选择日志类型和日志严重性。

 **注：**如果您选择一个严重性级别，则所有更高的严重性级别都将自动选中。

□□□ 单击 **Apply Changes**（应用更改）。

系统将保存日志设置并更新设备。

## 添加新服务器

□□□ 打开 **Remote Log Server Settings**（远程日志服务器设置）页面。

□□□ 单击 **Add**（添加）以显示 **Add Remote Log Server**（添加远程日志服务器）页面。


 **注：**在添加新的服务器之前，需要先确定远程日志服务器的 IP 地址。

图 6-20. 添加远程日志服务器设置



□□□ 填写对话框中的字段并单击 **Apply Changes**（应用更改）。

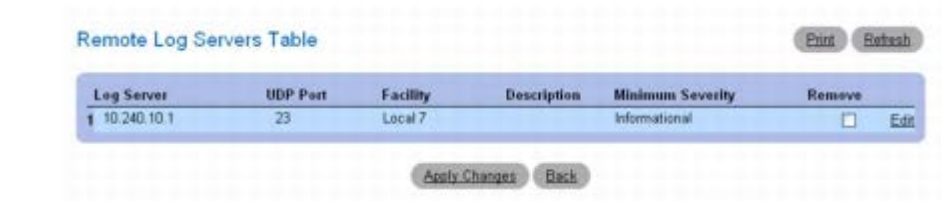
只有当返回到 **Remote Log Server Settings**（远程日志服务器设置）页面后，**Remote Log Server Settings**（远程日志服务器设置）页面才会在 **Log Server**（日志服务器）列表中显示服务器。

## 查看/删除日志服务器

□□□ 打开 **Remote Log Server Settings**（远程日志服务器设置）页面。

□□□ 单击 **Show All**（全部显示）以显示 **Remote Log Servers Table**（远程日志服务器表）页面。

图 6-21. 显示所有日志服务器



Log Server	UDP Port	Facility	Description	Minimum Severity	Remove
10.240.10.1	23	Local 7		Informational	<input type="checkbox"/> <a href="#">Edit</a>

□□□ 要删除服务器，请选择相应的 **Remove**（删除）复选框。

□□□ 单击 **Apply Changes**（应用更改）。

系统将删除服务器并更新设备。

## 使用 CLI 命令处理远程服务器日志

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 系统日志命令。

---

## 定义 IP 寻址

**IP Addressing (IP 寻址)** 页面用于分配管理接口和默认网关 IP 地址、与域名系统协商、设置默认域名、执行主机名称映射以及定义 ARP 和 DHCP 参数。

要显示 **IP Addressing (IP 寻址)** 页面，请在树视图中单击 **System (系统) ® IP Addressing (IP 寻址)**。此页面用于访问以下功能：

- [管理接口](#)
- [域名服务器 \(DNS\)](#)
- [默认域名](#)
- [主机名映射](#)
- [ARP 表](#)
- UDP 中继

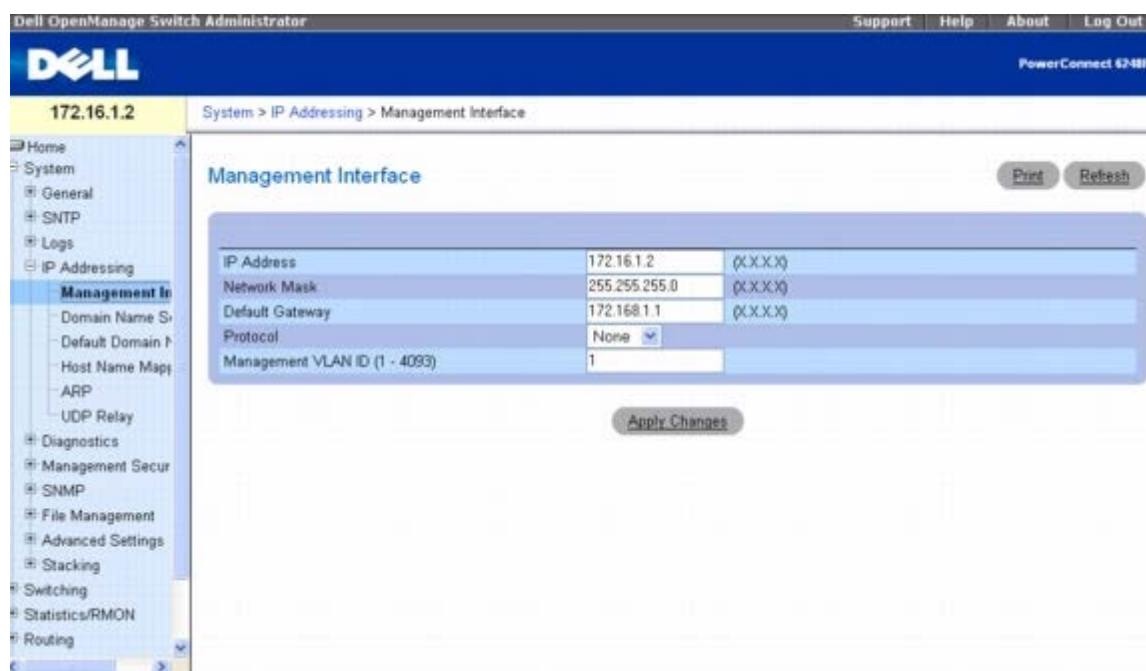
## 管理接口

**Management Interface (管理接口)** 菜单页面用于分配管理接口 IP 地址、子网掩码、默认网关 IP 地址以及启用或禁用引导协议。

要显示 **Management Interface (管理接口)** 页面，请在树视图中单击 **System (系统) ® IP Addressing (IP 寻址) ® Management Interface (管理接口)**。

图 6-22. 管理接口






管理接口

**Management Interface**（管理接口）页面包含以下字段：

**IP Address**（IP 地址）— 显示管理接口的 IP 地址。

**Network Mask**（网络掩码）— 源 IP 地址的子网掩码。

 **注：** IP 地址的每一部分都必须以非零开头。例如，001.100.192.6 和 192.001.10.3 为无效的 IP 地址。

**Default Gateway**（默认网关）— 设置默认网关 IP 地址。

**Protocol**（协议）— 使用下拉式菜单选择 Bootp、DCHP 或 None（无）。

**Management VLAN ID (1–4093)**（管理 VLAN ID [1-4093]）— 在 1 至 4093 范围内设置管理 VLAN ID。

 **注意：** 更改管理 VLAN 会断开您的 Web 会话。

## 修改管理接口 IP 地址参数

□□□ 打开 **Management Interface**（管理接口）页面。

□□□ 在 **IP Address**（IP 地址）字段中修改 IP 地址。

□□□ 修改其它字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将修改参数并更新设备。

## 使用 CLI 命令定义 IP 接口参数

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- IP 路由命令。



## 域名服务器 (DNS)

域名系统用于将用户定义的域名转换为 IP 地址。每次分配域名后，此服务都会将该名称转换为数字 IP 地址。例如，将 **www.ipexample.com** 转换为 192.87.56.2。域名系统服务器维护域名数据库及其对应的 IP 地址。

**Domain Name Server (DNS) (域名服务器 [DNS])** 页面用于启用和激活特定 DNS 服务器。

要显示 **Domain Name Server (域名服务器)** 页面，请在树视图中单击 **System (系统)** ® **IP Addressing (寻址)** ® **Domain Name Server (域名服务器)**。

图 6-23. 域名服务器



**Domain Name Server (DNS) (域名服务器 [DNS])** 页面包含以下字段：

**DNS Status (DNS 状态)** — 允许或禁止将 DNS 名称转换为 IP 地址。

**DNS Server (DNS 服务器)** — 包含 DNS 服务器的列表。DNS 服务器在 **Add DNS Server (添加 DNS 服务器)** 页面中添加。

**Remove (删除)** — 如果选择该选项，将删除所选 DNS 服务器。

### 添加 DNS 服务器

□□□ 打开 **Domain Name Server (DNS) (域名服务器 [DNS])** 页面。

□□□ 单击 **Add (添加)**。

系统将显示 **Add DNS Server (添加 DNS 服务器)** 页面：

图 6-24. 添加 DNS 服务器



□□□ 定义相关的字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将定义新的 DNS 服务器并更新设备。

## 使用 CLI 命令配置 DNS 服务器

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

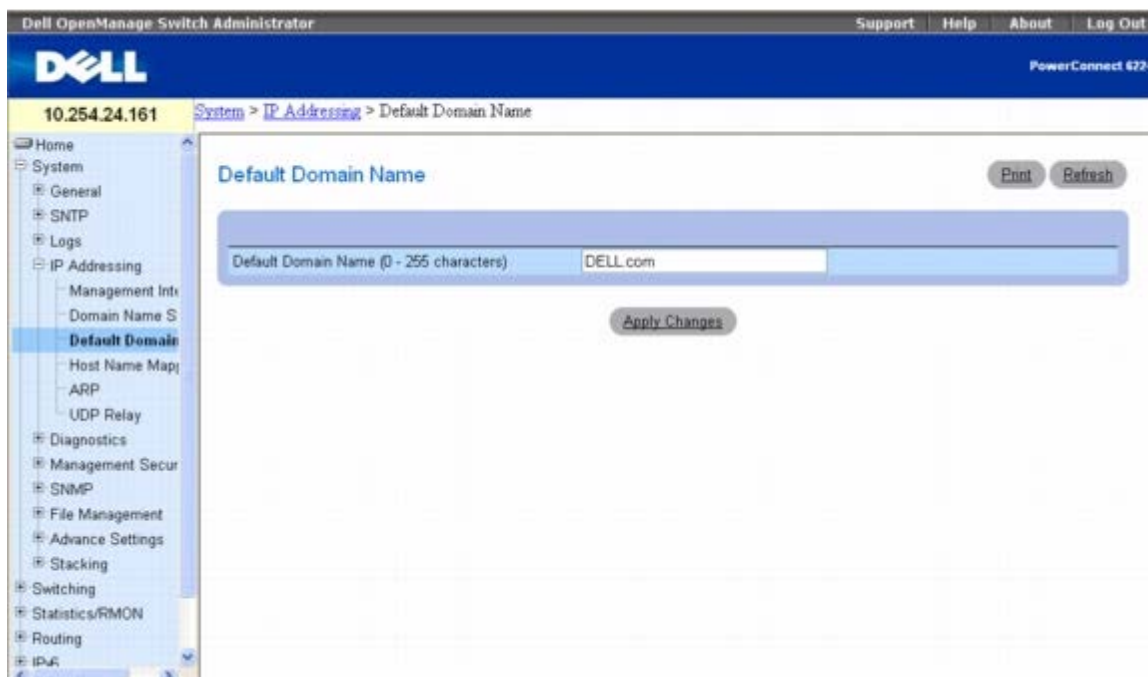
- IP 寻址命令。

## 默认域名

**Default Domain Name**（默认域名）页面用于查看和定义默认 DNS 域名。

要显示 **Default Domain Name**（默认域名）页面，请单击 **System**（系统）® **IP Addressing**（IP 寻址）® **Default Domain Name**（默认域名）。

图 6-25. 默认域名



**Default Domain Name**（默认域名）页面包含以下字段：

**Default Domain Name (0–255 characters)**（默认域名 [0 至 255 个字符]）— 包含用户定义的默认域名。配置后，默认域名将应用于所有未限定主机名。

## 使用 CLI 命令定义 DNS 域名

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

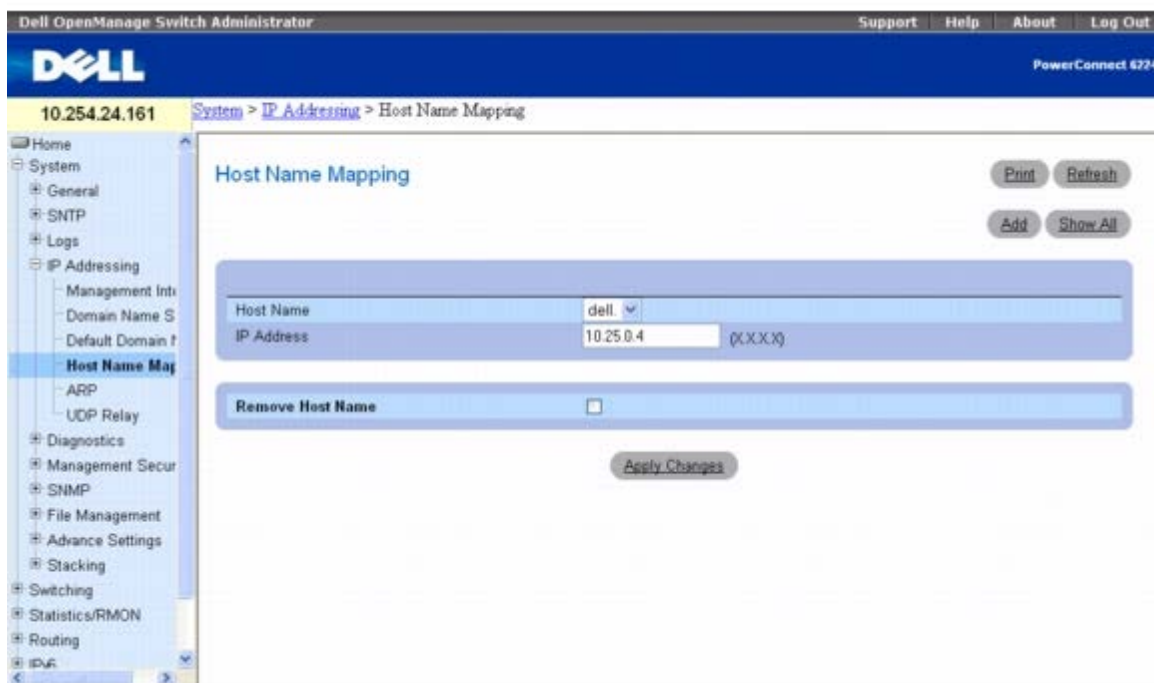
- IP 寻址命令。

## 主机名映射

**Host Name Mapping**（主机名映射）页面用于向静态主机名称分配 IP 地址。**Host Name Mapping**（主机名映射）页面可以为每个主机提供一个 IP 地址。

要显示 **Host Name Mapping**（主机名映射）页面，请单击 **System**（系统）® **IP Addressing**（IP 寻址）® **Host Name Mapping**（主机名映射）。

图 6-26. 主机名映射



**Host Name Mapping**（主机名映射）页面包含以下字段：

**Host Name**（主机名）— 包含主机名称列表。主机名在 **Add Static Host Name Mapping**（添加静态主机名映射）页面中定义。每个主机提供一个 IP 地址。

**IP Address**（IP 地址）— 提供分配给指定主机名的 IP 地址。

**Remove Host Name**（删除主机名）— 如果选中，将删除主机名映射。

## 添加主机域名

□□□ 打开 **Host Name Mapping**（主机名映射）页面。

□□□ 单击 **Add**（添加）。

系统将显示 **Add Static Host Name Mapping**（添加静态主机名映射）页面：

图 6-27. 添加静态主机名映射

□□□ 定义相关的字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将把 IP 地址映射到主机名并更新设备。

## 显示静态主机名映射表

□□□ 打开 **Host Name Mapping**（主机名映射）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **Static Hosts Name Mapping Table**（静态主机名映射表）：

图 6-28. 静态主机名映射表

Host Name	IP Address	Remove
dell	10.25.0.4	<input type="checkbox"/>

## 从 IP 地址映射中删除主机名

□□□ 打开 **Host Name Mapping**（主机名映射）页面。

□□□ 单击 **Show All**（全部显示）。

系统将打开 **Host Name Mapping Table**（主机名映射表）。

□□□ 选择一个 Host Name Mapping Table（主机名映射表）条目。

□□□ 选中 **Remove**（删除）复选框。

□□□ 单击 **Apply Changes**（应用更改）。

系统将删除主机名映射表条目并更新设备。

## 使用 CLI 命令将 IP 地址映射至域主机名

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

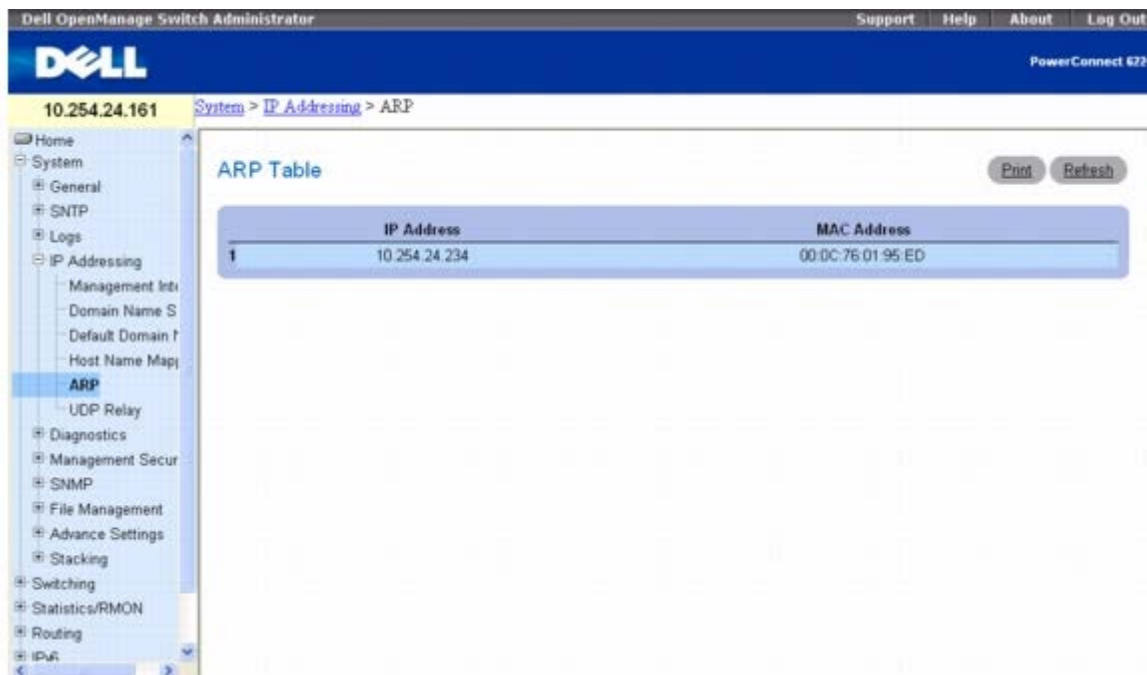
- IP 寻址命令。

## ARP 表

**ARP Table (ARP 表)** 页面用于查看 IP 接口的 ARP 参数。ARP 表显示了每个 MAC 地址及其对应的 IP 地址。

要显示 **ARP Table (ARP 表)** 页面，请在树视图中单击 **System (系统)** ® **IP Addressing (IP 寻址)** ® **ARP**。

图 6-29. ARP 表



**ARP Table (ARP 表)** 页面包含以下字段：

**IP Address (IP 地址)** — 站点 IP 地址，该地址与下面填写的 MAC 地址相关。

**MAC Address (MAC 地址)** — 站点 MAC 地址，在 ARP 表中该地址与 IP 地址相关。

## 使用 CLI 命令查看 ARP 表

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- IP 寻址命令。

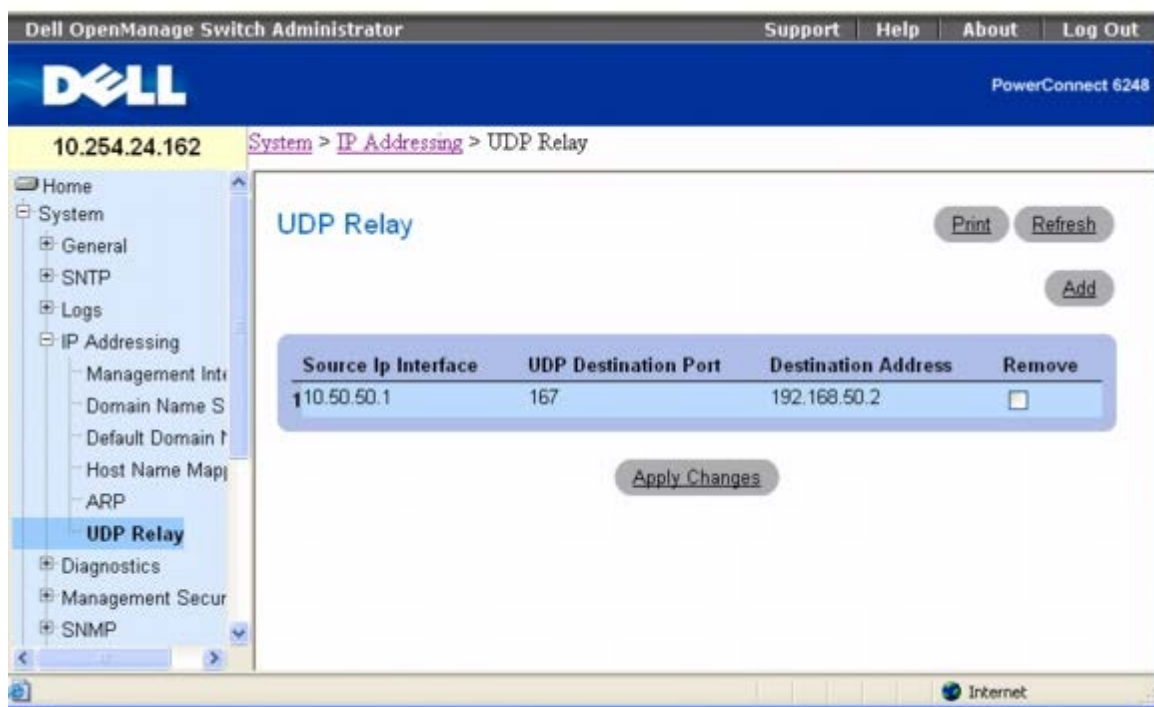
## UDP 中继

UDP 中继使设备可以将特定 UDP 广播从一个接口转发到另一个接口。通常，IP 广播信息包不可以从一个接口转发到另一个接口，但某些应用程序使用 UDP 广播以检测服务的可用性。其它服务则要求对 UDP 广播信息包进行路由，从而向子网中的其它客户端提供服务。UDP 中继还允许从工作站浏览到不同网络上的服务器。

**UDP Relay (UDP 中继)** 页面用于添加、显示或删除 UDP 中继配置。

要显示 **UDP Relay (UDP 中继)** 页面，请单击 **System (系统)** ® **IP Addressing (IP 寻址)** ® **UDP Relay (UDP 中继)**。

图 6-30. UDP 中继



**UDP Relay**（UDP 中继）页面包含以下字段：

**Source IP Interface**（源 IP 接口）— 中继 UDP 信息包的输入 IP 接口。如果字段为 255.255.255.255，则来自所有接口的 UDP 信息包都会被中继。以下地址范围无效：

0.0.0.0 至 0.255.255.255

127.0.0.0 至 127.255.255.255

**UDP Destination Port (1–65535)**（UDP 目的地端口 [1-65535]）— UDP 信息包的中继目的地 UDP 端口 ID 编号。下表列出了 UDP 端口分配。

UDP 端口号	缩写	应用程序
7	Echo	回显
11	SysStat	在线用户
<b>15</b>	NetStat	<b>NetStat</b>
17	Quote	当日引用
19	CHARGEN	字符发生器
20	FTP-data	FTP 数据
21	FTP	FTP
37	Time	时间
42	NAMESERVER	主机名服务器
43	NICNAME	人名
53	DOMAIN	域名服务器
69	TFTP	小型文件传输
111	SUNRPC	Sun Microsystems Rpc
123	NTP	网络时间
<b>137</b>	NetBiosNameService	NT 服务器与工作站的连接
<b>138</b>	NetBiosDatagramService	NT

服务器与工作站的连接		
139	NetBios	SessionServiceNT 服务器与工作站的连接
161	SNMP	简单网络管理
162	SNMP-trap	简单网络管理陷阱
513	who	Unix Rwho Daemon
514	syslog	系统日志
525	timed	Time Daemon

Destination Address (目的地地址) — 接收 UDP 信息包中继的 IP 接口。如果此字段为 0.0.0.0，将丢弃 UDP 信息包。如果字段为 255.255.255.255，则 UDP 信息包会被中继至所有接口。

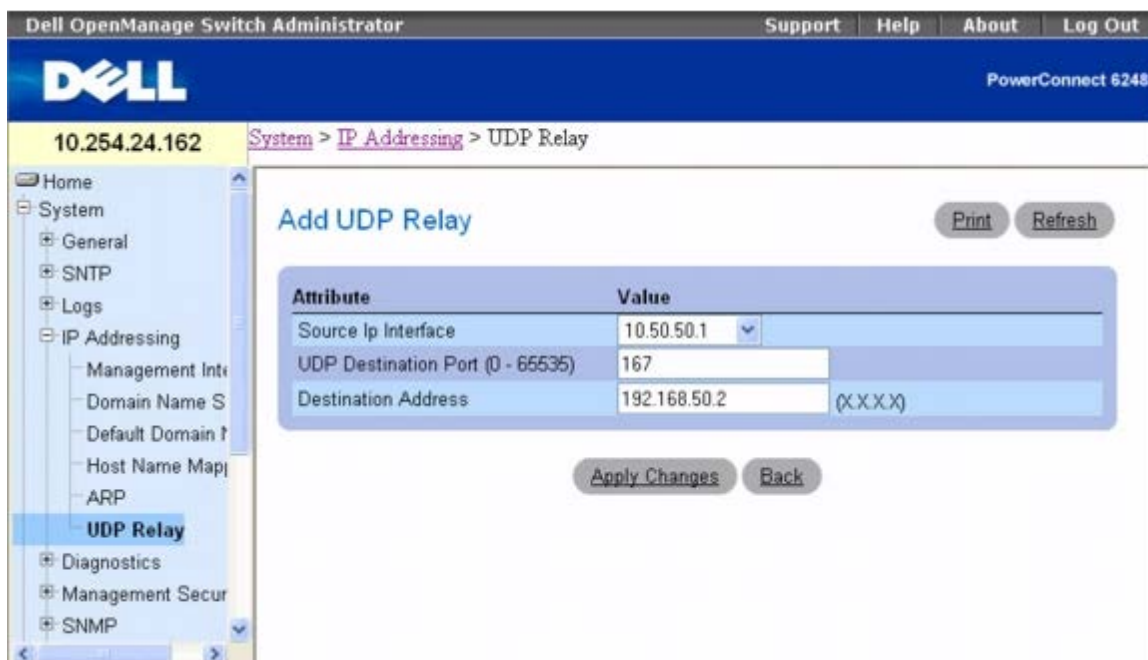
**Remove** (删除) — 选中此复选框将删除指定的 UDP 中继。

## 添加 UDP 中继条目

□□□ 打开 **UDP Relay** (UDP 中继) 页面。

□□□ 单击 **Add** (添加) 以显示 **Add UDP Relay** (添加 UDP 中继) 页面：

图 6-31. 添加 UDP 中继




□□□ 填写 **Source IP Interface** (源 IP 接口)、**UDP Destination Port** (UDP 目的地端口) 和 **Destination Address** (目的地地址) 字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将添加 UDP 中继并更新设备。

□□□ 单击 **Back** (上一步) 以返回到 **UDP Relay** (UDP 中继) 页面。

 **注：** 如果启用 UDP 中继而不指定 UDP 端口号，设备默认将 UDP 广播信息包转发至以下设备：IEN-116 Name Service (端口 42)、DNS (端口 53)、NetBIOS Name Server (端口 137)、NetBIOS Datagram Server (端口 138)、TACACS Server (端口 49) 和 Time Service (端口 37)。



## 删除 UDP 中继条目

- 打开 **UDP Relay** (UDP 中继) 页面。
- 选择要删除的条目旁边的 **Remove** (删除) 复选框。
- 单击 **Apply Changes** (应用更改)。

系统将删除 **UDP Relay** (UDP 中继) 条目并更新设备。

## 使用 CLI 配置 UDP 中继信息

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- IP 寻址命令。

---

## 运行电缆诊断程序

**Diagnostics** (诊断程序) 菜单页面用于执行铜质和光纤的虚拟电缆检测。

要显示 **Diagnostics** (诊断程序) 页面，请在树视图中单击 **System** (系统) ® **Diagnostics** (诊断程序)。

此页面用于访问以下功能：

- [用于铜质电缆的集成电缆检测](#)
- [光学收发器诊断程序](#)

## 用于铜质电缆的集成电缆检测

**Integrated Cable Test for Copper Cables** (用于铜质电缆的集成电缆检测) 页面用于对铜质电缆执行检测。电缆检测可以提供有关电缆何处发生故障、上一次执行电缆检测的时间以及发生的电缆故障的类型等信息。检测程序使用时域反射计 (TDR) 技术来检测连接至端口的铜质电缆的质量和特性。最多可以检测 120 米长的电缆。除近似电缆长度检测之外，通常在端口处于断开状态时检测电缆。

要显示 **Integrated Cable Test for Copper Cables** (用于铜质电缆的集成电缆检测) 页面，请在树视图中单击 **System** (系统) ® **Diagnostics** (诊断程序) ® **Integrated Cable Test** (集成电缆检测)。

图 6-32. 用于铜质电缆的集成电缆检测





**Integrated Cable Test for Copper Cables**（用于铜质电缆的集成电缆检测）页面包含以下字段：

**Interface**（接口）— 电缆连接的接口。

**Test Result**（检测结果）— 电缆检测结果。可能的值包括：

**No Cable**（无电缆）— 没有电缆连接至端口。

**Open Cable**（开放电缆）— 电缆断开。

**Short Cable**（短路电缆）— 电缆出现短路。

**OK**（正常）— 电缆通过检测。

**Fiber Cable**（光纤）— 光纤与端口相连。

**Cable Fault Distance**（电缆故障距离）— 电缆发生故障的位置与端口之间的距离。

**Last Update**（上次更新）— 上一次检测端口的时间。

**Cable Length**（电缆长度）— 近似的电缆长度。仅当端口处于连接状态并以 1 Gbps 的速率运行时才能执行该检测。

## 执行电缆检测

□□□ 请确保铜质电缆的两端均连接至设备。

□□□ 打开 **Integrated Cable Test for Copper Cables**（用于铜质电缆的集成电缆检测）页面。

□□□ 单击 **Run Test**（运行检测）。

系统将执行铜质电缆检测，并将结果显示在 **Integrated Cable Test for Copper Cables**（用于铜质电缆的集成电缆检测）页面中。

## 显示集成电缆检测结果表

□□□ 打开 **Integrated Cable Test for Copper Cables**（用于铜质电缆的集成电缆检测）页面。

□□□ 单击 **Show All**（全部显示）。

□□□ 请从下拉式菜单中选择所需的单元。

网页将显示 **Integrated Cable Test Results Table**（集成电缆检测结果表）页面，其中包含所选单元上的每个端口的上一次检测结果。

图 6-33. 集成电缆检测结果表



Interface	Test Result	Cable Fault Distance (m)	Last Update	Cable Length (m)
1/g1	Test has not been performed			
1/g2	Test has not been performed			
1/g3	Test has not been performed			
1/g4	Test has not been performed			
1/g5	Test has not been performed			
1/g6	Test has not been performed			
1/g7	Test has not been performed			
1/g8	Test has not been performed			
1/g9	Test has not been performed			
1/g10	Test has not been performed			
1/g11	Test has not been performed			

## 使用 CLI 命令执行铜质电缆检测

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- PHY 诊断程序命令。

## 光学收发器诊断程序

**Optical Transceiver Diagnostics**（光学收发器诊断程序）页面用于对光纤电缆执行检测。

要显示 **Optical Transceiver Diagnostics**（光学收发器诊断程序）页面，请在树视图中单击 **System**（系统）® **Diagnostics**（诊断程序）® **Optical Transceiver Diagnostics**（光学收发器诊断程序）。


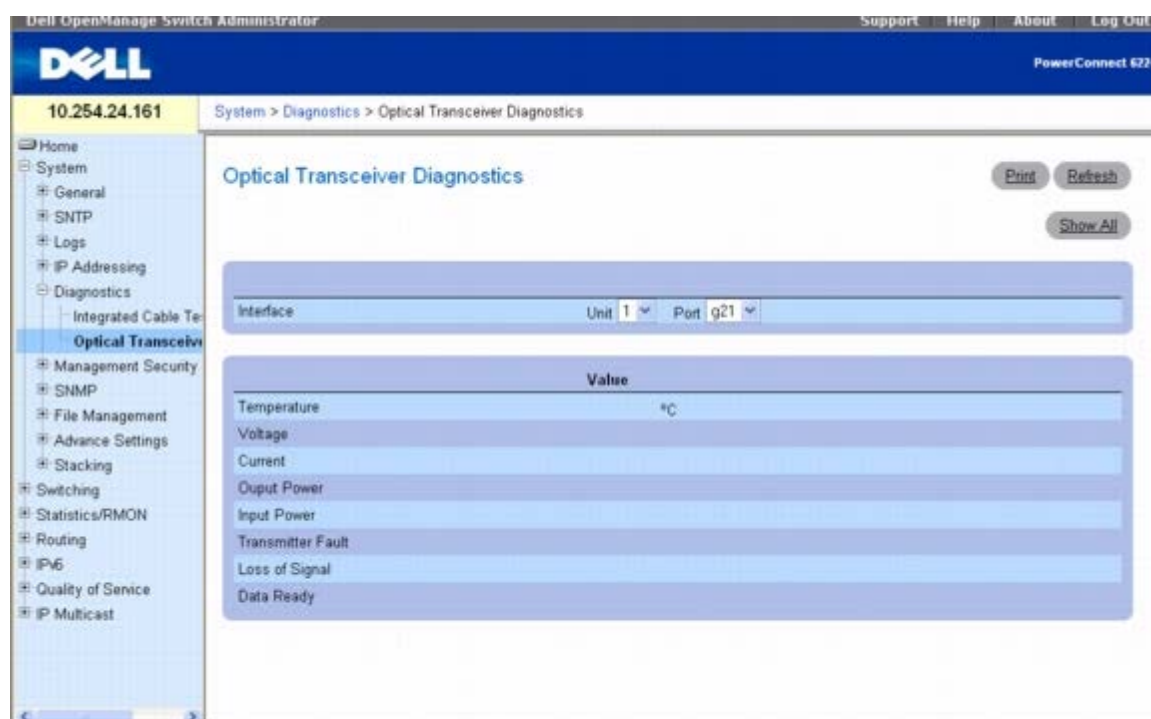
 **注：**只有存在连接，才能执行光学收发器诊断程序。

图 6-34. 光学收发器诊断程序



**Optical Transceiver Diagnostics**（光学收发器诊断程序）页面包含以下字段：

**Interface**（接口）— 检测电缆时使用的端口 IP 地址。

**Temperature**（温度）— 电缆工作温度（C）。

**Voltage**（电压）— 电缆工作电压。

**Current**（电流）— 电缆工作电流。

**Output Power**（输出功率）— 输出功率传输率。

**Input Power**（输入功率）— 输入功率传输率。

**Transmitter Fault**（传输故障）— 表示在传输过程中发生故障。

**Loss of Signal**（信号损失）— 电缆是否存在信号损失。

**Data Ready**（数据就绪）— 表示收发器是否成功加电并作好数据准备。



注：Finisar 收发器不支持传输故障诊断检测。光纤分析功能仅适用于支持 SFF-4872 数字诊断标准的 SFP。

## 显示光学收发器诊断程序检测结果表

□□□ 打开 **Optical Transceiver Diagnostics**（光学收发器诊断程序）页面。

□□□ 单击 **Show All**（全部显示）。

□□□ 请从下拉式菜单中选择所需的单元。

图 6-35. 光学收发器诊断程序表

Interface	Temperature (°C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	Transmitter Fault	Loss of Signal (dB)
1/g45							
1/g46							
1/g47							
1/g48							

检测运行后，将显示 **Optical Transceiver Diagnostics Table**（光学收发器诊断程序表）页面。

## 使用 CLI 命令执行光纤电缆检测

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- PHY 诊断程序命令。

## 管理设备安全保护

**Management Security**（管理安全保护）菜单页面用于为端口、用户和服务器安全保护设置管理安全保护参数。

要显示 **Management Security**（管理安全保护）页面，请在树视图中单击 **System**（系统）® **Management Security**（管理安全保护）。此页面用于访问以下功能：

- [访问配置文件](#)
- [验证配置文件](#)
- [选择验证](#)
- [密码管理](#)
- [本地用户数据库](#)
- [线路密码](#)
- [启用密码](#)
- [TACACS+ 设置](#)
- [RADIUS 设置](#)
- [Telnet 服务器](#)
- [拒绝服务](#)

## 访问配置文件

**Access Profile**（访问配置文件）页面用于定义存取设备的配置文件和规则。您可以限制对特定管理功能、特定入口接口、源 IP 地址或源 IP 子网的访问。

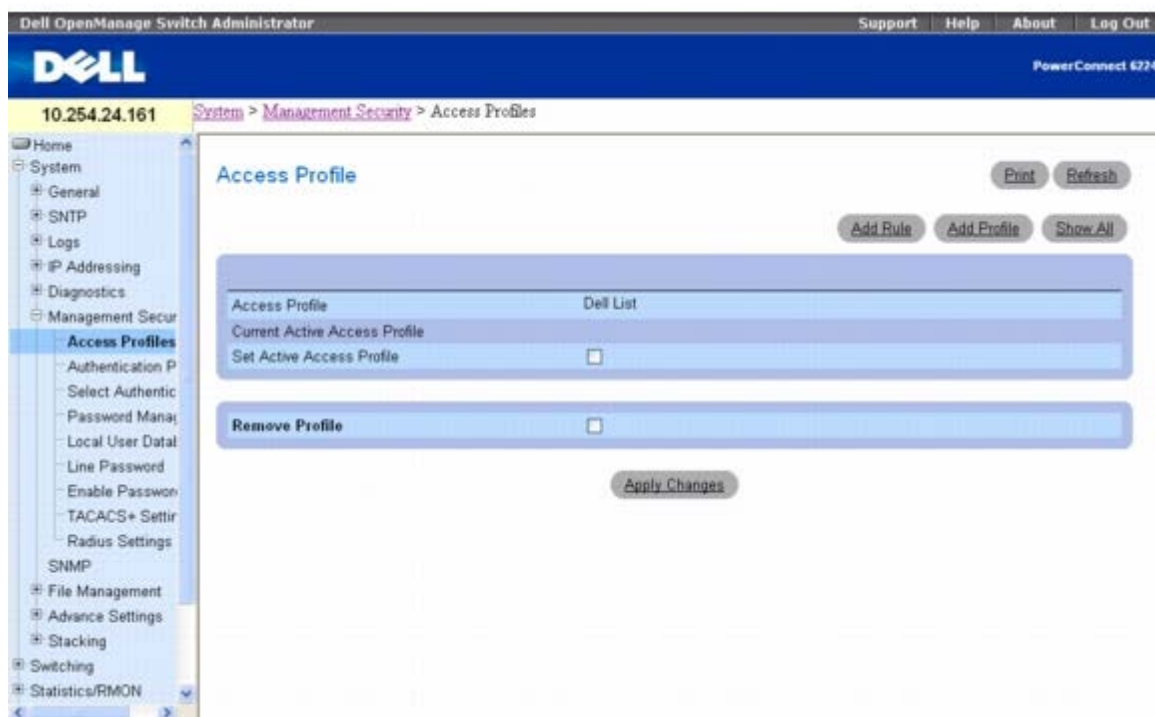
可以针对 Web (HTTP)、安全 Web (HTTPS)、Telnet、SSH 和 SNMP 等各种类型的管理访问方法分别定义管理访问。

管理访问列表包含用来确定哪些用户可以通过哪些方法管理设备的规则。此外，还可以用来禁止用户访问设备。

**Access Profile**（访问配置文件）页面用于配置管理列表以及将列表应用于特定接口。

要显示 **Access Profile**（访问配置文件）页面，请在树视图中单击 **System**（系统）® **Management Security**（管理安全保护）® **Access Profiles**（访问配置文件）。

图 6-36. 访问配置文件




**Access Profile**（访问配置文件）— 显示访问配置文件。

**Current Active Access Profile**（当前活动访问配置文件）— 当前处于活动状态的配置文件。

**Set Access Profile Active**（将访问配置文件设为激活）— 激活访问配置文件。

**Remove Profile**（删除配置文件）— 如果选择该选项，会从 **Access Profile**（访问配置文件）列表中删除访问配置文件。

 **注：** 将访问配置文件分配给一个接口后，将拒绝通过其它接口进行访问。如果没有激活任何访问配置文件，则无法访问设备。

## 显示访问配置文件

□□□ 打开 **Access Profiles**（访问配置文件）页面。

□□□ 单击 **Show All**（全部显示）以显示 **Profile Rules Table**（配置文件规则表）页面。

图 6-37. 配置文件规则表

Interface	Management Method	Source IP Address	Subnet Mask	Action	Priority	Remove	
1	1/g1	SNMP	132.25.39.115	255.255.255.255	PERMIT	1	<input type="checkbox"/> Edit
2	1/g12	SSH	192.168.22.15	255.255.255.255	PERMIT	3	<input type="checkbox"/> Edit

## 添加访问配置文件

□□□ 打开 **Access Profiles**（访问配置文件）页面。

□□□ 单击 **Add Profile**（添加配置文件）。

系统将显示 **Add an Access Profile**（添加访问配置文件）页面。

图 6-38. 添加访问配置文件

□□□ 在 **Access Profile Name**（访问配置文件名称）文本框中输入配置文件的名称。

□□□ 填写以下字段：

**Management Method**（管理方法）— 从下拉框中选择。策略受所选管理的限制。

**Interface**（接口）— 如果策略应含有根据接口而设置的规则，请选择此复选框。接口可以是物理接口、LAG 或 VLAN。

**Source IP Address**（源 IP 地址）— 如果策略应包含根据发送管理通信的客户端的 IP 地址设置的规则，请选择 **Source IP Address**（源 IP 地址）复选框。在提供的字段中填写详细的源 IP 地址和掩码。请注意，掩码可以以两种格式提供：带点的 IP 格式（例如 255.255.255.0）或前缀长度（例如 32）。

**Action**（动作）— 选择当符合上述所选规则时，应执行的动作。使用下拉框并选择“Permit（允许）”或“Deny（拒绝）”以允许或拒绝访问。

**Rule Priority**（规则优先级）— 配置规则优先级。规则将以优先级从小到大的顺序对接入管理请求进行验证。如果符合规则的条件，则执行动作并忽略其下的规则。例如，如果首先配置一条规则，其源 IP 为 10.10.10.10，优先级为 1，并设置为“允许”，然后配置另一条规则，其源 IP 为 10.10.10.10，优先级为 2，并设为“拒绝”，则激活配置文件后，将允许访问而忽略第二条规则。

□□□ 单击 **Apply Changes**（应用更改）。

系统将添加新的访问配置文件并更新设备。

## 激活访问配置文件

□□□ 打开 **Access Profiles**（访问配置文件）页面。

□□□ 选中 **Set Access Profile Active**（将访问配置文件设为激活）复选框。

□□□ 单击 **Apply Changes**（应用更改）。

设备的访问配置文件将启用。

## 将规则添加至访问配置文件

□□□ 打开 **Access Profiles**（访问配置文件）页面。

**Access Profile**（访问配置文件）字段显示了在 **Add An Access Profile Rule**（添加访问配置文件规则）页面中添加规则的配置文件。

□□□ 单击 **Add Rule**（添加规则）。

系统将显示 **Add An Access Profile Rule**（添加访问配置文件规则）页面。

图 6-39. 添加访问配置文件规则

□□□ 填写对话框中的字段：

**Management Method**（管理方法）— 从下拉框中选择。策略受所选管理的限制。

**Interface**（接口）— 如果策略应含有根据接口而设置的规则，请选择此复选框。接口可以是物理接口、LAG 或 VLAN。

**Source IP Address**（源 IP 地址）— 如果策略应包含根据发送管理通信的客户端的 IP 地址设置的规则，请选择 **Source IP Address**（源 IP 地址）复选框。在提供的文本框中填写详细的源 IP 地址和掩码。请注意，掩码可以以两种格式提供 - 带点的 IP 格式（例如 255.255.255.0）或前缀长度（例如 32）。

**Action**（动作）— 选择当符合上述所选规则时，应执行的动作。使用下拉框并选择“Permit（允许）”或“Deny（拒绝）”以允许或拒绝访问。

**Rule Priority**（规则优先级）— 配置规则优先级。规则将以优先级从小到大的顺序对接入管理请求进行验证。如果符合规则的条件，则执行动作并忽略其下的规则。例如，如果首先配置一条规则，其源 IP 为 10.10.10.10，优先级为 1，并设置为“允许”，然后配置另一条规则，其源 IP 为 10.10.10.10，优先级为 2，并设为“拒绝”，则激活配置文件后，将允许访问而忽略第二条规则。

□□□ 单击 **Apply Changes**（应用更改）。

系统将把规则添加至访问配置文件并更新设备。

## 删除规则

□□□ 打开 **Access Profiles**（访问配置文件）页面。

□□□ 单击 **Show All**（全部显示）以显示 **Profile Rules Table**（配置文件规则表）页面。

□□□ 选择一条规则。

□□□ 选中 **Remove**（删除）复选框。

□□□ 单击 **Apply Changes**（应用更改）。



系统将删除规则并更新设备。

## 使用 CLI 命令定义访问配置文件

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

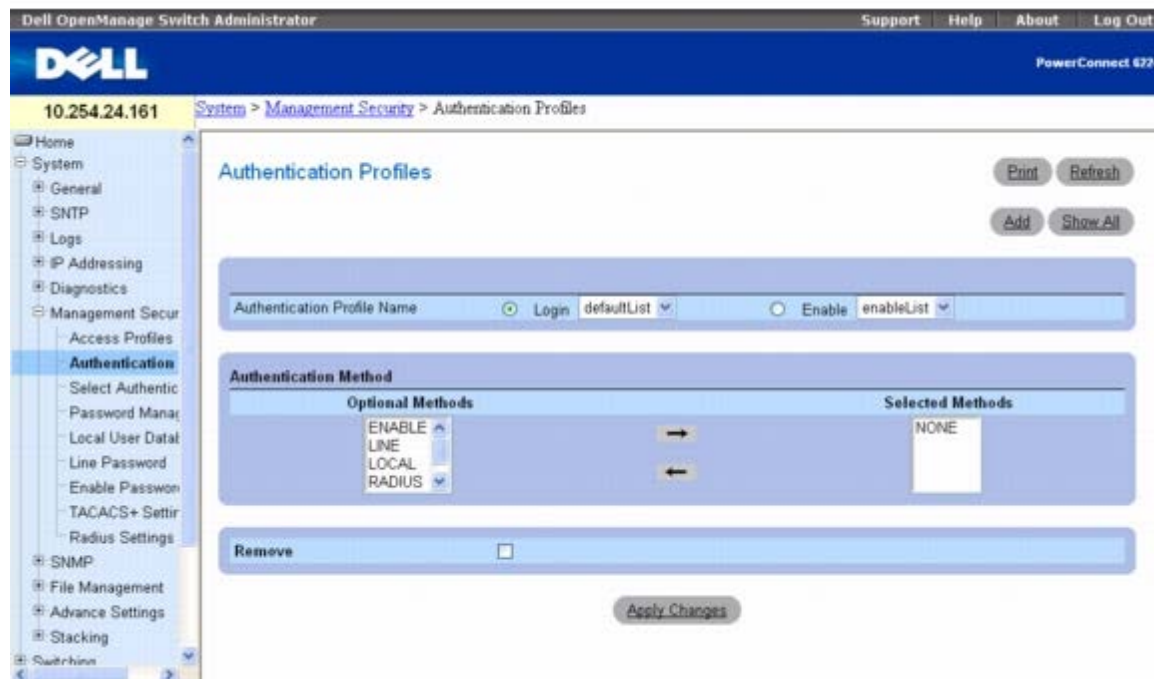
- 管理 ACL 命令。

## 验证配置文件

用户验证发生于本地和外部服务器。**Authentication Profiles**（验证配置文件）页面用于选择设备上的用户验证方法。

要显示 **Authentication Profiles**（验证配置文件）页面，请在树视图中单击 **System**（系统）**®** **Management Security**（管理安全保护）**®** **Authentication Profiles**（验证配置文件）。

图 6-40. 验证配置文件



**Authentication Profiles**（验证配置文件）页面包含以下字段：

### Authentication Profile Name（验证配置文件名称）

显示用户定义的验证配置文件将添加到的列表。使用单选按钮，选择将验证配置文件应用于交换机的登录操作部分或启用操作部分，以及选择两种可用列表之一：

**Login**（登录）— 允许您登录到交换机。选项包括 **defaultList**、**networkList** 以及任何用户定义的登录验证配置文件。

**Enable**（启用）— 启用特权模式。

### Authentication Method（验证方法）



**Optional Methods**（可选方法）— 用户验证方法。可能的选项包括：

**None**（无）— 不进行用户验证。


**Local**（本地）— 用户验证发生于设备级别；设备检查用户名和密码以进行验证。

**RADIUS**— 在 RADIUS 服务器上进行用户验证。有关 RADIUS 服务器的详细信息，请参阅 [RADIUS 设置](#)。

**TACACS+**— 在 TACACS+ 服务器上进行用户验证。有关 TACACS+ 服务器的详细信息，请参阅 [TACACS+ 设置](#)。

**Line**（线路）— 使用线路密码进行用户验证。

**Enable**（启用）— 使用启用密码进行验证。

 **注：** 用户验证按照方法选择顺序进行。如果在验证过程中出现错误，将使用下一个选定方法。例如，如果首先选择了 **Local**（本地），然后选择了 **RADIUS** 选项，则首先在本地验证用户，然后通过外部 **RADIUS** 服务器验证用户。

**Selected Methods**（选定方法）— 选定的验证方法。

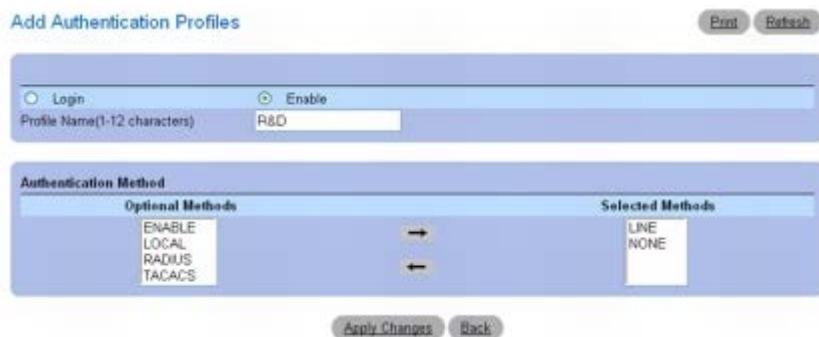
**Remove**（删除）— 删除选定的配置文件。

## 添加验证配置文件


□□□ 打开 **Authentication Profiles**（验证配置文件）页面。

□□□ 单击 **Add**（添加）以显示 **Add Authentication Profile**（添加验证配置文件）页面。

图 6-41. 添加验证配置文件



□□□ 在 **Profile Name**（配置文件名称）字段中输入配置文件的名称，长度为 1 至 12 个字符。

 **注：** 配置文件名称不应包含空格。

□□□ 单击 **Apply Changes**（应用更改）。

即创建一个配置文件。您可以使用 **System**（系统）® **Management Security**（管理安全保护）® **Select Authentication**（选择验证）网页激活验证配置文件。

## 修改验证配置文件

□□□ 打开 **Authentication Profiles**（验证配置文件）页面。

□□□ 在 **Authentication Profile Name**（验证配置文件名称）字段的列表选择一个元素。

□□□ 使用箭头选择一个或多个 **Optional Methods**（可选方法）。

□□□ 单击 **Apply Changes**（应用更改）。

用户验证配置文件将被更新到设备。

## 删除验证配置文件条目

□□□ 打开 **Authentication Profiles**（验证配置文件）页面。

□□□ 单击 **Show All**（全部显示）。

系统将打开 **Authentication Profiles Table**（验证配置文件表）。

图 6-42. 验证配置文件表

Login Authentication Profiles			Methods	Remove
1	defaultList		NONE,LINE	<input type="checkbox"/> Edit

Enable Authentication Profiles			Methods	Remove
1	enableList		NONE	<input type="checkbox"/> Edit
2	R&D		LINE,NONE	<input type="checkbox"/> Edit

□□□ 选择要删除的配置文件旁边的 **Remove**（删除）复选框。

□□□ 单击 **Apply Changes**（应用更改）。

系统即删除条目。

## 使用 CLI 命令配置验证配置文件

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

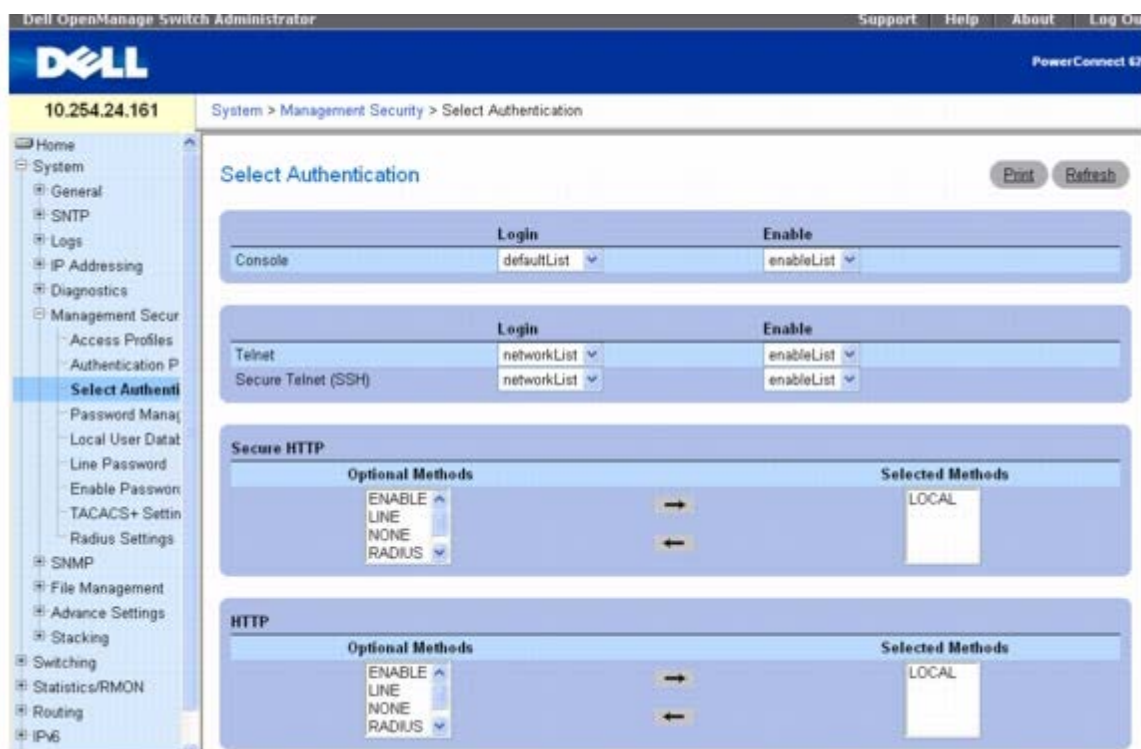
- AAA 命令。

## 选择验证

定义配置文件后，您可以将其应用于管理访问方法。你如，可以使用 **Authentication Profile List 1** 验证控制台用户，而使用 **Authentication Profile List 2** 验证 Telnet 用户。

要显示 **Select Authentication**（选择验证）页面，请在树视图中单击 **System**（系统）® **Management Security**（管理安全保护）® **Select Authentication**（选择验证）。

图 6-43. 选择验证



**Select Authentication** (选择验证) 页面包含以下字段：

**Console** (控制台) — 用于验证控制台用户的验证配置文件。

**Telnet**— 用于验证 Telnet 用户的验证配置文件。

**Secure Telnet (SSH)** (安全 Telnet [SSH]) — 用于验证安全命令解释程序 (SSH) 用户的验证配置文件。SSH 使客户端可以与设备建立安全和加密的远程连接。

**Secure HTTP and HTTP** (安全 HTTP 和 HTTP) — 分别用于安全 HTTP 访问和 HTTP 访问的验证方法。可能的字段值包括：

**None** (无) — 访问时不使用任何验证方法。

**Local** (本地) — 在本地进行验证。

**RADIUS**— 在 RADIUS 服务器上验证。

**TACACS+**— 在 TACACS+ 服务器上验证。

**Local, None** (本地, 无) — 首先在本地进行验证。

**RADIUS, None** (RADIUS, 无) — 首先在 RADIUS 服务器上验证。如果验证无法实施, 则不使用任何验证方法。如果无法联系远程服务器以验证用户, 则验证无法实施。如果可以联系远程服务器, 则优先处理来自远程服务器的响应。

**TACACS+, None** (TACACS+, 无) — 首先在 TACACS+ 服务器上验证。如果验证无法实施, 则不使用任何验证方法。如果无法联系远程服务器以验证用户, 则验证无法实施。如果可以联系远程服务器, 则优先处理来自远程服务器的响应。

**Local, RADIUS** (本地, RADIUS) — 首先在本地进行验证。如果无法在本地验证, 则使用 RADIUS 服务器验证管理方法。如果 RADIUS 服务器不能验证管理方法, 则会话将被禁止。

**Local, TACACS+** (本地, TACACS+) — 首先在本地进行验证。如果无法在本地验证, 则使用 TACACS+ 服务器验证管理方法。如果 TACACS+ 服务器不能验证管理方法, 则会话将被禁止。

**RADIUS, Local** (RADIUS, 本地) — 首先在 RADIUS 服务器上验证。如果无法在 RADIUS 服务器验证, 则在本地验证会话。如果会话不能在本地验证, 将会被禁止。

**TACACS+, Local** (TACACS+, 本地) — 首先在 TACACS+ 服务器上验证。如果无法在 TACACS+ 服务器验证, 则在本地验证会话。如果会话不能在本地验证, 将会被禁止。

**Local, RADIUS, None** (本地, RADIUS, 无) — 首先在本地进行验证。如果无法在本地验证, 则使用 RADIUS 服务器验证管理方法。如果 RADIUS 服务器不能验证管理方法, 则允许进行会话。

**RADIUS, Local, None (RADIUS, 本地, 无)** — 首先在 RADIUS 服务器上验证。如果无法在 RADIUS 服务器验证, 则在本地验证会话。如果会话不能在本地验证, 则允许进行会话。

**Local, TACACS+, None (本地, TACACS+, 无)** — 首先在本地进行验证。如果无法在本地验证, 则使用 TACACS+ 服务器验证管理方法。如果 TACACS+ 服务器不能验证管理方法, 则允许进行会话。

**TACACS+, Local, None (TACACS+, 本地, 无)** — 首先在 TACACS+ 服务器上验证。如果无法在 TACACS+ 服务器验证, 则在本地验证会话。如果会话不能在本地验证, 则允许进行会话。

## 将验证方法列表应用于控制台会话

□□□ 打开 **Select Authentication** (选择验证) 页面。

□□□ 在 **Console** (控制台) 字段中选择一个验证配置文件。

□□□ 单击 **Apply Changes** (应用更改)。

系统将向控制台会话分配一个验证方法列表。

## 将验证配置文件应用于 Telnet 会话

□□□ 打开 **Select Authentication** (选择验证) 页面。

□□□ 在 **Telnet** 字段中选择一个验证配置文件。

□□□ 单击 **Apply Changes** (应用更改)。

系统将向 Telnet 会话分配验证配置文件。

## 将验证配置文件应用于安全 Telnet (SSH) 会话

□□□ 打开 **Select Authentication** (选择验证) 页面。

□□□ 在 **Secure Telnet (SSH)** (安全 Telnet [SSH]) 字段中选择一个验证配置文件。

□□□ 单击 **Apply Changes** (应用更改)。

系统将向安全 Telnet (SSH) 会话分配验证配置文件。

## 为 HTTP 会话分配验证顺序

□□□ 打开 **Select Authentication** (选择验证) 页面。

□□□ 在 **HTTP** 下的 **Optional Methods** (可选方法) 字段中选择一个验证方法, 然后单击右箭头按钮。

所选验证方法将移至 **Selected Methods** (选定方法) 字段。

□□□ 重复这一操作, 直至 **Selected Methods** (选定方法) 字段显示所需验证顺序。

□□□ 单击 **Apply Changes** (应用更改)。

系统将向 HTTP 会话分配一个验证顺序。

## 使用 CLI 命令分配访问方法、验证配置文件或验证顺序

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- AAA 命令。

## 为安全 HTTP 会话分配验证顺序

□□□ 打开 **Select Authentication**（选择验证）页面。

□□□ 在 **Secure HTTP**（安全 HTTP）下的 **Optional Methods**（可选方法）字段中选择一个验证方法，然后单击右箭头按钮。

所选验证方法将移至 **Selected Methods**（选定方法）字段。

□□□ 重复这一操作，直至 **Selected Methods**（选定方法）字段显示所需验证顺序。

□□□ 单击 **Apply Changes**（应用更改）。

系统将向安全 HTTP 会话分配一个验证顺序。

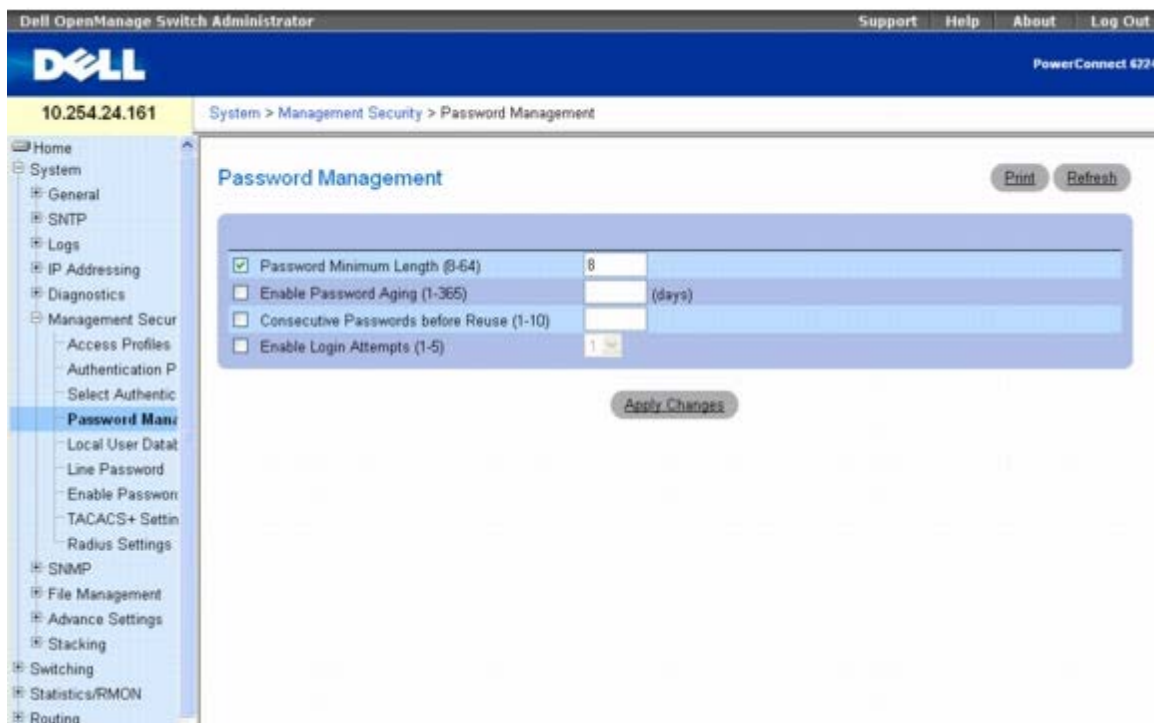
## 密码管理

密码管理可提高网络安全性，还可改进密码控制。SSH、Telnet、HTTP、HTTPS 和 SNMP 的访问密码均分配有安全保护功能，包括：

- 定义最小密码长度
- 密码过期
- 防止频繁重复使用密码
- 在若干次登录尝试失败后锁定用户

要显示 **Password Management**（密码管理）页面，请在树视图中单击 **System**（系统）® **Management Security**（管理安全保护）® **Password Management**（密码管理）。

图 6-44. 密码管理




**Password Management**（密码管理）页面包含以下字段：

**Password Minimum Length (8–64)**（最小密码长度 [8-64]）— 如果选择该选项，则表示最小密码长度。例如，管理员可以定义所有线路密码必须至少包含 10 个字符。

**Enable Password Aging (1–365)**（启用密码存在时间 [1-365]）— 如果选择该选项，表示密码在经过多长的时间之后会过期。字段的取值范围为 1 至 365 天。只有当交换机时钟与 SNMP 服务器同步时，密码存在时间功能才有效。有关详细信息，请参阅《CLI 参考指南》中的“时钟命令”一节。

**Consecutive Passwords Before Reuse (1–10)**（重新使用前的连续密码数 [1-10]）— 表示在经过多少次密码变更后，才能重新使用旧密码。可能的字段值为 1 至 10。

 **注：**用户在密码过期前，会收到更改密码的通知。Web 用户则不会收到该通知。

**Enable Login Attempts (1–5)**（启用登录尝试 [1-5]）— 如果选择该选项，则当用户使用错误的密码尝试登录一定次数后，会被锁定于设备之外。例如，如果登录尝试的次数定义为五次，且用户使用不正确的密码尝试登录了五次，则在第六次尝试时，设备会将用户锁定。之后，需要由超级用户来重新启用该用户帐户。字段范围为 1 至 5 次尝试。

## 定义密码约束

□□□ 打开 **Password Management**（密码管理）页面。

□□□ 定义相关的字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将定义密码约束并更新设备。

## 使用 CLI 命令定义密码约束

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

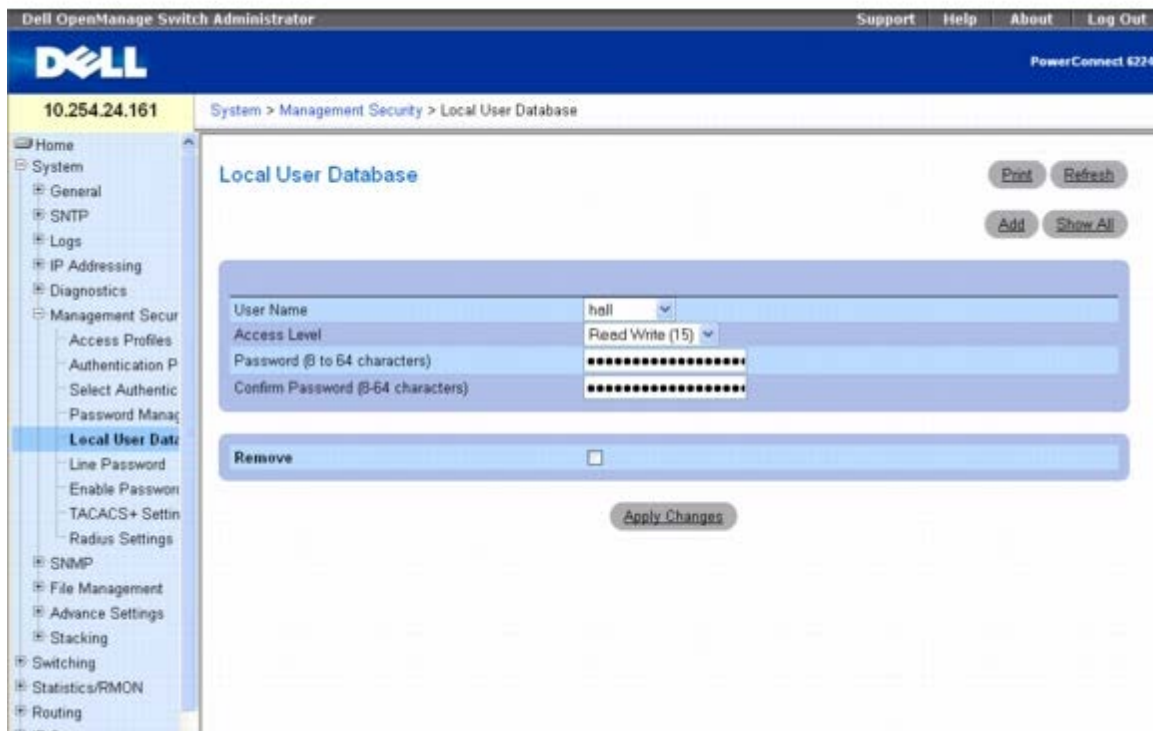
- 密码管理命令。

## 本地用户数据库

**Local User Database**（本地用户数据库）页面用于定义用户密码和访问权限，以及重新激活帐户被锁定的用户。

要显示 **Local User Database**（本地用户数据库）页面，请在树视图中单击 **System**（系统）® **Management Security**（管理安全保护）® **Local User Database**（本地用户数据库）。

图 6-45. 本地用户数据库



**Local User Database**（本地用户数据库）页面包含以下字段：

**User Name**（用户名）— 用户的列表。

**Access Level**（访问级别）— 用户访问级别。最低的用户访问级别为 **1**（只读），最高的级别为 **15**（读/写）。要暂时禁止某一用户访问，请将其级别设为 0（仅当用户的级别为 15 时才可进行这一设置）。

**Password (8–64 characters)**（密码 [8 至 64 个字符]）— 用户定义的密码。

**Confirm Password**（确认密码）— 确认用户定义的密码。

**Remove**（删除）— 如果选择该选项，将从本地用户数据库中删除用户。

## 为用户分配访问权限

□□□ 打开 **Local User Database**（本地用户数据库）页面。

□□□ 在 **User Name**（用户名）字段中选择一个用户。

□□□ 根据需要定义各个字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将定义用户访问权限和密码并更新设备。



## 将用户添加到本地用户数据库

□□□ 打开 **Local User Database**（本地用户数据库）页面。

□□□ 单击 **Add**（添加）以显示 **Add User**（添加用户）页面。

系统将显示 **Add a New User**（添加新用户）页面。


图 6-46. 添加新用户

Attribute	Value
User Name (1 to 20 characters)	<input type="text"/>
Access Level	Read Write (15)
Password (8 to 64 characters)	.....
Confirm Password (8-64 characters)	.....

□□□ 填写各字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将定义新用户并更新设备。

 **注：**您最多可以在设备上定义八个本地用户。

## 在本地用户数据库中显示用户

□□□ 打开 **Local User Database**（本地用户数据库）页面。

□□□ 单击 **Show All**（全部显示）以显示 **Local User Table**（本地用户表）页面。

系统将显示本地用户数据库的所有成员。

图 6-47. 本地用户表

	User Name	Access Level	Remove	
1	amylover	Read Write	<input type="checkbox"/>	Edit
2	hopekiser	Read Write	<input type="checkbox"/>	Edit
3	hail	Read Write	<input type="checkbox"/>	Edit

## 从本地用户数据库删除用户

□□□ 打开 **Local User Database**（本地用户数据库）页面。

□□□ 单击 **Show All**（全部显示）以显示 **Local User Table**（本地用户表）页面。

□□□ 选择一个 **User Name**（用户名）。

□□□ 选中 **Remove**（删除）复选框。

□□□ 单击 **Apply Changes**（应用更改）。



系统将删除用户并更新设备。

## 使用 CLI 命令分配用户

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

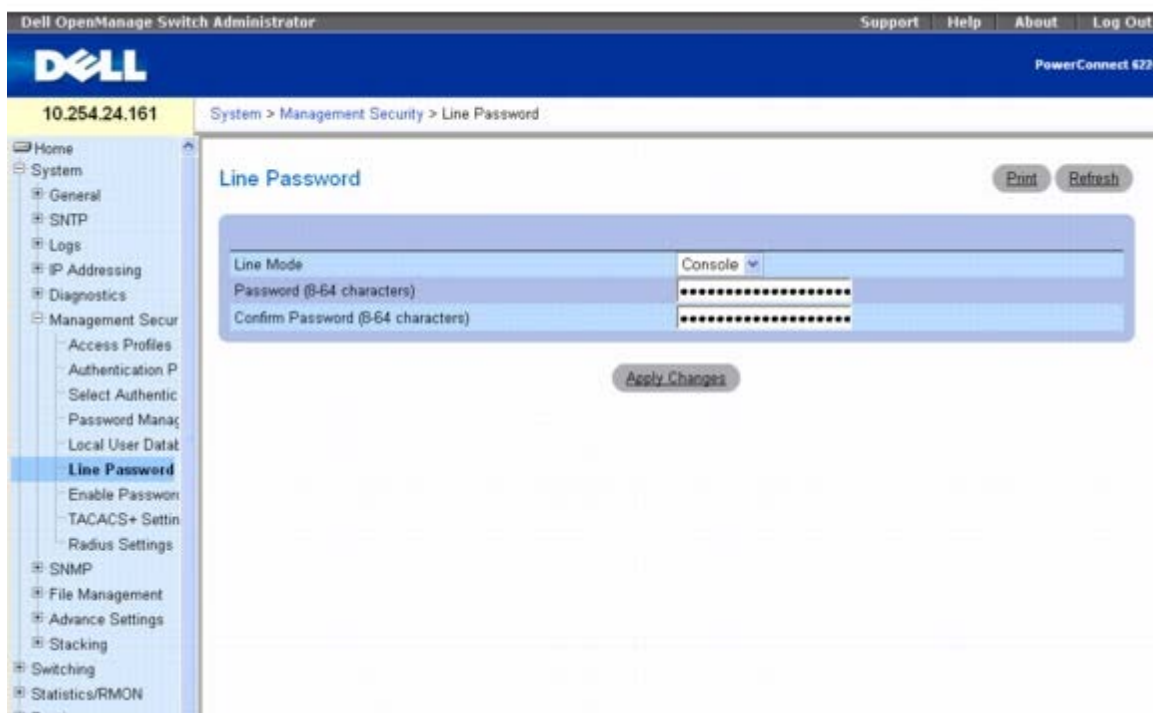
- AAA 命令。

## 线路密码

**Line Password**（线路密码）页面用于定义管理方法的线路密码。

要显示 **Line Password**（线路密码）页面，请在树视图中单击 **System**（系统）® **Management Security**（管理安全保护）® **Line Password**（线路密码）。

图 6-48. 线路密码



**Line Password**（线路密码）页面包含以下字段：

**Line Mode**（线路模式）— 一个下拉式菜单，指定是通过控制台、Telnet 还是安全 Telnet (SSH) 会话来访问设备。

**Line Password (8 – 64 characters)**（线路密码 [8 至 64 个字符]）— 用于通过控制台、Telnet 或安全 Telnet 会话访问设备的线路密码。密码将以 \*\*\*\*\* 格式显示。

**Confirm Password (8 – 64 characters)**（确认密码 [8 至 64 个字符]）— 确认新的线路密码。密码将以 \*\*\*\*\* 格式显示。

## 定义线路密码

□□□ 打开 **Line Password**（线路密码）页面。

□□□ 选择是通过控制台、Telnet 还是安全 Telnet (SSH) 会话来访问设备。

□□□ 为用来连接设备的会话类型定义 **Line Password**（线路密码）字段。

□□□ 确认 **Line Password**（线路密码）。

□□□ 单击 **Apply Changes**（应用更改）。

系统将定义会话类型的线路密码并更新设备。

## 使用 CLI 命令设定线路密码

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

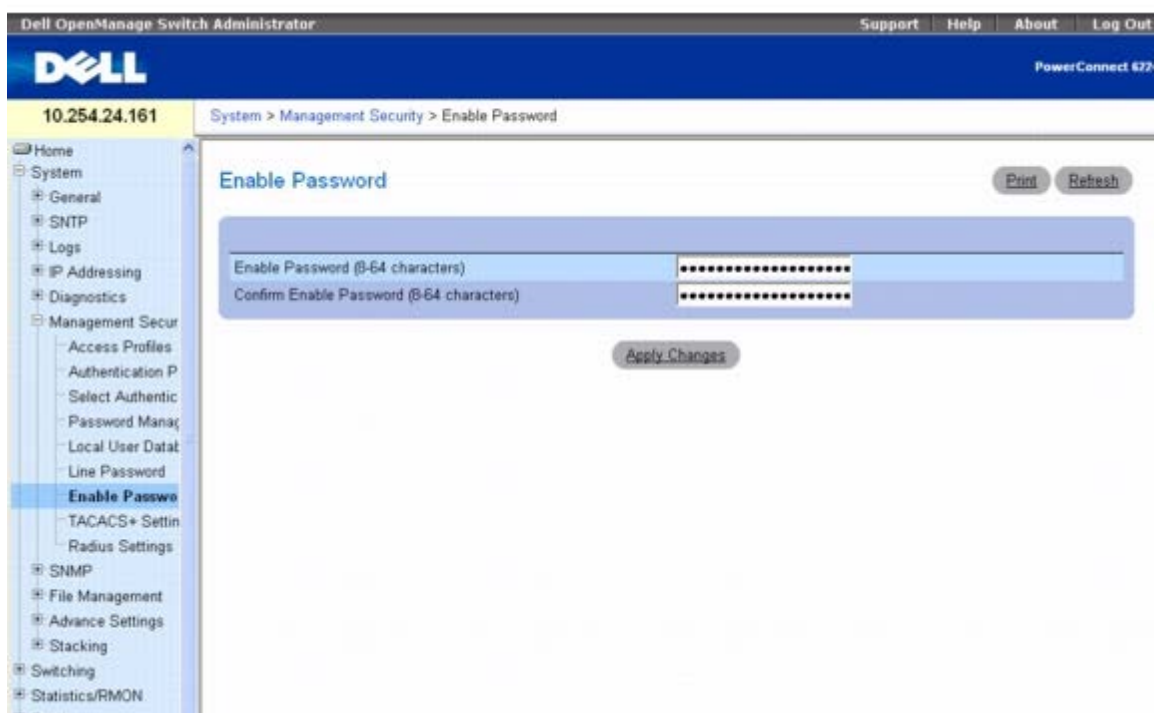
- AAA 命令。

## 启用密码

**Enable Password**（启用密码）页面可以设置本地密码，以控制对普通和优先级别的访问。

要显示 **Enable Password**（启用密码）页面，请在树视图中单击 **System**（系统）® **Management Security**（管理安全保护）® **Enable Password**（启用密码）。

图 6-49. 启用密码



**Enable Password**（启用密码）页面包含以下字段：

**Enable Password (8–64 characters)**（启用密码 [8 至 64 个字符]）— 启用对普通和优先级别的访问控制密码。密码将以 \*\*\*\*\* 格式显示。

**Confirm Enable Password**（确认启用密码）— 确认新的启用密码。密码将以 \*\*\*\*\* 格式显示。

## 定义启用密码

□□□ 打开 **Enable Password**（启用密码）页面。

□□□ 指定启用密码。

□□□ 确认启用密码。

□□□ 单击 **Apply Changes** (应用更改)。

系统将设置启用密码。

## 使用 CLI 命令设定启用密码

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- AAA 命令。

## TACACS+ 设置

设备提供对终端访问控制器访问控制系统 (TACACS+) 客户端的支持。TACACS+ 为访问设备的用户的验证提供了集中式安全保护。

TACACS+ 提供了集中式用户管理系统，同时还保持了与 RADIUS 和其它验证过程的一致性。TACACS+ 提供以下服务：

- 验证 — 登录时验证用户名和用户定义的密码。
- 授权 — 登录时执行。完成验证会话后，将使用通过验证的用户名开始授权会话。TACACS+ 服务器将检查用户权限。

TACACS+ 协议通过在设备与 TACACS+ 服务器之间交换加密协议，确保网络的安全保护。

**TACACS+ Settings** (TACACS+ 设置) 页面含有带内管理端口的用户定义设置和默认的 TACACS+ 设置。

要显示 **TACACS+ Settings** (TACACS+ 设置) 页面，请在树视图中单击 **System** (系统) ® **Management Security** (管理安全保护) ® **TACACS+ Settings** (TACACS+ 设置)。

图 6-50. TACACS+ 设置

The screenshot shows the Dell OpenManage Switch Administrator interface. The top navigation bar includes 'Support', 'Help', 'About', and 'Log Out'. The main header displays the Dell logo and 'PowerConnect 6224'. The breadcrumb trail is 'System > Management Security > TACACS+ Settings'. The left sidebar shows a tree view with 'Management Secur' expanded to 'TACACS+ Settings'. The main content area has a title 'TACACS+ Settings' and buttons for 'Print', 'Refresh', 'Add', and 'Show All'. Below the title are two sections: 'TACACS+ Server' and 'Default Parameters'. The 'TACACS+ Server' section has fields for 'Host Name/IP Address', 'Priority (0 - 65535)', 'Authentication Port (0 - 65535)', 'Key String (0 - 128 characters)', and 'Timeout for Reply (1 - 30) (sec)'. There are 'Use Default' checkboxes for the 'Key String' and 'Timeout for Reply' fields. The 'Default Parameters' section has fields for 'Key String (0 - 128 characters)' and 'Timeout for Reply (1 - 30) (sec)'. An 'Apply Changes' button is at the bottom.

**TACACS+ Settings** (TACACS+ 设置) 页面包含以下字段：

**Host Name / IP Address** (主机名/IP 地址) — 指定 TACACS+ 服务器。

**Priority (0–65535)** (优先级 [0-65535]) — 指定 TACACS+ 服务器的使用顺序。默认值为 0。

**Authentication Port (0–65535)** (验证端口 [0-65535]) — 通过其进行 TACACS+ 会话的端口号。默认端口为 49。

**Key String (0–128 Characters)** (密钥字符串 [0 至 128 个字符]) — 定义用于设备与 TACACS+ 服务器之间的 TACACS+ 通信的验证和密钥。此密钥必须与 TACACS+ 服务器上使用的加密相匹配。选中 **Use Default** (使用默认值) 复选框将使用默认值。

**Timeout for Reply (1–30)** (答复超时 [1-30]) — 设备与 TACACS+ 服务器之间连接超时之前所经过的时间。字段范围为 1 至 30 秒。选中 **Use Default** (使用默认值) 将选择工厂默认值。

**Status** (状态) — 设备与 TACACS+ 服务器之间的连接状态。可能的字段值包括：

**Connected** (已连接) — 设备与 TACACS+ 服务器之间当前已连接。

**Not Connected** (未连接) — 设备与 TACACS+ 服务器之间当前未连接。

“Default Parameters (默认参数)” 页面区域中的字段含有自动应用于 TACACS+ 服务器的值。

**Key String (0–128 Characters)** (密钥字符串 [0 至 128 个字符]) — 输入用于设备与 TACACS+ 服务器之间的 TACACS+ 通信的默认验证和密钥。

**Timeout for Reply (1–30)** (答复超时 [1-30]) — 输入设备与 TACACS+ 服务器之间连接超时之前所经过的全局用户配置时间。

## 定义 TACACS+ 参数

□□□ 打开 **TACACS+ Settings** (TACACS+ 设置) 页面。

□□□ 根据需要定义各个字段。

□□□ 单击 **Apply Changes** (应用更改)。

TACACS+ 设置将被更新到设备。

## 添加 TACACS+ 服务器

□□□ 打开 **TACACS+ Settings** (TACACS+ 设置) 页面。

□□□ 单击 **Add** (添加)。

系统将显示 **Add TACACS+ Host** (添加 TACACS+ 主机) 页面。

图 6-51. 添加 TACACS+ 主机

Field	Value	Options
Host Name/IP Address	10.240.13.45	(XXXX)
Priority (0 - 65535)	258	
Authentication Port (0 - 65535)	43	
Key String (0 - 128 characters)	.....	<input type="checkbox"/> Use Default
Timeout for Reply (1 - 30)	5	(sec) <input type="checkbox"/> Use Default

□□□ 根据需要定义各个字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将添加 TACACS+ 服务器并更新设备。

## 显示 TACACS+ 服务器列表

□□□ 打开 **TACACS+ Settings** (TACACS+ 设置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将打开 **TACACS+ Servers Table** (TACACS+ 服务器表)。

图 6-52. TACACS+ 服务器表

	Host IP Address	Priority	Authentication Port	Timeout For Reply (sec)	Status	Remove
1	10.240.13.45	258	43	5	Not Connected	<input type="checkbox"/> Edit

## 从 TACACS+ 服务器列表中删除 TACACS+ 服务器

□□□ 打开 **TACACS+ Settings** (TACACS+ 设置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将打开 **TACACS+ Servers Table** (TACACS+ 服务器表)。

□□□ 选择一个 **TACACS+ Servers Table** (TACACS+ 服务器表) 条目。

□□□ 选中 **Remove** (删除) 复选框。

□□□ 单击 **Apply Changes** (应用更改)。

系统将删除 TACACS+ 服务器并更新设备。

## 使用 CLI 命令定义 TACACS+ 服务器

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- TACACS+ 命令。

## RADIUS 设置

远程认证拨入用户服务 (RADIUS) 服务器为网络提供了附加安全保护。RADIUS 服务器维护用户数据库，其中含有每个用户的验证信息。RADIUS 服务器为以下操作提供了集中式的验证方法：

- Telnet 访问
- Web 访问
- 控制台对交换机的访问
- 访问控制端口 (802.1x)

**RADIUS Settings** (**RADIUS** 设置) 页面包含用户定义的 RADIUS 设置和默认的 RADIUS 设置。

要显示 **RADIUS Settings** (**RADIUS** 设置) 页面，请在树视图中单击 **System** (系统) @ **Management Security** (管理安全保护) @ **RADIUS Settings** (**RADIUS** 设置)。

图 6-53. RADIUS 设置

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb path is System > Management Security > RADIUS. The page title is RADIUS Settings. There are buttons for Print, Refresh, Add, and Show All. The RADIUS Server configuration table is as follows:

RADIUS Server	
IP Address	10.24.100.18
Priority (0-65535)	256
Authentication Port (0-65535)	1043
Number of Retries (1-10)	4 <input type="checkbox"/> Use Default
Timeout for Reply (1-30)	20 (sec) <input type="checkbox"/> Use Default
Deadtime (0-2000)	500 (min) <input type="checkbox"/> Use Default
Key String (0-128 characters)	drowyek <input type="checkbox"/> Use Default
Source IP Address	10.240.1.87 (X.X.X.X) <input type="checkbox"/> Use Default
Usage Type	Login

The Default Parameters configuration table is as follows:

Default Parameters	
Default Retries (1-10)	3
Default Timeout for Reply (1-30)	20 (sec)
Default Deadtime (0-2000)	1000 (min)
Default Key String (0-128 characters)	key
Source IP Address	202.241.43 (X.X.X.X)

**RADIUS Settings** (**RADIUS** 设置) 页面包含以下字段：

**IP Address** (IP 地址) — RADIUS 服务器的 IP 地址。

**Priority (0–65535)** (优先级 [0–65535]) — 表示端口的优先级。可能的值为 0 至 65535。

**Authentication Port (0–65535)** (验证端口 [0–65535]) — 标识用于确认 RADIUS 服务器验证的验证端口。

**Number of Retries (1–10)** (重试次数 [1–10]) — 在失败前发送至 RADIUS 服务器的请求传输次数。可能的字段值为 1 至 10。默认值为 3。如果没有指定特定于主机的值，每台主机都将应用同一个全局值。选中 **Use Default** (使用默认值) 复选框将使用用户定义的默认值。


**Timeout for Reply (1–30)** (答复超时 [1–30]) — 指定超时之前设备等待 RADIUS 服务器答复的时间 (以秒为单位)。可能的字段值为 1 至 30。默认值为 3。如果没有指定特定于主机的值，每台主机都将应用同一个全局值。选中 **Use Default** (使用默认值) 复选框将使用用户定义的默认值。

**DeadTime (0–2000)** (无响应时间 [0–2000]) — 指定 RADIUS 服务器不处理服务请求的时间 (以分钟为单位)。其范围为 0 至 2000。如果没有指定特定主机的值，每台主机都将应用同一个全局值。选中 **Use Default** (使用默认值) 复选框将使用用户定义的默认值。

**Key String (0–128 Characters)** (密钥字符串 [0 至 128 个字符]) — 用于验证和加密设备与 RADIUS 服务器之间所有 RADIUS 通信的密钥字符串。该密钥必须与 RADIUS 加密相符。如果没有指定特定主机的值，每台主机都将应用同一个全局值。选中 **Use Default** (使用默认值) 复选框将使用用户定义的默认值。

**Source IP Address** (源 IP 地址) — 访问 RADIUS 服务器的设备的 IP 地址。选中 **Use Default** (使用默认值) 复选框将使用用户定义的默认值。

**Usage Type** (使用类型) — 用于选择 RADIUS 使用类型的下拉框。

 **注：** 本页中的默认参数由用户定义。

**Default Retries (1–10)** (默认重试次数 [1–10]) — 在失败发生前发送至 RADIUS 服务器的默认请求传输次数。

**Default Timeout for Reply (1–30)** (默认答复超时 [1–30]) — 超时之前设备等待 RADIUS 服务器答复的默认时间 (以秒为单位)。可



能的字段值为 1 至 30。

**Default Deadtime (0–2000)** (默认无响应时间 **[0-2000]**) — 指定 RADIUS 服务器不处理服务请求的默认时间 (以分钟为单位)。范围为 0 至 2000。

**Default Key String (0–128 characters)** (默认密钥字符串 **[0 至 128 个字符]**) — 用于验证和加密设备与 RADIUS 服务器之间所有 RADIUS 通信的默认密钥字符串。该密钥必须与 RADIUS 加密相符。

**Source IP Address** (源 IP 地址) — 访问 RADIUS 服务器的设备的默认 IP 地址。

## 添加 RADIUS 服务器

□□□ 打开 **RADIUS Settings** (**RADIUS 设置**) 页面。

□□□ 单击 **Add** (添加)。

系统将显示 **Add RADIUS Server** (添加 RADIUS 服务器) 页面。

图 6-54. 添加 RADIUS 服务器

□□□ 定义对话框中的字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将添加新的 RADIUS 服务器并更新设备。

## 定义 RADIUS 参数

□□□ 打开 **RADIUS Settings** (**RADIUS 设置**) 页面。

□□□ 定义对话框中的字段。

□□□ 单击 **Apply Changes** (应用更改)。

RADIUS 设置将被更新到设备。

## 修改 RADIUS 服务器设置

□□□ 打开 **RADIUS Settings** (**RADIUS 设置**) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **RADIUS Servers Table** (**RADIUS 服务器表**)。

图 6-55. RADIUS 服务器表

	IP Address	Priority	Authentication Port	Number of Retries	Timeout For Reply (sec)	Deadtime (min)	Source IP Address	Usage Type	Remove
1	10.240.10.13	2	23	45	56	3	10.240.13.45	Login	<input type="checkbox"/> Edit
2	10.240.10.40	4	25	34	53	2	10.240.13.15	Login	<input type="checkbox"/> Edit
3	10.240.10.14	2	23	43	57	1	10.240.13.45	Login	<input type="checkbox"/> Edit

□□□ 单击所选条目的 **Edit**（编辑）链接。

□□□ 在 **RADIUS Settings**（RADIUS 设置）页面中更改 RADIUS 服务器的设置。

□□□ 单击 **Apply Changes**（应用更改）。

系统将修改 RADIUS 服务器设置并更新设备。

## 删除 RADIUS 服务器列表中的 RADIUS 服务器

□□□ 打开 **RADIUS Settings**（RADIUS 设置）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **RADIUS Servers Table**（RADIUS 服务器表）。

□□□ 选择一个 RADIUS 服务器并选中 **Remove**（删除）复选框。

□□□ 单击 **Apply Changes**（应用更改）。

系统将从列表中删除 RADIUS 服务器。

## 使用 CLI 命令定义 RADIUS 服务器

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- Radius 命令。

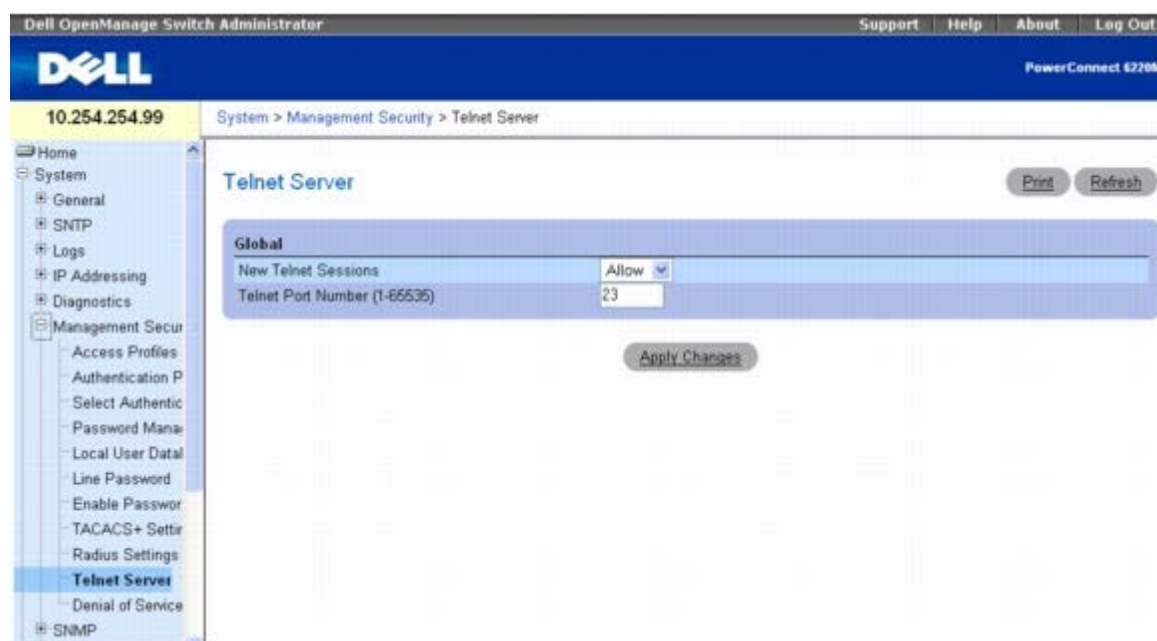
## Telnet 服务器

**Telnet Server**（Telnet 服务器）页面用于启用或禁用交换机上的 Telnet 服务或者修改 Telnet 端口。

要显示 **Telnet Server**（Telnet 服务器）页面，请单击 **System**（系统）® **Management Security**（管理安全保护）® **Telnet Server**（Telnet 服务器）。

图 6-56. Telnet 服务器





**Telnet Server** (**Telnet** 服务器) 页面包含以下字段：

**New Telnet Sessions** (新 **Telnet** 会话) — 控制入站 **Telnet** 会话的管理模式。如果将此模式设置为 **Block** (阻塞)，将不允许新的 **Telnet** 会话，但不会中断现有的会话。默认值为 **Allow** (允许)。

**Telnet Port Number** (**Telnet** 端口号) — 可以用来启动 **Telnet** 会话的端口号。系统将对交换机上的新入站 **Telnet** 会话使用此端口。修改了 **Telnet** 服务器端口之后，新的入站 **Telnet** 会话将使用新的端口，但现有的 **Telnet** 会话不会受到影响。

## 修改 **Telnet** 服务器设置

□□□ 打开 **Telnet Server Configuration** (**Telnet** 服务器配置) 页面。

□□□ 配置相关的字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存设置并更新设备。

## 使用 **CLI** 命令配置 **Telnet** 服务器

有关执行此功能的 **CLI** 命令的信息，请参阅《**CLI** 参考指南》的以下章节：

- **Telnet** 服务器命令

## 拒绝服务

拒绝服务是指通过多种攻击使主机服务中断或导致网络不稳定。**Denial of Service** (拒绝服务) 页面用于配置设置以帮助阻止拒绝服务攻击。

要显示 **Denial of Service** (拒绝服务) 页面，请在树视图中单击 **System** (系统) ® **Management Security** (管理安全保护) ® **Denial of Service** (拒绝服务)。

图 6-57. 拒绝服务



**Denial of Service**（拒绝服务）页面包含以下字段：

**Denial of Service SIP=DIP**（拒绝服务 **SIP=DIP**）— 启用 SIP=DIP DoS 防御功能将使交换机丢弃源 IP 地址等于目的地 IP 地址的那些信息包。

**Denial of Service First Fragment**（拒绝服务第一碎片）— 启用第一碎片 DoS 防御功能将使交换机丢弃 TCP 报头小于所配置的最小 TCP 报头大小（Min TCP Hdr Size [最小 TCP 报头大小]）的那些信息包。

**Denial of Service Min TCP Hdr Size**（拒绝服务最小 TCP 报头大小）— 指定允许的最小 TCP 报头大小。如果启用了第一碎片 DoS 防御功能，交换机将丢弃 TCP 报头大小小于所配置的这个值的那些信息包。

**Denial of Service TCP Fragment**（拒绝服务 TCP 碎片）— 启用 TCP 碎片 DoS 防御功能将使交换机丢弃 IP 碎片偏移量等于一的那些信息包。

**Denial of Service TCP Flag**（拒绝服务 TCP 标记）— 启用 TCP 标记 DoS 防御功能将使交换机丢弃符合以下任一条件的那些信息包：

- 设置了 TCP 标记 SYN，且 TCP 源端口小于 1024
- TCP 控制标记设置为 0，TCP 序列号设置为 0
- 设置了 TCP 标记 FIN、URG 和 PSH，且 TCP 序列号设置为 0
- 同时设置了 TCP 标记 SYN 和 FIN

**Denial of Service L4 Port**（拒绝服务 L4 端口）— 启用 L4 端口 DoS 防御功能将使交换机丢弃 TCP/UDP 源端口等于 TCP/UDP 目的地端口的那些信息包。

**Denial of Service ICMP**（拒绝服务 ICMP）— 启用 ICMP DoS 防御功能将使交换机丢弃类型被设置为 ECHO\_REQ (ping)、大小大于所配置的 ICMP 信息包大小（ICMP Pkt Size [ICMP 信息包大小]）的那些 ICMP 信息包。

**Denial of Service Max ICMP Pkt Size**（拒绝服务最大 ICMP 信息包大小）— 指定允许的最大 ICMP 信息包大小。如果启用了 ICMP DoS 防御功能，交换机将丢弃大小大于所配置的这个值的那些 ICMP ping 信息包。

## 配置拒绝服务设置

□□□ 打开 **Denial of Service**（拒绝服务）页面。

□□□ 指定所需的设置。

□□□ 单击 **Apply Changes**（应用更改）。

系统将使用新的设置更新设备。

## 使用 CLI 命令配置拒绝服务设置


有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 拒绝服务命令。

---

## 定义 SNMP 参数

简单网络管理协议 (SNMP) 提供了一种管理网络设备的方法。设备支持 SNMP 版本 1、SNMP 版本 2 和 SNMP 版本 3。

 **注：**默认情况下，设备自动启用 SNMPv2。要启用 SNMPv3，必须为设备定义本地引擎 ID。本地引擎 ID 默认设置为交换机 MAC 地址，但是当交换机以堆栈模式工作时，需要手动为堆栈配置本地引擎 ID。该本地引擎 ID 的定义必须在网络中唯一。这一点非常重要，因为堆栈中的默认引擎 ID 是主单元的 MAC 地址。如果主单元出现故障，并由另一单元所取代，则需要更改相应 MAC 地址。有关如何配置本地引擎 ID 的信息，请参阅 [SNMP 全局参数](#)。

## SNMP v1 和 v2

SNMP 代理程序保持了一份变量列表，用于管理设备。这些变量在管理信息库 (MIB) 中定义。MIB 提供了代理程序控制的变量。SNMP 代理程序定义了 MIB 规格格式以及用于通过网络访问信息的格式。对 SNMP 代理程序的访问权限由访问字符串控制。

## SNMP v3

SNMP v3 也可向 SNMPv1 和 SNMPv2 PDU 应用访问控制和新的陷阱机制。此外，SNMPv3 定义了用户安全保护模式 (USM)，包括：

- 验证 — 提供数据完整性和数据来源验证。
- 隐私 — 保护信息内容不致泄露。密码块链接 (CBC) 用于加密。既可以对 SNMP 信息启用验证，也可以对 SNMP 信息同时启用验证和隐私。但不可以在没有启用验证的情况下启用隐私。
- 合时性 — 防止信息延迟或信息冗余。SNMP 代理程序将传入信息与信息时间相比较。
- 密钥管理 — 定义密钥的生成，密钥的更新和密钥的使用。

本设备支持基于对象 ID (OID) 的 SNMP 通知筛选器。系统使用 OID 管理设备功能。SNMP v3 支持以下功能：

- 安全保护
- 功能访问控制
- 陷阱

验证或隐私密钥在 SNMPv3 用户安全保护模式 (USM) 中修改。

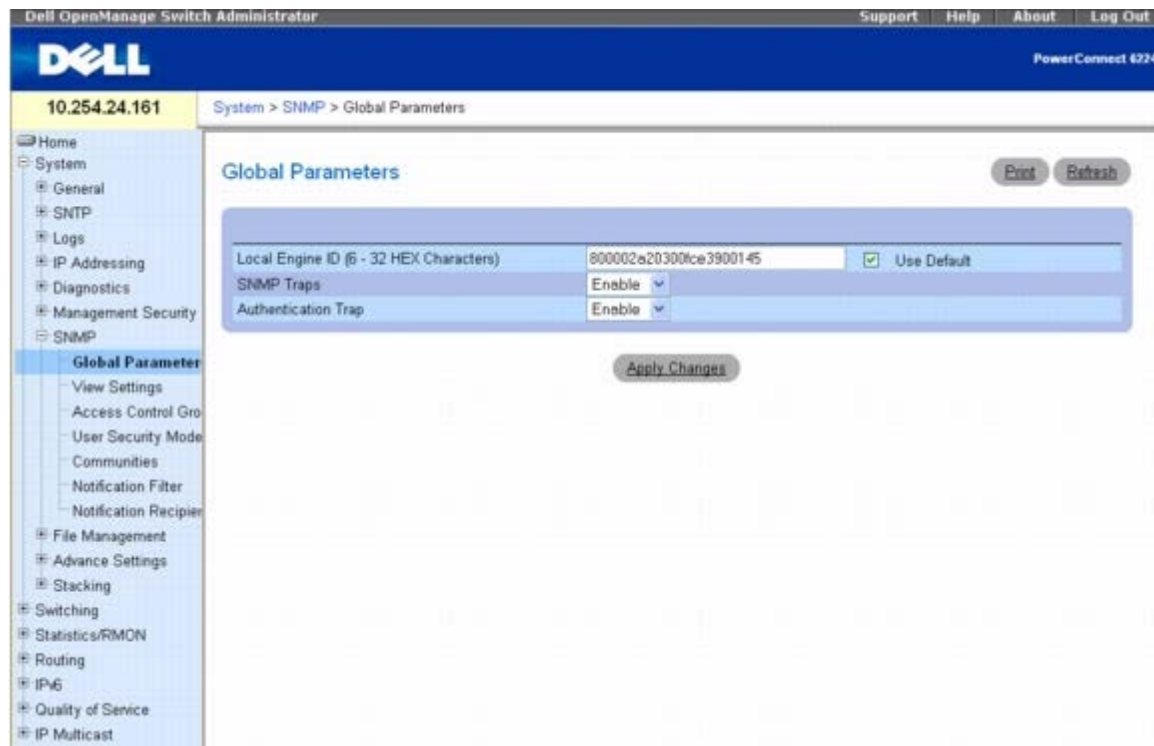
SNMP 页面用于定义 SNMP 参数。要显示 SNMP 页面，请在树视图中单击 **System (系统) ® SNMP**。

## SNMP 全局参数

**Global Parameters (全局参数)** 页面用于启用 SNMP 和验证通知。

要显示 **Global Parameters**（全局参数）页面，请在树视图中单击 **System**（系统）**»** **SNMP** **»** **Global Parameters**（全局参数）。

图 6-58. 全局参数



**Global Parameters**（全局参数）页面包含以下参数：

**Local Engine ID (6 – 32 hexadecimal character)**（本地引擎 ID [6 至 32 个十六进制字符]）— 设置本地 SNMP 引擎 ID。

**Use Default**（使用默认值）— 配置设备使用默认 SNMP 引擎 ID。

**SNMP Traps**（SNMP 陷阱）— 启用或禁用发送 SNMP 通知的设备。

**Authentication Trap**（验证陷阱）— 启用或禁用验证失败时发送 SNMP 陷阱的设备。

## 设置本地 SNMP 引擎 ID

- 打开 **Global Parameters**（全局参数）页面。
- 在 **Local Engine ID**（本地引擎 ID）字段中键入所需的十六进制 ID。
- 单击 **Apply Changes**（应用更改）。

系统将设置新的本地引擎 ID 并更新设备。

## 使用默认 SNMP 引擎 ID

- 打开 **Global Parameters**（全局参数）页面。
- 单击 **Use Default**（使用默认值）复选框。
- 单击 **Apply Changes**（应用更改）。

系统将根据 MAC 地址创建默认 SNMP 引擎 ID 并更新设备。

## 启用 SNMP 陷阱

□□□ 打开 **Global Parameters** (全局参数) 页面。

□□□ 在 **SNMP Traps** (SNMP 陷阱) 字段中选择 **Enable** (启用)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将启用 SNMP 通知并更新设备。

## 启用验证陷阱

□□□ 打开 **Global Parameters** (全局参数) 页面。

□□□ 在 **Authentication Trap** (验证陷阱) 字段中选择 **Enable** (启用)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将启用验证通知并更新设备。

## 使用 CLI 命令启用 SNMP 通知

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- SNMP 命令。

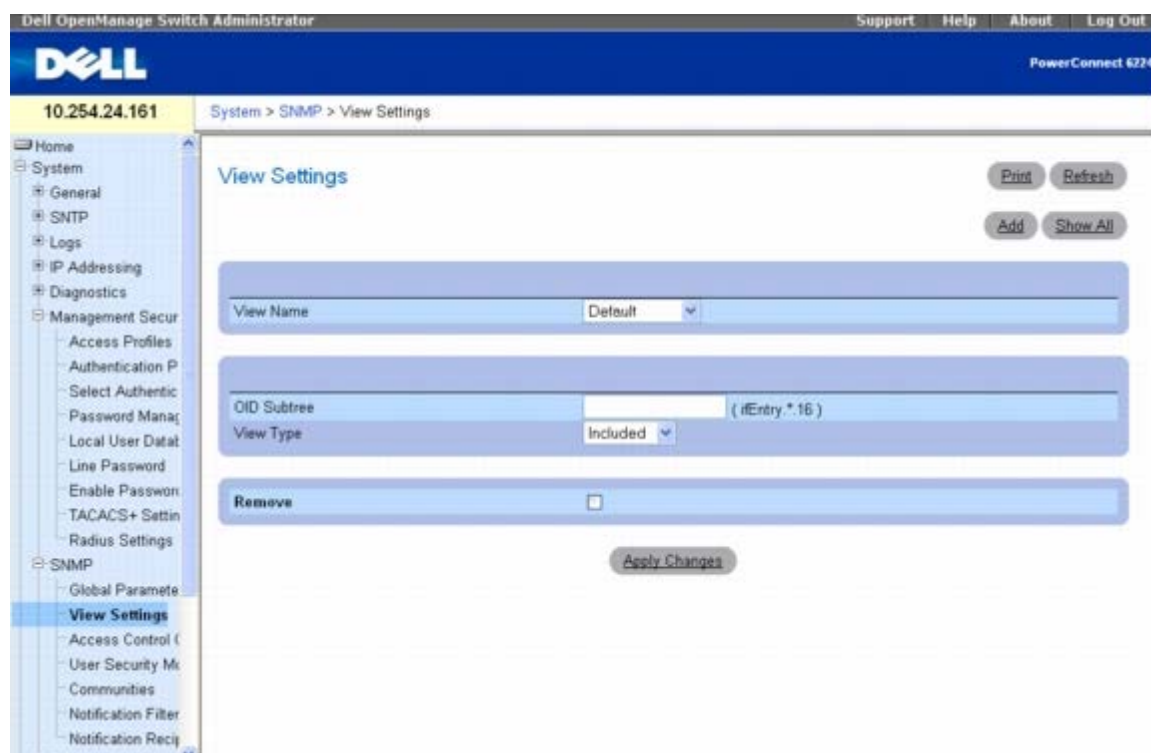
## SNMP 视图设置

此页面用于创建定义了可访问的设备功能和禁止使用的设备功能的视图。您可以创建含有或不含有对应于接口 OID 的视图。

**SNMP View Settings** (SNMP 视图设置) 页面用于定义 SNMP 视图。

要显示 **SNMP View Settings** (SNMP 视图设置) 页面，请在树视图中单击 **System** (系统) ® **SNMP** ® **View Settings** (视图设置)。

图 6-59. SNMP 视图设置



**SNMP View Settings (SNMP 视图设置)** 页面包含以下字段：

**View Name (视图名称)** — 包含用户定义的视图的列表。视图名称最多可以包含 30 个字母数字字符。

**OID Subtree (OID 子树)** — 指定有效的 SNMP OID 字符串，可包含 \* 等元字符。

**View Type (视图类型)** — 指定包含还是排除视图中的对象 ID。

**Remove (删除)** — 选中以删除显示的视图类型。

## 添加视图

□□□ 打开 **SNMP View Settings (SNMP 视图设置)** 页面。

□□□ 单击 **Add (添加)** 。

系统将显示 **Add View (添加视图)** 页面：

图 6-60. 添加视图



□□□ 定义相关的字段。

□□□ 单击 **Apply Changes (应用更改)** 。

系统将添加 SNMP 视图并更新设备。

## 显示视图表

□□□ 打开 **SNMP View Settings** (SNMP 视图设置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **View Table** (视图表) 页面：

图 6-61. 视图表



## 删除 SNMP 视图

□□□ 打开 **SNMP View Settings** (SNMP 视图设置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **View Table** (视图表) 页面。

□□□ 选择一个 SNMP 视图。

□□□ 选中 **Remove** (删除) 复选框。

□□□ 单击 **Apply Changes** (应用更改)。

系统将删除 SNMP 视图并更新设备。

## 使用 CLI 命令定义 SNMP 视图

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- SNMP 命令。

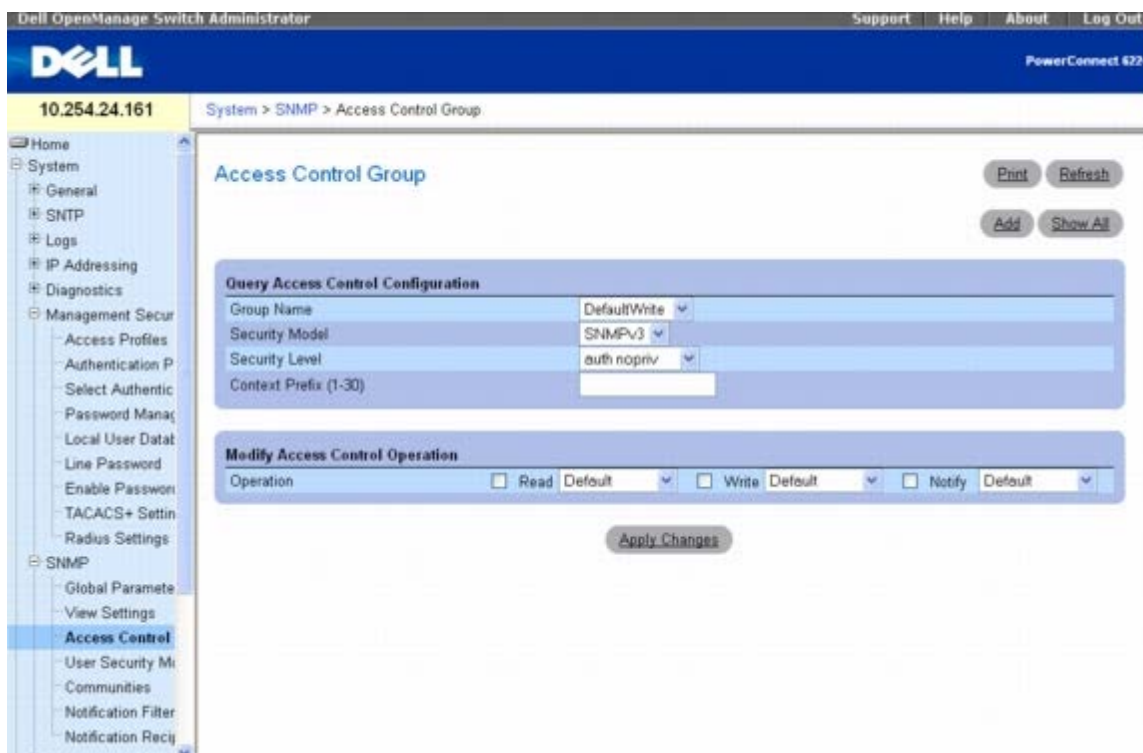
## 访问控制组

**Access Control Group** (访问控制组) 页面用于查看有关创建 SNMP 组和分配 SNMP 访问权限的信息。组允许网络管理员向特定设备功能或功能类型分配访问权限。

要显示 **Access Control Group** (访问控制组) 页面，请在树视图中单击 **System** (系统) ® **SNMP** ® **Access Control Group** (访问控制组)。

图 6-62. 访问控制组





**Access Control Group**（访问控制组）页面包含以下字段：

**Group Name**（组名称）— 包含一列用户定义的组名称，访问控制规则将应用于这些组。组名称最多可以包含 30 个字母数字字符。

**Security Model**（安全保护模式）— 定义组所具有的 SNMP 版本。可能的字段值包括：

**SNMPv1** — 组定义的是 SNMPv1。

**SNMPv2** — 组定义的是 SNMPv2。

**SNMPv3** — 组定义的是 SNMPv3 安全保护模式 (USM)。

**Security Level**（安全保护级别）— 组所具有的安全保护级别。安全保护级别仅适用于 SNMPv3 组。可能的字段值包括：

**noauth no priv** — 没有向组分配“验证”或“隐私”安全保护级别。

**auth nopriv** — 验证 SNMP 信息但不进行加密。

**auth priv** — 验证 SNMP 信息并进行加密。

**Context Prefix (1-30)**（上下文前缀 [1-30]）— 此字段使用户能够输入上下文名称的前 1 至 30 个字符来指定上下文的名称。

**Operation**（操作）— 定义组访问权限。可能的字段值包括：

**Read**（读）— 选择将管理访问限制为查看代理程序内容的视图。如果没有选择任何视图，则可以查看除团体表、SNMPv3 用户和访问表外的所有对象。

**Write**（写）— 选择允许对代理程序内容进行读/写管理访问的视图。

**Notify**（通知）— 选择允许发送 SNMP 陷阱或通告的视图。

## 添加 SNMP 组

□□□ 打开 **Access Control Configuration**（访问控制配置）页面。

□□□ 单击 **Add**（添加）。

系统将显示 **Add an Access Control Configuration**（添加访问控制配置）页面：



图 6-63. 添加访问控制配置

□□□ 根据需要定义各个字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将添加组并更新设备。

## 显示访问表

□□□ 打开 **Access Control Configuration** (访问控制配置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Access Table** (访问表) 页面：

图 6-64. 访问表

Group Name	Context Prefix	SNMP Version	Security Level	Read	Write	Notify	Remove
1 DefaultRead		SNMPV1	NoAuth NoPriv	Default		Default	<input type="checkbox"/>
2 DefaultRead		SNMPV2	NoAuth NoPriv	Default		Default	<input type="checkbox"/>
3 DefaultSuper		SNMPV1	NoAuth NoPriv	DefaultSuper	DefaultSuper	DefaultSuper	<input type="checkbox"/>
4 DefaultSuper		SNMPV2	NoAuth NoPriv	DefaultSuper	DefaultSuper	DefaultSuper	<input type="checkbox"/>
5 DefaultWrite		SNMPV1	NoAuth NoPriv	Default	Default	Default	<input type="checkbox"/>
6 DefaultWrite		SNMPV2	NoAuth NoPriv	Default	Default	Default	<input type="checkbox"/>

## 删除组

□□□ 打开 **Access Control Configuration** (访问控制配置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将打开 **Access Table** (访问表)。

□□□ 选择一个组。

□□□ 选中 **Remove** (删除) 复选框。

□□□ 单击 **Apply Changes** (应用更改)。

系统将删除组并更新设备。

## 使用 CLI 命令定义 SNMP 访问控制

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

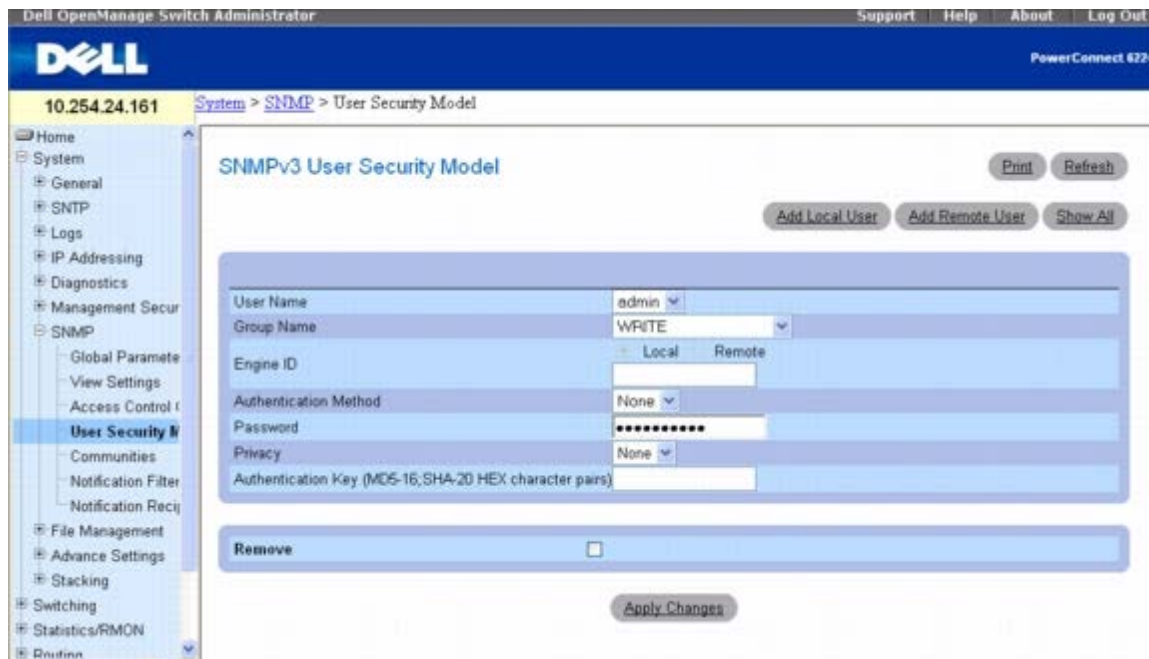
- SNMP 命令。

## SNMPv3 用户安全保护模式 (USM)

**SNMPv3 User Security Model (USM) (SNMPv3 用户安全保护模式 [USM])** 页面用于为 SNMP 组分配系统用户和定义用户验证方法。

要显示 **SNMPv3 User Security Model (USM) (SNMPv3 用户安全保护模式 [USM])** 页面，请在树视图中单击 **System (系统) @ SNMP @ User Security Model (用户安全保护模式)**。

图 6-65. SNMPv3 用户安全保护模式 (USM)



**SNMPv3 User Security Model (USM) (SNMPv3 用户安全保护模式 [USM])** 页面包含以下字段：

**User Name** (用户名) — 包含用户定义的用户名列表。

**Group Name** (组名称) — 包含用户定义的 SNMP 组列表。SNMP 组在 **Access Control Group (访问控制组)** 页面中定义。

**Engine ID** (引擎 ID) — 选择所选用户是否与本地或特定远程 SNMPv3 设备关联。

Remote Engine ID (远程引擎 ID) — 表示用户配置于远程 SNMPv3 设备。

**Authentication Method** (验证方法) — 指定用来验证用户的验证方法。可能的字段值包括：

**None** (无) — 不使用用户验证。

**MD5** — 使用 HMAC-MD5-96 验证级别验证用户。用户应指定一个密码。

**SHA** — 使用 HMAC-SHA-96 验证级别验证用户。用户应输入一个密码。

**Password** (密码) — 修改用户为组定义的密码。密码最多可以包含 32 个字符。仅当验证方法为 MD5 或 SHA 密码，才可以定义密码。您需要在 **Add Local User (添加本地用户)** 页面中定义密码。

**Privacy** (隐私) — 指定是否使用验证密钥。选择以下值之一：

**None** (无) — 不使用验证密钥。

**des** — 对验证密钥使用 CBC-DES 对称加密密码。

**des-key** (des 密钥) — 使用预生成的 HMAC-MD5-96 验证密钥。

**Authentication Key (MD5-16; SHA-20 HEX character pairs)** (验证密钥 [MD5-16; SHA-20 十六进制字符对]) — 指定验证密钥。只有验证方法为 MD5 或 SHA，才会定义验证密钥。

**Remove** (删除) — 如果选择该选项，将从指定组中删除指定用户。

## 向组添加 **SNMPv3** 本地用户

□□□ 打开 **SNMPv3 User Security Model** (**SNMPv3** 用户安全保护模式) 页面。

□□□ 单击 **Add Local User** (添加本地用户)。

系统将显示 **Add Local User** (添加本地用户) 页面：

图 6-66. 添加本地用户

The screenshot shows the 'Add Local User' configuration page. It features a title bar with 'Add Local User' and 'Exit' and 'Refresh' buttons. The main form area contains several fields: 'LocalEngineID' with the value '800002x20300fe3900145', 'User Name (1-32 characters)', 'Group Name' set to 'DefaultRead', 'Authentication Method' set to 'None', 'Password (1-32 characters)', 'Privacy' set to 'None', and 'Authentication Key (MD5-16, SHA-20 HEX character pairs)'. At the bottom of the form are 'Apply Changes' and 'Back' buttons.

□□□ 定义相关的字段。

□□□ 单击 **Apply Changes** (应用更改)。

□□□ 系统会将用户添加至组并更新设备。

## 向组添加 **SNMPv3** 远程用户

□□□ 打开 **SNMPv3 User Security Model** (**SNMPv3** 用户安全保护模式) 页面。

□□□ 单击 **Add Remote User** (添加远程用户)。

系统将显示 **Add Remote User** (添加远程用户) 页面：

图 6-67. 添加远程用户

The screenshot shows the 'Add Remote User' configuration page. It features a title bar with 'Add Remote User' and 'Exit' and 'Refresh' buttons. The main form area contains several fields: 'Remote Engine ID (6-32 HEX Characters)', 'User Name (1-32 characters)', 'Group Name' set to 'DefaultRead', 'Authentication Method' set to 'None', 'Password (1-32 characters)', 'Privacy' set to 'None', and 'Authentication Key (MD5-16, SHA-20 HEX character pairs)'. At the bottom of the form are 'Apply Changes' and 'Back' buttons.

□□□ 定义相关的字段。

□□□ 单击 **Apply Changes**（应用更改）。

□□□ 系统会将用户添加至组并更新设备。

## 查看用户安全保护模式表

□□□ 打开 **SNMPv3 User Security Model (USM)**（SNMPv3 用户安全保护模式 [USM]）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **User Security Model Table**（用户安全保护模式表）。

图 6-68. 用户安全保护模式表

User Name	Group Name	Remote Engine ID	Authentication	Remove
1 Admin	DefaultRead	800002a20300fc:e3900145	NONE	<input type="checkbox"/>
2 pppin	DefaultRead	800002a20300fc:e3900145	NONE	<input type="checkbox"/>
3 gandaf	DefaultRead	800002a20300fc:e3900145	NONE	<input type="checkbox"/>

## 删除用户安全保护模式表条目

□□□ 打开 **User Security Model**（用户安全保护模式）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **User Security Model Table**（用户安全保护模式表）页面。

□□□ 选择一个条目。

□□□ 选中 **Remove**（删除）复选框。

□□□ 单击 **Apply Changes**（应用更改）。

系统将删除条目并更新设备。

## 使用 CLI 命令定义 SNMP 用户

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

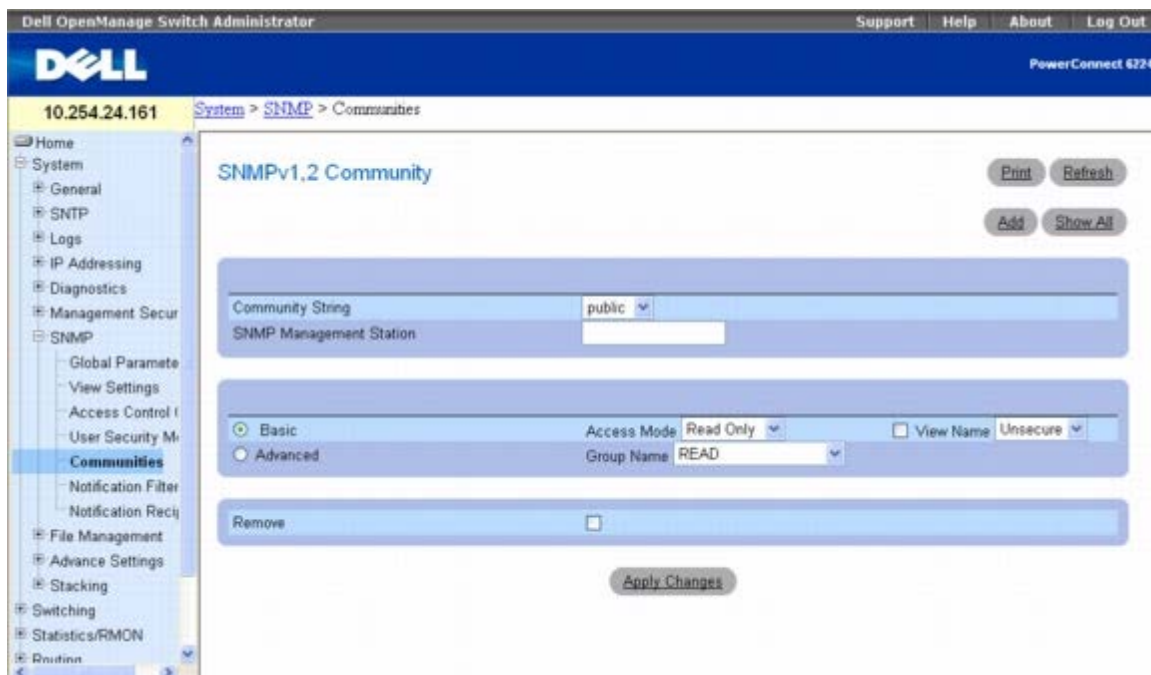
- SNMP 命令。

## 团体

通过在 **SNMPv1,2 Community**（SNMPv1,2 团体）页面中定义团体来对访问权限进行管理。更改团体名称时，访问权限也随之更改。SNMP 团体只能对 SNMP v1 和 SNMP v2 进行定义。

要显示 **SNMPv1,2 Community**（SNMPv1,2 团体）页面，请在树视图中单击 **System**（系统）® **SNMP**® **Communities**（团体）。

图 6-69. SNMPv1,2 团体



SNMPv1,2 Community (SNMPv1,2 团体) 页面包含以下字段：

**Community String** (团体字符串) — 包含用户定义的团体字符串列表，这些字符串用作向设备验证 SNMP 管理站的密码。团体字符串最多可以包含 20 个字符。

**SNMP Management Station** (SNMP 管理站) — 包含团体字符串所定义的管理站 IP 地址列表。

**Basic** (基本) — 为所选团体启用 SNMP 基本模式。可能的字段值包括：

**Access Mode** (访问模式) — 定义团体的访问权限。可能的字段值包括：

**Read-Only** (只读) — 团体对视图中配置的 MIB 对象拥有只读访问。

**Read-Write** (读/写) — 团体对视图中配置的 MIB 对象拥有读/修改访问。

**Super User** (超级用户) — 团体对所有 MIB 对象拥有读/修改访问。

**View Name** (视图名称) — 包含用户定义的视图的列表。

**Advanced** (高级) — 包含用户定义的组列表。如果选择了 SNMP 高级模式，所选团体将启用组所对应的 SNMP 访问控制规则。在高级模式中，可以对特定 SNMP 团体启用 SNMP 组。SNMP 高级模式只能对 SNMPv3 进行定义。

**Remove** (删除) — 如果选择该选项，将删除团体。

## 添加新团体

□□□ 打开 **SNMPv1,2 Community** (SNMPv1,2 团体) 页面。

□□□ 单击 **Add** (添加)。

系统将显示 **Add SNMPv1,2 Community** (添加 SNMPv1,2 团体) 页面：

图 6-70. 添加 SNMPv1,2 团体

□□□ 填写相关字段。

除 **SNMPv1,2 Community** (**SNMPv1,2** 团体) 页面中的字段外, **Add SNMPv1,2 Community** (添加 **SNMPv1,2** 团体) 页面还包含 **All (0.0.0.0)** (所有 **[0.0.0.0]**) 字段, 表示团体可以用于任何管理站。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存新团体并更新设备。

## 显示团体

□□□ 打开 **SNMPv1,2 Community** (**SNMPv1,2** 团体) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Basic Table** (基本表) 页面。

图 6-71. 基本表

Management Station	Community String	Access Mode	View Mode	Remove
1 All	private	Read Only	Default	<input type="checkbox"/>
2 All	public	Read Write	Default	<input type="checkbox"/>

Community String	Management Station	Group Name
1 private	All	DefaultRead
2 public	All	DefaultWrite

## 删除团体

□□□ 打开 **SNMPv1,2 Community** (**SNMPv1,2** 团体) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Basic Table** (基本表) 页面。

□□□ 选择一个团体并选中 **Remove** (删除) 复选框。

□□□ 单击 **Apply Changes** (应用更改)。

系统将删除团体条目并更新设备。

## 使用 CLI 命令配置团体

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- SNMP 命令。

## 通知筛选器

**Notification Filter**（通知筛选器）页面用于根据 OID 设置筛选陷阱。每个 OID 都与某种设备功能或功能类型关连。**Notification Filter**（通知筛选器）页面还可以筛选通知。



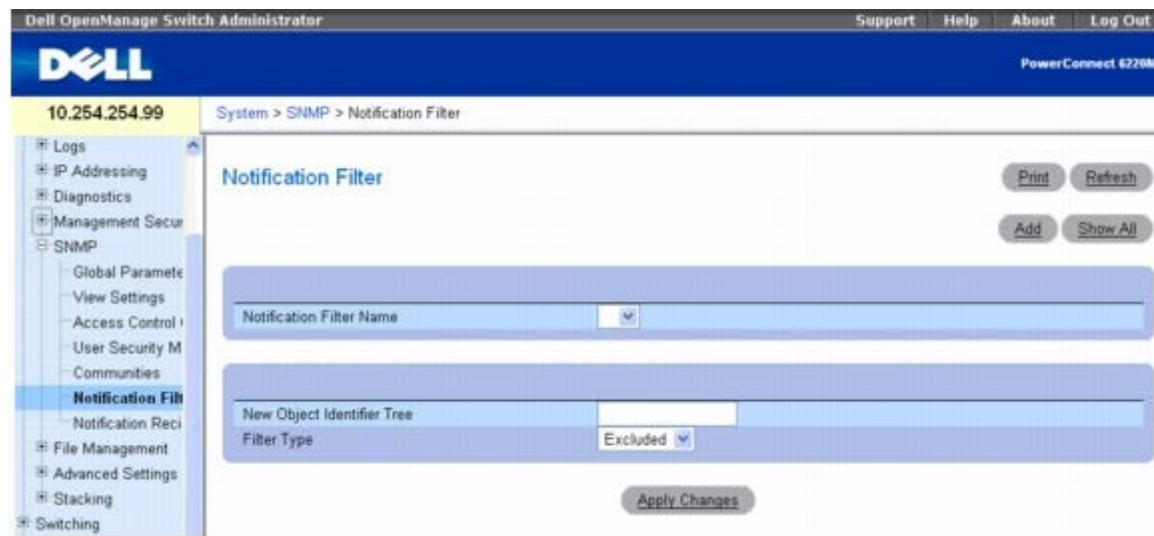
要显示 **Notification Filter**（通知筛选器）页面，请在树视图中单击 **System**（系统） **SNMP**  **Notification Filter**（通知筛选器）。

图 6-72. 通知筛选器



**Notification Filter**（通知筛选器）页面包含以下字段：

**Notification Filter Name**（通知筛选器名称）— 包含用户定义的通知筛选器列表。通知筛选器名称最多可以包含 30 个字符。

**New Object Identifier Tree**（新对象标识符树）— 显示了为所选筛选器配置的 OID。此字段可以编辑。

**Filter Type**（筛选器类型）— 表示是否向陷阱接收设备发送关于 OID 的通告或陷阱。

**Excluded**（排除）— 禁止发送 OID 陷阱或通告。

**Included**（包含）— 发送 OID 陷阱或通告。

## 添加 SNMP 筛选器

□□□ 打开 **Notification Filter**（通知筛选器）页面。

□□□ 单击 **Add**（添加）。

系统将显示 **Add Filter**（添加筛选器）页面：

图 6-73. 添加筛选器



Filter Name (1 - 30 characters)	UserFilter1
New Object Identifier Tree	1.3.6.1.2.1.1.7
Filter Type	Included

□□□ 定义相关的字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将添加新的筛选器并更新设备。

## 显示筛选器表

□□□ 打开 **Notification Filter**（通知筛选器）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **Filter Table**（筛选器表）页面，上面显示了为所选筛选器名称配置的所有筛选器：

图 6-74. 显示通知

Object ID Subtree	Filter Type	Remove
-------------------	-------------	--------

## 删除筛选器

□□□ 打开 **Notification Filter**（通知筛选器）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **Show Notification**（显示通知）页面。

□□□ 选择 **Filter Table**（筛选器表）条目。

□□□ 选中 **Remove**（删除）复选框。

系统将删除筛选器条目并更新设备。

## 使用 CLI 命令配置通知筛选器

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- SNMP 命令。



## 通知接收设备

**Notification Recipients**（通知接收设备）页面用于查看信息以定义筛选器，从而确定是否向特定的用户发送陷阱以及所发送的陷阱类型。SNMP 通知筛选器提供以下服务：

- 识别管理陷阱目标
- 筛选陷阱
- 选择陷阱生成参数
- 提供访问控制检查

要显示 **Notification Recipients**（通知接收设备）页面，请在树视图中单击 **System**（系统）® **SNMP** ® **Notification Recipient**（通知接收设备）。

图 6-75. 通知接收设备

**Notification Recipients**（通知接收设备）页面包含以下字段：

**Recipient IP**（接收设备 IP）— 包含用户定义的通知接收设备 IP 地址列表。

**Notification Type**（通知类型）— 发送的通知类型。可能的字段值包括：

**Trap**（陷阱）— 发送陷阱。

**Inform**（通告）— 发送通告。

**SNMPv1,2**— 为所选的接收设备启用 SNMP 版本 1 或版本 2。可能的字段值包括：

**Community String**（团体字符串）— 显示与通知一起发送的团体字符串。

**Notification Version**（通知版本）— 确定通知的版本。可能的字段值包括：

**SNMP V1**— 发送 SNMP 版本 1 陷阱。如果选择的通知类型为通告，则无法选择 SNMPv1。

**SNMP V2**— 发送 SNMP 版本 2 陷阱。

**SNMPv3**— 为所选的接收设备启用 SNMP 版本 3。可能的字段值包括：

**User Name** (用户名) — 选择现有的用户以生成通知。

**Security Level** (安全保护级别) — 通知具有的安全保护级别。可能的字段值包括：

**NoAu NoPriv**— 不验证或加密信息包。

**Auth NoPriv**— 验证信息包。

**Auth Priv**— 验证并加密信息包。

**UDP Port (1-65535)** (UDP 端口 [1-65535]) — 使用 UDP 端口发送通知。默认值为 162。

**Filter Name** (筛选器名称) — 选择此复选框可向通知应用用户定义的 SNMP 筛选器 (从下拉式菜单中选择)。

**Timeout (1-300)** (超时 [1-300]) — 发送通知前设备等待的时间 (秒)。默认值为 15 秒。

**Retries (1-255)** (重试 [1-255]) — 设备重发通告请求的最高次数。默认值为 3。

## 添加新的通知接收设备

□□□ 打开 **Notification Recipients** (通知接收设备) 页面。

□□□ 单击 **Add** (添加)。

系统将显示 **Notification Recipients** (通知接收设备) 页面：

图 6-76. 添加通知接收设备

□□□ 定义相关的字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将添加通知接收设备并更新设备。

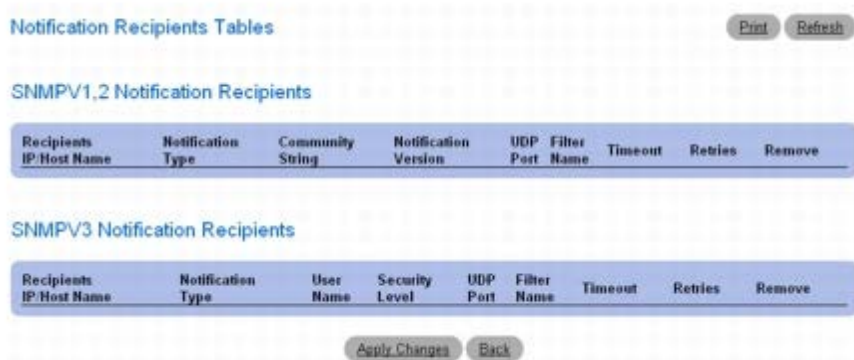
## 显示通知接收设备表

□□□ 打开 **Notification Recipients** (通知接收设备) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将打开 **Notification Recipient Tables** (通知接收设备表) 页面：

图 6-77. 通知接收设备表



## 删除通知接收设备

□□□ 打开 **Notification Recipients**（通知接收设备）页面。

□□□ 单击 **Show All**（全部显示）。

系统将打开 **Notification Recipient Tables**（通知接收设备表）页面。

□□□ 为 **SNMPV1,2 Notification Recipient**（SNMPV1,2 通知接收设备）和/或 **SNMPv3 Notification Recipient Tables**（SNMPv3 通知接收设备表）中的一个或多个通知接收设备选中 **Remove**（删除）复选框。

□□□ 单击 **Apply Changes**（应用更改）。

系统将删除接收设备并更新设备。

## 使用 CLI 命令定义 SNMP 通知接收设备

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- SNMP 命令。

## 管理文件

**File Management**（文件管理）菜单页面用于管理设备软件、映像文件和配置文件。文件可通过 TFTP 服务器下载或加载。系统处理两种版本的软件。运行较旧软件版本的系统将忽略（不加载）较新软件版本所生成的配置文件。当运行较旧软件版本的系统发现由配置较新软件版本所生成的文件时，系统将向用户显示一则相应的警告。

## 管理文件概览

管理文件结构由以下文件组成：

- 启动配置文件 — 在设备断电或重新引导时维护完整的设备配置。启动文件可以维护配置命令，并且正在运行的配置文件中的配置命令可以保存到启动文件。
- 正在运行的配置文件 — 包含所有启动文件命令以及在当前会话过程中输入的所有命令。设备断电或重新引导后，所有存储在正在运行的配置文件中的命令均会丢失。启动期间，启动文件中的所有命令将被复制到正在运行的配置文件中，并应用于设备。会话期间，输入的所有新命令将被添加到正在运行的配置文件中存在的命令中。命令不会被覆盖。要更新启动文件，必须先将正在运行的配置文件复制到启动配置文件中，然后再断开设备的电源连接。下次重新启动设备时，这些命令将从启动配置文件复制回正在运行的配置文件中。

- 备份配置文件 — 包含设备配置的备份副本。正在运行的配置文件或启动文件被复制到备份文件时，备份文件将发生更改。复制到备份文件的命令将替换备份文件中保存的现有命令。可以将备份文件的内容复制到正在运行的配置文件或启动配置文件中。也可以将内容从远程 TFTP 服务器复制到备份文件和启动文件，或者从备份文件和启动文件复制到远程服务器。
- 映像文件 — 系统映像被保存到两个称为映像（映像 1 和映像 2）的快擦写存储器扇区中。活动映像存储活动副本，另一个映像存储次副本。设备从活动映像进行引导并运行。如果活动映像损坏，系统将自动从非活动映像进行引导。这种安全功能可用于防止引导升级过程中出现故障。

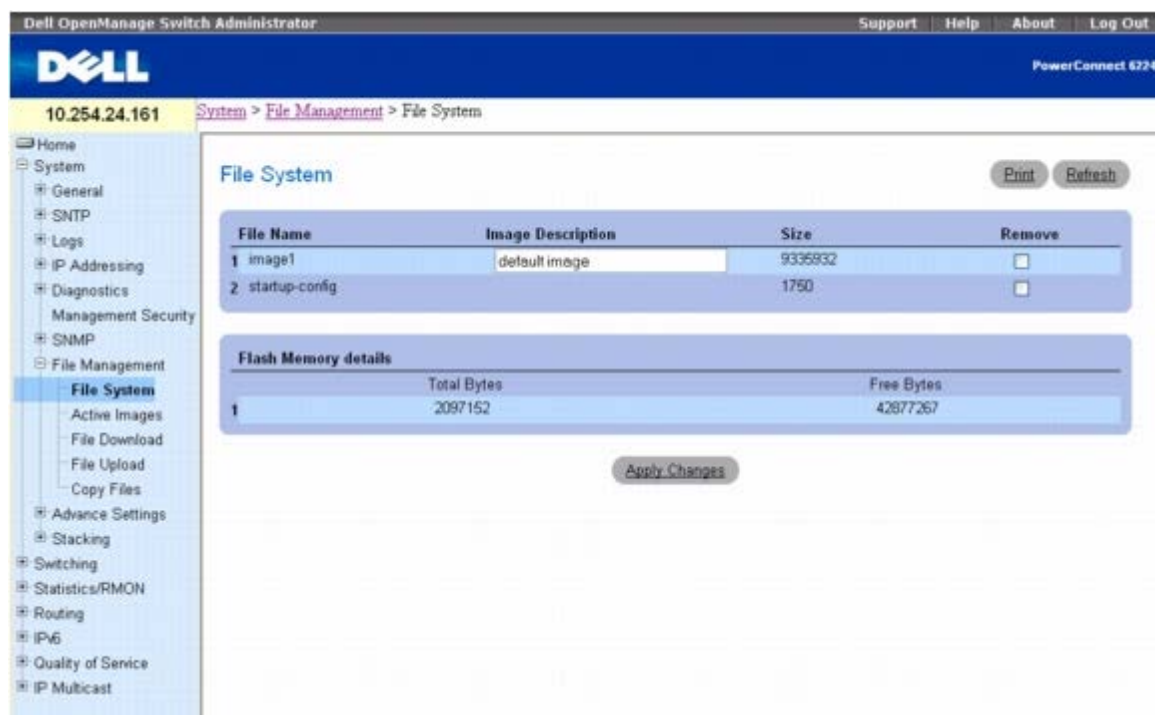
要显示 **File Management**（文件管理）页面，请在树视图中单击 **System**（系统）® **File Management**（文件管理）。

## 文件系统

**File System**（文件系统）页面用于查看设备上的文件列表。

要显示 **File System**（文件系统）页面，请在树视图中单击 **System**（系统）® **File Management**（文件管理）® **File System**（文件系统）。

图 6-78. 文件系统



**File System**（文件系统）页面包含以下字段：

**File Name**（文件名）— 文件系统中文件的名称列表。

**Image Description (0-128)**（映像说明 **[0-128]**）— 此字段用于配置和显示映像说明。最多可以输入 128 个字符的说明。

**Size**（大小）— 显示所指定的文件的大小。

**Remove**（删除）— 选择以删除指定的文件。

**Flash Memory Details**（快擦写存储器详情）— 显示快擦写存储器的状况。

**Total Bytes**（总计字节）— 显示当前使用的快擦写存储器容量。

**Free Bytes**（可用字节）— 显示可用的快擦写存储器容量。

## 删除文件

□□□ 打开 **File System**（文件系统）页面。

□□□ 使用 **File Name**（文件名）字段选择要删除的文件。

□□□ 选中 **Remove**（删除）复选框。

□□□ 单击 **Apply Changes**（应用更改）。

系统即删除文件。

## 使用 CLI 命令查看文件

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

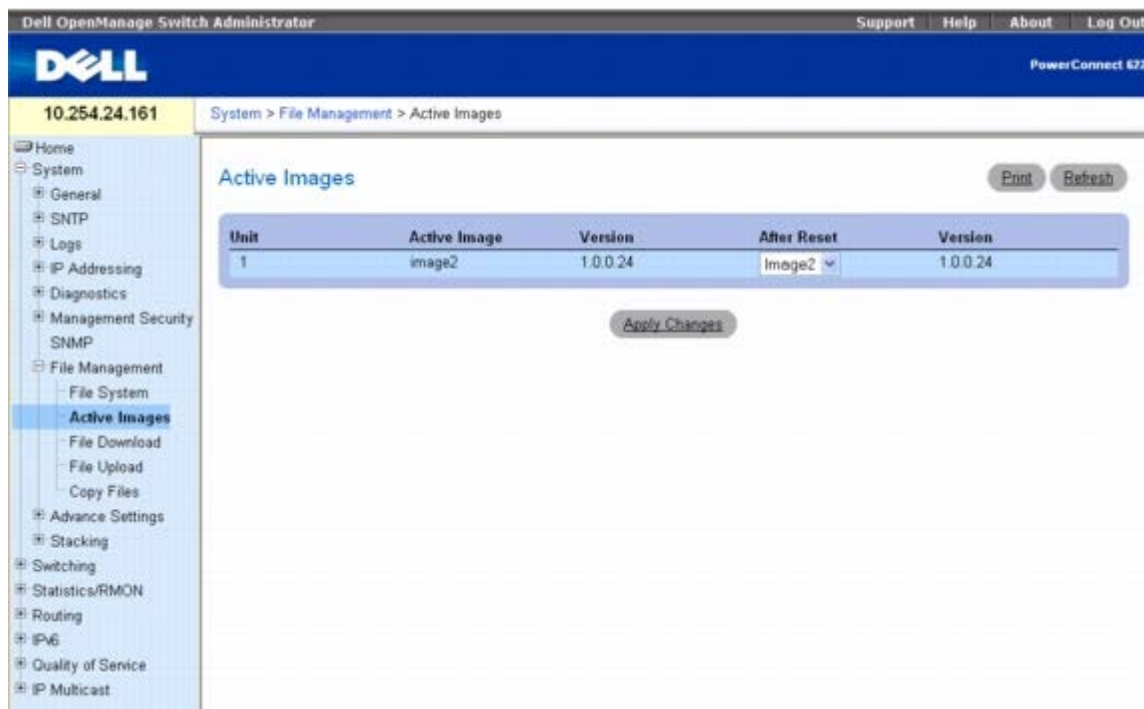
- 配置和映像文件命令

## 活动映像

**Active Image**（活动映像）页面用于设置引导映像。

要显示 **Active Image**（活动映像）页面，请在树视图中单击 **System**（系统）® **File Management**（文件管理）® **Active Image**（活动映像）。

图 6-79. 活动映像



**Active Image**（活动映像）页面包含以下字段：

**Unit**（单元）— 表示堆栈内的系统的单元编号。

**Active Image**（活动映像）— 显示当前活动映像的名称。

**Version**（版本）— 显示当前活动映像的版本号。

**After Reset**（重置后）— 从下拉式菜单中选择在下一次重置后激活的映像。

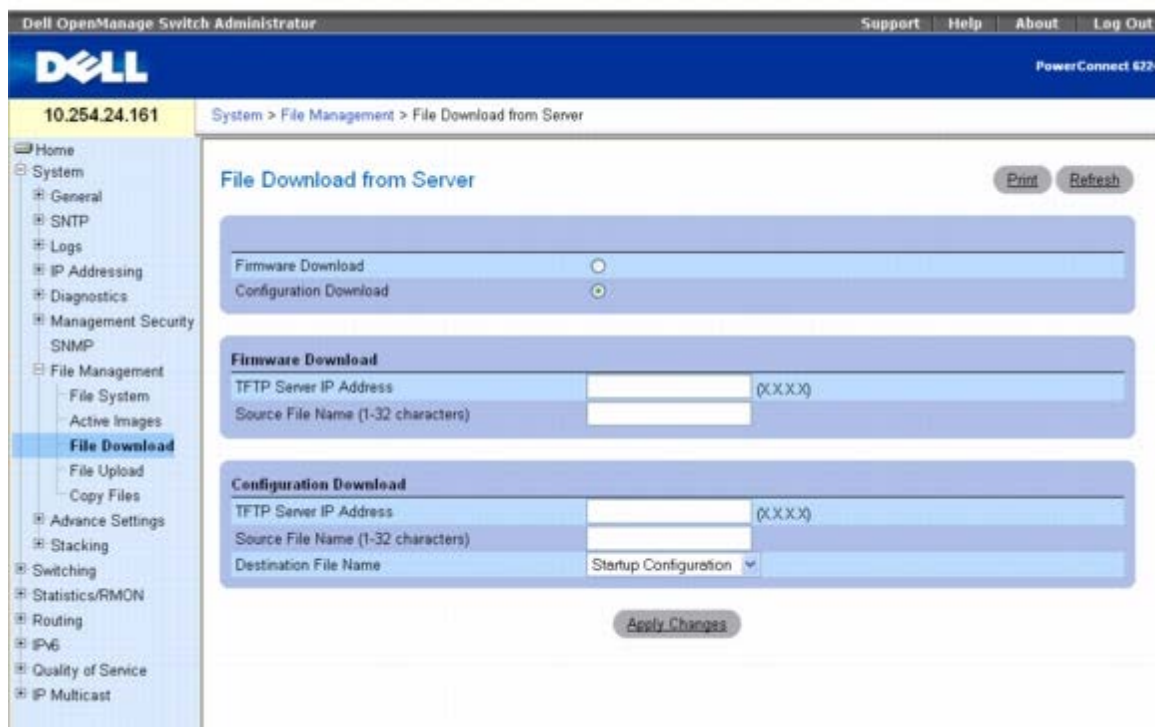
**Version** (版本) — 显示要在下一次重置后激活的映像的版本号。

## 从服务器下载文件

**File Download From Server** (从服务器下载文件) 页面用于从 TFTP 服务器将配置 (ASCII) 和映像 (二进制) 文件下载到设备。

要显示 **File Download From Server** (从服务器下载文件) 页面，请在树视图中单击 **System** (系统) ® **File Management** (文件管理) ® **File Download** (文件下载)。

图 6-80. 从服务器下载文件



**File Download From Server** (从服务器下载文件) 页面包含以下字段：

**Firmware Download** (固件下载) — 如果选择，表示将下载固件文件。选择此选项后，**Configuration Download** (配置下载) 字段将呈灰色。

**Configuration Download** (配置下载) — 如果选择，表示将下载配置文件。如果选择了 **Configuration Download** (配置下载)，**Firmware Download** (固件下载) 字段将呈灰色。

### 固件下载

**TFTP Server IP Address** (TFTP 服务器 IP 地址) — 要下载的固件文件所在的 TFTP 服务器 IP 地址。

**Source File Name (1 – 32 characters)** (源文件名 [1 至 32 个字符]) — TFTP 服务器上的文件的文件名，并带有相对于 tftpboot 目录的路径。例如，如果在远程服务器上配置了 TFTP，且 tftpboot 目录为 `e:\tftp`，文件 `test.scr` 位于 `e:\tftp\latest\test.scr`，则输入 `\latest\test.scr`。

### 配置下载

**TFTP Server IP Address** (TFTP 服务器 IP 地址) — 要下载的配置文件所在的 TFTP 服务器 IP 地址。

**Source File Name (1 – 32 characters)** (源文件名 [1 至 32 个字符]) — TFTP 服务器上的文件的名称。

**Destination File Name** (目的地文件名) — 存放下载的配置文件的目的地文件。可能的值包括：



**Startup Configuration**（启动配置）— 下载启动配置文件。

**Backup Configuration**（备份配置）— 下载备份配置文件。

## 下载文件

□□□ 打开 **File Download From Server**（从服务器下载文件）页面。

□□□ 检验 TFTP 服务器的 IP 地址，并确保要下载的软件映像或引导文件存在于 TFTP 服务器上。

□□□ 填写 **TFTP Server IP Address**（TFTP 服务器 IP 地址）和 **Source File Name**（源文件名）（不带 TFTP 服务器 IP 地址）字段。

 **注：**建议您不要覆盖活动映像。

□□□ 单击 **Apply Changes**（应用更改）。


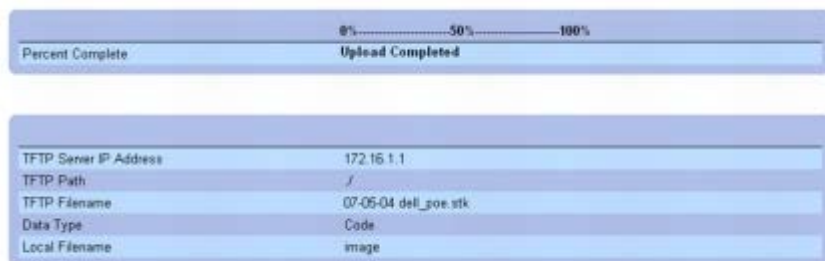
 **注：**开始下载文件之后，页面会刷新，并会显示一个传输状态字段以表明已传输的字节数。在下载完文件之前，Web 界面会一直被禁用。

图 6-81. 文件下载进度



软件将被下载到设备。

## 使用 CLI 命令下载文件

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 配置和映像文件命令。

## 文件加载

**File Upload to Server**（将文件加载至服务器）页面用于从设备将配置（ASCII）和映像（二进制）文件下载到 TFTP 服务器。

要显示 **File Upload to Server**（将文件加载至服务器）页面，请在树视图中单击 **System**（系统）® **File Management**（文件管理）® **File Upload**（文件加载）。

图 6-82. 将文件加载至服务器



The screenshot shows the 'File Upload to Server' configuration page in the Dell OpenManage Switch Administrator. The page is divided into three main sections: 'Firmware Upload', 'Software Image Upload', and 'Configuration Upload'. Each section has input fields for 'TFTP Server IP Address' and 'Destination File Name'. The 'Configuration Upload' section also has a 'Transfer File Name' dropdown menu. The interface includes a navigation sidebar on the left and a top navigation bar with 'Support', 'Help', 'About', and 'Log Out' links.

**File Upload to Server** (将文件加载至服务器) 页面包含以下字段：

**Firmware Upload** (固件加载) — 表示加载固件文件。如果选择了 **Firmware Upload** (固件加载)，则 **Configuration Upload** (配置加载) 字段将呈灰色。

**Configuration Upload** (配置加载) — 表示加载配置文件。如果选择了 **Configuration Upload** (配置加载)，**Firmware Upload** (固件加载) 字段将呈灰色。

### 软件映像加载

**TFTP Server IP Address** (TFTP 服务器 IP 地址) — 加载软件映像的 TFTP 服务器 IP 地址。

**Destination File Name (1 – 32 characters)** (目的地文件名 [1 至 32 个字符]) — 文件加载后所具有的名称。

**Transfer File Name** (传输文件名称) — 选择要加载的源文件。

### 配置加载

**TFTP Server IP Address** (TFTP 服务器 IP 地址) — 加载配置文件的 TFTP 服务器 IP 地址。

**Destination File Name (1 – 32 characters)** (目的地文件名 [1 至 32 个字符]) — 文件加载后所具有的名称。

**Transfer File Name** (传输文件名称) — 选择要加载的源文件。有效的字段值包括：

**Running Configuration** (运行的配置) — 加载正在运行的配置文件。

**Startup Configuration** (启动配置) — 加载启动配置文件。

**Backup Configuration** (备份配置) — 加载备份配置文件。

### 加载文件

□□□ 打开 **File Upload to Server** (将文件加载至服务器) 页面。

□□□ 定义对话框中的适用字段。

□□□ 单击 **Apply Changes**（应用更改）。


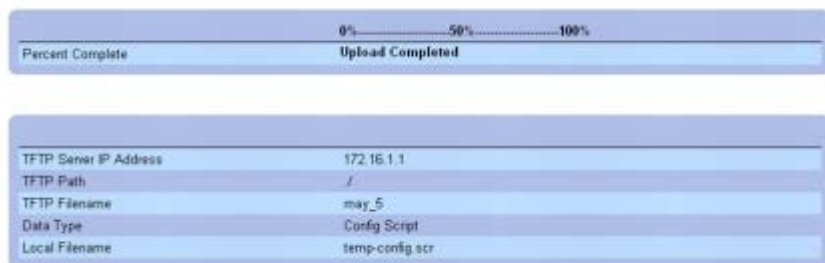
 **注：**开始加载文件之后，页面会刷新，并会显示一个传输状态字段以表明已传输的字节数。在加载完文件之前，Web 界面会一直被禁用。

图 6-83. 文件加载进度



软件将被加载到服务器。

## 使用 CLI 命令加载文件

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 配置和映像文件命令。

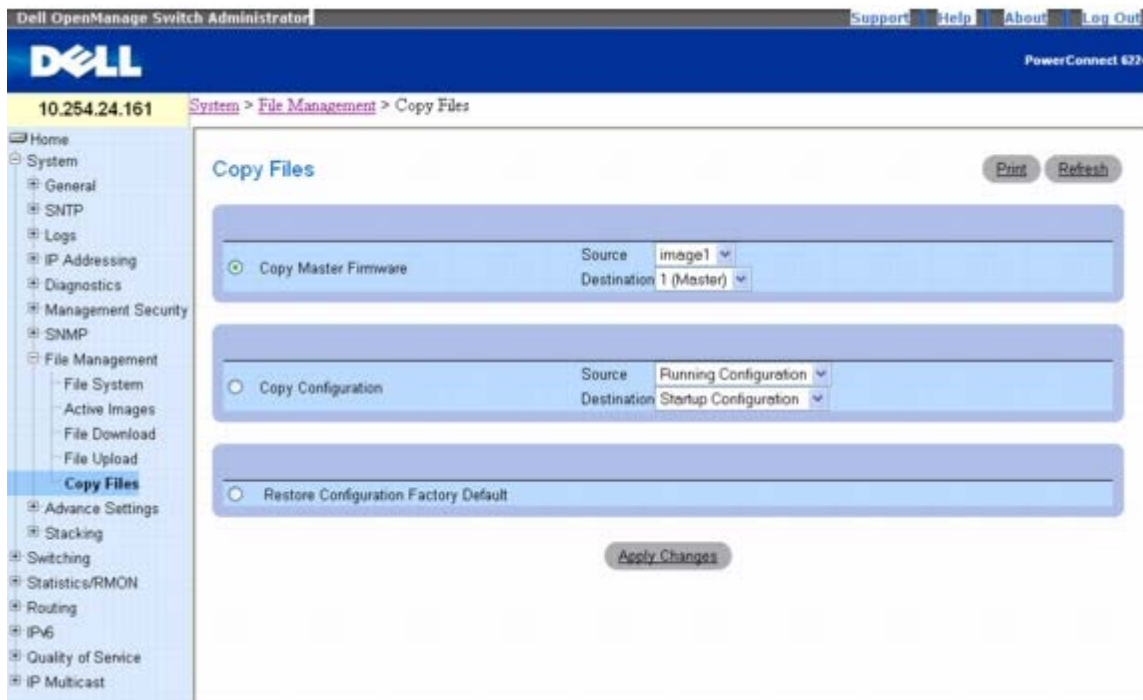
## 复制文件

“Copy Files（复制文件）”网页可用于：

- 在文件系统内复制映像
- 向远程服务器复制映像和从远程服务器复制映像
- 将图像备份至本地或远程系统
- 从本地或远程系统恢复映像
- 在文件系统内备份配置文件

要显示 **Copy Files**（复制文件）页面，请在树视图中单击 **System**（系统）® **File Management**（文件管理）® **Copy File**（复制文件）。

图 6-84. 复制文件



**Copy Files**（复制文件）页面包含以下字段：

**Copy Master Firmware**（复制主固件）— 指定复制软件映像文件。

**Source**（源）— 复制文件时使用的来源软件映像文件。

**Destination**（目的地）— 文件复制到的目的地单元。

**Copy Configuration**（复制配置）— 指定复制配置文件。

**Source**（源）— 复制文件时使用的来源配置文件（运行中的、启动、备份）。

**Destination**（目的地）— 复制文件时使用的目的地配置文件（运行中的、启动、备份）。

**Restore Configuration Factory Defaults**（恢复配置出厂默认值）— 如果选择该选项，将指定应重置出厂默认配置文件。如果未选取，则保留当前的配置设置。

## 复制文件

□□□ 打开 **Copy Files**（复制文件）页面。

□□□ 选择 **Copy**（复制）或 **Restore**（恢复）并填写相应字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统即复制文件。

## 使用 CLI 命令复制文件

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 配置和映像文件命令

## 定义高级设置

高级设置用于设置设备的其它全局属性。只有在设备重置之后，才能应用对这些属性所作的更改。请在树视图中单击 **System**（系统）® **Advanced Settings**（高级设置）以显示 **Advanced Settings**（高级设置）页面。

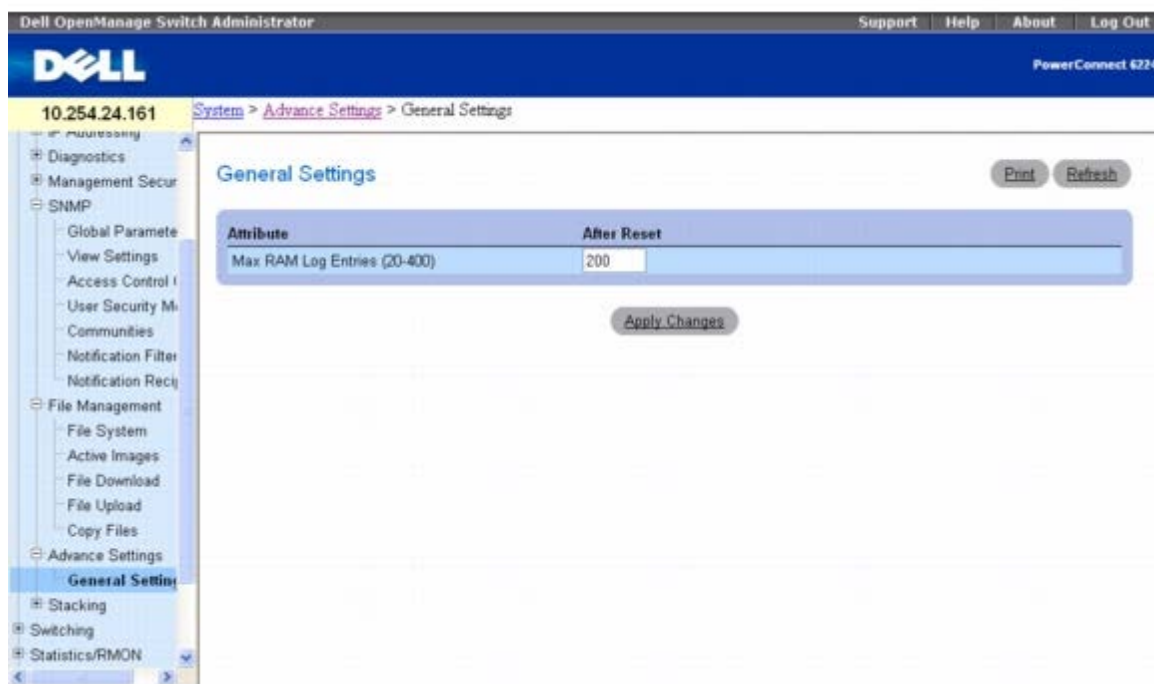
**Advanced Settings**（高级设置）页面包含用于配置常规设置的链接。

## 常规设置

**General Settings**（常规设置）页面用于定义常规设备参数。

要显示 **General Settings**（常规设置）页面，请在树视图中单击 **System**（系统）® **Advanced Settings**（高级设置）® **General Settings**（常规设置）。

图 6-85. 常规设置



**General Settings**（常规设置）页面包含以下字段：

**Attribute**（属性）— RAM 日志表条目的最大数目。默认值为 200。

**After Reset**（重置后）— 设备重置后的最大条目数目。通过在此列中输入一个值，可向字段表分配内存。

### 调整 RAM 日志条目的大小分配

- 打开 **General Settings**（常规设置）页面。
- 根据需要在 **After Reset**（重置后）字段中输入新的值。
- 单击 **Apply Changes**（应用更改）。

分配至 RAM 日志条目的空间将在下一次设备重置后生效。

### 使用 CLI 命令查看常规设置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 系统日志命令

## 定义堆栈

“Stacking（堆栈）”菜单用于设置设备的堆栈特性。只有在设备重置之后，才能应用对这些属性所作的更改。请在树视图中单击 **System（系统）** @ **Stacking（堆栈）**，以显示 **Stacking（堆栈）** 页面。此页面用于访问以下功能：

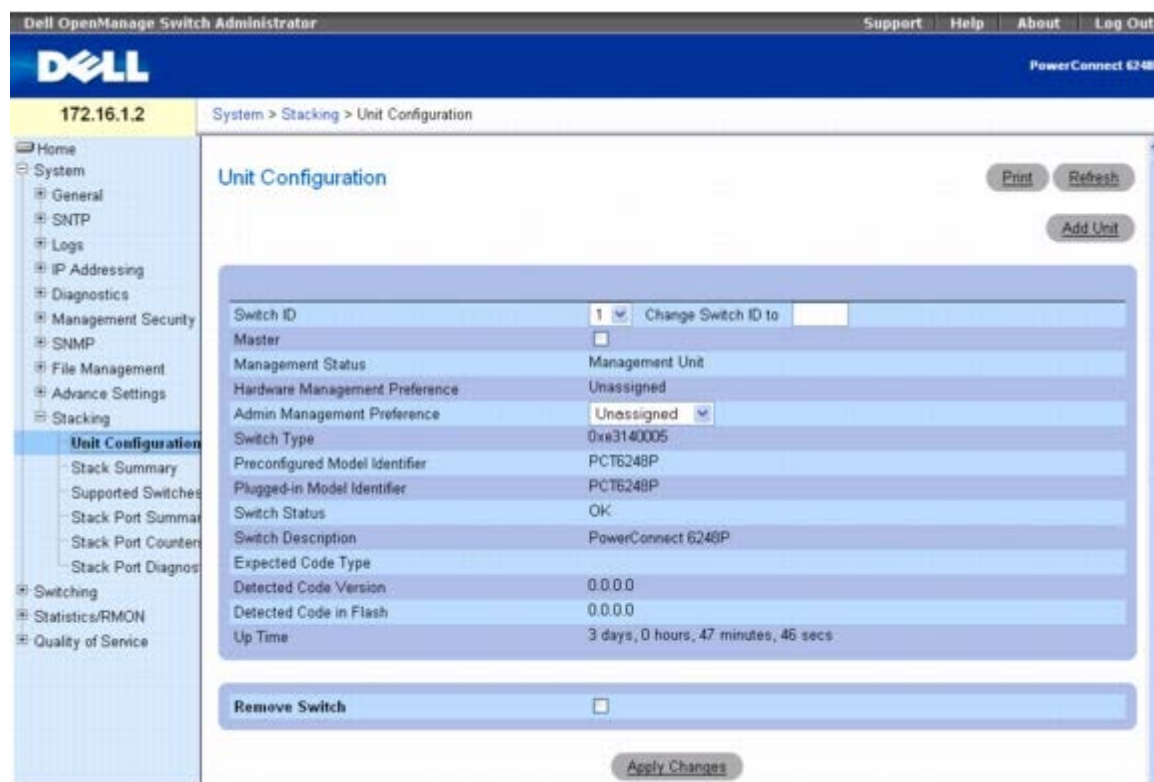
- [单元配置](#)
- [堆栈摘要](#)
- [支持的交换机](#)
- [堆栈端口摘要](#)
- [堆栈端口计数器](#)
- [堆栈端口诊断程序](#)

## 单元配置

**Unit Configuration（单元配置）** 页面用于定义常规设备参数。

要显示 **Unit Configuration（单元配置）** 页面，请在树视图中单击 **System（系统）** @ **Stacking（堆栈）** @ **Unit Configuration（单元配置）**。

图 6-86. 单元配置



**Unit Configuration（单元配置）** 页面包含以下字段：

**Switch ID（交换机 ID）** — 指定要配置的单元。

**Change Switch ID to** (将交换机 ID 变更为) — 更改所选单元的单元编号。

**Master** (主) — 选择该选项可让单元成为优先于其它单元的主 (管理) 单元。此设置的默认值为 **Unassigned** (未分配)。

**Management Status** (管理状态) — 显示所选的单元是 **Management Unit** (管理单元) 还是 **Stack Member** (堆栈成员)。

**Hardware Management Preference** (硬件管理首选项) — 选择作为管理单元的管理首选项，取决于硬件配置。

**Admin Management Preference** (系统管理首选项) — 确定单元是否能成为主交换机。取值范围为 **Disable** (禁用) (单元不支持主交换机功能) 一直到 **Preference 15** (首选 15)。单元的值越高，就越优先运行管理功能。此外，还可以将其值设置为 **Unassigned** (未分配)，表示首选项未配置，并由堆栈单元来选择主单元。

**Switch Type** (交换机类型) — 为系统指定的用于确定交换机类型的硬件 ID。

**Preconfigured Model Identifier** (预配置的型号标识符) — 用于识别所选单元预配置型号的 16 字节字符串。

**Plugged-in Model Identifier** (插件型号标识符) — 用于识别所选单元插件型号的 16 字节字符串。

**Switch Status** (交换机状态) — 显示所选单元的状态。可能的值包括：

**OK** (正常) — 单元就绪并正常工作。

**Unsupported** (不支持) — 设备就绪，但无法作为堆栈成员工作。

**Code Mismatch** (代码不匹配) — 交换机的软件与主单元的配置不匹配。

**Config Mismatch** (配置不匹配) — 交换机的配置与主单元的配置不匹配。

**Not Present** (不存在) — 所选的单元不存在。

**Switch Description** (交换机说明) — 用于标识设备的 80 个字节的数据字段。

**Expected Code Type** (预期代码类型) — 显示预期的代码标识符。

**Detected Code Version** (检测到的代码版本) — 运行的代码版本发布号和版本号。

**Detected Code in Flash** (可擦写式存储器中检测到的代码) — 在可擦写式存储器中检测到的代码发布号和版本号。

**Up Time** (运行时间) — 显示自上次重置后单元运行的时间。

**Remove Switch** (移除交换机) — 选择该选项可从堆栈中移除交换机。

## 定义单元配置

打开 **Unit Configuration** (单元配置) 页面。

根据需要在字段中输入新的值。

单击 **Apply Changes** (应用更改)。

更改将在下次设备重置后生效。

## 移除交换机

打开 **Unit Configuration** (单元配置) 页面。

选中 **Remove Switch** (移除交换机) 复选框。

单击 **Apply Changes** (应用更改)。

更改将在下次设备重置后生效。

## 添加单元

**Add Unit**（添加单元）页面用于定义常规设备参数。

要显示 **Supported Switches**（支持的交换机）页面，请在树视图中单击 **System**（系统）® **Stacking**（堆栈）® **Unit Configuration**（单元配置），然后单击 **Add Unit**（添加单元）。

图 6-87. 添加单元



**Add Unit**（添加单元）页面包含以下字段：

**Switch ID**（交换机 ID）— 显示所选交换机在堆栈中的交换机 ID。管理员用户可以重新指定所选交换机的交换机 ID。只有具有 15 级访问权限的用户才能通过 Web 界面更改此字段。

**Switch Type**（交换机类型）— 表示为交换机指定的硬件 ID。

## 添加单元

□□□ 打开 **Unit Configuration**（单元配置）页面。

□□□ 单击 **Add Unit**（添加单元）。

系统将显示 **Add Unit**（添加单元）页面。

□□□ 根据需要，在 **Switch ID**（交换机 ID）字段中输入新的值。

□□□ 从 **Switch Type**（交换机类型）下拉式列表中选择所需的值。

□□□ 单击 **Apply Changes**（应用更改）。

更改将在下次设备重置后生效。

## 使用 CLI 命令查看配置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 系统管理命令

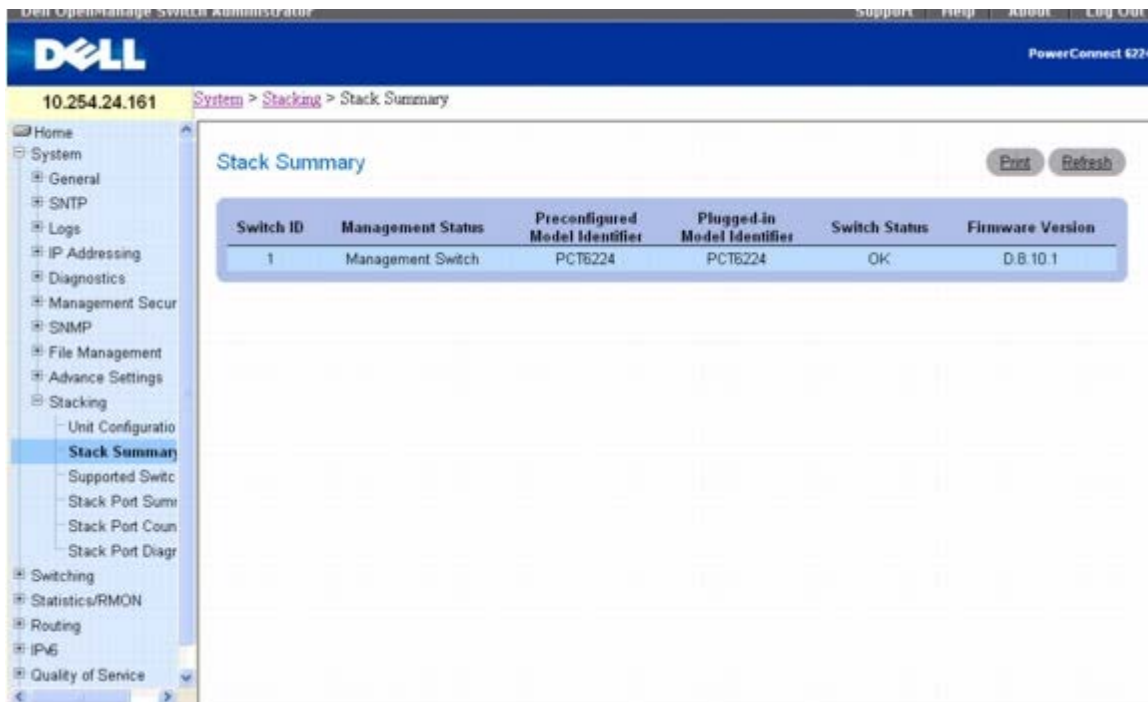
## 堆栈摘要

**Stack Summary**（堆栈摘要）页面用于查看参与堆栈的交换机摘要信息。

要显示 **Stack Summary**（堆栈摘要）页面，请在树视图中单击 **System**（系统）® **Stacking**（堆栈）® **Stack Summary**（堆栈摘要）。

图 6-88. 堆栈摘要





**Stacking Summary**（堆栈摘要）页面包含以下字段：

**Switch ID**（交换机 ID）— 单元的交换机 ID。堆栈中允许的最大单元数目为 8。

**Management Status**（管理状态）— 此字段用于表明交换机是管理交换机、堆栈成员还是状态尚未被指定。

**Pre-configured Model Identifier**（预配置的型号标识符）— 此字段显示设备制造商为标识预配置的设备而指定的 16 个字符字段。

**Plugged-in Model Identifier**（插件型号标识符）— 此字段显示设备制造商为标识插件设备而指定的 16 个字符字段。

**Switch Status**（交换机状态）— 表示单元的状态。有五种可能的状态值：

OK（正常）— 单元就绪并正常工作。

Unsupported（不支持）— 单元不允许堆栈。

Code Mismatch（代码不匹配）— 单元中的软件映像与堆栈主交换机所使用的软件映像不匹配。

Config Mismatch（配置不匹配）— 此单元中的配置文件与堆栈主交换机所使用的配置文件不匹配。

Not Present（不存在）— 单元不存在。

**Firmware Version**（固件版本）— 表示在此单元上检测到的代码版本。

## 使用 CLI 命令查看堆栈摘要

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 系统管理命令

## 支持的交换机

**Supported Switches**（支持的交换机）页面用于查看每种支持堆栈的交换机类型的有关信息，以及支持的交换机的有关信息。

要显示 **Supported Switches**（支持的交换机）页面，请在树视图中单击 **System**（系统）® **Stacking**（堆栈）® **Supported Switches**（支持的交换机）。

图 6-89. 支持的交换机



**Supported Switches** (支持的交换机) 页面包含以下字段：

**Supported Switches** (支持的交换机) — 下拉式列表允许选择支持的交换机。

**Switch Index** (交换机索引) — 将索引添加到支持的交换机类型数据库中。

**Switch Type** (交换机类型) — 为交换机指定的硬件 ID。

**Switch Model ID** (交换机型号 ID) — 显示用于标识支持的交换机型号的 16 字节字符串。

**Description** (说明) — 显示用于标识设备的 256 个字节的数据字段。

**Management Preference** (管理首选项) — 确定单元是否能成为主交换机。如果值设为零，则单元不支持主交换机功能。单元的值越高，就越优先运行管理功能。此字段的值由设备制造商设置。

**Expected Code Type** (预期代码类型) — 显示预期代码版本的发布号和版本号。

## 查看支持的交换机特性

□□□ 打开 **Supported Switches** (支持的交换机) 页面。

□□□ 从 **Supported Switch** (支持的交换机) 下拉式列表中选择所需的交换机。

## 使用 CLI 命令查看支持的交换机

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 系统管理命令

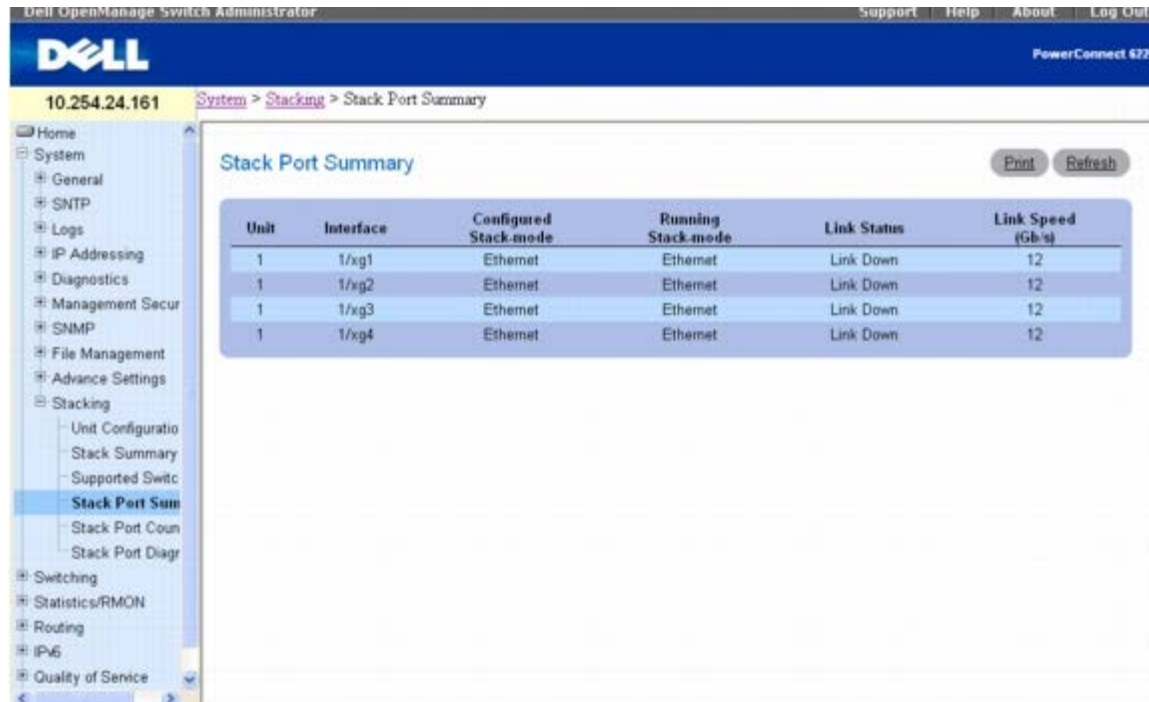
## 堆栈端口摘要

**Stack Port Summary** (堆栈端口摘要) 页面用于查看存在的堆栈式端口。该屏幕显示了单元、堆栈式接口、接口的配置模式、运行模式以及

堆栈式端口的链接状态和链接速度。

要显示 **Stack Port Summary**（堆栈端口摘要）页面，请在树视图中单击 **System**（系统）® **Stacking**（堆栈）® **Stack Port Summary**（堆栈端口摘要）。

图 6-90. 堆栈端口摘要



**Stack Port Summary**（堆栈端口摘要）页面包含以下字段：

**Unit**（单元）— 单元的 ID 号。

**Interface**（接口）— 标识分配给单元的堆栈接口。

**Configured Stack Mode**（配置的堆栈模式）— 表示每个单元是否都参与堆栈。

**Running Stack Mode**（运行堆栈模式）— 表示每个单元是否正在参与堆栈。

**Link Status**（链路状态）— 表示每个单元的堆栈接口是否正在工作。

**Link Speed (Gb/s)**（链路速度 [Gb/s]）— 表示每个单元链路的标称速度。

## 使用 CLI 命令查看堆栈端口摘要

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 系统管理命令

## 堆栈端口计数器

**Stack Port Counters**（堆栈端口计数器）页面用于查看已发送和已接收统计数据，包括数据速率和错误率。

要显示 **Stack Port Counters**（堆栈端口计数器）页面，请在树视图中单击 **System**（系统）® **Stacking**（堆栈）® **Stack Port Counters**（堆栈端口计数器）。

图 6-91. 堆栈端口计数器

Dell OpenManage Switch Administrator

Support Help About Log Out

PowerConnect 6200

10.254.24.161 System > Stacking > Stack Port Counters

System

- General
- SNTP
- Logs
- IP Addressing
- Diagnostics
- Management Secur
- SNMP
- File Management
- Advance Settings
- Stacking
  - Unit Configuratio
  - Stack Summary
  - Supported Switc
  - Stack Port Sumi
  - Stack Port Coun
  - Stack Port Diagr
- Switching
- Statistics/RMON
- Routing
- IPv6
- Quality of Service
- IP Multicast

Stack Port Counters

Print Refresh

Unit	Interface	Data Rate (Mb/s)	Transmit Error Rate (Errors/sec)	Total Errors	Data Rate (Mb/s)	Receive Error Rate (Errors/sec)	Total Errors
1	1/xg1	0	0	0	0	0	0
1	1/xg2	0	0	0	0	0	0
1	1/xg3	0	0	0	0	0	0
1	1/xg4	0	0	0	0	0	0

**Stack Port Counters** (堆栈端口计数器) 页面包含以下字段：

**Unit** (单元) — 表示查看的附属交换机。

**Interface** (接口) — 表示接口的名称。

**Data Rate (Mb/s)** (数据速率 [Mb/s]) — 表示发送数据的速度。

**Transmit Error Rate (Errors/sec)** (发送错误率 [错误/秒]) — 表示发送数据时每秒发生的错误次数。

**Total Errors** (总计错误) — 发送的总计错误次数。

**Data Rate (Mb/s)** (数据速率 [Mb/s]) — 表示接收数据的速度。

**Receive Error Rate (Errors/sec)** (接收错误率 [错误/秒]) — 表示接收数据时每秒所发生的错误次数。

**Total Errors** (总计错误) — 接收的总计错误次数。

## 查看堆栈端口计数器

□□□ 打开 **Stack Port Counters** (堆栈端口计数器) 页面。

## 使用 CLI 命令查看堆栈端口计数器

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 系统管理命令

## 堆栈端口诊断程序

**Stack Port Diagnostics** (堆栈端口诊断程序) 页面仅供现场应用工程师 (FAE) 和开发人员使用。

[返回目录页面](#)



[返回目录页面](#)

# 配置 IP 电话和访问点支持功能

Dell™ PowerConnect™ 6200 系列用户指南

- [以太网供电配置](#)
- [配置用于介质端点设备的链路层发现协议 \(LLDP\)](#)
- [为语音 VLAN 配置端口](#)

本节将介绍系统提供的以下 IP 电话和访问点支持功能：

- [以太网供电配置](#)
- [配置用于介质端点设备的链路层发现协议 \(LLDP\)](#)
- [为语音 VLAN 配置端口](#)

---

## 以太网供电配置

以太网供电 (PoE) 功能不需要更新或修改网络基础设施，即可通过现有的 LAN 电缆为设备供电。当使用 PoE 时，无需将网络设备放在靠近电源的位置。可以将 PoE 用作电源的设备包括 IP 电话、无线访问点、IP 网关、PDA 以及远程音频和视频监测设备。

本节将介绍 **System** (系统) ® **General** (常规) ® **Power Over Ethernet** (以太网供电) 菜单页面中提供的 PoE 选项。这些选项包括为系统或每个接口配置和查看 PoE 信息。在 **Power Over Ethernet** (以太网供电) 菜单页面上，可以通过以下菜单页面来访问这些选项：

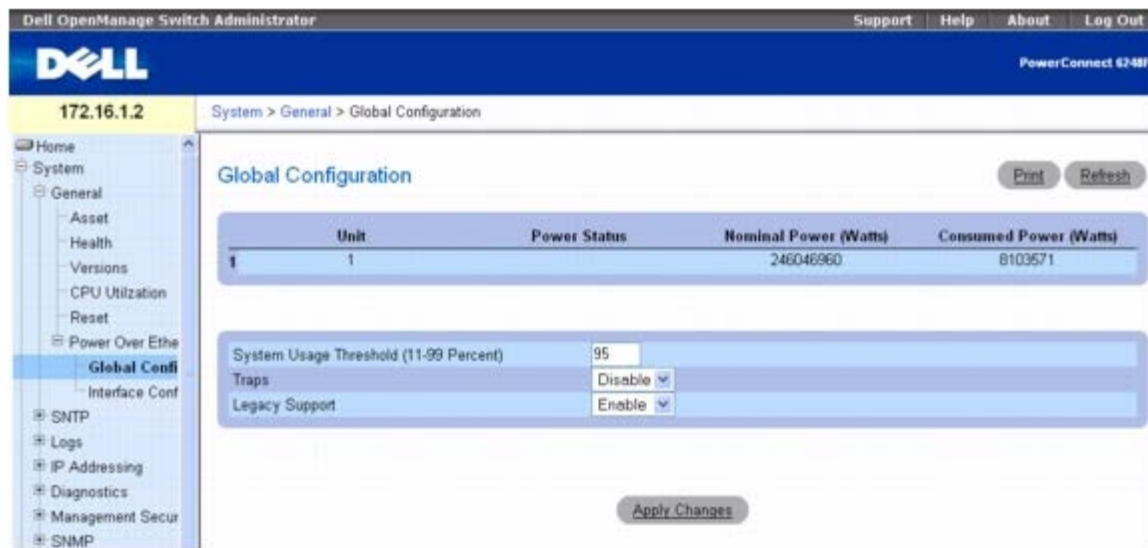
- [以太网供电配置](#)
- [接口配置](#)

## 全局配置

**Global Configuration** (全局配置) 页面用于配置和查看整个系统范围内的 PoE 参数，包括系统能耗、陷阱和旧有 PoE 设备支持。

要显示此页面，请在树视图中单击 **System** (系统) ® **General** (常规) ® **Power Over Ethernet** (以太网供电) ® **Global Configuration** (全局配置)。

图 7-1. 全局配置



**Global Configuration**（全局配置）页面包含以下字段：

**Unit**（单元）— 表示堆栈内的单元。

**Power Status**（电源状态）— 内联供电设备的工作状态。

**Nominal Power**（标称功率）— 内联供电设备的标称功率（以瓦特为单位）。

**Consumed Power**（能耗功率）— 以瓦特为单位的实测能耗功率。

**System Usage Threshold**（系统能耗阈值）— 以百分比表示的能耗阈值，用于比较实测的功率并在超过阈值时发出警报。

**Traps**（陷阱）— 表示启用还是禁用了内联供电陷阱。

**Legacy Support**（旧有设备支持）— 启用或禁用旧有 PoE 设备支持。

## 配置全局 PoE 设置

□□□ 打开 **Global Configuration**（全局配置）页面。

□□□ 配置系统能耗阈值、陷阱或旧有 PoE 设备支持。

□□□ 单击 **Apply Changes**（应用更改）。

系统将应用系统参数并更新设备。

## 使用 CLI 命令配置 PoE

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 以太网供电命令

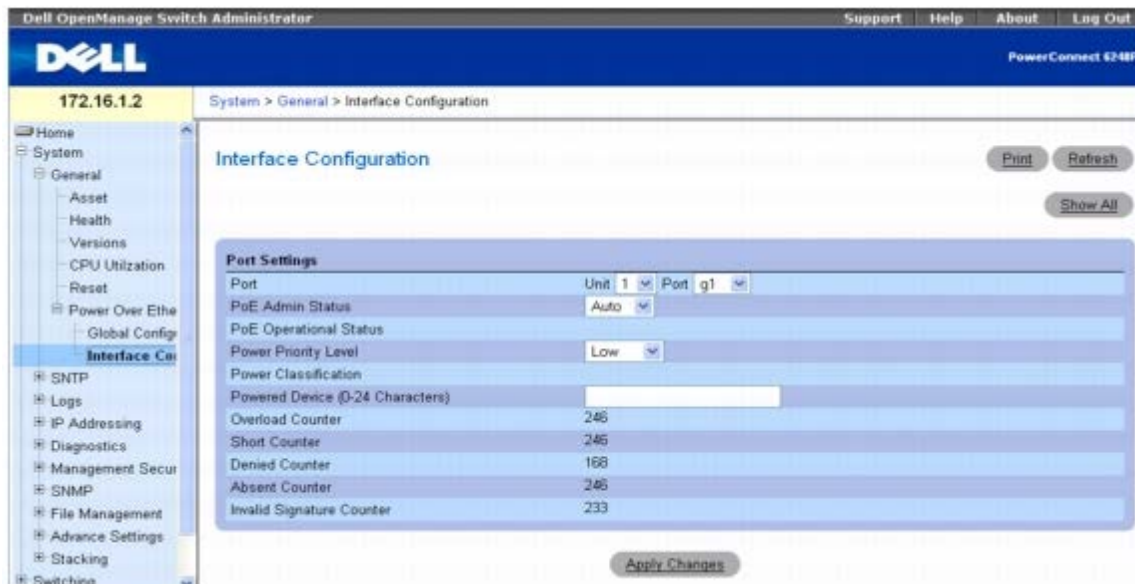
## 接口配置

**Interface Configuration**（接口配置）页面用于配置和查看每个端口的 PoE 参数。

要显示此页面，请在树视图中单击 **System**（系统）® **General**（常规）® **Power Over Ethernet**（以太网供电）® **Interface Configuration**（接口配置）。

图 7-2. 接口配置





**Interface Configuration** (接口配置) 页面包含以下字段：

**Port** (端口) — 指定 Unit (单元) 和要定义端口参数的 Port (端口)。

**PoE Admin Status** (PoE 管理状态) — 表明是否允许端口供电。

**Auto** (自动) — 端口自动为所连接的支持 PoE 的设备供电。

**Never** (从不) — 端口不为所连接的任何设备供电。

**PoE Operational Status** (PoE 工作状态) — 说明端口的内联供电设备的工作状态。工作状态可以是：

**Off** (关闭) — 表示没有供电。

**On** (打开) — 表示正在为设备供电。

**Test-Fail** (测试失败) — 表示端口有问题。

**Testing** (正在测试) — 表示端口正处于测试模式。

**Fault** (故障) — 表示端口由于故障而空闲。

**Searching** (正在搜索) — 表示端口没有处于以上任何状态。

**Power Priority Level** (供电优先级) — 从内联供电管理的角度考虑的端口优先级。供电优先级可以是：

- Critical (关键)
- High (高)
- Low (低)

**Power Classification** (能耗分级) — 用电设备的能耗范围。用电分级可以是：

- Class 0(0.44–12.95) (0 级 [0.44-12.95])
- Class 1(0.44–3.84) (1 级 [0.44-3.84])
- Class 2(3.84–6.49) (2 级 [3.84-6.49])
- Class 3(6.49–12.95) (3 级 [6.49-12.95])

**Powered Device** (用电设备) — 用电设备类型说明，最多包含 24 个字符。

**Overload Counter** (过载计数器) — 计算检测到过载情况的次数。

**Short Counter**（电量不足计数器）— 计算检测到电量不足情况的数量。

**Denied Counter**（断电计数器）— 计算断电的次数。

**Absent Counter**（缺席计数器）— 计算因检测不到用电设备而停止为用电设备供电的次数。

**Invalid Signature Counter**（无效签名计数器）— 计算检测到用电设备无效签名的次数。

## 为接口配置 PoE 设置

□□□ 打开 **Interface Configuration**（接口配置）页面。

□□□ 选择要配置的单元和端口。

□□□ 配置管理状态、供电优先级或者从端口供电的设备的名称。

□□□ 单击 **Apply Changes**（应用更改）。

系统将应用系统参数并更新设备。

## 显示以太网供电表

□□□ 打开 **Interface Configuration**（接口配置）页面。

□□□ 单击 **Show All**（全部显示）。

**Power Over Ethernet Table**（以太网供电表）页面显示和提供了所有接口的 PoE 摘要信息：

图 7-3. 以太网供电表

Port	Admin Status	Operational Status	Priority Level	Power Classification	Powered Device	
1	1/g1	Up	Failure	Low	Class 0	
2	1/g2	Up	Failure	Low	Class 0	
3	1/g3	Up	Failure	Low	Class 0	
4	1/g4	Up	Failure	Low	Class 0	
5	1/g5	Up	Failure	Low	Class 0	
6	1/g6	Up	Failure	Low	Class 0	

## 使用 CLI 命令配置 PoE

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 以太网供电命令

## 配置用于介质端点设备的链路层发现协议 (LLDP)

IEEE 802.1AB 标准说明了链路层发现协议 (LLDP)，并规定了在 LAN/MAN 环境下的数据网络中发现单元和检索单元功能的方法。交换的信息存储在 MIB 中，可供 SNMP 这样的网络管理系统 (NMS) 访问。这一框架可以进一步扩展，以允许某些领域（例如 VoIP 网络）的高端应用。

用于介质端点设备的链路层发现协议 (LLDP-MED) 扩展了 LLDP 标准，支持网络配置和策略、设备定位、以太网供电管理以及清单管理。

LLDP-MED 使用了 LLDP 中特定于组织的 TLV 扩展，并定义了新的 TLV 以便于在有线或无线 LAN/MAN 环境中部署 VoIP。它还强制采用了 LLDP 的某些可选 TLV，并建议不发送某些 TLV。

由于 LLDP-MED 采用了 LLDP 的框架，因此它需要满足同样的原始规格要求。框架格式、限制和含义都得以保留。

TLV 只收发信息；这些 TLV 不会自动将信息转换为配置。外部应用程序可以查询 MED MIB，并在配置功能时执行管理操作。

**LLDP-MED** 菜单页面包含以下功能的链接：

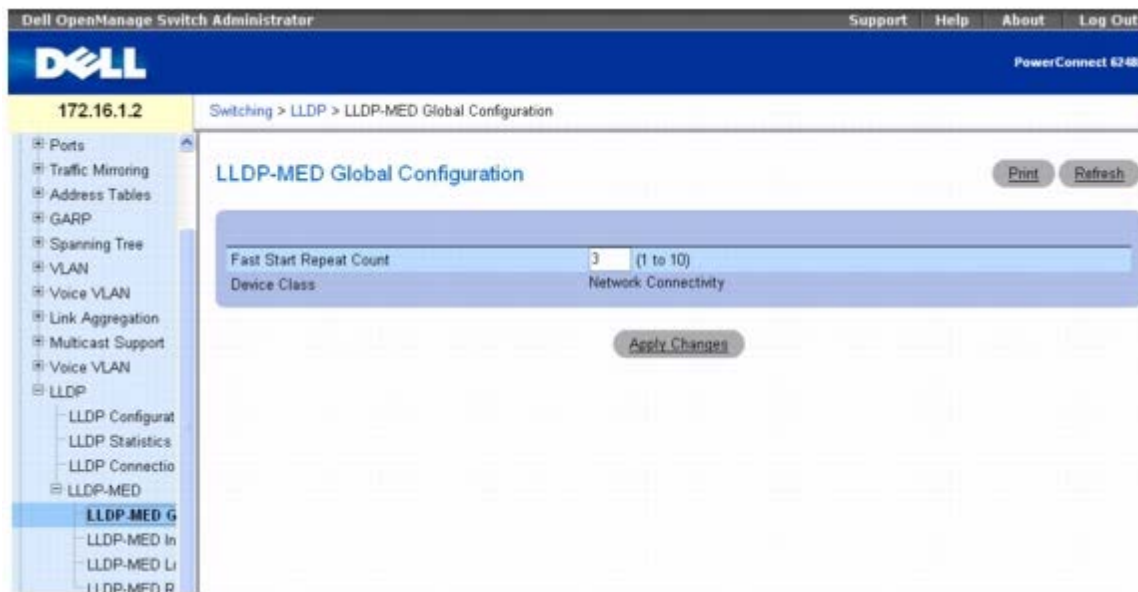
- [LLDP-MED 全局配置](#)
- [LLDP-MED 接口配置](#)
- [LLDP-MED 本地设备信息](#)
- [LLDP-MED 远程设备信息](#)

## LLDP-MED 全局配置

**LLDP-MED Global Configuration** (**LLDP-MED** 全局配置) 页面用于更改或查看影响整个系统的 LLDP-MED 参数。

要显示 **LLDP-MED Global Configuration** (**LLDP-MED** 全局配置) 页面，请在树视图中单击 **Switching** (交换) ® **LLDP** ® **LLDP-MED** ® **LLDP-MED Global Configuration** (**LLDP-MED** 全局配置)。

图 7-4. LLDP-MED 全局配置



**LLDP-MED Global Configuration** (**LLDP-MED** 全局配置) 页面包含以下字段：

**Fast Start Repeat Count** (快速启动重复计数) — 指定要在启用这种协议时发送的 LLDP PDU 的数量。范围为 1 至 10。快速重复计数的默认值为 4。

**Device Class** (设备类别) — 指定本地设备的 MED 分类。设备共分为四类，其中的三类表示实际端点 (I 类通用端点 [IP 通信控制器等等]、II 类介质端点 [会议桥等等]、III 类通信端点 [IP 电话等等])。第四类设备是网络连接设备，通常是 LAN 交换机/路由器、IEEE 802.11 桥接设备、IEEE 802.11 无线访问点等等。

### 修改 LLDP-MED 全局配置

□□□ 打开 **LLDP Configuration** (**LLDP** 配置) 页面。

□□□ 为 Fast Start Repeat Count (快速启动重复计数) 输入新的值。

□□□ 单击 **Apply Changes** (应用更改)。

系统将 LLDP-MED 参数保存至交换机。

## 使用 CLI 命令配置 LLDP-MED 全局设置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- LLDP 命令

## LLDP-MED 接口配置

**LLDP-MED Interface Configuration** (LLDP-MED 接口配置) 页面用于指定影响特定接口的 LLDP-MED 参数。


要显示 **LLDP-MED Interface Configuration** (LLDP-MED 接口配置) 页面，请在树视图中单击 **Switching** (交换) ® **LLDP** ® **LLDP-MED** ® **LLDP-MED Interface Configuration** (LLDP-MED 接口配置)。

图 7-5. LLDP-MED 接口配置



**LLDP-MED Interface Configuration** (LLDP-MED 接口配置) 页面包含以下字段：

**Interface** (接口) — 指定可以在其上配置 LLDP-MED - 802.1AB 的端口的列表。选择 **Port** (端口) 下拉式列表中的 **All** (全部) 将为系统中的所有接口配置相同的 LLDP-MED 设置。

 **注**：当选择了 **Port** (端口) 字段中的 **All** (全部) 时，此页面中的 LLDP-MED 模式和 **Notification** (通知) 模式将显示为 Disabled (已禁用)，所有 **Transmit TLVs** (发送 TLV) 复选框将被清除。即使为所有端口配置了相同的设置也会如此。请选择特定的接口或单击 **Show All** (全部显示) 以查看接口的 LLDP-MED 设置。

**LLDP-MED Mode** (LLDP-MED 模式) — 为所选的接口指定链路层数据协议介质端点 (LLDP-MED) 模式。启用 MED 将实际启用 LLDP 的发送和接收功能。

**Config Notification Mode** (配置通知模式) — 为所选的接口指定 LLDP-MED 拓扑通知模式。

**Transmit TLVs** (发送 TLV) — 为所选的接口指定要在 LLDP PDU 帧中发送 LLDP-MED 的哪些可选类型长度值 (TLV)。

**MED Capabilities** (MED 功能) — 在 LLDP 帧中发送功能 TLV。

**Network Policy** (网络策略) — 在 LLDP 帧中发送网络策略 TLV。

**Location Identification**（位置识别）— 在 LLDP 帧中发送位置 TLV。

**Extended Power via MDI - PSE**（通过 MDI - PSE 扩展的电源）— 在 LLDP 帧中发送扩展的 PSE TLV。

**Extended Power via MDI - PD**（通过 MDI - PD 扩展的电源）— 在 LLDP 帧中发送扩展的 PD TLV。

**Inventory**（清单）— 在 LLDP 帧中发送清单 TLV。

## 修改 LDP-MED 接口配置


□□□ 打开 **LLDP Configuration**（LLDP 配置）页面。

□□□ 指定单元并选择要配置的端口，或者选择 **All**（全部）为所有端口配置相同的设置。

□□□ 为一个或多个接口配置 LLDP-MED 设置。

□□□ 单击 **Apply Changes**（应用更改）。

系统将 LLDP-MED 参数保存至交换机。

 **注：**如果配置了 **All**（全部）端口，当此页面更新之后，将不会显示您应用的设置。请选择特定的接口或单击 **Show All**（全部显示）以查看接口的 LLDP-MED 设置。

## 显示接口摘要

□□□ 打开 **LLDP-MED Interface Configuration**（LLDP-MED 接口配置）页面。

□□□ 单击 **Show All**（全部显示）。

**LLDP-MED Interface Summary**（LLDP-MED 接口摘要）页面显示和提供了所有接口的 LLDP-MED 摘要信息：

图 7-6. LLDP-MED 接口摘要



Interface	Link Status	MED Status	Operational Status	Notification Status	Transmit TLV(s)
1/g1	Up	Disable	Disable	Disable	Capabilities Network Policy
1/g2	Down	Disable	Disable	Disable	Capabilities Network Policy
1/g3	Down	Disable	Disable	Disable	Capabilities Network Policy
1/g4	Down	Disable	Disable	Disable	Capabilities Network Policy
1/g5	Down	Disable	Disable	Disable	Capabilities Network Policy
-----					
1/g46	Down	Disable	Disable	Disable	Capabilities Network Policy
1/xg1	Down	Disable	Disable	Disable	Capabilities Network Policy
1/xg2	Down	Disable	Disable	Disable	Capabilities Network Policy
1/xg3	Down	Disable	Disable	Disable	Capabilities Network Policy
1/xg4	Down	Disable	Disable	Disable	Capabilities Network Policy

## 使用 CLI 命令配置 LLDP-MED 接口设置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

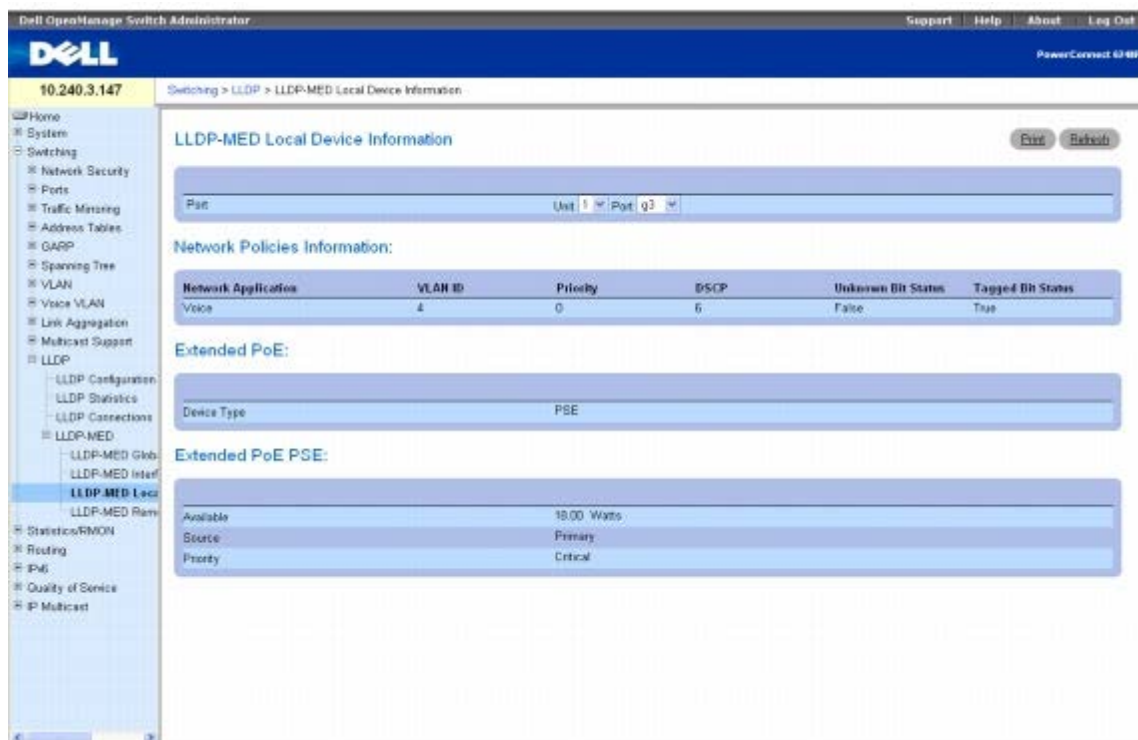
- LLDP 命令

## LLDP-MED 本地设备信息

**LLDP-MED Local Device Information** (LLDP-MED 本地设备信息) 页面用于查看为每个端口公布的 LLDP 本地数据。

要显示 **LLDP-MED Local Device Information** (LLDP-MED 本地设备信息) 页面，请在树视图中单击 **Switching** (交换) ® **LLDP** ® **LLDP-MED** ® **LLDP-MED Local Device Information** (LLDP-MED 本地设备信息)。

图 7-7. LLDP-MED 本地设备信息



**LLDP-MED Local Device Information** (LLDP-MED 本地设备信息) 页面包含以下字段：

**Port** (端口) — 选择单元和端口，以显示为端口公布的 LLDP 本地数据。端口下拉式列表中只包含启用了 LLDP-MED 的那些端口。

**Network Policies Information** (网络策略信息) — 如果 LLDP 帧中存在网络策略 TLV，则会显示以下信息：

**Network Application** (网络应用) — 指定本地设备在策略中公布的介质应用类型。端口可能会收到一个或多个类型，包括：

- unknown
- voicesignaling
- guestvoice
- guestvoicesignalling
- softphonevoice
- videoconferencing
- streamingvideo
- videosignalling



**Vlan Id** — 指定与特定的策略类型相关的 VLAN ID。

**Priority** (优先级) — 指定与特定的策略类型相关的优先级。

**DSCP** — 指定与特定的策略类型相关的 DSCP。

**Unknown Bit Status** (未知位状态) — 指定与特定的策略类型相关的未知位。

**Tagged Bit Status** (已标记位状态) — 指定与特定的策略类型相关的已标记位。

**Inventory** (清单) — 如果 LLDP 帧中存在清单 TLV，则会显示以下信息：

**Hardware Revisions** (硬件修订版本) — 指定硬件版本。

**Firmware Revisions** (固件修订版本) — 指定固件版本。

**Software Revisions** (软件修订版本) — 指定软件版本。

**Serial Number** (序列号) — 指定序列号。

**Manufacturer Name** (制造商名称) — 指定制造商名称。

**Model Name** (型号名称) — 指定型号名称。

**Asset ID** (资产 ID) — 指定资产 ID。

**Location Information** (位置信息) — 如果 LLDP 帧中存在位置 TLV，则会显示以下信息：

**Sub Type** (子类型) — 指定位置信息的类型。

**Location Information** (位置信息) — 将位置信息指定为给定类型的位置 ID 字符串。

**Extended PoE** (扩展的 PoE) — 如果本地设备是一个 PoE 设备，则会显示以下信息：

**Device Type** (设备类型) — 指定电源设备的类型。

**Extended PoE PSE** (扩展的 PoE PSE) — 如果 LLDP 帧中存在扩展的 PSE TLV，则会显示以下信息：

**Available** (可用) — 以十分之一瓦特为单位指定本地设备的端口可以提供的供电设备功率值。

**Source** (电源) — 指定此端口的电源。

**Priority** (优先级) — 指定 PSE 端口的供电优先级。

**Extended PoE PD** (扩展的 PoE PD) — 如果 LLDP 帧中存在扩展的 PD TLV，则会显示以下信息：

**Required** (所需值) — 以十分之一瓦特为单位指定本地设备的端口所需的供电设备功率值。

**Source** (电源) — 指定此端口的电源。

**Priority** (优先级) — 指定 PD 端口的供电优先级。

## 使用 CLI 命令查看 LLDP-MED 本地设备信息

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- LLDP 命令

## LLDP-MED 远程设备信息

**LLDP-MED Remote Device Information** (LLDP-MED 远程设备信息) 页面用于查看为远程设备公布的 LLDP 数据。

要显示 **LLDP-MED Remote Device Information** (LLDP-MED 远程设备信息) 页面，请在树视图中单击 **Switching** (交换) ® **LLDP** ® **LLDP-MED** ® **LLDP-MED Remote Device Information** (LLDP-MED 远程设备信息)。



图 7-8. LLDP-MED 远程设备信息

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "LLDP-MED Remote Device Information" and includes a "Local Interface" dropdown menu set to "1/g3". The interface is divided into several sections:

- Capability Information:**
  - Supported Capabilities: Capabilities, Network Policy, Location, Extended PD, Inventory
  - Enabled Capabilities: Capabilities, Network Policy, Location, Extended PD, Inventory
  - Device Class: Endpoint Class III
- Display Network Policies:**

Network Application	VLAN ID	Priority	DSCP	Unknown Bit Status	Tagged Bit Status
Voice	777	7	5	False	True
- Inventory Information:**

Hardware Revision	7.7.7.7
Firmware Revision	m m
Software Revision	software revision 4.5
Serial Number	serial number 777
Manufacturer Name	Broadcom Corp.
Model Name	Model XGS3
Asset ID	asset 1717
- Location Information:**

Sub Type	Location Information
ELIN	100777100777
- Extended PoE:**

Device Type	PD
-------------	----
- Extended PoE PD:**

Required	7.00 Watts
Source	Local
Priority	High

**LLDP-MED Remote Device Information** (LLDP-MED 远程设备信息) 页面包含以下字段:

**Local Interface** (本地接口) — 指定启用了 LLDP-MED 的所有端口的列表。

**Capability Information** (功能信息) — 指定此端口上通过 MED TLV 接收到的支持的功能和启用的功能。

**Supported Capabilities** (支持的功能) — 指定此端口上通过 MED TLV 接收到的支持的功能。

**Enabled Capabilities** (启用的功能) — 指定此端口上通过 MED TLV 接收到的启用的功能。

**Device Class** (设备类别) — 指定远程连接到端口的设备所公布的设备类别。

**Network Policy Information** (网络策略信息) — 如果此端口上的 LLDP 帧中收到了网络策略 TLV, 则会显示以下信息:

**Network Application** (网络应用) — 指定本地设备在策略中公布的介质应用类型。端口可能会收到一个或多个应用类型, 包括:

- unknown
- voicesignaling
- guestvoice
- guestvoicesignalling
- softphonevoice
- videoconferencing
- streamingvideo
- videesignalling

**Vlan Id** — 指定与特定的策略类型相关的 VLAN ID。

**Priority** (优先级) — 指定与特定的策略类型相关的优先级。

**DSCP** — 指定与特定的策略类型相关的 DSCP。

**Unknown Bit Status** (未知位状态) — 指定与特定的策略类型相关的未知位。

**Tagged Bit Status** (已标记位状态) — 指定与特定的策略类型相关的已标记位。

**Inventory** (清单) — 如果 LLDP 帧中存在清单 TLV，则会显示以下信息：

**Hardware Revisions** (硬件修订版本) — 指定远程设备的硬件版本。

**Firmware Revisions** (固件修订版本) — 指定远程设备的固件版本。

**Software Revisions** (软件修订版本) — 指定远程设备的软件版本。

**Serial Number** (序列号) — 指定远程设备的序列号。

**Manufacturer Name** (制造商名称) — 指定远程设备的制造商名称。

**Model Name** (型号名称) — 指定远程设备的型号名称。

**Asset ID** (资产 ID) — 指定远程设备的资产 ID。

**Location Information** (位置信息) — 如果 LLDP 帧中存在位置 TLV，则会显示以下信息：

**Sub Type** (子类型) — 指定位置信息的类型。

**Location Information** (位置信息) — 将位置信息指定为给定类型的位置 ID 字符串。

**Extended PoE** (扩展的 PoE) — 指定远程设备是否是一个 PoE 设备。

**Device Type** (设备类型) — 指定连接到此端口的远程设备的 PoE 设备类型。

**Extended PoE PSE** (扩展的 PoE PSE) — 如果此端口上的 LLDP 帧中收到了扩展的 PSE TLV，则会显示以下信息：

**Available** (可用) — 以十分之一瓦特为单位指定远程端口的 PSE 功率值。

**Source** (电源) — 指定远程端口的 PSE 电源。

**Priority** (优先级) — 指定远程端口的 PSE 供电优先级。

**Extended PoE PD** (扩展的 PoE PD) — 如果此端口上的 LLDP 帧中收到了扩展的 PD TLV，则会显示以下信息：

**Required** (所需值) — 指定远程端口的 PD 功率要求。

**Source** (电源) — 指定远程端口的电源。

**Priority** (优先级) — 指定远程端口的 PD 供电优先级。

## 使用 CLI 命令查看 LLDP-MED 远程设备信息

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- LLDP 命令

## 为语音 VLAN 配置端口

语音 VLAN 功能使交换机端口能够按指定的优先级传送语音通信。优先级能够分离端口收到的语音通信和数据通信。语音 VLAN 的一个主要优点是，当端口的数据通信量很大时，可以保证 IP 电话的音质不会下降。系统会使用经过端口的通信的源 MAC 地址来识别 IP 电话数据流。

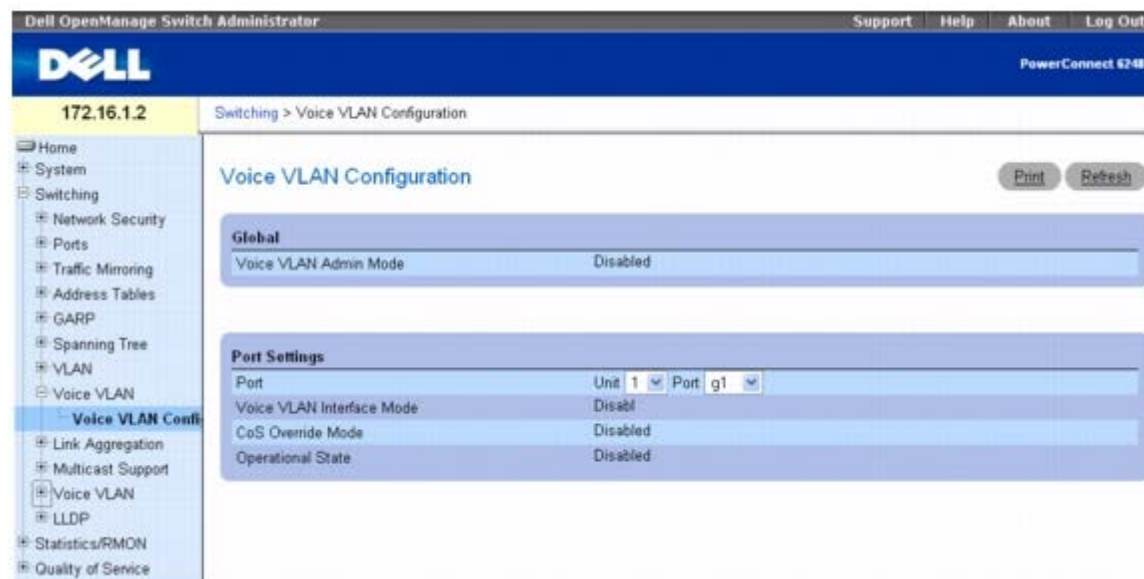
**Voice VLAN**（语音 VLAN）页面包含用于配置全局语音 VLAN 设置和端口语音 VLAN 设置的链接。

## 语音 VLAN 配置

**Voice VLAN Configuration**（语音 VLAN 配置）页面用于配置和查看应用于整个系统和特定接口的语音 VLAN 设置。

要显示此页面，请在树视图中单击 **Switching**（交换）® **Voice VLAN**（语音 VLAN）® **Voice VLAN Configuration**（语音 VLAN 配置）。

图 7-9. 语音 VLAN 配置



**Voice VLAN Configuration**（语音 VLAN 配置）页面包含以下字段：

**Voice VLAN Admin Mode**（语音 VLAN 管理模式）— 从下拉式菜单中为交换机的语音 VLAN 选择管理模式。默认设置为已禁用。

**Port**（端口）— 选择要查看或配置的接口。

**Voice VLAN Interface Mode**（语音 VLAN 接口模式）— 为所选的接口选择语音 VLAN 模式。默认设置为已禁用。模式可以是：

**Disable**（禁用）— 禁用端口上的语音 VLAN。

**None**（无）— 允许 IP 电话使用自己的配置来发送未标记的语音通信。

**VLAN ID** — 为语音通信配置 VLAN 标记。VLAN ID 的范围为 1 至 4093。

**dot1p** — 为语音通信配置语音 VLAN 802.1p 优先级标记。优先级标记的范围为 0 至 7。

**Untagged**（未标记）— 将电话配置为发送未标记的语音通信。

**CoS Override Mode (CoS 覆盖模式)** — 为所选的接口选择 Cos 覆盖模式。默认设置为已禁用。

**Operational State (操作状态)** — 即指定的接口上的语音 VLAN 的操作状态。

## 配置语音 VLAN 设置

打开 **Voice VLAN Configuration** (语音 VLAN 配置) 页面。

为系统或每个端口配置设置。

单击 **Apply Changes** (应用更改)。

系统将应用系统参数并更新设备。

## 使用 CLI 命令配置语音 VLAN

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 语音 VLAN 命令

---

[返回目录页面](#)

[返回目录页面](#)

## 配置交换信息

Dell™ PowerConnect™ 6200 系列用户指南

- [配置网络安全保护](#)
- [配置生成树协议](#)
- [配置端口](#)
- [配置 VLAN](#)
- [配置通信镜像](#)
- [聚合端口](#)
- [配置地址表](#)
- [管理多点传送支持](#)
- [配置 GARP](#)
- [配置链路层发现协议 \(LLDP\)](#)

本节介绍了有关网络安全保护、端口、地址表、GARP、VLAN、生成树、端口聚合和多点传送支持的所有系统操作和一般信息。

**Switching** (交换) 菜单页面包含以下功能的链接:

- [配置网络安全保护](#)
- [配置端口](#)
- [配置通信镜像](#)
- [配置地址表](#)
- [配置 GARP](#)
- [配置生成树协议](#)
- [配置 VLAN](#)
- [聚合端口](#)
- [管理多点传送支持](#)
- [配置链路层发现协议 \(LLDP\)](#)

---

## 配置网络安全保护

**Network Security** (网络安全保护) 菜单页面用于通过基于端口的验证、锁定的端口、DHCP 筛选配置和访问控制列表来设置网络安全保护。

要显示 **Network Security** (网络安全保护) 页面, 请在树视图中单击 **Switching** (交换) ® **Network Security** (网络安全保护)。

**Network Security** (网络安全保护) 菜单页面包含以下功能的链接:

- [基于端口的验证](#)
- [多台主机](#)
- [经验证的用户](#)
- [端口安全保护](#)
- [DHCP 筛选](#)
- 访问控制列表
- [ACL 捆绑配置](#)

## 基于端口的验证

在基于端口的验证模式中，如果全局启用 802.1x，而且端口上任何一个连接至该端口的申请方成功验证，将导致所有用户均可无限制使用该端口。在此模式下，任何指定时间内一个端口仅允许一个申请方尝试验证。此模式下的端口可双向控制。这是默认验证模式。

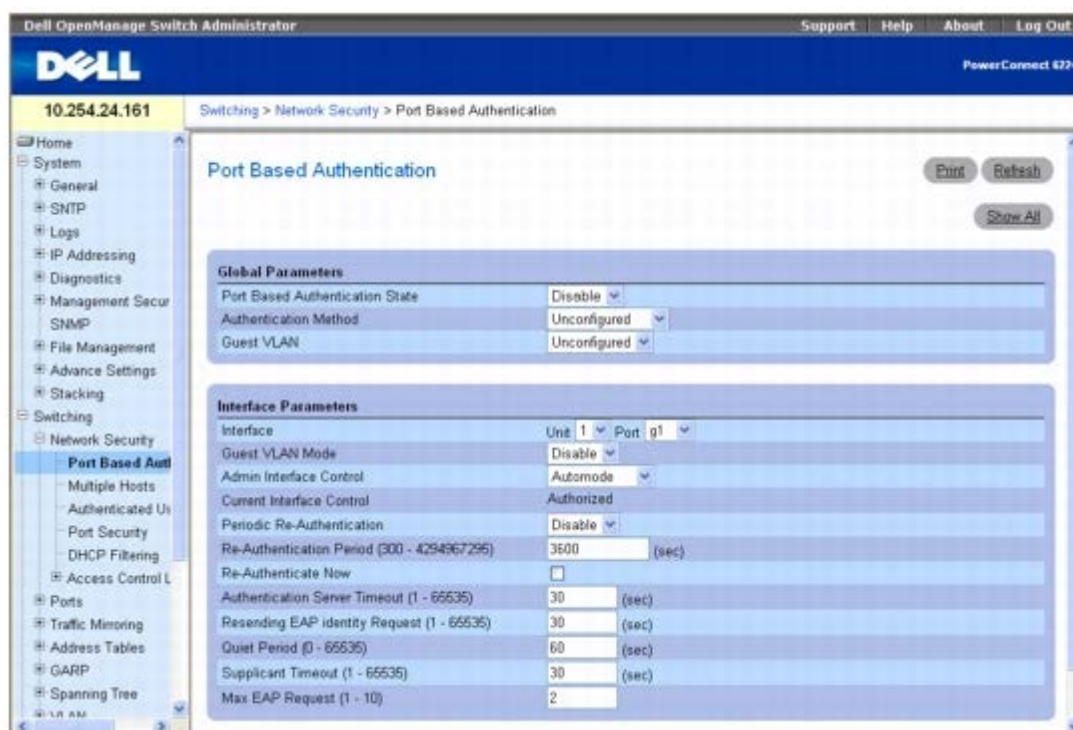
802.1x 网络有三个组件：

- **Authenticators** (验证方) — 指定允许系统访问之前要验证的端口。
- **Supplicants** (申请方) — 指定连接至请求访问系统服务的经验证端口的主机。
- **Authentication Server** (验证服务器) — 指定外部服务器（例如代表验证方执行验证的 RADIUS 服务器），并指示用户是否有权访问系统服务。

**Port Based Authentication** (基于端口的验证) 页面用于配置端口的常规 802.1x 参数。

要显示 **Port Based Authentication** (基于端口的验证) 页面，请在树视图中单击 **Switching** (交换) ® **Network Security** (网络安全保护) ® **Port Based Authentication** (基于端口的验证)。

图 8-1. 基于端口的验证



**Port Based Authentication** (基于端口的验证) 页面包含以下字段：

### 全局参数

**Port Based Authentication State** (基于端口的验证状态) — 允许在交换机上进行基于端口的验证。可能的字段值包括：

- Enable** (启用) — 在交换机上启用基于端口的验证。
- Disable** (禁用) — 在交换机上禁用基于端口的验证。

**Authentication Method** (验证方法) — 选择使用的验证方法。可能的字段值包括：

- Unconfigured** (未配置) — 表示尚未选择验证方法。
- None** (无) — 表示没有使用任何验证方法。

**RADIUS** — 表示在 RADIUS 服务器上验证。

**RADIUS, None (RADIUS, 无)** — 表示在 RADIUS 服务器上验证。如果 RADIUS 服务器不可用，则不使用任何验证方法。

**None, RADIUS (无, RADIUS)** — 表示没有使用任何验证方法。如果需要验证，则在 RADIUS 服务器上验证。

**Guest VLAN (来宾 VLAN)** — 为所有端口指定来宾 VLAN。可能的字段值包括：

**Unconfigured (未配置)** — 没有为所有端口配置来宾 VLAN。

**VLAN ID**— 显示系统中配置的 VLAN 的 ID。选择要用作所有端口的来宾 VLAN 的 VLAN。

## 接口参数

**Interface (接口)** — 选择受影响的 Unit (单元) 和 Port (端口)。

**Guest VLAN Mode (来宾 VLAN 模式)** — 在此接口上启用或禁用来宾 VLAN 模式。

**Admin Interface Control (管理接口控制)** — 定义端口授权状态。可能的字段值包括：

**Automode (自动模式)** — 自动检测接口模式。

**Authorized (已授权)** — 在未经验证的情况下，将接口置于已授权状态。接口在未进行基于客户端端口的验证的情况下发送和接收正常通信。

**Unauthorized (未授权)** — 通过将接口置于未授权状态，拒绝选定接口对系统进行访问。交换机无法通过该接口向客户端提供验证服务。

**Current Interface Control (当前接口控制)** — 显示当前端口的授权状态。

**Periodic Re-Authentication (定期重新验证)** — 如果启用该选项，则会定期重新验证选定的端口。

**Re-Authentication Period (300-4294967295) (重新验证间隔 [300-4294967295])** — 表明要重新验证选定端口的时间段。字段值以秒为单位。字段默认值为 3600 秒。

**Re-Authenticate Now (立即重新验证)** — 如果选定该选项，将强制立即重新验证端口。

**Authentication Server Timeout (1-65535) (验证服务器超时 [1-65535])** — 定义交换机模块将请求重新发送到验证服务器之前经过的时间。字段值以秒为单位。字段默认值为 30 秒。

**Resending EAP Identity Request (1-65535) (重新发送 EAP 标识请求 [1-65535])** — 定义重新发送 EAP 请求之前经过的时间。字段值以秒为单位。字段默认值为 30 秒。

**Quiet Period (0-65535) (无提示周期 [1-65535])** — 定义交换机在验证交换失败之后处于无提示状态的时间。可能的字段范围为 0 至 65535。字段值以秒为单位。字段默认值为 60 秒。

**Supplicant Timeout (1-65535) (申请方超时 [1-65535])** — 定义 EAP 请求被重新发送到用户之前经过的时间。字段值以秒为单位。字段默认值为 30 秒。

**Max EAP Requests (1-10) (最大 EAP 请求次数 [1-10])** — 定义交换机因未收到回复而重新启动验证过程之前发送 EAP 请求的最大次数。可能的字段范围为 1 至 10。字段默认值为 2 次重试。

## 显示基于端口的验证表

打开 **Port Based Authentication (基于端口的验证)** 页面。

单击 **Show All (全部显示)**。

系统将打开 **Port Based Authentication Table (基于端口的验证表)** 页面，其中显示了表的左侧：

图 8-2. 基于端口的验证表



Port Based Authentication Table Print Refresh

Unit: 1

Ports	Admin Port Control	Current Port Control	Periodic Re-Authentication	Re-Authentication Period	Re-Authenticate Now	On Per
1 1/g1	Autmode	Authorized	Disable	3600	<input type="checkbox"/>	60
2 1/g2	Autmode	Authorized	Disable	3600	<input type="checkbox"/>	60
3 1/g3	Autmode	Authorized	Disable	3600	<input type="checkbox"/>	60
4 1/g4	Autmode	Authorized	Disable	3600	<input type="checkbox"/>	60
5 1/g5	Autmode	Authorized	Disable	3600	<input type="checkbox"/>	60
-----						
23 1/g23	Autmode	Authorized	Disable	3600	<input type="checkbox"/>	60
24 1/g24	Autmode	Authorized	Disable	3600	<input type="checkbox"/>	60
25 1/xg1	Autmode	Authorized	Disable	3600	<input type="checkbox"/>	60
26 1/xg2	Autmode	Authorized	Disable	3600	<input type="checkbox"/>	60
27 1/xg3	Autmode	Authorized	Disable	3600	<input type="checkbox"/>	60
28 1/xg4	Autmode	Authorized	Disable	3600	<input type="checkbox"/>	60

Apply Changes Back

使用水平滚动条或者单击屏幕底部的右箭头，以显示表的右侧。

**Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **Port Based Authentication Table** (基于端口的验证表)。

## 重新验证一个端口

打开 **Port Based Authentication** (基于端口的验证) 页面。

选中 **Edit** (编辑) 复选框以选择要重新验证的 **Unit/Port** (单元/端口)。

选中 **Reauthenticate Now** (立即重新验证) 复选框。

单击 **Apply Changes** (应用更改)。

系统将重新验证指定的端口并更新设备。

## 在基于端口的验证表中重新验证多个端口

打开 **Port Based Authentication** (基于端口的验证) 页面。

单击 **Show All** (全部显示)。

系统将显示 **Port Based Authentication Table** (基于端口的验证表)。

选中 **Edit** (编辑) 复选框以选择要重新验证的 **Units/Ports** (单元/端口)。

要定期重新验证，请将 **Periodic Re-Authentication** (定期重新验证) 设置为 **Enable** (启用)，并为所需的所有端口指定 **Re-Authentication Period** (重新验证间隔)。

要立即重新验证，请选中要重新验证的所有端口的 **Reauthenticate Now** (立即重新验证) 复选框。

单击 **Apply Changes** (应用更改)。

系统将重新验证 (立即或定期) 指定端口并更新设备。

## 更改管理端口控制

打开 **Port Based Authentication**（基于端口的验证）页面。

单击 **Show All**（全部显示）。

系统将显示 **Port Based Authentication Table**（基于端口的验证表）。

滚动到表的右侧，并选中要配置的每个端口的 **Edit**（编辑）复选框。根据需要将所选端口的 **Admin Port Control**（管理端口控制）更改为 **Authorized**（已授权）、**Unauthorized**（未授权）或 **Automode**（自动模式）。只有 **Automode**（自动模式）实际使用 dot1x 进行授权。**Authorized**（已授权）和 **Unauthorized**（未授权）是手工覆盖。

单击 **Apply Changes**（应用更改）。

系统将为指定的端口更新 Admin Port Control（管理端口控制）并更新设备。

## 使用 CLI 命令启用基于端口的验证

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 802.1X 命令

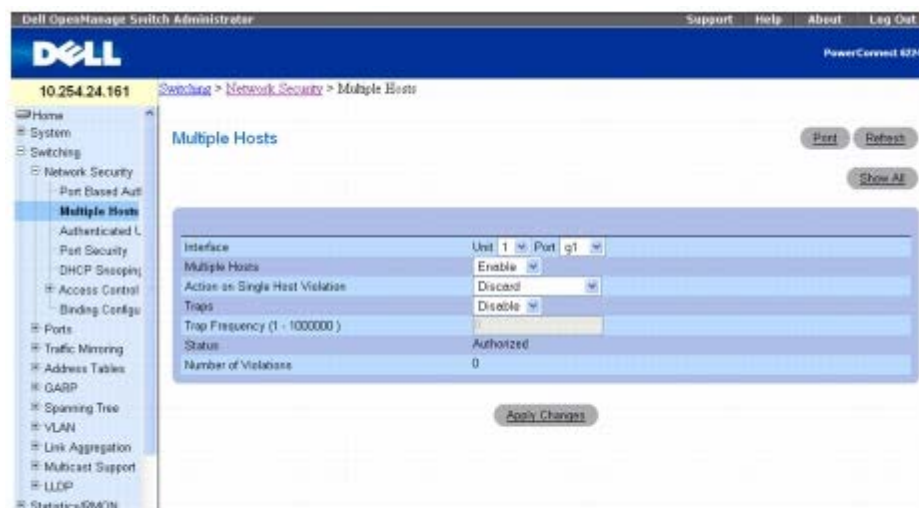
## 多台主机

端口处于多台主机模式下时，只需要一台交换机在该端口上进行验证。一旦验证成功，该端口上的所有交换机都可访问网络。如果端口由于任何原因变成非授权状态，则所有交换机均不能访问网络，而必须重新启动验证过程。

**Multiple Hosts**（多台主机）页面提供了用于为特定端口定义基于端口的高级验证设置的信息。

要显示 **Multiple Hosts**（多台主机）页面，请在树视图中单击 **Switching**（交换）® **Network Security**（网络安全保护）® **Multiple Host**（多台主机）。

图 8-3. 多台主机



**Multiple Hosts**（多台主机）页面包含以下字段：

**Interface**（接口）— 指定要配置基于端口的高级验证设置的 **Unit**（单元）和 **Port**（端口）号。

**Multiple Hosts**（多台主机）— 启用或禁用一台主机以授权多台主机进行系统访问。必须启用此设置，以便在选定的端口上禁用入口筛选或使用锁定端口的安全保护。

**Action on Single Host Violation**（单台主机侵入操作）— 定义对以单台主机模式到达的信息包所采取的操作，这些信息包来自其 MAC 地

址不是客户端（申请方）MAC 地址的主机。可能的字段值包括：

**Forward**（转发）— 转发来自未知源的信息包。但是，不记忆 MAC 地址。

**Discard**（丢弃）— 丢弃来自任何未记忆源的信息包。这是默认值。

**Discard Shut Down**（丢弃并关闭）— 丢弃来自任何未记忆源的信息包并关闭端口。在激活端口或重新启动交换机之前，端口保持关闭状态。

**Traps**（陷阱）— 在发生侵入时允许或禁止向主机发送陷阱。

**Trap Frequency (1-1000000)**（陷阱频率 [1-1000000]）— 定义向主机发送陷阱的间隔时间段。默认值为 10 秒。安全保护陷阱每 10 秒钟发送一次侵入的次数。

**Status**（状态）— 显示主机的状态。可能的字段值包括：

**Authorized**（已授权）— 表示端口控制当前处于自动模式下，而且客户端具有端口的完全访问权限。

**Unauthorized**（未授权）— 表示端口控制为 *Force Unauthorized*（强制未授权），端口链路断开或端口控制为 **Auto**（自动），但未通过该端口验证客户端。

**Not in auto mode**（不在自动模式下）— 表示端口控制为 *Forced Authorized*（强制授权），而且客户端具有端口的完全访问权限。

**Single-host Lock**（单台主机锁定）— 表示端口控制为 **Auto**（自动）并已通过该端口对单个客户端进行了验证。

**No Single Host**（非单台主机）— 表示已启用 **Multiple Host**（多台主机）。

**Number of Violations**（侵入数目）— 显示以单台主机模式到达接口的信息包的数目，这些信息包来自其 MAC 地址不是客户端（申请方）MAC 地址的主机。

## 显示多台主机表

□□□ 打开 **Multiple Hosts**（多台主机）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **Multiple Host Table**（多台主机表）。

图 8-4. 多台主机表

Port	Enable Multiple Hosts	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations	Edit
1 1/g1	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
2 1/g2	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
3 1/g3	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
4 1/g4	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
-----							
48 1/g48	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
49 1/g1	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
50 1/g2	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
51 1/g3	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
52 1/g4	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>

□□□ **Unit**（单元）下拉式菜单用于查看堆栈中其它单元（如果存在）的 **Multiple Host Table**（多台主机表）。

## 对一个端口启用/禁用多台主机

□□□ 打开 **Multiple Hosts**（多台主机）页面。

□□□ 在 **Interface**（接口）中选择受影响的 **Unit**（单元）和 **Port**（端口）。

□□□ 根据需要定义变量。

□□□ 单击 **Apply Changes**（应用更改）。

系统将对指定端口启用多台主机并更新设备。

## 对多个端口启用/禁用多台主机

□□□ 打开 **Multiple Hosts**（多台主机）页面。

□□□ 单击 **Show All**（全部显示）以显示 **Multiple Host Table**（多台主机表）。

□□□ 选中与需配置端口相关联的 **Edit**（编辑）复选框

□□□ 更改端口的变量

□□□ 单击 **Apply Changes**（应用更改）。

系统将更新所编辑的端口并更新设备。

## 使用 CLI 命令配置高级端口验证

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

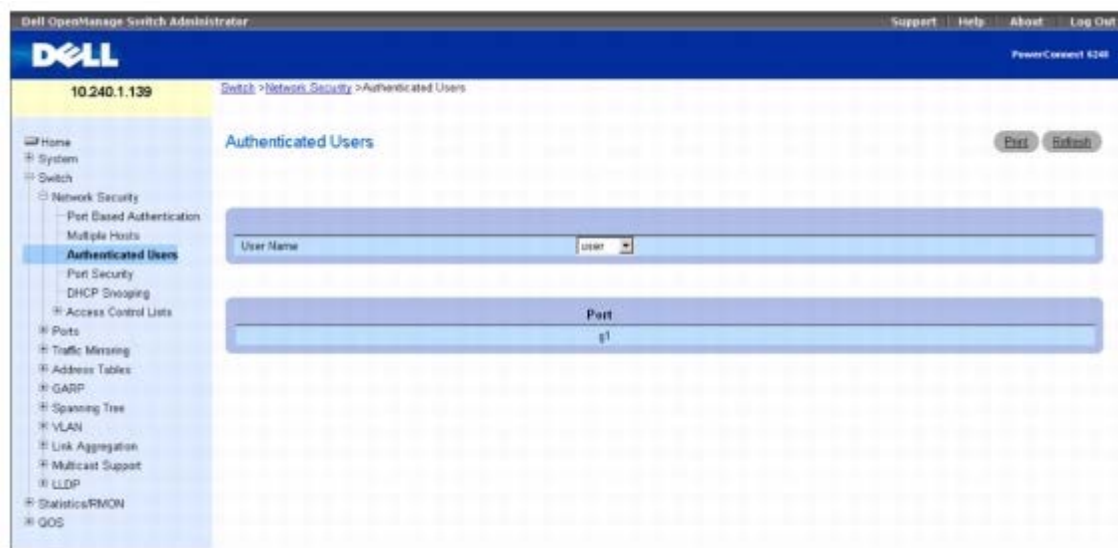
- 802.1X 命令

## 经验证的用户

**Authenticated Users**（经验证的用户）页面用于显示用户端口访问列表。

要显示 **Authenticated Users**（经验证的用户）页面，请在树视图中单击 **Switching**（交换）® **Network Security**（网络安全保护）® **Authenticated Users**（经验证的用户）。

图 8-5. 经验证的用户



**Authenticated Users**（经验证的用户）页面包含以下字段：

**User Name**（用户名）— 从通过 RADIUS 服务器授权的用户的列表中指定一名用户。

**Port**（端口）— 列出用于验证的端口。

## 使用 CLI 命令显示经验证的用户

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 802.1X 命令

## 端口安全保护

可以针对每个端口启用端口安全保护。如果端口被锁定，则只能转发其源 MAC 地址为允许的信息包。所有其它信息包都将被丢弃。可用两种方法之一定义允许的 MAC 地址：动态或静态。请注意，如果端口被锁定，两种方法可同时使用。

动态锁定对 Port Security（端口安全保护）采用“首次到达”机制。您可对锁定的端口指定可记忆的地址数目。未达到限定数目前，端口将正常记忆并转发具有未知源 MAC 地址的信息包。一旦达到限定数目，端口将不再记忆地址。端口将丢弃所有源 MAC 地址尚未记忆的信息包。请注意，您可以将可允许动态条目的数值设为零，从而有效禁用动态锁定。

静态锁定允许您指定端口上允许的 MAC 地址列表。信息包的处理方式与动态锁定相同：端口只转发其源 MAC 地址为允许的信息包。

要查看特定端口上记忆的 MAC 地址、向端口添加静态 MAC 地址或删除静态 MAC 地址条目，请参阅[配置地址表](#)。

禁用的端口只能在 **Configuring Ports**（配置端口）页面中激活。

要显示 **Port Security**（端口安全保护）页面，请在树视图中单击 **Switching**（交换）® **Network Security**（网络安全保护）® **Port Security**（端口安全保护）。

图 8-6. 端口安全保护



**Interface** (接口) — 选择要配置端口安全保护设置的 **Unit** (单元) 和 **Port** (端口) 或 **LAG**。

**Set Port** (设置端口) — 允许锁定端口/LAG。一旦端口锁定，将从数据库中删除该端口上被交换机动态记忆的所有当前地址。

**Action on Violation** (侵入操作) — 指定对到达端口/LAG 的信息包所采取的操作。在端口/LAG 解除锁定的情况下，该字段灰显。可能的值包括：

**Discard** (丢弃) — 丢弃来自任何未记忆源的信息包。这是默认值。

**Forward** (转发) — 转发来自未知源的信息包。不记忆 **MAC** 地址。

**Shutdown** (关闭) — 丢弃来自任何未记忆其源地址的信息包并发送陷阱。此外，入口端口将禁用。

**Traps** (陷阱) — 启用或禁用当锁定端口/LAG 上接收到信息包时发送陷阱。

**Trap Frequency (1-1000000)** (陷阱频率 [1-1000000]) — 指定两次陷阱之间的时间间隔 (以秒为单位)。

**Max Learned Addresses (1-100)** (最大记忆地址数量 [1-100]) — 指定端口可以记忆的安全 **MAC** 地址的最大数量。

## 定义锁定端口

□□□ 打开 **Port Security** (端口安全保护) 页面。

□□□ 选择接口类型和编号。

□□□ 在 **Set Port** (设置端口) 下拉式菜单中选择 **Locked** (锁定)。

□□□ 填写其余字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统会将锁定的端口/LAG 添加到 **Port Security** (端口安全保护) 表并更新设备。

## 查看端口安全保护表

□□□ 打开 **Port Security** (端口安全保护) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Port Security** (端口安全保护) 表。

图 8-7. 端口安全保护表



Port Security Table Print Refresh

Unit 1

Ports	Current Port Control	Set Port	Set Port Action	Trap	Trap Frequency	Edit
1 1/g1	Link Up	Unlock ▼	Discard ▼	Disable ▼	30	<input checked="" type="checkbox"/>
2 1/g2	Link Down	Unlock ▼	Discard ▼	Disable ▼	30	<input type="checkbox"/>
3 1/g3	Link Up	Unlock ▼	Discard ▼	Disable ▼	30	<input type="checkbox"/>
-----						
26 1/g2	Link Down	Unlock ▼	Discard ▼	Disable ▼	30	<input type="checkbox"/>
27 1/g3	Link Down	Unlock ▼	Discard ▼	Disable ▼	30	<input type="checkbox"/>
28 1/g4	Link Down	Unlock ▼	Discard ▼	Disable ▼	30	<input type="checkbox"/>

Apply Changes Back

□□□ **Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **Port Security Table** (端口安全保护表)。

## 定义多个锁定端口

□□□ 打开 **Port Security** (端口安全保护) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Port Security** (端口安全保护) 表。

□□□ 对每个要更改参数的端口单击 **Edit** (编辑)。

□□□ 现在可根据需要编辑这些端口的字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将更改保存到 **Port Security** (端口安全保护) 表并更新设备。

## 使用 CLI 命令配置端口安全保护

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- 地址表命令

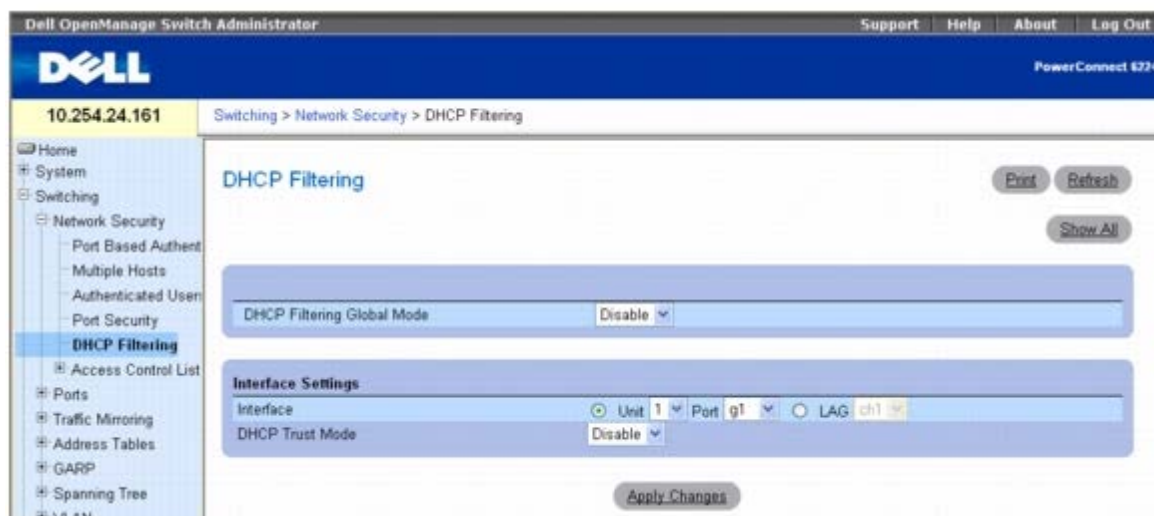
## DHCP 筛选

DHCP 筛选是一项很实用的功能, 可作为安全保护措施用于防范未经授权的 DHCP 服务器。已知攻击指的是未经授权的 DHCP 服务器对申请 IP 地址的客户端进行回应的情况。该服务器将客户端的网关配置为本机的 IP 地址。在此情况下, 客户端将其发向其它网络的 IP 通信全部发送至未经授权的主机。这为黑客提供了监测密码通信或使用“中间人”攻击的可乘之机。DHCP 筛选功能通过允许管理员将全部端口配置为可信端口或不可信端口而起作用。连接经授权 DHCP 服务器的端口应配置为可信端口。系统将转发可信端口接收到的所有 DHCP 回复。所有其它端口应配置为不可信。系统将丢弃接收到的所有 DHCP (或 BootP) 回复。

要显示 **DHCP Filtering** (DHCP 筛选) 页面, 请在树视图中单击 **Switching** (交换) ® **Network Security** (网络安全保护) ® **DHCP Filtering** (DHCP 筛选)。

图 8-8. DHCP 筛选





**DHCP Filtering** (DHCP 筛选) 页面包括以下字段：

**DHCP Filtering Global Mode** (DHCP 筛选全局模式) — 打开和关闭 DHCP Filtering (DHCP 筛选) 功能。默认设置为 Disabled (已禁用)。

**Interface** (接口) — 指定受影响的 Unit (单元) 和 Port (端口) 或 LAG。从下拉式菜单中选择所需 Unit (单元) 和 Port (端口) 或 LAG。

**DHCP Trust Mode** (DHCP 信任模式) — 启用或禁用信任模式。默认值为 Disable (禁用)。

## 添加 DHCP 筛选

□□□ 打开 **DHCP Filtering** (DHCP 筛选) 页面。

□□□ 指定受影响的 **Interface** (接口) 或 **LAG**。

□□□ 将 **DHCP Filtering Global Mode** (DHCP 筛选全局模式) 和 **DHCP Filtering Trust Mode** (DHCP 筛选信任模式) 设置为所需的设置。

□□□ 单击 **Apply Changes** (应用更改)。

系统将更新设备。

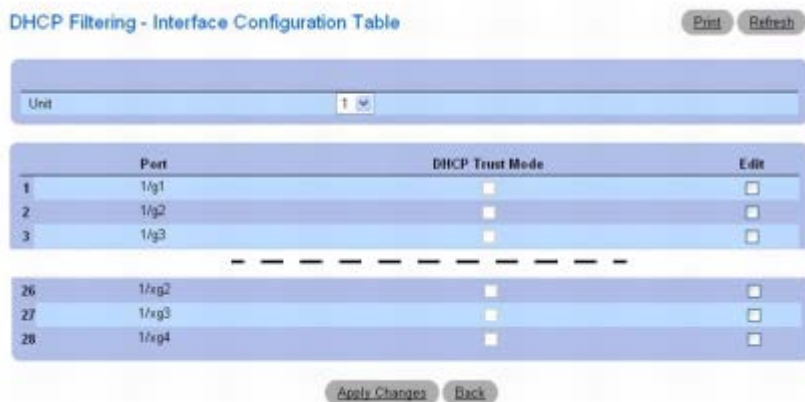
## 显示 DHCP 筛选接口配置表

□□□ 打开 **DHCP Filtering** (DHCP 筛选) 页面。

□□□ 单击 **Show All** (全部显示)。

**DHCP Filtering Table** (DHCP 筛选表) 页面将显示所有端口、其所在单元及其 **DHCP Trust Modes** (DHCP 信任模式)。

图 8-9. DHCP 筛选接口配置表



□□□ **Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **DHCP Filtering Table** (DHCP 筛选表)。

## 在多个端口上配置 DHCP 筛选

□□□ 打开 **DHCP Filtering** (DHCP 筛选) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **DHCP Filtering Interface Configuration** (DHCP 筛选接口配置) 表。

□□□ 对每个要配置的端口单击 **Edit** (编辑)。

□□□ 根据需要对这些端口启用或禁用 **DHCP Trust Mode** (DHCP 信任模式) 字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将更改保存到 DHCP Filtering Interface Configuration (DHCP 筛选接口配置) 表并更新设备。

## 使用 CLI 命令配置 DHCP 筛选

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- DHCP 筛选命令

## IP ACL 配置

访问控制列表 (ACL) 使网络管理员可以定义特定入口端口的分类操作和规则。交换机最多可支持 100 个 ACL。但是, 硬件的资源是有限的, 因此可能无法充分支持 100 个完全装入的 ACL。

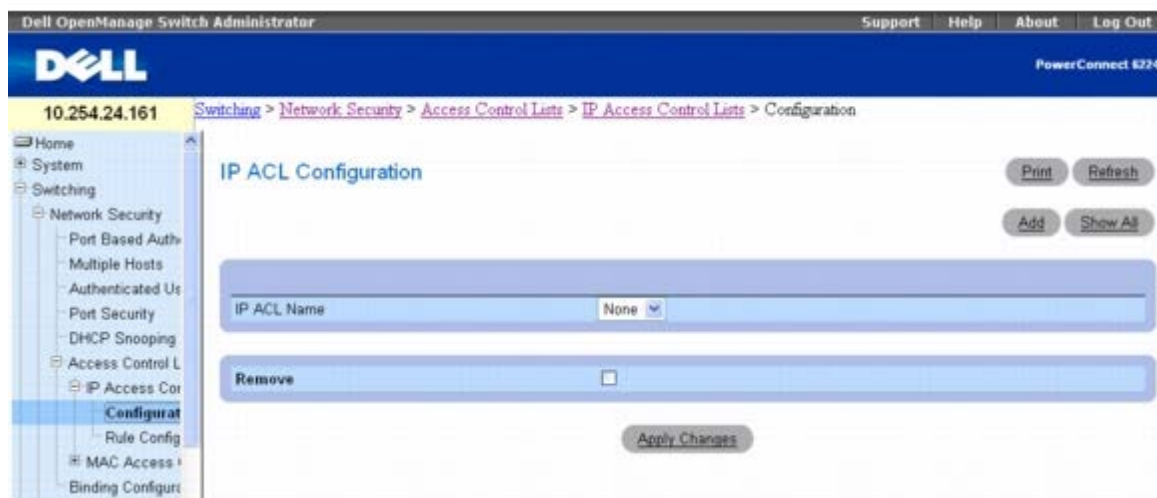
系统将在入口筛选信息包。如果筛选规则匹配, 则系统将采取某种操作, 包括丢弃信息包或禁用端口。例如: 网络管理员定义了一条 ACL 规则, 规定端口 20 可以接收 TCP 信息包。但是, 如果接收到 UDP 信息包, 系统将丢弃该信息包。

ACL 由访问控制条目 (ACE) 或称规则 (由确定通信分类的筛选器组成) 构成。每个 ACL 中可定义的规则总数为 10。

**IP ACL Configuration** (IP ACL 配置) 页面用于添加或删除基于 IP 的 ACL。

要显示 **IP ACL Configuration** (IP ACL 配置) 页面, 请在树视图中单击 **Switching** (交换) ® **Network Security** (网络安全保护) ® **Access Control Lists** (访问控制列表) ® **IP Access Control Lists** (IP 访问控制列表) ® **Configuration** (配置)。

图 8-10. IP ACL 配置



**IP ACL Configuration (IP ACL 配置)** 页面包含以下字段：

**IP ACL Name (IP ACL 名称)** — 指定用户定义的 ACL 名称。

**Remove (删除)** — 删除 IP ACL 字段中选择的 IP ACL。

## 添加基于 IP 的 ACL

□□□ 打开 **IP ACL Configuration (IP ACL 配置)** 页面。

□□□ 单击 **Add (添加)**。

系统将显示 **Add IP ACL (添加 IP ACL)** 页面。

图 8-11. 添加 IP ACL



□□□ 将所需的 **ACL Name (ACL 名称)** 输入到相关的输入项字段中。

□□□ 单击 **Apply Changes (应用更改)**。

系统将添加基于 IP 的 ACL 并更新设备。

## 删除基于 IP 的 ACL

□□□ 打开 **IP ACL Configuration (IP ACL 配置)** 页面，并从 **IP ACL** 下拉式菜单中选择要删除的 ACL。

□□□ 选中 **Remove ACL (删除 ACL)** 复选框。

□□□ 单击 **Apply Changes (应用更改)**。

系统将删除基于 IP 的 ACL 并更新设备。

## 显示 IP ACL

□□□ 打开 **IP ACL Configuration (IP ACL 配置)** 页面。

□□□ 单击 **Show All (全部显示)**。

**IP ACL Table (IP ACL 表)** 中将显示所有 IP ACL 及其相关数据。

图 8-12. IP ACL 表

	IP ACL Name	Rules	Direction	Interface	VLAN
1	ALC1	1	NONE	NONE	
2	ACL2	1	NONE	NONE	

## 使用 CLI 命令添加基于 IP 的 ACL

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- ACL 命令

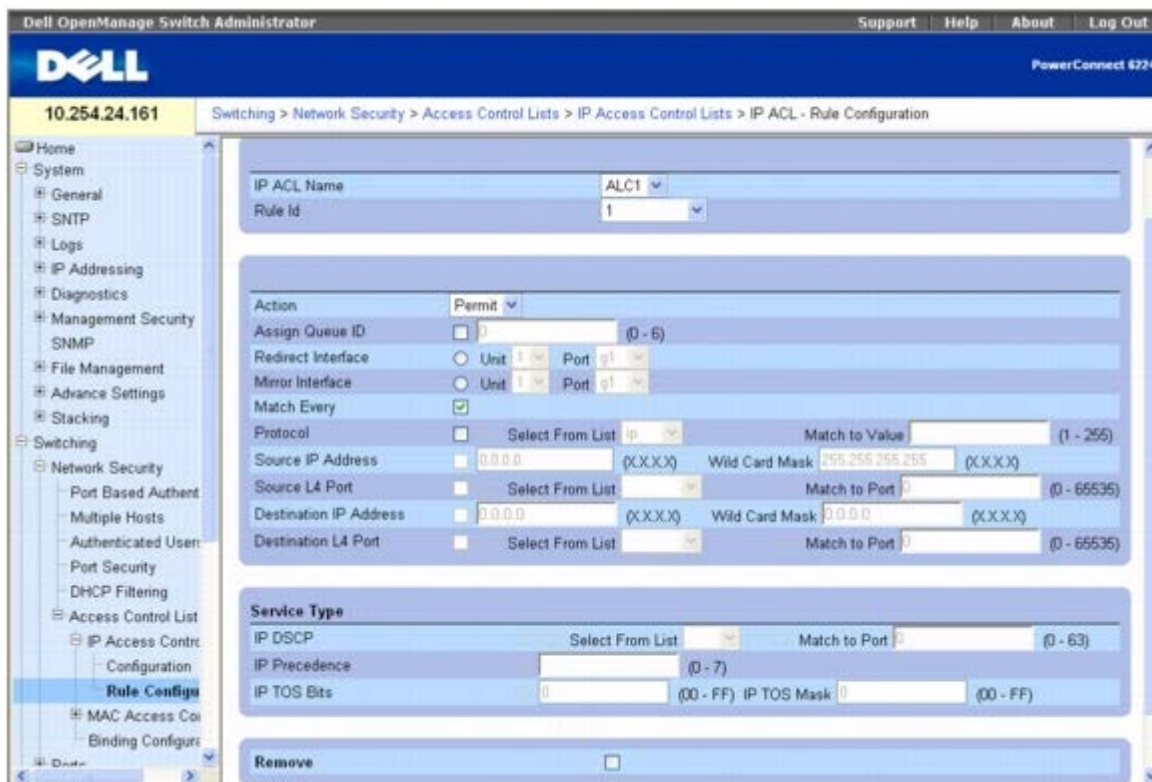
## IP ACL 规则配置

**IP ACL Rule Configuration (IP ACL 规则配置)** 页面用于定义基于 IP 的 ACL 所使用的规则。访问列表定义包括指定匹配标准的通信是正常转发还是丢弃的规则。此外，您还可指定将通信分配给特定队列、用于某些通信的筛选器、更改 VLAN 标签、关闭端口和/或将通信重定向到特定端口。

**注意：** 在 ACL 列表的末尾有一条隐式“拒绝所有”规则。这意味着，如果将 ACL 应用于信息包而且如果没有显式规则匹配，则使用最后的隐式“拒绝所有”规则并丢弃信息包。

要显示 **IP ACL Rule Configuration (IP ACL 规则配置)** 页面，请在树视图中单击 **Switching (交换)** ® **Network Security (网络安全保护)** ® **Access Control Lists (访问控制列表)** ® **IP Access Control Lists (IP 访问控制列表)** ® **Rule Configuration (规则配置)**。

图 8-13. IP ACL — 规则配置 (标准)



**IP ACL Rule Configuration (IP ACL 规则配置)** 页面包含以下字段：

**IP ACL Name (IP ACL 名称)** — 指定现有的 IP ACL。使用“[IP ACL 配置](#)”页面设置新的 IP ACL。

**Rule ID (规则 ID)** — 选择或创建用户定义的 ACL。输入现有的 Rule ID (规则 ID) 或新创建一个，创建需要在下拉式菜单中选择 Create (创建) 并在随后的字段内输入所需的新 Rule ID (规则 ID)。单击 **Apply Changes (应用更改)** 之后，新的 ID 即创建成功。每个 ACL 最多可创建 10 条规则。

**Action (操作)** — 选择 ACL 转发操作。在下拉式菜单中选择选项，应用转发操作。可能的值包括：

**Permit (允许)** — 转发符合 ACL 标准的信息包。

**Deny (拒绝)** — 丢弃符合 ACL 标准的信息包。

**Assign Queue ID (分配队列 ID)** — 单击此复选框以应用此标准，然后输入一个介于 0 到 6 之间的识别号。

**Redirect Interface (重定向接口)** — 从接口下拉式列表选择一个可以将符合此规则的信息包重定向到的接口。

**Mirror Interface (镜像接口)** — 从接口下拉式列表选择一个可以将符合此规则的信息包镜像到的接口。

**Logging (记录)** — 当选中此复选框时，将允许记录特定的 ACL。系统只支持记录 Deny (拒绝) 操作。

**Match Every (全部匹配)** — 要求信息包与该 ACL 标准匹配。选中复选框以应用此标准。Match Every (全部匹配) 与其它筛选规则互斥，因此一旦选中，屏幕上其它规则均不可选。

**Protocol (协议)** — 要求信息包协议与此处所列的协议匹配。选中复选框以应用此标准，然后选择下列选项之一：

**Select from List (从列表中选择)** — 从协议下拉列表中选择规则可基于其上的协议。

**Match to Value (与值匹配)** — 单击添加用户定义的 Protocol ID (协议 ID)，信息包应通过此 ID 与规则匹配。

**Source IP Address (源 IP 地址)** — 要求信息包源端口 IP 地址与此处所列的地址匹配。选中复选框并输入地址以应用此标准。

**Wild Card Mask (通配符掩码)** — 指定源 IP 地址的通配符掩码。通配符掩码将确定要使用的位以及要忽略的位。通配符掩码 255.255.255.255 表示所有位都不重要。通配符 0.0.0.0 表示所有位都重要。选中 **Source IP Address (源 IP 地址)** 复选框时，此字段为必填项。

**Source L4 Port (源 L4 端口)** — 要求信息包的 TCP/UDP 源端口与此处所列的端口匹配。选中复选框以应用此标准，然后在下拉式菜单中选择下列选项之一：

**Select From List**（从列表中选择）— 在源端口列表中单击选择规则可基于其上的源端口。

**Match to Port**（与端口匹配）— 单击添加用户定义的 Port ID（端口 ID），信息包应通过此 ID 与规则匹配。

**Destination IP Address**（目的地 IP 地址）— 要求信息包目的地端口 IP 地址与此处所列的地址匹配。选中复选框并输入地址以应用此标准。

**Wild Card Mask**（通配符掩码）— 指定目的地 IP 地址的通配符掩码。选中 **Destination IP Address**（目的地 IP 地址）复选框时，此字段为必填项。

**Destination L4 Port**（目的地 L4 端口）— 要求信息包 TCP/UDP 目的地端口与此处所列的端口匹配。选中复选框以应用此标准，然后选择下列选项之一：

**Select From List**（从列表中选择）— 在目的地端口列表中选择规则可基于其上的目的地端口。

**Match to Port**（与端口匹配）— 单击添加用户定义的 Port ID（端口 ID），信息包应通过此 ID 与规则匹配。

## 服务类型字段

选择以下三个要用于信息包与 **ACL** 匹配的 **Match**（匹配）字段之一：

**IP DSCP** — 将信息包 DSCP 值与规则进行匹配。使用 DSCP 值或 IP 优先级值，将信息包与 **ACL** 进行匹配。

**Select From List**（从列表中选择）— 从 DSCP 关键字值列表中选择。

**Match to Port**（与端口匹配）— 单击添加用户定义的 Port ID（端口 ID）。

**IP Precedence**（IP 优先级）— 选中后，将信息包 IP Precedence（IP 优先级）值与规则进行匹配。输入 IP Precedence（IP 优先级）值进行匹配。使用 DSCP 值或 IP 优先级值，将信息包与 **ACL** 进行匹配。


**IP TOS Bits**（IP TOS 位）— 选中后，对 IP 头中的 Type of Service（服务类型）位进行匹配。

**TOS Bits**（TOS 位）— 要求信息包 TOS 字段中的位与在此输入的两字节十六位数字相匹配。

**TOS Mask**（TOS 掩码）— 指定用于同信息包中 IP TOS 字段相比较的比特位置。

**Remove**（删除）— 当选中 **Remove**（删除）复选框并单击 **Apply Changes**（应用更改）时，将删除规则 ID。

## 修改基于 IP 的规则

 **注：** 只有在其所属 ACL 未与接口捆绑的情况下，才能修改规则。

□□□ 打开 **IP ACL Rule Configuration**（IP ACL 规则配置）页面。

□□□ 从 **IP ACL** 下拉式菜单中选择所需的 ACL。

□□□ 从 **Rule ID**（规则 ID）下拉式菜单中选择所需的规则。

□□□ 根据需要修改其余字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将修改基于 IP 的规则并更新设备。

## 为基于 IP 的 ACL 添加新的规则

□□□ 打开 **IP ACL Rule Configuration**（IP ACL 规则配置）页面。

□□□ 从 **IP ACL** 下拉式菜单中选择所需的 ACL。



□□□ 从 **Rule ID** (规则 ID) 下拉式菜单中选择 **Create Rule** (创建规则) 并输入一个新的 ID 编号。

□□□ 按需要定义其余字段。

□□□ 单击 **Apply Changes** (应用更改)。

新的规则将被分配至指定的基于 IP 的 ACL。

## 使用 CLI 命令定义基于 IP 的 ACL 规则

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

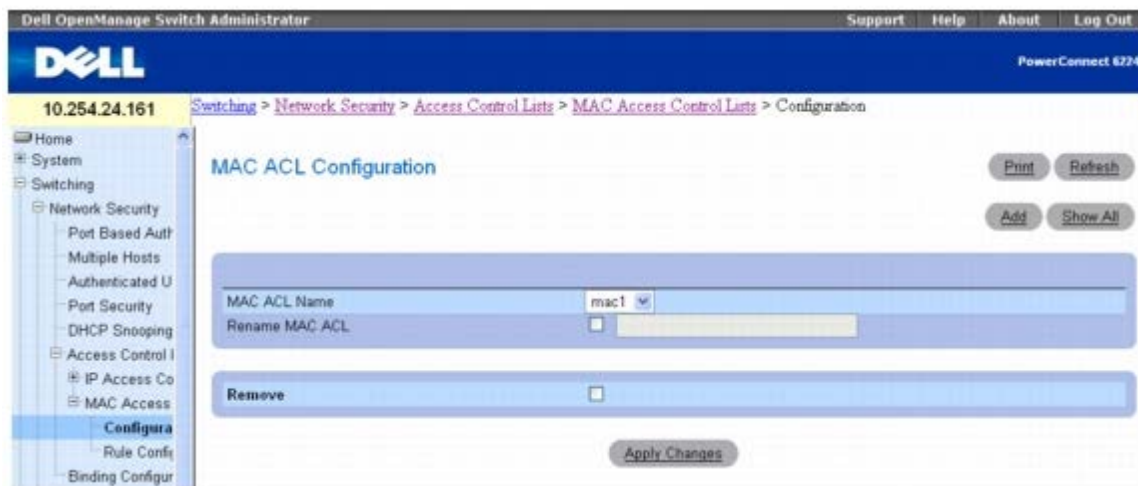
- ACL 命令

## MAC ACL 配置

**MAC ACL Configuration** (MAC ACL 配置) 页面使网络管理员能够定义基于 MAC 的 ACL。有关 ACL 的说明，请参阅“[IP ACL 配置](#)”。

要显示 **MAC ACL Configuration** (MAC ACL 配置) 页面，请在树视图中单击 **Switching** (交换) ⑥ **Network Security** (网络安全保护) ⑥ **Access Control Lists** (访问控制列表) ⑥ **MAC Access Control Lists** (MAC 访问控制列表) ⑥ **Configuration** (配置)。

图 8-14. MAC ACL 配置



**MAC ACL Configuration** (MAC ACL 配置) 页面包含以下字段：

**MAC ACL Name** (MAC ACL 名称) — 用户定义的 ACL 名称。

**Rename MAC ACL** (重命名 MAC ACL) — 要重命名 MAC ACL，请选中该复选框并在字段中输入新的 MAC ACL 名称。

**Remove** (删除) — 选中该字段，然后单击 **Apply Changes** (应用更改) 按钮，以删除 MAC ACL 字段中列出的 MAC ACL。

## 添加基于 MAC 的 ACL

□□□ 打开 **MAC ACL Configuration** (MAC ACL 配置) 页面。

□□□ 单击 **Add** (添加) 以显示 **Add MAC ACL** (添加 MAC ACL) 页面。

图 8-15. 添加 MAC ACL



□□□ 将所需的 **MAC ACL Name** (**MAC ACL** 名称) 输入到输入项字段中。

□□□ 单击 **Apply Changes** (应用更改)。

系统将添加基于 MAC 的 ACL 并更新设备。

## 删除基于 MAC 的 ACL

□□□ 打开 **MAC ACL Configuration** (**MAC ACL** 配置) 页面，并从 **MAC ACL** 下拉式菜单中选择要删除的 ACL。

□□□ 选中 **Remove** (删除) 复选框。

□□□ 单击 **Apply Changes** (应用更改)。

系统将删除基于 MAC 的 ACL 并更新设备。

## 显示 MAC ACL

□□□ 打开 **MAC ACL Configuration** (**MAC ACL** 配置) 页面。

□□□ 单击 **Show All** (全部显示)。

屏幕上将显示所有 MAC ACL 及其相关数据。

图 8-16. MAC ACL 表

MAC ACL Name	Rules	Direction	Interface	VLAN
1 big_mac	1	NONE	NONE	NONE

## 使用 CLI 命令配置基于 MAC 的 ACL

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

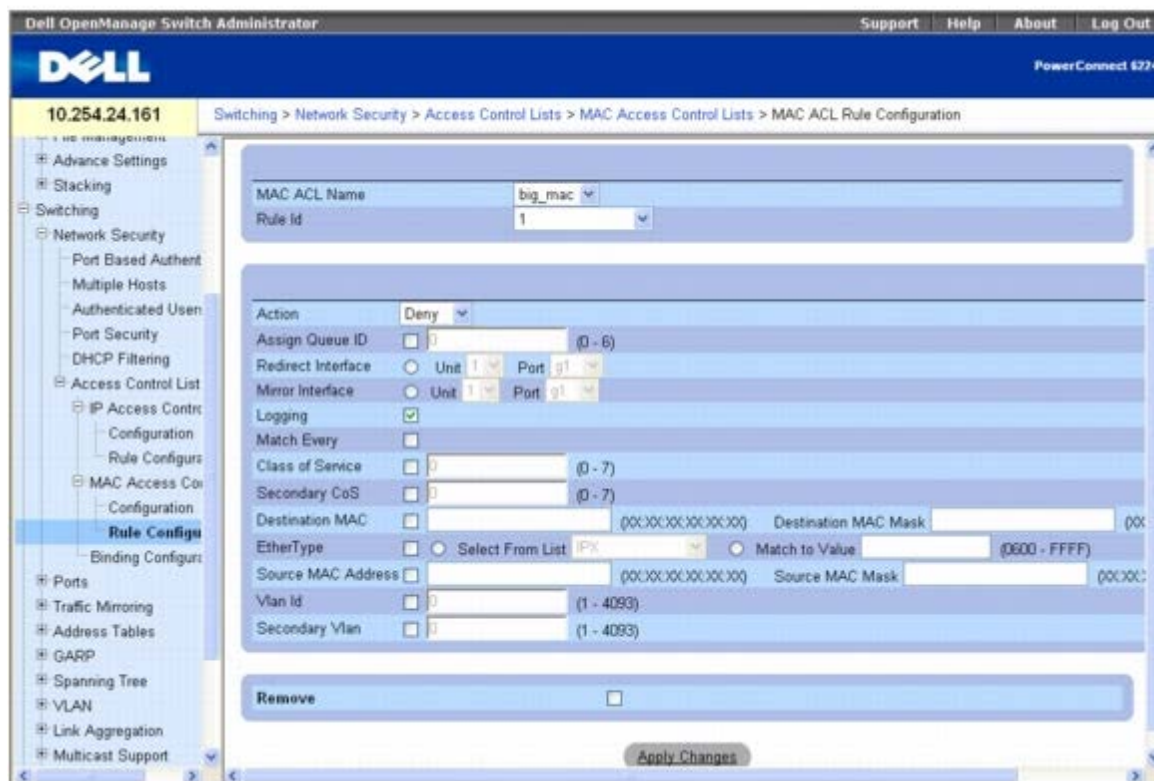
- ACL 命令

## MAC ACL 规则配置

**MAC ACL Rule Configuration** (**MAC ACL** 规则配置) 页面用于定义基于 MAC 的 ACL 所使用的规则。访问列表定义包括指定匹配标准的通信是正常转发还是丢弃的规则。每个列表中的最后一条规则是默认的“拒绝所有”规则。

要显示 **MAC ACL Rule Configuration** (**MAC ACL** 规则配置) 页面，请在树视图中单击 **Switching** (交换) ® **Network Security** (网络安全保护) ® **Access Control Lists** (访问控制列表) ® **MAC Access Control Lists** (**MAC** 访问控制列表) ® **Rule Configuration** (规则配置)。

图 8-17. MAC ACL - 规则配置



**MAC ACL Rule Configuration (MAC ACL 规则配置)** 页面包含以下字段：

**MAC ACL Name (MAC ACL 名称)** — 指定现有的 MAC ACL。使用 [MAC ACL Configuration \(MAC ACL 配置\)](#) 页面设置新的 MAC ACL。

**Rule ID (规则 ID)** — 选择或创建用户定义的 ACL。输入现有的 Rule ID (规则 ID) 或新建一个，创建需要在下拉式菜单中选择 Create (创建) 并在随后的字段内输入所需的新 Rule ID (规则 ID)。单击 **Apply Changes (应用更改)** 之后，新的 ID 即创建成功。

**Action (操作)** — 选择 ACL 转发操作，该操作可以是以下值之一：

**Permit (允许)** — 转发符合 ACL 标准的信息包。

**Deny (拒绝)** — 丢弃符合 ACL 标准的信息包。

**Assign Queue ID (分配队列 ID)** — 单击此复选框以应用此标准，然后输入一个介于 0 到 6 之间的识别号。

**Redirect Interface (重定向接口)** — 从接口下拉式列表选择一个可以将符合此规则的信息包重定向到的接口。

**Mirror Interface (镜像接口)** — 从接口下拉式列表选择一个可以将符合此规则的信息包镜像到的接口。

**Logging (记录)** — 单击此复选框将允许对此 ACL 进行记录。此功能只适用于 Deny (拒绝) 操作。

**Match Every (全部匹配)** — 要求信息包与该 ACL 标准匹配。选中复选框以应用此标准。

**Class of Service (服务级别)** — 要求信息包 CoS 与此处列出的 CoS 值匹配。选中该复选框，并输入 0 至 7 之间的 CoS 值以应用此标准。

**Secondary CoS (第二级 CoS)** — 要求信息包第二级 CoS 与此处列出的 CoS 值匹配。选中该复选框，并输入 0 至 7 之间的 CoS 值以应用此标准。

**Destination MAC Address (目的地 MAC 地址)** — 要求信息包目的地端口 MAC 地址与此处所列的地址匹配。选中复选框并输入地址以应用此标准。

**Destination MAC Mask (目的地 MAC 掩码)** — 如果需要，输入与 Destination MAC (目的地 MAC) 相关的 MAC Mask (MAC 掩码) 进行匹配。

**EtherType (以太网类型)** — 要求信息包 EtherType (以太网类型) 与此处所列的 EtherType (以太网类型) 匹配。选中复选框并从列表中选择或输入 EtherType ID (以太网类型 ID)：

**Select from List**（从列表中选择）— 从下拉式菜单中选择所需的 EtherType（以太网类型）。

**Match to Port**（与端口匹配）— 输入所需端口号进行匹配。

**Source MAC Address**（源 MAC 地址）— 要求信息包源端口 MAC 地址与此处所列的地址匹配。选中复选框并输入地址以应用此标准。


**Source MAC Mask**（源 MAC 掩码）— 如果需要，输入源 MAC 地址要进行匹配的 MAC 掩码。

**Vlan Id**— 要求信息包 VLAN ID 与此处所列的 ID 匹配。选中复选框并输入 VLAN ID 以应用此标准。可能的字段值为 1 至 4093。

**Secondary Vlan**（次级 Vlan）— 要求信息包次级 VLAN ID 与此处所列的 ID 匹配。选中复选框并输入次级 VLAN ID 以应用此标准。可能的字段值为 1 至 4093。

**Remove**（删除）— 当选中 **Remove**（删除）复选框并单击 **Apply Changes**（应用更改）时，将删除 MAC ACL 规则。

## 修改基于 MAC 的规则

 **注：** 只有在其所属 ACL 未与接口捆绑的情况下，才能修改规则。

打开 **MAC ACL Rule Configuration**（MAC ACL 规则配置）页面。

从 **MAC ACL** 下拉式菜单中选择所需的 ACL。

从 **Rule ID**（规则 ID）下拉式菜单中选择所需的规则。

根据需要修改其余字段。

单击 **Apply Changes**（应用更改）。

系统将修改基于 MAC 的规则并更新设备。

## 为基于 MAC 的 ACL 添加新的规则

打开 **MAC ACL Rule Configuration**（MAC ACL 规则配置）页面。

从 **MAC ACL** 下拉式菜单中选择所需的 ACL。

为 **Rule ID**（规则 ID）指定 **Create New Rule**（创建新规则）。

输入新的 ID 数字。

按需要定义其余字段。

单击 **Apply Changes**（应用更改）。

新的规则将被分配至指定的基于 MAC 的 ACL。

## 从基于 MAC 的 ACL 中删除规则

选择 ACL。

从 **Rule ID**（规则 ID）下拉式菜单中选择规则。

选中 **Remove**（删除）复选框。

单击 **Apply Changes**（应用更改）。

系统将删除基于 MAC 的 ACL 并更新设备。

## 使用 CLI 命令定义基于 MAC 的 ACL 规则

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- ACL 命令

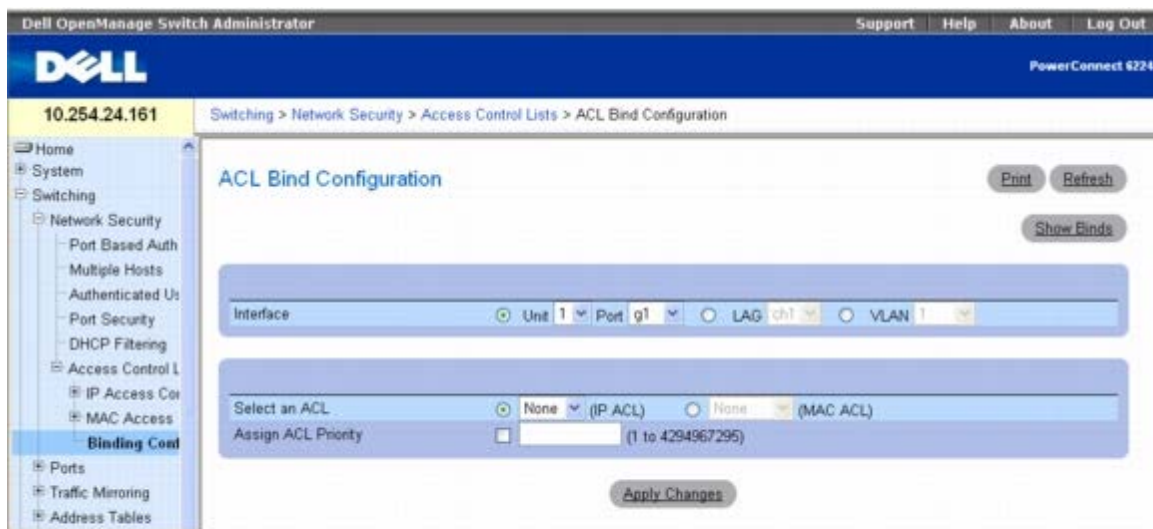
## ACL 捆绑配置

当 ACL 与接口捆绑时，所有已定义的规则都将应用于所选接口。**ACL Bind Configuration (ACL 捆绑配置)** 页面用于为 ACL 列表分配 ACL 优先级和接口。

在 Web 界面中，您可以配置入口方向的 ACL 规则，以使规则应用于端口收到的信息包。在 CLI 中，您可以配置入口或出口方向的 ACL 规则。出口 ACL 会对从端口流出的通信实施安全规则。您可以对任何物理（包括 10G）接口、LAG 或路由端口应用 ACL。

要显示 **ACL Bind Configuration (ACL 捆绑配置)** 页面，请在树视图中单击 **Switching (交换)** ® **Network Security (网络安全保护)** ® **Access Control Lists (访问控制列表)** ® **Binding Configuration (捆绑配置)**。

图 8-18. ACL 捆绑配置



**ACL Bind Configuration (ACL 捆绑配置)** 页面包含以下字段：

**Interface (接口)** — 此单选按钮可以按 Unit/port (单元/端口)、LAG 或 VLAN 选择接口。

**Select an ACL (选择 ACL)** — 选择传入信息包要匹配的 ACL 类型。信息包可与基于 IP 或基于 MAC 的 ACL 进行匹配。

**Assign ACL Priority (分配 ACL 优先级)** — 分配此 ACL 的优先级。如果有一个以上的 ACL 应用于一个接口，则系统首先检查最高优先级 ACL 的匹配标准。

### 将 ACL 分配给接口

□□□ 打开 **ACL Bind Configuration (ACL 捆绑配置)** 页面。

□□□ 在 **Interface (接口)** 字段中，指定要配置的 Unit (单元) 和 Port (端口)、LAG 或 VLAN。

□□□ 在 **Select an ACL (选择 ACL)** 字段中选择 IP 或 MAC ACL。



**注：**只要将 ACL 分配给端口、LAG 或 VLAN，则不匹配 ACL 的入口接口的数据流将匹配默认规则，即 Drop（丢弃）不匹配的信息包。

□□□ 在 **Assign ACL Priority**（分配 ACL 优先级）中指定优先级。

□□□ 单击 **Apply Changes**（应用更改）。

ACL 将连接至指定的接口。

## 删除 ACL 中的接口

□□□ 打开 **ACL Bind Configuration**（ACL 捆绑配置）页面。

□□□ 单击 **Show All**（全部显示）。

□□□ 在 **Interface**（接口）字段中，指定 **Unit**（单元）和 **Port**（端口）、LAG 或 VLAN 以查看该接口的 ACL 捆绑。

□□□ 选择一个或多个要删除的 ACL 的 **Remove**（删除）复选框。

□□□ 单击 **Apply Changes**（应用更改）。

系统将从接口中删除指定的 ACL。

## 使用 CLI 命令分配 ACL 成员关系

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- ACL 命令

---

## 配置端口

**Ports**（端口）菜单页面提供了用于配置端口功能的链接，其中包括风暴控制和端口镜像等以及用于执行虚拟端口检测的高级功能。

要显示该页面，请在树视图中单击 **Switching**（交换）® **Ports**（端口）。**Ports**（端口）菜单页面包含以下功能的链接：

- [全局参数](#)
- [端口配置](#)
- [受保护的端口配置](#)
- [LAG 配置](#)
- [风暴控制](#)

## 全局参数

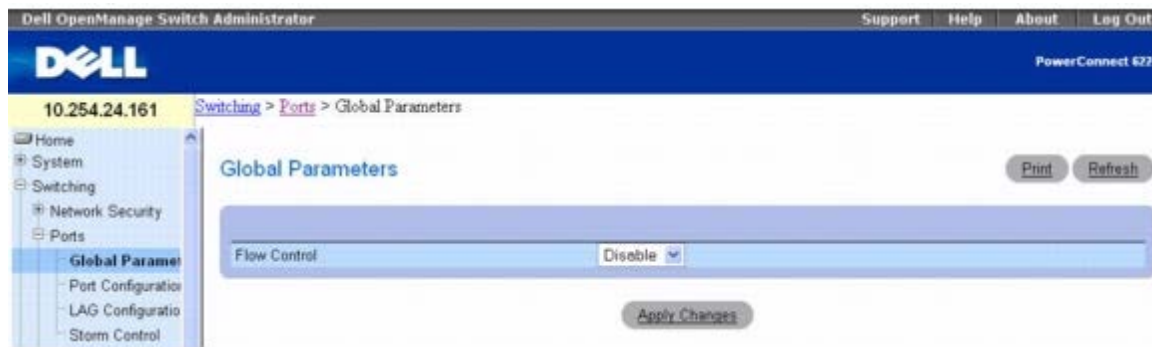
使用 **Global Parameters**（全局参数）配置 **Flow Control**（流控制）。**Flow Control**（流控制）允许在指定时间段内抑制来自一个交换机的通信量，而且只对直接连接的交换机进行定义。只能对配置为全双工操作模式的端口设置 **Flow Control**（流控制）。因为设置为自适应的端口可能无法添加为 LAG 成员，LAG 成员端口的流控制不能配置为自动。



**注：**Flow Control（流控制）与防队列头阻塞模式不兼容。交换机可在任一模式下工作，但不能同时使用两种模式。

要显示 **Global Parameters**（全局参数）页面，请在树视图中单击 **Switching**（交换）® **Ports**（端口）® **Global Parameters**（全局参数）。

图 8-19. 全局参数



**Global Parameters**（全局参数）页面包含以下字段：

**Flow Control**（流控制）— 从下拉式菜单中选择启用或禁用。此命令将影响堆栈中所有端口。默认值为已启用。

**Enable**（启用）— 打开交换机的入口背压机制。

**Disable**（禁用）— 交换机操作恢复为防队列头阻塞。

## 启用入口背压

- 打开 **Ports Global Parameters**（端口全局参数）页面。
- 从 **Flow Control**（流控制）字段的下拉式菜单中选择 **Enable**（启用）。
- 单击 **Apply Changes**（应用更改）。
- 系统将立即启用入口背压。

## 使用 CLI 命令配置流控制

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 以太网配置命令

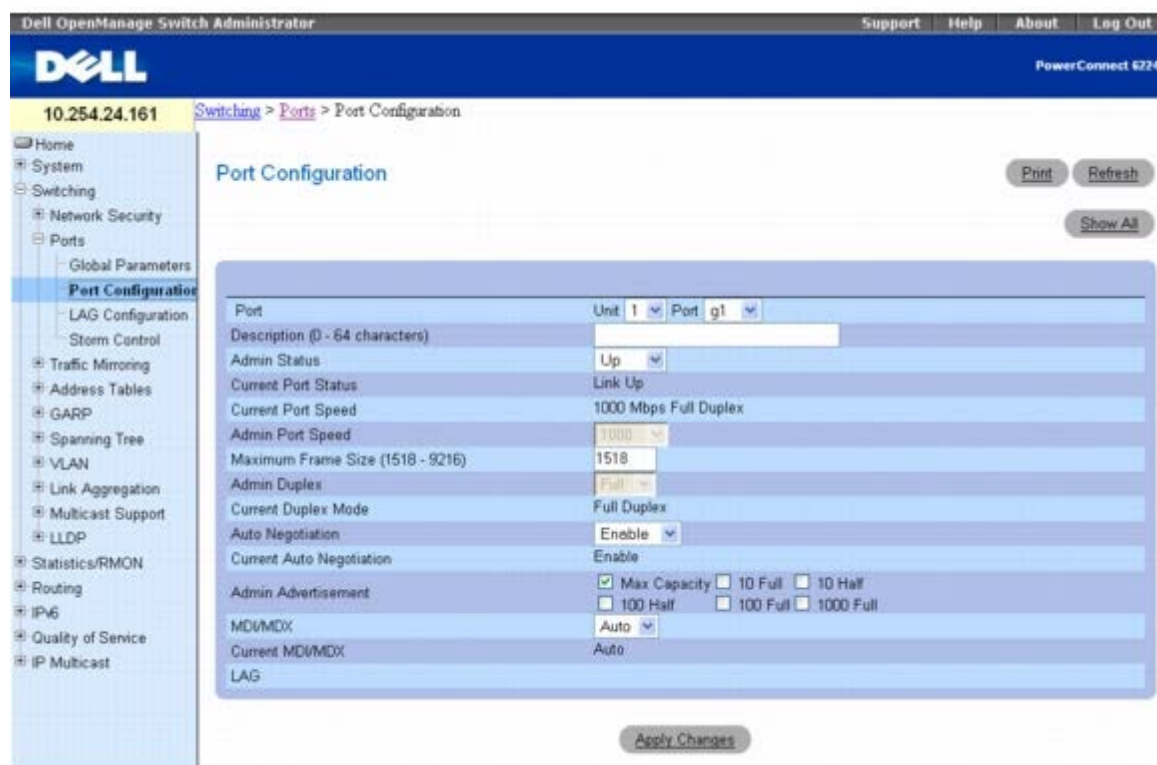
## 端口配置

**Port Configuration**（端口配置）页面用于定义端口参数。

要显示 **Port Configuration**（端口配置）页面，请在树视图中单击 **Switching**（交换）® **Ports**（端口）® **Port Configuration**（端口配置）。

图 8-20. 端口配置





**Port Configuration** (端口配置) 页面包含以下字段：

**Port** (端口) — 指定 Unit (单元) 和为其定义了端口参数的 Port (端口)。

**Description (0-64 Characters)** (说明 [0 至 64 个字符]) — 提供接口的简短说明，例如 Ethernet (以太网)。

**Admin Status** (管理状态) — 启用 (Up) 或禁用 (Down) 通过端口转发通信。

**Current Port Status** (当前端口状态) — 指定端口当前处于运行状态还是未运行状态。

**Current Port Speed** (当前端口速率) — 显示同步端口的实际速率 (以 bps 为单位)。

**Admin Port Speed** (管理端口速率) — 将端口速率强制设为所选的值 - 10M、100M、1000M 或 10000M。

**Maximum Frame Size (1518-9216)** (最大帧尺寸 [1518-9216]) — 指定阈值，系统将丢弃包大小不在此数值范围内的信息包。默认值为 1518。

**Admin Duplex** (管理双工) — 指定端口的双工模式。选项为 Full (全双工) 或 Half (半双工)。

**Full** (全双工) — 表示接口支持在交换机和客户端之间同时进行双向传输。

**Half** (半双工) — 表示接口在同一时间内仅支持在交换机和客户端之间进行单向传输。

**Current Duplex Mode** (当前双工模式) — 显示同步端口双工模式。

**Auto Negotiation** (自适应) — 在端口上启用 Auto Negotiation (自适应)。

Auto Negotiation (自适应) 是两个链接伙伴之间的协议，使一个端口可以将其传输速率、双工模式和流控制能力通知给伙伴端口。

**Current Auto Negotiation** (当前自适应) — 显示当前的 Auto Negotiation (自适应) 设置。

**Admin Advertisement** (管理公布) — 指定端口要公布的功能。可能的字段值包括：

**Max Capability** (最大功能) — 表示可接受所有端口速率和 Duplex (双工) 模式设置。

**10 Half (10M 半双工)** — 表示该端口的设置公布为 10 mbps 速率和半双工模式。

**10 Full (10M 全双工)** — 表示该端口的设置公布为 10 mbps 速率和全双工模式。

**100 Half (100M 半双工)** — 表示该端口的设置公布为 100 mbps 速率和半双工模式。

**100 Full (100M 全双工)** — 表示该端口的设置公布为 100 mbps 速率和全双工模式。



**1000 Full (1000M 全双工)** — 表示该端口的设置公布为 1000 mbps 速率和全双工模式。

**MDI/MDX** — 使交换机可以辨认绞接电缆和非绞接电缆。

应专门使集线器和交换机布线方式与终端站点布线方式完全相反，以便在将集线器或交换机连接至终端站点时，可以使用直通以太网电缆，并且能够正确匹配成对电缆。将两台集线器/交换机互相连接或将两个终端站点互相连接时，使用绞接电缆可以确保正确成对连接。

可能的值包括：

**On** (打开) — 使交换机可以检测连接的类型。

**Off** (关闭) — 需要有正确的电缆类型与交换机连接。

**Auto** (自动) — 系统自动设置该值。

**Current MDI/MDX** (当前 MDI/MDX) — 表示当前交换机的 MDX 设置。可能的字段值包括：

**MDI** — 当前 MDI 的设置为 MDI。

**MDX** — 当前 MDI 的设置为 MDX。

**Auto** (自动) — 系统自动设置该值。

**LAG** — 如果此端口是 LAG 成员，则显示 LAG 编号。

## 定义端口参数

□□□ 打开 **Port Configuration** (端口配置) 页面。

□□□ 在 **Unit** (单元) 和 **Port** (端口) 字段中选择单元和端口。

□□□ 定义屏幕上可用的字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将端口参数保存至交换机。

## 显示端口表

□□□ 打开 **Port Configuration** (端口配置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Port Configuration Table** (端口配置表)。

图 8-21. 端口配置表



□□□ **Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **Port Configuration Table** (端口配置表)。

## 复制端口配置设置

□□□ 打开 **Port Configuration** (端口配置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Port Configuration Table** (端口配置表)。

□□□ 在 **Copy Parameters From** (复制参数来源) 中指定作为复制来源的 **Unit** (单元) 和 **Port** (端口)。

□□□ 对要接收这些参数的每个 **Port** (端口) 单击 **Copy To** (复制至)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将复制 **Port Configuration** (端口配置) 设置并更新设备。

## 修改多个端口的端口配置设置

□□□ 打开 **Port Configuration** (端口配置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Port Configuration Table** (端口配置表)。

□□□ 对每个要修改的 **Port** (端口) 单击 **Edit** (编辑)。

□□□ 根据需要编辑 **Port Configuration** (端口配置) 字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 **Port Configuration** (端口配置) 设置并更新设备。

## 使用 CLI 命令配置端口

有关执行此功能的 **CLI** 命令的信息, 请参阅《CLI 参考指南》的以下章节:

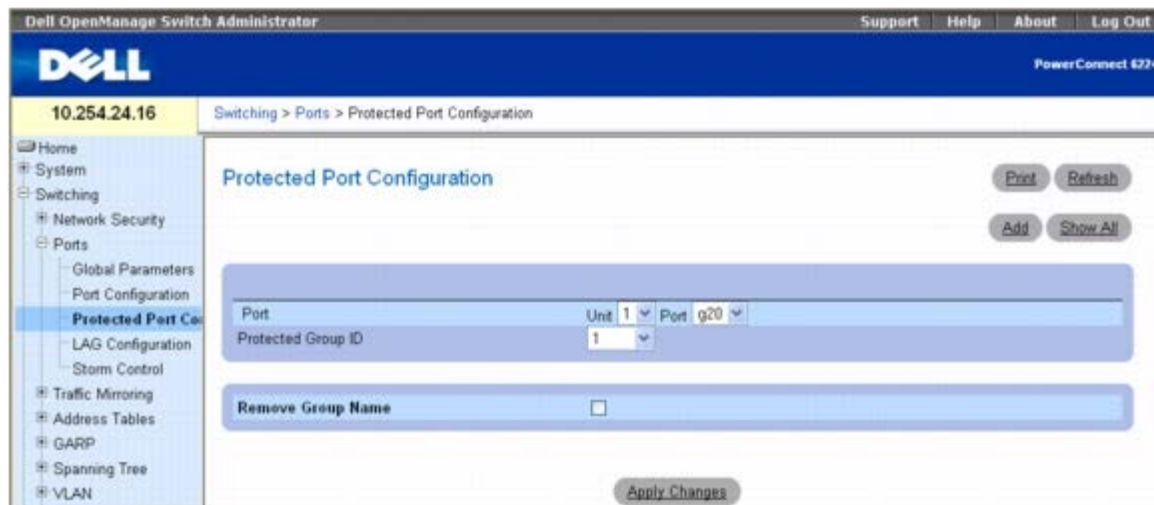
- 以太网配置命令

## 受保护的端口配置

**Protected Port Configuration**（受保护的端口配置）页面用于指定具有第 2 层安全保护功能的专用 VLAN 边缘 (PVE) 端口，这种功能会在同一个 VLAN 的成员端口之间提供基于端口的安全保护功能。受保护端口上的通信仅发送到上行链路端口，而不能发送到 VLAN 内的其他端口。

要显示 **Protected Port Configuration**（受保护的端口配置）页面，请在树视图中单击 **Switching**（交换）® **Ports**（端口）® **Protected Port Configuration**（受保护的端口配置）。

图 8-22. 受保护的端口配置



**Protected Port Configuration**（受保护的端口配置）页面包含以下字段：

**Port**（端口）— 指定 Unit（单元）和为其定义了端口参数的 Port（端口）。

**Protected Group ID**（受保护的组 ID）— 此下拉式菜单用于为组 0、1 或 2 分配端口。

**Remove Group Name**（删除组名称）— 选中此复选框将解除所选的端口与受保护的组之间的关联。

## 显示受保护的端口表

□□□ 打开 **Protected Port Configuration**（受保护的端口配置）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **Protected Ports Summary**（受保护的端口摘要）表。

图 8-23. 受保护的端口摘要表



□□□ 选中 **Remove**（删除）复选框并单击 **Apply Changes**（应用更改）以解除端口与受保护的组之间的关联。

□□□ **Unit**（单元）下拉式菜单用于查看堆栈中其它单元（如果存在）的 **Protected Port Summary**（受保护的端口摘要）表。

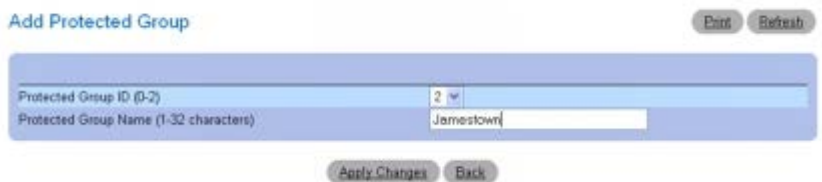
## 添加受保护的端口组

□□□ 打开 **Protected Port Configuration**（受保护的端口配置）页面。

□□□ 单击 **Add**（添加）。

系统将显示 **Add Protected Group**（添加受保护的组）。

图 8-24. 添加受保护的组



□□□ 使用下拉式菜单为 **Protected Group ID**（受保护的组 ID）分配数字标识 0、1 或 2。

□□□ 输入 **Protected Group Name (1–32 characters)**（受保护的组名称 [1 至 32 个字符]）。

□□□ 单击 **Apply Changes**（应用更改）。

系统将复制 Protected Group（受保护的组）设置并更新设备。

## 使用 CLI 命令配置受保护的端口

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

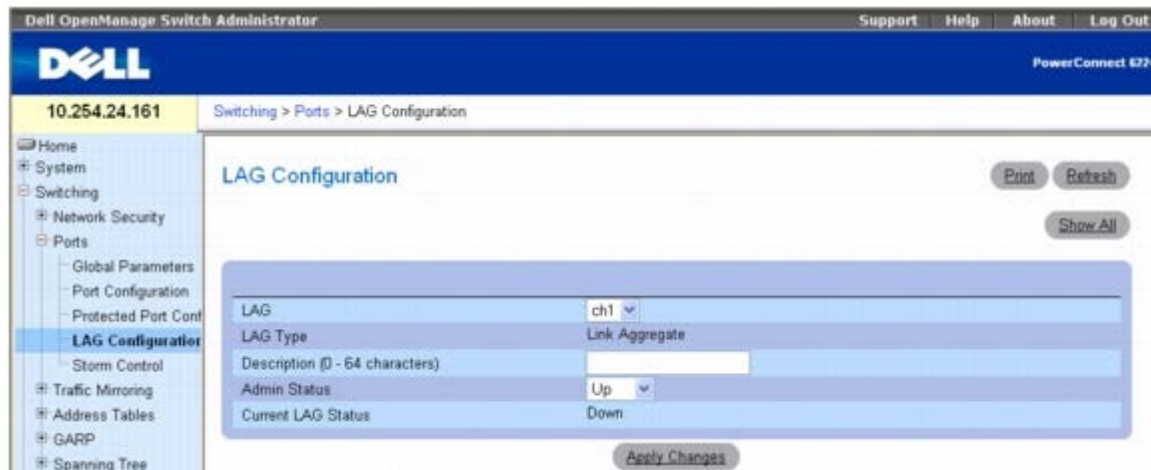
- 受保护的交换机端口命令

## LAG 配置

Link Aggregation（链路聚合）允许将一条或更多全双工 Ethernet（以太网）链路聚合在一起，形成 Link Aggregation Group (LAG)（链路聚合组 [LAG]）。交换机将 LAG 视为一条单独的链路。

要显示 **LAG Configuration (LAG 配置)** 页面，请在树视图中单击 **Switching (交换)** ® **Ports (端口)** ® **LAG Configuration (LAG 配置)**。

图 8-25. LAG 配置



**LAG Configuration (LAG 配置)** 页面包含以下字段：

**LAG** — 包含 LAG 号的列表。

**LAG Type (LAG 类型)** — 组成 LAG 的端口类型。

**Description (0-64 Characters)** (说明 [0 至 64 个字符]) — 端口的说明。

**Admin Status** (管理状态) — 启用或禁用通过选定的 LAG 转发通信。

**Current LAG Status** (当前 LAG 状态) — 表明所选的 LAG 已打开还是已关闭。

## 定义 LAG 参数

□□□ 打开 **LAG Configuration (LAG 配置)** 页面。

□□□ 在 **LAG** 字段中选择一个 LAG。

□□□ 定义屏幕上可用的字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将 LAG 参数保存至交换机。

## 显示 LAG 配置表

□□□ 打开 **LAG Configuration (LAG 配置)** 页面。

□□□ 单击 **Show All** (全部显示)。

□□□ 系统将显示 **LAG Configuration Table (LAG 配置表)**。

图 8-26. LAG 配置表

LAG Configuration Table Print Refresh

LAG	Description	LAG Type	Admin Status	Current Flow Control	Edit
1 lag1		Link Aggregation	Up	Disable	<input type="checkbox"/>
2 lag2		Link Aggregation	Up	Disable	<input type="checkbox"/>
3 lag3		Link Aggregation	Up	Disable	<input type="checkbox"/>
4 lag4		Link Aggregation	Up	Disable	<input type="checkbox"/>
5 lag5		Link Aggregation	Up	Disable	<input type="checkbox"/>
6 lag6		Link Aggregation	Up	Disable	<input type="checkbox"/>
7 lag7		Link Aggregation	Up	Disable	<input type="checkbox"/>
8 lag8		Link Aggregation	Up	Disable	<input type="checkbox"/>

Apply Changes Back

## 编辑 LAG 参数

□□□ 打开 **LAG Configuration** (LAG 配置) 页面。

□□□ 单击 **Show All** (全部显示)。

□□□ 系统将显示 **LAG Configuration Table** (LAG 配置表)。

□□□ 为所有要修改的 LAG 选中 **Edit** (编辑)。

□□□ 现在可以根据需要编辑 **Admin Status** (管理状态) 和 **Description** (说明)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将 LAG 参数保存至交换机。

## 使用 CLI 命令配置 LAG

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 端口信道命令

## 风暴控制

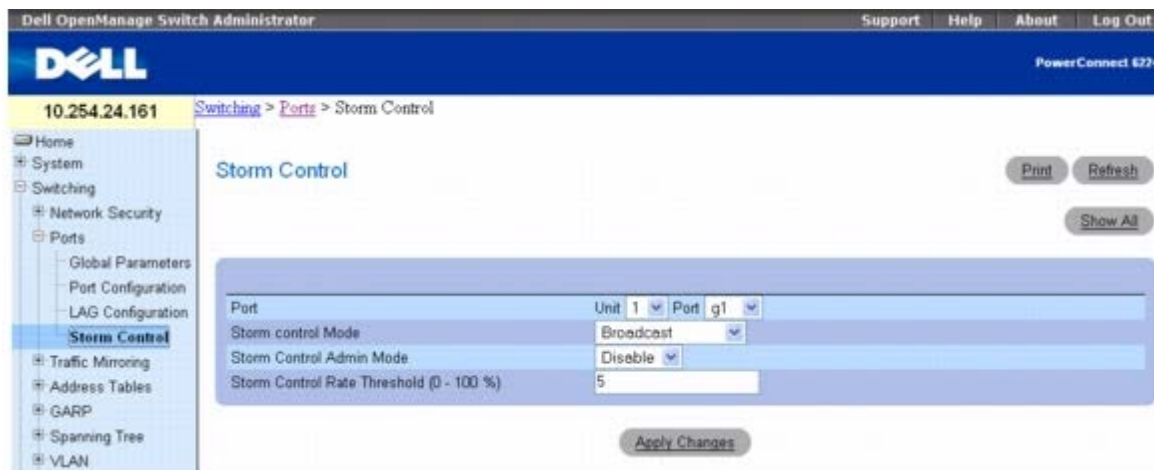
广播风暴是过多的广播信息同时通过单个端口在网络中发送的结果。转发信息回复会使网络资源过载和/或导致网络超时。

交换机测量各个端口上传入的广播/多点传送/未知单点传送信息包速率，并在速率超出定义值时丢弃信息包。通过定义信息包类型和信息包发送速率来对每个接口启用风暴控制。

**Storm Control** (风暴控制) 页面用于启用和配置风暴控制。

要显示 **Storm Control** (风暴控制) 接口，请在树视图中单击 **Switching** (交换) ® **Ports** (端口) ® **Storm Control** (风暴控制)。

图 8-27. 风暴控制



**Storm Control** (风暴控制) 页面包含以下字段：

**Port** (端口) — 指定 **Unit** (单元) 和为其启用了风暴控制的 **Port** (端口)。

**Storm Control Mode** (风暴控制模式) — 指定受风暴控制影响的广播模式。

**Broadcast** (广播) — 一旦接口上 L2 广播通信的入口速率增加超出配置的阈值范围，则该通信将会被丢弃。

**Multicast** (多点传送) — 一旦接口上 L2 多点传送通信的入口速率增加超出配置的阈值范围，则该通信将会被丢弃。

**Unknown Unicast** (未知单点传送) — 一旦接口上未知 L2 单点传送 (目的地查找失败) 通信的入口速率增加超出配置的阈值范围，则该通信将会被丢弃。

**Storm Control Admin Mode** (风暴控制管理模式) — 启用或禁用风暴控制。

**Storm Control Rate Threshold (0-100%)** (风暴控制速率阈值 [0-100%]) — 指定未知信息包转发的最大速率。该范围是总阈值的百分比。

## 定义风暴控制端口参数

□□□ 打开 **Storm Control** (风暴控制) 界面。

□□□ 编辑屏幕中的字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将风暴控制端口参数保存至交换机。

## 显示风暴控制设置表

□□□ 打开 **Storm Control** (风暴控制) 界面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Storm Control Settings Table** (风暴控制设置表)。

图 8-28. 风暴控制设置表



## Storm Control Settings Table

Print Refresh

Unit								
Unit	Broadcast Control Mode	Broadcast Rate Threshold	Multicast Control Mode	Multicast Rate Threshold	Unicast Control Mode	Unicast Rate Threshold	Edit	
1	1/g1	Disable	5	Disable	5	Disable	5	<input checked="" type="checkbox"/>
2	1/g2	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>
3	1/g3	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>
-----								
26	1/xg2	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>
27	1/xg3	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>
28	1/xg4	Disable	5	Disable	5	Disable	5	<input type="checkbox"/>

Apply Changes Back

□□□ **Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **Storm Control Settings Table** (风暴控制设置表)。

## 修改广播控制

□□□ 打开 **Storm Control** (风暴控制) 界面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Storm Control Settings Table** (风暴控制设置表)。

□□□ 对每个要修改 **Broadcast Control** (广播控制) 的端口选中 **Edit** (编辑)。

□□□ 根据需要编辑 **Broadcast Control** (广播控制)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将风暴控制端口参数保存至交换机。

## 使用 CLI 命令配置风暴控制

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- 以太网配置命令

## 配置通信镜像

通信镜像允许用户配置交换机, 以便将镜像源端口上的信息包副本发送至镜像目的地端口。镜像可基于端口或基于流。

**Traffic Mirroring** (通信镜像) 菜单页面用于定义端口镜像会话和配置基于流的镜像。

要显示此页面, 请在树视图中单击 **Switching** (交换) @ **Traffic Mirroring** (通信镜像)。**Traffic Mirroring** (通信镜像) 菜单页面包含以下功能的链接:

- [端口镜像](#)
- [基于流的镜像](#)

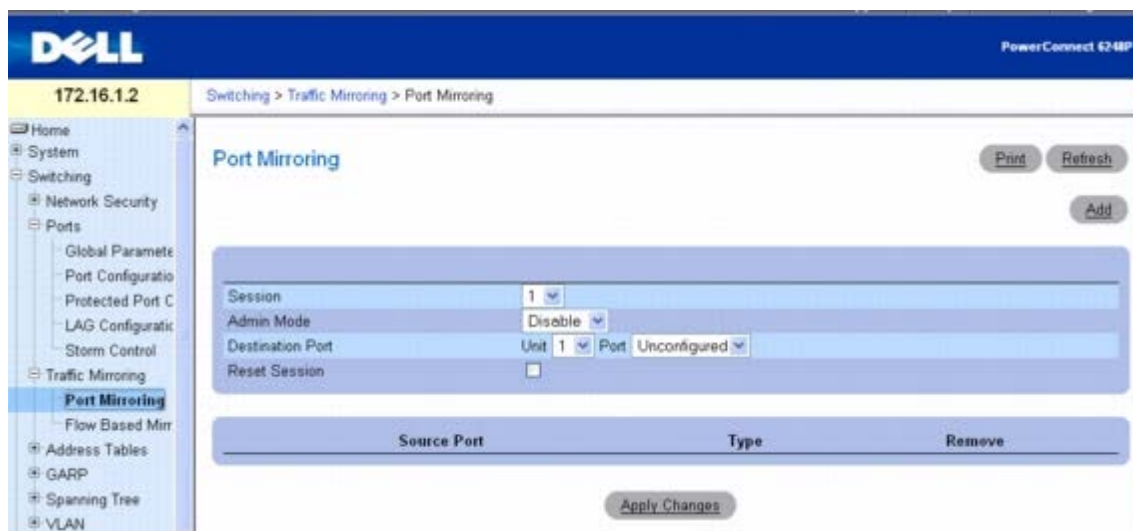
## 端口镜像

端口镜像选择网络分析器要分析的网络通信。其对象是交换机的特定端口。这样，多个交换机配置为源端口，而一个交换机端口配置为目的地端口。您能够配置在源端口上对通信进行镜像的方式。源端口上接收的信息包、在端口上发送的信息包或接收和发送的全部信息包均可映射镜像到目的地端口。

复制到目的地端口的信息包与在网线上的原始信息包格式相同。这意味着，如果镜像复制接收的信息包，则复制的信息包如同其在源端口接收时一样带有 VLAN 标签或没有 VLAN 标签。如果镜像复制发送的信息包，则复制的信息包如同其在源端口发送时一样带有 VLAN 标签或没有 VLAN 标签。

要显示 **Port Mirroring**（端口镜像）页面，请在树视图中单击 **Switching**（交换）® **Traffic Mirroring**（通信镜像）® **Port Mirroring**（端口镜像）。

图 8-29. 端口镜像



**Port Mirroring**（端口镜像）页面包含以下字段：

**Session**（会话）— 指定监测会话。

**Admin Mode**（管理模式）— 启用或禁用端口镜像。


**Destination Port**（目的地端口）— 选择端口通信可复制到的端口。

**Reset Session**（重置会话）— 使您重置端口监测会话。

**Source Port**（源端口）— 系统将列出已经在 **Add Source Port**（添加源端口）页面中添加的源端口。

**Type**（类型）— 系统将显示源端口上予以监测的通信类型。

## 添加端口镜像会话

 **注：**当端口变为目的地镜像后，将会从 VLAN 或 LAG 中删除。

□□□ 打开 **Port Mirroring**（端口镜像）页面。

□□□ 单击 **Add**（添加）以显示 **Add Source Port**（添加源端口）页面。

图 8-30. 添加源端口



□□□ 配置以下字段：

**Session**（会话）— 选择要监测的会话。

**Source Port**（源端口）— 选择单元和要镜像其通信的端口。最多可向目的地端口镜像四个源端口。

**Type**（类型）— 指定要镜像的通信类型。可能的字段值包括：

**TX** — 仅监测发送的信息包。

**RX** — 仅监测接收的信息包。

**TX and RX**（**TX** 和 **RX**）— 监测发送和接收的信息包。

□□□ 单击 **Apply Changes**（应用更改）。

系统将对单元和端口启用新的端口镜像并更新设备。系统将在 **Port Mirroring**（端口镜像）窗口的 **Source Port**（源端口）中显示源端口。

## 修改端口镜像会话

□□□ 打开 **Port Mirroring**（端口镜像）页面。

□□□ 修改字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将修改端口镜像会话字段并更新设备。

## 删除端口镜像会话

□□□ 打开 **Port Mirroring**（端口镜像）页面。

□□□ 选中 **Remove Session**（删除会话）复选框。

□□□ 单击 **Apply Changes**（应用更改）。

系统将删除端口镜像会话并更新设备。

## 使用 **CLI** 命令配置端口镜像会话

有关执行此功能的 **CLI** 命令的信息，请参阅《**CLI 参考指南**》的以下章节：

- 端口监测命令

## 基于流的镜像

基于流的镜像功能构建于 QoS 中的 Diffserv 组件之上。在 QoS 中，用户创建通信类以定义匹配标准，然后创建策略以定义对该通信类采取的措施。

基于流的镜像使用户将特定类型的通信复制到单一的目的地端口。这提供了灵活性：交换机无需镜像端口上的所有入口或出口通信，而是可以镜像该通信的子集。您可以配置交换机镜像基于 Layer 2（第 2 层）、Layer 3（第 3 层）和 Layer 4（第 4 层）信息的流。

**Flow Based Mirroring**（基于流的镜像）页面用于指定基于流的镜像端口。

要显示 **Flow Based Mirroring**（基于流的镜像）页面，请在树视图中单击 **Switching**（交换）® **Traffic Mirroring**（通信镜像）® **Flow Based Mirroring**（基于流的镜像）。

图 8-31. 基于流的镜像



**Flow Based Mirroring**（基于流的镜像）页面包含以下字段：

**Policy Name**（策略名称）— 选择与通信类相关联的策略。Policy Name（策略名称）使用 Diffserv“[策略配置](#)”网页进行定义。

**Member Classes**（成员类）— 选择与此策略相关联的通信类。Member Class（成员类）使用 Diffserv“[类配置](#)”网页进行定义。

**Copy to Interface**（复制到接口）— 当选定时，此功能允许将信息包复制到单元/端口或 LAG。

## 将镜像复制到目的地端口

□□□ 打开 **Flow Based Mirroring**（基于流的镜像）页面。

□□□ 指定 **Policy Name**（策略名称）和 **Member Class**（成员类），并在 **Copy to Interface**（复制到接口）中选择目的地单元和端口。

□□□ 单击 **Apply Changes**（应用更改）。

系统将基于流的镜像细节复制至指定端口并更新设备。

## 使用 CLI 命令配置基于流的镜像

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- QOS 命令

## 配置地址表

MAC 地址存储在静态或动态地址表中。静态地址由您定义。动态地址由系统记忆，并在超时后删除。定址到其中一个表存储的目的地的信息包将被立即转发到端口。静态和动态地址表可按 **Interface**（接口）、**VLAN** 或 **VLAN Name**（VLAN 名称）进行排序。此外，静态和动态地址表可添加地址。

要显示 **Address Tables**（地址表）菜单页面，请在树视图中单击 **Switching**（交换）® **Address Tables**（地址表）。**Address Tables**（地址表）页面包含以下功能的链接：

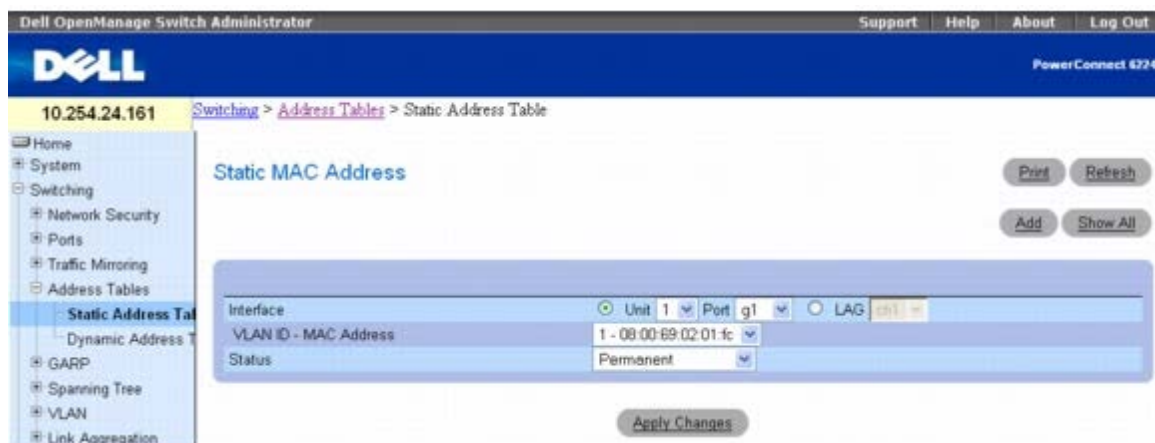
- [静态地址表](#)
- [动态地址表](#)

## 静态地址表

**Static MAC Address**（静态 MAC 地址）页面包含静态 MAC 地址的列表。可以在 Static MAC Address Table（静态 MAC 地址表）中添加和删除静态地址。

要显示 **Static MAC Address**（静态 MAC 地址）页面，请在树视图中单击 **Switching**（交换）® **Address Tables**（地址表）® **Static Address Table**（静态地址表）。


图 8-32. 静态 MAC 地址



**Static MAC Address**（静态 MAC 地址）页面包含以下字段：

**Interface**（接口）— 指定要应用静态 MAC 地址的 Unit（单元）和 Port（端口）或 LAG。要查看不同 Unit/Port（单元/端口）或 LAG 的地址，请更改此处列出的 Interface（接口）。

**VLAN ID - MAC Address**（VLAN ID - MAC 地址）— 指定连接至 MAC Address（MAC 地址）的 VLAN ID 以及当前静态地址列表中列出的 MAC 地址。

 **注：**系统将只显示分配给指定接口和 VLAN 的 MAC 地址。

**Status**（状态）— 指定 MAC 地址的状态。可能的值包括：

- Permanent**（永久）— MAC 地址是永久性的。
- Secure**（固定）— 保证锁定端口的 MAC 地址不被删除。
- Delete on Reset**（重置时删除）— 重启动交换机时删除 MAC 地址。
- Delete on Timeout**（超时时删除）— 发生超时时删除 MAC 地址。

## 添加静态 MAC 地址

□□□ 打开 **Static MAC Address**（静态 MAC 地址）页面。

□□□ 单击 **Add**（添加）。

系统将显示 **Add Static MAC Address**（添加静态 MAC 地址）页面。

图 8-33. 添加静态 MAC 地址

□□□ 根据需要填写各字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将新的静态地址添加至 **Static MAC Address Table**（静态 MAC 地址表）中，并更新设备。

## 修改静态 MAC 地址表中的静态地址

□□□ 打开 **Static MAC Address**（静态 MAC 地址）页面。

□□□ 修改字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将修改静态 MAC 地址并更新设备。

## 显示静态 MAC 地址表

□□□ 打开 **Static MAC Address**（静态 MAC 地址）页面。

□□□ 单击 **Show All**（全部显示）。

**Static MAC Address Table**（静态 MAC 地址表）将显示全部现有的静态 MAC 地址。

图 8-34. 静态 MAC 地址表

#	MAC	VLAN ID	Interface	Status	Remove
1	08:00:69:02:01:FC	1	1/g1	Permanent	<input checked="" type="checkbox"/>
2	08:A6:69:02:01:28	2	1/g5	Permanent	<input checked="" type="checkbox"/>

## 从静态地址表中删除静态地址

□□□ 打开 **Static MAC Address**（静态 MAC 地址）页面。

□□□ 单击 **Show All**（全部显示）以显示 **Static MAC Address Table**（静态 MAC 地址表）。

□□□ 对要删除的地址选中 **Remove**（删除）复选框。

□□□ 单击 **Apply Changes**（应用更改）。

系统将删除静态 IP 地址并更新设备。

## 使用 CLI 命令配置静态地址参数

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 地址表命令

## 动态地址表

**Dynamic Address Table** (动态地址表) 页面包含用于查询动态地址表中信息的字段，包括接口类型、MAC 地址、VLAN 和表排序关键字。转发至地址存储在地址表中的信息包将被直接转发至那些端口。

**Dynamic Address Table** (动态地址表) 也包含动态 MAC 地址从表中删除之前存在时间的信息。

要显示 **Dynamic Address Table** (动态地址表)，请在树视图中单击 **Switching** (交换) ® **Address Tables** (地址表) ® **Dynamic Address Table** (动态地址表)。

图 8-35. 动态地址表

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb path is Switching > Address Tables > Dynamic Address Table. The main content area is titled 'Address Tables - Dynamic Address Table'. It features a configuration section with 'Address Aging (10 - 1000000)' set to 359 seconds and a 'Clear Table' checkbox. Below this is an 'Apply Changes' button. The 'Query By' section has radio buttons for 'Interface', 'MAC Address', and 'VLAN ID'. The 'Interface' option is selected, and dropdown menus for 'Unit', 'Port', and 'LAG' are visible. A 'Query' button is located below the query section. At the bottom, the 'Current Address Table' is displayed as a table with columns for VLAN ID, MAC Address, and Interface.

VLAN ID	MAC Address	Interface
VLAN 1	00:0c:76:05:e2:82	1/g3
VLAN 1	00:0f:fe:1c:12:67	1/g3
VLAN 1	00:11:98:1a:45:03	1/g3
VLAN 1	00:fc:e3:90:01:45	

**Dynamic Address Table** (动态地址表) 包含以下字段：

**Address Aging (10-1000000)** (地址存在时间 [10-1000000]) — 指定动态 MAC 地址被删除前的存在时间，以秒为单位。默认值为 300 秒。

**Clear Table** (清除表) — 当选中此复选框并单击 **Apply Changes** (应用更改) 时，将清除表中所有动态 MAC 地址。

**Dynamic Address Table** (动态地址表) 可通过下列条件查询：

**Interface** (接口) — 指定要查询地址的 Unit (单元) 和 Port (端口)。

**LAG** — 指定要查询地址的 LAG。



**MAC Address** (**MAC** 地址) — 指定要查询地址的 **MAC** 地址。

**VLAN ID** — 指定要查询地址的 **VLAN** 号 (**MAC** 地址与其相连接)。

**Current Address Table** (当前地址表) 包含系统将信息包直接转发至端口所依据的动态地址参数。**Current Address Table** (当前地址表) 包含以下字段：

**VLAN ID** — 显示 **VLAN Tag** (**VLAN** 标签) 值。

**MAC Address** (**MAC** 地址) — 显示 **MAC** 地址。

**Interface** (接口) — 显示端口号。

## 定义存在时间

□□□ 打开 **Dynamic Address Table** (动态地址表) 页面。

□□□ 定义 **Address Aging** (地址存在时间) 字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改存在时间并更新设备。

## 查询动态地址表

□□□ 打开 **Dynamic Address Table** (动态地址表) 页面。

□□□ 定义查询 **Dynamic Address Table** (动态地址表) 所依据的参数。

查询条目可依据 **Interface** (接口)、**LAG**、**MAC Address** (**MAC** 地址) 或 **VLAN ID**。

□□□ 单击 **Query** (查询) 查询 **Dynamic Address Table** (动态地址表)。

## 从动态地址表中删除数据

□□□ 打开 **Dynamic Address Table** (动态地址表) 页面。

□□□ 选中 **Clear Table** (清除表) 复选框。

□□□ 单击 **Apply Changes** (应用更改)。

系统将清除 **Dynamic Address Table** (动态地址表) 中所有的数据。

## 使用 **CLI** 命令查询并排序动态地址

有关执行此功能的 **CLI** 命令的信息，请参阅《**CLI** 参考指南》的以下章节：

- 地址表命令

---

## 配置 **GARP**

通用属性注册协议 (**GARP**) 是一个通用协议，用于注册所有网络连接信息或成员关系类型信息。**GARP** 定义了一组关注给定网络属性 (例如

VLAN 或多点传送地址) 的交换机。**GARP Timers** (**GARP** 计时器) 页面可通过 **GARP** 菜单页面访问。

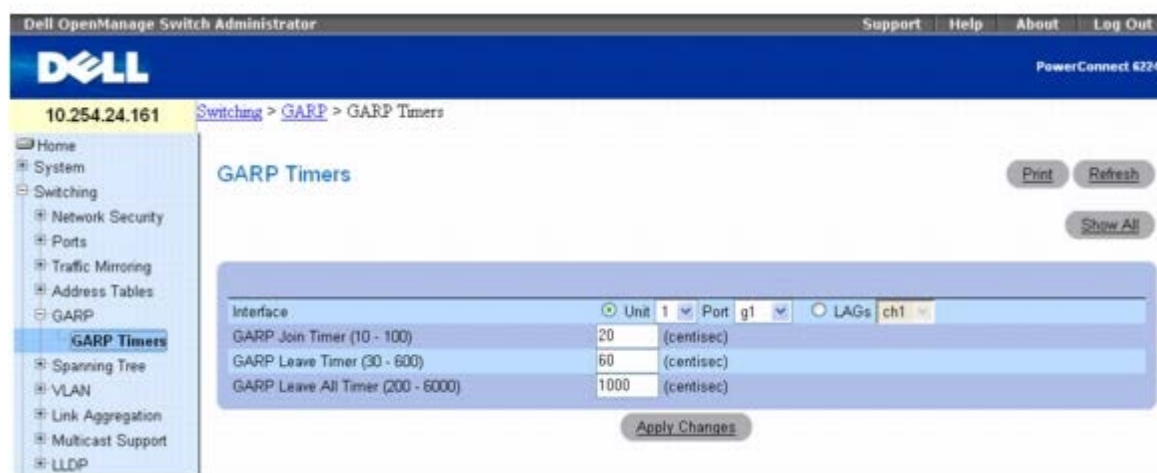
要显示 **GARP** 菜单页面，请在树视图中单击 **Switching** (交换) @ **GARP**。

## GARP 计时器

**GARP Timers** (**GARP** 计时器) 页面包含用于在交换机上启用 **GARP** 的字段。

要显示 **GARP Timers** (**GARP** 计时器) 页面，请在树视图中单击 **Switching** (交换) @ **GARP** @ **GARP Timers** (**GARP** 计时器)。

图 8-36. GARP 计时器



**GARP Timers** (**GARP** 计时器) 页面包含以下字段：

**Interface** (接口) — 指定要启用 **GARP** 计时器的 **Unit** (单元) 和 **Port** (端口) 或 **LAG**。

**GARP Join Timer (10-100)** (**GARP** 加入计时器 **[10-100]**) — 显示发送 PDU 的时间 (以厘秒为单位)。可能的字段范围为 10 至 100。默认值为 100 厘秒。

**GARP Leave Timer (30-600)** (**GARP** 离开计时器 **[30-600]**) — 显示交换机离开其 **GARP** 状态之前等待的时间 (以厘秒为单位)。发送/接收到的 **Leave All Time** (全部离开时间) 信息可以激活离开时间，接收到的 **Join** (加入) 信息可以取消离开时间。离开时间必须大于或等于加入时间的三倍。可能的字段范围为 30 至 600。默认值为 60 厘秒。

**GARP Leave All Timer (200-6000)** (**GARP** 全部离开计时器 **[200-6000]**) — 显示所有交换机离开 **GARP** 状态之前等待的时间 (以厘秒为单位)。全部离开时间必须大于离开时间。可能的字段范围为 200 至 6000。默认值为 1000 厘秒。

## 定义 GARP 计时器

□□□ 打开 **GARP Timers** (**GARP** 计时器) 页面。

□□□ 填写各字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统会将参数复制到 **GARP Timers Table** (**GARP** 计时器表) 中的选定端口或 **LAG**，并更新设备。

## 显示 GARP 计时器表中的参数

□□□ 打开 **GARP Timers** (**GARP** 计时器) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **GARP Timers Table** (**GARP** 计时器表)。

图 8-37. **GARP** 计时器表

Interface	GARP Join Timer	GARP Leave Timer	GARP Leave All Timer	Copy To	Edit	
1	1/g1	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
2	1/g2	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
3	1/g3	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
27	1/vg3	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
28	1/vg4	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
LAGs						
29	ch1	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
30	ch2	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
31	ch3	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
32	ch4	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
33	ch5	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
34	ch6	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
35	ch7	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
36	ch8	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>

□□□ **Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **GARP Timers Table** (**GARP** 计时器表)。

## 复制 **GARP** 计时器设置

□□□ 打开 **GARP Timers** (**GARP** 计时器) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **GARP Timers Table** (**GARP** 计时器表)。

□□□ 在 **Copy Parameters From** (复制参数来源) 中指定作为复制来源的 **Unit** (单元) 和 **Port** (端口)。

□□□ 对要接收这些参数的每个 **Interface** (接口) 单击 **Copy To** (复制至)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将复制 **GARP Timers** (**GARP** 计时器) 设置并更新设备。

## 修改多个端口的 **GARP** 计时器设置

□□□ 打开 **GARP Timers** (**GARP** 计时器) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **GARP Timers Table** (**GARP** 计时器表)。

□□□ 对每个要修改的 **Interface** (接口) 单击 **Edit** (编辑)。

□□□ 根据需要编辑 **GARP Timers** (**GARP** 计时器) 字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 GARP Timers (GARP 计时器) 设置并更新设备。

## 使用 CLI 命令定义 GARP 计时器

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- GVRP 命令

---

## 配置生成树协议

生成树协议 (STP) 提供了树拓扑，用于任意排列网桥。STP 还在网络中的终端站点之间提供了一条路径，消除了环路。系统支持的生成树版本包括 Classic STP (经典 STP)、Multiple STP (多 STP) 和 Rapid STP (快速 STP)。

经典 STP 在终端站点之间提供单一路径，以避免并消除环路。有关配置经典 STP 的信息，请参阅“[STP 全局设置](#)”。

多生成树协议 (MSTP) 支持 Spanning Tree (生成树) 的多个实例，以便在不同接口上有效地引导 VLAN 通信。Spanning Tree (生成树) 的每个实例按照 IEEE 802.1w，即快速生成树 (RSTP) 中指定的方式工作，在工作中对 IEEE 802.1w 进行了细微的修改，但并不影响其最终效果 (主要效果之一是端口至 `Forwarding` [“转发”] 状态的快速转换)。RSTP 与传统 STP (IEEE 802.1d) 之间的区别在于其配置和识别全双工连接及终端站点相连端口的能力，因此它可实现端口至 `Forwarding` (“转发”) 状态的快速转换和 Topology Change Notification (拓扑更改通知) 的抑制。这些功能由参数 `pointtopoint` (“点到点”) 和 `edgeport` (“边缘端口”) 实现。MSTP 兼容 RSTP 和 STP。可作为 STP 网桥和 RSTP 网桥使用。MSTP 网桥可配置成同样功能的 RSTP 网桥或 STP 网桥。

要显示 **Spanning Tree** (生成树) 菜单页面，请在树视图中单击 **Switching** (交换) ® **Spanning Tree** (生成树)。此 **Spanning Tree** (生成树) 页面包含以下 STP 过程的链接：

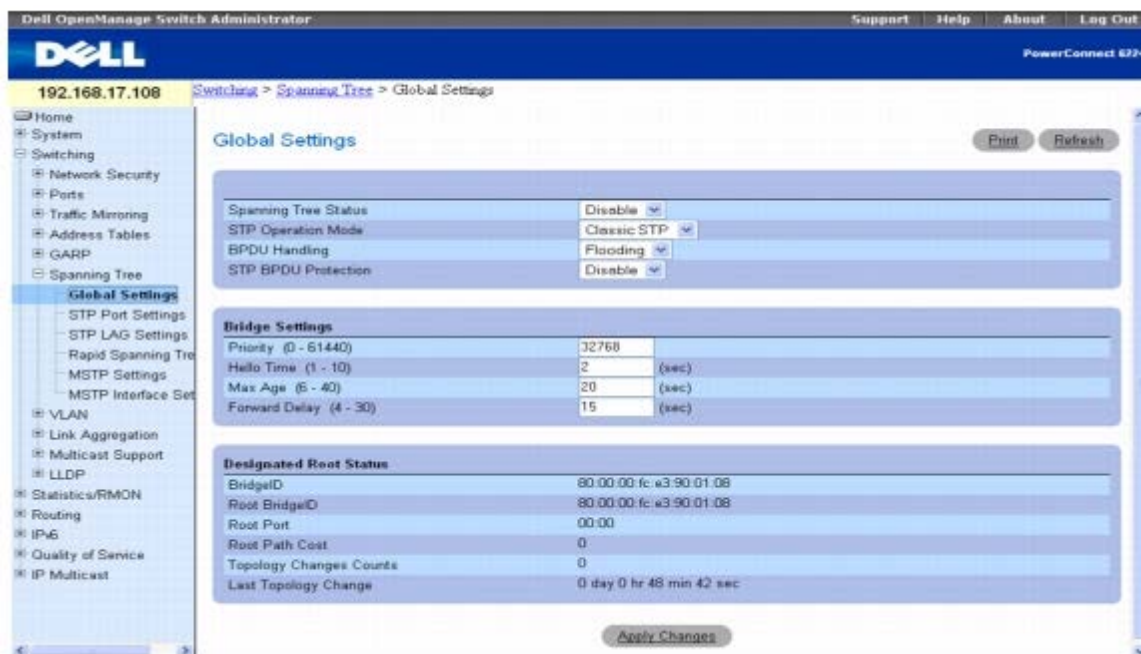
- [STP 全局设置](#)
- [STP 端口设置](#)
- [STP LAG 设置](#)
- [快速生成树](#)
- [MSTP 设置](#)
- [MSTP 接口设置](#)

## STP 全局设置

**STP Global Settings** (STP 全局设置) 页面包含用于在交换机上启用 STP 的字段。

要显示 **STP Global Settings** (STP 全局设置) 页面，请在树视图中单击 **Switching** (交换) ® **Spanning Tree** (生成树) ® **Global Settings** (全局设置)。

图 8-38. 生成树全局设置



STP Global Settings (STP 全局设置) 页面包含以下字段：

**Spanning Tree Status** (生成树状态) — 在交换机上启用或禁用 RSTP、STP 或 MSTP。

**STP Operation Mode** (STP 运行模式) — 指定在交换机上启用 STP 的 STP 模式。可能的字段值包括：**Classic STP** (经典 STP)、**Rapid STP** (快速 STP) 和 **Multiple STP** (多 STP)。

**BPDU Handling** (BPDU 处理) — 指定在接口上禁用了生成树时的网桥协议数据单元 (BPDU) 信息包处理方式。可能的字段值为 Filtering (筛选) 和 Flooding (多路发送)。默认值为 Flooding (多路发送)。

**STP BPDU Protection** (STP BPDU 保护) — 如果新的交换机试图加入现有的 STP 拓扑，则禁用端口。这可防止不属于 STP 最初部分的交换机影响 STP 拓扑。

如果设置为 Enable (启用)，当边缘端口接收到 BPDU 时，端口将被禁用。一旦端口被禁用，需要人工干预才能重新启用。

## 网桥设置

**Priority (0-61440)** (优先级 [0-61440]) — 指定网桥优先级值。交换机或网桥运行 STP 时，均会被分配一个优先级。交换 BPDU 后，优先级值最低的交换机将成为根网桥。

**Hello Time (1-10)** (问候间隔 [1-10]) — 指定交换机的 Hello time (问候间隔)，问候间隔表示根网桥在配置信息之间等待的时间 (以秒为单位)。默认值为 2。

**Max Age (6-40)** (最长存在时间 [6-40]) — 指定交换机的最长存在时间，最长存在时间表示网桥在执行拓扑更改之前等待的时间 (以秒为单位)。默认值为 20。

**Forward Delay (4-30)** (转发延迟 [4-30]) — 指定交换机的转发延迟时间，转发延迟时间表示在转发信息包之前网桥处于侦听和记忆状态的时间 (以秒为单位)。默认值为 15。

## 指定的根状态

**Bridge ID** (网桥 ID) — 显示网桥 ID。

**Root Bridge ID** (根网桥 ID) — 指定根网桥 ID。

**Root Port** (根端口) — 显示可提供从此网桥至根网桥最低开销路径的端口号。当网桥不是根网桥时，此选项非常重要。默认值为 0。

**Root Path Cost** (根路径开销) — 显示从此网桥至根网桥的路径开销。

**Topology Changes Counts** (拓扑更改计数) — 显示已发生的 STP 状态更改的总次数。

**Last Topology Change**（上次拓扑更改）— 显示自上次拓扑更改以来的总时间。时间以天/小时/分钟/秒钟的格式显示，例如 5 小时 10 分钟 4 秒。

## 定义 STP 全局参数

□□□ 打开 **STP Global Settings**（STP 全局设置）页面。

□□□ 在 **Spanning Tree Status**（生成树状态）字段中选择 **Enable**（启用）。

□□□ 在 **STP Operation Mode**（STP 运行模式）字段中指定 **STP** 模式的类型，并定义其余设置。

□□□ 单击 **Apply Changes**（应用更改）。

系统将在交换机上启用 STP。

## 要修改 STP 全局参数，请：

□□□ 打开 **STP Global Settings**（STP 全局设置）页面。

□□□ 根据需要修改此页面中的字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将修改 STP 参数并更新设备。

## 使用 CLI 命令定义 STP 全局参数

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 生成树命令

## STP 端口设置

**STP Port Settings**（STP 端口设置）页面用于为个别端口指定 STP 属性。

要显示 **STP Port Settings**（STP 端口设置）页面，请在树视图中单击 **Switching**（交换）® **Spanning Tree**（生成树）® **STP Port Settings**（STP 端口设置）。

图 8-39. STP 端口设置





**STP Port Settings** (STP 端口设置) 页面包含以下字段：

**Select a Port** (选择端口) — 指定 Unit (单元) 和要在其上启用 STP 的 Port (端口)。

**STP** — 在端口上启用或禁用 STP。

**Fast Link** (快速链路) — 一旦选中，则为端口启用 Fast Link (快速链路) 模式。如果为端口启用了 Fast Link (快速链路) 模式，则当端口链路良好时，**Port State** (端口状态) 将自动被置于 **Forwarding** (转发) 状态。在大型网络中，STP 聚合可能需要 30 至 60 秒。

**Port State** (端口状态) — 表示端口的当前 STP 状态。如果已启用该选项，端口状态将确定对通信所采取的转发操作。可能的端口状态包括：

**Disabled** (已禁用) — 此端口当前禁用 STP。端口记忆 MAC 地址时才转发通信。

**Blocking** (阻塞) — 端口当前已被阻塞，无法用于转发通信或记忆 MAC 地址。

**Listening** (侦听) — 端口当前处于侦听模式。端口既不能转发通信，也不能记忆 MAC 地址。

**Learning** (记忆) — 端口当前处于记忆模式。端口不能转发通信，但可以记忆新的 MAC 地址。

**Forwarding** (转发) — 端口当前处于转发模式。端口既可以转发通信，也可以记忆新的 MAC 地址。

**STP Root Guard** (STP 根保护) — 防止 Spanning Tree (生成树) 实例的根发生意外变化。当根网桥启用根保护并收到高级的 BPDU，该端口将转为根不一致状态，此状态等同于侦听状态。根网桥被强制。

**Role** (角色) — 显示此端口在 STP 拓扑中的角色。

**Speed** (速率) — 显示端口运行的速率。

**Path Cost (1-200000000)** (路径开销 [1-200000000]) — 指定在根路径开销计算中的端口代价。可以将路径开销调整为较高或较低的值，并且在路径被重新路由时可以用于转发通信。值为零表示根据端口的速率设置路径开销。默认值为 0。

**Priority (0-240)** (优先级 [0-240]) — 指定端口的优先级值。当网桥有两个端口连接在一个环路中时，优先级值用于确定端口的选择。默认值为 128。

**Designated Bridge ID** (指定的网桥 ID) — 显示指定的网桥的 ID。

**Designated Port ID** (指定的端口 ID) — 显示所选端口的 ID。

**Designated Cost** (指定的开销) — 显示参与 STP 拓扑的端口的开销。如果 STP 检测到环路，则端口开销越低，被阻塞的可能性越小。

**LAG** — 显示端口所连接到的 LAG。



## 在端口上启用 STP

□□□ 打开 **STP Port Settings** (STP 端口设置) 页面。

□□□ 在 **Select a Port** (选择端口) 字段中指定单元和要启用的端口。

□□□ 在 **STP** 字段中选择 **Enable** (启用)。

□□□ 根据需要编辑 **Fast Link** (快速链路)、**STP Root Guard** (STP 根保护)、**Path Cost** (路径开销) 和 **Priority** (优先级) 字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将在端口上启用 STP。

## 修改 STP 端口属性

□□□ 打开 **STP Port Settings** (STP 端口设置) 页面。

□□□ 根据需要修改 **Fast Link** (快速链路)、**STP Root Guard** (STP 根保护)、**Path Cost** (路径开销) 和 **Priority** (优先级) 字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 STP 端口参数并更新设备。

## 显示 STP 端口表

□□□ 打开 **STP Port Settings** (STP 端口设置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **STP Port Table** (STP 端口表)。

图 8-40. STP 端口表

The screenshot shows the 'STP Port Table' interface. At the top, there are 'Print' and 'Refresh' buttons. Below them is a search bar labeled 'Unit' with a dropdown arrow. The main part of the interface is a table with the following columns: Port, STP, Fast Link, STP Root Guard, State, Role, Path Cost, Priority, Designated Bridge ID, Designated Port ID, Designated Cost, and Edit. The table contains several rows of data, with the first three rows highlighted in blue. Below the table, there are 'Apply Changes' and 'Back' buttons.

Port	STP	Fast Link	STP Root Guard	State	Role	Path Cost	Priority	Designated Bridge ID	Designated Port ID	Designated Cost	Edit
1 1/g1	Enable	<input checked="" type="checkbox"/>	Disable	Manual forward Disabled	Disabled	0	128	80:00:00:fc:e3:90:01:45	00:00	0	<input checked="" type="checkbox"/>
2 1/g2	Enable	<input checked="" type="checkbox"/>	Disable	Disabled	Disabled	0	128	80:00:00:fc:e3:90:01:45	00:00	0	<input type="checkbox"/>
3 1/g3	Enable	<input checked="" type="checkbox"/>	Disable	Manual forward Disabled	Disabled	0	128	80:00:00:fc:e3:90:01:45	00:00	0	<input type="checkbox"/>
-----											
26 1/gp2	Enable	<input checked="" type="checkbox"/>	Disable	Disabled	Disabled	0	128	80:00:00:fc:e3:90:01:45	00:00	0	<input type="checkbox"/>
27 1/gp3	Enable	<input checked="" type="checkbox"/>	Disable	Disabled	Disabled	0	128	80:00:00:fc:e3:90:01:45	00:00	0	<input type="checkbox"/>
28 1/gp4	Enable	<input checked="" type="checkbox"/>	Disable	Disabled	Disabled	0	128	80:00:00:fc:e3:90:01:45	00:00	0	<input type="checkbox"/>

□□□ **Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **STP Port Table** (STP 端口表)。

## 修改多个端口的 STP 端口设置

打开 **STP Port Settings** (STP 端口设置) 页面。

单击 **Show All** (全部显示)。

系统将显示 **STP Port Table** (STP 端口表)。

对每个要修改的 Port (端口) 单击 **Edit** (编辑)。

根据需要编辑 STP 端口设置。

单击 **Apply Changes** (应用更改)。

系统将修改 STP Port (STP 端口) 设置并更新设备。

## 将快速链路应用于端口

打开 **STP Port Settings** (STP 端口设置) 页面。

单击 **Show All** (全部显示)。

系统将显示 **STP Port Table** (STP 端口表)。

对每个要修改的 Port (端口) 单击 **Edit** (编辑)。

选中 **Fast Link** (快速链路) 复选框为端口启用快速链路模式。如果为端口启用了 **Fast Link** (快速链路) 模式，则当端口链路良好时，**Port State** (端口状态) 将自动被置于 **Forwarding** (转发) 状态。

单击 **Apply Changes** (应用更改)。

系统将修改选定端口的 STP Port (STP 端口) 参数并更新设备。

## 使用 CLI 命令定义 STP Port (STP 端口) 设置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 生成树命令

## STP LAG 设置

**STP LAG Settings** (STP LAG 设置) 页面用于分配 STP 聚合端口参数。

要显示 **STP LAG Settings** (STP LAG 设置) 页面，请在树视图中单击 **Switching** (交换) ® **Spanning Tree** (生成树) ® **STP LAG Settings** (STP LAG 设置)。

图 8-41. STP LAG 设置



**STP LAG Settings (STP LAG 设置)** 页面包含以下字段：

**Select a LAG (选择 LAG)** — 指定您要对其修改 STP 设置的 LAG 号。

**STP** — 在 LAG 上启用或禁用 STP。默认值为启用。

**Fast Link (快速链路)** — 为 LAG 启用 Fast Link (快速链路) 模式。如果为 LAG 启用了 Fast Link (快速链路) 模式，则当 LAG 良好时，**Port State (端口状态)** 将自动被置为 **Forwarding (转发)** 状态。Fast Link (快速链路) 模式可以优化 STP 协议进行聚合所需的时间。在大型网络中，STP 聚合可能需要 30 至 60 秒。

**Port State (端口状态)** — 显示 LAG 的当前 STP 状态。如果启用该选项，LAG 状态将确定对通信所采取的转发操作。如果网桥发现故障 LAG，该 LAG 将被置于 **Broken (断开)** 状态。可能的 LAG 状态包括：

**Disabled (已禁用)** — LAG 当前禁用 STP。LAG 记忆 MAC 地址时才转发通信。

**Blocking (阻塞)** — LAG 已被阻塞，无法用于转发通信或记忆 MAC 地址。

**Listening (侦听)** — LAG 处于侦听模式，无法转发通信或记忆 MAC 地址。

**Learning (记忆)** — LAG 处于记忆模式，无法转发通信，但可以记忆新的 MAC 地址。

**Forwarding (转发)** — LAG 当前处于转发模式，可以转发通信和记忆新的 MAC 地址。

**Broken (断开)** — LAG 当前出现故障，无法用于转发通信。

**Role (角色)** — 显示此端口在 STP 拓扑中的角色。

**Path Cost (0-200000000) (路径开销 [0-200000000])** — 指定在根路径开销计算中的 LAG 代价。可以将路径开销调整为较高或较低的值，并且在路径被重新路由时可以用于转发通信。默认值为 0。

**Priority (0-240) (优先级 [0-240])** — 指定 LAG 的优先级值。当网桥有两个环路端口时，优先级值用于确定 LAG 的选择。优先级值介于 0 至 240 之间。

**Designated Bridge ID (指定的网桥 ID)** — 显示指定的网桥 ID。

**Designated Port ID (指定的端口 ID)** — 显示指定的端口 ID。

**Designated Cost (指定的开销)** — 显示参与 STP 拓扑的端口的开销。如果 STP 检测到环路，则端口开销越低，被阻塞的可能性越小。

## 修改一个 LAG 的 LAG STP 参数

□□□ 打开 **STP LAG Settings (STP LAG 设置)** 页面。

□□□ 从 **Select a LAG** (选择 LAG) 下拉式菜单中选择一个 LAG。

□□□ 根据需要修改字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 STP LAG 参数并更新设备。

## 显示 STP LAG 表

□□□ 打开 **STP LAG Settings** (STP LAG 设置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **STP LAG Table** (STP LAG 表)。

图 8-42. STP LAG 表

Port	STP	Fast Link	STP Root Guard	State	Role	Path Cost	Priority	Designated Bridge ID	Designated Port ID	Designated Cost
ch1	Enable	Enable	Disabled	Disabled	0	128	80:00:00:fc:a3:90:01:45	00:00	0	
ch2	Enable	Enable	Disabled	Disabled	0	128	80:00:00:fc:a3:90:01:45	00:00	0	
ch3	Enable	Enable	Disabled	Disabled	0	128	80:00:00:fc:a3:90:01:45	00:00	0	
ch4	Enable	Enable	Disabled	Disabled	0	128	80:00:00:fc:a3:90:01:45	00:00	0	
ch5	Enable	Enable	Disabled	Disabled	0	128	80:00:00:fc:a3:90:01:45	00:00	0	
ch6	Enable	Enable	Disabled	Disabled	0	128	80:00:00:fc:a3:90:01:45	00:00	0	
ch7	Enable	Enable	Disabled	Disabled	0	128	80:00:00:fc:a3:90:01:45	00:00	0	
ch8	Enable	Enable	Disabled	Disabled	0	128	80:00:00:fc:a3:90:01:45	00:00	0	

□□□ 在该表中，可以单击 **Fast Link** (快速链路) 并进行选择，然后单击 **Apply Changes** (应用更改) 来为个别 LAG 启用或禁用 Fast Link (快速链路) 和 STP Root Guard (STP 根保护)。

## 修改多个 LAG 的 LAG STP 参数

□□□ 打开 **STP LAG Settings** (STP LAG 设置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **STP LAG Table** (STP LAG 表)。

□□□ 为所有要修改的 LAG 选中 **Edit** (编辑)。

□□□ 根据需要修改字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改选定 LAG 的 STP LAG (STP LAG 端口) 参数并更新设备。

## 使用 CLI 命令定义 STP LAG 设置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 生成树命令

## 快速生成树

快速生成树协议 (RSTP) 检测并使用允许生成树更加快速聚合的网络拓扑，且不会创建转发环路。

要显示 **Rapid Spanning Tree** (快速生成树) 页面，请在树视图中单击 **Switching** (交换) ® **Spanning Tree** (生成树) ® **Rapid Spanning Tree** (快速生成树)。

图 8-43. 快速生成树



**Rapid Spanning Tree** (快速生成树) 页面包含以下字段：

**Interface** (接口) — 确定是在 Unit/Port (单元/端口) 上还是在 LAG 上启用 RSTP。单击 Unit/Port (单元/端口) 或 LAG 指定接口类型，然后从下拉式菜单中选择 Unit/Port (单元/端口) 或 LAG 进行配置。

**State** (状态) — 显示端口的生成树状态。

**Role** (角色) — 显示端口在 STP 拓扑中的生成树角色。

**Mode** (模式) — 显示管理模式以及模式为已启用还是已禁用。

**Fast Link Operational Status** (快速链路运行状态) — 表示为端口或 LAG 启用还是禁用快速链路。如果为端口启用了快速链路，则端口将自动被置为转发状态。此设置可以在“[STP 端口设置](#)”或“[STP LAG 设置](#)”页面中更改。

**Point-to-Point Operational Status** (点对点运行状态) — 显示点对点运行状态。

要建立点对点链路上的通信，起始 PPP 首先发送链路控制协议 (LCP) 信息包以配置和检测数据链路。建立链路并根据需要通过 LCP 协商了可选设备之后，起始 PPP 将发送网络控制协议 (NCP) 信息包以选择和配置一个或多个网络层协议。如果每个选定的网络层协议均已配置，则可以通过链路发送来自每个网络层协议的信息包。在显示 LCP 或 NCP 信息包关闭链路或发生某个外部事件之前，链路将一直保留用于通信的配置。这是实际的交换机端口链路类型。

## 显示快速生成树 (RSTP) 表

□□□ 打开 **Rapid Spanning Tree (RSTP)** (快速生成树 [RSTP]) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Rapid Spanning Tree Table** (快速生成树表)。

图 8-44. 快速生成树表

Rapid Spanning Tree Table Print Refresh

Unit

Interface	Role	Fast Link Operational Status	Point to Point Operational Status
1 1/g1	Designated	Disabled	Enable
2 1/g2	Disabled	Disabled	Disable
3 1/g3	Designated	Disabled	Enable
-----			
26 1/xg2	Disabled	Disabled	Disable
27 1/xg3	Disabled	Disabled	Disable
28 1/xg4	Disabled	Disabled	Disable
-----			
LAGs			
29 ch1	Disabled	False	Enable
30 ch2	Disabled	False	Enable
31 ch3	Disabled	False	Enable
32 ch4	Disabled	False	Enable
33 ch5	Disabled	False	Enable
34 ch6	Disabled	False	Enable
35 ch7	Disabled	False	Enable
36 ch8	Disabled	False	Enable

Back

□□□ Unit (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **Rapid Spanning Tree Table** (快速生成树表)。

## 使用 CLI 命令定义快速 STP 参数

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- 生成树命令

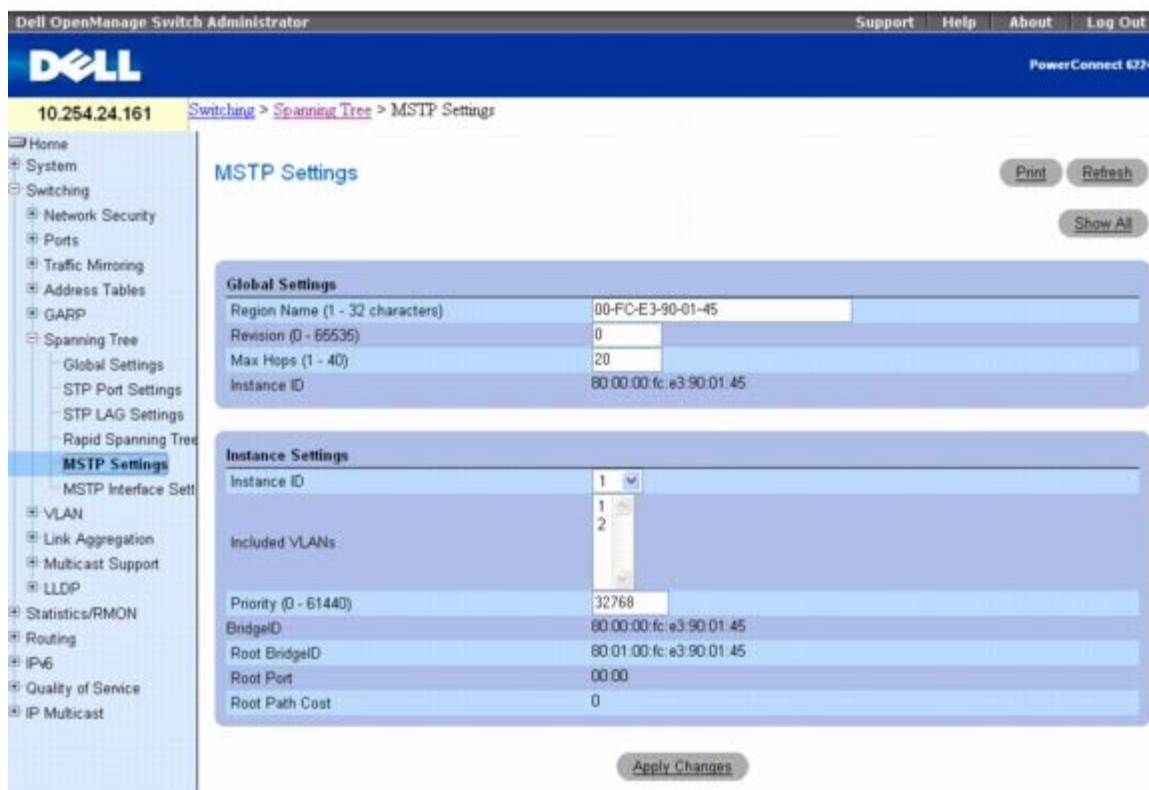
## MSTP 设置

多生成树协议 (MSTP) 支持 Spanning Tree (生成树) 的多个实例, 以便在不同接口上有效地引导 VLAN 通信。MSTP 兼容 RSTP 和 STP; MSTP 网桥可配置成同样功能的 RSTP 网桥或 STP 网桥。

要显示 **MSTP Settings** (MSTP 设置) 页面, 请在树视图中单击 **Switching** (交换) ® **Spanning Tree** (生成树) ® **MSTP Settings** (MSTP 设置)。

图 8-45. MSTP 设置





**MSTP Settings** (MSTP 设置) 页面包含以下字段，分为 **Global Settings** (全局设置) 和 **Instance Settings** (实例设置) 两个部分：

**Region Name (1–32 characters)** (域名称 [1 至 32 个字符]) — 指定用户定义的 MST 域名称。

**Revision (0–65535)** (修订版本 [0-65535]) — 指定无符号 16 位数字，表示当前 MST 配置的修订版本。修订版本号是 MST 配置中的必需部分。默认值为 0。

**Max Hops (1–40)** (最大跳数 [1-40]) — 指定丢弃 BPDU 之前在特定域中发生的总跳数。一旦 BPDU 被丢弃，端口信息将会过期。默认值为 20。

**Instance ID** (实例 ID) — 指定生成树实例的 ID。字段范围为 1 至 15，默认值为 1。

**Included VLANs** (包括的 VLAN) — 将选定的 VLAN 映射到选定的实例。每个 VLAN 只能属于一个实例。

**Priority (0–61440)** (优先级 [0-61440]) — 指定用于所选生成树实例的交换机优先级。默认值为 32768。

**Bridge ID** (网桥 ID) — 表示所选实例的网桥 ID。

**Root Bridge ID** (根网桥 ID) — 表示根网桥 (路径开销最低) 的网桥 ID。

**Root Port** (根端口) — 表示所选实例的根端口。

**Root Path Cost** (根路径开销) — 表示所选实例的路径开销。

## 修改 MSTP 设置：

□□□ 打开 **MSTP Settings** (MSTP 设置) 页面。

□□□ 根据需要修改 **Global Settings** (全局设置) 和 **Instance Settings** (实例设置) 部分中的字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 MSTP 参数并更新设备。

## 显示 MSTP VLAN 与实例映射表



□□□ 打开 **MSTP Settings** (MSTP 设置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **MSTP Settings Table** (MSTP 设置表)。

图 8-46. MSTP 设置表

Instance ID	VLAN	Instance ID (# 1-15)	Edit
1	1	0	<input type="checkbox"/>
2	3	0	<input type="checkbox"/>
3	5	0	<input type="checkbox"/>
4	7	0	<input type="checkbox"/>
5	888	0	<input type="checkbox"/>
6	2222	0	<input type="checkbox"/>

□□□ 要修改一个或多个 VLAN 的 Instance ID (实例 ID)，请为所需的 VLAN 选中 **Edit** (编辑)。

□□□ 对 Instance ID (实例 ID) 进行所需的修改。输入值 0 将删除 VLAN-to-Instance (VLAN 与实例) 映射。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改选定 VLAN 的 Instance ID (实例 ID) 并更新设备。

## 使用 CLI 命令定义 MST 实例

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 生成树命令

## MSTP 接口设置

**MSTP Interface Settings** (MSTP 接口设置) 页面用于将 MSTP 设置分配给特定的接口。

要显示 **MSTP Interface Settings** (MSTP 接口设置) 页面，请在树视图中单击 **Switching** (交换) ® **Spanning Tree** (生成树) ® **MSTP Interface Settings** (MSTP 接口设置)。

图 8-47. MSTP 接口设置



**MSTP Interface Settings (MSTP 接口设置)** 页面包含以下字段：

**Instance ID (实例 ID)** — 选择交换机上已配置的 MSTP 实例。可能的字段范围为 1 至 15。

**Interface (接口)** — 为此 MSTP 实例选择 Unit/Port (单元/端口) 或 LAG 作为接口。

**Port State (端口状态)** — 表示在特定实例中端口为已启用还是已禁用。

**Port Type (端口类型)** — 表示 MSTP 将端口用作点到点端口还是连接到集线器的端口，以及端口是在 MST 域内部还是一个边界端口。如果端口为边界端口，则还表示在链路另一端的交换机运行模式是 RSTP 还是 STP。

**Role (角色)** — 表示由 STP 算法分配以便提供给 STP 路径的端口角色。可能的字段值包括：

**Root (根)** — 提供将信息包转发给根交换机的最低开销路径。

**Designated (指定)** — 表示指定交换机通过其与 LAN 连接的端口或 LAG。

**Alternate (备用)** — 提供从接口到根交换机的备用路径。

**Backup (备份)** — 提供指定的 LAN 的备份路径。只有当两个端口通过点到点链路连接至一个环路中时，才会出现备份端口。当 LAN 有两个或多个连接到一个共享网段的连接时，也会出现备份端口。

**Disabled (已禁用)** — 表示端口未加入 Spanning Tree (生成树)。

**Priority (优先级)** — 定义用于指定实例的接口优先级。优先级范围为 0 至 240，步进为 16。默认值为 128。

**Path Cost (0–200000000) (路径开销 [0-200000000])** — 表示在 Spanning Tree (生成树) 实例计算中的端口代价。该值范围应始终为 0 至 200,000,000。默认值由端口的速率确定。默认值为：

- Port Channel (端口信道) -20,000
- 1000 mbps (千兆) -20,000
- 100 mbps-200,000
- 10 mbps-2,000,000

**Designated Bridge ID (指定的网桥 ID)** — 显示与链路或共享 LAN 连接的桥 ID 号，该链路或共享 LAN 连接至根。

**Designated Port ID (指定的端口 ID)** — 显示与链路或共享 LAN 连接的指定网桥的端口 ID 号，该链路或共享 LAN 连接至根。

**Designated Cost (指定的开销)** — 显示由链路或共享 LAN 至根的路径开销。

## 分配 MSTP 接口设置

- 打开 **MSTP Interface Settings** (MSTP 接口设置) 页面。
- 从下拉式菜单中选择 **Instance ID** (实例 ID)。
- 指定 **Port** (端口) 或 **LAG**, 然后从相应的下拉式菜单中选择接口。
- 指定 **Interface Priority** (接口优先级) 和 **Path Cost** (路径开销)。
- 单击 **Apply Changes** (应用更改)。

系统将保存接口设置并更新设备。

## 显示 MSTP 接口设置表

- 打开 **MSTP Settings** (MSTP 设置) 页面。
- 单击 **Show All** (全部显示)。

系统将显示 **MSTP Interface Table** (MSTP 接口表)。

图 8-48. MSTP 接口表

Interface	Role	Port Priority	Path Cost	Port State	Designated Cost	Designated Bridge ID	Designated Port ID	Edit
1 1/g1	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	8001	<input type="checkbox"/>
2 1/g2	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	8002	<input type="checkbox"/>
3 1/g3	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	8003	<input type="checkbox"/>
-----								
26 1/g2	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	801A	<input type="checkbox"/>
27 1/g3	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	801B	<input type="checkbox"/>
28 1/g4	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	801C	<input type="checkbox"/>

- **Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **MSTP Interface Table** (MSTP 接口表)。
- 要修改一个或多个接口的端口优先级或路径开销, 请选中所需接口的 **Edit** (编辑)。
- 根据需要对 **Port Priority** (端口优先级) 或 **Path Cost** (路径开销) 列中的值进行更改。
- 单击 **Apply Changes** (应用更改)。

系统将修改所选 **Interface** (接口) 中的字段并更新设备。

## 使用 CLI 命令定义 MSTP 接口

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- 生成树命令

## 配置 VLAN

为 Layer 2 switch（第 2 层交换机）添加虚拟 LAN (VLAN) 支持提供了桥接和路由的优点。VLAN 交换机如网桥一样基于 Layer 2 header（第 2 层标头）快速转发通信，同时如路由器一样将网络划分为逻辑网段，提供更好的管理、安全保护和多点传送通信的管理。

VLAN 是终端和与之相连的交换机端口的集合。逻辑分区可以有多种原因，如部门或项目成员关系。物理上的唯一要求是，终端和与之相接的端口都属于同一个 VLAN。

网络中的每个 VLAN 均有与之相关联的 VLAN ID，VLAN ID 在 VLAN 上发送的信息包第 2 层标头中的 IEEE 802.1Q 标签里。终端站点可能遗漏该标签或该标签的 VLAN 部分，在此情形下，接收信息包的第一个交换机端口可拒绝该信息包或使用默认 VLAN ID 为其插入一个标签。一个端口可处理一个以上 VLAN 的通信，但只能支持一个默认 VLAN ID。

要显示 VLAN 菜单页面，请在树视图中单击 **Switching（交换）® VLAN**。此 VLAN 页面包含以下功能的链接：

- [VLAN 成员关系](#)
- [VLAN 端口设置](#)
- [VLAN LAG 设置](#)
- [捆绑 MAC 至 VLAN](#)
- [捆绑 IP 子网至 VLAN](#)
- [协议组](#)
- [GVRP 参数](#)

## VLAN 成员关系

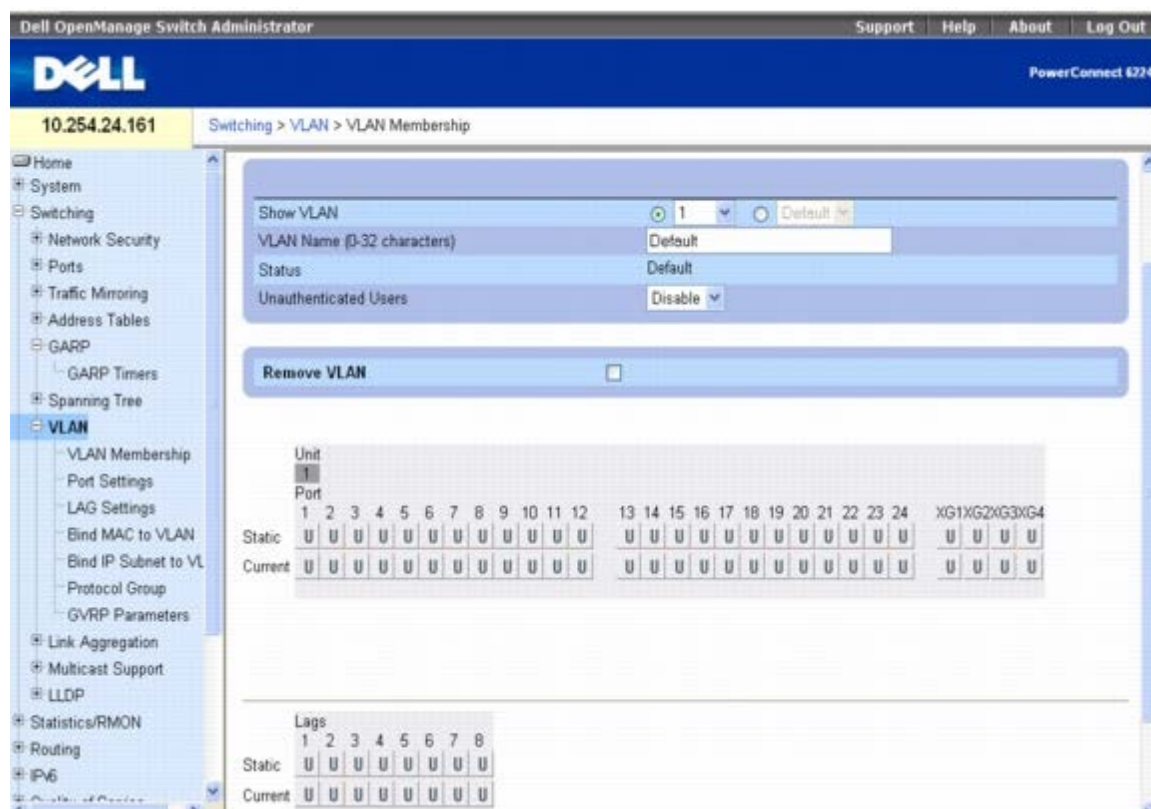
**VLAN Membership（VLAN 成员关系）** 页面用于定义存储在 VLAN 成员关系表中的 VLAN 组。交换机最多可支持 4094 个 VLAN。但是，您实际只能创建 4092 个 VLAN，因为：

- VLAN 1 是成员为所有端口的默认 VLAN，并且
- VLAN 4095 被指定为 "Discard VLAN"（“丢弃 VLAN”）。

可以创建的有效 VLAN 为 2-4093。VLAN 4094 保留。

要显示 **VLAN Membership（VLAN 成员关系）** 页面，请在树视图中单击 **Switching（交换）® VLAN ® VLAN Membership（VLAN 成员关系）**。

图 8-49. VLAN 成员关系



**VLAN Membership (VLAN 成员关系)** 页面分为两个部分：上面的部分包含定义整个 VLAN 成员关系的字段。下面的部分包含若干个表，表中定义了此 VLAN 上用于特定 Port and LAG（端口和 LAG）的成员关系设置。以下为 **VLAN Membership (VLAN 成员关系)** 字段：

**Show VLAN (显示 VLAN)** — 选择要显示的 VLAN。使用 **VLAN ID** 或 **VLAN Name (VLAN 名称)** 下拉式菜单选择 VLAN。

**VLAN Name (0–32) (VLAN 名称 [0–32])** — 表示用户定义的 VLAN 名称。此字段是通过 **Add** (添加) 按钮定义的。有效名称的长度范围为 0 至 32 个字符。

**Status (状态)** — 表示 VLAN 类型。可能的值包括：

**Dynamic (动态)** — 表示 VLAN 是通过 GVRP 动态创建的。

**Static (静态)** — 表示 VLAN 是由用户定义的并可修改。

**Default (默认)** — 表示 VLAN 是默认的 VLAN。

**Unauthenticated Users (未经验证的用户)** — 当选定 Enable (启用) 时，允许未经授权的交换机访问此 VLAN。

**Remove VLAN (删除 VLAN)** — 当选中此选项时，将从 VLAN Membership Table (VLAN 成员关系表) 中删除显示的 VLAN。

**VLAN Membership (VLAN 成员关系)** 表显示属于 VLAN 成员的 Ports (端口) 和 LAG，以及它们的状态是已标记 (T)、未标记 (U)、还是禁止 (F)。表中有两行：**Static** (静态) 和 **Current** (当前)。此页面中只有 **Static** (静态) 行可操作。**Current** (当前) 行则通过 GVRP 动态更新，或当更改 **Static** (静态) 行并单击 **Apply Changes** (应用更改) 时更新。

该页面的本部分有两个表：

**Ports (端口)** — 显示并将 VLAN 成员关系分配给端口。要分配成员关系，请在 **Static** (静态) 中单击特定的端口。每次单击将依次于 U、T 和空白间切换。定义请参见下表。

**LAGs** — 显示并将 VLAN 成员关系分配给 LAG。要分配成员关系，请在 **Static** (静态) 中单击特定的 LAG。每次单击将依次于 U、T 和空白间切换。定义请参见下表。

表 8-1. VLAN 端口成员关系定义

端口控制	定义
T	已标记：接口是 VLAN 的成员。通过接口转发的所有信息包均被标记。信息包包含 VLAN 信息。
U	未标记：接口是 VLAN 成员。通过接口转发的信息包均未标记。

F	禁止：表示禁止接口成为 VLAN 的成员。
空白	空白：接口不是 VLAN 成员。将不会转发与接口相关联的信息包。

## 添加新 VLAN

- 打开 **VLAN Membership** (VLAN 成员关系) 页面。
- 单击 **Add** (添加) 。

系统将显示 **Add VLAN** (添加 VLAN) 页面。

图 8-50. 添加 VLAN

- 输入新的 VLAN ID 和 VLAN Name (VLAN 名称) 。
- 单击 **Apply Changes** (应用更改) 。

系统将添加新 VLAN 并更新设备。

## 为端口或 LAG 分配 VLAN 成员关系

- 打开 **VLAN Membership** (VLAN 成员关系) 页面。
- 从 **VLAN ID** 或 **VLAN Name** (VLAN 名称) 下拉式菜单中选择一个 VLAN。
- 在 **VLAN Port Membership Table** (VLAN 端口成员关系表) 中，通过在 **Static** (静态) 行中单击为特定的 Port/LAG (端口/LAG) 分配值。每次单击将依次于 U、T 和空白 (不是成员) 间切换。
- 单击 **Apply Changes** (应用更改) 。

将根据所选的标识将 Port (端口) 或 LAG 分配给 VLAN，并用此标识更新 **Current** (当前) 行，同时更新设备。

## 修改 VLAN 成员关系组

- 打开 **VLAN Membership** (VLAN 成员关系) 页面。
- 从 **VLAN ID** 或 **VLAN Name** (VLAN 名称) 下拉式菜单中选择一个 VLAN。
- 根据需要修改字段。
- 在 **VLAN Port Membership Table** (VLAN 端口成员关系表) 中，通过在 **Static** (静态) 行中单击来更改 Port/LAG (端口/LAG) 的值。每次单击将依次于 U、T 和空白 (不是成员) 间切换。
- 单击 **Apply Changes** (应用更改) 。

系统将修改 VLAN 成员关系信息，并按照标识中的任何更改更新 **Current** (当前) 行，同时更新设备。



## 删除 VLAN

- 打开 **VLAN Membership** (VLAN 成员关系) 页面。
- 从 **VLAN ID** 或 **VLAN Name** (VLAN 名称) 下拉式菜单中选择一个 VLAN。
- 选中 **Remove VLAN** (删除 VLAN) 复选框。
- 单击 **Apply Changes** (应用更改)。

系统将删除所选 VLAN 并更新设备。

## 使用 CLI 命令定义 VLAN 成员关系组以及分配端口/LAG。

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- VLAN 命令

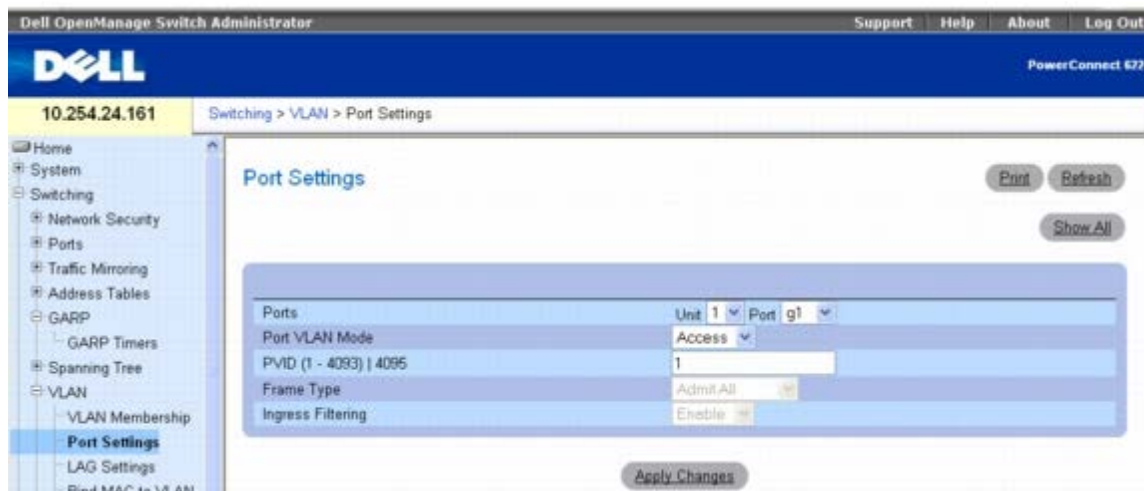
## VLAN 端口设置

在基于端口的 VLAN 中，通过基于接收端口 PVID 的指定端口桥接未标记通信。因为广播、多点传送和未知信息包只发送至 VLAN 成员端口，所以基于端口的 VLAN 可帮助优化网络通信样式。收到的有 VLAN 标签信息包使用此 VLAN ID 进行交换处理。

**VLAN Port Settings** (VLAN 端口设置) 页面用于将端口识别为 VLAN 的一部分以及定义和修改 VLAN 端口参数。

要显示 **VLAN Port Settings** (VLAN 端口设置) 页面，请在树视图中单击 **Switching** (交换) @ **VLAN** @ **Port Settings** (端口设置)。

图 8-51. VLAN 端口设置



**VLAN Port Settings** (VLAN 端口设置) 页面包含以下字段：

**Ports** (端口) — 指定 VLAN 中包含的 Unit (单元) 和 Port (端口)。

**Port VLAN Mode** (端口 VLAN 模式) — 表示端口的模式。可能的值包括：

**General** (常规) — 端口属于 VLAN，并且每个 VLAN 均由用户定义为已标记或未标记 (完全 802.1Q 模式)。

**Access** (访问) — 端口属于单个未标记 VLAN。端口处于 Access (访问) 模式时，不能指定端口 (信息包类型) 上接受的信息包类型。也不能在访问端口上启用/禁用入口筛选。

**Trunk** (主干) — 端口属于一个以上 VLAN，并且所有端口均将被标记 (可选的单个固有 VLAN 除外)。



**PVID (1–4093) | 4095** — 为未标记的信息包分配 VLAN ID。可能的值是 1 至 4093 或 4095。

**Frame Type** (帧类型) — 指定端口上接受的帧类型。默认设置为 **Admit All** (全部接受)。可能的值包括：

**Admit Tag Only** (仅接受标签) — 表示端口只接受已标记帧。

**Admit All** (全部接受) — 表示端口既接受已标记帧，也接受未标记帧。

**Ingress Filtering** (入口筛选) — 在端口上启用或禁用入口筛选。当 VLAN 标签与端口 VLAN 成员关系不匹配时，入口筛选将丢弃帧。

## 分配端口设置

□□□ 打开 **VLAN Port Settings** (VLAN 端口设置) 页面。

□□□ 从 **Unit** (单元) 和 **Port** (端口) 下拉式菜单中选择需要分配设置的端口。

□□□ 填写页面中的其余字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将定义 VLAN 端口设置并更新设备。

## 显示 VLAN 端口表

□□□ 打开 **VLAN Port Settings** (VLAN 端口设置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **VLAN Port Table** (VLAN 端口表)。

图 8-52. VLAN 端口表

Port	Port VLAN Mode	PVID	Frame Type	Ingress Filtering	Edit
1 1/g1	Access	1	Admit All	Enable	<input type="checkbox"/>
2 1/g2	Access	1	Admit All	Enable	<input type="checkbox"/>
3 1/g3	General	3	Admit All	Enable	<input type="checkbox"/>
26 1/xg2	Access	1	Admit All	Enable	<input type="checkbox"/>
27 1/xg3	Access	1	Admit All	Enable	<input type="checkbox"/>
28 1/xg4	Access	1	Admit All	Enable	<input type="checkbox"/>

**注：**如果选择的是 **Access** (访问) 端口，则不能指定端口 (信息包类型) 上接受的信息包类型。也不能在访问端口上启用或禁用入口筛选。

□□□ **Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **VLAN Port Table** (VLAN 端口表)。

## 修改多个端口的设置

□□□ 打开 **VLAN Port Settings** (VLAN 端口设置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **VLAN Port Table** (VLAN 端口表)。

□□□ 对每个要修改的 Port (端口) 单击 **Edit** (编辑)。

□□□ 根据需要编辑字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 VLAN 端口设置并更新设备。

## 使用 CLI 命令为 VLAN 组分配端口

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

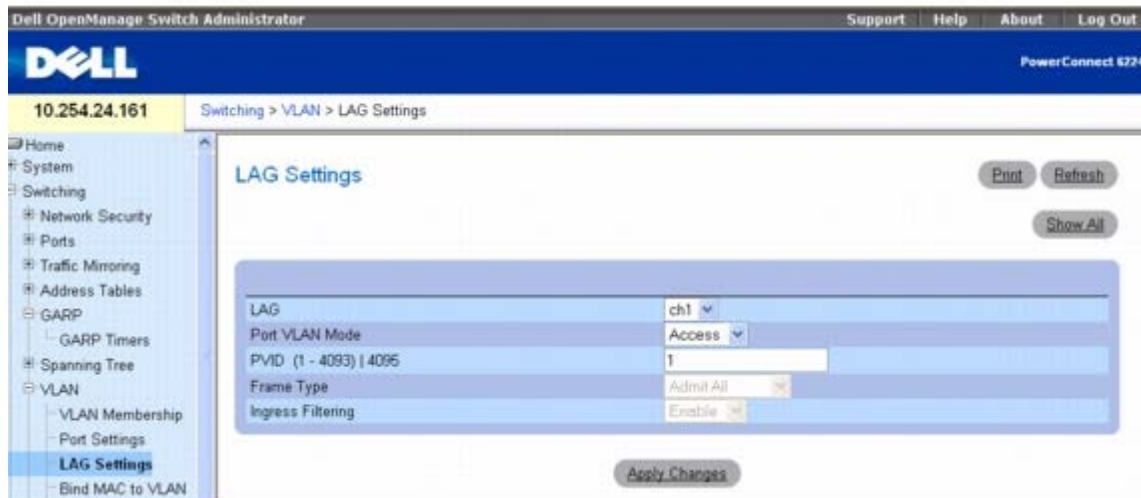
- VLAN 命令

## VLAN LAG 设置

**VLAN LAG Settings** (VLAN LAG 设置) 页面用于将 LAG 映射到 VLAN。进入交换机的未标记信息包按照 PVID 指定的 LAG ID 进行标记。

要显示 **VLAN LAG Settings** (VLAN LAG 设置) 页面，请在树视图中单击 **Switching** (交换) ® **VLAN** ® **LAG Settings** (LAG 设置)。

图 8-53. VLAN LAG 设置



**VLAN LAG Settings** (VLAN LAG 设置) 页面包含以下字段：

**LAG** — 指定 VLAN 中包含的 LAG 号。

**Port VLAN Mode** (端口 VLAN 模式) — 表示 LAG 的 Port VLAN Mode (端口 VLAN 模式)。可能的值包括：

**General** (常规) — LAG 属于 VLAN，并且每个 VLAN 均由用户定义为已标记或未标记 (完全 802.1Q 模式)。

**Access** (访问) — LAG 属于单个未标记 VLAN。

**Trunk** (主干) — LAG 属于一个以上 VLAN，并且所有端口均将被标记 (可选的单个固有 VLAN 除外)。

**PVID (1–4093) | 4095** — 为未标记的信息包分配 VLAN ID。可能的字段值是 1 至 4093 或 4095。

**Frame Type** (帧类型) — 指定 LAG 接受的信息包类型。Admit Tag Only (仅接受标签) 为默认设置。可能的值包括：

**Admit Tag Only**（仅接受标签）— LAG 只接受已标记信息包。

**Admit All**（全部接受）— LAG 既接受已标记信息包，也接受未标记信息包。

**Ingress Filtering**（入口筛选）— 启用或禁用于 LAG 进行的入口筛选。当 VLAN 标签与 LAG VLAN 成员关系不匹配时，入口筛选将丢弃信息包。

## 分配 VLAN LAG 设置

□□□ 打开 **VLAN LAG Settings**（VLAN LAG 设置）页面。

□□□ 从 **LAG** 下拉式菜单中选择一个 LAG。

□□□ 填写页面中的其余字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将定义 VLAN LAG 参数并更新设备。

## 显示 VLAN LAG 表

□□□ 打开 **VLAN LAG Settings**（VLAN LAG 设置）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **VLAN LAG Table**（VLAN LAG 表）。

图 8-54. VLAN LAG 表

VLAN LAG Table Print Refresh

Port	Port VLAN Mode	PVID	Frame Type	Ingress Filtering	Edit
1 ch1	Access	1	Admit All	Enable	<input type="checkbox"/>
2 ch2	Access	1	Admit All	Enable	<input type="checkbox"/>
3 ch3	Access	1	Admit All	Enable	<input type="checkbox"/>
4 ch4	Access	1	Admit All	Enable	<input type="checkbox"/>
5 ch5	Access	1	Admit All	Enable	<input type="checkbox"/>
6 ch6	Access	1	Admit All	Enable	<input type="checkbox"/>
7 ch7	Access	1	Admit All	Enable	<input type="checkbox"/>
8 ch8	Access	1	Admit All	Enable	<input type="checkbox"/>

## 修改多个 LAG 的设置

□□□ 打开 **VLAN LAG Settings**（VLAN LAG 设置）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **VLAN LAG Table**（VLAN LAG 表）。

□□□ 对每个要修改的 LAG 单击 **Edit**（编辑）。

□□□ 根据需要编辑字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将修改 VLAN LAG 设置并更新设备。

## 使用 CLI 命令为 VLAN 组分配 LAG

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

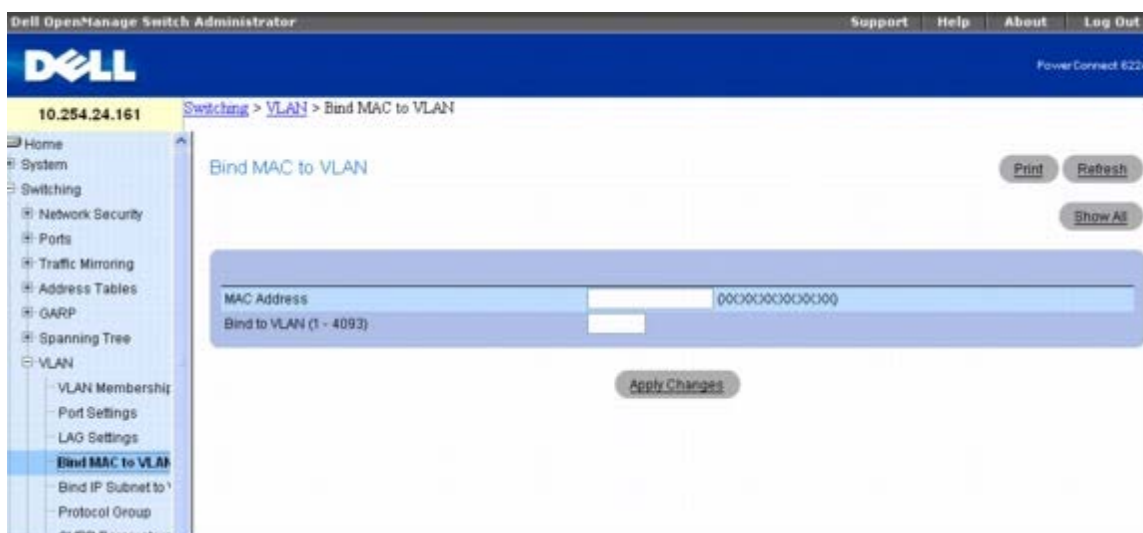
- VLAN 命令

## 捆绑 MAC 至 VLAN

**Bind MAC to VLAN**（捆绑 MAC 至 VLAN）页面用于将 MAC 条目映射到 VLAN 表。指定源 MAC 地址和 VLAN ID 后，该交换机的所有端口将共享 MAC 至 VLAN 配置。MAC 至 VLAN 表最多支持 128 个条目。

要显示 **Bind MAC to VLAN**（捆绑 MAC 至 VLAN）页面，请在树视图中单击 **Switching**（交换）® **VLAN** ® **Bind MAC to VLAN**（捆绑 MAC 至 VLAN）。

图 8-55. 捆绑 MAC 至 VLAN



**Bind MAC to VLAN**（捆绑 MAC 至 VLAN）页面包含以下字段：

**MAC Address**（MAC 地址）— 指定 VLAN 的 MAC Address（MAC 地址）。

**Bind to VLAN (1-4093)**（绑定 VLAN [1-4093]）— 指定 MAC 要绑定到的 VLAN。

### 分配捆绑 MAC 至 VLAN 设置

- 打开 **Bind MAC to VLAN**（捆绑 MAC 至 VLAN）页面。
- 输入要绑定 VLAN 的 MAC Address（MAC 地址）。
- 输入 MAC Address（MAC 地址）要绑定的 VLAN。
- 单击 **Apply Changes**（应用更改）。

现在，系统将绑定列出的 MAC Address（MAC 地址）和 VLAN 并更新设备。

### 显示 VLAN LAG 表

- 打开 **Bind MAC to VLAN**（捆绑 MAC 至 VLAN）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **MAC - VLAN Bind Table**（MAC - VLAN 捆绑表）。

图 8-56. MAC - VLAN 捆绑表

	MAC Address	Bind to VLAN	Remove	Edit
1	9500.4902.01FC	2	<input type="checkbox"/>	<input type="checkbox"/>
2	0686.6902.0127	110	<input type="checkbox"/>	<input type="checkbox"/>

## 修改多个 MAC 地址的 VLAN

□□□ 打开 **Bind MAC to VLAN**（捆绑 MAC 至 VLAN）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **MAC - VLAN Bind Table**（MAC - VLAN 捆绑表）。

□□□ 对具有要修改的 VLAN 的每个 MAC Address（MAC 地址）单击 **Edit**（编辑）。

□□□ 编辑 **Bind to VLAN**（绑定 VLAN）字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将修改 MAC to VLAN（MAC 至 VLAN）设置并更新设备。

## 删除 MAC - VLAN 条目

□□□ 打开 **Bind MAC to VLAN**（捆绑 MAC 至 VLAN）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **MAC - VLAN Bind Table**（MAC - VLAN 捆绑表）。

□□□ 对每个要删除的条目选中 **Remove**（删除）。

□□□ 单击 **Apply Changes**（应用更改）。

系统将删除条目并更新设备。

## 使用 CLI 命令捆绑 MAC 至 VLAN

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- VLAN 命令

## 捆绑 IP 子网至 VLAN

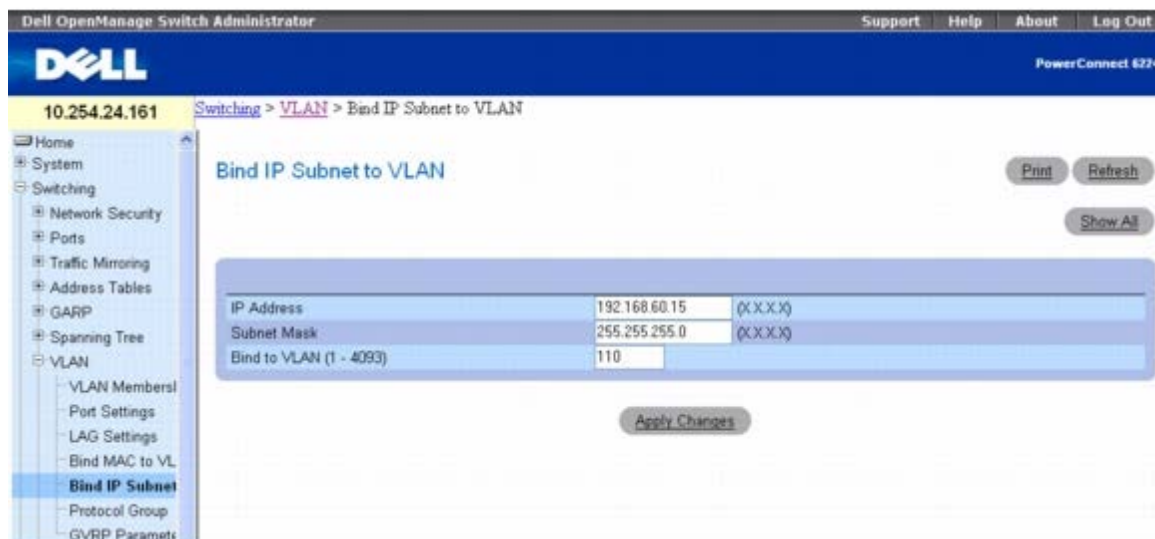
通过配置 IP Subnet to VLAN（IP 子网至 VLAN）表中的条目可定义 IP Subnet to VLAN（IP 子网至 VLAN）映射，该条目通过源 IP 地址、

网络掩码和所需 VLAN ID 指定。交换机中的所有端口共享 IP Subnet to VLAN（IP 子网至 VLAN）配置。此表中可配置最多 64 个条目。

**Bind IP Subnet to VLAN**（捆绑 IP 子网至 VLAN）页面用于为 VLAN 分配 IP Subnet（IP 子网）

要显示 **Bind IP Subnet to VLAN**（捆绑 IP 子网至 VLAN）页面，请在树视图中单击 **Switching**（交换）® **VLAN** ® **Bind IP Subnet to VLAN**（捆绑 IP 子网至 VLAN）。

图 8-57. 捆绑 IP 子网至 VLAN



**Bind IP Subnet to VLAN**（捆绑 IP 子网至 VLAN）页面包含以下字段：

**IP Address**（IP 地址）— 指定信息包源 IP 地址。

**Subnet Mask**（子网掩码）— 指定信息包源 IP 子网掩码。

**Bind to VLAN (1–4093)**（绑定 VLAN [1-4093]）— 指定要分配 IP Address（IP 地址）的 VLAN。

## 捆绑 IP 子网至一个 VLAN

□□□ 打开 **Bind IP Subnet to VLAN**（捆绑 IP 子网至 VLAN）页面。

□□□ 输入要绑定 VLAN 的 IP Address（IP 地址）。

□□□ 输入与 IP 地址相关联的 IP Subnet（IP 子网）。

□□□ 输入要分配 IP 地址和子网掩码的 VLAN ID。

□□□ 单击 **Apply Changes**（应用更改）。

现在，系统将绑定列出的 VLAN 和 IP Subnet（IP 子网）并更新设备。

## 显示 IP 子网 - VLAN 捆绑表

□□□ 打开 **Bind IP Subnet to VLAN**（捆绑 IP 子网至 VLAN）页面。

□□□ 单击 **Show All**（全部显示）。

□□□ 系统将显示 **IP Subnet - VLAN Bind Table**（IP 子网 - VLAN 捆绑表）。

图 8-58. IP 子网 - VLAN 捆绑表

IP Subnet - VLAN Bind Table Print Refresh

	IP Address	Subnet Mask	Bind to VLAN	Remove	Edit
1	192.168.12.0	255.255.255.0	110	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.13.0	255.255.255.0	110	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.60.0	255.255.255.0	110	<input type="checkbox"/>	<input type="checkbox"/>

Apply Changes Back

## 修改多个 IP 地址的 VLAN 绑定

□□□ 打开 **Bind IP Subnet to VLAN**（捆绑 IP 子网至 VLAN）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **IP Subnet - VLAN Bind Table**（IP 子网 - VLAN 捆绑表）。

□□□ 对每个要修改的条目单击 **Edit**（编辑）。

□□□ 根据需要编辑各字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将修改 Bind to VLAN（绑定 VLAN）设置并更新设备。

## 删除 MAC - IP 子网条目

□□□ 打开 **Bind IP Subnet to VLAN**（捆绑 IP 子网至 VLAN）页面。

□□□ 单击 **Show All**（全部显示）。

系统将显示 **IP Subnet - VLAN Bind Table**（IP 子网 - VLAN 捆绑表）。

□□□ 对每个要删除的条目选中 **Remove**（删除）。

□□□ 单击 **Apply Changes**（应用更改）。

系统将删除条目并更新设备。

## 使用 CLI 命令捆绑 IP 子网至 VLAN

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- VLAN 命令

## 协议组

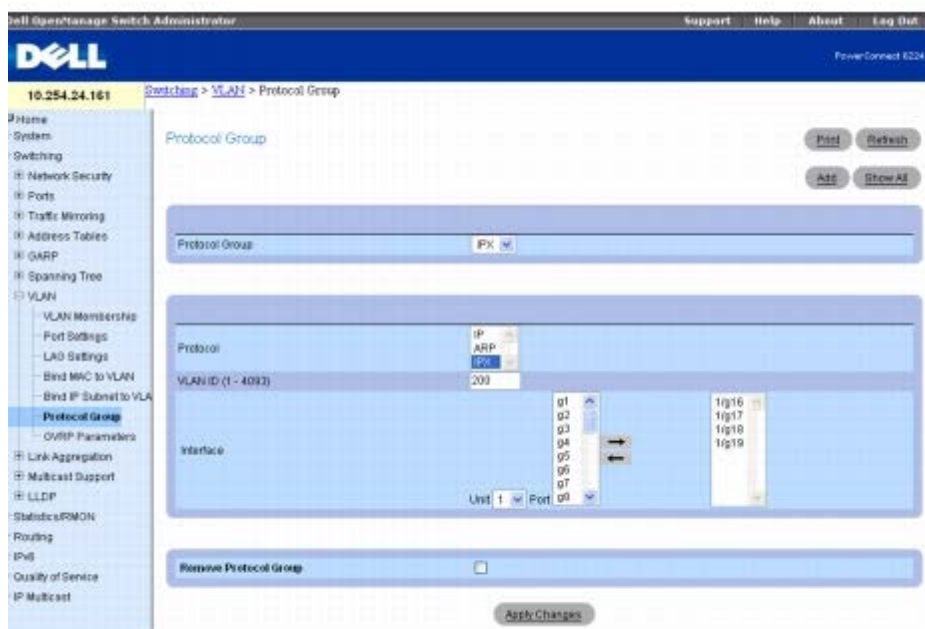
在基于协议的 VLAN 中，通过基于 VLAN 协议的指定端口桥接通信。用户定义的信息包筛选器确定特定的信息包是否属于特定的 VLAN。当网络段中包含运行多种协议的主机时，几乎总是采用基于协议的 VLAN。

**Protocol Group**（协议组）页面用于配置哪种 EtherTypes（以太网类型）要传送到哪个 VLAN，然后启用某些端口以便使用这些配置。

要显示 **Protocol Group**（协议组）页面，请在树视图中单击 **Switching**（交换）® **VLAN** ® **Protocol Group**（协议组）。



图 8-59. 协议组



**Protocol Group** (协议组) 页面包含以下字段：

**Protocol Group** (协议组) — 显示与协议组 ID 相关联的名称。单击 **Add** (添加) 按钮可以创建新的组。

**Protocol** (协议) — 指定与此组相关联的协议。

**VLAN ID (1-4093)** — 指定与此组相关联的 VLAN ID。

**Interface** (接口) — 选择要添加至此组或从此组中删除的接口。高亮度显示要添加至协议组的接口并单击右箭头。右侧列中显示的接口属于协议组。

**Remove Protocol Group** (删除协议组) — 当选中此复选框并单击 **Apply Changes** (应用更改) 时，删除屏幕上所显示的协议组。要同时删除多个协议组，请单击 **Show All** (全部显示) 并使用 **Protocol Group Table** (协议组表) 上的 **Remove** (删除) 复选框。

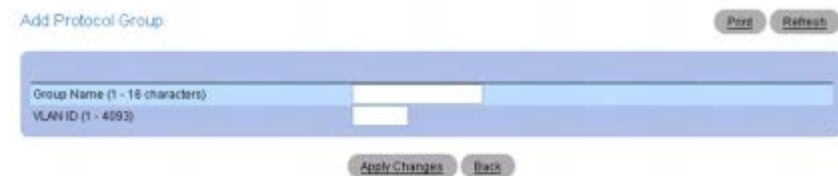
## 添加协议组

□□□ 打开 **Protocol Group** (协议组) 页面。

□□□ 单击 **Add** (添加) 。

系统将显示 **Add Protocol Group** (添加协议组) 页面。

图 8-60. 添加协议组



□□□ 输入新的 Protocol Group Name (协议组名称) 和 VLAN ID，以便与此组相关联。

□□□ 返回 Protocol Group (协议组) 页面。

□□□ 选择添加的 Protocol Group (协议组)，然后选择协议。

□□□ Interface

<Shift> [

在 (接口) 的第一列中，单击以高亮度显示要添加至协议组的接口。（要选择多个接口，请在单击鼠标的同时按下选择连续的多个接口] 或 <Ctrl> [选择不连续的多个接口]。）

选

□□□ 单击右箭头。

选定的接口移至第二列。第二列中的所有接口属于协议组。

□□□ 单击 **Apply Changes** (应用更改)。

系统将添加规则组并更新设备。

## 修改 VLAN 协议组设置

□□□ 打开 **Protocol Group** (协议组) 页面。

□□□ 在 **Protocol Group ID** (协议组 ID) 下拉式菜单中指定要修改的协议。

□□□ 根据需要更改 **Protocol** (协议) 或 **VLAN ID**。

□□□ 要添加 **Interface** (接口) 至组，单击以高亮度显示第一列中所需接口。（要选择多个接口，请在单击鼠标的同时按下 <Shift> [选择连续的多个接口] 或 <Ctrl> [选择不连续的多个接口]。）

□□□ 单击右箭头。

选定的接口移至第二列。第二列中的所有接口属于协议组。

□□□ 要从组中删除 **Interface** (接口)，单击以高亮度显示第二列中所需接口。

□□□ 单击左箭头。

选定的接口从第二列中删除。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 VLAN 协议组参数并更新设备。

## 从协议组表中删除多个协议

□□□ 打开 **Protocol Group** (协议组) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Protocol Group Table** (协议组表)。

图 8-61. 协议组表

Protocol Group Table Print Refresh

Group Name	Protocol	VLAN ID	Interface	Remove
1	IPX	200	1/g16 1/g17 1/g18 1/g19	<input type="checkbox"/> Edit
2	IPX2	110	1/g21 1/g22 1/g23 1/g24	<input type="checkbox"/> Edit

Apply Changes Back

□□□ 对希望删除的协议组选中 **Remove** (删除)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将删除协议并更新设备。

## 使用 CLI 命令配置协议组

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- VLAN 命令

## GVRP 参数

GARP VLAN Registration Protocol (GARP VLAN 注册协议) 提供了一种机制，允许网络交换机动态注册（和取消注册）与连接至同一段上的 MAC 网络交换机之间的 VLAN 成员关系信息，并允许该信息在支持 GVRP 的桥接 LAN 中所有网络交换机之间散布。

GVRP 的操作依赖于通用属性注册协议 (GARP) 提供的服务。GVRP 最多可创建 1024 个 VLAN。

**GVRP Global Parameters (GVRP 全局参数)** 页面用于全局启用 GVRP。您还可针对每个接口启用 GVRP。

要显示 **GVRP Global Parameters (GVRP 全局参数)** 页面，请在树视图中单击 **Switching (交换) ® VLAN ® GVRP Parameters (GVRP 参数)**。

图 8-62. GVRP 全局参数



**GVRP Global Parameters (GVRP 全局参数)** 页面包含以下字段：

**GVRP Global Status (GVRP 全局状态)** — 在交换机上启用或禁用 GVRP。默认情况下，GVRP 处于禁用状态。

**Interface (接口)** — 指定要启用 GVRP 的 Unit (单元) 和 Port (端口) 或 LAG。

**GVRP State (GVRP 状态)** — 在指定的接口上启用或禁用 GVRP。

**Dynamic VLAN Creation (动态 VLAN 创建)** — 允许或禁止通过 GVRP 创建 VLAN。

**GVRP Registration (GVRP 注册)** — 启用或禁用 GVRP 注册。

## 在交换机上启用 GVRP

□□□ 打开 **GVRP Global Parameters (GVRP 全局参数)** 页面。

在 **GVRP Global Status**（GVRP 全局状态）字段中选择 **Enable**（启用）。

单击 **Apply Changes**（应用更改）。

系统将在交换机上启用 GVRP。

## 通过 GVRP 启用 VLAN 注册

打开 **GVRP Global Parameters**（GVRP 全局参数）页面。

在 **GVRP Global Status**（GVRP 全局状态）字段中为所需的接口选择 **Enable**（启用）。

在 **GVRP Registration**（GVRP 注册）字段中选择 **Enable**（启用）。

单击 **Apply Changes**（应用更改）。

系统将在端口上启用 GVRP VLAN Registration（VLAN 注册）并更新设备。

## 显示 GVRP 端口参数表

打开 **GVRP Global Parameters**（GVRP 全局参数）页面。

单击 **Show All**（全部显示）。

系统将显示 **GVRP Port Parameters Table**（GVRP 端口参数表）。

图 8-63. GVRP 端口参数表

Interface	GVRP State	Dynamic VLAN Creation	GVRP Registration	Copy To	Edit
1 1/1g1	Disable	Disable	Disable	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2 1/1g2	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
3 1/1g3	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
-----					
26 1/1g2	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
27 1/1g3	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
28 1/1g4	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
LAGs					
29 1ag1	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
30 1ag2	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
31 1ag3	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
32 1ag4	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
33 1ag5	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
34 1ag6	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
35 1ag7	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>
36 1ag8	Disable	Disable	Disable	<input type="checkbox"/>	<input type="checkbox"/>

**Unit**（单元）下拉式菜单用于查看堆栈中其它单元（如果存在）的 **GVRP Port Parameters Table**（GVRP 端口参数表）。

## 复制 GVRP 参数

□□□ 打开 **GVRP Global Parameters** (GVRP 全局参数) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **GVRP Port Parameters Table** (GVRP 端口参数表)。

□□□ 在 **Copy Parameters From** (复制参数来源) 中指定作为复制来源的 Port (端口) 或 LAG。

□□□ 对要接收这些参数的每个 Interface/LAG (接口/LAG) 单击 **Copy To** (复制至)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将复制 GVRP Port Configuration (GVRP 端口配置) 设置并更新设备。

## 修改多个端口的 GVRP 参数

□□□ 打开 **GVRP Global Parameters** (GVRP 全局参数) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **GVRP Port Parameters Table** (GVRP 端口参数表)。

□□□ 对每个要修改的 Interface/LAG (接口/LAG) 单击 **Edit** (编辑)。

□□□ 根据需要编辑 GVRP Port Parameter (GVRP 端口参数) 字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将复制 GVRP Port Parameter (GVRP 端口参数) 设置并更新设备。

## 使用 CLI 命令配置 GVRP

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- GVRP 命令

---

## 聚合端口

Link Aggregation (链路聚合) 允许将一条或多条全双工 (FDX) 以太网链路聚合在一起，形成链路聚合组 (LAG)。这使网络交换机可将 LAG 视为一条单独的链路。

系统支持静态 LAG。如果端口作为静态成员添加至 LAG，则端口既不发送 ACPDU，也不接收 ACPDU。

要显示 **Link Aggregation** (链路聚合) 页面，请在树视图中单击 **Switching** (交换) ® **Link Aggregation** (链路聚合)。**Link Aggregation** (链路聚合) 页面包含以下功能的链接：

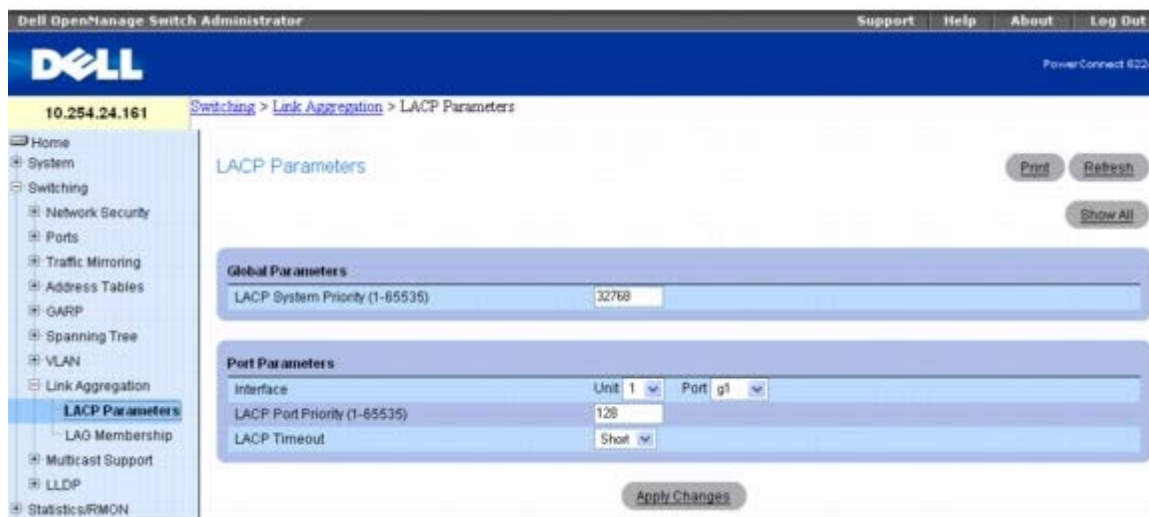
- [LACP 参数](#)
- [LAG 成员关系](#)
- [LAG 散列配置](#)
- [LAG 散列摘要](#)

## LACP 参数

系统通过定期交换 LACPDU 对 Link Aggregation（链路聚合）进行初始化和维护。**LACP Parameters（LACP 参数）** 页面用于配置 LACP LAG。

要显示 **LACP Parameters（LACP 参数）** 页面，请在树视图中单击 **Switching（交换）** ® **Link Aggregation（链路聚合）** ® **LACP Parameters（LACP 参数）**。

图 8-64. LACP 参数



**LACP Parameters（LACP 参数）** 页面分为两个部分：Global Parameters（全局参数）和 Port Parameters（端口参数）。以下是此页面中的字段：

### 全局参数

**LACP System Priority (1-65535)（LACP 系统优先级 [1-65535]）** — 表示全局设置的 LACP 优先级值。默认值为 1。

### 端口参数

**Interface（接口）** — 指定要分配超时和优先级值的单元和端口号。

**LACP Port Priority (1-65535)（LACP 端口优先级 [1-65535]）** — 指定用于被指定端口的 LACP 优先级值。默认值为 1。

**LACP Timeout（LACP 超时）** — 指定管理 LACP 超时。可能的值包括：

**Short（短）** — 指定短超时值。

**Long（长）** — 指定长超时值。这是默认设置。

### 定义链路聚合参数

□□□ 打开 **LACP Parameters（LACP 参数）** 页面。

□□□ 根据需要填写各字段。

□□□ 单击 **Apply Changes（应用更改）**。

系统将定义参数并更新设备。

## 显示 LACP 参数表

□□□ 打开 **LACP Parameters** (**LACP** 参数) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **LACP Parameters Table** (**LACP** 参数表)。

图 8-65. LACP 参数表

Port	Port Priority	LACP Timeout	Edit
1	128	Long	<input checked="" type="checkbox"/>
2	128	Long	<input type="checkbox"/>
3	128	Long	<input type="checkbox"/>
-----			
26	128	Long	<input type="checkbox"/>
27	128	Long	<input type="checkbox"/>
28	128	Long	<input type="checkbox"/>

□□□ **Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **LACP Parameters Table** (**LACP** 参数表)。

## 修改多个端口的 LACP 参数

□□□ 打开 **LACP Parameters** (**LACP** 参数) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **LACP Parameters Table** (**LACP** 参数表)。

□□□ 对每个要修改的 Port (端口) 单击 **Edit** (编辑)。

□□□ 根据需要编辑各字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 LACP 参数设置并更新设备。

## 使用 CLI 命令配置 LACP 参数

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- LACP 命令

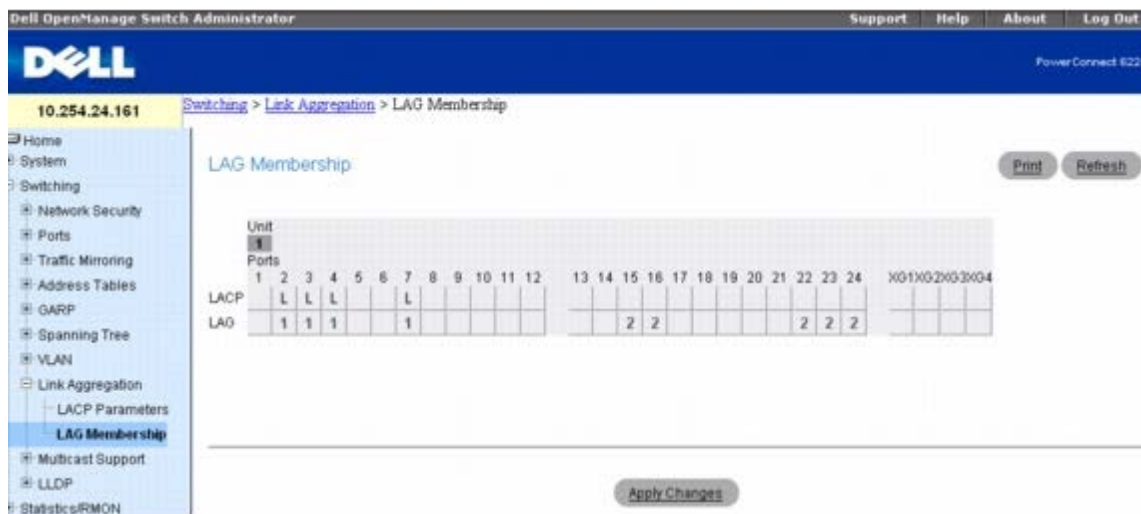
## LAG 成员关系



交换机支持每个系统 18 个 LAG，每个 LAG 8 个端口。**LAG Membership** (LAG 成员关系) 页面用于为 LAG 和 LACP 分配端口。

要显示 **LAG Membership** (LAG 成员关系) 页面，请在树视图中单击 **Switching** (交换) ® **Link Aggregation** (链路聚合) ® **LAG Membership** (LAG 成员关系)。

图 8-66. LAG 成员关系



**LAG Membership** (LAG 成员关系) 页面包含以下字段：

**LACP** — 将 LAG 端口聚合至 LACP 成员关系。如果端口在 LAG 行中有编号，可在 LACP 行中单击以便将 LACP 切换为 On (开)。每次单击将在 L (LACP) 和空白 (无 LACP) 间切换。

**LAG** — 向 LAG 添加端口，并指示端口从属的特定 LAG。每次单击将从 1 至 18 依次切换 LAG 号，然后回归空白 (未分配 LAG)。

## 向 LAG 添加端口

□□□ 打开 **LAG Membership** (LAG 成员关系) 页面。

□□□ 在 **LAG** 行中单击以便将端口切换到所需的 LAG。

系统将显示该端口的 LAG 号。每次单击时 LAG 号均会增加，直至达到 18，然后回归空白 (未分配 LAG)。

□□□ 单击 **Apply Changes** (应用更改)。

系统会将端口分配给选定的 LAG 并更新设备。

## 向 LACP 添加 LAG 端口

□□□ 打开 **LAG Membership** (LAG 成员关系) 页面。

□□□ 在 **LAG** 行中单击，以便将所需的 LAG 端口切换到 L。

 **注：** 必须先将端口分配给 LAG 后才能将其聚合至 LACP。

□□□ 单击 **Apply Changes** (应用更改)。

系统会将端口聚合至 LACP 并更新设备。

## 使用 CLI 命令向 LAG 和 LACP 分配端口

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

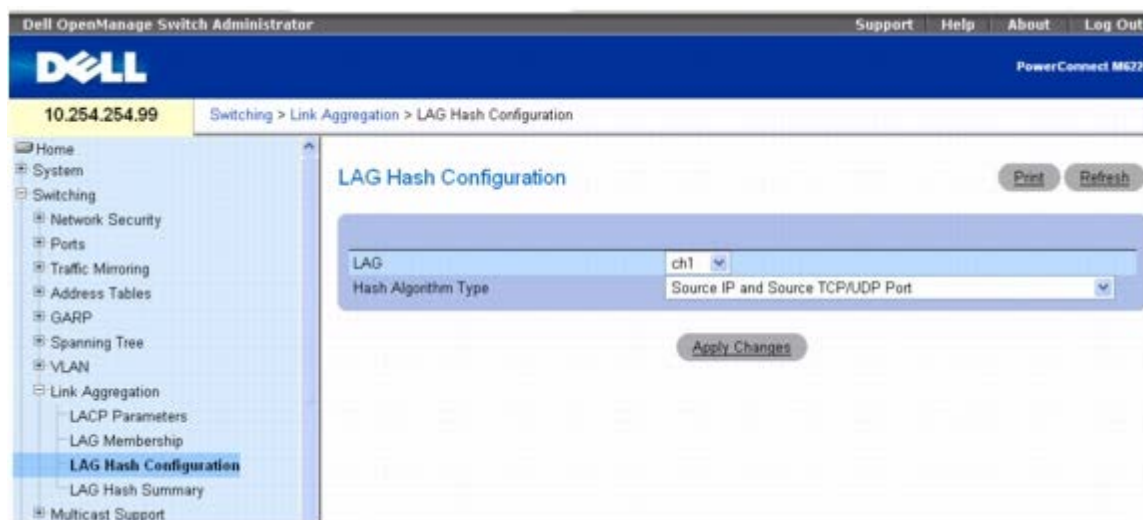
- 端口信道命令

## LAG 散列配置

使用 LAG 散列算法可以设置聚合器链路上的通信分布模式。您可以为每个主干设置散列类型。

要显示 **LAG Hash Configuration** (LAG 散列配置) 页面，请在树视图中单击 **Switching** (切换) ® **Link Aggregation** (链路聚合) ® **LAG Hash Configuration** (LAG 散列配置)。

图 8-67. LAG 散列配置



**LAG Hash Configuration** (LAG 散列配置) 页面包含以下字段：

**LAG** — 下拉式菜单会列出 LAG 号。

**Hash Algorithm Type** (散列算法类型) — 用于单点传送通信流的散列算法的类型可以是：

- Source MAC, VLAN, EtherType, SourceModule and Port Id (源 MAC、VLAN、以太网类型、源模块和端口 ID)
- Destination MAC, VLAN, EtherType, SourceModule and Port Id (目的地 MAC、VLAN、以太网类型、源模块和端口 ID)
- Source IP and Source TCP/UDP Port (源 IP 和源 TCP/UDP 端口) (默认设置)
- Destination IP and Destination TCP/UDP Port (目的地 IP 和目的地 TCP/UDP 端口)
- Source/Destination MAC, VLAN, EtherType, source MODID/port (源/目的地 MAC、VLAN、以太网类型、源 MODID/端口)
- Source/Destination IP and source/destination TCP/UDP port (源/目的地 IP 和源/目的地 TCP/UDP 端口)

## 配置 LAG 散列

□□□ 打开 **LAG Hash Configuration** (LAG 散列配置) 页面。

□□□ 选择要配置的 LAG 和要分配给该 LAG 的散列算法。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改参数并更新设备。

## 使用 CLI 命令配置 LAG 散列

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 端口信道命令

## LAG 散列摘要

**LAG Hash Summary**（LAG 散列摘要）页面会列出系统中的信道以及为它们分配的散列算法类型。

要显示 **LAG Hash Summary**（LAG 散列摘要）页面，请在树视图中单击 **Switching**（切换）® **Link Aggregation**（链路聚合）® **LAG Hash Summary**（LAG 散列摘要）。

图 8-68. LAG 散列摘要

LAGs	Hash Algorithm Type
1 ch1	Source IP and Source TCP/UDP Port
2 ch2	Source IP and Source TCP/UDP Port
3 ch3	Source IP and Source TCP/UDP Port
4 ch4	Source IP and Source TCP/UDP Port
5 ch5	Source IP and Source TCP/UDP Port
6 ch6	Source IP and Source TCP/UDP Port
7 ch7	Source IP and Source TCP/UDP Port
8 ch8	Source IP and Source TCP/UDP Port
9 ch9	Source IP and Source TCP/UDP Port
10 ch10	Source IP and Source TCP/UDP Port
11 ch11	Source IP and Source TCP/UDP Port
12 ch12	Source IP and Source TCP/UDP Port
13 ch13	Source IP and Source TCP/UDP Port
14 ch14	Source IP and Source TCP/UDP Port
15 ch15	Source IP and Source TCP/UDP Port
16 ch16	Source IP and Source TCP/UDP Port
17 ch17	Source IP and Source TCP/UDP Port
18 ch18	Source IP and Source TCP/UDP Port

**LAG Hash Summary**（LAG 散列摘要）页面包含以下字段：

**LAGs** — 列出 LAG 号。

**Hash Algorithm Type**（散列算法类型）— 显示与 LAG 相关的单点传送通信流所使用的散列算法类型。

## 使用 CLI 命令查看 LAG 散列算法摘要

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 端口信道命令

## 管理多点传送支持

交换机使用 **Layer 2 Multicast Forwarding Database**（第 2 层多点传送转发数据库）决定如何转发到达带有多点传送目的地 **MAC** 地址的信息包。通过限定多点传送，只将其转发至交换机上的特定端口，可防止将通信转发到网络中无需该通信的部分。

一旦信息包进入交换机，则交换机将目的地 **MAC** 地址与 **VLAN ID** 组合，并在 **Layer 2 Forwarding database**（第 2 层转发数据库）中进行搜索。如果未发现匹配项，则根据交换机配置将该信息包多路发送至 **VLAN** 中的所有端口或丢弃。如果发现匹配项，则信息包只被转发至是该多点传送组成员的端口。

要显示 **Multicast Support**（多点传送支持）菜单页面，请在树视图中单击 **Switching**（交换）® **Multicast Support**（多点传送支持）。此 **Multicast Support**（多点传送支持）页面包含以下功能的链接：

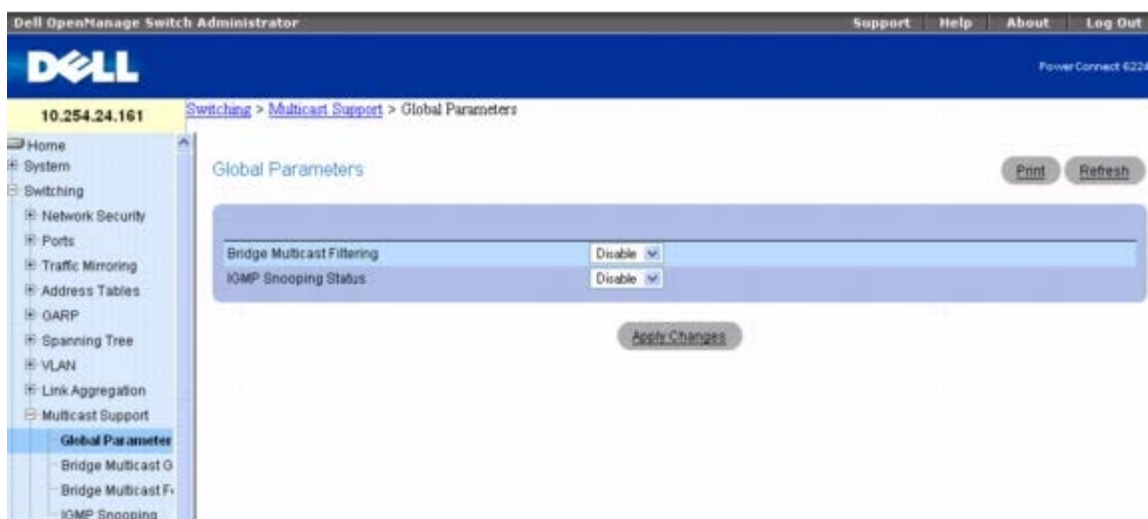
- [多点传送全局参数](#)
- [网桥多点传送组](#)
- [网桥多点传送转发](#)
- [IGMP 监测](#)

## 多点传送全局参数

**Multicast Global Parameters**（多点传送全局参数）页面用于在交换机上启用网桥多点传送筛选或 **IGMP 监测**。用于这些功能的参数可在[网桥多点传送转发](#)和 [IGMP 监测](#)网页上进行修改。

要显示 **Multicast Global Parameters**（多点传送全局参数）页面，请在树视图中单击 **Switching**（交换）® **Multicast Support**（多点传送支持）® **Global Parameters**（全局参数）。

图 8-69. 多点传送全局参数



**Multicast Global Parameters**（多点传送全局参数）页面包含以下字段：

**Bridge Multicast Filtering**（网桥多点传送筛选）— 启用或禁用网桥多点传送筛选。默认值为禁用。

**IGMP Snooping Status**（**IGMP 监测状态**）— 启用或禁用 **IGMP 监测**。默认值为禁用。

### 在交换机上启用网桥多点传送筛选

□□□ 打开 **Multicast Global Parameters**（多点传送全局参数）页面。

□□□ 在 **Bridge Multicast Filtering**（网桥多点传送筛选）字段中选择 **Enable**（启用）。

□□□ 单击 **Apply Changes** (应用更改)。

系统将在交换机上启用网桥多点传送。

## 使用 CLI 命令启用多点传送转发和/或 IGMP 监测

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

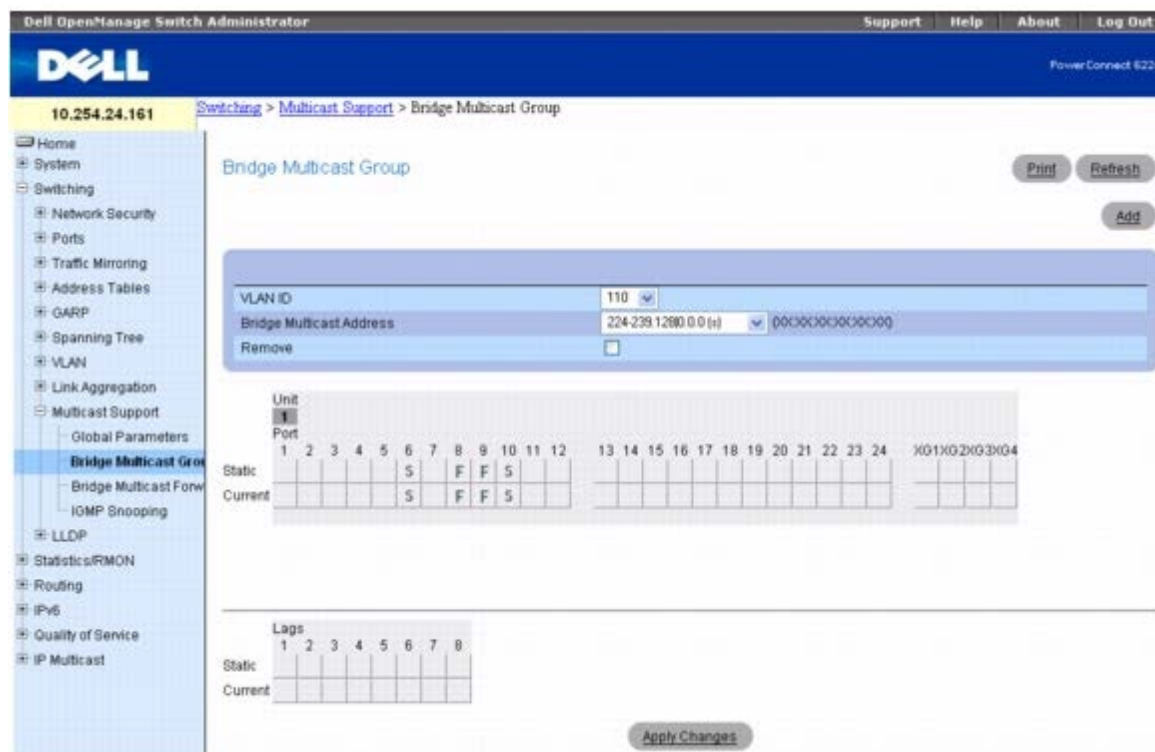
- 地址表命令

## 网桥多点传送组

**Bridge Multicast Group** (网桥多点传送组) 页面用于创建新的多点传送服务组或修改分配至现有多点传送服务组的端口和 LAG。Port (端口) 和 LAG 表中会显示连接的接口，并反映每个接口加入到 Multicast group (多点传送组) 的方式。

要显示 **Bridge Multicast Group** (网桥多点传送组) 页面，请在树视图中单击 **Switching** (交换) ® **Multicast Support** (多点传送支持) ® **Bridge Multicast Group** (网桥多点传送组)。

图 8-70. 网桥多点传送组



**Bridge Multicast Group** (网桥多点传送组) 页面包含以下字段：

**VLAN ID**— 选择要添加至多点传送组的 VLAN 或修改现有多点传送组中的端口。

**Bridge Multicast Address** (网桥多点传送地址) — 表示与所选 VLAN ID 相关联的多点传送组 MAC 地址/IP 地址。使用 **Add** (添加) 按钮可以为 VLAN ID 关联新的地址。

**Remove** (删除) — 一旦选中，则删除网桥多点传送地址。

## 端口和 LAG 成员表

**Bridge Multicast Group** (网桥多点传送组) 表会显示哪些端口和 LAG 是多点传送组的成员，以及它们的状态为静态 (S)、动态 (D) 还是禁

止 (F)。表中有两行：**Static** (静态) 和 **Current** (当前)。此页面中只有 **Static** (静态) 行可操作。**Current** (当前) 行会在更改 **Static** (静态) 行并单击 **Apply Changes** (应用更改) 时更新。

**Bridge Multicast Group** (网桥多点传送组) 页面包含两个可编辑的表：

**Unit and Ports** (单元和端口) — 显示并将多点传送组成员关系分配给端口。要分配成员关系，请在 **Static** (静态) 中单击特定的端口。每次单击将依次于 S、F 和空白定义请参见下表。

**LAGs**— 显示并将多点传送组成员关系分配给 LAG。要分配成员关系，请在 **Static** (静态) 中单击特定的 LAG。每次单击将依次于 S、F 和空白定义请参见下表。

下表包含端口/LAG IGMP 管理设置定义。

表 8-2. 端口/LAG IGMP 管理设置

端口控制	定义
D	动态：表示端口/LAG 已动态加入多点传送组 (在 <i>Current</i> [当前] 行中显示)。
S	静态：将端口作为 <i>Static</i> (静态) 行中的静态成员连接到多点传送组。一旦单击 <b>Apply Changes</b> (应用更改)，将显示在 <i>Current</i> (当前) 行中。
空白	空白：表示端口未连接至多点传送组。

## 添加网桥多点传送地址

□□□ 打开 **Bridge Multicast Group** (网桥多点传送组) 页面。

□□□ 单击 **Add** (添加)。

系统将显示 **Add Bridge Multicast Group** (添加网桥多点传送组) 页面。

图 8-71. 添加网桥多点传送组

□□□ 从下拉式菜单中选择 **VLAN ID**。

□□□ 定义 **New Bridge Multicast IP or MAC** (新的网桥多点传送 IP 或 MAC) 地址。

□□□ 在 **Bridge Multicast Group** (网桥多点传送组) 表中，通过在 **Static** (静态) 行中单击为特定的端口/LAG 分配配置。每次单击将依次于 S、F 和空白 (不是成员) 间切换。

□□□ 单击 **Apply Changes** (应用更改)。

系统将网桥多点传送地址分配至多点传送组，将端口/LAG 分配至组 (**Current** [当前] 行中的值随 **Static** [静态] 设置变化而更新)，



并更新设备。

## 将接口分配至现有的多点传送组

□□□ 打开 **Bridge Multicast Group** (网桥多点传送组) 页面。

□□□ 从下拉式菜单中选择 **VLAN ID**。

系统将显示关联的 **Bridge Multicast Address** (网桥多点传送地址)。

□□□ 在 **Bridge Multicast Group** (网桥多点传送组) 表中, 通过在 **Static** (静态) 行中单击为特定的端口/LAG 分配配置。每次单击将依次于 S、F 和空白 (不是成员) 间切换。

□□□ 单击 **Apply Changes** (应用更改)。

系统将接口分配至多点传送组, 按照 **Static** (静态) 设置更新 **Current** (当前) 行中的值并更新设备。

## 删除网桥多点传送组

□□□ 打开 **Bridge Multicast Group** (网桥多点传送组) 页面。

□□□ 从下拉式菜单中选择要删除的与网桥多点传送组相关联的 **VLAN ID**。

系统将显示 **Bridge Multicast Address** (网桥多点传送地址) 和分配的端口/LAG。

□□□ 选中 **Remove** (删除) 复选框。

□□□ 单击 **Apply Changes** (应用更改)。

系统将删除所选的网桥多点传送组并更新设备。

## 使用 CLI 命令管理多点传送服务成员

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- 地址表命令

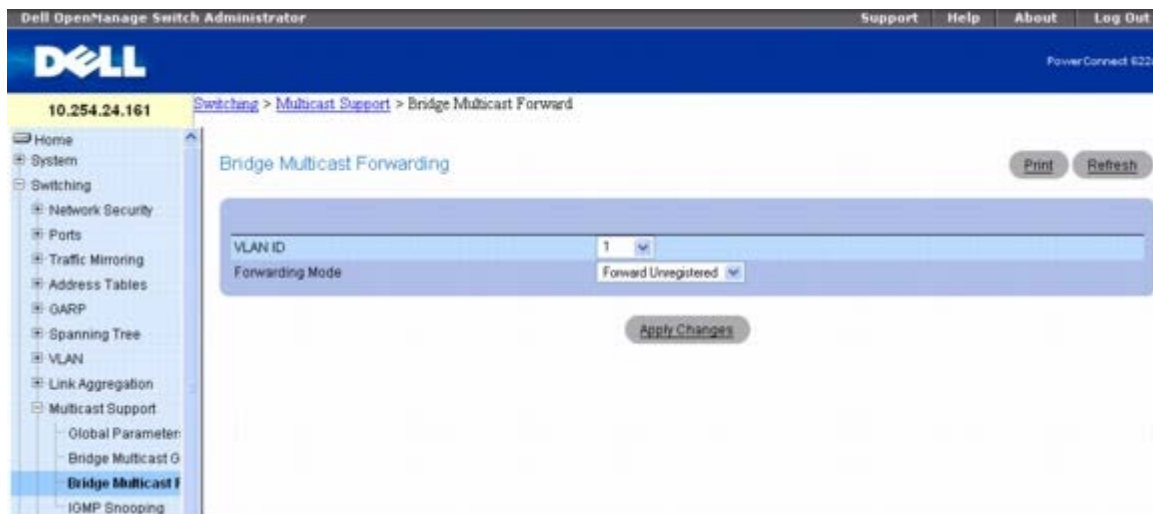
## 网桥多点传送转发

**Bridge Multicast Forward** (网桥多点传送转发) 页面用于启用连接至交换机 (与相邻的多点传送交换机相连) 的端口或 LAG。一旦启用 IGMP Snooping (IGMP 监测), 多点传送信息包将转发至相应的端口或 VLAN。

要显示 **Bridge Multicast Forward** (网桥多点传送转发) 页面, 请在树视图中单击 **Switching** (交换) ® **Multicast Support** (多点传送支持) ® **Bridge Multicast Forward** (网桥多点传送转发)。

图 8-72. 网桥多点传送转发





**Bridge Multicast Forward**（网桥多点传送转发）页面包含以下字段和两个可编辑的表：

**VLAN ID** — 选择受影响的 VLAN。

**Forwarding Mode**（转发模式）— 指定所选 VLAN 的多点传送转发模式。可能的值包括：

**Forward Unregistered**（转发未注册）— 允许转发目的地地址与早前 IGMP Membership Report（IGMP 成员关系报告）中所宣布任何组的地址均不匹配的 IPv4 多点传送信息包。

**Forward All**（全部转发）— 允许转发注册和未注册的多点传送信息包。

**Filter Unregistered**（筛选未注册）— 禁止转发目的地地址与早前 IGMP Membership Report（IGMP 成员关系报告）中所宣布任何组的地址均不匹配的 IPv4 多点传送信息包。

更改网桥多点传送转发模式。

- 打开 **Bridge Multicast Forward**（网桥多点传送转发）页面。
- 从下拉式菜单中选择 **VLAN ID**。
- 从下拉式菜单中选择 **Forwarding Mode**（转发模式）以分配 VLAN。
- 单击 **Apply Changes**（应用更改）。

系统将按照 **Forwarding Mode**（转发模式）设置更新 VLAN 并更新设备。

使用 **CLI** 命令管理连接至多点传送路由器的 **LAG** 和端口

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

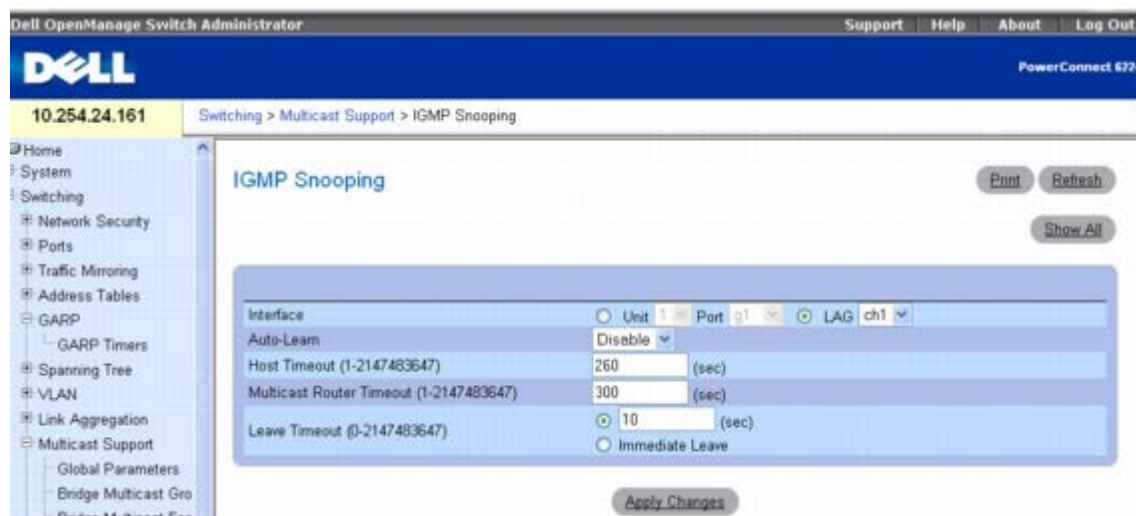
- 地址表命令

## IGMP 监测

**IGMP Snooping**（IGMP 监测）页面用于添加 IGMP 成员。

要显示 **IGMP Snooping**（IGMP 监测）页面，请在树视图中单击 **Switching**（交换）® **Multicast Support**（多点传送支持）® **IGMP Snooping**（IGMP 监测）。

图 8-73. IGMP 监测



**IGMP Snooping** (**IGMP** 监测) 页面包含以下字段：

**Interface** (接口) — 选择受影响的单元和端口。

**Auto-Learn** (自动记忆) — 在交换机上启用或禁用自动记忆。

**Host Timeout** (主机超时) — 指定 IGMP 监测条目过期前的时间。默认时间为 260 秒。

**Multicast Router Timeout** (多点传送路由器超时) — 指定多点传送路由器条目过期前的时间。默认值为 300 秒。

**Leave TimeOut** (离开超时) — 指定在接收到端口离开信息之后、条目过期之前的时间 (以秒为单位)。输入一个时间值作为超时的时段，或单击 **Immediate Leave** (立即离开) 指定立即超时。默认超时为 10 秒。

## 在交换机上启用 **IGMP** 监测

- 打开 **IGMP Snooping** (**IGMP** 监测) 页面。
- 在 **Interface** (接口) 字段中选择要配置的单元和端口。
- 根据需要填写页面中的各个字段。
- 单击 **Apply Changes** (应用更改)。

系统将在交换机上启用 **IGMP** 监测。

## 显示 **IGMP** 监测表

- 打开 **IGMP Snooping** (**IGMP** 监测) 页面。
- 单击 **Show All** (全部显示)。

系统将显示 **IGMP Snooping Table** (**IGMP** 监测表)。

图 8-74. **IGMP** 监测表



□□□ **Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **IGMP Snooping Table** (IGMP 监测表)。

## 修改多个端口或 LAG 的 IGMP 监测设置

□□□ 打开 **IGMP Snooping** (IGMP 监测) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **IGMP Snooping Table** (IGMP 监测表)。

□□□ 对每个要修改的端口或 LAG 单击 **Edit** (编辑)。

□□□ 根据需要编辑 IGMP Snooping (IGMP 监测) 字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 IGMP Snooping (IGMP 监测) 设置并更新设备。

## 将 IGMP 监测设置复制到多个端口或 LAG

□□□ 打开 **IGMP Snooping** (IGMP 监测) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **IGMP Snooping Table** (IGMP 监测表)。

□□□ 单击 **Copy Parameters From** (复制参数来源)。

□□□ 选择一个单元/端口或 LAG 作为所需参数的来源。

□□□ 为要将这些参数复制到的单元/端口或 LAG 单击 **Copy To** (复制至)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 IGMP Snooping (IGMP 监测) 设置并更新设备。

## 使用 CLI 命令配置 IGMP 监测

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- IGMP 监测命令

## 配置链路层发现协议 (LLDP)

链路层发现协议 (LLDP) 是 IEEE 802.1AB 定义的标准，允许驻留在 802 LAN 上的站点公布主要功能和物理描述。此信息可通过网络管理器查看，用于在 LAN 上识别系统拓扑及检测有问题的配置。

LLDP 是单向协议；不存在请求/响应顺序。信息由执行发送功能的站点公布，由执行接收功能的站点接收和处理。可以在每个端口单独启用/禁用发送和接收功能。默认情况下，发送和接收在所有端口上均被禁用。该应用负责根据端口的配置状态和运行状态，适当地启动发送和接收状态机。

LLDP 菜单页面包含以下功能的链接：

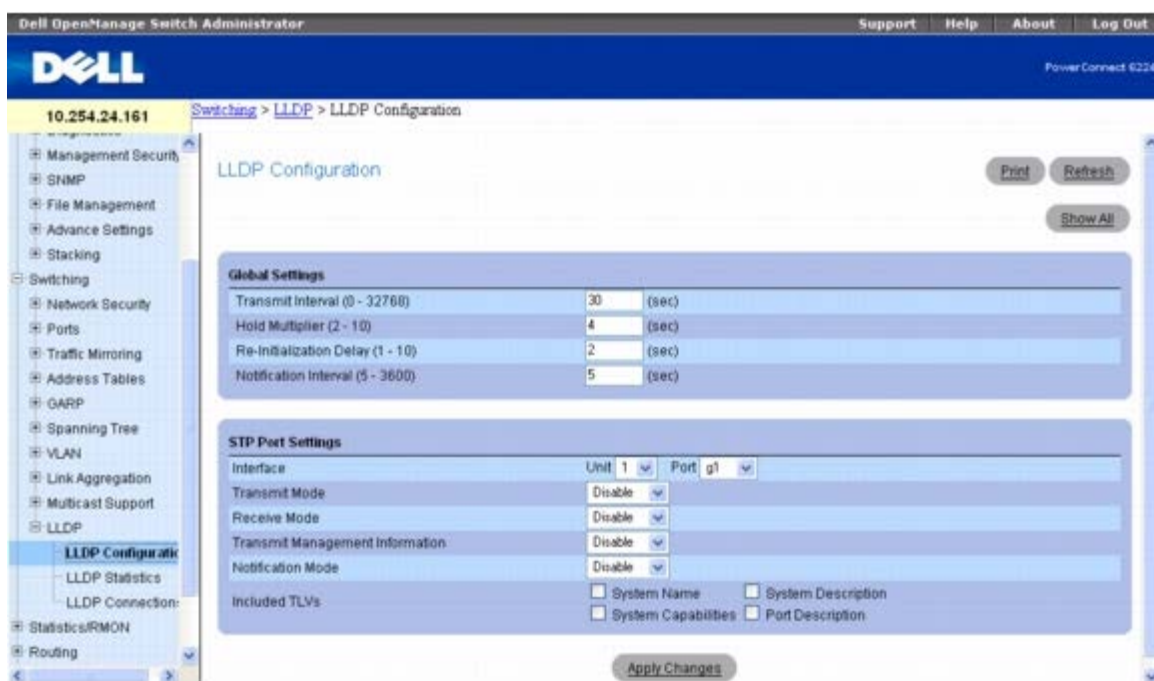
- [LLDP 配置](#)
- [LLDP 统计数据](#)
- [LLDP 连接](#)

## LLDP 配置

LLDP Configuration (LLDP 配置) 页面用于指定 LLDP 参数。通过此页面既可指定用于整个系统的参数，也可指定用于特定接口的参数。

要显示 **LLDP Configuration (LLDP 配置)** 页面，请在树视图中单击 **Switching (交换) @ LLDP @ LLDP Configuration (LLDP 配置)**。

图 8-75. LLDP 配置



**LLDP Configuration** (**LLDP** 配置) 页面包含以下字段：

## 全局设置

**Transmit Interval (1-32768)** (发送时间间隔 [**1-32768**]) — 指定发送帧的时间间隔。默认值为 30 秒。

**Hold Multiplier (2-10)** (保持放大器 [**2-10**]) — 指定要分配给 TTL 的发送时间间隔放大器。默认值为 4。

**Re-Initialization Delay (1-10)** (重新初始化延迟时间 [**1-10**]) — 指定重新初始化之前的延迟时间。默认值为 2 秒。

**Notification Interval (5-3600)** (通知时间间隔 [**5-3600**]) — 限制通知的发送。默认值为 5 秒。

## 端口设置

**Interface** (接口) — 指定这些参数所影响的端口。

**Transmit Mode** (发送模式) — 启用或禁用发送功能。默认设置为已禁用。

**Receive Mode** (接收模式) — 启用或禁用接收功能。默认设置为已禁用。

**Transmit Management Information** (发送管理信息) — 启用或禁用管理地址实例的发送。默认值为已禁用。

**Notification Mode** (通知模式) — 启用或禁用远程更改通知。默认设置为已禁用。

**Included TLVs** (包括的 **TLV**) — 选择要发送的 TLV 信息。选择包括：System Name (系统名称)、System Capabilities (系统能力)、System Description (系统描述) 和 Port Description (端口描述)。

## 修改 LLDP 配置

打开 **LLDP Configuration** (**LLDP** 配置) 页面。

根据需要定义各个字段。

单击 **Apply Changes** (应用更改)。

系统将 LLDP 参数保存至交换机。

## 显示 LLDP 接口设置表

打开 **LLDP Configuration** (**LLDP** 配置) 页面。

单击 **Show All** (全部显示)。

系统将显示 **LLDP Interface Settings Table** (**LLDP** 接口设置表)。

图 8-76. LLDP 接口设置表



□□□ **Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **LLDP Interface Settings Table** (LLDP 接口设置表)。

## 复制 LLDP 接口设置

□□□ 打开 **LLDP Configuration** (LLDP 配置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **LLDP Interface Settings Table** (LLDP 接口设置表)。

□□□ 在 **Copy Parameters From** (复制参数来源) 中指定作为复制来源的 **Unit** (单元) 和 **Port** (端口)。

□□□ 对要接收这些参数的每个 **Unit/Port** (单元/端口) 单击 **Copy To** (复制至)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将复制 LLDP Interface (LLDP 接口) 设置并更新设备。

## 修改多个端口的 LLDP 接口设置

□□□ 打开 **LLDP Configuration** (LLDP 配置) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **LLDP Interface Settings Table** (LLDP 接口设置表)。

□□□ 对每个要修改的 **Unit/Port** (单元/端口) 单击 **Edit** (编辑)。

□□□ 根据需要编辑 LLDP Interface (LLDP 接口) 字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 LLDP Interface (LLDP 接口) 设置并更新设备。

## 使用 CLI 命令配置 LLDP 配置

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- LLDP 命令



## LLDP 统计数据

LLDP Statistics (LLDP 统计数据) 页面用于查看与 LLDP 有关的统计数据。

要显示 **LLDP Statistics** (LLDP 统计数据) 页面，请在树视图中单击 **Switching** (交换) ® **LLDP** ® **LLDP Statistics** (LLDP 统计数据)。

图 8-77. LLDP 统计数据

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "LLDP Statistics" and includes a "Unit" dropdown menu set to "1". Below this, a summary table shows the following values:

Last Update	0d 00:00:00
Total Inserts	0
Total Deletes	0
Total Drops	0
Total Ageouts	0

Below the summary is a table with the following data:

Interface	Transmit Total	Receive Total	Discards	Errors	Ageouts	TLV Discards	TLV
1/g1	0	0	0	0	0	0	0
1/g2	0	0	0	0	0	0	0
1/xg3	0	0	0	0	0	0	0
1/xg4	0	0	0	0	0	0	0

A "Clear Statistics" button is located at the bottom of the table.

**LLDP Statistics** (LLDP 统计数据) 页面包含以下字段：

### 系统范围的统计数据

**Last Update** (上一次更新) — 显示上一次创建、修改或删除远程数据条目的系统运行时间值。

**Total Inserts** (总插入次数) — 显示由远程交换机发布的完整信息集插入表中的次数。

**Total Deletes** (总删除次数) — 显示由远程交换机发布的完整信息集从表中删除的次数。

**Total Drops** (总丢弃次数) — 显示由远程交换机发布的完整信息集因资源不足而无法插入的次数。

**Total Ageouts** (总过期次数) — 显示任何远程数据条目因 TTL (存活时间) 期满而删除的次数。

### 端口统计数据

**Interface** (接口) — 显示该行统计数据应用的 **Unit** (单元) 和 **Port** (端口)。

**Transmit Total** (发送总数) — 显示所指示端口上发送的 LLDP 帧总数。



**Receive Total**（接收总数）— 显示所指示端口上接收的有效 LLDP 帧总数。

**Discards**（丢弃数）— 显示所指示端口上接收并因任何原因而丢弃的 LLDP 帧数量。

**Errors**（错误数）— 显示所指示端口上接收的无效 LLDP 帧数量。

**Ageouts**（过期数）— 显示所指示端口上某个远程数据条目因 TTL 期满而删除的次数。

**TLV Discards**（TLV 丢弃数）— 显示所指示端口上接收并因任何原因而被 LLDP 代理丢弃的 LLDP TLVs (Type, Length, Value sets) (LLDP TLV [类型、长度、值集]) 数量。

**TLV Unknowns**（TLV 未知数）— 显示所指示端口上接收而不能被 LLDP 代理识别的 LLDP TLV 数量。

**Unit**（单元）下拉式菜单用于查看堆栈中其它单元（如果存在）的 **LLDP Statistics**（LLDP 统计数据）。

**Clear Statistics**（清除统计数据）按钮用于将所有 LLDP Statistics（LLDP 统计数据）重置为零。

## 使用 CLI 命令显示 LLDP 统计数据

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- LLDP 命令

## LLDP 连接

**LLDP Connections**（LLDP 连接）页面用于查看启用了 LLDP 的端口列表。系统将显示基本连接详情。

要显示 **LLDP Connections**（LLDP 连接）页面，请在树视图中单击 **Switching**（交换）® **LLDP** ® **LLDP Connections**（LLDP 连接）。

图 8-78. LLDP 连接表

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb navigation is 'Switching > LLDP > LLDP Connections'. The page title is 'LLDP Connections'. There are 'Print' and 'Refresh' buttons. A 'Unit' dropdown menu is set to '1'. Below is a table with the following data:

Local Interface	Chassis ID	Port ID	System Name
1/a7	00:FC:E3:90:01:54	00:FC:E3:90:01:56	
1/a11	00:FC:E3:90:01:4B	00:FC:E3:90:01:4D	dell_141

There is a 'Clear Table' button below the table.

**LLDP Connections**（LLDP 连接）页面会显示以下端口详情：

**Local Interface**（本地接口）— 指定堆栈中的单元和端口。

**Chassis ID**（机箱 ID）— 标识 802 LAN 设备的机箱。

**Port ID**（端口 ID）— 标识发送 LLDPDU 的端口号。

**System Name** (系统名称) — 标识远程设备的系统名称。

**Unit** (单元) 下拉式菜单用于查看堆栈中其它单元 (如果存在) 的 **LLDP Connections** (LLDP 连接)。

**Clear Table** (清除表) 按钮用于从 **LLDP Connections** (LLDP 连接) 表中删除所有信息。

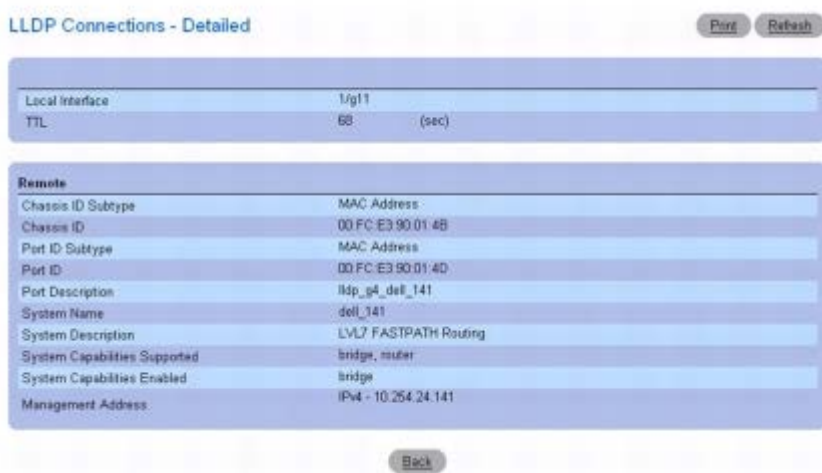
## 查看 LLDP 连接的详情

□□□ 打开 **LLDP Connections** (LLDP 连接) 页面。

□□□ 在 **Local Interface** (本地接口) 字段中单击接口，以查看该设备的详情。

系统将显示该设备的 **LLDP Connections - Detailed** (LLDP 连接 - 详情) 页面。

图 8-79. LLDP 连接详情



□□□ **Back** (返回) 按钮用于返回到 **LLDP Connections** (LLDP 连接) 页面。

## 使用 CLI 命令查看 LLDP 连接

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- LLDP 命令

[返回目录页面](#)

[返回目录页面](#)

# 查看统计数据/RMON


Dell™ PowerConnect™ 6200 系列用户指南

- [表视图](#)
- [RMON](#)
- [图表](#)

借助远程监测 (RMON) 功能, 网络管理员可以通过远程访问了解网络的性能和状态。受支持的监测组有四种, 它们定义为 RMON 标准的部分: 统计数据、历史记录、报警和事件。

本节说明了 **Statistics/RMON** (统计数据/RMON) 菜单页面中可用的 RMON 选项。这些选项包括以表形式查看统计数据、编辑和查看 RMON 统计数据, 以及以图表形式显示端口和 LAG 统计数据。在 **Statistics/RMON** (统计数据/RMON) 菜单页面上, 可以通过以下菜单页面来访问这些选项:

- [表视图](#)
- [RMON](#)
- [图表](#)

 注: CLI 命令并非对所有统计数据/RMON 页面均可用。

## 表视图

**Table Views** (表视图) 菜单页面包含一些以表形式显示统计数据的网页的链接。要显示此页面, 请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **Table Views** (表视图)。在此菜单页面中可以访问以下网页:

- [接口统计数据](#)
- [以太网类统计数据](#)
- [GVRP 统计数据](#)
- [EAP 统计数据](#)
- [使用摘要](#)
- [计数器摘要](#)

## 接口统计数据

**Interface Statistics** (接口统计数据) 页面用于显示接收到和已发送的信息包的统计数据。用于接收到和已发送的信息包的字段是相同的。

要显示此页面, 请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **Table Views** (表视图) ® **Interface Statistics** (接口统计数据)。

图 9-1. 接口统计数据

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "Interface Statistics". At the top, there are configuration options: "Interface" (Unit No: 1, Port: g1, LAG: ch1), "Refresh Rate" (No Refresh), "Print", and "Refresh" buttons. Below this, there are two tables: "Receive Statistics" and "Transmit Statistics".

Receive Statistics	
Total Bytes(Octets)	128
Unicast Packets	2
Multicast Packets	0
Broadcast Packets	0
Packets with Errors	0

Transmit Statistics	
Total Bytes(Octets)	4490654
Unicast Packets	992
Multicast Packets	17362
Broadcast Packets	14355

**Interface Statistics** (接口统计数据) 页面包含以下字段:

**Interface** (接口) — 选择要为其显示统计数据的物理接口 (单元、端口) 或 LAG 接口。

**Refresh Rate** (刷新率) — 指定刷新统计数据之前经过的时间。可能的字段值包括: No Refresh (无刷新)、15、30 和 60 秒。默认值为 No Refresh (无刷新)。

## 接收的统计数据

**Total Bytes (Octets)** (字节总数 [八位位组]) — 显示选定的接口上接收到的八位位组的总数。

**Unicast Packets** (单点传送信息包) — 显示选定的接口上接收到的单点传送信息包的总数。

**Multicast Packets** (多点传送信息包) — 显示选定的接口上接收到的多点传送信息包的总数。

**Broadcast Packets** (广播信息包) — 显示选定的接口上接收到的广播信息包的总数。

**Packets with Errors** (包含错误的信息包) — 显示选定的接口上接收到的包含错误的信息包的总数。

## 发送统计数据

**Total Bytes (Octets)** (字节总数 [八位位组]) — 显示选定的接口上发送的八位位组的总数。

**Unicast Packets** (单点传送信息包) — 显示选定的接口上发送的单点传送信息包的总数。

**Multicast Packets** (多点传送信息包) — 显示选定的接口上发送的多点传送信息包的总数。

**Broadcast Packets** (广播信息包) — 显示选定的接口上发送的广播信息包的总数。

## 显示接口统计数据

□□□ 打开 **Interface Statistics** (接口统计数据) 页面。

□□□ 指定一个接口。

系统将显示指定接口的统计数据。

## 使用 CLI 命令查看接口统计数据

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

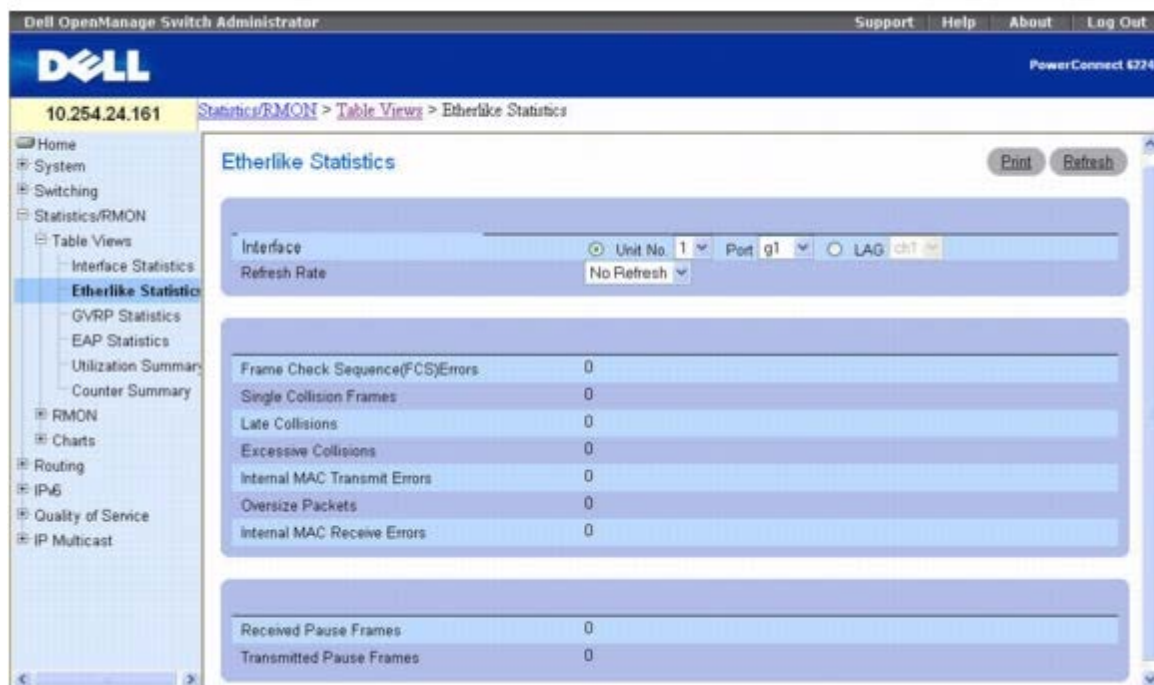
- 以太网配置命令

## 以太网类统计数据

**Etherlike Statistics** (以太网类统计数据) 页面用于显示接口统计数据。

要显示此页面，请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **Table Views** (表视图) ® **Etherlike Statistics** (以太网类统计数据)。

图 9-2. 以太网类统计数据



**Etherlike Statistics** (以太网类统计数据) 页面包含以下字段：

**Interface** (接口) — 选择要为其显示统计数据的物理接口 (单元、端口) 或 LAG 接口。

**Refresh Rate** (刷新率) — 指定刷新统计数据之前经过的时间。可能的字段值包括：No Refresh (无刷新)、15、30 和 60 秒。默认值为 No Refresh (无刷新)。

**Frame Check Sequence (FCS) Errors** (帧检查顺序 [FCS] 错误) — 显示选定的接口上接收到的 FCS 错误的数量。

**Signal Collision Frames** (信号冲突帧) — 显示选定的接口上接收到的信号冲突帧错误的数量。

**Late Collisions** (推迟冲突) — 显示选定的接口上接收到的推迟冲突的数量。

**Excessive Collisions** (严重冲突) — 显示选定的接口上接收到的严重冲突的数量。

**Internal MAC Transmit Errors** (内部 MAC 发送错误) — 显示选定的接口上内部 MAC 发送错误的数量。

**Oversize Packets** (超大信息包) — 显示接收到的长度大于 1518 个八位位组 (不包括成帧位，但包括 FCS 八位位组) 和其它格式良好的信息包的总数。

**Internal MAC Receive Errors** (内部 MAC 接收错误) — 显示选定的接口上内部 MAC 接收到的错误的数量。

**Received Pause Frames** (接收到的暂停帧) — 显示选定的接口上接收到的暂停帧的数量。

**Transmitted Pause Frames** (发送的暂停帧) — 显示选定的接口上发送的暂停帧的数量。

## 显示接口的以太网类统计数据

□□□ 打开 **Etherlike Statistics** (以太网类统计数据) 页面。

□□□ 指定一个接口。

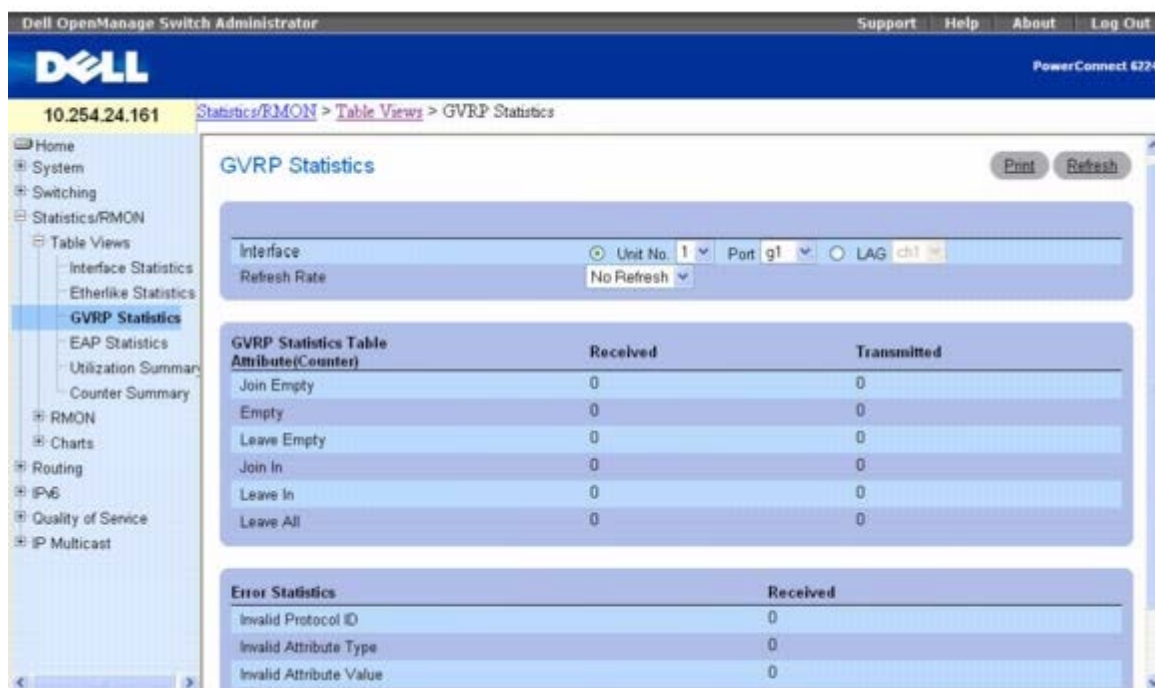
系统将显示指定接口的统计数据。

## GVRP 统计数据

**GVRP Statistics** (GVRP 统计数据) 页面用于显示 GVRP 的交换机统计数据。

要显示此页面，请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **Table Views** (表视图) ® **GVRP Statistics** (GVRP 统计数据)。

图 9-3. GVRP 统计数据



**GVRP Statistics** (GVRP 统计数据) 页面包含以下字段：

**Interface** (接口) — 选择要为其显示统计数据的物理接口 (单元、端口) 或 LAG 接口。

**Refresh Rate** (刷新率) — 指定刷新统计数据之前经过的时间。可能的字段值包括：No Refresh (无刷新)、15、30 和 60 秒。默认值为 No Refresh (无刷新)。

## GVRP 统计数据表属性 (计数器) - 接收和发送

**Join Empty** (加入空) — 显示交换机的 GVRP 加入空统计数据。

**Empty** (空) — 显示交换机的 GVRP 空统计数据。

**Leave Empty** (保留空) — 显示交换机的 GVRP 保留空统计数据。

**Join In** (加入) — 显示交换机的 GVRP 加入统计数据。

**Leave In** (保留) — 显示交换机的 GVRP 保留统计数据。

**Leave All** (全部离开) — 显示交换机的 GVRP 全部离开统计数据。

**Error Statistics** (错误统计数据) - **Received** (接收)

**Invalid Protocol ID** (无效协议 ID) — 显示交换机的 GVRP 无效协议 ID 统计数据。

**Invalid Attribute Type** (无效属性类型) — 显示交换机的 GVRP 无效属性类型统计数据。

**Invalid Attribute Value** (无效属性值) — 显示交换机的 GVRP 无效属性值统计数据。

**Invalid Attribute Length** (无效属性长度) — 显示交换机的 GVRP 无效属性长度统计数据。

**Invalid Event** (无效事件) — 显示交换机的 GVRP 无效事件统计数据。

## 显示接口的 **GVRP** 统计数据

打开 **GVRP Statistics** (GVRP 统计数据) 页面。

在 **Interface** (接口) 字段中选择接口。

系统将显示指定接口的 GVRP 统计数据。

## 使用 **CLI** 命令查看 **GVRP** 统计数据

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- GVRP 命令

## EAP 统计数据

**EAP Statistics** (EAP 统计数据) 页面用于显示有关特定端口上接收到的 EAP 信息包的信息。有关 EAP 的详细信息, 请参阅[基于端口的验证](#)。

要显示 **EAP Statistics** (EAP 统计数据) 页面, 请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **Table Views** (表视图) ® **EAP Statistics** (EAP 统计数据)。

图 9-4. EAP 统计数据



The screenshot shows the Dell OpenManage Switch Administrator interface. The top navigation bar includes 'Support', 'Help', 'About', and 'Log Out'. The main header displays the Dell logo and 'PowerConnect 6200'. The breadcrumb trail is 'Statistics/RMON > Table Views > EAP Statistics'. The left sidebar contains a tree view with categories like System, Switching, Statistics/RMON, and RMON. The main content area is titled 'EAP Statistics' and features a 'Print' and 'Refresh' button. Below the title, there are dropdown menus for 'Interface', 'Unit No' (set to 1), 'Port' (set to g1), and 'Refresh Rate' (set to No Refresh). A table displays the following statistics:

Frames Received	0
Frames Transmitted	0
Start Frames Received	0
Log off Frames Received	0
Response ID Frames Received	0
Response Frames Received	0
Request Frames Transmitted	0
Request ID Frames Transmitted	0
Invalid Frames Received	0
Length Error Frames Received	0
Last Frames Version	0
Last Frames Source	0000.0000.0000

**Interface** (接口) — 指定对其进行轮询以获得统计数据的接口。

**Refresh Rate** (刷新率) — 指定刷新统计数据之前经过的时间。可能的字段值包括: No Refresh (无刷新)、15、30 和 60 秒。默认值为 No Refresh (无刷新)。

**Frames Received** (接收到的帧) — 显示端口上接收到的有效 EAPOL 帧的数量。

**Frames Transmitted** (发送的帧) — 显示通过端口发送的 EAPOL 帧的数量。

**Start Frames Received** (接收到的启动帧) — 显示端口上接收到的 EAPOL 启动帧的数量。

**Log off Frames Received** (接收到的注销帧) — 显示端口上接收到的 EAPOL 注销帧的数量。

**Respond ID Frames Received** (接收到的响应 ID 帧) — 显示端口上接收到的 EAP 响应 ID 帧的数量。

**Respond Frames Received** (接收到的响应帧) — 显示端口上接收到的有效 EAP 响应帧的数量。

**Request ID Frames Received** (接收到的请求 ID 帧) — 显示端口上接收到的 EAP 请求 ID 帧的数量。

**Request Frames Transmitted** (发送的请求帧) — 显示通过端口发送的 EAP 请求帧的数量。

**Request ID Frames Transmitted** (发送的请求 ID 帧) — 显示通过端口发送的 EAP 请求 ID 帧的数量。

**Invalid Frames Received** (接收到的无效帧) — 显示该端口上接收到的无法识别的 EAPOL 帧的数量。

**Length Error Frames Received** (接收到的长度错误帧) — 显示该端口上接收到的具有无效信息包正文长度的 EAPOL 帧的数量。

**Last Frames Version** (最近帧的版本) — 显示与最近一次接收到的 EAPOL 帧相关的协议版本号。

**Last Frames Source** (最近帧的源) — 显示与最近一次接收到的 EAPOL 帧相关的源 MAC 地址。

## 显示接口的 EAP 统计数据

□□□ 打开 **EAP Statistics** (EAP 统计数据) 页面。

□□□ 在 **Interface** (接口) 字段中选择一个接口。

系统将显示所选接口的 EAP 统计数据。

## 使用 CLI 命令查看 EAP 统计数据

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 802.1X 命令

## 使用摘要

**Utilization Summary**（使用摘要）页面用于显示接口的使用统计数据。

要显示此页面，请在树视图中单击 **Statistics/RMON**（统计数据/RMON）® **Table Views**（表视图）® **Utilization Summary**（使用摘要）。

图 9-5. 使用摘要

The screenshot shows the 'Utilization Summary' page in the Dell OpenManage Switch Administrator. The page has a navigation tree on the left with 'Statistics/RMON' selected. The main content area displays a table with columns: Interface, Interface Status, Interface Utilization %, Unicast Received %, Non Unicast Packets Received %, and Error Packets Received %. Below this is a section for 'Global System LAGs' with a similar table. The interface includes a 'Unit' dropdown set to '1' and a 'Refresh Rate' dropdown set to 'No Refresh'.

Interface	Interface Status	Interface Utilization %	Unicast Received %	Non Unicast Packets Received %	Error Packets Received %
1 1/g1	Up	0	0	0	0
2 1/g2	Down	0	0	0	0
3 1/g3	Up	0	0	0	0

Global System LAGs					
Interface	Interface Status	Interface Utilization %	Unicast Received %	Non Unicast Packets Received %	Error Packets Received %
1 ch1	Down	0	0	0	0
2 ch2	Down	0	0	0	0
3 ch3	Down	0	0	0	0
4 ch4	Down	0	0	0	0
5 ch5	Down	0	0	0	0
6 ch6	Down	0	0	0	0
7 ch7	Down	0	0	0	0
8 ch8	Down	0	0	0	0

**Utilization Summary**（使用摘要）页面包含以下字段：

**Unit**（单元）— 指定要为其显示统计数据的单元。

**Refresh Rate**（刷新率）— 指定刷新统计数据之前经过的时间。可能的字段值包括：No Refresh（无刷新）、15、30 和 60 秒。默认值为 No Refresh（无刷新）。

**Interface**（接口）— 指定要为其显示统计数据的接口。

**Interface Status**（接口状态）— 显示接口的状态。

**Interface Utilization %**（接口使用百分比）— 显示基于接口的双工模式的网络接口使用百分比。该读数的范围为 0 至 200%。最大读数 200%（全双工连接）表示通过接口的通信使用了传入和传出连接的 100% 带宽。对于半双工连接，最大读数为 100%。

**Unicast Received %**（单点传送接收百分比）— 显示接口上接收到的单点传送信息包的百分比。

**Non Unicast Packets Received %** (非单点传送信息包接收百分比) — 显示接口上接收到的非单点传送信息包的百分比。

**Error Packets Received %** (错误信息包接收百分比) — 显示接口上接收到的包含错误的信息包的数量。

## 使用 CLI 命令查看接口使用统计数据

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- RMON 命令

## 计数器摘要

**Counter Summary** (计数器摘要) 页面用于显示接口使用统计数据的数字总和, 而不是百分比。

要显示此页面, 请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **Table Views** (表视图) ® **Counter Summary** (计数器摘要)。

图 9-6. 计数器摘要

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb path is Statistics/RMON > Table Views > Counter Summary. The page title is Counter Summary. There are 'Print' and 'Refresh' buttons. A 'Unit' dropdown is set to '1'. The 'Refresh Rate' dropdown is set to 'No Refresh'. The main table shows interface statistics for three interfaces: 1/g1 (Up), 1/g2 (Down), and 1/g3 (Down). Below this is a section for Global System LAGs with 8 entries, all showing a 'Down' status and zero packet counts.

Interface	Interface Status	Received Unicast Packets	Transmit Unicast Packets	Received Non Unicast Packets	Transmit Non Unicast Packets	Received Errors	Transmit Errors
1 1/g1	Up	6639503	6339	365892	133960	0	0
2 1/g2	Down	0	0	0	0	0	0
3 1/g3	Down	0	0	0	0	0	0

Global System LAGs							
1	ch1	Down	0	0	0	0	0
2	ch2	Down	0	0	0	0	0
3	ch3	Down	0	0	0	0	0
4	ch4	Down	0	0	0	0	0
5	ch5	Down	0	0	0	0	0
6	ch6	Down	0	0	0	0	0
7	ch7	Down	0	0	0	0	0
8	ch8	Down	0	0	0	0	0

**Counter Summary** (计数器摘要) 页面包含以下字段:

**Unit** (单元) — 指定要为其显示统计数据的单元。

**Refresh Rate** (刷新率) — 指定刷新统计数据之前经过的时间。可能的字段值包括: No Refresh (无刷新)、15、30 和 60 秒。默认值为 No Refresh (无刷新)。

**Interface** (接口) — 指定要为其显示统计数据的接口。

**Interface Status** (接口状态) — 显示接口的状态。

**Received Unicast Packets** (接收的单点传送信息包) — 显示接口上接收到的单点传送信息包的数量。

**Transmit Unicast Packets** (发送的单点传送信息包) — 显示从接口发送的单点传送信息包的数量。

**Received Non Unicast Packets** (接收的非单点传送信息包) — 显示接口上接收到的非单点传送信息包的数量。

**Transmit Non Unicast Packets** (发送的非单点传送信息包) — 显示从接口发送的非单点传送信息包的数量。

**Received Errors** (接收的错误) — 显示接口上接收到的错误的数量。

**Transmit Errors** (发送的错误) — 显示从接口发送的错误的数量。

## 设置刷新率

打开 **Counter Summary** (计数器摘要) 页面。

从下拉式菜单中选择 **Refresh Rate** (刷新率)。

系统将以所选频率刷新所显示的接口的统计数据。

## 使用 CLI 命令查看数字端口使用统计数据

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- RMON 命令

---

# RMON

借助远程监测 (RMON) 功能, 网络管理员可以通过远程访问了解网络的性能和状态。

要显示 **RMON** 菜单页面, 请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **RMON**。 **RMON** 菜单页面包含以下功能的链接:

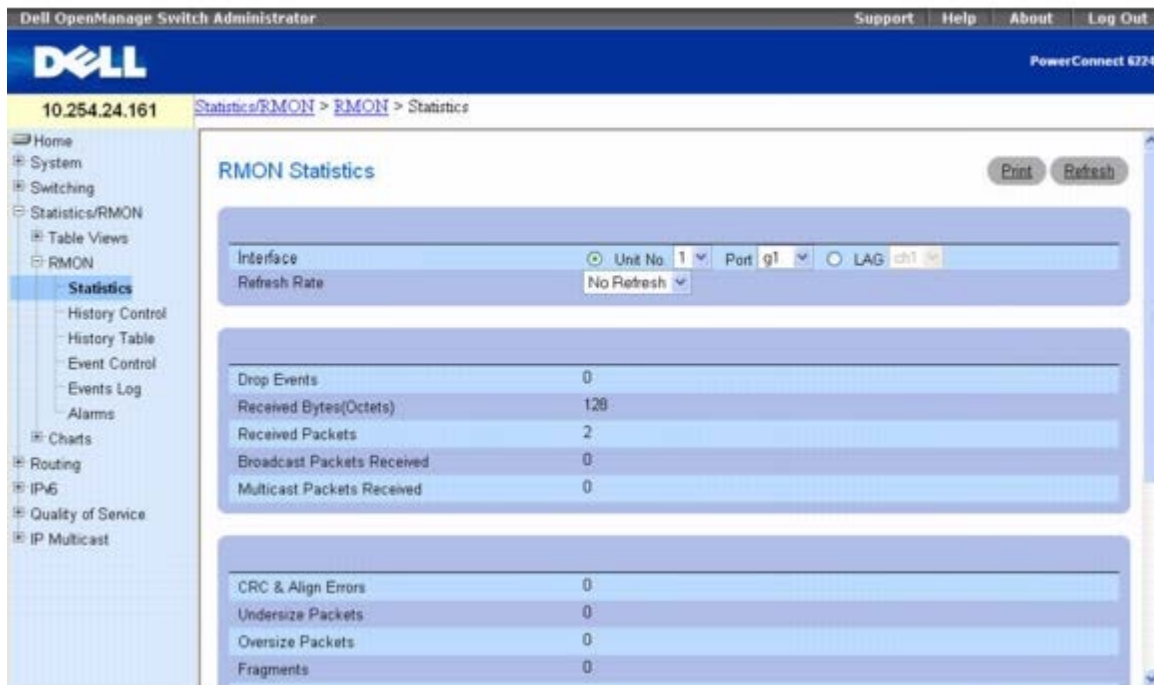
- [RMON 统计数据](#)
- [RMON 历史记录控制统计数据](#)
- [RMON 历史记录表](#)
- [RMON 事件控制](#)
- [RMON 事件日志](#)
- [RMON 警报](#)

## RMON 统计数据

**RMON Statistics** (**RMON** 统计数据) 页面用于显示有关交换机使用的详细信息, 例如信息包处理统计数据和交换机发生的错误。

要显示此页面, 请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **RMON** ® **Statistics** (统计数据)。

图 9-7. RMON 统计数据



**RMON Statistics (RMON 统计数据)** 页面包含以下字段:

**Interface (接口)** — 指定是否为单元或 LAG 显示统计数据以及显示哪个单元/LAG。

**Refresh Rate (刷新率)** — 指定刷新统计数据之前经过的时间。可能的字段值包括: No Refresh (无刷新)、15、30 和 60 秒。默认值为 No Refresh (无刷新)。

**Drop Events (丢弃事件数)** — 显示自上一次刷新交换机以来接口上发生的丢弃事件的数量。

**Received Bytes (Octets) (接收到的字节数 [八位位组])** — 显示自上一次刷新交换机以来接口上接收到的八位位组的数量。该数量包括坏信息包和 FCS 八位位组,但不包括成帧位。

**Received Packets (接收的信息包)** — 显示自上一次刷新交换机以来接口上接收到的信息包的数量,包括坏信息包、多点传送信息包和广播信息包。

**Broadcast Packets Received (接收的广播信息包)** — 显示自上一次刷新交换机以来接口上接收到的完好广播信息包的数量。该数量不包括多点传送信息包。

**Multicast Packets Received (接收的多点传送信息包)** — 显示自上一次刷新交换机以来接口上接收到的完好多点传送信息包的数量。

**CRC & Align Errors (CRC 和校准错误)** — 显示自上一次刷新交换机以来接口上发生的 CRC 和校准错误的数量。

**Undersize Packets (超小信息包)** — 显示自上一次刷新交换机以来接口上接收到的超小信息包 (少于 64 个八位位组) 的数量。

**Oversize Packets (超大信息包)** — 显示自上一次刷新交换机以来接口上接收到的超大信息包 (超过 1518 个八位位组) 的数量。

**Fragments (碎片)** — 显示自上一次刷新交换机以来接口上接收到的碎片 (少于 64 个八位位组的信息包,不包括成帧位,但包括 FCS 八位位组) 的数量。

**Jabbers (无用信息)** — 显示在取样会话过程中接收到的长度大于 1518 个八位位组并带有 FCS 的信息包的数量。

**Collisions (冲突)** — 显示自上一次刷新交换机以来接口上接收到的冲突的数量。

**Frames of 64 Bytes (64 字节帧)** — 显示自上一次刷新交换机以来接口上接收到的 64 字节帧的数量。

**Frames of 65 to 127 Bytes (65 至 127 字节帧)** — 显示自上一次刷新交换机以来接口上接收到的 65 至 127 字节帧的数量。

**Frames of 128 to 255 Bytes (128 至 255 字节帧)** — 显示自上一次刷新交换机以来接口上接收到的 128 至 255 字节帧的数量。

**Frames of 256 to 511 Bytes (256 至 511 字节帧)** — 显示自上一次刷新交换机以来接口上接收到的 256 至 511 字节帧的数量。

**Frames of 512 to 1023 Bytes (512 至 1023 字节帧)** — 显示自上一次刷新交换机以来接口上接收到的 512 至 1023 字节帧的数量。



**Frames of 1024 to 1518 Bytes (1024 至 1518 字节帧)** — 显示自上一次刷新交换机以来接口上接收到的 1024 至 1518 字节帧的数量。

## 查看接口统计数据

□□□ 打开 **RMON Statistics Group (RMON 统计数据组)** 页面。

□□□ 在 **Interface (接口)** 字段中选择一个接口。

系统将显示所选接口的统计数据。

## 使用 CLI 命令查看 RMON 统计数据

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- RMON 命令

## RMON 历史记录控制统计数据

**RMON History Control (RMON 历史记录控制数据)** 页面用于维护每个端口的统计数据历史记录。对于每个接口（物理端口或端口信道），可以定义使用的存储区数以及每个存储区快照之间的时间间隔。

要显示此页面，请在树视图中单击 **Statistics/RMON (统计数据/RMON) ® RMON ® History Control (历史记录控制)**。

图 9-8. RMON 历史记录控制



**RMON History Control (RMON 历史记录控制)** 页面包含以下字段：

**History Entry (历史记录条目)** — 在 **RMON History Control Table (RMON 历史记录控制表)** 中选择条目号。

**Source Interface (源接口)** — 指定获取历史记录样例的接口。

**Owner (0-20 characters) (物主 [0 至 20 个字符])** — 指明请求 RMON 信息的 RMON 站点或用户。

**Max No. of Samples to Keep (1-65535) (要保存的最大样例数 [1-65535])** — 设置此接口的历史记录存储区数。

**Current No. of Samples in List** (列表中的当前样例数) — 显示当前获取的样例数。

**Sampling Interval (1-3600)** (取样间隔 [1-3600]) — 设置从端口取样的频率。可能的值为 1 至 3600 秒。默认值为 1800 秒 (30 分钟)。

**Remove** (删除) — 选中后, 将删除显示的 **RMON History Control Table** (RMON 历史记录控制表) 条目。

## 添加历史记录控制条目

□□□ 打开 **RMON History Control** (RMON 历史记录控制) 页面。

□□□ 单击 **Add** (添加)。

系统将显示 **Add History Entry** (添加历史记录条目) 页面。

图 9-9. 添加历史记录条目

□□□ 填写此页面上的字段并单击 **Apply Changes** (应用更改)。

条目将被添加至 **RMON History Control Table** (RMON 历史记录控制表)。

## 显示 RMON 历史记录控制表

□□□ 打开 **RMON History Control** (RMON 历史记录控制) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **RMON History Control Table** (RMON 历史记录控制表)。

图 9-10. RMON 历史记录控制表

History Entry No.	Source Interface	Sampling Interval	Current Number of Samples	Owner	Remove
1	1/g1	1800	10		<input type="checkbox"/>

## 删除历史记录控制表条目

□□□ 打开 **RMON History Control** (RMON 历史记录控制) 页面。

□□□ 选中要删除的历史记录条目行中的 **Remove** (删除) 复选框。

□□□ 单击 **Apply Changes** (应用更改)。



系统将删除表条目并更新设备。

## 使用 CLI 命令查看 RMON 历史记录控制

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- RMON 命令

## RMON 历史记录表

RMON History Table (RMON 历史记录表) 页面用于显示特定接口的网络取样统计信息。每个表条目表示在单个取样过程中编译的所有计数器值。

要显示 **RMON History Table (RMON 历史记录表)** 页面，请在树视图中单击 **Statistics/RMON (统计数据/RMON) ® RMON ® History Table (历史记录表)**。

图 9-11. RMON 历史记录表

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb path is Statistics/RMON > RMON > RMON History Table. The interface includes a navigation tree on the left with 'History Table' selected. The main content area displays the RMON History Table configuration and a data table.

**RMON History Table Configuration:**

History Entry No.	3
Owner	RTP
Source Interface	1/g1
Max No. of Samples to Keep	15
Sampling Interval	45 (sec)

**RMON History Table Data:**

Sample No.	Drop Events	Received Bytes (Octets)	Received Packets	Broadcast Packets	Multicast Packets	CRC Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Utilization
1	0	48595	210	42	13	0	0	0	0	0	0	0

**RMON History Table (RMON 历史记录表)** 页面包含以下字段：

**History Entry No.** (历史记录条目号) — 选择要在 **RMON History Table (RMON 历史记录表)** 中显示的历史记录条目号。

**Owner** (物主) — 显示 RMON 统计数据组的物主名称 (如果有)。

**Source Interface** (源接口) — 表示正在其上收集统计数据的接口或 LAG。

**Max No. of Samples to Keep** (要保存的最大样例数) — 确定历史记录表中每个历史记录条目号的列表长度。

**Sampling Interval** (取样间隔) — 以秒为单位设置连续取样之间的间隔。

**Sample No.** (样例号) — 指明表中信息反映的特定样例。

**Drop Events** (丢弃事件数) — 显示由于缺少资源而导致端口丢弃信息包的事件总数。请注意，此数量并不一定是丢弃的信息包数；它只是检测到这种情况的次数。

**Received Bytes (Octets)** (接收的字节数 [八位位组]) — 显示在网络中接收到的八位位组数据 (包括坏信息包中的数据) 的总数量，其中不包括成帧位，但包括帧检查顺序 (FCS) 八位位组。

**Received Packets** (接收的信息包) — 显示在取样间隔期间接收到的信息包的总数 (包括坏信息包、广播信息包和多点传送信息包)。

**Broadcast Packets** (广播信息包) — 显示接收到的已传送到广播地址的良好信息包的总数。请注意，该数量不包括多点传送信息包。

**Multicast Packets** (多点传送信息包) — 显示接收到的已传送到多点传送地址的良好信息包的总数。请注意，此数量不包括传送到广播地址的

信息包。

**CRC Align Errors** (CRC 校准错误) — 显示接收到的长度在 64 和 1518 个八位位组之间 (含这两个数字) 的信息包的总数, 但是这些信息包包含具有整数个八位位组的坏 FCS (FCS 错误) 或具有非整数个八位位组的坏 FCS (校准错误)。

**Undersize Packets** (超小信息包) — 显示接收到的长度小于 64 个八位位组 (不包括成帧位, 但包括 FCS 八位位组) 和其它格式良好的信息包的总数。

**Oversize Packets** (超大信息包) — 显示接收到的长度大于 1518 个八位位组 (不包括成帧位, 但包括 FCS 八位位组) 和其它格式良好的信息包的总数。

**Fragments** (碎片) — 显示接收到的长度小于 64 个八位位组 (不包括成帧位, 但包括 FCS 八位位组) 的信息包的总数, 但是这些信息包包含具有整数个八位位组的坏 FCS (FCS 错误) 或具有非整数个八位位组的坏 FCS (校准错误)。

**Jabbers** (无用信息) — 显示接收到的长度大于 1518 个八位位组 (不包括成帧位, 但包括 FCS 八位位组) 的信息包的总数, 并且这些信息包包含具有整数个八位位组的坏帧检查顺序 (FCS) (FCS 错误) 或具有非整数个八位位组的坏 FCS (校准错误)。

**Collisions** (冲突) — 显示在此以太网段上存在的冲突的最佳估计总数。

**Utilization** (使用) — 估计在取样会话期间接口上的主物理层网络使用情况。该值用百分比表示。

## 查看特定历史记录条目的统计数据

□□□ 打开 **RMON History Table** (RMON 历史记录表) 页面。

□□□ 在 **History Entry No.** (历史记录条目号) 字段中选择一个条目。

随后屏幕上将显示条目的统计数据。

## 使用 CLI 命令查看 RMON 历史记录控制

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

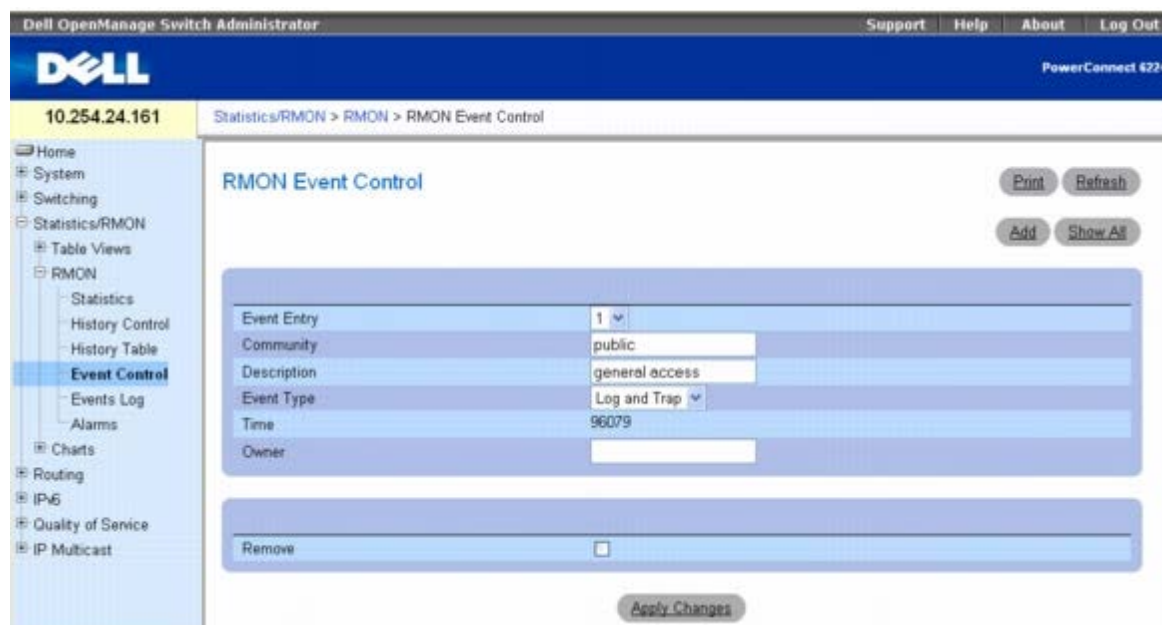
- RMON 命令

## RMON 事件控制

**RMON Events Control** (RMON 事件控制) 页面用于定义 RMON 事件。当超过特定 RMON 计数器的阈值时, RMON 报警将使用这些事件强制执行某种操作。事件信息可以存储在日志中, 也可以作为陷阱发送到陷阱接收设备。

要显示此页面, 请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **RMON** ® **Event Control** (事件控制)。

图 9-12. RMON 事件控制



**RMON Event Control** (**RMON** 事件控制) 页面包含以下字段:

**Event Entry** (事件条目) — 选择事件。

**Community** (团体) — 指定事件所属的团体。

**Description** (说明) — 说明用户定义的事件。

**Event Type** (事件类型) — 选择事件类型。可能的值包括:

**Log** (日志) — 事件类型为日志条目。

**Trap** (陷阱) — 事件类型为陷阱。

**Log and Trap** (日志和陷阱) — 事件类型既是日志条目, 又是陷阱。

**None** (无) — 无事件。

**Time** (时间) — 显示事件发生的时间。

**Owner** (物主) — 列出定义事件的交换机或用户。

**Remove** (删除) — 选中后, 将从事件表中删除事件。

## 添加 RMON 事件

□□□ 打开 **RMON Event Control** (**RMON** 事件控制) 页面。

□□□ 单击 **Add** (添加) 。

系统将显示 **Add an Event Entry** (添加事件条目) 页面。

图 9-13. 添加事件条目

Field	Value
Event Entry	2
Community	
Description	
Event Type	None
Owner	

□□□ 填写本页面中的字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统会将事件添加到 **RMON Event Table** (RMON 事件表) 中并更新设备。

## 修改 RMON 事件

□□□ 打开 **RMON Event Control** (RMON 事件控制) 页面。

□□□ 单击 **Show All** (全部显示) 以显示 **Event Control Table** (事件控制表) 页面。

□□□ 选中要更改的事件条目的 **Edit** (编辑) 复选框。

□□□ 根据需要修改该页面上的字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将修改 **RMON Events Table** (RMON 事件表) 条目并更新设备。

## 显示 RMON 事件控制表

□□□ 打开 **RMON Event Control** (RMON 事件控制) 页面。

□□□ 单击 **Show All** (全部显示)。

系统将显示 **Event Control Table** (事件控制表) 页面。

图 9-14. 事件控制表

Event Entry	Community	Description	Event Type	Time	Owner	Remove	Edit
-------------	-----------	-------------	------------	------	-------	--------	------

## 删除 RMON 事件条目

□□□ 打开 **RMON Event Control** (RMON 事件控制) 页面。

□□□ 从 **Event Entry** (事件条目) 字段的下拉式菜单中选择要删除的事件, 然后选中 **Remove** (删除)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将删除表条目并更新设备。

## 使用 CLI 命令定义交换机事件

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

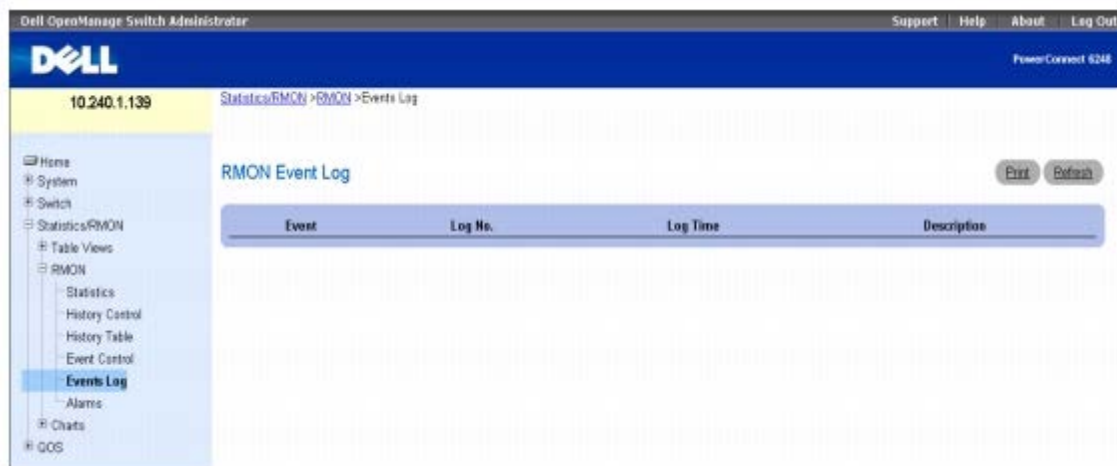
- RMON 命令

## RMON 事件日志

**RMON Event Log** (RMON 事件日志) 页面用于显示 RMON 事件的列表。

要显示此页面，请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **RMON** ® **Events Log** (事件日志)。

图 9-15. RMON 事件日志



**RMON Event Log** (RMON 事件日志) 页面包含以下字段：

**Event** (事件) — 显示 RMON 事件日志条目号。

**Log No.** (日志编号) — 显示日志编号。

**Log Time** (日志时间) — 显示输入日志条目的时间。

**Description** (说明) — 说明日志条目。

## 使用 CLI 命令定义交换机事件

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

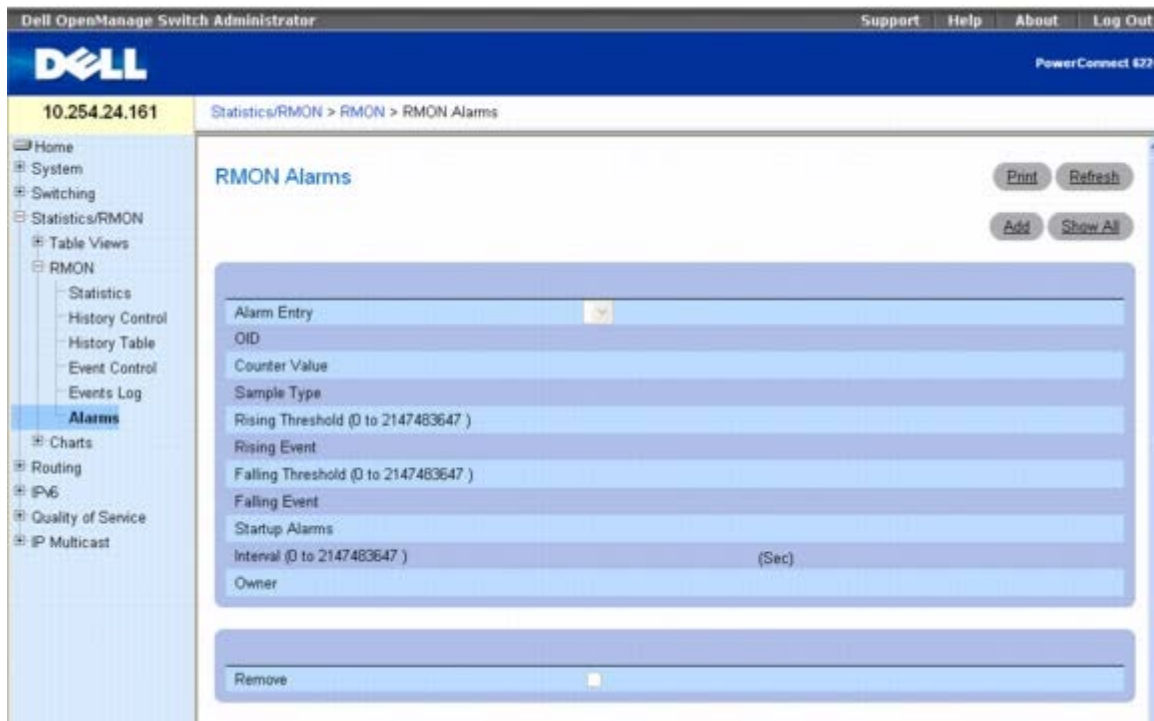
- RMON 命令

## RMON 警报

**RMON Alarms** (RMON 警报) 页面用于设置网络警报。当超过经配置的 RMON 计数器的某些阈值时，就会发出警报。警报将触发事件发生。事件可以作为 RMON 事件组的一部分来配置。有关事件的详细信息，请参阅 [RMON 事件日志](#)。

要显示此页面，请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **RMON** ® **Alarms** (警报)。

图 9-16. RMON 警报



**RMON Alarms (RMON 警报)** 页面包含以下字段:

**Alarm Entry** (警报条目) — 从下拉式菜单中选择特定警报。

**OID** — 指定对象标识符。

**Counter Value** (计数器值) — 显示经过计数的所选事件的数目。

**Sample Type** (样例类型) — 显示所选变量的取样方法, 并将其值与阈值进行比较。可能的字段值包括:

**Delta** (增量) — 从当前值中减去上一次取样值。将差值与阈值进行比较。

**Absolute** (绝对) — 在取样间隔结束时将值直接与阈值进行比较。这是默认设置。

**Rising Threshold (0-2147483647)** (上升阈值 [0-2147483647]) — 指定触发上升阈值警报的上升计数器值。上升阈值显示在图形栏顶部。每个被监测的变量均被指定一种颜色。默认值为 100。

**Rising Event** (上升事件) — 显示报告警报的机制, 包括日志、陷阱或二者的结合。如果选择日志, 则在交换机或管理系统中均无保存机制。但是, 如果不重置交换机, 事件将保留在交换机日志表中。如果选择陷阱, 则将通过陷阱机制生成和报告 SNMP 陷阱。可以使用同一机制保存陷阱。

**Falling Threshold (0-2147483647)** (下降阈值 [0-2147483647]) — 指定触发下降阈值警报的下降计数器值。下降阈值以图形形式显示在图形栏顶部。每个被监测的变量均被指定一种颜色。默认值为 20。

**Falling Event** (下降事件) — 显示报告警报的机制, 包括日志、陷阱或二者的结合。如果选择日志, 则在交换机或管理系统中均无保存机制。但是, 如果不重置交换机, 事件将保留在交换机日志表中。如果选择陷阱, 则将通过陷阱机制生成和报告 SNMP 陷阱。可以使用同一机制保存陷阱。

**Startup Alarms** (启动警报) — 显示事件的类型。选项包括上升、上升-下降和下降。

**Interval (0-2147483647)** (间隔 [0-2147483647]) — 显示警报的间隔时间。默认值为 100。

**Owner** (物主) — 显示定义警报的交换机或用户。

**Remove** (删除) — 选中后, 将删除 RMON 警报。

## 添加警报表条目

打开 **RMON Alarms (RMON 警报)** 页面。

**Add**

单击 [Add](#) (添加)。

系统将显示 **Add an Alarm Entry** (添加警报条目) 页面。

图 9-17. 添加警报条目

□□□ 根据需要填写本页面中的字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将添加 RMON 警报并更新设备。

## 显示警报表

□□□ 打开 **RMON Alarms** (RMON 警报) 页面。

□□□ 单击 **Show All** (全部显示)。

此时会显示 **RMON Alarms Table** (RMON 警报表) 的左侧部分。

图 9-18. RMON 警报表

Alarm Entry	OID	Counter Value	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event
1	1	0	Absolute	100	1	20	2

□□□ 单击屏幕底部的右箭头可查看表的右侧部分。

## 删除一个警报表条目

□□□ 打开 **RMON Alarms** (RMON 警报) 页面。

□□□ 在 **Alarm Entry** (警报条目) 下拉式菜单中选择一个条目。

□□□ 选中 **Remove** (删除) 复选框, 然后单击 **Apply Changes** (应用更改)。

系统将删除条目并更新设备。

## 删除多个警报表条目



□□□ 打开 **RMON Alarms** (**RMON 警报**) 页面。

□□□ 单击 **Show All** (全部显示)。

此时会显示 **RMON Alarms Table** (**RMON 警报表**)。

□□□ 对于每个要删除的警报条目, 选中 **Remove** (删除)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将删除条目并更新设备。

## 使用 **CLI** 命令定义交换机警报

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- **RMON 命令**

---

## 图表

**Chart** (图表) 菜单页面包含一些网页的链接, 使用这些网页可以在图形上绘制统计数据。要显示 **Charts** (图表) 菜单页面, 请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **Charts** (图表)。 **Charts** (图表) 菜单页面包含以下功能的链接:

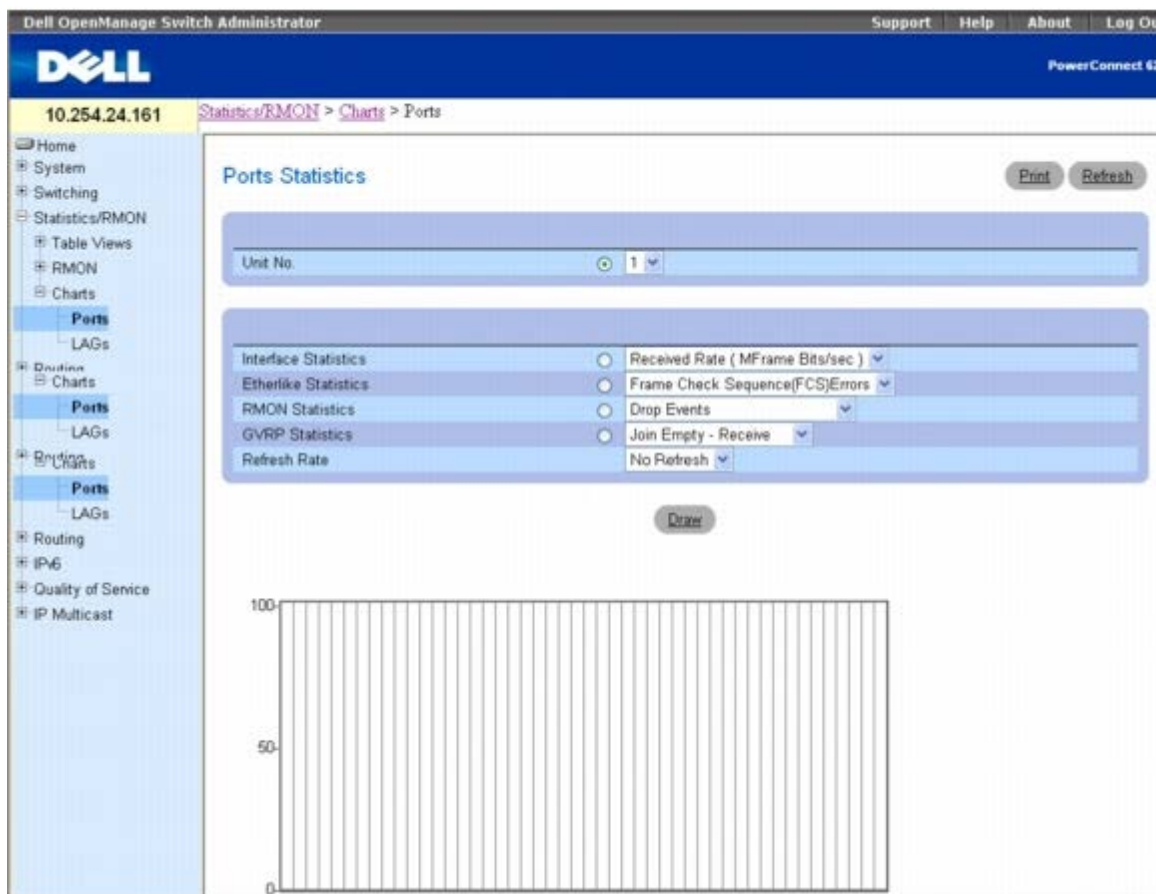
- [端口统计数据](#)
- [LAG 统计数据](#)

## 端口统计数据

**Ports Statistics** (端口统计数据) 页面用于在图形上绘制与端口相关的统计数据。

要显示此页面, 请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **Charts** (图表) ® **Ports** (端口)。

图 9-19. 端口统计数据



**Ports Statistics** (端口统计数据) 页面包含以下字段:

**Unit No.** (单元编号) — 选择要显示的端口。

**Interface Statistics** (接口统计数据) — 单击时选择接口统计数据, 并且从下拉式菜单中指定要绘制的接口统计数据的类型。默认值为 Received Rate (接收的速率) (MFrame 位/秒)。

**Etherlike Statistics** (以太网类统计数据) — 单击时选择以太网类统计数据, 并且从下拉式菜单中指定要绘制的以太网类统计数据的类型。默认值为 Frame Check Sequence (FCS) Errors (帧检查顺序 [FCS] 错误)。

**RMON Statistics** (RMON 统计数据) — 单击时选择 RMON 统计数据, 并且从下拉式菜单中指定要绘制的 RMON 统计数据的类型。默认值为 Drop Events (丢弃事件数)。

**GVRP Statistics** (GVRP 统计数据) — 单击时选择 GVRP 统计数据, 并且从下拉式菜单中指定要绘制的 GVRP 统计数据的类型。默认值为 Join Empty - Receive (加入空 - 接收)。

**Refresh Rate** (刷新率) — 选择刷新统计数据之前经过的时间。可能的字段值包括: No Refresh (无刷新)、15、30 和 60 秒。默认刷新率为 No Refresh (无刷新)。

## 显示端口统计数据

- 打开 **Ports Statistics** (端口统计数据) 页面。
- 选择要为其绘制统计数据图表的端口。
- 单击与要绘制统计数据相关联的单选按钮。
- 从相关下拉式菜单中选择统计数据的类型。
- 从 **Refresh Rate** (刷新率) 下拉式菜单中选择所需的刷新率。
- 单击 **Draw** (绘图)。

系统将在图形上绘制选定的统计数据。

## 使用 CLI 命令查看端口统计数据

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

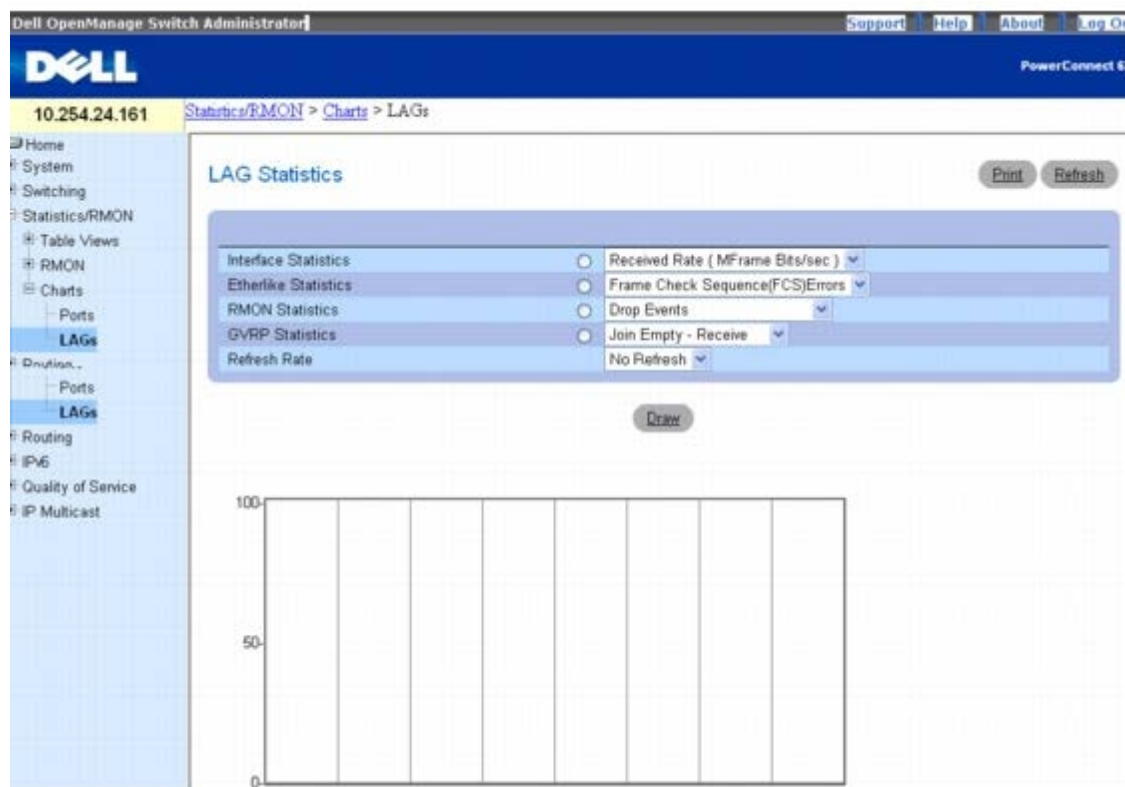
- 系统管理命令
- RMON 命令
- GVRP 命令

## LAG 统计数据

**LAG Statistics** (**LAG 统计数据**) 页面用于在图形上绘制与 LAG 相关的统计数据。

要显示此页面，请在树视图中单击 **Statistics/RMON** (统计数据/RMON) ® **Charts** (图表) ® **LAGs (LAG)**。

图 9-20. LAG 统计数据



**LAG Statistics** (**LAG 统计数据**) 页面包含以下字段：

**Interface Statistics** (接口统计数据) — 单击时选择接口统计数据，并且从下拉式菜单中指定要绘制的接口统计数据的类型。默认值为 Received Rate (接收的速率)。

**Etherlike Statistics** (以太网类统计数据) — 单击时选择以太网类统计数据，并且从下拉式菜单中指定要绘制的以太网类统计数据的类型。默认值为 Frame Check Sequence Errors (帧检查顺序错误)。

**RMON Statistics** (RMON 统计数据) — 单击时选择 RMON 统计数据，并且从下拉式菜单中指定要绘制的 RMON 统计数据的类型。默认值为 Drop Events (丢弃事件数)。

**GVRP Statistics** (GVRP 统计数据) — 单击时选择 GVRP 统计数据，并且从下拉式菜单中指定要绘制的 GVRP 统计数据的类型。默认值为

Join Empty - Receive (加入空 - 接收)。

**Refresh Rate** (刷新率) — 选择刷新统计数据之前经过的时间。可能的字段值包括: No Refresh (无刷新)、15、30 和 60 秒。默认刷新率为 15 秒。

## 显示 LAG 统计数据

□□□ 打开 **LAG Statistics** (LAG 统计数据) 页面。

□□□ 单击与要绘制统计数据相关联的单选按钮。

□□□ 从相关下拉式菜单中选择统计数据的类型。

□□□ 从 **Refresh Rate** (刷新率) 下拉式菜单中选择所需的刷新率。

□□□ 单击 **Draw** (绘图)。

系统将在图形上绘制定选的统计数据。

## 使用 CLI 命令查看 LAG 统计数据

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- 系统管理命令
- RMON 命令
- GVRP 命令

---

[返回目录页面](#)

[返回目录页面](#)

# 配置路由

## Dell™ PowerConnect™ 6200 系列用户指南

- [ARP](#)
- [IP](#)
- [OSPF](#)
- [BOOTP/DHCP 中继代理](#)
- [RIP](#)
- [路由器发现](#)
- [路由器](#)
- [VLAN 路由](#)
- [VRRP](#)
- [通道](#)
- [回送](#)


6200 系列支持 IP 路由功能。**Routing**（路由）菜单页面用于配置 VLAN 路由。

当信息包进入交换机时，将会检查目的地 MAC 地址，看其是否与配置的任何路由接口匹配。如果匹配，该设备会搜索主机表以查找匹配的目的地 IP 地址。如果找到匹配项，信息包即会路由至该主机。如果没有匹配项，交换机就会对目的地 IP 地址执行最长的前缀匹配。如果找到匹配项，信息包将路由至下一跃距。如果没有匹配项，则信息包路由至默认路由中指定的下一跃距。如果没有配置默认路由，信息包将传递到 6200 系列软件进行适当的处理。

路由表可以包含由管理员静态增加或者通过 RIP 或 OSPF 动态增加的条目。主机表可以包含由管理员静态增加或通过 ARP 动态增加的条目。

**Routing**（路由）菜单页面包含以下功能的链接：

- [ARP](#)
- [IP](#)
- [OSPF](#)
- [BOOTP/DHCP 中继代理](#)
- [RIP](#)
- [路由器发现](#)
- [路由器](#)
- [VLAN 路由](#)
- [VRRP](#)
- [通道](#)
- [回送](#)

 注：CLI 命令并不适用于所有路由页面。

## ARP

6200 系列使用 ARP 协议将第 2 层 MAC 地址与第 3 层 IPv4 地址相关联。此外，管理员可以通过静态方式向 ARP 表添加条目。

ARP 是 Internet 协议 (IP) 的必要部分，用于将 IP 地址转换为介质访问控制 (MAC) 地址，由局域网 (LAN)（如以太网）定义。如果需要发送 IP 信息包的站点与目的地不在同一个子网中，则站点必须知道 IP 目的地或下一跃距路由器的 MAC 地址。这可通过广播 ARP 请求信息包来实现，预定接收者将通过单点传送包含其 MAC 地址的 ARP 回复来响应。在获取 MAC 地址后，便可将其添加至 IP 信息包的第 2 层标头的目的地地址字段。

ARP 高速缓存是网络上每个站点本地维护的表格。该高速缓存的构建或维护没有特定的要求，但至少需要包含通过处理 ARP 协议包所获取的信

息。对于以太网，该信息由 0x0806 EtherType 字段表示。站点通过检查 ARP 包有效载荷字段中的源信息来获取 ARP 高速缓存条目，这对 ARP 请求或响应都一样。因此，当 ARP 请求被广播到 LAN 段或虚拟 LAN (VLAN) 上的所有站点时，每个接收者都可以在其各自的 ARP 高速缓存中存储发送方的 IP 和 MAC 地址。ARP 响应是单点传送，通常只能由请求方看见。请求方会在其 ARP 高速缓存中存储发送方信息。在 ARP 高速缓存中，新信息总是替换原有的信息。

ARP 高速缓存可以支持 896 个条目，但用户可将其配置为任何介于 256 和 896 之间的值。当多个网络接口由一台设备支持（例如路由器）时，可以所有接口都使用同一 ARP 高速缓存，也可以每个接口使用各自的缓存。如果每个接口的网络地址并非唯一，则后一种方法非常有用，但在分配以太网 MAC 地址时，需采用单一 ARP 高速缓存。

如果 IP 地址原来与某一特定 MAC 地址关联，但后来使用其它 MAC 地址找到了该 IP 地址，表示设备在网络中发生移动；如果找不到该 IP 地址，则表示设备可能已从网络中消失（即已经被重新配置、断开连接或关闭电源）。为避免在 ARP 高速缓存中形成旧信息，必须以网络中出现的新信息自动更新 ARP 高速缓存中的条目，定期刷新条目以确定地址是否仍然存在，或者在过期间隔（通常在配置中指定）后将未识别为 ARP 包发送方的条目从高速缓存中删除。

ARP 菜单页面包含用于配置和显示 ARP 详细信息的网页的链接。要显示此页面，请在树视图中单击 **Routing**（路由）® **ARP**。在此菜单页面中可以访问以下网页：

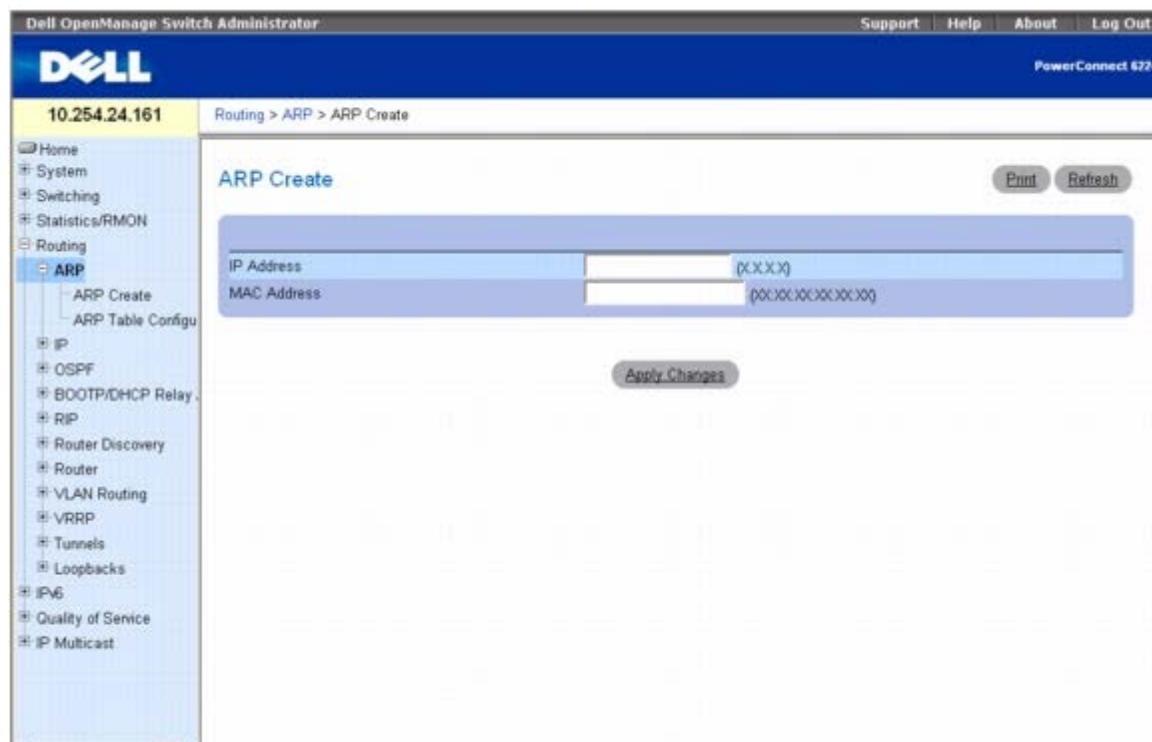
- [ARP 创建](#)
- [ARP 表配置](#)

## ARP 创建

**ARP Create**（ARP 创建）页面用于添加地址解析协议表条目。

要显示此页面，请在树视图中单击 **Routing**（路由）® **ARP** ® **ARP Create**（ARP 创建）。

图 10-1. ARP 创建



**ARP Create**（ARP 创建）页面包含以下字段：

**IP Address**（IP 地址）— 输入要添加的 IP 地址。它必须是子网上连接到交换机一个现有路由接口的设备的 IP 地址。

**MAC Address**（MAC 地址）— 设备的单点传送 MAC 地址。地址由六个两位数的十六进制数字组成，之间以冒号分隔，例如 00:06:29:32:81:40。

## 添加条目到 ARP 表

□□□ 打开 **ARP Create**（ARP 创建）页面。

□□□ 指定要关联的地址。

□□□ 单击 **Apply Changes**（应用更改）。

这些地址即存储在 ARP 高速缓存中。

## 使用 CLI 添加条目到 ARP 表

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

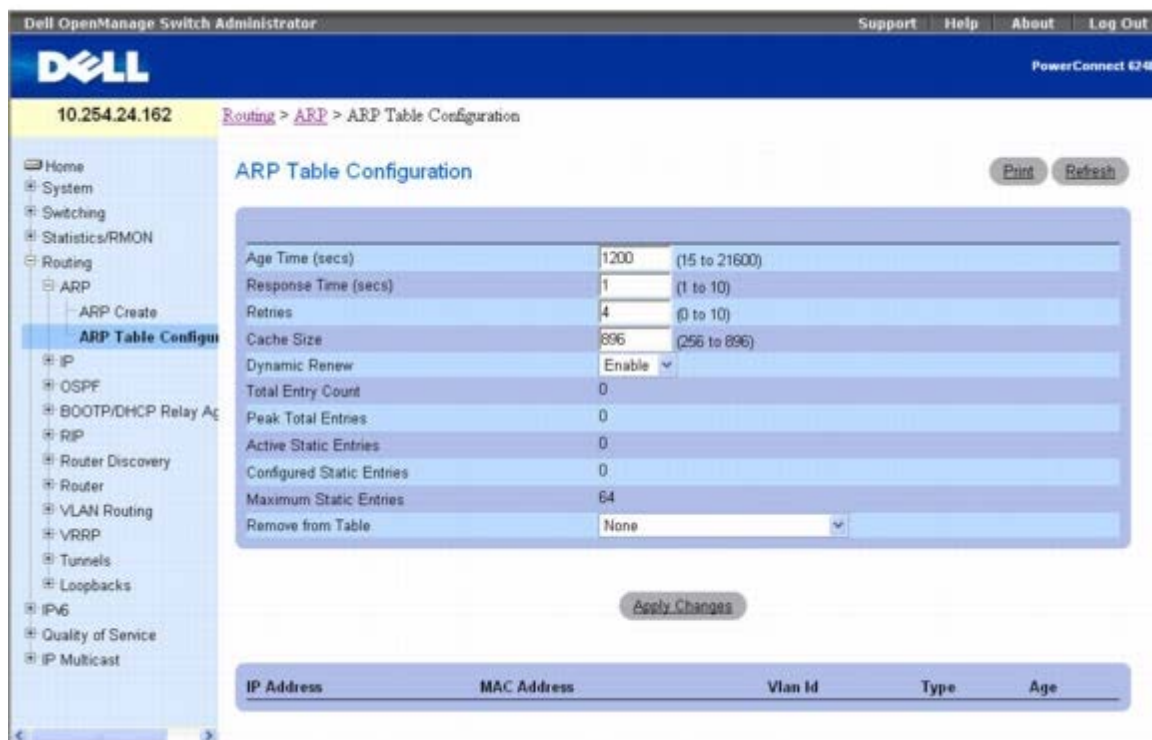
- ARP 命令

## ARP 表配置

此页面用于更改地址解析协议表的配置参数，也可以用于显示该表的内容。

要显示此页面，请在树视图中单击 **Routing**（路由）⑥ **ARP** ⑥ **ARP Table Configuration**（ARP 表配置）。

图 10-2. ARP 表配置



ARP Table Configuration（ARP 表配置）页面包括以下字段：

**Age Time (secs)**（存在时间【秒】）— 输入您希望交换机用于 ARP 条目过期时间的值。必须输入有效的整数，表示 ARP 条目过期所需的秒数。此字段的范围是 15 到 21600 秒。Age Time（存在时间）的默认值是 1200 秒。

**Response (secs)**（响应时间【秒】）— 输入您希望交换机用于 ARP 响应超时的值。必须输入有效的整数，表示交换机等待响应 ARP 请求的秒数。此字段的范围是 1 到 10 秒。Response Time（响应时间）的默认值是 1 秒。

**Retries**（重试次数）— 输入一个整数以指定重试 ARP 请求的最大次数。此字段的范围是 0 到 10，Retries（重试次数）的默认值为 4。



**Cache Size**（高速缓存大小）— 输入一个整数以指定 ARP 高速缓存可以容纳的最大条目数。此字段的范围是 256 到 896，Cache Size（高速缓存大小）的默认值为 896。

**Dynamic Renew**（动态更新）— 控制 ARP 组件是否自动更新动态类型的 ARP 过期条目。默认设置为 ENABLED（启用）。

**Total Entry Count**（总条目数）— ARP 表中的条目总数。

**Peak Total Entries**（最大条目数）— Total Entry Count（总条目数）可以达到的最大值。只 ARP 表的高速缓存大小值有改变，此计数器就会重新开始计数。

**Active Static Entries**（活动的静态条目）— ARP 表中活动静态条目的总数。

**Configured Static Entries**（配置的静态条目）— ARP 表中配置的静态条目总数。

**Maximum Static Entries**（最大静态条目数）— 可以定义的最大静态条目数。

**Remove from Table**（从表中删除）— 用于从 ARP 表中删除特定条目。下列选项用于指定要删除的 ARP 条目类型：

- All Dynamic Entries（所有动态条目）
- All Dynamic and Gateway Entries（所有动态和网关条目）
- Specific Dynamic Gateway Entry（特定的动态网关条目）
- Specific Static Entry（特定的静态条目）

ARP 表显示于页面底部，包括以下字段：

**IP Address**（IP 地址）— 子网上连接到交换机一个路由接口的设备的 IP 地址。

**MAC Address**（MAC 地址）— 设备的单点传送 MAC 地址。地址由六个两位数的十六进制数字组成，之间以冒号分隔，例如 00:06:29:32:81:40。

**VLAN ID** — 与 ARP 条目关联的路由接口。

**Type**（类型）— ARP 条目的类型。

**Age**（时间）— 条目自上次刷新后已在 ARP 表中存在的时间。格式为小时:分钟:秒钟。

## 配置 ARP 表

打开 **ARP Table Configuration**（ARP 表配置）页面。

按需要更改参数。

单击 **Apply Changes**（应用更改）。

将会保存更改并更新 ARP 表。

## 使用 CLI 命令配置 ARP 表

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- ARP 命令

---

## IP

IP 菜单页面包含用于配置和显示 IP 路由数据的网页的链接。要显示此页面，请在树视图中单击 **Routing**（路由）® **IP**。在此菜单页面中可以访问以下网页：

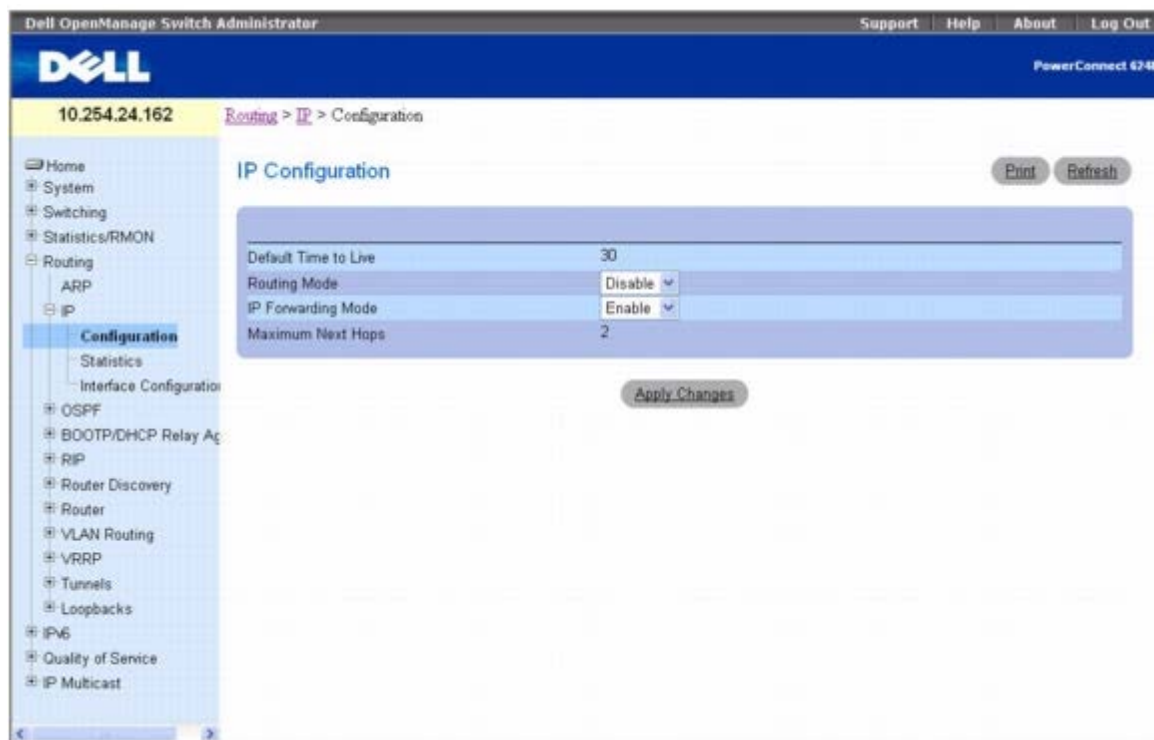
- [IP 配置](#)
- [IP 统计数据](#)
- [IP 接口配置](#)

## IP 配置

**IP Configuration** (IP 配置) 页面用于配置与接口相对的交换机的参数。

要显示此页面，请在树视图中单击 **Routing** (路由) @ **IP** @ **Configuration** (配置)。

图 10-3. IP 配置



**IP Configuration** (IP 配置) 页面包含以下字段：

**Default Time to Live** (默认生存时间) — 如果 TTL 值不是由传输层协议提供，则此值将插入交换机所生成的数据包 IP 标头的 Time-To-Live (生存时间) 字段，成为默认值。

**Routing Mode** (路由模式) — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用)。必须先为交换机启用路由，然后才可通过任何接口进行路由。路由也可以按 VLAN 接口启用或禁用。默认值为 **Disable** (禁用)。

**IP Forwarding Mode** (IP 转发模式) — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用)。这将启用或禁用 IP 帧的转发。默认值为 **Enable** (启用)。

**Maximum Next Hops** (下一跃距最大数) — 交换机支持的最大跃距数。这是一个静态常量。

### 配置 IP 路由参数

□□□ 打开 **IP Configuration** (IP 配置) 页面。

□□□ 按需要更改参数。

□□□ 单击 **Apply Changes** (应用更改)。

将会保存更改并更新路由参数。

## 使用 CLI 命令配置 IP 路由参数

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- IP 路由命令
- VLAN 命令

## IP 统计数据

**IP Statistics** (**IP 统计数据**) 页面中报告的统计数据如 RFC 1213 所示。

要显示此页面，请在树视图中单击 **Routing** (路由) @ **IP** @ **Statistics** (统计数据)。

图 10-4. IP 统计数据

IP Statistics	
IpnReceives	520
IpnHdrErrors	0
IpnAddrErrors	0
IpnForwDatagrams	0
IpnUnknownProtos	0
IpnDiscards	0
IpnDelivers	479
IpnOutRequests	699
IpnOutDiscards	0
IpnOutNoRoutes	0
IpnReasmTimeout	0
IpnReasmReqds	0
IpnReasmOKs	0
IpnReasmFails	0
IpnFragOKs	0
IpnFragFails	0
IpnFragCreates	0
IpnRoutingDiscards	0
IcmplnMsgs	0
IcmplnErrors	0

**IP Statistics** (**IP 统计数据**) 页面包含以下字段：

**IpnReceives** — 从接口收到的输入数据包总数，包括错误收到的数据包。

**IpnHdrErrors** — 因 IP 标头错误而被丢弃的输入数据包数目，这些错误包括校验和错误、版本号不匹配、其它格式错误、超过生存时间、在处理其 IP 选项时发现的错误等。

**IpnAddrErrors** — 由于 IP 标头的目的地字段 IP 地址不是以该实体为有效的接收地址而丢弃的输入数据包数目。此计数包括无效的地址（例如 0.0.0.0）和其类别不受支持的地址（例如类别 E）。对于因未使用 IP 网关而无法转发数据包的实体，此计数器包括由于目的地地址不是本地地址而丢弃的数据包。

**IpnForwDatagrams** — 此实体不是数据包最终 IP 目的地的输入数据包数目，因此实体尝试找到可将数据包转发到最终目的地的路线。在非 IP 网关的实体中，此计数器只包括通过此实体源路由，并且源路由选项处理成功的数据包。

**IpnUnknownProtos** — 以本地为接收地址、已成功接收但由于协议未知或不受支持而丢弃的数据包数目。

**IpnDiscards** — 没有遇到妨碍其继续处理的问题而被丢弃（例如由于缺乏缓冲区空间）的输入 IP 数据包数目。请注意，此计数器不包括在等

待重组时丢弃的任何数据包。

**IpInDelivers** — 已成功传递到 IP 用户协议（包括 ICMP）的输入数据包总数。

**IpOutRequests** — 本地 IP 用户协议（包括 ICMP）提供给请求 IP 以进行传输的 IP 数据包总数。请注意，此计数器不包括计入 ipForwDatagrams 的任何数据包。

**IpOutDiscards** — 没有遇到妨碍其到达目的地的问题而被丢弃（例如由于缺乏缓冲区空间）的输出 IP 数据包数目。请注意，此计数器将包括已计入 ipForwDatagrams 的符合此（自主）丢弃标准的数据包。

**IpOutNoRoutes** — 由于找不到将其传送至目的地的路线而被丢弃的 IP 数据包数目。请注意，此计数器包括已计入 ipForwDatagrams 中的符合此“无路线”标准的数据包，还包括主机因其所有默认网关均已关闭而无法路由的任何数据包。

**IpReasmTimeout** — 收到的碎片在该实体内等待重组时被保留的最大秒数。

**IpReasmReqds** — 所收到的需要在该实体内重组的 IP 碎片数目。

**IpReasmOKs** — 已成功重组的 IP 数据包数目。

**IpReasmFails** — IP 重组算法检测到的失败（由于超时、错误等原因）数目。请注意，这不一定等于被丢弃的 IP 碎片数目，因为有些算法在收到碎片时即将其合并，从而无法记录碎片数目。

**IpFragOKs** — 已在该实体内成功分割的 IP 数据包数目。

**IpFragFails** — 由于必须在该实体内分割但又无法分割（例如因为它们设置了 Don't Fragment [不要分割] 的标志）而被丢弃的 IP 数据包数目。

**IpFragCreates** — 由于在该实体内进行分割而生成的 IP 数据包碎片数目。

**IpRoutingDiscards** — 选择为即使有效也要丢弃的路由条目数。丢弃这种条目的一个可能原因是为其它路由条目释放缓冲区空间。

**IcmpInMsgs** — 实体收到的 ICMP 信息数目。请注意，此计数器包括已计入 icmpInErrors 的所有信息。

**IcmpInErrors** — 实体已收到但被确定为具有 ICMP 特定错误（ICMP 校验和错误、长度错误等）的 ICMP 信息数目。

**IcmpInDestUnreachs** — 收到的 ICMP Destination Unreachable（ICMP 无法到达目的地）信息数目。

**IcmpInTimeExcds** — 收到的 ICMP Time Exceeded（ICMP 超过时间）信息数目。

**IcmpInParmProbs** — 收到的 ICMP Parameter Problem（ICMP 参数问题）信息数目。

**IcmpInSrcQuenchs** — 收到的 ICMP Source Quench（ICMP 来源结束）信息数目。

**IcmpInRedirects** — 收到的 ICMP Redirect（ICMP 重定向）信息数目。

**IcmpInEchos** — 收到的 ICMP Echo（ICMP 回音）（请求）信息数目。

**IcmpInEchoReps** — 收到的 ICMP Echo Reply（ICMP 回音答复）信息数目。

**IcmpInTimestamps** — 收到的 ICMP Timestamp（时间戳）（请求）信息数目。

**IcmpInTimestampReps** — 收到的 ICMP Timestamp Reply（ICMP 时间戳答复）信息数目。

**IcmpInAddrMasks** — 收到的 ICMP Address Mask Request（ICMP 地址掩码请求）信息数目。

**IcmpInAddrMaskReps** — 收到的 ICMP Address Mask Reply（ICMP 地址掩码答复）信息数目。

**IcmpOutMsgs** — 该实体试图发送的 ICMP 信息总数。请注意，此计数器包括计入 icmpOutErrors 的所有数目。

**IcmpOutErrors** — 该实体因为在 ICMP 内发现问题（例如缺少缓冲区）而未发送的 ICMP 信息数目。此值不包括在 ICMP 层外部发现的错误，例如 IP 无法路由结果数据包。在某些应用中，可能不存在形成此计数器值的错误类型。

**IcmpOutDestUnreachs** — 发送的 ICMP Destination Unreachable（ICMP 无法到达目的地）信息数目。

**IcmpOutTimeExcds** — 发送的 ICMP Time Exceeded（ICMP 超过时间）信息数目。

**IcmpOutParmProbs** — 发送的 ICMP Parameter Problem（ICMP 参数问题）信息数目。

**IcmpOutSrcQuenchs** — 发送的 ICMP Source Quench（ICMP 来源结束）信息数目。

**IcmpOutRedirects** — 发送的 ICMP Redirect（ICMP 重定向）信息数目。对于主机，此对象始终为零，因为主机不发送重定向信息。

**IcmpOutEchos** — 已发送的 ICMP Echo (ICMP 回音) (请求) 信息数目。

**IcmpOutEchoReps** — 已发送的 ICMP Echo Reply (ICMP 回音答复) 信息数目。

**IcmpOutTimestamps** — ICMP Timestamp (时间戳) (请求) 信息数目。

**IcmpOutTimestampReps** — 发送的 ICMP Timestamp Reply (ICMP 时间戳答复) 信息数目。

**IcmpOutAddrMasks** — 发送的 ICMP Address Mask Request (ICMP 地址掩码请求) 信息数目。

**IcmpOutAddrMaskReps** — 发送的 ICMP Address Mask Reply (ICMP 地址掩码答复) 信息数目。

## 刷新 IP 统计数据

□□□ 打开 **IP Statistics** (IP 统计数据) 页面。

□□□ 单击 **Refresh** (刷新)。

屏幕将显示交换机中数据的目前状态。

## 使用 CLI 命令显示 IP 统计数据

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

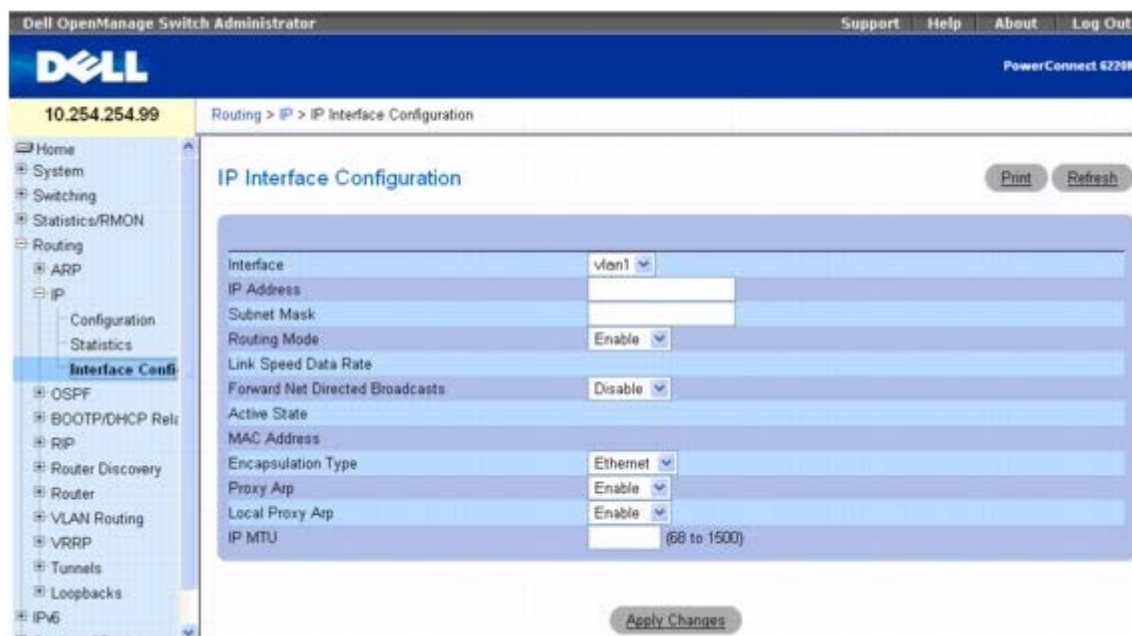
- IP 路由命令

## IP 接口配置

**IP Interface Configuration** (IP 接口配置) 页面用于更新此交换机的 IP 接口数据。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **IP** ® **Interface Configuration** (接口配置)。

图 10-5. IP 接口配置



**IP Interface Configuration** (IP 接口配置) 页面包含以下字段：

**Interface** (接口) — 从下拉式菜单中选择要配置的接口。此下拉式菜单包含在 **Switching** (交换) ® **VLAN** ® **VLAN Membership** (VLAN 成员关系) ® **Add** (添加) 页面中创建的回送接口和 VLAN。

**IP Address** (IP 地址) — 输入接口的 IP 地址。

**Subnet Mask** (子网掩码) — 输入接口的子网掩码。这也称作子网/网络掩码，定义接口的 IP 地址中用于标识所连网络的部分。

**Routing Mode** (路由模式) — 设置启用或禁用接口的路由。默认值为 **Enable** (启用)。

**Link Speed Data Rate** (链路速度数据速率) — 一个表示指定接口的物理链接数据速率的整数。此数据仅适用于物理接口，以兆位/秒 (Mbps) 为单位。

**Forward Net Directed Broadcasts** (转发网络传送的广播) — 选择如何处理网络传送的广播信息包。如果从下拉式菜单中选择 **Enable** (启用)，将会转发网络传送的广播。如果选择 **Disable** (禁用)，则会将其丢弃。默认值为 **Disable** (禁用)。

**Active State** (活动状态) — 指定接口的状态为 **Active** (活动) 或 **Inactive** (非活动)。如果链路良好并且处于转发状态，则认为接口为活动状态。

**MAC Address** (MAC 地址) — 指定接口的固化物理地址。地址由六个两位数的十六进制数字组成，之间以冒号分隔，例如 00:06:29:32:81:40。此值适用于物理接口。对于逻辑接口，例如 VLAN 路由接口，该字段将显示系统 MAC 地址。

**Encapsulation Type** (封装类型) — 从下拉式菜单中为指定接口所发送的信息包选择链路层封装类型。可能的值为 **Ethernet** (以太网) 和 **SNAP**。默认值为 **Ethernet** (以太网)。

**Proxy ARP** (代理 ARP) — 从下拉式菜单中选择对指定的接口禁用还是启用代理 ARP。

**Local Proxy ARP** (本地代理 ARP) — 从下拉式菜单中选择对指定的接口禁用还是启用本地代理 ARP。

**IP MTU** — 指定接口上发送的 IP 信息包的最大传输单位 (MTU)。有效范围是 68 至 1500。默认值为 1500。

## 修改 IP 接口

打开 **IP Interface Configuration** (IP 接口配置) 页面。

按需要更改值。

单击 **Apply Changes** (应用更改)。

将会保存更改并更新 IP 接口。

## IP 接口配置 CLI 命令

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- IP 寻址命令
- IP 路由命令
- ARP 命令

---

## OSPF

开放最短路径优先 (Open Shortest Path First, OSPF) 路由协议是一个内部网关协议 (IGP)。每个 OSPF 路由器都将创建域中所有路由器和网络的最短路径树。路由信息定期通过链路状态更新信息包传播，并且在网络拓扑发生变动时也会传播。此信息接收、处理和存储于各个路由器的 OSPF 数据库。数据库交换中心所必需的信息部分是与路由器关联的接口数目和 IP 地址。OSPF 将次 IP 地址视为连接到路由器的末节网络。因此，即使在 OSPF 路由域中公布了这些网络，也不能在次地址上建立邻居。另请注意，所有次 IP 地址都必须与主 IP 地址位于同一个区域中，这样才会被 OSPF 公布。在 6200 系列实施中一直是这样，因为区域配置是以接口（而非网络）为基础。

**OSPF** 菜单页面包含用于配置和显示 OSPF 参数和数据的网页的链接。要显示此页面，请在树视图中单击 **Routing** (路由) ® **OSPF**。在此菜



单页面中可以访问以下网页：

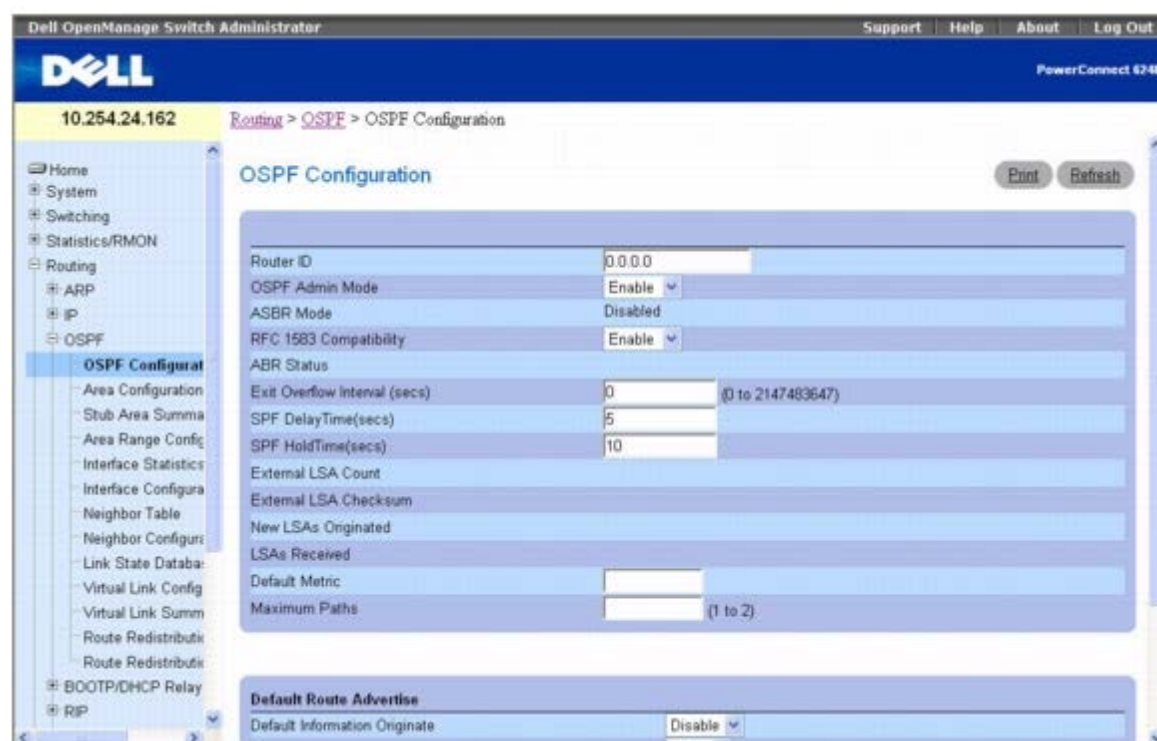
- [OSPF 配置](#)
- [区域配置](#)
- [末节区域摘要](#)
- [区域范围配置](#)
- [接口统计数据](#)
- [接口配置](#)
- [邻居列表](#)
- [邻居配置](#)
- [链路状态数据库](#)
- [虚拟链路配置](#)
- [虚拟链路摘要](#)
- [路由重新分配配置](#)
- [路由重新分配摘要](#)

## OSPF 配置

**OSPF Configuration** (OSPF 配置) 页面用于在路由器上启用 OSPF 和配置相关的 OSPF 设置。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **OSPF** ® **Configuration** (配置)。

图 10-6. OSPF 配置



**OSPF Configuration** (OSPF 配置) 页面包含以下字段：



**Router ID (路由器 ID)** — 用于唯一标识自治系统 (AS) 中路由器的 32 位点分十进制格式整数。如果要更改路由器 ID，必须先禁用 OSPF。在设置新的路由器 ID 之后，必须重新启用 OSPF 才能使更改生效。默认值为 0.0.0.0，但这并非有效的路由器 ID。

**OSPF Admin Mode (OSPF 管理模式)** — 从下拉式菜单中选择 Enable (启用) 或 Disable (禁用)。如果选择 Enable (启用)，将会为交换机激活 OSPF。默认值为 Disable (禁用)。必须先配置 Router ID (路由器 ID)，然后才可操作 OSPF。

 **注：**在路由器上启用 OSPF 之后，OSPF 将一直保持启用状态，直到路由器重置。

**ASBR Mode (ASBR 模式)** — 反映 ASBR 模式是 Enabled (启用) 还是 Disabled (禁用)。Enable (启用) 表示路由器是一种自治系统边界路由器。路由器若被配置为重新分发从其它协议获取的路线，将自动变成 ASBR。

**RFC 1583 Compatibility (RFC 1583 兼容性)** — 从下拉式菜单中选择 Enable (启用) 或 Disable (禁用)，以指定在从公布同一目的地的多个 AS-external-LSA 中选择时所用的优先级规则。如果选择 Enable (启用)，优先级规则是 RFC 1583 定义的规则。如果选择 Disable (禁用)，则优先级规则是 OSPF-2 标准 (RFC 2328) 的第 16.4.1 条中定义的规则，当同一目的地的 AS-external-LSA 产生于不同的区域时，这些规则将会阻止路由循环。默认值为 Enable (启用)。为防止路由循环，应选择 Disable (禁用)，但根据 RFC 2328，仅当路由域中的所有 OSPF 路由器都可以操作时才选择此选项。

**ABR Status (ABR 状态)** — 此字段的值为 Enabled (启用) 或 Disabled (禁用)。Enabled (启用) 表示路由器是区域边界路由器。Disabled (禁用) 表示路由器不是区域边界路由器。

**Exit Overflow Interval (sec) (退出溢出间隔 [秒])** — 路由器进入溢出状态后，在尝试离开溢出状态之前应等待的秒数。这可使路由器重新产生非默认 AS-external-LSA。如果输入 0，路由器将不会离开溢出状态，直到重新启动。范围是 0 至 2147483647 秒。

**SPF DelayTime (secs) (SPF 延迟时间 [秒])** — 输入秒数，延迟时间 (秒) 是 OSPF 收到拓扑更改和开始 SPF 计算之间的间隔。它可以是 0 到 65535 的整数。默认时间为 5 秒。0 表示没有延迟；也就是说，SPF 计算会立即开始。

**SPF HoldTime(secs) (SPF 保留时间 [秒])** — 两次连续 SPF 计算之间的最短时间 (秒)。可以从 0 到 65535 的整数。默认值为 10 秒。0 表示没有延迟；也就是说，两次 SPF 计算都可以完成，完成一次后立即进行另一次。

**External LSA Count (外部 LSA 计数)** — 链路状态数据库中的外部 (LS 类型 5) LSA (链路状态公布) 数目。

**External LSA Checksum (外部 LSA 校验和)** — 链路状态数据库中外部 LSA (链路状态公布) 的 LS 校验和总和。此总和用于确定路由器的链路状态数据库是否有变动，并用于比较两个路由器的链路状态数据库。此值为十六进制。

**New LSAs Originated (产生的新 LSA)** — 在任何指定的 OSPF 区域中，一个路由器会产生几个 LSA。每个路由器都会产生一个路由器-LSA。如果路由器还是任何区域网络的指定路由器，则会为这些网络产生网络-LSA。此值表示该路由器产生的 LSA 数目。

**LSAs Received (收到的 LSA)** — 已收到并被确定为新实例的 LSA (链路状态公布) 数目。此数字不包括更新的自我产生的 LSA 实例。

**Default Metric (默认跃点)** — 为重新分配的路由设置默认跃点数。若已设置，此字段将显示默认跃点数；若尚未设置，则留空。有效值为 1 到 16777214。

**Maximum Paths (最大路径数)** — 配置 OSPF 可以报告给指定目的地的最大路径数。有效值为 1 到 2。

默认路由公布

**Default Information Originate (产生默认信息)** — 启用或禁用默认路由公布。

**Always (始终)** — 当设置为 True (真) 时设置路由器公布 0.0.0.0/0.0.0.0。

**Metric (跃点)** — 指定默认路由的跃点。有效值为 1 到 16777214。

**Metric Type (跃点类型)** — 设置默认路由的跃点类型。选项有 External Type 1 (外部类型 1) 和 External Type 2 (外部类型 2)。默认值为 External Type 2 (外部类型 2)。

## 修改 OSPF 配置

打开 **OSPF Configuration (OSPF 配置)** 页面。

按需要更改值。

单击 **Apply Changes (应用更改)**。

将会保存更改并更新 OSPF 接口。

## OSPF 配置 CLI 命令

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- OSPF 命令

## 区域配置

当通过 **Routing**（路由）® **OSPF**® **Interface Configuration**（接口配置）在接口上启用 OSPF 之后，即可使用 **OSPF Area Configuration**（OSPF 区域配置）页面创建末节区域配置和 NSSA。要显示此网页，至少必须有一个路由器启用 OSPF。

要显示此页面，请在树视图中单击 **Routing**（路由）® **OSPF**® **Area Configuration**（区域配置）。

图 10-7. OSPF 区域配置



**OSPF Area Configuration**（OSPF 区域配置）页面包含以下字段：

**Area**（区域）— 从下拉式菜单中选择要显示的区域。在选择区域之后，**Stub Area Information**（末节区域信息）中的字段将会显示。

**Area ID**（区域 ID）— OSPF 区域。Area ID（区域 ID）是一个 32 位点分十进制格式整数，用于唯一标识路由器接口所连接到的区域。

**External Routing**（外部路由）— 区域的路由器功能定义，包括 AS-external-LSA 是否多路发送至整个区域。如果区域是末节区域，则可以使用这些选项配置外部路由功能，否则唯一的选项便是 **Import External LSAs**（导入外部 LSA）。

**SPF Runs**（SPF 运行数）— 使用此区域的链路状态数据库计算区域内部路由表的次数。此操作通常使用 Dijkstra 算法来完成。

**Area Border Router Count**（区域边界路由器计数）— 此区域内可到达的区域边界路由器的总数。初始值为零，在每个 SPF 通道中都要计算此值。

**Area LSA Count**（区域 LSA 计数）— 此区域链路状态数据库中的链路状态公布总数，不包括 AS 外部 LSA。

**Area LSA Checksum**（区域 LSA 校验和）— 在此区域的链路状态数据库中包含的链路状态公布的 LS 校验和的 32 位未签名总和。此总和不包括外部（LS 类型 5）链路状态公布。此总和用于确定路由器的链路状态数据库是否有变动，并用于比较两个路由器的链路状态数据库。此值为十六进制。

**Stub Area Information**（末节区域信息）

**Import Summary LSAs**（导入摘要 LSA）— 从下拉式菜单中选择 **Enable**（启用）或 **Disable**（禁用）。如果选择 **Enable**（启用），摘要 LSA 将导入末节区域。

**Metric Value**（跃点值）— 为公布到末节区域的默认路由输入要应用的跃点值。有效值的范围是 1 到 16,777,215。

**Metric Type**（跃点类型）— 选择在 **Metric Value**（跃点值）字段中指定的跃点类型。

**Translator Role**（转换器角色）— 将 NSSA 转换器角色配置为始终/候选。

**Translator Stability Interval**（转换器稳定性间隔）— 为选择的 NSSA 配置转换器稳定性间隔。

**No-Redistribute Mode**（不重新分配模式）— 为选择的 NSSA 配置路由重新分配。

**Translator State**（转换器状态）— 显示转换器的当前状态。

## 配置 OSPF 区域

□□□ 打开 **OSPF Area Configuration**（OSPF 区域配置）页面。

□□□ 指定要配置的区域。

□□□ 按需要指定其余字段的值。

□□□ 单击 **Apply Changes**（应用更改）。

OSPF 即被定义和配置。

## 显示 OSPF 区域配置

□□□ 打开 **OSPF Area Configuration**（OSPF 区域配置）页面。

□□□ 从下拉式菜单中选择要显示的 OSPF 区域。

将显示该区域的 OSPF 区域配置。

## 删除 OSPF 区域配置

请采用以下步骤删除 NSSA 配置或末节区域配置。

□□□ 打开 **OSPF Area Configuration**（OSPF 区域配置）页面。

□□□ 从下拉式菜单中选择要删除的 OSPF 区域配置。

该配置即会显示。

□□□ 单击 **Delete**（删除）。

该 OSPF 区域配置即被删除。

## 配置 OSPF 区域 CLI 命令

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- OSPF 命令

## 末节区域摘要

**OSPF Stub Area Summary**（OSPF 末节区域摘要）页面用于显示 OSPF 末节区域详细信息。

要显示此页面，请在树视图中单击 **Routing**（路由）® **OSPF** ® **Stub Area Summary**（末节区域摘要）。

图 10-8. OSPF 末节区域摘要



**OSPF Stub Area Summary**（OSPF 末节区域摘要）页面包含以下字段：

**Area ID**（区域 ID）— 末节区域的区域 ID。

**Type of Service**（服务类型）— 与末节跃点相关的服务类型。交换机只支持 Normal（正常）。

**Metric Value**（跃点值）— 显示配置的跃点值。

**Metric Type**（跃点类型）— 适用于末节区域的有效跃点类型有：

- **OSPF Metric**（OSPF 跃点）— 常规 OSPF 跃点
- **Comparable Cost**（相当的成本）— 与 OSPF 跃点相当的 External Type 1（外部类型 1）跃点
- **Non-comparable Cost**（不相当的成本）— 被认为大于 OSPF 跃点成本的 External Type 2（外部类型 2）跃点

**Import Summary LSAs**（导入摘要 LSA）— 是否启用或禁用导入摘要 LSA。

## 显示 OSPF 末节区域 CLI 命令

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- OSPF 命令

## 区域范围配置

**OSPF Area Range Configuration (OSPF 区域范围配置)** 页面用于配置和显示指定 NSSA 的区域范围。

要显示此页面，请在树视图中单击 **Routing (路由)** ⑥ **OSPF** ⑥ **Area Range Configuration (区域范围配置)**。

图 10-9. OSPF 区域范围配置



**OSPF Area Range Configuration (OSPF 区域范围配置)** 页面包含以下字段：

**Area ID (区域 ID)** — 从下拉式菜单中选择要显示的区域。

**IP Address (IP 地址)** — 为选择的区域输入地址范围的 IP 地址。

**Subnet Mask (子网掩码)** — 为选择的区域输入地址范围的子网掩码。

**LSDB Type (LSDB 类型)** — 选择与指定区域和地址范围关联的链路公布的类型。默认类型为 Network Summary (网络摘要)。

**Advertisement (公布)** — 从下拉式菜单中选择 Enable (启用) 或 Disable (禁用)。如果选择 Enable (启用)，地址范围将通过网络摘要 LSA 在区域外部公布。默认值为 Enable (启用)。

**Add (添加)** — 如果要添加区域范围，请选中 Add (添加) 复选框。

**OSPF 区域范围表**

**Area ID (区域 ID)** — 显示 OSPF 区域。

**IP Address (IP 地址)** — 显示区域地址范围的 IP 地址。

**Subnet Mask (子网掩码)** — 显示区域地址范围的子网掩码。

**LSDB Type (LSDB 类型)** — 显示地址范围和区域的链路公布类型。

**Advertisement (公布)** — 显示地址范围和区域的公布模式。

**Remove (删除)** — 删除指定的区域条目。

## 定义 OSPF 区域范围

□□□ 打开 **OSPF Area Range Configuration (OSPF 区域范围配置)** 页面。

□□□ 输入 Area ID (区域 ID)、IP Address (IP 地址)、Subnet Mask (子网掩码)、LSDB Type (LSDB 类型) 和

Advertisement（公布）。

单击 **Add**（添加）复选框。

单击 **Apply Changes**（应用更改）。

OSPF 区域范围即被定义和配置。所有已配置的 OSPF 区域范围显示在 **OSPF Area Range Configuration**（OSPF 区域范围配置）页面上的表格中。

## 删除 OSPF 区域范围配置

打开 **OSPF Area Range Configuration**（OSPF 区域范围配置）页面。

选中要删除的 **Area ID**（区域 ID）行中的 **Remove**（删除）复选框。

单击 **Apply Changes**（应用更改）。

该地址范围将从区域配置中删除。

## OSPF 区域配置 CLI 命令

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- OSPF 命令

## 接口统计数据

**OSPF Interface Statistics**（OSPF 接口统计数据）页面用于显示所选接口的统计数据。信息仅在启用了 OSPF 时才会显示。

要显示此页面，请在树视图中单击 **Routing**（路由）® **OSPF** ® **Interface Statistics**（接口统计数据）。

图 10-10. OSPF 接口统计数据





**OSPF Interface Statistics (OSPF 接口统计数据)** 页面包含以下字段：

**Interface (接口)** — 从下拉式菜单中选择要显示其数据的接口。

**OSPF Area ID (OSPF 区域 ID)** — 选定路由器接口所属的 OSPF 区域。OSPF Area ID (OSPF 区域 ID) 是一个 32 位点分十进制格式整数，用于唯一标识接口所连接到的区域。

**Area Border Router Count (区域边界路由器计数)** — 此区域内可到达的区域边界路由器的总数。初始值为零，在每个 SPF 通道中都要计算此值。

**AS Border Router Count (AS 边界路由器计数)** — 此区域内可到达的自治系统边界路由器的总数。初始值为零，在每个 SPF 通道中都要计算此值。

**Area LSA Count (区域 LSA 计数)** — 此区域链路状态数据库中的链路状态公布总数，不包括 AS 外部 LSA。

**IP Address (IP 地址)** — 接口的 IP 地址。

**Interface Events (接口事件)** — 指定 OSPF 接口更改其状态或发生错误的次数。

**Virtual Events (虚拟事件)** — 此虚拟链路中发生状态更改或出错的次数。

**Neighbor Events (邻居事件)** — 此邻居关系更改其状态的次数或错误发生的次数。

**External LSA Count (外部 LSA 计数)** — 链路状态数据库中的外部 (LS 类型 5) 链路状态公布的数目。

## 显示 OSPF 接口统计数据

□□□ 打开 **OSPF Interface Statistics (OSPF 接口统计数据)** 页面。

□□□ 从下拉式菜单中选择要显示其数据的接口。

该接口的统计数据将会显示。

## 使用 CLI 命令显示 OSPF 接口统计数据

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：



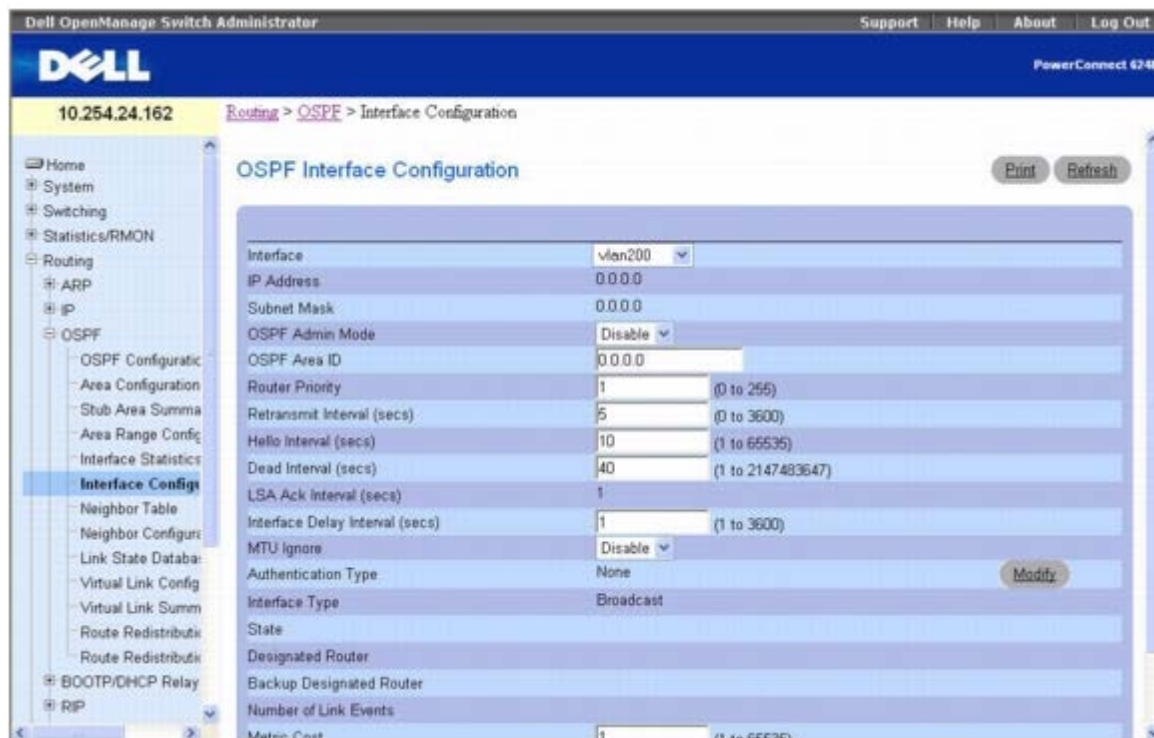
- OSPF 命令

## 接口配置

**OSPF Interface Configuration** (OSPF 接口配置) 页面用于配置 OSPF 接口。

要显示此页面，请在树视图中单击 **Routing** (路由) @ **OSPF** @ **Interface Configuration** (接口配置)。

图 10-11. OSPF 接口配置



**OSPF Interface Configuration** (OSPF 接口配置) 页面包含以下字段：

**Interface** (接口) — 从下拉式菜单中选择要显示数据或配置的接口。

**IP Address** (IP 地址) — 显示 VLAN 接口的地址。

**Subnet Mask** (子网掩码) — 显示 VLAN 接口的子网掩码。

**OSPF Admin Mode** (OSPF 管理模式) — 可以从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用)。默认值为 **Disable** (禁用)。配置 OSPF 参数时可以不启用 OSPF 管理模式，但只有启用管理模式后才会生效。仅当启用 **Admin Mode** (管理模式) 后，才会显示以下信息：**State** (状态)、**Designated Router** (指定路由器)、**Backup Designated Router** (备份指定路由器)、**Number of Link Events** (链路事件数)、**LSA Ack Interval** (LSA 确认间隔) 和 **Metric Cost** (跃点成本)。为使 OSPF 发挥全部功能，必须通过 **IP Interface Configuration** (IP 接口配置) 页面输入有效的 **IP Address** (IP 地址) 和 **Subnet Mask** (子网掩码)。

 **注：** 在路由器上启用 OSPF 之后，OSPF 将一直保持启用状态，直到路由器重置。

**OSPF Area ID** (OSPF 区域 ID) — 输入一个点分十进制格式的 32 位整数，用于唯一标识路由器接口所连接的 OSPF 区域。如果分配不存在的区域 ID，则使用默认值创建区域。

**Router Priority** (路由器优先级) — 输入所选接口的 OSPF 优先级。接口优先级的指定值范围是 0 至 255 间的整数。默认值为 1，路由器的优先级最高。值 0 表示路由器不适合成为此网络上的指定路由器。

**Retransmit Interval (secs)** (重新发送间隔 [秒]) — 输入指定接口的 OSPF 重新发送间隔。这是指属于此路由器接口的邻居的链路状态公布的间隔秒数。当重新发送数据库说明和链路状态请求信息包时，也可以使用此值。有效值的范围是 0 至 3600 秒 (1 小时)。默认值为 5 秒。

**Hello Interval (secs)** (问候间隔 [秒]) — 以秒为单位输入指定接口的 OSPF 问候间隔。对于连接到网络中的所有路由器而言，此参数必须相同。有效值范围是 1 到 65,535。默认值是 10 秒。

**Dead Interval (secs)** (无响应间隔 [秒]) — 以秒为单位输入指定接口的 OSPF 无响应间隔。这是指路由器等待接收来自邻居路由器的问候信息包的时间。在此时间之后，如果仍未收到问候信息包，将认定邻居路由器已关闭。对于连接到网络中的所有路由器而言，此参数必须相同。此值应乘以问候间隔（例如 4）。有效值范围是 1 到 2147483647。默认值是 40。

**LSA Ack Interval (LSA 确认间隔)** — LSA 确认信息包发送之间的秒数间隔，其值必须小于 Retransmit Interval（重新发送间隔）。

**Interface Delay Interval (secs)** (接口延迟间隔 [秒]) — 输入指定接口的 OSPF 传输延迟。这是指在选定接口传输链路状态更新信息包估计所需的秒数。有效值的范围是 1 至 3600 秒（1 小时）。默认值为 1 秒。

**MTU Ignore (MTU 忽略)** — 对收到的信息包禁用 OSPF MTU 不匹配检测。默认值为 Disable（禁用）。

**Authentication Type** (验证类型) — 要选择除 None（无）以外的验证类型，请单击 **Modify**（修改）按钮，以打开一个新网页。在该网页中，可以从下拉式菜单中选择验证类型。可能的值包括：

- **None**（无）— 这是初始的接口状态。如果从第二个屏幕的下拉式菜单中选择此选项并单击 **Apply Changes**（应用更改），将会返回到第一个屏幕，而不运行任何验证协议。
- **Simple**（简单）— 如果选择 Simple（简单），系统将提示您输入验证密钥。网络上发送的所有信息包的 OSPF 标头中都含有该密钥的明文形式。网络中的所有路由器必须使用同一密钥配置。
- **Encrypt**（加密）— 如果选择 Encrypt（加密），系统将提示您输入验证密钥和验证 ID。加密使用 MD5 Message-Digest 算法。网络中的所有路由器必须使用同一密钥和 ID 配置。

**Interface Type** (接口类型) — OSPF 接口类型始终为广播。

**State** (状态) — 选定路由器接口的当前状态。可能的值包括：

- **Down**（关闭）— 这是初始的接口状态。在此状态下，较低层的协议已指明此接口无法使用。在此状态下，系统将接口参数设置为初始值。所有接口计时器均被禁用，并且没有任何邻居与接口相关联。
- **Loopback**（回送）— 在此状态下，路由器的网络接口以硬件或软件回送。接口不能用于常规数据通信。但是，仍然有可能需要通过向接口发送 ICMP ping，或者通过位错误检测等操作，获取此接口质量的相关信息。因此，IP 信息包仍要求能够发送到处于 Loopback（回送）状态的接口。为此，这些接口在路由器 LSA 中公布为单一主机路由，其目的地为 IP 接口地址。
- **Waiting**（等待）— 路由器正在尝试通过监测接收到的问候信息包来确定网络（备份）指定路由器的身份。在路由器过渡到等待状态以外的状态之前，路由器无法成为 Backup Designated Router（备份指定路由器）和 Designated Router（指定路由器）。这样能阻止对（备份）指定路由器进行不必要的更改。
- **Designated Router**（指定路由器）— 此路由器本身是所连网络上的指定路由器，并且与连接到网络上的所有其他路由器均建立邻接关系。该路由器还必须为网络节点生成一个网络 LSA。网络 LSA 包含连接到网络上的所有路由器（包括指定路由器本身）的链路。
- **Backup Designated Router**（备份指定路由器）— 此路由器本身是所连网络上的备份指定路由器。如果现有的指定路由器发生故障，则该路由器会升级为指定路由器。该路由器与连接到网络上的所有其他路由器均建立邻接关系。在多路发送过程中，备份指定路由器执行的功能与指定路由器稍有不同。
- **Other Designated Router**（其它指定路由器）— 接口连接到广播或 NBMA 网络，在该网络上已将其他路由器选择为指定路由器或备份指定路由器。路由器尝试与指定路由器和备份指定路由器形成邻接关系。

State (状态) 仅在启用 OSPF 管理模式后才会显示。

**Designated Router** (指定路由器) — 此网络中的指定路由器向公布路由器显示的标识。此处按路由器 ID 来标识指定路由器。值 0.0.0.0 表示不存在指定路由器。此字段仅在启用 OSPF 管理模式后才会显示。

**Backup Designated Router** (备份指定路由器) — 此网络中的备份指定路由器向公布路由器显示的标识。此处按路由器 ID 来标识备份指定路由器。如果不存在备份指定路由器，则将该值设置为 0.0.0.0。此字段仅在启用 OSPF 管理模式后才会显示。

**Number of Link Events** (链路事件数) — 这是指定 OSPF 接口更改其状态的次数。此字段仅在启用 OSPF 管理模式后才会显示。

**Metric Cost** (跃点成本) — 输入此接口上的 TOS (服务类型) 成本值。跃点成本的范围为 1 到 65,535。仅当 OSPF 在接口上初始化之后，Metric Cost (跃点成本) 才可配置/显示。

## 配置 OSPF 接口配置

□□□ 打开 **OSPF Interface Configuration**（OSPF 接口配置）页面。

□□□ 指定要配置的接口。

□□□ 按需要指定其余字段的值。

□□□ 单击 **Apply Changes**（应用更改）。

OSPF 接口即被配置。

## 显示 OSPF 接口配置

□□□ 打开 **OSPF Interface Configuration**（OSPF 接口配置）页面。

□□□ 从下拉式菜单中选择要显示其数据的 VLAN 接口。

此接口的配置数据将会显示。

## 使用 CLI 命令配置 OSPF 接口

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- OSPF 命令

## 邻居列表

**OSPF Neighbor Table**（OSPF 邻居列表）页面用于显示 OSPF 邻居表列表。指定某个特定邻居 ID 时，将给定邻居的详细信息。以下信息仅在启用了 OSPF 时才会显示。

要显示此页面，请在树视图中单击 **Routing**（路由）® **OSPF** ® **Neighbor Table**（邻居列表）。

图 10-12. OSPF 邻居列表



**OSPF Neighbor Table** (OSPF 邻居列表) 页面包含以下字段：

**Interface** (接口) — 从下拉式菜单中选择要显示其数据的接口。

**Router ID** (路由器 ID) — 点分十进制格式的 32 位整数，用于表示邻居接口。

**IP Address** (IP 地址) — 邻居路由器与所连网络之间接口的 IP 地址。当协议信息包沿此邻接路由器单点传送时，它将用作目的地 IP 地址。如果邻居路由器被选作指定路由器，它还在路由器 LSA 中用作所连网络的 Link ID (链路 ID)。从邻居收到问候信息包时，可以获取邻居 IP 地址。对于虚拟链路，邻居 IP 地址在路由表创建过程中获取。

**Neighbor Interface Index** (邻居接口索引) — 标识邻居接口索引的接口。

## 使用 CLI 命令显示 OSPF 邻居列表

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- OSPF 命令

## 邻居配置

**OSPF Neighbor Configuration** (OSPF 邻居配置) 页面用于显示所选邻居 ID 的 OSPF 邻居配置。指定特定邻居 ID 后，将显示邻居的详细信息。以下信息仅在启用 OSPF 并且该接口有邻居时才会显示。IP 地址就是邻居的 IP 地址。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **OSPF** ® **Neighbor Configuration** (邻居配置)。

图 10-13. OSPF 邻居配置



**OSPF Neighbor Configuration (OSPF 邻居配置)** 页面包含以下字段：

**Interface (接口)** — 从下拉式菜单中选择在其中启用路由的 VLAN 接口。

**Neighbor IP Address (邻居 IP 地址)** — 选择要显示其数据的邻居 IP 地址。

**Router ID (路由器 ID)** — 点分十进制格式的 32 位整数，用于标识邻居路由器。

**Options (选项)** — 邻居所支持的可选 OSPF 功能。OSPF Options (选项) 字段存在于 OSPF 问候信息包、数据库说明信息包以及所有链路状态公布中。Options (选项) 字段可让 OSPF 路由器支持 (或不支持) 可选功能，以及让 OSPF 路由器与其它 OSPF 路由器沟通其功能。通过此机制，在一个 OSPF 路由域中可以混合不同功能的路由器。Options (选项) 值是一个位图，表示邻居的功能。

**Router Priority (路由器优先级)** — 显示指定邻居的 OSPF 优先级。邻居优先级是一个介于 0 至 255 的整数。值 0 表示路由器无法成为此网络上的指定路由器。

**State (状态)** — 邻居可以具有以下状态：

- **Down (故障)** — 这是邻居对话的初始状态。它表示最近没有收到邻居的信息。在 NBMA 网络上，虽然频率减少，但是仍会将问候信息包发送到故障邻居。
- **Attempt (尝试)** — 此状态仅适用于连接到 NBMA 网络的邻居。它表示最近没有从邻居接收到任何信息，但是应更加努力地与邻居取得联系。通过按照问候间隔发送邻居问候信息包来实现此操作。
- **Init** — 此状态表示最近已收到来自邻居的问候信息包，但是，尚未与邻居建立双向通信（即路由器本身没有出现在邻居的问候信息包中）。此状态（或更高状态）的所有邻居均列在从关联接口发送的问候信息包中。
- **2-Way (双向)** — 在此状态下，两个路由器之间的通信是双向的。双向通信已由问候协议操作来确保。在开始建立邻接关系的短时间内，该状态是最高级状态。（备份）指定路由器是从双向或更高状态下的邻居集内选择的。
- **Exchange Start (交换开始)** — 这是在两个邻居路由器之间创建邻接关系的第一步。此步骤的目标是决定哪个路由器是主路由器，以及决定初始 DD 顺序号。在此状态或更高状态下的邻居对话称为邻接关系。
- **Exchange (交换)** — 在此状态下，路由器正在通过向邻居发送数据库说明信息包来说明整个链路状态数据库。在此状态下，也会发送链路状态请求信息包来询问邻居最近的 LSA。交换状态或更高状态下的所有邻接关系均用于多路发送过程。这些邻接关系完全能够发送和接收所有类型的 OSPF 路由协议信息包。
- **Loading (正在载入)** — 在此状态下，将向邻居发送链路状态请求信息包，询问在交换状态下已经发现（但尚未接收到）的最近 LSA。
- **Full (完全)** — 在此状态下，邻居路由器完全邻接。这些邻接显示在路由器 LSA 和网络 LSA 中。



**Events** (事件) — 此邻居关系更改其状态的次数或错误发生的次数。

**Permanence** (永久) — 此变量显示条目的状态。Dynamic (动态) 和 Permanence (永久) 会查明邻居如何变成已知。

**Hello Suppressed** (抑制问候) — 这表示是否禁止向邻居发送问候。

**Retransmission Queue Length** (重新发送队列长度) — 重新发送队列的当前长度。

## 显示 OSPF 邻居配置

□□□ 打开 **OSPF Neighbor Configuration** (OSPF 邻居配置) 页面。

□□□ 选择要显示的接口和 IP 地址。

邻居配置即会显示。

## 使用 CLI 命令显示 OSPF 邻居配置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- OSPF 命令

## 链路状态数据库

**OSPF Link State Database** (OSPF 链路状态数据库) 页面用于显示 OSPF 链路状态信息。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **OSPF** ® **Link State Database** (链路状态数据库)。

图 10-14. OSPF 链路状态数据库

Router ID	Area ID	LSA Type	LS ID	Age	Sequence	Checksum	Options
1.1.1.1	0.0.0.0	Router Links	1.1.1.1	336	-2147483641	0x8858	-E --
2.2.2.2	0.0.0.0	Router Links	2.2.2.2	340	-2147483640	0xac41	-E --
2.2.2.2	0.0.0.0	Network Links	13.1.1.2	460	-2147483647	0xb64e	-E --
1.1.1.1	0.0.0.0	Network Summary	17.1.1.0	365	-2147483646	0xba80	-E --
2.2.2.2	0.0.0.0	Network Summary	17.1.1.0	351	-2147483646	0x42fd	-E --
2.2.2.2	0.0.0.0	Summary ASBR	1.1.1.1	361	-2147483647	0xfc52	-E --
1.1.1.1	0.0.0.1	Router Links	1.1.1.1	340	-2147483644	0xb25c	-E --
2.2.2.2	0.0.0.1	Router Links	2.2.2.2	341	-2147483643	0xc946	-E --
2.2.2.2	0.0.0.1	Network Links	17.1.1.2	366	-2147483647	0xb27e	-E --
1.1.1.1	0.0.0.1	Network Summary	13.1.1.0	365	-2147483646	0xee50	-E --
2.2.2.2	0.0.0.1	Network Summary	13.1.1.0	445	-2147483645	0x74ce	-E --

**OSPF Link State Database** (OSPF 链路状态数据库) 页面包含以下字段：

**Router ID** (路由器 ID) — 用于唯一标识自治系统 (AS) 中路由器的 32 位点分十进制格式整数。在 IP Configuration (IP 配置) 页面上设

置 **Router ID**（路由器 ID）。如果要更改路由器 ID，必须先禁用 OSPF。在设置新的路由器 ID 之后，必须重新启用 OSPF 才能使更改生效。默认值为 0.0.0.0，但这并非有效的路由器 ID。

**Area ID**（区域 ID）— 其中一个路由器接口连接到的 OSPF 区域的 ID。Area ID（区域 ID）是一个 32 位点分十进制格式整数，用于唯一标识接口连接到的区域。

**LSA Type**（LSA 类型）— 链路状态公布的格式和功能。可能的值包括：

- Router Links（路由器链路）
- Network Links（网络链路）
- Network Summary（网络摘要）
- ASBR Summary（ASBR 摘要）
- AS 外部

**LS ID** — 链路状态 ID，标识路由器域中公布所描述的部分。LS ID 的值取决于公布的 LS 类型。

**Age**（存在时间）— 自从链路状态第一次公布后所经过的时间（单位为秒）。

**Sequence**（顺序）— 顺序号字段是签名的 32 位整数。它用于检测旧的和重复的链路状态公布。顺序号越大，公布越新。

**Checksum**（校验和）— 校验和用于检测公布中数据是否损坏。当公布正在多路发送或保留在路由器内存中时，可能发生这种损坏。此字段是公布全部内容的校验和，除了 LS 存在时间字段。

**Options**（选项）— 链路状态公布标头中的 **Options**（选项）字段表示哪些可选功能与公布相关联。可能的值包括：

- **Q** — 这能够支持 QoS 通信工程。
- **E** — 说明大量发送 AS-external-LSA 的方式。
- **MC** — 这说明根据标准规范转发 IP 多点传送数据包的方式。
- **O** — 这说明是否支持不透明 LSA。
- **V** — 说明是否支持 VPN/COS 的 OSPF++ 扩展。

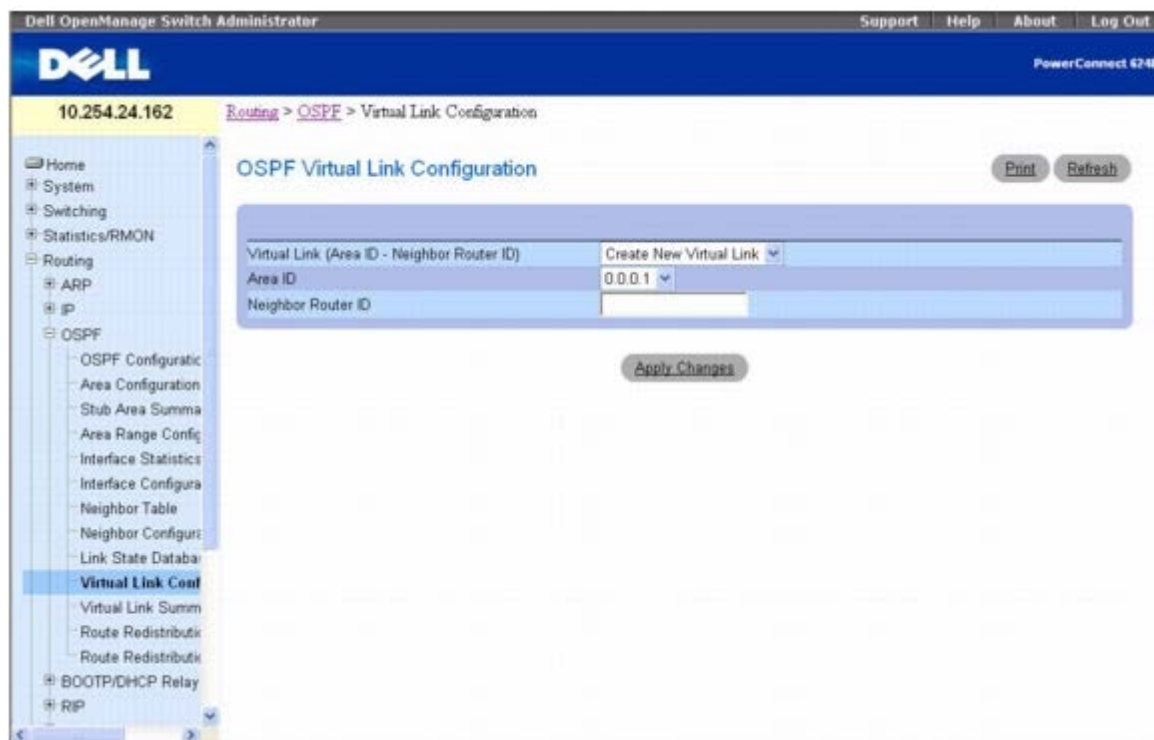
## 虚拟链路配置

**Virtual Link Configuration**（虚拟链路配置）页面用于创建或配置特定区域和邻居的虚拟接口信息。必须先配置有效的 OSPF 区域才可显示此页面。

要显示此页面，请在树视图中单击 **Routing**（路由）® **OSPF**® **Virtual Link Configuration**（虚拟链路配置）。

图 10-15. OSPF 虚拟链路配置 - 创建





**OSPF Virtual Link Configuration (OSPF 虚拟链路配置)** 页面包含以下字段：

**Virtual Link (Area ID - Neighbor Router ID)** (虚拟链路 [区域 ID - 邻居路由器 ID]) — 选择要显示或配置数据的虚拟链路。它包括 Area ID (区域 ID) 和 Neighbor Router ID (邻居路由器 ID)。要创建新的虚拟链路，请从下拉式菜单中选择 **Create New Virtual Link** (新建虚拟链路) 以定义新的虚拟链路。当选择了 **Create New Virtual Link** (新建虚拟链路) 时，会显示以下字段：

**Area ID** (区域 ID) — 32 位点分十进制格式的整数，用于唯一标识路由器接口所连接到的区域。

**Neighbor Router ID** (邻居路由器 ID) — 32 位点分十进制格式的整数，用于唯一标识作为虚拟链路一部分的邻居路由器。

**Hello Interval** (问候间隔) — 以秒为单位输入指定接口的 OSPF 问候间隔。对于连接到网络中的所有路由器而言，此参数必须相同。有效值范围是 1 到 65535。默认值是 10 秒。

**Dead Interval** (无响应间隔) — 以秒为单位输入指定接口的 OSPF 无响应间隔。这是指路由器等待接收来自邻居路由器的问候信息包的时间。在此时间之后，如果仍未收到问候信息包，将认定邻居路由器已关闭。对于连接到网络中的所有路由器而言，此参数必须相同。此值应乘以问候间隔 (例如 4)。有效值范围是 1 到 65535。默认值是 40 秒。

**Interface Delay Interval (secs)** (接口延迟间隔 [秒]) — 虚拟链路的 OSPF 传输延迟 (以秒为单位)。它指定在此接口传输链路状态更新信息包估计所需的秒数。

**State** (状态) — 选定虚拟链路的当前状态。下述状态之一：

- **Down** (关闭) — 这是初始的接口状态。在此状态下，较低层的协议已指明此接口无法使用。在此状态下，系统将接口参数设置为初始值。所有接口计时器均被禁用，并且没有任何邻居与接口相关联。
- **Waiting** (等待) — 路由器正在尝试通过监测接收到的问候信息包来确定 (备份) 指定路由器的身份。在路由器过渡到等待状态以外的状态之前，路由器无法成为 **Backup Designated Router** (备份指定路由器) 和 **Designated Router** (指定路由器)。这样能阻止对 (备份) 指定路由器进行不必要的更改。
- **Point-to-Point** (点到点) — 接口可操作，并且连接到虚拟链路。在进入此状态时，路由器会尝试与邻居路由器建立邻接关系。每隔问候间隔时间 (秒) 便向邻居发送问候信息包。
- **Designated Router** (指定路由器) — 此路由器本身是所连网络上的指定路由器，并且与连接到网络上的所有其他路由器均建立邻接关系。该路由器还必须为网络节点生成一个网络 LSA。网络 LSA 包含连接到网络上的所有路由器 (包括指定路由器本身) 的链路。
- **Backup Designated Router** (备份指定路由器) — 此路由器本身是所连网络上的备份指定路由器。如果现有的指定路由器发生故障，则该路由器会升级为指定路由器。该路由器与连接到网络上的所有其他路由器均建立邻接关系。在多路发送过程中，备份指定路由器执行的功能与指定路由器稍有不同。
- **Other Designated Router** (其它指定路由器) — 接口连接到广播或 NBMA 网络，在该网络上已将其他路由器选择为指定路由器或备份指定路由器。路由器尝试与指定路由器和备份指定路由器形成邻接关系。

**Neighbor State**（邻居状态）— 虚拟邻居关系的状态。

**Retransmit Interval**（重新发送间隔）— 输入指定接口的 OSPF 重新发送间隔。这是指属于此路由器接口的邻居的链路状态公布的间隔秒数。当重新发送数据库说明和链路状态请求信息包时，也可以使用此值。有效值的范围是 0 至 3600 秒（1 小时）。默认值为 5 秒。

**Authentication Type**（验证类型）— 要选择除 None（无）以外的验证类型，请单击 **Configure Authentication**（配置验证）按钮，以打开一个新屏幕，在该屏幕中，可以从下拉式菜单中选择验证类型。选项包括：

- **None**（无）— 这是初始的接口状态。如果从第二个屏幕的下拉式菜单中选择此选项并单击 **Apply Changes**（应用更改），将会返回到第一个屏幕。
- **Simple**（简单）— 如果选择 **Simple**（简单），系统将提示您输入验证密钥。网络上发送的所有信息包的 OSPF 标头中都含有该密钥的明文形式。网络中的所有路由器必须使用同一密钥配置。
- **Encrypt**（加密）— 如果选择 **Encrypt**（加密），系统将提示您输入验证密钥和验证 ID。加密使用 MD5 Message-Digest 算法。网络中的所有路由器必须使用同一密钥和 ID 配置。

**Authentication Key**（验证密钥）— 输入指定接口的 OSPF 验证密钥。如果不选择使用验证，系统将不提示您输入密钥。如果选择 **Simple**（简单）验证，则不能使用超过 8 个字符的密钥。如果选择 **Encrypt**（加密），密钥最长可达 16 个字符。密钥值仅在您以读/写权限登录后才会显示，否则显示为星号。

**Authentication ID**（验证 ID）— 输入要用于验证的 ID。仅在选择 **Encrypt**（加密）作为验证类型后才会提示输入 ID。ID 是介于 0 和 255（含）之间的数字。

## 定义新的虚拟链路

□□□ 打开 **OSPF Virtual Link Configuration**（OSPF 虚拟链路配置）页面。

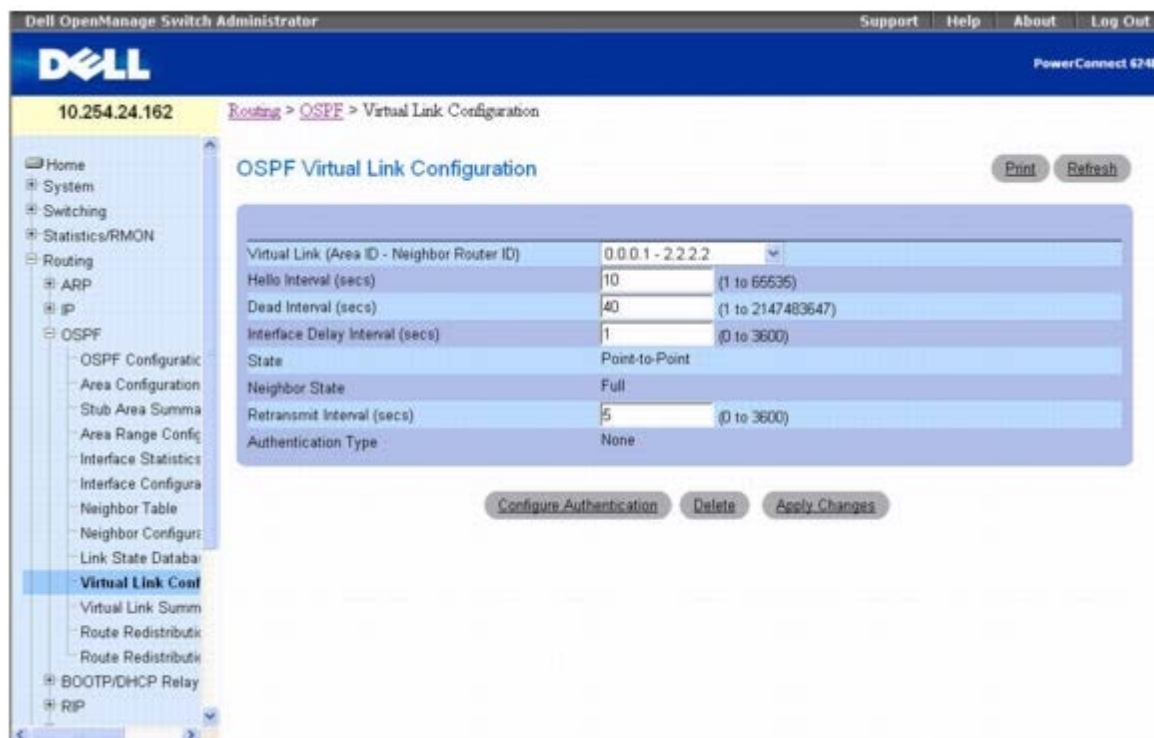
□□□ 从 **Virtual Link (Area ID - Neighbor Router ID)**（虚拟链路 [区域 ID - 邻居路由器 ID]）下拉式菜单中选择 **Create New Virtual Link**（新建虚拟链路）。

□□□ 指定新虚拟链路的邻居路由器 ID。

□□□ 单击 **Apply Changes**（应用更改）。

在创建虚拟链路时，其余字段将显示。

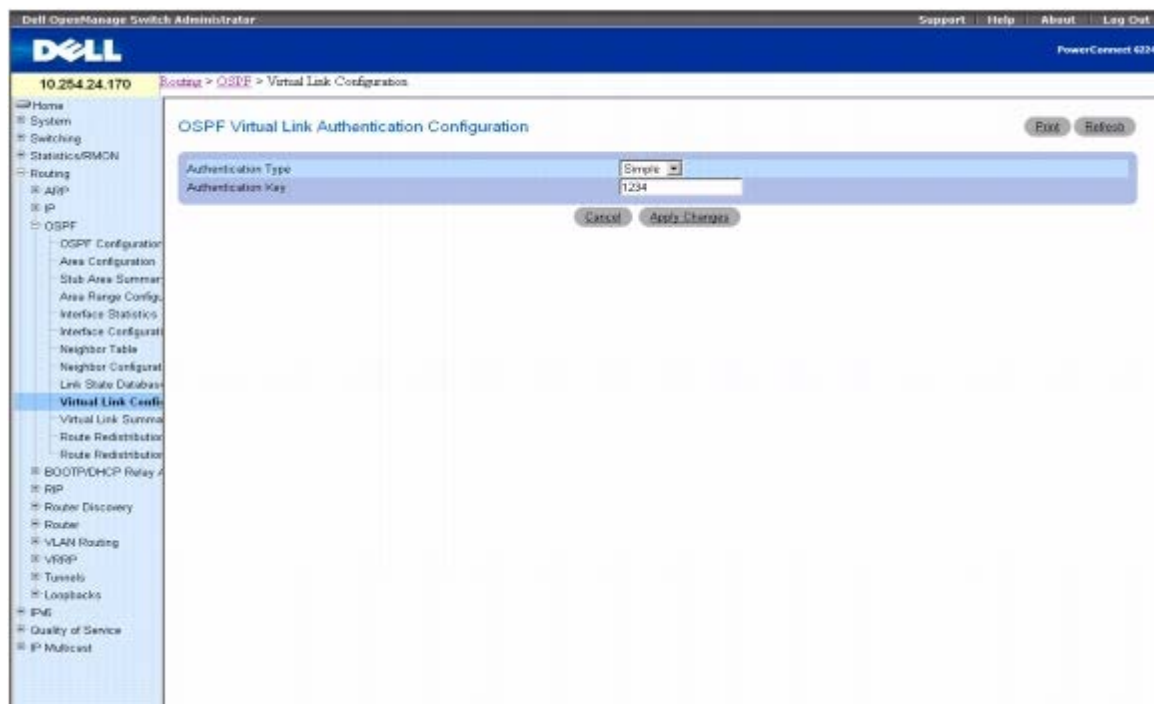
图 10-16. OSPF 虚拟链路配置



□□□ 单击 **Configure Authentication**（配置验证）修改验证。

系统将显示以下页面：

图 10-17. OSPF 虚拟链路验证配置



□□□ 选择 **Authentication Type**（验证类型）和 **Authentication Key**（验证密钥）的值。

□□□ 完成后单击 **Apply Changes**（应用更改）。

## 配置虚拟链路数据

□□□ 打开 **OSPF Virtual Link Configuration**（OSPF 虚拟链路配置）页面。

□□□ 指定要配置的区域 ID 和邻居路由器 ID。

□□□ 按需要在字段中输入数据。

□□□ 单击 **Configure Authentication**（配置验证）修改验证。

□□□ 完成后单击 **Apply Changes**（应用更改）。

将会配置指定 ID 的虚拟链路数据并更新设备。

## 显示虚拟链路数据

□□□ 打开 **OSPF Virtual Link Configuration**（OSPF 虚拟链路配置）页面。

□□□ 指定要显示的区域 ID 和邻居路由器 ID。

这些 ID 的虚拟链路数据将会显示。

## 删除虚拟链路

□□□ 打开 **OSPF Virtual Link Configuration**（OSPF 虚拟链路配置）页面。

□□□ 指定与要删除的虚拟链路关联的 Area ID（区域 ID）和 Neighbor Router ID（邻居路由器 ID）。

相关的虚拟链路数据将会显示。

□□□ 单击 **Delete**（删除）。

系统将删除虚拟链路，并更新设备。

## 使用 CLI 命令配置虚拟链路数据

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- OSPF 命令

## 虚拟链路摘要

**OSPF Virtual Link Summary**（OSPF 虚拟链路摘要）页面用于显示所有已配置的虚拟链路。

要显示此页面，请在树视图中单击 **Routing**（路由）® **OSPF**® **Virtual Link Summary**（虚拟链路摘要）。

图 10-18. OSPF 虚拟链路摘要



**OSPF Virtual Link Summary (OSPF 虚拟链路摘要)** 页面包含以下字段：

**Area ID (区域 ID)** — 要显示其数据的虚拟链路标识的区域 ID 部分。Area ID (区域 ID) 和 Neighbor Router ID (邻居路由器 ID) 共同定义虚拟链路。

**Neighbor Router ID (邻居路由器 ID)** — 虚拟链路标识的邻居部分。可以在与公共 (非主干网) 区域具有接口的任何区域边界路由器对之间配置虚拟链路。

**Hello Interval(secs) (问候间隔 [秒])** — 虚拟链路的 OSPF 问候间隔 (秒)。对于连接到网络中的所有路由器而言，问候间隔值必须相同。

**Dead Interval(secs) (无响应间隔 [秒])** — 虚拟链路的 OSPF 无响应间隔 (秒)。这是指路由器等待接收来自邻居路由器的问候信息包的时间。在此时间之后，如果仍未收到问候信息包，将认定邻居路由器已关闭。对于连接到公共网络的所有路由器而言，此参数必须相同，并且必须是问候间隔的倍数 (即，4)。

**Retransmit Interval(secs) (重新发送间隔 [秒])** — 虚拟链路的 OSPF 重新发送间隔 (秒)。该字段指定属于此路由器接口的邻接关系的链路状态公布的间隔时间。当重新发送数据库说明和链路状态请求信息包时，也可以使用此值。

**Iiftransit Delay Interval (Iiftransit 延迟间隔)** — 虚拟链路的 OSPF 发送延迟 (单位为秒)。它指定在此接口传输链路状态更新信息包估计所需的秒数。

## 使用 CLI 命令显示虚拟链路摘要

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- OSPF 命令

## 路由重新分配配置

**OSPF Route Redistribution Configuration (OSPF 路由重新分配配置)** 页面用于配置通过 Static (静态)、Connected (已连接) 和 RIP 获取路由后，如何在 OSPF 中重新分配这些路由。您可以选择重新分配从以上所有项或选定项获取的路由。

要显示此页面，请在树视图中单击 **Routing (路由)** ® **OSPF** ® **Route Redistribution Configuration (路由重新分配配置)**。

图 10-19. OSPF 路由重新分配配置





**OSPF Route Redistribution Configuration (OSPF 路由重新分配配置)** 页面包含以下字段：

**Configured Source** (配置的来源) — 为 OSPF 配置的协议，用以重新分配通过此协议获取的路由。只有来源路由已经被 OSPF 相应配置，才可用于重新分配。Create (创建) 可用于配置新的来源路由。

**Available Source** (可用来源) — 可用于 OSPF 重新分配路由的协议配置。此框仅在选择 Create (创建) 作为 Configured Source (配置的来源) 时才会显示。可能的值包括 Static (静态)、Connected (已连接) 和 RIP。

**Metric** (跃点) — 为重新分配的路由设置跃点值。如果来源已预先配置，此字段将显示跃点值。有效值为 0 到 16777214。

**Metric Type** (跃点类型) — 从下拉式菜单中为重新分配的路由选择 OSPF 跃点类型。

**Tag** (标签) — 设置重新分配的路由中的标签字段。如果来源已预先配置，此字段将显示标签值，否则显示 0。有效值为 0 到 4294967295。

**Subnets** (子网) — 从下拉式菜单中选择是否重新分配子网路由。

**Distribute List** (分配列表) — 选择一个访问列表，该访问列表将对目的地协议重新分配的路由进行过滤。只有允许的路由会被重新分配。如果此命令引用不存在的访问列表，则允许所有路由。此下拉式菜单列出了在 **Switching** (交换) ® **Network Security** (网络安全保护) ® **Access Control Lists** (访问控制列表) ® **IP Access Control Lists** (IP 访问控制列表) 页面中配置的 ACL。在用于路由过滤时，访问列表中使用到的字段包括：

- 来源 IP 地址和网络掩码
- 目的地 IP 地址和网络掩码
- 动作 (允许或延迟)

所有其它字段 (来源和目的地端口、优先、服务类型等) 将被忽略。

来源 IP 地址将与路由目的地 IP 地址相比较。访问列表规则中的来源 IP 网络掩码被视为通配符掩码，表示来源 IP 地址中哪些位必须与路由的目的地地址匹配。(请注意，掩码中的 1 表示不考虑对应的地址位。)

当访问列表规则包括目的 IP 地址和网络掩码 (扩充的访问列表) 时，目的地 IP 地址将与路由目的地网络掩码相比较。访问列表中的目的地网络掩码用作通配符掩码，表示路由的目的地掩码中哪些位会影响过滤操作。

## 创建 OSPF 路由重新分配来源

如果没有配置重新分配，系统在 Configured Source (配置的来源) 中仅显示 Create (创建)，并在 Available Source (可用来源) 中显示可

能的来源。选择 **Available Source**（可用来源），输入配置数据并单击 **Apply Changes**（应用更改）之后，项目将显示在 **Configured Source**（配置的来源）下拉式列表中，并从 **Available Source**（可用来源）下拉式列表中删除。

□□□ 打开 **OSPF Route Redistribution Configuration**（OSPF 路由重新分配配置）页面。

□□□ 在 **Configured Source**（配置的来源）字段中指定 **Create**（创建）。

□□□ 从 **Available Source**（可用来源）字段中选择 **Static**（静态）、**Connected**（已连接）或 **RIP**。

□□□ 完成后单击 **Apply Changes**（应用更改）。

系统将配置路由重新分配数据，并更新设备。

## 修改 **OSPF** 路由重新分配数据

□□□ 打开 **OSPF Route Redistribution Configuration**（OSPF 路由重新分配配置）页面。

□□□ 从 **Configured Source**（配置的来源）下拉式列表中选择来源。

□□□ 按需要在字段中输入数据。

□□□ 完成后单击 **Apply Changes**（应用更改）。

系统将配置路由重新分配数据，并更新设备。

## 使用 **CLI** 命令配置 **OSPF** 路由重新分配数据

有关执行此功能的 CLI 命令的信息，请参阅《*CLI 参考指南*》的以下章节：

- **OSPF 命令**

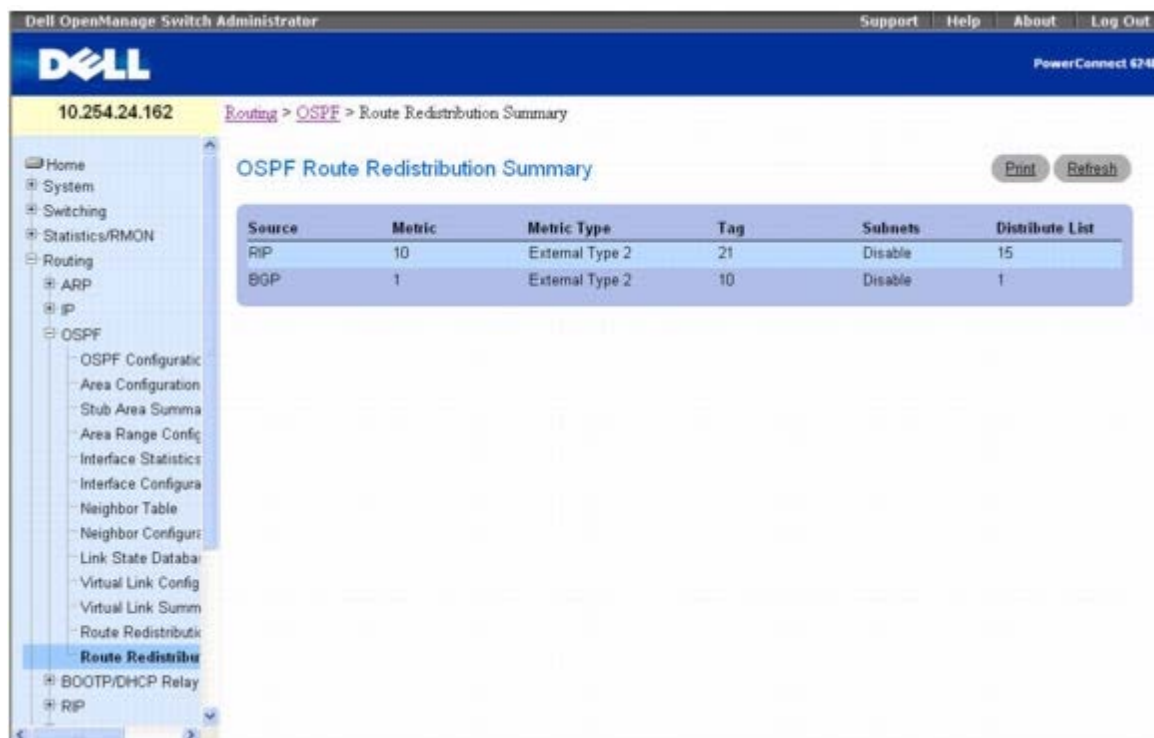
## 路由重新分配摘要

**OSPF Route Redistribution Summary**（OSPF 路由重新分配摘要）页面用于显示 OSPF 路由重新分配配置。

要显示此页面，请在树视图中单击 **Routing**（路由）® **OSPF**® **Route Redistribution Summary**（路由重新分配摘要）。

图 10-20. OSPF 路由重新分配摘要





**OSPF Route Redistribution Summary**（OSPF 路由重新分配摘要）页面包含以下字段：

**Source**（来源）— OSPF 要重新分配的来源路由。

**Metric**（跃点）— 为指定来源路由重新分配的路由的跃点。未配置时，将显示 Unconfigured（未配置）。

**Metric Type**（跃点类型）— 重新分配的路由的 OSPF 跃点类型。

**Tag**（标签）— 重新分配的路由中的标签字段。如果来源已预先配置，此字段将显示标签值，否则显示 0。

**Subnets**（子网）— 指定是否应重新分配子网路由。

**Distribute List**（分配列表）— 用于过滤目的地协议重新分配的路由的访问列表。

## 使用 CLI 命令显示路由重新分配摘要

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- OSPF 命令

## BOOTP/DHCP 中继代理

BootP/DHCP 中继代理可让 BootP/DHCP 客户端和服务器通过不同的子网交换 BootP/DHCP 信息。该中继代理接收来自客户端的请求，并检查有效的跃距和 giaddr 字段。如果跃距数大于配置值，该代理会认为信息包通过代理进行循环而将其丢弃。如果 giaddr 字段为零，则代理必须用接收请求的接口的 IP 地址填写此字段。代理将有效的信息包单点传送到下一个配置的目的地。服务器用指向最接受客户端（如 giaddr 字段所指）的中继代理的单点传送 BOOTREPLY 进行响应。从服务器收到 BOOTREPLY 之后，代理会在收到 BOOTREQUEST 的接口上以广播或单点传送方式转发此答复。此接口可由 giaddr 字段标识。

当客户用高速调制解调器连接到 Internet 时，6200 系列 DHCP 组件还支持使用 DHCP 中继代理选项来确定来源线路。中继代理在转发请求到服务器时会插入这些选项，并在向客户端发送答复时将其删除。

如果接口有多个 IP 地址，中继代理应使用配置的主 IP 地址作为其中继代理 IP 地址。

**BOOTP/DHCP Relay Agent**（BOOTP/DHCP 中继代理）菜单页面包含用于配置和显示 BOOTP/DHCP 中继代理的网页链接。要显示此页面，请在树视图中单击 **Routing**（路由）® **BOOTP/DHCP Relay Agent**（BOOTP/DHCP 中继代理）。在此菜单页面中可以访问以下

网页：

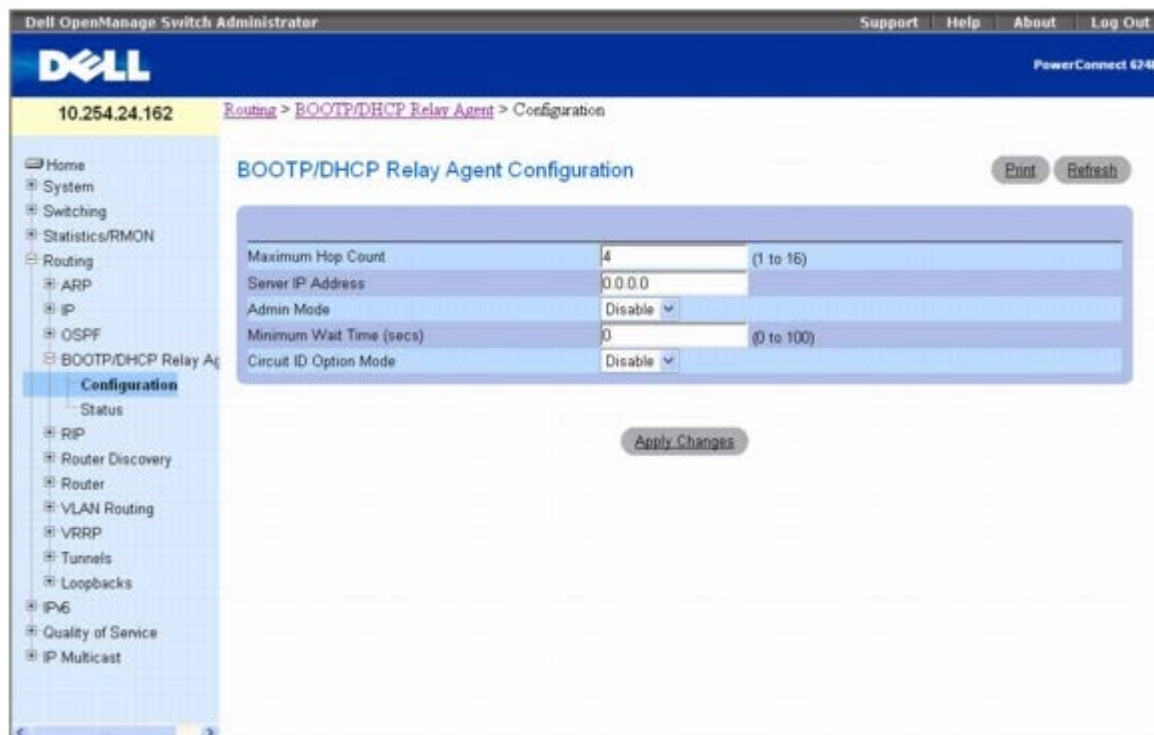
- [BOOTP/DHCP 中继代理配置](#)
- [BOOTP/DHCP 中继代理状态](#)

## BOOTP/DHCP 中继代理配置

**BOOTP/DHCP Relay Agent Configuration (BOOTP/DHCP 中继代理配置)** 页面用于配置和显示 BOOTP/DHCP 中继代理。

要显示此页面，请在树视图中单击 **Routing (路由)** ⑥ **BOOTP/DHCP Relay Agent (BOOTP/DHCP 中继代理)** ⑥ **Configuration (配置)**。

图 10-21. BOOTP/DHCP 中继代理配置



**BOOTP/DHCP Relay Agent Configuration (BOOTP/DHCP 中继代理配置)** 页面包含以下字段：

**Maximum Hop Count (最大跃距数)** — 输入客户端请求在被丢弃之前可以经过的最大跃距数。

**Server IP Address (服务器 IP 地址)** — 输入 BOOTP/DHCP 服务器的 IP 地址或下一个 BOOTP/DHCP 中继代理的 IP 地址。

**Admin Mode (管理模式)** — 从下拉式菜单中选择 **Enable (启用)** 或 **Disable (禁用)**。如果选择 **Enable (启用)**，BOOTP/DHCP 请求会转发到您 **Server IP address (服务器 IP 地址)** 字段中输入的 IP 地址。

**Minimum Wait Time(secs) (最短等待时间 [秒])** — 以秒为单位输入时间。此值与客户端请求信息包中的时间戳相比较，后者表示客户端开机后所经过的时间。只有在时间戳超过最短等待时间后才会转发信息包。

**Circuit ID Option Mode (线路 ID 选项模式)** — 从下拉式菜单中选择 **Enable (启用)** 或 **Disable (禁用)**。如果选择 **Enable (启用)**，则中继代理在转发 Option 82 标头信息到服务器之前，会将其添加到 DHCP 请求信息包中，并在向客户端转发响应时将其删除。

### 配置 BOOTP/DHCP

打开 **BOOTP/DHCP Configuration (BOOTP/DHCP 配置)** 页面。

按需要在字段中输入数据。

□□□ 完成后单击 **Apply Changes**（应用更改）。

系统将配置 BOOTP/DHCP 数据，并更新设备。

## 使用 CLI 命令配置 BOOTP/DHCP

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

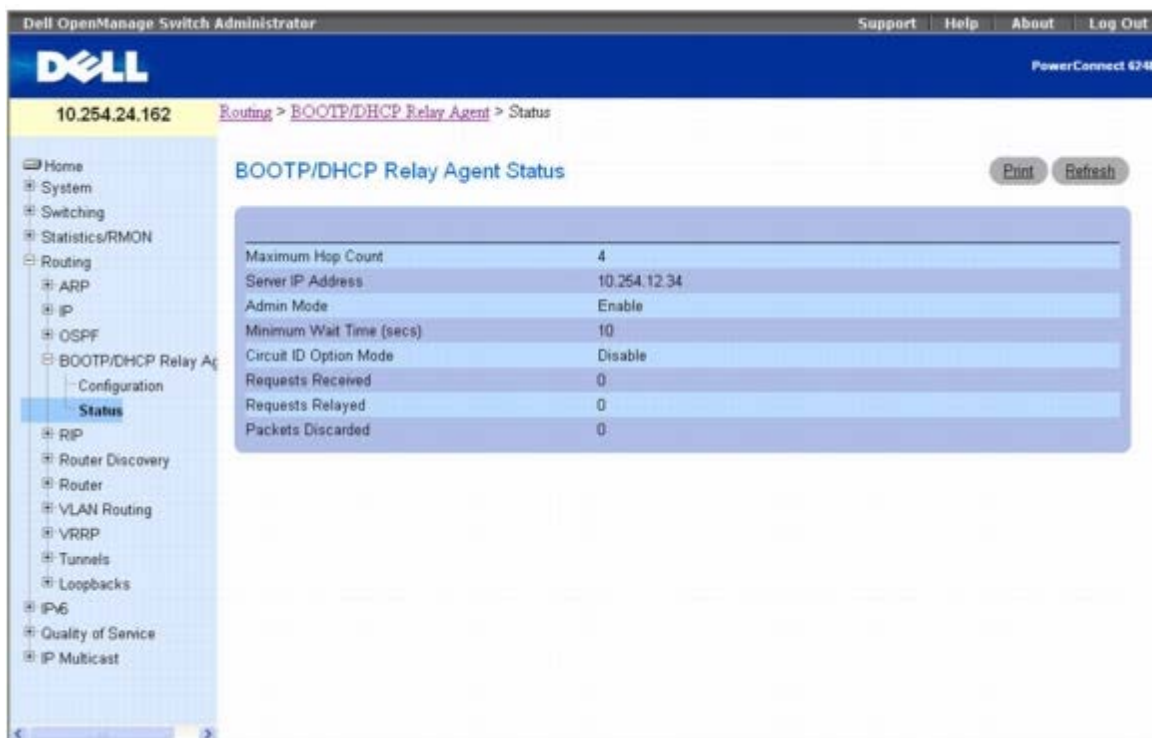
- DHCP 和 BOOTP 中继命令

## BOOTP/DHCP 中继代理状态

**BOOTP/DHCP Relay Agent Status**（BOOTP/DHCP 中继代理状态）页面用于显示 BOOTP/DHCP 中继代理配置和状态信息。

要显示此页面，请在树视图中单击 **Routing**（路由）® **BOOTP/DHCP Relay Agent**（BOOTP/DHCP 中继代理）® **Status**（状态）。

图 10-22. BOOTP/DHCP 中继代理状态



**BOOTP/DHCP Status**（BOOTP/DHCP 状态）页面会显示以下字段：

**Maximum Hop Count**（最大跃距数）— 客户端请求在被丢弃之前可以经过的最大跃距数。

**Server IP Address**（服务器 IP 地址）— BOOTP/DHCP 服务器的 IP 地址或下一个 BOOTP/DHCP 中继代理的 IP 地址。

**Admin Mode**（管理模式）— 中继的管理模式。如果在配置页面上选择 **Enable**（启用），BOOTP/DHCP 请求会转发到您在 **Server IP address**（服务器 IP 地址）字段中输入的 IP 地址。

**Minimum Wait Time(secs)**（最短等待时间【秒】）— 以秒为单位的最短时间。此值与客户端请求信息包中的时间戳相比较，后者表示客户端开机后所经过的时间。只有在时间戳超过最短等待时间后才会转发信息包。

**Circuit ID Option Mode**（线路 ID 选项模式）— 这是中继代理选项，其值可为 **Enabled**（启用）或 **Disabled**（禁用）。如果选择 **Enable**（启用），则中继代理在转发 **Option 82** 标头信息到服务器之前，会将其添加到 DHCP 请求信息包中，并在向客户端转发响应时将其删除。

**Requests Received**（收到的请求）— 自上次交换机重置后从所有客户端收到的 BOOTP/DHCP 请求总数。

**Requests Relayed**（中继的请求）— 自上次交换机重置后转发到服务器的 BOOTP/DHCP 请求总数。

**Packets Discarded**（丢弃的信息包）— 自上次交换机重置后被此中继代理丢弃的 BOOTP/DHCP 信息包总数。

## 使用 CLI 命令显示 BOOTP/DHCP

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- DHCP 和 BOOTP 中继命令

---

## RIP

RIP 是基于 Bellman-Ford 算法的内部网关协议 (IGP)，主要针对较小的网络（网络直径不超过 15 个跃距）。路由信息定期通过 RIP 更新信息包传播，且在网络拓扑发生变动时也会传播。在收到 RIP 更新时，根据路由表中是否存在指定的路由，路由器可能会在其路由表中修改、删除或添加路由。路由首选项通过用以表示目的地距离的可配置跃点传送。

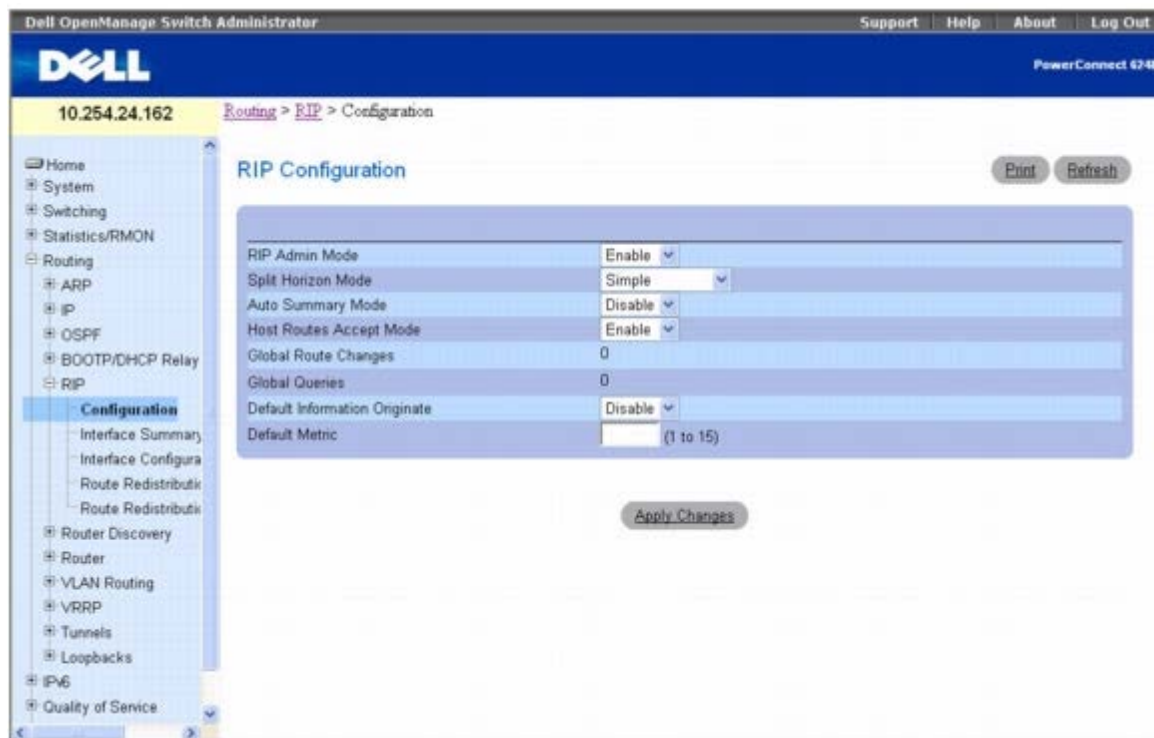
**RIP** 菜单页面包含用于配置和显示 RIP 参数和数据的网页的链接。要显示此页面，请在树视图中单击 **Routing**（路由）® **RIP**。在此菜单页面中可以访问以下网页：

- [RIP 配置](#)
- [RIP 接口摘要](#)
- [RIP 接口配置](#)
- [RIP 路由重新分配配置](#)
- [RIP 路由重新分配摘要](#)

## RIP 配置

**RIP Configuration**（RIP 配置）页面用于在全局模式中启用和配置或禁用 RIP。要显示此页面，请在树视图中单击 **Routing**（路由）® **RIP** ® **Configuration**（配置）。

图 10-23. RIP 配置



**RIP Configuration (RIP 配置)** 页面包含以下字段：

**RIP Admin Mode (RIP 管理模式)** — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用)。如果选择 **Enable** (启用)，交换机将启用 RIP。默认值为 **Disable** (禁用)。

**Split Horizon Mode (水平分割模式)** — 从下拉式菜单中选择 **None** (无)、**Simple** (简单) 或 **Poison Reverse** (毒性反转)。默认值为 **Simple** (简单)。如果使用水平分割这一方法，可避免在将更新发送到最初获取该路由的路由器时，如果路由器包括该路，将会造成的问题。选项如下：

- **None** (无) — 这种情况下不作特殊处理。
- **Simple** (简单) — 将更新发送到最初获取该路由的路由器时，路由不包括在更新中。
- **Poison Reverse** (毒性反转) — 将更新发送到最初获取该路由的路由器时，路由包括在更新中，但跃点则被设置为无限大。

**Auto Summary Mode (自动摘要模式)** — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用)。如果选择 **Enable** (启用)，则相邻路由组将汇总为一个条目以减少条目总数。默认值为 **Enable** (启用)。

**Host Routes Accept Mode (主机路由接受模式)** — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用)。如果选择 **Enable** (启用)，则路由器接受主机路由。默认值为 **Enable** (启用)。

**Global Route Changes (全局路由更改)** — 显示 RIP 对 IP 路由数据库作出的路由更改数。此计数不包括路由存在时间的刷新。

**Global Queries (全局查询)** — 显示从其它系统发送到 RIP 查询的响应数。

**Default Information Originate (产生默认信息)** — 启用或禁用默认路由公布。

**Default Metric (默认跃点)** — 为重新分配的路由设置默认跃点数。若已设置，此字段将显示默认跃点数；若尚未设置，则留空。有效值是 1 至 15。

## 配置 RIP

□□□ 打开 **RIP Configuration (RIP 配置)** 页面。

□□□ 按需要在字段中输入数据。

□□□ 完成后单击 **Apply Changes (应用更改)**。

系统将配置 RIP，并更新设备。

## 使用 CLI 命令配置 RIP

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

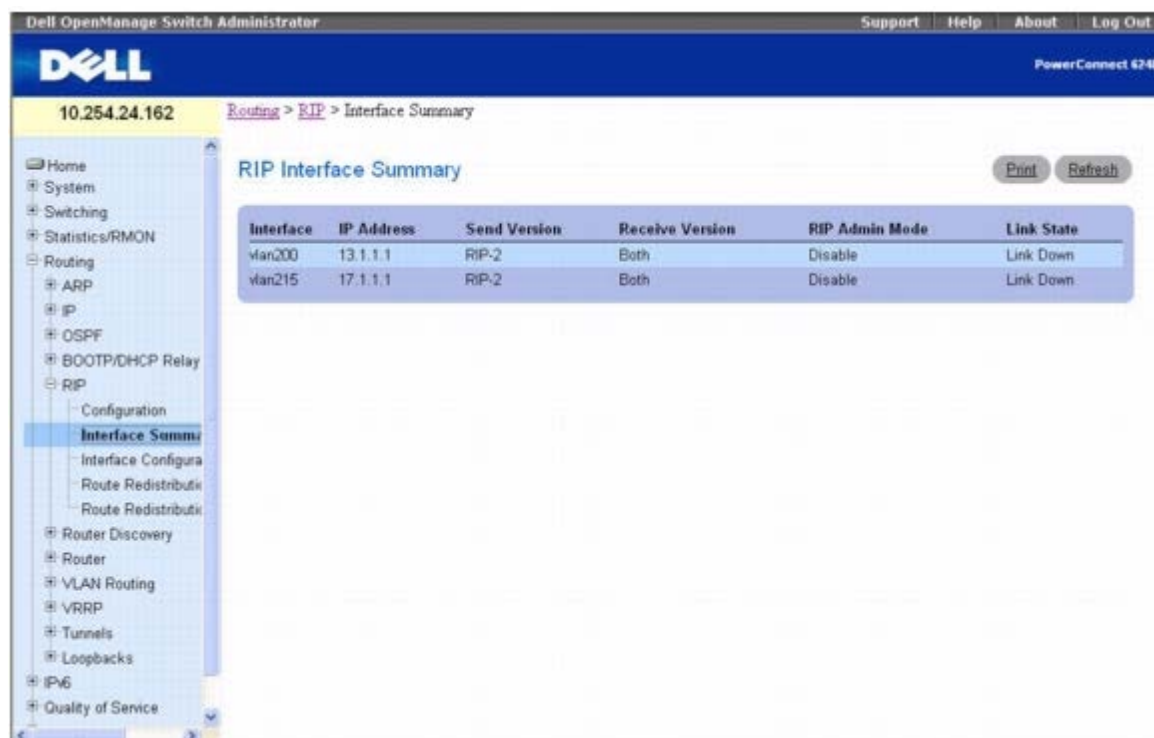
- 路由信息协议 (RIP) 命令

## RIP 接口摘要

**RIP Interface Summary** (RIP 接口摘要) 页面用于显示接口的 RIP 配置状态。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **RIP** ® **Interface Summary** (接口摘要)。

图 10-24. RIP 接口摘要



**RIP Interface Summary** (RIP 接口摘要) 页面会显示以下字段：

**Interface** (接口) — 接口，例如启用了 RIP 的路由 VLAN。

**IP Address** (IP 地址) — 路由器接口的 IP 地址。

**Send Version** (发送版本) — 指定从接口发送的 RIP 控制信息包所对应的 RIP 版本。默认值 RIP-2。可能的值为：

- **RIP-1** — 使用广播发送 RIP 版本 1 信息包。
- **RIP-1c** — RIP 版本 1 兼容模式。使用广播发送 RIP 版本 2 格式的信息包。
- **RIP-2** — 使用多点传送发送 RIP 版本 2 信息包。
- **None** (无) — 不发送 RIP 控制信息包。

**Receive Version** (接收版本) — 指定接口接收哪些 RIP 版本控制信息包。默认值为 **Both** (两者)。可能的值包括：



- **RIP-1** — 只接收 RIP 版本 1 格式的信息包。
- **RIP-2** — 只接收 RIP 版本 2 格式的信息包。
- **Both** (两者) — 接收任何格式的信息包。
- **None** (无) — 不接收 RIP 控制信息包。

**RIP Admin Mode** (RIP 管理模式) — 指定在接口上启用还是禁用 RIP。

**Link State** (链路状态) — 指定打开还是关闭 RIP 接口。

## 使用 CLI 命令显示 RIP 接口摘要

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 路由信息协议 (RIP) 命令

## RIP 接口配置

**RIP Interface Configuration** (RIP 接口配置) 页面用于在特定接口上启用并配置或者禁用 RIP。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **RIP** ® **Interface Configuration** (接口配置)。

图 10-25. RIP 接口配置



**RIP Interface Configuration** (RIP 接口配置) 页面包含以下字段：

**Interface** (接口) — 从下拉式菜单中选择要配置其数据的接口。

**Send Version** (发送版本) — 路由器以其路由更新发送的 RIP 版本。默认值 RIP-2。可能的值为：

- **RIP-1** — 通过广播发送 RIP 版本 1 格式的信息包。



- **RIP-1c** — RIP 版本 1 兼容模式。通过广播发送 RIP 版本 2 格式的信息包。
- **RIP-2** — 使用多点传送发送 RIP 版本 2 信息包。
- **None** (无) — 不发送 RIP 控制信息包。

**Receive Version** (接收版本) — 路由器必须接受的路由更新 RIP 版本。默认值为 **Both** (两者)。可能的值包括：

- **RIP-1** — 只接受 RIP 版本 1 格式的信息包。
- **RIP-2** — 只接受 RIP 版本 2 格式的信息包。
- **Both** (两者) — 接受任何格式的信息包。
- **None** (无) — 不接受任何 RIP 控制信息包。

**RIP Admin Mode** (RIP 管理模式) — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用)。在接口上启用 RIP 版本 1 或版本 1c 之前，必须先在对的接口上启用网络传送的广播模式。默认值为 **Disable** (禁用)。

**Authentication Type** (验证类型) — 要选择除 **None** (无) 以外的验证类型，请单击 **Modify** (修改) 按钮，以打开一个新屏幕，在该屏幕中，可以从下拉式菜单中选择验证类型。可能的值包括：

- **None** (无) — 这是初始的接口状态。如果从第二个屏幕的下拉式菜单中选择此选项并单击 **Apply Changes** (应用更改)，将会返回到第一个屏幕，而不运行任何验证协议。
- **Simple** (简单) — 如果选择 **Simple** (简单)，系统将提示您输入验证密钥。网络上发送的所有信息包的 RIP 表头中都含有该密钥的明文形式。网络中的所有路由器必须使用同一密钥配置。
- **Encrypt** (加密) — 如果选择 **Encrypt** (加密)，系统将提示您输入验证密钥和验证 ID。加密使用 MD5 Message-Digest 算法。网络中的所有路由器必须使用同一密钥和 ID 配置。

**IP Address** (IP 地址) — 显示路由器接口的 IP 地址。

**Link State** (链路状态) — 指定打开还是关闭 RIP 接口。

**Bad Packets Received** (收到的坏信息包) — 显示被发现无效或损坏的 RIP 信息包数目。这明确不包括已发送的包含新信息的完整更新。

**Bad Routes Received** (接收的坏路由) — 显示有效的 RIP 信息包中由于任何原因被忽略的路由数量，例如如此接口上实际发送的已触发的 RIP 更新数量。这明确不包括已发送的包含新信息的完整更新。

**Updates Sent** (已发送的更新) — 显示已发送的路由更新数目。

## 配置 RIP 接口

打开 **RIP Interface Configuration** (RIP 接口配置) 页面。

指定要为其配置数据的接口。

按需要在字段中输入数据：

**Send Version** (发送版本) — 从下拉框中选择 **None** (无)、**RIP-1**、**RIP-1c** 或 **RIP2**。

**Receive Version** (接收版本) — 从下拉框中选择 **None** (无)、**RIP-1**、**RIP-2** 或 **Both** (两者)。

**RIP Admin Mode** (RIP 管理模式) — 选择 **Enable** (启用) 或 **Disable** (禁用)。

**Authentication Type** (验证类型) — 单击 **Modify** (修改) 按钮配置不同的验证类型。

完成后单击 **Apply Changes** (应用更改)。

系统将配置 RIP 接口，并更新设备。

## 选择验证方法

□□□ 打开 **RIP Interface Configuration** (**RIP** 接口配置) 页面。

□□□ 指定要为其配置验证方法的接口。

□□□ 单击 **Modify** (修改)。

**Authentication Method** (验证方法) 页面将会显示。

□□□ 从下拉式菜单中选择 **Authentication Type** (验证类型)：None (无)、Simple (简单) 或 Encrypt (加密)。

□□□ 如果指定 Simple (简单) 或 Encrypt (加密) 为 **Authentication Type** (验证类型)，将会显示其它字段。输入 **Authentication Key** (验证密钥) (Simple [简单] 或 Encrypt [加密]) 和 **Authentication Key ID** (验证密钥 ID) (Encrypt [加密])。

□□□ 单击 **Apply Changes** (应用更改)。

□□□ 系统将会更新验证方法和设备。

## 使用 CLI 命令配置 RIP 接口

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

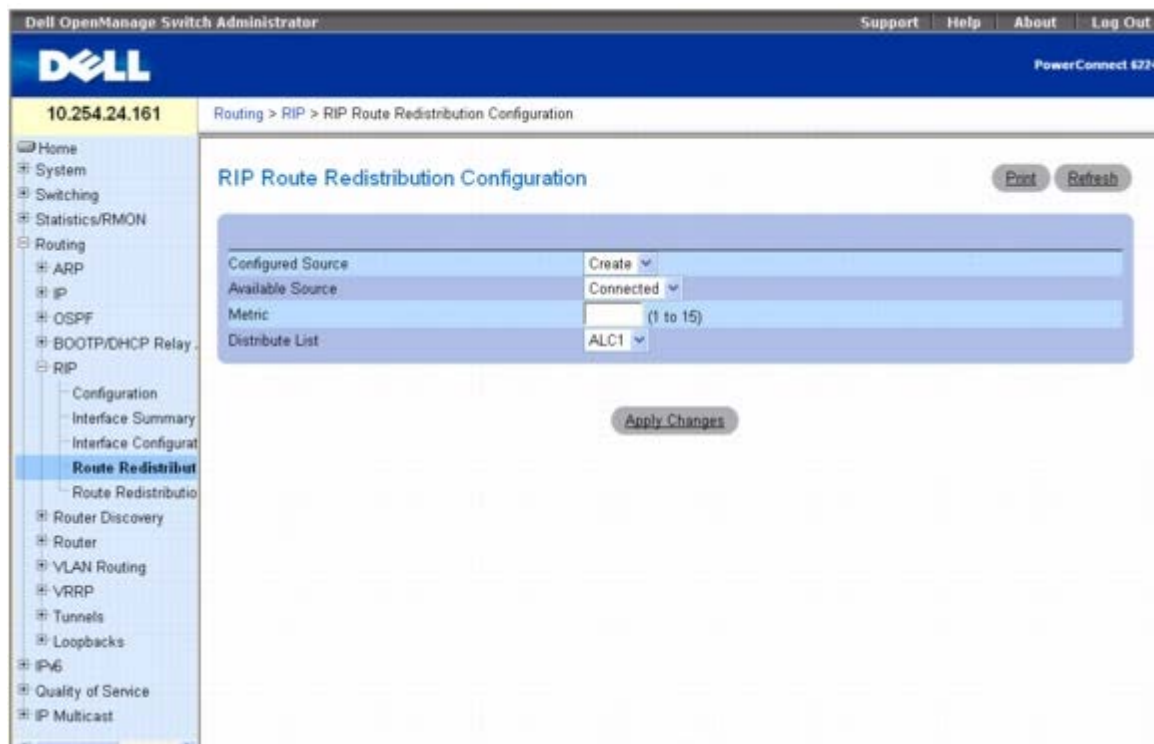
- 路由信息协议 (RIP) 命令

## RIP 路由重新分配配置

**RIP Route Redistribution Configuration** (**RIP** 路由重新分配配置) 页面用于配置 RIP 路由重新分配参数。每个字段允许的值显示在字段旁边。如果输入了任何无效的值，将会显示一则警报信息和所有有效值的列表。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **RIP** ® **Route Redistribution Configuration** (路由重新分配配置)。

图 10-26. RIP 路由重新分配配置



**RIP Route Redistribution Configuration (RIP 路由重新分配配置)** 页面包含以下字段：

**Configured Source** (配置的来源) — 此选择框是一个动态选择器，只包括已经配置为由 RIP 重新分配的来源路由。Create (创建) 用于配置可用的来源路由。

**Available Source** (可用来源) — 此选择框是一个动态选择器，只包括之前已经配置为由 RIP 重新分配的来源路由。此选择框仅在选择 Create (创建) 选项作为 Configured Source (配置的来源) 时才会显示。可能的值包括：

- **Static** (静态)
- **Connected** (已连接)
- **OSPF**

**Metric** (跃点) — 设置要用作重新分配的路由跃点的跃点值。如果源是预配置源且可以修改，则此字段显示跃点。有效值为 1 到 15。

**Distribute List** (分配列表) — 此选择框用于设置访问列表，该访问列表将对目的地协议重新分配的路由进行过滤。只有允许的路由会被重新分配。

此下拉式菜单列出了通过 **Switching** (交换) ® **Network Security** (网络安全保护) ® **Access Control Lists** (访问控制列表) ® **IP Access Control Lists** (IP 访问控制列表) 下的页面配置的 ACL。在用于路由过滤时，访问列表中使用到的字段包括：

- 来源 IP 地址和网络掩码
- 目的地 IP 地址和网络掩码
- 动作 (允许或延迟)

所有其它字段 (来源和目的地端口、优先、服务类型等) 将被忽略。

来源 IP 地址将与路由目的地 IP 地址相比较。访问列表规则中的来源 IP 网络掩码被视为通配符掩码，表示来源 IP 地址中哪些位必须与路由的目的地地址匹配。(请注意，掩码中的 1 表示不考虑对应的地址位。)

当访问列表规则包括目的 IP 地址和网络掩码 (扩充的访问列表) 时，目的地 IP 地址将与路由目的地网络掩码相比较。访问列表中的目的地网络掩码用作通配符掩码，表示路由的目的地掩码中哪些位会影响过滤操作。

## 创建配置的路由

□□□ 打开 **RIP Route Redistribution Configuration** (**RIP** 路由重新分配配置) 页面。

□□□ 选择要配置的 **Available Source** (可用来源)。

□□□ 指定其余字段的值。

□□□ 单击 **Apply Changes** (应用更改)。

系统即会配置指定的来源，并更新设备。

## 修改配置的路由

□□□ 打开 **RIP Route Redistribution Configuration** (**RIP** 路由重新分配配置) 页面。

□□□ 选择要修改的 **Configured Source** (配置的路由)。

□□□ 按需要更改此屏幕上的值。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存指定的更改，并更新设备。

## 使用 CLI 命令配置 RIP 路由重新分配

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 路由信息协议 (RIP) 命令

## RIP 路由重新分配摘要

**RIP Route Redistribution Summary** (**RIP** 路由重新分配摘要) 页面用于显示路由重新分配配置。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **RIP** ® **Route Redistribution Summary** (路由重新分配摘要)。

图 10-27. RIP 路由重新分配摘要



**RIP Route Redistribution Summary** (RIP 路由重新分配摘要) 页面包含以下字段：

**Source** (来源) — RIP 要重新分配的来源路由。

**Metric** (跃点) — 为源路由指定重新分配的路由的跃点。未配置时，将显示 **Unconfigured** (未配置)。

**Match** (匹配) — 选择 OSPF 为 **Source** (来源) 时重新分配的路由列表。该列表可能包括一个或多个：

- Internal (内部)
- External 1 (外部 2)
- External 2 (外部 2)
- NSSA-External 1 (NSSA 外部 2)
- NSSA-External 2 (NSSA 外部 2)
- N.A. (if not OSPF) (不详 [如果并非 OSPF])

**Distribute List** (分配列表) — 用于过滤目的地协议将重新分配的路由的访问列表。如果尚未配置 **Distribute List** (分配列表)，该字段为空白。

## 使用 CLI 命令显示 RIP 路由重新分配摘要

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 路由信息协议 (RIP) 命令

## 路由器发现

路由器发现协议供主机用来查找子网上可操作的路由器。路由器发现信息有两种类型：“路由器公布”和“路由器恳求”。协议要求每个路由器定期公布与之关联的 IP 地址。主将机侦听这些公布，并搜索邻居路由器的 IP 地址。

**Router Discovery** (路由器发现) 菜单页面包含用于配置和显示路由器发现数据的网页的链接。要显示此菜单，请在树视图中单击 **Routing** (路由) @ **Router Discovery** (路由器发现)。在此菜单页面中可以访问以下网页：

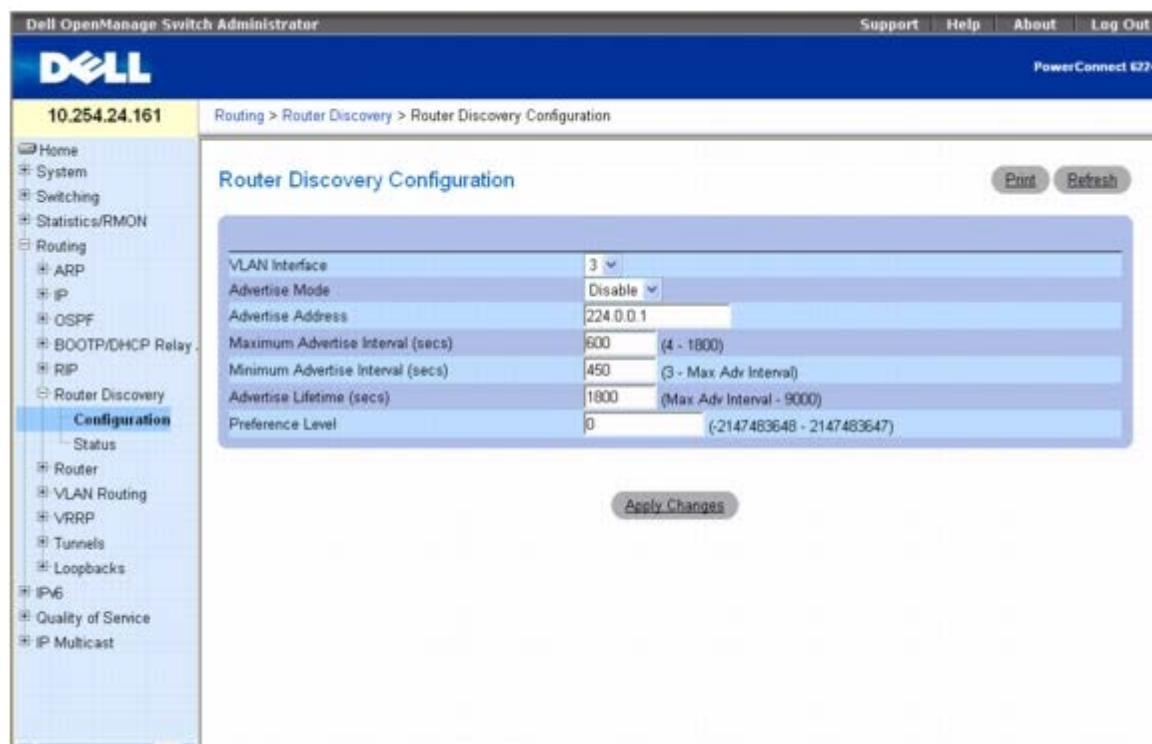
- [路由器发现配置](#)
- [路由器发现状态](#)

## 路由器发现配置

**Router Discovery Configuration** (路由器发现配置) 页面用于输入或更改路由器发现参数。

要显示此页面，请在树视图中单击 **Routing** (路由) @ **Router Discovery** (路由器发现) @ **Configuration** (配置)。

图 10-28. 路由器发现配置



**Router Discovery Configuration** (路由器发现配置) 页面包含以下字段：

**VLAN Interface** (VLAN 接口) — 选择要配置其数据的路由器接口。

**Advertise Mode** (公布模式) — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用)。如果选择 **Enable** (启用)，将会从所选的接口发送路由器公布。

**Advertise Address** (公布地址) — 输入要用于公布路由器的 IP 地址。

**Maximum Advertise Interval(secs)** (最大公布间隔 [秒]) — 输入从接口发送的路由器公布之间允许的最长时间间隔 (秒)。

**Minimum Advertise Interval(secs)** (最小公布间隔 [秒]) — 输入从接口发送的路由器公布之间允许的最短时间间隔 (秒)。

**Advertise Lifetime(secs)** (公布使用寿命 [秒]) — 输入从接口发送的路由器公布的使用寿命 (秒)。这是公布的地址被主机视为有效路由器地址的最长时间。

**Preference Level** (优先级别) — 指定路由器作为默认路由器的优先级别 (与同一子网中的其它路由器相对)。数字越大的地址优先级越高。必须输入整数。

## 配置路由器发现

□□□ 打开 **Router Discovery Configuration**（路由器发现配置）页面。

□□□ 选择要配置的路由器接口。

□□□ 按需要配置其余字段的数据。

□□□ 单击 **Apply Changes**（应用更改）。

系统将保存指定的配置更改，并更新设备。

## 使用 CLI 命令配置路由器发现

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

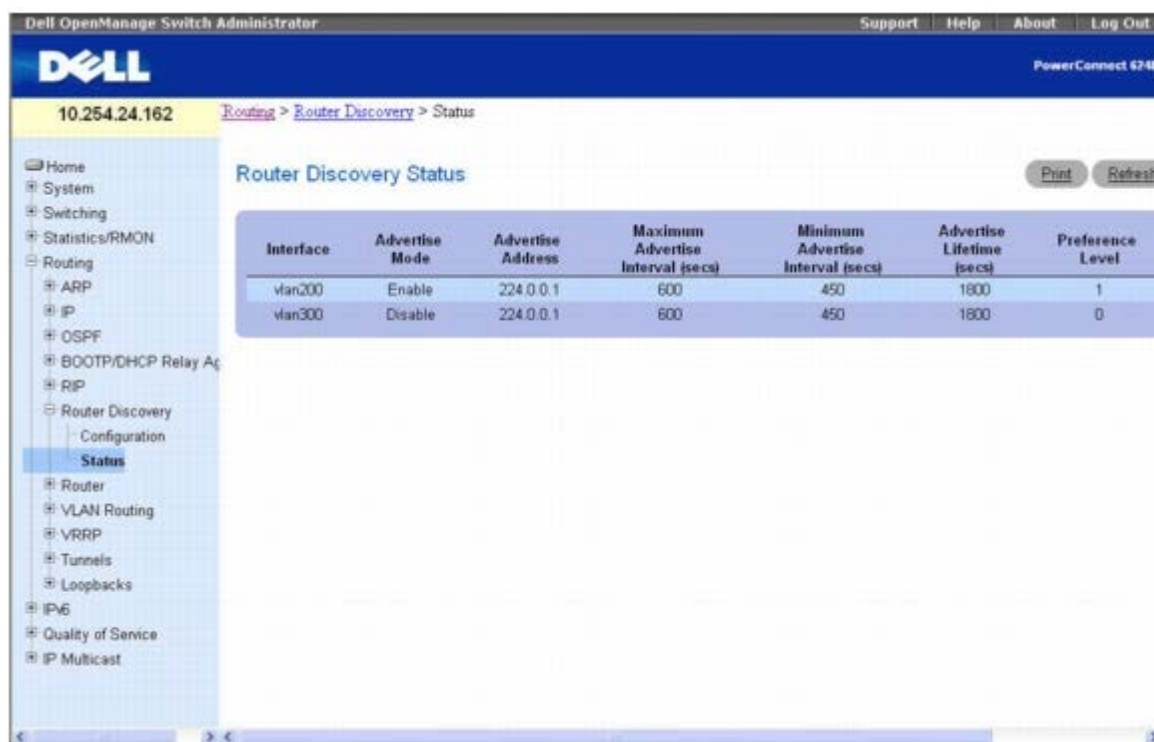
- 路由器搜索协议命令

## 路由器发现状态

**Router Discovery Status**（路由器发现状态）页面用于显示每个端口的路由器发现数据。

要显示此页面，请在树视图中单击 **Routing**（路由）® **Router Discovery**（路由器发现）® **Status**（状态）。

图 10-29. 路由器发现状态



Interface	Advertise Mode	Advertise Address	Maximum Advertise Interval (secs)	Minimum Advertise Interval (secs)	Advertise Lifetime (secs)	Preference Level
vlan200	Enable	224.0.0.1	600	450	1800	1
vlan300	Disable	224.0.0.1	600	450	1800	0

**Router Discovery Status**（路由器发现状态）页面显示了以下字段：

**Interface**（接口）— 显示其数据的路由器接口。

**Advertise Mode**（公布模式）— 值为 Enable（启用）或 Disable（禁用）。Enable（启用）表示在该接口上启用路由器发现。

**Advertise Address**（公布地址）— 用于公布路由器的 IP 地址。

**Maximum Advertise Interval(secs)**（最大公布间隔【秒】）— 从接口发送的路由器公布之间允许的最长时间间隔（秒）。

**Minimum Advertise Interval(secs)**（最小公布间隔【秒】）— 从接口发送的路由器公布之间允许的最短时间间隔（秒）。



**Advertise Lifetime(secs)** (公布使用寿命 [秒]) — 从接口发送的路由器公布的使用寿命 (秒)。这是公布的地址被主机视为有效路由器地址的最长时间。

**Preference Level** (优先级别) — 路由器作为默认路由器的优先级别 (与同一子网中的其它路由器相对)。数字越大的地址优先级越高。

## 使用 **CLI** 命令显示路由器搜索状态

有关执行此功能的 **CLI** 命令的信息，请参阅《*CLI 参考指南*》的以下章节：

- 路由器搜索协议命令

---

## 路由器

**Router** (路由器) 菜单页面包含用于配置和显示路由表的网页的链接。要显示此页面，请在树视图中单击 **Routing** (路由) ® **Router** (路由器)。在此菜单页面中可以访问以下网页：

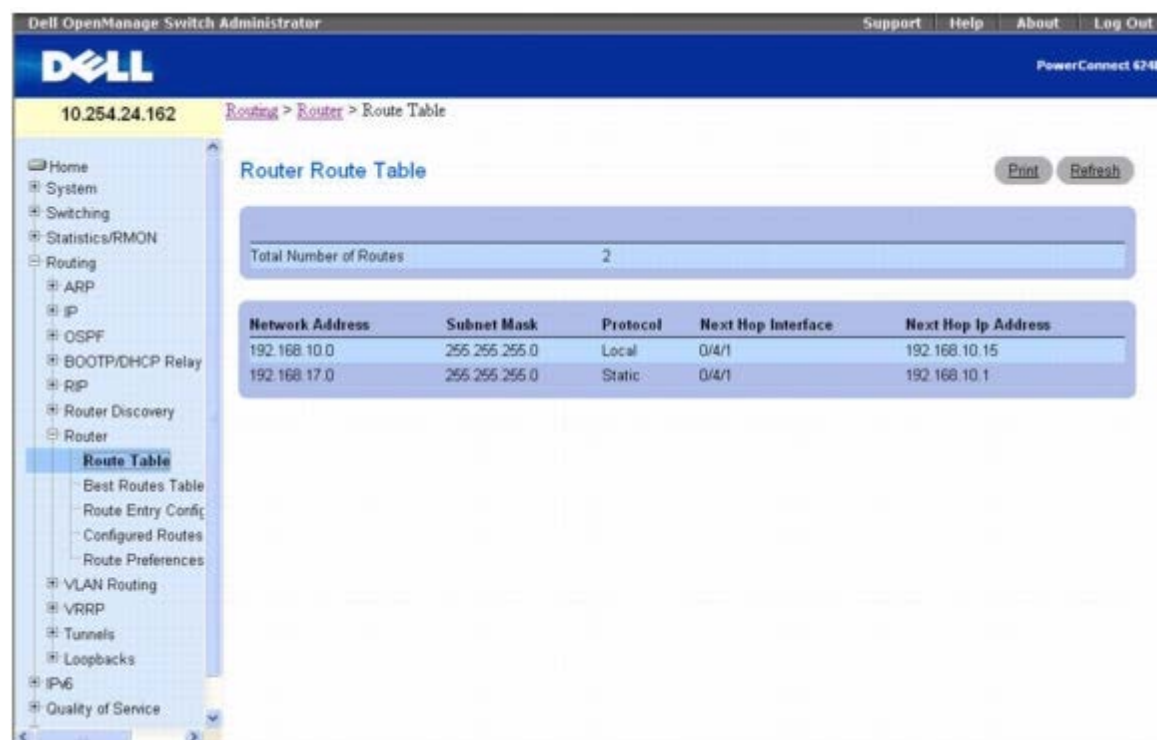
- [路由表](#)
- [最佳路由表](#)
- [路由条目配置](#)
- [配置的路由](#)
- [路由优先级配置](#)

## 路由表

**Router Route Table** (路由器路由表) 页面用于显示路由表配置。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **Router** (路由器) ® **Route Table** (路由表)。

图 10-30. 路由器路由表



**Router Route Table** (路由器路由表) 页面包含以下字段：

**Total Number of Routes** (路由总数) — 路由表中的路由总数。

**Network Address** (网络地址) — 目的地的 IP 路由前缀。

**Subnet Mask** (子网掩码) — 也称为子网/网络掩码，是指 IP 接口地址中用于标识所连网络的部分。

**Protocol** (协议) — 此字段指出哪些协议创建了指定的路由。可能的值包括：

- Local (本地)
- Static (静态)
- Default (默认)
- OSPF Intra (OSPF 域内)
- OSPF Inter (OSPF 域间)
- OSPF Type-1 (OSPF 类型 2)
- OSPF Type-2 (OSPF 类型 2)
- RIP

**Next Hop Interface** (下一跃距接口) — 转发通信量到目的地时使用的外发路由器接口。

**Next Hop IP Address** (下一跃距 IP 地址) — 转发通信量到目的地路径中的下一个路由器 (如果有) 时使用的外发路由器 IP 地址。下一个路由器必定是邻居或通往直接相连网络的本地接口 IP 地址。

## 使用 CLI 命令显示路由器路由表

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

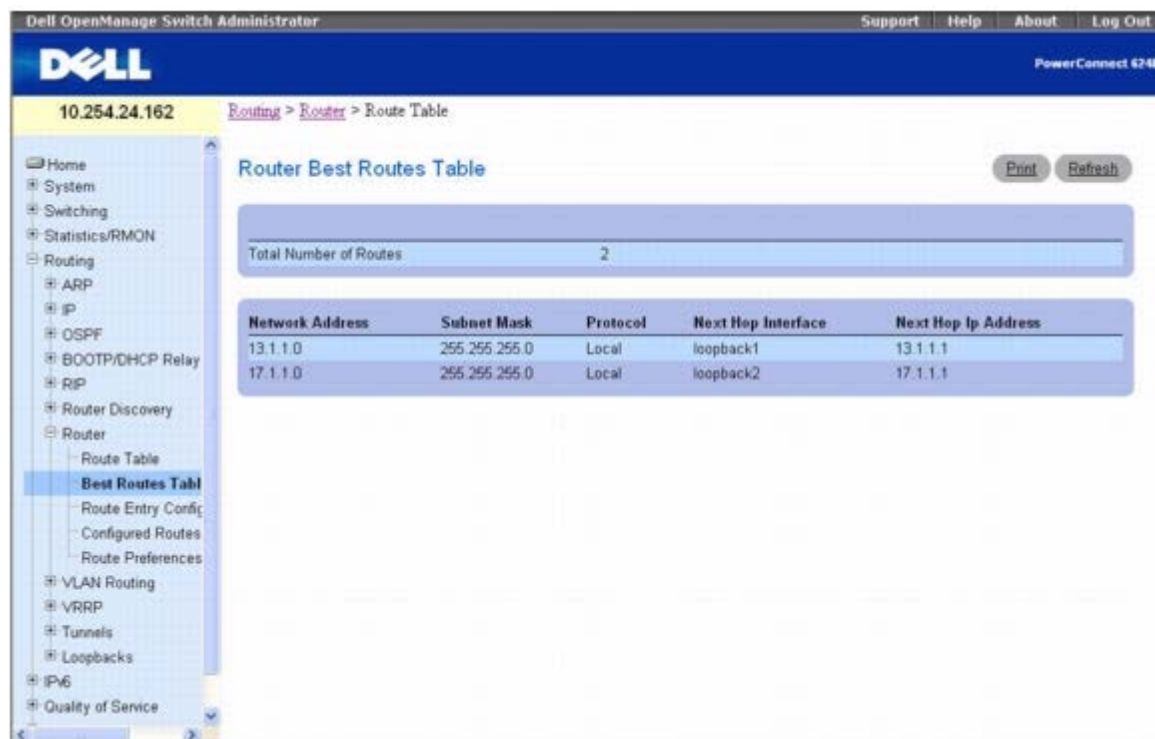
- IP 路由命令

## 最佳路由表

**Router Best Routes Table**（路由器最佳路由表）页面用于显示路由表中的最佳路由。

要显示此页面，请在树视图中单击 **Routing**（路由）**Router**（路由器）**Best Routes Table**（最佳路由表）。

图 10-31. 路由器最佳路由表



**Router Best Routes Table**（路由器最佳路由表）页面包含以下字段：

**Total Number of Routes**（路由总数）— 路由表中的路由总数。

**Network Address**（网络地址）— 目的地的 IP 路由前缀。

**Subnet Mask**（子网掩码）— 也称为子网/网络掩码，是指 IP 接口地址中用于标识所连网络的部分。

**Protocol**（协议）— 此字段指出哪些协议创建了指定的路由。可能的值包括：

- Local（本地）
- Static（静态）
- Default（默认）
- OSPF Intra（OSPF 域内）
- OSPF Inter（OSPF 域间）
- OSPF Type-1（OSPF 类型 2）
- OSPF Type-2（OSPF 类型 2）
- RIP

**Next Hop Interface**（下一跃距接口）— 转发通信量到目的地时使用的外发路由器接口。

**Next Hop IP Address**（下一跃距 IP 地址）— 转发通信量到目的地路径中的下一个路由器（如果有）时使用的外发路由器 IP 地址。下一个路由器必定是邻居或通往直接相连网络的本地接口 IP 地址。

## 使用 CLI 命令显示最佳路由表

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

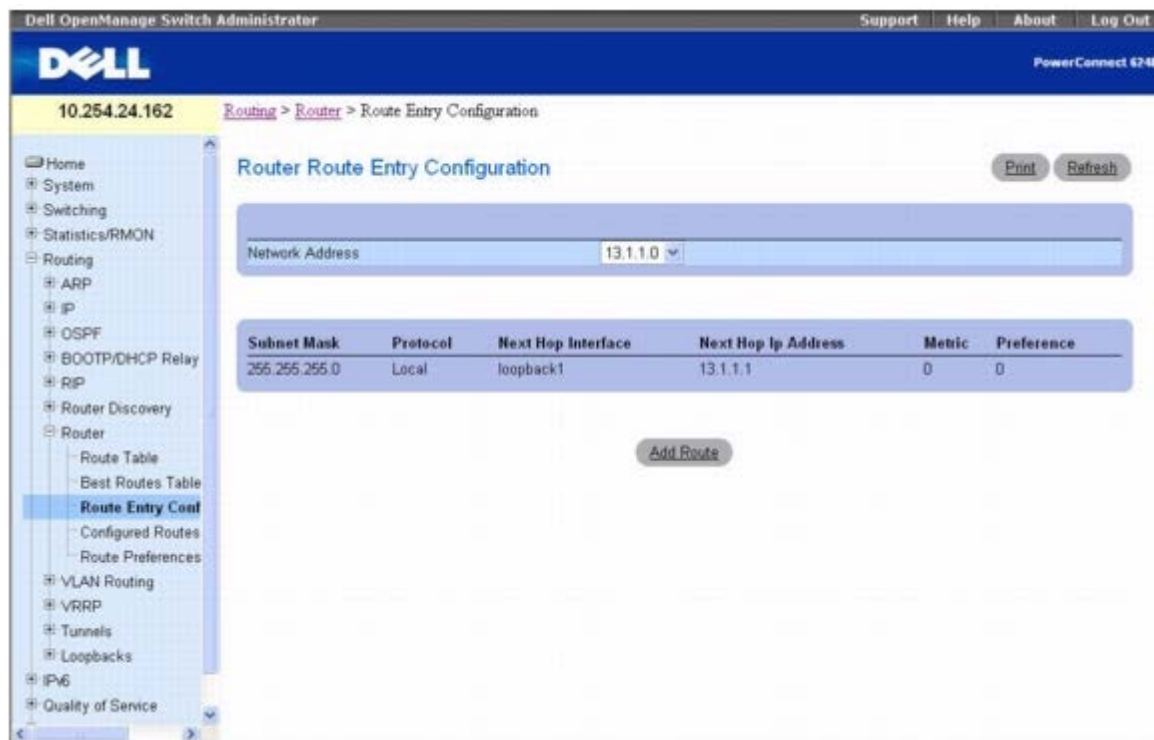
- IP 路由命令

## 路由条目配置

**Router Route Entry Configuration**（路由器路由条目配置）页面用于新增和配置路由器路由。

要显示此页面，请在树视图中单击 **Routing**（路由）⑥ **Router**（路由器）⑥ **Route Entry Configuration**（路由条目配置）。

图 10-32. 路由器路由条目配置



**Router Route Entry Configuration**（路由器路由条目配置）页面包含以下字段：

**Network Address**（网络地址）— 从下拉式菜单中选择目的地 IP 路由前缀。要创建路由，必须存在有效的路由接口，并且下一跃距 IP 地址与该路由接口必须位于同一网络上。路由接口在 **IP Interface Configuration**（IP 接口配置）页面中创建。可以在 **Route Table**（路由表）页面上查看有效的下一跃距 IP 地址。

**Subnet Mask**（子网掩码）— 也称为子网/网络掩码，是指 IP 接口地址中用于标识所连网络的部分。

**Protocol**（协议）— 此字段指出哪些协议创建了指定的路由。可能的值包括：

- Local（本地）
- Static（静态）
- Default（默认）
- OSPF Intra（OSPF 域内）
- OSPF Inter（OSPF 域间）
- OSPF Type-1（OSPF 类型 2）

- OSPF Type-2 (OSPF 类型 2)
- RIP

**Next Hop Interface** (下一跃距接口) — 转发通信量到目的地时使用的外发路由器接口。

**Next Hop IP Address** (下一跃距 IP 地址) — 转发通信量到目的地路径中的下一个路由器 (如果有) 时使用的外发路由器 IP 地址。下一个路由器必定是邻居或通往直接相连网络的本地接口 IP 地址。在创建路由时, 下一跃距 IP 地址与路由接口必须位于同一网络上。可以在 **Route Table** (路由表) 页面上查看有效的下一跃距 IP 地址。

**Metric** (跃点) — 到达目的地的路径管理成本。如果未输入值, 则使用默认值 1。范围是 0-255。此字段只在创建静态路由时显示。

**Preference** (首选项) — 为配置的下一跃距指定首选项值。

## 添加路由器路由

□□□ 打开 **Router Route Entry Configuration** (路由器路由条目配置) 页面。

□□□ 单击 **Add Route** (添加路由)。

屏幕将刷新, **Router Route Entry Configuration** (路由器路由条目配置) 页面会显示新的字段, 如 [图 10-33](#) 所示。

图 10-33. 添加路由 - 默认路由类型



The screenshot shows the 'Router Route Entry Configuration' page. At the top right, there are 'Print' and 'Refresh' buttons. Below them is a blue header bar. Underneath, there are two input fields: 'Route Type' with a dropdown menu set to 'Default', and 'Next Hop IP Address' with an empty text box. At the bottom, there are 'Cancel' and 'Apply Changes' buttons.

□□□ 在 **Route Type** (路由类型) 旁边, 使用下拉框添加 **Default** (默认) 路由或 **Static** (静态) 路由。

如果选择 **Static** (静态), 此页面会刷新, 并会显示新的字段, 如 [图 10-34](#) 所示。

**Default** (默认) — 在 **Next Hop IP Address** (下一跃距 IP 地址) 字段中输入默认的网关地址。

**Static** (静态) — 输入 **Network Address** (网络地址)、**Subnet Mask** (子网掩码)、**Next Hop IP Address** (下一跃距 IP 地址) 和 **Preference** (首选项)。

图 10-34. 路由条目配置 - 添加静态路由类型



The screenshot shows the 'Router Route Entry Configuration' page after selecting 'Static' for the route type. The 'Route Type' dropdown is now set to 'Static'. Below it, there are four input fields: 'Network Address', 'Subnet Mask', 'Next Hop IP Address', and 'Preference' with a value of '1' and a range '(1 to 255)' indicated. The 'Apply Changes' button is highlighted.

□□□ 单击 **Apply Changes** (应用更改)。

系统将会添加新路由, 并打开 **Configured Routes** (配置的路由) 页面。

## 使用 CLI 命令添加路由器路由

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

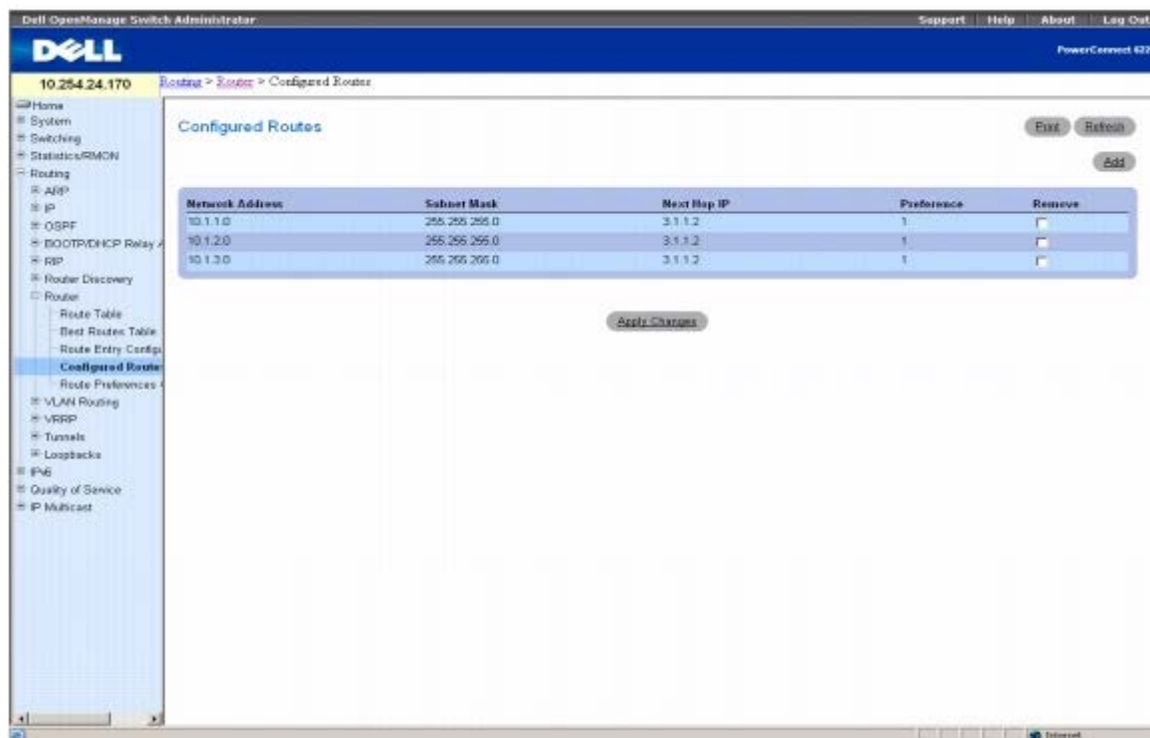
- IP 路由命令

## 配置的路由

**Configured Routes**（配置的路由）页面用于显示已经配置的路由。

要显示此页面，请在树视图中单击 **Routing**（路由）**Router**（路由器）**Configured Routes**（配置的路由）。

图 10-35. 配置的路由



**Configured Routes**（配置的路由）页面会显示以下字段：

**Network Address**（网络地址）— 目的地的 IP 路由前缀。

**Subnet Mask**（子网掩码）— 也称为子网/网络掩码，是指 IP 接口地址中用于标识所连网络的部分。

**Next Hop IP**（下一跃距 IP）— 转发通信量到目的地时使用的外发路由器 IP 地址。

**Preference**（首选项）— 显示为添加的路由所配置的首选项。

**Remove**（删除）— 使用此复选框可删除配置的路由。

## 添加路由器路由

□□□ 打开 **Configured Routes**（配置的路由）页面。

□□□ 单击 **Add**（添加）。

**Router Route Entry Configuration**（路由器路由条目配置）页面将会显示，如[图 10-33](#) 所示。

□□□ 在 **Route Type**（路由类型）旁边，使用下拉框添加 **Default**（默认）路由或 **Static**（静态）路由。

**Default**（默认）— 在 **Next Hop IP Address**（下一跃距 IP 地址）字段中输入默认的网关地址。[图 10-33](#) 显示了当 **Route Type**（路由类型）值为默认值时显示的字段。

**Static**（静态）— 输入 **Network Address**（网络地址）、**Subnet Mask**（子网掩码）、**Next Hop IP Address**（下一跃距 IP 地址）和 **Preference**（首选项）。[图 10-34](#) 显示了当 **Route Type**（路由类型）值为 **Static**（静态）时显示的字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将会添加新路由，并且返回到 **Configured Routes**（配置的路由）页面。

## 使用 CLI 命令显示配置的路由

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- IP 路由命令

## 路由优先级配置

**Router Route Preferences Configuration**（路由器路由优先级配置）页面用于配置每个协议的默认优先级（例如静态路由为 60）。取值的范围为 1 到 255，并且独立于路由跃点。大多数路由协议使用路由跃点来确定协议已知的最短路径，与任何其他协议无关。

通过选择优先级值最小的路由，可选择到目的地的最佳路由。当存在多个到目的地的路由时，可使用优先级值来确定首选路由。如果优先级值相同，则选择具有最佳路由跃点的路由。为避免出现跃点不匹配的问题（即 RIP 和 OSPF 跃点不能直接相比），必须为每个协议配置不同的优先级值。

要显示此页面，请在树视图中单击 **Routing**（路由）**Router**（路由器）**Route Preferences Configuration**（路由优先级配置）。

图 10-36. 路由器路由优先级配置

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "Router Route Preferences Configuration". It contains a table with the following data:

Local	0	
Static	1	(1 to 255)
OSPF Intra	8	(1 to 255)
OSPF Inter	10	(1 to 255)
OSPF Type-1	13	(1 to 255)
OSPF Type-2	150	(1 to 255)
RIP	15	(1 to 255)

Below the table is an "Apply Changes" button. The left sidebar shows a navigation tree with "Route Preference" selected under the "Router" category.

**Router Route Preferences Configuration**（路由器路由优先级配置）页面包含以下字段：

**Local**（本地）— 此字段显示本地路由优先级值。



**Static**（静态）— 路由器中的静态路由优先级值。默认值为 1。范围是 1 至 255。

**OSPF Intra**（OSPF 域内）— 路由器中的 OSPF 域内路由优先级值。默认值为 8。范围为 1 到 255。OSPF 规范 (RFC 2328) 要求必须按以下顺序向通过 OSPF 获取的路由指定优先级：域内 < 域间 < 类型 1 < 类型 2。

**OSPF Inter**（OSPF 域间）— 路由器中的 OSPF 域间路由优先级值。默认值为 10。范围为 1 到 255。OSPF 规范 (RFC 2328) 要求必须按以下顺序向通过 OSPF 获取的路由指定优先级：域内 < 域间 < 类型 1 < 类型 2。

**OSPF Type-1**（OSPF 类型 1）— 路由器中的 OSPF 类型 1 路由优先级值。默认值为 13。范围为 1 到 255。OSPF 规范 (RFC 2328) 要求必须按以下顺序向通过 OSPF 获取的路由指定优先级：域内 < 域间 < 类型 1 < 类型 2。

**OSPF Type-2**（OSPF 类型 2）— 路由器中的 OSPF 类型 2 路由优先级值。默认值为 150。范围为 1 到 255。OSPF 规范 (RFC 2328) 要求必须按以下顺序向通过 OSPF 获取的路由指定优先级：域内 < 域间 < 类型 1 < 类型 2。

**RIP** — 路由器中的 RIP 路由优先级值。默认值为 15。范围是 1 至 255。

## 配置路由优先级

□□□ 打开 **Route Preferences Configuration**（路由优先级配置）页面。

□□□ 在此页面中定义适当的字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将配置路由优先级，并更新设备。

## 使用 CLI 命令配置路由优先级

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- OSPF 命令

---

## VLAN 路由

配置 6200 系列软件时，可以让一些 VLAN 支持路由。也可以另一种方式配置软件，使得在处理 VLAN 上的通信量时，将 VLAN 作为一个路由器端口处理。

当端口以桥接（默认值）而非路由的方式启用时，将对入站信息包执行所有正常的网桥处理，然后与 VLAN 相关联。端口 MAC 目的地地址 (MAC DA) 和 VLAN ID 用于搜索 MAC 地址表。如果 VLAN 启用了路由，并且入站单点传送信息包以内部网桥路由器接口为 MAC DA，则会路由该信息包。入站多点传送信息包将转发到 VLAN 中的所有端口，如果接收的 VLAN 是一个路由的 VLAN，信息包还会转发到内部网桥路由器接口。

由于一个端口可以配置为属于多个 VLAN，因此可以为该端口上的所有 VLAN 或只为该端口上的某些 VLAN 启用 VLAN 路由。VLAN 路由可将多个物理端口设于同一个子网中。当 VLAN 覆盖多个物理网络，或者需要进一步分区或设置更高安全级别时，也可以使用 VLAN 路由。本节介绍如何配置 6200 系列软件来支持 VLAN 路由。一个端口可以用作 VLAN 端口或路由器端口，但不能同时用作两者。不过，VLAN 端口所属的 VLAN 本身可以用作一个路由器端口。

**VLAN Routing**（VLAN 路由）菜单页面包含用于显示 VLAN 路由参数和数据的网页的链接。要显示此页面，请在树视图中单击 **Routing**（路由）® **VLAN Routing**（VLAN 路由）。在此菜单页面中可以访问以下网页：

- [VLAN 路由摘要](#)

## VLAN 路由摘要

**VLAN Routing Summary**（VLAN 路由摘要）页面用于显示系统上配置的 VLAN 路由接口的有关信息。

要显示此页面，请在树视图中单击 **Routing**（路由）® **VLAN Routing**（VLAN 路由）® **Summary**（摘要）。

图 10-37. VLAN 路由摘要



**VLAN Routing Summary**（VLAN 路由摘要）页面会显示以下字段：

**VLAN ID** — 其数据显示在当前表格行中的 VLAN 的 ID。

**MAC Address**（MAC 地址）— 分配给 VLAN 路由接口的 MAC 地址。

**IP Address**（IP 地址）— 为 VLAN 路由接口配置的 IP 地址。请注意，如果创建了 VLAN 但未配置 IP 地址，则该页面默认显示 IP 地址 0.0.0.0。要配置 IP 地址，请转至 **IP** ® **Interface Configuration**（接口配置）。

**Subnet Mask**（子网掩码）— 为 VLAN 路由接口配置子网掩码。第一次配置 VLAN 路由接口时该值为 0.0.0.0，必须在 IP Interface Configuration（IP 接口配置）页面上输入。

## 使用 CLI 命令显示 VLAN 路由摘要

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- IP 寻址命令
- 虚拟 LAN 路由命令

## VRRP

在默认路由器失败时，虚拟路由器冗余协议提供了动态选择备份路由器的方案。这样做的目标是尽量缩短由于默认网关路由器失败的“黑洞”期。在“黑洞”期间，发送给路由器的所有通信量都会丢失，直到失败被检测到为止。虽然通常采用默认的静态路由配置，但如果默认路由器失败，这种方法很容易受到单一失败点的影响。VRRP 提倡“虚拟路由器”的概念。虚拟路由器与一个或多个用作默认网关的 IP 地址相关联。如果控制这些 IP 地址的 VRRP 路由器（以前称为“主路由器”）失败，IP 地址组和默认转发角色将由备份 VRRP 路由器接管。

**VRRP** 菜单页面包含用于配置和显示参数和数据的网页链接。要显示此页面，请在树视图中单击 **Routing**（路由）® **VRRP**。在此菜单页面中可以访问以下网页：

- [VRRP 配置](#)
- [虚拟路由器配置](#)

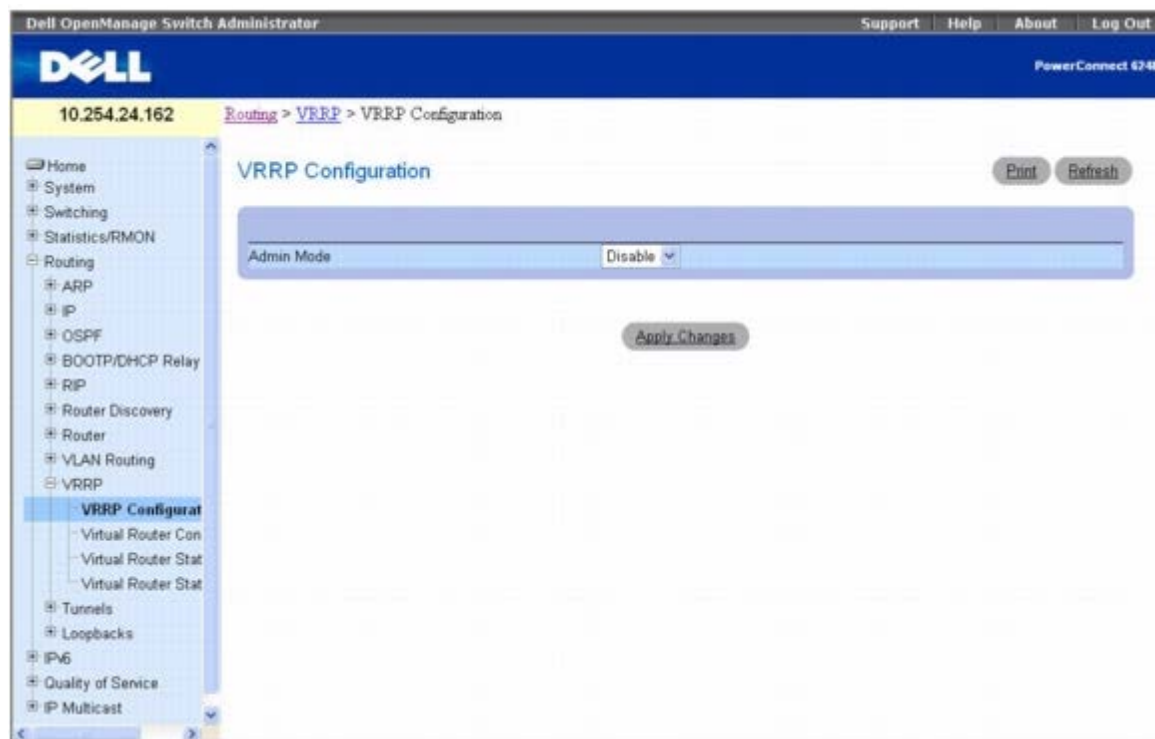
- [虚拟路由器状态](#)
- [虚拟路由器统计数据](#)

## VRRP 配置

**VRRP Configuration** (VRRP 配置) 页面用于启用或禁用虚拟路由器的管理状态。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **VRRP** ® **VRRP Configuration** (VRRP 配置)。

图 10-38. VRRP 配置



**VRRP Configuration** (VRRP 配置) 页面包含以下字段：

**Admin Mode** (管理模式) — 将路由器中 VRRP 的管理状态设置为活动或非活动。从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用)。默认值为 **Disable** (禁用)。

### 使用 CLI 命令更改 VRRP 状态

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

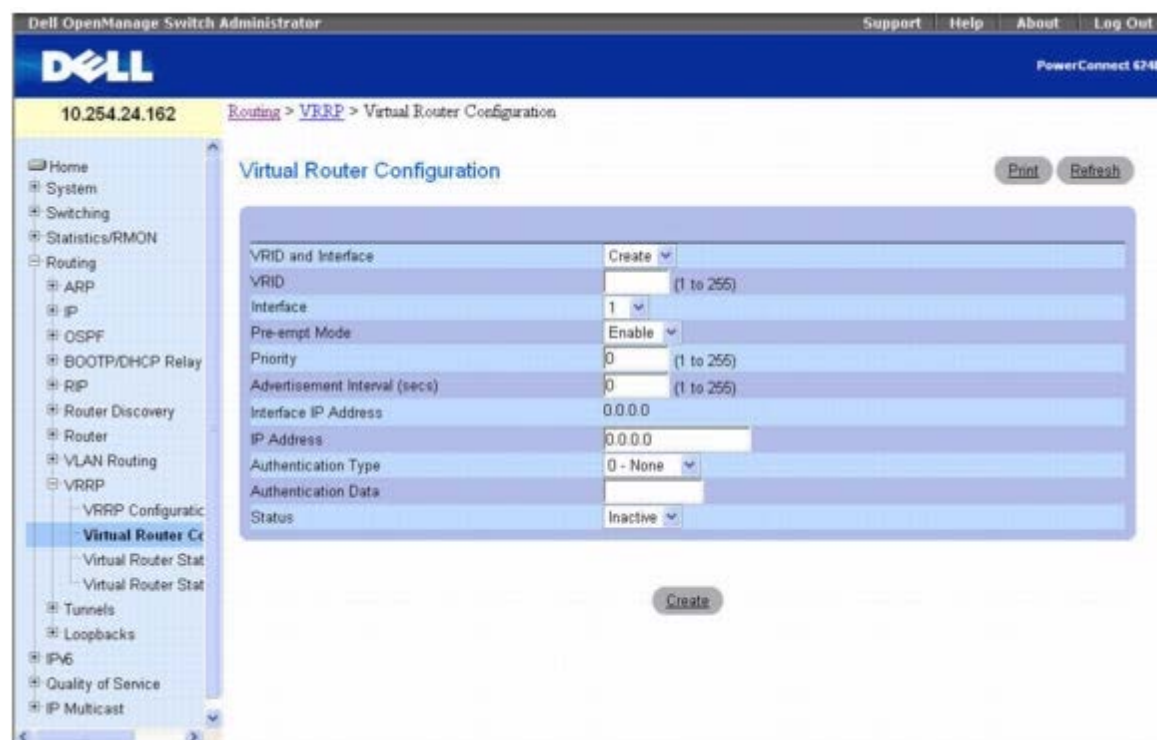
- [虚拟路由器冗余协议命令](#)

## 虚拟路由器配置

**Virtual Router Configuration** (虚拟路由器配置) 页面可用于创建新的虚拟路由器或配置现有路由器。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **VRRP** ® **Virtual Router Configuration** (虚拟路由器配置)。

图 10-39. 虚拟路由器配置



**Virtual Router Configuration** (虚拟路由器配置) 页面包含以下字段：

**VRID and Interface** (VRID 和接口) — 从下拉式菜单中选择 **Create** (创建) 以配置新的虚拟路由器，或从按接口编号和 VRID 列出的现有虚拟路由器中选择一个。

**VRID** — 此字段仅在创建新的虚拟路由器时才可配置，在这种情况下可以输入范围为 1 到 255 的 VRID。

**Interface** (接口) — 此字段仅在创建新的虚拟路由器时才可配置，在这种情况下可从下拉式菜单中选择新虚拟路由器的接口。

**Pre-empt Mode** (抢先模式) — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用)。选择 **Enable** (启用) 后，如果备份路由器的优先级大于主路由器的优先级，并且主路由器的 IP 地址并非该虚拟路由器的 IP 地址，则备份路由器会取代主路由器。默认值为 **Enable** (启用)。

**Priority** (优先级) — 输入 VRRP 路由器用来选择主虚拟路由器的优先级值。如果虚拟路由器 IP 地址与接口 IP 地址相同，则无论输入何值，优先级值都会调整为 255。如果虚拟路由器 IP 地址与接口 IP 地址不相同，并输入 255 的优先级，则优先级值将调整为默认值 100。

**Advertisement Interval(secs)** (公布间隔 [秒]) — 输入此虚拟路由器发送公布信息包的时间间隔 (秒)。请入 1 到 255 的数字，默认值为 1 秒。

**Interface IP Address** (接口 IP 地址) — 表示与所选接口关联的 IP 地址。

**IP Address** (IP 地址) — 输入与虚拟路由器关联的 IP 地址。默认值为 0.0.0.0，必须在按 **Create** (创建) 之前更改此值。

**Authentication Type** (验证类型) — 从下拉式菜单中选择虚拟路由器的验证类型。默认值为 **None** (无)。选项包括：

- **0-None** (无) — 不执行验证。
- **1-Simple** (简单) — 使用文本密码执行验证。

**Authentication Data** (验证数据) — 如果选择了简单验证，请输入密码。

**Status** (状态) — 从下拉式菜单中选择活动或非活动，以开始或停止使用虚拟路由器。默认值为非活动。

如果要配置次 VRRP 地址，请先为虚拟路由器配置一个 IP 地址 (主地址)。然后可以添加多个次地址到该接口。

## 创建新的虚拟路由器

□□□ 打开 **Virtual Router Configuration** (虚拟路由器配置) 页面。

□□□ 从 VRID and Interface (VRID 和接口) 下拉式菜单中选择 **Create** (创建)。

□□□ 指定新虚拟路由器的 **VRID** 和接口。

□□□ 按需要定义其余字段。

□□□ 单击 **Create**（创建）。

系统将保存新的虚拟路由器，并更新设备。

## 配置虚拟路由器

□□□ 打开 **Virtual Router Configuration**（虚拟路由器配置）页面。

□□□ 选择虚拟路由器的 **VRID** 和接口进行配置。

□□□ 按需要更改字段。

□□□ 单击 **Apply Changes**（应用更改）。

系统将保存配置，并更新设备。

## 使用 **CLI** 命令配置虚拟路由器

有关执行此功能的 **CLI** 命令的信息，请参阅《**CLI** 参考指南》的以下章节：

- 虚拟路由器冗余协议命令

## 虚拟路由器状态

**Virtual Router Status**（虚拟路由器状态）页面用于显示虚拟路由器状态。

要显示此页面，请在树视图中单击 **Routing**（路由）® **VRRP**® **Virtual Router Status**（虚拟路由器状态）。

图 10-40. 虚拟路由器状态

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb navigation is 'Routing > VRRP > Virtual Router Status'. The page title is 'Virtual Router Status'. There are 'Print' and 'Refresh' buttons. A table displays the status of two VRRP instances:

VRID	VLANID	Priority	Preempt Mode	Advertisement Interval(secs)	Virtual Ip Address	Interface Ip Address	Owner	VMAC Address
20	vlan200	4	Enable	1	10.50.50.50	192.168.30.15	False	00:00:5E:00:01:00
110	vlan300	60	Disable	30	10.50.50.52	0.0.0.0	False	00:00:5E:00:01:00

Virtual Router Status (虚拟路由器状态) 页面会显示以下字段：

**VRID** — 虚拟路由器标识符。

**VLANID** - 表示与 VRID 关联的接口。

**Priority** (优先级) — VRRP 路由器用来选择主虚拟路由器的优先级值。

抢先模式

- **Enable** (启用) — 如果虚拟路由器是备份路由器，并且其优先级大于主虚拟路由器的优先级，而主虚拟路由器的 IP 地址并非该虚拟路由器的 IP 地址，则它会取代主路由器。
- **Disable** (禁用) — 如果虚拟路由器是备份路由器，即使其优先级更高，也不会取代主路由器。

**Advertisement Interval(secs)** (公布间隔 [秒]) — 此虚拟路由器发送公布信息包的时间间隔 (秒)。

**Virtual IP Address** (虚拟 IP 地址) — 与虚拟路由器关联的 IP 地址。

**Interface IP Address** (接口 IP 地址) — 与虚拟路由器使用的接口相关联的实际 IP 地址。

**Owner** (所有者) — 如果虚拟 IP 地址与接口 IP 地址相同，将设置为 True (真)，否则设置为 False (假)。如果此参数设置为 True (真)，则虚拟路由器是虚拟 IP 地址的所有者，并且在其活动时始终成为主路由器的首选。

**VMAC Address** (VMAC 地址) — 与虚拟路由器关联的虚拟 MAC 地址，包括一个组织内唯一的 24 位标识符、一个标识 VRRP 地址块的 16 位常数和一个 8 位 VRID。虚拟 MAC 地址的形式为 00:00:5e:00:01:XX，其中 XX 是 VRID。

**Auth Type** (验证类型) — 用于虚拟路由器的验证类型。

- None (无) — 指定验证类型为无。
- Simple (简单) — 指定验证类型为简单文本密码。

**State** (工作模式) — 虚拟路由器的当前工作模式：

- Initialize (初始化)
- Master (主)
- Backup (备份)



**Status** (状态) — 虚拟路由器的当前状态：

- Inactive (非活动)
- Active (活动)

**Secondary IP Address** (次 IP 地址) — 为主 VRRP 配置的次 VRRP 地址。

## 使用 CLI 命令显示路由器状态

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 虚拟路由器冗余协议命令

## 虚拟路由器统计数据

**Virtual Router Statistics** (虚拟路由器统计数据) 页面用于显示指定虚拟路由器的统计数据。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **VRRP** ® **Virtual Router Statistics** (虚拟路由器统计数据)。

图 10-41. 虚拟路由器统计数据

Virtual Router Statistics	
Router Checksum Errors	0
Router Version Errors	0
Router VRID Errors	0
VRID and VLAN ID	20 - vlan200
VRID	20
VLAN ID	vlan200
Up Time	0 days 0 hrs 32 mins 40 secs
State Transitioned to Master	1
Advertisement Received	1834
Advertisement Interval Errors	0
Authentication Failure	0
IP TTL Errors	0
Zero Priority Packets Received	0
Zero Priority Packets Sent	0
Invalid Type Packets Received	0
Address List Errors	0
Invalid Authentication Type	0
Authentication Type Mismatch	0
Packet Length Errors	0

**Virtual Router Statistics** (虚拟路由器统计数据) 页面包括以下字段。其中许多字段仅在 VRRP 配置有效时才会显示。

**Router Checksum Errors** (路由器校验和错误) — 所收到的 VRRP 信息包中，具有无效 VRRP 校验和值的总数。

**Router Version Errors** (路由器版本错误) — 所收到的 VRRP 信息包中，具有未知或不受支持的版本号的总数。

**Router VRID Errors** (路由器 VRID 错误) — 所收到的 VRRP 信息包中，其 VRID 对此虚拟路由器无效的总数。

**VRID and VLAN ID (VRID 和 VLAN ID)** — 从按接口编号和 VRID 列出的现有虚拟路由器列表中，选择要显示其统计信息的虚拟路由器。



**VRID** — 所选虚拟路由器的 VRID。

**VLAN ID** — 所选虚拟路由器的接口。

**Up Time** (运行时间) — 自从虚拟路由器过渡到初始化状态后所经过的时间，以天数、小时数、分钟数和秒钟数表示。

**State Transitioned to Master** (工作模式过渡到主路由器) — 此虚拟路由器过渡到主路由器模式的总次数。

**Advertisement Received** (收到的公布) — 此虚拟路由器收到的 VRRP 公布总数。

**Advertisement Interval Errors** (公布间隔错误) — 所收到的 VRRP 公布信息包中，其公布间隔不同于为本地虚拟路由器配置的公布间隔的总数。

**Authentication Failure** (验证失败) — 所收到的 VRRP 信息包中，未通过验证检查的总数。

**IP TTL Errors** (IP TTL 错误) — 虚拟路由器收到的 VRRP 信息包中，IP TTL (生存时间) 不等于 255 的总数。

**Zero Priority Packets Received** (收到的零优先级信息包) — 虚拟路由器收到的 VRRP 信息包中，优先级为 0 的总数。

**Zero Priority Packets Sent** (发送的零优先级信息包) — 虚拟路由器发送的 VRRP 信息包中，优先级为 0 的信息包总数。

**Invalid Type Packets Received** (收到的无效类型信息包) — 虚拟路由器收到的 VRRP 信息包中，Type (类型) 字段为无效值的总数。

**Address List Errors** (地址列表错误) — 所收到的信息包中，其地址列表与虚拟路由器本地配置的地址列表不匹配的总数。

**Invalid Authentication Type** (无效的验证类型) — 所收到的信息包中，验证类型未知的总数。

**Authentication Type Mismatch** (验证类型不匹配) — 所收到的信息包中，其验证类型不同于本地配置的验证方法的总数。

**Packet Length Errors** (信息包长度错误) — 所收到的信息包中，其长度小于 VRRP 标头长度的信息包总数。

## 显示虚拟路由器统计数据

打开 **Virtual Router Statistics** (虚拟路由器统计数据) 页面。

从 **VRID** and **VLANID** (**VRID** 和 **VLANID**) 字段中选择要显示其统计信息的虚拟路由器。此信息仅在 VRRP 配置有效时才会显示。

## 使用 CLI 命令显示虚拟路由器统计数据

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- [虚拟路由器冗余协议命令](#)

---

## 通道

6200 系列可创建、删除和管理通道接口。这些是通过用户配置创建和删除的动态接口。

有两类通道用于简化从 IPv4 网络到 IPv6 网络的过渡：配置的通道和自动通道。区别在于，配置的通道使用通道的目的地或端点明确配置。而自动通道则不同，它使用路由到通道中的信息包的目的地地址推断通道的端点。

6200 系列支持点对点通道。点对点接口只提供基于接口的路由（无需指定明确的下一跃距地址），并允许定义未编号的接口。

**Tunnels** (通道) 菜单页面包含用于配置和显示通道参数和数据的网页的链接。要显示此页面，请在树视图中单击 **Routing** (路由) ® **Tunnels** (通道)。在此菜单页面中可以访问以下网页：

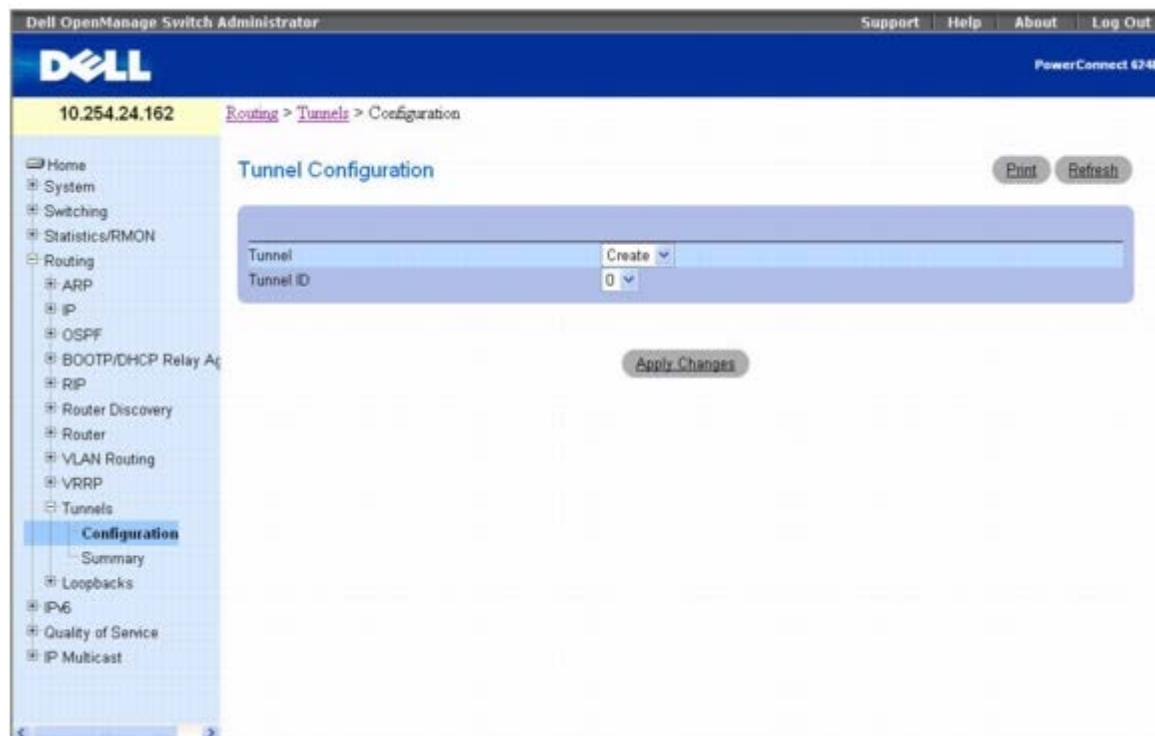
- [通道配置](#)
- [通道摘要](#)

## 通道配置

**Tunnels Configuration**（通道配置）页面用于创建、配置或删除通道。

要显示此页面，请在树视图中单击 **Routing**（路由）® **Tunnels**（通道）® **Configuration**（配置）。

图 10-42. 通道配置



**Tunnels Configuration**（通道配置）页面包含以下字段：

**Tunnel**（通道）— 使用下拉式菜单从当前配置的通道 ID 列表中选择。如果创建的通道接口数尚未达到最大数，则 **Create**（创建）也会包含在选项之中。

**Tunnel ID**（通道 ID）— 从通道选择器中选择 **Create**（创建）时，就会显示可用的通道 ID 列表。必须选择一个通道 ID 以与新建的通道关联，并单击 **Apply Changes**（应用更改），页面上的其余字段然后才会显示。

**Mode**（模式）— 通道模式的选择器。IPv6-in-IPv4 是唯一支持的模式。

**Link Local Only Mode**（仅链路本地模式）— 使用链路本地地址在此接口上启用 IPv6。只有在尚未指定明确的 IPv6 地址的情况下，才可配置此选项。

**IPv6 Address**（IPv6 地址）— 为所选的通道接口选择 IPv6 地址。如果配置的地址未达到最大数目，则有效的选项将包括 **Add**（添加）。

**IPv6 Address**（IPv6 地址）— 从 IPv6 Address（IPv6 地址）选择器中选择 **Add**（添加）时，此 IPv6 地址输入字段将会显示。地址必须以前缀/长度的格式输入。

也可以选择指定 64 位扩展唯一标识符（EUI-64）。

**Source**（来源）— 选择所需的来源：IPv4 Address（IPv4 地址）或 Interface（接口）。如果选择 **Address**（地址），则必须以点分十进制表示法输入此通道的来源地址。如果选择 **Interface**（接口），则必须选择此通道的来源接口。与所选接口关联的地址用作来源地址。

**Destination Address**（目的地地址）— 此通道的 IPv4 目的地地址（点分十进制表示法）。

## 创建新通道

□□□ 打开 **Tunnels Configuration**（通道配置）页面。

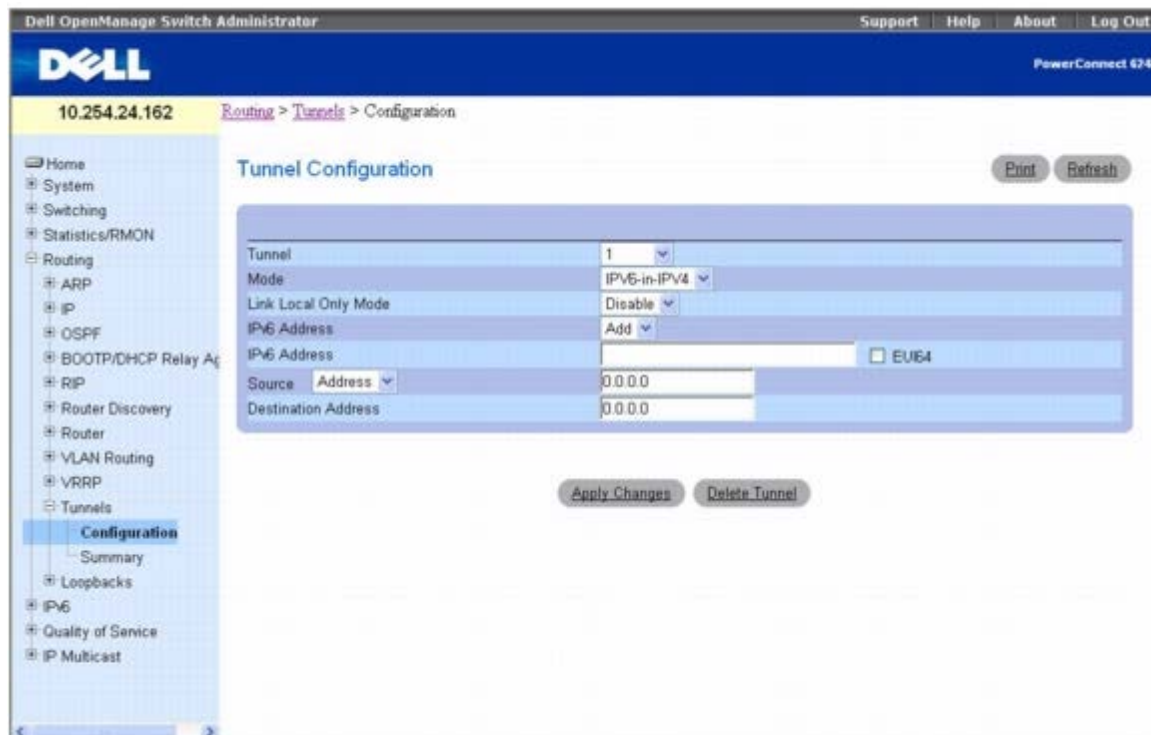
□□□ 从 **Tunnel**（通道）下拉式菜单中选择 **Create**（创建）。

□□□ 在 **Tunnel ID**（通道 ID）字段中指定要使用的 ID。

□□□ 单击 **Apply Changes**（应用更改）。

系统将会删除 Tunnel ID（通道 ID）字段，并显示其余的通道字段。

图 10-43. 通道配置 - 输入项



□□□ 根据需要配置字段。

□□□ 在其余字段中输入所需的值。

□□□ 单击 **Apply Changes**（应用更改）。

系统将保存新通道，并更新设备。

## 修改现有通道

□□□ 打开 **Tunnels Configuration**（通道配置）页面。

□□□ 在 **Tunnel**（通道）下拉式菜单中指定要修改的通道。

□□□ 根据需要更改其余字段中的值。

□□□ 单击 **Apply Changes**（应用更改）。

系统将保存新配置，并更新设备。

## 删除通道

□□□ 打开 **Tunnels Configuration**（通道配置）页面。

□□□ 在 **Tunnel**（通道）下拉式菜单中指定要删除的通道。

□□□ 单击 **Delete Tunnel**（删除通道）。

系统将删除该通道，并更新设备。

## 使用 CLI 命令配置通道

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

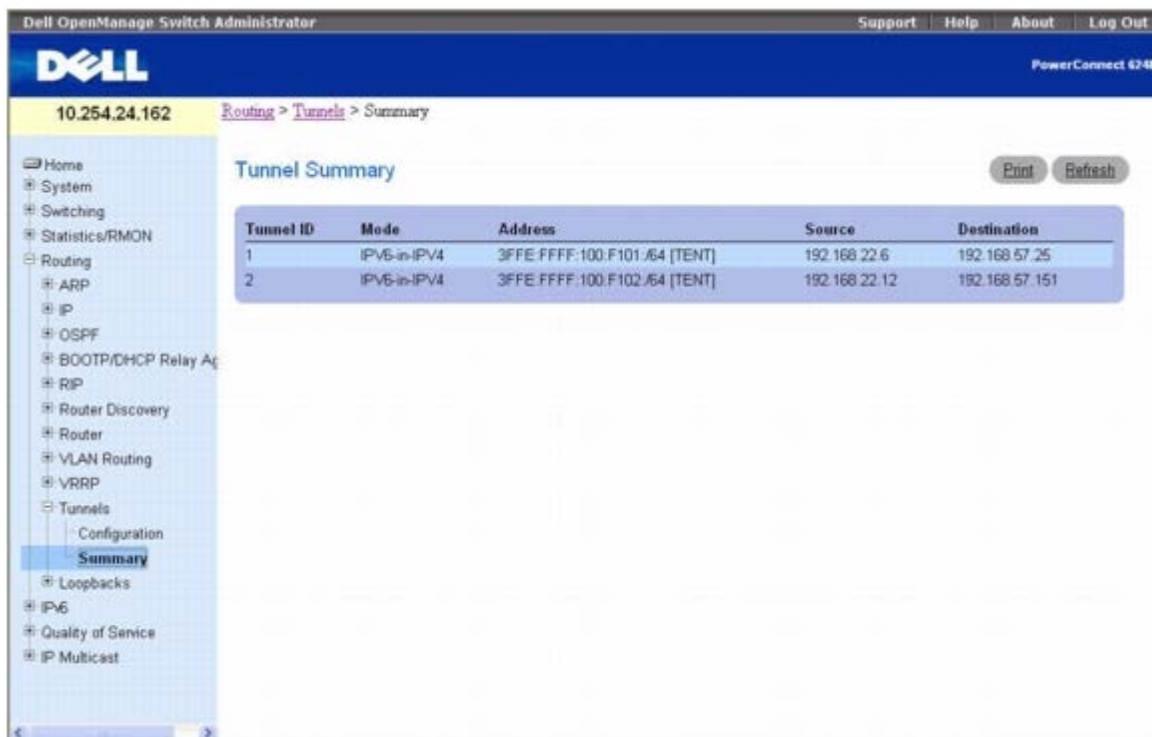
- 通道接口命令

## 通道摘要

**Tunnels Summary**（通道摘要）页面用于显示已配置通道的摘要。

要显示此页面，请在树视图中单击 **Routing**（路由）® **Tunnels**（通道）® **Summary**（摘要）。

图 10-44. 通道摘要



**Tunnels Summary**（通道摘要）页面包含以下字段：

**Tunnel ID**（通道 ID）— 通道的 ID。

**Mode**（模式）— 通道的对应模式。

**Address**（地址）— 通道的 IPv6 地址。

**Source**（来源）— 对应的通道来源地址。如果已配置接口，则接口和地址都会显示。如果来源接口尚未配置地址，则文本 'unconfigured'（未配置）会显示在地址的位置。

**Destination**（目的地）— 对应的通道目的地地址。

## 使用 CLI 命令显示通道摘要

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 通道接口命令

## 回送

6200 系列可创建、删除和管理回送接口。它们是通过用户配置创建和删除的动态接口。6200 系列支持多个回送接口。

回送接口设置为始终运行。因此，它可用于为其它交换机所引用的设备配置一个稳定的 IP 地址。此接口为发送的信息包提供来源地址，并且可以接收本地和远程信息包。它通常由路由协议所使用。

回送的作用方式与交换系统中的网络端口不一样。特别地，回送接口没有邻居。它是一个虚拟设备，用于分配本地地址，以便能够使用此地址与路由器通信。该地址始终运行，并可接收来自任何现有活动接口的通信量。因此，只要可从远程客户端访问回送地址，该地址便可用于通过各种服务（例如 telnet 和 ssh）与路由器通信。这样，在接收信息包的处理方面，回送地址与路由器的本地地址有着相同的表现。

**Loopbacks** (回送) 菜单页面包含用于配置和显示回送参数和数据的网页链接。要显示此页面，请在树视图中单击 **Routing** (路由) ® **Loopbacks** (回送)。在此菜单页面中可以访问以下网页：

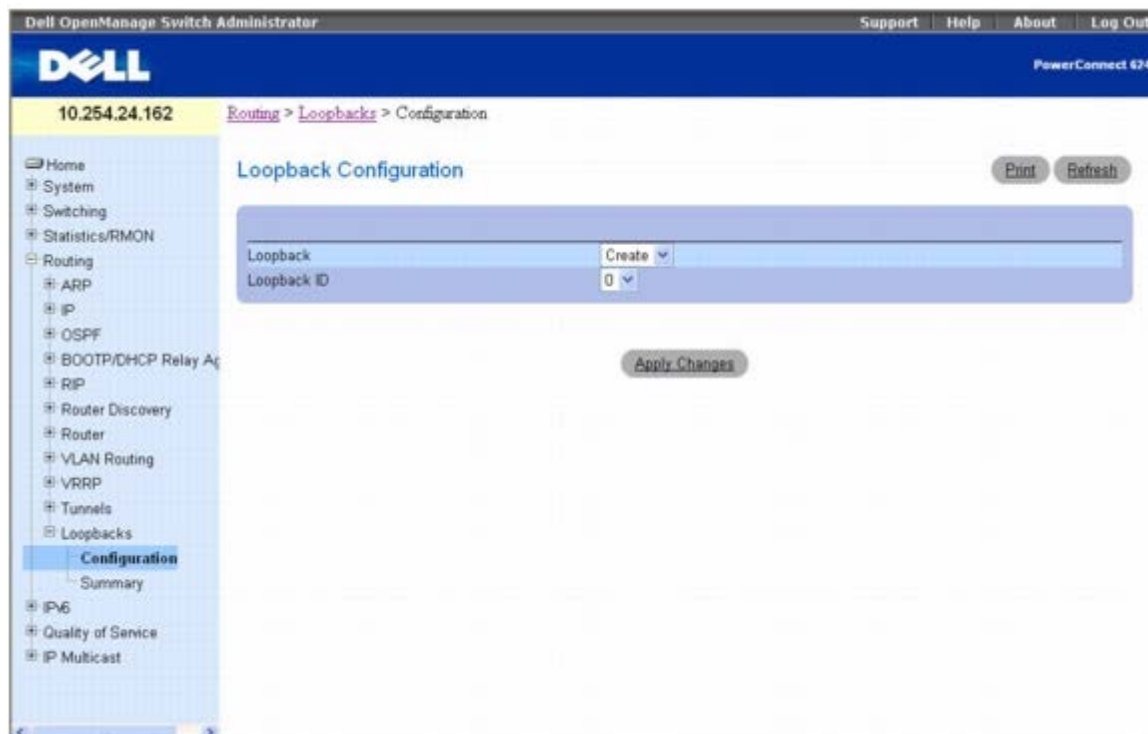
- 回送配置
- 回送摘要

## 回送配置

**Loopbacks Configuration** (回送配置) 页面用于创建、配置或删除回送接口。也可以设置或删除回送的次地址。

要显示此页面，请在树视图中单击 **Routing** (路由) ® **Loopbacks** (回送) ® **Configuration** (配置)。

图 10-45. 回送配置



**Loopbacks Configuration** (回送配置) 页面包含以下字段：

**Loopback**（回送）— 使用下拉式菜单从当前配置的回送接口列表中选择。如果已创建的回送接口未达到最大数目，则 **Create**（创建）也包含于有效的选项当中。

**Loopback ID**（回送 ID）— 在 **Loopback**（回送）字段中选择 **Create**（创建）后，将显示可用的回送 ID 列表。

**Protocol**（协议）— 选择 **IPv4** 或 **IPv6** 以配置回送接口的相应属性。选定的协议会影响此页面上显示的字段。

**Link Local Only Mode**（仅链路本地模式）— 使用链路本地地址在此接口上启用 **IPv6**。此选项仅在指定的协议为 **IPv6** 时显示，并且仅在没有指定明确的 **IPv6** 地址的情况下才可配置。

**IPv6 Address (IPv6 地址)** — 为选定的回送接口选择已配置的 **IPv6** 地址列表。如果配置的地址未达到最大数目，则有效的选项将包括 **Add**（添加）。此选项仅在指定的协议为 **IPv6** 时显示。

**IPv6 Address (IPv6 地址)** — 从 **IPv6 Address (IPv6 地址)** 选择器中选择 **Add**（添加）时，此 **IPv6** 地址输入字段将会显示。以前缀/长度的格式输入地址。此选项仅在指定的协议为 **IPv6** 时显示。

**EU164** — 也可以选择指定 64 位扩展唯一标识符 (**EUI-64**)。此选项仅在指定的协议为 **IPv6** 时显示。

**IPv4 Address (IPv4 地址)** — 此接口的主 **IPv4** 地址（点分十进制表示法）。此选项仅在指定的协议为 **IPv4** 时显示。

**IPv4 Subnet Mask (IPv4 子网掩码)** — 此接口的主 **IPv4** 子网掩码（点分十进制表示法）。此选项仅在指定的协议为 **IPv4** 时显示。

配置了主地址后，以下字段将会显示。可以配置多个次地址。

**Secondary Address**（次地址）— 从下拉式菜单中为选定的回送接口选择配置的 **IPv4** 次地址。在此可以通过选择 **Add Secondary IP Address**（添加次 IP 地址），在 **Secondary IP Address**（次 IP 地址）字段中输入新的地址，前提是配置的次地址未达到最大数目。必须先配置主地址，然后才可添加次地址。

**Secondary IP Address**（次 IP 地址）— 此接口的次 **IP** 地址（点分十进制表示法）。输入字段仅在选择 **Add Secondary**（添加次地址）时才可见。

**Secondary Subnet Mask**（次子网掩码）— 接口的次子网掩码（点分十进制表示法）。输入字段仅在选择 **Add Secondary**（添加次地址）时才可见。

## 创建新的回送 (IPv4)

□□□ 打开 **Loopbacks Configuration**（回送配置）页面。

□□□ 从 **Loopback**（回送）下拉式菜单中选择 **Create**（创建）。

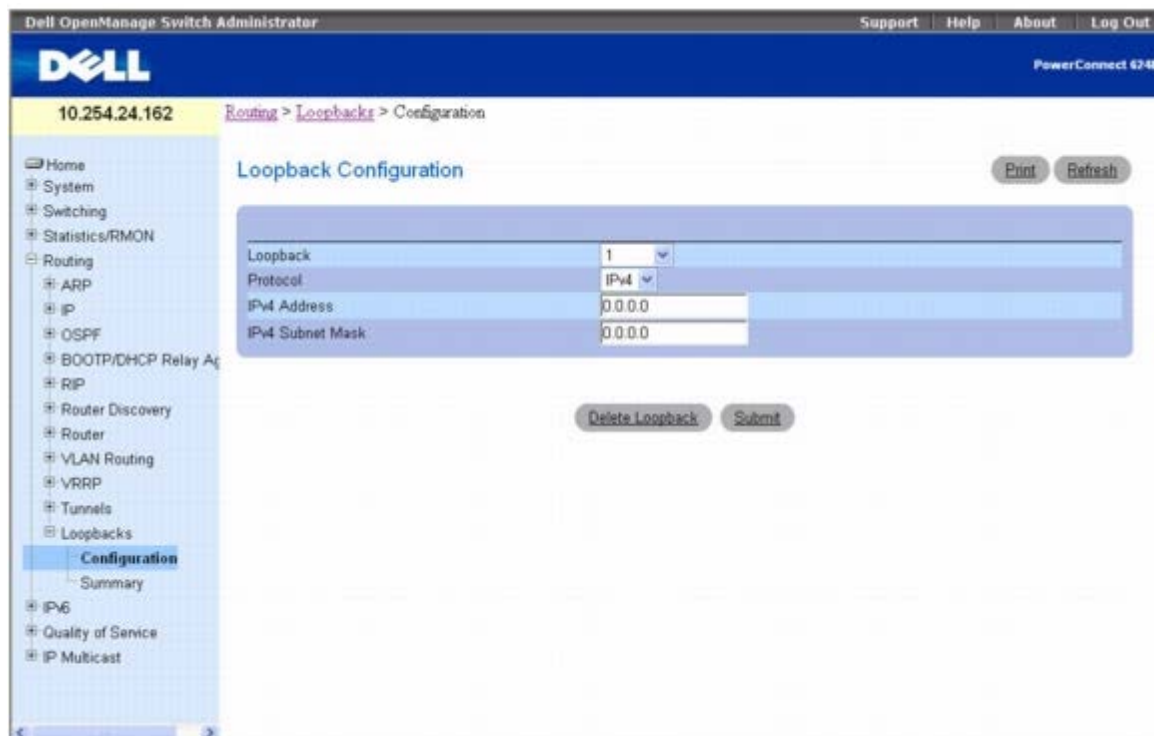
□□□ 在 **Loopback ID**（回送 ID）字段中指定要使用的 ID。

□□□ 单击 **Apply Changes**（应用更改）。

Loopback ID（回送 ID）字段将会消失，并显示其余的回送字段。

图 10-46. 回送配置 - IPv4 输入项





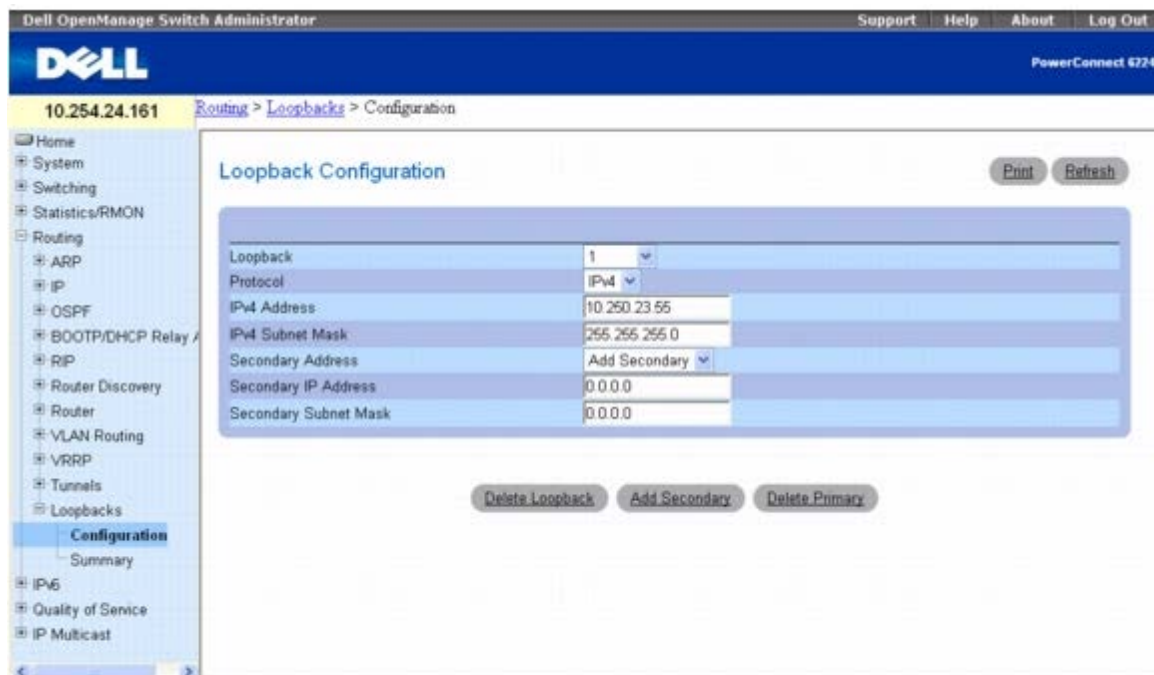
□□□ 在 **Protocol**（协议）字段中输入 **IPv4**。

□□□ 在其余字段中输入所需的值。

□□□ 单击 **Submit**（提交）。

系统将会保存新的回送，并且重新显示带有次地址配置字段的网页。

图 10-47. 回送配置 - 添加次地址



□□□ 填写 **Secondary Address**（次地址）、**Secondary IP Address**（次 IP 地址）和 **Secondary Subnet Mask**（次子网掩码）字段。



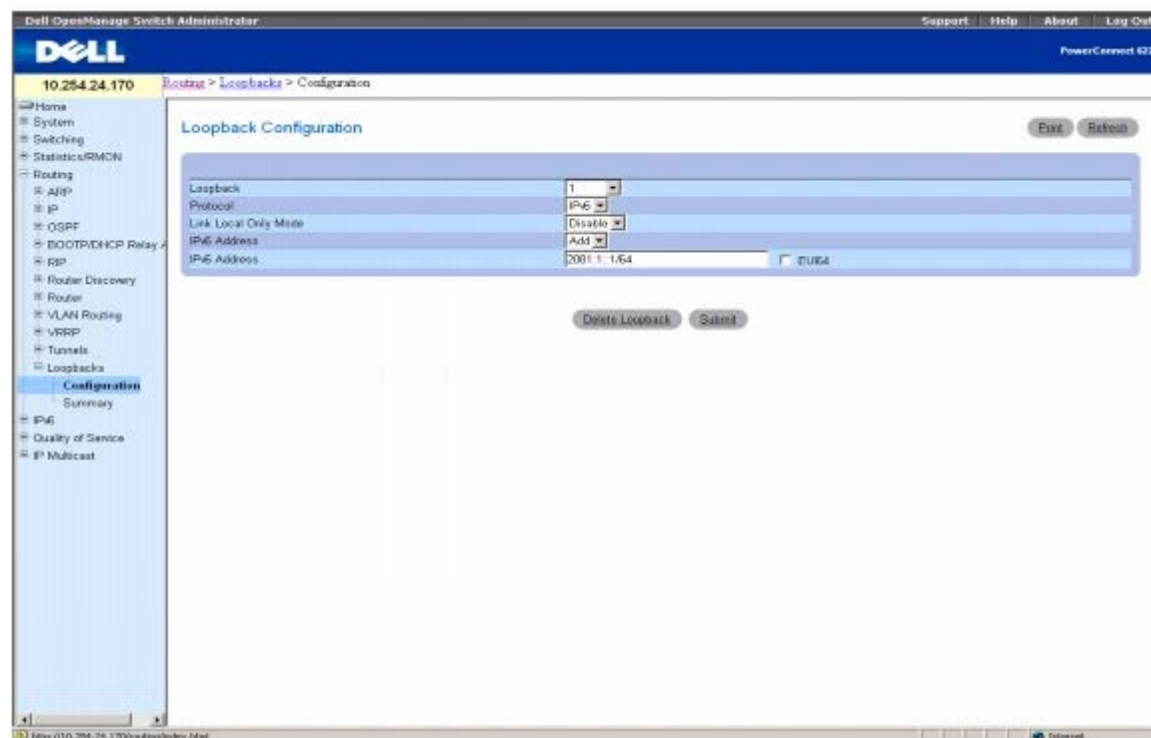
□□□ 单击 **Add Secondary**（添加次地址）按钮。系统将会保存次地址，并且重新显示带有主回送地址和次回送地址的网页。

## 创建新的回送 (IPv6)

- 打开 **Loopbacks Configuration**（回送配置）页面。
- 从 **Loopback**（回送）下拉式菜单中选择 **Create**（创建）。
- 在 **Loopback ID**（回送 ID）字段中指定要使用的 ID。
- 单击 **Apply Changes**（应用更改）。

Loopback ID（回送 ID）字段将会消失，并显示其余的回送字段。

图 10-48. 回送配置 - IPv6 输入项



- 从 **Protocol**（协议）字段的下拉框中选择 **IPv6**。
- 添加 **IPv6 Address**（IPv6 地址）。
- 在其余字段中输入所需的值。
- 单击 **Submit**（提交）。

系统将保存新的回送，并更新设备。

## 配置现有回送

- 打开 **Loopback Configuration**（回送配置）页面。
- 在 **Loopback**（回送）下拉式菜单中指定要配置的回送。
- 根据需要更改其余字段中的值。

□□□ 单击 **Apply Changes**（应用更改）。

系统将保存新配置，并更新设备。

## 删除回送

□□□ 打开 **Loopback Configuration**（回送配置）页面。

□□□ 在 **Loopback**（回送）下拉式菜单中指定要删除的回送。

□□□ 单击 **Delete Loopback**（删除回送）。

系统将删除回送，并更新设备。

## 删除次地址

□□□ 打开 **Loopback Configuration**（回送配置）页面。

□□□ 指定关联的回送。

□□□ 指定要删除的次地址。

□□□ 单击 **Delete Selected Secondary**（删除选定的次地址）。

系统将删除该次地址，并更新设备。

## 使用 CLI 命令配置回送

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

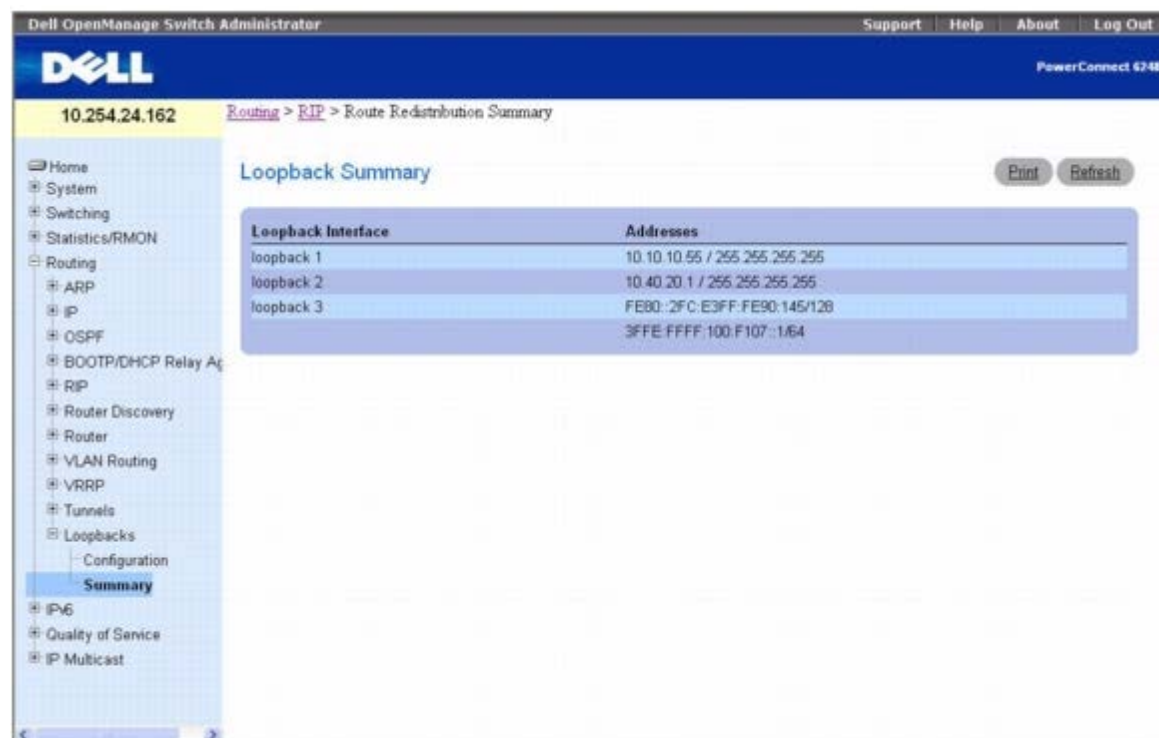
- 回送接口命令
- IP 寻址命令
- IPv6 路由命令

## 回送摘要

**Loopbacks Summary**（回送摘要）页面用于显示已配置回送的摘要。

要显示此页面，请在树视图中单击 **Routing**（路由）® **Loopbacks**（回送）® **Summary**（摘要）。

图 10-49. 回送摘要



**Loopbacks Summary** (回送摘要) 页面会显示以下字段：

**Loopback Interface** (回送接口) — 已配置的回送接口的 ID。

**Addresses** (地址) — 在回送接口上配置的地址列表。

## 使用 CLI 命令显示回送摘要

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- 回送接口命令

---

[返回目录页面](#)

[返回目录页面](#)

# 配置 IPv6

Dell™ PowerConnect™ 6200 系列用户指南

- [全局配置](#)
- [接口配置](#)
- [接口摘要](#)
- [IPv6 统计数据](#)
- [IPv6 邻居列表](#)
- [DHCPv6](#)
- [OSPFv3](#)
- [IPv6 路由](#)

IPv6 是下一代 Internet 协议。与 IPv4 的 32 位地址不同，IPv6 的地址为 128 位，它解决了 IPv4 遇到的地址耗尽问题，并且不要求进行网络地址转换 (NAT)。而在 IPv4 网络中，需要使用这种转换来减少给定网络所需的全局唯一 IP 地址数。IPv6 的集合地址通过著名的地址组合，可以大大减小全局路由表的大小。安全性的集成度更高，网络配置简单化但更加灵活。

IPv6 可与 IPv4 共存于 6200 系列上。由于结合了 IPv4，因此可以在回送接口和 VLAN 接口上启用 IPv6 路由。每个 L3 路由接口都可用于 IPv4、IPv6 或这两种协议。对于 IPv6，在 L3（例如 UDP 和 TCP）上运行的 IP 协议不会发生变化。因此，一个 CPU 堆栈即可用于 IPv4 和 IPv6 传输，一个套接层接口可提供对这两者的访问。路由协议能够计算一个 IP 版本或这两个 IP 版本的路由。

IPv6 菜单页面包含以下功能的链接：

- [全局配置](#)
- [接口配置](#)
- [接口摘要](#)
- [IPv6 统计数据](#)
- [IPv6 邻居列表](#)
- [DHCPv6](#)
- [OSPFv3](#)
- [IPv6 路由](#)



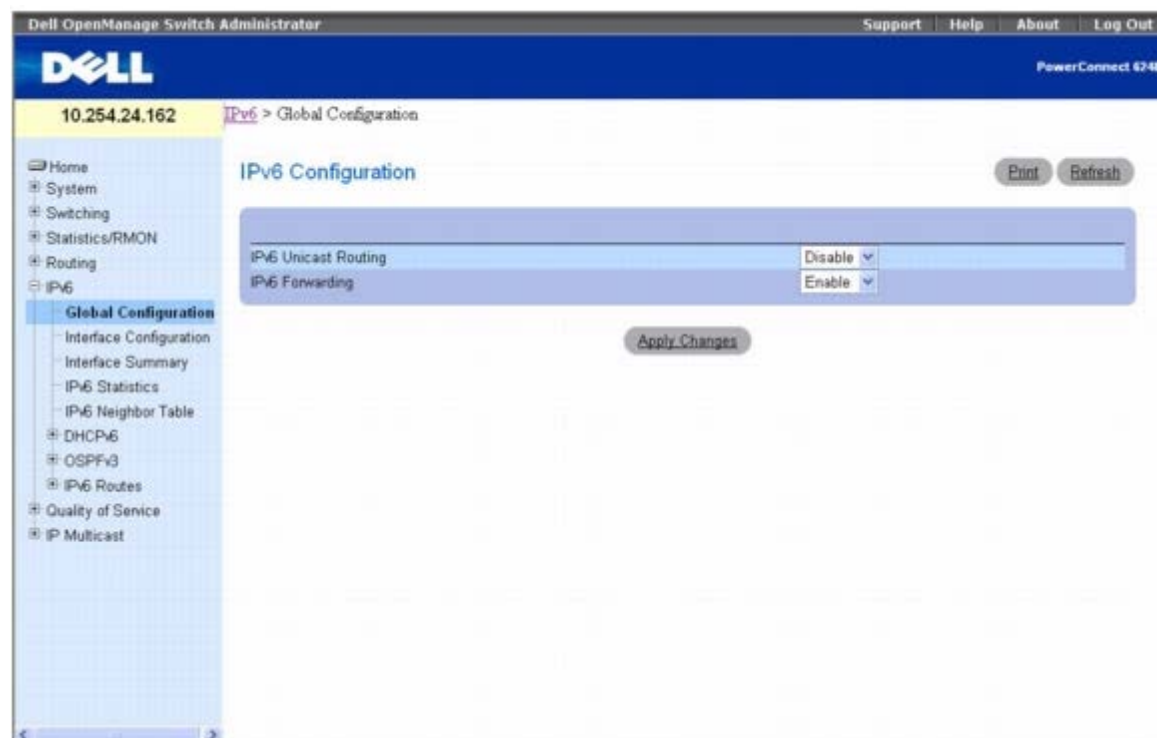
注：CLI 命令并不适用于所有 IPv6 页面。

## 全局配置

**Global Configuration**（全局配置）页面用于在路由器上启用 IPv6 转发功能，并且能够转发 IPv6 单点传送数据包。

要显示此页面，请在树视图中单击 **IPv6 ® Global Configuration**（全局配置）。

图 11-1. IPv6 全局配置



**IPv6 Global Configuration (IPv6 全局配置)** 页面包含以下字段:

**IPv6 Unicast Routing (IPv6 单点传送路由)** — 在路由器上全局启用或禁用 IPv6 单点传送路由功能。默认值为 Disable (禁用)。

**IPv6 Forwarding (IPv6 转发)** — 在路由器上启用或禁用 IPv6 帧的转发功能。默认值为 Enable (启用)。

## 配置 IPv6 参数

□□□ 打开 **IPv6 Global Configuration (IPv6 全局配置)** 页面。

□□□ 从下拉式菜单中启用或禁用单点传送路由。

□□□ 从下拉式菜单中启用或禁用 IPv6 帧转发。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存设置并更新设备。

## 使用 CLI 命令配置 IPv6

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

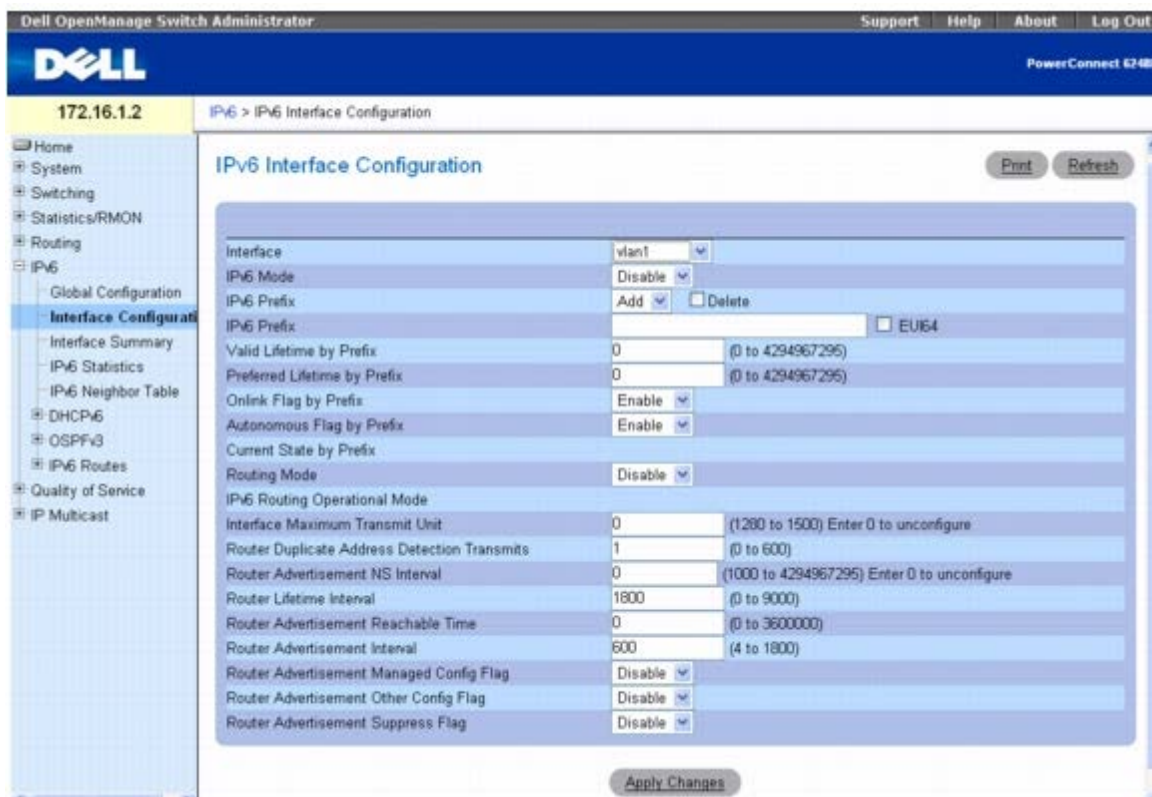
- IPv6 路由命令

## 接口配置

**Interface Configuration (接口配置)** 页面用于配置 IPv6 接口参数。

要显示此页面, 请在树视图中单击 **IPv6 @ Interface Configuration (接口配置)**。

图 11-2. IPv6 接口配置



**IPv6 Interface Configuration (IPv6 接口配置)** 页面包含以下字段:

**Interface (接口)** — 选择要配置的接口。选择更改时, 屏幕将会刷新, 所有字段都要根据新选定的端口进行更新。仅显示启用路由功能的接口和通道。

**IPv6 Mode (IPv6 模式)** — 启用 IPv6 模式时, 接口能够在没有全局地址的情况下进行 IPv6 操作。在这种情况下, 将使用基于 EUI-64 的本地链路地址。此选择器将列出两个 IPv6 模式选项: Enable (启用) 和 Disable (禁用)。默认值为 Disable (禁用)。

**IPv6 Prefix (IPv6 前缀)** — 选择在此接口上 Add (添加) 或 Delete (删除) IPv6 前缀。如果添加前缀, 则在下面的 IPv6 Prefix (IPv6 前缀) 字段中指定该前缀。单击 **Delete** (删除) 可删除显示的 IPv6 前缀。

**IPv6 Prefix (IPv6 前缀)** — 为接口指定 IPv6 前缀及其长度。选择更改时, 屏幕将刷新, 并且将根据所选 IPv6 地址更新有效使用寿命、首选使用寿命、链路连通标记和自治标记。

**EUI-64** — 选中后, 需指定 64 位单点传送前缀。

**Valid Lifetime by Prefix (每个前缀的有效使用寿命)** — 要置于 **Prefix Information (前缀信息)** 选项的 **Valid Lifetime (有效使用寿命)** 字段中的路由器公布值 (以秒为单位)。此前缀可用于在这段时间内确定链路连通。使用无状态地址自动配置功能来从此前缀生成地址的那些主机可以在这段时间内使用这些地址。如果自动配置的地址的存在时间已超过首选使用寿命, 但尚未达到有效使用寿命, 则被视为“不推荐的地址”。根据 RFC 2462 的定义, 不推荐的地址是“分配给接口的地址, 不提倡、但也没有严格禁止使用这种地址”。不推荐的地址不应在新的通信中用作源地址, 但发往或发自不推荐的地址的信息包还是会正常处理。当切换到优先地址会导致特定的上层活动 (例如现有的 TCP 连接) 遇到困难时, 不推荐的地址可以在通信中继续用作源地址。有效范围为 0 至 4,294,967,295 秒。

**Preferred Lifetime by Prefix (每个前缀的首选使用寿命)** — 要置于 **Prefix Information (前缀信息)** 选项的 **Preferred Lifetime (首选使用寿命)** 中的路由器公布值 (以秒为单位)。使用无状态地址自动配置功能从前缀生成的地址在这段时间内一直是“首选”地址。根据 RFC 2462 的定义, 首选地址是“分配给接口的地址, 可以不受限制地被上层协议使用”。首选地址可以用作发自 (或发往) 接口的信息包的源 (或目的地) 地址。范围为 0 至 4,294,967,295 秒。

**Onlink Flag by Prefix (每个前缀的链路连通标记)** — 指定可用于确定链路连通的所选前缀。默认值为 Enable (启用)。此选择器将列出两个链路连通标记选项: Enable (启用) 和 Disable (禁用)。

**Autonomous Flag by Prefix (每个前缀的自治标记)** — 指定可用于自治地址配置的所选前缀。默认值为 Disable (禁用)。此选择器将列出两个自治标记选项: Enable (启用) 和 Disable (禁用)。

**Current State by Prefix (每个前缀的当前状态)** — 所选 IPv6 前缀的接口工作状态。

**Routing Mode (路由模式)** — 指定接口的路由模式。此选择器将列出两个路由模式选项: Enable (启用) 和 Disable (禁用)。默认值为 Disable (禁用)。

**IPv6 Routing Operational Mode (IPv6 路由工作模式)** — 指定接口的工作状态。默认值为 **Disable** (禁用)。

**Interface Maximum Transmit Unit (接口最大传输单元)** — 指定接口上的最大传输单元。如果值为 0, 则此接口不能实现路由功能。如果启用路由功能, 则将此值设为 0 是无效的。MTU 的有效范围是 1280 至 1500。

**Router Duplicate Address Detection Transmits (路由器重复地址检测传输)** — 指定接口上重复地址检测传输的次数。DAD 传输次数必须在 0 至 600 范围内。

**Router Advertisement NS Interval (路由器公布 NS 间隔)** — 指定从接口发送的路由器公布的重新传输时间字段。值 0 表示未指定此路由器的间隔。邻居请求间隔的范围是 1000 至 4294967295。

**Router Lifetime Interval (路由器使用寿命间隔)** — 指定从接口发送的路由器公布使用寿命字段。此值必须大于或等于最大公布间隔。0 表示路由器不用作默认路由器。路由器使用寿命范围是 0 至 9000。

**Router Advertisement Reachable Time (路由器公布可达时间)** — 指定在邻居发现 (ND) 确认后认为邻居可达的路由器公布时间。可达时间范围是 0 至 3600000。

**Router Advertisement Interval (路由器公布间隔)** — 指定从接口发送路由器公布所允许的最大时间间隔。默认值为 600。最大公布间隔范围是 4 至 1800。

**Router Advertisement Managed Config Flag (路由器公布管理配置标记)** — 指定路由器公布管理的地址配置标记。为真时, 端节点使用 DHCPv6。为假时, 端节点自动配置地址。管理标记的默认值为 **Disable** (禁用)。

**Router Advertisement Other Config Flag (路由器公布其它配置标记)** — 指定路由器公布的其它有状态配置标记。其它配置标记的默认值为 **Disable** (禁用)。

**Router Advertisement Suppress Flag (路由器公布抑制标记)** — 指定接口上的路由器公布抑制情况。抑制标记的默认值为 **Disable** (禁用)。

## 配置 IPv6 接口

打开 **IPv6 Interface Configuration (IPv6 接口配置)** 页面。

根据需要修改字段。

单击 **Apply Changes** (应用更改)。

系统将保存 IPv6 接口修改信息并更新设备。

## 使用 CLI 命令配置 IPv6 接口

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- IPv6 路由命令

---

## 接口摘要

**Interface Summary (接口摘要)** 页面用于显示所有 IPv6 接口的设置。

要显示此页面, 请在树视图中单击 **IPv6 ® Interface Summary (接口摘要)**。

图 11-3. IPv6 接口摘要



Dell OpenManage Switch Administrator  
Support Help About Log Out  
PowerConnect 6248  
10.254.24.162

IPv6 Interface Summary

Interface	Routing Mode	Admin Mode	Operational Mode	IPv6 Prefix/Prefix Length	State	IPv6 Address	State
1/g1	Disabled	Enabled	Disabled				
1/g2	Disabled	Enabled	Disabled				
1/g3	Disabled	Enabled	Disabled				
1/g4	Disabled	Enabled	Disabled				
1/g5	Disabled	Enabled	Disabled				
1/g6	Disabled	Enabled	Disabled				
1/g7	Disabled	Enabled	Disabled				
1/g8	Disabled	Enabled	Disabled				
1/g9	Disabled	Enabled	Disabled				
1/g10	Disabled	Enabled	Disabled				
1/g11	Disabled	Enabled	Disabled				
1/g12	Disabled	Enabled	Disabled				
1/g13	Disabled	Enabled	Disabled				
1/g14	Disabled	Enabled	Disabled				
1/g15	Disabled	Enabled	Disabled				
1/g16	Disabled	Enabled	Disabled				
1/g17	Disabled	Enabled	Disabled				
1/g18	Disabled	Enabled	Disabled				
1/g19	Disabled	Enabled	Disabled				
1/g20	Disabled	Enabled	Disabled				

**IPv6 Interface Summary (IPv6 接口摘要)** 页面包含以下字段:

**Interface (接口)** — 指定其设置显示在当前表行中的接口。

**Routing Mode (路由模式)** — 指定接口的路由模式。

**Admin Mode (管理模式)** — 指定接口的管理模式。

**Operational Mode (工作模式)** — 指定接口的工作模式。

**IPv6 Prefix/PrefixLength (IPv6 前缀/前缀长度)** — 指定接口上已配置的 IPv6 地址。

**State (状态)** — 指定接口是活动的还是不活动的。

## 使用 CLI 命令显示 IPv6 接口摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- IPv6 路由命令

## IPv6 统计数据

**IPv6 Statistics (IPv6 统计数据)** 页面用于显示一个或所有接口的 IPv6 通信统计数据。

要显示此页面, 请在树视图中单击 **IPv6** ® **IPv6 Statistics (IPv6 统计数据)**。

图 11-4. IPv6 统计数据

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area displays 'IPv6 Statistics' for the interface 'All'. The statistics table is as follows:

IPv6 Statistics	
Total Datagrams Received	0
Received Datagrams Locally Delivered	0
Received Datagrams Discarded Due To Header Errors	0
Received Datagrams Discarded Due To MTU	0
Received Datagrams Discarded Due To No Route	0
Received Datagrams With Unknown Protocol	0
Received Datagrams Discarded Due To Invalid Address	0
Received Datagrams Discarded Due To Truncated Data	0
Received Datagrams Discarded Other	0
Received Datagrams Reassembly Required	0
Datagrams Successfully Reassembled	0
Datagrams Failed To Reassemble	0
Datagrams Forwarded	0
Datagrams Locally Transmitted	0
Datagrams Transmit Failed	0

**IPv6 Statistics (IPv6 统计数据)** 页面包含以下字段:

**Interface (接口)** — 选择要显示统计数据的接口。选择更改时, 屏幕将会刷新, 所有字段都要根据新选定的接口进行更新。

#### IPv6 统计数据

**Total Datagrams Received (接收到的数据包总数)** — 从接口收到的输入数据包总数, 包括错误收到的数据包。

**Received Datagrams Locally Delivered (接收到的本地发送的数据包)** — 成功发送到 IPv6 用户协议 (包括 ICMP) 的数据包总数。在这些数据包发送到的接口处, 此计数器增加, 而该接口并不一定是某些数据包的输入接口。

**Received Datagrams Discarded Due To Header Errors (接收到的因标头错误而丢弃的数据包)** — 因输入数据包的 IPv6 标头中存在错误而丢弃的数据包数目, 这些错误包括版本号不匹配、其它格式错误、超出跃距计数、处理 IPv6 选项时发现错误等。

**Received Datagrams Discarded Due To MTU (接收到的因 MTU 而丢弃的数据包)** — 由于输入数据包的大小超过发送接口的链路 MTU 而无法转发的数据包数目。

**Received Datagrams Discarded Due To No Route (接收到的因无路由而丢弃的数据包)** — 由于无法找到路由将输入数据包传输到目的地而丢弃的数据包数目。

**Received Datagrams With Unknown Protocol (接收到的协议未知的数据包)** — 标为本地地址、已成功接收但由于协议未知或不受支持而丢弃的数据包数目。在这些数据包发送到的接口处, 此计数器增加, 而该接口并不一定是某些数据包的输入接口。

**Received Datagrams Discarded Due To Invalid Address (接收到的因地址无效而丢弃的数据包)** — 由于 IPv6 标头的目的地字段中的 IPv6 地址不是该实体要接收的有效地址而丢弃的输入数据包数目。此计数包括无效的地址 (例如 ::0) 和不支持的地址 (例如未分配前缀的地址)。对于因未使用 IPv6 路由器而无法转发数据包的实体, 此计数器包括由于目的地地址不是本地地址而丢弃的数据包。

**Received Datagrams Discarded Due To Truncated Data (接收到的因截断数据而丢弃的数据包)** — 由于数据包帧承载的数据不足而丢弃的输入数据包的数目。

**Received Datagrams Discarded Other (接收到的因其它原因而丢弃的数据包)** — 没有遇到妨碍其继续处理的问题但被丢弃 (例如由于缺乏缓冲区空间) 的输入 IPv6 数据包数目。请注意, 此计数器不包括在等待重组时丢弃的任何数据包。

**Received Datagrams Reassembly Required (接收到的需要重组的数据包)** — 接收到的需要在此接口重组的 IPv6 碎片的数目。请注意, 在这些碎片发送到的接口处, 此计数器增加, 而该接口并不一定是某些碎片的输入接口。

**Datagrams Successfully Reassembled (成功重组的数据包)** — 经过成功重组的 IPv6 数据包的数目。请注意, 在这些数据包发送到的接口处, 此计数器增加, 而该接口并不一定是某些碎片的输入接口。

**Datagrams Failed To Reassemble (无法重组的数据包)** — IPv6 重组算法检测到的失败 (由于超时、错误等原因) 次数。请注意, 这不等于被丢弃的 IPv6 碎片数目, 因为有些算法 (特别是 RFC 815 中的算法) 在收到碎片时即将其合并, 从而无法记录碎片数目。在这些碎片发送到的接口处, 此计数器增加, 而该接口并不一定是某些碎片的输入接口。

**Datagrams Forwarded** (转发的数据包) — 此实体接收到并转发到数据包最终目的地的输出数据包的数目。在不是作为 IPv6 路由器的实体中, 此计数器只包括通过此实体安排源路由的数据包, 其中源路由处理成功。请注意, 对于成功转发的数据包, 发送接口的计数器增加。

**Datagrams Locally Transmitted** (本地发送的数据包) — 此实体已从该输出接口成功发送的数据包的数目。

**Datagrams Transmit Failed** (发送失败的数据包) — 此实体无法成功发送的数据包的数目。

**Datagrams Successfully Fragmented** (成功碎片化的数据包) — 在此输出接口处已成功碎片化的 IPv6 数据包的数目。

**Datagrams Failed To Fragment** (无法碎片化的数据包) — 在此接口处无法碎片化的输出数据包的数目。

**Datagrams Fragments Created** (已创建碎片的数据包) — 由于该输出接口内的碎化而生成的输出数据包碎片的数目。

**Multicast Datagrams Received** (接收到的多点传送数据包) — 接口接收到的多点传送数据包的数目。

**Multicast Datagrams Transmitted** (发送的多点传送数据包) — 接口发送的多点传送数据包的数目。

#### ICMPv6 统计数据

**Total ICMPv6 Messages Received** (接收到的 ICMPv6 信息总数) — 接口接收到的 ICMP 信息的总数, 其中包括计入 ipv6IfIcmpInErrors 的所有数目。请注意, 此接口是将 ICMP 信息发送到的接口, 该接口并不一定是信息的输入接口。

**ICMPv6 Messages With Errors Received** (接收到的包含错误的 ICMPv6 信息) — 接口接收到但确定其有 ICMP 特定错误 (ICMP 校验和错误、长度错误等) 的 ICMP 信息的数目。

**ICMPv6 Destination Unreachable Messages Received** (接收到的 ICMPv6 目的地无法到达的信息) — 接口接收到的 ICMP 目的地无法到达信息的数目。

**ICMPv6 Messages Prohibited Administratively Received** (接收到的 ICMPv6 管理性禁止信息) — 接口接收到的 ICMP 目的地无法到达/通信管理性禁止的信息的数目。

**ICMPv6 Time Exceeded Messages Received** (接收到的 ICMPv6 超时信息) — 接口接收到的 ICMP 超时信息的数目。

**ICMPv6 Parameter Problem Messages Received** (接收到的 ICMPv6 参数问题信息) — 接口接收到的 ICMP 参数问题信息的数目。

**ICMPv6 Packet Too Big Messages Received** (接收到的 ICMPv6 信息包太大的信息) — 接口接收到的 ICMP 信息包太大的信息的数目。

**ICMPv6 Echo Request Messages Received** (接收到的 ICMPv6 回音请求信息) — 接口接收到的 ICMP 回音 (请求) 信息的数目。

**ICMPv6 Echo Reply Messages Received** (接收到的 ICMPv6 回音答复信息) — 接口接收到的 ICMP 回音答复信息的数目。

**ICMPv6 Router Solicit Messages Received** (接收到的 ICMPv6 路由器恳求信息) — 接口接收到的 ICMP 路由器恳求信息的数目。

**ICMPv6 Router Advertisement Messages Received** (接收到的 ICMPv6 路由器公布信息) — 接口接收到的 ICMP 路由器公布信息的数目。

**ICMPv6 Neighbor Solicit Messages Received** (接收到的 ICMPv6 邻居恳求信息) — 接口接收到的 ICMP 邻居恳求信息的数目。

**ICMPv6 Neighbor Advertisement Messages Received** (接收到的 ICMPv6 邻居公布信息) — 接口接收到的 ICMP 邻居公布信息的数目。

**ICMPv6 Redirect Messages Received** (接收到的 ICMPv6 重定向信息) — 接口接收到的 ICMPv6 重定向信息的数目。

**ICMPv6 Group Membership Query Messages Received** (接收到的 ICMPv6 组员资格查询信息) — 接口接收到的 ICMPv6 组员资格查询信息的数目。

**ICMPv6 Group Membership Response Messages Received** (接收到的 ICMPv6 组员资格响应信息) — 接口接收到的 ICMPv6 组员资格响应信息的数目。

**ICMPv6 Group Membership Reduction Messages Received** (接收到的 ICMPv6 组员资格削减信息) — 接口接收到的 ICMPv6 组员资格削减信息的数目。

**Total ICMPv6 Messages Transmitted** (发送的 ICMPv6 信息总数) — 此接口尝试发送的 ICMP 信息的总数。请注意, 此计数器包括计入 icmpOutErrors 的所有数目。

**ICMPv6 Messages Not Transmitted Due To Error** (因错误未发送的 ICMPv6 信息) — 此接口因为在 ICMP 内发现问题 (例如缺少缓冲区) 而未发送的 ICMP 信息的数目。此值不能包括在 ICMP 层外部发现的错误, 例如 IPv6 无法路由结果数据包。在某些应用中, 可能不存

在形成此计数器值的错误类型。

**CMPv6 Destination Unreachable Messages Transmitted** (发送的 **ICMPv6** 目的地无法到达的信息) — 接口发送的 ICMP 目的地无法到达信息的数目。

**ICMPv6 Messages Prohibited Administratively Transmitted** (发送的管理性禁止的 **ICMPv6** 信息) — 发送的 ICMP 目的地无法到达/通信管理性禁止的信息的数目。

**ICMPv6 Time Exceeded Messages Transmitted** (发送的 **ICMPv6** 超时信息) — 接口发送的 ICMP 超时信息的数目。

**ICMPv6 Parameter Problem Messages Transmitted** (发送的 **ICMPv6** 参数问题信息) — 接口发送的 ICMP 参数问题信息的数目。

**ICMPv6 Packet Too Big Messages Transmitted** (发送的 **ICMPv6** 信息包太大的信息) — 接口发送的 ICMP 信息包太大的信息的数目。

**ICMPv6 Echo Request Messages Transmitted** (发送的 **ICMPv6** 回音请求信息) — 接口发送的 ICMP 回音 (请求) 信息的数目。

**ICMPv6 Echo Reply Messages Transmitted** (发送的 **ICMPv6** 回音答复信息) — 接口发送的 ICMP 回音答复信息的数目。

**ICMPv6 Router Solicit Messages Transmitted** (发送的 **ICMPv6** 路由器恳求信息) — 接口发送的 ICMP 路由器恳求信息的数目。

**ICMPv6 Router Advertisement Messages Transmitted** (发送的 **ICMPv6** 路由器公布信息) — 接口发送的 ICMP 路由器公布信息的数目。

**ICMPv6 Neighbor Solicit Messages Transmitted** (发送的 **ICMPv6** 邻居恳求信息) — 接口发送的 ICMP 邻居恳求信息的数目。

**ICMPv6 Neighbor Advertisement Messages Transmitted** (发送的 **ICMPv6** 邻居公布信息) — 接口发送的 ICMP 邻居公布信息的数目。

**ICMPv6 Redirect Messages Transmitted** (发送的 **ICMPv6** 重定向信息) — 发送的重定向信息的数目。

**ICMPv6 Group Membership Query Messages Transmitted** (发送的 **ICMPv6** 组员资格查询信息) — 发送的 ICMPv6 组员资格查询信息的数目。

**ICMPv6 Group Membership Response Messages Transmitted** (发送的 **ICMPv6** 组员资格响应信息) — 发送的 ICMPv6 组员资格响应信息的数目。

**ICMPv6 Group Membership Reduction Messages Transmitted** (发送的 **ICMPv6** 组员资格削减信息) — 发送的 ICMPv6 组员资格削减信息的数目。

**ICMPv6 Duplicate Address Detects** (检测到的 **ICMPv6** 重复地址) — 接口检测到的重复地址的数目。

## 显示 IPv6 统计数据

□□□ 打开 **IPv6 Statistics** (IPv6 统计数据) 页面。

□□□ 从 **Interface** (接口) 下拉式菜单中选择要显示的接口。

系统将显示所选接口的统计数据。

## 使用 CLI 命令显示 IPv6 和 ICMPv6 统计数据

有关执行此功能的 CLI 命令的信息, 请参阅 «CLI 参考指南» 的以下章节:

- IPv6 路由命令

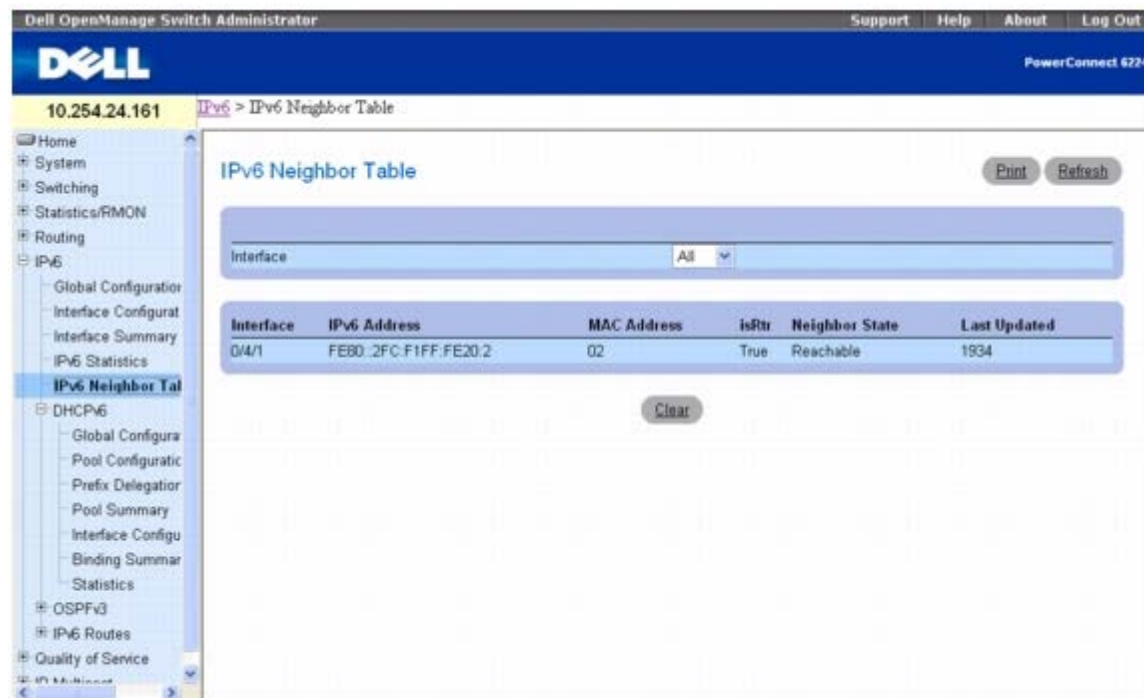
---

## IPv6 邻居列表

**IPv6 Neighbor Table** (IPv6 邻居列表) 页面用于显示指定接口的 IPv6 邻居详细信息。

要显示此页面，请在树视图中单击 **IPv6 @ IPv6 Neighbor Table (IPv6 邻居列表)**。

图 11-5. IPv6 邻居列表



**IPv6 Neighbor Table (IPv6 邻居列表)** 页面包含以下字段：

**Interface (接口)** — 选择要显示邻居状态信息的接口。

**Interface (接口)** — 指定其设置显示在当前表行中的接口。

**IPv6 Address (IPv6 地址)** — 指定邻居或接口的 IPv6 地址。

**MAC Address (MAC 地址)** — 指定与接口关联的 MAC 地址。

**isRtr** — 表示邻居是否为路由器。如果邻居是路由器，则该值为 **TRUE**。如果邻居不是路由器，则该值为 **FALSE**。

**Neighbor State (邻居状态)** — 指定邻居高速缓存条目的状态。下面是 IPv6 邻居查找高速缓存中动态条目的状态：

- **Incmp** — 正在对条目进行地址解析。一条邻居请求信息已发送到目标的请求节点多点传送地址，但是对应的邻居公布信息尚未收到。
- **Reachable (可到达)** — 在最后的可到达时间（毫秒）内接收到肯定的确认，指出到邻居的转发路径工作正常。当设备处于 **REACH** 状态时，不会在发送信息包时执行任何特殊操作。
- **Stale (旧)** — 自上次收到转发路径工作正常的肯定确认之后，已经超过了可到达时间（毫秒）。当设备处于 **STALE** 状态时，直到发送信息包时才执行操作。
- **Delay (延迟)** — 自上次收到转发路径工作正常的肯定确认之后，已经超过了可到达时间（毫秒）。在最后 **DELAY\_FIRST\_PROBE\_TIME** 秒内发送出信息包。如果在进入 **DELAY** 状态后 **DELAY\_FIRST\_PROBE\_TIME** 秒内未收到可到达确认，则发送邻居请求信息并将该状态更改为 **PROBE**。
- **Probe (探测器)** — 在接收到可到达确认之前，每隔 **RetransTimer** 毫秒重新发送邻居请求信息，从而主动获取可到达确认。

**Last Updated (上次更新时间)** — 自地址经确认可到达后所经过的时间。

## 显示 IPv6 邻居列表

□□□ 打开 **IPv6 Neighbor Table (IPv6 邻居列表)** 页面。

□□□ 从 **Interface** (接口) 下拉式菜单中选择要显示的接口。

系统将显示所选接口的邻居详细信息。

## 使用 CLI 命令显示 IPv6 邻居列表

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- IPv6 路由命令

---

## DHCPv6

通常情况下, 在客户端 (例如主机) 和服务器 (例如路由器) 之间使用 DHCP 来分配 IP 地址、网关和其它网络定义, 例如 DNS、NTP 和/或会话初始化协议 (SIP) 参数。但是, IPv6 本身可以通过 IPv6 邻居发现协议 (NDP) 和使用路由器公布信息来自动配置 IP 地址。因此, DHCPv6 在网络中所起的作用不同于 DHCPv4 的作用, 因为前者对 IP 地址分配的依赖性较弱。

有一列 DHCP 选项通常受 DHCPv4 的支持, 同时还需要受 DHCPv6 的支持, 并且必须进行配置。



**注:** 最重要的选项是 DNS Server (DNS 服务器) 选项, 可在 **IPv6 ® DHCPv6 ® Pool Configuration** (池配置) 网页中进行配置。

**DHCPv6** 菜单页面包含一些网页链接, 这些网页可用于定义和显示 DHCPv6 参数和数据。要显示此页面, 请在树视图中单击 **IPv6 ® DHCPv6**。在此菜单页面中可以访问以下网页:

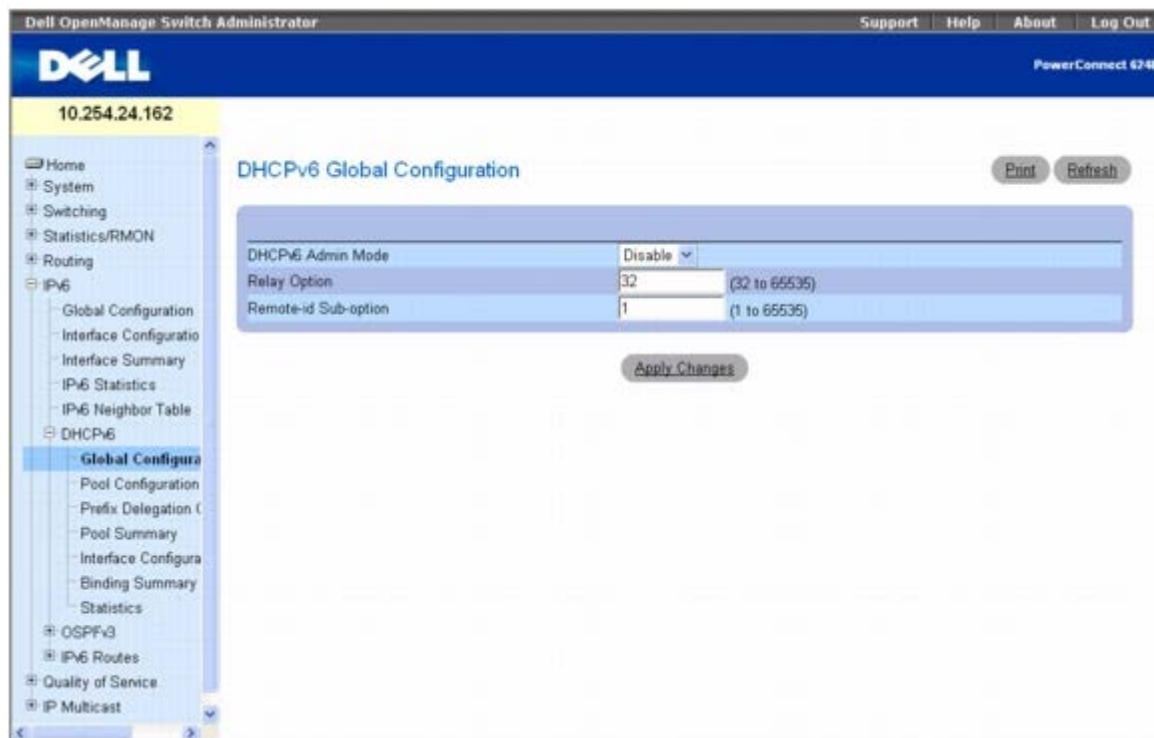
- [DHCPv6 全局配置](#)
- [DHCPv6 池配置](#)
- [前缀代理配置](#)
- [DHCPv6 池摘要](#)
- [DHCPv6 接口配置](#)
- [DHCPv6 服务器捆绑摘要](#)
- [DHCPv6 统计数据](#)

## DHCPv6 全局配置

**DHCPv6 Global Configuration** (**DHCPv6 全局配置**) 页面用于配置 DHCPv6 全局参数。要显示此页面, 请在树视图中单击 **IPv6 ® DHCPv6 ® Global Configuration** (全局配置)。

图 11-6. DHCPv6 全局配置





**DHCPv6 Global Configuration (DHCPv6 全局配置)** 页面包含以下字段:

**DHCPv6 Admin Mode (DHCPv6 管理模式)** — 在交换机上指定 DHCPv6 操作。可能值包括 Enable (启用) 和 Disable (禁用)；默认值为 Disable (禁用)。

**Relay Option (中继选项)** — 指定 Relay Agent Information Option (中继代理信息选项) 值。所允许的值范围是 32 至 65535，表示在中继代理和服务器之间交换的值。每个值的意义各不相同，其中 1 至 39 已经过标准化。默认值 32 表示 OPTION\_INFORMATION\_REFRESH\_TIME。

**Remote-id Sub-option (远程 ID 子选项)** — 可以指定一个数字来表示 Relay Agent Information Option Remote-ID Sub-option (中继代理信息选项远程 ID 子选项) 类型。所允许的值范围介于 1 和 65535 之间。默认值为 1。

## 配置 DHCPv6 全局参数

□□□ 打开 **DHCPv6 Global Configuration (DHCPv6 全局配置)** 页面。

□□□ 根据需要修改字段。

□□□ 单击 **Apply Changes (应用更改)**。

系统将保存 DHCPv6 参数修改信息并更新设备。

## 使用 CLI 命令配置 DHCPv6 全局参数

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- DHCPv6 命令

## DHCPv6 池配置

用于 IPv6 客户端的 DHCP 连接到一台配置为使用设置池的参数的服务器。池由池名称来标识，包含 DNS 服务器的 IPv6 地址和域名。



**Pool Configuration** (池配置) 页面用于创建池和/或配置池参数。

要显示此页面，请在树视图中单击 **IPv6** ® **DHCPv6** ® **Pool Configuration** (池配置)。

图 11-7. 池配置 - 创建

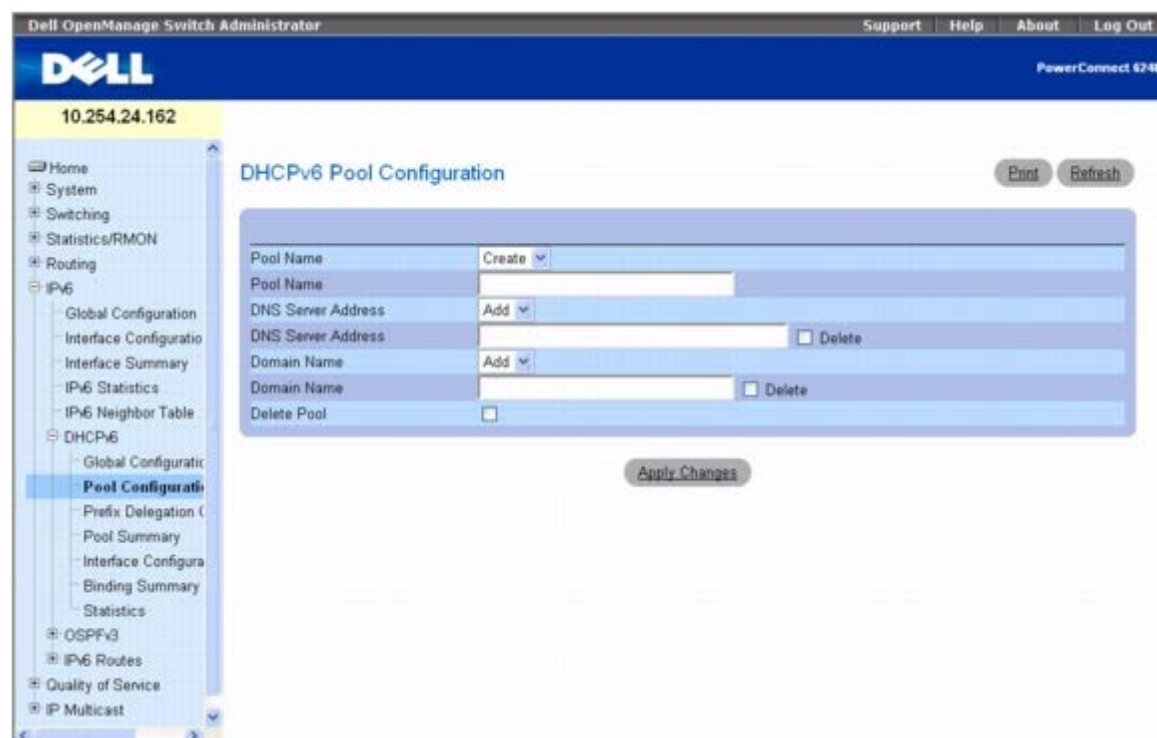


图 11-8. 池配置 - 显示



**Pool Configuration** (池配置) 页面包含以下字段：

**Pool Name** (池名称) — 一个下拉式菜单，列出所有已配置的池名称。选择 **Create** (创建) 时，该页面上字段的数据被清空，以准备生成新的池信息。

**Pool Name** (池名称) — 显示从上一字段中选择的池，或者在选择 **Create** (创建) 时输入 DHCPv6 池的唯一名称。最多可以输入 31 个字母

数字字符。

**DNS Server Address (DNS 服务器地址)** — 一个下拉式菜单, 指定特定 DHCPv6 池内 DNS 服务器的 IPv6 地址。从该菜单中选择 **Add** (添加) 时, 以下字段的数据将被清空, 以准备添加新地址。

**DNS Server Address (DNS 服务器地址)** — 显示从上一字段中选择的 DNS 服务器地址。在上一字段中选择 **Add** (添加) 时, 输入一个新的 DNS 服务器地址。单击 **Delete** (删除) 从此池中删除某个地址。单击 **Apply Changes** (应用更改) 后, 该地址将被删除。

**Domain Name (域名)** — 一个下拉式菜单, 指定在特定 DHCPv6 池内配置的域名列表。从该菜单中选择 **Add** (添加) 时, 以下字段的数据将被清空, 以准备添加新名称。

**Domain Name (域名)** — 显示从上一字段中选择 DNS 域名。在上一字段中选择 **Add** (添加) 时, 输入一个新的 DNS 域名。最多可以输入 255 个字母数字字符。单击 **Delete** (删除) 从此池中删除某个域名。单击 **Apply Changes** (应用更改) 后, 该名称将被删除。

**Delete Pool (删除池)** — 选中此框后, 将删除显示的池。单击 **Apply Changes** (应用更改) 后, 该池将被删除。

## 创建 DHCPv6 池

- 打开 **Pool Configuration** (池配置) 页面。
- 从 **Pool Name** (池名称) 下拉式菜单中选择 **Create** (创建)。
- 在 **Pool Name** (池名称) 字段中输入新名称。
- 指定一个要与此池关联的现有 DNS 服务器地址, 或者创建一个新地址。
- 指定一个要与此池关联的现有域名, 或者创建一个新域名。
- 单击 **Apply Changes** (应用更改)。

系统将保存新池并更新设备。如果指定了新的 DNS 服务器地址或域名, 系统也会进行保存。

## 修改 DHCPv6 池参数

- 打开 **Pool Configuration** (池配置) 页面。
- 从 **Pool Name** (池名称) 下拉式菜单中选择要更改参数的池。
- 更改指定池的 DNS 服务器地址或设置一个新地址。
- 更改指定池的域名或设置一个新域名。
- 单击 **Apply Changes** (应用更改)。

系统将保存 DHCPv6 池参数修改信息并更新设备。

## 删除 DHCPv6 池或参数

- 打开 **Pool Configuration** (池配置) 页面。
- 从 **Pool Name** (池名称) 下拉式菜单中选择要受影响的池。
- 如果要删除此池的 DNS 服务器地址, 请单击 **Delete** (删除) 框。
- 如果要删除此池的域名, 请单击 **Delete** (删除) 框。
- 如果要删除整个池, 请单击 **Delete Pool** (删除池) 框。
- 单击 **Apply Changes** (应用更改)。

系统将删除池或池参数设置并更新设备。

## 使用 CLI 命令配置 DHCPv6 池参数

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

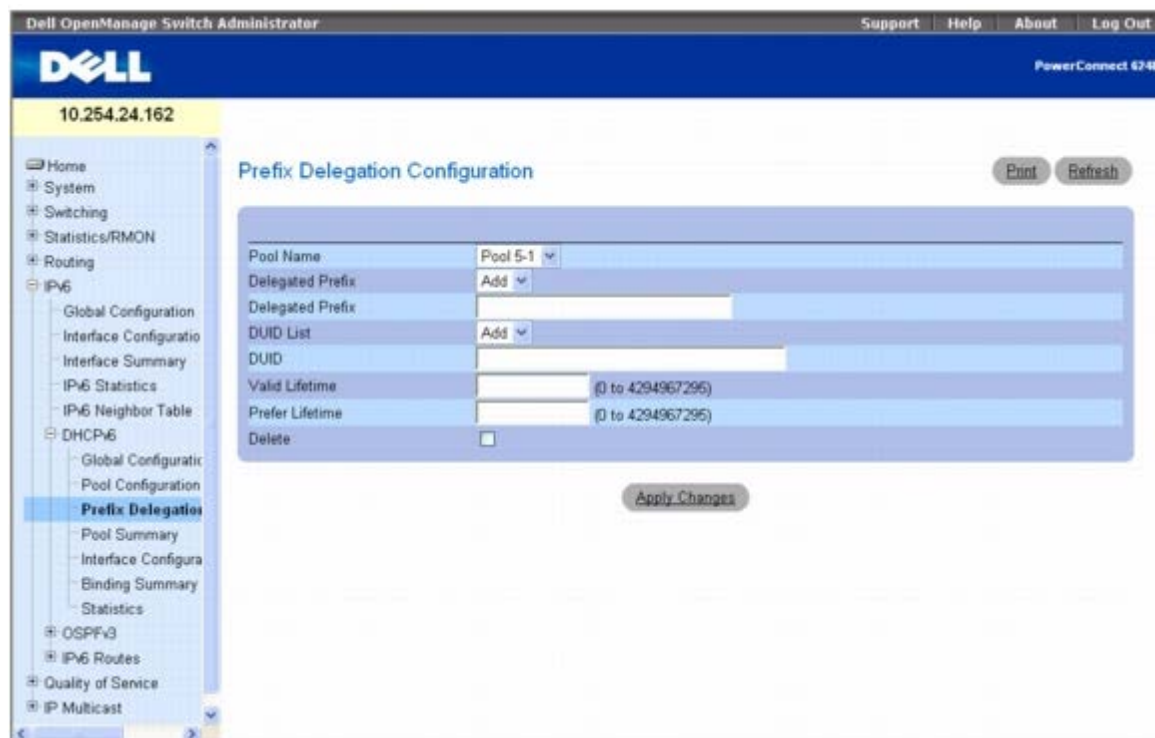
- DHCPv6 命令

## 前缀代理配置

**Prefix Delegation Configuration**（前缀代理配置）页面用于为池配置代理前缀。在可以配置代理前缀之前，必须至少使用 [DHCPv6 池配置](#) 创建一个池。

要显示此页面，请在树视图中单击 **IPv6** ® **DHCPv6** ® **Prefix Delegation Configuration**（前缀代理配置）。

图 11-9. 前缀代理配置



**Prefix Delegation Configuration**（前缀代理配置）页面包含以下字段：

**Pool Name**（池名称）— 指定已配置的所有池名称。选择要配置的池。

**Delegated Prefix**（代理前缀）— 一个下拉式菜单，指定要与特定池关联的代理 IPv6 前缀。选择 **Add**（添加）可以为此池定义新的代理前缀。

**Delegated Prefix**（代理前缀）— 显示所选代理前缀或允许输入一个新前缀。

**DUID List**（DUID 列表） - 一个下拉式菜单，选择客户端的唯一 DUID 值。选择 **Add**（添加）可以为此池定义新的 DUID 值。

**DUID** - 显示选定的 DUID 值或允许输入一个新值。

**Valid Lifetime**（有效使用寿命）— 指定代理前缀的有效使用寿命（以秒为单位）。

**Prefer Lifetime**（首选使用寿命）— 指定代理前缀的首选使用寿命（以秒为单位）。

**Delete** (删除) — 选中并单击 **Apply Changes** (应用更改) 后, 将删除显示池的前缀代理配置。

## 配置池的代理前缀

□□□ 打开 **Prefix Delegation Configuration** (前缀代理配置) 页面。

□□□ 选择要配置的池。

□□□ 指定代理前缀。

□□□ 根据需要修改其余字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存代理前缀和参数并更新设备。

## 使用 CLI 命令配置代理前缀

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- DHCPv6 命令

## DHCPv6 池摘要

**Pool Summary** (池摘要) 页面用于显示所有 DHCPv6 池的设置。显示 Pool Summary (池摘要) 之前, 必须至少使用 [DHCPv6 池配置](#) 创建一个池。

要显示此页面, 请在树视图中单击 **IPv6** ® **DHCPv6** ® **Pool Summary** (池摘要)。

图 11-10. 池摘要



**Pool Summary** (池摘要) 页面包含以下字段:

**Pool Name** (池名称) — 选择要显示的池。

**DNS Server** (DNS 服务器) — 显示关联的 DNS 服务器的 IPv6 地址。

**Domain Name** (域名) — 显示 DNS 域名。

**Host IP Address** (主机 IP 地址) — 显示代理前缀的 IPv6 地址和掩码长度。

**DUID** — 用于标识客户端的唯一 DUID 值的标识符。

**Valid Lifetime** (有效使用寿命) — 指定代理前缀的有效使用寿命 (以秒为单位)。

**Prefer Lifetime** (首选使用寿命) — 显示代理前缀的首选使用寿命 (以秒为单位)。

## 使用 CLI 命令显示池摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

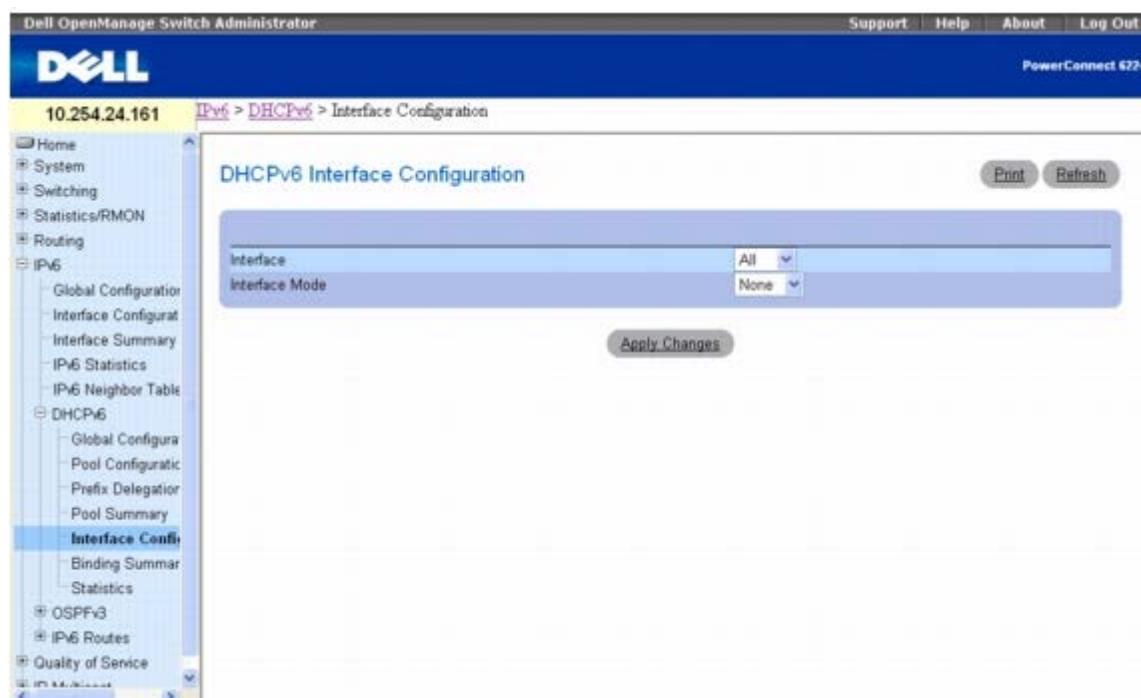
- DHCPv6 命令

## DHCPv6 接口配置

**DHCPv6 Interface Configuration** (DHCPv6 接口配置) 页面用于配置 DHCPv6 接口。

要显示此页面, 请在树视图中单击 **IPv6** ® **DHCPv6** ® **Interface Configuration** (接口配置)。

图 11-11. DHCPv6 接口配置



**DHCPv6 Interface Configuration** (DHCPv6 接口配置) 页面包含以下字段:

**Interface** (接口) — 选择正在配置 DHCPv6 服务器功能的接口。

**Interface Mode** (接口模式) — 将 DHCPv6 模式配置为 Server (服务器) 或 Relay (中继)。DHCPv6 服务器和 DHCPv6 中继功能是互斥的。

**Pool Name** (池名称) — 选择包含无状态和/或前缀代理参数的 DHCPv6 池。当接口模式为 Server (服务器) 时, 将显示此字段。

**Rapid Commit** (快速提交) — 快速提交是一个可选参数。指定该参数后, 可允许客户端和服务端之间快速交换。当接口模式为 **Server** (服务器) 时, 将显示此字段。

**Preference** (优先级) — 选择客户端使用的优先级值, 以确定多个 DHCPv6 服务器之间的优先级。所允许的值范围介于 0 至 4294967295 之间。当接口模式为 **Server** (服务器) 时, 将显示此字段。

**Delete** (删除) — 选中此框并单击 **Apply Changes** (应用更改) 后, 将删除此配置。当 **Interface Mode** (接口模式) 为 **Server** (服务器) 或 **Relay** (中继) 时, 将显示此字段。

**Relay Interface** (中继接口) — 选择要到达中继服务器的接口。当接口模式为 **Relay** (中继) 时, 将显示此字段。

**Destination IP Address** (目的地 IP 地址) — 选择 DHCPv6 中继服务器的 IPv6 地址。当接口模式为 **Relay** (中继) 时, 将显示此字段。

**Remote ID** (远程 ID) — 选择中继代理信息选项。远程 ID 需要衍生自 DHCPv6 服务器 DUID 和中继接口号, 或者可以将其指定为用户定义字符串。当接口模式为 **Relay** (中继) 时, 将显示此字段。

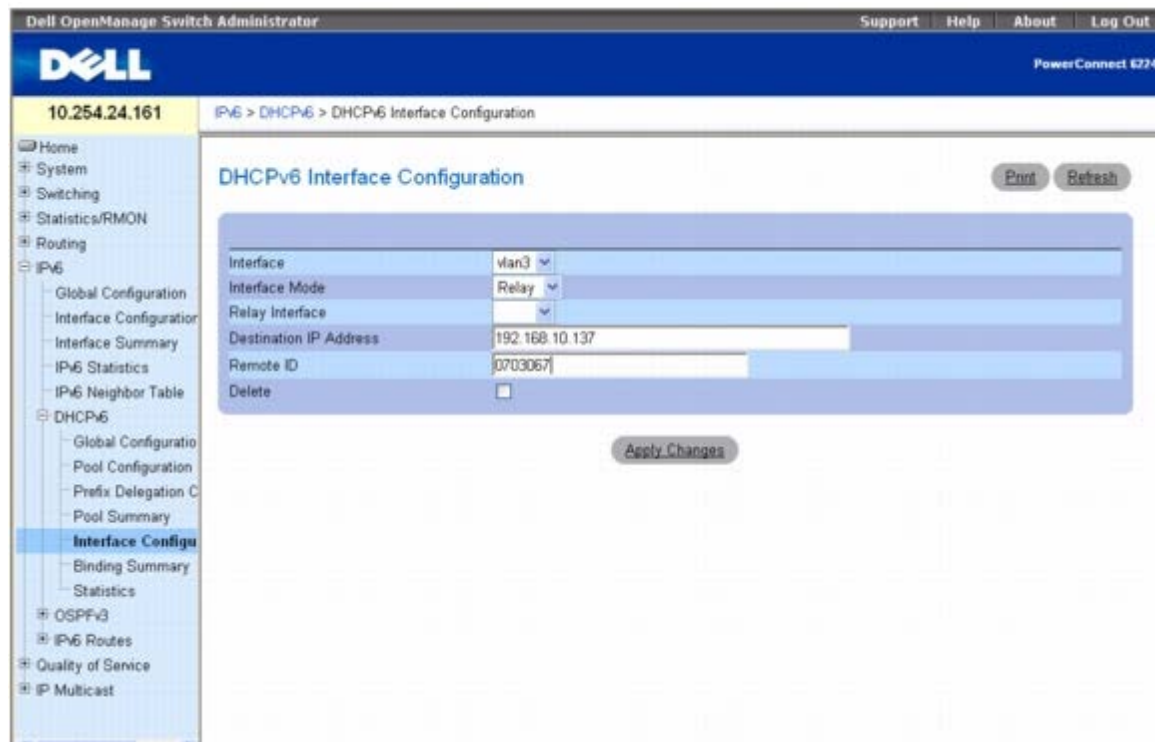
## 在中继接口模式下配置 DHCPv6 接口

□□□ 打开 **DHCPv6 Interface Configuration** (DHCPv6 接口配置) 页面。

□□□ 指定所需的接口, 然后从 **Interface Mode** (接口模式) 下拉式菜单中选择 **Relay** (中继)。

系统将显示以下屏幕:

图 11-12. DHCPv6 接口配置 - 中继



□□□ 根据需要修改字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存 DHCPv6 接口配置并更新设备。

## 使用 CLI 命令配置 DHCPv6 接口



有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- DHCPv6 命令

## 在服务器接口模式下配置 DHCPv6 接口

□□□ 打开 **DHCPv6 Interface Configuration** (DHCPv6 接口配置) 页面。

□□□ 指定所需的接口, 然后从 **Interface Mode** (接口模式) 下拉式菜单中选择 **Server** (服务器)。

系统将显示以下屏幕:

图 11-13. DHCPv6 接口配置 - 服务器



□□□ 根据需要修改字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存 DHCPv6 接口配置并更新设备。

## 使用 CLI 命令配置 DHCPv6 接口

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- DHCPv6 命令

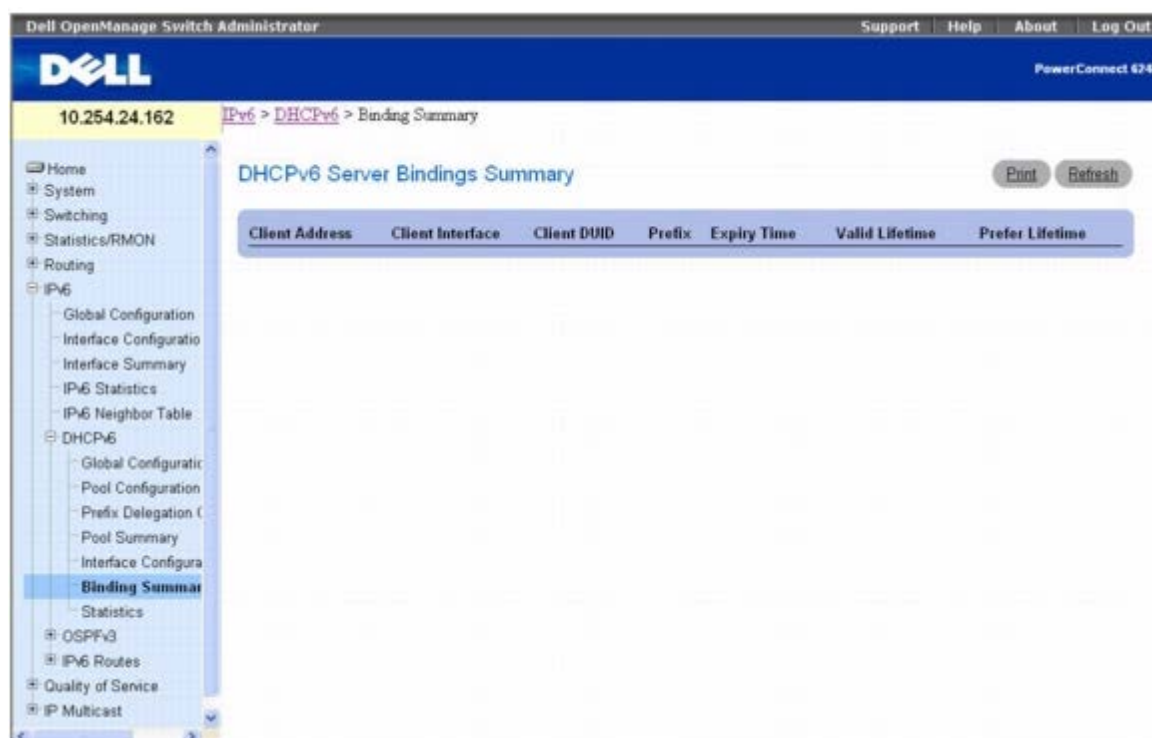
## DHCPv6 服务器捆绑摘要

**Server Bindings Summary** (服务器捆绑摘要) 页面用于显示所有 DHCPv6 服务器捆绑。

要显示此页面, 请在树视图中单击 **IPv6 @ DHCPv6 @ Bindings Summary** (捆绑摘要)。



图 11-14. 服务器捆绑摘要



**Server Bindings Summary** (服务器捆绑摘要) 页面包含以下字段:

**Client Address** (客户端地址) — 指定与捆绑关联的客户端的 IPv6 地址。

**Client Interface** (客户端接口) — 指定发生客户端捆绑的接口号。

**Client DUID** (客户端 DUID) — 指定客户端的 DHCPv6 唯一标识符。

**Prefix** (前缀) - 指定与此捆绑关联的前缀的类型。

**Expiry Time** (过期时间) — 指定在与捆绑关联的前缀过期之前所经过的秒数。

**Valid Lifetime** (有效使用寿命) — 指定与捆绑关联的前缀的有效使用寿命值 (以秒为单位)。

**Prefer Lifetime** (首选使用寿命) — 指定与捆绑关联的前缀的首选使用寿命值 (以秒为单位)。

## 使用 CLI 命令显示服务器捆绑

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

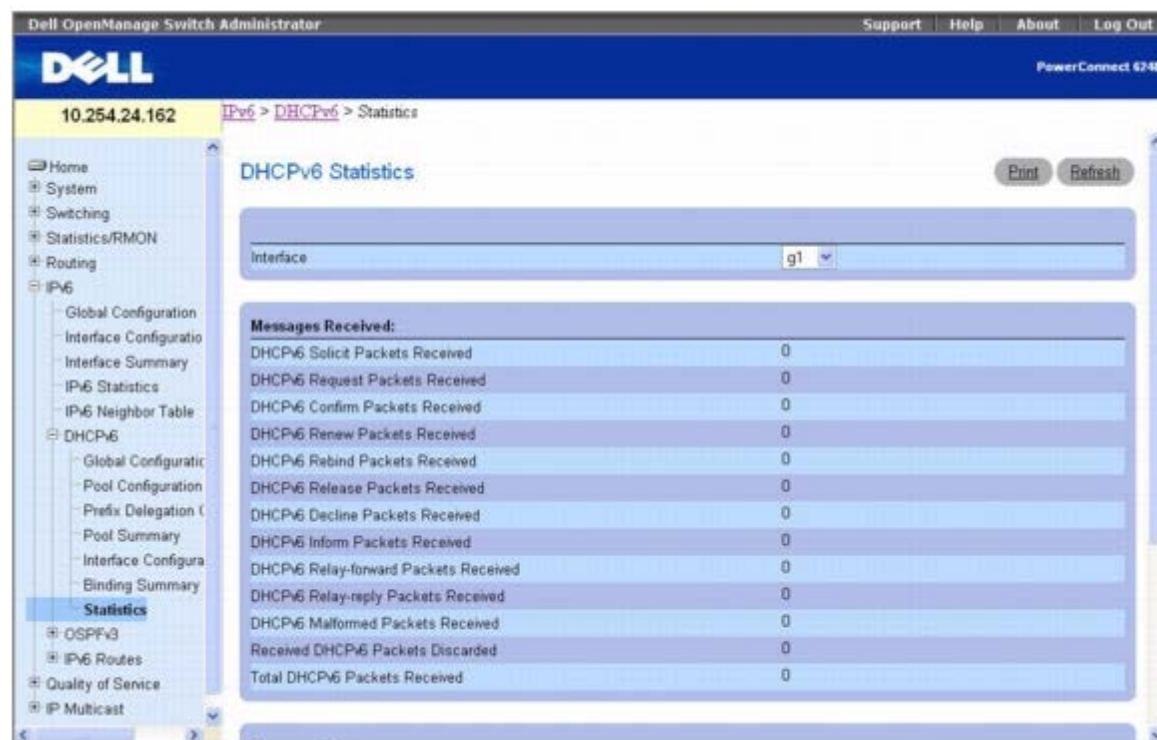
- DHCPv6 命令

## DHCPv6 统计数据

**DHCPv6 Statistics** (DHCPv6 统计数据) 页面用于显示一个或所有接口的 DHCPv6 统计数据。

要显示此页面, 请在树视图中单击 **IPv6** ® **DHCPv6** ® **Statistics** (统计数据)。

图 11-15. DHCPv6 统计数据



**DHCPv6 Statistics (DHCPv6 统计数据)** 页面会显示以下字段:

**Interface (接口)** — 选择要为其显示或配置数据的接口。选择 **All (全部)** 后, 系统将显示所有接口的数据。

接收到的信息

本节说明接收到信息的所有接口级别统计数据的集合。

**DHCPv6 Solicit Packets Received (接收到的 DHCPv6 恳求信息包)** — 指定恳求信息包的数目。

**DHCPv6 Request Packets Received (接收到的 DHCPv6 请求信息包)** — 指定请求信息包的数目。

**DHCPv6 Confirm Packets Received (接收到的 DHCPv6 确认信息包)** — 指定确认信息包的数目。

**DHCPv6 Renew Packets Received (接收到的 DHCPv6 更新信息包)** — 指定更新信息包的数目。

**DHCPv6 Rebind Packets Received (接收到的 DHCPv6 重捆信息包)** — 指定重捆信息包的数目。

**DHCPv6 Release Packets Received (接收到的 DHCPv6 发放信息包)** — 指定发放信息包的数目。

**DHCPv6 Decline Packets Received (接收到的 DHCPv6 拒绝信息包)** — 指定拒绝信息包的数目。

**DHCPv6 Inform Packets Received (接收到的 DHCPv6 通知信息包)** — 指定通知信息包的数目。

**DHCPv6 Relay-forward Packets Received (接收到的 DHCPv6 中继转发信息包)** — 指定中继转发信息包的数目。

**DHCPv6 Relay-reply Packets Received (接收到的 DHCPv6 中继答复信息包)** — 指定中继答复信息包的数目。

**DHCPv6 Malformed Packets Received (接收到的 DHCPv6 格式错误信息包)** — 指定格式错误信息包的数目。

**Received DHCPv6 Packets Discarded (接收到的丢弃 DHCPv6 信息包)** — 指定被丢弃的信息包的数目。

**Total DHCPv6 Packets Received (接收到的 DHCPv6 信息包总数)** — 指定接收到的信息包的总数。

发送的信息

本节说明发送信息的所有接口级别统计数据的集合。

**DHCPv6 Advertisement Packets Transmitted (发送的 DHCPv6 公布信息包)** — 指定公布信息包的数目。

**DHCPv6 Reply Packets Transmitted (发送的 DHCPv6 答复信息包)** — 指定答复信息包的数目。

**DHCPv6 Reconfig Packets Transmitted (发送的 DHCPv6 重新配置信息包)** — 指定重新配置信息包的数目。

**DHCPv6 Relay-forward Packets Transmitted** (发送的 **DHCPv6** 中继转发信息包) — 指定中继转发信息包的数目。

**DHCPv6 Relay-reply Packets Transmitted** (发送的 **DHCPv6** 中继答复信息包) — 指定中继答复信息包的数目。

**Total DHCPv6 Packets Sent** (发送的 **DHCPv6** 信息包总数) — 指定发送的信息包的总数。

**Clear** (清除) — 重置接口信息包计数器。

## 显示 **DHCPv6** 统计数据

□□□ 打开 **DHCPv6 Statistics** (**DHCPv6** 统计数据) 页面。

□□□ 从 **Interface** (接口) 下拉式菜单中选择要显示的接口。

系统将为选定的接口显示 **DHCPv6** 统计数据。

## 使用 **CLI** 命令显示 **DHCPv6** 统计数据

有关执行此功能的 **CLI** 命令的信息, 请参阅 «**CLI 参考指南**» 的以下章节:

- **DHCPv6** 命令

---

# OSPFv3

**OSPFv3** 是 IPv6 的开放最短路径优先 (**Open Shortest Path First**, **OSPF**) 路由协议。**OSPFv3** 在链路状态数据库、域间/域内、**AS** 外部路由和虚拟链路概念方面与 **OSPFv2** 相似。它与 **IPv4** 协议在很多方面都不相同, 包括以下方面: 通过本地链路地址实现对等; 协议是链路而非网络中心; 寻址语义已移动至叶 **LSA**, 最终均可用于 **IPv4** 和 **IPv6**。此外, 为了能够在通道上操作, 还支持点到点链路。

可以同时启用 **OSPF** 和 **OSPFv3**。**OSPF** 与 **IPv4** 结合使用, **OSPFv3** 则与 **IPv6** 结合使用。

**OSPFv3** 菜单页面包含一些网页链接, 这些网页可用于定义和显示 **OSPFv3** 参数和数据。要显示此页面, 请在树视图中单击 **IPv6** ® **OSPFv3**。

在此菜单页面中可以访问以下网页:

- [OSPFv3 配置](#)
- [OSPFv3 区域配置](#)
- [OSPFv3 末节区域摘要](#)
- [OSPFv3 区域范围配置](#)
- [OSPFv3 接口配置](#)
- [OSPFv3 接口统计数据](#)
- [OSPFv3 邻居](#)
- [OSPFv3 邻居列表](#)
- [OSPFv3 链路状态数据库](#)
- [OSPFv3 虚拟链路配置](#)
- [OSPFv3 虚拟链路摘要](#)
- [OSPFv3 路由重新分配配置](#)

- [OSPFv3 路由重新分配摘要](#)

## OSPFv3 配置

**OSPFv3 Configuration (OSPFv3 配置)** 页面用于为交换机激活并配置 OSPFv3。

要显示此页面，请在树视图中单击 **IPv6** **OSPFv3** **Configuration (配置)**。

图 11-16. OSPFv3 配置



**OSPFv3 Configuration (OSPFv3 配置)** 页面包含以下字段：

**Router ID (路由器 ID)** — 用于唯一标识自治系统 (AS) 中路由器的 32 位点分十进制格式整数。如果要更改路由器 ID，必须先禁用 OSPFv3。在设置新的路由器 ID 之后，必须重新启用 OSPFv3 才能使更改生效。虽然值 0.0.0.0 不是一个有效路由器 ID，但可作为默认值，并且必须在按下 **Apply Changes (应用更改)** 按钮之前进行更改。

**OSPFv3 Admin Mode (OSPFv3 管理模式)** — 从下拉式菜单中选择 **Enable (启用)** 或 **Disable (禁用)**。如果选择 **Enable (启用)**，将会为交换机激活 OSPFv3。默认值为 **Enable (启用)**。必须先配置 **Router ID (路由器 ID)**，然后才可操作 OSPFv3。也可以通过在 IPv6 路由器 OSPF 模式下发出 CLI 命令 `router-id` 完成上述操作。

**注：** OSPFv3 在路由器上被初始化之后，将一直保持被初始化的状态，直到路由器重置。

**ASBR Mode (ASBR 模式)** — 反映 ASBR 模式是 **Enabled (启用)** 还是 **Disabled (禁用)**。**Enable (启用)** 表示路由器是一种自治系统边界路由器。路由器若被配置为重新分发从其它协议获取的路线，将自动变成 ASBR。

**ABR Status (ABR 状态)** — 此字段的值为 **Enable (启用)** 或 **Disable (禁用)**。仅当配置有效时，才会显示此字段。**Enabled (启用)** 表示路由器是区域边界路由器。**Disabled (禁用)** 表示路由器不是区域边界路由器。

**Exit Overflow Interval (secs) (退出溢出间隔 [秒])** — 路由器进入溢出状态后，在尝试离开溢出状态之前应等待的秒数。这可让路由器重新产生非默认 AS 外部 LSA。如果输入 0，路由器将不会离开溢出状态，直到重新启动。范围是 0 至 2147483647 秒。

**External LSA Count (外部 LSA 计数)** — 链路状态数据库中的外部 (LS 类型 5) LSA (链路状态公布) 数目。

**External LSA Checksum (外部 LSA 校验和)** — 链路状态数据库中外部 LSA (链路状态公布) 的 LS 校验和总和。此总和用于确定路由器的链路状态数据库是否有变动，并用于比较两个路由器的链路状态数据库。

**New LSAs Originated (产生的新 LSA)** — 在任何指定的 OSPFv3 区域中，一个路由器会产生几个 LSA。每个路由器都会产生一个路由器

**LSA**。如果路由器还是任何区域网络的指定路由器，则会为这些网络产生网络 LSA。此值表示该路由器产生的 LSA 数目。

**LSAs Received** (收到的 LSA) — 已收到并被确定为新实例的 LSA (链路状态公布) 数目。此数字不包括更新的自我产生的 LSA 实例。

**External LSDB Limit** (外部 LSDB 限制) — 可以存储在数据库中的 AS 外部 LSA 的最大数目。值 -1 表示可存储的数目没有限制。有效值范围是 -1 至 2147483647。

**Default Metric** (默认跃点) — 设置重新分配的路由的默认跃点。如果已经设置一个跃点，此字段将显示默认跃点；如果先前未配置，则此字段为空。有效值是 1 至 16777214。

**Maximum Paths** (最大路径数) — 配置 OSPFv3 可以报告给指定目的地的最大路径数。有效值是 1 至 2。

**Default Information Originate** (产生默认信息) — 启用或禁用默认路由公布。请注意，只能在将 Default Information Originate (默认信息生成) 设置为 Enable (启用) 时，才能配置 Always (始终)、Metric (跃点) 和 Metric Type (跃点类型) 的值。如果将 Default Information Originate (默认信息生成) 设置为 Enable (启用)，并且已经配置 Always (始终)、Metric (跃点) 和 Metric Type (跃点类型) 的值，则将 Default Information Originate (默认信息生成) 重新设置为禁用时，便将 Always (始终)、Metric (跃点) 和 Metric Type (跃点类型) 的值设为默认值。

**Always** (始终) — 设置为 True (真) 时，设置路由器公布 ::/0。

**Metric** (跃点) — 指定默认路由的跃点。有效值是 0 至 16777214。

**Metric Type** (跃点类型) — 设置默认路由的跃点类型。有效值包括 External Type 1 (外部类型 1) 和 External Type 2 (外部类型 2)。

## 配置 OSPFv3

打开 **OSPFv3 Configuration (OSPFv3 配置)** 页面。

根据需要修改字段。

单击 **Apply Changes** (应用更改)。

系统将保存 OSPFv3 配置并更新设备。

## 使用 CLI 命令配置 OSPFv3

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- OSPFv3 命令

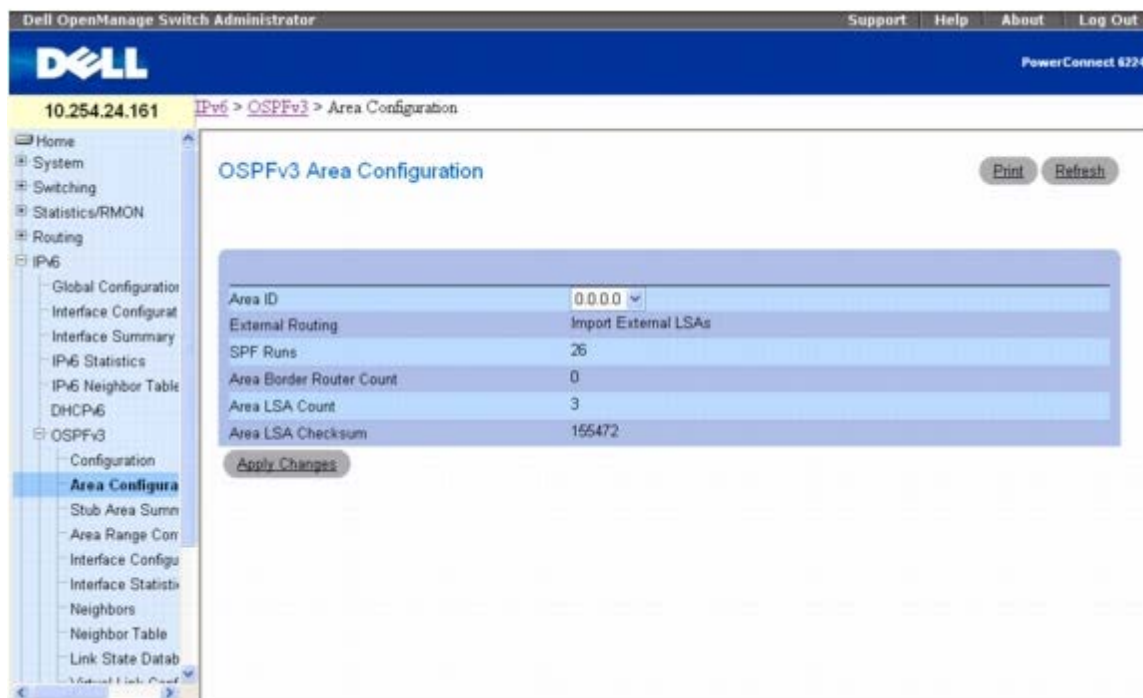
## OSPFv3 区域配置

**OSPFv3 Area Configuration (OSPFv3 区域配置)** 页面用于创建并配置 OSPFv3 区域。

要显示此页面，请在树视图中单击 **IPv6 @ OSPFv3 @ Area Configuration** (区域配置)。

图 11-17. OSPFv3 区域配置





**OSPFv3 Area Configuration (OSPFv3 区域配置)** 页面包含以下字段:

**Area ID (区域 ID)** — OSPFv3 区域。Area ID (区域 ID) 是一个 32 位点分十进制格式整数，用于唯一标识路由器接口所连接到的区域。

**External Routing (外部路由)** — 区域的路由器功能定义，包括 AS 外部 LSA 是否多路发送至整个区域。如果区域是末节区域，则可以使用这些选项配置外部路由功能，否则唯一的选项便是 **Import External LSAs (导入外部 LSA)**。

**SPF Runs (SPF 运行数)** — 使用此区域的链路状态数据库计算区域内部路由表的次数。此操作通常使用 **Dijkstra** 算法来完成。

**Area Border Router Count (区域边界路由器计数)** — 此区域内可到达的区域边界路由器的总数。初始值为零，在每个 SPF 通道中都要计算此值。

**Area LSA Count (区域 LSA 计数)** — 此区域链路状态数据库中的链路状态公布总数，不包括 AS 外部 LSA。

**Area LSA Checksum (区域 LSA 校验和)** — 在此区域的链路状态数据库中包含的链路状态公布的 LS 校验和的 32 位未签名总和。此总和不包括外部 (LS 类型 5) 链路状态公布。此总和用于确定路由器的链路状态数据库是否有变动，并用于比较两个路由器的链路状态数据库。此值为十六进制。

## 配置 OSPFv3 区域

□□□ 打开 **OSPFv3 Area Configuration (OSPFv3 区域配置)** 页面。

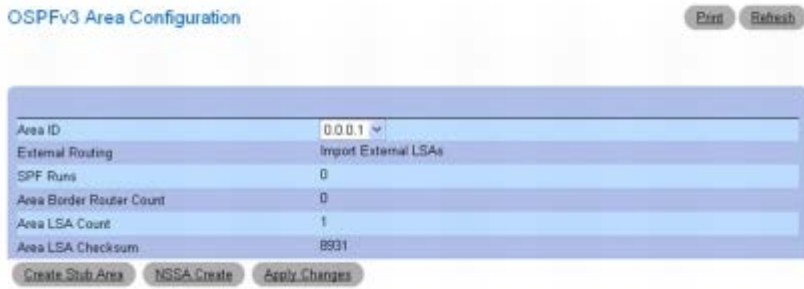
□□□ 根据需要修改字段。

□□□ 单击 **Apply Changes (应用更改)**。

系统将保存该配置并更新设备。

该网页将再次显示，并带有 **Create Stub Area (创建末节区域)** 和 **NSSA Create (NSSA 创建)** 按钮。

图 11-18. OSPFv3 区域配置 - 创建末节区域和 NSSA 创建



## 配置 OSPFv3 末节区域

□□□ 打开 **OSPFv3 Area Configuration (OSPFv3 区域配置)** 页面。

□□□ 根据需要修改字段。

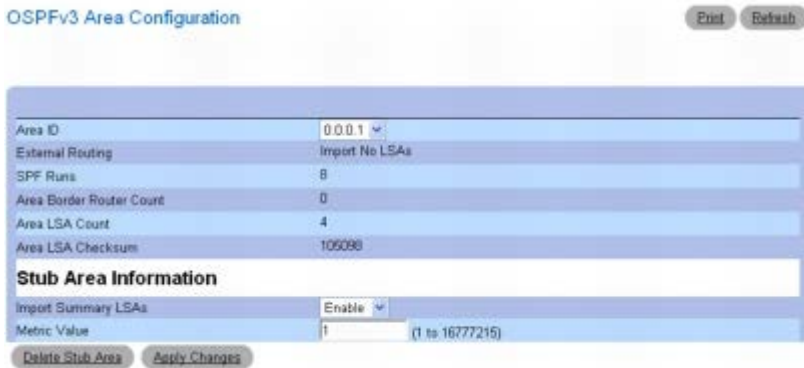
□□□ 单击 **Apply Changes** (应用更改)。

该网页将再次显示，并带有 **Create Stub Area** (创建末节区域) 和 **NSSA Create** (NSSA 创建) 按钮。请参阅[图 11-18](#)。

□□□ 单击 **Create Stub Area** (创建末节区域)。

系统将显示 **Stub Area Information** (末节区域信息) 字段。

图 11-19. OSPFv3 末节区域配置



□□□ 填写其余字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存末节区域信息并更新设备。

## 配置 OSPFv3 NSSA 区域

□□□ 打开 **OSPFv3 Area Configuration (OSPFv3 区域配置)** 页面。

□□□ 根据需要修改字段。

□□□ 单击 **Apply Changes** (应用更改)。

该网页将再次显示，并带有 **Create Stub Area** (创建末节区域) 和 **NSSA Create** (NSSA 创建) 按钮。请参阅[图 11-18](#)。

□□□ 在 **OSPFv3 Area Configuration (OSPFv3 区域配置)** 网页上单击 **NSSA Create** (NSSA 创建)。



该网页将再次显示，并且显示 NSSA 配置选项。

图 11-20. OSPFv3 区域配置 - NSSA

OSPFv3 Area Configuration	
Area ID	0.0.0.1
External Routing	Import NSSAs
SPF Runs	10
Area Border Router Count	0
Area LSA Count	3
Area LSA Checksum	9843
NSSA Specific Information	
Import Summary LSAs	Enable
Default Information Originate	False
Default Metric	10 (1 to 16777214)
Default Metric Type	Non-comparable Cost
Translator Role	Candidate
Translator Stability Interval	40 (0 to 3600)
No-Redistribute Mode	Enable
Translator State	Elected

□□□ 填写其余字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存 NSSA 信息并更新设备。

## 删除 OSPFv3 末节区域信息

□□□ 打开包含已配置末节区域信息的 **OSPFv3 Area Configuration (OSPFv3 区域配置)** 页面。

□□□ 单击 **Delete Stub Area** (删除末节区域)。

□□□ 单击 **Apply Changes** (应用更改)。

## 删除 OSPFv3 NSSA 信息

□□□ 打开包含已配置 NSSA 信息的 **OSPFv3 Area Configuration (OSPFv3 区域配置)** 页面。

□□□ 单击 **NSSA Delete** (NSSA 删除)。

□□□ 单击 **Apply Changes** (应用更改)。

## 使用 CLI 命令配置 OSPFv3 区域

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

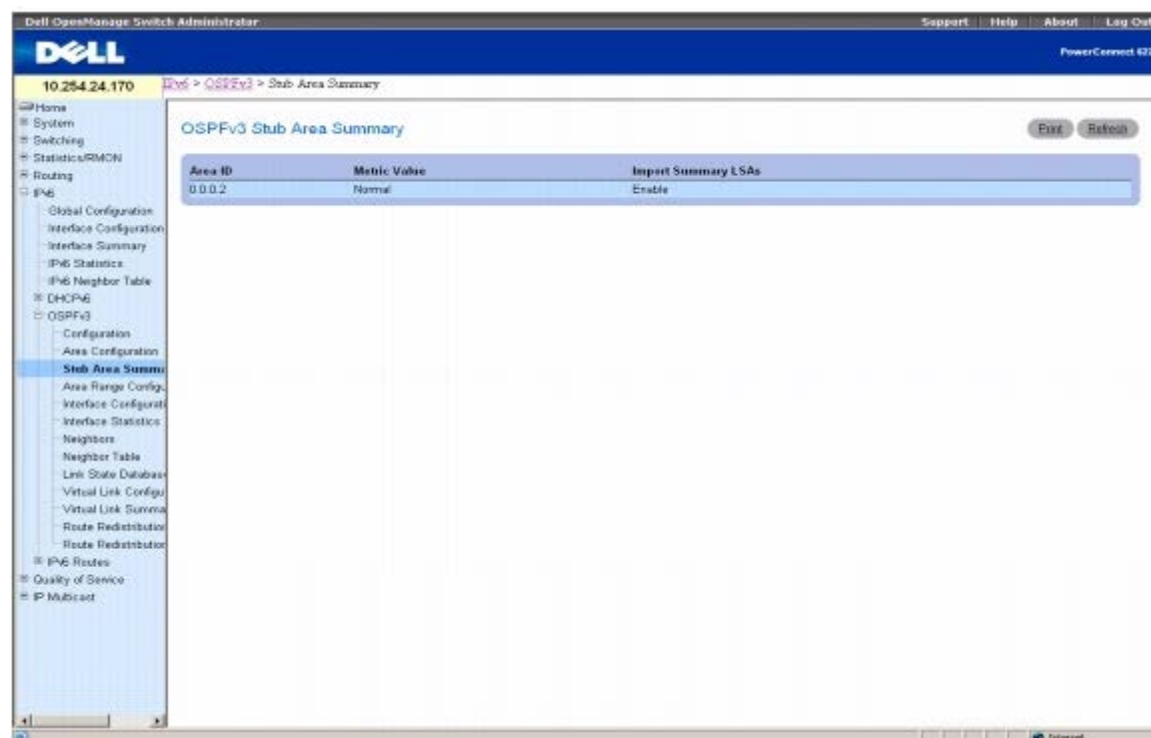
- OSPFv3 命令

## OSPFv3 末节区域摘要

**OSPFv3 Stub Area Summary** (OSPFv3 末节区域摘要) 页面用于显示 OSPFv3 末节区域详细信息。

要显示此页面, 请在树视图中单击 **IPv6** ® **OSPFv3** ® **Stub Area Summary** (末节区域摘要)。

图 11-21. OSPFv3 末节区域摘要



**OSPFv3 Stub Area Summary** (OSPFv3 末节区域摘要) 页面包含以下字段:

**Area ID** (区域 ID) — 末节区域的区域 ID。

**Metric Value** (跃点值) — 应用于公布到该区域的默认路由的跃点值。

**Import Summary LSAs** (导入摘要 LSA) — 是否启用或禁用导入摘要 LSA。

## 使用 CLI 命令显示 OSPFv3 末节区域摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

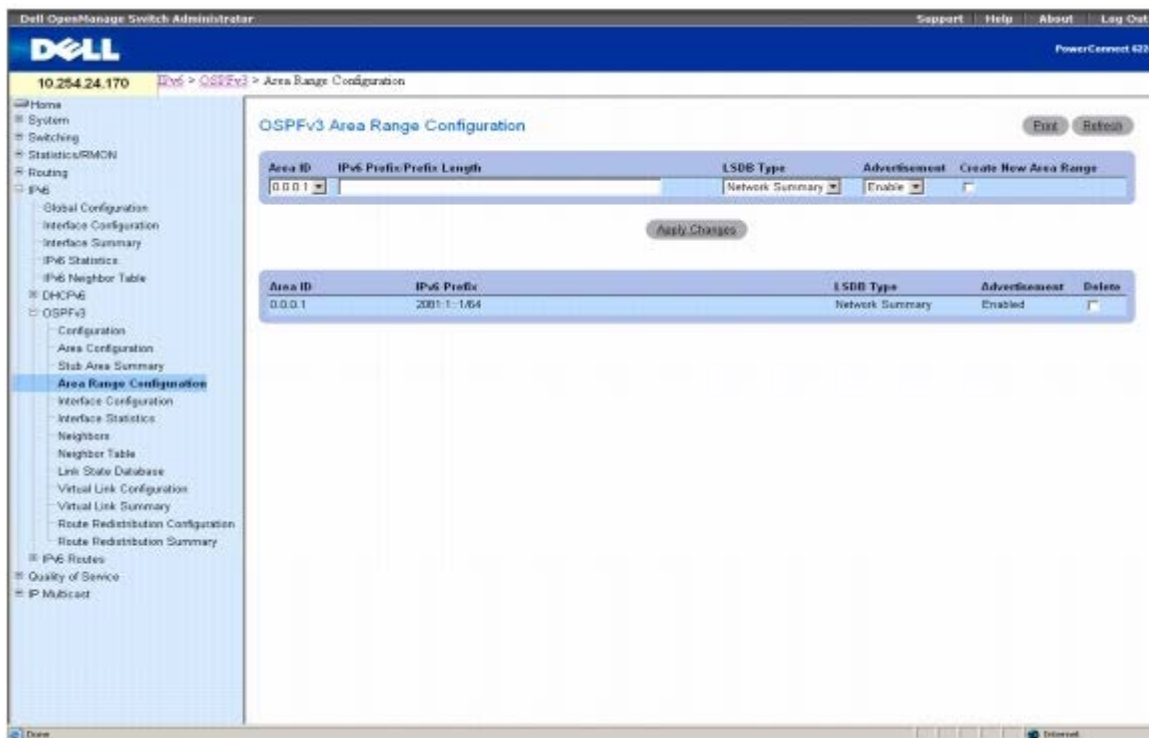
- OSPFv3 命令

## OSPFv3 区域范围配置

**OSPFv3 Area Range Configuration** (OSPFv3 区域范围配置) 页面用于配置 OSPFv3 区域范围。

要显示此页面, 请在树视图中单击 **IPv6** ® **OSPFv3** ® **Area Range Configuration** (区域范围配置)。

图 11-22. OSPFv3 区域范围配置



**OSPFv3 Area Range Configuration (OSPFv3 区域范围配置)** 页面包含以下字段:

**Area ID (区域 ID)** — 选择要为其配置数据的区域。

**IPv6 Prefix/Prefix Length (IPv6 前缀/前缀长度)** — 输入所选区域地址范围的 IPv6 前缀/前缀长度。

**LSDB Type (LSDB 类型)** — 选择与指定区域和地址范围关联的链路公布类型。默认类型为 Network Summary (网络摘要)。

**Advertisement (公布)** — 从下拉式菜单中选择 Enable (启用) 或 Disable (禁用)。如果选择 Enable (启用), 地址范围将通过网络摘要 LSA 在区域外部公布。默认值为 Enable (启用)。

**Create New Area Range (创建新的区域范围)** — 单击此复选框可使用指定的值创建新的 OSPFv3 区域范围。

**Area ID (区域 ID)** — OSPFv3 区域。

**IPv6 Prefix (IPv6 前缀)** — 区域地址范围的 IPv6 前缀。

**LSDB Type (LSDB 类型)** — 地址范围和区域的链路公布类型。

**Advertisement (公布)** — 地址范围和区域的公布模式。

**Delete (删除)** — 单击此复选框可删除指定的 OSPFv3 区域范围。

## 配置 OSPFv3 区域范围

□□□ 打开 **OSPFv3 Area Range Configuration (OSPFv3 区域范围配置)** 页面。

□□□ 根据需要修改字段。

□□□ 单击 **Apply Changes (应用更改)**。

系统将保存 OSPFv3 区域范围并更新设备。

## 使用 CLI 命令配置 OSPFv3 区域范围

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- OSPFv3 命令

## OSPFv3 接口配置

**OSPFv3 Interface Configuration** (OSPFv3 接口配置) 页面用于创建并配置 OSPFv3 接口。

要显示此页面,请在树视图中单击 **IPv6** ® **OSPFv3** ® **Interface Configuration** (接口配置)。

图 11-23. OSPFv3 接口配置



**OSPFv3 Interface Configuration** (OSPFv3 接口配置) 页面包含以下字段:

**Interface** (接口) — 选择要为其显示或配置数据的接口。

**IP Address** (IP 地址) — 接口的 IPv6 地址。

**OSPFv3 Admin Mode** (OSPFv3 管理模式) — 可以从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用)。默认值为 **Disable** (禁用)。可以在不启用 OSPFv3 Admin Mode (OSPFv3 管理模式) 的情况下配置 OSPFv3 参数,但是直到启用 Admin Mode (管理模式) 后,这些参数才生效。仅当启用 Admin Mode (管理模式) 后,才会显示以下信息: **State** (状态)、**Designated Router** (指定路由器)、**Backup Designated Router** (备份指定路由器)、**Number of Link Events** (链路事件数)、**LSA Ack Interval** (LSA 确认间隔) 和 **Metric Cost** (跃点成本)。为了 OSPFv3 完全发挥作用,接口必须具有有效的 IPv6 前缀/前缀长度。在接口配置模式下,通过 CLI 使用 `ipv6 address` 命令可以完成此操作。

OSPFv3 在路由器上被初始化之后,将一直保持被初始化的状态,直到路由器重置。

**OSPFv3 Area ID** (OSPFv3 区域 ID) — 输入唯一标识所选路由器接口连接到的 OSPFv3 区域的 32 位点分十进制整数。如果分配不存在的区域 ID,则使用默认值创建区域。

**Router Priority** (路由器优先级) — 输入所选接口的 OSPFv3 优先级。接口优先级的指定值范围是 0 至 255 间的整数。默认值为 1,路由器的优先级最高。值 0 表示路由器不适合成为此网络上的指定路由器。

**Retransmit Interval (secs)** (重新发送间隔 [秒]) — 输入指定接口的 OSPFv3 重新发送间隔。这是指属于此路由器接口的邻居的链路状态公布的间隔秒数。当重新发送数据库说明和链路状态请求信息包时,也可以使用此值。有效值的范围是 0 至 3600 秒 (1 小时)。默认值为 5 秒。

**Hello Interval (secs)** (问候间隔 [秒]) — 以秒为单位输入指定接口的 OSPFv3 问候间隔。对于连接到网络中的所有路由器而言,此参数必须相同。有效值范围是 1 到 65,535。默认值是 10 秒。

**Dead Interval (secs)** (无响应间隔 [秒]) — 为指定接口输入 OSPFv3 无响应间隔 (以秒为单位)。这是指路由器等待接收来自邻居路由器的问候信息包的时间。在此时间之后, 如果仍未收到问候信息包, 将认定邻居路由器已关闭。对于连接到网络中的所有路由器而言, 此参数必须相同。此值应乘以问候间隔 (例如 4)。有效值范围是 1 到 2147483647。默认值是 40。

**LSA Ack Interval (secs)** (LSA 确认间隔 [秒]) — 显示 LSA 确认信息包发送之间的秒数, 该值必须小于重新发送间隔。

**Interface Delay Interval (secs)** (接口延迟间隔 [秒]) — 输入指定接口的 OSPFv3 传输延迟。这是指在所选接口传输链路状态更新信息包估计所需的秒数。有效值的范围是 1 至 3600 秒 (1 小时)。默认值为 1 秒。

**MTU Ignore** (MTU 忽略) — 对收到的信息包禁用 OSPFv3 MTU 不匹配检测。默认值为 Disable (禁用)。

**Interface Type** (接口类型) — 输入接口类型, 可设置为广播模式或点到点模式。默认接口类型为广播。

**State** (状态) — 所选路由器接口的当前状态。下述状态之一:

- **Down** (关闭) — 这是初始的接口状态。在此状态下, 较低层的协议已指明此接口无法使用。在此状态下, 系统将接口参数设置为初始值。所有接口计时器均被禁用, 并且没有任何邻居与接口相关联。
- **Loopback** (回送) — 在此状态下, 路由器的网络接口以硬件或软件回送。接口不能用于常规数据通信。但是, 仍然有可能需要通过向接口发送 ICMP ping, 或者通过位错误检测等操作, 获取此接口质量的相关信息。因此, IP 信息包仍要求能够发送到处于 Loopback (回送) 状态的接口。为此, 这些接口在路由器 LSA 中公布为单一主机路由, 其目的地为 IP 接口地址。
- **Waiting** (等待) — 路由器正在尝试通过监测接收到的问候信息包来确定网络 (备份) 指定路由器的身份。在路由器过渡到等待状态以外的状态之前, 路由器无法成为 Backup Designated Router (备份指定路由器) 和 Designated Router (指定路由器)。这样能阻止对 (备份) 指定路由器进行不必要的更改。
- **Designated Router** (指定路由器) — 此路由器本身是所连网络上的指定路由器, 并且与连接到网络上的所有其它路由器均建立邻接关系。该路由器还必须为网络节点生成一个网络 LSA。网络 LSA 包含连接到网络上的所有路由器 (包括指定路由器本身) 的链路。
- **Backup Designated Router** (备份指定路由器) — 此路由器本身是所连网络上的备份指定路由器。如果现有的指定路由器发生故障, 则该路由器会升级为指定路由器。该路由器与连接到网络上的所有其它路由器均建立邻接关系。在多路发送过程中, 备份指定路由器执行的功能与指定路由器稍有不同。
- **Other Designated Router** (其它指定路由器) — 接口连接到广播或 NBMA 网络, 在该网络上已将其它路由器选择为指定路由器或备份指定路由器。路由器尝试与指定路由器和备份指定路由器形成邻接关系。

仅当启用 OSPFv3 管理模式后, 才显示 State (状态)。

**Designated Router** (指定路由器) — 此网络中的指定路由器向公布路由器显示的标识。此处按路由器 ID 来标识指定路由器。值 0.0.0.0 表示不存在指定路由器。仅当启用 OSPFv3 管理模式后, 才显示此字段。

**Backup Designated Router** (备份指定路由器) — 此网络中的备份指定路由器向公布路由器显示的标识。此处按路由器 ID 来标识备份指定路由器。如果不存在备份指定路由器, 则将该值设置为 0.0.0.0。仅当启用 OSPFv3 管理模式后, 才显示此字段。

**Number of Link Events** (链路事件数) — 这是指定 OSPFv3 接口更改其状态的次数。仅当启用 OSPFv3 管理模式后, 才显示此字段。

**Metric Cost** (跃点成本) — 输入此接口上的 TOS (服务类型) 成本值。跃点成本的范围介于 1 和 65,535 之间。仅当在接口上初始化 OSPFv3 时, 才可配置 Metric Cost (跃点成本)。

## 配置 OSPFv3 接口

打开 **OSPFv3 Interface Configuration** (OSPFv3 接口配置) 页面。

选择要配置 OSPFv3 的接口。

根据需要修改其余字段。

单击 **Apply Changes** (应用更改)。

系统将配置 OSPFv3 接口并更新设备。

## 使用 CLI 命令配置 OSPFv3 接口

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

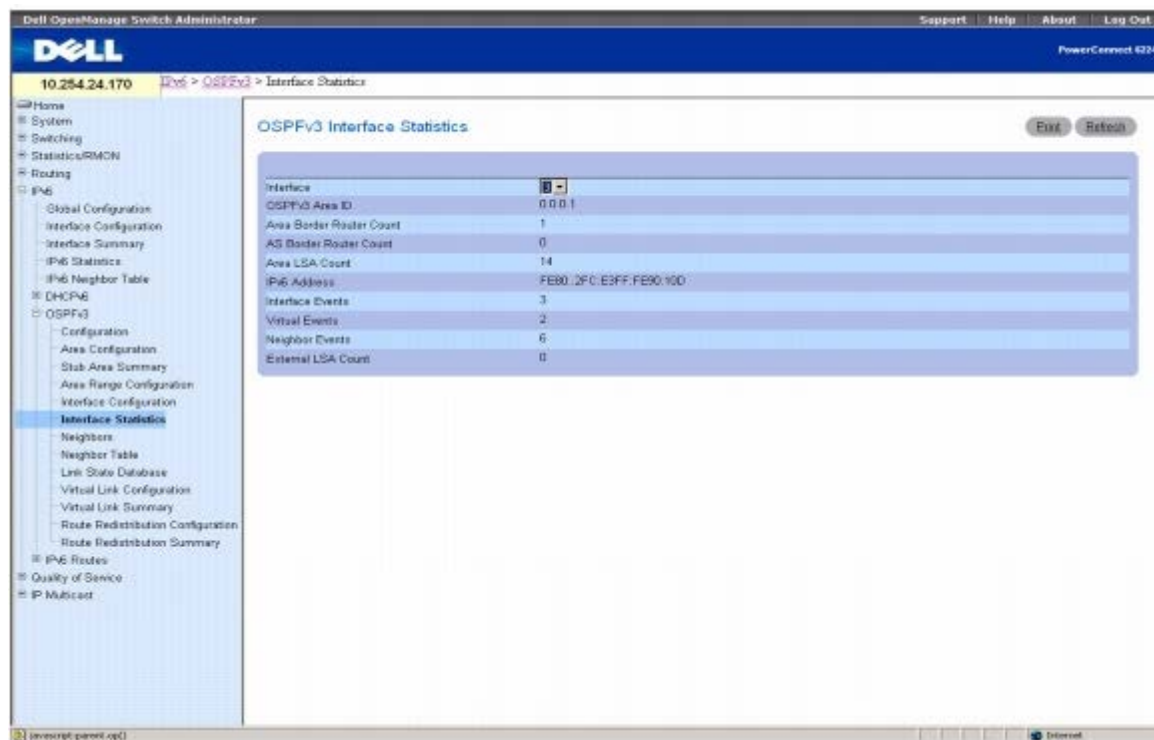
- OSPFv3 命令

## OSPFv3 接口统计数据

**OSPFv3 Interface Statistics** (OSPFv3 接口统计数据) 页面用于显示 OSPFv3 接口统计数据。仅当启用 OSPF 时，才显示此信息。

要显示此页面，请在树视图中单击 **IPv6** ® **OSPFv3** ® **Interface Statistics** (接口统计数据)。

图 11-24. OSPFv3 接口统计数据



**OSPFv3 Interface Statistics** (OSPFv3 接口统计数据) 页面会显示以下字段：

**Interface** (接口) — 选择要为其显示数据的接口。

**OSPF Area ID** (OSPF 区域 ID) — 所选路由器接口所属的 OSPF 区域。OSPF Area ID (OSPF 区域 ID) 是一个 32 位点分十进制格式整数，用于唯一标识接口所连接到的区域。

**Area Border Router Count** (区域边界路由器计数) — 此区域内可到达的区域边界路由器的总数。初始值为零，在每个 SPF 通道中都要计算此值。

**AS Border Router Count** (AS 边界路由器计数) — 此区域内可到达的自制系统边界路由器的总数。初始值为零，在每个 SPF 通道中都要计算此值。

**Area LSA Count** (区域 LSA 计数) — 此区域链路状态数据库中的链路状态公布总数，不包括 AS 外部 LSA。

**IPv6 Address** (IPv6 地址) - 接口的 IP 地址。

**Interface Events** (接口事件) — 指定 OSPF 接口更改其状态或发生错误的次数。

**Virtual Events** (虚拟事件) — 此虚拟链路中发生状态更改或出错的次数。

**Neighbor Events** (邻居事件) — 此邻居关系更改其状态的次数或错误发生的次数。

**External LSA Count** (外部 LSA 计数) — 链路状态数据库中的外部 (LS 类型 5) 链路状态公布的数目。



## 显示 OSPFv3 接口统计数据

□□□ 打开 **OSPFv3 Interface Statistics** (OSPFv3 接口统计数据) 页面。

□□□ 从 **Interface** (接口) 下拉式菜单中选择要显示的接口。

系统将显示接口的统计数据。

## 使用 CLI 命令显示 OSPFv3 接口统计数据

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

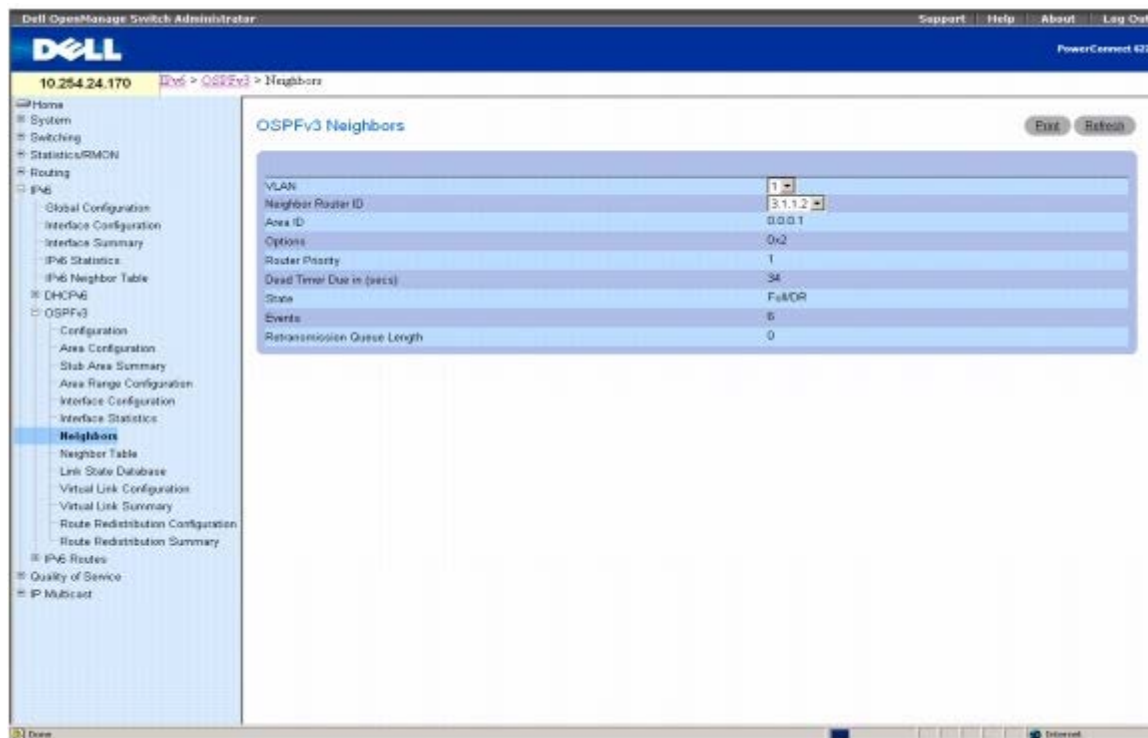
- OSPFv3 命令

## OSPFv3 邻居

**OSPFv3 Neighbors** (OSPFv3 邻居) 页面用于显示所选邻居 ID 的 OSPF 邻居配置。指定某个特定邻居 ID 时, 将给定有关该邻居的详细信息。仅当启用 OSPF 且接口具有邻居时, 才显示邻居信息。IP 地址就是邻居的 IP 地址。

要显示此页面, 请在树视图中单击 **IPv6** ® **OSPFv3** ® **Neighbors** (邻居)。

图 11-25. OSPFv3 邻居



**OSPFv3 Neighbors** (OSPFv3 邻居) 页面包含以下字段:

**Interface** (接口) — 选择要为其显示或配置数据的接口。

**Neighbor Router ID** (邻居路由器 ID) — 选择要为其显示数据的邻居的 IP 地址。

**Area ID** (区域 ID) — 点分十进制格式的 32 位整数, 用于标识邻居路由器。

**Options** (选项) — 邻居所支持的可选 OSPF 功能。邻居的可选 OSPF 功能也会列在问候信息包中。这样, 如果在某些关键 OSPF 功能中存在不匹配情况, 便可拒绝接收到的问候信息包 (即, 邻居关系甚至没有开始形成)。



**Router Priority** (路由器优先级) — 显示指定邻居的 OSPF 优先级。邻居优先级是一个介于 0 至 255 的整数。值 0 表示路由器无法成为此网络上的指定路由器。

**Dead Timer Due in (secs)** (故障计时器到期时间 [秒]) — 如果问候信息包没有到达, 则指定在邻居宣布故障之前所经过的时间。

**State** (状态) — 邻居可以具有以下状态:

- **Down** (故障) — 这是邻居对话的初始状态。它表示最近没有从邻居接收到任何信息。在 NBMA 网络上, 虽然频率减少, 但是仍会将问候信息包发送到故障邻居。
- **Attempt** (尝试) — 此状态仅适用于连接到 NBMA 网络的邻居。它表示最近没有从邻居接收到任何信息, 但是应更加努力地与邻居取得联系。通过按照问候间隔发送邻居问候信息包来实现此操作。
- **Init** — 此状态表示最近已收到来自邻居的问候信息包, 但是, 尚未与邻居建立双向通信 (即路由器本身没有出现在邻居的问候信息包中)。此状态 (或更高状态) 的所有邻居均列在从关联接口发送的问候信息包中。
- **2-Way** (双向) — 在此状态下, 两个路由器之间的通信是双向的。双向通信已由问候协议操作来确保。在开始建立邻接关系的短时间内, 该状态是最高级状态。(备份) 指定路由器是从双向或更高状态下的邻居集内选择的。
- **Exchange Start** (交换开始) — 这是在两个邻居路由器之间创建邻接关系的第一步。此步骤的目标是决定哪个路由器是主路由器, 以及决定初始 DD 顺序号。在此状态或更高状态下的邻居对话称为邻接关系。
- **Exchange** (交换) — 在此状态下, 路由器正在通过向邻居发送数据库说明信息包来说明整个链路状态数据库。在此状态下, 也会发送链路状态请求信息包来询问邻居最近的 LSA。交换状态或更高状态下的所有邻接关系均用于多路发送过程。这些邻接关系完全能够发送和接收所有类型的 OSPF 路由协议信息包。
- **Loading** (正在载入) — 在此状态下, 将向邻居发送链路状态请求信息包, 询问在交换状态下已经发现 (但尚未接收到) 的最近 LSA。
- **Full** (完全) — 在此状态下, 邻居路由器完全邻接。现在, 这些邻接关系将显示在路由器 LSA 和网络 LSA 中。

**Events** (事件) — 此邻居关系更改其状态的次数或错误发生的次数。

**Retransmission Queue Length** (重新发送队列长度) — 重新发送队列的当前长度。

## 显示 OSPFv3 邻居

打开 **OSPFv3 Neighbors** (OSPFv3 邻居) 页面。

从 **Interface** (接口) 下拉式菜单中选择要显示的接口。

选择要显示的 **Neighbor Router ID** (邻居路由器 ID)。

系统将显示所选接口 **Neighbor ID** (邻居 ID) 的统计数据。

## 使用 CLI 命令显示 OSPFv3 邻居

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

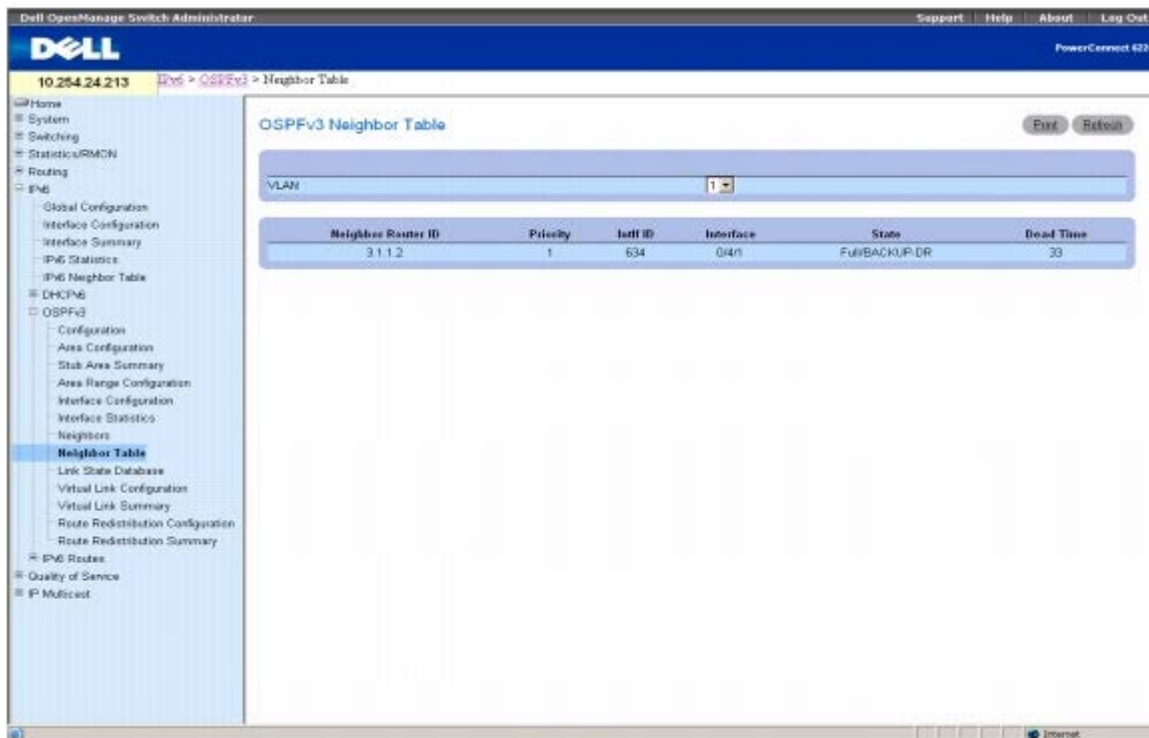
- OSPFv3 命令

## OSPFv3 邻居列表

**OSPFv3 Neighbor Table** (OSPFv3 邻居列表) 页面用于显示 OSPFv3 邻居表列表。指定某个特定邻居 ID 时, 将给定邻居的详细信息。仅当启用 OSPF 时, 才显示邻居列表。

要显示此页面, 请在树视图中单击 **IPv6** ® **OSPFv3** ® **Neighbor Table** (邻居列表)。

图 11-26. OSPFv3 邻居列表



**OSPFv3 Neighbor Table (OSPFv3 邻居列表)** 页面包含以下字段:

**Interface (接口)** — 选择要为其显示或配置数据的接口。

**Neighbor Router ID (邻居路由器 ID)** — 点分十进制格式的 32 位整数, 用于表示邻居接口。

**Priority (优先级)** — 此邻居在指定路由器选择算法中的优先级。值 0 表示邻居不适合成为此网络上的指定路由器。

**IntfID** — 此链路上邻居在其问候信息包中公布的接口 ID。

**Interface (接口)** — 标识邻居接口索引的插槽/端口。

**State (状态)** — 与此邻居的关系的状态。

**Dead Time (无响应时间)** — 自从邻接邻居接收到上一问候所经过的秒数。对于状态小于或等于 **Init** 的邻居, 将此值设置为 0。

## 显示 OSPFv3 邻居列表

□□□ 打开 **OSPFv3 Neighbor Table (OSPFv3 邻居列表)** 页面。

□□□ 从 **Interface (接口)** 下拉式菜单中选择要显示的接口。

系统将显示所选接口的 OSPF 邻居列表。

## 使用 CLI 命令显示 OSPFv3 邻居列表

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

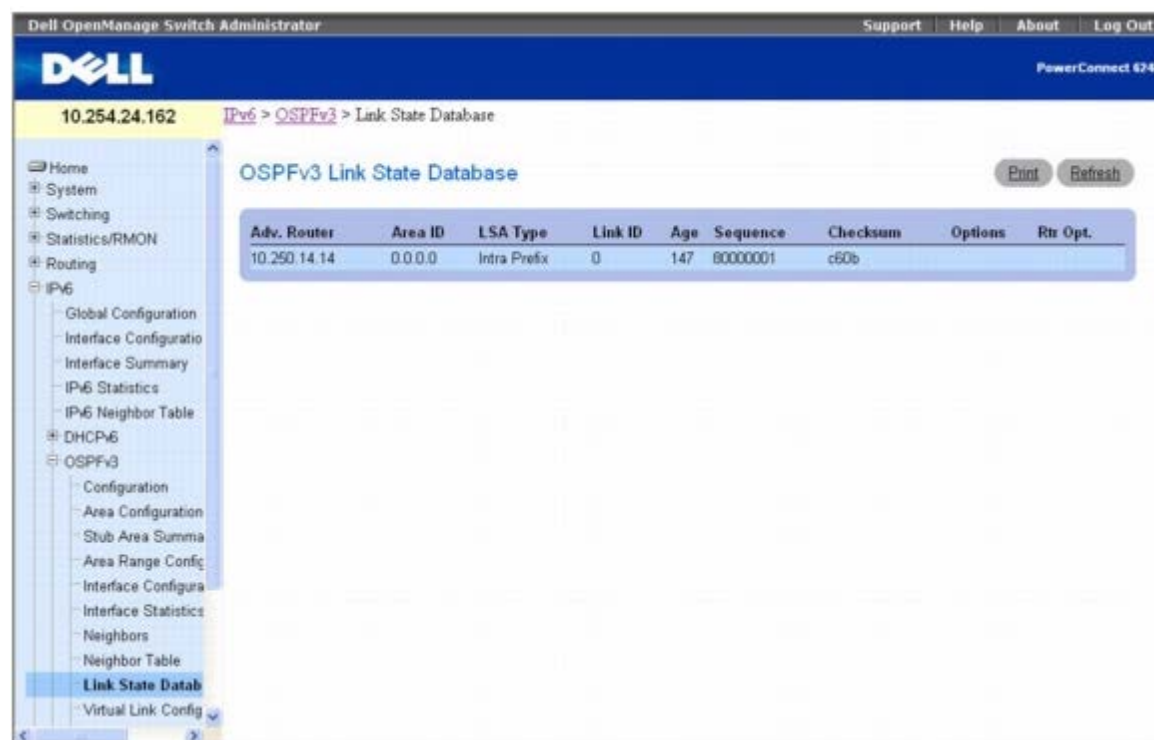
- OSPFv3 命令

## OSPFv3 链路状态数据库

**OSPFv3 Link State Database (OSPFv3 链路状态数据库)** 页面用于显示链路状态数据库。

要显示此页面，请在树视图中单击 **IPv6 ® OSPFv3 ® Link State Database (链路状态数据库)**。

图 11-27. OSPFv3 链路状态数据库



**OSPFv3 Link State Database (OSPFv3 链路状态数据库)** 页面包含以下字段：

**Adv. Router** (公布路由器) — 用于唯一标识自治系统 (AS) 中路由器的 32 位点分十进制格式整数。Router ID (路由器 ID) 是在 OSPFv3 Configuration (OSPFv3 配置) 页面上设置的。

**Area ID** (区域 ID) — 其中一个路由器接口连接到的 OSPF 区域的 ID。Area ID (区域 ID) 是一个 32 位点分十进制格式整数，用于唯一标识接口连接到的区域。

**LSA Type** (LSA 类型) — 链路状态公布的格式和功能。RFC 2740 A.4 小节中定义的类型可以是：

- Router-LSA (路由器 LSA)
- Network-LSA (网络 LSA)
- Inter-Area-Prefix-LSA (域间前缀 LSA)
- Inter-Area-Router-LSA (域间路由器 LSA)
- AS-External-LSA (AS 外部 LSA)
- Type-7-LSA (类型 7 LSA)
- Link-LSA (链路 LSA)
- Intra-Area-Prefix-LSA (域内前缀 LSA)

**Link ID** (链路 ID) — 链路状态 ID 标识公布正在描述的路由域。LS ID 的值取决于公布的 LS 类型。

**Age** (存在时间) — 自从链路状态第一次公布后所经过的时间 (单位为秒)。

**Sequence** (顺序) — 顺序号字段是签名的 32 位整数。它用于检测旧的和重复的链路状态公布。顺序号越大，公布越新。

**Checksum** (校验和) — 校验和用于检测公布中数据是否损坏。当公布正在多路发送或保留在路由器内存中时，可能发生这种损坏。此字段是公布全部内容的校验和，除了 LS 存在时间字段。

**Options** (选项) — 链路状态公布标头中的 **Options** (选项) 字段表示哪些可选功能与公布相关联。选项如下:

- V6 — 当清除此选项时, 会从 IPv6 路由计算中排除链路。
- E — 说明大量发送 AS 外部 LSA 的方式。
- MC — 说明是否按照规范转发 IP 多点传送数据包。
- N — 说明如何处理类型 7 LSA。
- R — 表明发送方是否是一个活动路由器。R 选项是路由器比特, 当清除此选项时, 将无法计算通过公布节点的路由。
- DC — 说明系统如何处理请求电路。

**Rtr Opt.** — 显示特定于路由器的选项。

## 使用 CLI 命令显示 OSPFv3 链路状态数据库

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

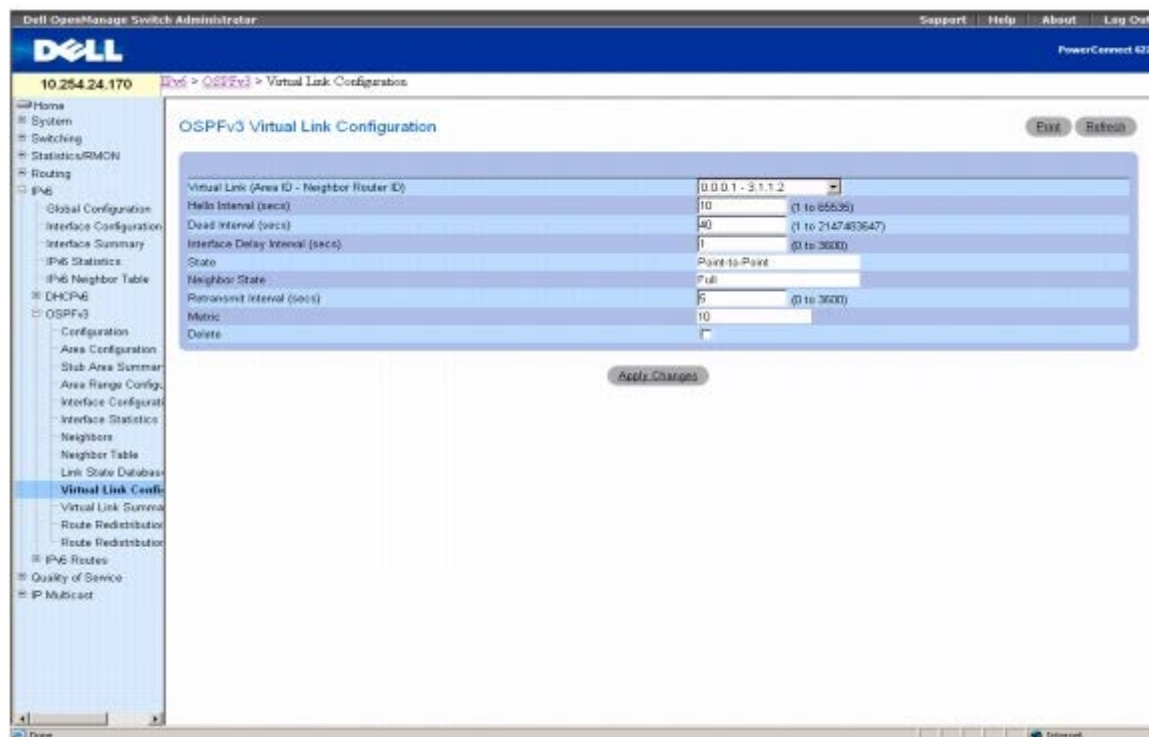
- OSPFv3 命令

## OSPFv3 虚拟链路配置

**OSPFv3 Virtual Link Configuration** (OSPFv3 虚拟链路配置) 页面用于定义新的虚拟链路或配置现有虚拟链路。要显示此页面, 必须通过 OSPFv3 Area Configuration (OSPFv3 区域配置) 页面定义一个有效 OSPFv3 区域。

要显示此页面, 请在树视图中单击 **IPv6** ® **OSPFv3** ® **Virtual Link Configuration** (虚拟链路配置)。

图 11-28. OSPFv3 虚拟链路配置



**OSPFv3 Virtual Link Configuration** (OSPFv3 虚拟链路配置) 页面包含以下字段:

**Create New Virtual Link** (创建新的虚拟链路) — 从下拉式菜单中选择此选项可定义新的虚拟链路。虚拟链路标识的区域部分是固定的: 系

系统将提示您在新屏幕上输入 Neighbor Router ID (邻居路由器 ID)。

**Virtual Link (Area ID - Neighbor Router ID)** (虚拟链路 [区域 ID - 邻居路由器 ID]) — 选择要显示或配置数据的虚拟链路。它包括 Area ID (区域 ID) 和 Neighbor Router ID (邻居路由器 ID)。

**Hello Interval (secs)** (问候间隔 [秒]) — 以秒为单位输入指定接口的 OSPF 问候间隔。对于连接到网络中的所有路由器而言, 此参数必须相同。有效值范围是 1 到 65,535。默认值是 10 秒。

**Dead Interval (secs)** (无响应间隔 [秒]) — 以秒为单位输入指定接口的 OSPF 无响应间隔。这是指路由器等待接收来自邻居路由器的问候信息包的时间。在此时间之后, 如果仍未收到问候信息包, 将认定邻居路由器已关闭。对于连接到网络中的所有路由器而言, 此参数必须相同。此值应乘以问候间隔 (例如 4)。有效值范围是 1 到 2147483647。默认值是 40。

**Interface Delay Interval (secs)** (接口延迟间隔 [秒]) — 输入指定接口的 OSPF 传输延迟。这是指在所选接口传输链路状态更新信息包估计所需的秒数。有效值的范围是 1 至 3600 秒 (1 小时)。默认值为 1 秒。

**State** (状态) — 所选虚拟链路的当前状态。下述状态之一:

- **Down** (关闭) — 这是初始的接口状态。在此状态下, 较低层的协议已指明此接口无法使用。在此状态下, 系统将接口参数设置为初始值。所有接口计时器均被禁用, 并且没有任何邻居与接口相关联。
- **Waiting** (等待) — 路由器正在尝试通过监测接收到的问候信息包来确定 (备份) 指定路由器的身份。在路由器过渡到等待状态以外的状态之前, 路由器无法成为 Backup Designated Router (备份指定路由器) 和 Designated Router (指定路由器)。这样能阻止对 (备份) 指定路由器进行不必要的更改。
- **Point-to-Point** (点到点) — 接口可操作, 并且连接到虚拟链路。在进入此状态时, 路由器会尝试与邻居路由器建立邻接关系。每隔问候间隔时间 (秒) 便向邻居发送问候信息包。
- **Designated Router** (指定路由器) — 此路由器本身是所连网络上的指定路由器, 并且与连接到网络上的所有其它路由器均建立邻接关系。该路由器还必须为网络节点生成一个网络 LSA。网络 LSA 包含连接到网络上的所有路由器 (包括指定路由器本身) 的链路。
- **Backup Designated Router** (备份指定路由器) — 此路由器本身是所连网络上的备份指定路由器。如果现有的指定路由器发生故障, 则该路由器会升级为指定路由器。该路由器与连接到网络上的所有其它路由器均建立邻接关系。在多路发送过程中, 备份指定路由器执行的功能与指定路由器稍有不同。
- **Other Designated Router** (其它指定路由器) — 接口连接到广播或 NBMA 网络, 在该网络上已将其它路由器选择为指定路由器或备份指定路由器。路由器尝试与指定路由器和备份指定路由器形成邻接关系。

**Neighbor State** (邻居状态) — 虚拟邻居关系的状态。

**Retransmit Interval** (重新发送间隔) — 输入指定接口的 OSPF 重新发送间隔。这是指属于此路由器接口的邻居的链路状态公布的间隔秒数。当重新发送数据库说明和链路状态请求信息包时, 也可以使用此值。有效值的范围是 1 至 3600 秒 (1 小时)。默认值为 5 秒。

**Metric** (跃点) — 虚拟链路使用的跃点值。

**Delete** (删除) — 从路由器配置中删除指定的虚拟链路。

## 创建新的虚拟链路

□□□ 打开 **OSPFv3 Virtual Link Configuration (OSPFv3 虚拟链路配置)** 页面。

□□□ 从下拉式菜单中选择 **Create New Virtual Link** (创建新的虚拟链路) 以定义新的虚拟链路。

□□□ 输入 **Neighbor Router ID** (邻居路由器 ID)。

□□□ 单击 **Create** (创建)。

系统将创建新的链路, 并返回 **Virtual Link Configuration** (虚拟链路配置) 页面。

## 配置虚拟链路

□□□ 打开 **OSPFv3 Virtual Link Configuration (OSPFv3 虚拟链路配置)** 页面。

- 选择要配置的虚拟链路。
- 根据需要修改其余字段。
- 单击 **Apply Changes** (应用更改)。
- 系统将配置 OSPFv3 虚拟链路并更新设备。

## 使用 CLI 命令配置 OSPFv3 虚拟链路

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

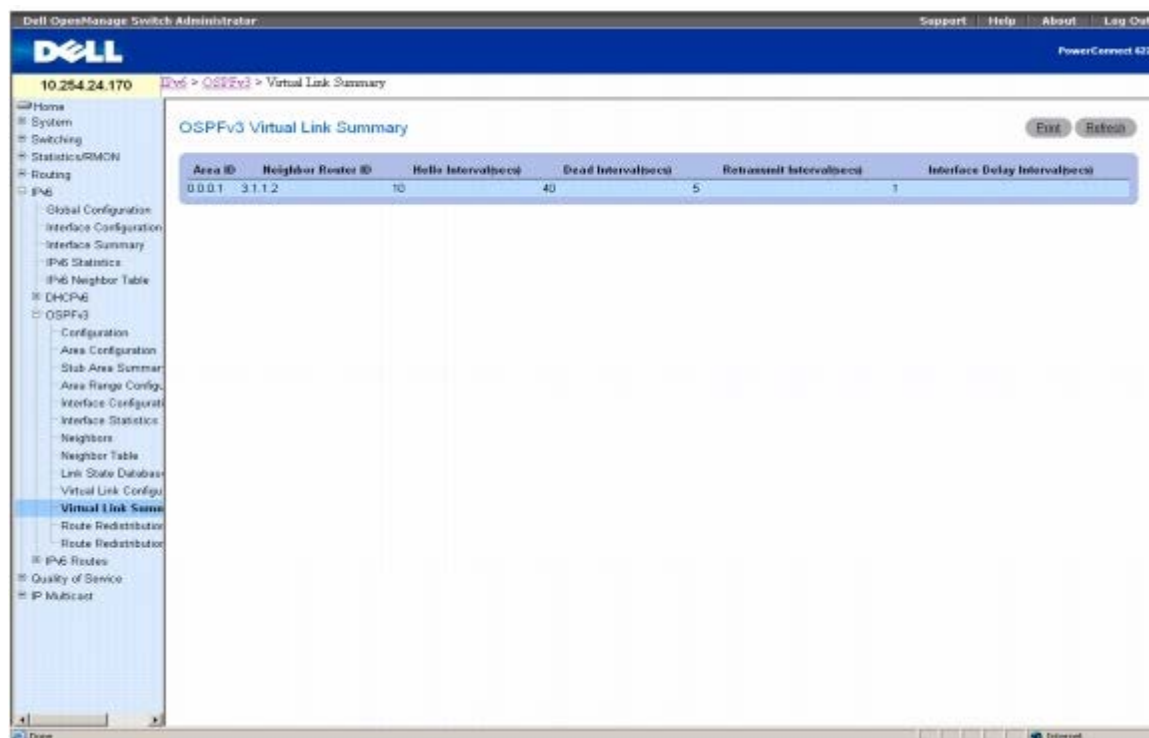
- OSPFv3 命令

## OSPFv3 虚拟链路摘要

**OSPFv3 Virtual Link Summary** (OSPFv3 虚拟链路摘要) 页面用于按 Area ID (区域 ID) 和 Neighbor Router ID (邻居路由器 ID) 显示虚拟链路数据。

要显示此页面，请在树视图中单击 **IPv6** ® **OSPFv3** ® **Virtual Link Summary** (虚拟链路摘要)。

图 11-29. OSPFv3 虚拟链路摘要



**OSPFv3 Virtual Link Summary** (OSPFv3 虚拟链路摘要) 页面会显示以下字段：

**Area ID** (区域 ID) — 要显示其数据的虚拟链路标识的区域 ID 部分。Area ID (区域 ID) 和 Neighbor Router ID (邻居路由器 ID) 共同定义虚拟链路。

**Neighbor Router ID** (邻居路由器 ID) — 虚拟链路标识的邻居部分。可以在与公共 (非主干网) 区域具有接口的任何区域边界路由器对之间配置虚拟链路。

**Hello Interval (secs)** (问候间隔 [秒]) — 虚拟链路的 OSPF 问候间隔 (秒)。对于连接到网络中的所有路由器而言，问候间隔值必须相同。



**Dead Interval (secs)** (无响应间隔 [秒]) — 虚拟链路的 OSPF 无响应间隔 (秒)。这是指路由器等待接收来自邻居路由器的问候信息包的时间。在此时间之后, 如果仍未收到问候信息包, 将认定邻居路由器已关闭。对于连接到公共网络的所有路由器而言, 此参数必须相同, 并且必须是问候间隔的倍数 (即, 4)。

**Retransmit Interval (secs)** (重新发送间隔 [秒]) — 虚拟链路的 OSPF 重新发送间隔 (秒)。该字段指定属于此路由器接口的邻接关系的链路状态公布的间隔时间。当重新发送数据库说明和链路状态请求信息包时, 也可以使用此值。

**Interface Delay Interval (secs)** (接口延迟间隔 [秒]) — 虚拟链路的 OSPF 发送延迟 (单位为秒)。它指定在此接口传输链路状态更新信息包估计所需的秒数。

## 使用 CLI 命令显示 OSPFv3 虚拟链路摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

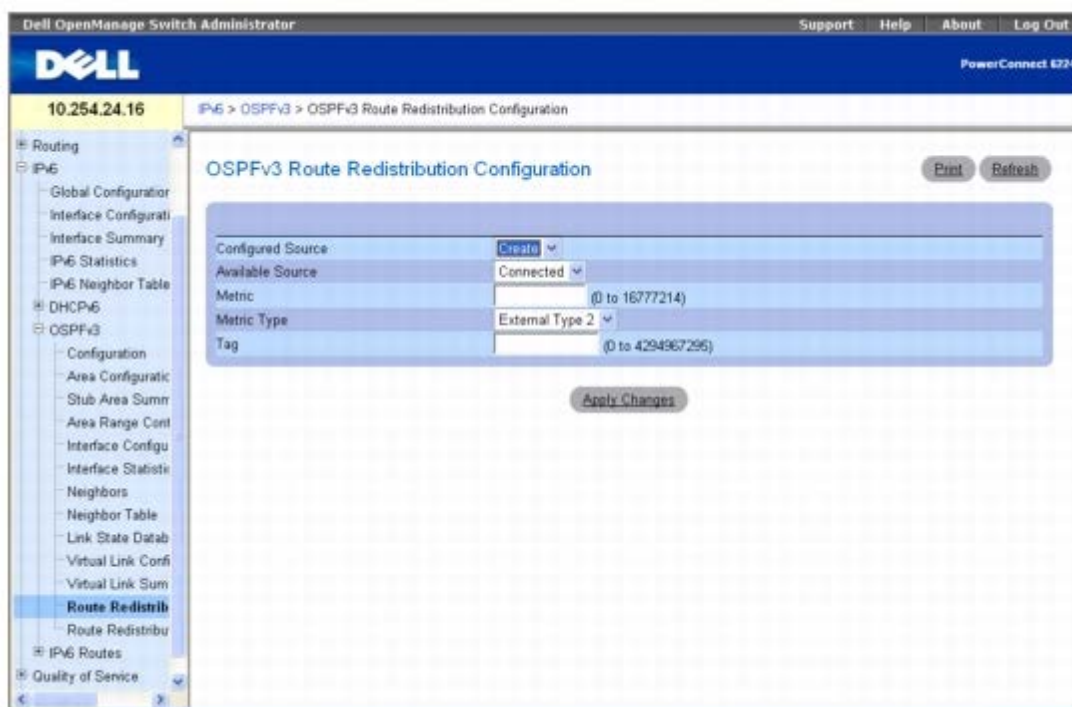
- OSPFv3 命令

## OSPFv3 路由重新分配配置

**OSPFv3 Route Redistribution Configuration** (OSPFv3 路由重新分配配置) 页面用于配置路由重新分配。

要显示此页面, 请在树视图中单击 **IPv6** ® **OSPFv3** ® **Route Redistribution Configuration** (路由重新分配配置)。

图 11-30. OSPFv3 路由重新分配配置



**OSPFv3 Route Redistribution Configuration** (OSPFv3 路由重新分配配置) 页面包含以下字段:

**Configured Source** (配置的来源) — 此下拉式菜单是一个动态选择器, 填充的只是由 OSPF 为重新分配目的而配置的那些源路由。选择框中最顶端的选项是 Create (创建), 允许配置 Available Source (可用源) 路由中的其它源路由。有效值包括 Static (静态)、Connected (已连接) 和 Create (创建)。

**Available Source** (可用源) — 此下拉式菜单是一个动态选择器, 填充的只是由 OSPF 为重新分配目的而先前尚未配置的那些源路由。仅当将 Create (创建) 选项选择为 Configured Source (配置的来源) 时, 才显示此菜单。有效值包括 Static (静态) 和 Connected (已连接)。

**Metric** (跃点) — 设置要用作重新分配的路由跃点的跃点值。如果来源是预配置来源并可以修改, 则此字段显示跃点。有效值是 0 至 16777214。



**Metric Type** (跃点类型) — 设置重新分配的路由的 OSPF 跃点类型。

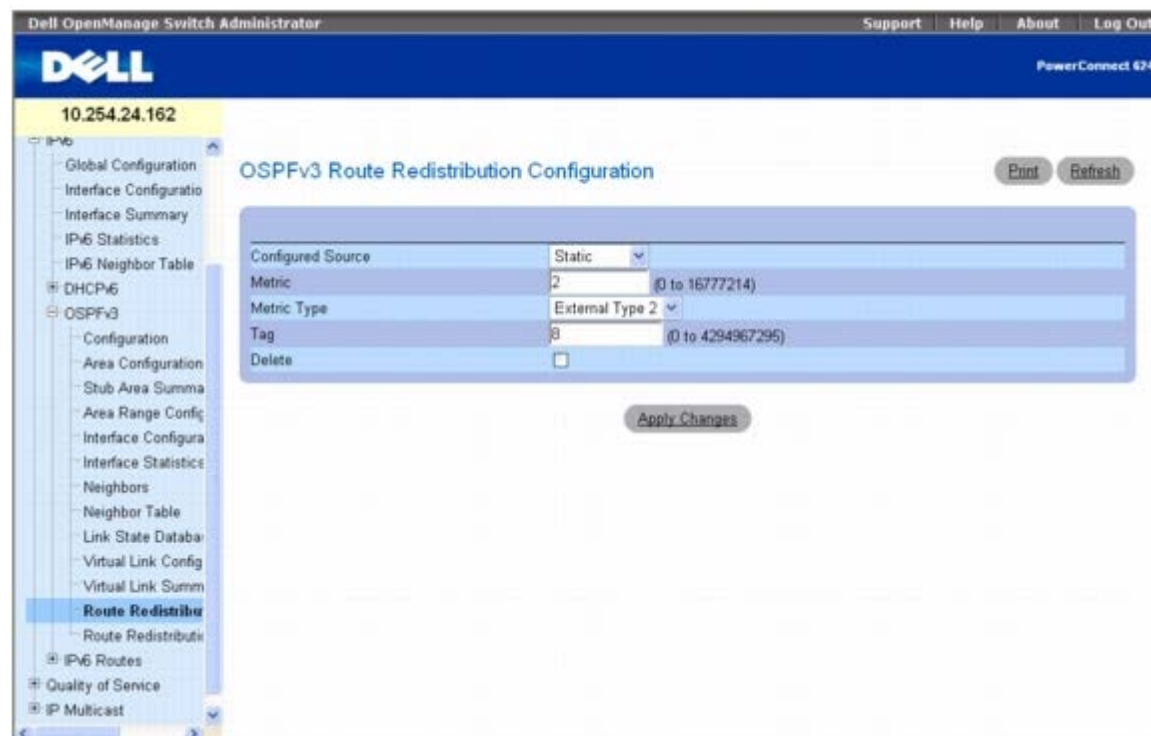
**Tag** (标签) — 设置重新分配的路由中的标签字段。如果来源是预配置来源，则此字段显示标签，否则显示 0。有效值是 0 至 4294967295。

## 配置 OSPFv3 路由重新分配

□□□ 打开 **OSPFv3 Route Redistribution Configuration** (OSPFv3 路由重新分配配置) 页面。

□□□ 指定 **Create** (创建) 以设置新的配置来源，或者指定 **Connected** (已连接) 或 **Static** (静态) 以修改现有的配置来源。

图 11-31. OSPFv3 路由重新分配配置 - 配置来源



□□□ 根据需要设置或修改其余的字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将配置 OSPFv3 的所选路由重新分配并更新设备。

## 使用 CLI 命令配置 OSPFv3 路由重新分配

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

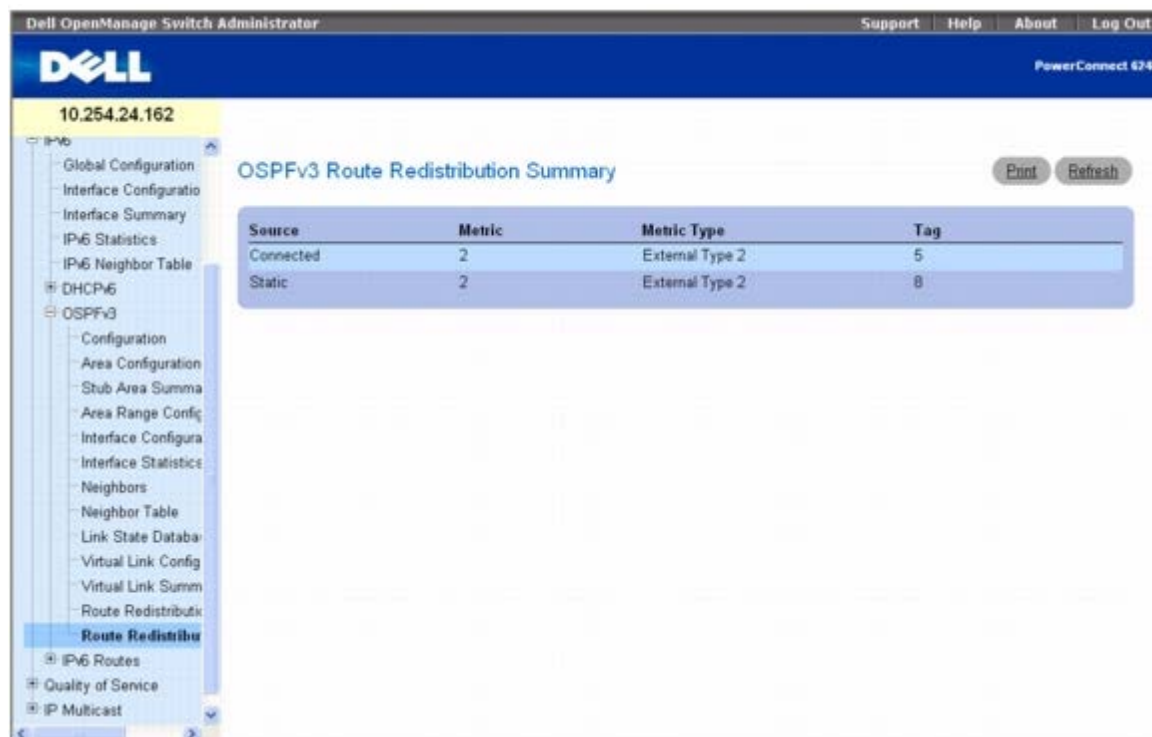
- OSPFv3 命令

## OSPFv3 路由重新分配摘要

**OSPFv3 Route Redistribution Summary** (OSPFv3 路由重新分配摘要) 页面用于按来源显示路由重新分配设置。

要显示此页面，请在树视图中单击 **IPv6 @ OSPFv3 @ Route Redistribution Summary** (路由重新分配摘要)。

图 11-32. OSPFv3 路由重新分配摘要



**OSPFv3 Route Redistribution Summary** (OSPFv3 路由重新分配摘要) 页面会显示以下字段:

**Source** (来源) — OSPF 要重新分配的来源路由。

**Metric** (跃点) — 为源路由指定重新分配的路由的跃点。未配置时, 将显示 **Unconfigured** (未配置)。

**Metric Type** (跃点类型) — 重新分配的路由的 OSPF 跃点类型。

**Tag** (标签) — 重新分配的路由中的标签字段。如果来源是预配置的来源, 则此字段显示标签, 否则显示 0。

## 使用 CLI 命令显示 OSPFv3 路由重新分配摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- OSPFv3 命令

## IPv6 路由

**IPv6 Routes** (IPv6 路由) 菜单页面包含一些网页链接, 这些页面用于定义和显示 IPv6 路由参数和数据。要显示此页面, 请在树视图中单击 **IPv6 ® IPv6 Routes** (IPv6 路由)。在此菜单页面中可以访问以下网页:

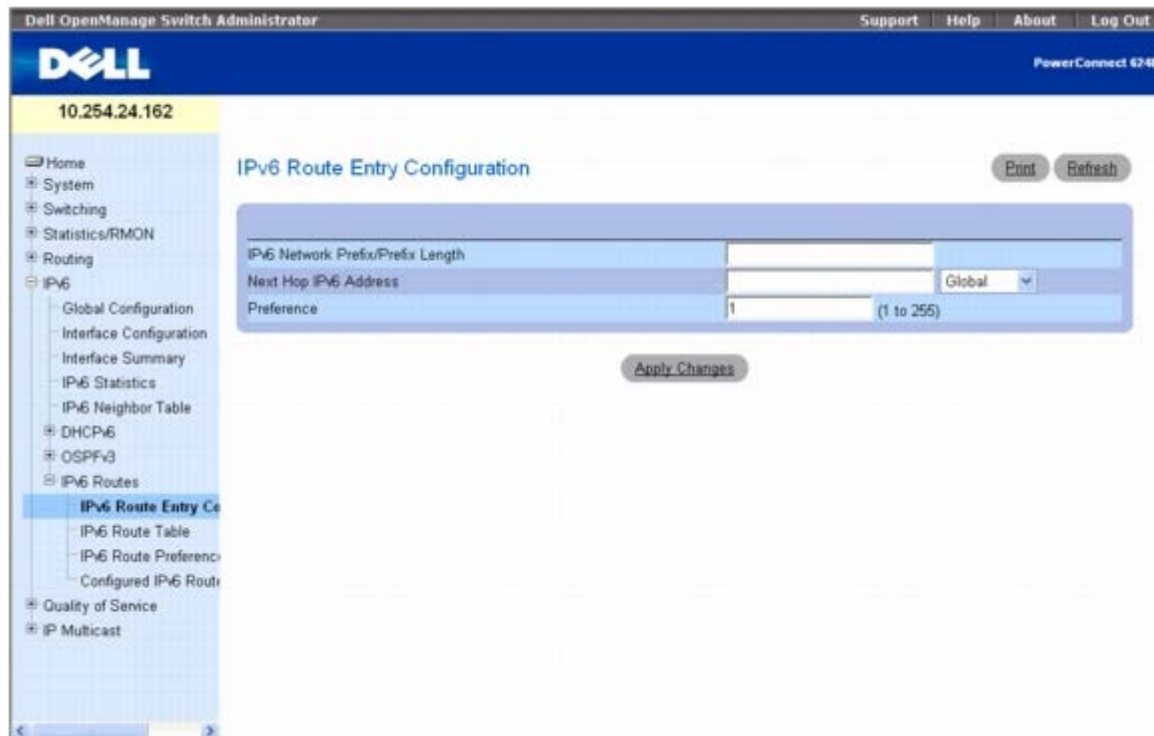
- [IPv6 路由条目配置](#)
- [IPv6 路由表](#)
- [IPv6 路由优先级](#)
- [已配置 IPv6 路由](#)

## IPv6 路由条目配置

**IPv6 Route Entry Configuration (IPv6 路由条目配置)** 页面用于配置 IPv6 路由的信息。

要显示此页面，请在树视图中单击 **IPv6** ® **IPv6 Routes (IPv6 路由)** ® **IPv6 Route Entry Configuration (IPv6 路由条目配置)**。

图 11-33. IPv6 路由条目配置



**IPv6 Route Entry Configuration (IPv6 路由条目配置)** 页面包含以下字段：

**IPv6 Network Prefix/PrefixLength (IPv6 网络前缀/前缀长度)** — 输入有效 IPv6 网络地址和前缀。

**Next Hop IPv6 Address (下一跃距 IPv6 地址)** — 输入 IPv6 下一跃距地址。如果指定的下一跃距 IPv6 地址为本地链路 IPv6 地址，则指定本地链路 IPv6 下一跃距地址的接口。从下拉式菜单中选择 **Global (全局)** 或 **Link-local (本地链路)** 以应用此地址。

**Preference (优先级)** — 输入给定路由的优先级值。有效值范围是 1 至 255，默认值为 1。

## 配置 IPv6 路由条目

□□□ 打开 **IPv6 Route Entry Configuration (IPv6 路由条目配置)** 页面。

□□□ 根据需要修改字段。

□□□ 单击 **Apply Changes (应用更改)**。

系统将配置 IPv6 路由条目并更新设备。

## 使用 CLI 命令配置路由条目

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

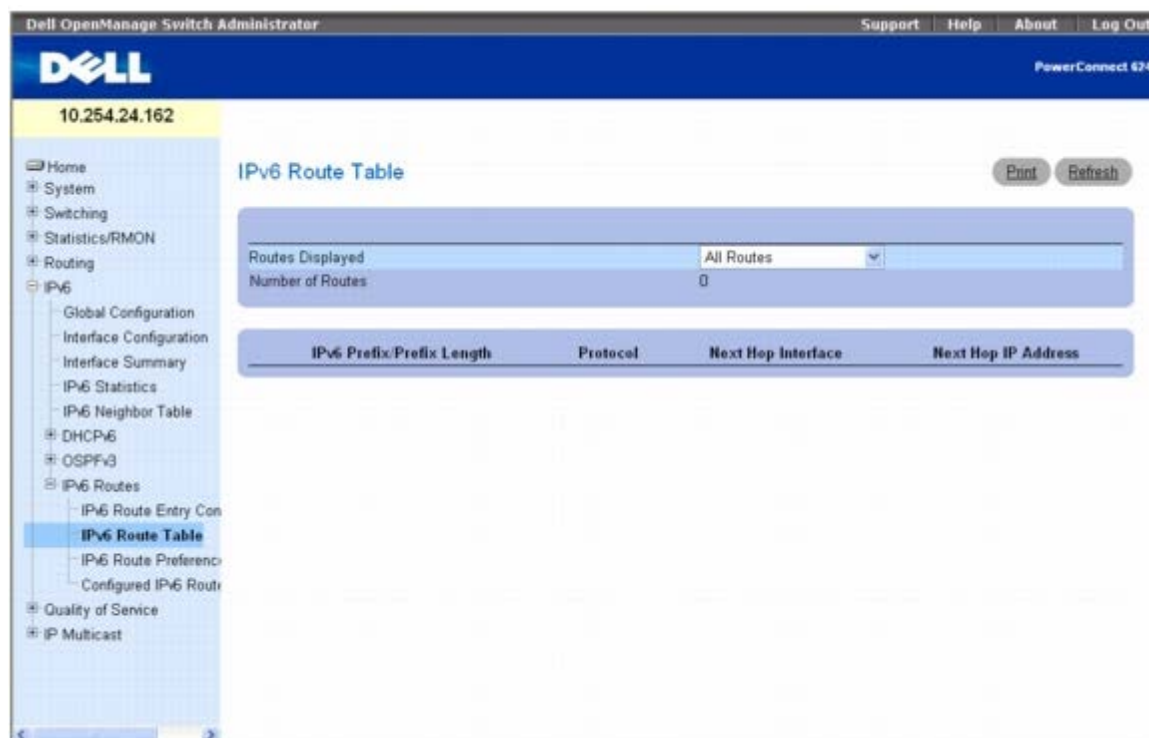
- IPv6 路由命令

## IPv6 路由表

**IPv6 Route Table (IPv6 路由表)** 页面用于显示所有活动的 IPv6 路由及其设置。

要显示此页面，请在树视图中单击 **IPv6** ® **IPv6 Routes (IPv6 路由)** ® **IPv6 Route Table (IPv6 路由表)**。

图 11-34. IPv6 路由表



**IPv6 Route Table (IPv6 路由表)** 页面包含以下字段：

**Routes Displayed** (显示的路由) — 从下拉式菜单中选择可查看 **Configured Routes** (已配置路由)、**Best Routes** (最佳路由) 或 **All Routes** (所有路由)。

**Number of Routes** (路由数) — 显示路由表中所选路由类型的活动路由/最佳路由的总数。

**IPv6 Prefix/Prefix Length** (IPv6 前缀/前缀长度) — 显示活动路由的网络前缀和前缀长度。

**Protocol** (协议) — 显示活动路由的协议类型。

**Next Hop Interface** (下一跃距接口) — 显示路由处于活动状态的接口。

**Next Hop IP Address** (下一跃距 IP 地址) — 显示活动路由的下一跃距 IPv6 地址。

## 显示 IPv6 路由表

□□□ 打开 **IPv6 Route Table (IPv6 路由表)** 页面。

□□□ 从 **Routes Displayed** (显示的路由) 字段中选择要显示的路由类型。

系统将显示选定的路由。

## 使用 CLI 命令显示 IPv6 路由表

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

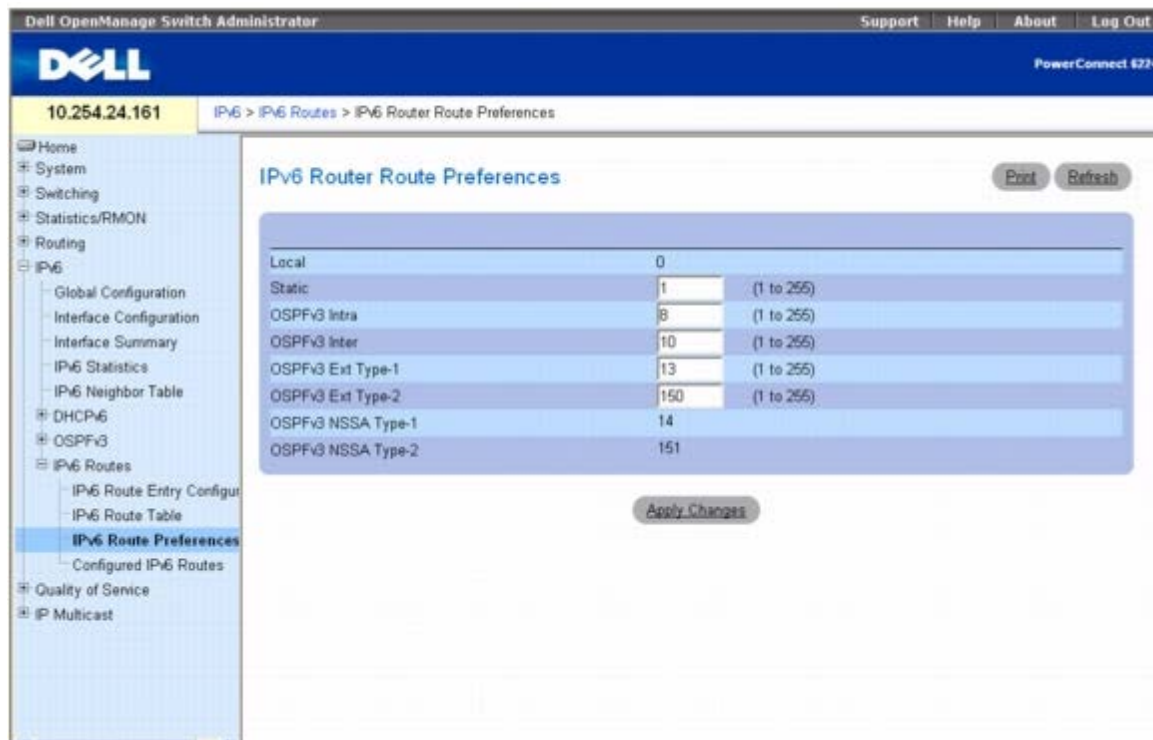
- IPv6 路由命令

## IPv6 路由优先级

**IPv6 Route Preferences (IPv6 路由优先级)** 页面用于配置每个协议的默认优先级。这些值是 1 至 255 范围内的任意值，与路由跃点无关。大多数路由协议使用路由跃点来确定协议已知的最短路径，与任何其它协议无关。通过选择优先级值最小的路由，可选择到目的地的最佳路由。当存在多个到目的地的路由时，可使用优先级值来确定首选路由。如果优先级值相同，则选择具有最佳路由跃点的路由。要避免跃点不匹配问题，必须为每个协议配置不同的首选值。

要显示此页面，请在树视图中单击 **IPv6** ® **IPv6 Routes (IPv6 路由)** ® **IPv6 Route Preferences (IPv6 路由优先级)**。

图 11-35. IPv6 路由优先级



**IPv6 Route Preferences (IPv6 路由优先级)** 页面包含下面所示的字段。在每种情况下，值最小表示优先级最高。

**Local** (本地) — 显示本地优先级，且不可配置。值为 0，优先级最高。

**Static** (静态) — 路由器的静态路由优先级值。默认值为 1。范围是 1 至 255。

**OSPFv3 Intra (OSPFv3 域内)** — 路由器中 OSPFv3 域内路由优先级值。默认值为 8。范围是 1 至 255。OSPFv3 规格要求必须根据以下顺序为通过 OSPFv3 获取的路由指定优先级：域内 < 域间 < 类型 1 < 类型 2。

**OSPFv3 Inter (OSPFv3 域间)** — 路由器中 OSPFv3 域间路由优先级值。默认值为 10。范围是 1 至 255。OSPFv3 规格要求必须根据以下顺序为通过 OSPFv3 获取的路由指定优先级：域内 < 域间 < 类型 1 < 类型 2。

**OSPFv3 Type-1 (OSPFv3 类型 1)** — 路由器中 OSPFv3 类型 1 路由优先级值。默认值为 13。范围是 1 至 255。OSPFv3 规格要求必须根据以下顺序为通过 OSPFv3 获取的路由指定优先级：域内 < 域间 < 类型 1 < 类型 2。

**OSPFv3 Type-2 (OSPFv3 类型 2)** — 路由器中 OSPFv3 类型 2 路由优先级值。默认值为 150。范围是 1 至 255。OSPFv3 规格要求必须根据以下顺序为通过 OSPFv3 获取的路由指定优先级：域内 < 域间 < 类型 1 < 类型 2。

**OSPFv3 NSSA Type-1 (OSPFv3 NSSA 类型 1)** — 显示路由器中 OSPFv3 NSSA 类型 1 路由优先级值。

**OSPFv3 NSSA Type-2 (OSPFv3 NSSA 类型 2)** — 显示路由器中 OSPFv3 NSSA 类型 2 路由优先级值。

### 配置 IPv6 路由优先级

□□□ 打开 **IPv6 Route Preferences (IPv6 路由优先级)** 页面。

□□□ 为每个协议配置默认优先级。

□□□ 单击 **Apply Changes** (应用更改)。

系统将配置 IPv6 路由优先级并更新设备。

## 使用 CLI 命令配置 IPv6 路由优先级

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

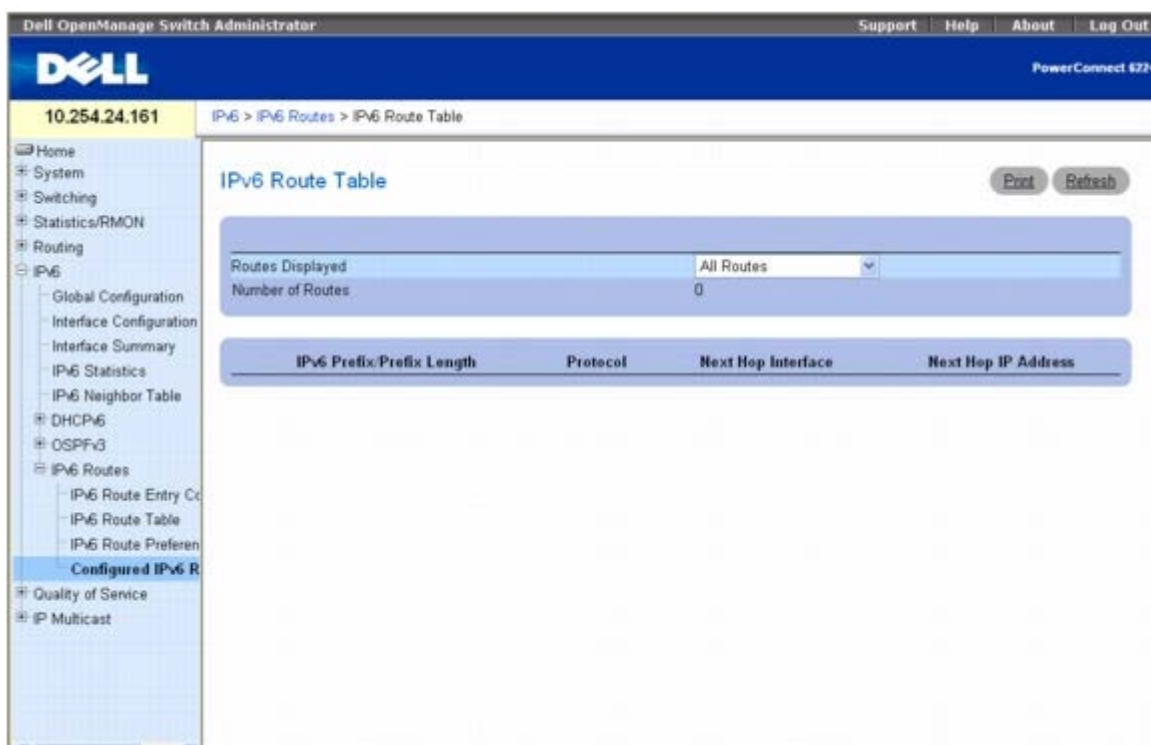
- IPv6Routing 命令

## 已配置 IPv6 路由

**Configured IPv6 Routes** (已配置 IPv6 路由) 页面用于显示选定的 IPv6 路由。

要显示此页面, 请在树视图中单击 **IPv6** ® **IPv6 Routes** (IPv6 路由) ® **Configured IPv6 Routes** (已配置 IPv6 路由)。

图 11-36. 已配置 IPv6 路由



**Configured IPv6 Routes** (已配置 IPv6 路由) 页面包含以下字段:

**Routes Displayed** (显示的路由) — 选择可查看 **Configured Routes** (已配置路由)、**Best Routes** (最佳路由) 或 **All Routes** (所有路由)。

当选择了 **Configured Routes** (已配置的路由) 时, 会显示以下字段:

**IPv6 Prefix/Prefix Length** (IPv6 前缀/前缀长度) — 显示配置的路由的网络前缀和前缀长度。

**Next Hop IP** (下一跃距 IP) — 显示已配置路由的下一跃距 IPv6 地址。

**Next Hop Interface** (下一跃距接口) — 显示已配置路由的下一跃距接口。

**Preference** (优先级) — 显示已配置路由的路由优先级。

**Delete** (删除) — 单击此框和 **Refresh** (刷新) 按钮后, 将删除显示的路由。

当选择了 **Best Routes** (最佳路由) 或 **All Routes** (所有路由) 选项时, 会显示以下字段:

**Number of Routes** (路由数) — 显示最佳路由或所有路由的数量。

**IPv6 Prefix/Prefix Length** (IPv6 前缀/前缀长度) — 显示配置的路由的网络前缀和前缀长度。

**Protocol** (协议) — 显示配置的路由所使用的协议。

**Next Hop Interface** (下一跃距接口) — 显示已配置路由的下一跃距接口。

**Next Hop IP** (下一跃距 IP) — 显示配置的路由的下一跃距 IPv6 地址。

## 显示 IPv6 路由

打开 **Configured IPv6 Routes** (配置的 IPv6 路由) 页面。

从 **Routes Displayed** (显示的路由) 下拉式菜单中选择要查看的路由。

系统将显示选定的路由及其配置。

## 使用 CLI 命令显示 IPv6 路由

有关执行此功能的 CLI 命令的信息, 请参阅 «CLI 参考指南» 的以下章节:

- IPv6 路由命令

---

[返回目录页面](#)



[返回目录页面](#)

# 配置服务质量

**Dell™ PowerConnect™ 6200** 系列用户指南

- [服务质量概览](#)
- [配置差别服务](#)
- [服务级别](#)

本节将概述服务质量 (QoS) 和解释 Quality of Service (服务质量) 菜单页面 - Differentiated Services (差别服务) 和 Class of Service (服务级别) - 上可用的 QoS 功能。

---

## 服务质量概览

对一般的交换机而言，每个物理端口均由一个或多个用于在附加网络上传输信息包的队列组成。一个端口通常由多个队列组成，从而根据用户定义的标准优先处理某些信息包。当信息包在某个端口中排队等待传输时，其服务速率取决于队列的配置方式，也可能取决于端口中其它队列目前的通信量。如果需要延迟，则信息包停留在队列中直至调度程序授权队列进行传输。当队列已满时，信息包将无法在传输队列中停留，交换机将丢弃这些信息包。

QoS 是一种提供连续、可预测数据传输的方式，它通过区分有严格时限要求的信息包与更能容许延迟的信息包来完成数据传输。在具有 QoS 功能的网络中，有严格时限要求的信息包会被“特殊处理”。为此，网络中的所有元素都必须具有 QoS 功能。如果至少有一个节点不具有 QoS 功能，则网络路径中会出现缺陷，而整个信息包流的性能也会降低。

要显示 Quality of Service (服务质量) 菜单页面，请在树视图中单击 **Quality of Service** (服务质量)。在此菜单页面上，可以使用两种类型的 QoS 链接，分别为：

- [配置差别服务](#)
  - [服务级别](#)
- 

## 配置差别服务

### DiffServ 概览

QoS 功能包括差别服务 (DiffServ) 支持，这种支持可以根据定义的逐跳行为 (per-hop behavior) 将通信量分类为数据流及进行某些 QoS 处理。

标准的 IP 网络设计为提供“尽力而为”的数据传输服务。“尽力而为”服务是指网络会及时传输数据，但并不保证一定能实现。网络发生堵塞时，信息包可能延迟，不时发送或被丢弃。对于一般的互联网应用（如电子邮件和文件传输），服务质量的轻微下降是可以接受的且在大部分情况下不容易被觉察。相反，任何服务质量的下降都会对具有严格时限要求的应用（如语音或多媒体）产生意想不到的后果。

### 定义 DiffServ

要使用 QoS 的 DiffServ，则可通过 **Differentiated Services** (差别服务) 菜单页面访问的网页必须首先用于定义以下类别及其标准：

□□□ 类：创建类和定义类标准

□□□ 策略：创建策略、将类与策略关联及定义策略声明

□□□ 服务：将策略添加到入站接口

信息包根据定义的标准进行分类和处理。分类标准由类定义。处理策略属性定义。策略属性可以根据每类实例进行定义，而出现匹配时将应用这些属性。策略可以包含多个类。当策略处于活动状态时，将根据类所匹配的信息包采取相应措施。

信息包处理将从测试信息包的类匹配标准开始。策略适用于在该策略内有类匹配的信息包。

**Differentiated Services**（差别服务）菜单页面包含各个 Diffserv 配置和显示功能的链接。

要显示此页面，请在树视图中单击 **Quality of Service**（服务质量）® **Differentiated Services**（差别服务）。Differentiated Services（差别服务）菜单页面含有指向以下功能的链接：

- [Diffserv 配置](#)
- [类配置](#)
- [类标准](#)
- [策略配置](#)
- [策略类定义](#)
- [服务配置](#)
- [服务详细统计数据](#)

## Diffserv 配置

**Diffserv Configuration**（Diffserv 配置）页面用于显示“DiffServ 一般状态组”信息，该信息包括当前管理模式设置以及每个主 DiffServ 专用 MIB 表的当前行数 and 最大行数。

要显示此页面，请在树视图中单击 **Quality of Service**（服务质量）® **Differentiated Services**（差别服务）® **Diffserv Configuration**（Diffserv 配置）。

图 12-1. Diffserv 配置

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb path is: Quality of Service > Differentiated Services > Diffserv Configuration. The page title is "Diffserv Configuration". There are "Print" and "Refresh" buttons. The "Diffserv Admin Mode" is set to "Enable". Below this is a table of MIB Tables:

MIB Table	Current Size/Max Size
Class Table	0 / 32
Class Rule Table	0 / 192
Policy Table	2 / 64
Policy Instance Table	0 / 768
Policy Attributes Table	0 / 2304
Policy Attributes Table	1 / 632

At the bottom of the table area, there is an "Apply Changes" button.

**Diffserv Configuration**（Diffserv 配置）页面包含以下字段：

**Diffserv Admin Mode**（Diffserv 管理模式）— 打开和关闭管理模式。禁用此字段时，DiffServ 配置将保留且可以更改，但处于不活动状态。启用此字段时，Differentiated Services（差别服务）处于活动状态。

## MIB Table (MIB 表)

**Class Table** (类表) — 显示类表的当前行数和最大行数。

**Class Rule Table** (类规则表) — 显示类规则表的当前行数和最大行数。

**Policy Table** (策略表) — 显示策略表的当前行数和最大行数。

**Policy Instance Table** (策略实例表) — 显示策略实例表的当前行数和最大行数。

**Policy Attributes Table** (策略属性表) — 显示策略属性表的当前行数和最大行数。

**Service Table** (服务表) — 显示服务表的当前行数和最大行数。

## 更改 Diffserv 管理模式

□□□ 打开 **Diffserv Configuration** (Diffserv 配置) 页面。

□□□ 通过从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用) 来打开或关闭 **Diffserv Admin Mode** (Diffserv 管理模式)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将更改 Diffserv 管理模式并更新设备。

## 使用 CLI 命令显示 MIB 表

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

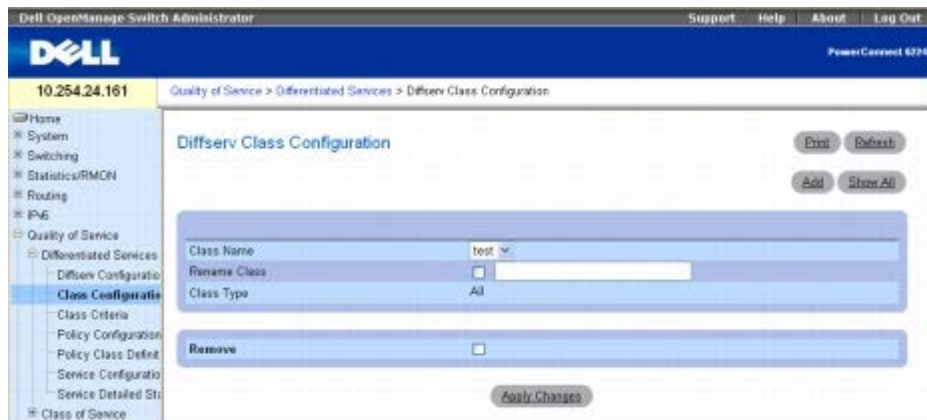
- QoS 命令

## 类配置

**Diffserv Class Configuration** (Diffserv 类配置) 页面用于添加新的 Diffserv 类名称，或者重命名或删除现有的类。

要显示此页面，请在树视图中单击 **Quality of Service** (服务质量) ® **Differentiated Services** (差别服务) ® **Class Configuration** (类配置)。

图 12-2. Diffserv 类配置



**Diffserv Class Configuration** (Diffserv 类配置) 页面包含以下字段：

**Class Name** (类名称) — 选择要重命名或删除的类名称。单击 **Add** (添加) 设置新的类名称。

**Rename Class** (重命名类) — 选中此复选框并输入新的类名称时即可重命名显示的类。

**Class Type** — **Class Type** **All**

(类类型) 列出所有类类型。硬件目前唯一支持的 (类类型) 值为 (所有)。

All (所有) — 所有为类定义的各种匹配标准都应满足信息包匹配。All (所有) 表示所有匹配标准的逻辑 AND (与)。

**Remove** (删除) — 选中此选项并单击 **Apply Changes** (应用更改) 时即可删除显示的类名称。

## 重命名类配置

- 打开 **Class Configuration** (类配置) 页面。
- 从 **Class Name** (类名称) 下拉式菜单中选择要更改的类名称。
- 单击 **Rename Class** (重命名类) 复选框并在旁边的字段中键入新的名称。
- 单击 **Apply Changes** (应用更改)。

系统将重命名类配置并更新设备。

## 添加 Diffserv 类配置

- 打开 **Class Configuration** (类配置) 页面。
- 单击 **Add** (添加)。

系统将显示 **Add Diffserv Class** (添加 Diffserv 类) 页面。

图 12-3. 添加 Diffserv 类



- 在 **Class Name** (类名称) 字段中键入新的名称。
- 单击 **Apply Changes** (应用更改)。

系统将添加 **Class Name** (类名称) 并更新设备。

## 删除类配置

- 打开 **Class Configuration** (类配置) 页面。
- 从 **Class Name** (类名称) 下拉式菜单中选择要删除的类名称。
- 选中 **Remove** (删除) 复选框。
- 单击 **Apply Changes** (应用更改)。

系统将删除相关的类配置并更新设备。

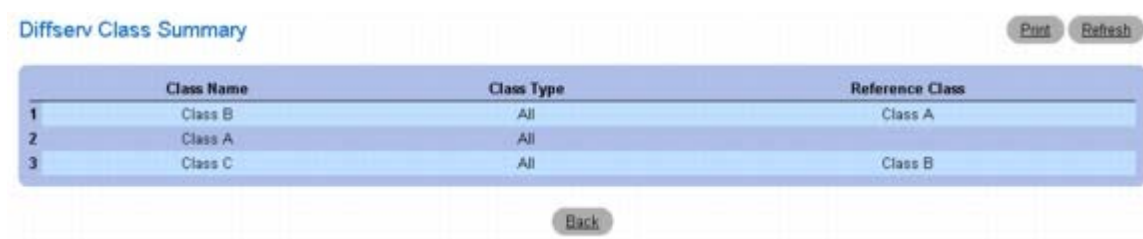
显示类配置

□□□ 打开 **Class Configuration**（类配置）页面。

□□□ 单击 **Show All**（全部显示）。

所有类配置均显示在 **Diffserv Class Summary**（Diffserv 类摘要）页面上。

图 12-4. Diffserv 类摘要



	Class Name	Class Type	Reference Class
1	Class B	All	Class A
2	Class A	All	Class A
3	Class C	All	Class B

## 使用 CLI 命令添加类配置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- QoS 命令

## 类标准

**Diffserv Class Criteria**（Diffserv 类标准）页面用于定义要与 DiffServ 类关联的标准。当收到信息包时，这些 DiffServ 类用于区分信息包的优先级。

要显示此页面，请在树视图中单击 **Quality of Service**（服务质量）® **Differentiated Services**（差别服务）® **Class Criteria**（类标准）。

图 12-5. Diffserv 类标准

**Diffserv Class Criteria** (**Diffserv** 类标准) 页面包含以下字段：

**Class Name** (类名称) — 选择要为其指定标准的类名称。

**Class Type** (类类型) — 显示类类型。唯一支持的可配置类类型为 **All** (所有)。

## 匹配属性

使用以下字段将信息包与类匹配。单击要用作类标准的各个字段的复选框，然后在相关字段中输入数据。一个类中可以有多于一个匹配标准。该逻辑在此标准中是布尔“逻辑与”。

**Source IP Address** (源 IP 地址) — 要求信息包源端口 IP 地址与此处所列的地址匹配。

**Subnet Mask** (子网掩码) — 源 IP 地址的子网掩码。选中 **Source IP Address** (源 IP 地址) 复选框时，此字段为必填项。

**Destination IP Address** (目的地 IP 地址) — 要求信息包目的地端口 IP 地址与此处所列的地址匹配。

**Subnet Mask** (子网掩码) — 目的地 IP 地址的子网掩码。选中 **Destination IP Address** (目的地 IP 地址) 复选框时，此字段为必填项。

**Source L4 Port** (源 L4 端口) — 要求信息包 TCP/UDP 源端口与此处所列的端口匹配。选择以下选项之一：

**Select From List** (从列表中选择) — 单击可选择要与信息包匹配的公认源端口的列表。

**Match to Port** (与端口匹配) — 单击可添加用户定义的要与信息包匹配的端口 ID。

**Destination L4 Port** (目的地 L4 端口) — 要求信息包 TCP/UDP 目的地端口与此处所列的端口匹配。选择以下选项之一：

**Select From List** (从列表中选择) — 选择要与信息包匹配的公认目的地端口的列表。



**Match to Port**（与端口匹配）— 单击可添加用户定义的要与信息包匹配的端口 ID。

**Protocol**（协议）— 要求信息包协议与此处所列的协议匹配。选择以下选项之一：

**Select from List**（从列表中选择）— 从协议下拉式列表中选择。

**Match to Protocol ID**（与协议 ID 匹配）— 输入要与信息包匹配的协议 ID。

**EtherType**（以太网类型）— 要求帧的以太网类型与此处所列的以太网类型匹配。选择以下选项之一：

**Select from List**（从列表中选择）— 从 Ethertypes（以太网类型）下拉式列表中选择。

**Match to Port**（与端口匹配）— 输入要与信息包匹配的以太网类型 ID。

**Class of Service (CoS)**（服务级别 [CoS]）— 要求传入信息包 CoS 与此处输入的 CoS 匹配。

**Source MAC Address**（源 MAC 地址）— 要求传入信息包源 MAC 地址与此处输入的地址匹配。

**Source MAC Mask**（源 MAC 掩码）— 指定源 MAC 地址的通配符掩码。通配符掩码将确定要使用的位以及要忽略的位。通配符掩码 255.255.255.255 表示所有位都不重要。通配符 0.0.0.0 表示所有位都重要。选中 **Source MAC Address**（源 MAC 地址）复选框时，此字段为必填项。

**Destination MAC Address**（目的地 MAC 地址）— 要求传入信息包目的地 MAC 地址与此处输入的地址匹配。

**Destination MAC Mask**（目的地 MAC 掩码）— 指定目的地 MAC 地址的通配符掩码。通配符掩码将确定要使用的位以及要忽略的位。通配符掩码 255.255.255.255 表示所有位都不重要。通配符 0.0.0.0 表示所有位都重要。选中 **Destination MAC Address**（目的地 MAC 地址）复选框时，此字段为必填项。

**VLAN ID** — 要求传入信息包 VLAN ID 与此处输入的 VLAN ID 匹配。

**Secondary VLAN ID**（次 VLAN ID）— 要求传入信息包次 VLAN ID 与此处输入的 VLAN ID 匹配。

**Reference Class**（引用类）— 选择要开始引用标准的类。选中 **Add Diffserv Class**（添加 Diffserv 类）复选框，然后从相应的下拉式菜单中选择以前配置的 Diffserv 类：

## Service Type Criteria（服务类型标准）

单击可选择以下三个要用于匹配信息包与类标准的匹配字段之一：

**IP DSCP** — 选择此字段时会将信息包的 DSCP 与类标准匹配。从下拉式菜单中选择 DSCP 类型或输入要匹配的 DSCP 值。

**IP Precedence**（IP 优先级）— 选择此字段并输入值时会将信息包的 IP 优先级值与类标准的值匹配。

**IP TOS Bits**（IP TOS 位）— 选择此字段并输入值时会将 IP 标头中信息包的服务类型位与类标准的位匹配。

**Match Every**（全部匹配）— 选中 **Match Every**（全部匹配）复选框时要求信息包与每个标准匹配。

## 定义类标准

打开 **Diffserv Class Criteria**（Diffserv 类标准）页面。

从下拉式菜单中选择要为其输入匹配属性的 **Class Name**（类名称）。

选择要为此类匹配的属性并指定属性标准。

单击 **Apply Changes**（应用更改）。

系统会将标准添加到此类并更新设备。

## 使用 CLI 命令配置类标准

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：



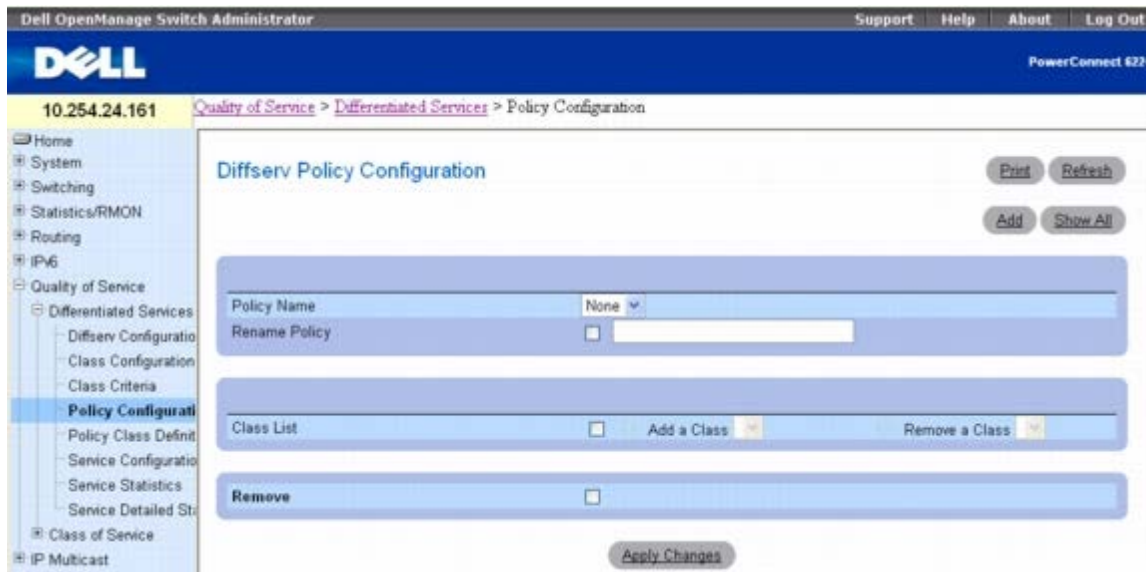
- QoS 命令

## 策略配置

**Diffserv Policy Configuration (Diffserv 策略配置)** 页面用于将类集合与一个或多个策略声明关联。

要显示此页面，请在树视图中单击 **Quality of Service (服务质量) @ Differentiated Services (差别服务) @ Policy Configuration (策略配置)**。

图 12-6. Diffserv 策略配置



**Diffserv Policy Configuration (Diffserv 策略配置)** 页面包含以下字段：

**Policy Name (策略名称)** — 选择要与类关联的策略名称。

**Rename Policy (重命名策略)** — 选择此复选框，输入新的名称并单击 **Apply Changes (应用更改)** 时即可重命名策略。

**Class List (类列表)** — 为策略配置类关联。

**Add a Class (添加类)** — 将从下拉式菜单中所选类与策略关联。

**Remove a Class (删除类)** — 将所选类从策略中删除。

**Remove (删除)** — 将所选策略名称从设备中删除。

## 将类与策略关联或者删除关联

□□□ 打开 **Diffserv Policy Configuration (Diffserv 策略配置)** 页面。

□□□ 选择要与类关联的 **Policy Name (策略名称)**。

□□□ 在 **Class List (类列表)** 字段中，选择该复选框，然后单击 **Add a Class (添加类)** 或 **Remove a Class (删除类)** 单选按钮，然后从相关的下拉式菜单中选择 **class (类)**。

使用 **Add a Class (添加类)** 可以将类与该策略相关联。使用 **Remove a Class (删除类)** 可以将类从该策略中删除。

□□□ 从相关的下拉式菜单中选择会受影响的类。

□□□ 单击 **Apply Changes (应用更改)**。

系统将保存修改的策略并更新设备。

## 重命名策略

□□□ 打开 **Diffserv Policy Configuration** (**Diffserv** 策略配置) 页面。

□□□ 选择要重命名的 **Policy Name** (策略名称)。

□□□ 选中 **Rename Policy** (重命名策略) 复选框并在旁边的字段中输入新的名称，即可重命名策略。

系统将保存修改的策略名称并更新设备。

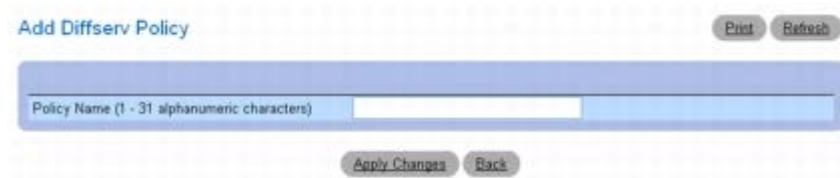
## 添加新的策略名称

□□□ 打开 **Diffserv Policy Configuration** (**Diffserv** 策略配置) 页面。

□□□ 单击 **Add** (添加)。

系统将显示 **Add Diffserv Policy** (添加 **Diffserv** 策略) 页面。

图 12-7. 添加 **Diffserv** 策略



□□□ 输入新的 **Policy Name** (策略名称)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存新的策略并更新设备。

## 显示策略摘要

□□□ 打开 **Policy Configuration** (策略配置) 页面。

□□□ 单击 **Show All** (全部显示)。

**Diffserv Policy Summary** (**Diffserv** 策略摘要) 页面将显示所有策略名称、策略类型和成员类。

图 12-8. **Diffserv** 策略摘要



	Policy Name	Member Classes
1	Policy1	
2	Policy2	

## 删除策略配置

□□□ 打开 **Diffserv Policy Configuration** (Diffserv 策略配置) 页面。

□□□ 从 **Policy Name** (策略名称) 下拉式菜单中选择要删除的策略名称。

□□□ 选中 **Remove** (删除) 复选框。

□□□ 单击 **Apply Changes** (应用更改)。

系统将删除相关的策略配置并更新设备。

## 使用 CLI 命令定义策略配置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

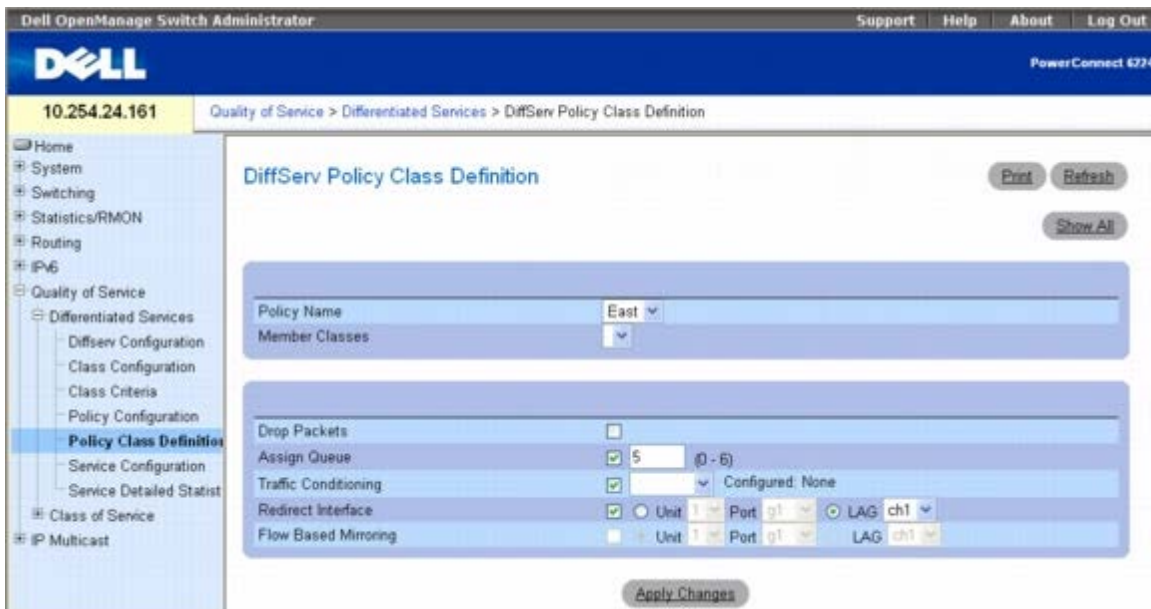
- QoS 命令

## 策略类定义

**Diffserv Policy Class Definition** (Diffserv 策略类定义) 页面用于将类与策略关联及定义此策略类实例的属性。

要显示此页面，请在树视图中单击 **Quality of Service** (服务质量) ® **Differentiated Services** (差别服务) ® **Policy Class Definition** (策略类定义)。

图 12-9. Diffserv 策略类定义



**Diffserv Policy Class Definition** (Diffserv 策略类定义) 页面包含以下字段：

**Policy Name** (策略名称) — 从下拉式菜单中选择要与成员类关联的策略。

**Member Classes** (成员类) — 从下拉式菜单中选择要与此策略名称关联的成员类。

**Drop Packets** (丢弃信息包) — 选择此字段以丢弃此策略类的信息包。

**Assign Queue** (分配队列) — 将此策略的信息包分配给队列。有效范围是 0 至 6。

**Traffic Conditioning** (通信调节) — 选中此字段并从下拉式菜单中选择条件时会对某类通信进行调节。此字段会影响与此策略类匹配的通信的处理方式。从 **None** (无)、**Marking** (标记) 和 **Policing** (管制) 中选择。选择 **Marking** (标记) 或 **Policing** (管制) 时，屏幕会发生变化并显示相关字段。

- **None**（无）：指定在处理信息包时不进行任何通信调节。这是默认设置。
- **Marking**（标记）：允许标记信息包中的以下字段之一：IP DSCP、IP Precedence（IP 优先级）或 Class of Service（服务级别）。有关选择 **Marking**（标记）时所显示字段的信息，请参阅[信息包标记通信条件](#)。
- **Policing**（管制）：允许您配置管制的执行方式及配置被视为符合性和非符合性信息包的执行情况。有关选择 **Policing**（管制）时所显示字段的详细信息，请参阅[管制通信条件](#)。

**Redirect Interface**（重定向接口）— 显示 Redirect Interface（重定向接口）是否应用于此策略类，并指定使用的接口或 LAG。

**Flow Based Mirroring**（基于流的镜像）— 显示 Flow Based Mirroring（基于流的镜像）是否应用于此策略类，并指定使用的接口或 LAG。

## 定义策略类实例

□□□ 打开 **Diffserv Policy Class Definition**（Diffserv 策略类定义）页面。

□□□ 选择要关联的策略和成员类。

□□□ 使用页面上其余字段指定要应用于此策略类实例的属性。

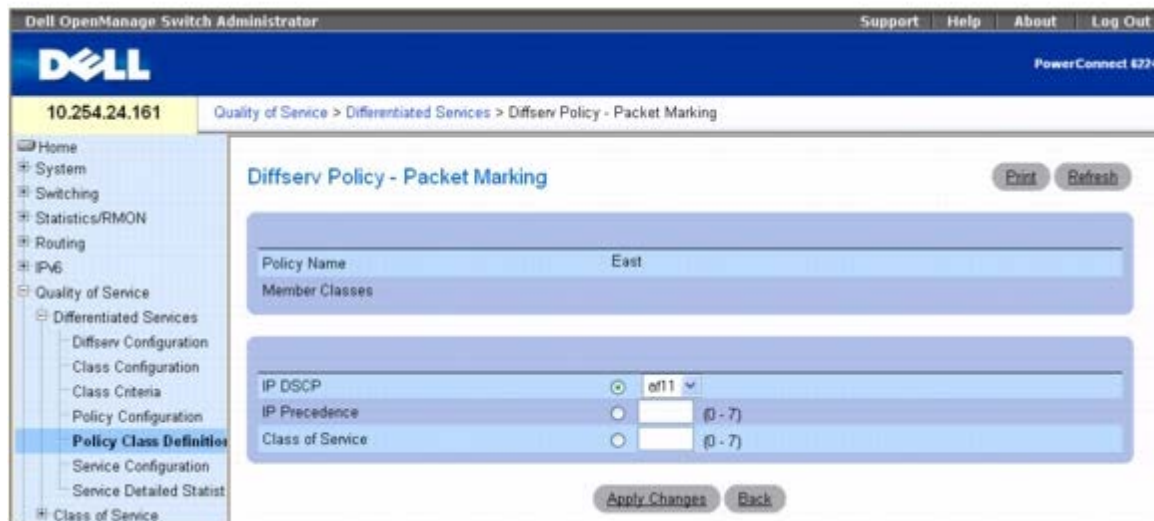
□□□ 单击 **Apply Changes**（应用更改）。

系统将定义策略类并更新设备。

## 信息包标记通信条件

如果将 **Marking**（标记）选择为 **Traffic Condition**（通信条件），则将显示以下 Packet Marking（信息包标记）页面。

图 12-10. 策略类定义 - 信息包标记



**Diffserv Policy - Packet Marking**（Diffserv 策略 - 信息包标记）页面包含以下字段：

**Policy Name**（策略名称）— 显示与成员类关联的策略。

**Member Classes**（成员类）— 显示与此策略名称关联的成员类。

您可以选择标记信息包中的以下字段之一：

**IP DSCP** — 选择要标记的 IP DSCP。从下拉式菜单中选择或直接在 User Value（用户值）字段中输入。

**IP Precedence**（IP 优先级）— 选择要标记的指定 IP Precedence（IP 优先级）队列号。

**Class of Service**（服务级别）— 选择要标记的指定 Class of Service（服务级别）队列号。

## 为策略类实例配置信息包标记

□□□ 从 **Diffserv Policy Class Definition**（Diffserv 策略类定义）页面的 **Traffic Conditioning**（通信调节）下拉式菜单中选择 **Marking**（标记）。

系统将显示 **Packet Marking**（信息包标记）页面，如图 12-10 所示。

□□□ 选择要为该策略类标记的 IP DSCP、IP Precedence（IP 优先级）或 Class of Service（服务级别）。

□□□ 选择或输入此字段的值。

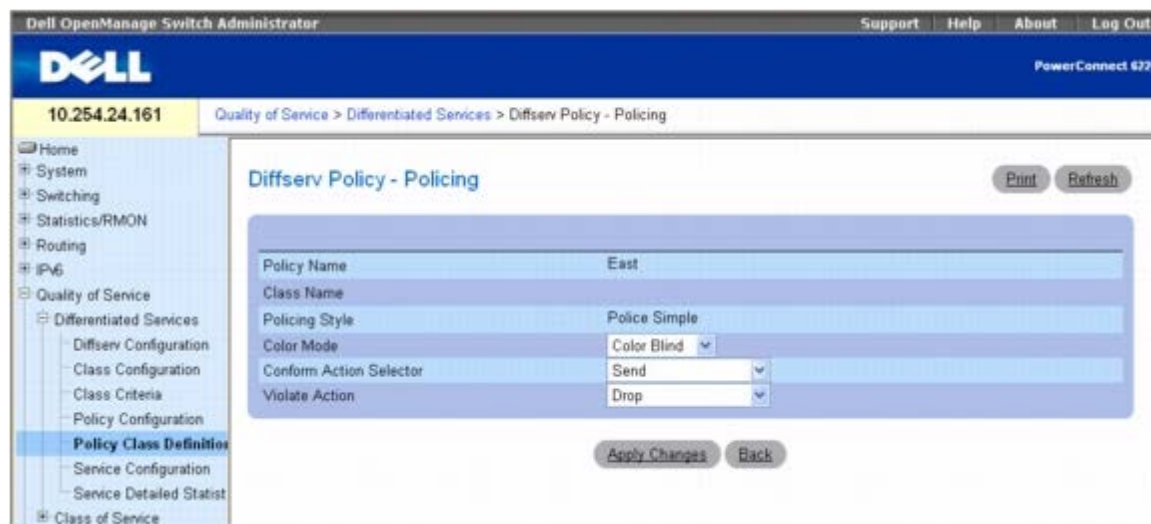
□□□ 单击 **Apply Changes**（应用更改）。

系统将定义策略类并更新设备。

## 管制通信条件

如果将 **Policing**（管制）选择为 **Traffic Condition**（通信条件），则将显示以下 **Diffserv Policy - Policing**（Diffserv 策略 - 管制）页面。

图 12-11. 策略类定义 - 管制



**Diffserv Policy - Policing**（Diffserv 策略 - 管制）页面包含以下字段：

**Policy Name**（策略名称）— 显示要为其配置管制的策略。

**Class Name**（类名称）— 显示与此策略名称关联的成员类。

**Policing Style**（管制样式）— 选择所使用的管制样式。

**Color Mode**（颜色模式）— 选择所使用的颜色管制类型。从下拉式菜单中选择 **Color Blind**（不识色）或 **Color Aware**（识色）。

**Conform Action Selector**（符合动作选择器）— 选择被视为符合性（小于管制速率）的信息包的执行情况。其选项包括 **Send**（发送）、**Drop**（丢弃）、**Mark CoS**（标记 CoS）、**Mark IP DSCP**（标记 IP DSCP）和 **Mark IP Precedence**（标记 IP 优先级）。

**Violate Action**（违反动作）— 选择被视为非符合性（大于管制速率）的信息包的执行情况。其选项包括 **Send**（发送）、**Drop**（丢弃）、**Mark CoS**（标记 CoS）、**Mark IP DSCP**（标记 IP DSCP）和 **Mark IP Precedence**（标记 IP 优先级）。

## 为策略类实例配置管制

□□□ 从 **Diffserv Policy Class Definition** (Diffserv 策略类定义) 页面的 **Traffic Conditioning** (通信调节) 下拉式菜单中选择 **Policing** (管制)。

系统将显示 **Diffserv Policy - Policing** (Diffserv 策略 - 管制) 页面，如[图 12-11](#) 所示。

□□□ 检查并选择一个或多个要用于此策略类的管制标准。

□□□ 选择或输入各个所选字段的值。

□□□ 单击 **Apply Changes** (应用更改)。

系统将显示如下 **Policy Rate Configuration** (策略速率配置) 页面。

图 12-12. 策略速率配置

Policy Name	East
Class Name	test
Color Mode	Color Blind
Committed Rate (Kbps)	(1 to 4294967295) Kbps
Committed Burst Size (KB)	(1 to 128) KBytes
Conform Action	Send
Violate Action	Drop

□□□ 为 Committed Rate (允许的速率) 和/或 Committed Burst Size (允许的正常突发大小) 输入所需的标准值。

□□□ 单击 **Apply Changes** (应用更改)。

系统会将管制配置为指定的策略类实例并更新设备。

## 使用 CLI 命令定义策略类

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- QoS 命令

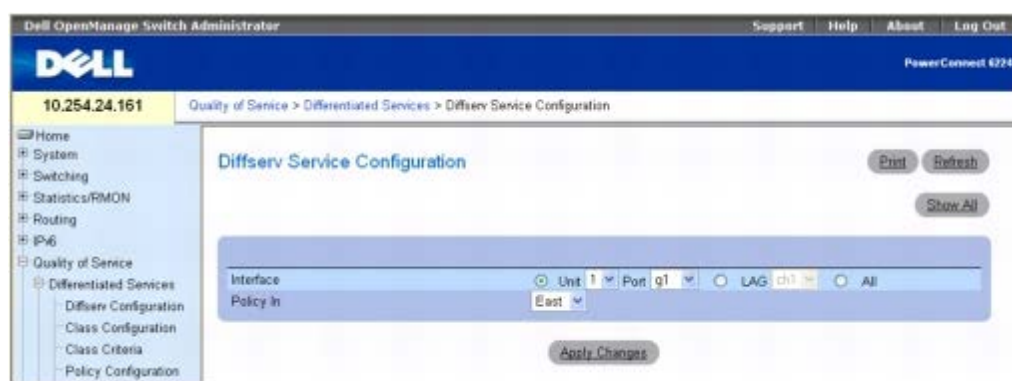
## 服务配置

**Diffserv Service Configuration** (Diffserv 服务配置) 页面用于激活端口上的策略。

要显示此页面，请在树视图中单击 **Quality of Service** (服务质量) ® **Differentiated Services** (差别服务) ® **Service Configuration** (服务配置)。

图 12-13. Diffserv 服务配置





**Diffserv Service Configuration (Diffserv 服务配置)** 页面包含以下字段：

**Interface (接口)** — 从下拉式菜单中选择会受影响的接口 (Unit/Port [单元/端口]、LAG 或 All [所有])。

**Policy In (关联策略)** — 从下拉式菜单中选择要与端口关联的策略。

## 激活端口上的策略

□□□ 打开 **Diffserv Service Configuration (Diffserv 服务配置)** 页面。

□□□ 请从下拉式菜单中选择接口。

□□□ 请从下拉式菜单中选择策略。

□□□ 单击 **Apply Changes (应用更改)**。

系统将激活接口上的策略并更新设备。

## 显示 Diffserv 服务摘要

□□□ 打开 **Diffserv Service Configuration (Diffserv 服务配置)** 页面。

□□□ 单击 **Show All (全部显示)**。

系统将显示 Diffserv Service Summary (Diffserv 服务摘要) 页面。

图 12-14. Diffserv 服务摘要

Interface	Direction	Operation Status	Policy Name
1/g1	In	Down	East

## 使用 CLI 命令将策略分配至端口

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- QoS 命令



## 服务详细统计数据

**Diffserv Service Detailed Statistics** (**Diffserv** 服务详细统计数据) 页面用于显示某个端口和类的信息包详细信息。

要显示此页面，请在树视图中单击 **Quality of Service** (服务质量) ® **Differentiated Services** (差别服务) ® **Service Detailed Statistics** (服务详细统计数据)。

图 12-15. Diffserv 服务详细统计数据



**Diffserv Service Detailed Statistics** (**Diffserv** 服务详细统计数据) 页面包含以下字段：

**Counter Mode Selector** (计数器模式选择器) — 要显示的统计数据的类型。Packets (信息包) 是唯一可用的类型。

**Interface** (接口) — 选择要为其显示服务统计数据的信息包的 Unit (单元) 和 Port (端口) 或者 LAG。

**Direction** (方向) — 选择要为其显示服务统计数据的信息包的方向。

**Policy Name** (策略名称) — 显示与所选接口关联的策略。

**Operational Status** (操作状态) — 显示此端口上的策略是否处于活动状态。

**Member Classes** (成员类) — 选择要显示八位位组统计数据的成员类。

**Offered Packets** (提供的信息包) — 显示匹配策略的信息包数。

**Discarded Packets** (丢弃的信息包) — 显示被策略丢弃的信息包数。

## 显示服务统计数据

□□□ 打开 **Diffserv Service Detailed Statistics** (**Diffserv** 服务详细统计数据) 页面。

□□□ 根据需要填写各字段。

系统会显示指定接口、方向和类的信息包统计数据。

## 使用 CLI 命令配置服务统计数据

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- QoS 命令

## 服务级别

借助服务级别 (CoS) 队列功能，可以直接配置交换机排队功能的某些方面。当不需要差别服务的复杂度时，服务级别便能为不同类型的网络通信提供所需的 QoS 保障。信息包到达接口的优先级可用于通过映射表将信息包导入相应的出站 CoS 队列。用户可以在队列（或端口）级上配置影响队列映射的 CoS 队列特性，如最小保证带宽、传输速率整理等。

每个端口支持七个队列。尽管硬件支持八个队列，但始终要保留一个队列供堆栈系统内部使用。

要显示此页面，请在树视图中单击 **Quality of Service**（服务质量）® **Class of Service**（服务级别）。**Class of Service**（服务级别）菜单页面包含以下功能的链接：

- [映射表配置](#)
- [接口配置](#)
- [接口队列配置](#)

## 映射表配置

交换机上的每个端口都可以配置为信任信息包字段之一（802.1p、IP Precedence [IP 优先级] 或 IP DSCP），或不信任任何信息包的优先级指定（不信任模式）。如果将端口设置为信任模式，则端口将使用适合于所使用信任字段的映射表。此映射表表示到信息包的 CoS 队列应在相应的出口端口上转发。当然，映射表中必须有用于各种用途的信任字段，如果不是这样的话，则必须进行默认操作。这些操作包括，根据由当前 802.1p 映射表映射至通信级别的现有端口默认优先级，将信息包作为一个整体指引到为入口端口配置的特定 CoS 级别。

另外，如果将端口配置为不信任，则端口将不信任所有传入信息包优先级指定，而是使用端口默认优先级值。所有到达不信任端口入口的信息包都会根据配置的入口端口默认优先级，被指引到相应出口端口上的特定 CoS 队列。此过程也用于无法实现信任端口映射的情况，例如当非 IP 信息包到达配置为信任 IP DSCP 值的端口时。

**Mapping Table Configuration**（映射表配置）页面用于定义将服务级别分配至信息包的方式。

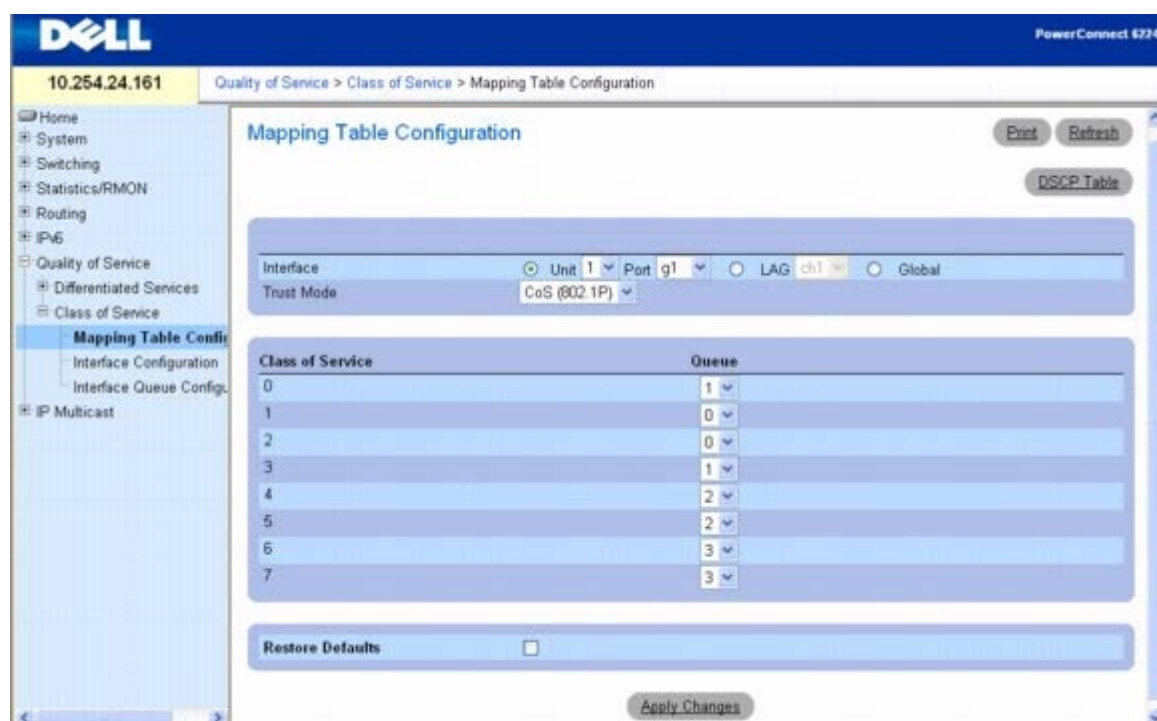
要显示此页面，请在树视图中单击 **Quality of Service**（服务质量）® **Class of Service**（服务级别）® **Mapping Table Configuration**（映射表配置）。

**Mapping Table Configuration**（映射表配置）页面上所选的 Trust Mode（信任模式）会影响显示页面及从页面访问字段的方式。此处有三种信任模式可供使用：

- Untrusted (None)（不信任 [无]）
- CoS(802.1P)
- IP DSCP

CoS(802.1P) 为默认模式，因此当从 **Class of Service**（服务级别）菜单页面中选择 **802Mapping Table Configuration**（映射表配置）时显示的就是此页面。

图 12-16. 映射表配置 — CoS (802.1P)



## CoS (802.1P) 信任模式

**CoS (802.1P) Mapping Table Configuration** (映射表配置) 页面包含以下字段：

**Interface** (接口) — 选择要应用服务级别配置的接口。选择一个单元和端口或 LAG，或者选择 **Global** (全局) 以便将配置类应用于所有接口。

**Trust Mode** (信任模式) — 选择要应用的信任模式。**CoS (802.1P)** 为默认设置。

**Class of Service** (服务级别) — 在单独的行中列出每个服务级别，因此可以将单个队列分配给每个服务级别。

**Queue** (队列) — 从下拉式菜单中选择各个 **Class of Service** (服务级别) 的队列。最初显示的是默认队列。

**Restore Defaults** (恢复默认设置) — 选中此字段并单击 **Apply Changes** (应用更改) 时即可恢复默认队列值。

## 配置 CoS (802.1P) 信任模式

□□□ 打开 **Mapping Table Configuration** (映射表配置) 页面。

□□□ 选择会受影响的单元和端口或 LAG，或者选择 **Global** (全局) 以便将设置应用于所有接口。

□□□ 选择一个 **Trust Mode** (信任模式)。

□□□ 选择与各个 **Class of Service** (服务级别) 关联的 **Queue** (队列)。

□□□ 单击 **Apply Changes** (应用更改)。

系统会将所作的更改应用于所选的接口并更新设备。

## 恢复队列默认设置

□□□ 打开 **Mapping Table Configuration** (映射表配置) 页面。

□□□ 单击 **Restore Defaults** (恢复默认设置) 复选框。

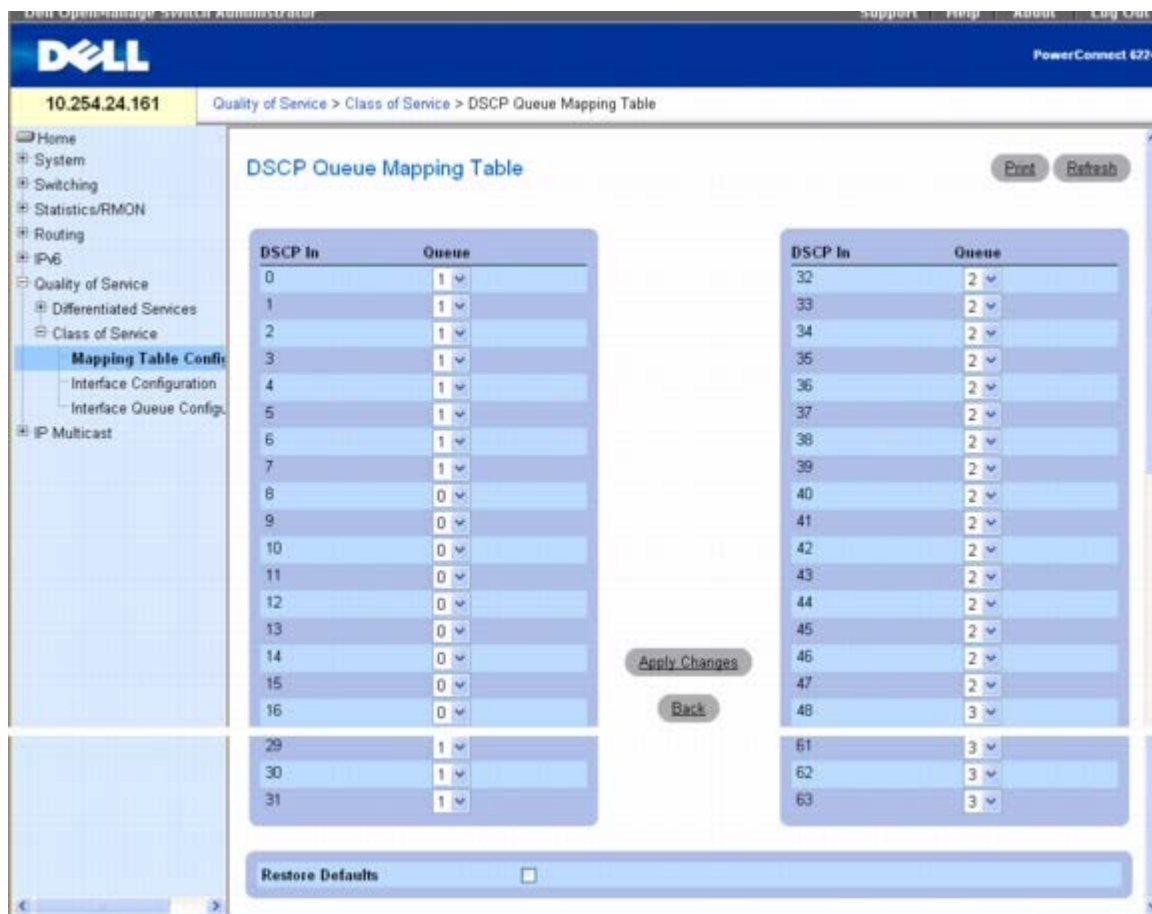
□□□ 单击 **Apply Changes** (应用更改)。

队列将返回其各个服务级别的默认设置，设备也将更新。

## 配置 IP DSCP 表

要访问 **DSCP Queue Mapping Table** (DSCP 队列映射表)，请在树视图中单击 **Quality of Service** (服务质量) ® **Class of Service** (服务级别) ® **Mapping Table Configuration** (映射表配置)，然后单击 **DSCP Table** (DSCP 表) 链接。

图 12-17. DSCP 队列映射表



**DSCP Queue Mapping Table** (DSCP 队列映射表) 页面包含以下字段：

**DSCP In** — 检查并选择为标准，然后输入要在信息包中使用的 DiffServ Code Point (DiffServ 代码点)。此字段用于确定要将信息包发送到哪个队列。

**Queue ID** (队列 ID) — 选择要接收信息包的队列。

## 恢复队列默认设置

□□□ 打开 **DSCP Queue Mapping Table** (DSCP 队列映射表) 页面。

□□□ 单击 **Restore Defaults** (恢复默认设置) 复选框。

□□□ 单击 **Apply Changes** (应用更改)。

队列值将返回其默认设置，设备也将更新。

## 使用 CLI 命令映射表配置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

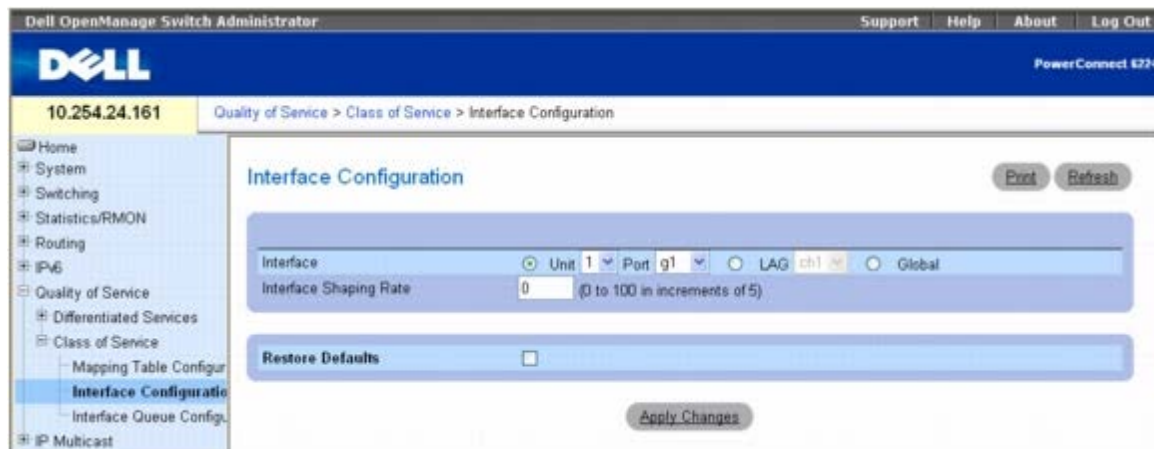
- QoS 命令

## 接口配置

**Interface Configuration**（接口配置）页面用于单独指定 CoS 配置的端口并将接口整理速率应用于所选的端口。

要显示 **Interface Configuration**（接口配置）页面，请在树视图中单击 **Quality of Service**（服务质量）⑥ **Class of Service**（服务级别）⑦ **Interface Configuration**（接口配置）。

图 12-18. 接口配置



**Interface Configuration**（接口配置）页面包含以下字段：

**Interface**（接口）— 选择受 **Interface Shaping Rate**（接口整理速率）影响的接口。

**Interface Shaping Rate**（接口整理速率）— 设置可为端口保留的通信量上限。指定的值代表最大协商带宽的百分比。有效值为 0 至 100，以 5 为增量。

**Restore Defaults**（恢复默认设置）— 选中此字段时即可将默认接口整理速率恢复为所选的接口。

## 定义接口配置

□□□ 打开 **Interface Configuration**（接口配置）页面。

□□□ 选择会受影响的单元和端口或 LAG，或者选择 **Global**（全局）以便将设置应用于所有接口。

□□□ 输入要应用于这些端口的 **Interface Shaping Rate**（接口整理速率）。

□□□ 单击 **Apply Changes**（应用更改）。

系统会将新的 **Interface Shaping Rate**（接口整理速率）应用于所选的接口并更新设备。

## 恢复默认整理速率

□□□ 打开 **Interface Configuration**（接口配置）页面。



单击 **Restore Defaults**（恢复默认设置）复选框。

单击 **Apply Changes**（应用更改）。

系统会将所有端口都恢复为默认整理速率并更新设备。

## 使用 CLI 命令定义接口配置

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- QoS 命令

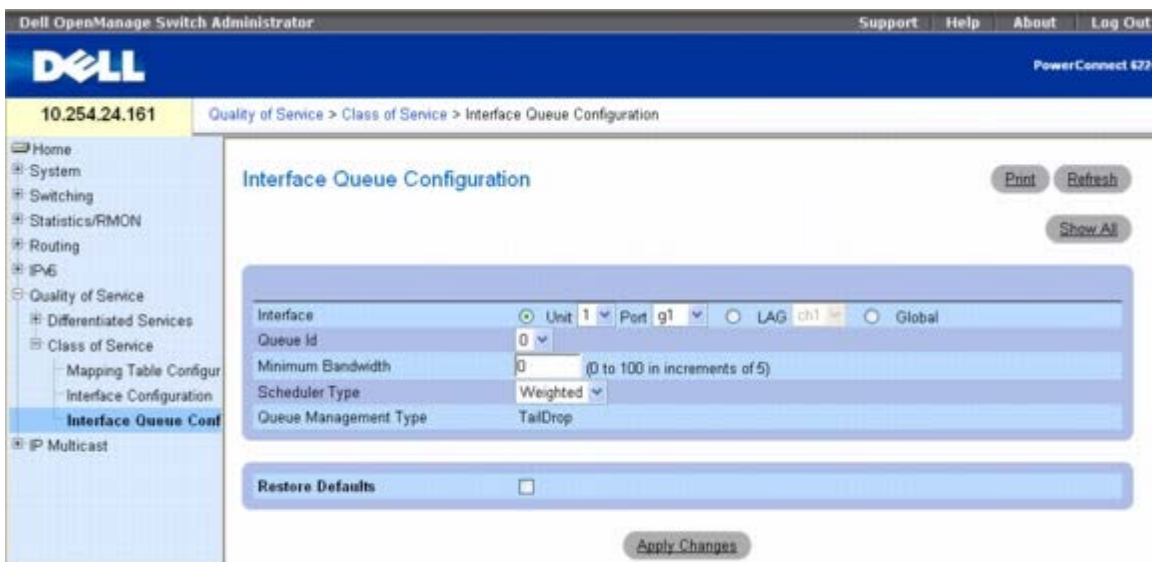
## 接口队列配置

**Interface Queue Configuration**（接口队列配置）页面用于通过配置交换机外出队列来定义特定队列所发生的情况。用户可以配置参数，从而控制队列所使用的带宽量、网络发生堵塞时的队列长度以及端口中所有队列集合的信息包传输计划。每个端口都有自己的 CoS 队列相关配置。

您可以通过对 CoS 队列参数进行全局配置或每个端口配置来简化配置过程。全局配置更改会自动应用于系统中的所有端口。

要显示 **Interface Queue Configuration**（接口队列配置）页面，请在树视图中单击 **Quality of Service**（服务质量）® **Class of Service**（服务级别）® **Interface Queue Configuration**（接口队列配置）。

图 12-19. 接口队列配置



**Interface Queue Configuration**（接口队列配置）页面包含以下字段：

**Interface**（接口）— 指定正在配置的 **Interface**（接口）（Unit/Port [单元/端口]、LAG 或 Global [全局]）。

**Queue ID**（队列 ID）— 从下拉式菜单中选择要配置的队列。

**Minimum Bandwidth**（最小带宽）— 选择端口最大协商带宽的的百分比。指定百分比为 0 至 100，以 5 为增量。

**Scheduler Type**（调度程序类型）— 从下拉式菜单中选择队列处理类型。选项包括 **Weighted**（加权）和 **Strict**（严格）。如果是基于每个队列进行定义，则用户可以为不同类型的通信创建所需的服务特性。

**Weighted**（加权）— 加权轮流会将加权与各个队列关联。这是默认设置。

**Strict**（严格）— 严格优先级服务，即队列中最高优先级的通信首先处理。

**Queue Management Type**（队列管理类型）— 显示用于所有信息包的信息包类型管理，即 Taildrop（尾部丢弃）。队列中的所有信息包在网络发生堵塞之前都是安全的。此时，系统将丢弃任何已排队的附加信息包。

## 配置接口队列

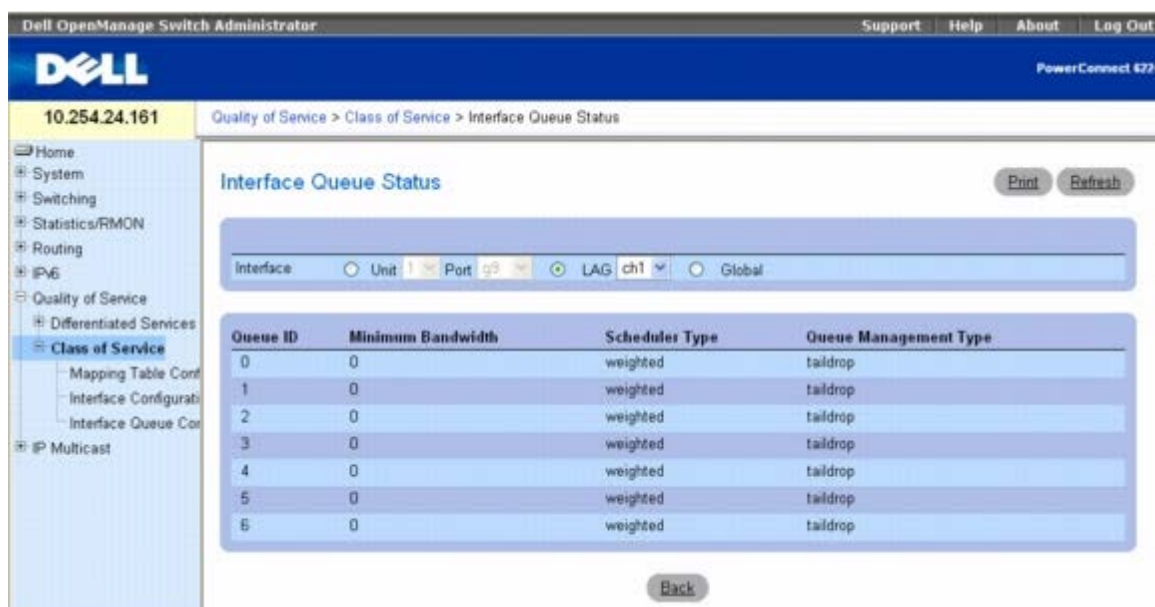
- 打开 **Interface Queue Configuration**（接口队列配置）页面。
- 从 **Interface Unit**（接口单元）和 **Port**（端口）下拉式菜单中选择会受影响的端口。
- 使用其余字段配置此端口的队列及其设置。
- 单击 **Apply Changes**（应用更改）。

系统将配置队列并更新设备。

## 显示接口队列设置

- 打开 **Interface Queue Configuration**（接口队列配置）页面。
  - 单击 **Show All**（全部显示）。
- 系统将显示 **Interface Queue Status**（接口队列状态）页面。
- 选择 **Unit/Port**（单元/端口）、**LAG** 或 **Global**（全局）。

图 12-20. 接口队列状态



## 使用 CLI 命令配置接口队列

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- QoS 命令

[返回目录页面](#)



[返回目录页面](#)

# 配置 IP 多点传送

Dell™ PowerConnect™ 6200 系列用户指南

- [DVMRP](#)
- [IGMP](#)
- [多点传送](#)
- [PIM-DM](#)
- [PIM-SM](#)

多点传送协议用于将多点传送信息包从一个源发送到多个接收器。它们有助于改善带宽利用，减少主机和路由器处理，因而非常适于视频/音频会议、白板工具、证券发行报价机等应用。

多点传送应用程序发送一份信息包并为其寻址到一组要接收它的接收器（多点传送组地址），而不是寻址到一个接收器（单点传送地址）。多点传送依靠网络将信息包仅转发到需要接收它们的网络和主机。

能够/启用多点传送的路由器会根据多点传送路由信息库 (MRIB) 转发多点传送信息包。路由器上运行的多点传送协议在构建多点传送分发树期间，将在 MRIB 中创建这些路由。不同的 IP 多点传送路由协议使用不同的技术来构造这些多点传送分发树。

如果多点传送通信要流经一部分不支持多点传送的网络（没有多点传送功能的路由器），则多点传送信息包会被压缩到 IP 数据包中，作为单点传送信息包发送。当通道远程端的多点传送路由器接收到信息包时，该路由器会剥除 IP 压缩，将信息包作为 IP 多点传送信息包转发。这个在 IP 中压缩多点传送信息包的过程称为通道机制。

要显示 **IP Multicast (IP 多点传送)** 菜单页面，请在树视图中单击 **IP Multicast (IP 多点传送)**。**IP Multicast (IP 多点传送)** 菜单页面包含指向以下过程的链接：

- [DVMRP](#)
- [IGMP](#)
- [多点传送](#)
- [PIM-DM](#)
- [PIM-SM](#)

---

## DVMRP

DVMRP 与所有启用 DVMRP 的路由器交换信息查询包，同时建立双向邻居关系并创建邻居列表。它还交换报告信息包并创建单点传送拓扑表，用该表构建多点传送路径选择表。而后，该表将用于路由由多点传送信息包。由于每个 DVMRP 路由器都使用相同的单点传送路由协议，因此就避免了路由循环。

**DVMRP** 菜单页面包含一些网页的链接，这些网页可用于定义和显示 DVMRP 参数和数据。要显示此页面，请在树视图中单击 **IP Multicast (IP 多点传送) @ DVMRP**。

在此菜单页面中可以访问以下网页：

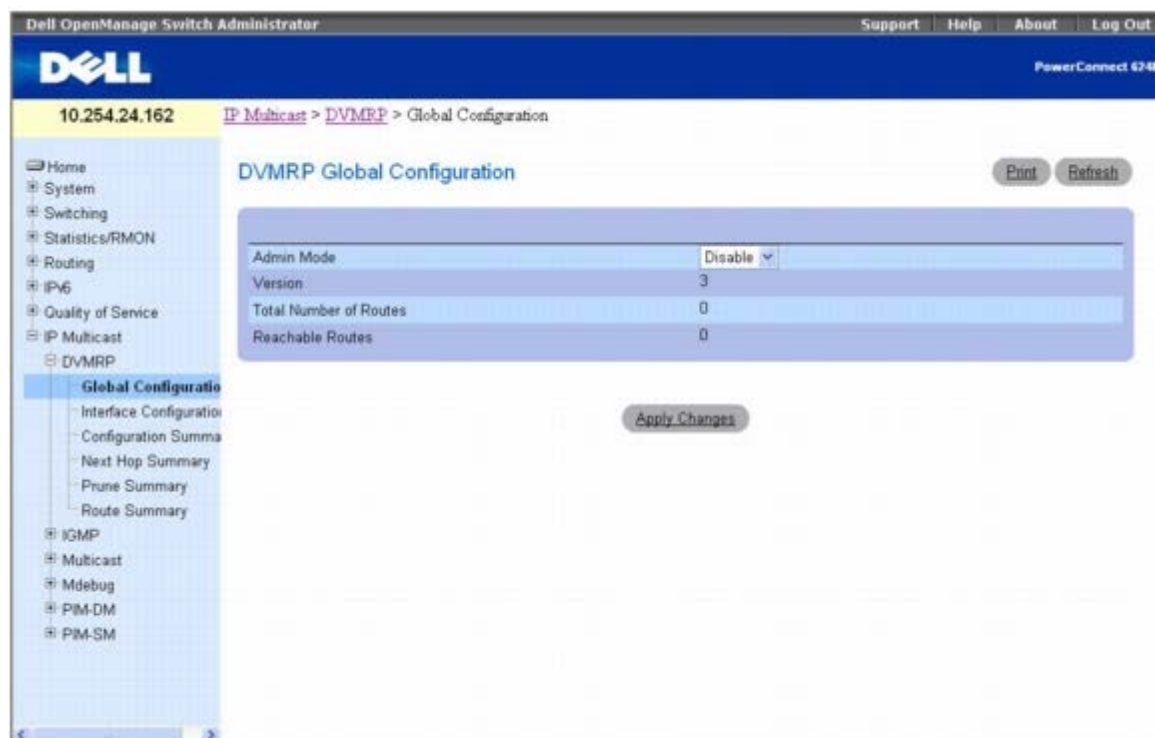
- [DVMRP 全局配置](#)
- [DVMRP 接口配置](#)
- [DVMRP 配置摘要](#)
- [下一跃距摘要](#)
- [删减摘要](#)
- [路由摘要](#)

## DVMRP 全局配置

**DVMRP Global Configuration** (DVMRP 全局配置) 页面用于配置全局 DVMRP 设置。

要显示此页面,请在树视图中单击 **IP Multicast** (IP 多点传送) ® **DVMRP** ® **Global Configuration** (全局配置)。

图 13-1. DVMRP 全局配置



**DVMRP Global Configuration** (DVMRP 全局配置) 页面包含以下字段:

**Admin Mode** (管理模式) — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用)。这样可将 DVMRP 的管理状态设置为活动或非活动。默认值为 **Disable** (禁用)。

**Version** (版本) — DVMRP 版本字符串的当前值。

**Total Number of Routes** (路由总数) — DVMRP 路径选择表中的路由数。

**Reachable Routes** (可到达路由) — DVMRP 路径选择表中跃点非无限的路由数。

### 设置 DVMRP 管理模式

□□□ 打开 **DVMRP Global Configuration** (DVMRP 全局配置) 页面。

□□□ 将 **Admin Mode** (管理模式) 设置为 **Enable** (启用) 或 **Disable** (禁用), 以打开或关闭 DVMRP。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存 DVMRP 配置并更新设备。

### 使用 CLI 命令配置 DVMRP

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

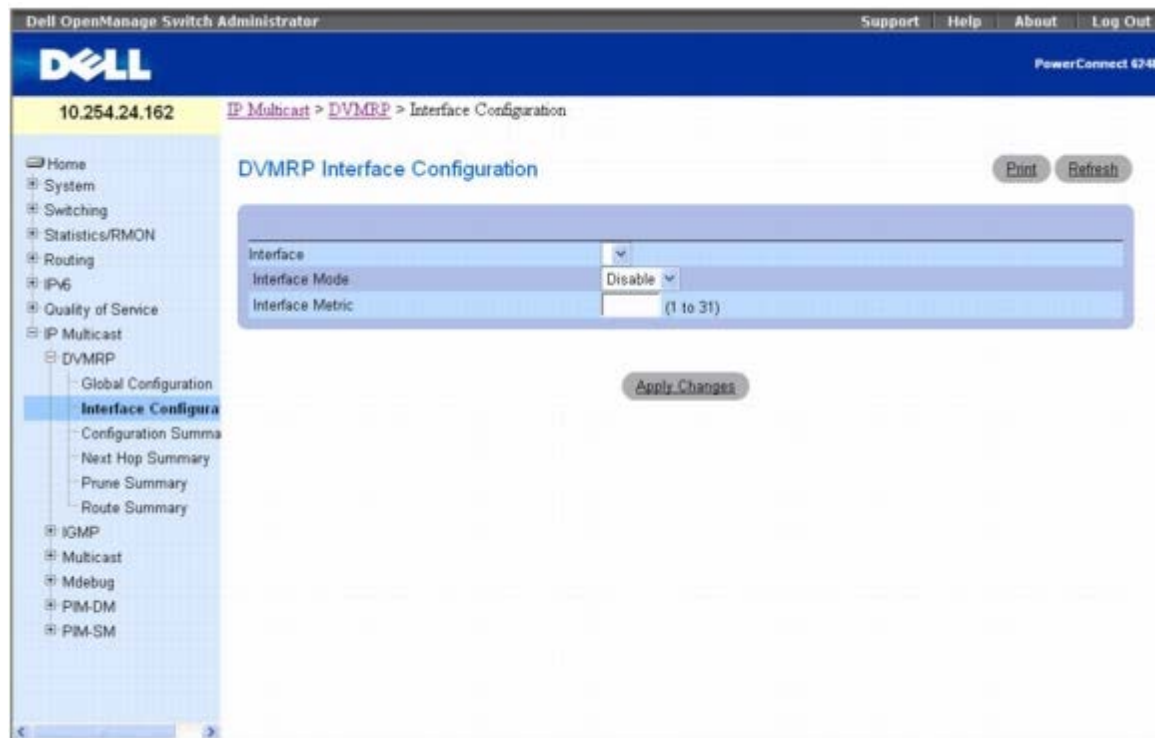
- DVMRP 命令

## DVMRP 接口配置

**DVMRP Interface Configuration** (DVMRP 接口配置) 页面用于配置 DVMRP 接口。在配置 DVMRP 接口前, 必须先至少配置一个路由器接口。否则您会看到一条信息, 告诉您没有路由器接口可用, 而配置屏幕也不会显示。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **DVMRP** ® **Interface Configuration** (接口配置)。

图 13-2. DVMRP 接口配置



**DVMRP Interface Configuration** (DVMRP 接口配置) 页面包含以下字段:

**Interface** (接口) — 选择要为其配置数据的接口。在配置 DVMRP 接口前, 必须先至少配置一个路由器接口。

**Interface Mode** (接口模式) — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用), 设置所选 DVMRP 路由接口的管理模式。

**Interface Metric** (接口跃点数) — 为选定的接口输入 DVMRP 跃点数。在 DVMRP 信息中将此值作为到达此网络的成本发送。有效值是 1 至 31。

### 配置 DVMRP 接口

□□□ 打开 **DVMRP Interface Configuration** (DVMRP 接口配置) 页面。

□□□ 从 **Interface** (接口) 字段选择要配置的接口。

□□□ 根据需要修改其余字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存接口配置并更新设备。

## 使用 CLI 命令配置 DVMRP 接口

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- DVMRP 命令

## DVMRP 配置摘要

**DVMRP Configuration Summary** (DVMRP 配置摘要) 页面用于显示或打印所选接口的 DVMRP 配置和数据。必须先至少配置一个路由器接口, 才能显示 DVMRP 接口的数据。否则您会看到一条信息, 告诉您没有路由器接口可用, 而配置摘要屏幕也不会显示。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **DVMRP** ® **Configuration Summary** (配置摘要)。

图 13-3. DVMRP 配置摘要



**DVMRP Configuration Summary** (DVMRP 配置摘要) 页面包含以下字段:

**Interface** (接口) — 选择要为其显示数据的接口。必须先至少配置一个路由器接口, 才能显示 DVMRP 接口的数据。

接口参数

**Interface Mode** (接口模式) — 显示所选 DVMRP 路由接口的管理模式, 其值为 **Enable** (启用) 或 **Disable** (禁用)。

**Protocol State** (协议状态) — 显示 DVMRP 协议在所选接口上的操作状态, 其值为 **Operational** (可操作) 或 **Non-operational** (不可操作)。

**Local Address** (本地地址) — 显示从所选接口发送的信息包中作为源地址使用的 IP 地址。

**Interface Metric** (接口跃点数) — 显示用于计算所选接口距离向量的跃点数。

接口统计数据

**Generation ID** (世代 ID) — 显示路由器用于所选接口的 DVMRP 世代 ID。每次启动 (重启) 接口时就会重置此值, 并将其放到删减信息中。如果世代 ID 发生变化, 就是告知邻居路由器应放弃此前关于此路由器的所有信息。

**Received Bad Packets** (接收的坏信息包) — 所选接口上接收到的无效信息包的数量。

**Received Bad Routes**（接收的坏路由）— 所选接口上接收到的无效路由的数量。

**Sent Routes**（发送的路由）— 在选定的接口上发送的路由数量。

邻居参数

**Neighbor IP**（邻居 IP）— 邻居的 IP 地址，显示的信息就是该邻居的信息。

**State**（状态）— 所选接口上指定的邻居路由器的状态：活动或停机。

**Neighbor Uptime**（邻居正常运行时间）— 所选接口上指定的邻居的 DVMRP 正常运行时间。此时间从邻居得知邻居输入项之时算起。

**Neighbor Expiry Time**（邻居过期时间）— 所选接口上指定的邻居的 DVMRP 过期时间。这是此邻居输入项过期前剩余的时间，如果邻居路由器的状态是停机，则此字段不适用。

**Generation ID**（世代 ID）— 所选接口上指定的邻居的 DVMRP 世代 ID。

**Major Version**（主版本）— 所选接口上指定的邻居的 DVMRP 主版本。

**Minor Version**（次版本）— 所选接口上指定的邻居的 DVMRP 次版本。

**Capabilities**（功能）— 所选接口上指定的邻居的 DVMRP 功能。

**Received Routes**（接收的路由）— 所选接口上接收的指定邻居的路由数。

**Received Bad Packets**（接收的坏信息包）— 所选接口上接收到的指定邻居的无效信息包数量。

**Received Bad Routes**（接收的坏路由）— 所选接口上接收到的指定邻居的无效路由数量。

## 使用 CLI 命令显示 DVMRP 配置摘要

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

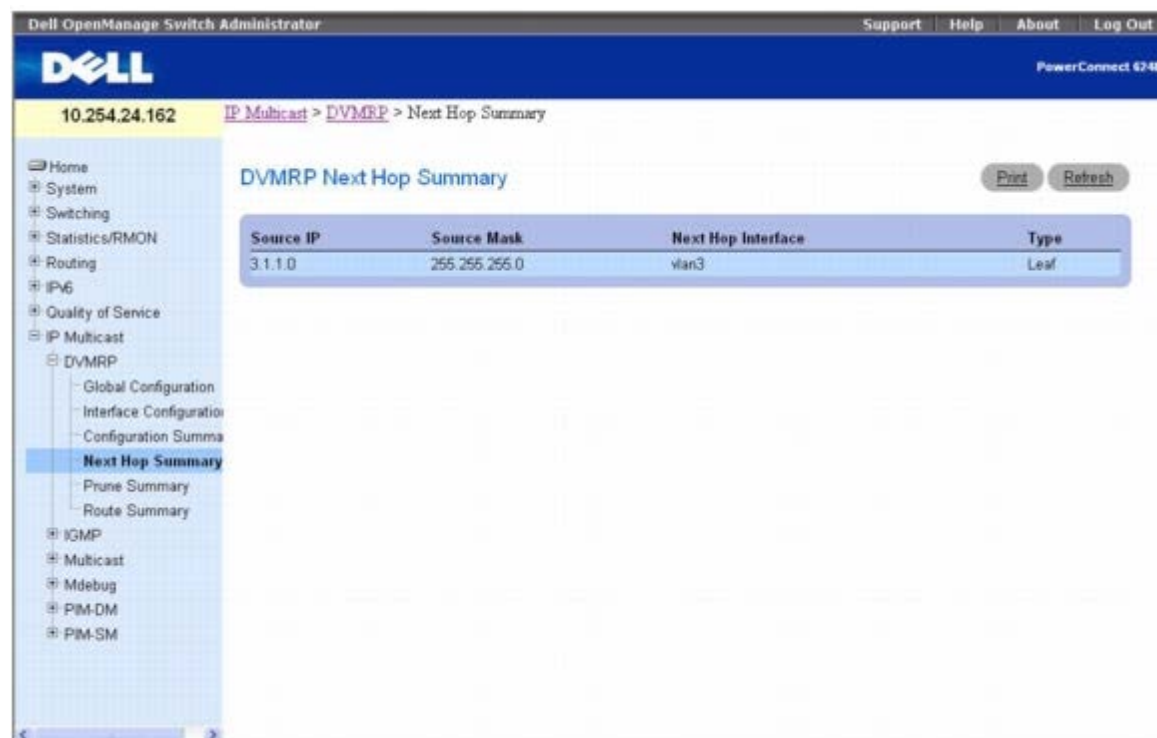
- DVMRP 命令

## 下一跃距摘要

**Next Hop Summary**（下一跃距摘要）页面用于按源 IP 显示或打印下一跃距摘要。

要显示此页面，请在树视图中单击 **IP Multicast**（IP 多点传送）® **DVMRP** ® **Next Hop Summary**（下一跃距摘要）。

图 13-4. 下一跃距摘要



**Next Hop Summary** (下一跃距摘要) 页面包含以下字段:

**Source IP** (源 IP) — 显示 IP 地址, 该地址将与源掩码一起用于识别此表格输入项的源网络。

**Source Mask** (源掩码) — 显示和源 IP 地址结合使用的网络掩码。

**Next Hop Interface** (下一跃距接口) — 显示下一跃距的发送接口。

**Type** (类型) — 显示下一跃距类型。类型为 **Leaf** (叶) 表示发送接口上不存在下游相关邻居。否则, 类型将为 **Branch** (分支)。

## 使用 CLI 命令显示下一跃距摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

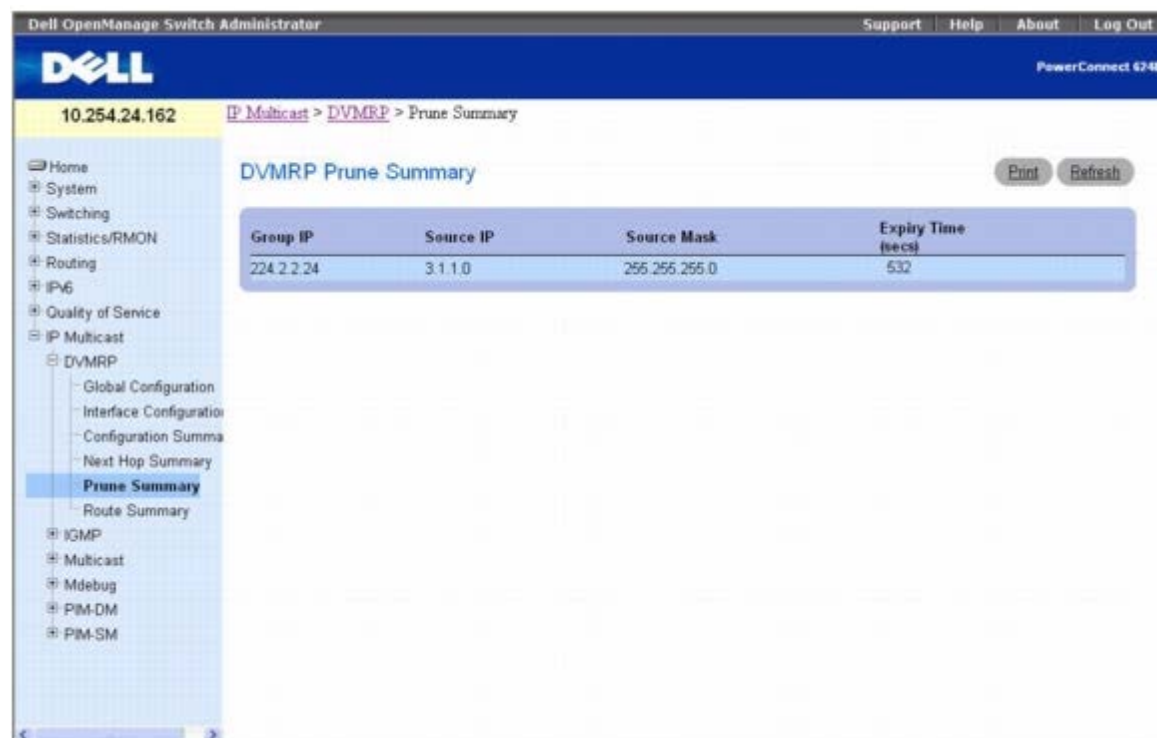
- DVMRP 命令

## 删减摘要

**Prune Summary** (删减摘要) 页面用于按组 IP 显示或打印删减摘要。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **DVMRP** ® **Prune Summary** (删减摘要)。

图 13-5. 删减摘要



**Prune Summary** (删减摘要) 页面会显示以下字段:

**Group IP** (组 IP) — 删减的组地址。

**Source IP** (源 IP) — 删减的源或源网络地址。

**Source Mask** (源掩码) — 将与源 IP 地址结合使用的子网掩码, 以识别删减的源或源网络。

**Expiry Time (secs)** (过期时间 [秒]) — 此删减在上游邻居处过期前剩余的时间。如果没有从下游邻居接收到删减信息, 则此字段设置为默认删减使用寿命计时器的值, 否则设置为收到的最小值或默认计时器值 (以较小者为准)。

## 使用 CLI 命令显示删减摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- DVMRP 命令

## 路由摘要

**Route Summary** (路由摘要) 页面用于显示或打印 DVMRP 路由摘要。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **DVMRP** ® **Route Summary** (路由摘要)。

图 13-6. 路由摘要



Dell OpenManage Switch Administrator

Support Help About Log Out

PowerConnect 6248

10.254.24.162 IP Multicast > DVMRP > Route Summary

DVMRP Route Summary

Source Address	Source Mask	Upstream Neighbor	Interface	Metric	Expiry Time (secs)	UP Time (secs)
9.0.0.0	255.0.0.0	0.0.0.0	vlan9	0	0	224
15.0.0.0	255.0.0.0	0.0.0.0	vlan10	0	0	224
20.20.15.0	255.255.255.0	9.1.1.3	vlan9	4	0	205
20.20.20.0	255.255.255.0	9.1.1.3	vlan9	4	0	205

**Route Summary** (路由摘要) 页面会显示以下字段:

**Source Address** (源地址) - 与源掩码结合使用的网络地址, 以识别此输入项的源。

**Source Mask** (源掩码) — 与源地址结合使用的子网掩码, 以识别此输入项的源。

**Upstream Neighbor** (上游邻居) — 上游邻居 (例如 RPF 邻居) 的地址, 从该邻居接收到来自这些源的 IP 数据包。

**Interface** (接口) — 接收到这些源发送的 IP 数据包的接口。如果值为 0, 通常表示路由是不存在下一跃距接口的集合。

**Metric** (跃点数) — 到源子网的距离, 以跃距计。

**Expiry Time** (过期时间) — 在此输入项过期前剩余的最少时间。

**Up Time** (运行时间) — 从路由器得知此输入项代表的路由之时算起的时间。

## 使用 CLI 命令显示 DVMRP 路由摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- DVMRP 命令

## IGMP

Internet 组管理协议 (IGMP) 由 IPv4 系统 (主机和路由器) 用于将它们 IP 多点传送组成员关系报告给任何邻近的多点传送路由器。6200 系列担当 IGMP 协议的多点传送路由器角色, 这意味着它将收集进行有效多点传送路由所需的成员关系信息。当前在 6200 系列中支持的多点传送路由协议是 DVMRP、PIM-DM 和 PIM-SM。

6200 系列支持 IGMP 第 3 版。第 3 版增加了对源筛选的支持, 该功能让系统可以报告对接收信息包的兴趣: 是仅接收自特定源地址发送到特定多点传送地址的信息包 (这是支持源特定多点传送 [SSM] 所必需的), 还是接收自特定源地址之外的所有地址发送到特定多点传送地址的信息包。第 3 版的设计使其可与第 1 版和第 2 版协同工作。

**IGMP** 菜单页面包含一些网页的链接, 这些网页可用于定义和显示 IGMP 参数和数据。要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送) @ IGMP**。

在此菜单页面中可以访问以下网页:

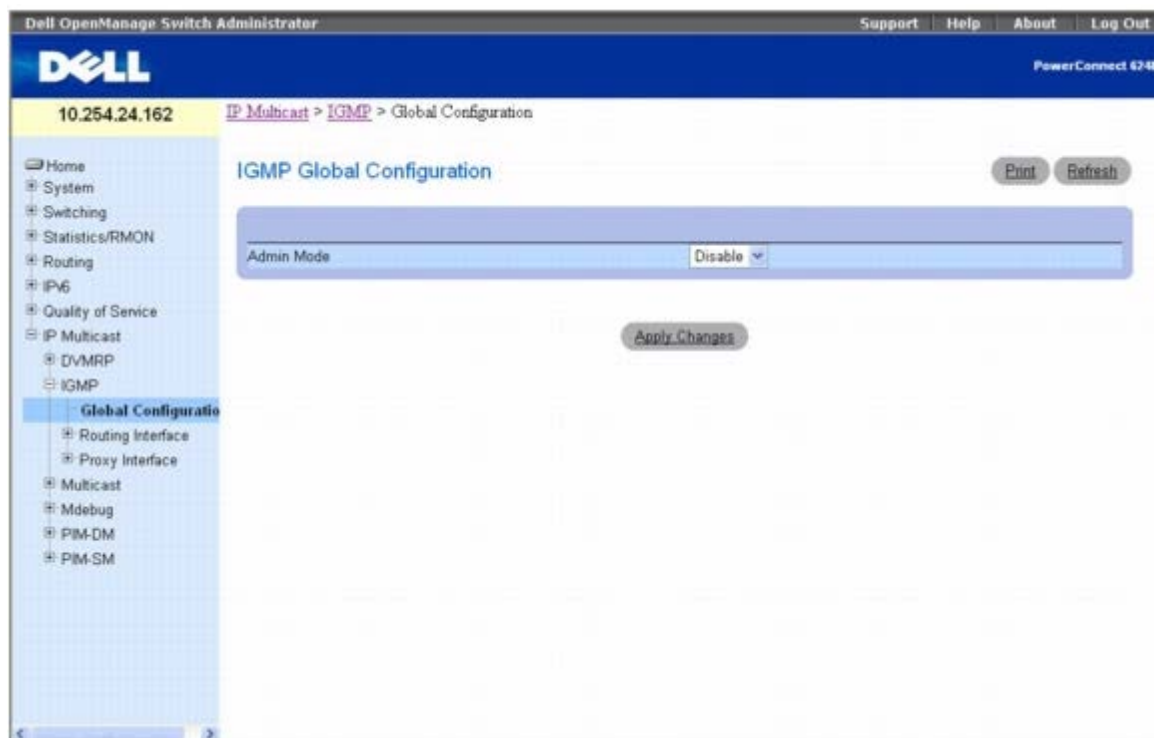
- [IGMP 全局配置](#)
- [路由接口](#)
- [代理接口](#)

## IGMP 全局配置

**IGMP Global Configuration (IGMP 全局配置)** 页面用于将系统上的 IGMP 设置为活动或不活动。

要显示此页面,请在树视图中单击 **IP Multicast (IP 多点传送) ® IGMP ® Global Configuration (全局配置)**。

图 13-7. IGMP 全局配置



**IGMP Global Configuration (IGMP 全局配置)** 页面包含以下字段:

**Admin Mode (管理模式)** — 从下拉式菜单中选择 **Enable (启用)** 或 **Disable (禁用)**, 将路由器中 IGMP 的管理状态设置为活动或不活动。默认值为 **Disable (禁用)**。

### 设置 IGMP 模式

- 打开 **IGMP Global Configuration (IGMP 全局配置)** 页面。
- 将 **Admin Mode (管理模式)** 设置为 **Enable (启用)** 或 **Disable (禁用)**, 以打开或关闭 IGMP。
- 单击 **Apply Changes (应用更改)**。

系统将保存 IGMP 配置并更新设备。

### 使用 CLI 命令设置 IGMP 模式

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- IGMP 命令

## 路由接口

**Routing Interface** (路由接口) 菜单页面包含一些网页的链接, 这些网页可用于配置和显示 IGMP 路由参数和数据。要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送) @ IGMP @ Routing Interface (路由接口)**。在此菜单页面中可以访问以下网页:

- [IGMP 接口配置](#)
- [IGMP 配置摘要](#)
- [IGMP 高速缓存信息](#)
- [IGMP 接口详细成员关系信息](#)

## IGMP 接口配置

**IGMP Interface Configuration (IGMP 接口配置)** 页面用于配置和/或显示路由器接口参数。必须先至少配置一个有效的路由接口, 才能访问此页面和配置 IP 多点传送 IGMP。

要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送) @ IGMP @ Routing Interface (路由接口) @ Interface Configuration (接口配置)**。

图 13-8. IGMP 接口配置



**IGMP Interface Configuration (IGMP 接口配置)** 页面包含以下字段:

**Interface (接口)** — 从下拉式菜单中选择要显示数据或配置的接口。

**Interface Mode (接口模式)** — 从下拉式菜单中选择 **Enable (启用)** 或 **Disable (禁用)**, 设置所选接口上 IGMP 的管理状态。默认值为 **Disable (禁用)**。

**Version** (版本) — 输入要在所选接口上配置的 IGMP 版本。有效值从 1 到 3, 默认值是 3。只有在启用 IGMP 接口模式时, 才能配置此字段。

**Robustness** (坚固) — 输入坚固值。此变量允许调整子网上预期的信息包丢失。如果您预计子网上发生丢失的可能性很大, 则应该为此参数输入一个较高的值。IGMP 可以耐受 (坚固变量-1) 信息包丢失。有效值从 1 到 255。默认值是 2。

**Query Interval (secs)** (查询间隔 [秒]) — 输入要在此接口上发送 IGMP 主机查询信息包的频率, 以秒为单位。有效值从 1 到 3600。默认值是 125。

**Query Max Response Time (1/10 of a second)** (查询最长响应时间 [1/10 秒]) — 输入要在此接口上的 IGMPv2 查询中公布的最长查询响应时间, 以十分之一秒为单位。默认值是 100。有效值从 0 到 255。

**Startup Query Interval (secs)** (启动查询间隔 [秒]) — 输入在选定的接口上两次启动查询发送之间的秒数。有效值从 1 到 300。默认值是 31。

**Startup Query Count** (启动查询计数) — 输入启动时要发送的查询数。有效值从 1 到 20。默认值是 2。

**Last Member Query Interval (1/10 of a second)** (最后成员查询间隔 [1/10 秒]) — 输入最后成员查询间隔, 以十分之一秒为单位。这是要插入到为响应离组信息而发送的组特定查询中的最长响应时间, 也是两条组特定查询信息之间的时间。有效值从 0 到 255。默认值是 10。此值不用于 IGMP 第 1 版。

**Last Member Query Count** (最后成员查询计数) — 输入在收到离组报告时要发送的查询数。有效值从 1 到 20。默认值是 2。

## 配置 IGMP 路由接口

□□□ 打开 **IGMP Interface Configuration (IGMP 接口配置)** 页面。

□□□ 从 **Interface** (接口) 字段选择要配置的接口。

□□□ 根据需要修改其余字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存接口配置并更新设备。

## 使用 CLI 命令配置 IGMP 路由接口

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- IGMP 命令

## IGMP 配置摘要

**IGMP Configuration Summary (IGMP 配置摘要)** 页面用于显示 IGMP 路由参数和数据。您必须至少配置一个 IGMP 路由器接口才能访问此页面。

要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送) ® IGMP ® Routing Interface (路由接口) ® Configuration Summary (配置摘要)**。

图 13-9. IGMP 配置摘要

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb navigation is: IP Multicast > IGMP > Routing Interface > Configuration Summary. The main content area is titled "IGMP Configuration Summary" and shows the configuration for interface "vlan3".

**Interface Parameters**

Interface Mode	Enable
IP Address	3.1.1.2
Subnet Mask	255.255.255.0
Protocol State	Operational
Version	3
Query Interval (secs)	125
Query Max Response Time (1/10 of a second)	100
Robustness	2
Startup Query Interval (secs)	31
Startup Query Count	2
Last Member Query Interval (1/10 of a second)	10
Last Member Query Count	2

**Interface Statistics**

Querier	3.1.1.2
Querier Status	Querier
Querier Up Time (secs)	1832
Querier Expiry Time (secs)	0
Wrong Version Queriers	0
Number of Joins	0
Number of Groups	0

**IGMP Configuration Summary (IGMP 配置摘要)** 页面会显示以下字段:

**Interface** (接口) — 选择要为其显示数据的接口。

接口参数

**Interface Mode** (接口模式) — 所选接口上的 IGMP 的管理状态。

**IP Address** (IP 地址) — 所选接口的 IP 地址。

**Subnet Mask** (子网掩码) — 所选接口的 IP 地址子网掩码。

**Protocol State** (协议状态) — 所选接口上的 IGMP 的操作状态。

**Version** (版本) — 所选接口上配置的 IGMP 版本。

**Query Interval (secs)** (查询间隔 [秒]) — 在选定的接口上发送 IGMP 主机查询信息包的频率。

**Query Max Response Time (1/10 of a second)** (查询最长响应时间 [1/10 秒]) — 在从所选接口发送的 IGMPv2 查询中公布的最长查询响应时间。

**Robustness** (坚固) — 所选接口的坚固参数。此变量允许调整子网上预期的信息包丢失。如果预计子网上发生丢失的可能性很大,则可增大坚固变量。IGMP 可以耐受 (坚固变量-1) 信息包丢失。

**Startup Query Interval (secs)** (启动查询间隔 [秒]) — 在选定的接口上发送启动查询的间隔。

**Startup Query Count** (启动查询计数) — 启动时要发送的查询数。

**Last Member Query Interval (1/10 of a second)** (最后成员查询间隔 [1/10 秒]) — 最后成员查询间隔是要插入到为响应离组信息而发送的组特定查询中的最长响应时间,也是两条组特定查询信息之间的时间。可调整此值来修改网络的离开等待时间。如果减少该值,则会导致检测组中最后成员丢失的时间减少。此值不用于 IGMP 第 1 版。

**Last Member Query Count** (最后成员查询计数) — 在收到离组报告时要发送的查询数。

接口统计数据

**Querier** (查询器) — IGMP 查询器在 IP 子网上的地址,选定的接口与该子网连接。



**Querier Status** (查询器状态) — 表明选定的接口是处于查询器模式还是非查询器模式。

**Querier Up Time (secs)** (查询器运行时间 [秒]) — 自 IGMP 接口查询器最后一次更改以来的时间, 以秒为单位。

**Querier Expiry Time (secs)** (查询器过期时间 [秒]) — 其它查询器存在计时器过期前的剩余时间, 以秒为单位。如果本地系统就是查询器, 则此值为零。

**Wrong Version Queries** (错误版本查询) — 在输入项的整个使用寿命中, 在选定的接口上收到 IGMP 版本与接口所配置 IGMP 版本不匹配的查询数。IGMP 要求 LAN 上所有路由器都配置为运行相同版本的 IGMP。因此, 如果收到任何版本号错误的查询, 就说明配置有误。

**Number of Joins** (加入数) — 在选定的接口上添加组成员关系的次数, 也就是将关于此接口的输入项添加到高速缓存表的次数。这样可以表明接口上的 IGMP 活动量。

**Number of Groups** (组数量) — 高速缓存表中所选接口的当前输入项数。

## 使用 CLI 命令显示 IGMP 路由配置

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- IGMP 命令

## IGMP 高速缓存信息

**IGMP Cache Information** (IGMP 高速缓存信息) 页面用于显示 IP 多点传送组地址的高速缓存参数和数据。您必须至少配置一个 IGMP 路由器接口才能访问此页面。而且必须在选定的接口上收到组成员关系报告, 才能在此处显示数据。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **IGMP** ® **Routing Interface** (路由接口) ® **Cache Information** (高速缓存信息)。

图 13-10. IGMP 高速缓存信息

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb navigation is: IP Multicast > IGMP > Routing Interface > Cache Information. The page title is "IGMP Cache Information". There are "Print" and "Refresh" buttons. The configuration section shows:

Interface	vlan20
Multicast Group IP	225.0.1.1
Last Reporter	2.1.1.100

The statistics table shows:

Up Time (secs)	147
Expiry Time (secs)	113
Version 2 Host Timer (secs)	113
Compatibility	v2

**IGMP Cache Information** (IGMP 高速缓存信息) 页面会显示以下字段:

**Interface** (接口) — 选择要为其显示数据的接口。

**Multicast Group IP** (多点传送组 IP) — 选择要显示数据的 IP 多点传送组地址。如果选定的接口上没有收到组成员关系报告, 则不能进行选

择, 在此页面上也不会显示数据。

**Last Reporter** (最后报告者) — 在选定的接口 IP 多点传送组地址接收到的最后一份组成员关系报告的来源 IP 地址。

**Up Time** (运行时间) — 自创建此输入项以来经过的时间。

**Expiry Time** (过期时间) — 在此输入项过期前剩余的最少时间。

**Version 1 Host Timer** (第 1 版主机计时器) — 本地路由器认定连接到此接口的 IP 子网上不再有任何 IGMP 第 2 版成员之前剩余的时间。当收到 IGMPv1 成员关系报告时, 此计时器将重置为组成员关系计时器。此计时器非零时, 本地路由器会忽略它在所选接口上收到的关于此组的任何 IGMPv2 离开信息。只有针对 IGMP 第 1 版配置此接口后, 才会显示此字段。

**Version 2 Host Timer** (第 2 版主机计时器) — 本地路由器认定连接到此接口的 IP 子网上不再有任何 IGMP 第 2 版成员之前剩余的时间。当收到 IGMPv2 成员关系报告时, 此计时器将重置为组成员关系计时器。此计时器非零时, 本地路由器会忽略它在所选接口上收到的关于此组的任何 IGMPv1 和 IGMPv3 离开信息。只有针对 IGMP 第 2 版配置此接口后, 才会显示此字段。

**Compatibility** (兼容性) — 此参数显示该组在指定接口上的组兼容性模式 (v1、v2 和 v3)。

**Filter Mode** (筛选模式) — 在此接口上指定组的源筛选模式 (Include [包括]/Exclude [排除]/NA [无])。如果 NA (无) 模式处于活动状态, 则此字段为空白。

## 使用 CLI 命令显示高速缓存信息

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

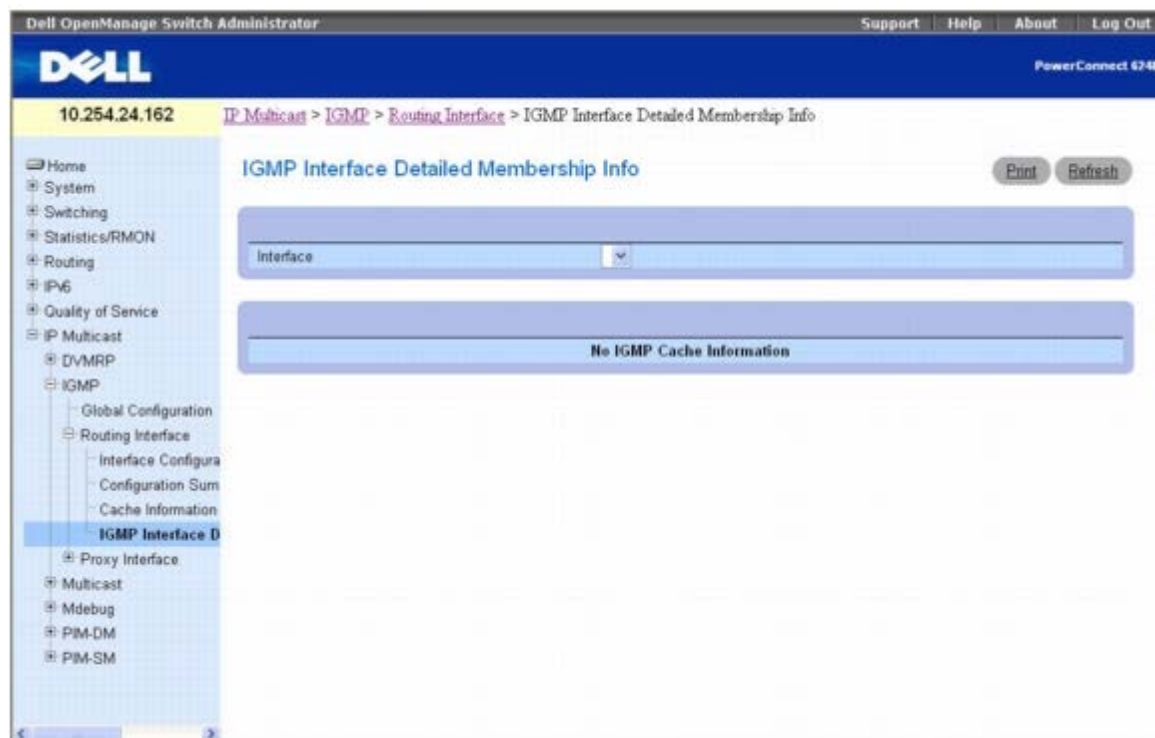
- IGMP 命令

## IGMP 接口详细成员关系信息

**IGMP Interface Detailed Membership Info** (IGMP 接口详细成员关系信息) 页面用于显示接口的详细成员关系信息。您必须至少配置一个 IGMP 路由器接口才能访问此页面。而且必须在选定的接口上收到组成员关系报告, 才能在此处显示数据。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **IGMP** ® **Routing Interface** (路由接口) ® **IGMP Interface Detailed Membership Info** (IGMP 接口详细成员关系信息)。

图 13-11. IGMP 接口详细成员关系信息





**IGMP Interface Detailed Membership Info** (IGMP 接口详细成员关系信息) 页面会显示以下字段:

**Interface** (接口) — 选择要为其显示数据的接口。

**Multicast Group IP** (多点传送组 IP) — 选择要显示数据的 IP 多点传送组地址。如果选定的接口上没有收到组成员关系报告, 则不能进行选择, 其余字段也不会显示。

**Interface** (接口) — 转发多点传送信息包的接口。

**Group Compatibility Mode** (组兼容性模式) — 在指定接口上此组的组兼容性模式 (v1、v2 和 v3)。

**Source Filter Mode** (源筛选模式) — 在此接口上指定组的源筛选模式 (Include [包括]/Exclude [排除]/NA [无])。

**Source Hosts** (源主机) — 此多点传送地址所含的源地址。

**Expiry Time** (过期时间) — 对于此多点传送组所含的每个源地址的过期时间间隔。经过此段时间后, 指定的源输入项即过期。

## 显示 IGMP 接口详细成员关系

□□□ 打开 **IGMP Interface Detailed Membership Info** (IGMP 接口详细成员关系信息) 页面。

□□□ 从 **Interface** (接口) 下拉式菜单中选择要显示的接口。

□□□ 选择所需的 **Multicast Group IP** (多点传送组 IP)。

系统将显示此接口和多点传送组 IP 的详细成员关系信息。

## 使用 CLI 命令显示 IGMP 接口详细成员关系

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- IGMP 命令

## 代理接口

IGMP 代理的用途是使多点传送路由器能了解多点传送组成员关系信息, 并能根据组成员关系信息转发多点传送信息包。IGMP 代理只能在某些不需要多点传送路由协议 (即 DVMRP、PIM-DM 和 PIM-SM) 的树状拓扑中工作, 原因是此类拓扑不支持生成树等用于纠正信息包路由循环的功能。

**Proxy Interface** (代理接口) 菜单页面包含一些网页的链接, 这些网页可用于定义和显示代理接口参数和数据。要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **IGMP** ® **Proxy Interface** (代理接口)。在此菜单页面中可以访问以下网页:

- [IGMP 代理接口配置](#)
- [IGMP 代理配置摘要](#)
- [IGMP 代理接口成员关系信息](#)
- [IGMP 代理接口成员关系详细信息](#)

## IGMP 代理接口配置

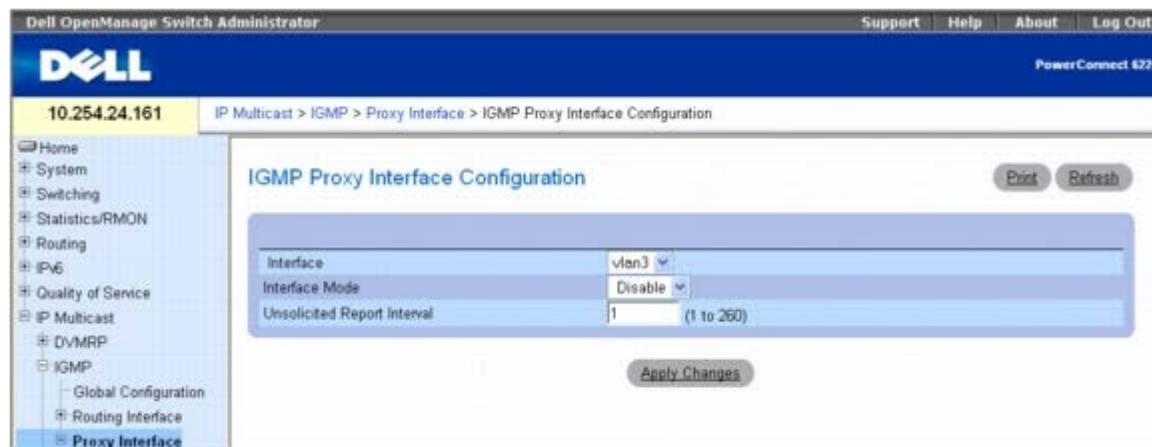
IGMP 代理由 IGMP 路由器 (IPv4 系统) 来使用, 这样系统便能代表系统通过标准 IGMP 路由器接口发现的主机发出 IGMP 主机信息。因此, 该功能可为驻留在路由器接口上的所有主机充当代理。

**IGMP Proxy Interface Configuration** (IGMP 代理接口配置) 页面用于配置 IGMP 接口。您必须先至少配置一个路由器接口, 才能为

IGMP 代理接口配置或显示数据，而且该接口不能是 IGMP 路由接口。

要显示此页面，请在树视图中单击 **IP Multicast (IP 多点传送) ® IGMP ® Proxy Interface (代理接口) ® Interface Configuration (接口配置)**。

图 13-12. IGMP 代理接口配置



**IGMP Proxy Interface Configuration (IGMP 代理接口配置)** 页面包含以下字段：

**Interface (接口)** — 从下拉式菜单中选择要为其显示数据或配置的接口。您必须先至少配置一个路由器接口，才能为 IGMP 代理接口配置或显示数据，而且该接口不能是 IGMP 路由接口。只有在禁用接口模式时，才可配置此字段。

**Interface Mode (接口模式)** — 从下拉式菜单中选择 **Enable (启用)** 或 **Disable (禁用)**，设置所选接口上的 IGMP 代理的管理状态。默认值为 **Disable (禁用)**。要启用 IGMP 代理接口模式，应启用路由、IGMP 和多点传送全局管理模式。

**Unsolicited Report Interval (主动报告间隔)** — 输入主动的时间间隔值，以秒为单位。**Unsolicited Report Interval (主动报告间隔)** 是主机对组内成员关系重复进行初始报告的时间间隔。有效值从 **1** 到 **260**。默认值是 **1**。

## 配置 IGMP 代理接口

□□□ 打开 **IGMP Proxy Interface Configuration (IGMP 代理接口配置)** 页面。

□□□ 从 **Interface (接口)** 下拉式菜单中选择要显示的接口。

□□□ 根据需要修改其余字段。

□□□ 单击 **Apply Changes (应用更改)**。

系统将保存代理接口配置并更新设备。

## 使用 CLI 命令配置 IGMP 代理接口

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- IGMP 代理命令

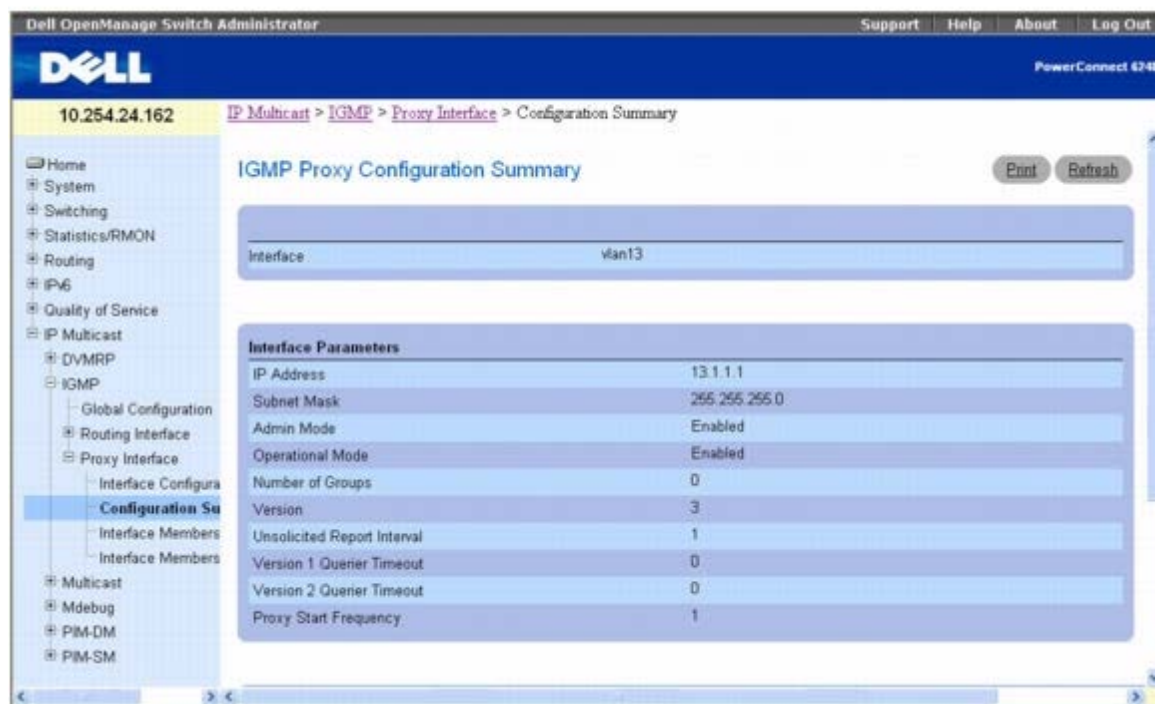
## IGMP 代理配置摘要

**IGMP Proxy Configuration Summary (IGMP 代理配置摘要)** 页面用于按接口显示代理接口配置。您必须先至少配置一个路由器接口，才能在此页面上显示数据。

要显示此页面，请在树视图中单击 **IP Multicast (IP 多点传送) ® IGMP ® Proxy Interface (代理接口) ® Configuration**

**Summary** (配置摘要)。

图 13-13. IGMP 代理配置摘要



**IGMP Proxy Configuration Summary** (IGMP 代理配置摘要) 页面会显示以下字段:

**Interface** (接口) — 显示启用 IGMP 代理的接口。只能有一个 IGMP 代理接口。

**IP Address** (IP 地址) — IGMP 代理接口的 IP 地址。

**Subnet Mask** (子网掩码) — IGMP 代理接口的 IP 地址子网掩码。

**Admin Mode** (管理模式) — 所选接口上 IGMP 代理的管理状态。

**Operational Mode** (工作模式) — IGMP 代理接口的工作状态。

**Number of Groups** (组数量) — 高速缓存表中 IGMP 代理接口的当前多点传送组输入项数。

**Version** (版本) — IGMP 代理接口上配置的 IGMP 版本。

**Unsolicited Report Interval** (主动报告间隔) — Unsolicited Report Interval (主动报告间隔) 是主机对组内成员关系重复进行初始报告的时间间隔。默认值: 1 秒。

**Version 1 Querier Timeout** (第 1 版查询器超时) — 较早的 IGMP 第 2 版查询器超时值, 以秒为单位。较早版本查询器间隔是在收到较早版本查询时, 将主机过渡回 IGMPv3 模式的超时。在收到较早版本查询时, 主机会将其 Older Version Querier Present Timer (较早版本查询器存在计时器) 设置为 Older Version Querier Interval (较早版本查询器间隔)。

**Version 2 Querier Timeout** (第 2 版查询器超时) — 较早的 IGMP 第 2 版查询器超时值, 以秒为单位。

**Proxy Start Frequency** (代理启动频率) — 启动代理的次数。

**Proxy Interface Statistics** (代理接口统计数据) — 收到的查询、收到/发送的报告、收到/发送的离开。

## 使用 CLI 命令显示 IGMP 代理接口配置

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

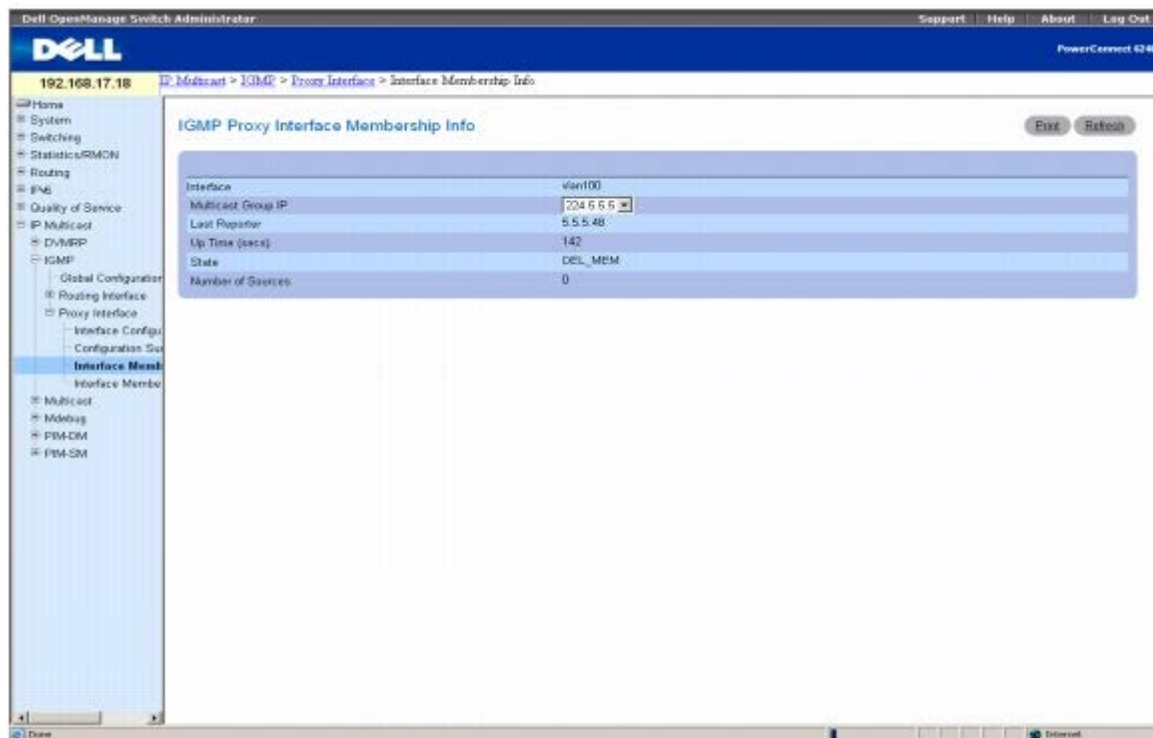
- IGMP 代理命令

## IGMP 代理接口成员关系信息

**IGMP Proxy Interface Membership Info** (IGMP 代理接口成员关系信息) 页面用于显示特定 IP 多点传送组地址的接口成员关系信息数据。您必须先至少配置一个路由器接口, 才能显示接口成员关系信息, 而且该接口不能是 IGMP 路由接口。此外, 如果选定的接口上没有收到组成员关系报告, 则此页面上不会显示数据。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **IGMP** ® **Proxy Interface** (代理接口) ® **Interface Membership Info** (接口成员关系信息)。

图 13-14. IGMP 代理接口成员关系信息



**IGMP Proxy Interface Membership Info** (IGMP 代理接口成员关系信息) 页面会显示以下字段:

**Interface** (接口) — 显示启用 IGMP 代理的接口。

**Multicast Group IP** (多点传送组 IP) — 选择要显示数据的 IP 多点传送组地址。如果选定的接口上没有收到组成员关系报告, 则不能进行选择, 也不会显示下列数据。

**Last Reporter** (最后报告者) — 在 IGMP 代理接口 IP 多点传送组地址接收到的最后一份成员关系报告的来源 IP 地址。

**Up Time (secs)** (运行时间 [秒]) — 自创建此输入项以来经过的时间。

**State** (状态) — 主机输入项的状态。主机可以处于多种状态之一。非成员状态 - 主机不属于接口上的组。延迟成员状态 - 主机属于接口上的组, 而且报告计时器正在运行。报告计时器用于发出报告。空闲成员状态 - 主机属于接口上的组, 但没有报告计时器在运行。

**Number of Sources** (源数量) — 所选多点传送组中存在的源主机数量。

## 使用 CLI 命令显示 IGMP 代理接口成员关系信息

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

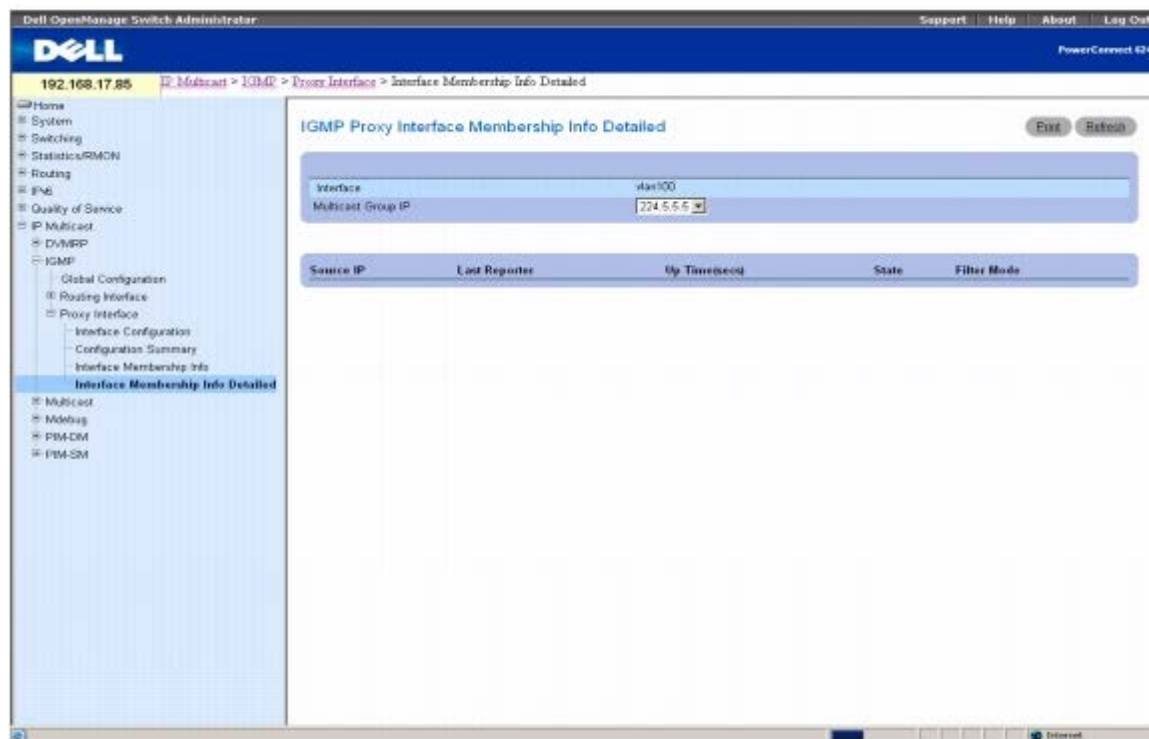
- IGMP 代理命令

## IGMP 代理接口成员关系详细信息

**IGMP Proxy Interface Membership Info Detailed** (IGMP 代理接口成员关系详细信息) 页面用于显示详细的接口成员关系数据。您必须先至少配置一个路由器接口, 才能显示详细的接口成员关系信息, 而且该接口不能是 IGMP 路由接口。此外, 如果选定的接口上没有收到组成员关系报告, 则不能显示数据。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **IGMP** ® **Proxy Interface** (代理接口) ® **Interface Membership Info Detailed** (接口成员关系详细信息)。

图 13-15. IGMP 代理接口成员关系详细信息



**IGMP Proxy Interface Membership Info Detailed** (IGMP 代理接口成员关系详细信息) 页面包含以下字段:

**Interface** (接口) — 选择要为其显示数据的接口。

**Multicast Group IP** (多点传送组 IP) — 选择要显示数据的 IP 多点传送组地址。如果选定的接口上没有收到组成员关系报告, 则不能进行选择, 也不会显示任何不可配置数据。

**Source IP** (源 IP) — 此参数显示该多点传送地址所含的源地址。

**Last Reporter** (最后报告者) — 在所选接口 IP 多点传送组地址接收到的最后一份组成员关系报告的来源 IP 地址。

**Up Time (secs)** (正常运行时间 [秒]) — 显示在高速缓存表中创建该输入项以来的正常运行时间。

**State** (状态) — 主机输入项的状态。主机可以处于下列状态之一:

**Non-member State** (非成员状态) — 主机不属于接口上的组。

**Delaying Member State** (延迟成员状态) — 主机属于接口上的组, 而且报告计时器正在运行。报告计时器用于发出报告。

**Idle Member State** (空闲成员状态) — 主机属于接口上的组, 但没有报告计时器在运行。

**Filter Mode** (筛选模式) — 在 IGMP 代理接口上指定组的组筛选模式 (Include [包括]/Exclude [排除]/None [无])。

## 显示 IGMP 代理接口成员关系详细信息

□□□ 打开 **IGMP Proxy Interface Membership Info Detailed** (IGMP 代理接口成员关系详细信息) 页面。

□□□ 从 **Interface** (接口) 下拉式菜单中选择要显示的接口。

□□□ 选择所需的 **Multicast Group IP** (多点传送组 IP)。

系统将显示此接口和多点传送组 IP 的详细成员关系数据。

## 使用 CLI 命令显示 IGMP 代理接口成员关系详细信息

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- IGMP 代理命令

---

## 多点传送

**Multicast** (多点传送) 菜单页面包含一些网页的链接, 这些网页可用于定义和显示多点传送 参数和数据。要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送) @ Multicast (多点传送)**。在此菜单页面中可以访问以下网页:

- [多点传送全局配置](#)
- [多点传送接口配置](#)
- [多点传送 Mroute 摘要](#)
- [多点传送静态路由配置](#)
- [多点传送静态路由摘要](#)
- [多点传送管理边界配置](#)
- [多点传送管理边界摘要](#)

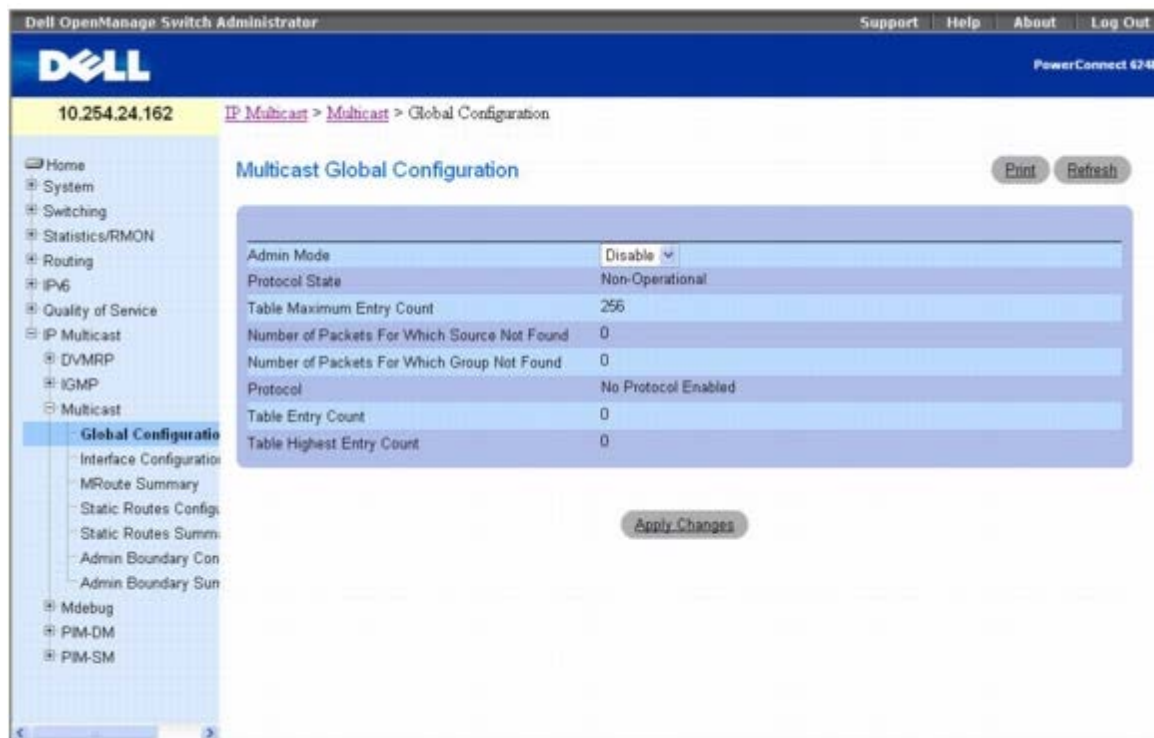
## 多点传送全局配置

**Multicast Global Configuration** (多点传送全局配置) 页面用于配置路由器中多点传送的管理状态, 以及显示全局多点传送参数。

要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送) @ Multicast (多点传送) @ Global Configuration (全局配置)**。

图 13-16. 多点传送全局配置





**Multicast Global Configuration** (多点传送全局配置) 页面包含以下字段:

**Admin Mode** (管理模式) — 选择 **Enable** (启用) 或 **Disable** (禁用) 以设置路由器中多点传送转发的管理状态。默认值为 **Disable** (禁用)。

**Protocol State** (协议状态) — 多点传送转发模块的操作状态。

**Table Maximum Entry Count** (表格最大输入项计数) — IP 多点传送路径选择表中的最大输入项数。

**Number Of Packets For Which Source Not Found** (未找到源的信息包数量) — 本应进行路由但未能通过 RPF 检查的多点传送信息包数量。

**Number Of Packets For Which Group Not Found** (未找到组的信息包数量) — 本应进行路由但未找到多点传送路由的多点传送信息包数量。

**Protocol** (协议) — 当前在路由器上激活的多点传送路由协议 (如果有)。

**Table Entry Count** (表格输入项计数) — 多点传送路由表中当前存在的多点传送路由输入项数量。

**Table Highest Entry Count** (表格最高输入项计数) — 多点传送路由表中已存在的多点传送路由输入项最高数量。

## 配置多点传送转发管理模式

- 打开 **Multicast Global Configuration** (多点传送全局配置) 页面。
- 在 **Admin Mode** (管理模式) 中选择 **Enable** (启用) 或 **Disable** (禁用)。
- 单击 **Apply Changes** (应用更改)。

系统将保存多点传送全局配置并更新设备。

## 使用 CLI 命令配置/显示多点传送转发参数

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- 多点传送命令

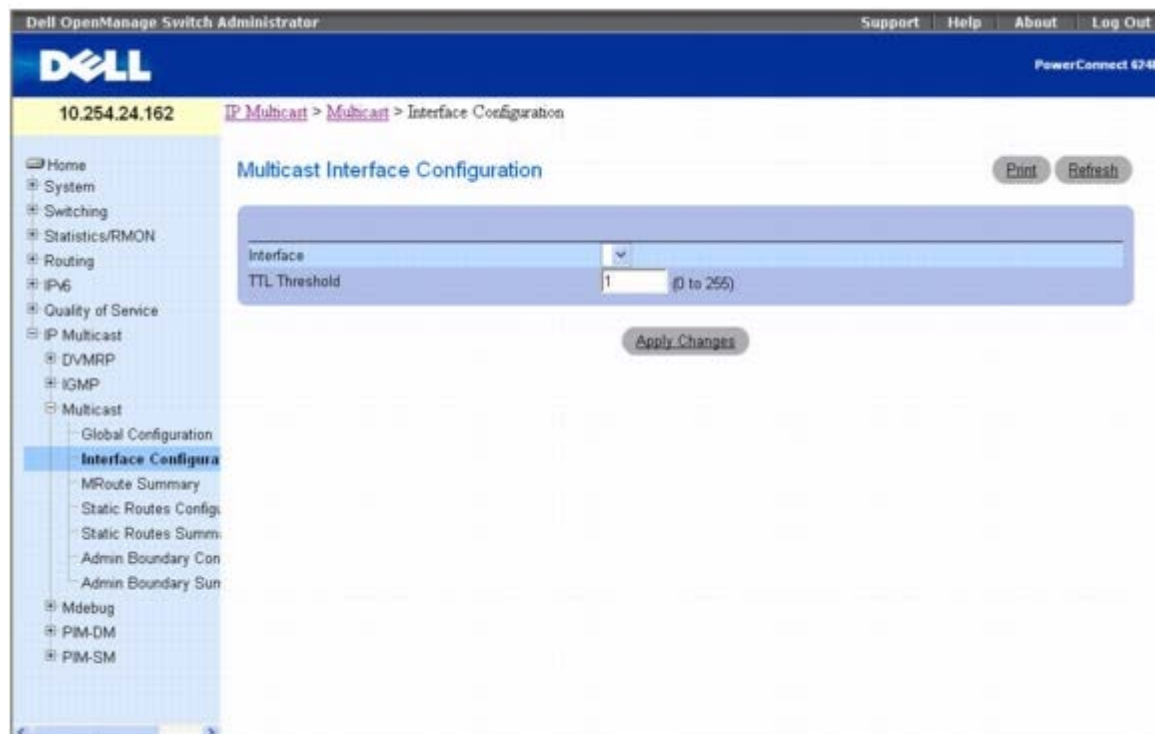


## 多点传送接口配置

**Multicast Interface Configuration** (多点传送接口配置) 页面用于配置多点传送接口的 TTL 阈值。您必须至少先配置一个路由器接口, 此页面上的字段才能显示。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **Multicast** (多点传送) ® **Interface Configuration** (接口配置)。

图 13-17. 多点传送接口配置



**Multicast Interface Configuration** (多点传送接口配置) 页面包含以下字段:

**Interface** (接口) — 从下拉式菜单中选择要配置的路由接口。

**TTL Threshold** (TTL 阈值) — 输入 TTL 阈值, 低于此值时不会从选定的接口转发多点传送数据信息包。输入一个介于 0 到 255 之间的数字。如果输入 0, 则会转发所选接口的所有多点传送信息包。您必须至少先配置一个路由器接口, 才能看见此字段。

### 配置多点传送接口

□□□ 打开 **Multicast Interface Configuration** (多点传送接口配置) 页面。

□□□ 从 **Interface** (接口) 下拉式菜单中选择要配置的接口。

□□□ 输入所需的 **TTL Threshold** (TTL 阈值)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存多点传送接口配置并更新设备。

### 使用 CLI 命令配置多点传送接口

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

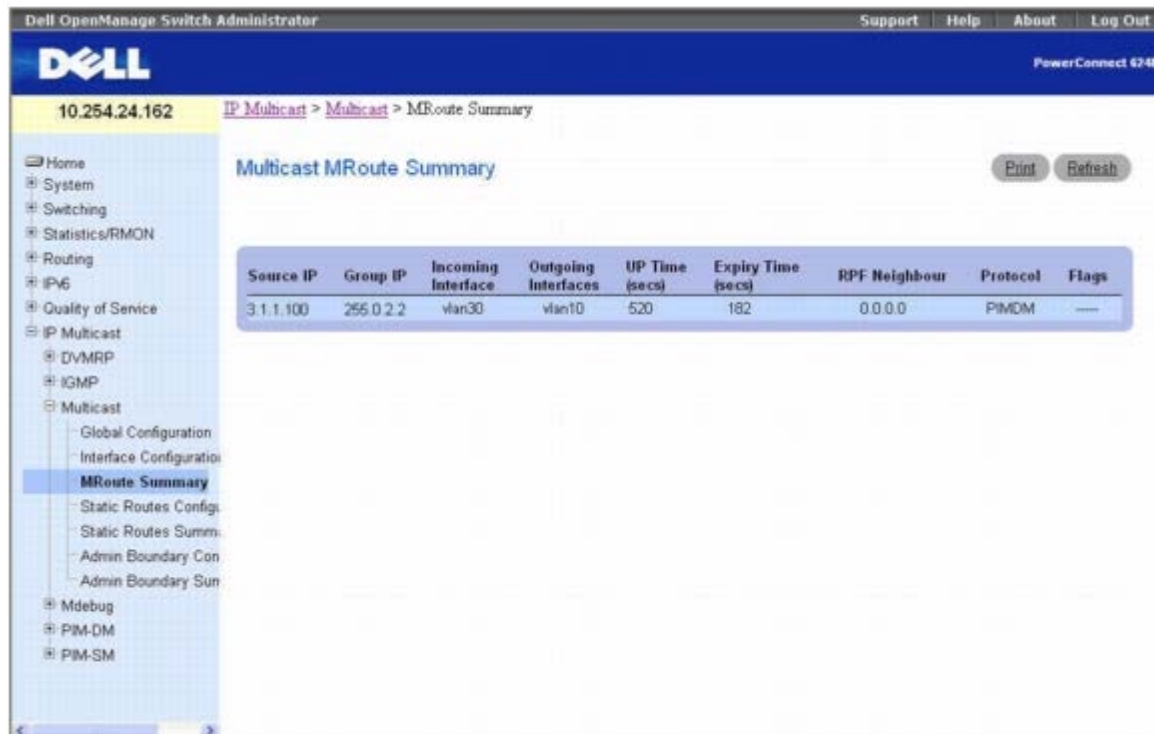
- 多点传送命令

## 多点传送 Mroute 摘要

**Multicast Mroute Summary** (多点传送 **Mroute** 摘要) 页面用于显示 Mroute 数据。

要显示此页面,请在树视图中单击 **IP Multicast** (IP 多点传送) ® **Multicast** (多点传送) ® **Mroute Summary** (**Mroute** 摘要)。

图 13-18. 多点传送 Mroute 摘要



**Multicast Mroute Summary** (多点传送 **Mroute** 摘要) 页面会显示以下字段:

**Source IP** (源 IP) — 与组 IP 结合的多点传送信息包源 IP 地址,用于识别 Mroute 表输入项。

**Group IP** (组 IP) — 目的地组 IP 地址。

**Incoming Interface** (接入接口) — 此源/组的多点传送信息包所到达的接入接口。

**Outgoing Interface** (发送接口) — 转发此源/组的多点传送信息包的发送接口列表。

**Up Time (secs)** (运行时间 [秒]) — 自创建此输入项以来经过的时间,以秒为单位。

**Expiry Time (secs)** (过期时间 [秒]) — 此输入项过期并从表中删除前的时间,以秒为单位。

**RPF Neighbor** (RPF 邻居) — 逆向路径转发邻居的 IP 地址。

**Protocol** (协议) — 创建此输入项的多点传送路由协议。可能协议如下:

- PIM-DM
- PIM-SM
- DVMRP

**Flags** (标记) — 如果运行的多点传送路由协议是 PIM-SM,则此字段中显示的值有效。可能值是 RPT 或 SPT。如果是其它协议,则显示“----”。

## 使用 CLI 命令显示 MRoute 摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

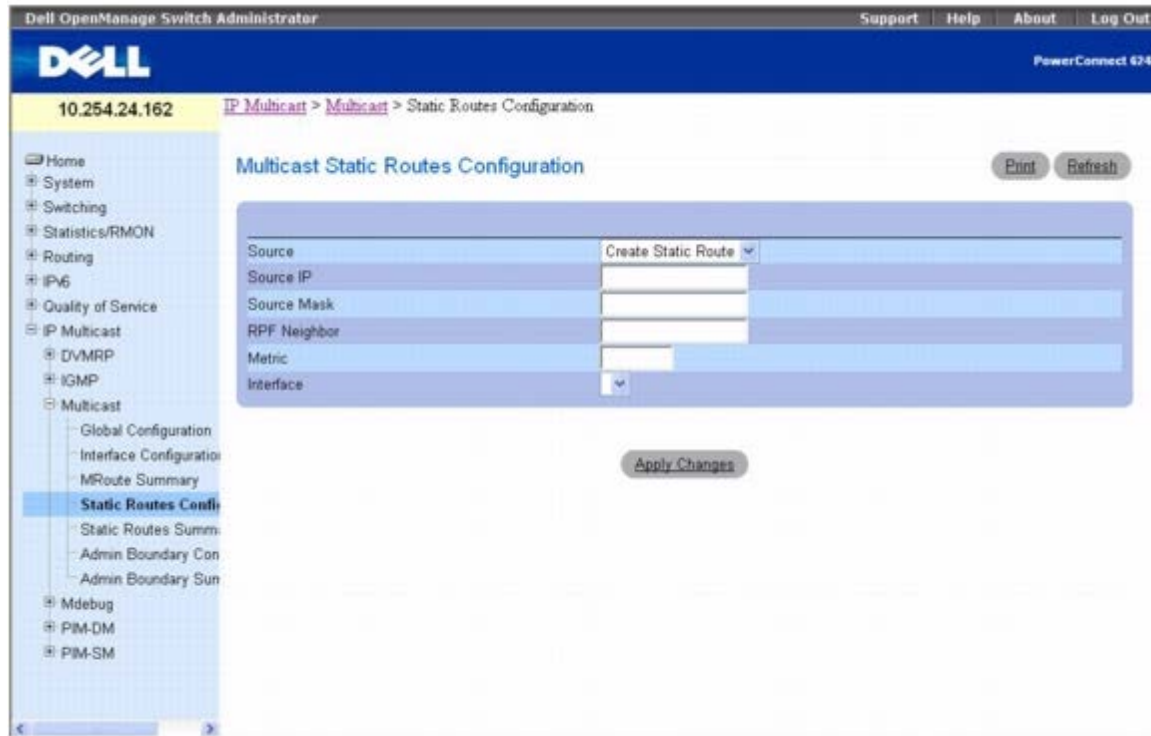
- 多点传送命令

## 多点传送静态路由配置

**Multicast Static Routes Configuration** (多点传送静态路由配置) 页面用于在 Mroute 表中配置新的静态输入项或修改现有输入项。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **Multicast** (多点传送) ® **Static Routes Configuration** (静态路由配置)。

图 13-19. 多点传送静态路由配置



**Multicast Static Routes Configuration** (多点传送静态路由配置) 页面包含以下字段:

**Source** (源) — 选择 **Create Static Route** (创建静态路由), 可在 Mroute 表中配置新静态路由, 也可从下拉式菜单中选择一个现有输入项。

**Source IP** (源 IP) — 输入可识别所创建输入项的多点传送信息包源的 IP 地址。

**Source Mask** (源掩码) — 输入要应用到源 IP 地址的子网掩码。

**RPF Neighbor** (RPF 邻居) — 输入通往源的路径上邻居路由器的 IP 地址。

**Metric** (跃点数) — 输入通往多点传送源的路径的链路状态成本。范围是 0 至 255, 默认值是 1。您可以选择配置的静态路由, 然后编辑此字段来更改该路由的跃点数。

**Interface** (接口) — 从下拉式菜单中选择接口号。这是连接到给定源 IP 地址的邻居路由器的接口。

## 配置静态路由

□□□ 打开 **Static Routes** (静态路由) 页面。

□□□ 在 **Source** (源) 字段中选择 **Create Static Route** (创建静态路由) 以配置新的静态输入项, 或选择一个现有输入项。

□□□ 根据需要修改其余字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存新的或修改后的静态路由并更新设备。

## 使用 CLI 命令配置静态路由

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

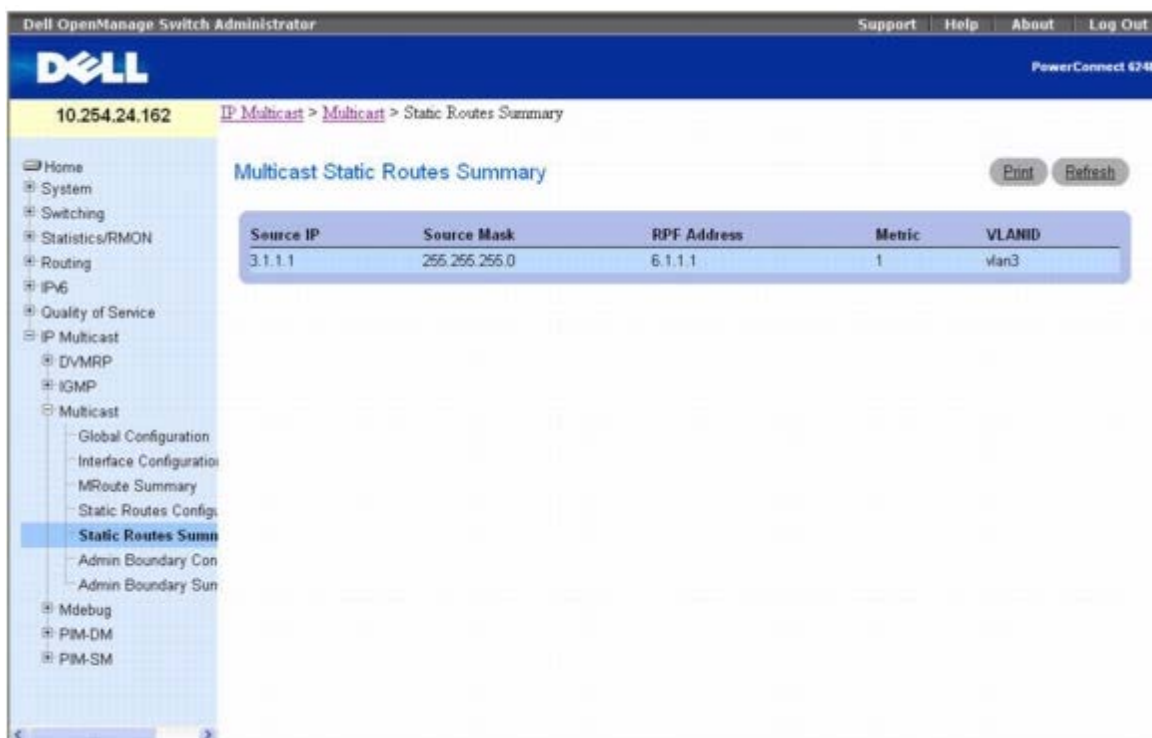
- 多点传送命令

## 多点传送静态路由摘要

**Multicast Static Routes Summary** (多点传送静态路由摘要) 页面用于显示静态路由及其配置。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **Multicast** (多点传送) ® **Static Routes Summary** (静态路由摘要)。

图 13-20. 多点传送静态路由摘要



**Multicast Static Routes Summary** (多点传送静态路由摘要) 页面会显示以下字段:

**Source IP** (源 IP) — 识别此路由的多点传送信息包源的 IP 地址。

**Source Mask** (源掩码) — 要应用到源 IP 地址的子网掩码。

**RPF Address** (RPF 地址) — RPF 邻居的 IP 地址。

**Metric** (跃点数) — 通往多点传送源的路径的链路状态成本。范围是 0 至 255。

**VLANID** — 接入 VLAN 的号码, 该 VLAN 的 IP 地址可用作给定源 IP 地址的 RPF。

## 使用 CLI 命令显示静态路由摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

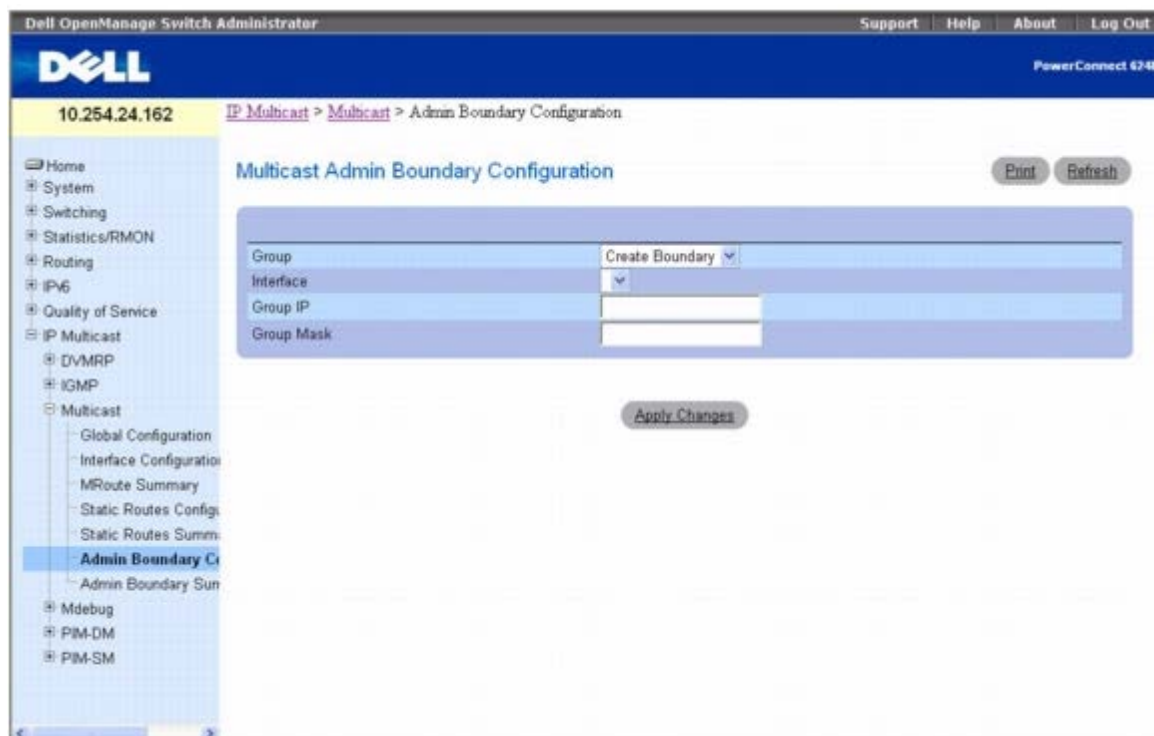
- 多点传送命令

## 多点传送管理边界配置

管理范围边界的定义是: 一种在给定路由接口上用于阻止给定范围的多点传送地址的多点传送通信进入和外出的方法。**Multicast Admin Boundary Configuration** (多点传送管理边界配置) 页面用于配置新的或现有的管理范围边界。要查看该页面, 您必须配置有效的路由接口和多点传送。

要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送) @ Multicast (多点传送) @ Admin Boundary Configuration (管理边界配置)**。

图 13-21. 多点传送管理边界配置



**Multicast Admin Boundary Configuration** (多点传送管理边界配置) 页面包含以下字段:

**Group** (组) — 可从下拉式菜单中选择 **Create Boundary** (创建边界) 来创建新的管理范围边界, 也可选择一个现有边界规格来显示或更新其配置。

**Interface** (接口) — 选择要配置管理范围边界的路由器接口。

**Group IP** (组 IP) — 输入多点传送组地址作为要排除的地址范围的起点。该地址必须在 239.0.0.0 到 239.255.255.255 的范围内。

**Group Mask** (组掩码) — 输入要应用到多点传送组地址的掩码。掩码和组 IP 结合起来就可确定所选接口的管理范围地址的范围。

## 配置管理边界

□□□ 打开 **Multicast Admin Boundary Configuration** (多点传送管理边界配置) 页面。

□□□ 在 **Group IP** (组 IP) 字段中选择 **Create Boundary** (创建边界) 以配置新的管理范围边界, 或选择一个现有输入项。

□□□ 根据需要修改其余字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存新的或修改后的管理范围边界并更新设备。

## 使用 CLI 命令配置管理边界

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

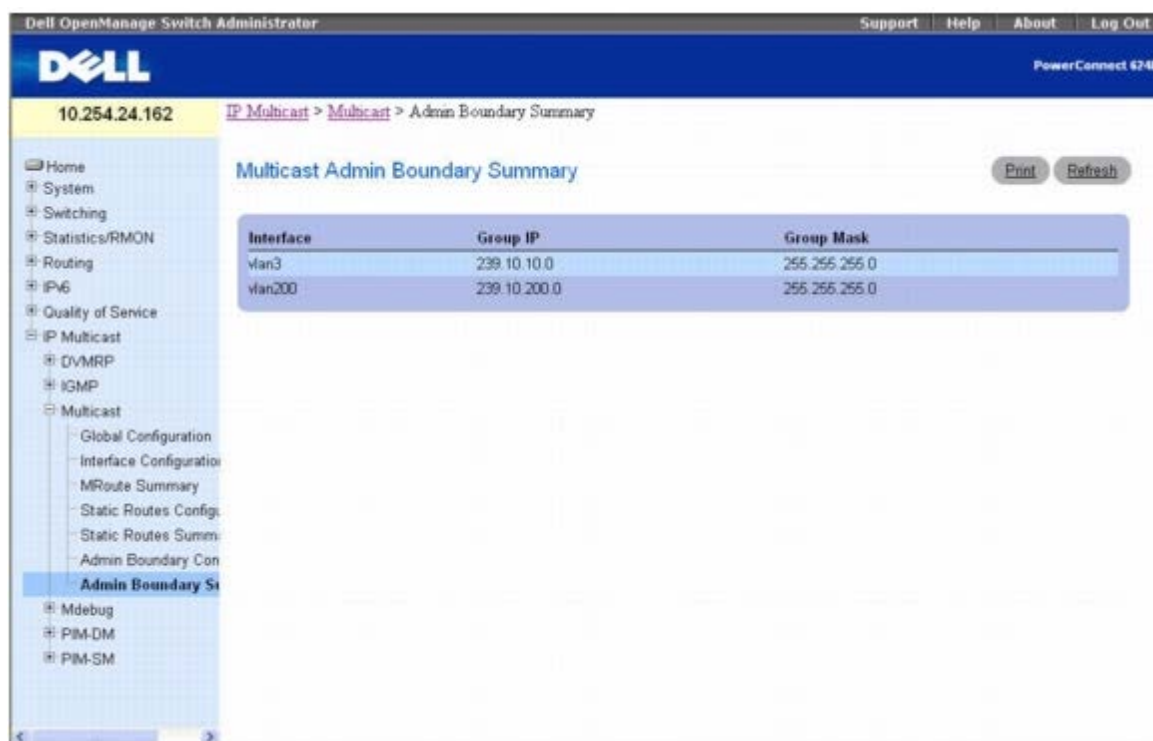
- 多点传送命令

## 多点传送管理边界摘要

**Multicast Admin Boundary Summary** (多点传送管理边界摘要) 页面用于显示现有的管理范围边界。

要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送)** ® **Multicast (多点传送)** ® **Admin Boundary Summary (管理边界摘要)**。

图 13-22. 多点传送管理边界摘要



**Multicast Admin Boundary Summary** (多点传送管理边界摘要) 页面会显示以下字段:

**Interface** (接口) — 应用管理范围地址范围的路由器接口。

**Group IP** (组 IP) — 多点传送组地址作为要排除的地址范围的起点。

**Group Mask** (组掩码) — 应用到多点传送组地址的掩码。掩码和组 IP 结合起来就可确定所选接口的管理范围地址的范围。

## 使用 CLI 命令显示多点传送管理边界摘要



有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- 多点传送命令

---

## PIM-DM

PIM-DM 协议是简单的、协议无关的多点传送路由协议。它使用现有的单点传送路径选择表和加入/删减/嫁接机制来构建树。PIM-DM 创建基于源的最短路径分布树, 该树使用 RPF。它不能用于构建共享分布树, 这一点和 PIM-SM 不一样。PIM-DM 假定当发送方开始发送数据时, 所有下游路由器和主机都希望接收多点传送数据包。PIM-DM 一开始会将多点传送通信多路发送至整个网络。而没有任何下游邻居的路由器会将不需要的通信删减发回。除了删减信息外, PIM-DM 还会利用嫁接和认定信息。每当新的主机希望加入组时, 就会使用嫁接信息。认定信息用于停止同一多路访问网络上的重复流。

PIM-DM 有两个版本。第 2 版不使用 IGMP 信息; 而是使用压缩在 IP 封装中的信息, 协议号为 103。在第 2 版中, 引入了问候信息以取代查询信息。

PIM-DM 适用于:

- 密集分布的接收器
- 少数发送器对多数接收器 (由于频繁多路发送)
- 大量多点传送通信
- 稳定通信流

**PIM-DM** 菜单页面包含一些网页的链接, 这些网页可用于定义和显示 **PIM-DM** 参数和数据。要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送) ® PIM-DM**。

在此菜单页面中可以访问以下网页:

- [PIM-DM 全局配置](#)
- [PIM-DM 接口配置](#)
- [PIM-DM 接口摘要](#)

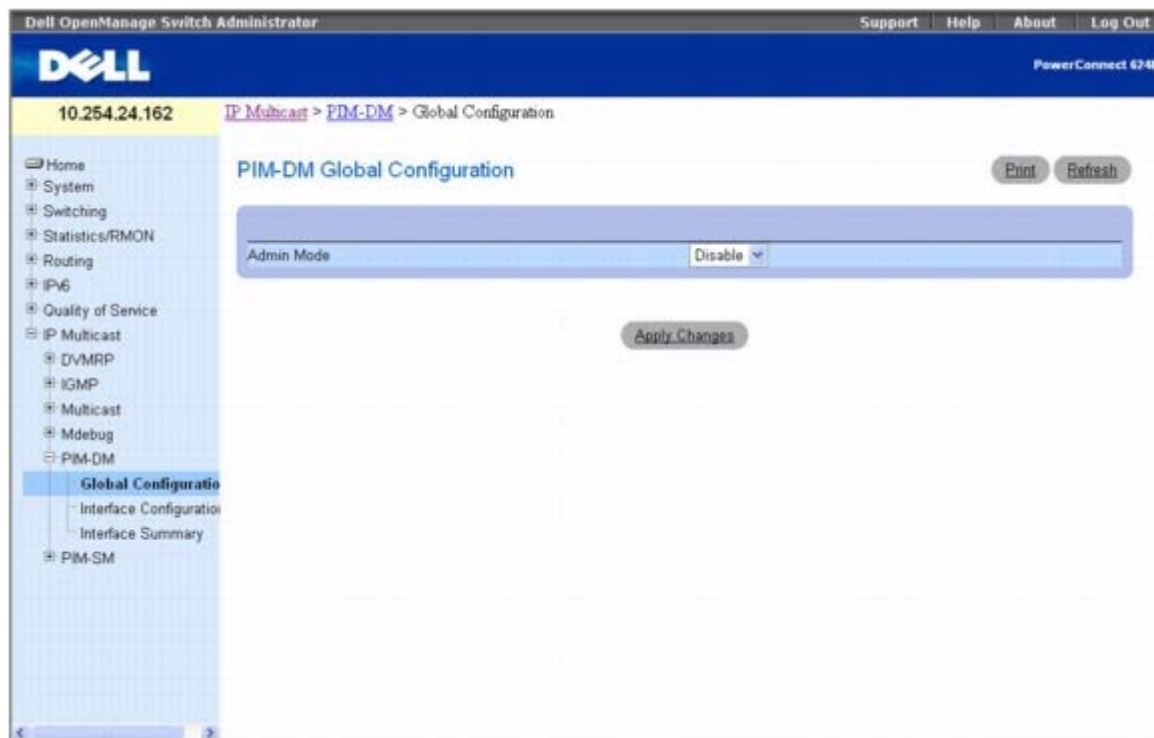
## PIM-DM 全局配置

**PIM-DM Global Configuration (PIM-DM 全局配置)** 页面用于配置 PIM-DM 在此系统上的管理状态。

要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送) ® PIM-DM ® Global Configuration (全局配置)**。

图 13-23. PIM-DM 全局配置





**PIM-DM Global Configuration (PIM-DM 全局配置)** 页面包含以下字段:

**Admin Mode** (管理模式) — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用), 设置 PIM-DM 在系统上的管理状态。默认值为 **Disable** (禁用)。

## 配置 PIM-DM

□□□ 打开 **PIM-DM Global Configuration (PIM-DM 全局配置)** 页面。

□□□ 将 **Admin Mode** (管理模式) 设置为 **Enable** (启用) 或 **Disable** (禁用), 以打开或关闭 PIM-DM。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存 PIM-DM 配置并更新设备。

## 使用 CLI 命令配置 PIM-DM

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

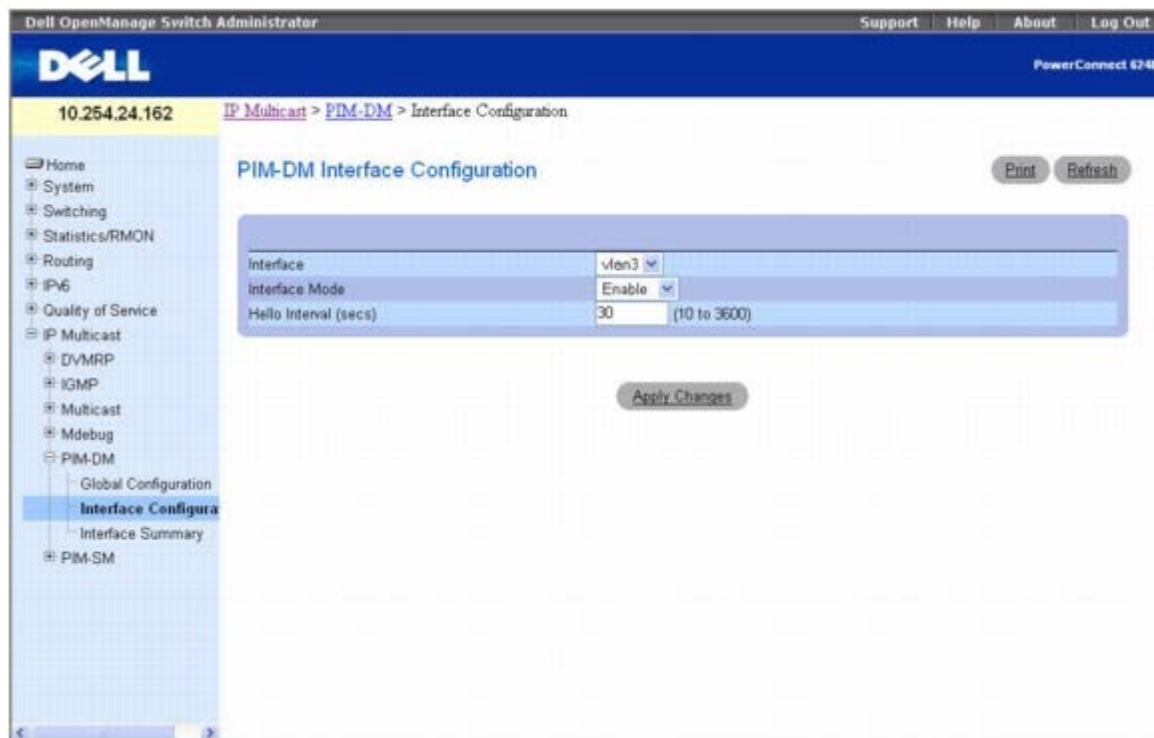
- PIM-DM 命令

## PIM-DM 接口配置

**PIM-DM Interface Configuration (PIM-DM 接口配置)** 页面用于借助 PIM-DM 配置特定接口。必须在 **PIM-DM Global Configuration (PIM-DM 全局配置)** 页面上启用 PIM-DM, 才能显示此接口配置页面。

要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送) ® PIM-DM ® Interface Configuration (接口配置)**。

图 13-24. PIM-DM 接口配置



**PIM-DM Interface Configuration (PIM-DM 接口配置)** 页面包含以下字段:

**Interface (接口)** — 选择要为其显示或配置数据的接口。您必须先至少配置一个路由器接口，才能配置或显示 PIM-DM 接口的数据，否则会显示错误信息。

**Interface Mode (接口模式)** — 从下拉式菜单中选择 **Enable (启用)** 或 **Disable (禁用)**，设置所选接口的 PIM-DM 管理状态。默认值为 **Disable (禁用)**。

**Hello Interval (secs) (问候间隔 [秒])** — 输入从选定的接口每次发送 PIM 问候信息所间隔的秒数。默认值是 30。有效值从 10 到 3600。

## 为接口配置 PIM-DM

□□□ 打开 **PIM-DM Interface Configuration (PIM-DM 接口配置)** 页面。

□□□ 从 **Interface (接口)** 字段选择要配置的接口。

□□□ 根据需要修改其余字段。

□□□ 单击 **Apply Changes (应用更改)**。

系统将保存接口配置并更新设备。

## 使用 CLI 命令为接口配置 PIM-DM

有关执行此功能的 CLI 命令的信息，请参阅《CLI 参考指南》的以下章节：

- PIM-DM 命令

## PIM-DM 接口摘要

**PIM-DM Interface Summary (PIM-DM 接口摘要)** 页面用于显示 PIM-DM 接口及其设置。必须在此路由器上至少将一个接口设置为

PIM-DM, 才能显示该页面。

要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送) @ PIM-DM @ Interface Summary (接口摘要)**。

图 13-25. PIM-DM 接口摘要



**PIM-DM Interface Summary (PIM-DM 接口摘要)** 页面包含以下字段:

**Interface (接口)** — 选择要为其显示数据的接口。必须先至少配置一个路由器接口, 才能显示 PIM-DM 接口的数据, 否则会显示错误信息。

接口参数

**Interface Mode (接口模式)** — 所选接口的 PIM-DM 管理状态。默认值为 **Disable (禁用)**。

**Protocol State (协议状态)** — 所选接口上的 PIM-DM 协议的操作状态。

**Hello Interval (secs) (问候间隔 [秒])** — 在所选接口上发送 PIM 问候信息的频率。

**IP Address (IP 地址)** — 所选接口的 IP 地址。

接口统计数据

**Neighbor Count (邻居计数)** — 所选接口上的 PIM 邻居数。

**Designated Router (指定路由器)** — 所选 PIM 接口上的指定路由器。对于点对点接口, 此字段是 0.0.0.0。

接口邻居

**Neighbor IP (邻居 IP)** — PIM 邻居的 IP 地址, 此输入项包含该邻居的信息。

**Up Time (hh:mm:ss) (运行时间 [小时:分钟:秒钟])** — 自从此 PIM 邻居 (最后一次) 成为本地路由器的邻居以来所经过的时间。

**Expiry Time (hh:mm:ss) (过期时间 [小时:分钟:秒钟])** — 此 PIM 邻居过期前的最短剩余时间。

## 使用 CLI 命令显示 PIM-DM 接口摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- PIM-DM 命令

## PIM-SM

PIM-SM 用于有效地将多点传送通信路由到多点传送组，这些组可以跨越广域网，并且组内带宽可以是一个约束条件。PIM-SM 默认使用共享树并实施基于源的树，以此提高效率。此数据阈值速率用于在树之间切换。PIM-SM 假定没有主机需要多点传送通信，除非它们明确提出要求。它以定义的集合点 (RP) 为中心创建共享分布树，从该点将源通信中继到接收器。发送器先将多点传送数据发送到 RP，后者再将数据沿共享树发送到接收器。以 RP 为中心的共享树不一定提供最短/最佳路径。在这种情况下，PIM-SM 提供切换至更高效的源特定树的方法。

**PIM-SM** 菜单页面包含一些网页的链接，这些网页可用于定义和显示 PIM-SM 参数和数据。要显示此页面，请在树视图中单击 **IP Multicast (IP 多点传送) @ PIM-SM**。

在此菜单页面中可以访问以下网页：

- [PIM-SM 全局配置](#)
- [PIM-SM 全局状态](#)
- [PIM-SM 接口配置](#)
- [PIM-SM 接口摘要](#)
- [组件摘要](#)
- [RP 设置摘要](#)
- [候选 RP 摘要](#)
- [静态 RP 配置](#)

## PIM-SM 全局配置

**PIM-SM Global Configuration (PIM-SM 全局配置)** 页面用于配置此系统的全局 PIM-SM 设置。

要显示此页面，请在树视图中单击 **IP Multicast (IP 多点传送) @ PIM-SM @ Global Configuration (全局配置)**。

图 13-26. PIM-SM 全局配置



**PIM-SM Global Configuration (PIM-SM 全局配置)** 页面包含以下字段:

**Admin Mode** (管理模式) — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用), 设置 PIM-SM 在系统上的管理状态。在启用 PIM-SM 前, 您必须启用 IGMP。默认值为 **Disable** (禁用)。

**Join/Prune Interval (secs)** (加入/删减间隔 [秒]) — 输入发送 PIM-SM 加入/删减信息的间隔。有效值为 10 至 3600 秒。默认值为 60。

**Data Threshold Rate (Kbps)** (数据阈值速率 [Kbps]) — 输入以千比特/秒为单位的最小源数据速率, 高于此速率时最后跃距路由器会切换至源特定的最短路径树。有效值从 0 到 2000 千比特/秒。默认值是 50。

**Register Threshold Rate (Kbps)** (寄存器阈值速率 [Kbps]) — 输入以千比特/秒为单位的最小源数据速率, 高于此速率时集合点路由器会切换至源特定的最短路径树。有效值从 0 到 2000 千比特/秒。默认值是 50。

## 配置 PIM-SM

- 打开 **PIM-SM Global Configuration (PIM-SM 全局配置)** 页面。
- 将 **Admin Mode** (管理模式) 设置为 **Enable** (启用) 或 **Disable** (禁用), 以打开或关闭 PIM-SM。
- 根据需要修改其余字段。
- 单击 **Apply Changes** (应用更改)。

系统将保存接口配置并更新设备。

## 使用 CLI 命令配置 PIM-SM

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

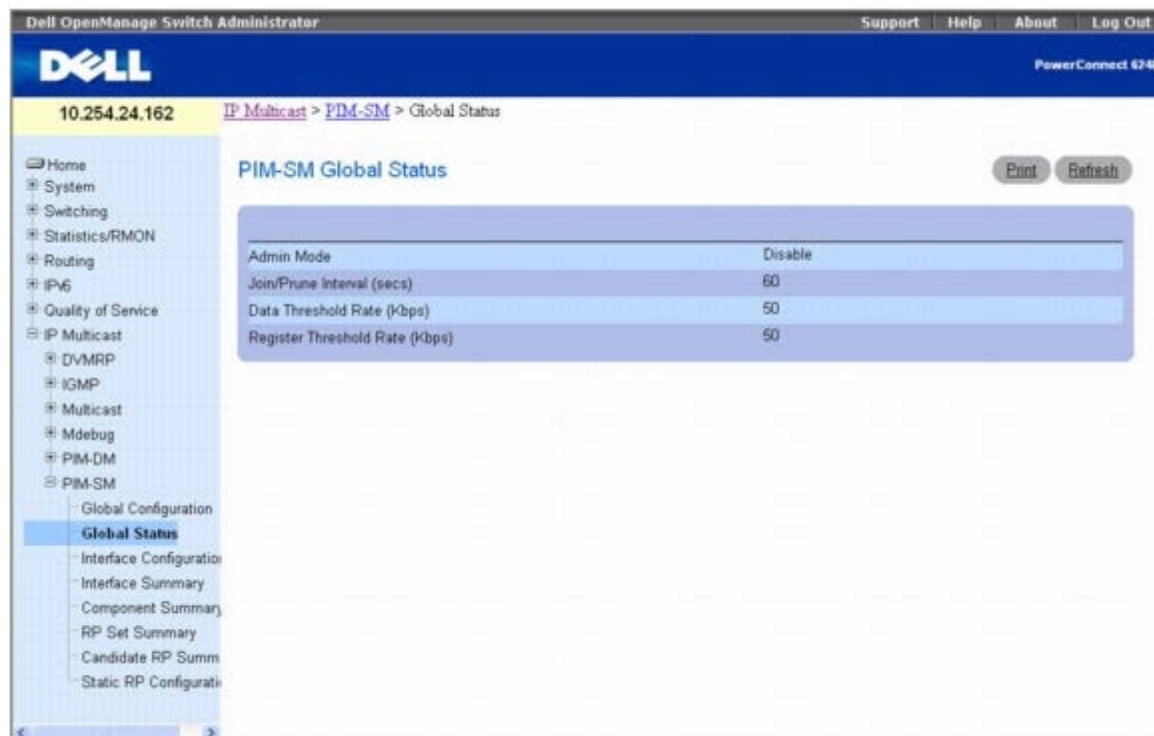
- PIM-SM 命令

## PIM-SM 全局状态

**PIM-SM Global Status** (PIM-SM 全局状态) 页面用于显示在 **PIM-SM Global Configuration** (PIM-SM 全局配置) 页面上选择的全局设置。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **PIM-SM** ® **Global Status** (全局状态)。

图 13-27. PIM-SM 全局状态



**PIM-SM Global Status** (PIM-SM 全局状态) 页面包含以下字段:

**Admin Mode** (管理模式) — PIM-SM 在路由器中的管理状态: Enable (启用) 或 Disable (禁用)。

**Join/Prune Interval (secs)** (加入/删减间隔 [秒]) — 发送 PIM-SM 加入/删减信息的间隔。

**Data Threshold Rate (Kbps)** (数据阈值速率 [Kbps]) — 以千比特/秒为单位的最小源数据速率, 高于此速率时最后跃距路由器会切换至源特定的最短路径树。

**Register Threshold Rate (Kbps)** (寄存器阈值速率 [Kbps]) — 以千比特/秒为单位的最小源数据速率, 高于此速率时集合点路由器会切换至源特定的最短路径树。

## 使用 CLI 命令配置 PIM-SM 全局状态

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- PIM-SM 命令

## PIPIM-SM 接口配置

**PIM-SM Interface Configuration** (PIM-SM 接口配置) 页面用于为接口配置 PIM-SM。必须在 **PIM-SM Global Configuration** (PIM-SM 全局配置) 页面上启用 PIM-SM, 才能显示此接口配置页面。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **PIM-SM** ® **Interface Configuration** (接口配置)。

图 13-28. PIM-SM 接口配置





**PIM-SM Interface Configuration (PIM-SM 接口配置)** 页面包含以下字段:

**Interface** (接口) — 选择要为其显示或配置数据的接口。要显示或配置数据, 必须至少存在一个路由接口。

**Mode** (模式) — 从下拉式菜单中选择 **Enable** (启用) 或 **Disable** (禁用), 以设置 PIM-SM 在此接口上的管理状态。默认值为 **Disable** (禁用)。

**Hello Interval (secs)** (问候间隔 [秒]) — 输入在此接口上发送 PIM 问候信息的间隔时间, 以秒为单位。有效值为 10 至 3600 秒。默认值为 30。

**CBSR Preference** (CBSR 首选项) — 输入本地接口作为候选自举路由器的首选项值。值 -1 用于表明本地接口不是候选 BSR 接口。有效值从 -1 到 255。默认值是 0。

**CBSR Hash Mask Length** (CBSR 散列掩码长度) — 输入此接口被选为自举路由器时要在自举信息中公布的 CBSR 散列掩码长度。此散列掩码长度在散列算法中用于为特定组选择 RP。有效值从 0 到 32。默认值是 30。

**CRP Preference** (CRP 首选项) — 输入本地接口作为候选自举路由器的首选项值。值 -1 用于表明本地接口不是候选 BSR 接口。有效值从 -1 到 255。默认值是 0。

## 为接口配置 PIM-SM

□□□ 打开 **PIM-SM Interface Configuration (PIM-SM 接口配置)** 页面。

□□□ 从 **Interface** (接口) 字段选择要配置的接口。

□□□ 从 **Mode** (模式) 字段中选择 **Enable** (启用)。

□□□ 根据需要修改其余字段。

□□□ 单击 **Apply Changes** (应用更改)。

系统将保存接口配置并更新设备。

## 使用 CLI 命令为接口配置 PIM-SM

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:



- PIM-SM 命令

## PIM-SM 接口摘要

**PIM-SM Interface Summary (PIM-SM 接口摘要)** 页面用于显示 PIM-SM 接口及其设置。必须在此路由器上至少将一个接口设置为 PIM-SM, 才能显示此页面。

要显示此页面, 请在树视图中单击 **IP Multicast (IP 多点传送) @ PIM-SM @ Interface Summary (接口摘要)**。

图 13-29. PIM-SM 接口摘要



**PIM-SM Interface Summary (PIM-SM 接口摘要)** 页面包含以下字段:

**Interface (接口)** — 选择要为其显示数据的接口。

**Mode (模式)** — PIM-SM 在路由器中的管理状态: Enable (启用) 或 Disable (禁用)。

**Protocol State (协议状态)** — PIM-SM 协议在所选接口上的操作状态, 其值为 Operational (可操作) 或 Non-operational (不可操作)。

**IP Address (IP 地址)** — 所选 PIM 接口的 IP 地址。

**Net Mask (网络掩码)** — 所选 PIM 接口的 IP 地址网络掩码。

**Designated Router (指定路由器)** — 所选 PIM 接口上的指定路由器。对于点对点接口, 此对象的值为 0.0.0.0。

**Hello Interval (secs) (问候间隔 [秒])** — 在所选接口上发送 PIM 问候信息的频率。

**CBSR Preference (CBSR 首选项)** — 本地接口作为候选自举路由器的首选项值。值 -1 用于表明本地接口不是候选 BSR 接口。

**CBSR Hash Mask Length (CBSR 散列掩码长度)** — 此接口被选为自举路由器时要在自举信息中公布的 CBSR 散列掩码长度。此散列掩码长度在散列算法中用于为特定组选择 RP。

**CRP Preference (CRP 首选项)** — 本地接口作为候选自举路由器的首选项值。值 -1 用于表明本地接口不是候选 BSR 接口。

**Neighbor Count (邻居计数)** — 所选接口上的 PIM 邻居数。

**IP Address (IP 地址)** — 此输入项的 PIM 邻居的 IP 地址。

**Up Time (hh:mm:ss)** (运行时间 [小时:分钟:秒钟]) — 自从此 PIM 邻居 (最后一次) 成为本地路由器的邻居以来所经过的时间。

**Expiry Time (hh:mm:ss)** (过期时间 [小时:分钟:秒钟]) — 此 PIM 邻居过期前的最短剩余时间。

## 显示 PIM-SM 接口摘要

□□□ 打开 **PIM-SM Interface Summary** (PIM-SM 接口摘要) 页面。

□□□ 从 **Interface** (接口) 下拉式菜单中选择要显示的接口。

系统将显示此接口的 PIM-SM 配置数据。

## 使用 CLI 命令显示 PIM-SM 接口摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- PIM-SM 命令

## 组件摘要

**Component Summary** (组件摘要) 页面用于显示 PIM-SM 组件数据。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **PIM-SM** ® **Component Summary** (组件摘要)。

图 13-30. 组件摘要

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb navigation is IP Multicast > PIM-SM > Component Summary. The main content area is titled "PIM-SM Component Summary" and contains a table with the following data:

Component Index	Component BSR Address	Component BSR Expiry Time (hh:mm:ss)	Component CRP Hold Time (hh:mm:ss)
1	3.1.1.2	00:00:20	00:00:20

**Component Summary** (组件摘要) 页面会显示以下字段:

**Component Index** (组件索引) — 识别组件索引的唯一号码。

**Component BSR Address** (组件 BSR 地址) — 本地 PIM 区域的自举路由器 (BSR) 的 IP 地址。

**Component BSR Expiry Time (hh:mm:ss)** (组件 BSR 过期时间 [小时:分钟:秒钟]) — 声明本地域中自举路由器之前的最短剩余时

间。

**Component CRP Hold Time (hh:mm:ss)** (组件 CRP 保持时间 [小时:分钟:秒钟]) — 当组件在本地域中是候选集合点时的保持时间。

## 使用 CLI 命令显示 PIM-SM 组件摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- PIM-SM 命令

## RP 设置摘要

**PIM-SM RP Set Summary** (PIM-SM RP 设置摘要) 页面用于显示 PIM-SM 路由器的静态 RP 信息。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **PIM-SM** ® **RP Set Summary** (RP 设置摘要)。

图 13-31. PIM-SM RP 设置摘要

The screenshot shows the Dell OpenManage Switch Administrator interface. The breadcrumb navigation is IP Multicast > PIM-SM > RP Set Summary. The main content area is titled 'PIM-SM RP Set Summary' and contains a table with the following data:

Group Address	Group Mask	Address	Hold Time(hh:mm:ss)	Expiry Time(hh:mm:ss)	Component
224.0.0.0	240.0.0.0	3.1.1.2	00:01:40	00:02:30	1

**PIM-SM RP Set Summary** (PIM-SM RP 设置摘要) 页面在表中显示以下字段:

**Group Address** (组地址) — 显示 IP 多点传送组地址。

**Group Mask** (组掩码) — 显示多点传送组地址掩码。

**Address** (地址) — 显示候选 RP 的 IP 地址。

**Hold Time (hh:mm:ss)** (保持时间 [小时:分钟:秒钟]) — 候选 RP 的保持时间。如果本地路由器不是 BSR, 则此值为 0。

**Expiry Time (hh:mm:ss)** (过期时间 [小时:分钟:秒钟]) — 声明候选 RP 停止前的最短剩余时间。

**Component** (组件) — 唯一识别组件的号码。连接到单独域中的每个协议实例都有一个不同的索引值。

## 使用 CLI 命令显示 RP 设置摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

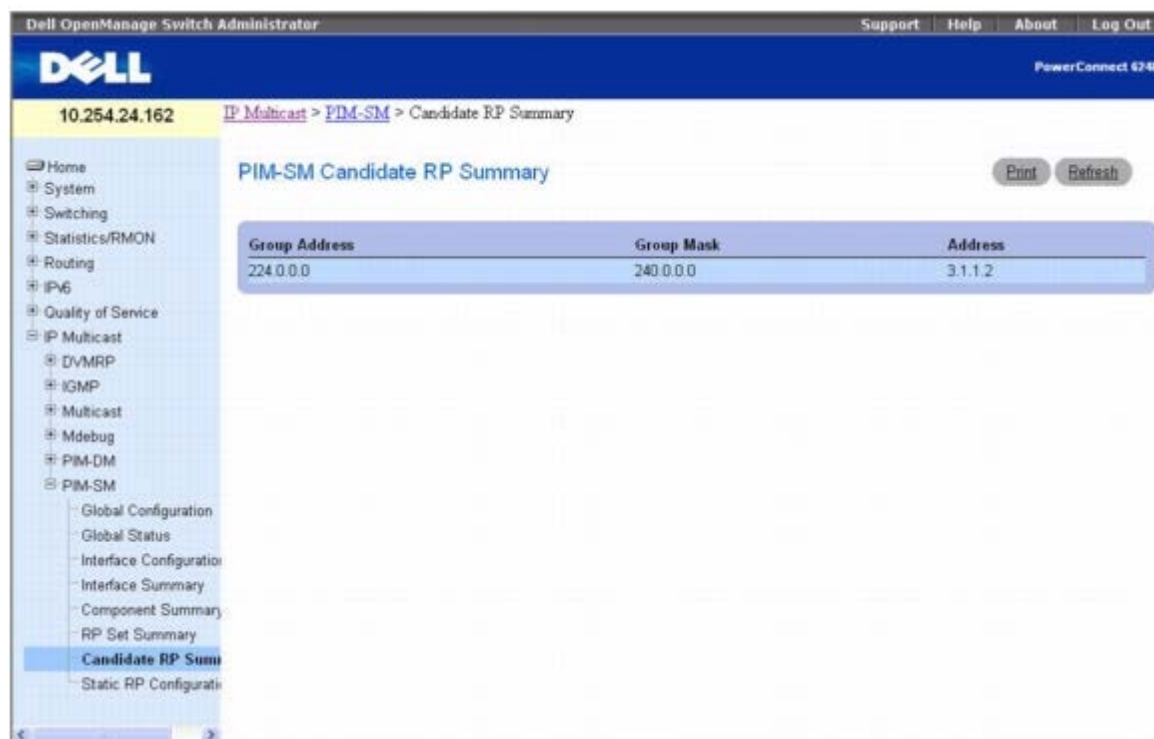
- PIM-SM 命令

## 候选 RP 摘要

**PIM-SM Candidate RP Summary** (PIM-SM 候选 RP 摘要) 页面用于为每个 IP 多点传送组显示候选集合点 (RP) 的 PIM 信息。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **PIM-SM** ® **Candidate RP Summary** (候选 RP 摘要)。

图 13-32. PIM-SM 候选 RP 摘要



**PIM-SM Candidate RP Summary** (PIM-SM 候选 RP 摘要) 页面在表中显示以下字段:

**Group Address** (组地址) — 在候选 RP 公布中发送的组地址。

**Group Mask** (组掩码) — 在候选 RP 公布中发送的组地址掩码, 用于完整地识别路由器在被选为集合点时所支持的组范围。

**Address** (地址) — 显示被公布为候选 RP 的接口的单点传送地址。

## 使用 CLI 命令显示 PIM-SM 候选 RP 摘要

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

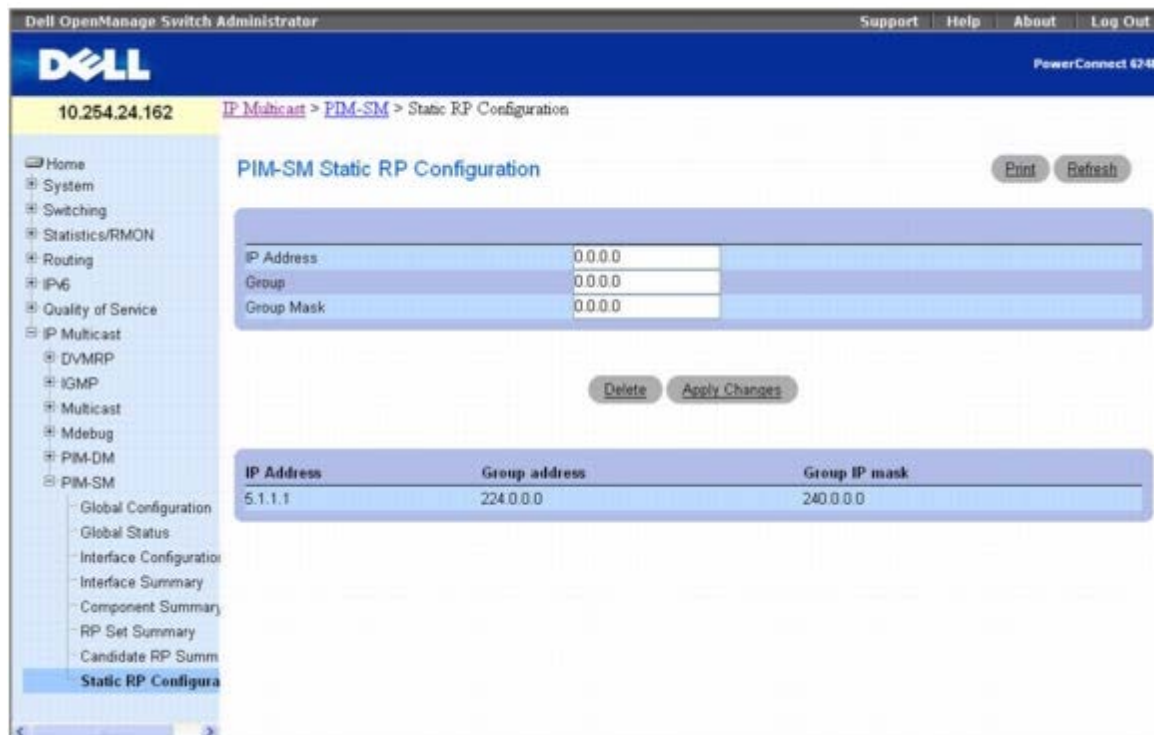
- PIM-SM 命令

## 静态 RP 配置

**Static RP Configuration** (静态 RP 配置) 页面用于为 PIM-SM 路由器创建指定的静态 RP IP 地址。

要显示此页面, 请在树视图中单击 **IP Multicast** (IP 多点传送) ® **PIM-SM** ® **Static RP Configuration** (静态 RP 配置)。

图 13-33. 静态 RP 配置



**Static RP Configuration** (静态 RP 配置) 页面包含以下字段:

**IP Address** (IP 地址) — 要创建的 RP 的 IP 地址。

**Group** (组) — 要创建的 RP 的组地址。

**Group Mask** (组掩码) — 要创建的 RP 的组 IP 掩码。

现有配置显示在页面底部的表中。

## 配置静态 RP

□□□ 打开 **Static RP Configuration** (静态 RP 配置) 页面。

□□□ 在静态 RP 配置中输入 **IP Address** (IP 地址)、**Group** (组) 的 IP 地址和 **Group Mask** (组掩码)。

□□□ 单击 **Apply Changes** (应用更改)。

系统将创建 PIM-SM 路由器的指定静态 RP IP 地址并更新设备。

## 使用 CLI 命令配置静态 RP

有关执行此功能的 CLI 命令的信息, 请参阅《CLI 参考指南》的以下章节:

- PIM-SM 命令

[返回目录页面](#)

[返回目录页面](#)

## 获得帮助

### Dell™ PowerConnect™ 6200 系列用户指南

- [寻求帮助](#)
- [Dell 企业培训和认证](#)
- [订购时遇到的问题](#)
- [产品信息](#)
- [退回部件要求保修或退款](#)
- [致电之前](#)
- [与 Dell 联络](#)

---


## 寻求帮助


当您的计算机出现问题时，可以完成以下步骤进行诊断并排除故障：

□□□ 填写 [诊断程序检验表](#)。

□□□ 利用 Dell 支持（位于 [support.dell.com](http://support.dell.com)）上的多种 Dell 在线服务获得有关安装和故障排除过程的帮助。请参阅 [联机服务](#) 以在线获得 Dell 支持服务详细列表。


□□□ 如果上述步骤无法解决问题，请参阅 [与 Dell 联络](#)。

 **注：** 致电 Dell 支持时，请使用计算机旁边的电话，以使支持人员能够通过所有必要的步骤来帮助您。

 **注：** 并非在所有国家和地区均可使用 Dell 的快速服务代码系统。

Dell 自动电话系统提示时，输入您的快速服务代码，从而将电话直接转至相应的技术支持人员。如果您没有快速服务代码，请打开 **Dell Accessories**（Dell 附件）文件夹并双击 **Express Service Code**（快速服务代码）图标，然后按照提示进行操作。

有关使用 Dell 支持的说明，请参阅 [支持服务](#)。

 **注：** 以下部分服务并非在美国本土以外的所有地区都能使用。有关其可用性的信息，请致电当地的 Dell 代表。

## 联机服务

您可以通过以下网站了解 Dell 的产品和服务：

[www.dell.com](http://www.dell.com)

[www.dell.com/ap/](http://www.dell.com/ap/)（仅限于亚太国家和地区）

[www.dell.com/jp](http://www.dell.com/jp)（仅限于日本）

[www.euro.dell.com](http://www.euro.dell.com)（仅限于欧洲）

[www.dell.com/la](http://www.dell.com/la)（拉丁美洲和加勒比国家和地区）

[www.dell.ca](http://www.dell.ca)（仅限于加拿大）

您可以通过以下网站和电子邮件地址访问 Dell 支持：

- Dell 支持网站



**support.dell.com**

**support.jp.dell.com** (仅限于日本)

**support.euro.dell.com** (仅限于欧洲)

- Dell 支持电子邮件地址

mobile\_support@us.dell.com

support@us.dell.com

la-techsupport@dell.com (仅限于拉丁美洲和加勒比国家和地区)

apsupport@dell.com (仅限于亚太国家和地区)

- Dell 市场营销电子邮件地址

apmarketing@dell.com (仅限于亚太国家和地区)

sales\_canada@dell.com (仅限于加拿大)

- 匿名文件传输协议 (FTP)

**ftp.dell.com**

使用用户名 `anonymous` 登录，并将您的电子邮件地址用作密码。

## Automated Order-Status Service (订单状态自动查询服务)

要查询您订购的任何 Dell 产品的状态，您可以访问 **support.dell.com** 或者致电订单状态自动查询服务部门电话录音将提示您输入用于查找和介绍订单的信息。要获得您所在地区可以拨打的电话号码，请参阅[与 Dell 联络](#)。

## 支持服务

Dell 支持服务可以每周 7 天、每天 24 小时解答有关 Dell 硬件的问题。我们的支持人员使用基于计算机的诊断程序，可以快速准确地解答您的问题。

要与 Dell 的支持服务部门联络，请参阅[致电之前](#)，然后查看适用于您所在区域的联络信息。

---

## Dell 企业培训和认证

Dell 可以提供企业培训与认证；有关详情，请访问 **www.dell.com/training**。并非在所有国家和地区均可提供此服务。

---

## 订购时遇到的问题

如果您的订购出现问题，例如缺少或装错部件或帐单错误，请与 Dell 联络寻求客户帮助。致电时，请准备好发票或装箱单。要获得您所在地区可以拨打的电话号码，请参阅[与 Dell 联络](#)。

---

## 产品信息

要了解 Dell 提供的其它产品的信息或者订购产品，请访问 Dell 网站 **www.dell.com**。要获得适用于您所在地区的销售人员联系电话号码，请



参阅[与 Dell 联络](#)。

## 退回部件要求保修或退款

无论您是要求维修还是退款，请按以下说明准备好所有要退回的项目：

致电 Dell 获得退回材料授权号，并在包装箱外侧的显著位置清楚地注明此号码。

要获得您所在地区可以拨打的电话号码，请参阅[与 Dell 联络](#)。

附上发票复印件和一封说明退回原因的信函。

附上诊断程序检验表副本（请参阅[诊断程序检验表](#)），包括您所执行的测试以及 Dell 诊断程序报告的所有错误信息。

如果您要求信用退回，请附上退回产品的所有附件（例如电源电缆、介质 [如 CD 和软盘] 及指南）。

使用原来的（或相当的）包装材料包装退回的设备。

您必须支付运费，同时还应为退回的所有产品投保，并承担产品在运送至 Dell 公司途中丢失的风险。本公司不接受以货到付款 (C.O.D.) 方式寄送的包裹。

如果退回的物品不符合上述任何要求，Dell 接收部门会拒绝接收并将其退回给您。

## 致电之前



**注：**致电时，请准备好您的快速服务代码。此代码可以帮助 Dell 的自动支持电话系统快速转接您的电话。

请务必填写诊断程序检验表（请参阅[诊断程序检验表](#)）。如果可能，请在致电 Dell 以寻求帮助之前打开计算机，同时使用靠近计算机的电话。Dell 可能会要求您在键盘上键入某些命令、传达操作期间的详细信息或者尝试只能在计算机上执行的其它故障排除步骤。确保可以使用计算机说明文件。



**警告：**在操作计算机内部之前，请按照《产品信息指南》中的安全说明操作。

诊断程序检验表
姓名：
日期：
地址：
电话号码：
服务标签（计算机背面或底部的条形码）：
快速服务代码：
退回材料授权号（如果 Dell 支持部门的技术人员已为您提供）：
操作系统及其版本：
设备：
扩充卡：
您是否已连接到网络？ 是 否
网络、版本和网络适配器：
程序及其版本：


请参阅操作系统的说明文件以确定系统启动文件的内容。如果计算机与打印机相连，请打印每个文件。否则请在致电 Dell 之前记下每个文件的内容。

错误信息、蜂鸣音代码或诊断代码：

问题说明和您执行的故障排除步骤：

## 与 Dell 联络

美国客户请致电 800-WWW.DELL (800.999.3355)。

 **注：**如果没有有效的 Internet 连接，您可以在购物发票、装箱单、帐单或 Dell 产品目录中查找联络信息。

Dell 提供了多种在线和电话的支持及服务选项。这些支持和服务选项因产品和国家或地区而异，有些服务可能没有在您所在的国家或地区提供。要与 Dell 联络以解决销售、技术支持或客户服务方面的问题，您可以：

访问 **support.dell.com**。

在页面底部的 **Choose A Country/Region**（选择国家/地区）下拉式菜单中指明您所在的国家或地区。

单击页面左侧的 **Contact Us**（与我们联络）。

根据需要选择相应的服务或支持链接。

选择用来与 Dell 联络的便捷方法。

---

[返回目录页面](#)