Dell™ PowerConnect™ 34XX 系统用户指南

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：警告表示可能会导致财产损失、人身伤害甚至死亡。

2005 年 3 月

返回目录页面

简介

Dell™ PowerConnect™ 34XX 系统用户指南

PowerConnect 3424/3448 和 PowerConnect 3424P/3448P 是可堆栈使用的、高级多层设备。PowerConnect 装置既可用作独立的、多层交换设备，又可用作最多包含六个堆栈成员的可堆栈使用设备。

本用户指南介绍有关安装、配置和维护该设备的信息。

系统说明

PowerConnect 3424/3448 和 PowerConnect 3424P/3448P 将多功能性与最小管理相结合。PowerConnect 3424 和 3448 系列包括以下设备类型：

- PowerConnect 3424
- PowerConnect 3424P
- PowerConnect 3448
- PowerConnect 3448P

PowerConnect 3424

PowerConnect 3424 提供了 24 个 10/100 Mbps 端口和两个 SFP 端口，以及两个可用于在独立设备中传输通信的铜质端口（堆栈设备时用作堆栈端口）。该设备还提供了一个 RS-232 控制台端口。PowerConnect 3424 是一种可堆栈使用的设备，但也可作为独立设备运行。

PowerConnect 3424P

PowerConnect 3424P 提供了 24 个 10/100 Mbps 端口和两个 SFP 端口，以及两个可用于在独立设备中传输通信的铜质端口（堆栈设备时用作堆栈端口）。该设备还提供了一个 RS-232 控制台端口。PowerConnect 3424P 是一种可堆栈使用的设备，但也可作为独立设备运行。PowerConnect 3424P 还提供了以太网电源 (PoE)。

图 1-1. PowerConnect 3424 和 PowerConnect 3424P

PowerConnect 3448

PowerConnect 3448 提供了 48 个 10/100 Mbps 端口和两个 SFP 端口，以及两个可用于在独立设备中传输通信的铜质端口（堆栈设备时用作堆栈端口）。该设备还提供了一个 RS-232 控制台端口。PowerConnect 3448 是一种可堆栈使用的设备，但也可用作独立设备。

PowerConnect 3448P

PowerConnect 3448P 提供了 48 个 10/100 Mbps 端口、两个 SFP 端口和两个铜质端口，当设备在独立模式下时，这两个铜质端口可用于传输通信，当设备为堆栈的一部分时，这两个铜质端口可用作堆栈端口。该设备还提供了一个 RS-232 控制台端口。此外，PowerConnect 3448P 提供了 PoE。

图 1-2. PowerConnect 3448 和 PowerConnect 3448P

堆栈概览

PowerConnect 3424/P 和 PowerConnect 3448/P 堆栈提供了通过单点进行的多交换机管理，就好像所有堆栈成员是一个装置。所有堆栈成员均通过用于管理堆栈的单个 IP 地址被访问。从以下位置管理堆栈：

- 基于 Web 的界面
- SNMP 管理站点

- 命令行界面 (CLI)

PowerConnect 3424/P 和 PowerConnect 3448/P 设备支持每个堆栈最多堆栈六个装置，也可作为独立装置运行。

在堆栈设置过程中，选择一个交换机作为堆栈主装置，选择另一个堆栈成员作为备份主装置。选择所有其它设备作为堆栈成员，并为它们分配唯一的装置 ID。

交换机软件则是针对每个堆栈成员单独下载的。但是，堆栈中的所有装置必须运行相同的软件版本。

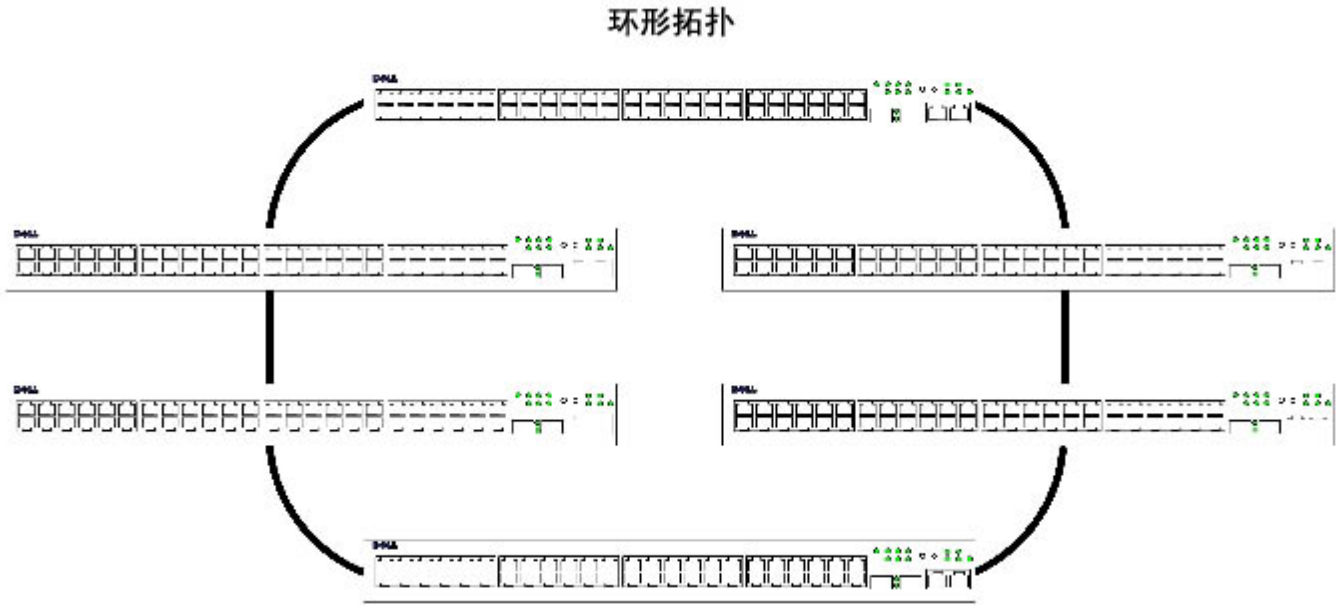
交换机堆栈和配置由堆栈主装置维护。在发生以下事件时，堆栈主装置将检测端口并对其进行重新配置，以最大限度地降低对运行的影响：

- 装置故障
- 装置间堆栈链路故障
- 插入装置
- 卸下堆栈装置

了解堆栈拓扑

PowerConnect 3400 系列在环形拓扑中运行。堆栈环形拓扑是指堆栈中的所有设备彼此连接形成一个环。堆栈中的每个设备将接收数据并将数据发送至它连接的设备。信息包将通过堆栈继续传送，直到信息包到达其目的地。系统将查找用于发送通信的最佳路径。

图 1-3. 堆栈环形拓扑



环形中的设备不正常运行或链路损坏时，环形拓扑中所涉及的大部分问题将发生。使用 PowerConnect 3424/P 和 PowerConnect 3448/P 堆栈，系统将自动切换至堆栈故障时转移拓扑，而无需停止系统。SNMP 信息是自动生成的，无需任何堆栈管理操作。但是，必须修复堆栈链路或堆栈成员以确保堆栈的完整性。

解决了堆栈问题之后，可以将设备重新连接至堆栈而无需中断，并恢复环形拓扑。

堆栈故障时转移拓扑

如果在堆栈拓扑中出现故障，堆栈将恢复为堆栈故障时转移拓扑。在堆栈故障时转移拓扑中，设备将在链式结构中运行。堆栈主装置可确定信息包发送位置。除了顶部和底部的装置，其余装置均连接至两个相邻的设备。

堆栈成员和装置 ID

对于堆栈配置，堆栈装置 ID 非常重要。堆栈运行在引导进程中确定。运行模式由初始化进程中选定的装置 ID 确定。例如，如果用户选择独立模式，设备将在引导进程中作为独立设备引导。

设备装置出厂时设置有独立装置的默认装置 ID。如果设备作为独立装置运行，则所有堆栈 LED 都不亮。

用户选择不同的装置 ID 后，则不会被删除并保持有效（即使重设装置）。

装置 ID 1 和装置 ID 2 是专用于启用主装置的装置。装置 ID 3 至装置 ID 6 可以定义给堆栈成员。

主装置引导时或者插入或卸下堆栈成员时，主装置将启动堆栈查找进程。

注：如果查找到具有相同装置 ID 的两个成员，则堆栈将继续运行，但是，仅加入时间较长的装置才可以加入堆栈。将向用户发送信息，通知某个装置无法加入堆栈。

卸下和替换堆栈成员

装置 1 和装置 2 是启用主装置的装置。可以将装置 1 和装置 2 指定为主装置或备份主装置。在配置进程中执行堆栈主装置分配。根据以下判断过程，可以选择其中一个启用主装置的堆栈成员作为主装置，选择另一个启用主装置的堆栈成员作为备份主装置：

- 如果仅存在一个启用堆栈主装置的装置，则选择它作为主装置。
- 如果存在两个启用主装置的堆栈成员，并且其中一个已手动配置为堆栈主装置，则选择该手动配置的成员作为堆栈主装置。
- 如果存在两个启用主装置的装置并且均未手动配置为主装置，则选择运行时间较长的装置作为堆栈主装置。
- 如果存在两个启用主装置的装置并且均已手动配置为主装置，则选择运行时间较长的装置作为堆栈主装置。
- 如果两个启用主装置的堆栈成员处于同一时间，则选择装置 1 作为堆栈主装置。

注：如果两个堆栈成员插入的时间间隔在十分钟内，则认为它们处于同一时间。

例如，装置 2 被插入一个十分钟周期的第一分钟，装置 1 被插入同一周期的第五分钟，则认为这两个装置处于同一时间。如果有两个处于同一时间的启用主装置的堆栈成员，则选择装置 1 作为主装置。

堆栈主装置和备份主装置将维护热备份。热备份将确保在发生故障时转移时，备份主装置可以替换堆栈主装置。这将保证堆栈继续正常运行。

在热备份过程中，仅当静态配置时，主装置和备份主装置才会同步。配置堆栈主装置时，堆栈主装置必须同步堆栈备份主装置。不保存动态配置，例如，不保存动态记忆的 MAC 地址。

堆栈中的每个端口具有特定的装置 ID、端口类型和端口号，它们是配置命令和配置文件的一部分。仅能从设备堆栈主装置管理配置文件，包括：

- 保存到 FLASH
- 将配置文件加载到外部 TFTP 服务器
- 从外部 TFTP 服务器下载配置文件

注：即使堆栈被重设和/或端口不再存在，所有已配置端口的堆栈配置仍会保存。

只要执行重新引导，就执行拓扑查找，并且主装置将记忆堆栈中的所有装置。装置 ID 将保存在装置中，并通过拓扑查找被记忆。如果某个装置尝试在没有选定主装置的情况下进行引导，并且该装置没有在独立模式下运行，则该装置将不会引导。

只能通过明确的用户配置更改配置文件。在出现以下情况时配置文件不会自动修改：

- 添加装置
- 卸下装置
- 为装置重新分配装置 ID
- 装置在堆栈模式和独立模式之间进行切换

每次重新引导系统时，主装置中的启动配置文件均将用于配置堆栈。

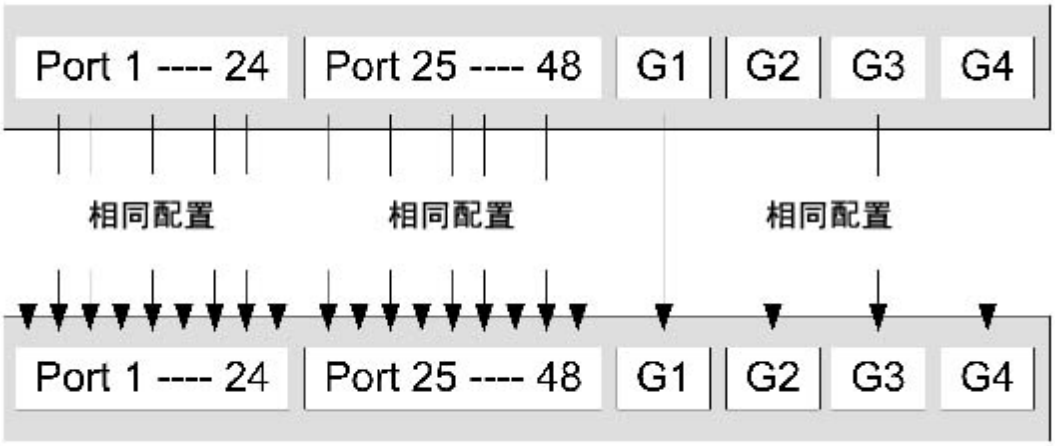
如果从堆栈中卸下堆栈成员，然后由具有相同的装置 ID 的装置替换，则新的堆栈成员将使用原来的设备配置进行配置。只有物理存在的端口才会在 PowerConnect OpenManage Switch Administrator 主页中显示，并且可以通过 Web 管理系统进行配置。不存在的端口可以通过 CLI 或 SNMP 界面进行配置。

交换堆栈成员

如果用具有相同装置 ID 的堆栈成员替换具有相同装置 ID 的现有堆栈成员，则先前的设备配置将应用于该插入的堆栈成员。如果新插入设备的端口比先前设备多或少，则相应的端口配置将应用于新的堆栈成员。例如，

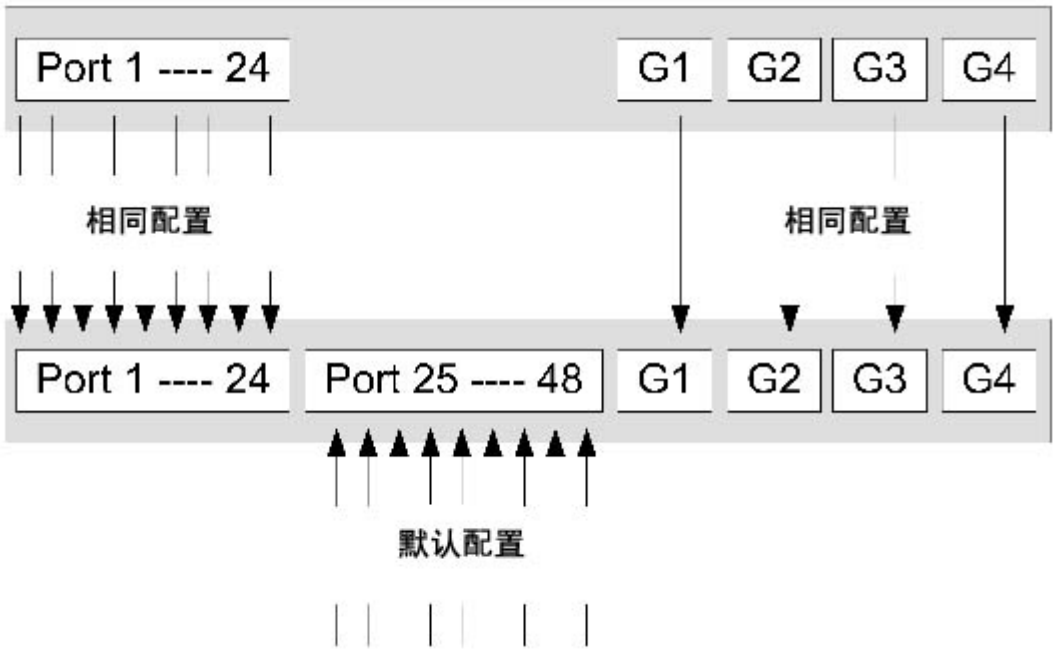
- 如果用 PowerConnect 3424/P 替换 PowerConnect 3424/P，则所有端口配置保持不变。
- 如果用 PowerConnect 3448/P 替换 PowerConnect 3448/P，则所有端口配置保持不变。

图 1-4. 用 PowerConnect 3448/P 替换 PowerConnect 3448/P



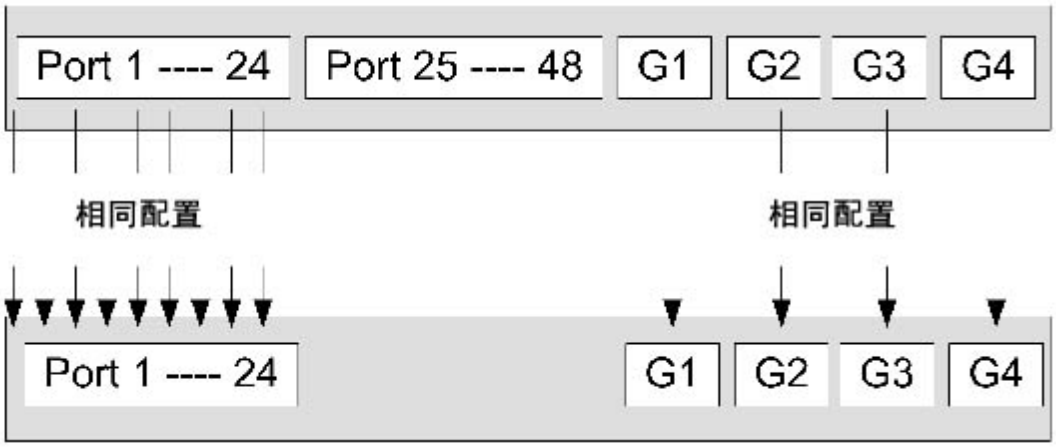
- 如果用 PowerConnect 3448/P 替换 PowerConnect 3424/P，则第一个 3448/P 24 FE 端口将接收 3424/P 24 FE 端口配置。GE 端口配置将保持不变。其余端口将接收默认端口配置。

图 1-5. 用 PowerConect 3424/P 端口替换 PowerConnect 3448/P 端口



- 如果用 PowerConnect 3424/P 替换 PowerConnect 3448/P，则 PowerConnect 3424/P 24 FE 端口将接收第一个 24 FE PowerConnect 3448/P 端口配置。GE 端口配置将保持不变。

图 1-6. 用 PowerConect 3448/P 端口替换 PowerConnect 3424/P 端口



从堆栈主装置切换至备份堆栈主装置

如果出现以下情况，则备份主装置将替换堆栈主装置：

- 堆栈主装置出现故障或从堆栈中卸下。
- 从堆栈主装置到堆栈成员的链接失败。
- 通过 Web 界面或 CLI 执行软切换。

堆栈主装置与备份主装置间的切换导致有限服务丢失。如果出现故障，则重新记忆所有动态表。正在运行的配置文件在堆栈主装置和备份主装置之间同步，并继续在备份主装置上运行。

功能概览

本节介绍了设备功能。有关所有已更新的设备功能的完整列表，请参阅最新版本软件的版本注释。

以太网电源

以太网电源 (PoE) 通过现有的 LAN 电缆为设备供电，而无需更新或修改网络基础设施。PoE 使网络设备无需放置于电源旁边。PoE 可用于以下应用：

- IP 电话

- 无线访问点
- IP 网关
- PDA
- 音频和视频远程监测

有关以太网电源的详细信息，请参阅“管理以太网电源”。

队列头阻塞

队列头 (HOL) 阻塞会导致由于通信竞争同一出口端口资源而引起的通信延迟和帧丢失。HOL 阻塞会对信息包进行排队，先传输队列头的信息包，然后再传输队列尾的信息包。

流控制支持 (IEEE 802.3X)

流控制通过请求高速设备抑制发送信息包，从而使低速设备可以与高速设备进行通信。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“定义端口配置”或“定义 LAG 参数”。

背压支持

在半双工链路中，接收端口通过占用链路使其不能用于其它通信来防止缓冲区溢出。

有关为端口或 LAG 配置流控制的信息，请参阅“定义端口配置”或“定义 LAG 参数”。

虚拟电缆测试 (VCT)

VCT 用于检测和报告铜质链接线路中的故障（例如断路和短路）。有关测试电缆的详细信息，请参阅“运行电缆诊断程序”。

MDI/MDIX 支持

启用自适应时，设备将自动检测连接到 RJ-45 端口的电缆是绞接电缆还是直通电缆。

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“定义端口配置”或“定义 LAG 参数”。

自适应

自适应使设备可以公布运行模式。自适应功能提供了在共用点对点链路网段的两个设备之间交换信息的方法，以及自动将两个设备配置为可以最大程度地利用其传输能力的方法。

PowerConnect 3400 系列通过提供端口公告增强了自适应功能。端口公告使系统管理员可以配置公布的端口速率。

有关自适应的详细信息，请参阅“定义端口配置”或“定义 LAG 参数”。

支持 MAC 地址的功能

MAC 地址容量支持

设备最多支持 8K MAC 地址。设备保留了供系统使用的特定 MAC 地址。

静态 MAC 条目

可以在桥接表中手动输入 MAC 条目，并作为从传入帧记忆 MAC 条目的一种替代方法。这些用户定义的条目不受存在时间的限制，并且在重启动或重新引导时不会丢失。

有关详情，请参阅“定义静态地址”。

自动记忆 MAC 地址

设备允许从传入信息包自动学习 MAC 地址。MAC 地址存储在桥接表中。

自动管理 MAC 地址的存在时间

在给定时间段内没有接收到任何通信的 MAC 地址将成为过期 MAC 地址。这样可以防止桥接表溢出。

有关配置 MAC 地址过期时间的详细信息，请参阅“查看动态地址”。

可识别 VLAN 的基于 MAC 的交换

设备始终执行可识别 VLAN 的桥接。不执行经典桥接 (IEEE802.1D)，经典桥接中的帧仅根据其目的地 MAC 地址进行传输。但是，可以为未标记的帧配置类似的功能。定址到与任一端口均不相关的目的地 MAC 地址的帧将被多路发送至相关 VLAN 的所有端口。

MAC 多点传送支持

多点传送服务是一种有限制的广播服务，它允许采用一对多和多对多的连接形式进行信息分发。第 2 层多点传送服务是将单个帧发往特定多点传送地址，再从该地址将帧的副本传输至相关端口。

有关详情，请参阅“设定全部多点传送参数”。

第 2 层功能

IGMP 监测

IGMP 监测用于在设备将 IGMP 帧内容从工作站点传输至上游多点传送路由器时对 IGMP 帧内容进行检查。设备通过帧识别为多点传送会话配置的工作站点，以及发送多点传送帧的多点传送路由器。

有关详情，请参阅“IGMP 监测”。

端口镜像

通过将传入和传出信息包的副本从被监测端口传输至监测端口，端口镜像可以监测和镜像网络通信。用户可以指定哪个目标端口接收通过指定源端口的所有通信副本。

有关详情，请参阅“定义端口镜像会话”。

广播风暴控制

风暴控制用于限制设备接收和传输的多点传送帧和广播帧的数量。

传输第 2 层帧时，广播帧和多点传送帧将一起传输至相关 VLAN 中的所有端口。这会占用带宽并载入所有端口上连接的所有节点。

有关详情，请参阅“启用风暴控制”。

支持 VLAN 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。

有关详情，请参阅“配置 VLAN”。

基于端口的虚拟 LAN (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。

有关详情，请参阅“定义 VLAN 端口设置”。

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，设备将在属于处于活动状态的基础“生成树协议功能”拓扑的所有端口上注册和传播 VLAN 成员关系。

有关详情，请参阅“配置 GVRP 参数”。

专用 VLAN

专用 VLAN 端口（第 2 层安全保护功能）用于提供同一广播域中端口间的隔离。

有关专用 VLAN 的详细信息，请参阅“配置专用 VLAN”。

生成树协议功能

生成树协议（STP）

802.1d 生成树是标准的第 2 层交换机要求，允许网桥自动防止和解决 L2 传输环路。交换机使用经过专门格式化的帧来交换配置信息并在端口上有选择地启用和禁用传输。

有关详情，请参阅“配置生成树协议”。

快速链路

STP 聚合最多需要 30 至 60 秒钟。在此期间，STP 检测可能存在的环路，并留出时间以传播状态更改，并使相关设备能够做出响应。对于很多应用程序而言，30 至 60 秒钟的响应时间都被认为过长。“Fast Link”（快速链路）选项可以避免这种延迟，它可以在不存在传输环路的网络拓扑中使用。

有关为端口和 LAG 启用快速链路的详细信息，请参阅“定义 STP 端口设置”或“定义静态地址”。

IEEE 802.1w 快速生成树

生成树可以为各主机提供 30 至 60 秒钟的时间来确定其端口是否正在传输通信。快速生成树（RSTP）用于检测网络拓扑的使用情况，以启用更快速的聚合，并且不会产生传输环路。

有关详情，请参阅“定义快速生成树”。

IEEE 802.1s 多个生成树

多个生成树（MSTP）操作可以将 VLAN 映射到 STP 实例中。MSTP 提供了不同的负载平衡方案。分配给各个 VLAN 的信息包将在 MSTP 区域（MST

区域）中沿着不同的路径发送。区域是一个或多个可以用于发送帧的 MSTP 网桥。标准区域使管理员可以将 VLAN 通信分配到唯一的路径。

有关详情，请参阅“配置生成树协议”。

链路聚合

链路聚合

最多可以定义八个聚合链路（每个聚合链路最多具有八个成员端口），从而形成单个链路聚合组（LAG）。这具有以下优点：

- 物理链路中断时可以进行容错保护
- 更高的带宽连接
- 提高了带宽粒度
- 高带宽服务器连通性

LAG 由具有相同速率并被设置为全双工运行的端口组成。

有关详情，请参阅“定义 LAG 参数”。

链路聚合和 LACP

在不中断的基础上，LACP 在链路中使用同级交换以确定不同链路的聚合功能，并不断在给定的一对设备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、捆绑和监测系统内捆绑的端口。

有关详情，请参阅“聚合端口”。

BootP 和 DHCP 客户端

DHCP 允许系统启动时从网络服务器接收附加的设置参数。DHCP 服务是一个不中断的进程。DHCP 是对 BootP 的扩展。

有关 DHCP 的详细信息，请参阅“定义 DHCP IP 接口参数”。

服务质量功能

服务级别 802.1p 支持

IEEE 802.1p 信号技术是 OSI 第 2 层标准，用于在数据链路/MAC 子层标记网络通信和排定网络通信的优先级。802.1p 通信将被分类并传送至目的地。不会建立或强制执行带宽预留或限制。802.1p 是从 802.1Q (VLAN) 标准衍生出来的标准。802.1p 建立了八个级别的优先级，类似于 IP 优先级 IP 标头位字段。

有关详情，请参阅“配置服务质量”。

设备管理功能

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 警报和陷阱的详细信息，请参阅“定义 SNMP 参数”。

SNMP 版本 1、2 和 3

基于 UDP/IP 协议的简单网络管理协议 (SNMP) 可以控制对系统的访问。为此，定义了一个团体条目列表，每个条目均由一个团体字符串及其访问权限构成。共有 3 个 SNMP 安全保护级别：只读、读写和超级。只有超级用户才可以访问团体表。

有关详情，请参阅“定义 SNMP 参数”。

基于 Web 的管理

使用基于 Web 的管理，可以通过任何 Web 浏览器来管理系统。系统包含一个支持 HTML 页面的嵌入式 Web 服务器 (EWS)，通过这些页面可以监测和配置系统。系统在内部将基于 Web 的输入转换为配置命令、MIB 变量设置和其它与管理相关的设置。

配置文件下载和加载

设备配置存储在一个配置文件中。配置文件包含整个系统和端口特定设备配置。系统可以用一组 CLI 命令的形式显示配置文件，对这些命令的存储和操作类似于文本文件。

有关详情，请参阅“管理文件”。

TFTP 小型文件传输协议

设备支持通过 TFTP 加载/下载引导映像、软件和配置。

远程监测

远程监测（RMON）是对 SNMP 的扩展，它使网络通信监测功能更加全面（相对于允许网络设备管理和监测的 SNMP）。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，使系统可以从整个网络中捕获实时信息。

有关详情，请参阅“查看统计数据”。

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。CLI 解释器提供命令和关键字自动完成功能，可以帮助用户并减少输入量。

系统日志

系统日志是用于向一组远程服务器发送事件通知的协议，在这些远程服务器中事件通知可以被存储、检查和处理。系统可以实时发送重要事件的通知，并保存这些事件的记录以供将来使用。

有关系统日志的详细信息，请参阅“管理日志”。

SNTP

简单网络时间协议（SNTP）可以确保将网络以太网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。时间源通过层来建立。层定义与参考时钟的时间差。层越高（最高为零），时钟越准确。

有关详情，请参阅“配置 SNTP 设置”。

域名系统

域名系统 (DNS) 用于将用户定义的域名转换为 IP 地址。每次分配域名后，DNS 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。DNS 服务器维护域名数据库及其对应的 IP 地址。

有关详情，请参阅“配置域名系统”。

Traceroute

Traceroute 将查找信息包在传输过程中所经过的 IP 路由。可以从用户执行模式或优先模式执行 CLI Traceroute 公用程序。

安全保护功能

SSL

安全套接层 (SSL) 是一种通过保密、验证和数据完整性等方式确保数据事务处理安全的应用程序级协议。它依靠证书和公用及专用密钥。

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。

有关详情，请参阅“配置基于端口的验证”。

锁定端口支持

锁定端口通过仅允许具有特定 MAC 地址的用户访问特定端口来增强网络的安全保护。可以在该端口上手动定义或记忆这些地址。当帧经过锁定端口并且帧的源 MAC 地址与该端口无关联时，将调用保护机制。

有关详情，请参阅“配置端口安全保护”。

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，数据库中包含各个用户的验证信息（例如用户名、密码和帐户信息）。

有关详情，请参阅“配置 RADIUS 设置”。

SSH

安全命令解释程序（SSH）是一个提供了到设备的安全远程连接的协议。SSH 版本 2 为当前支持的版本。SSH 服务器特性使 SSH 客户端可以建立与设备的安全加密连接。此连接所提供的功能类似于入站的 Telnet 连接。SSH 使用 RSA 和 DSA 公用密钥加密法进行设备连接和验证。

TACACS+

TACACS+ 为访问设备的用户的验证提供了集中式的安全保护。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。

有关详情，请参阅“定义 TACACS+ 设置”。

密码管理

密码管理提供了增强的网络安全保护和改进的密码控制。给用于 SSH、Telnet、HTTP、HTTPS 和 SNMP 访问的密码设定了安全保护功能。有关密码管理的详细信息，请参阅“管理密码”。

附加 CLI 说明文件

说明文件 CD 中的 CLI 参考指南介绍了有关用于配置设备的 CLI 命令的信息。说明文件提供了有关命令说明、语法、默认值、原则和示例的信息。

返回目录页面

返回目录页面

硬件说明

Dell™ PowerConnect™ 34XX 系统用户指南

端口说明

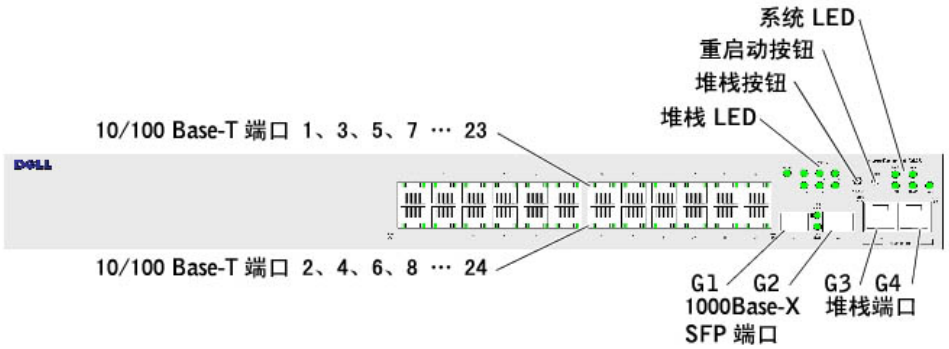
PowerConnect 3424 端口说明

PowerConnect 3424 设备配置了以下端口：

- 24 个高速以太网端口 — 指定为 10/100Base-T 端口的 RJ-45 端口
- 2 个光纤端口 — 指定为 1000Base-X SFP 端口
- 2 个吉位端口 — 指定为 1000Base-T 端口
- 控制台端口 — 基于 RS-232 的端口

下图说明了 PowerConnect 3424 前面板。

图 2-1. PowerConnect 3424 前面板



前面板包含 24 个 RJ-45 端口，编号为 1 至 24。上面一排端口用奇数 1 至 23 进行标记，下面一排端口用偶数 2 至 24 进行标记。此外，前面板还包含光纤端口 G1 和 G2 以及铜质端口 G3 和 G4。端口 G3 和 G4 既可用作堆栈端口，又可用于在独立设备中传输网络通信。

前面板上有两个按钮。堆栈 ID 按钮用于选择装置编号。另一个按钮是用于手动重启动设备的重启动按钮。重启动按钮没有伸出装置的前面板表面，因此防止了意外按到该按钮而重启动设备。前面板上有所有设备 LED。

下图说明了 PowerConnect 3424 背面板：

图 2-2. PowerConnect 3424 背面板

背面板包含 RPS 连接器、控制台端口和电源连接器。

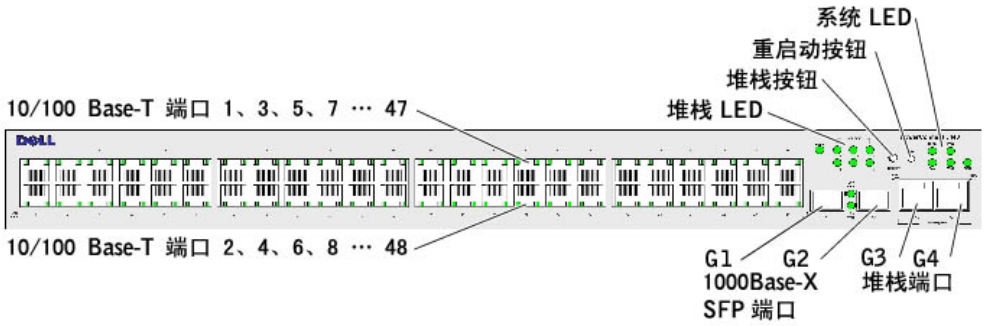
PowerConnect 3448 端口说明

PowerConnect 3448 设备配置了以下端口：

- 48 个 FE 端口 — 指定为 10/100Base-T 端口的 RJ-45 端口
- 2 个光纤端口 — 指定为 1000Base-X SFP 端口
- 2 个吉位端口 — 指定为 1000Base-T 端口
- 控制台端口 — 基于 RS-232 控制台的端口

下图说明了 PowerConnect 3448 前面板。

图 2-3. PowerConnect 3448 前面板



前面板包含 48 个 RJ-45 端口，编号为 1 至 48。上面一排端口用奇数 1 至 47 进行标记，下面一排端口用偶数 2 至 48 进行标记。此外，前面板还包含光纤端口 G1 和 G2 以及铜质端口 G3 和 G4。端口 G3 和 G4 既可用作堆栈端口，又可用于在独立设备中传输网络通信。

前面板上有两个按钮。堆栈 ID 按钮用于选择装置编号。另一个按钮是用于手动重启动设备的重启动按钮。重启动按钮没有伸出装置的前面板表面，因此防止了意外按到该按钮而重启动设备。前面板上有所有设备 LED。

下图说明了 PowerConnect 3448 背面板：

图 2-4. PowerConnect 3448 背面板

背面板包含 RPS 连接器、控制台端口和电源连接器。

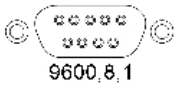
SFP 端口

超小型可插入式 (SFP) 端口是一种双线串行界面 (TWSI)，它通过被指定为 1000Base-SX 或 LX 的复杂可编程逻辑设备 (CPLD) 进行通信。

RS-232 控制台端口

一个用于终端连接的 DB-9 连接器可用于调试、软件下载等。默认波特率为 9,600 bps。可以将波特率配置为 2400 bps 到最大为 115,200 bps。

图 2-5. 控制台端口



物理尺寸

PowerConnect 3424/P 和 PowerConnect 3448/P 设备的物理尺寸如下所示：

PoE 型号：

- 宽度 — 440 mm (17.32 英寸)
- 厚度 — 387 mm (15.236 英寸)
- 高度 — 43.2 mm (1.7 英寸)

非 PoE 设备：

- 宽度 — 440 mm (17.32 英寸)
- 厚度 — 257 mm (10.118 英寸)
- 高度 — 43.2 mm (1.7 英寸)

LED 定义

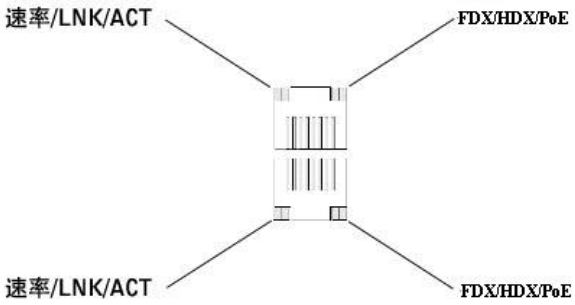
前面板上有发光二极管 (LED)，这些发光二极管表明链路状态、电源设备状态、风扇状态以及系统诊断程序的状态。

端口 LED

每个 10/100/1000 Base-T 端口和 10/100 Base-T 端口均具有两个 LED。速率 LED 位于端口的左侧，链路/双工/活动 LED 位于右侧。

下图说明了 PowerConnect 3424/P 和 PowerConnect 3448/P 交换机上的 10/100 Base-T 端口 LED：

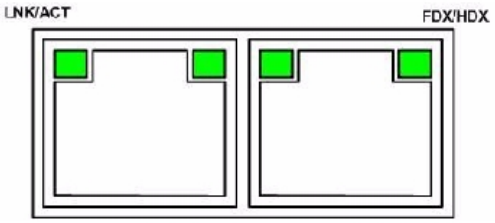
图 2-6. 基于 RJ-45 的铜质的 10/100 BaseT LED



PowerConnect 3424/P 和 PowerConnect 3448/P 上的 RJ-45 100 Base-T 端口具有两个标记为 LNK/ACT 的 LED。

下图说明了 100 Base-T LED。

图 2-7. RJ-45 1000 BaseT LED



下表介绍了用于 PowerConnect 3424 和 PowerConnect 3448 的 RJ-45 LED 指示灯：

表 2-1. PowerConnect 3424 和 PowerConnect 3448 RJ-45 100BaseT LED 指示灯

LED	颜色	说明
链路/活动/速率	呈绿色稳定亮起	端口正在以 100 Mbs 的速率运行。
	呈绿色闪烁	端口正在以 100 Mbps 的速率发送或接收数据。
	呈黄色稳定亮起	端口正在以 10 Mbs 的速率运行。
	呈黄色闪烁	端口正在以 10 Mbps 的速率发送或接收数据。
	不亮	端口当前未运行。
FDX	呈绿色稳定亮起	端口当前正在以全双工模式运行。
	不亮	端口当前正在以半双工模式运行。

下表介绍了用于 PowerConnect 3424P 和 PowerConnect 3448P 的 RJ-45 LED 指示灯：

表 2-2. PowerConnect 3424P 和 PowerConnect 3448P 基于 RJ-45 铜质的 100BaseT LED 指示灯

LED	颜色	说明
速率/链路/活动	呈绿色稳定亮起	端口当前的链接速率为 100 Mbps。
	呈绿色闪烁	端口当前正在以 100 Mbps 的速率运行。
	不亮	端口当前正在以 10 Mbps 的速率运行，或未链接。
PoE	呈绿色稳定亮起	检测到用电设备 (PD)，并且它正在以正常负载运行。有关用电设备的详细信息，请参阅“管理以太网电源”。
	呈琥珀色稳定亮起	用电设备出现过载或短路。有关以太网电源故障的详细信息，请参阅“管理以太网电源”。

	呈琥珀色闪烁	用电设备的电源设计量超出预定义的电源分配。有关以太网电源的电源分配的详细信息，请参阅“管理以太网电源”。
不亮	未检测到任何用电设备。	

吉位端口 LED

下表介绍了吉位（堆栈端口）LED：

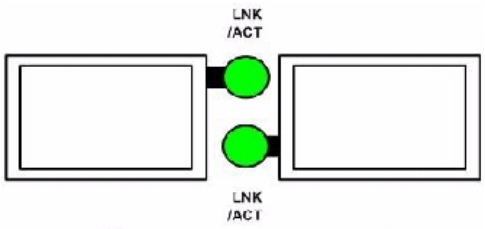
表 2-3. PowerConnect 3424 和 PowerConnect 3448 基于 RJ-45 铜质的 100BaseT LED 指示灯

LED	颜色	说明
链路/活动/速率	呈绿色稳定亮起	端口正在以 1000 Mbs 的速率运行。
	呈绿色闪烁	端口正在以 1000 Mbps 的速率发送或接收数据。
	呈黄色稳定亮起	端口正在以 10 Mbs 或 100 Mbs 的速率运行。
	呈黄色闪烁	端口正在以 10 Mbps 或 100 Mbps 的速率发送或接收数据。
	不亮	端口当前未运行。
FDX	呈绿色稳定亮起	端口当前正在以全双工模式运行。
	不亮	端口当前正在以半双工模式运行。

SFP LED

每个 SFP 端口均具有一个标记为 LNK/ACT 的 LED。在 PowerConnect 3424/P 和 PowerConnect 3448/P 设备上，LED 位于端口之间，且是圆形的。下图说明了每个设备上的 LED。

图 2-8. SFP 端口 LED



下表说明了 SFP 端口 LED 指示灯的信息：

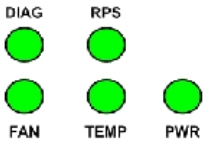
表 2-4. SFP 端口 LED 指示灯

LED	颜色	说明
链路/活动	呈绿色稳定亮起	已建立链路。
	呈绿色闪烁	端口当前正在发送或接收数据。
	不亮	端口当前未链接。

系统 LED

PowerConnect 3424/P 和 PowerConnect 3448/P 设备的系统 LED 提供了有关电源设备、风扇、温度状况和诊断程序的信息。下图说明了系统 LED。

图 2-9. 系统 LED



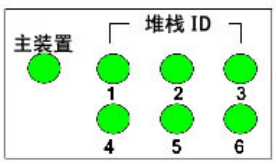
下表说明了系统 LED 指示灯。

表 2-5. 系统 LED 指示灯

LED	颜色	说明
电源设备 (PWR)	呈绿色稳定亮起	交换机电源已打开。
	不亮	交换机电源未打开。
冗余电源设备 (RPS) (型号：3424 和 3448)	呈绿色稳定亮起	RPS 当前正在运行。
	呈红色稳定亮起	RPS 出现故障。
	不亮	未插入冗余电源设备。
冗余电源设备 (RPS) (型号：3424P 和 3448P)	呈绿色稳定亮起	RPS 当前正在运行。
	不亮	冗余电源设备出现故障或未插入电源插座。
诊断程序 (DIAG)	呈绿色闪烁	当前正在进行系统诊断检测程序。
	呈绿色稳定亮起	已成功通过系统诊断检测程序。
	呈红色稳定亮起	未通过系统诊断检测程序。
	不亮	系统运行正常。
温度 (TEMP)	呈红色稳定亮起	设备已超出允许的温度范围。
	不亮	设备在允许的温度范围内运行。
风扇 (FAN)	呈绿色稳定亮起	设备的所有风扇运行正常。
	呈红色稳定亮起	设备的一个或多个风扇未运行。

堆栈 LED 表明了装置在堆栈中所处的位置。下图说明了前面板上的 LED。

图 2-10. 堆栈 LED



堆栈 LED 的编号为 1 至 6。每个堆栈装置均有一个亮起的堆栈 LED，用于表明其装置 ID 编号。如果堆栈 LED 1 或 2 亮起，则表明设备为堆栈主装置或备份主装置。

表 2-6. 堆栈 LED 指示灯

LED	颜色	说明
所有堆栈 LED	不亮	交换机当前为独立设备。
堆栈 LED 1 至 6 (S1-S6)	呈绿色稳定亮起	设备被指定为堆栈装置 N。

	不亮	设备未被指定为堆栈装置 N。
堆栈主装置 LED	呈绿色稳定亮起	设备为堆栈主装置
	不亮	设备不是堆栈主装置。

电源设备

该设备具有一个内部电源装置（交流装置），并带有一个连接器，可以将 PowerConnect 3424/P 和 PowerConnect 3448/P 设备连接至 PowerConnect EPS-470 装置，或将 PowerConnect 3424 和 PowerConnect 3448 设备连接至 PowerConnect RPS-600 装置。PowerConnect 3424/P 和 PowerConnect 3448/P 设备具有一个内部电源设备（12 伏特）。

使用两个电源装置的运行通过负载共享进行调节。电源设备 LED 表明电源设备的状态。

PowerConnect 3424/P 和 PowerConnect 3448/P 设备具有一个 470W (12V/-48V) 的内部电源设备，共有 370W 用于 24 端口 PoE 设备。

交流电源装置

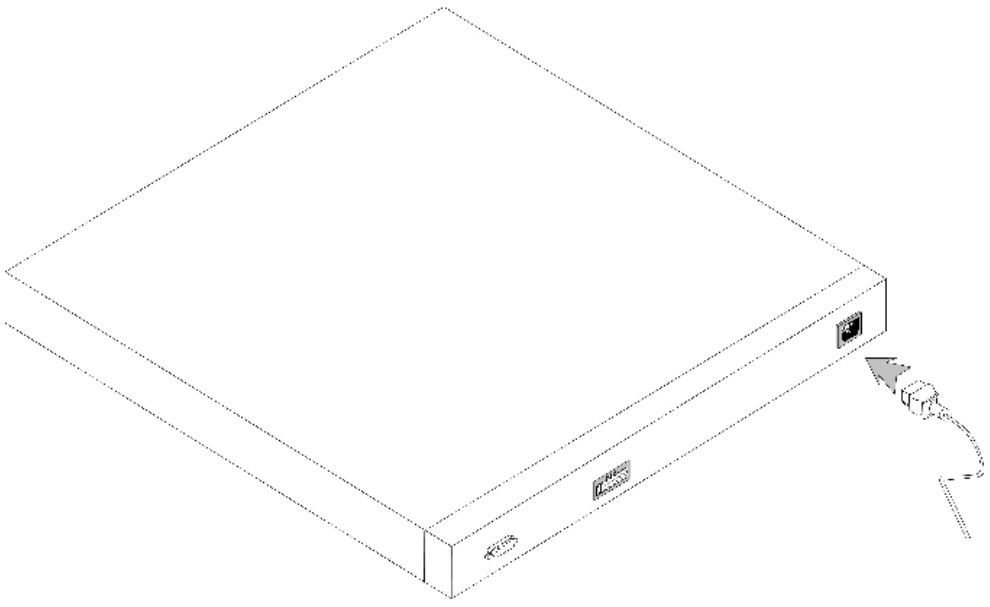
交流电源装置在 90 至 264 VAC、47 至 63 Hz 范围内运行。交流电源装置使用标准连接器。LED 指示灯位于前面板上，它可以表明交流装置是否已连接。

直流电源装置

PowerConnect 3424 和 PowerConnect 3448 交换机连接至外部 RPS-600 装置以提供冗余电源选件。不需要进行任何配置。前面板"RPS"LED 用于表明是否连接了外部 RPS-600。有关 RPS LED 的定义，请参见表 2-5。

PowerConnect 3424/P 和 PowerConnect 3448/P 交换机连接至外部 EPS-470 装置以提供冗余电源选件。不需要进行任何配置。前面板"RPS"LED 用于表明是否连接了外部 EPS-470。有关 RPS LED 的定义，请参见表 2-5。

图 2-11. 电源连接



如果设备连接至不同的电源，则电源断电导致出现故障的可能性将会下降。

堆栈 ID 按钮

设备前面板包含一个用于为堆栈主装置和堆栈成员手动选择装置 ID 的堆栈 ID 按钮。

必须在引导设备的 15 秒内选择堆栈主装置和堆栈成员。如果未在 15 秒内选择堆栈主装置，将以独立模式引导设备。要为设备选择装置 ID，请重新引导设备。

堆栈主装置接收装置 ID 1 或装置 ID 2。如果装置 1 和装置 2 均存在，则未被选择的装置用作备份主装置。堆栈成员接收单独的装置 ID（3 至 6）。例如，如果堆栈中有四个装置，则主装置为 1 或 2，根据主装置的装置 ID，备份主装置为 1 或 2，第三个堆栈成员为 3，第四个堆栈成员为 4。

注：设备不会自动检测独立装置。如果已选择装置 ID，则按堆栈 ID 按钮若干次，直到没有任何堆栈 LED 亮起。

重启动按钮

PowerConnect 3424/P 和 PowerConnect 3448/P 交换机具有重启动按钮，它位于前面板上，用于手动重启动设备。如果重启动了主装置设备，则将重启动整个堆栈。如果仅重启动某个成员装置，则不会重启动其余堆栈成员。

交换机的单个重启动电路可以在通电或低电压条件下激活。

通风系统

具有 PoE 功能的 PowerConnect 3424/P 和 PowerConnect 3448/P 交换机具有五个内置风扇。没有 PoE 功能的 PowerConnect 3424 和 PowerConnect 3448 设备具有两个内置风扇。风扇运行可以通过观察 LED 来验证，该 LED 可以表明是否有一个或多个风扇出现故障。

返回目录页面

返回目录页面

安装 PowerConnect 3424/P 和 PowerConnect 3448/P

Dell™ PowerConnect™ 34XX 系统用户指南

现场准备

PowerConnect 3424/P 和 PowerConnect 3448/P 设备可以安装在标准 48.26 cm (19 英寸) 的设备机架中、放置在桌面上或安装在墙上。在安装装置之前，请验证所选的安装位置符合以下现场要求：

- 电源要求 — 装置应安装在方便插拔的电源插座 (100 - 240 VAC, 50 - 60 Hz) 旁边。
- 一般要求 — 通过检查前面板上的 LED 已亮起，确保正确安装了冗余电源设备 (RPS)。
- PoE 型号要求 — 通过检查前面板上的 PoE LED 已亮起，确保正确安装了 RPS。
- 空间要求 — 正面有足够空间以便操作员进行操作。请留出用于布线、电源连接和通风的空间。
- 布线要求 — 布线应远离电气干扰源 (例如无线电发送器、广播放大器、电线和荧光照明装置) 。
- 周围环境要求 — 装置运行环境温度范围为 0 至 50°C (32 至 122°F) ，相对湿度最大为 95%，非冷凝。

打开包装

套件内容

打开设备的包装时，请确保包含以下项目：

- 设备/交换机
- 交流电源电缆
- RS-232 绞接电缆
- 自粘橡皮垫
- 用于机架安装的机架安装套件或墙上安装套件
- 说明文件 CD
- 产品信息指南

打开设备的包装

注：打开设备的包装之前，请检查包装，如有损坏立即报告。

1. 将包装箱放在清洁的平面上。
2. 打开包装箱或取下包装箱顶盖。
3. 小心地从包装箱中取出设备，并将其放置在稳固清洁的表面上。
4. 取下所有包装材料。
5. 检查设备及附件是否有损坏。如有损坏立即报告。

安装设备

以下安装说明适用于 PowerConnect 3424/P 和 PowerConnect 3448/P 设备。控制台端口位于背面板上。电源连接器位于背面板上。连接冗余电源设备 (RPS) 为可选操作，但是建议您执行此操作。RPS 连接器位于设备的背面板上。

在机架中安装

警告：有关连接或支持交换机的设备的安全信息，请阅读《产品信息指南》中包含的安全信息。

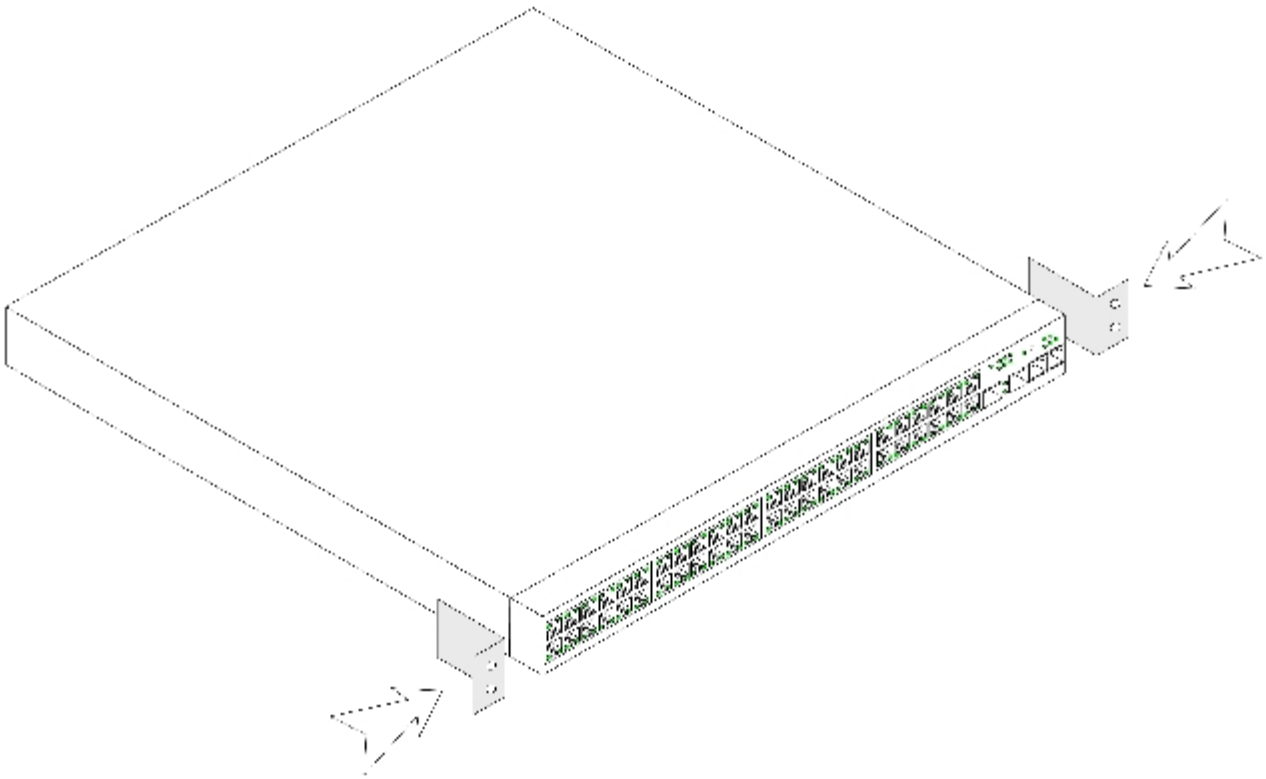
警告：在机架或机柜中安装设备之前，请从装置上断开所有电缆的连接。

警告：将多个设备安装在机架中时，请按照从下到上的顺序安装设备。

1. 将附带的机架固定支架放在设备的一侧，确保设备上的安装孔与机架固定支架上的安装孔对齐。

   下图说明了安装支架的位置。

图 3-1. 用于机架安装的支架安装



2. 将附带的螺钉插入机架安装孔，并用螺丝刀拧紧。

3. 重复此过程，以安装设备另一侧的机架固定支架。

4. 将装置放入 48.26 cm (19 英寸) 机架中，确保设备上的机架安装孔与机架上的安装孔对齐。

5. 用机架螺钉（未提供）将装置固定到机架中。先拧紧下部的一对螺钉，然后再拧紧上部的一对螺钉。请确保通风孔未被堵塞。

在平面上安装

如果设备不安装在机架中，则必须安装在平面上。此平面必须能够支持设备和设备电缆的重量。

1. 将自粘橡皮垫连接至机箱底部各个带标记的位置。

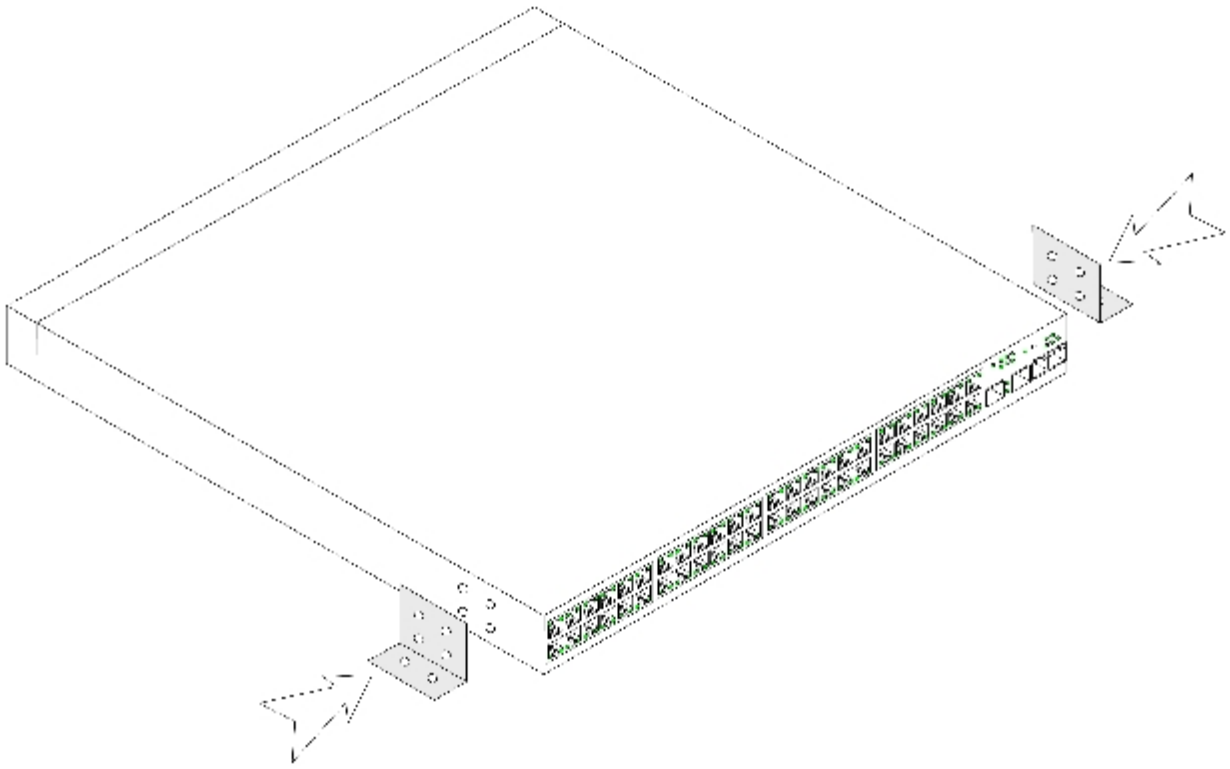
2. 将设备放置在平面上，在两侧各留出 5.08 cm（2 英寸）的空间，并在背面留出 12.7 cm（5 英寸）的空间。

3. 确保设备能够正常通风。

将设备安装在墙上

1. 将附带的墙固定支架放在设备的一侧，确保设备上的安装孔与机架固定支架上的安装孔对齐。下图说明了安装支架的位置。

图 3-2. 用于墙上安装的支架安装



2. 将附带的螺钉插入机架安装孔，并用螺丝刀拧紧。

3. 重复此过程，以安装设备另一侧的墙固定支架。

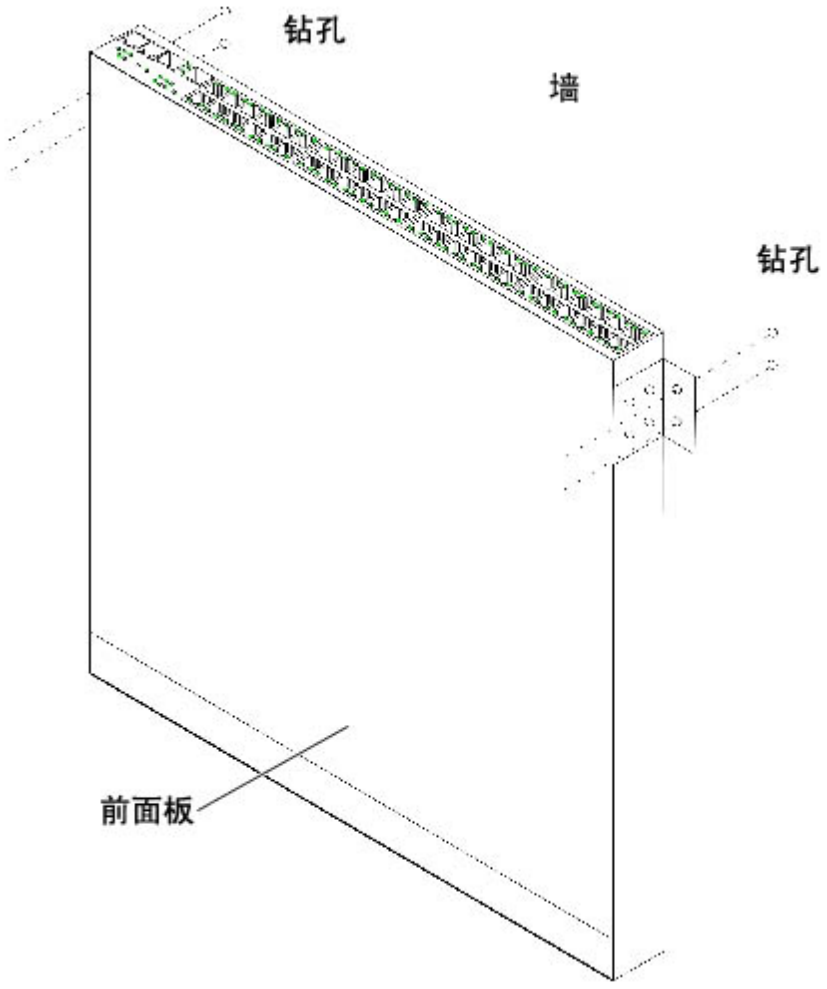
4. 将设备放在墙上打算安装设备的位置。

5. 在墙上标记出为固定设备而必须准备的螺钉的位置。

6. 在标记的位置钻孔并将所有插头（未提供）放入孔中。

7. 用螺钉（未提供）将装置固定到墙上。请确保通风孔未被堵塞。

图 3-3. 将设备安装在墙上



连接至终端

1. 将 RS-232 绞接电缆连接至 ASCII 终端或运行终端仿真软件的台式机系统的串行连接器。

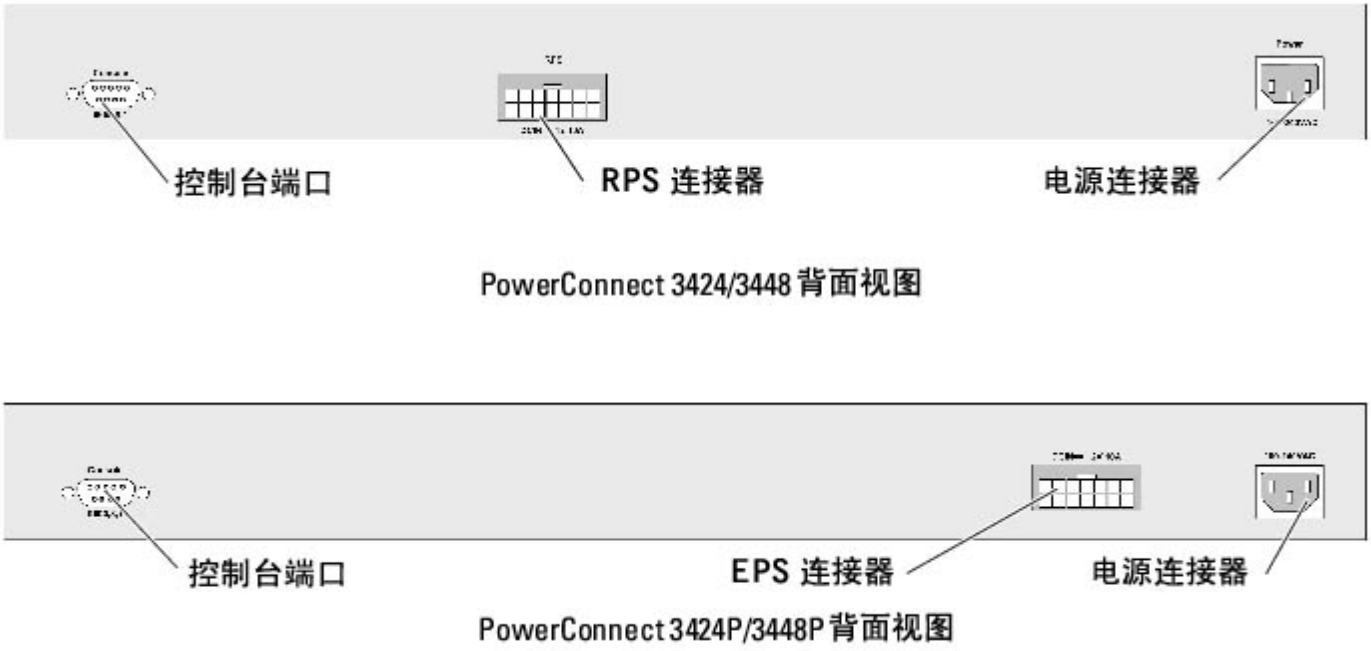
2. 将电缆另一端的 DB-9 内孔连接器连接至设备串行端口连接器。

将设备连接至电源设备

将附带的交流电源电缆连接至背面板上的交流电源连接器。

注：此时不要将电源电缆连接至接地的交流电源插座。请按照“启动和配置设备”中的详细步骤将设备连接至电源。

图 3-4. 背面板电源连接器



将设备连接至电源后，请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。

安装堆栈

概览

每个设备均可作为独立设备运行，也可作为堆栈中的成员。每个堆栈最多支持六个设备或 192 个端口。

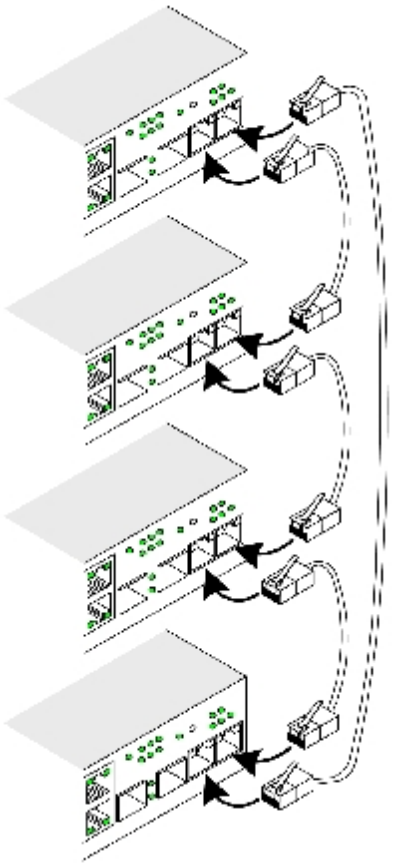
所有堆栈必须具有主装置，并且可能具有备份主装置，而连接至堆栈的任何其它设备则作为成员。

堆栈 PowerConnect 3400 系列交换机

每个 PowerConnect 3400 系列堆栈均具有一个主装置，可能还具有备份主装置，而其余装置则作为堆栈成员。

PowerConnect 3400 系列交换机将 RJ-45 吉位以太网端口 (G3 和 G4) 用于堆栈。这使设备增添了堆栈功能，而无需添加其它设备附件。要将设备堆栈在一起，请将标准 5 类电缆的一端插入堆栈中最顶部设备的端口 G3，并将另一端插入堆栈中该设备下方紧邻着它的设备的端口 G4。重复此过程，直到已连接所有设备。将堆栈中最底部设备的端口 G3 连接至堆栈中最顶部设备的端口 G4。

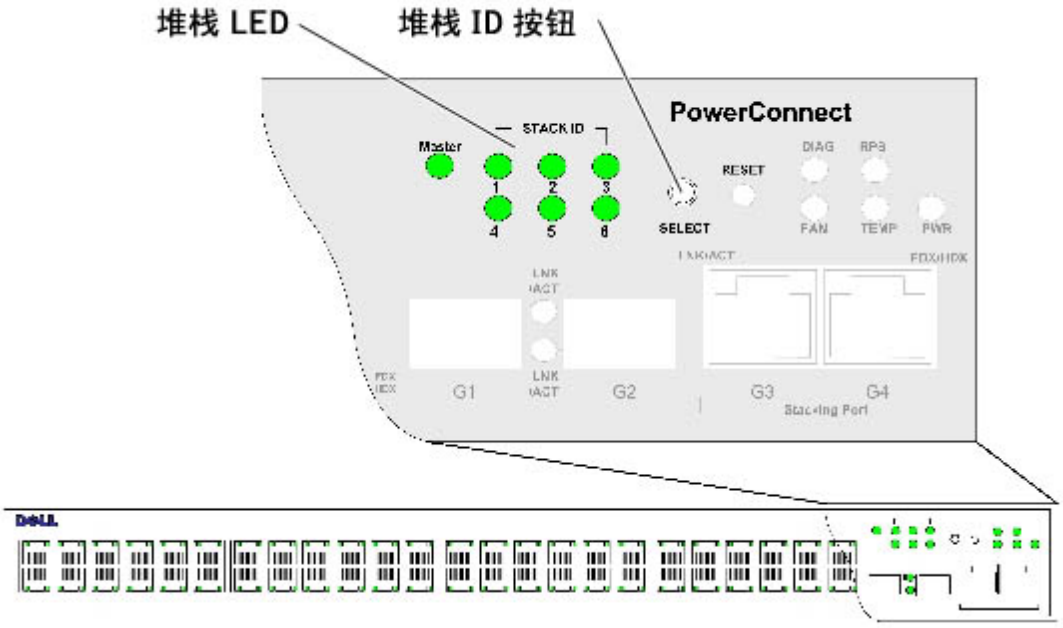
图 3-5. 堆栈电缆图



注：在堆栈模式中，指定为 G3 和 G4 的端口不会显示在 EWS 中。设备上不存在此效果。这是因为端口接收了堆栈的不同索引。

使用堆栈 ID 按钮在设备前面板上执行堆栈装置标识。

图 3-6. 堆栈配置和标识面板



每个堆栈设备均具有用于定义堆栈中装置的位置和功能的唯一标识装置 ID。如果设备为独立装置，则堆栈 LED 不亮。默认设置为独立。

装置 ID 是使用堆栈 ID 按钮手动配置的。装置 ID 由堆栈 ID LED 表明。装置 ID 1 和 2 专用于主装置和备份主装置，装置 ID 3 至 6 用于成员装置。

装置 ID 选择过程

装置 ID 选择过程如下所示：

1. 请确保已通过 RS-232 绞接电缆将独立/主装置设备控制台端口连接至 VT100 终端设备或 VT100 终端仿真器。
2. 找到交流电源插座。
3. 取消激活交流电源插座。
4. 将设备连接至交流电源插座。
5. 激活交流电源插座。

   通电时，配置的 LED 编号（对应于先前保存的装置 ID）将开始闪烁。LED 将闪烁 15 秒。在此期间，通过按堆栈 ID 按钮直到亮起相应的堆栈 ID LED 来选择特定的堆栈 ID。

6. 选择过程 — 要增大堆栈 ID LED 编号，请继续按堆栈 ID 按钮。当 LED 6 闪烁时，按堆栈 ID 按钮会将设备配置为独立设备。再次按堆

栈 ID 按钮可将堆栈 ID 提高至 1。装置 1 和装置 2 为启用主装置的装置。有关主装置选择过程的信息，请参阅“堆栈概览”。

7. 结束选择过程 — 15 秒的闪烁时间过后，将完成装置 ID 选择过程。该时段结束时，堆栈 ID 按钮将不起作用，装置 ID 将设置为 LED ID 闪烁所对应的值。

注：一次应针对一个装置执行这些步骤，直到所有堆栈成员均通电，并且已选择它们的堆栈 ID。一次针对一个装置执行这些步骤可以允许有足够的时间为每个装置选择堆栈 ID。但是，在给设备通电之前，应按照“堆栈电缆图”使用电缆连接整个堆栈。

启动和配置设备

完成所有外部连接之后，请将终端连接至设备以配置设备。“高级配置”一节中介绍了如何执行其它高级功能。

注：继续操作之前，请阅读该产品的版本注释。可以从 Dell 支持 Web 站点 support.dell.com 下载版本注释。

注：建议您从 Dell 支持 Web 站点 support.dell.com 获取用户说明文件的最新版本。

连接至设备

要配置设备，必须将设备连接至控制台。但是，如果设备是堆栈的一部分，仅堆栈中名为主装置的那个设备需要连接至终端。因为堆栈作为单个设备运行，仅配置主装置。

将终端连接至设备

设备提供了控制台端口，可以连接至运行终端仿真软件的终端台式机系统，以监测和配置设备。控制台端口连接器为 DB-9 插头连接器，用作连接数据终端设备 (DTE) 的连接器。

要使用控制台端口，需要满足以下要求：

- VT100 兼容终端，或者配备串行端口并运行 VT100 终端仿真软件的台式机或便携式系统
- 一根 RS-232 绞接电缆，其 DB-9 内孔连接器用于连接控制台端口，相应的连接器用于连接终端

要将终端连接至设备控制台端口，请：

1. 将附带的 RS-232 绞接电缆连接至运行 VT100 终端仿真软件的终端。

2. 选择相应的串行端口（串行端口 1 或串行端口 2），以连接至控制台。

3. 将数据速率设置为 9600 波特。

4. 将数据格式设置为 8 个数据位、1 个停止位以及无奇偶校验。

5. 将流控制设置为无。

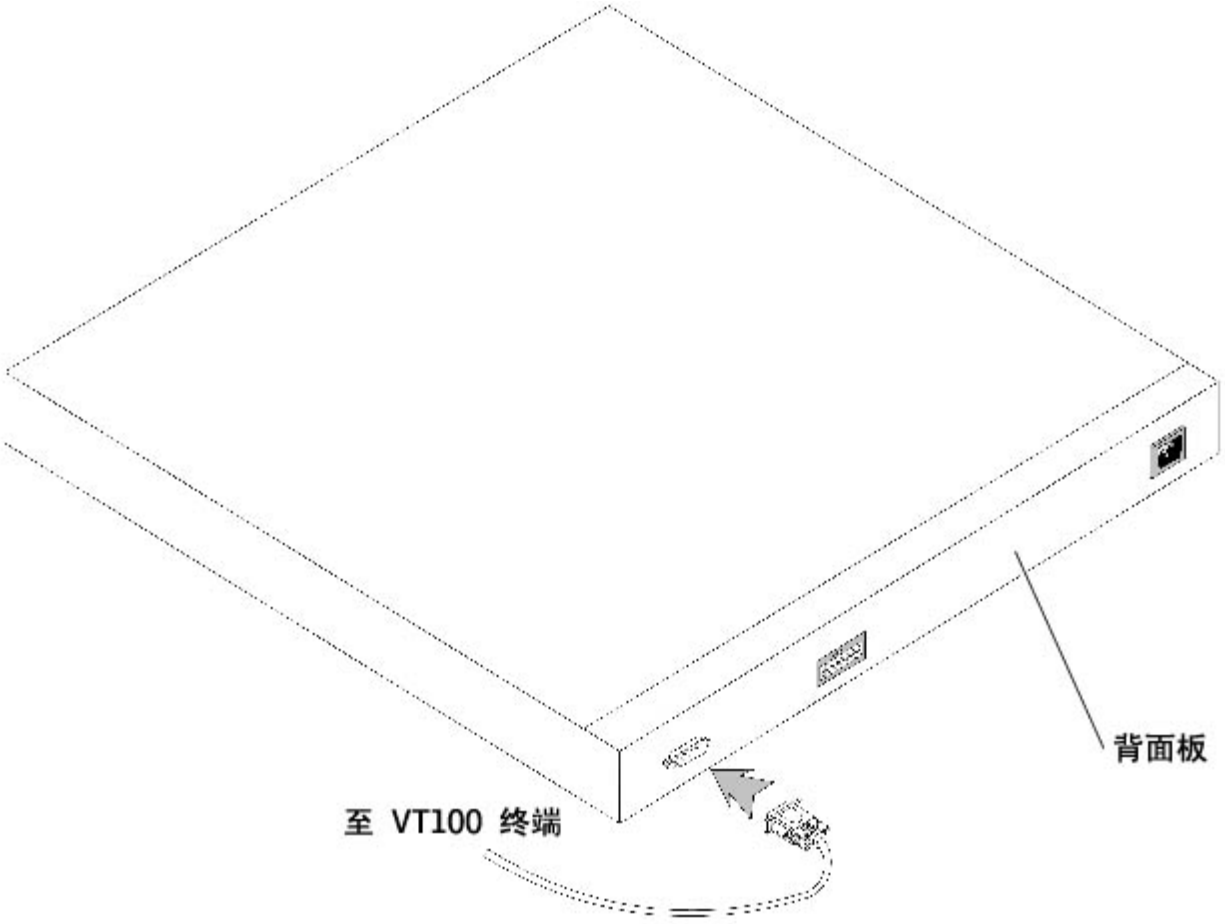
6. 在“Properties”（属性）下，选择“VT100 for Emulation”（VT100 仿真）模式。

7. 选择“Terminal keys”（终端键）作为“Function, Arrow, and Ctrl keys”（功能键、箭头键和 Ctrl 键用作）的设置。确保此设置为“Terminal keys”（终端键）（而不是“Windows keys”[Windows 键]）。

注意：在 Microsoft® Windows® 2000 中使用超级终端时，请确保已安装 Windows 2000 Service Pack 2 或更高版本。使用 Windows 2000 Service Pack 2 可以确保超级终端的 VT100 仿真中的箭头键正常工作。有关 Windows 2000 Service Pack 的信息，请访问 www.microsoft.com。

8. 将 RS-232 绞接电缆的内孔连接器直接连接至主装置/独立设备上的设备控制台端口，并拧紧固定螺钉。PowerConnect 3400 系列控制台端口位于背面板上。

图 3-7. 连接至 PowerConnect 3400 系列控制台端口



注：控制台可以连接至堆栈中任一装置上的控制台端口，但是，仅从堆栈主装置（装置 ID 1 或 2）执行堆栈管理。

返回目录页面

返回目录页面

配置 PowerConnect 3424/P 和 3448/P

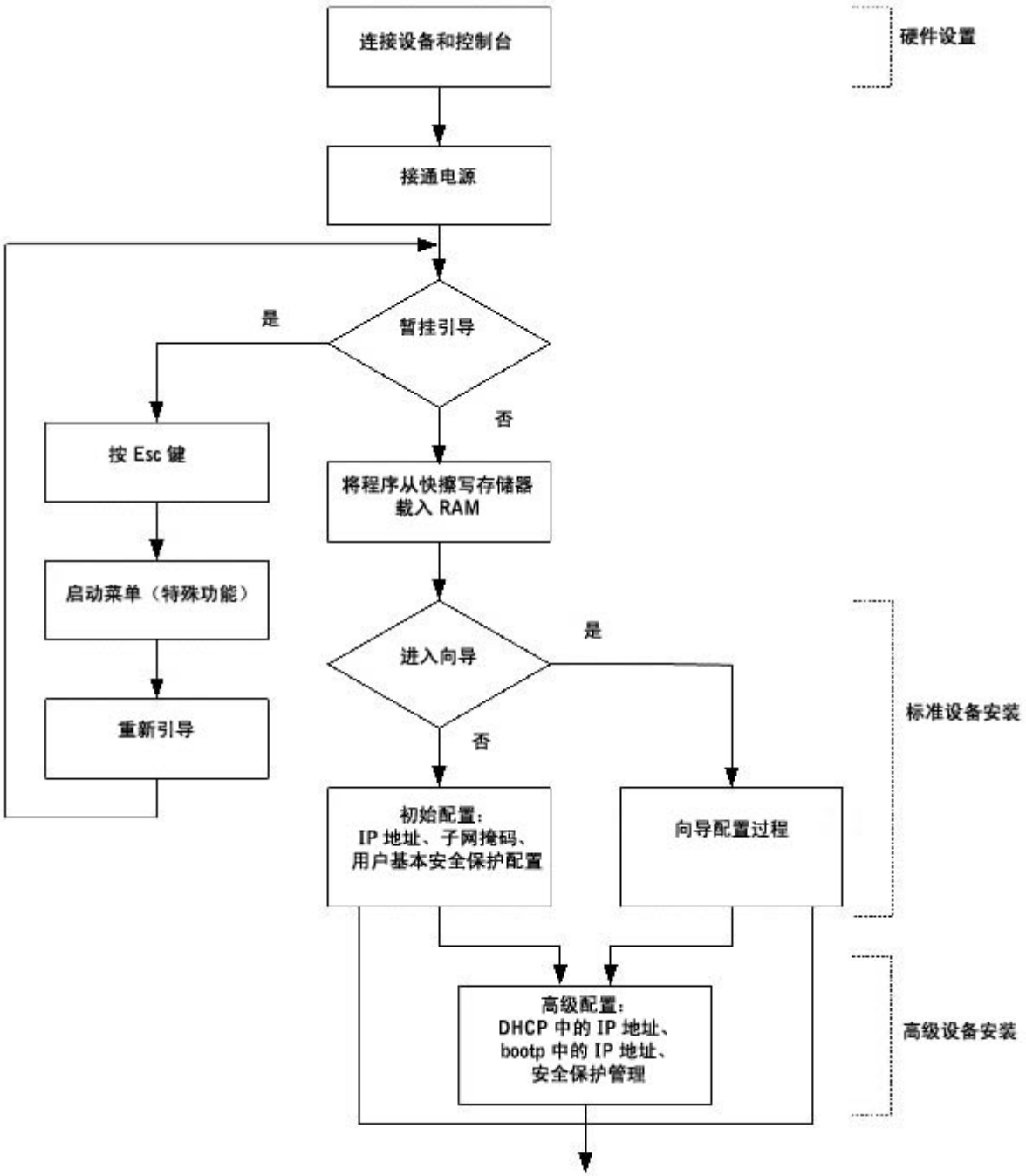
Dell™ PowerConnect™ 34XX 系统用户指南

配置程序

完成所有设备外部连接之后，请将终端连接至设备以监测引导及其它过程。安装和配置过程的顺序如下图所示：

注：继续操作之前，请阅读该产品的版本注释。可以从 support.dell.com 下载该产品的版本注释。

图 4-1. 安装和配置流程



引导交换机

当电源打开并已连接了本地终端时，交换机将进行开机自测（POST）。POST 在每次设备进行初始化时运行，它会检查硬件组件，以确定设备是否完全运行，然后再完全引导设备。如果检测到严重问题，程序流将停止。如果 POST 成功完成，有效的可执行映像将被载入到 RAM 中。终端上将显示 POST 信息，表明检测成功或失败。

此引导进程大约运行 30 秒钟。

初始配置

注：继续操作之前，请阅读该产品的版本注释。可以从 Dell 支持 Web 站点 support.dell.com 下载该产品的版本注释。

注：初始配置假定了以下内容：

- PowerConnect 设备以前从未进行过配置，其状态与收到该设备时的状态相同。
- PowerConnect 设备已成功引导。
- 控制台连接已建立，并且控制台提示符已显示在 VT100 终端设备的屏幕上。

初始设备配置通过控制台端口进行。初始配置之后，可以从已连接的控制台端口对设备进行管理，也可以通过在初始配置期间定义的界面来对设备进行远程管理。

如果是第一次引导设备，或者由于尚未对设备进行配置而使配置文件为空，系统将提示用户使用设置向导。设置向导将引导用户完成初始设备配置，并启动设备使之以尽可能快的速度运行。

注：配置设备之前，请从网络管理员处获取以下信息：

- 要分配给 VLAN 1 接口的 IP 地址，设备通过此接口进行管理（默认情况下，每个端口都是 VLAN 1 的成员）
- 网络的 IP 子网掩码
- 用于配置默认路由的默认网关（下一路程段路由器）IP 地址。
- SNMP 团体字符串和 SNMP 管理系统 IP 地址（可选）
- 用户名和密码

设置向导将引导您完成初始交换机配置，并启动系统使之以尽可能快的速度运行。您可以跳过此设置向导，而通过设备 CLI 模式手动配置设备。

通过设置向导可以配置以下字段。

- SNMP 团体字符串和 SNMP 管理系统 IP 地址（可选）
- 用户名和密码

设备 IP 地址

- 默认网关 IP 地址

系统将显示以下信息：

Welcome to Dell Easy Setup Wizard（欢迎使用 Dell 简易设置向导）

The Setup Wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible.You can skip the setup wizard, and enter CLI mode to manually configure the switch.（此设置向导将引导您完成初始交换机配置，并启动系统使之以尽可能快的速度运行。您可以跳过此设置向导而进入 CLI 模式手动配置交换机。）
The system will prompt you with a default answer; by pressing enter, you accept the default.（系统将出现提示并附有默认答案；可以按 enter 键接受此默认值。）
You must respond to the next question to run the setup wizard within 60 seconds, otherwise the system will continue with normal operation using the default system configuration.（您必须在 60 秒内回答下一个问题以运行设置向导，否则系统将使用默认系统配置继续正常运行。）

Would you like to enter the Setup Wizard (you must answer this question within 60 seconds? (Y/N)[Y]Y（您要进入设置向导吗？ [您必须在 60 秒内回答此问题。] (Y/N)[Y]Y）
You can exit the Setup Wizard at any time by entering [ctrl+Z].（您可以通过输入 [ctrl+Z] 随时退出设置向导。）

如果您输入 [N]，则将退出此设置向导。如果您未在 60 秒内作出回答，将自动退出设置向导并且系统将显示 CLI 控制台提示符。

如果您输入 [Y]，设置向导将为您提供交互式引导，以完成初始设备配置。

注：如果未在 60 秒内作出回答，并且网络中存在 BootP 服务器，则系统将从 BootP 服务器检索地址。

注：您可以通过输入 [ctrl+Z] 随时退出设置向导。

向导步骤 1

系统将显示以下信息：

The system is not setup for SNMP management by default.（默认情况下，系统设置不能用于 SNMP 管理。）
To manage the switch using SNMP (required for Dell Network Manager) you can（要使用 SNMP [Dell 网络管理员所需] 管理交换机，您可以）

- Setup the initial SNMP version 2 account now.（立即设置初始 SNMP 版本 2 帐户。）
- Return later and setup additional SNMP v1/v3 accounts.（随后返回，再设置 SNMP v1/v3 帐户。）

For more information on setting up SNMP accounts, please see the user documentation.（有关设置 SNMP 帐户的详细信息，请参阅用户说明文件。）

Would you like to setup the SNMP management interface now? (Y/N)[Y]Y（您要立即设置 SNMP 管理界面吗？(Y/N)[Y]Y）

输入 [N] 将跳到步骤 2。

输入 [Y] 将继续执行此设置向导。系统将显示以下信息：

```
To setup 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.（要设置 SNMP 管理帐户，您必须指定管理系统 IP 地址以及特定管理系统用来访问交换机的团体字符串或密码。向导将自动为此帐户分配最高访问级别 [权限级别 15]。）
You can use Dell Network Manager or CLI to change this setting, and to add additional management systems.For more information on adding management systems, see the user documentation.（您可以使用 Dell 网络管理员或 CLI 更改此设置或添加其它管理系统。有关添加管理系统的详细信息，请参阅用户说明文件。）
To add a management station:（要添加管理站点，请：）
Please enter the SNMP community string to be used:[Dell_Network_Manager]（输入要使用的 SNMP 团体字符串：[Dell_Network_Manager]）
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]（输入管理系统的 IP 地址 (A.B.C.D) 或可以从任何管理站点进行管理的通配符 (0.0.0.0)：[0.0.0.0]）
```

输入以下内容：

- SNMP 团体字符串，例如 Dell_Network_Manager。
- 管理系统的 IP 地址 (A.B.C.D)，或可以从任何管理站点进行管理的通配符 (0.0.0.0)。

注：不能使用以零开头的 IP 地址和掩码。

按 Enter 键。

向导步骤 2

系统将显示以下信息：

```
Now we need to setup your initial privilege (Level 15) user account.（现在需要设置您的初始权限 [级别 15] 用户帐户。）
This account is used to login to the CLI and Web interface.（此帐户用于登录 CLI 和 Web 界面。）
You may setup other accounts and change privilege levels later.（您可以在以后设置其他帐户和更改权限级别。）
For more information on setting up user accounts and changing privilege levels, see the user documentation.（有关设置用户帐户和更改权限级别的详细信息，请参阅用户说明文件。）
To setup a user account:（要设置用户帐户，请：）
Enter the user name<1-20>:[admin]（输入用户名<1 至 20 个字符>：[admin]）
Please enter the user password:*（输入用户密码：*）
Please reenter the user password:*（再次输入用户密码：*）
```

输入以下内容：

- 用户名，例如“admin”
- 密码和确认密码。

注：如果第一次输入的密码与第二次的确认密码不相同，系统将提示您重新输入直至二者相同。

按 Enter 键。

向导步骤 3

系统将显示以下信息：

```
Next, an IP address is setup. (下一步，设置 IP 地址。)

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.To setup an IP address: (IP 地址将定义在所有端口均是其成员的默认 VLAN (VLAN #1) 上。此 IP 地址用于访问 CLI、Web 界面或交换机的 SNMP 界面。要设置 IP 地址：请)

Please enter the IP address of the device (A.B.C.D):[1.1.1.1] (输入设备的 IP 地址 (A.B.C.D)：[1.1.1.1])

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

输入 IP 地址和 IP 子网掩码，例如 IP 地址为 1.1.1.1，IP 子网掩码为 255.255.255.0。

按 Enter 键。

向导步骤 4

系统将显示以下信息：

```
Finally, setup the default gateway. (最后，设置默认网关。)
Please enter the IP address of the gateway from which this network is reachable (e.g. 192.168.1.1).Default gateway (A.B.C.D):[0.0.0.0] (请输入网关的 IP 地址，通过它可以访问此网络 [例如 192.168.1.1]。默认网关 (A.B.C.D)：[0.0.0.0])
```

输入默认网关。

按 Enter 键。系统将显示以下信息（按照所述的示例参数）：

```
This is the configuration information that has been collected: (已收集的配置信息如下：)

================================================================

SNMP Interface = Dell_Network_Manager@0.0.0.0
User Account setup = admin
Password = *
Management IP address = 1.1.1.1 255.255.255.0
Default Gateway = 1.1.1.2

================================================================
```

向导步骤 5

系统将显示以下信息：

```
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:(Y/N)[Y]Y（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中。如果信息不正确，请选择 (N) 清除配置并重新启动向导：(Y/N)[Y]Y）
```

输入 [N] 将重新启动设置向导。

输入 [Y] 将完成设置向导。系统将显示以下信息：

```
Configuring SNMP management interface（正在配置 SNMP 管理界面）
Configuring user account...... （正在配置用户帐户.....）
Configuring IP and subnet...... （正在配置 IP 和子网.....）

Thank you for using Dell Easy Setup Wizard.You will now enter CLI mode.（感谢使用 Dell 简易设置向导。现在，您将进入 CLI 模式。）
```

向导步骤 6

系统将显示 CLI 提示符。

高级配置

本节介绍了有关 IP 地址的动态分配和基于验证、授权和计费 (AAA) 机制的安全保护管理的信息，包括以下主题：

- 通过 DHCP 配置 IP 地址
- 通过 BOOTP 配置 IP 地址
- 安全保护管理和密码配置

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。

从 DHCP 服务器检索 IP 地址

使用 DHCP 协议检索 IP 地址时，此设备用作 DHCP 客户端。重启动设备时，DHCP 命令保存在配置文件中（不包括 IP 地址）。要从 DHCP 服务器检索 IP 地址，请执行以下步骤：

1. 选择并连接 DHCP 服务器的任何端口或具有 DHCP 服务器的子网的任何端口，以便检索 IP 地址。

2. 输入以下命令，以使用选定的端口来获取 IP 地址。在以下示例中，命令基于配置中使用的端口类型。

   - 分配动态 IP 地址：

```
console# configure
console(config)# interface ethernet 1/e1
console(config-if)# ip address dhcp hostname powerconnect
console(config-if)# exit
console(config)#
```

   - 分配动态 IP 地址（在 VLAN 上）：

```
console# configure
console(config)# interface ethernet vlan 1
console(config-if)# ip address dhcp hostname device
console(config-if)# exit
console(config)#
```

   接口将自动获取 IP 地址。

3. 要验证 IP 地址，请在系统提示符后输入 show ip interface 命令，如以下示例所示。

```
console# show ip interface
IP Address I/F Type
-------------- ------ -------
100.1.1.1/24 vlan 1 dynamic
```

注：要为 DHCP 服务器检索 IP 地址，没有必要删除设备配置。

注：复制配置文件时，请避免使用包含以下说明的配置文件，该说明指出在连接至同一 DHCP 服务器（或具有相同配置的服务器）的接口上启用 DHCP。在此实例中，设备检索到新的配置文件并从中进行引导。然后，设备将按照新配置文件中的命令启用 DHCP，DHCP 将命令该设备再次重新加载相同的文件。

注：如果要配置 DHCP IP 地址，系统将动态检索该地址，并且 `ip address dhcp` 命令将保存在配置文件中。如果主配置失败，备份配

置将再次尝试检索 DHCP 地址。这可能导致以下结果之一：

- 分配了相同的 IP 地址。
- 分配了不同的 IP 地址，但可能导致丢失与管理站点的连接。
- DHCP 服务器可能关闭，从而导致 IP 地址检索失败或可能丢失与管理站点的连接。

从 BOOTP 服务器获取 IP 地址

设备支持标准 BOOTP 协议，该协议使设备可以从网络中的任何标准 BOOTP 服务器自动下载其 IP 主机配置。在这种情况下，此设备用作 BOOTP 客户端。

要从 BOOTP 服务器检索 IP 地址，请：

1. 选择任一端口并将其连接至 BOOTP 服务器或包含此类服务器的子网，以检索 IP 地址。
2. 在系统提示符后，输入 delete startup configuration 命令，以从快擦写存储器中删除启动配置。

设备会在未进行配置的情况下重新引导，并在 60 秒钟内开始发送 BOOTP 请求。设备将自动获取 IP 地址。

注：设备重新引导开始时，通过在 ASCII 终端或键盘输入任何内容均可以在 BOOTP 过程完成之前自动取消该过程，设备不会从 BOOTP 服务器获取 IP 地址。

以下示例说明了此过程：

```
console> enable

console# delete startup-config

Startup file was deleted

console# reload

You haven't saved your changes.Are you sure you want to continue (y/n) [n]?

This command will reset the whole system and disconnect your current session.Do you want to continue
(y/n) [n]?

*************************************************

/* the device reboots */
```

要验证此 IP 地址，请输入 show ip interface 命令。

此设备现已配置了 IP 地址。

安全保护管理和密码配置

系统安全保护是通过验证、授权和计费（AAA）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“Startup”（启动）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设备。

配置安全保护密码

您可以为以下服务配置安全保护密码：

- 终端
- Telnet
- SSH
- HTTP
- HTTPS

注：密码由用户定义。

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。必须设置为优先级 15 才能启用对设备的访问权限和配置权限。虽然可以为用户名分配优先级 15（不使用密码），但建议您始终指定密码。如果没有指定的密码，则具有权限的用户可以使用任何密码访问 Web 界面。

注：可以使用密码管理命令强制密码过期或使用密码过期设置来保护密码。有关详情，请参阅“安全保护管理和密码配置”。

配置初始终端密码

要配置初始终端密码，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 george
```

- 通过终端会话首次登录设备时，请在密码提示符后输入 `george`。
- 将设备的模式更改为启用时，请在密码提示符后输入 `george`。

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 bob
```

- 通过 Telnet 会话首次登录设备时，请在密码提示符后输入 `bob` 。
- 将设备模式更改为启用时，请输入 `bob`。

配置初始 SSH 密码

要配置初始 SSH 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 ssh

console(config-line)# login authentication default

console(config-line)# enable authentication default

console(config-line)# password jones.
```

- 通过 SSH 会话首次登录设备时，请在密码提示符后输入 jones。
- 将设备的模式更改为启用时，请输入 jones。

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 user1 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

console(config)# username admin password user1 level 15
```

配置为使用终端、Telnet 或 SSH 会话以便使用 HTTPS 会话时，只需一次性输入以下命令。

注：在 Web 浏览器中，为要显示的页面内容启用 SSL 2.0 或更高版本。

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

console(config)# ip https server
```

首次启用 HTTP 或 HTTPS 会话时，请输入 admin 作为用户名，并输入 user1 作为密码。

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。

启动程序

“Startup”（启动）菜单程序

从“Startup”（启动）菜单调用的程序包括软件下载、快擦写处理和密码恢复。仅有技术支持人员可以使用诊断程序，并且诊断程序未在本说明文件中公开。

可以在引导设备时进入“Startup”（启动）菜单。在 POST 检测之后必须立即输入用户输入。

要进入“Startup”（启动）菜单，请：

1. 打开电源并等待自动引导信息。

```
************************************************

***************** SYSTEM RESET *****************

************************************************

Boot1 Checksum Test.............................PASS

Boot2 Checksum Test.............................PASS

Flash Image Validation Test.....................PASS

BOOT Software Version 1.0.0.05 Built 06-Jan-2005 14:46:49

Carrier board, based on PPC8247

128 MByte SDRAM.I-Cache 16 KB.D-Cache 16 KB.Cache Enabled.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

2. 显示自动引导信息时，按 <Enter> 键进入“Startup”（启动）菜单。“Startup”（启动）菜单程序可以通过使用 ASCII 终端或 Windows 超级终端来完成。

```
[1] Download Software

[2] Erase Flash File

[3] Password Recovery Procedure
```

```
[4] Enter Diagnostic Mode

[5] Set Terminal Baud-Rate

[6] Back
```

以下各节将介绍可用的“Startup”（启动）菜单选项。

注：从“Startup”（启动）菜单中选择选项时，必须考虑到超时：如果在 35 秒钟（默认值）内未作出选择，则设备将超时。可以通过 CLI 更改此默认值。

注：只有技术支持人员可以运行诊断模式（选项 [4]）。因此，本指南中并不介绍进入诊断模式。

下载软件 – 选项 [1]

当必须下载新版本以替换损坏的文件、更新或升级系统软件时，请执行软件下载程序。要从“Startup”（启动）菜单下载软件，请：

1. 在“Startup”（启动）菜单中，按 [1] 键。系统将显示以下提示：

```
Downloading code using XMODEM

****************************************************************

*** Running SW Ver.1.0.0.30 Date 09-Jan-2005 Time 14:30:02

****************************************************************

HW version is

Base Mac address is:00:00:b0:45:54:00

Dram size is :128M bytes

Dram first block size is :36864K bytes

Dram first PTR is :0x1C00000

Flash size is:16M

Loading running configuration.

Number of configuration items loaded: 5

Loading startup configuration.

Number of configuration items loaded: 5

Device configuration:
```

```
Slot 1 - PowerConnect 3424 HW Rev. 0.0

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

-- Unit Number 1 Standalone --

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

BOXP_high_appl_init:dpssIpcInitStandAlone

Tapi Version:v1.3.1.6P_01_03

Core Version:v1.3.1.6P_01_02

01-Jan-2000 01:01:19 %INIT-I-InitCompleted:Initialization task is completed

01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG:FAN# 1 status changed - operational.

01-Jan-2000 01:01:19 %Entity-I-SEND-ENT-CONF-CHANGE-TRAP:entity configuration change trap.

01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG:FAN# 2 status changed - operational.

01-Jan-2000 01:01:19 %Box-I-PS-STAT-CHNG:PS# 1 status changed - operational.
```

2. 使用超级终端时，单击超级终端菜单栏上的“Transfer”（传输）。

3. 在“Filename”（文件名）字段中，输入要下载的文件的文件路径。

4. 确保在“Protocol”（协议）字段中已选择 Xmodem 协议。

5. 按“Send”（发送）。软件将被下载。

注：软件下载之后，设备将自动重新启动。

清除快擦写文件 – 选项 [2]

某些情况下，必须删除设备配置。如果配置被删除，则必须重新配置通过 CLI、EWS 或 SNMP 配置的所有参数。

要删除设备配置，请：

1. 在“Startup”（启动）菜单中，在两秒钟内按 [2] 键以删除快擦写文件。系统将显示以下信息：

```
Warning!About to erase a Flash file.

Are you sure (Y/N)? y
```

2. 按 Y 键。系统将显示以下信息。

```
Write Flash file name (Up to 8 characters, Enter for none.):config

File config (if present) will be erased after system initialization

======== Press Enter To Continue ========
```

3. 输入 config 作为快擦写文件的名称。配置被删除，设备将重新引导。

4. 重复设备初始配置。

密码恢复 – 选项 [3]

如果密码丢失，可以从“Startup”（启动）菜单调用密码恢复程序。该程序允许您对设备进行一次性访问，无需使用密码。

要仅为本地终端恢复丢失的密码，请：

1. 在“Startup”（启动）菜单中，键入 [3] 并按 <Enter> 键。密码被删除。

输入您的选择或按 'ESC' 键退出：

当前密码将被忽略！

注：要确保设备安全，请重新配置适用的管理方法的密码。

进入诊断模式 – 选项 [4]

仅用于技术支持。

设置终端波特率 – 选项 [5]

要设置终端波特率，请键入 [5] 并按 <Enter> 键。

输入您的选择或按 'ESC' 键退出：

设置新设备波特率： 38,400

通过 TFTP 服务器下载软件

本节包含通过 TFTP 服务器下载设备软件（系统和引导映像）的说明。下载软件之前，必须先配置 TFTP 服务器。

系统映像下载

从存储系统映像副本的快擦写存储区域解压缩系统映像时，设备将引导并运行。下载新的映像之后，该映像将被保存在分配给其它系统映像副本的另一个区域中。

除非选择其它映像，否则，下次引导时，设备将解压缩并运行当前的活动系统映像。

要通过 TFTP 服务器下载系统映像，请：

1. 确保已在其中一个设备端口上配置 IP 地址，并且可以将 ping 发送至 TFTP 服务器。
2. 确保要下载的文件已保存在 TFTP 服务器上（arc 文件）。
3. 输入 show version 命令以验证设备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
SW version 1.0.0.30 (date 27-Jan-2005 time 13:42:41)
Boot version 1.0.0.05 (date 27-Jan-2005 time 15:12:20)
HW version
```

4. 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
Images currently available on the Flash
Image-1 active (selected for next boot)
Image-2 not active
console#
```

5. 输入 copy tftp://{tftp address}/{file name} image 命令，以将新的系统映像复制到设备。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（image-2，如示例中所示）。以下是一个信息显示示例：

```
console# copy tftp://176.215.31.3/file1.ros image

Accessing file `file1' on 176.215.31.3:

Loading file1 from 176.215.31.3:

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy took 00:01:11 [hh:mm:ss]
```

感叹号表示复制过程正在进行。每个感叹号 (!) 对应于已成功传输的 512 个字节。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。

6. 通过输入引导系统命令来为下一个引导选择映像。然后，输入 show bootvar 命令，以验证是否已为下一次引导选择了一个副本，此副本表示为 boot system 命令中的参数。

以下是一个信息显示示例：

```
console# boot system image-2

console# show bootvar

Images currently available on the Flash

Image-1 active

Image-2 not active (selected for next boot)
```

如果未通过输入 boot system 命令选择下一次引导的映像，则系统将从当前活动映像进行引导。

7. 输入 reload 命令。系统将显示以下信息：

```
console# reload

This command will reset the whole system and disconnect your current session.Do you want to continue
(y/n)[n]?
```

8. 输入 y。设备将重新引导。

引导映像下载

从 TFTP 服务器载入一个新的引导映像，并将其编程至快擦写存储器，以更新引导映像。当设备通电时，将载入引导映像。用户无法控制引导映像副本。要通过 TFTP 服务器下载引导映像，请：

1. 确保已在其中一个设备端口上配置 IP 地址，并且可以将 ping 发送至 TFTP 服务器。

2. 确保要下载的文件已保存在 TFTP 服务器上（rfb 文件）。

3. 输入 show version 命令以验证设备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

SW version 1.0.0.30 (date 27-Jan-2005 time 13:42:41)

Boot version 1.0.0.05 (date 27-Jan-2005 time 15:12:20)

HW version
```

4. 输入 copy tftp://{tftp address}/{file name} boot 命令，以将引导映像复制到设备。以下是一个信息显示示例：

```
console# copy tftp://176.215.31.3/332448-10018.rfb boot

Erasing file..done.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy: 2739187 bytes copied in 00:01:13 [hh:mm:ss]
```

5. 输入 reload 命令。系统将显示以下信息：

```
console# reload

This command will reset the whole system and disconnect your current session.Do you want to continue
(y/n)[n]?
```

6. 输入 y。设备将重新引导。

端口默认设置

配置设备端口的一般信息包括对自适应机制的简短说明和交换端口的默认设置。

自适应

自适应在所有交换 10/100/1000BaseT 端口上启用了对速率、双工模式和流控制的自动检测。默认情况下，各个端口均启用了自适应。

自适应是在两个链接伙伴之间建立的一种机制，这种机制使一个端口可以将其传输速率、双工模式和流控制（默认情况下，流控制处于禁用状态）能力通知到伙伴端口。然后两个端口以二者之间的最高共同标准运行。

如果连接的 NIC 不支持自适应或者未被设置为自适应，则必须将设备交换端口和 NIC 均手动设置为具有相同的速率和双工模式。

如果链路另一端的站点尝试与配置为全双工的设备 100BaseT 端口自适应，则自适应将导致此站点尝试以半双工运行。

MDI/MDIX

设置支持对所有交换 10/100/1000BaseT 端口上的直通电缆和绞接电缆进行自动检测。该功能是自适应的一部分，并在启用自适应时启用该功能。

启用了 MDI/MDIX（带有绞接电缆的介质相关接口）后，电缆选择中的错误自动纠正将可用，它将对直通电缆和不相关的绞接电缆进行区分。（终端站点的标准布线称为 MDI [介质相关接口]，集线器和交换机的标准布线称为 MDIX。）

流控制

设备支持对配置为全双工模式的端口启用 802.3x 流控制。默认情况下，此功能被禁用。可以在各个端口上启用此功能。流控制机制允许接收方向发送方发出信号，指出传输必须暂时停止以避免缓冲区溢出。

背压

设备支持对配置为半双工模式的端口启用背压。默认情况下，此功能被禁用。可以在各个端口上启用此功能。背压机制可以暂时防止发送者发送其它通信。接收者可能会占用链路，从而导致链路对其它通信不可用。

交换端口默认设置

下表介绍了端口的默认设置。

表 4-7. 端口默认设置

功能	默认设置
端口速率和模式	10/100BaseT 铜质端口：自适应 100 Mbps 全双工

	10/100/1000BaseT 铜质/SFP 端口：自适应 1000 Mbps 全双工
端口传输状态	已启用
端口标记	无标记
流控制	关闭（在入口被禁用）
背压	关闭（在入口被禁用）

返回目录页面

返回目录页面

使用 Dell OpenManage Switch Administrator

Dell™ PowerConnect™ 34XX 系统用户指南

本节介绍了 Dell OpenManage Switch Administrator 用户界面。

启动应用程序

注：启动应用程序之前，必须定义 IP 地址。有关详情，请参阅“初始配置”。

1. 打开 Web 浏览器。
2. 在地址栏中输入设备 IP 地址，并按 <Enter> 键。
3. 显示“Log In”（登录）窗口时，输入用户名和密码。

注：密码区分大小写，并且只能为字母数字。

4. 单击“OK”（确定）。

系统将显示“Dell OpenManage™ Switch Administrator”主页。

了解界面

主页包含以下视图：

- 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 — 位于主页右侧，提供了设备视图、信息或表区域和配置说明。

图 5-1. Switch Administrator 组件

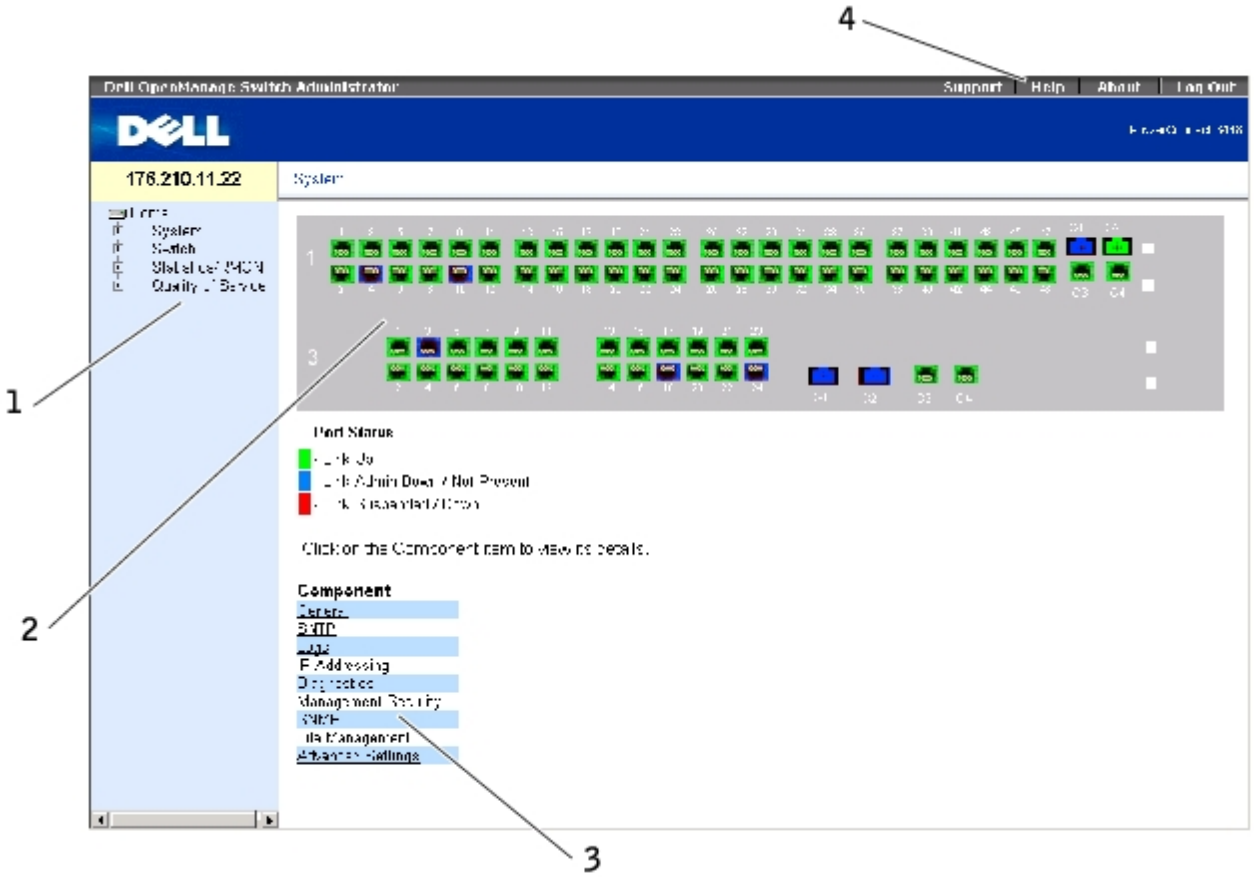


表 5-8 列出了界面组件及其相应的编号。

表 5-8. 界面组件

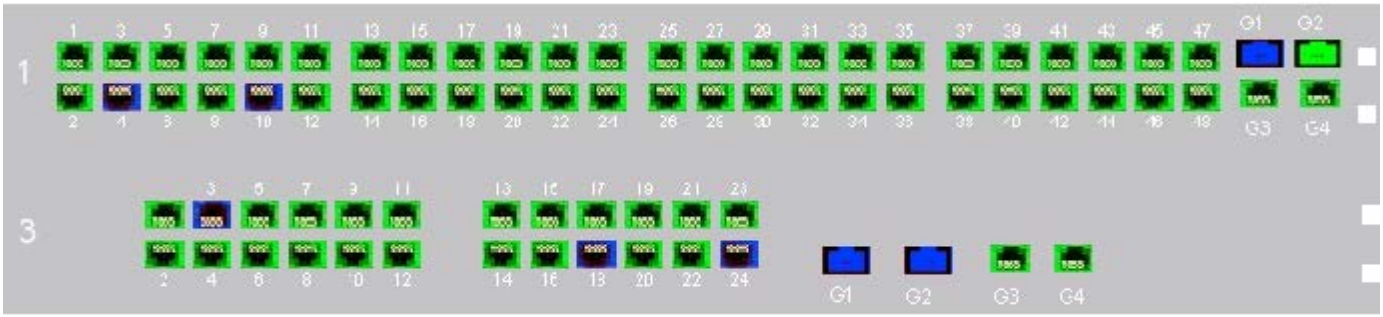
组件	说明
1	树视图包含各种设备功能的列表。可以展开树视图中的分支以查看特定功能下的所有组件，也可以折叠分支以隐藏功能组件。向右拖动垂直条，可以扩展树区域以显示组件的全名。
2	设备视图提供了有关设备端口、当前配置和状态、表信息和功能组件的信息。 根据选定的选项，设备视图底部的区域可以显示其它设备信息和/或配置参数的对话框。

3	组件列表包含功能组件的列表。也可以通过在树视图中展开功能来查看组件。
4	信息按钮使您可以访问有关设备的信息和 Dell 支持。有关详情，请参阅“信息按钮”。

设备图示

主页包含设备前面板的图示。

图 5-2. PowerConnect 设备端口指示灯



端口颜色表明特定端口当前是否处于活动状态。端口可以具有以下颜色：

表 5-9. PowerConnect 端口和堆栈指示灯

组件	说明
端口指示灯	
绿色	端口当前已启用。
红色	端口上出现了错误。
蓝色	端口当前已禁用。
红色	设备当前在堆栈中未链接。

注：PowerConnect OpenManage Switch Administrator 中的 PowerConnect 前面板上不反映端口 LED。只能通过查看实际设备确定 LED 状态。但是，堆栈 LED 反映堆栈端口的状态。有关 LED 的详细信息，请参阅“LED 定义”。

使用 Switch Administrator 按钮

本节介绍了 OpenManage Switch Administrator 界面上的按钮。界面上的按钮分为以下几类：

信息按钮

信息按钮使您可以访问联机支持和联机帮助，以及有关 OpenManage Switch Administrator 界面的信息。

表 5-10. 信息按钮

按钮	说明
“Support”（支持）	打开位于 support.dell.com 的 Dell 支持页面。
“Help”（帮助）	联机帮助包含可帮助您配置和管理设备的信息。联机帮助页面是上下文相关的。例如，如果打开的是“IP Addressing”（IP 定址）页面，则单击“Help”（帮助）将显示该页面的帮助主题。
“About”（关于）	包含版本号和 Dell 版权信息。
“Log Out”（退出）	打开“Log Out”（退出）窗口。

设备管理按钮

设备管理按钮为配置设备信息提供了一种简单方法，其中包括以下按钮：

表 5-11. 设备管理按钮

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

字段定义

用户定义的字段将可以包含 1 至 159 个字符，除非 OpenManage Switch Administrator Web 页面上另有说明。可以使用除以下字符以外的其它所有字母或字符：

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

通过 CLI 访问设备

可以通过与终端端口的直接连接或通过 Telnet 连接来管理设备。如果是通过 Telnet 连接进行访问，请确保在开始使用 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“初始配置”。

注：使用 CLI 远程访问设备之前，请确保已将软件下载到设备。

终端连接

1. 接通设备电源并等待，直至启动完成。
2. 系统显示 **Console>** 提示符时，键入 **enable**，并按 <Enter> 键。

3. 配置设备并输入必要的命令以完成所需的任务。

4. 任务完成后，输入 exit 退出优先执行模式命令。

系统将退出会话。

注：如果其他用户以优先执行命令模式登录至系统，则当前用户将被注销而新用户将登录进来。

Telnet 连接

Telnet 为终端仿真 TCP/IP 协议。通过 TCP/IP 协议网络可以将 RS-232 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。

设备最多同时支持四个 Telnet 会话来管理设备。可以通过 Telnet 会话使用所有 CLI 命令。

启动 Telnet 会话：

1. 选择“Start”（开始）>“Run”（运行）。

系统将打开“Run”（运行）窗口。

2. 在“Run”（运行）窗口的“Open”（打开）字段中键入 **Telnet <IP** 地址>。

3. 单击“OK”（确定）。

Telnet 会话将开始。

使用 CLI

本节介绍了使用 CLI 的信息。

命令模式概览

CLI 分为几种命令模式。每种命令模式均有其特定的命令集。在终端提示符后输入问号将显示可用于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进入另一种命令模式。

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终端配置的任务，还用于访问配置子系统（例如 CLI）。要进入下一个级别，即优先执行模式，需要密码（如果已配置）。

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。不需要密码。

全局配置模式在全局级别管理设备配置。

接口配置模式在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。不需要密码。

用户执行模式

登录至设备后，执行命令模式处于启用状态。用户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。密码将在屏幕上显示，并区分大小写。

要查看并列出优先执行模式命令，请：

1. 在提示符后，键入 **enable**，并按 <Enter> 键。
2. 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，请在命令提示符后键入问号。

要从优先执行模式返回用户执行模式，请键入 **disable** 并按 <Enter> 键。

以下示例说明了访问优先执行模式，然后再返回用户执行模式。

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

使用 exit 命令可以返回先前模式。例如，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，请在优先执行模式提示符后键入 configure 命令并按 <Enter> 键。全局配置模式提示符显示为设备主机名后跟 (config) 和井号 #。

```
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优先执行模式，请键入 exit 命令或使用 <Ctrl>+<Z> 组合键。

以下示例说明了如何访问全局配置模式并返回优先执行模式：

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

有关 CLI 模式的完整列表，请参阅《Dell™ PowerConnect™ 3424/P 和 PowerConnect 3448/P CLI 指南》。

返回目录页面

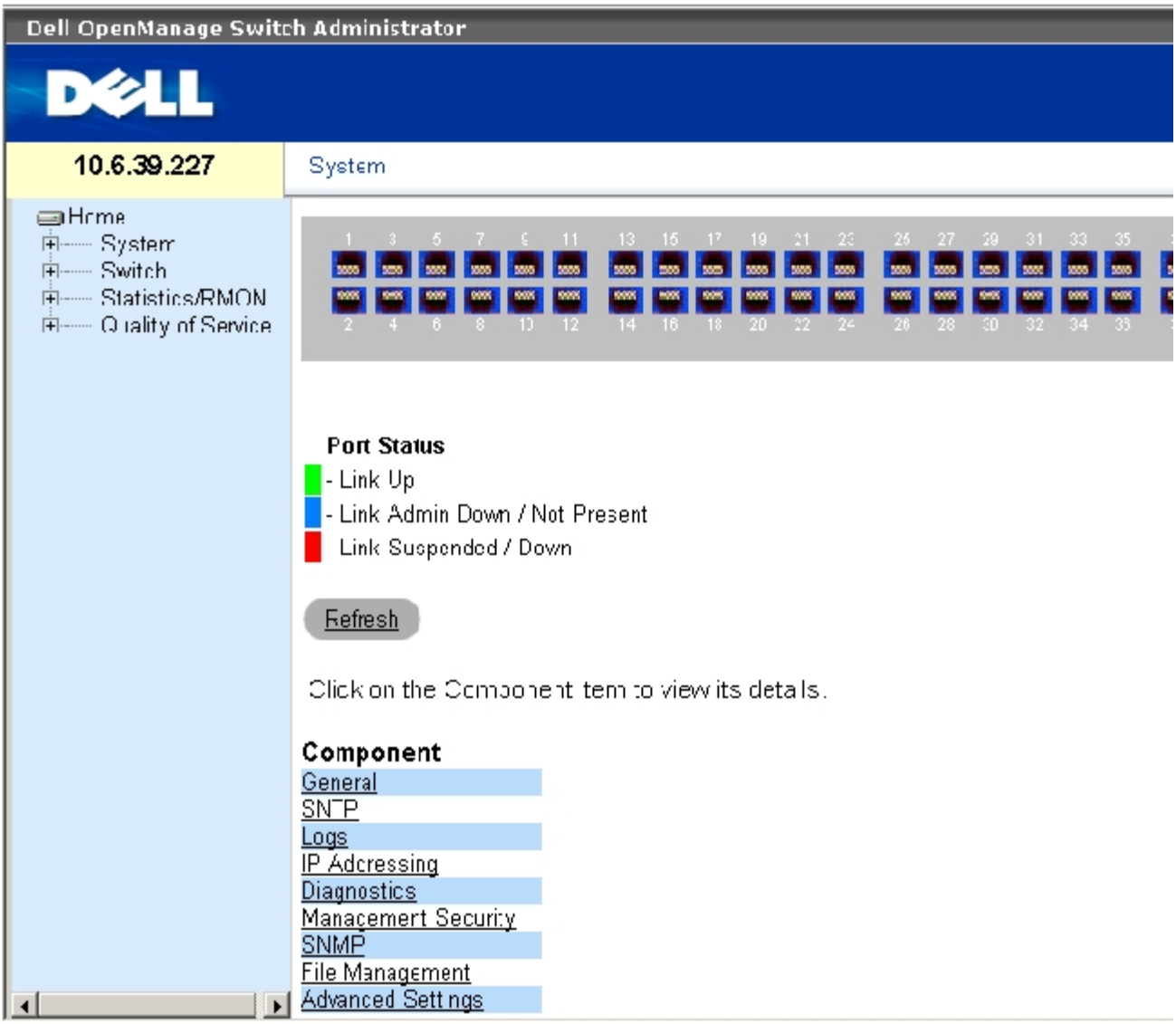
返回目录页面

配置系统信息

Dell™ PowerConnect™ 34XX 系统用户指南

本节介绍了用于定义系统参数（包括安全保护功能）、下载交换机软件以及重启动交换机的信息。要打开“System”（系统）页面，请在树视图中单击“System”（系统）。

图 6-1. 系统



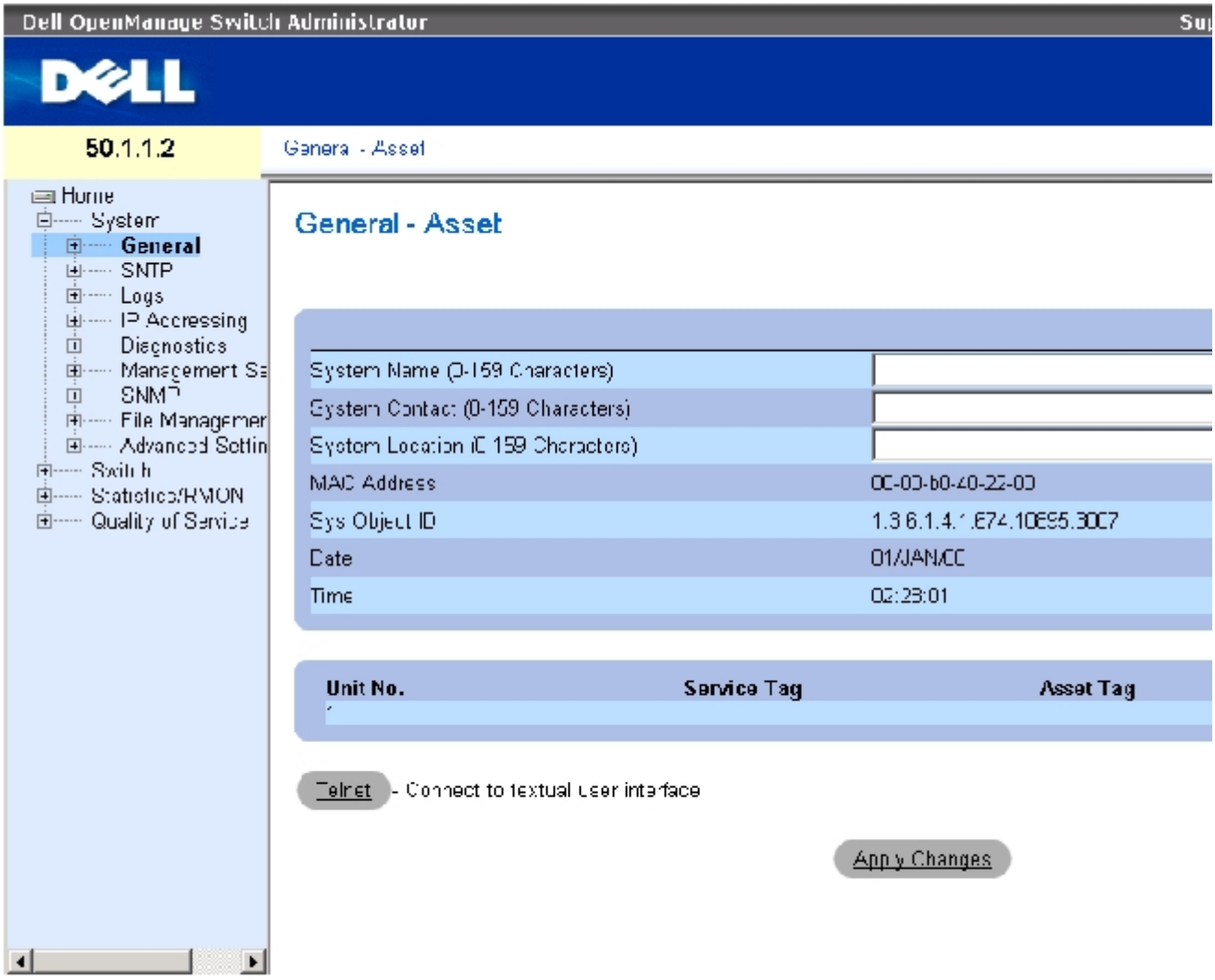
定义常规交换机信息

“General”（常规）页面包含指向网络管理员可以配置交换机参数的页面的链接。

查看交换机资产信息

“Asset”（资产）页面包含用于配置和查看常规设备信息的参数，包括系统名称、位置、联系人、系统 MAC 地址、系统对象 ID、日期、时间和系统重设后运行时间。要打开“Asset”（资产）页面，请在树视图中单击“System”（系统）→“General”（常规）→“Asset”（资产）。

图 6-2. 资产



“Asset” （资产）页面包含以下字段：

“System Name (0-159 Characters)” （系统名称 [0 至 159 个字符]） — 定义用户定义的设备名称。

“System Contact (0-159 Characters)” （系统联系人 [0 至 159 个字符]） — 表示联系人的姓名。

“System Location (0-159 Characters)” （系统位置 [0 至 159 个字符]） — 系统当前运行的位置。

“MAC Address” （MAC 地址） — 表示设备 MAC 地址。

“Sys Object ID” （系统对象 ID） — 实体中包含的网络管理子系统的供应商授权标识。

“Date (DD/MM/YY)” （日期 [DD/MM/YY]） — 当前日期。日期格式为日、月、年；例如，10/OCT/03 表示 2003 年 10 月 10 日。

“Time (HH:MM:SS)” （时间 [HH:MM:SS]） — 表示时间。时间格式为小时、分钟、秒；例如，20:12:21 表示晚上八点十二分二十一秒。

“Unit No.”（装置号）— 表示要显示设备资产信息的装置号。

“Service Tag”（服务标签）— 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]）— 表示用户定义的设备参考。

“Serial No.”（序列号）— 设备序列号。

定义系统信息

1. 打开“Asset”（资产）页面。
2. 定义相关的字段。
3. 单击“Apply Changes”（应用更改）。

系统将定义系统参数，并更新设备。

启动 Telnet 会话

1. 打开“Asset”（资产）页面。
2. 单击“Telnet”。

系统将启动 Telnet 会话。

使用 CLI 命令配置设备信息

下表概括了用于查看和设置“Asset”（资产）页面中显示的字段的等效 CLI 命令。

表 6-12. 资产的 CLI 命令

CLI 命令	说明
hostname 名称	表示或修改设备主机名称。
snmp-server contact 文本	设置系统联系人。

snmp-server location 文本	输入设备位置信息。
clock set hh:mm:ss 日 月 年	手动设置系统时钟和日期。
show clock [detail]	显示系统时钟的时间和日期。
show system id	显示服务标签信息。
show system	显示系统信息。
asset-tag 文本	设置设备资产标签。
show stack <1-6>	显示系统堆栈信息。
show system [unit 装置]	显示系统信息。
show system id [unit 装置]	显示系统标识信息。

以下是使用 CLI 命令定义设备主机名称、系统联系人和设备位置并设置系统时钟的时间和日期的示例：

```
console(config)# hostname dell

dell (config)# snmp-server contact Dell_Tech_Supp

dell (config)# snmp-server location New_York

dell (config)# exit

Console(config)# snmp-server host 10.1.1.1 management 2

Console# clock set 13:32:00 7 Mar 2002

Console# show clock

15:29:03 Jun 17 2002
```

以下是使用 CLI 命令显示独立设备的系统信息的示例：

console# **show system id**	
Service tag :	
Serial number : 51	
Asset tag :	
console# **show system**	

System Description:	Ethernet Switch
System Up Time (days,hour:min:sec):	0,00:00:57
System Contact:	
System Name:	CARRIER-1
System Location:	
System MAC Address:	00:00:00:08:12:51
System Object ID:	1.3.6.1.4.1.674.10895.3006
Type:	PowerConnect 3424
Main Power Supply Status:	OK
Fan 1 Status:	NOT OPERATIONAL
Fan 2 Status:	NOT OPERATIONAL
Temperature (Celsius):	30
Temperature Sensor Status:	OK

以下是使用 CLI 命令显示堆栈设备的系统信息的示例：

```
console# show system id

Unit  Serial number  Asset tag  Service tag
----  -------------  ---------  -----------
1     893658972      mkt-1      89788978
2     893658973      mkt-2      89788979
3     893658974      mkt-3      89788980
4     893658975      mkt-4      89788981
5     893658976      mkt-5      89788982
6     893658977      mkt-6      89788983

console# show system

Unit  Type
```

----	----------				
1	PowerConnect 3424				
2	PowerConnect 3424				
3	PowerConnect 3428				
4	PowerConnect 3424P				
5	PowerConnect 3424P				
6	PowerConnect 3424P				
Unit	Main Power Supply		Redundant Power Supply		
----	----------		----------		
1	OK				
2	OK				
3	OK				
4	OK		OK		
5	OK		OK		
6	OK		OK		
Unit	Fan1	Fan2	Fan3	Fan4	Fan5
----	----	----	----	----	----
1	OK	OK			
2	OK	OK			
3	OK	OK			
4	OK	OK	OK	OK	OK
5	OK	OK	OK	OK	OK
6	OK	OK	OK	OK	OK
Unit	Temperature (Celsius)		Temperature Sensor Status		
----	----------		----------		
1	30		OK		
2	30		OK		

3	30		OK		
4	30		OK		
5	30		OK		
6	30		OK		

定义系统时间设置

“Time Synchronization” (时间同步) 页面包含用于定义本地硬件时钟和外部 SNTP 时钟的系统时间参数的字段。如果系统时间一直使用外部 SNTP 时钟，则当外部 SNTP 时钟出现故障时，系统时间将恢复为本地硬件时钟。可以在设备上启用夏令时。以下是特定国家/地区的夏令时开始和结束时间列表：

- 阿尔巴尼亚 — 3 月的最后一个周末至 10 月的最后一个周末。
- 澳大利亚 — 从 10 月底至 3 月底。
- 澳大利亚 – 塔斯马尼亚 — 从 10 月初至 3 月底。
- 亚美尼亚 — 3 月的最后一个周末至 10 月的最后一个周末。
- 奥地利 — 3 月的最后一个周末至 10 月的最后一个周末。
- 巴哈马 — 从 4 月至 10 月，与美国夏令时一致。
- 白俄罗斯 — 3 月的最后一个周末至 10 月的最后一个周末。
- 比利时 — 3 月的最后一个周末至 10 月的最后一个周末。
- 巴西 — 从 10 月的第三个星期日至 3 月的第三个星期六。在夏令时期间，巴西东南部大部分地区的时钟向前拨一个小时。
- 智利 — 复活节岛 3 月 9 日至 10 月 12 日。3 月的第一个星期日或 3 月 9 日以后。
- 中国 — 中国不实行夏令时。
- 加拿大 — 从 4 月的第一个星期日至 10 月的最后一个星期日。夏令时通常由省政府和地方政府规定。某些自治区可能存在例外。
- 古巴 — 从 3 月的最后一个星期日至 10 月的最后一个星期日。
- 塞浦路斯 — 3 月的最后一个周末至 10 月的最后一个周末。

- 丹麦 — 3 月的最后一个周末至 10 月的最后一个周末。
- 埃及 — 4 月的最后一个星期五至 9 月的最后一个星期四。
- 爱沙尼亚 — 3 月的最后一个周末至 10 月的最后一个周末。
- 芬兰 — 3 月的最后一个周末至 10 月的最后一个周末。
- 法国 — 3 月的最后一个周末至 10 月的最后一个周末。
- 德国 — 3 月的最后一个周末至 10 月的最后一个周末。
- 希腊 — 3 月的最后一个周末至 10 月的最后一个周末。
- 匈牙利 — 3 月的最后一个周末至 10 月的最后一个周末。
- 印度 — 印度不实行夏令时。
- 伊朗 — 从 3 月 1 日至 9 月 1 日。
- 伊拉克 — 从 4 月 1 日至 10 月 1 日。
- 爱尔兰 — 3 月的最后一个周末至 10 月的最后一个周末。
- 以色列 — 根据年份不同而有所变化。
- 意大利 — 3 月的最后一个周末至 10 月的最后一个周末。
- 日本 — 日本不实行夏令时。
- 约旦 — 3 月的最后一个周末至 10 月的最后一个周末。
- 拉脱维亚 — 3 月的最后一个周末至 10 月的最后一个周末。
- 黎巴嫩 — 3 月的最后一个周末至 10 月的最后一个周末。
- 立陶宛 — 3 月的最后一个周末至 10 月的最后一个周末。

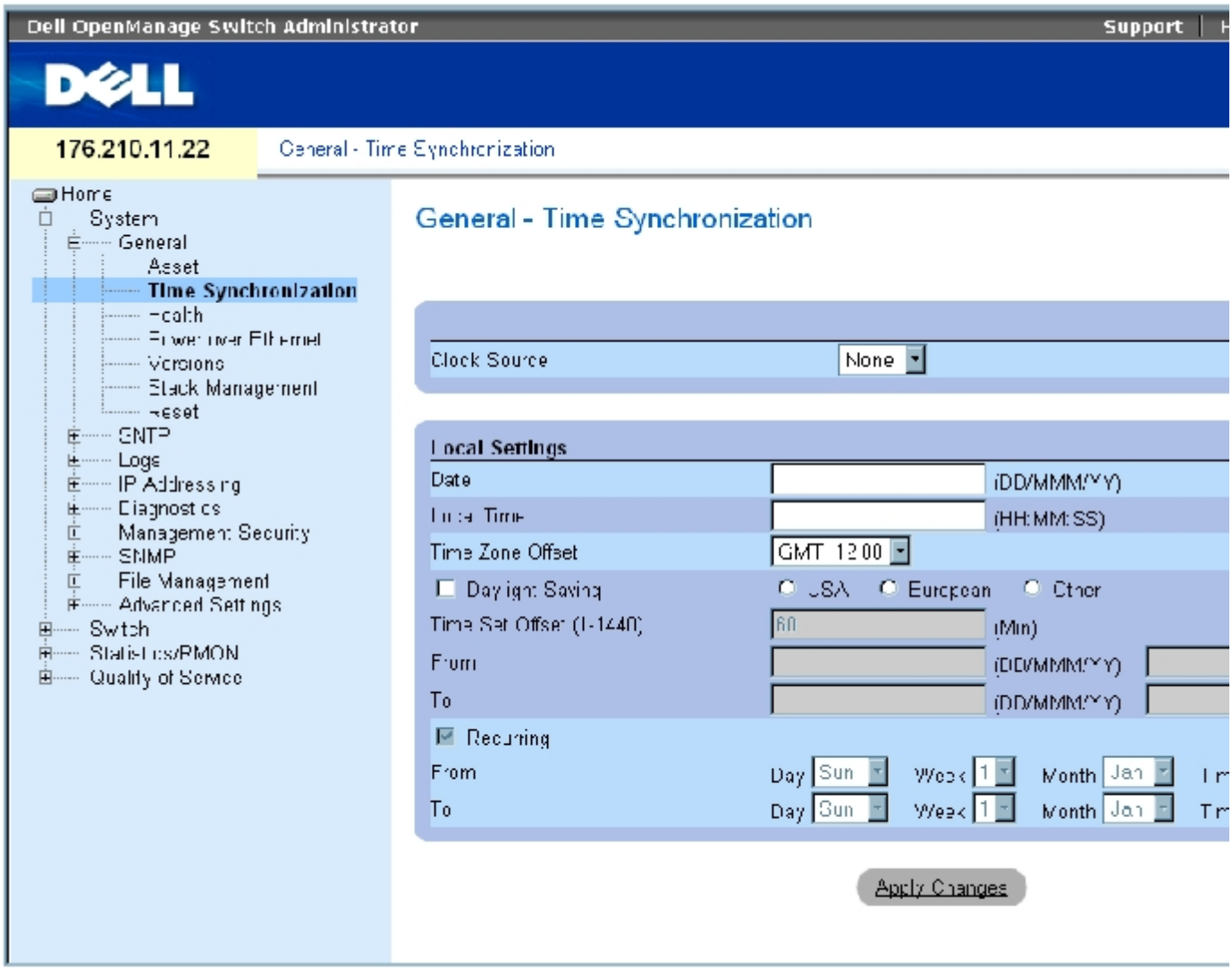
- 卢森堡 — 3 月的最后一个周末至 10 月的最后一个周末。
- 马其顿 — 3 月的最后一个周末至 10 月的最后一个周末。
- 墨西哥 — 从 4 月第一个星期日 02:00 至 10 月最后一个星期日 02:00。
- 摩尔多瓦 — 3 月的最后一个周末至 10 月的最后一个周末。
- 黑山 — 3 月的最后一个周末至 10 月的最后一个周末。
- 荷兰 — 3 月的最后一个周末至 10 月的最后一个周末。
- 新西兰 — 从 10 月的第一个星期日至 3 月的第一个星期日或 3 月 15 日以后。
- 挪威 — 3 月的最后一个周末至 10 月的最后一个周末。
- 巴拉圭 — 从 4 月 6 日至 9 月 7 日。
- 波兰 — 3 月的最后一个周末至 10 月的最后一个周末。
- 葡萄牙 — 3 月的最后一个周末至 10 月的最后一个周末。
- 罗马尼亚 — 3 月的最后一个周末至 10 月的最后一个周末。
- 俄罗斯 — 3 月的最后一个周末至 10 月的最后一个周末。
- 塞尔维亚 — 3 月的最后一个周末至 10 月的最后一个周末。
- 斯洛伐克共和国 — 3 月的最后一个周末至 10 月的最后一个周末。
- 南非 — 南非不实行夏令时。
- 西班牙 — 3 月的最后一个周末至 10 月的最后一个周末。
- 瑞典 — 3 月的最后一个周末至 10 月的最后一个周末。
- 瑞士 — 3 月的最后一个周末至 10 月的最后一个周末。

- 叙利亚 — 从 3 月 31 日至 10 月 30 日。
- 台湾地区 — 台湾地区不实行夏令时。
- 土耳其 — 3 月的最后一个周末至 10 月的最后一个周末。
- 英国 — 3 月的最后一个周末至 10 月的最后一个周末。
- 美国 — 从 4 月第一个星期日 02:00 至 10 月最后一个星期日 02:00。

有关 SNTP 的详细信息，请参阅“配置 SNTP 设置”。

要打开“Time Synchronization”（时间同步）页面，请在树视图中单击“System”（系统）→“General”（常规）→“Time Synchronization”（时间同步）。

图 6-3. 时间同步



“Time Synchronization” (时间同步) 页面包含以下字段：

时钟源

“Clock Source” (时钟源) — 用于设置系统时钟的源。可能的字段值包括：

“SNTP” — 表示通过 SNTP 服务器设置系统时间。有关详情，请参阅“配置 SNTP 设置”。

“None” (无) — 表示不通过外部源设置系统时间。

本地设置

“Date” (日期) — 定义系统日期。日期字段格式为 DD/MMM/YY；例如，04/May/50。

“Local Time”（本地时间）— 定义系统时间。本地时间字段格式为 HH/MM/SS；例如，21/15/03。

“Time Zone Offset”（时区偏移）— 格林威治标准时间（GMT）与本地时间之间的差值。例如，巴黎的时区偏移为 GMT +1:00，而纽约的本地时间为 GMT –5:00。

夏令时设置分为两种：在特定年份中的特定日期，或与年份无关的常年定期设置。对于特定年份中的特定设置，请完成“Daylight Savings”（夏令时）区域；对于常年定期设置，请完成“Recurring”（常年定期）区域。

“Daylight Savings”（夏令时）— 在设备上启用基于设备位置的夏令时（DST）。可能的字段值包括：

“USA”（美国）— 设备在 4 月第一个星期日 2 a.m. 切换至 DST，在 10 月最后一个星期日 2 a.m. 恢复为标准时间。

“European”（欧洲）— 设备在 3 月最后一个星期日 1:00 am 切换至 DST，在 10 月最后一个星期日 1:00 am 恢复为标准时间。“European”（欧洲）选项适用于欧盟成员国，其它欧洲国家/地区使用欧盟标准。

“Other”（其它）— DST 由用户根据设备位置来定义。如果选择“Other”（其它），则必须定义“From”（从）和“To”（至）字段。

“Time Set Offset (1-1440)”（时间设置偏移 [1-1440]）— 对于美国和欧洲以外的国家/地区，可以以分钟为单位设置 DST 的时间。默认时间为 60 分。

“From”（从）— 定义美国或欧洲以外的国家/地区的 DST 开始时间；格式为：DD/MMM/YY 占用一个字段，时间占用另一个字段。例如，DST 开始于 2007 年 10 月 25 日 5:00 am，则这两个字段分别定义为 25/Oct/07 和 05:00。可能的字段值包括：

“Date”（日期）— DST 开始的日期。可能的字段范围是 1 至 31。

“Month”（月份）— DST 开始年份中的月份。可能的字段范围是 1 月至 12 月。

“Year”（年份）— 配置的 DST 开始的年份。

“Time”（时间）— DST 开始的时间。时间字段格式为小时:分钟，例如 05:30。

“To”（至）— 定义美国或欧洲以外的国家/地区的 DST 结束时间；格式为：DD/MMM/YY 占用一个字段，时间占用另一个字段。例如，DST 结束于 2008 年 3 月 23 日 12:00 am，则这两个字段分别定义为 23/Mar/08 和 12:00。可能的字段值包括：

“Date”（日期）— DST 结束的日期。可能的字段范围是 1 至 31。

“Month”（月份）— DST 结束年份中的月份。可能的字段范围是 1 月至 12 月。

“Year”（年份）— 配置的 DST 结束的年份。

“Time”（时间）— DST 结束的时间。时间字段格式为小时:分钟；例如，05:30。

“Recurring”（常年定期）— 定义美国或欧洲以外国家/地区的 DST 开始时间，其中 DST 常年不变。可能的字段值包括：

“From”（从）— 定义每年 DST 开始的时间。例如，本地 DST 开始于每年 4 月第二个星期日 5:00 am。可能的字段值包括：

“Day”（日）— 每年 DST 从周几开始。可能的字段范围是星期日至星期六。

“Week”（周）— 每年 DST 从该月的第几周开始。可能的字段范围是 1 至 5。

“Month”（月份）— 每年 DST 从哪一个月开始。可能的字段范围是 1 月至 12 月。

“Time”（时间）— 每年 DST 开始的时间。时间字段格式为小时:分钟，例如 02:10。

“To”（至）— 定义每年 DST 结束的定期时间。例如，本地 DST 结束于每年 10 月第四个星期五 5:00 am。可能的字段值包括：

“Day”（日）— 每年 DST 在周几结束。可能的字段范围是星期日至星期六。

“Week”（周）— 每年 DST 在该月的第几周结束。可能的字段范围是 1 至 5。

“Month”（月份）— 每年 DST 在哪一个月结束。可能的字段范围是 1 月至 12 月。

“Time”（时间）— 每年 DST 结束的时间。时间字段格式为小时:分钟；例如，05:30。

选择时钟源

1. 打开“Time Synchronization”（时间同步）页面。
2. 定义“Clock Source”（时钟源）字段。
3. 单击“Apply Changes”（应用更改）。

系统将选定时钟源，并更新设备。

定义本地时钟设置

1. 打开“Time Synchronization”（时间同步）页面。

2. 定义字段。

3. 单击“Apply Changes”（应用更改）。

系统将应用本地时钟设置。

使用 CLI 命令定义时钟设置

下表概括了用于设置“Time Synchronization”（时间同步）页面显示的字段的等效 CLI 命令。

注：在设置夏时制前必须完成以下步骤：

1. 配置夏令时。

2. 定义时区。

3. 设置时钟。

例如：

```
console(config)# clock summer-time recurring usa
console(config)# clock time zone 2 zone TMZ2
console(config)# clock set 10:00:00 apr 15 2004
```

表 6-13. 时钟设置的 CLI 命令

CLI	说明
clock source sntp	为系统时钟配置外部时间源。
clock time zone 小时偏移 [minutes 分钟偏移][zone 缩写]	设置用于显示的时区。
clock summer-time	将系统配置为自动切换至夏季时间（夏令时）。
clock summer-time recurring {usa | eu | 周 日 月 hh:mm 周 日 月 hh:mm} [offset 偏移] [zone 缩写]	将系统配置为自动切换至夏令时（根据美国和欧洲标准）。
clock summer-time date 日 月 年 hh:mm 日 月 年 hh:mm [offset 偏移] [zone 缩写]	将系统配置为在特定时期自动切换至夏季时间（夏令时）– 日/月/年格式。

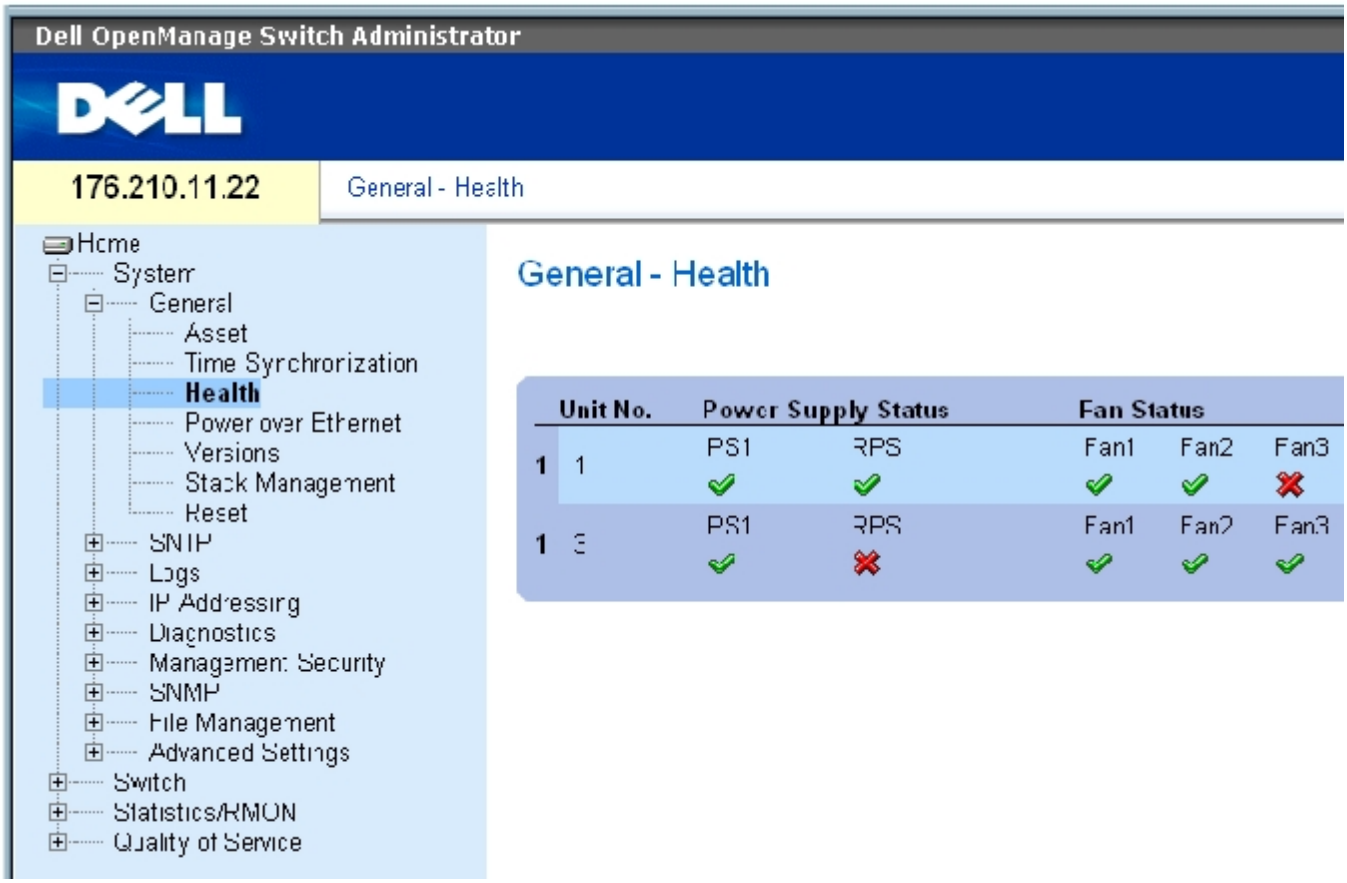
以下是 CLI 命令的示例：

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


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


console(config)# clock
source sntp


console(config)# interface
ethernet e14


console(config-if)# sntp
client enable


console(config-if)# exit


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

查看系统运行状况信息

“System Health”（系统运行状况）页面显示物理设备信息，包括关于设备的电源和通风源的信息。要打开“System Health”（系统运行状况）页面，请在树视图中单击“System”（系统）→“General”（常规）→“Health”（运行状况）。

图 6-4. 系统运行状况



“System Health”（系统运行状况）页面包含以下字段：

“Unit No.”（装置号）— 表示要显示设备资产信息的装置号。

“Power Supply Status”（电源设备状态）— 设备具有两个电源设备。在界面中，电源设备 1 显示为 PS1，冗余电源设备显示为 RPS。可能的字段值包括：

— 电源设备运行正常。

— 电源设备运行不正常。

“Not Present”（不存在）— 当前没有电源设备。

“Fan Status”（风扇状态）— 非 PoE 设备有两个风扇，PoE 设备有五个风扇。在界面中，每个风扇的表示形式为风扇加上风扇编号。可能的字段值包括：

— 风扇运行正常。

— 风扇运行不正常。

“Not Present”（不存在）— 当前没有风扇。

“Temperature”（温度）— 设备当前运行时的温度。设备温度以摄氏为单位显示。设备温度阈值为 0-40 C (32-104 F)。下表显示了以 5 摄氏为增量对应的华氏温度。

表 6-14. 摄氏到华氏的转换表

摄氏	华氏
0	32
5	41
10	50
15	59
20	68
25	77
30	86
35	95
40	104

使用 CLI 命令查看系统运行状况信息

下表概括了用于查看“System Health”（系统运行状况）页面中显示的字段的等效 CLI 命令。

表 6-15. 系统运行状况的 CLI 命令

CLI 命令	说明
show system [unit 装置]	显示系统信息。

以下是系统运行状况的 CLI 命令的示例。

Console> **show system**				
System Description:Ethernet switch				
System Up Time (days,hour:min:sec): 1,22:38:21				

System Contact:				
System Name:RS1				
System location:				
System MAC Address:00.10.B5.F4.00.01				
Sys Object ID: 1.3.6.1.4.1.674.10895.3004				
Type:PowerConnect 3424				
Temperature Sensors:				
Unit	Sensor	Temperature (Celsius)		Status
----	------	----------		------
1	1		41	OK
1	2		41	OK
2	1		42	OK
2	2		42	OK
Unit	Power Supply	Source	Status	
----	----------	------	------	
1	Main	AC	OK	
2	Secondary	AC	OK	
Unit	Fan	Status		
----	---	------		
1	CPU	OK		
2	CPU	OK		

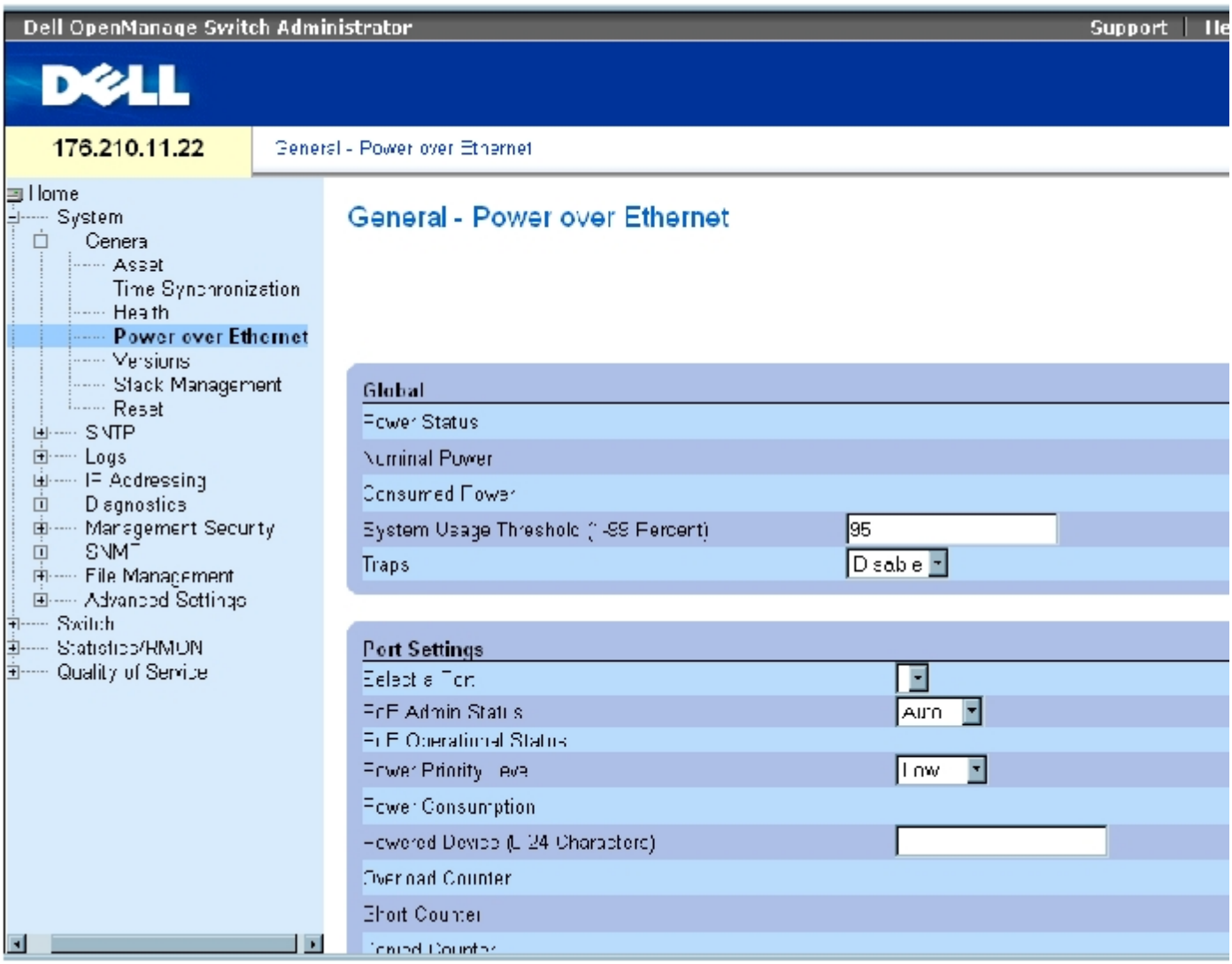
管理以太网电源

以太网电源 (PoE) 通过现有的 LAN 电缆为设备供电，无需更新或修改网络基础设施。以太网电源使网络设备摆脱了必须靠近电源放置的束缚。

用电设备是指接收 PowerConnect 电源设备供电的设备，例如 IP 电话。用电设备通过以太网端口与 PowerConnect 设备相连接。用电设备是通过 PowerConnect 3424P 的全部 24 个 FE 端口或 PowerConnect 3448P 的全部 48 个 FE 端口连接的。

要打开“Power Over Ethernet”（以太网电源）页面，请在树视图中单击“System”（系统）→“General”（常规）→“Power over Ethernet”（以太网电源）。

图 6-5. 以太网电源



“Power Over Ethernet”（以太网电源）页面包含以下部分：

- 全局设置
- 端口设置

全局设置

以太网电源全局设置部分包含以下字段：

“Power Status”（电源状态）— 表示内联电源的状态。

“On”（开）— 表示电源装置正在运行。

“Off”（关）— 表示电源装置没有运行。

“Faulty”（故障）— 表示电源装置正在运行，但出现了错误。例如，电源过载或短路。

“Nominal Power”（额定功率）— 表示设备实际可以提供的功率。此字段值以瓦特为单位显示。

“Consumed Power”（消耗功率）— 表示设备使用的功率。此字段值以瓦特为单位显示。

“System Usage Threshold (1-99 Percent)”（系统使用率阈值 [1-99%]）— 表示在生成警报前消耗的功率的百分比。此字段值为 1-99%。默认值为 95%。

“Traps”（陷阱）— 启用或禁用此字段可以接收或拒收 PoE 设备陷阱。默认设置为禁用该字段。

端口设置

“Select a Port”（选择端口）— 表示一个特定接口，已为其定义了 PoE 参数并被分配到连接至选定端口的可供电接口。

“PoE Admin Status”（PoE 管理状态）— 表示设备 PoE 模式。可能的字段值包括：

“Auto”（自动）— 启用设备发现协议，并为使用 PoE 模块的设备供电。设备发现协议使设备能够发现连接到设备接口的用电设备，并了解它们的分类。这是默认设置。

“Never”（从不）— 禁用设备发现协议，并停止为使用 PoE 模块的设备供电。

“PoE Operational Status”（PoE 运行状态）— 表示端口是否被启用以使用 PoE。可能的字段值包括：

“On”（开）— 表示设备正在为接口供电。

“Off”（关）— 表示设备没有为接口供电。

“Test Fail”（检测失败）— 表示用电设备检测失败。例如，无法启用端口和无法使用端口为用电设备供电。

“Testing”（正在检测）— 表示正在检测用电设备。例如，检测用电设备以确认它是否正在接收电源设备的供电。

“Searching”（正在搜索）— 表示 PowerConnect 设备当前正在搜索用电设备。“Searching”（正在搜索）是默认的 PoE 运行状态。

“Fault”（故障）— 表示 PowerConnect 设备检测到用电设备上出现故障。例如，无法读取用电设备内存。

“Power Priority Level”（供电优先级）— 确定在电源设备电力不足时供电的端口优先级。端口供电优先级是在电源设备电力不足时使用。此字段默认值为“Low”（低）。例如，如果电源设备以 99% 的使用率运行，端口 1 的优先级为高，而端口 3 的优先级为低，则优先为端口 1 供电，端口 3 可能会被断电。

“Critical”（紧急）— 设定最高供电优先级。

“High”（高）— 设定第二级供电优先级。

“Low”（低）— 设定最低供电优先级。

“Power Consumption”（电功率）— 表示为连接到选定接口的用电设备所设定的功率大小。设备是按用电设备分类的，并且 PowerConnect 设备将使用分类信息。这些字段值以瓦特为单位表示。可能的字段值包括：

“0.44 - 12.95”— 表示端口的电功率级别设定为 0.44 至 12.95 瓦特。

“0.44 - 3.8”— 表示端口的电功率级别设定为 0.44 至 3.8 瓦特。

“3.84 - 6.49”— 表示端口的电功率级别设定为 3.84 至 6.49 瓦特。

“6.49 - 12.95”— 表示端口的电功率级别设定为 6.49 至 12.95 瓦特。

“Power Device (0-24 characters)”（电源设备 [0 至 24 个字符]）— 提供用户定义的用电设备的说明。此字段最多可以包含 24 个字符。

“Overload Counter”（过载计数器）— 表示出现电源过载的总次数。

“Short Counter”（电量不足计数器）— 表示出现电量不足的总次数。

“Denied Counter”（断电计数器）— 表示用电设备被断电的次数。

“Absent Counter”（缺席计数器）— 表示因检测不到用电设备而使电源设备停止为用电设备供电的次数。

“Invalid Signature Counter”（无效签名计数器）— 表示收到无效签名的次数。签名是用电设备向 PSE 标识自身的方法。签名是在检测、分类或维护用电设备期间生成的。

定义 PoE 设置

1. 打开“Power Over Ethernet”（以太网电源）页面。
2. 定义字段。
3. 单击“Apply Changes”（应用更改）。

PoE 设置将被定义，并更新设备。

使用 CLI 命令管理 PoE

下表概括了用于查看“Power Over Ethernet”（以太网电源）页面中显示的字段的等效 CLI 命令。

表 6-16. POE 设置的 CLI 命令

CLI 命令	说明
power inline {auto | never}	配置接口上的内联电源的管理模式。
power inline powered-device 用电设备类型	添加用电设备类型的说明。
power inline priority {critical | high | low}	从内联电源管理的角度配置接口优先级。
power inline usage-threshold	配置用于触发警报的阈值
power inline traps enable	启用 PoE 设备陷阱
show power inline [以太网接口]	显示 PoE 配置信息

以下是 PoE CLI 命令的示例。

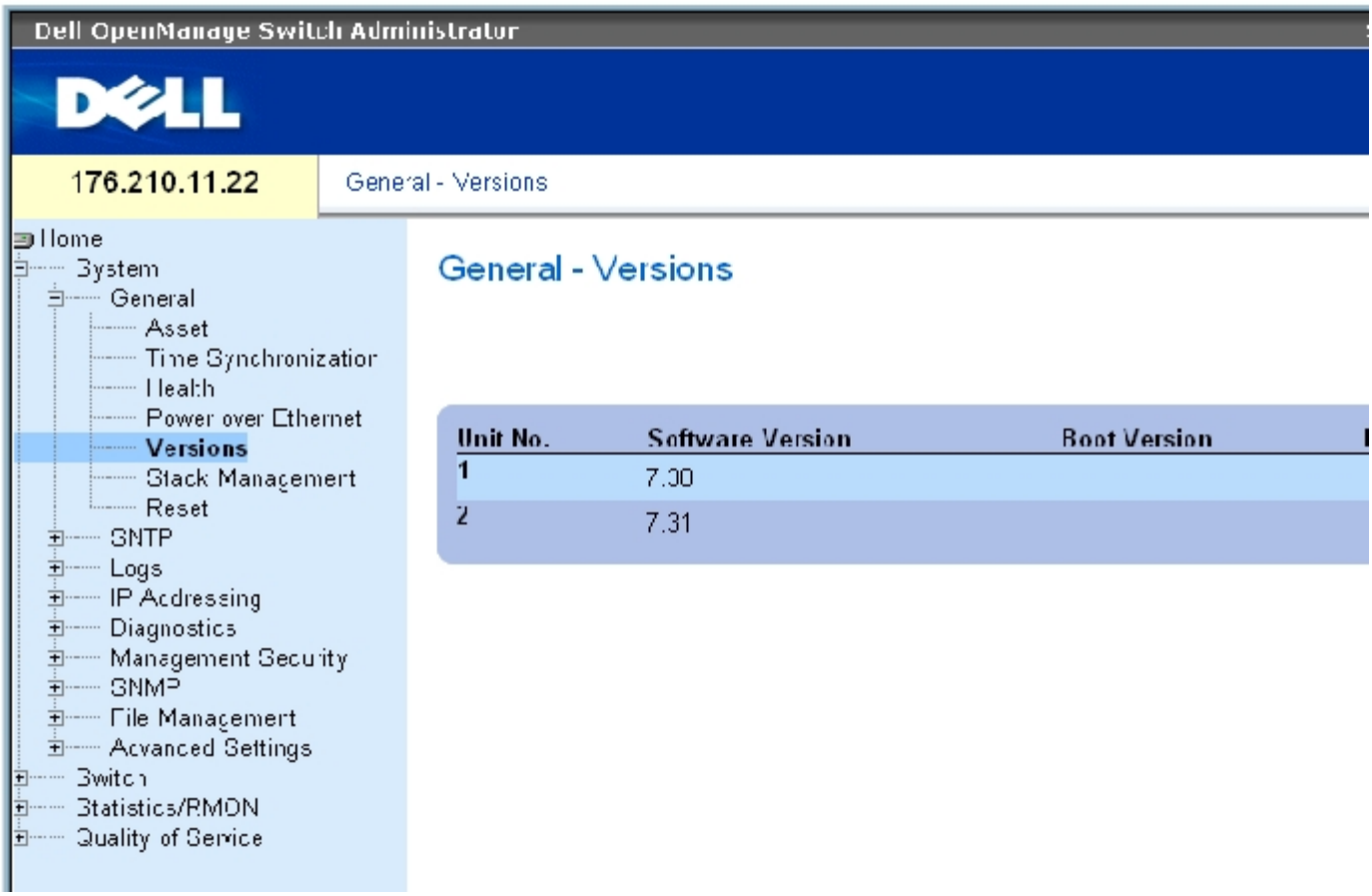
```
Console# show power inline
Power:On
Nominal Power:150 Watts
Consumed Power:120 Watts (80%)
Usage Threshold: 95%
Traps:Enabled
Port  Powered Device     State  Priority  Status  Classification [W]
----  ---------------   -----  --------  ------  ------------------
1/e1  IP Phone Model A  Auto   High      On      0.44 - 12.95
```

2/e1	Wireless AP Model	Auto	Low	On	0.44 – 3.84
3/e1		Auto	Low	Off	N/A
Console# **show power inline ethernet** 1/e1					
Port	Powered Device	State	Priority	Status	Classification [W]
----	---------------	-----	--------	------	------------------
1/1e	IP Phone Model A	Auto	High	On	0.44 – 12.95
Overload Counter: 1					
Short Counter: 0					
Denied Counter: 0					
Absent Counter: 0					
Invalid Signature Counter: 0					

查看版本信息

“Versions”（版本）页面包含有关当前运行的硬件和软件的版本信息。要打开“Versions”（版本）页面，请在树视图中单击“System”（系统）→“General”（常规）→“Versions”（版本）。

图 6-6. 版本



"Versions" (版本) 页面包含以下字段：

"Unit No." (装置号) — 表示要显示版本信息的装置号。

"Software Version" (软件版本) — 设备上当前运行的软件的版本。

"Boot Version" (引导版本) — 设备上当前运行的引导版本。

"Hardware Version" (硬件版本) — 当前的设备硬件版本。

使用 CLI 显示设备版本

下表概括了用于查看"Versions" (版本) 页面中显示的字段的等效 CLI 命令。

表 6-17. 版本的 CLI 命令

CLI 命令	说明
show version	显示系统版本信息。

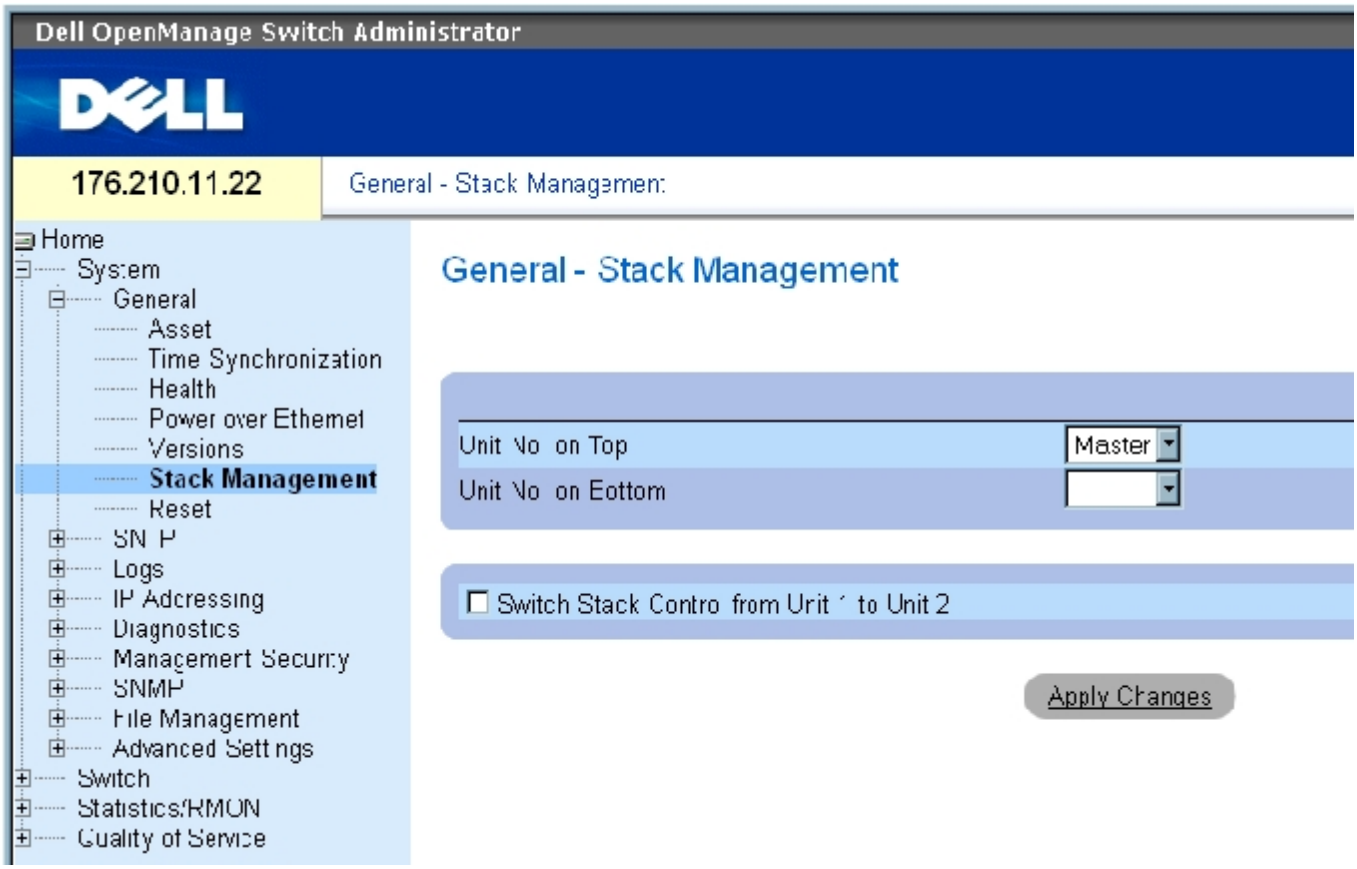
以下是 CLI 命令的示例：

```
console> show version

SW version 1.0.0.0 (date 23-Jan-2005 time 17:34:19)

Boot version 1.0.0.0 (date 11-Jan-2005 time 11:48:21)

HW version 1.0.0
```

管理堆栈成员

“Stack Management”（堆栈管理）页面使网络管理员可以重启动整个堆栈或特定设备。要打开“Stack Management”（堆栈管理）页面，请在树视图中单击“System”（系统）→“General”（常规）→“Stack Management”（堆栈管理）。

图 6-7. 堆栈管理



注：重启动设备之前，请保存对运行配置文件的所有更改。这样可以防止当前设备配置丢失。有关保存配置文件的详细信息，请参阅“管理文件”。

“Unit No. on Top”（顶部装置号）— 第一个堆栈成员编号。可能的值包括“Master”（主装置）和“1”、“2”、“3”、“4”、“5”、“6”。

“Unit No. on Bottom”（底部装置号）— 第二个堆栈成员编号。可能的值包括“Master”（主装置）和“1”、“2”、“3”、“4”、“5”、“6”。

“Switch Stack Control from Unit 1 to Unit 2”（将堆栈控制从装置 1 切换到装置 2）— 从当前堆栈主装置切换到备用主装置。

注：重启动主装置将重启动整个堆栈。

在堆栈主装置之间切换

1. 打开“Stack Management”（堆栈管理）页面。
2. 选取“Switch Stack Control from Unit 1 to Unit 2”（将堆栈控制从装置 1 切换到装置 2）复选框。
3. 单击“Apply Changes”（应用更改）。

   系统将显示一条确认信息。
4. 单击“OK”（确定）。

   设备将重启动。重启动设备后，系统将提示输入用户名和密码。

配置堆栈显示顺序

1. 打开“Stack Management”（堆栈管理）页面。
2. 通过定义顶部装置和底部装置来定义堆栈拓扑。这些装置必须处于相邻位置。
3. 单击“Apply Changes”（应用更改）。

   将重新配置在“System”（系统）页面的显示顺序。

使用 CLI 命令管理堆栈

下表概括了用于查看“Stack Management”（堆栈管理）页面中显示的字段的等效 CLI 命令。

表 6-18. 堆栈管理的 CLI 命令

CLI 命令	说明
reload	重新加载操作系统。
stack reload	重新加载堆栈成员。
stack master	强制选择堆栈主装置

以下是 CLI 命令的示例：

```
console# reload

Are you sure you want to erase running configuration (y/n) [n]
```

重启动设备

“Reset”（重启动）页面使您可以远程重启动设备。要打开“Reset”（重启动）页面，请在树视图中单击“System”（系统）→“General”（常规）→“Reset”（重启动）。

“Reset”（重启动）页面包含以下字段：

“Reset Unit No.”（重启动装置号）— 重启动选定堆栈成员。

注：重启动设备之前，请保存对启动配置文件的所有更改。这样可以防止当前设备配置丢失。有关保存配置文件的详细信息，请参阅“管理文件”。

重启动设备

1. 打开“Reset”（重启动）页面。
2. 在“Reset Unit Number”（重启动装置号）字段中选择一个装置。
3. 单击“Apply Changes”（应用更改）。

   系统将显示一条确认信息。
4. 单击“OK”（确定）。

设备将重启动。重启动设备后，系统将提示输入用户名和密码。

5. 输入用户名和密码以重新连接至 Web 界面。

使用 CLI 重启动设备

下表概括了用于通过 CLI 执行设备重启动的等效 CLI 命令：

表 6-19. 重启动的 CLI 命令

CLI 命令	说明
reload	重新加载操作系统。

以下是 CLI 命令的示例：

```
console >reload


This command will reset
the whole system and
disconnect your current
session.Do you want to
continue (y/n)[n]?
```

配置 SNTP 设置

交换机支持简单网络时间协议 (SNTP)。SNTP 确保网络交换机时钟时间同步准确，最多可准确到毫秒。时间同步由网络 SNTP 服务器来执行。SNTP 仅作为客户端运行，而无法为其它系统提供时间服务。

交换机可以向以下服务器类型轮询服务器时间：

- 单点传送
- 任意点传送
- 广播

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。交换机从 1 层和更高层接收时间。以下是层的示例：

- 0 层 — 表示将实时时钟用作时间源，例如 GPS 系统。

- 1 层 — 表示使用直接链接至 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 — 表示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回复的时间。
- T4 — 客户端接收到服务器回复的时间。

设备可以向以下服务器类型轮询服务器时间：单点传送、任意点传送和广播。

轮询单点传送信息用于轮询 IP 地址已知的服务器。设备上配置的 SNTP 服务器是唯一能够被轮询以获得同步信息的服务器。T1 至 T4 用于确定服务器时间。这是用于同步设备时间的首选方法，因为这种方法最可靠。如果选择这种方法，则仅可以从使用“SNTP Servers” (SNTP 服务器) 页面在设备上定义的 SNTP 服务器接受 SNTP 信息。

服务器 IP 地址未知时，可以使用轮询任意点传送信息。如果选择这种方法，则网络中的所有 SNTP 服务器均可以发送同步信息。设备将在其预先请求同步信息时同步。响应同步信息请求的前 3 个 SNTP 服务器的最佳响应（最低层）用于设置时间值。时间级别 T3 和 T4 用于确定服务器时间。

使用任意点传送轮询来获取同步设备时间的时间信息，优先于使用广播轮询获取时间信息。但是，这种方法的可靠性不如单点传送轮询，因为将从并未在设备上配置的 SNTP 服务器上接受 SNTP 信息包。

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 客户端侦听信息。如果启用广播轮询，将接受所有同步信息，即使它是设备尚未请求的信息。这是最不可靠的方法。

设备将通过主动请求信息来检索同步信息，或在每个轮询间隔时进行检索。如果启用了单点传送、任意点传送和广播轮询，系统将按以下顺序检索信息：

- 优先检索来自设备上定义的服务器的信息。如果未启用单点传送轮询或者设备上未定义任何服务器，设备将接受来自响应该设备的任何 SNTP 服务器的时间信息。
- 如果有多个单点传送设备进行响应，则优先检索来自最低层设备的同步信息。

- 如果服务器的层相同，则将接受来自首先响应的 SNTP 服务器的同步信息。

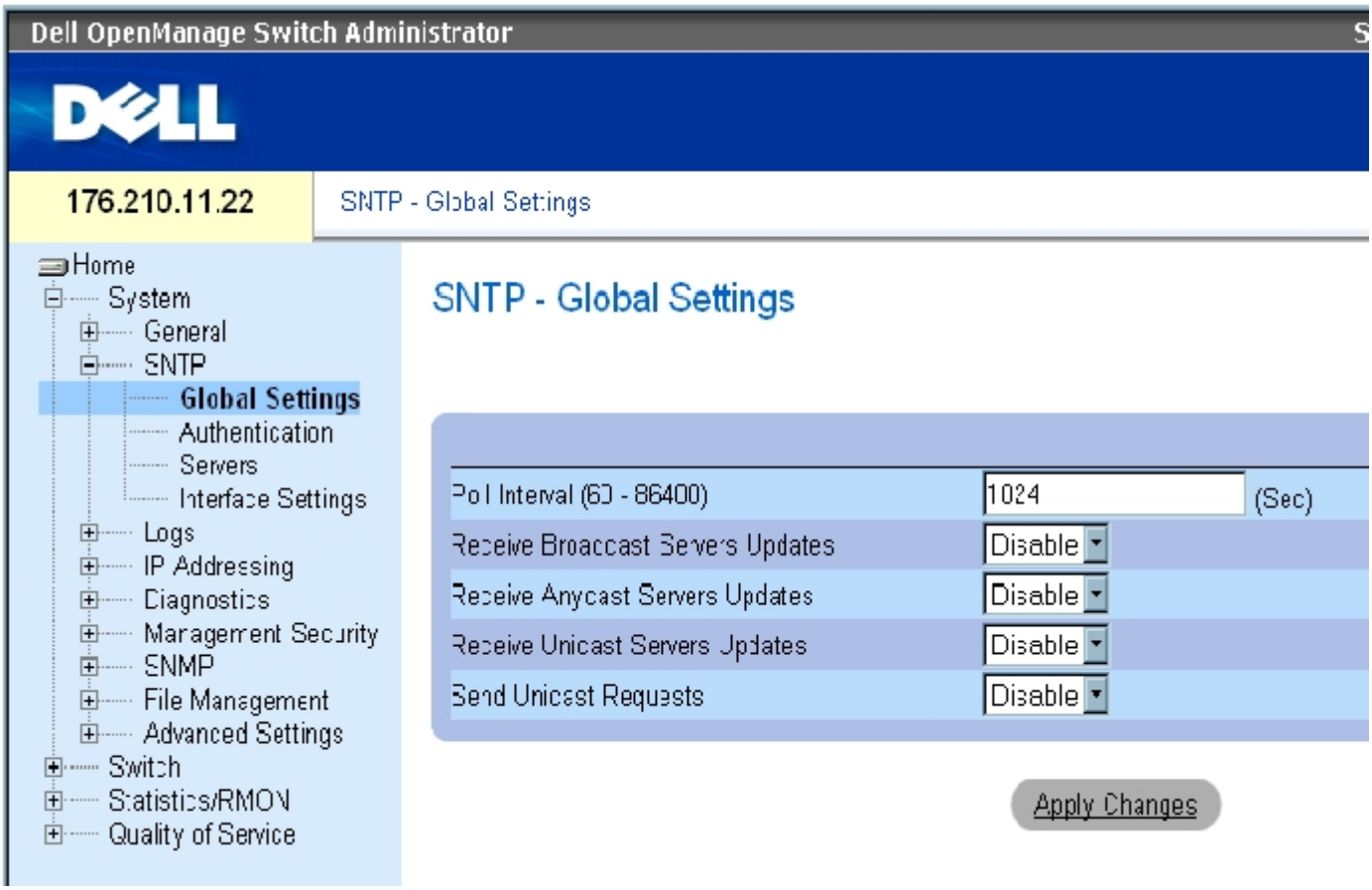
MD5（报文摘要 5）验证可以维护到 SNTP 服务器的设备同步路径的安全。MD5 是一种生成 128 位散列的算法。MD5 是 MD4 的一种变体，它增强了 MD4 的安全性。MD5 验证通信的完整性并验证通信的起点。

要打开“SNTP”页面，请在树视图中单击“System”（系统）→“SNTP”以打开“SNTP”页面。

定义 SNTP 全局参数

“SNTP Global Settings”（SNTP 全局设置）页面提供了用于全局定义 SNTP 参数的信息。要打开“SNTP Global Settings”（SNTP 全局设置）页面，请在树视图中单击“System”（系统）→“SNTP”→“SNTP Global Settings”（SNTP 全局设置）。

图 6-8. SNTP 全局设置



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

“Poll Interval (60-86400)”（轮询间隔 [60 至 86400]）— 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）。默认情况下，轮询间隔为 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。

“Receive Anycast Servers Updates”（接收任意点传送服务器更新）— 如果启用该选项，将轮询 SNTP 服务器以获得任意点传送服务器时间信息。如果同时启用“Receive Anycast Servers Update”（接收任意点传送服务器更新）和“Receive Broadcast Servers Update”（接收广播服务器更新）字段，则根据任意点传送服务器时间信息设置系统时间。

“Receive Unicast Servers Updates”（接收单点传送服务器更新）— 如果启用该选项，将轮询 SNTP 服务器以获得单点传送服务器时间信息。如果同时启用“Receive Broadcast Servers Updates”（接收广播服务器更新）、“Receive Anycast Servers Updates”（接收任意点传送服务器更新）和“Receive Unicast Servers Updates”（接收单点传送服务器更新）字段，则根据单点传送服务器时间信息设置系统时间。

“Send Unicast Requests”（发送单点传送请求）— 如果启用该选项，将向 SNTP 服务器发送 SNTP 单点传送服务器时间信息请求。

选择时钟源

1. 打开“Time Synchronization”（时间同步）页面。
2. 定义“Clock Source”（时钟源）字段。
3. 单击“Apply Changes”（应用更改）。

系统将选定时钟源，并更新设备。

定义本地时钟设置

1. 打开“Time Synchronization”（时间同步）页面。
2. 定义字段。
3. 单击“Apply Changes”（应用更改）。

系统将应用本地时钟设置。

使用 CLI 命令定义 SNTP 全局参数

下表概括了用于设置“SNTP Global Settings”（SNTP 全局设置）页面中显示的字段的等效 CLI 命令。

表 6-20. SNTP 全局参数 CLI 命令

CLI 命令	说明
sntp broadcast client enable	启用 SNTP 广播客户端
sntp anycast client enable	启用 SNTP 任意点传送客户端
sntp unicast client enable	启用 SNTP 预定义的单点传送客户端

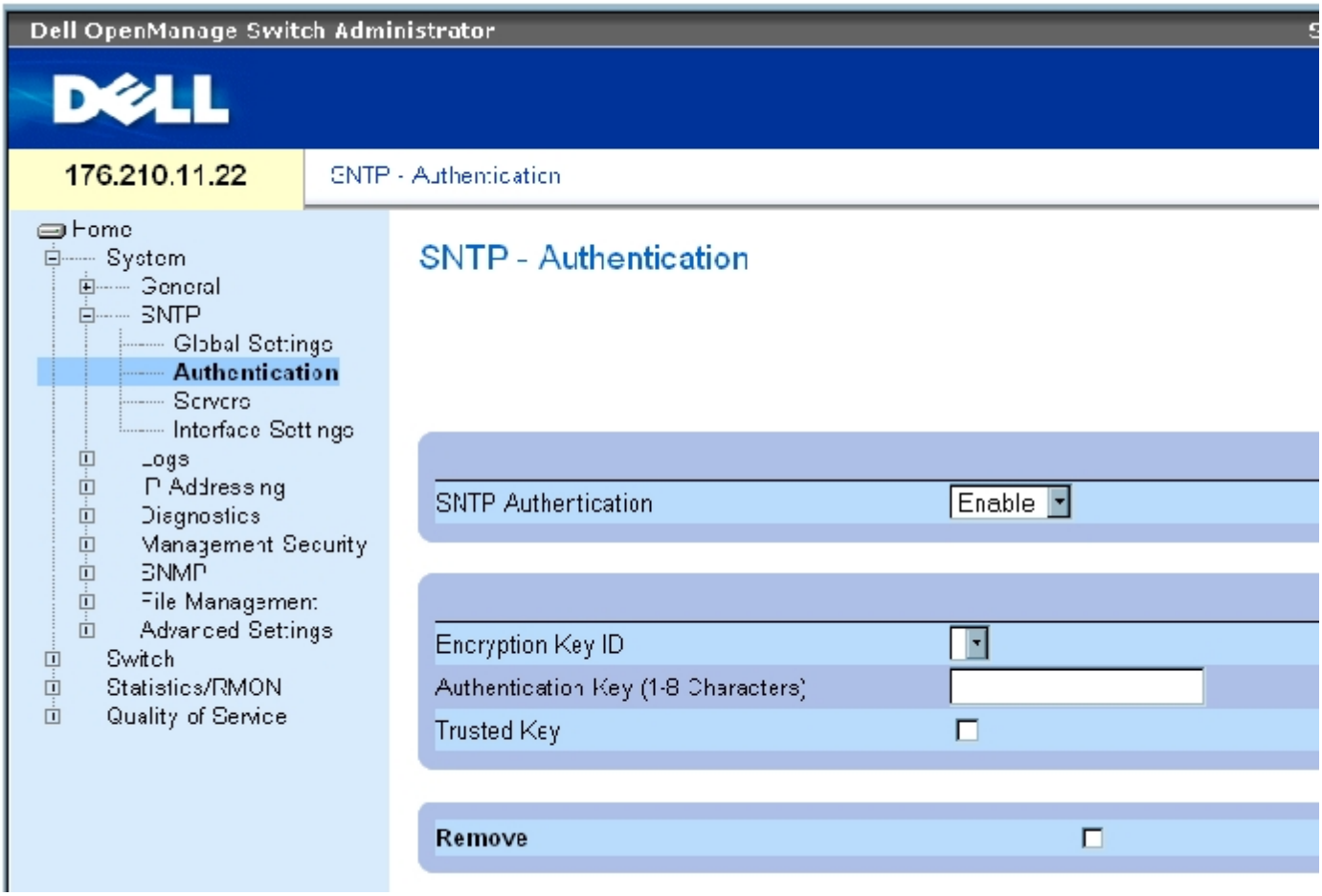
以下是 CLI 命令的示例：

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

定义 SNTP 验证方法

“SNTP Authentication”（SNTP 验证）页面用于在设备和 SNTP 服务器之间启用 SNTP 验证。还可以在“SNTP Authentication”（SNTP 验证）页面中选择用于验证 SNTP 服务器的方法。在树视图中单击“System”（系统）→“SNTP”→“Authentication”（验证）可以打开“SNTP Authentication”（SNTP 验证）页面。

图 6-9. SNTP 验证



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

“SNTP Authentication” (SNTP 验证) — 启用在设备和 SNTP 服务器之间验证 SNTP 会话 (启用时) 。

“Encryption Key ID” (密钥 ID) — 定义用于验证 SNTP 服务器和设备的密钥标识。该字段值最大可为 4294967295。

“Authentication Key (1-8 Characters)” (验证密钥 [1 至 8 个字符]) — 用于验证的密钥。

“Trusted Key” (信任密钥) — 表示验证 SNTP 服务器时使用的密钥 (单点传送) 。

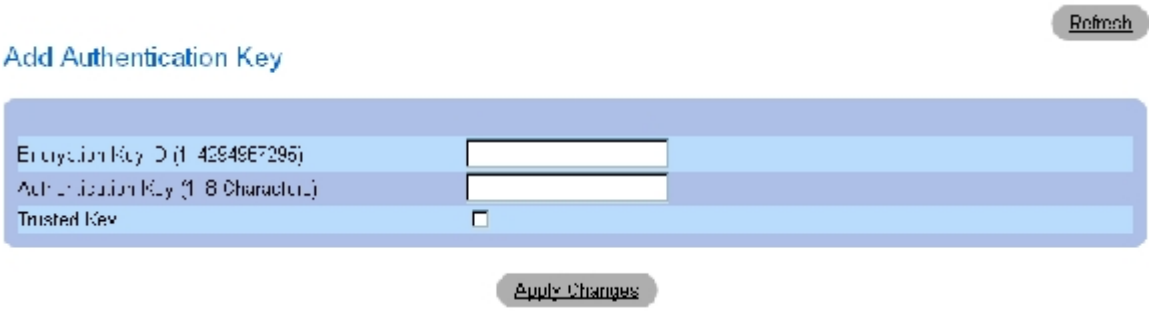
“Remove” (删除) — 如果选取此字段，将删除选定的验证密钥。

添加 SNTP 验证密钥

1. 打开“SNTP Authentication” (SNTP 验证) 页面。
2. 单击“Add” (添加) 。

系统将打开以下页面：

图 6-10. 添加验证密钥



3. 定义字段。

4. 单击“Apply Changes”（应用更改）。

系统将添加 SNTP 验证密钥，并更新设备。

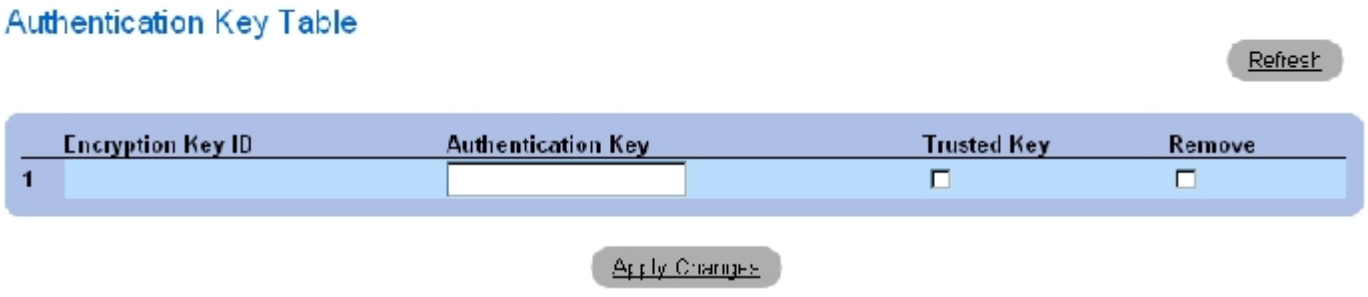
显示验证密钥表

1. 打开“SNTP Authentication”（SNTP 验证）页面。

2. 单击“Show All”（全部显示）。

系统将打开“Authentication Key Table”（验证密钥表）。

图 6-11. 验证密钥表



删除验证密钥

1. 打开“SNTP Authentication” (SNTP 验证) 页面。
2. 单击“Show All” (全部显示) 。

   系统将打开“Authentication Key Table” (验证密钥表) 。
3. 选择一个“Authentication Key Table” (验证密钥表) 条目。
4. 选取“Remove” (删除) 复选框。
5. 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

下表概括了用于设置“SNTP Authentication” (SNTP 验证) 页面中显示的字段的等效 CLI 命令。

表 6-21. SNTP 验证的 CLI 命令

CLI 命令	说明
sntp authenticate	定义从服务器接收到的简单网络时间协议 (SNTP) 通信的验证。
sntp trusted key	验证 SNTP 将与之同步的系统的标识。
sntp authentication-key 数字 md5 值	定义 SNTP 的验证密钥。

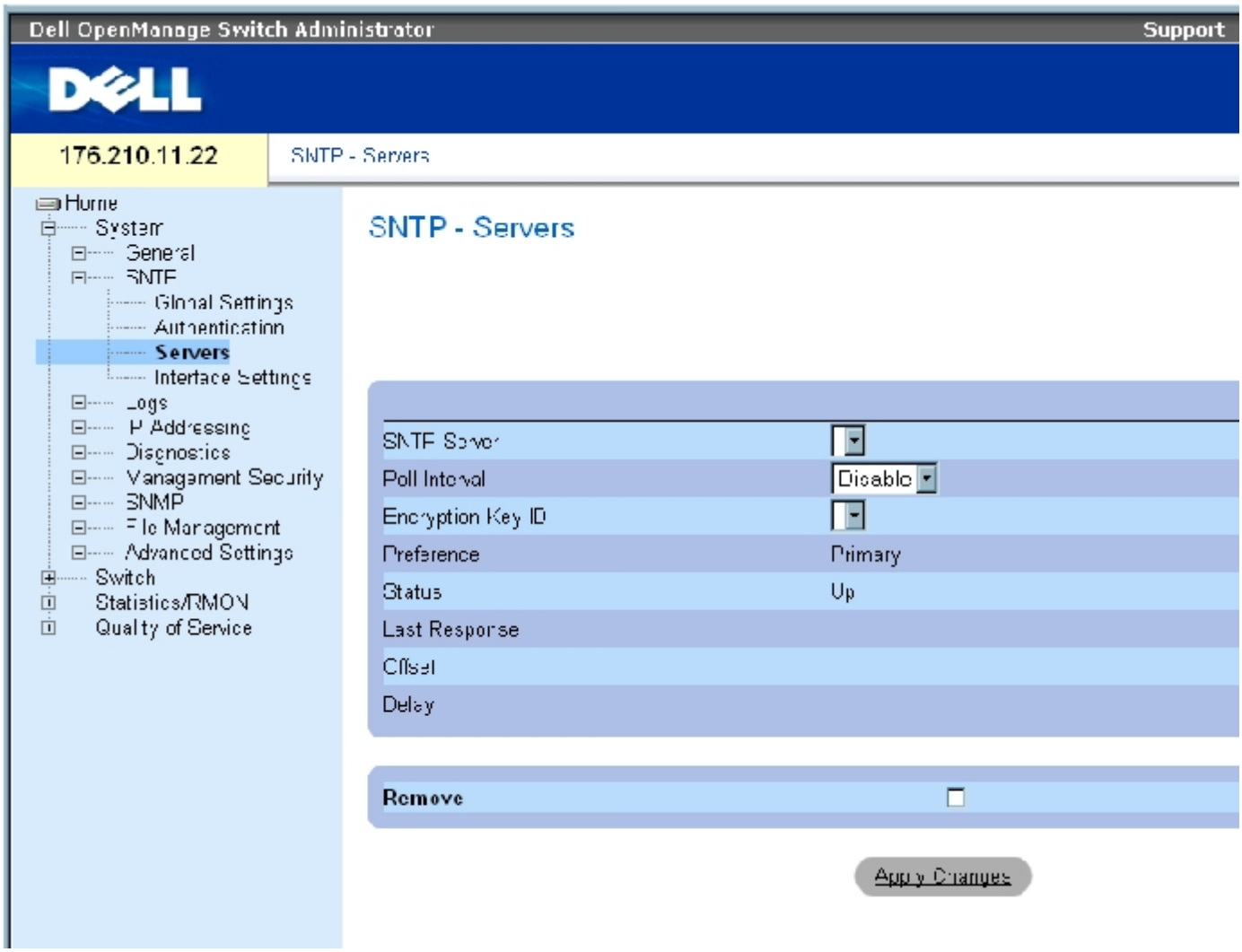
以下是 CLI 命令的示例：

```
console(config)# sntp
authentication-key 8 md5
Calked

console(config)# sntp
trusted-key 8

Console(config)# sntp
authenticate
```

定义 SNTP 服务器

您可以通过“SNTP Servers” (SNTP 服务器)页面启用 SNTP 服务器以及添加新的 SNTP 服务器。要打开“SNTP Servers” (SNTP 服务器)页面，请在树视图中单击“System” (系统) → “SNTP” → “Servers” (服务器) 。

图 6-12. SNTP 服务器



“SNTP Servers” (SNTP 服务器)页面包含以下字段：

“SNTP Server” (SNTP 服务器) — 选择用户定义的 SNTP 服务器 IP 地址。最多可以定义八个 SNTP 服务器。

“Poll Interval” (轮询间隔) — 启用向选定的 SNTP 服务器轮询系统时间信息 (启用时) 。

“Encryption Key ID” (密钥 ID) — 表示用于 SNTP 服务器和设备之间通信的密钥标识。范围是 1 至 4294967295。

“Preference” (首选项) — 提供 SNTP 系统时间信息的 SNTP 服务器。可能的字段值包括：

“Primary” (主) — 主服务器提供 SNTP 信息。

“Secondary”（次）— 备份服务器提供 SNTP 信息。

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

“Up”（良好）— SNTP 服务器当前运行正常。

“Down”（断开）— 表示 SNTP 服务器当前不可用。例如，SNTP 服务器当前未连接或处于断开状态。

“In progress”（正在进行）— 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”（上一次响应）— 上一次接收到 SNTP 服务器响应的时间。

“Offset”（偏移）— 设备本地时钟和从 SNTP 服务器获得的时间之间的时间戳差值。

“Delay”（延迟）— 到达 SNTP 服务器所需的时间。

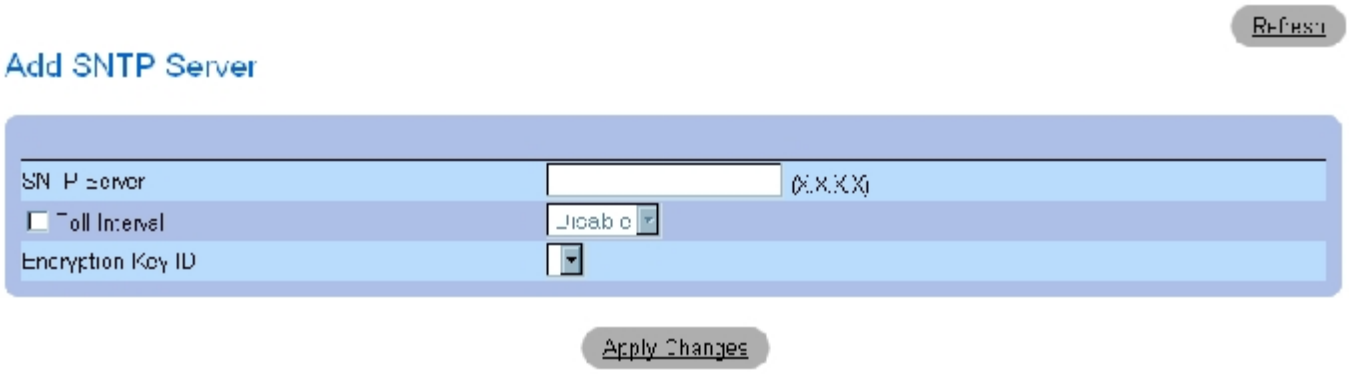
“Remove”（删除）— 如果选择此字段，将从“SNTP Servers”（SNTP 服务器）列表中删除特定的 SNTP 服务器。

添加 SNTP 服务器

1. 打开“SNTP Servers”（SNTP 服务器）页面。
2. 单击“Add”（添加）。

系统将打开“Add SNTP Server”（添加 SNTP 服务器）页面：

图 6-13. 添加 SNTP 服务器



3. 定义字段。

4. 单击“Apply Changes”（应用更改）。

系统将添加 SNTP 服务器，并更新设备。

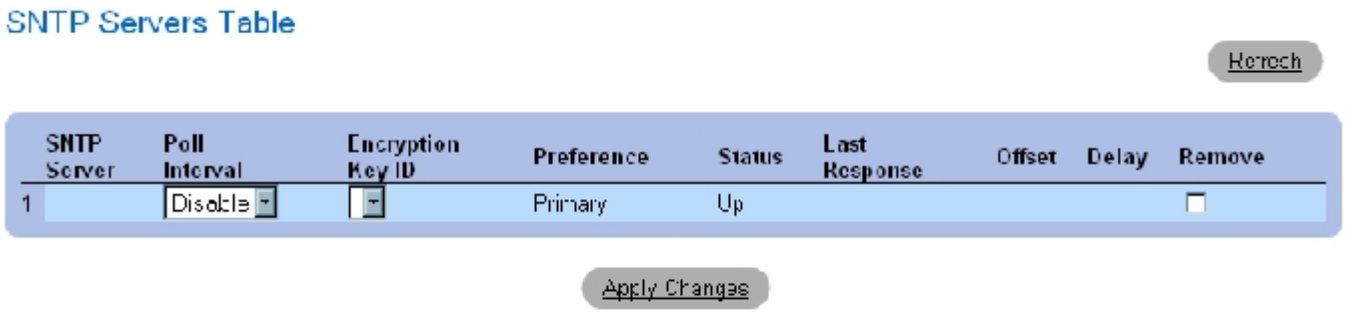
显示 SNTP 服务器表

1. 打开“SNTP Servers”（SNTP 服务器）页面。

2. 单击“Show All”（全部显示）。

系统将打开“SNTP Servers Table”（SNTP 服务器表）：

图 6-14. SNTP 服务器表



修改 SNTP 服务器

1. 打开“SNTP Servers”（SNTP 服务器）页面。

2. 单击“Show All”（全部显示）。

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

3. 选择一个 SNTP 服务器条目。

4. 修改相关的字段。

5. 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

1. 打开“SNTP Servers”（SNTP 服务器）页面。

2. 单击“Show All”（全部显示）。

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

3. 选择一个“SNTP Server”（SNTP 服务器）条目。

4. 选取“Remove”（删除）复选框。

5. 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 服务器设置

下表概括了用于设置“SNTP Server”（SNTP 服务器）页面中显示的字段的等效 CLI 命令。

表 6-22. SNTP 服务器 CLI 命令

CLI 命令	说明
sntp server IP 地址|主机名称 [poll] [key 密钥 ID]	配置设备以使用 SNTP 从服务器请求和接受 SNTP 通信。

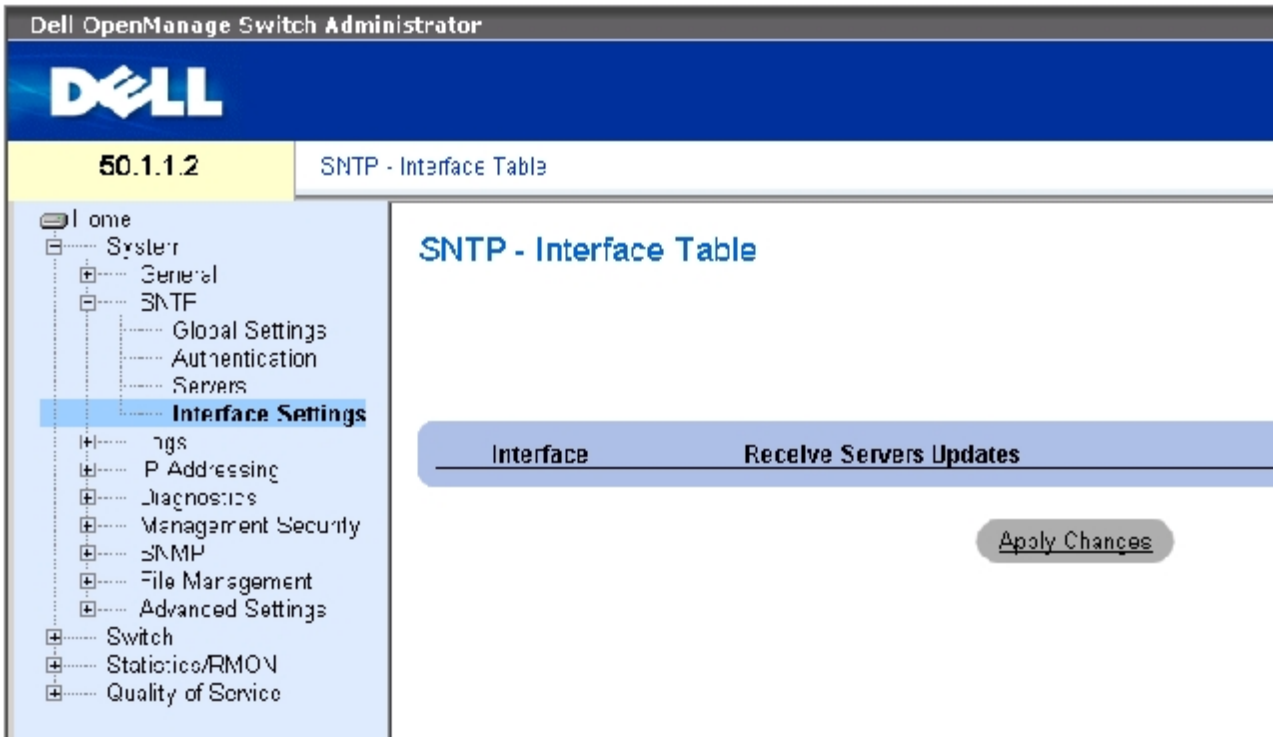
以下是 CLI 命令的示例：

```
Console(config)# sntp
server 100.1.1.1 poll key
10
```

定义 SNTP 接口

“SNTP Interface Settings” (SNTP 接口设置) 页面包含 SNTP 接口信息。要打开“SNTP Interface Settings” (SNTP 接口设置) 页面，请单击“System” (系统) → “SNTP” → “Interface Settings” (接口设置) 。

图 6-15. SNTP 接口设置



“SNTP Interface Settings” (SNTP 接口设置) 页面包含以下字段：

“Unit No.” (装置号) — 表示已启用 SNTP 接口的堆栈成员。

“Interface” (接口) — 包含可以在其上启用 SNTP 的接口列表。

“Receive Servers Updates” (接收服务器更新) — 在特定接口上启用或禁用 SNTP。

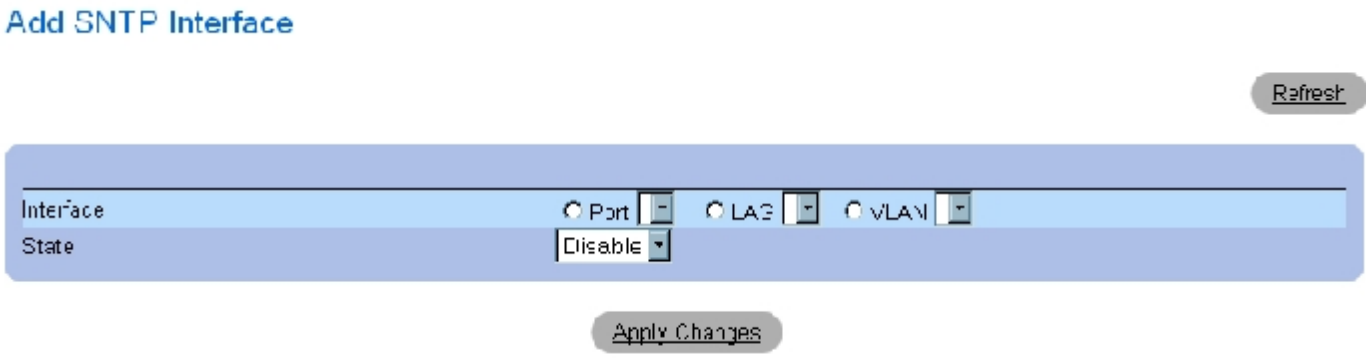
“Remove”（删除）— 如果选择此字段，将从特定接口删除 SNTP。

添加 SNTP 接口

1. 打开“SNTP Interface Settings”（SNTP 接口设置）页面。
2. 单击“Add”（添加）。

   系统将打开“Add SNTP Interface”（添加 SNTP 接口）页面。

图 6-16. 添加 SNTP 接口



3. 定义相关的字段。
4. 单击“Apply Changes”（应用更改）。

   系统将添加 SNTP 接口，并更新设备。

使用 CLI 命令定义 SNTP 接口设置

下表概括了用于设置“SNTP Interface Settings”（SNTP 接口设置）页面中显示的字段的等效 CLI 命令。

注：必须在接口上定义 IP 地址后才能将该接口定义为任意点传送接口或广播接口。

表 6-23. SNTP 接口设置的 CLI 命令

CLI 命令	说明

sntp client enable	在接口上启用简单网络时间协议（SNTP）客户端。
show sntp configuration	显示简单网络时间协议（SNTP）的配置。

以下是用于显示 SNTP 接口的 CLI 命令的示例：

```
Console# show sntp configuration
Polling interval:7200 seconds.

MD5 Authentication keys: 8, 9
Authentication is required for synchronization.
Trusted Keys: 8,9

Unicast Clients Polling:Enabled.
```

Server	Polling	Encryption Key
----------	--------	---------------
176.1.1.8	Enabled	9
176.1.8.179	Disabled	Disabled
Broadcast Clients:Enabled		
Broadcast Clients Poll:Enabled		
Broadcast Interfaces:1/e1, 1/e3		

管理日志

“Logs”（日志）页面包含指向各种日志页面的链接。要打开“Logs”（日志）页面，请在树视图中单击“System”（系统）→“Logs”（日志）。

定义全局日志参数

系统日志使您可以实时查看设备事件，并记录这些事件以便将来使用。系统日志记录和管理事件并报告错误或信息。

事件信息具有唯一的格式，即按照系统日志协议建议的信息格式报告所有错误。例如，系统日志和本地设备报告信息会被分配一个严重性代码，并

包含一个信息助记符，用于标识生成信息的源应用程序。允许按照紧急性或相关性筛选信息。由系统日志配置参数控制日志信息向各目的地的分配，例如日志缓冲区、日志文件或系统日志服务器。用户最多可以定义八个系统日志服务器。

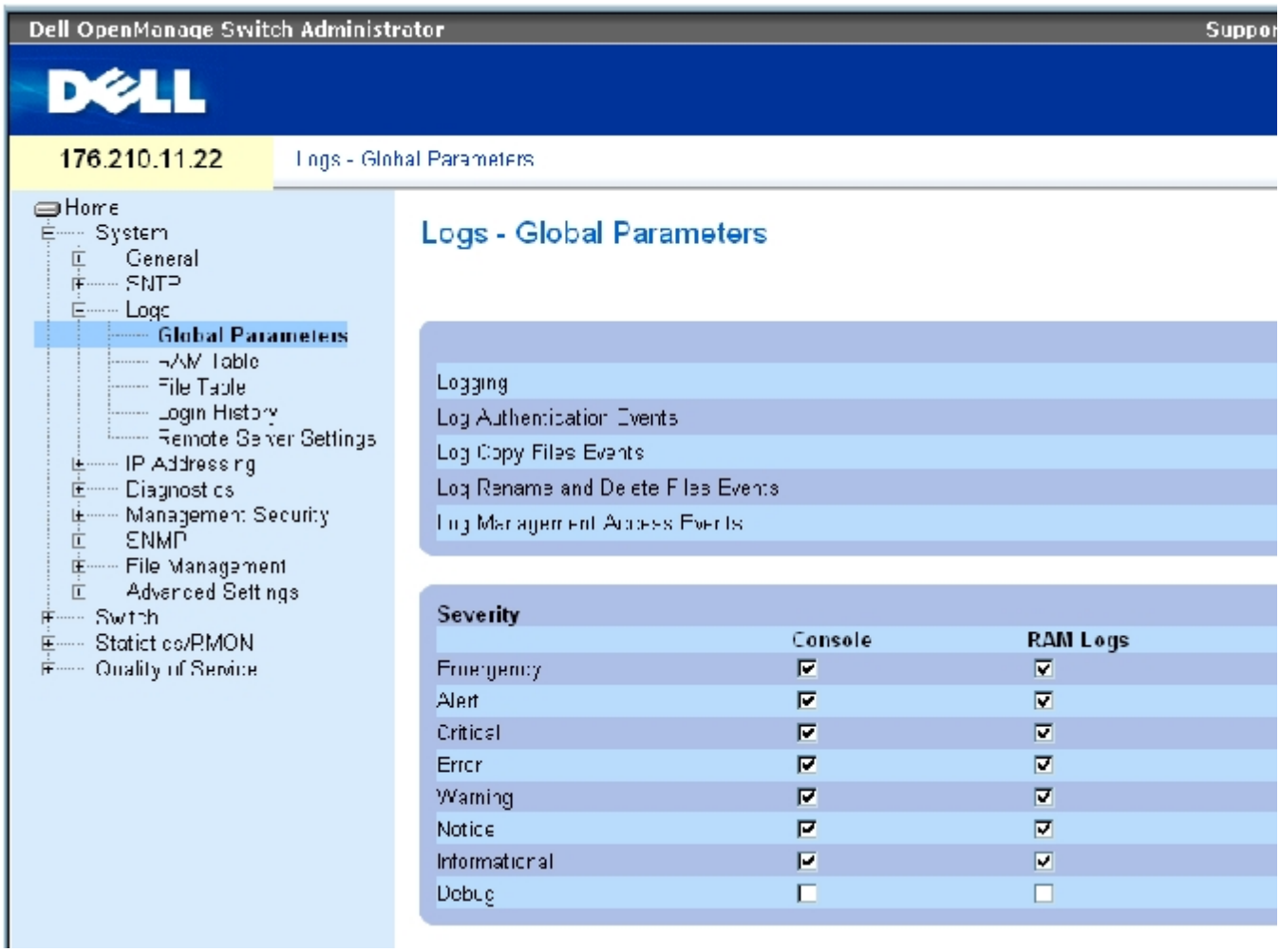
下表包含日志严重性级别：

表 6-24. 日志严重性级别

严重性类型	严重性级别	说明
紧急	0	系统无法运行。
警报	1	系统需要立即引起注意。
严重	2	系统处于严重状态。
错误	3	出现了系统错误。
警告	4	出现了系统警告。
注意	5	系统运行正常，但出现系统注意信息。
信息	6	提供设备信息。
调试	7	提供关于日志的详细信息。如果出现调试错误，请与 Dell 在线技术支持联络。

“Global Log Parameters”（全局日志参数）页面包含用于定义将哪些事件记录到哪些日志的字段。该页面包含用于全局启用日志的字段，以及用于定义日志参数的字段。严重性日志信息按照严重性从高到低的顺序列出。要打开“Global Log Parameters”（全局日志参数）页面，请在树视图中单击“System”（系统）→“Logs”（日志）→“Global Parameters”（全局参数）。

图 6-17. 全局日志参数



“Global Log Parameters”（全局日志参数）页面包含以下参数：

“Logging”（记录）— 为高速缓存、文件和服务器日志启用设备全局日志。默认情况下，控制台日志处于启用状态。

“Log Authentication Events”（验证事件日志）— 验证用户时生成日志。

“Log Copy Files Events”（复制文件事件日志）— 复制文件时生成日志。

“Log Rename and Delete Files Events”（重命名和删除文件事件日志）— 重命名或删除备份配置文件时生成日志。

“Log Management Access Events”（管理访问事件日志）— 使用管理方法访问设备时生成日志。例如，每次使用 SSH 访问设备时，都将生成一个设备日志。

“Severity”（严重性）— 以下为可用的严重性日志：

“Emergency”（紧急）— 最高级别的警告。如果设备停机或运行不正常，将在指定的记录位置保存紧急日志信息。

“Alert”（警报）— 第二级警告。如果设备出现严重故障，将保存警报日志；例如，试图下载不存在的配置文件。

“Critical”（严重）— 第三级警告。如果设备出现严重故障（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），系统将保存严重日志。

“Error”（错误）— 设备出现错误，例如，复制操作失败。

“Warning”（警告）— 最低级设备警告。例如，设备正在运行，但端口链接当前处于断开状态。

“Notice”（注意）— 提供重要的设备信息。

“Informational”（信息）— 提供设备信息。例如，端口当前状态良好。

“Debug”（调试）— 提供调试信息。

注：选定严重性级别后，所有高于此级别的严重性级别都将被自动选定。

“Global Log Parameters”（全局日志参数）页面还包含对应于各个日志系统的复选框：

“Console”（控制台）— 发送到控制台的日志的最低严重性级别。

“RAM Logs”（RAM 日志）— 发送到 RAM（高速缓存）中保存的日志文件的日志的最低严重性级别。

“Log File”（日志文件）— 发送到 FLASH 存储器中保存的日志文件的日志的最低严重性级别。

要启用日志，请：

1. 打开“Global Log Parameters”（全局日志参数）页面。
2. 在“Logging”（日志）下拉列表中选择“Enable”（启用）。
3. 在“Global Log Parameters”（全局日志参数）复选框中选择日志类型和日志严重性。
4. 单击“Apply Changes”（应用更改）。

系统将保存日志设置，并更新设备。

使用 CLI 命令启用日志

下表概括了用于设置“Global Log Parameters”（全局日志参数）页面中显示的字段的等效 CLI 命令。

表 6-25. 全局日志参数的 CLI 命令

CLI 命令	说明
logging on	启用错误信息记录。
logging {IP 地址 | 主机名称} [port 端口] [severity 级别] [facility 设备] [description 文本]	将信息记录到系统日志服务器。有关严重性级别的列表，请参阅“日志严重性级别”。
logging console 级别	根据严重性限制记录到控制台的信息。
logging buffered 级别	根据严重性限制内部缓冲区（RAM）显示的系统日志信息。
logging file 级别	根据严重性限制发送至日志文件的系统日志信息。
clear logging	清除日志。
clear logging file	清除日志文件中的信息。

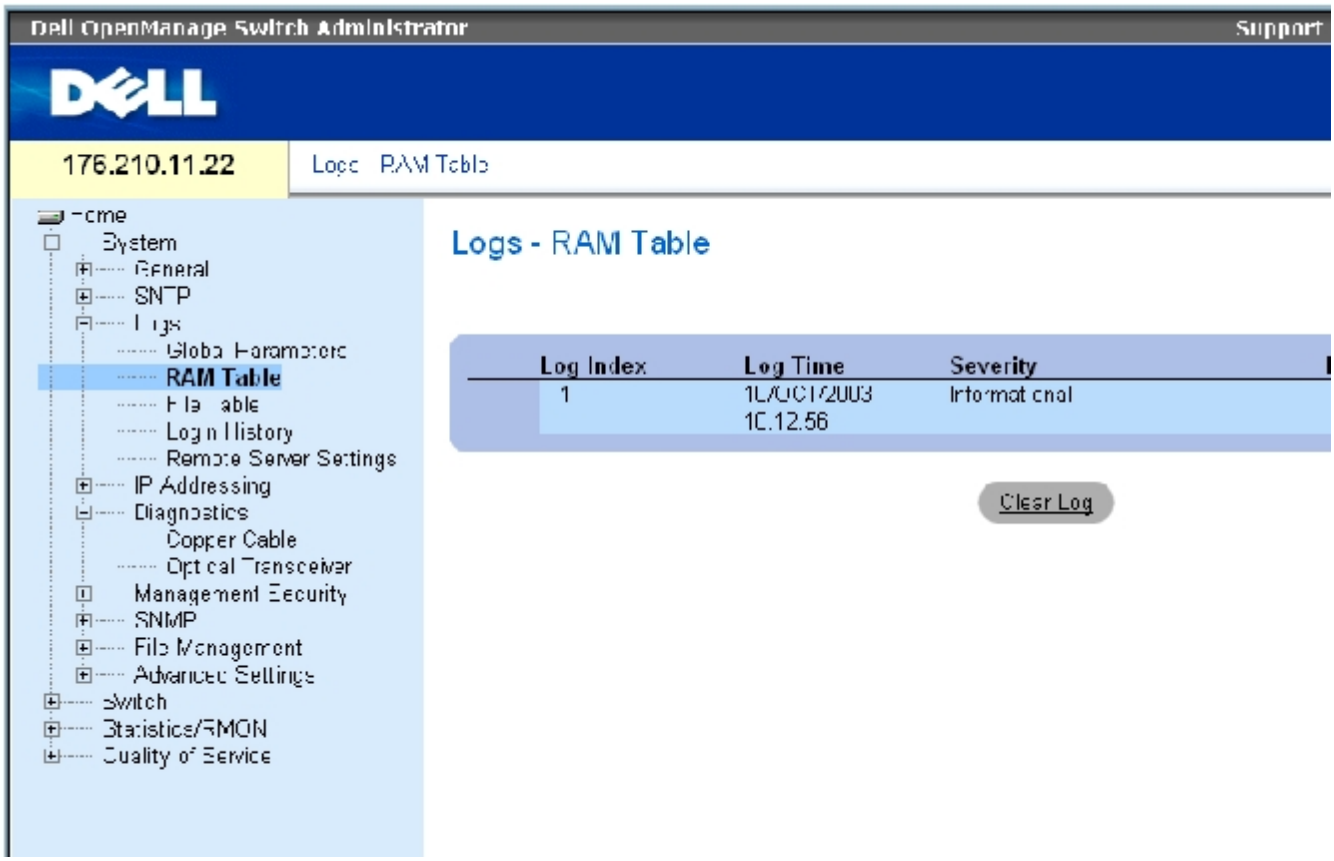
以下是 CLI 命令的示例：

```
console(config)# logging
on

console(config)# logging
console errors

console(config)# logging
buffered debugging

console(config)# logging
file alerts

console(config)# end

console# clear logging
file

Clear Logging File [y/n]y
```

查看 RAM 日志表

“RAM Log Table”（RAM 日志表）包含有关 RAM 中保存的日志条目的信息，包括日志输入时间、日志严重性以及日志说明。要打开“RAM Log Table”（RAM 日志表），请在树视图中单击“System”（系统）→“Logs”（日志）→“RAM Table”（RAM 表）。

图 6-18. RAM 日志表



“RAM Log Table” (RAM 日志表) 包含以下字段：

“Log Index” (日志索引) — “RAM Log Table” (RAM 日志表) 中的日志编号。

“Log Time” (记录时间) — 表示日志输入“RAM Log Table” (RAM 日志表) 的时间。

“Severity” (严重性) — 表示日志严重性。

“Description” (说明) — 日志条目的说明。

要删除日志信息，请：

1. 打开“RAM Log Table” (RAM 日志表)。
2. 单击“Clear Log” (清除日志)。

系统将从“RAM Log Table” (RAM 日志表) 中删除日志信息，并更新设备。

使用 CLI 命令查看和清除 RAM 日志表中的条目

下表概括了用于查看和清除“RAM Log Table” (RAM 日志表) 中显示的字段的等效 CLI 命令。

表 6-26. RAM 日志表的 CLI 命令

CLI 命令	说明
show logging	显示记录状态和存储在内部缓冲区中的系统日志信息。
clear logging	清除日志。

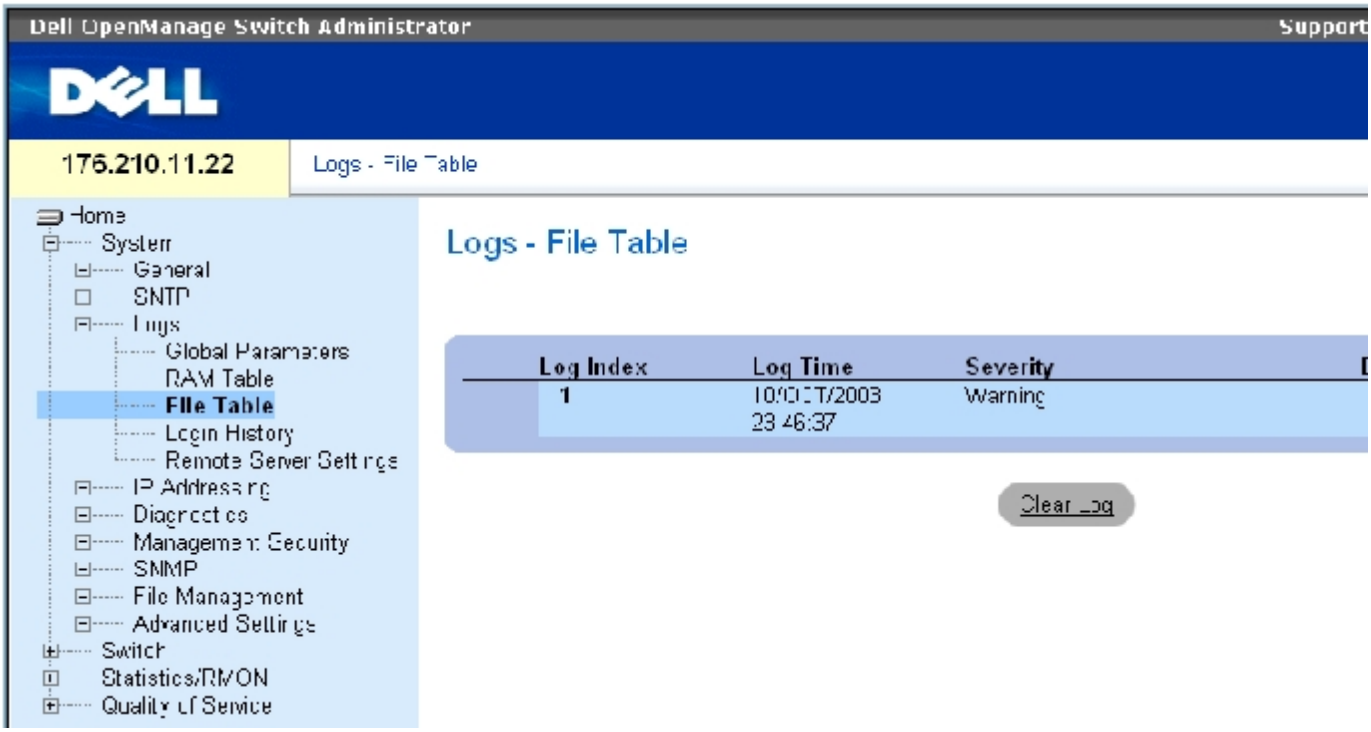
以下是 CLI 命令的示例：

```
console# show logging

Logging is enabled.

Console Logging:Level
info.Console Messages:0
Dropped.

Buffer Logging:Level
info.Buffer Messages:26
Logged, 26 Displayed, 200
Max.

File Logging:Level
error.File Messages:157
Logged, 26 Dropped.

1 messages were not logged

01-Jan-2000 01:03:42
:%INIT-I-Startup:Cold
Startup

01-Jan-2000 01:01:36
:%LINK-W-Down:1/e14

01-Jan-2000 01:01:36
:%LINK-W-Down:1/e13

01-Jan-2000 01:01:36
:%LINK-W-Down:1/e12

01-Jan-2000 01:01:36
:%LINK-W-Down:1/e15

01-Jan-2000 01:01:32
:%INIT-I-
InitCompleted:Initialization
task is completed




console# clear logging

Clear Logging Buffer [y/n]?
```

查看日志文件表

“Log File Table”（日志文件表）包含有关 FLASH 日志文件中保存的日志条目信息，包括日志输入时间、日志严重性以及日志信息说明。要打开“Log File Table”（日志文件表），请在树视图中单击“System”（系统）→“Logs”（日志）→“File Table”（文件表）。

图 6-19. 日志文件表



“Log File Table”（日志文件表）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。

“Log Time”（记录时间）— 表示日志输入“Log File Table”（日志文件表）的时间。

“Severity”（严重性）— 表示日志严重性。

“Description”（说明）— 日志信息文本。

使用 CLI 命令显示日志文件表

下表概括了用于查看和设置“Log File Table”（日志文件表）页面中显示的字段的等效 CLI 命令。

表 6-27. 日志文件表的 CLI 命令

CLI 命令	说明
show logging file	显示记录状态和存储在日志文件中的系统日志信息。
clear logging file	清除日志文件中的信息。

以下是 CLI 命令的示例：

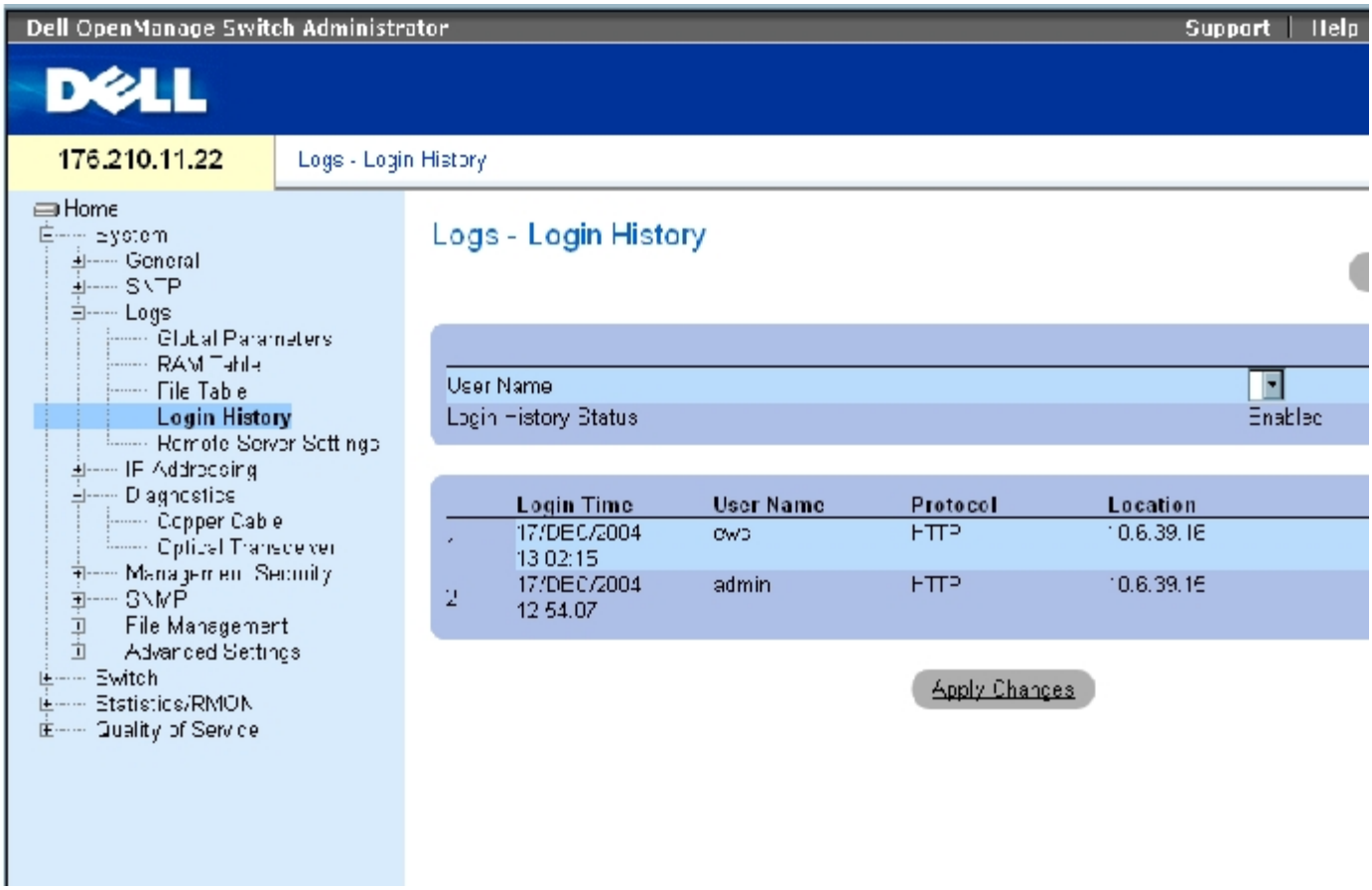
```
console# show logging file

Logging is enabled.

Console Logging:Level
info.Console Messages:0
Dropped.

Buffer Logging:Level
info.Buffer Messages:62
Logged, 62 Displayed, 200
Max.

File Logging:Level
debug.File Messages:11
Logged, 51 Dropped.

SysLog server 12.1.1.2
Logging:warning.Messages:14
Dropped.

SysLog server 1.1.1.1
Logging:info.Messages:0
Dropped.

01-Jan-2000 01:12:01
:%COPY-W-TRAP:The copy
operation was completed
successfully

01-Jan-2000 01:11:49
:%LINK-I-Up:1/e11

01-Jan-2000 01:11:46
:%LINK-I-Up:1/e12

01-Jan-2000 01:11:42
:%LINK-W-Down:1/e13

01-Jan-2000 01:11:35
:%LINK-I-Up:1/e14
```

查看设备登录历史记录

“Login History”（登录历史记录）页面包含用于查看和监视设备使用情况的信息，包括用户登录设备的时间和登录设备时使用的协议。

要打开“Login History”（登录历史记录）页面，请在树视图中单击“System”（系统）→“Logs”（日志）→“Login History”（登录历史记录）。

图 6-20. 登录历史记录



"Login History" (登录历史记录) 页面包含以下字段:

"User Name" (用户名) — 包含用户定义的设备用户名列表。

"Login History Status" (登录历史记录状态) — 表示设备上是否启用了密码历史记录日志。

"Login Time" (登录时间) — 表示所选用户登录到设备的时间。

"User Name" (用户名) — 表示登录到设备的用户。

"Protocol" (协议) — 表示用户登录到设备的方法。

"Location" (位置) — 表示访问设备时所在站点的 IP 地址。

查看登录历史记录

1. 打开"Login History" (登录历史记录) 页面。

2. 在“User Name”（用户名）字段中选择一个用户。

3. 单击“Apply Changes”（应用更改）。

系统将显示所选用户的登录信息。

使用 CLI 命令显示设备登录历史记录

下表概括了用于查看和设置“Login History”（登录历史记录）页面中显示的字段的等效 CLI 命令。

表 6-28. 设备登录历史记录的 CLI 命令

CLI 命令	说明
show users login-history	显示密码管理历史记录信息。

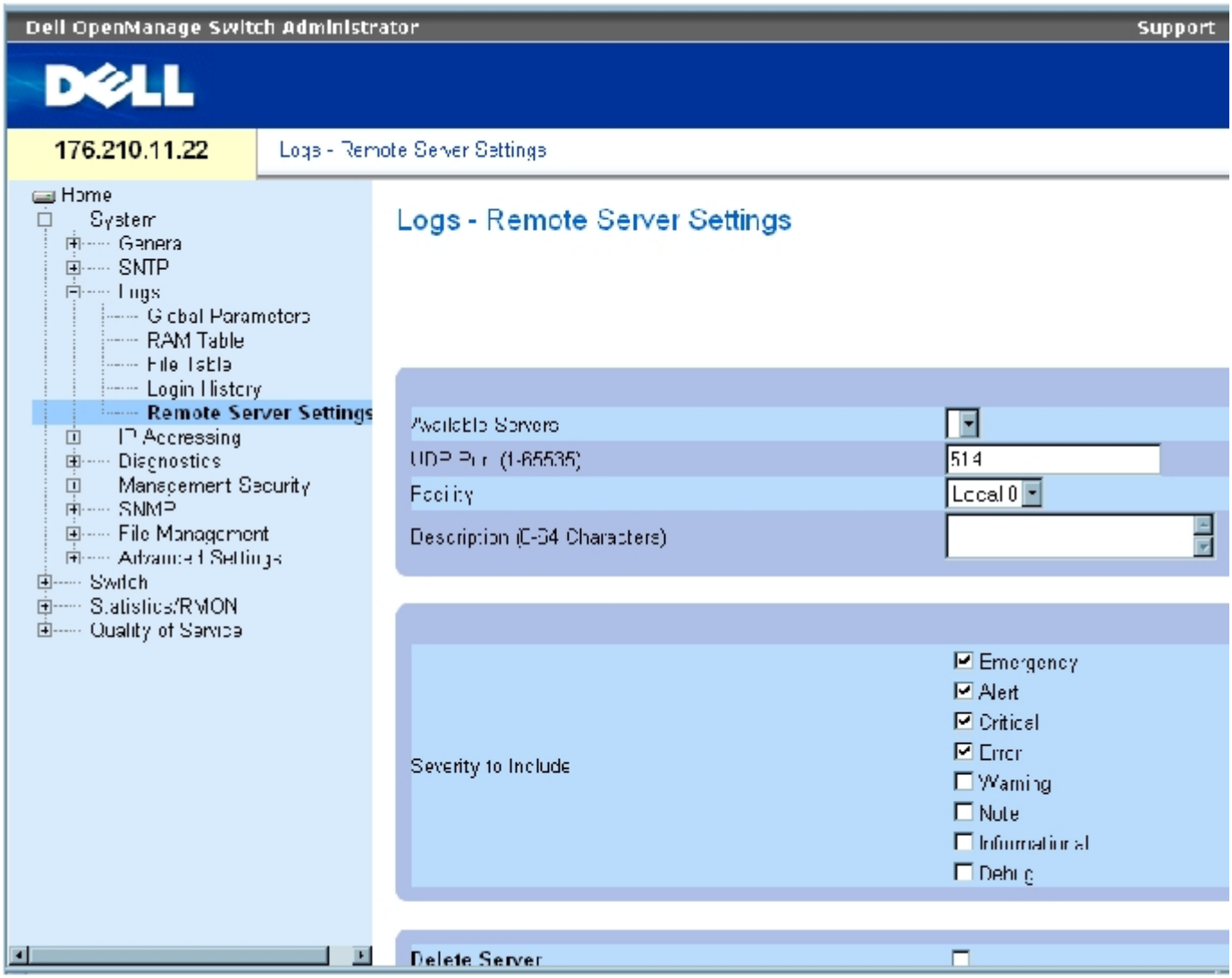
以下是 CLI 命令的示例：

```
console# show users login-history

Login Time          Username    Protocol    Location
------------------  --------    --------    ----------
Jan 1. 2005 23:58:17  Anna      HTTP        172.16.1.8
Jan 1. 2005 07:59:23  Errol     HTTP        172.16.0.8
Jan 1. 2005 08:23:48  Amy       Serial
Jan 1. 2005 08:29:29  Alan      SSH         172.16.0.8
Jan 1. 2005 08:42:31  Bob       HTTP        172.16.0.1
Jan 1. 2005 08:49:52  Cindy     Telnet      172.16.1.7
```

修改远程日志服务器定义

“Remote Log Server Settings”（远程日志服务器设置）页面包含用于查看和配置可用日志服务器的字段。此外，还可以定义新的日志服务器以及发送至各服务器的日志严重性。要打开“Remote Log Server Settings”（远程日志服务器设置）页面，请在树视图中单击“System”（系统）→“Logs”（日志）→“Remote Server Settings”（远程服务器设置）。

图 6-21. 远程日志服务器设置



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

“Available Servers”（可用服务器）— 包含可以接收日志的服务器的列表。

“UDP Port (1-65535)”（UDP 端口 [1 至 65535]）— 选定服务器上接收日志的 UDP 端口。可能范围为 1 至 65535。默认值为 514。

“Facility”（设备）— 定义从其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。如果分配了第二级设备，则第一级设备将被代替。为设备定义的所有应用程序在服务器上使用同一设备。此字段默认值为“Local 7”（本地 7）。可能的字段值包括：

“Local 0”（本地 0）至“Local 7”（本地 7）。

“Description (0-64 Characters)”（说明 [0 至 64 个字符]）— 用户定义的服务器说明。

“Delete Server”（删除服务器）— 如果选择此字段，将从“Available Servers”（可用服务器）列表中删除当前选定的服务器。

“Remote Log Server Settings”（远程日志服务器设置）页面还包含严重性列表。严重性定义与“Global Log Parameters”（全局日志参数）页面中的严重性定义相同。

要将日志发送至服务器，请：

1. 打开“Remote Log Server Settings”（远程日志服务器设置）页面。
2. 在“Available Servers”（可用服务器）下拉列表中选择服务器。
3. 定义字段。
4. 在“Severity to Include”（要包含的严重性）中选取要包含的日志严重性复选框。
5. 单击“Apply Changes”（应用更改）。

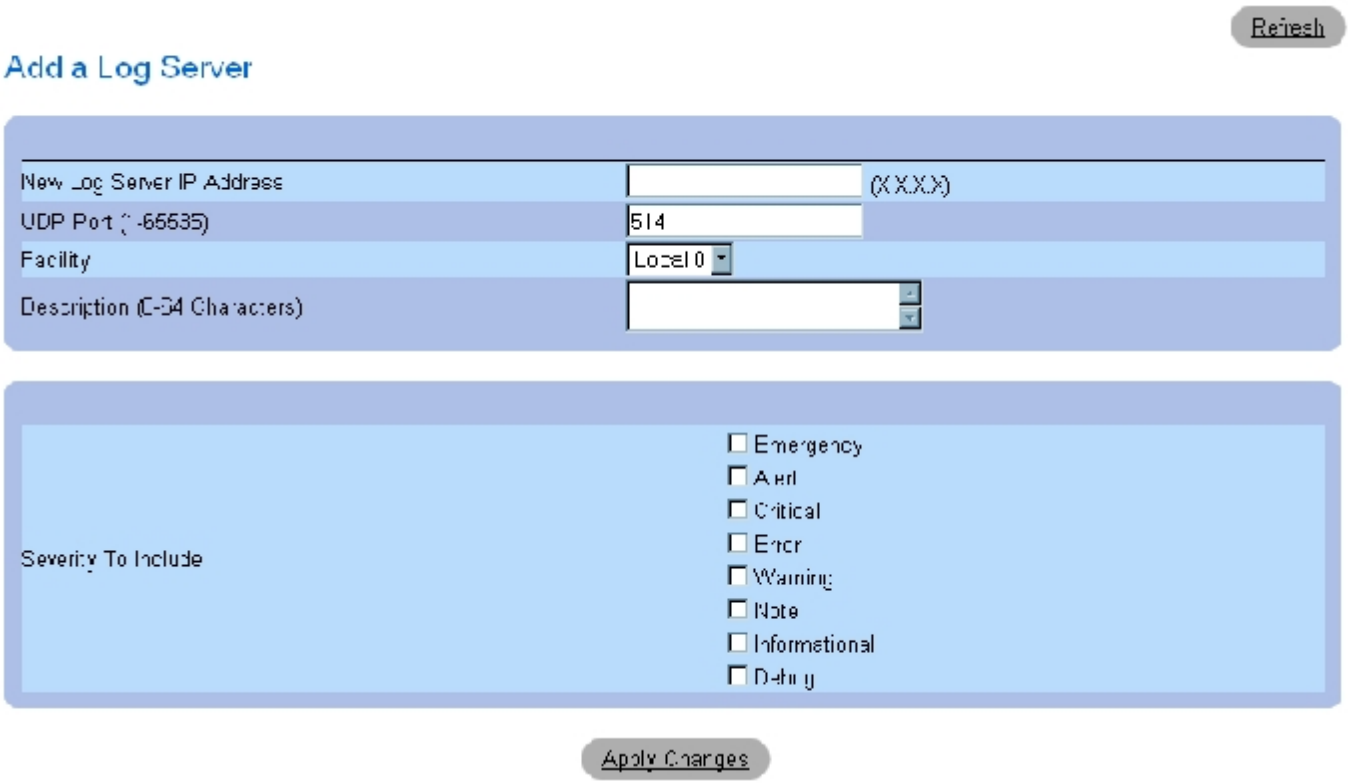
系统将保存日志设置，并更新设备。

要定义新服务器，请：

1. 打开“Remote Log Server Settings”（远程日志服务器设置）页面。
2. 单击“Add”（添加）。

系统将打开“Add a Log Server”（添加日志服务器）页面：

图 6-22. 添加日志服务器



“Add a Log Server”（添加日志服务器）页面包含以下附加字段：

“New Log Server IP Address”（新日志服务器 IP 地址）— 定义新日志服务器的 IP 地址。

3. 定义字段。

4. 单击“Apply Changes”（应用更改）。

系统将定义服务器并将其添加至“Available Servers”（可用服务器）列表。

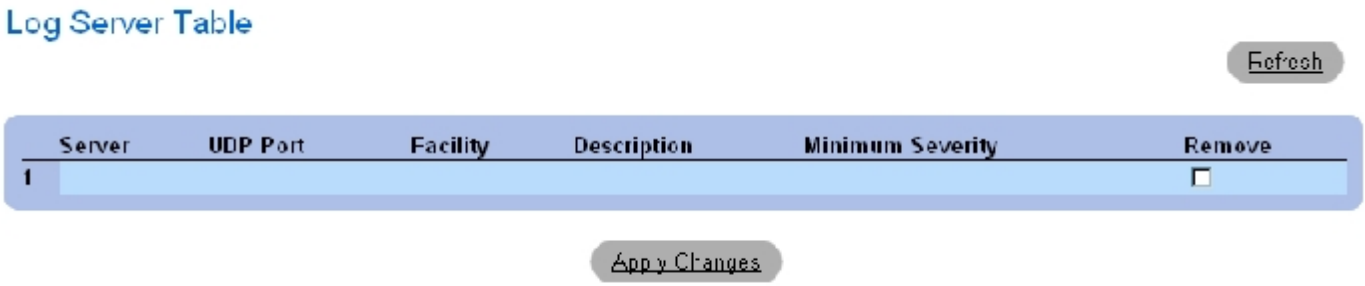
要显示远程日志服务器表，请：

1. 打开“Remote Log Server Settings”（远程日志服务器设置）页面。

2. 单击“Show All”（全部显示）。

系统将打开“Log Servers Table”（日志服务器表）页面：

图 6-23. 日志服务器表



要从“Log Servers Table”（日志服务器表）页面中删除日志服务器，请：

1. 打开“Remote Log Server Settings”（远程日志服务器设置）页面。
2. 单击“Show All”（全部显示）。

   系统将打开“Log Servers Table”（日志服务器表）页面。
3. 选择一个“Log Servers Table”（日志服务器表）条目。
4. 选取“Remove”（删除）复选框以删除选定的服务器。
5. 单击“Apply Changes”（应用更改）。

   系统将删除“Log Servers Table”（日志服务器表）条目，并更新设备。

使用 CLI 命令处理远程服务器日志

下表概括了用于处理远程日志服务器的等效 CLI 命令。

表 6-29. 远程日志服务器 CLI 命令

CLI 命令	说明
logging (IP 地址 | 主机名称) [port 端口] [severity 级别] [facility 设备] [description 文本]	将信息记录到远程服务器。
no logging	删除系统日志服务器。
show logging	显示记录状态和系统日志信息。

以下是 CLI 命令的示例：

```
console> enable

console# configure

console(config) # logging
10.1.1.1 severity critical

console(config)# end

console# show logging

Logging is enabled.

Console Logging:Level
debug.Console Messages:5
Dropped.

Buffer Logging:Level
debug.Buffer Messages:16
Logged, 16 Displayed, 200
Max.

File Logging:Level
error.File Messages:0
Logged, 209 Dropped.

SysLog server 31.1.1.2
Logging:error.Messages:22
Dropped.

SysLog server 5.2.2.2
Logging:info.Messages:0
Dropped.

SysLog server 10.2.2.2
Logging:critical.Messages:21
Dropped.

SysLog server 10.1.1.1
Logging:critical.Messages:0
Dropped.

1 messages were not logged

03-Mar-2004 12:02:03
:%LINK-I-Up:1/e11

03-Mar-2004 12:02:01
:%LINK-W-Down:1/e12

03-Mar-2004 12:02:01
:%LINK-I-Up:1/e13
```

定义 IP 定址

“IP Addressing”（IP 定址）页面包含用于分配接口和默认网关 IP 地址的链接，以及定义接口的 ARP 和 DHCP 参数的链接。要打开“IP Addressing”（IP 定址）页面，请在树视图中单击“System”（系统）→“IP Addressing”（IP 定址）。

定义默认网关

“Default Gateway”（默认网关）页面包含用于将网关分配给设备的字段。将信息包发送到远程网络时，信息包将被传输到默认的 IP。所配置的 IP 地址必须属于其中一个 IP 接口的同一 IP 地址子网。要打开“Default Gateway”（默认网关）页面，请在树视图中单击“System”（系统）→“IP Addressing”（IP 定址）→“Default Gateway”（默认网关）。

“Default Gateway”（默认网关）页面包含以下字段：

“User Defined”（定义的用户）— 设备的网关 IP 地址。

“Active”（活动）— 表示网关是否处于活动状态。

“Remove User Defined”（删除定义的用户）— 如果选择此字段，将从“Default Gateway”（默认网关）下拉式列表中删除设备的网关。

要选择设备的网关，请：

1. 打开“Default Gateway”（默认网关）页面。
2. 在“Default Gateway”（默认网关）下拉列表中选择一个 IP 地址。
3. 选取“Active”（活动）复选框。
4. 单击“Apply Changes”（应用更改）。

系统将选定设备的默认网关，并更新设备。

要删除设备的默认网关设备，请：

1. 打开“Default Gateway”（默认网关）页面。
2. 选取“Remove”（删除）复选框以删除默认网关。
3. 单击“Apply Changes”（应用更改）。

系统将删除默认网关条目，并更新设备。

使用 CLI 命令定义设备的网关

下表概括了用于设置“Default Gateway”（默认网关）页面中显示的字段的等效 CLI 命令。

表 6-30. 默认网关的 CLI 命令

CLI 命令	说明
ip default-gateway IP 地址	定义默认网关。
no ip default-gateway	删除默认网关。

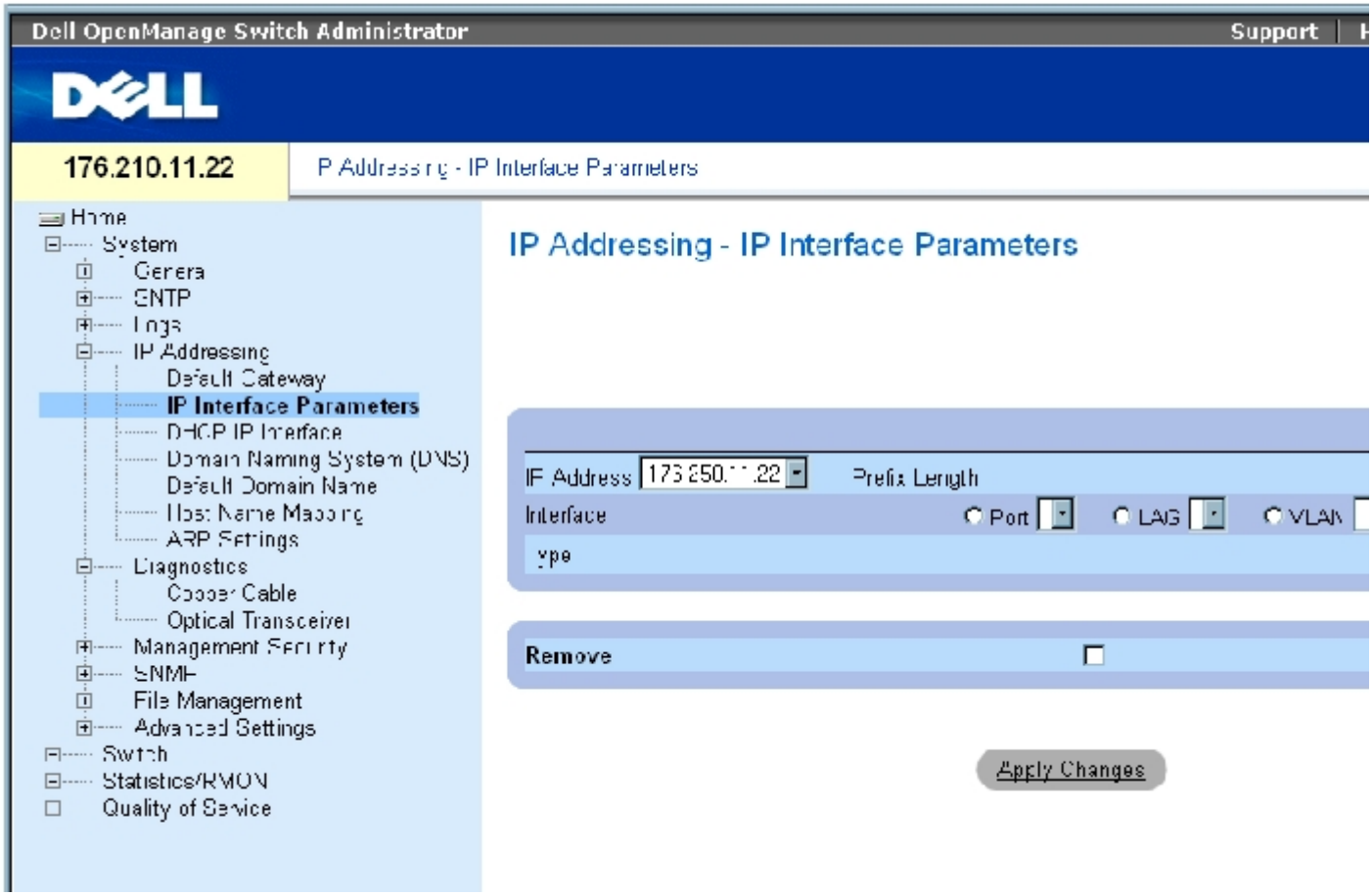
以下是 CLI 命令的示例：

```
console(config)# ip
default-gateway
196.210.10.1


console(config)# no ip
default-gateway
```

定义 IP 接口

“IP Interfaces Parameters”（IP 接口参数）页面包含用于为接口分配 IP 参数的字段。要打开“IP Interfaces Parameters”（IP 接口参数）页面，请在树视图中单击“System”（系统）→“IP Addressing”（IP 定址）→“IP Interface Parameters”（IP 接口参数）。

图 6-24. IP 接口参数



“IP Interfaces Parameters” (IP 接口参数) 页面包含以下参数：

“IP Address” (IP 地址) — 接口的 IP 地址。

“Prefix Length” (前缀长度) — 组成源 IP 地址前缀或源 IP 地址的网络掩码的位数。

“Source Interface” (源接口) — 为其定义 IP 地址的接口的类型。可以选择“Port” (端口)、“LAG”或“VLAN”。

“Type” (类型) — 表示 IP 地址是否是通过静态方式配置的。

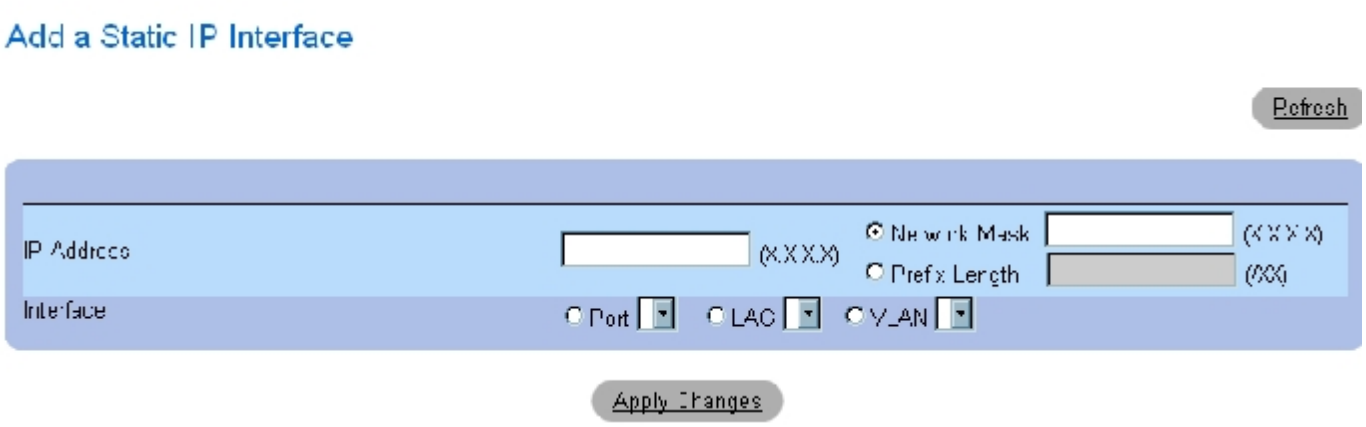
“Remove” (删除) — 如果选择此字段，将从“IP Address” (IP 地址) 下拉式菜单中删除接口。

添加 IP 接口

1. 打开“IP Interfaces Parameters” (IP 接口参数) 页面。
2. 单击“Add” (添加)。

系统将打开“Add a Static IP Interface”（添加静态 IP 接口）页面：

图 6-25. 添加静态 IP 接口



“Network Mask”（网络掩码）— 表示源 IP 地址的子网掩码。

3. 完成页面中的字段。

4. 单击“Apply Changes”（应用更改）。

系统会将新的 IP 地址添加至接口，并更新设备。

修改 IP 地址参数

1. 打开“IP Interfaces Parameters”（IP 接口参数）页面。

2. 在“IP Address”（IP 地址）下拉式菜单中选择一个 IP 地址。

3. 修改接口类型。

4. 单击“Apply Changes”（应用更改）。

系统将修改参数，并更新设备。

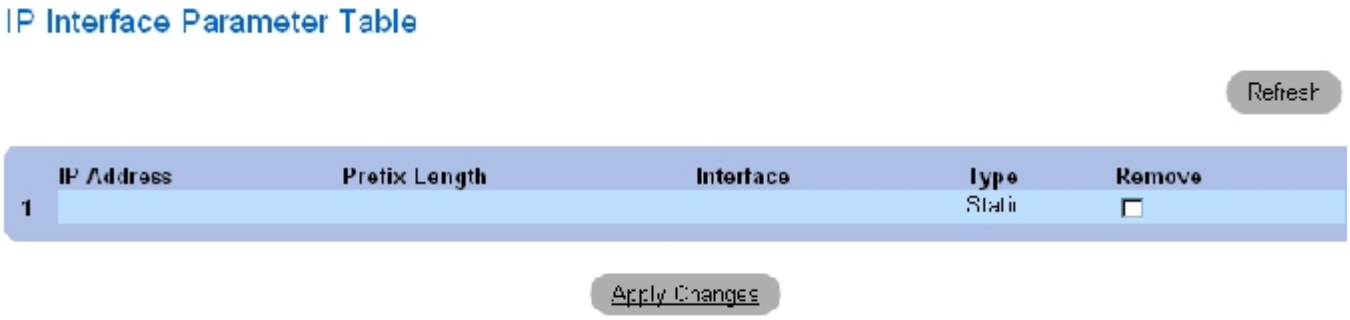
删除 IP 地址

1. 打开“IP Interfaces Parameters”（IP 接口参数）页面。

2. 单击“Show All”（全部显示）。

系统将打开“IP Interface Parameters Table”（IP 接口参数表）页面：

图 6-26. IP 接口参数表



3. 选择一个 IP 地址并选取“Remove”（删除）复选框。

4. 单击“Apply Changes”（应用更改）。

系统将删除选定的 IP 地址，并更新设备。

使用 CLI 命令定义 IP 接口

下表概括了用于设置“IP Interfaces Parameters”（IP 接口参数）页面中显示的字段的等效 CLI 命令。

表 6-31. IP 接口参数的 CLI 命令

CLI 命令	说明
ip address IP 地址 {掩码 | 前缀长度}	设置 IP 地址。
no ip address [IP 地址]	删除 IP 地址。
show ip interface [ethernet 接口号 | vlan VLAN ID | port-channel 号]	显示配置了 IP 的接口的可用性状态。

以下是 CLI 命令的示例：

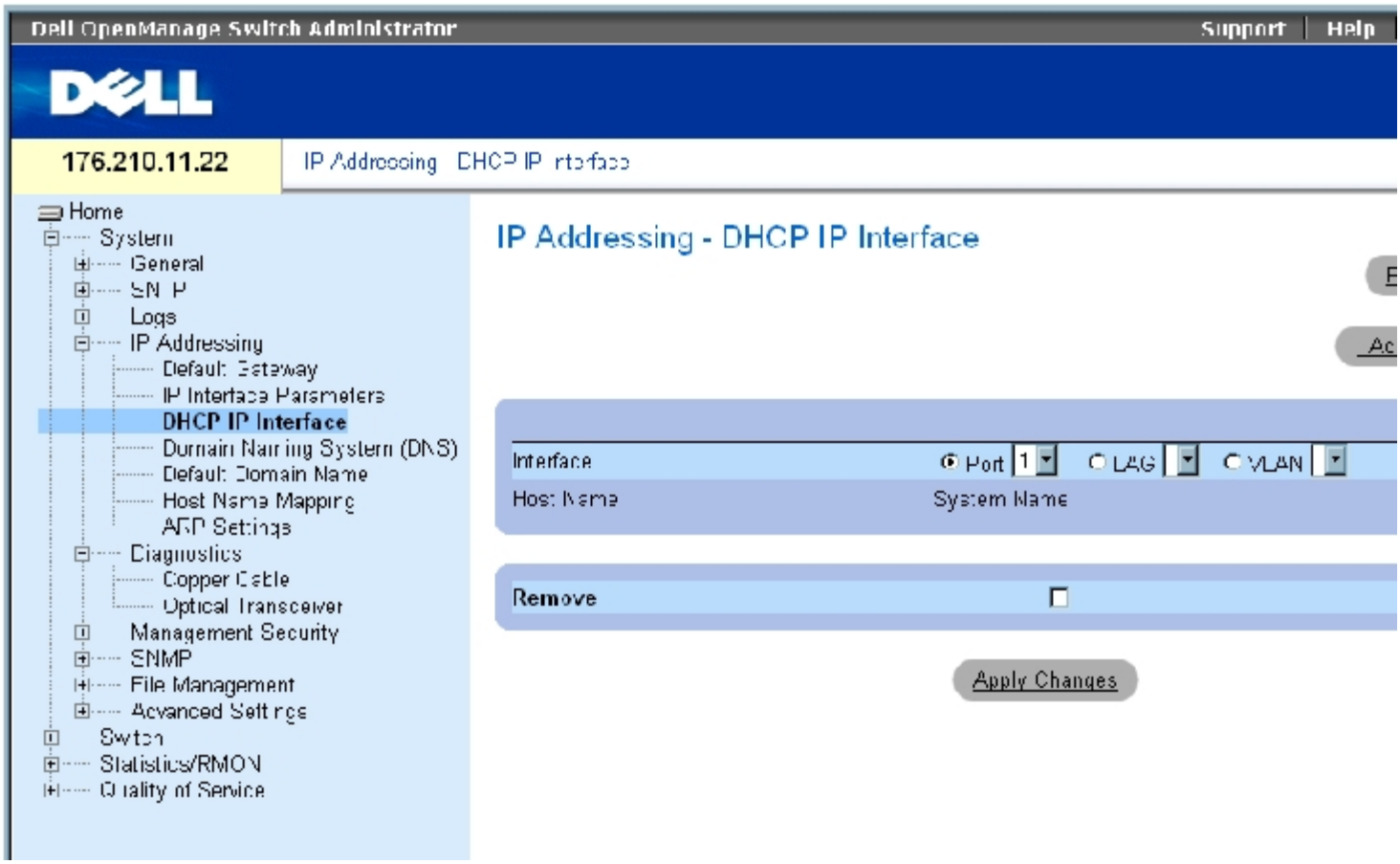
```
console(config)# interface
vlan 1
```

```
console(config-if)# ip
address 92.168.1.123
255.255.255.0


console(config-if)# no ip
address 92.168.1.123


console(config-if)# end


console# show ip interface
vlan 1


Gateway IP Address
Activity status


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


192.168.1.1 Active


IP address Interface Type


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


192.168.1.123/24 VLAN 1
Static
```

定义 DHCP IP 接口参数

“DHCP IP Interface” (DHCP IP 接口) 页面包含用于定义连接至设备的 DHCP 客户端的参数。要打开“DHCP IP Interface” (DHCP IP 接口) 页面，请在树视图中单击“System” (系统) → “IP Addressing” (IP 定址) → “DHCP IP Interface” (DHCP IP 接口) 。

图 6-27. DHCP IP 接口



“DHCP IP Interface” (DHCP IP 接口) 页面包含以下字段：

“Interface” (接口) — 连接至设备的特定接口。请单击“Port” (端口)、“LAG”或“VLAN”旁边的选项按钮，选择连接至设备的接口。

“Host Name” (主机名称) — 主机名称。

“Remove” (删除) — 如果选择此字段，将删除 DHCP 客户端。

添加 DHCP 客户端

1. 打开“DHCP IP Interface” (DHCP IP 接口) 页面。
2. 单击“Add” (添加)。

   系统将打开“Add DHCP IP Interface” (添加 DHCP IP 接口) 页面。
3. 完成页面中的信息。
4. 单击“Apply Changes” (应用更改)。

系统将添加 DHCP 接口，并更新设备。

修改 DHCP IP 接口

1. 打开“DHCP IP Interface” (DHCP IP 接口) 页面。
2. 修改字段。
3. 单击“Apply Changes” (应用更改) 。

系统将修改条目，并更新设备。

删除 DHCP IP 接口

1. 打开“DHCP IP Interface” (DHCP IP 接口) 页面。
2. 单击“Show All” (全部显示) 。

系统将打开“DHCP Client Table” (DHCP 客户端表) 。

3. 选择 DHCP 客户端条目。
4. 选取“Remove” (删除) 复选框。
5. 单击“Apply Changes” (应用更改) 。

系统将删除选定的条目，并更新设备。

使用 CLI 命令定义 DHCP IP 接口

下表概括了用于定义 DHCP 客户端的等效 CLI 命令。

表 6-32. DHCP IP 接口的 CLI 命令

CLI 命令	说明
ip address dhcp [hostname 主机名称]	通过动态主机配置协议 (DHCP) 获得以太网接口上的 IP 地址。

以下是 CLI 命令的示例：

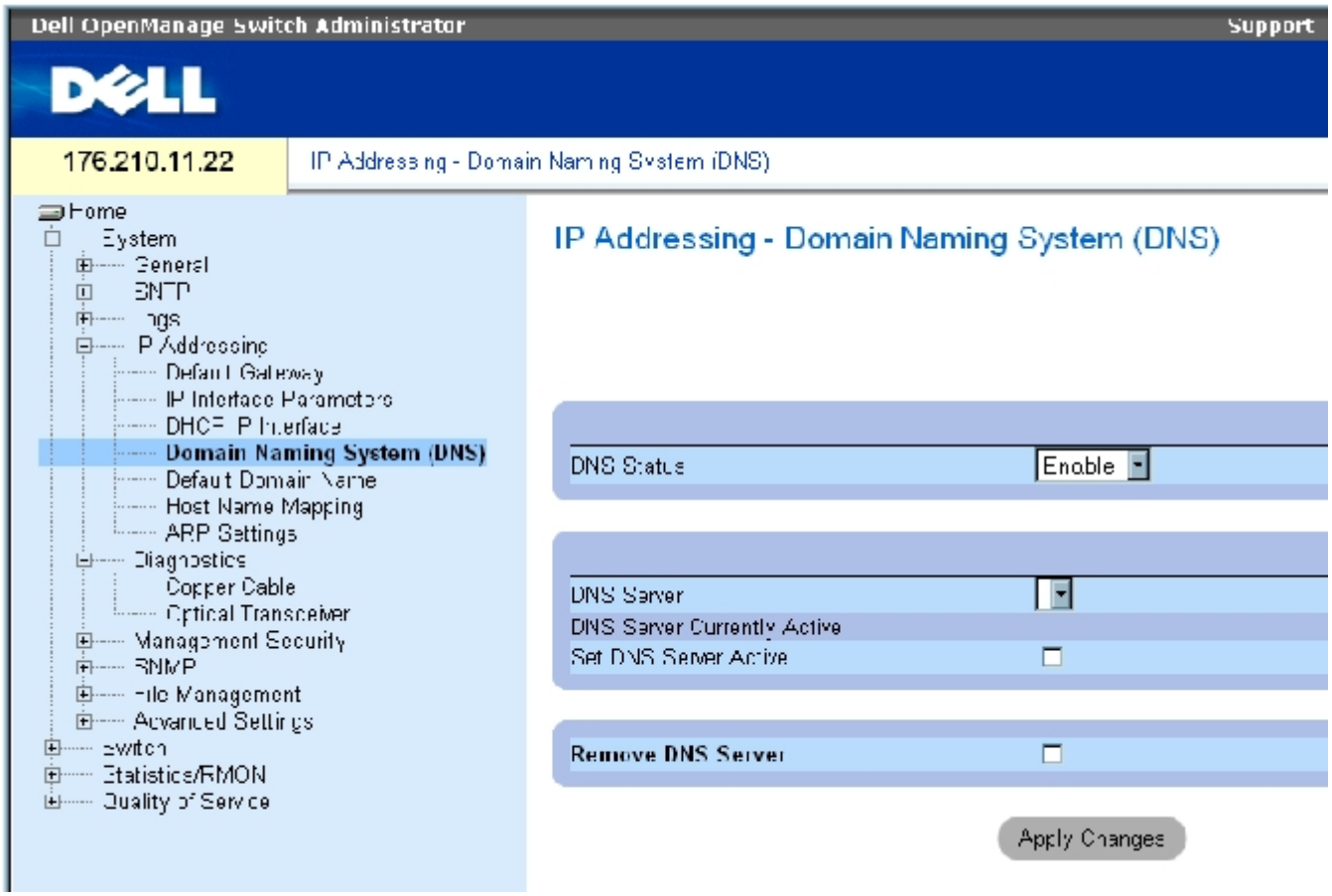
```
console(config)# interface
ethernet 1/e11

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

配置域名系统

域名系统 (DNS) 用于将用户定义的域名转换为 IP 地址。每次分配域名后，DNS 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。DNS 服务器维护域名数据库及其对应的 IP 地址。

“Domain Naming System (DNS)” (域命名系统 [DNS]) 页面包含用于启用和激活特定 DNS 服务器的字段。要打开“Domain Naming System (DNS)” (域命名系统 [DNS]) 页面，请在树视图中单击“System” (系统) → “IP Addressing” (IP 定址) → “Domain Naming System (DNS)” (域命名系统 [DNS]) 。

图 6-28. 域命名系统 (DNS)



“Domain Naming System (DNS)” (域命名系统 [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。在“Add DNS Server” (添加 DNS 服务器) 页面中添加 DNS 服务器。

“DNS Server Currently Active” (DNS 服务器当前处于活动状态) — 当前处于活动状态的 DNS 服务器。

“Set DNS Server Active” (将 DNS 服务器设置为活动状态) — 激活选定的 DNS 服务器。

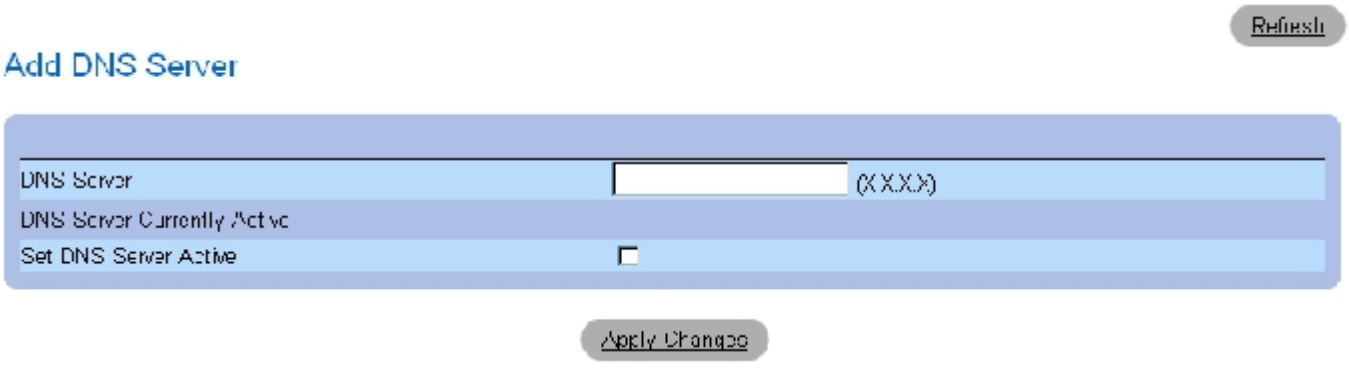
“Remove DNS Server” (删除 DNS 服务器) — 如果选择此字段，将删除选定的 DNS 服务器。

添加 DNS 服务器

1. 打开“Domain Naming System (DNS)” (域命名系统 [DNS]) 页面。
2. 单击“Add” (添加) 。

   系统将打开“Add DNS Server” (添加 DNS 服务器) 页面：

图 6-29. 添加 DNS 服务器



“DNS Server” (DNS 服务器) — DNS 服务器的 IP 地址。

3. 定义相关的字段。
4. 单击“Apply Changes” (应用更改) 。

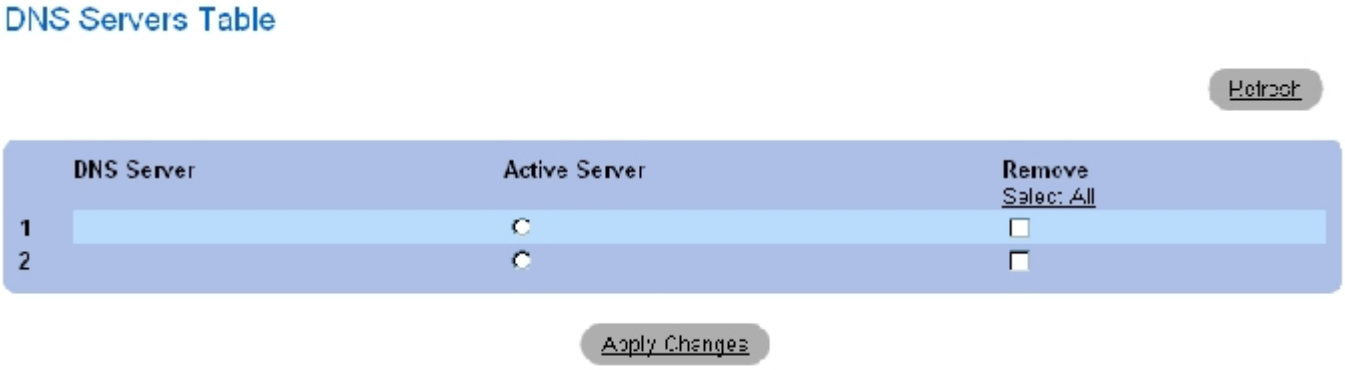
系统将定义新的 DNS 服务器，并更新设备。

显示 DNS 服务器表

1. 打开“Domain Naming System (DNS)” (域命名系统 [DNS]) 页面。
2. 单击“Show All” (全部显示) 。

系统将打开“DNS Server Table” (DNS 服务器表) 。

图 6-30. DNS 服务器表



删除 DNS 服务器

1. 打开“Domain Naming System (DNS)” (域命名系统 [DNS]) 页面。
2. 单击“Show All” (全部显示) 。

系统将打开“DNS Server Table” (DNS 服务器表) 页面。

3. 选择一个“DNS Server Table” (DNS 服务器表) 条目。
4. 选取“Remove” (删除) 复选框。
5. 单击“Apply Changes” (应用更改) 。

系统将删除选定的 DNS 服务器，并更新设备。

使用 CLI 命令配置 DNS 服务器

下表概括了用于配置 DNS 服务器的 CLI 命令。

表 6-33. DNS 服务器的 CLI 命令

CLI 命令	说明
ip name-server 服务器地址	设置可用名称服务器。最多可以设置八个名称服务器。
no ip name-server 服务器地址	删除名称服务器。
ip domain-name 名称	定义软件用来完成非限定主机名称的默认域名。
clear host {名称 | *}	从主机名称到地址高速缓存中删除条目。
show hosts [名称]	显示默认域名、名称服务器主机的列表、主机名称和地址的静态和高速缓存的列表。
ip domain-lookup	启用 DNS 系统以将主机名称转换为 IP 地址。

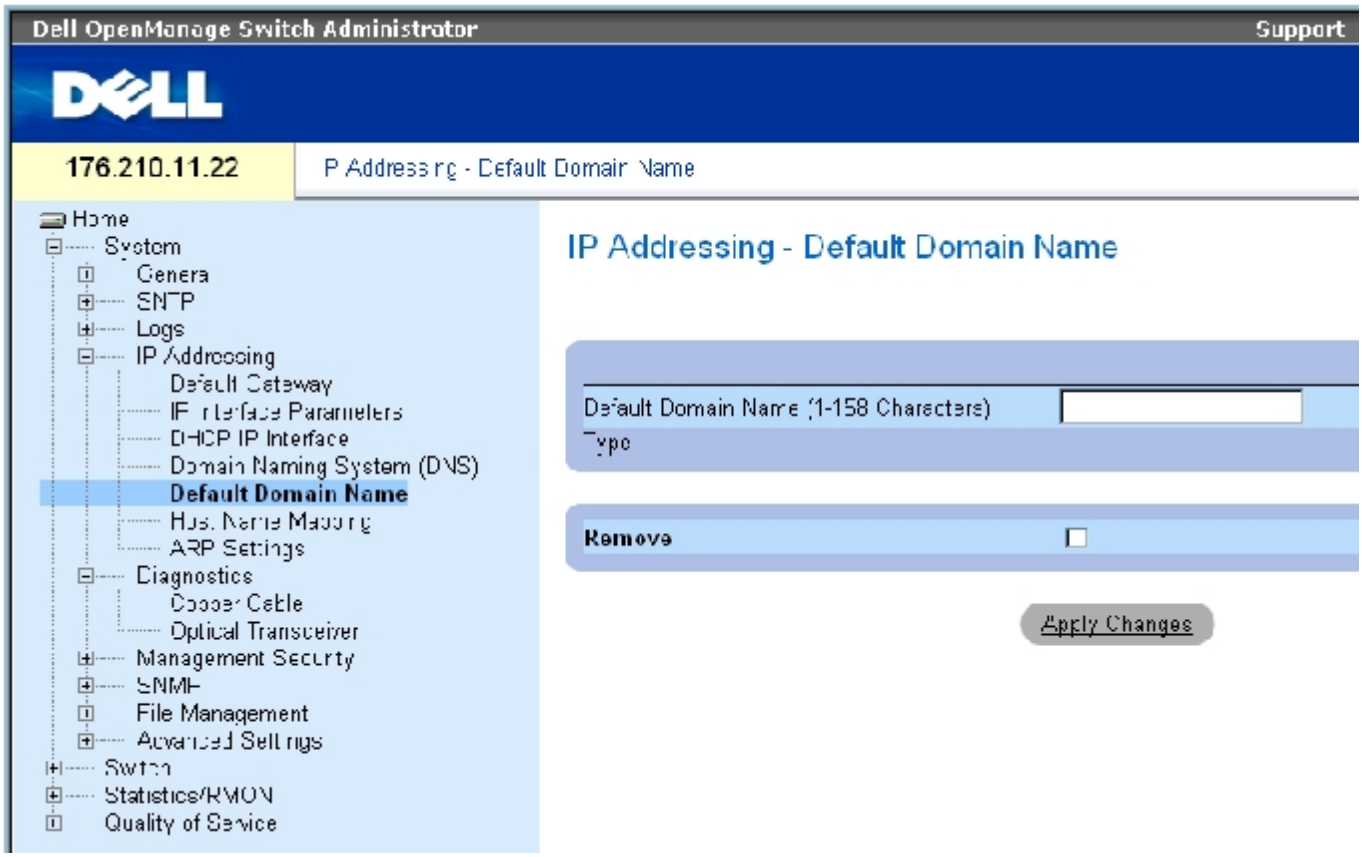
以下是 CLI 命令的示例：

```
console(config)# ip name-
server 176.16.1.18
```

定义默认域

“Default Domain Name” (默认域名) 页面提供用于定义默认 DNS 域名的信息。要打开“Default Domain Name” (默认域名) 页面，请单击“System” (系统) →“IP Addressing” (IP 定址) →“Default Domain Name” (默认域名) 。

图 6-31. 默认域名



“Default Domain Name”（默认域名）页面包含以下字段：

“Default Domain Name (1-158 characters)”（默认域名 [1 至 158 个字符]）— 包含用户定义的默认域名。定义此字段后，系统会将此默认域名应用到所有非限定主机名称上。

“Type”（类型）— IP 地址类型。可能的字段值包括：

“Dynamic”（动态）— 以动态方式创建 IP 地址。

“Static”（静态）— IP 地址是静态 IP 地址。

“Remove”（删除）— 如果选取此字段，将删除默认域名。

使用 CLI 命令定义 DNS 域名

下表概括了用于配置 DNS 域名的 CLI 命令：

表 6-34. DNS 域名的 CLI 命令

CLI 命令	说明

ip domain-name 名称	定义软件用来完成非限定主机名称的默认域名。
no ip domain-name	禁止使用域名系统 (DNS)。
show hosts [名称]	显示默认域名、名称服务器主机的列表、主机名称和地址的静态和高速缓存的列表。

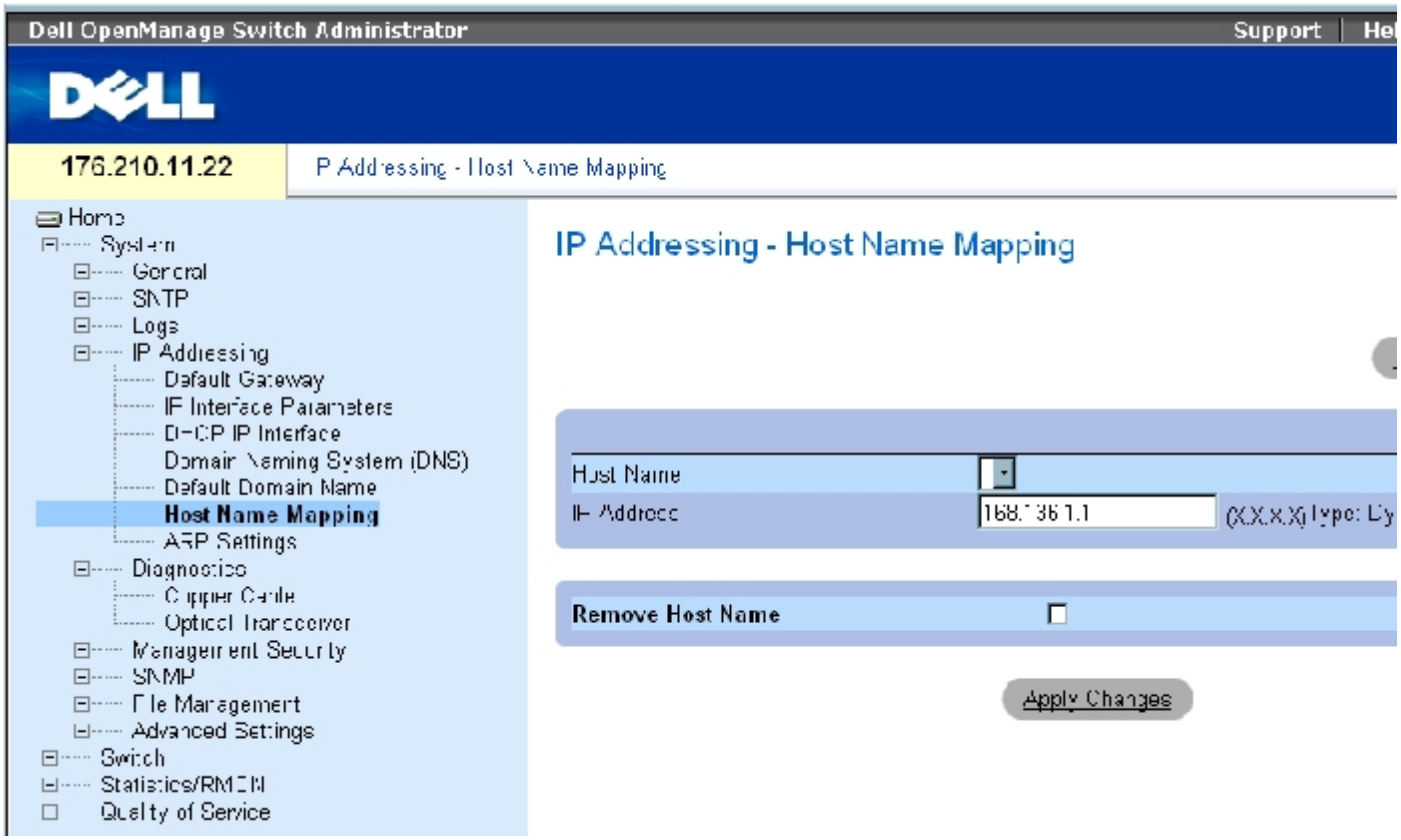
以下是 CLI 命令的示例：

```
console(config)# ip
domain-name dell.com
```

映射域主机

“Host Name Mapping” (主机名称映射) 页面提供用于为静态主机名称分配 IP 地址的参数。在此页面中，只能为每个主机分配一个 IP 地址。要打开“Host Name Mapping” (主机名称映射) 页面，请在树视图中单击“System” (系统) → “IP Addressing” (IP 定址) → “Host Name Mapping” (主机名称映射) 。

图 6-32. 主机名称映射



“Host Name Mapping” (主机名称映射) 页面包含以下字段：

“Host Name” (主机名称) — 包含主机名称列表。主机名称在“Add Host Name Mapping” (添加主机名称映射) 页面中定义。每个主机提供一

个 IP 地址。

“IP Address”（IP 地址）(X.X.X.X) — 提供分配给指定主机名称的 IP 地址。

“Type”（类型）— IP 地址类型。可能的字段值包括：

“Dynamic”（动态）— 以动态方式创建 IP 地址。

“Static”（静态）— IP 地址是静态 IP 地址。

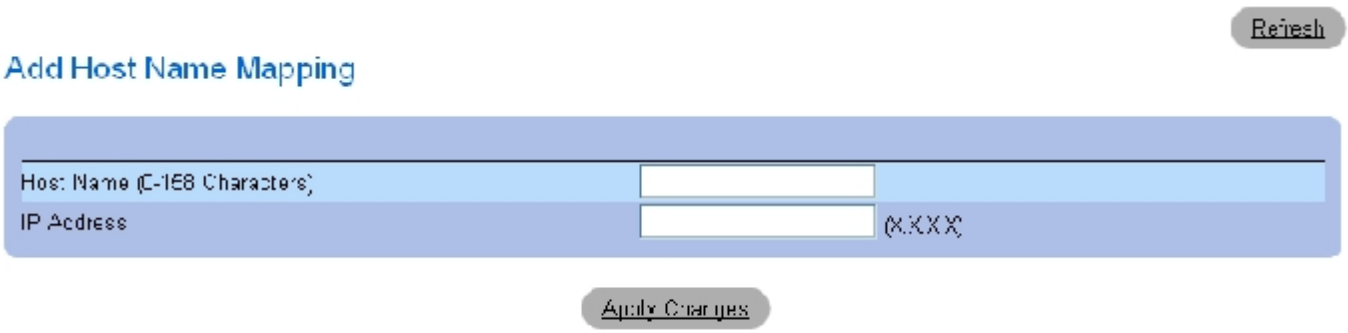
“Remove Host Name”（删除主机名称）— 如果选取此字段，将删除 DNS 主机映射。

添加主机域名

1. 打开“Host Name Mapping”（主机名称映射）页面。
2. 单击“Add”（添加）。

系统将打开“Add Host Name Mapping”（添加主机名称映射）页面。

图 6-33. 添加主机名称映射



3. 定义相关的字段。
4. 单击“Apply Changes”（应用更改）。

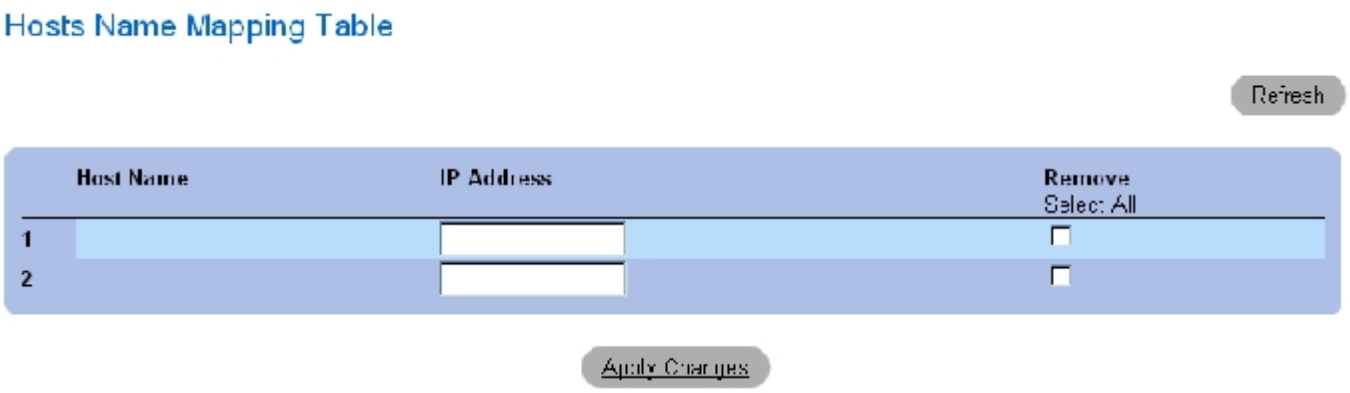
系统将把 IP 地址映射至主机名称，并更新设备。

显示主机名称映射表

1. 打开“Host Name Mapping”（主机名称映射）页面。
2. 单击“Show All”（全部显示）。

系统将打开“Hosts Name Mapping Table”（主机名称映射表）页面：

图 6-34. 主机名称映射表



从 IP 地址映射中删除主机名称

1. 打开“Host Name Mapping”（主机名称映射）页面。
2. 单击“Show All”（全部显示）。
3. 系统将打开“Hosts Name Mapping Table”（主机名称映射表）页面。
4. 选择一个“Host Name Mapping Table”（主机名称映射表）条目。
5. 选取“Remove”（删除）复选框。
6. 单击“Apply Changes”（应用更改）。

系统将删除“Host Mapping Table”（主机映射表）条目，并更新设备。

使用 CLI 命令将 IP 地址映射至域主机名称

下表概括了用于将域主机名称映射至 IP 地址的等效 CLI 命令。

表 6-35. 域主机名称的 CLI 命令

CLI 命令	说明
ip host 名称地址	在主机高速缓存中定义静态主机名称到地址映射
no ip host name	删除名称到地址映射。
clear host {名称 | *}	从主机名称到地址高速缓存中删除条目。
show hosts [名称]	显示默认域名、名称服务器主机的列表、主机名称和地址的静态和高速缓存的列表。

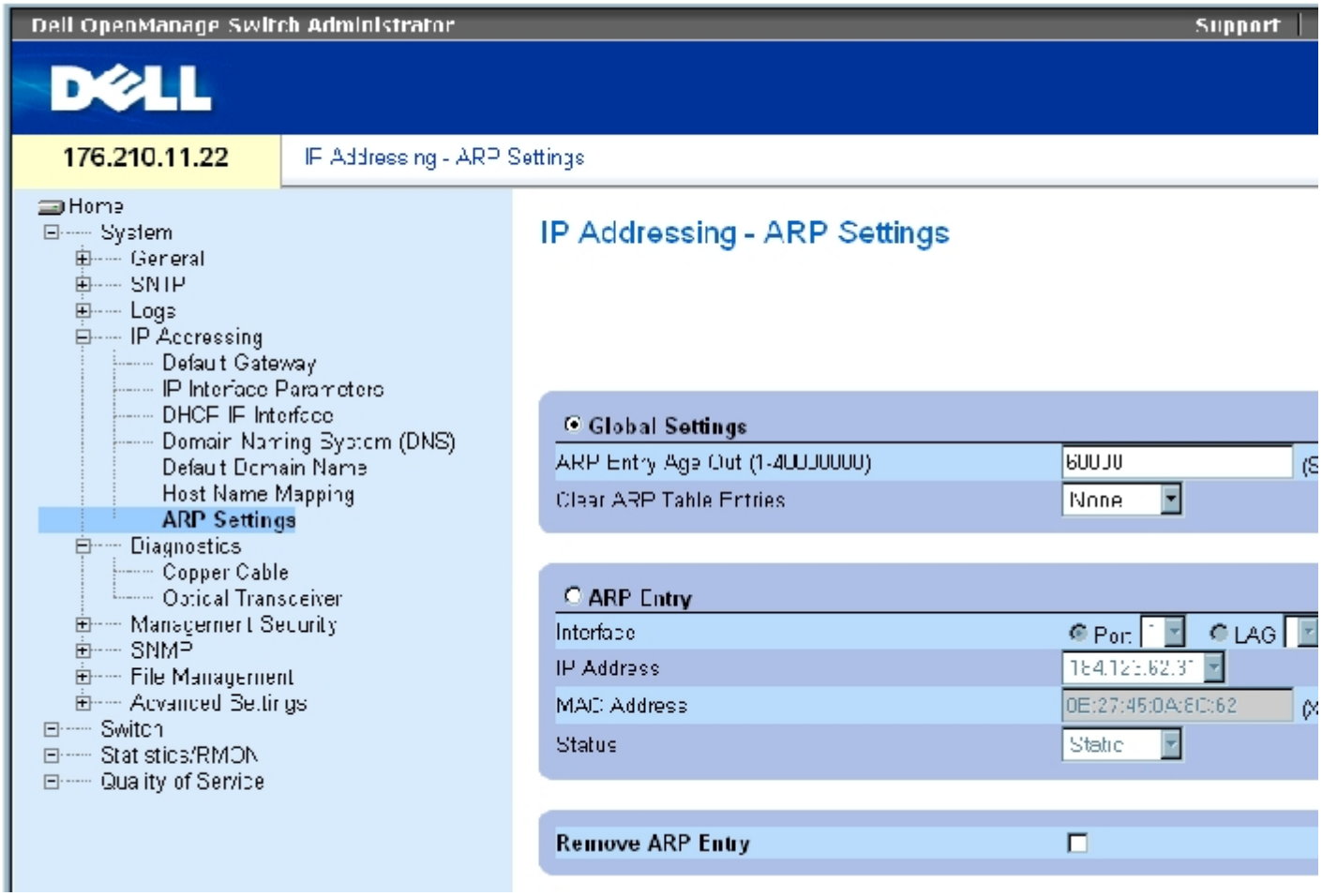
以下是 CLI 命令的示例：

```
console(config)# ip host
accounting.abc.com
176.10.23.1
```

定义 ARP 设置

地址解析协议 (ARP) 将 IP 地址转换为物理地址，并将 IP 地址映射为 MAC 地址。仅当某个主机的其它相邻主机的 IP 地址已知时，ARP 才允许该主机与其它主机进行通信。要打开“ARP Settings” (ARP 设置) 页面，请在树视图中单击“System” (系统) →“IP Addressing” (IP 定址) →“ARP”。

图 6-35. ARP 设置



"ARP Settings" (ARP 设置) 页面包含以下字段：

"Global Settings" (全局设置) — 选择此选项可以激活用于 ARP 全局设置的字段。

"ARP Entry Age Out (1-40000000)" (ARP 条目超时 [1 至 40000000]) — 对于所有设备，关于 ARP 表条目的 ARP 请求之间经过的时间 (秒)。在此时间段之后，该条目将从表中删除。范围为 1 至 40000000。默认值为 60000 秒。

"Clear ARP Table Entries" (清除 ARP 表条目) — 在所有设备上清除的 ARP 条目的类型。可能的值包括：

"None" (无) — 不清除 ARP 条目。

"All" (全部) — 清除所有 ARP 条目。

"Dynamic" (动态) — 仅清除动态 ARP 条目。

"Static" (静态) — 仅清除静态 ARP 条目。

"ARP Entry" (ARP 条目) — 选择此选项可以在单个以太网设备上激活用于 ARP 设置的字段。

“Interface”（接口）— 连接至设备的端口、LAG 或 VLAN 的接口编号。

“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。

“Status”（状态）— ARP 表条目状态。可能的字段值包括：

“Dynamic”（动态）— 动态记忆 ARP 条目。

“Static”（静态）— ARP 条目是静态条目。

“Remove ARP Entry”（删除 ARP 条目）— 如果选择此字段，将删除 ARP 条目。

要添加静态 ARP 表条目，请：

1. 打开“ARP Settings”（ARP 设置）页面。
2. 单击“Add”（添加）。

   系统将打开“Add ARP Entry”（添加 ARP 条目）页面。
3. 选择接口。
4. 定义字段。
5. 单击“Apply Changes”（应用更改）。

   系统将添加“ARP Table”（ARP 表）条目，并更新设备。

显示 ARP 表

1. 打开“ARP Settings”（ARP 设置）页面。
2. 单击“Show All”（全部显示）。

系统将打开“ARP Table”（ARP 表）页面。

删除 ARP 表条目

1. 打开“ARP Settings”（ARP 设置）页面。
2. 单击“Show All”（全部显示）。

系统将打开“ARP Table”（ARP 表）页面。

3. 选择一个表条目。
4. 选取“Remove”（删除）复选框。
5. 单击“Apply Changes”（应用更改）。

系统将删除选定的“ARP Table”（ARP 表）条目，并更新设备。

使用 CLI 命令配置 ARP

下表概括了用于设置“ARP Settings”（ARP 设置）页面中显示的字段的等效 CLI 命令。

表 6-36. ARP 设置的 CLI 命令

CLI 命令	说明
arp IP 地址 硬件地址 {ethernet 接口号 | vlan VLAN ID | port-channel 号}	在 ARP 高速缓存中添加永久性条目。
arp timeout 秒	配置条目在 ARP 高速缓存中的保留时间。
clear arp-cache	从 ARP 高速缓存中删除所有动态条目。
show arp	显示 ARP 表中的条目。
no arp	从 ARP 表中删除 ARP 条目。

以下是 CLI 命令的示例：

```
console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc
```

```
console(config)# arp timeout 12000

console(config)# exit

console# show arp

ARP timeout:12000 Seconds
```

Interface	IP address	HW address	Status
---------	----------	----------	------
1/e11	10.7.1.102	00:10:B5:04:DB:4B	Dynamic
1/e12	10.7.1.135	00:50:22:00:2A:A4	Static

运行电缆诊断程序

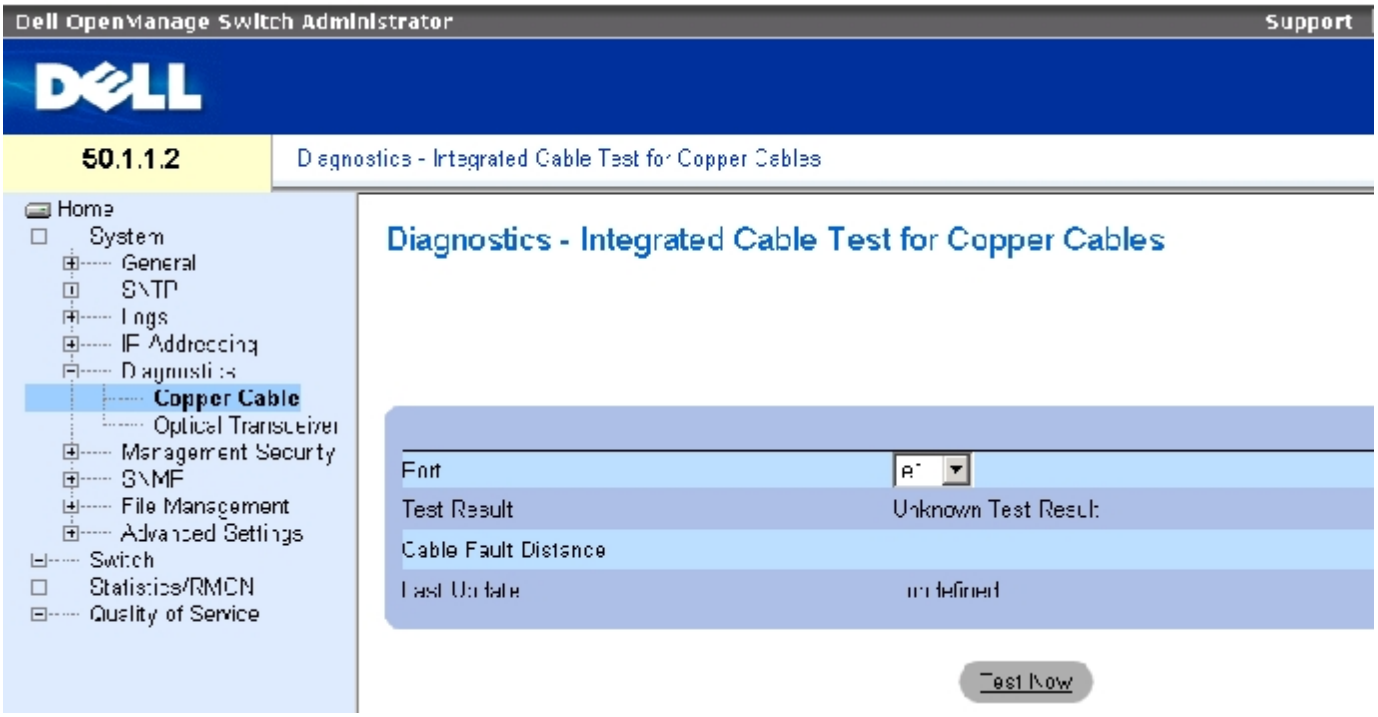
“Diagnostics”（诊断程序）页面包含指向用于对铜质电缆执行虚拟电缆检测的页面的链接。要打开“Diagnostics”（诊断程序）页面，请在树视图中单击“System”（系统）→“Diagnostics”（诊断程序）。

查看铜质电缆诊断程序

“Copper Cables”（铜质电缆）页面包含用于对铜质电缆执行检测的字段。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。

要打开“Copper Cables”（铜质电缆）页面，请在树视图中单击“System”（系统）→“Diagnostics”（诊断程序）→“Copper Cable”（铜质电缆）。

图 6-36. 铜质电缆的集成电缆检测



“Copper Cables”（铜质电缆）页面包含以下字段：

“Port”（端口）— 电缆连接的端口。

“Test Result”（检测结果）— 电缆检测结果。可能的字段值包括：

“No Cable”（没有电缆）— 没有电缆连接至端口。

“Open Cable”（电缆断路）— 电缆仅有一端连接。

“Short Cable”（电缆短路）— 电缆出现短路。

“OK”（通过）— 电缆通过检测。

“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”（上一次更新）— 上一次检测端口的时间。

“Approximate Cable Length”（近似电缆长度）— 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

1. 请确保铜质电缆的两端均连接至设备。

2. 打开“Copper Cables”（铜质电缆）页面。

3. 选择要检测的接口。

4. 单击“Test Now”（开始检测）。

系统将执行铜质电缆检测，并将结果显示在“Copper Cables”（铜质电缆）页面中。

显示虚拟电缆检测结果表

1. 打开“Copper Cables”（铜质电缆）页面。

2. 单击“Show All”（全部显示）。

系统将打开“Integrated Cable Test Results Table”（集成电缆检测结果表）页面。

注：此屏幕将显示先前已运行的检测的结果，但不立即对所有端口实际执行检测。

除了“Copper Cables”（铜质电缆）页面中的字段外，“Integrated Cable Test Results Table”（集成电缆检测结果表）还包含以下字段：

“Unit No.”（装置号）— 要显示的电缆的装置号。

使用 CLI 命令执行铜质电缆检测

下表包含了用于执行铜质电缆检测的 CLI 命令。

表 6-37. 铜质电缆检测的 CLI 命令

CLI 命令	说明
test copper-port tdr 接口	执行 VCT 检测。
show copper-port tdr 接口	显示上一次对端口进行的 VCT 检测的结果。
show copper-port cable-length接口	显示连接至端口的铜质电缆的估计长度。

以下是 CLI 命令的示例：

console> **enable**
Console# **test copper-port tdr** 1/e3
Cable is open at 100 meters.

Console# **show copper-port cable-length**	
Port	Length (meters)
----	---------------
1/e3	110-140
1/e4	Fiber

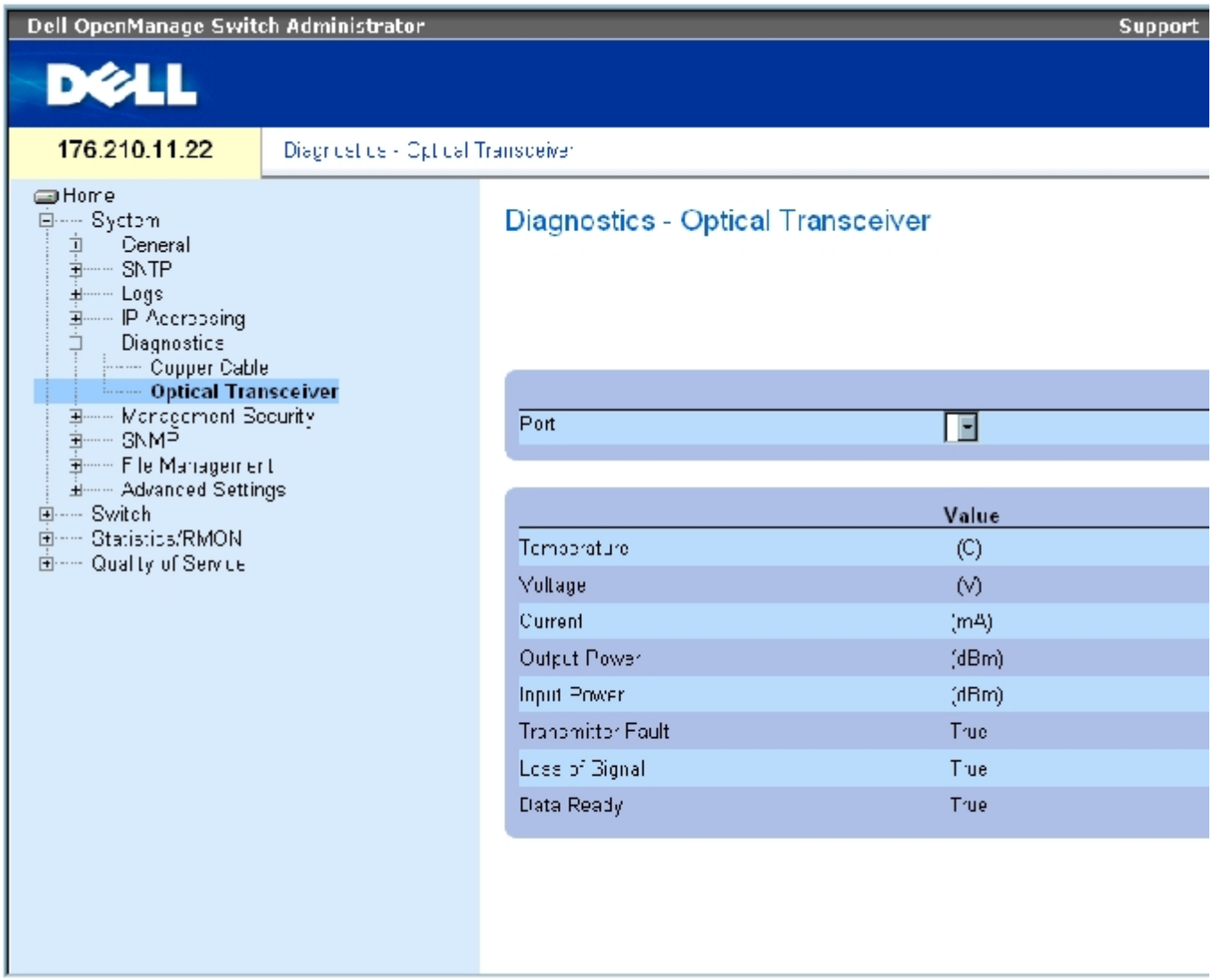
注：集成电缆检测程序（ICT）返回的电缆长度是一个近似值，它的范围为 50 米、50 至 80 米、80 至 110 米、110 至 120 米或大于 120 米。偏差最大可达 20 米，无法对 10 Mbps 链路运行电缆长度测量。

查看光收发机诊断程序

使用“Optical Transceiver”（光收发机）页面可以对光纤电缆执行检测。要打开“Optical Transceiver”（光收发机）页面，请在树视图中单击“System”（系统）→“Diagnostics”（诊断程序）→“Optical Transceiver”（光收发机）。

注：仅当链路存在时才能执行光收发机诊断程序。

图 6-37. 光收发机



“Optical Transceiver”（光收发机）页面包含以下字段：

“Port”（端口）— 检测电缆所在的端口 IP 地址。

“Temperature”（温度）— 电缆运行时的温度 (C)。

“Voltage”（电压）— 电缆运行时的电压。

“Current”（电流）— 电缆运行时的电流。

“Output Power”（输出功率）— 输出功率的传输速率。

“Input Power”（输入功率）— 输入功率的传输速率。

“Transmitter Fault”（发送器故障）— 表示传输时是否出现故障。

“Loss of Signal”（信号丢失）— 表示电缆中是否出现信号丢失。

“Data Ready”（数据就绪）— 收发机已通电并且数据已就绪。

显示光收发机诊断程序检测结果表

1. 打开“Optical Transceiver”（光收发机）页面。
2. 单击“Show All”（全部显示）。

系统将运行检测程序并打开“Optical Transceiver Diagnostics Table”（光收发机诊断程序表）页面。

除了“Optical Transceiver”（光收发机）页面中的字段外，“Optical Transceiver Diagnostics Table”（光收发机诊断程序表）还包含以下字段：

“Unit No.”（装置号）— 要显示的电缆的装置号。

- N/A — 不可用；N/S — 不支持；W — 警告；E — 错误

注：Finisair 收发机不支持发送器故障诊断测试。

注：光纤分析功能只能对支持数字诊断标准 SFF--872 的 SFP 使用。

使用 CLI 命令执行光纤电缆检测

下表包含了用于执行光纤电缆检测的 CLI 命令。

表 6-38. 光纤电缆检测 CLI 命令

CLI 命令	说明
show fiber-ports optical- transceiver [接口] [详细信息]	显示光收发机诊断程序。

以下是 CLI 命令的示例：

Console# show fiber-ports optical-transceiver detailed							
Port	**Temp [C]**	**Voltage**	**Current**	**Output [mA]**	**Input**	**POWER TX**	**LOS**

			[Volt]		[mWatt]	[mWatt]	Fault
----	----	------	-----	------	------	------	-----
1/e1	48	5.15	50	1.789	1.789	No	No
1/e2	43	5.15	10	1.789	1.789	No	No

管理交换机安全保护

通过“Management Security”（管理安全保护）页面可以访问包含用于设置端口、设备管理方法、用户和服务器安全保护的安全保护参数的字段的安全保护页面。要打开“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）。

定义访问配置文件

“Access Profiles”（访问配置文件）页面包含用于定义访问设备所使用的配置文件和规则的字段。由入口接口和源 IP 地址或源 IP 子网进行定义，可以将对管理功能的访问限制到用户组。

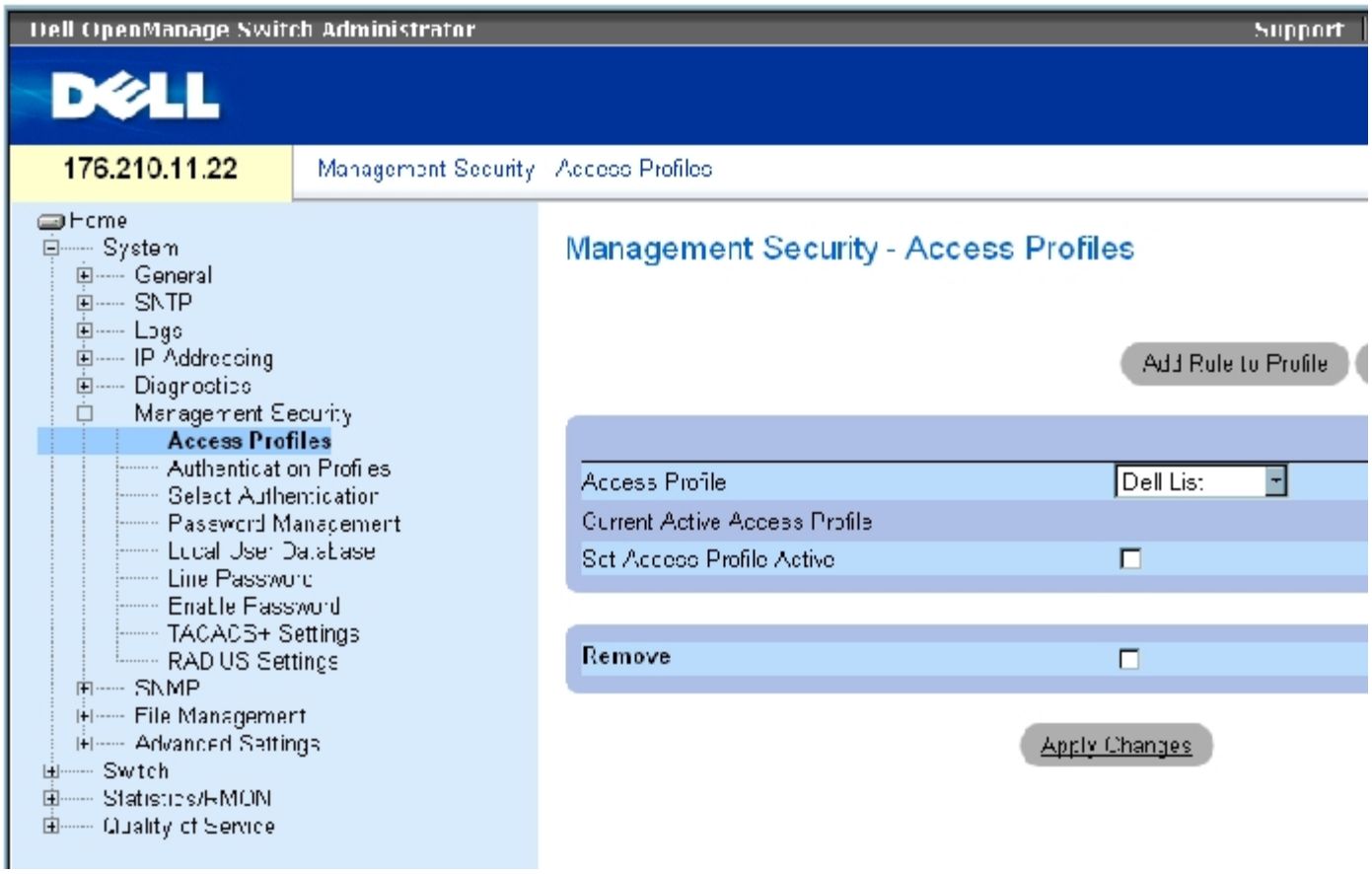
可以针对 Web (HTTP)、安全 Web (HTTPS)、Telnet 和安全 Telnet 等各种类型的管理访问方法分别定义管理访问。

在用户组之间，对各种管理方法的访问可能不同。例如，用户组 1 只能通过 HTTPS 会话访问设备，而用户组 2 通过 HTTPS 和 Telnet 会话都可以访问设备。

管理访问列表最多包含 256 条规则，这些规则用于确定哪些用户可以通过哪些方法管理设备。还可以禁止用户访问设备。

“Access Profiles”（访问配置文件）页面包含用于配置管理列表并将其应用于特定接口的字段。要打开“Access Profiles”（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 6-38. 访问配置文件



“Access Profiles”（访问配置文件）页面包含以下字段：

“Access Profile”（访问配置文件）— 用户定义的访问配置文件列表。访问配置文件列表包含默认值“Console Only”（仅控制台）。选择此访问配置文件后，将仅使用控制台连接执行设备的活动管理。

“Current Active Access Profile”（当前活动的访问配置文件）— 当前处于活动状态的访问配置文件。

“Set Access Profile Active”（将访问配置文件设置为活动状态）— 激活访问配置文件。

“Remove”（删除）— 如果选择此字段，将从“Access Profile Name”（访问配置文件名称）列表中删除访问配置文件。

激活配置文件

1. 打开“Access Profiles”（访问配置文件）页面。
2. 在“Access Profiles”（访问配置文件）字段中选择一个访问配置文件。
3. 选取“Set Access Profile Active”（将访问配置文件设置为活动状态）复选框。
4. 单击“Apply Changes”（应用更改）。

系统将激活访问配置文件。

添加访问配置文件

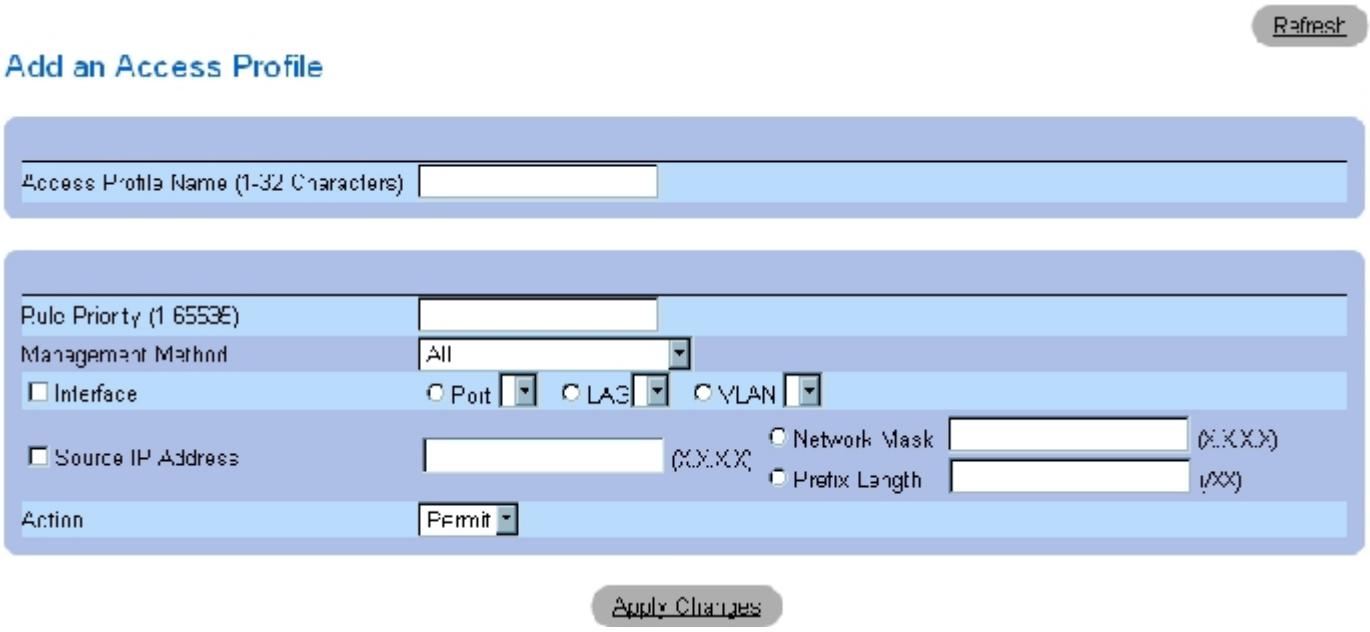
规则用作筛选器，用于确定规则优先级、设备管理方法、接口类型、源 IP 地址和网络掩码以及设备管理访问操作。可以禁止或允许用户进行管理访问。规则优先级设置应用规则的次序。

要定义访问配置文件的规则，请：

1. 打开“Access Profiles”（访问配置文件）页面。
2. 单击“Add Profile”（添加配置文件）。

系统将打开“Add An Access Profile”（添加访问配置文件）页面：

图 6-39. 添加访问配置文件



“Add an Access Profile”（添加访问配置文件）页面包含以下附加字段：

“Access Profile Name”（访问配置文件名称）（1 至 32 个字符）— 用户定义的访问配置文件名称。访问配置文件名称最多可包含 32 个字符。

“Rule Priority (1-65535)”（规则优先级 [1 至 65535]）— 规则优先级。信息包与规则进行匹配时，用户组会被授予或被拒绝对设备管理的访问权。使用此字段定义规则优先级即可设置规则顺序。由于根据第一适用原则对信息包进行匹配，因此在将信息包与规则进行匹配时，规则编号非常重要。可以在“Profile Rules Table”（配置文件规则表）中查看规则优先级。

“Management Method”（管理方法）— 为其定义了访问配置文件的管理方法。具有此访问配置文件的用户会被拒绝或允许通过选定的管理方法（线路）访问设备。

“Interface”（接口）— 要对其应用规则的接口类型。这是一个可选字段。通过选取复选框并选择相应的选项按钮及接口，可以将规则应用于选定的端口、LAG 或 VLAN。

注：将访问配置文件分配给一个接口将拒绝通过其它接口进行访问。如果未将访问配置文件分配给任何接口，则可以通过所有接口访问设备。

“Source IP Address”（源 IP 地址）(X.X.X.X) — 规则适用的接口源 IP 地址。这是一个可选字段，它表示规则对子网是有效的。

“Network Mask”（网络掩码）(X.X.X.X) — IP 子网掩码。

“Prefix Length”（前缀长度）(/XX) — 组成源 IP 地址前缀或源 IP 地址的网络掩码的位数。

“Action”（操作）— 定义是允许还是拒绝对定义的接口进行管理访问。

3. 定义“Access Profile Name”（访问配置文件名称）字段。

4. 定义相关的字段。

5. 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。

将规则添加至访问配置文件

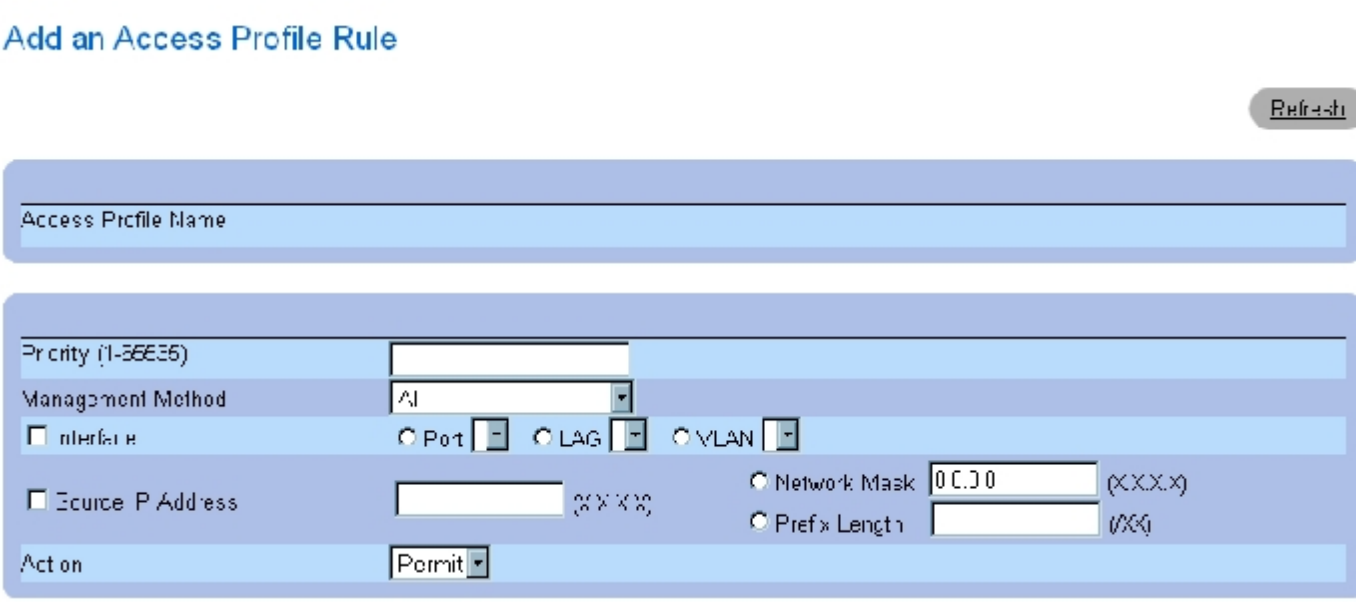
注：必须定义第一条规则才能开始通信与访问配置文件的匹配。

1. 打开“Access Profiles”（访问配置文件）页面。

2. 单击“Add Rule to Profile”（将规则添加至配置文件）。

系统将打开“Add an Access Profile Rule”（添加访问配置文件规则）页面：

图 6-40. 添加访问配置文件规则



3. 完成字段。

4. 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。

查看配置文件规则表

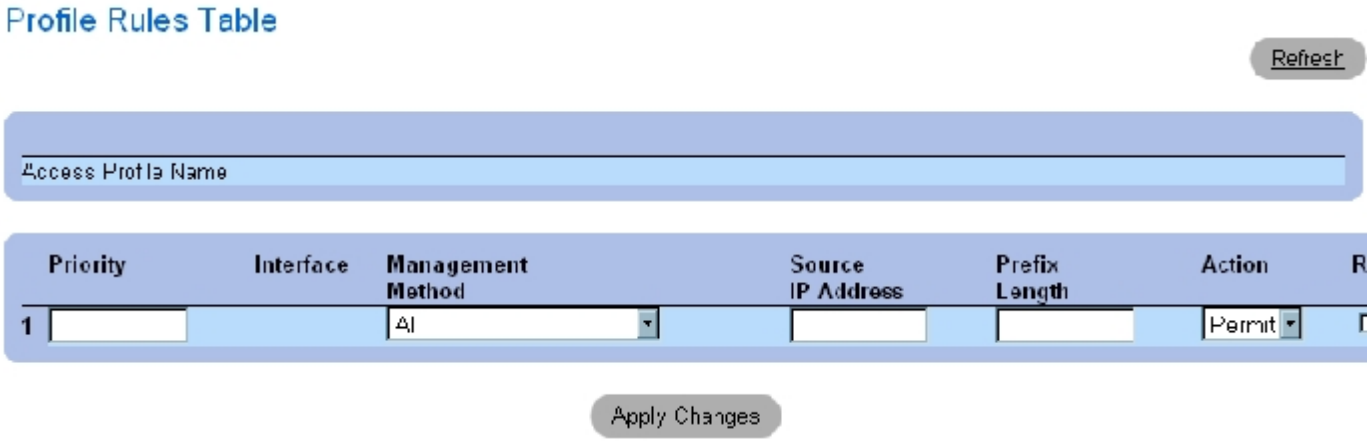
注：“Profile Rules Table”（配置文件规则表）中规则的显示顺序非常重要。信息包需匹配符合规则条件的第一条规则。

1. 打开“Access Profiles”（访问配置文件）页面。

2. 单击“Show All”（全部显示）。

系统将打开“Profile Rules Table”（配置文件规则表）页面：

图 6-41. 配置文件规则表



删除规则

1. 打开“Access Profiles”（访问配置文件）页面。
2. 单击“Show All”（全部显示）。

   系统将打开“Profile Rules Table”（配置文件规则表）页面。
3. 选择一条规则。
4. 选取“Remove”（删除）复选框。
5. 单击“Apply Changes”（应用更改）。

   系统将删除选定的规则，并更新设备。

使用 CLI 命令定义访问配置文件

下表概括了用于设置“Access Profiles”（访问配置文件）页面中显示的字段的等效 CLI 命令。

表 6-39. 访问配置文件的 CLI 命令

CLI 命令	说明
management access-list 名称	定义用于管理的访问列表，并进入用于配置的访问列表环境。

permit [ethernet 接口号	vlan VLAN ID	port-channel 号] [service 服务]	为管理访问列表设置端口允许条件。
permit ip-source IP 地址 [mask 掩码	前缀长度] [ethernet 接口号	vlan VLAN ID	port-channel 号] [service 服务]	为管理访问列表和选定的管理方法设置端口允许条件。
deny [ethernet 接口号	vlan VLAN ID	port-channel 号] [service 服务]	为管理访问列表和选定的管理方法设置端口拒绝条件。
deny ip-source IP 地址 [mask 掩码	前缀长度] [ethernet 接口号	vlan VLAN ID	port-channel 号] [service 服务]	为管理访问列表和选定的管理方法设置端口拒绝条件。
management access-class {console-only	名称}	定义将哪个访问列表用作活动管理连接。
show management access-list [名称]	显示活动的管理访问列表。
show management access-class	显示有关管理访问类的信息。

以下是 CLI 命令的示例：

```
console(config)#
management access-list
mlist

console(config-macl)#
permit ethernet 1/e1

console(config-macl)#
permit ethernet 1/e2

console(config-macl)#
deny ethernet 1/e3

console(config-macl)#
deny ethernet 1/e4

console(config-macl)#
exit

console(config)#
management access-class
mlist

console(config)# exit

console# show management
access-list

mlist

-----

permit ethernet 1/e1

permit ethernet 1/e2

deny ethernet 1/e3
```

```
deny ethernet 1/e4


! (Note:all other access
implicitly denied)


Console# show management
access-class


Management access-class
is enabled, using access
list mlist
```

定义验证配置文件

“Authentication Profiles”（验证配置文件）页面包含用于选择设备上的用户验证方法的字段。用户验证可通过以下方式进行：

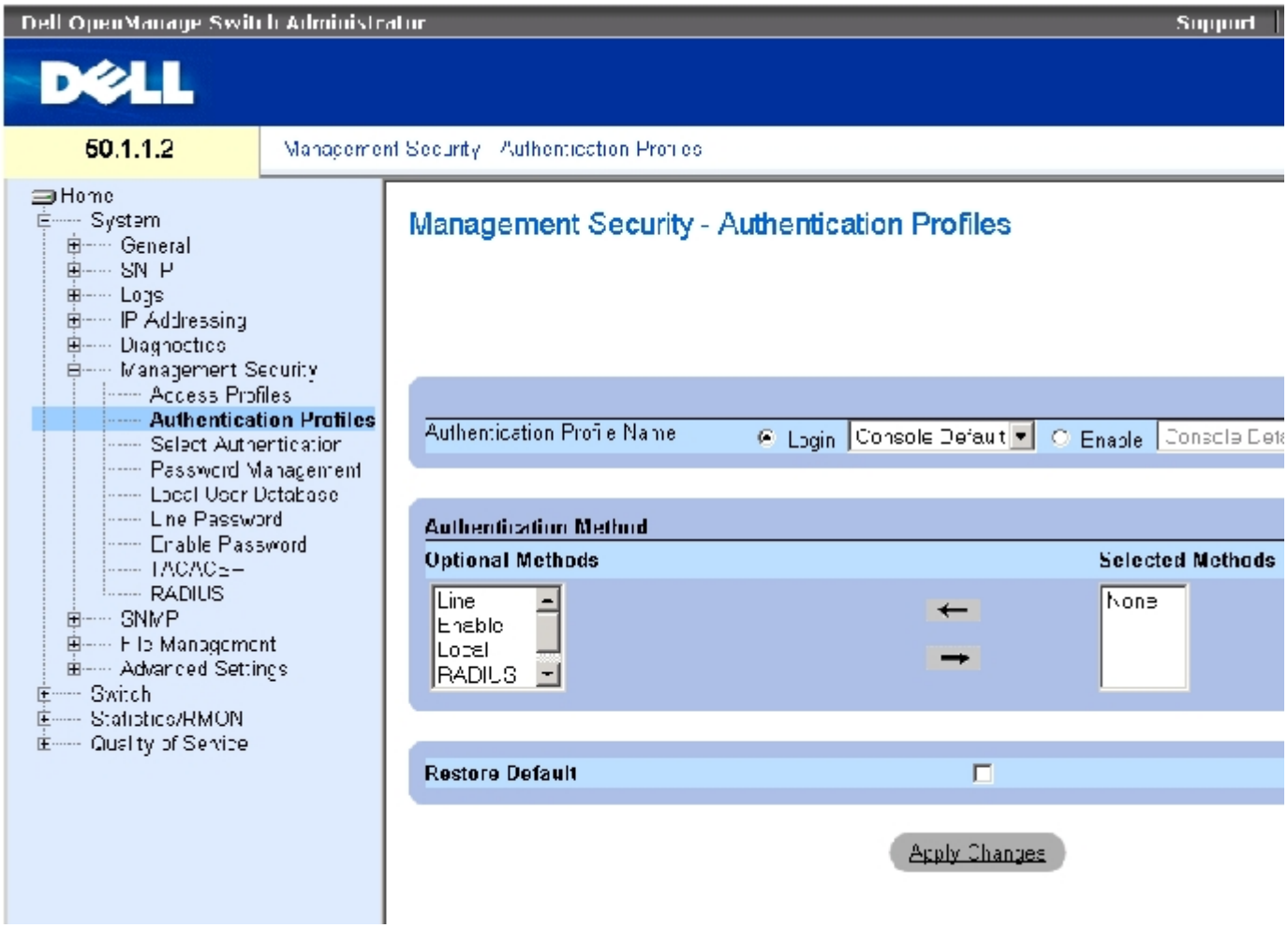
- 本地
- 通过外部服务器

也可以将用户验证设置为“None”（无）。

用户验证按照方法选择顺序进行。例如，如果同时选择“Local”（本地）和“RADIUS”选项，则首先在本地验证用户。如果本地用户数据库为空，则再通过 RADIUS 服务器进行用户验证。如果使用第一种方法验证失败，验证过程将结束。

如果在验证过程中出现错误，将使用下一个选定方法。要打开“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 6-42. 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）— 用户定义的验证配置文件列表，可以向其中添加用户定义的验证配置文件。默认为“Network Default”（网络默认值）和“Console Default”（控制台默认值）。

- “Login”（登录）— 指定用于登录密码的用户定义的验证配置文件列表。
- “Enable”（启用）— 指定用于启用密码的用户定义的验证配置文件列表。

“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）— 在设备级别进行用户验证。设备将检查用户名和密码以进行验证。

“RADIUS”— 在 RADIUS 服务器进行用户验证。有关详情，请参阅“配置 RADIUS 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。

“TACACS+”— 在 TACACS+ 服务器进行用户验证。

“Restore Default”（恢复默认设置）— 恢复设备上的默认用户验证方法。仅用于默认配置文件。

“Remove”（删除）— 如果选择此字段，将删除所选配置文件。无法删除活动的配置文件。仅用于用户定义的配置文件。

要选择验证配置文件，请：

1. 打开“Authentication Profiles”（验证配置文件）页面。
2. 在“Authentication Profile Name”（验证配置文件名称）字段中选择一个配置文件。
3. 使用导航箭头选择验证方法。验证按照验证方法列出的顺序进行。
4. 单击“Apply Changes”（应用更改）。

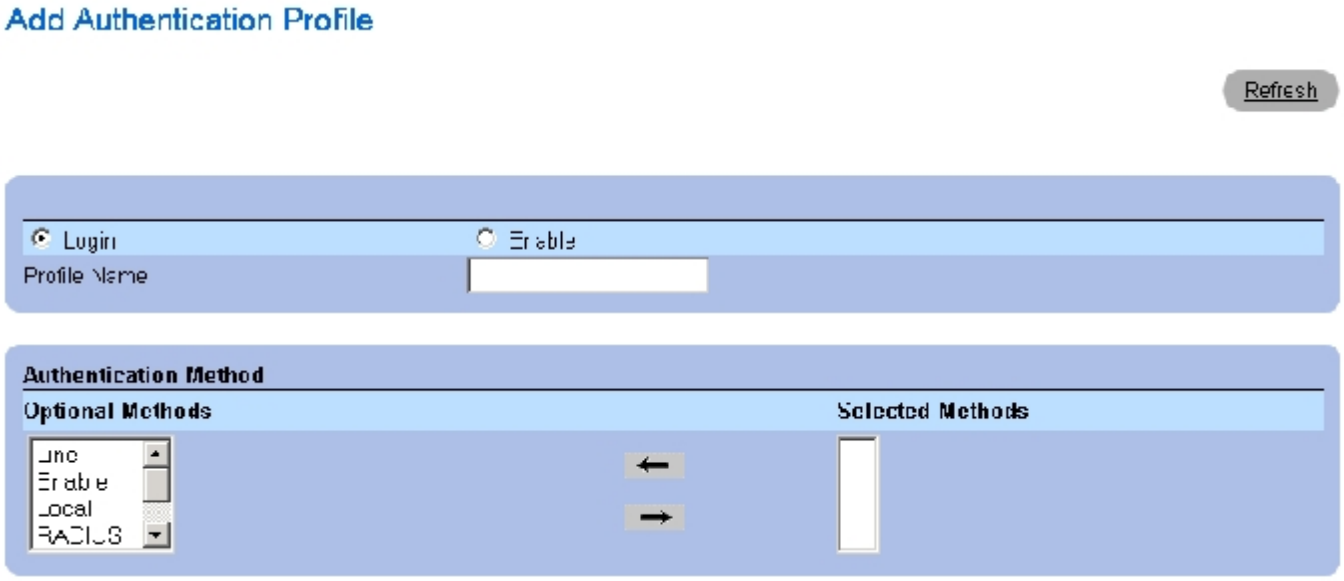
用户验证配置文件将被更新到设备。

要添加验证配置文件，请：

1. 打开“Authentication Profiles”（验证配置文件）页面。
2. 单击“Add”（添加）。

系统将打开“Add Authentication Profile”（添加验证配置文件）页面：

图 6-43. 添加验证配置文件



3. 配置该配置文件。

注：请勿在新配置文件的名称中包含空格。

4. 单击“Apply Changes”（应用更改）。

验证配置文件将被更新到设备。

要显示验证配置文件表，请：

1. 打开“Authentication Profiles”（验证配置文件）页面。
2. 单击“Show All”（全部显示）。

系统将打开“Authentication Profiles Table”（验证配置文件表）页面。

删除验证配置文件：

1. 打开“Authentication Profiles”（验证配置文件）页面。
2. 单击“Show All”（全部显示）。

系统将打开“Authentication Profile Table”（验证配置文件表）页面。

3. 选择验证配置文件。

4. 选取“Remove”（删除）复选框。

5. 单击“Apply Changes”（应用更改）。

系统将删除选定的验证配置文件。

使用 CLI 命令配置验证配置文件

下表概括了用于设置“Authentication Profiles”（验证配置文件）页面中显示的字段的等效 CLI 命令。

表 6-40. 验证配置文件的 CLI 命令

CLI 命令	说明
aaa authentication login {default | 列表名称} 方法 1 [方法 2.]	配置登录验证。
no aaa authentication login {default | 列表名称}	删除登录验证配置文件。

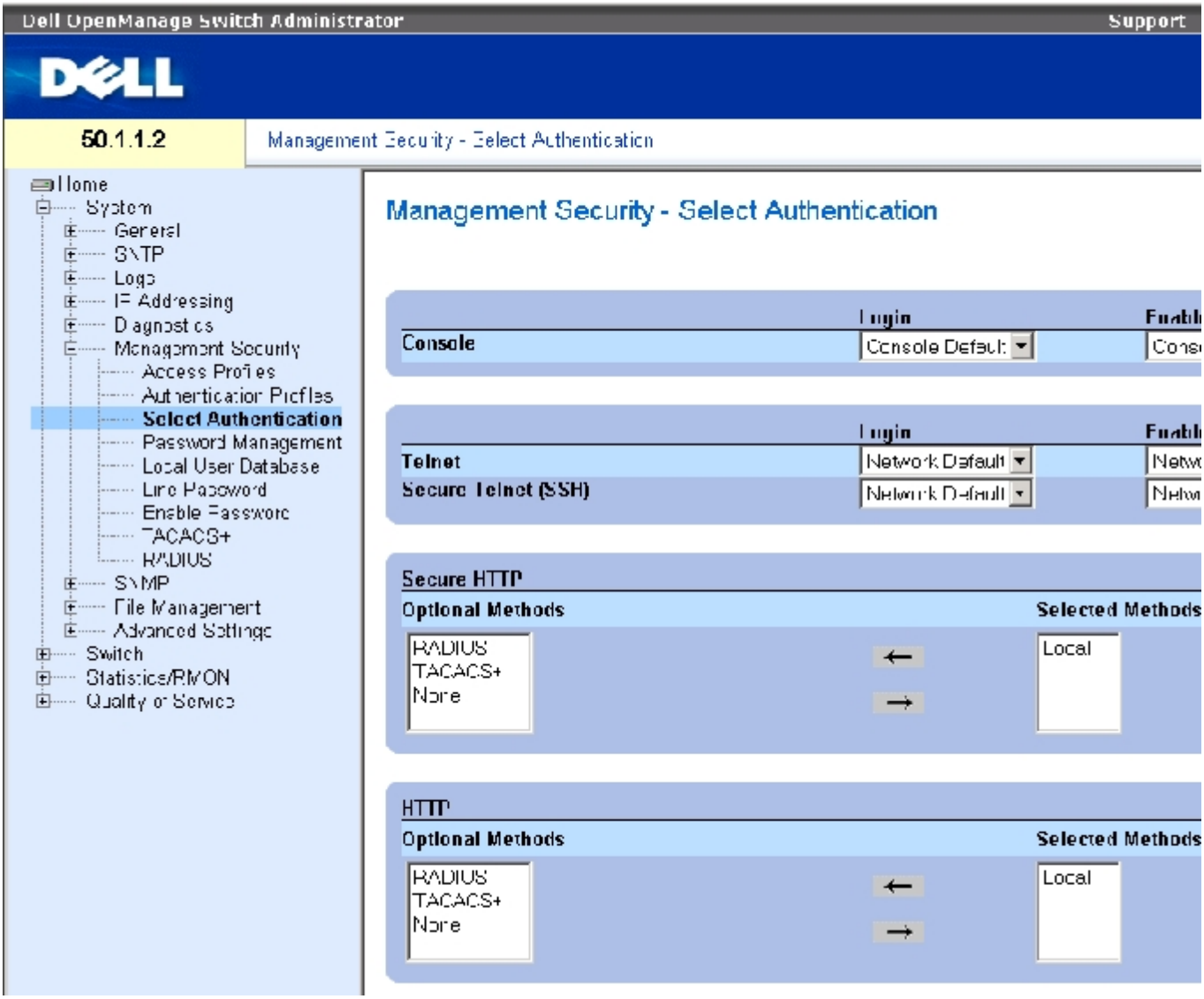
以下是 CLI 命令的示例：

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


console(config)# no aaa
authentication login
default
```

选择验证配置文件

定义验证配置文件后，便可以将验证配置文件应用到管理访问方法。例如，可以用验证方法列表 1 验证控制台用户，用验证方法列表 2 验证 Telnet 用户。要打开“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 6-44. 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。

“Login” (登录) — 指定用户登录到控制台界面时所使用的验证配置文件。

“Enable” (启用) — 指定用户从控制台界面启用优先执行模式时所使用的验证配置文件。

“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。

“HTTP”和“Secure HTTP” (安全 HTTP) — 分别用于 HTTP 访问和安全 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 服务器进行验证。

“TACACS+”— 在 TACACS+ 服务器进行验证。

将验证列表应用于控制台会话

1. 打开“Select Authentication”（选择验证）页面。
2. 在“Console”（控制台）字段中选择一个验证配置文件。
3. 单击“Apply Changes”（应用更改）。

控制台会话将被分配一个验证列表。

将验证配置文件应用于 Telnet 会话

1. 打开“Select Authentication”（选择验证）页面。
2. 在“Telnet”字段中选择一个验证配置文件。
3. 单击“Apply Changes”（应用更改）。

Telnet 会话将被分配一个验证列表。

将验证配置文件应用于安全 Telnet（SSH）会话

1. 打开“Select Authentication”（选择验证）页面。
2. 在“Secure Telnet (SSH)”（安全 Telnet [SSH]）字段中选择一个验证配置文件。
3. 单击“Apply Changes”（应用更改）。

安全 Telnet (SSH) 会话将被分配一个验证配置文件。

为 HTTP 会话分配验证顺序

1. 打开“Select Authentication” (选择验证) 页面。
2. 在“HTTP”字段中选择一个验证顺序。
3. 单击“Apply Changes” (应用更改) 。

HTTP 会话将被分配一个验证顺序。

为安全 HTTP 会话分配验证顺序

1. 打开“Select Authentication” (选择验证) 页面。
2. 在“Secure HTTP” (安全 HTTP) 字段中选择一个验证顺序。
3. 单击“Apply Changes” (应用更改) 。

安全 HTTP 会话将被分配一个验证顺序。

使用 CLI 命令分配访问验证配置文件或验证顺序

下表概括了用于设置“Select Authentication” (选择验证) 页面中显示的字段的等效 CLI 命令。

表 6-41. 选择验证的 CLI 命令

CLI 命令	说明
enable authentication [default | 列表名称]	表示从远程 Telnet、控制台或 SSH 访问更高权限级别时的验证方法列表。
login authentication [default | 列表名称]	表示远程 Telnet、控制台或 SSH 的登录验证方法列表。
ip http authentication 方法 1 [方法 2.]	表示 HTTP 服务器的验证方法。

ip https authentication 方法 1 [方法 2.]	表示 HTTPS 服务器的验证方法。
show authentication methods	显示有关验证方法的信息。

以下是 CLI 命令的示例：

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

console(config-line)# login authentication default

console(config-line)# exit

console(config)# ip http authentication radius local

console(config)# ip https authentication radius local

console(config)# exit


console# show authentication methods

Login Authentication Method Lists

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

Console_Default : None
Network_Default : Local


Enable Authentication Method Lists

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

Console_Default : Enable None
Network_Default : Enable

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

SSH	Default	Default
http	: Local	
https	: Local	
dot1x	:	

管理密码

密码管理能够增强网络安全保护并改进密码控制。用于访问 SSH、Telnet、HTTP、HTTPS 和 SNMP 的密码均被设定了安全保护功能，这些功能包括：

- 定义最小密码长度
- 密码过期
- 防止频繁地重复使用密码
- 在用户若干次登录尝试失败后，将其锁定

启用密码管理后，密码的存在时间将立即启动。超过用户定义的时间/日期时，密码即过期。在密码过期前十天，设备将显示一条密码过期警告信息。

密码过期后，用户还可以再登录三次。在最后三次登录期间，系统将显示附加的警告信息，提示用户必须立即更改密码。如果不更改密码，用户将被系统锁定，而只能使用控制台进行登录。密码警告将记录到系统日志文件中。

如果重新定义权限级别，则用户也必须重新定义。但是，密码的存在时间是从初始用户定义时开始计算过期时间。

要打开“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 6-45. 密码管理

“Password Management”（密码管理）页面包含以下字段：

“Password Minimum Length (8-64)”（密码最小长度 [8 至 64]）— 如果选取此字段，则表示最小密码长度。例如，管理员可以定义所有的密码都必须至少包含 10 个字符。

“Consecutive Passwords Before Re-use”（重用密码前该密码的连续更改次数）— 表示一个密码在能够重新使用之前需要被更改的次数。可能的字段值为 1 至 10。

注：系统会在密码过期前通知用户，并要求用户必须更改密码。但是，系统不会对 Web 用户显示此通知。

“Enable Login Attempts”（启用登录尝试）— 如果选取此字段，则当使用错误密码尝试登录的次数超过用户定义的次数，设备会将用户锁定。例如，如果选取了此字段并将其配置为 5，而且用户使用不正确的密码尝试登录已达五次，则设备将在用户第六次尝试登录时将其锁定。可能的字段值为 1 至 5。

定义密码管理

1. 打开“Password Management”（密码管理）页面。
2. 定义字段。
3. 单击“Apply Changes”（应用更改）。

系统将定义密码管理，并更新设备。

使用 CLI 命令管理密码

下表概括了用于设置“Password Management” （密码管理）页面中显示的字段的等效 CLI 命令。

表 6-42. 使用 CLI 命令管理密码

CLI 命令	说明
password min-length 长度	定义最小密码长度。
password history 次数	定义一个密码在能够重新使用之前需要被更改的次数。
password lock-out 次数	定义在用户被设备锁定之前输入错误密码的次数。
show password configuration	显示密码管理信息。

以下是 CLI 命令的示例：

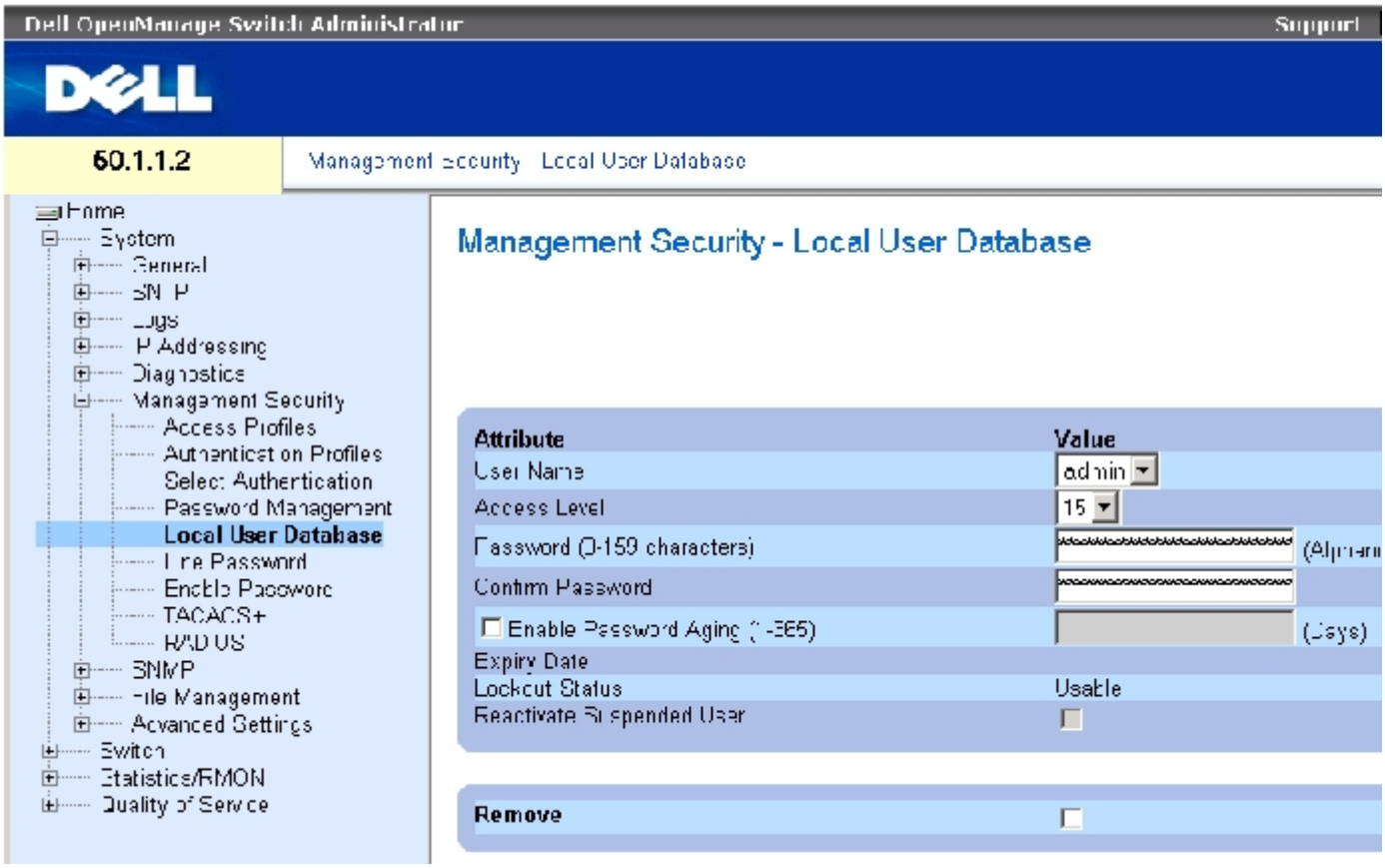
```
console # show passwords configuration

Minimal length: 0

History:Disabled

History hold time:no limit

Lockout control:disabled


Enable Passwords

Level   Password Aging  Password Expiry date  Lockout
-----   --------        ------------          -------
1       -               -                     -
15      -               -                     -
```

Line Passwords				
Line	Password Aging	Password Expiry date	Lockout	
-------	--------	----------	-------	
Telnet	-	-	-	
SSH	-	-	-	
Console	-	-	-	
console # **show users accounts**				
Username	Privilege	Password Aging	Password Expiry Date	Lockout
--------	---------	--------	---------	------
nim	15	39	18-Feb-2005	

定义本地用户数据库

“Local User Database”（本地用户数据库）页面包含用于定义用户、密码和访问级别的字段。要打开“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 6-46. 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，最高的用户访问级别为 15。访问级别为 15 的用户是具有权限的用户，只有这些用户才能访问和使用 OpenManage Switch Administrator。

“Password (0-159 Characters)”（密码 [0 至 159 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。

“Enable Password Aging (1-365)”（启用密码存在时间 [1 至 365]）— 如果选择此字段，则表示密码过期前经过的时间（以天为单位）。

“Expiry Date”（过期日期）— 表示用户定义的密码的过期日期。

“Lockout Status”（闭锁状态）— 如果在“Password Management”（密码管理）页面中选取了“Enable Login Attempts”（启用登录尝试）复选框，此字段将用于指定自用户上次成功登录后尝试验证失败的次数。当用户帐户被锁定后，请指定“LOCKOUT”（闭锁）。

“Reactivate Suspended User”（重新激活暂挂用户）— 如果选择此字段，将重新激活指定用户的访问权限。如果尝试登录不成功，可以暂挂访问权限。

“Remove”（删除）— 如果选择此字段，将从“User Name”（用户名）列表中删除用户。

要为用户分配访问权限，请：

1. 打开“Local User Database”（本地用户数据库）页面。
2. 在“User Name”（用户名）字段中选择一个用户。
3. 定义字段。
4. 单击“Apply Changes”（应用更改）。

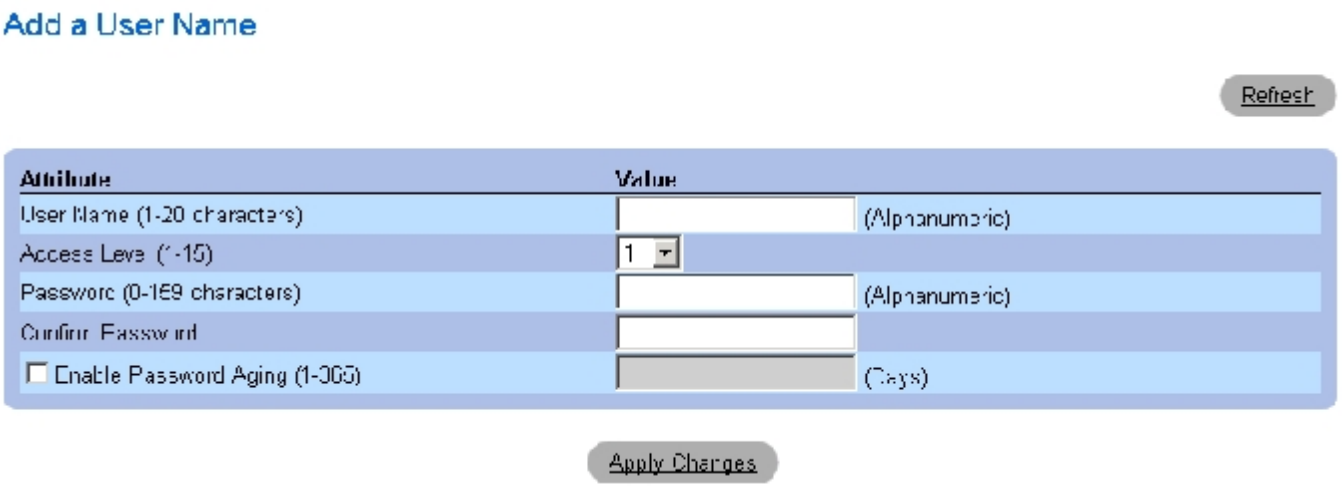
系统将定义用户访问权限和密码，并更新设备。

要定义新用户，请：

1. 打开“Local User Database”（本地用户数据库）页面。
2. 单击“Add”（添加）。

系统将打开“Add User”（添加用户）页面：

图 6-47. 添加用户



3. 定义字段。

4. 单击“Apply Changes”（应用更改）。

系统将定义新用户，并更新设备。

要显示本地用户表，请：

1. 打开“Local User Database”（本地用户数据库）页面。
2. 单击“Show All”（全部显示）。

系统将打开“Local User Table”（本地用户表）：

图 6-48. 本地用户表

要重新激活暂挂用户，请：

1. 打开“Local User Database”（本地用户数据库）页面。
2. 单击“Show All”（全部显示）。

系统将打开“Local User Table”（本地用户表）。

3. 选择一个用户名条目。
4. 选取“Reactivate Suspended User”（重新激活暂挂用户）复选框。
5. 单击“Apply Changes”（应用更改）。

系统将重新激活用户访问权限，并更新设备。

要删除用户，请：

1. 打开“Local User Database”（本地用户数据库）页面。
2. 单击“Show All”（全部显示）。

   系统将打开“Local User Table”（本地用户表）。
3. 选择一个用户名。
4. 选取“Remove”（删除）复选框。
5. 单击“Apply Changes”（应用更改）。

   系统将删除选定的用户，并更新设备。

使用 CLI 命令设定用户

下表概括了用于设置“Local User Database”（本地用户数据库）页面中显示的字段的等效 CLI 命令。

表 6-43. 本地用户数据库 CLI 命令

CLI 命令	说明
username 名称 [password 密码] [level 级别] [encrypted]	建立基于用户名的验证系统。
set username 名称 active	重新激活暂挂用户的访问权限。

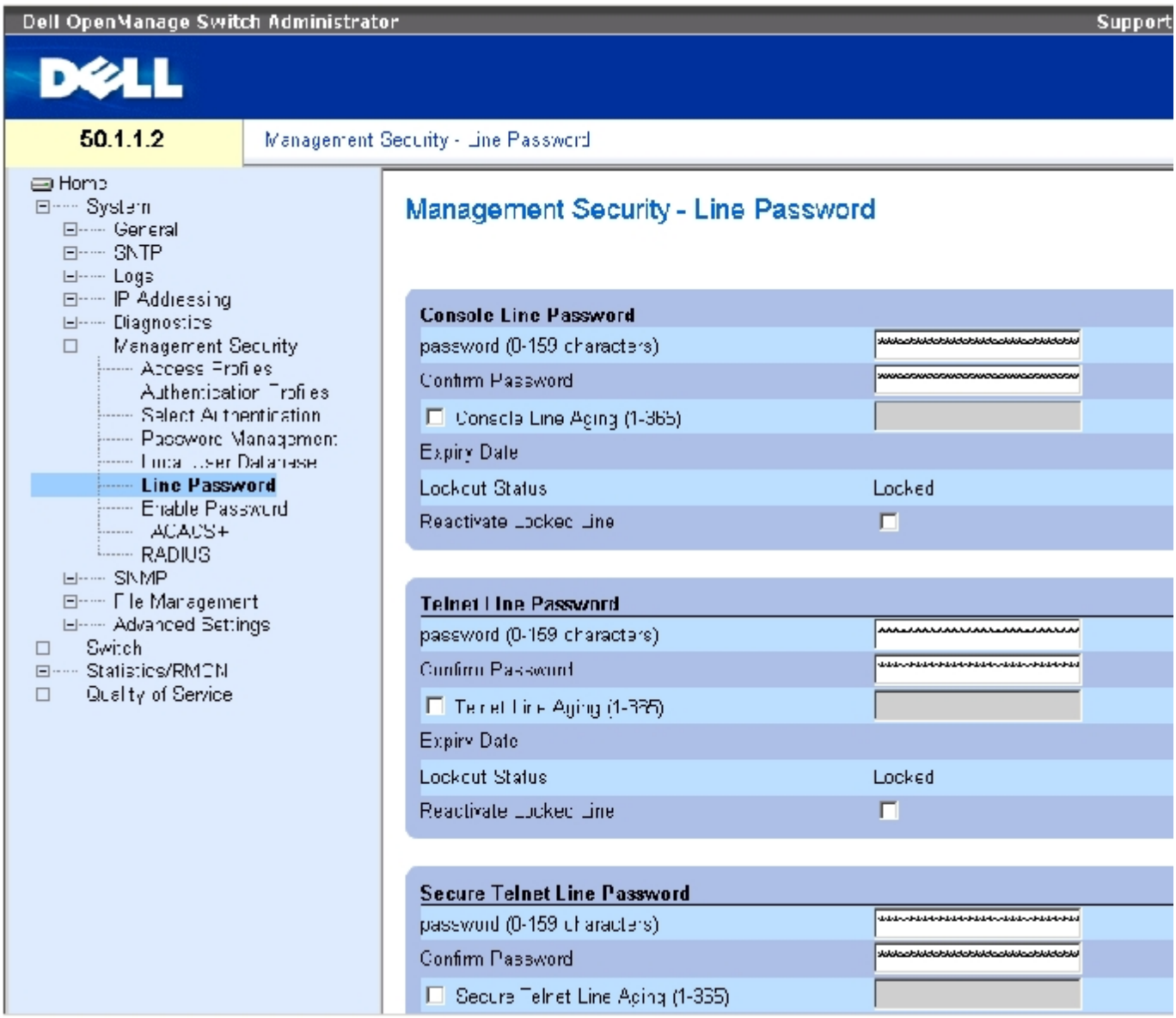
以下是 CLI 命令的示例：

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


console# set username bob
active
```

定义线路密码

“Line Password”（线路密码）页面包含用于定义管理方法的线路密码的字段。要打开“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 Passwords”（线路密码）。

图 6-49. 线路密码



“Line Password”（线路密码）页面包含以下字段：

“Console Line Password”（控制台的线路密码）/“Telnet Line Password”（Telnet 的线路密码）/“Secure Telnet Line Password”（安全 Telnet 的线路密码）— 用于通过控制台、Telnet 或安全 Telnet 会话访问设备的线路密码。

用于控制台/Telnet/安全 Telnet 的“Confirm Password”（确认密码）— 确认新的线路密码。密码将以 ***** 形式显示。

“Console Line Aging (1-365)”（控制台线路的存在时间 [1 至 365]）/“Telnet Line Aging (1-365)”（Telnet 线路的存在时间 [1 至 365]）/“Secure Telnet Line Aging (1-365)”（安全 Telnet 线路的存在时间 [1 至 365]）— 如果选择此字段，则表示在线路密码过期前经过的时间（以天为单位）。

控制台/Telnet/安全 Telnet 的“Expiry Date”（过期日期）— 表示线路密码的过期日期。

控制台/Telnet/安全 Telnet 的“Lockout Status”（闭锁状态）— 如果在“Password Management”（密码管理）页面中选取了“Enable Login Attempts”（启用登录尝试）复选框，此字段将用于指定自用户上次成功登录后尝试验证失败的次数。当用户帐户被锁定后，请指定“LOCKOUT”（闭锁）。

控制台/Telnet/安全 Telnet 的“Reactivate Locked Line”（重新激活锁定线路）— 如果选择此字段，将为控制台/Telnet/安全 Telnet 会话重新激活线路密码。如果尝试登录不成功，可以暂挂访问权限。

定义控制台会话的线路密码

1. 打开“Line Password”（线路密码）页面。
2. 定义“Console Line Password”（控制台线路密码）字段。
3. 单击“Apply Changes”（应用更改）。

系统将定义控制台会话的线路密码，并更新设备。

定义 Telnet 会话的线路密码

1. 打开“Line Password”（线路密码）页面。
2. 定义“Telnet Line Password”（Telnet 线路密码）字段。
3. 单击“Apply Changes”（应用更改）。

系统将定义 Telnet 会话的线路密码，并更新设备。

定义安全 Telnet 会话的线路密码

1. 打开“Line Password”（线路密码）页面。
2. 定义“Secure Telnet Line Password”（安全 Telnet 线路密码）字段。
3. 单击“Apply Changes”（应用更改）。

系统将定义安全 Telnet 会话的线路密码，并更新设备。

使用 CLI 命令设定线路密码

下表概括了用于设置“Line Password”（线路密码）页面中显示的字段的等效 CLI 命令。

表 6-44. 线路密码的 CLI 命令

CLI 命令	说明
password 密码 [encrypted]	表示线路上的密码。

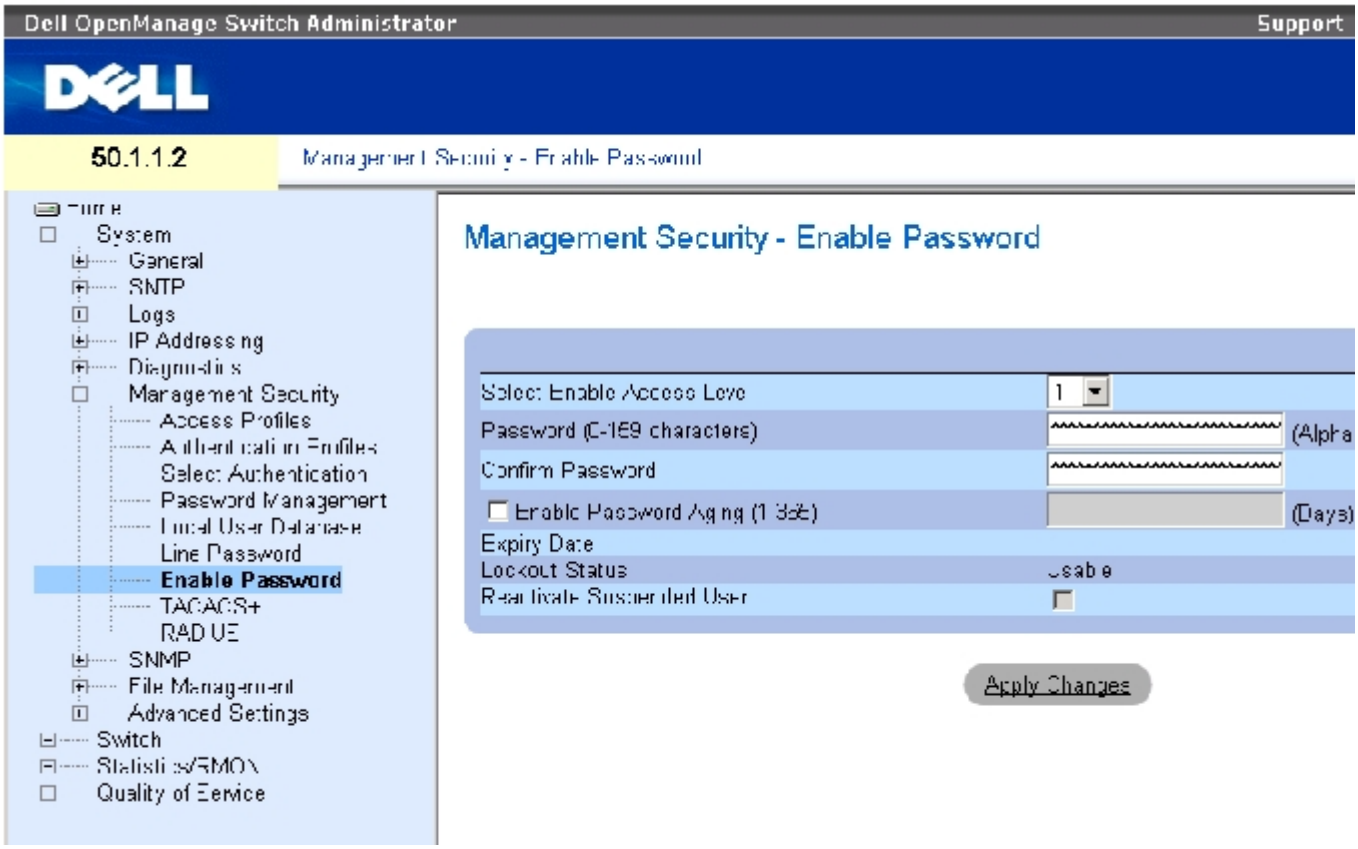
以下是 CLI 命令的示例：

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

定义启用密码

“Enable Password”（启用密码）页面用于设置本地密码，以控制对普通级别和优先级别的访问。要打开“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 Passwords”（启用密码）。

图 6-50. 启用密码



“Enable Password” （启用密码）页面包含以下字段：

“Select Enable Access Level” （选择启用访问级别） — 与启用密码相关联的访问级别。可能的字段值为 1 至 15。

“Password (0-159 Characters)” （密码 [0 至 159 个字符]） — 当前的启用密码。

“Confirm Password” （确认密码） — 确认新的启用密码。密码将以 ***** 形式显示。

“Enable Password Aging (1-365)” （启用密码存在时间 [1 至 365]） — 如果选择此字段，则表示密码过期前经过的时间（以天为单位）。

“Expiry Date” （过期日期） — 表示启用密码的过期日期。

“Lockout Status” （闭锁状态） — 如果在“Password Management” （密码管理）页面中选取了“Enable Login Attempts” （启用登录尝试）复选框，此字段将用于指定自用户上次成功登录后尝试验证失败的次数。当用户帐户被锁定后，请指定“LOCKOUT” （闭锁）。

“Reactivate Suspended User” （重新激活暂挂用户） — 如果选择此字段，将重新激活指定用户的访问权限。如果尝试登录不成功，可以暂挂访问权限。

要定义新的启用密码，请：

1. 打开“Enable Password” （启用密码）页面。

2. 定义字段。

3. 单击“Apply Changes”（应用更改）。

系统将定义新的启用密码，并更新设备。

使用 CLI 命令设定启用密码

下表概括了用于设置“Enable Password”（启用密码）页面中显示的字段的等效 CLI 命令。

表 6-45. 修改启用密码的 CLI 命令

CLI 命令	说明
enable password [level 级别] 密码 [encrypted]	设置本地密码以控制对用户和权限级别的访问。

以下是 CLI 命令的示例：

```
console(config)# enable
password level 15 secret
```

定义 TACACS+ 设置

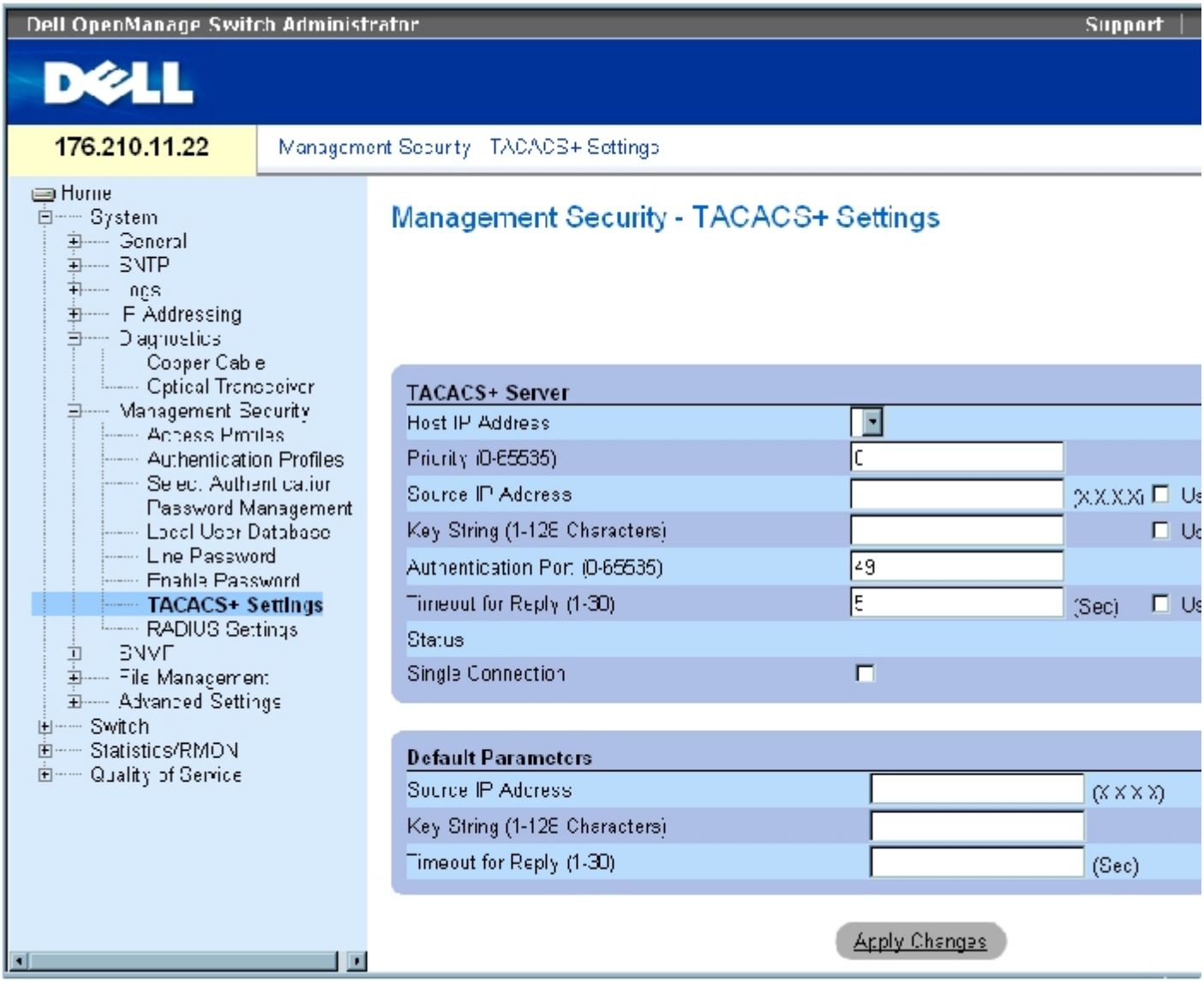
设备提供对终端访问控制器访问控制系统（TACACS+）客户端的支持。TACACS+ 为访问设备的用户的验证提供了集中式的安全保护。

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+ 协议通过设备与 TACACS+ 服务器之间加密的协议交换确保网络完整性。要打开“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+”。

图 6-51. TACACS+ 设置



“TACACS+ Settings” (TACACS+ 设置) 页面包含以下字段：

“Host IP Address” (主机 IP 地址) — 表示 TACACS+ 服务器 IP 地址。

“Priority (0-65535)” (优先级 [0 至 65535]) — 表示使用 TACACS+ 服务器的顺序。默认值为 0。

“Source IP Address” (源 IP 地址) — 用于设备与 TACACS+ 服务器之间的 TACACS+ 会话的设备源 IP 地址。

“Key String (0-128 Characters)” (密钥字符串 [0 至 128 个字符]) — 定义设备与 TACACS+ 服务器之间的 TACACS+ 通信的验证和加密密钥。此密钥必须与 TACACS+ 服务器上使用的加密密钥相匹配。此密钥已被加密。

“Authentication Port (0-65535)” (验证端口 [0 至 65535]) — 通过其进行 TACACS+ 会话的端口号。默认端口号为 49。

“Timeout for Reply (1-30)” (回复超时 [1 至 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。

“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）— 当前设备与 TACACS+ 服务器之间有连接。

“Not Connected”（未连接）— 当前设备与 TACACS+ 服务器之间无连接。

“Single Connection”（单一连接）— 如果选择此字段，将在设备与 TACACS+ 服务器之间维护单一打开的连接。

TACACS+ 默认参数是用户定义的默认值。默认设置将应用于新定义的 TACACS+ 服务器。如果未定义默认值，则将系统默认值应用于新的 TACACS+ 服务器。

以下是 TACACS+ 默认值：

“Source IP Address”（源 IP 地址）— 用于设备和 TACACS+ 服务器之间的 TACACS+ 会话的默认设备源 IP 地址。默认的源 IP 地址为 0.0.0.0。

“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 TACACS+ 服务器之间所有通信的默认密钥字符串。此密钥已被加密。

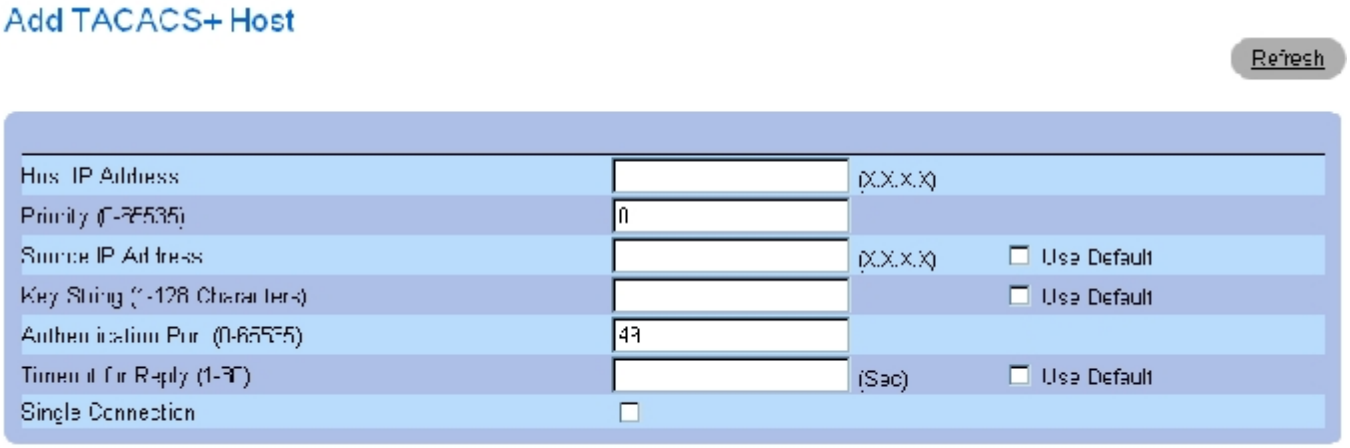
“Timeout for Reply (1-30)”（回复超时 [1 至 30]）— 设备与 TACACS+ 连接超时之前所经过的默认时间。默认值为 5 秒。

添加 TACACS+ 服务器

1. 打开“TACACS+ Settings”（TACACS+ 设置）页面。
2. 单击“Add”（添加）。

   系统将打开“Add TACACS+ Host”（添加 TACACS+ 主机）页面。

图 6-52. 添加 TACACS+ 主机



3. 定义字段。

4. 单击“Apply Changes”（应用更改）。

系统将添加 TACACS+ 服务器，并更新设备。

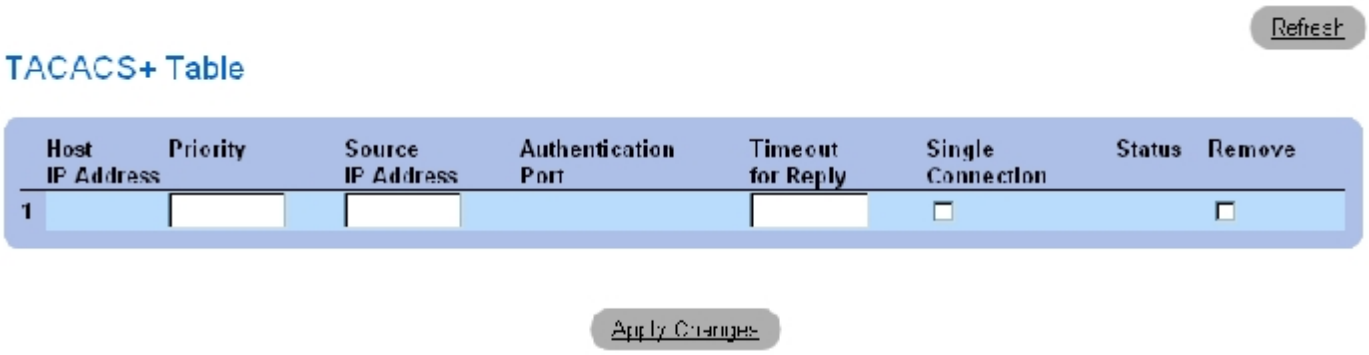
显示 TACACS+ 表

1. 打开“TACACS+ Settings”（TACACS+ 设置）页面。

2. 单击“Show All”（全部显示）。

系统将打开“TACACS+ Table”（TACACS+ 表）：

图 6-53. TACACS+ 表



删除 TACACS+ 服务器

1. 打开“TACACS+ Table” (TACACS+ 表) 页面。
2. 单击“Show All” (全部显示) 。

   系统将打开“TACACS+ Table” (TACACS+ 表) :
3. 选择一个“TACACS+ Table” (TACACS+ 表) 条目。
4. 选取“Remove” (删除) 复选框。
5. 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+ 设置

下表概括了用于设置“TACACS+ Settings” (TACACS+ 设置) 页面中显示的字段的等效 CLI 命令。

表 6-46. TACACS+ 的 CLI 命令

CLI 命令	说明
tacacs-server host {IP 地址 | 主机名称} [single-connection] [port 端口号] [timeout 超时] [key 密钥字符串] [source 源] [priority 优先级]	表示 TACACS+ 主机。
tacacs-server key 密钥字符串	表示设备与 TACACS+ 服务器之间所有 TACACS+ 通信的验证和加密密钥。此密钥必须与 TACACS+ 守护程序中使用的加密相匹配。 (范围为0 至 128 个字符。)
tacacs-server timeout 超时	表示超时值 (以秒为单位) 。 (范围为 1 - 30.)
tacacs-server source-ip 源	表示源 IP 地址。 (范围为有效的 IP 地址。)
show tacacs [IP 地址]	显示 TACACS+ 服务器的配置和统计数据。

以下是 CLI 命令的示例:

```
console# show tacacs
```

Device Configuration						
IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority
----------	----------	----	----------	-------	----------	----------
12.1.1.2	Not Connected	49	Yes	1	12.1.1.1	1
Global values						

TimeOut: 5						
Device Configuration ----------						
Source IP: 0.0.0.0						
console#						

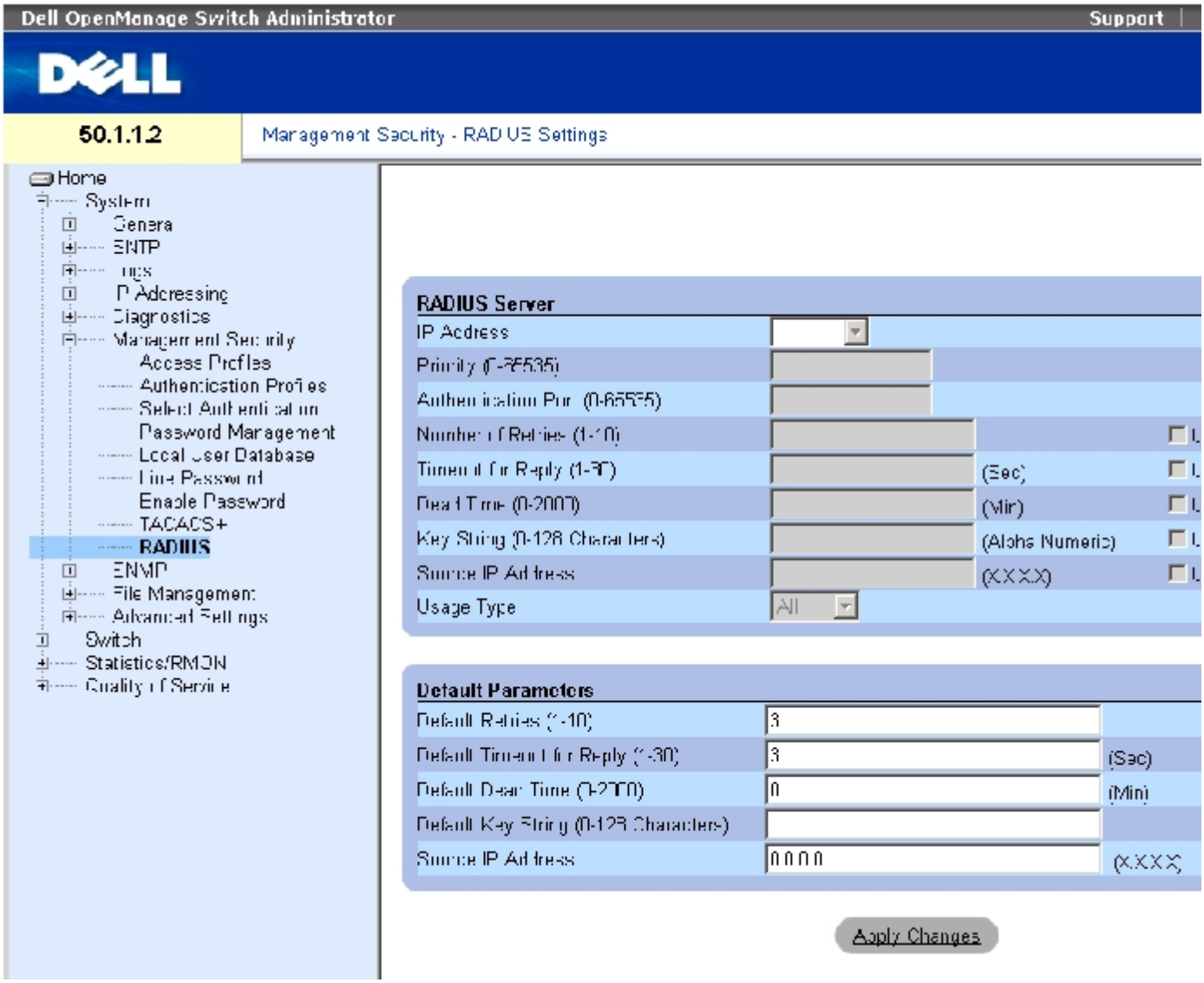
配置 RADIUS 设置

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。最多可以定义四个 RADIUS 服务器。RADIUS 服务器为以下操作提供了集中式的验证方法：

- Telnet 访问
- 安全命令解释程序访问
- Web 访问
- 控制台访问

要打开“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”。

图 6-54. RADIUS 设置



"RADIUS Settings" (RADIUS 设置) 页面包含以下字段：

"IP Address" (IP 地址) — 验证服务器 IP 地址的列表。

"Priority (0-65535)" (优先级 [0 至 65535]) — 服务器的优先级。可能的值为 0 至 65535，其中 0 表示最高优先级。此选项用于配置查询服务器的顺序。

"Authentication Port" (验证端口) — 标识验证端口。验证端口用于验证 RADIUS 服务器验证。

"Number of Retries (1-10)" (重试次数 [1 至 10]) — 表示在失败前发送至 RADIUS 服务器的请求被传输的次数。可能的字段值为 1 至 10。

"Timeout for Reply (1-30)" (回复超时 [1 至 30]) — 表示在重试查询或切换至下一个服务器之前，设备等待 RADIUS 服务器回复的时间 (以秒为单位) 。可能的字段值为 1 至 30。

“Dead Time (0-2000)”（停用时间 [0 至 2000]）— 表示不经过 RADIUS 服务器进行服务请求的时间（以分钟为单位）。范围为 0 至 2000。

“Key String (1-128 Characters)”（密钥字符串 [1 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。此密钥已被加密。

“Source IP Address”（源 IP 地址）— 表示用于与 RADIUS 服务器进行通信的源 IP 地址。

“Usage Type”（使用类型）— 表示服务器的使用类型。它可以是以下值之一：“login”（登录）、“802.1x”或“all”（全部）。如果未指定，则默认为“all”（全部）。

以下字段设置了 RADIUS 的默认值：

注：如果未指定主机特定的超时、重试次数或停用时间值，则全局值（默认值）将应用于各主机。

“Default Retries (1-10)”（默认重试次数 [1 至 10]）— 表示在失败前发送至 RADIUS 服务器的请求被传输的默认次数。

“Default Timeout for Reply (1-30)”（默认回复超时 [1 至 30]）— 表示超时之前设备等待 RADIUS 服务器回复的默认时间（以秒为单位）。默认值为 5 秒。

“Default Dead time (0-2000)”（默认停用时间 [0 至 2000]）— 表示不经过 RADIUS 服务器进行服务请求的默认时间（以分钟为单位）。范围为 0 至 2000。

“Default Key String (1-128 Characters)”（默认密钥字符串 [1 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。此密钥已被加密。

“Source IP Address”（源 IP 地址）— 表示用于与 RADIUS 服务器进行通信的默认源 IP 地址。默认的源 IP 地址为 0.0.0.0。

要定义 RADIUS 参数，请：

1. 打开“RADIUS Settings”（RADIUS 设置）页面。
2. 定义字段。
3. 单击“Apply Changes”（应用更改）。

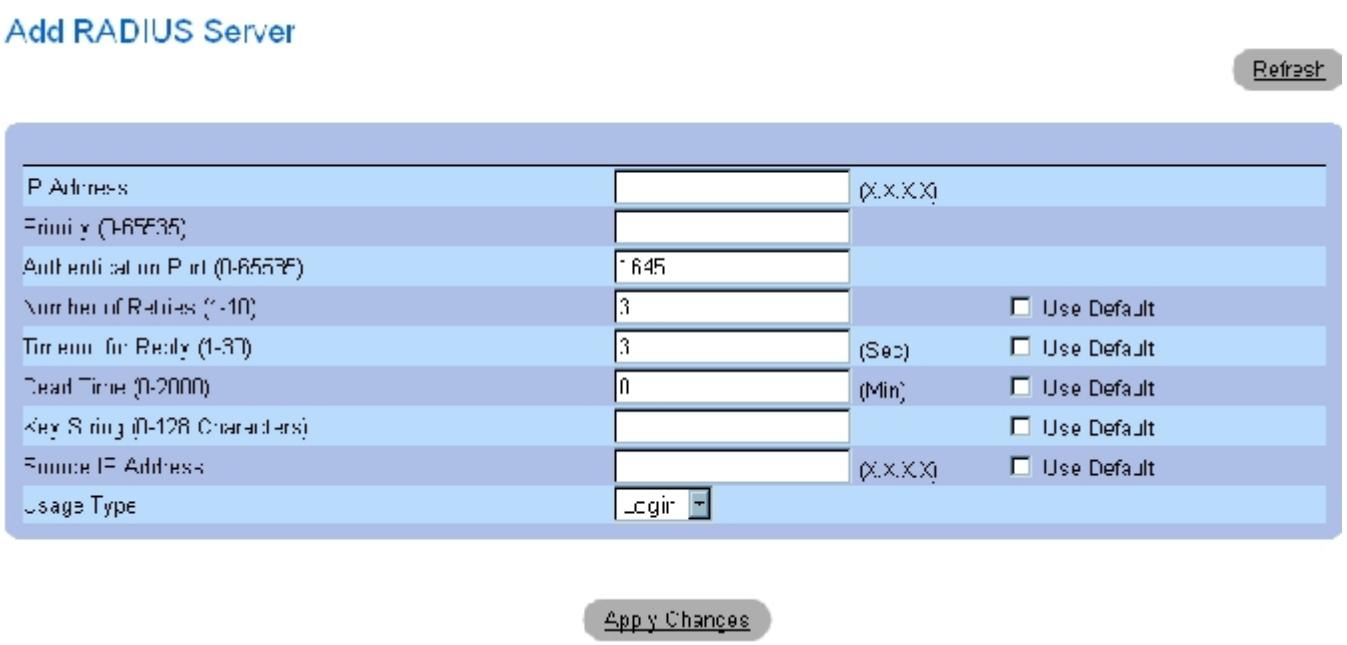
RADIUS 设置将被更新到设备。

要添加 RADIUS 服务器，请：

1. 打开“RADIUS Settings” (RADIUS 设置) 页面。
2. 单击“Add” (添加) 。

系统将打开“Add RADIUS Server” (添加 RADIUS 服务器) 页面：

图 6-55. 添加 RADIUS 服务器



3. 定义字段。
4. 单击“Apply Changes” (应用更改) 。

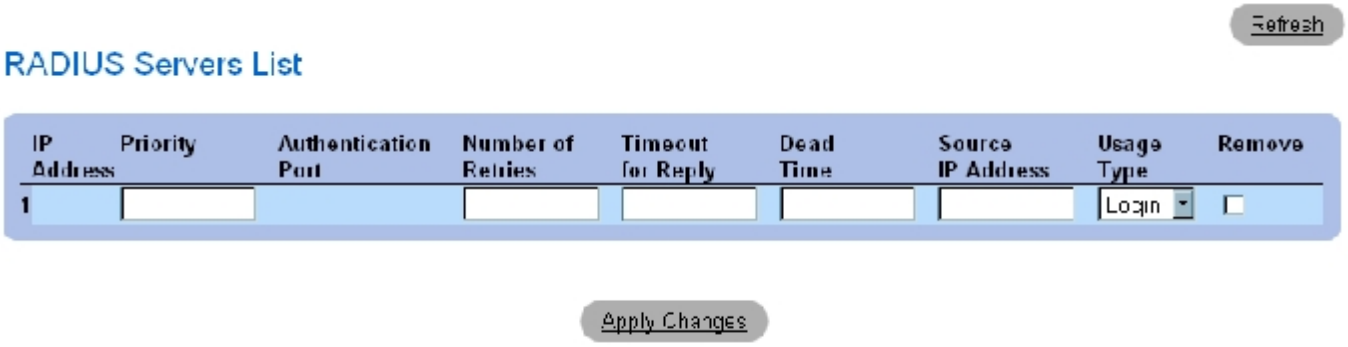
系统将添加新的 RADIUS 服务器，并更新设备。

要显示 RADIUS 服务器列表，请：

1. 打开“RADIUS Settings” (RADIUS 设置) 页面。
2. 单击“Show All” (全部显示) 。

系统将打开“RADIUS Servers List” (RADIUS 服务器列表)：

图 6-56. RADIUS 服务器列表



删除 RADIUS 服务器

1. 打开“RADIUS Settings” (RADIUS 设置)页面。
2. 单击“Show All” (全部显示)。

系统将打开“RADIUS Servers List” (RADIUS 服务器列表)。

3. 选择一个“RADIUS Servers List” (RADIUS 服务器列表)条目。
4. 选取“Remove” (删除)复选框。
5. 单击“Apply Changes” (应用更改)。

系统将删除 RADIUS 服务器，并更新设备。

使用 CLI 命令定义 RADIUS 服务器

下表概括了用于定义“RADIUS Settings” (RADIUS 设置)页面中显示的字段的等效 CLI 命令。

表 6-47. RADIUS 服务器的 CLI 命令

CLI 命令	说明
	设置路由器等待服务器主机回复的时

radius-server timeout 超时	间间隔。
radius-server retransmit 重试次数	指定软件搜索 RADIUS 服务器主机列表的次数。
radius-server deadtime停用时间	配置要被忽略的不可用服务器。
radius-server key 密钥字符串	为路由器与 RADIUS 环境之间的所有 RADIUS 通信设置验证和加密密钥。
radius-server hostIP 地址 [**auth-port**验证端口号] [**timeout** 超时] [**retransmit** 重试次数] [**deadtime** 停用时间] [**key** 密钥字符串] [**source** 源] [**priority** 优先级]	指定 RADIUS 服务器主机。
show radius-servers	显示 RADIUS 服务器设置。

以下是 CLI 命令的示例：

```
Console(config)# radius-server timeout 5

Console(config)# radius-server retransmit 5

Console(config)# radius-server deadtime 10

Console(config)# radius-server key dell-server

Console(config)# radius-server host 196.210.100.1 auth-port 127timeout 20

Console# show radius-servers

IP address Auth Acct TimeOut Retransmit Deadtime Source IP Priority

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

172.16.1.1 164 51646 3 3 0 01 172.16.1.2 164 51646 3 3 0 02
```

定义 SNMP 参数

简单网络管理协议（SNMP）提供了管理网络设备的方法。交换机支持以下 SNMP 版本：

- SNMPv1（第 1 版）
- SNMPv2（第 2 版）
- SNMPv3（第 3 版）

SNMP v1 和 v2

SNMP 代理可以维护用于管理交换机的变量列表。变量在管理信息库（MIB）中进行定义。MIB 提供了代理控制的变量。SNMP 代理定义了 MIB 规范格式，以及通过网络访问信息的格式。访问 SNMP 代理的权限由访问字符串控制。

默认情况下将启用 SNMPv1 和 v2。

SNMP v3

SNMP v3 还将访问控制和新的陷阱机制应用于 SNMPv1 和 SNMPv2 PDU。此外，还为 SNMPv3 定义了用户安全保护模型（USM），该模型包括：

- “Authentication”（验证）— 提供数据完整性和数据原始验证。
- “Privacy”（保密）— 避免泄漏信息内容。使用密码块链接（CBC）进行加密。可以对 SNMP 信息启用验证，也可以对其同时启用验证和保密。但不能在未启用验证的情况下启用保密。
- “Timeliness”（及时）— 避免信息延迟或信息冗余。SNMP 代理会将外来信息与信息的时间信息进行比较。
- “Key Management”（密钥管理）— 定义密钥生成、密钥更新和密钥使用。

交换机支持基于对象 ID（OID）的 SNMP 通知过滤器。系统将使用 OID 来管理交换机功能。SNMP v3 支持以下功能：

- 安全保护
- 功能访问控制
- 陷阱

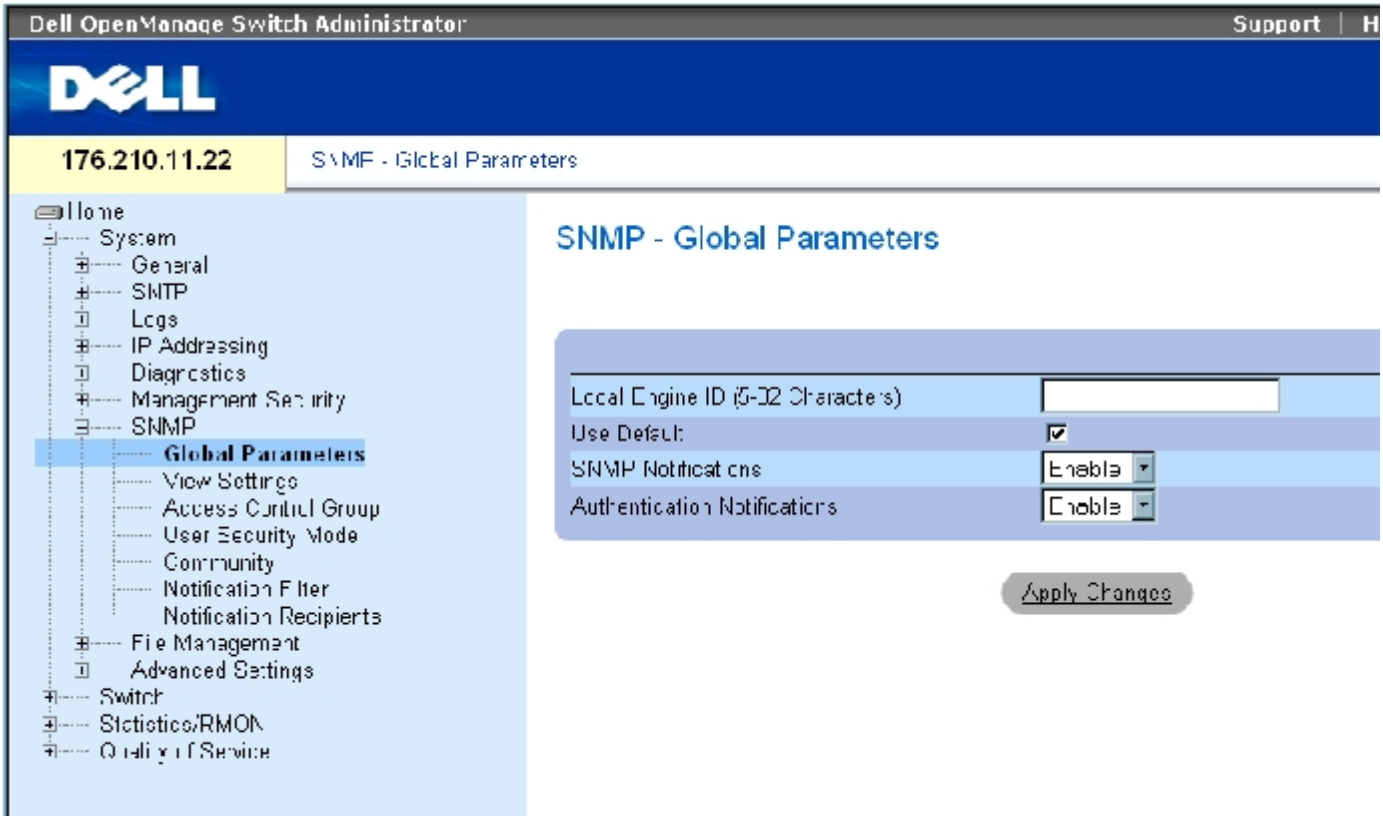
可以在用户安全保护模型（USM）中修改验证或保密密钥。

仅当本地引擎 ID 处于启用状态时，才能启用 SNMPv3。

定义 SNMP 全局参数

"SNMP Global Parameters" (SNMP 全局参数) 页面允许启用 SNMP 和验证通知。要打开"SNMP Global Parameters" (SNMP 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 6-57. SNMP 全局参数



"SNMP Global Parameters" (SNMP 全局参数) 页面包含以下字段：

"Local Engine ID" (本地引擎 ID) — 表示本地设备引擎 ID。此字段值为一个十六进制字符串。十六进制字符串的每个字节是两个十六进制数字。每个字节可由句点或冒号隔开。必须在启用 SNMPv3 之前定义引擎 ID。

对于独立设备，请选择默认引擎 ID，此 ID 由企业编号和默认 MAC 地址组成。

对于可堆栈系统，请配置引擎 ID 并验证此引擎 ID 对于管理域是否唯一。这样可以避免网络中的两个设备具有同一个引擎 ID。

"Use Defaults" (使用默认值) — 使用设备生成的引擎 ID。默认的引擎 ID 是基于设备 MAC 地址，并按照以下标准进行定义：

前 4 个八位位组 — 第一位 = 1，其余三位是 IANA 企业编号 = 674。

第 5 个八位位组 — 设置为 3 以表示后跟 MAC 地址。

最后 6 个八位位组 — 设备的 MAC 地址。

“SNMP Notifications”（SNMP 通知）— 启用或禁用路由器发送 SNMP 通知。

“Authentication Notifications”（验证通知）— 启用或禁用路由器在验证失败时发送 SNMP 陷阱。

启用 SNMP 通知

1. 打开“SNMP Global Parameters”（SNMP 全局参数）页面。
2. 在“SNMP Notifications”（SNMP 通知）字段中选择“Enable”（启用）。
3. 单击“Apply Changes”（应用更改）。

系统将启用 SNMP 通知，并更新设备。

启用验证通知

1. 打开“SNMP Global Parameters”（SNMP 全局参数）页面。
2. 在“Authentication Notifications”（验证通知）字段中选择“Enable”（启用）。
3. 单击“Apply Changes”（应用更改）。

使用 CLI 命令启用 SNMP 通知

下表概括了用于查看“SNMP Global Parameters”（SNMP 全局参数）页面中显示的字段的等效 CLI 命令。

表 6-48. SNMP 通知命令

CLI 命令	说明

snmp-server enable traps	启用路由器发送简单网络管理协议陷阱
snmp-server trap authentication	启用路由器在验证失败时发送简单网络管理协议陷阱
show snmp	查看 SNMP 通信的状态。
snmp-server engine ID local {引擎 ID 字符串 | default}	表示本地设备引擎 ID。此字段值为一个十六进制字符串。十六进制字符串的每个字节是两个十六进制数字。每个字节可由句点或冒号隔开。必须在启用 SNMPv3 之前定义引擎 ID。

以下是 CLI 命令的示例：

```
Console(config)# snmp-server enable traps

Console(config)# snmp-server trap authentication

Console# show snmp

Community-String        Community-Access        View name       IP address
----------------        ----------------        ---------       ----------
public                  read only               view-1          All

Community-String        Group name              IP address      Type
----------------        ----------              ----------      ----

Traps are enabled.

Authentication-failure trap is enabled.

Version 1,2 notifications

Target Address  Type  Community  Version  Udp Port  Filter name  To Sec  Retries
--------------  ----  ---------  -------  --------  -----------  ------  -------

Version 3 notifications

Target Address  Type  Username  Security Level  Udp Port  Filter name  To Sec  Retries
--------------  ----  --------  --------------  --------  -----------  ------  -------
```

System Contact:Robert	
System Location:Marketing	

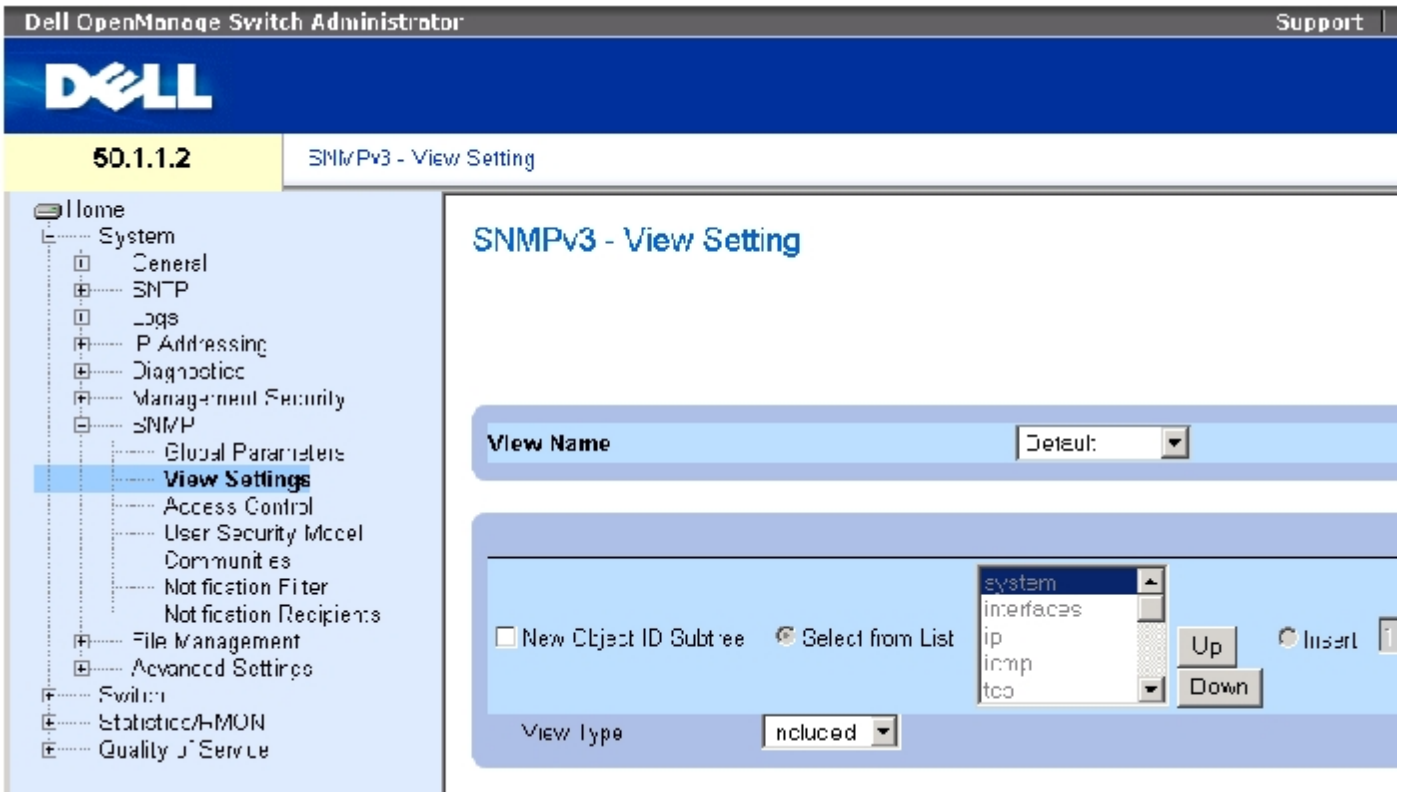
定义 SNMP 视图设置

SNMP 视图可以提供或限制对设备功能或功能相关内容的访问权。例如，可以将视图定义为：SNMP 组 A 对于多点传送组具有只读 (R/O) 权限，而 SNMP 组 B 对于多点传送组具有读写 (R/W) 权限。功能访问权是通过 MIB 名称或 MIB 对象 ID 来授予的。

可以使用上箭头和下箭头来浏览 MIB 树和 MIB 分支。

要打开“SNMPv3 View Settings” (SNMPv3 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 6-58. SNMPv3 视图设置



“SNMPv3 View Settings” (SNMPv3 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列表。视图名称最多可以包含 30 个字母数字字符。

“New Object ID Subtree” (新对象 ID 子树) — 表示在所选 SNMP 视图中包括或排除的设备功能 OID。

“Selected from List”（从列表中选择）— 使用“Up”（向上）和“Down”（向下）按钮在所有设备 OID 的列表中滚动来选择设备功能 OID。

“Insert”（插入）— 指定设备功能 OID。

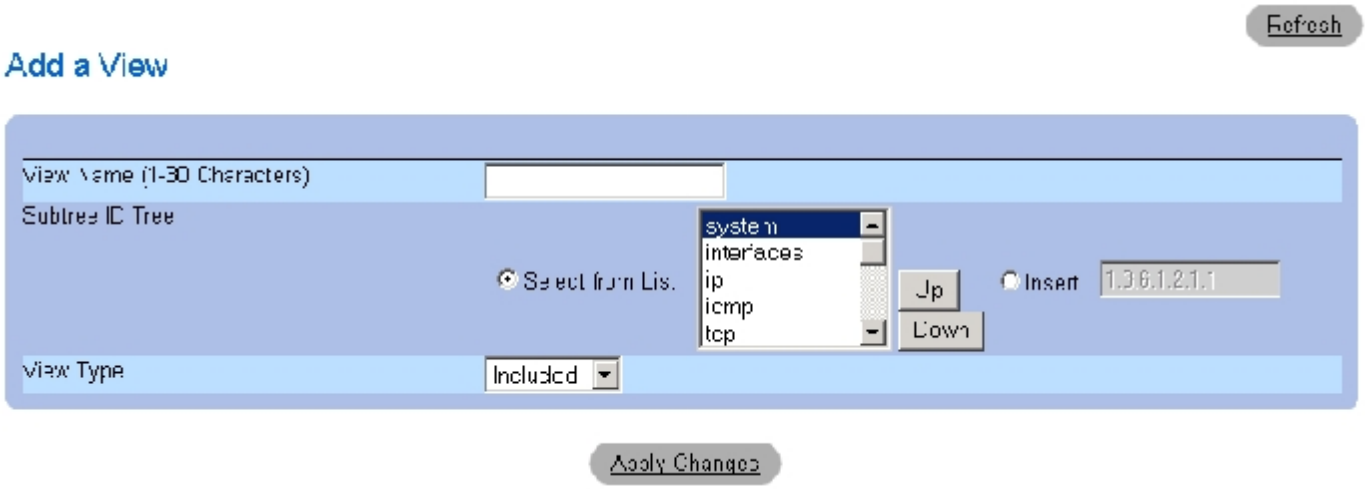
“View Type”（视图类型）— 表示在所选 SNMP 视图中将包括还是排除定义的 OID 分支。

添加视图

1. 打开“SNMPv3 View Settings”（SNMPv3 视图设置）页面。
2. 单击“Add”（添加）。

系统将打开“Add A View”（添加视图）页面：

图 6-59. 添加视图



3. 定义各字段。
4. 单击“Apply Changes”（应用更改）。

系统将添加 SNMP 视图，并更新设备。

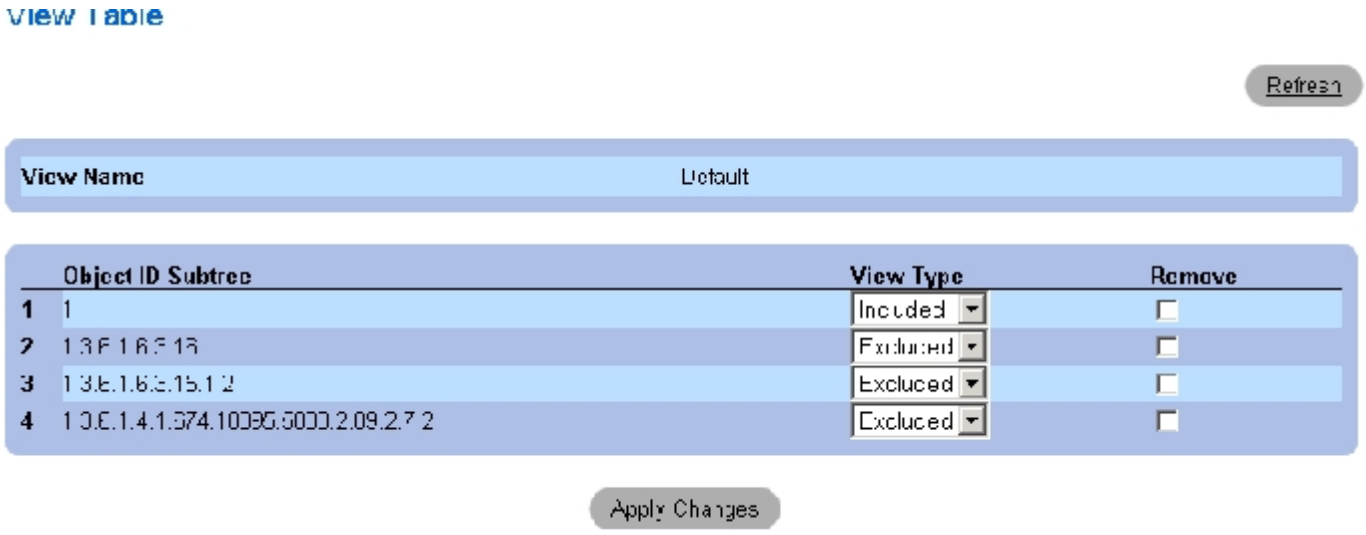
显示视图表

1. 打开“SNMPv3 View Settings”（SNMPv3 视图设置）页面。

2. 单击“Show All”（全部显示）。

系统将打开“View Table”（视图表）页面：

图 6-60. 视图表



使用 CLI 命令定义 SNMPv3 视图

下表概括了用于定义“SNMPv3 View Settings”（SNMPv3 视图设置）页面中显示的字段的等效 CLI 命令。

表 6-49. SNMP 视图的 CLI 命令

CLI 命令	说明
snmp-server view 视图名称 **OID** 树 **{included | excluded}**	创建或更新视图条目。
show snmp views[视图名称]	显示视图配置。

以下是 CLI 命令的示例：

```
Console(config)# snmp-server view user1
1 included

Console(config)# end

Console# show snmp views
```

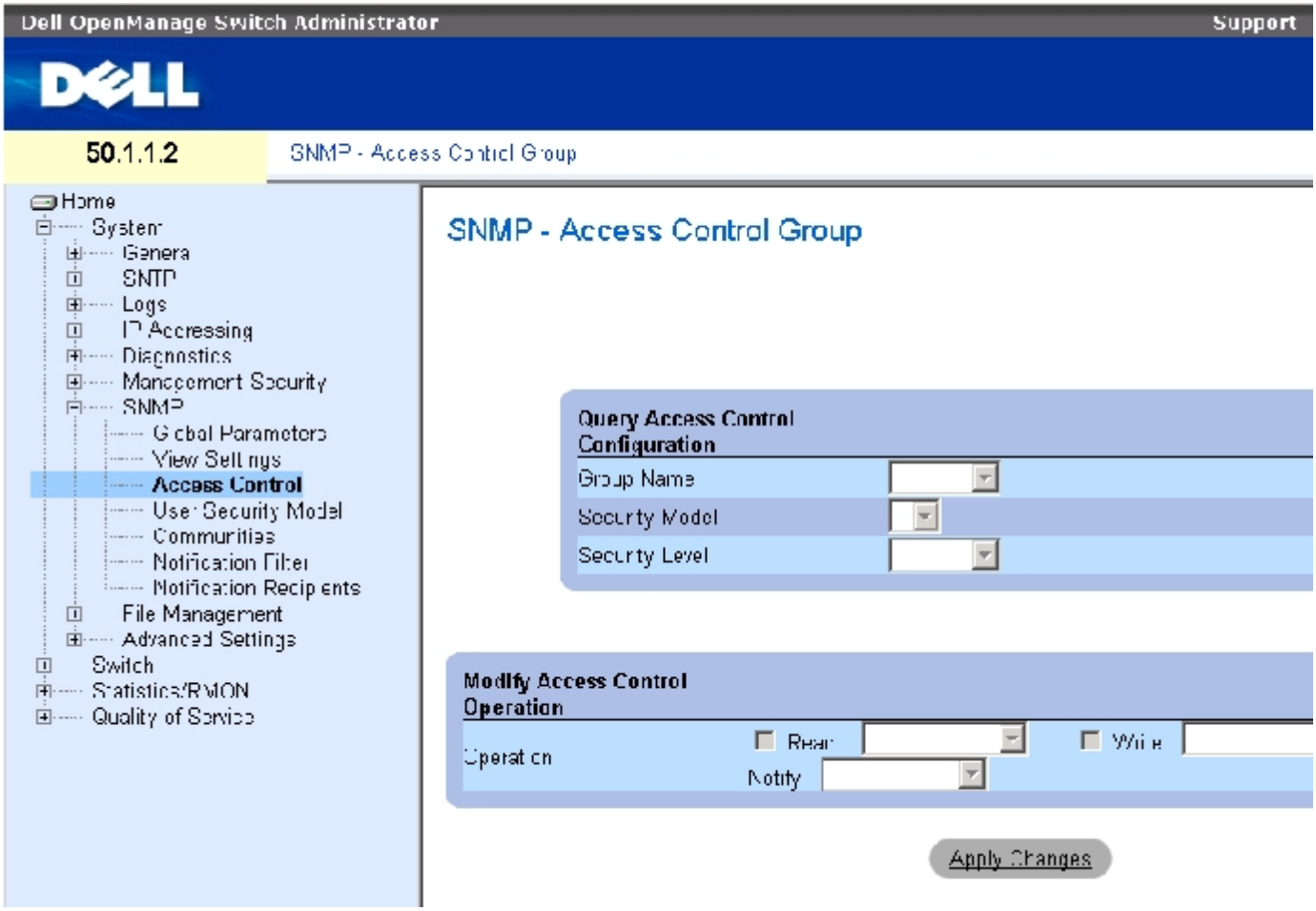

Name	OID Tree	Type
user1	iso	included
Default	iso	included
Default	snmpVacmMIB	excluded
Default	usmUser	excluded
Default	rndCommunityTable	excluded
DefaultSuper	iso	included

定义 SNMP 访问控制

“Access Control”（访问控制）页面提供了用于创建 SNMP 组和设定对 SNMP 组的 SNMP 访问控制权限的信息。组允许网络管理员设定对特定设备功能或功能相关内容的访问权限。

要打开“Access Control Group”（访问控制组）页面，请在树视图中单击“System”（系统）→“SNMP”→“Access Control”（访问控制）。

图 6-61. 访问控制组



“Access Control Group” （访问控制组）包含以下字段：

“Group Name” （组名） — 应用访问控制规则的用户定义的组。此字段范围最多为 30 个字符。

“SNMP Version” （SNMP 版本） — 定义与组关联的 SNMP 版本。可能的字段值包括：

“SNMPv1” — 为组定义 SNMPv1。

“SNMPv2” — 为组定义 SNMPv2。

“SNMPv3” — 为组定义 SNMPv3。

“Security Level” （安全保护级别） — 与组关联的安全保护级别。安全保护级别仅适用于 SNMPv3。可能的字段值包括：

“No Authentication” （无验证） — 不为组设定验证或保密安全保护级别。

“Authentication” （验证） — 验证 SNMP 信息，并确保验证 SNMP 信息原文。

“Privacy” （保密） — 对 SNMP 信息进行加密。

“Operation”（操作）— 定义组访问权限。可能的字段值包括：

“Read”（读取）— 管理访问权限被限制为只读，并且不能对已设定的 SNMP 视图进行更改。

“Write”（写入）— 管理访问权限为读写，并且可以对已设定的 SNMP 视图进行更改。

“Notify”（通知）— 发送已设定的 SNMP 视图的陷阱。

定义 SNMP 组

1. 打开“Access Control Group”（访问控制组）页面。
2. 单击“Add”（添加）。

系统将打开“Add an Access Control Group”（添加访问控制组）页面：

图 6-62. 添加访问控制组

3. 定义“Add an Access Control Group”（添加访问控制组）页面中的字段。
4. 单击“Apply Changes”（应用更改）。

系统将添加组，并更新设备。

显示访问表

1. 打开“Access Control Group”（访问控制组）页面。
2. 单击“Show All”（全部显示）。

   系统将打开“Access Table”（访问表）：

图 6-63. 访问表

删除 SNMP 组

1. 打开“Access Control Group”（访问控制组）页面。
2. 单击“Show All”（全部显示）。

   系统将打开“Access Table”（访问表）。
3. 选择一个 SNMP 组。
4. 选取“Remove”（删除）复选框。
5. 单击“Apply Changes”（应用更改）。

   系统将删除 SNMP 组，并更新设备。

使用 CLI 命令定义 SNMP 访问控制

下表概括了用于定义“Access Control Group”（访问控制组）页面中显示的字段的等效 CLI 命令。

表 6-50. SNMP 访问控制的 CLI 命令

CLI 命令	说明
snmp-server group 组名 **{v1 | v2 | v3 {noauth | auth | priv}}** **[read** 读取视图] **[write** 写入视图] **[notify** 通知视图 **]**	配置新的简单网络管理协议（SNMP）组，或配置将 SNMP 用户映射到 SNMP 视图的表。
show snmp groups [组名]	显示组配置

以下是 CLI 命令的示例：

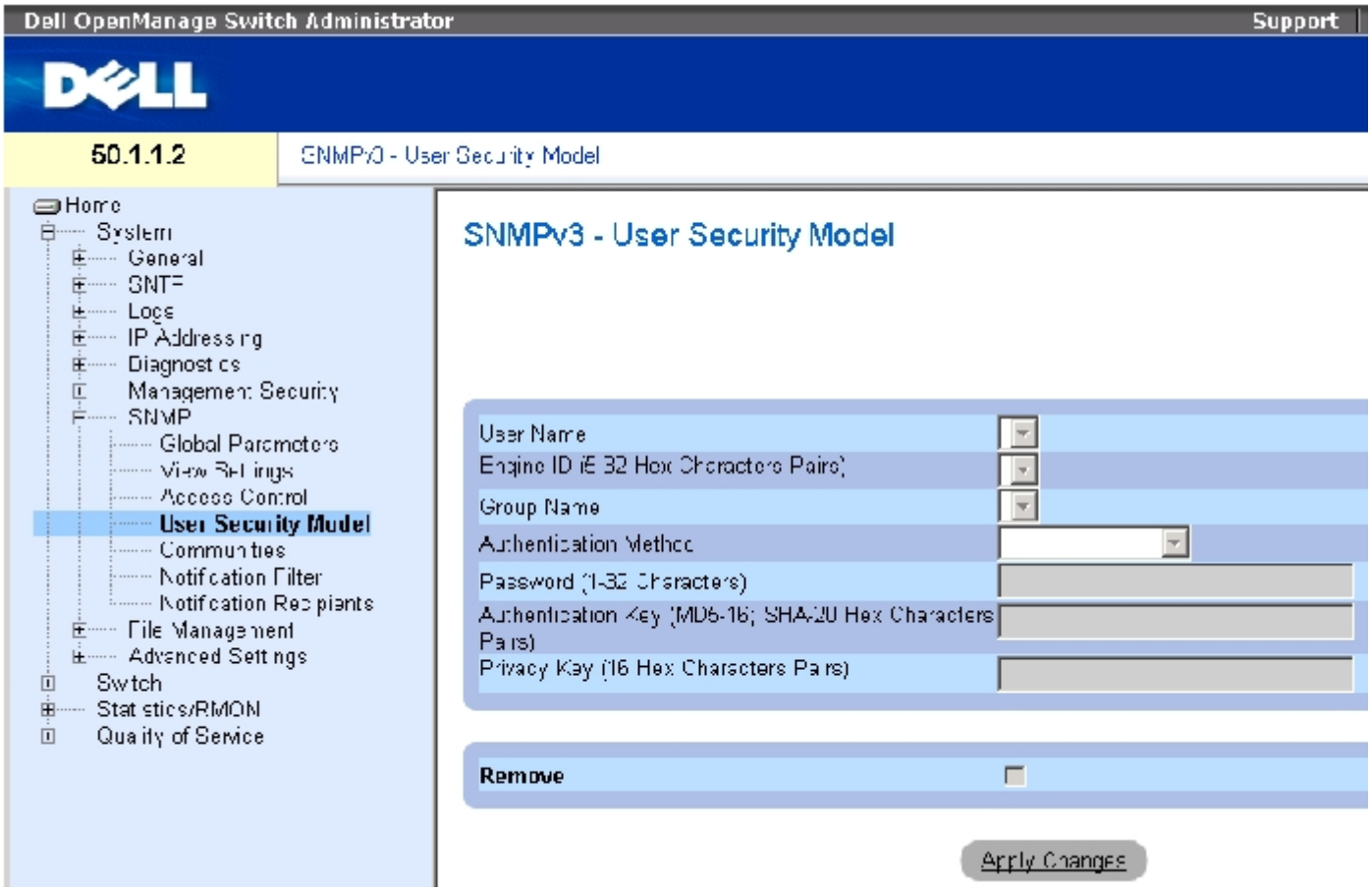
```
console (config)# snmp-
server group user-group
v3 priv read user- view
```

设定 SNMP 用户安全保护

“SNMPv3 User Security Model (USM)”（SNMPv3 用户安全保护模型 [USM]）页面可用于将系统用户分配到 SNMP 组，以及定义用户验证方法。

要打开“SNMPv3 User Security Model (USM)”（SNMPv3 用户安全保护模型 [USM]）页面，请在树视图中单击“System”（系统）→“SNMP”→“User Security Model”（用户安全保护模型）。

图 6-64. SNMPv3 用户安全保护模型 (USM)



“SNMPv3 User Security Model (USM)” （SNMPv3 用户安全保护模型 [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。此字段范围最多为 30 个字母数字字符。

“Engine ID” （引擎 ID） — 表示用户是连接到本地 SNMP 实体，还是连接到远程 SNMP 实体。更改或删除本地 SNMP 引擎 ID 将删除 SNMPv3 用户数据库。

“Local” （本地） — 表示用户连接到本地 SNMP 实体。

“Remote” （远程） — 表示用户连接到远程 SNMP 实体。如果定义了引擎 ID，远程设备将接收通知信息。

“Group Name” （组名） — 包含用户定义的 SNMP 组列表。SNMP 组是在“Access Control Group” （访问控制组）页面中定义的。

“Authentication Method” （验证方法） — 用于验证用户的验证方法。可能的字段值包括：

“MD5 Key” （MD5 密钥） — 使用 HMAC-MD5 算法验证用户。

“SHA Key” （SHA 密钥） — 使用 HMAC-SHA-96 验证级别验证用户。

“MD5 Password” （MD5 密码） — 表示使用 HMAC-MD5-96 密码进行验证。用户必须输入密码。

“SHA Password”（SHA 密码）— 使用 HMAC-SHA-96 验证级别验证用户。用户必须输入密码。

“None”（无）— 不使用用户验证。

“Password (0-32 Characters)”（密码 [0 至 32 个字符]）— 修改组的用户定义的密码。密码最多可以包含 32 个字母数字字符。

“Authentication Key (MD5-16; SHA-20 hexa chars)”（验证密钥 [MD5 - 16 个十六进制字符；SHA - 20 个十六进制字符]）— 定义 HMAC-MD5-96 或 HMAC-SHA-96 验证级别。通过输入验证密钥和保密密钥来定义验证密钥。如果只需要验证，则为 MD5 定义 16 字节。如果同时需要保密和验证，则为 MD5 定义 32 字节。十六进制字符串的每个字节是两个十六进制数字。每个字节可由句点或冒号进行分隔。

“Privacy Key (16 hexa characters)”（保密密钥 [16 个十六进制字符]）— 如果只需要验证，则定义 20 字节。如果同时需要保密和验证，则定义 16 字节。十六进制字符串的每个字节是两个十六进制数字。每个字节可由句点或冒号隔开。

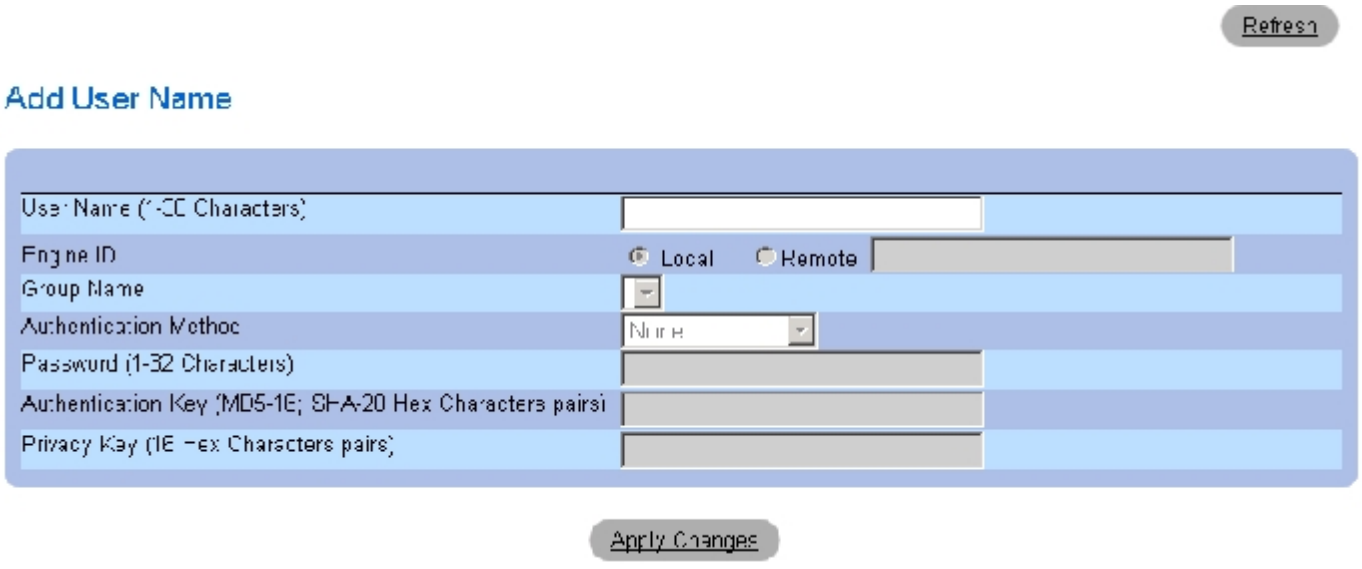
“Remove”（删除）— 如果选取此字段，将从指定组中删除用户。

向组中添加用户

1. 打开“SNMPv3 User Security Model (USM)”（SNMPv3 用户安全保护模型 [USM]）页面。
2. 单击“Add”（添加）。

系统将打开“Add SNMPv3 User Name”（添加 SNMPv3 用户名）页面：

图 6-65. 添加 SNMPv3 用户名



3. 定义相关的字段。

4. 单击“Apply Changes”（应用更改）。

系统会将用户添加到组中，并更新设备。

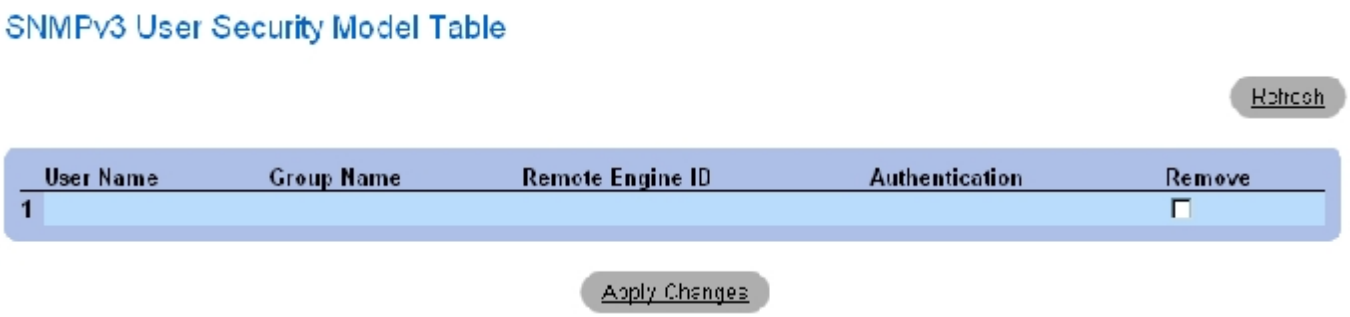
显示用户安全保护模型表

1. 打开“SNMPv3 User Security Model (USM)”（SNMPv3 用户安全保护模型 [USM]）页面。

2. 单击“Show All”（全部显示）。

系统将打开“User Security Model Table”（用户安全保护模型表）：

图 6-66. 用户安全保护模型表



删除用户安全保护模型表条目

1. 打开“SNMPv3 User Security Model (USM)”（SNMPv3 用户安全保护模型 [USM]）页面。

2. 单击“Show All”（全部显示）。

系统将打开“User Security Model Table”（用户安全保护模型表）。

3. 选择一个“User Security Model Table”（用户安全保护模型表）条目。

4. 选取“Remove”（删除）复选框。

5. 单击“Apply Changes”（应用更改）。

系统将删除“User Security Model Table”（用户安全保护模型表）条目，并更新设备。

使用 CLI 命令定义 SNMPv3 用户

下表概括了用于定义“SNMPv3 User Security Model (USM)”（SNMPv3 用户安全保护模型 [USM]）页面中显示的字段的等效 CLI 命令。

表 6-51. SNMPv3 用户的 CLI 命令

CLI 命令	说明
snmp-server user 用户名 组名 [**remote** 引擎 ID 字符串][**auth-md5** 密码 **| auth-sha password | auth-md5-key md5 des** 密钥 **| auth- sha-key sha des** 密钥]	配置新的 SNMP V3 用户。
show snmp users [用户名]	显示用户配置。

以下是 CLI 命令的示例：

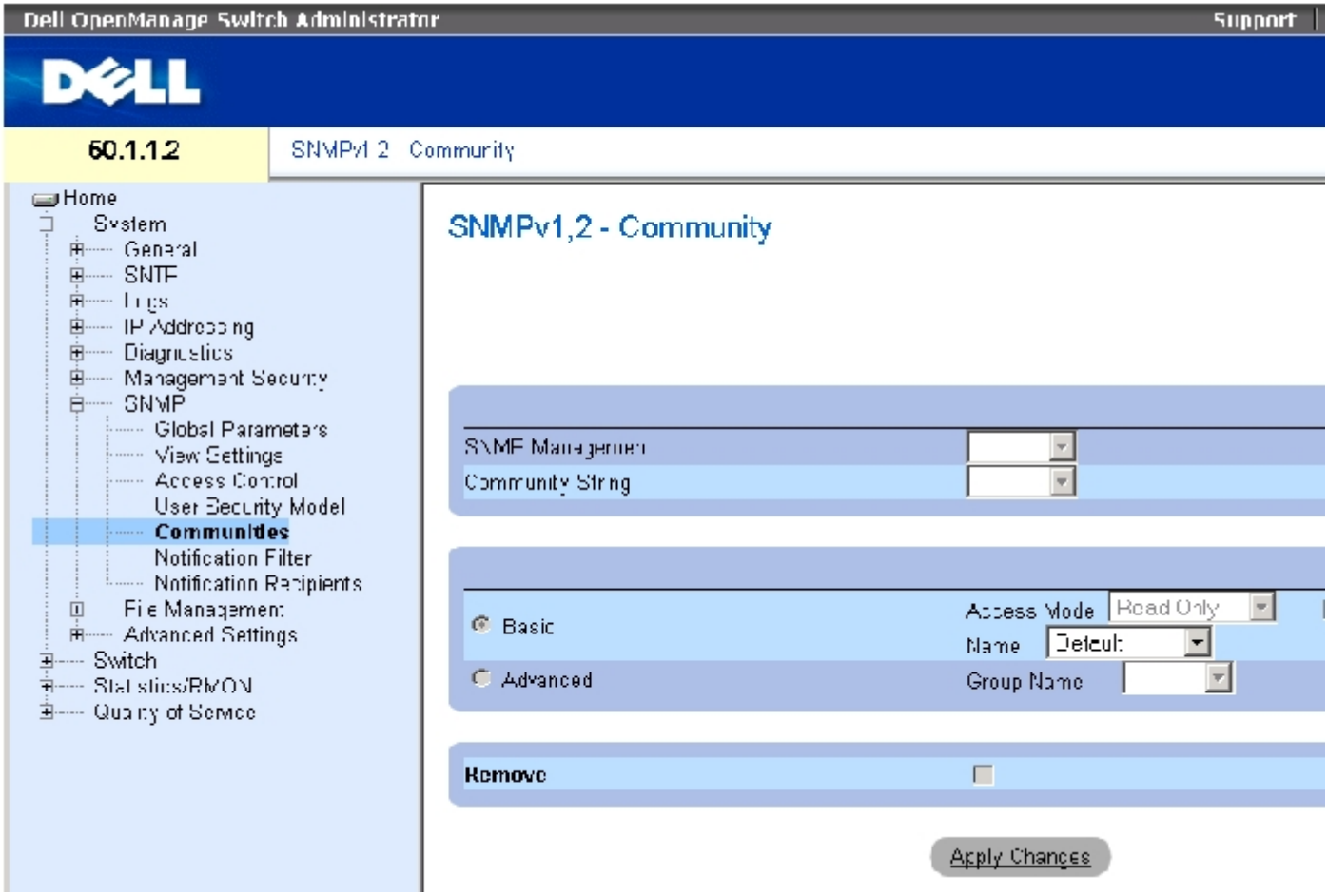
```
console (config)# snmp-server user John user-group auth-md5 1234

console(config)# end

console# show snmp users
```

Name	Group Name	Auth Method	Remote
----------	----------	----------	----------
John	user-group	md5	

定义 SNMP 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 团体只是为 SNMP v1 和 SNMP v2 定义的。要打开“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 6-67. SNMPv1,2 团体



“SNMPv1,2 Community” (SNMPv1,2 团体) 页面包含以下字段：

“SNMP Management Station” (SNMP 管理站点) — 为其定义 SNMP 团体的管理站点 IP 地址。

“Community String” (团体字符串) — 相当于密码，用于验证连接至设备的管理站点。

“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) 管理访问被限制为只读，不能对团体进行更改。

“Read Write” (读写) 管理访问为读写模式，可以对设备配置进行更改，但不能对团体进行更改。

“SNMP-Admin” (SNMP 管理) 用户具有访问所有设备配置选项以及修改团体的权限。

“View Name” (视图名称) — 包含用户定义的 SNMP 视图列表。

“Name”（名称）— 指定用于 SNMPv1、v2 的团体名称。

“Advanced”（高级）— 包含用户定义的组列表。选定 SNMP 高级模式后，将为选定团体启用组成组的 SNMP 访问控制规则。高级模式还将为特定 SNMP 团体启用 SNMP 组。SNMP 高级模式只能与 SNMPv3 结合定义。可能的字段值为：

“Group Name”（组名）— 指定在 SNMP 高级模式下运行时组的名称。

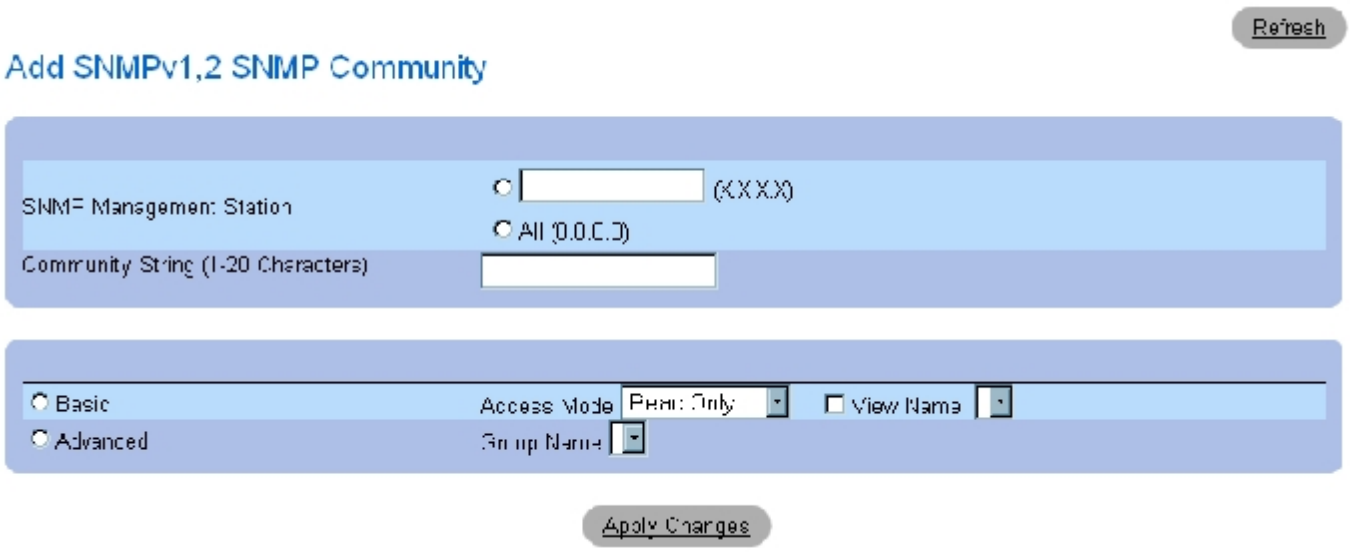
“Remove”（删除）— 如果选取此字段，将删除团体。

定义新团体

1. 打开“SNMPv1,2 Community”（SNMPv1,2 团体）页面。
2. 单击“Add”（添加）。

系统将打开“Add SNMP Community”（添加 SNMP 团体）页面：

图 6-68. 添加 SNMP 团体



3. 完成相关的字段。
4. 单击“Apply Changes”（应用更改）。

系统将保存新团体，并更新设备。

删除团体

1. 打开“SNMPv1,2 Community” (SNMPv1,2 团体) 页面。
2. 单击“Show All” (全部显示) 。

   系统将打开“Community Table” (团体表) 页面。
3. 选择一个团体并选取“Remove” (删除) 复选框。
4. 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

下表概括了用于查看“SNMPv1,2 Community” (SNMPv1,2 团体) 中显示的字段的等效 CLI 命令。

表 6-52. SNMP 团体的 CLI 命令

CLI 命令	说明
snmp-server community 团体 **[ro | rw | su] [IP** 地址**][view** 视图名称**]**	设置团体访问字符串以允许对 SNMP 协议进行访问。
snmp-server community-group 团体组名 **[IP** 地址**]**	设置团体访问字符串以允许基于组访问权限对 SNMP 协议进行限制性访问。
show snmp	显示当前的 SNMP 设备配置。

以下是 CLI 命令的示例：

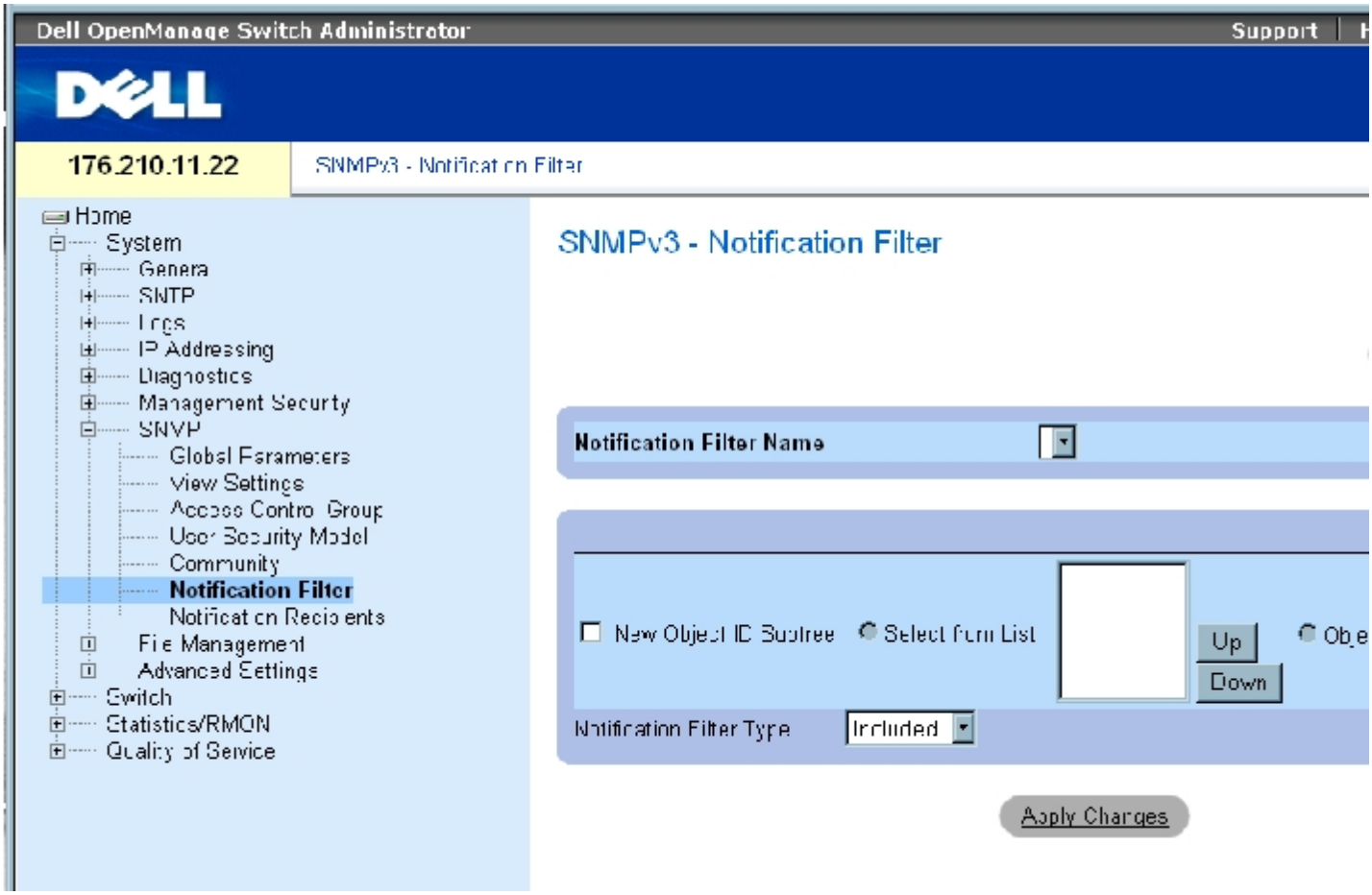
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

定义 SNMP 通知过滤器

“Notification Filter”（通知过滤器）页面允许根据 OID 过滤陷阱。每个 OID 都链接到一个设备功能或功能相关内容。网络管理员还可以使用“Notification Filter”（通知过滤器）页面来过滤通知。

要打开“Notification Filter”（通知过滤器）页面，请在树视图中单击“System”（系统）→“SNMP”→“Notification Filters”（通知过滤器）。

图 6-69. 通知过滤器



“Notification Filter”（通知过滤器）页面包含以下字段：

“Notification Filter Name”（通知过滤器名称）— 用户定义的通知过滤器。

“New Object Identifier Tree”（新对象标识符树）— 已为其发送或阻塞了通知的 OID。如果过滤器已连接到 OID，则将生成陷阱或通知，并发送给陷阱接收设备。对象 ID 是从“Select from List”（从列表中选择）或“Object ID List”（对象 ID 列表）中选择的。

“Notification Filter Type”（通知过滤器类型）— 表示是否将关于 OID 的通知或陷阱发送给陷阱接收设备。

“Excluded”（排除）— 限制发送 OID 陷阱或通知。

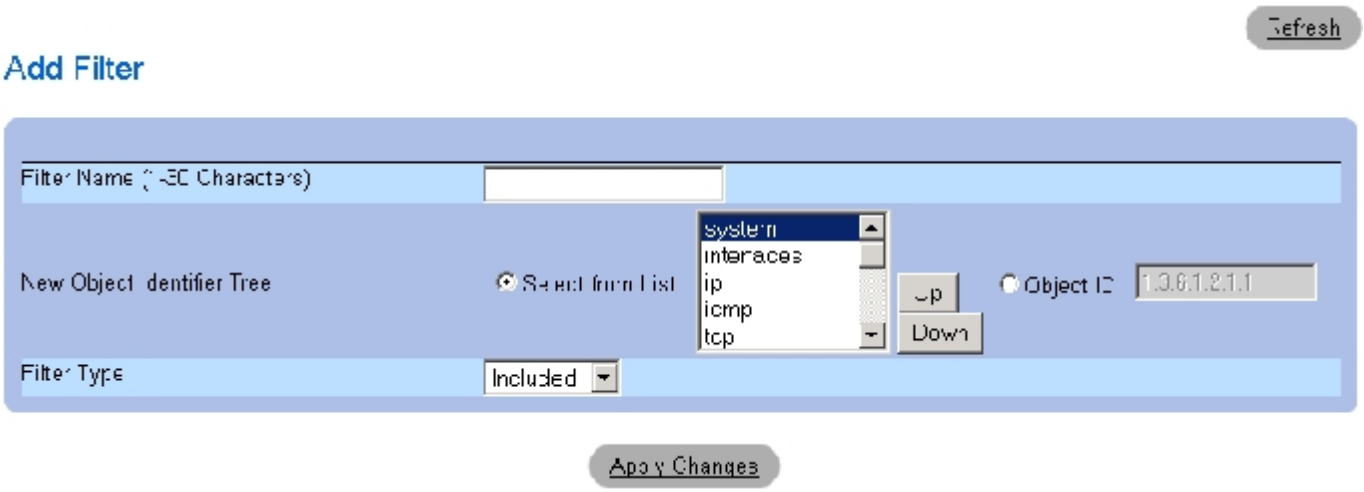
“Included”（包括）— 发送 OID 陷阱或通知。

添加 SNMP 过滤器

1. 打开“Notification Filter”（通知过滤器）页面。
2. 单击“Add”（添加）。

   系统将打开“Add Filter”（添加过滤器）页面：

图 6-70. 添加过滤器



3. 定义相关的字段。
4. 单击“Apply Changes”（应用更改）。

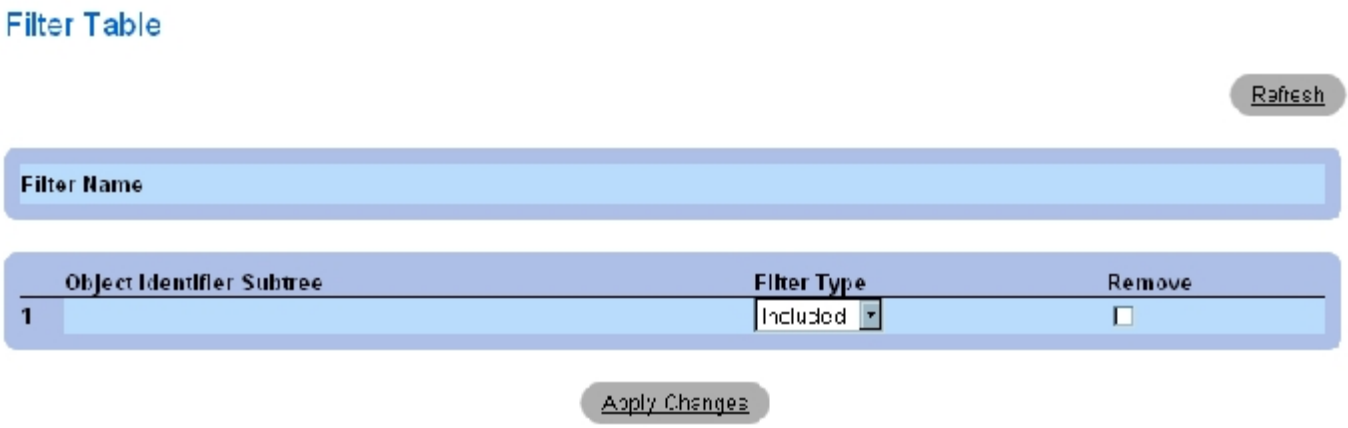
   系统将添加新过滤器，并更新设备。

显示过滤器表

1. 打开“Notification Filter”（通知过滤器）页面。
2. 单击“Show All”（全部显示）。

   系统将打开“Filter Table”（过滤器表）：

图 6-71. 过滤器表



删除过滤器

1. 打开“Notification Filter”（通知过滤器）页面。
2. 单击“Show All”（全部显示）。

   系统将打开“Filter Table”（过滤器表）。
3. 选择一个“Filter Table”（过滤器表）条目。
4. 选取“Remove”（删除）复选框。

   系统将删除过滤器条目，并更新设备。

使用 CLI 命令配置通知过滤器

下表概括了用于定义“Notification Filter”（通知过滤器）页面中显示的字段的等效 CLI 命令。

表 6-53. SNMP 通知过滤器的 CLI 命令

CLI 命令	说明
snmp-server filter 过滤器名称 OID 树 **{included | excluded}**	创建或更新 SNMP 通知过滤器。
show snmp filters[过滤器名称]	显示 SNMP 通知过滤器配置

以下是 CLI 命令的示例：

```
Console (config)# snmp-server filter user1 iso included
Console(config)# end
Console # show snmp filters

Name        OID Tree        Type
----------  --------------  --------
user1       iso             Included
```

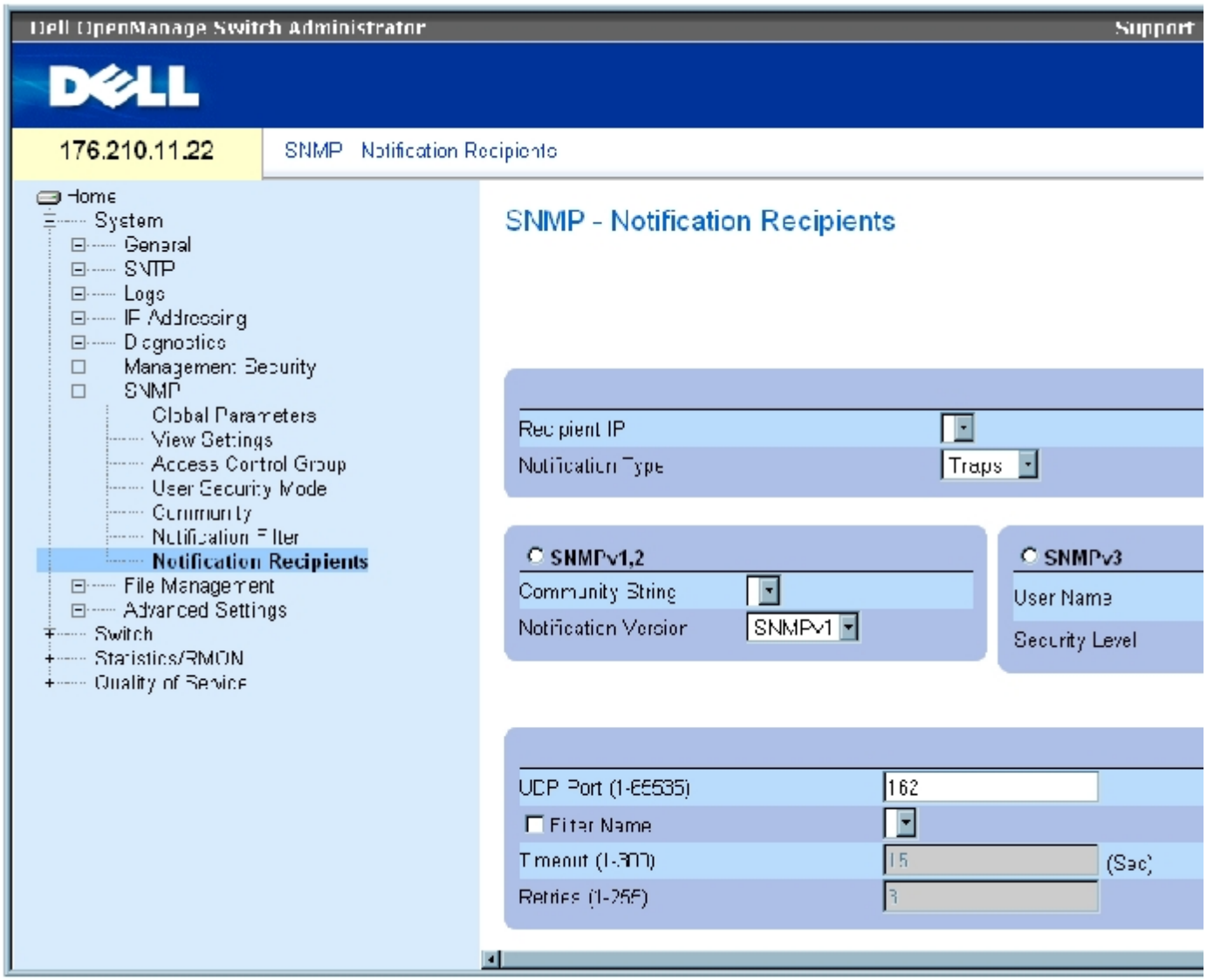
定义 SNMP 通知接收设备

“Notification Recipients”（通知接收设备）页面包含用于定义过滤器的信息，这些过滤器可以确定是否将陷阱发送给特定用户以及发送的陷阱类型。SNMP 通知过滤器提供以下服务：

- 标识管理陷阱目标
- 陷阱过滤
- 选择陷阱生成参数
- 提供访问控制检查

要打开“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 6-72. 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）— 表示陷阱发送到的 IP 地址。

“Notification Type”（通知类型）— 发送的通知。可能的字段值包括：

“Trap”（陷阱）— 发送陷阱。

“Inform”（通知）— 发送通知。

“SNMPv1,2”— 为选定的接收设备启用 SNMP 版本 1 和版本 2。为 SNMPv1 和 SNMPv2 定义以下字段：

“Community String (1-20 Characters)”（团体字符串 [1 至 20 个字符]）— 标识陷阱管理员的团体字符串。

“Notification Version”（通知版本）— 确定陷阱类型。可能的字段值包括：

“SNMP V1” — 发送 SNMP 版本 1 陷阱。

“SNMP V2” — 发送 SNMP 版本 2 陷阱。

“SNMPv3” — 使用 SNMPv3 发送和接收陷阱。为 SNMPv3 定义以下字段：

“User Name” （用户名） — 接收 SNMP 通知的用户。

“Security Level” （安全保护级别） — 定义验证信息包的方法。可能的字段值包括：

“No Authentication” （无验证） — 不验证也不加密信息包。

“Authentication” （验证） — 验证信息包。

“Privacy” （保密） — 验证并加密信息包。

“UDP Port (1-65535)” （UDP 端口 [1 至 65535]） — 用于发送通知的 UDP 端口。默认值为 162。

“Filter Name” （过滤器名称） — 包括或排除 SNMP 过滤器。

“Timeout (1-300)” （超时 [1 至 300]） — 设备在重新发送通知之前等待的时间（以秒为单位）。默认值为 15 秒。

“Retries (1-255)” （重试次数 [1 至 255]） — 设备重新发送通知请求的次数。默认值为 3。

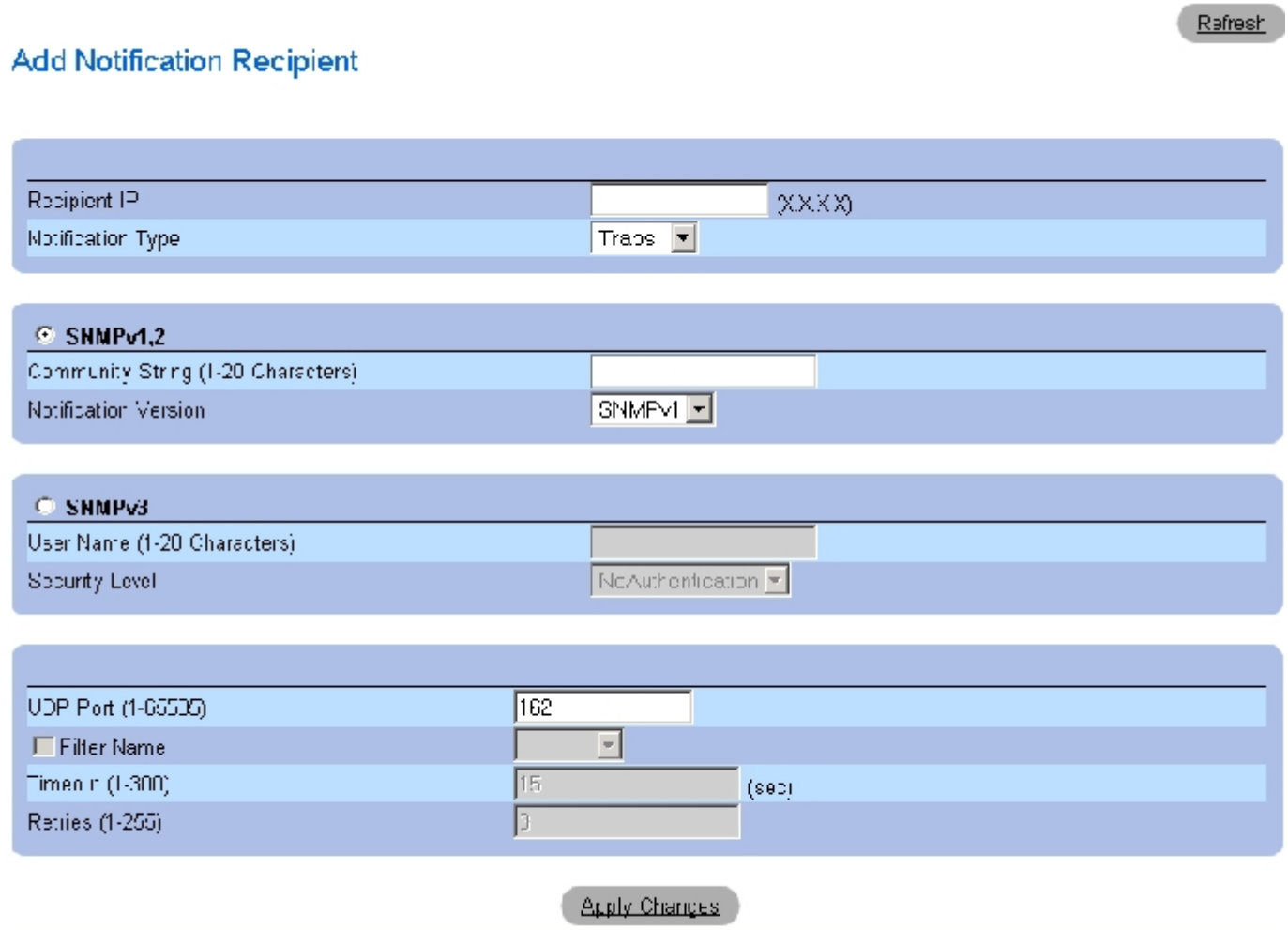
“Remove Notification Recipient” （删除通知接收设备） — 如果选取此字段，将删除选定的通知接收设备。

添加新的陷阱接收设备

1. 打开“Notification Recipients” （通知接收设备）页面。
2. 单击“Add” （添加）。

系统将打开“Add Notification Recipients” （添加通知接收设备）页面：

图 6-73. 添加通知接收设备



3. 定义相关的字段。

4. 单击“Apply Changes”（应用更改）。

系统将添加通知接收设备，并更新设备。

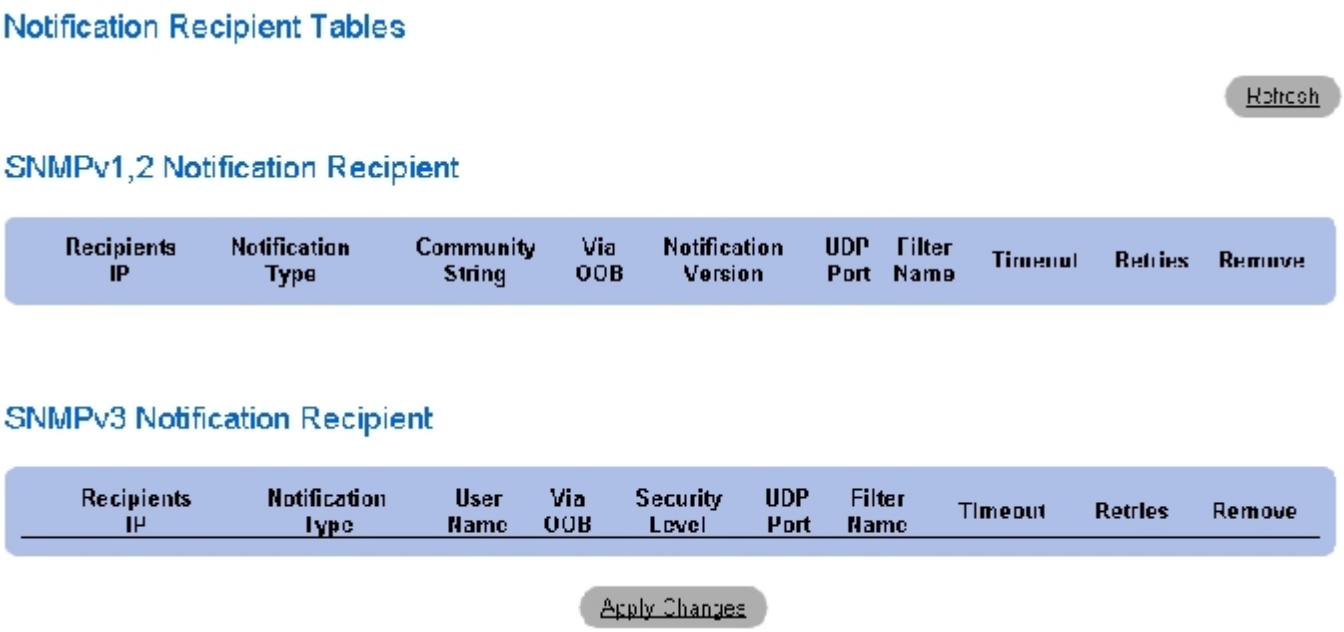
显示“Notification Recipients Tables”（通知接收设备表）

1. 打开“Notification Recipients”（通知接收设备）页面。

2. 单击“Show All”（全部显示）。

系统将打开“Notification Recipients Tables”（通知接收设备表）页面：

图 6-74. 通知接收设备表



删除通知接收设备

1. 打开“Notification Recipients”（通知接收设备）页面。
2. 单击“Show All”（全部显示）。

   系统将打开“Notification Recipients Tables”（通知接收设备表）页面。
3. 在“SNMPV1,2 Notification Recipient”（SNMPV1,2 通知接收设备）或“SNMPv3 Notification Recipient”（SNMPv3 通知接收设备）表中选择一个通知接收设备。
4. 选取“Remove”（删除）复选框。
5. 单击“Apply Changes”（应用更改）。

   系统将删除此接收设备，并更新设备。

使用 CLI 命令配置 SNMP 通知接收设备

下表概括了用于查看“Notification Recipients”（通知接收设备）页面中显示的字段的等效 CLI 命令。

表 6-54. SNMP 团体的 CLI 命令

CLI 命令	说明
snmp-server host {IP 地址	主机名称} 团体字符串 [**traps**	**informs**] [**1**	**2**] [**udp-port** 端口] [**filter** 过滤器名称] [**timeout** 秒数] [**retries** 重试次数]	创建或更新 SNMP 版本 1 或 2 中接收通知的通知接收设备。
snmp-server v3-host {IP 地址	主机名称} 用户名 [**traps**	**informs**] {**noauth**	**auth**	**priv**} [**udp-port** 端口] [**filter** 过滤器名称] [**timeout** 秒数] [**retries** 重试次数]	创建或更新 SNMP 版本 3 中接收通知的通知接收设备。
show snmp	显示当前的 SNMP 配置

以下是 CLI 命令的示例：

```
console(config)# snmp-server host 172.16.1.1 private

console(config)# end

console# show snmp
```

Community-String	Community-Access	View name	IP address
public	read only	user-view	All
private	read write	default	172.16.1.1
private	su	DefaultSuper	172.17.1.1

管理文件

使用“File Management”（文件管理）页面可以管理设备软件、映像文件和配置文件。文件可从 TFTP 服务器下载或加载。

管理文件概览

管理文件由以下文件构成：

- 启动配置文件 — 包含在启动时或重新引导后配置设备所需的命令。启动配置文件是通过将配置命令从运行配置文件或备份配置文件复制到启动配置文件来创建的。

- 运行配置文件 — 包含所有启动配置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，所有存储在运行配置文件中

的命令均会丢失。启动期间，启动配置文件中的所有命令将被复制到运行配置文件中，并应用于设备。会话期间，所有新命令将被添加到运行配置文件中存在的命令中。要更新启动配置文件，必须先将运行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。

- 备份配置文件 — 包含设备配置的备份副本。使用用户配置的名称最多能在设备上保存五个备份配置文件。当用户将运行配置文件或启动配置文件复制到用户命名的文件中时，将生成这些文件。可以将备份配置文件的内容复制到运行配置文件或启动配置文件中。

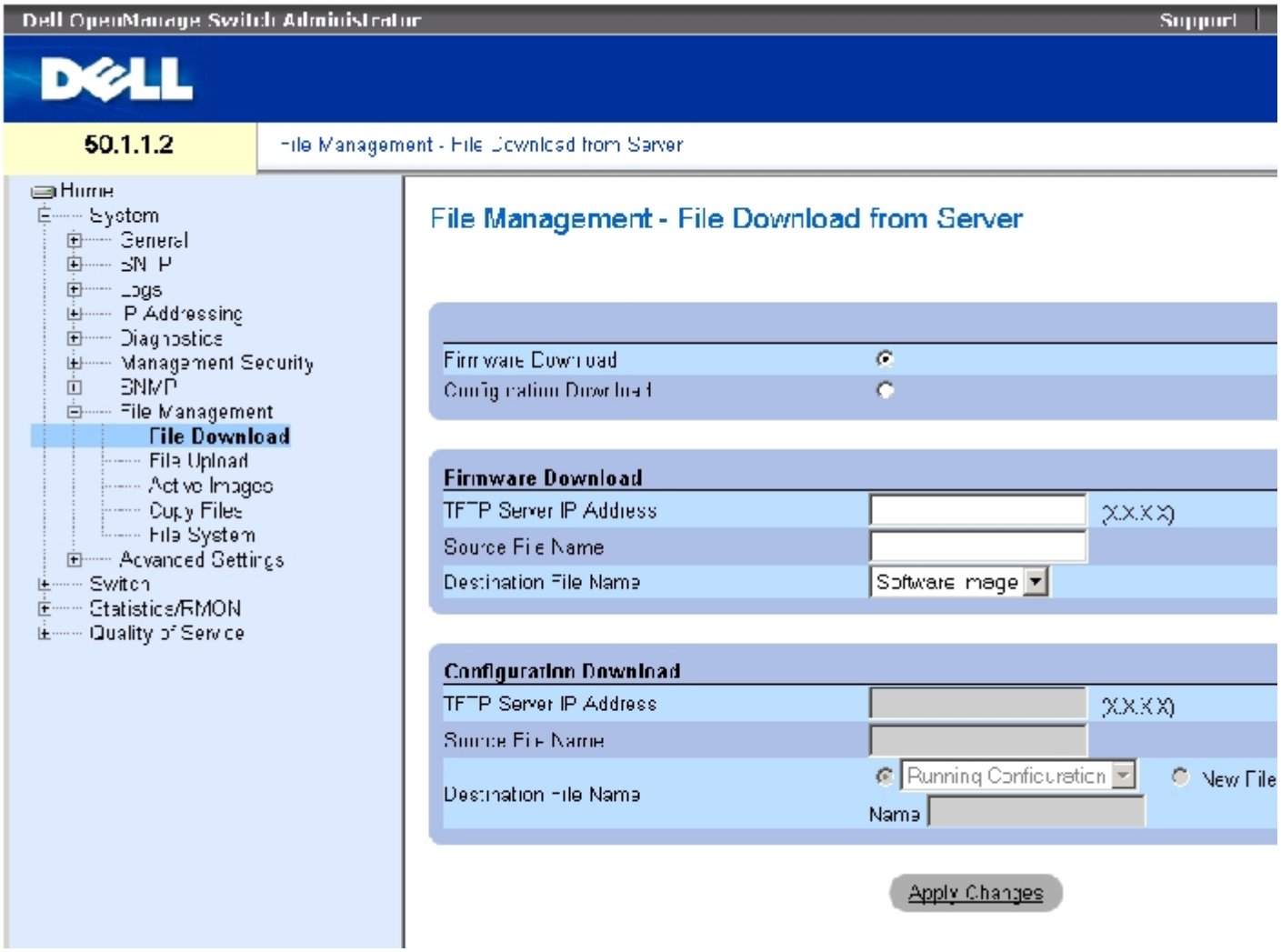
- 映像文件 — 系统文件映像保存在两个快擦写文件（称为映像 1 和映像 2）中。活动映像存储活动副本，另一个映像存储第二个副本。设备从活动映像进行引导并运行。如果活动映像被损坏，系统将自动从非活动映像进行引导。这种安全功能可用于防止软件升级过程中出现故障。

要打开“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）。

下载文件

“File Download from Server”（从服务器下载文件）页面包含用于将系统映像文件和配置文件从 TFTP 服务器下载到设备的字段。要打开“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 6-75. 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) — 下载固件文件。如果选择了"Firmware Download" (固件下载)，"Configuration Download" (配置下载)字段将呈灰色。

"Configuration Download" (配置下载) — 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。

"Firmware Download" (固件下载)

"TFTP Server IP Address" (TFTP 服务器 IP 地址) — 下载固件文件所在的 TFTP 服务器 IP 地址。

"Source File Name" (源文件名) — 表示要下载的文件。

"Destination File Name" (目标文件名) — 存放下载文件的目标文件的类型。可能的字段值包括：

"Software Image" (软件映像) — 下载映像文件。

“Boot Code”（引导代码）— 下载引导文件。

“Configuration Download”（配置下载）

“TFTP Server IP Address”（TFTP 服务器 IP 地址）— 下载配置文件所在的 TFTP 服务器 IP 地址。

“Source File Name”（源文件名）— 表示要下载的配置文件。

“Destination File Name”（目标文件名）— 存放下载配置文件的目标文件。可能的字段值包括：

“Running Configuration”（运行配置）— 将命令下载到运行配置文件中。

“Startup Configuration”（启动配置）— 下载启动配置文件并将其覆盖。

“User Defined Backup Configuration”（用户定义的备份配置）— 下载用户定义的备份配置文件，并将其覆盖。

“New File Name”（新文件名）— 下载可以指定为目标文件的新备份配置文件。

注：映像文件将覆盖非活动映像。建议指定在重启动后非活动映像将变为活动映像，然后在下载后重启动设备。

在下载映像文件的过程中，系统将打开一个对话框显示下载进度。下载完成后窗口将自动关闭。

下载文件

1. 打开“File Download from Server”（从服务器下载文件）页面。
2. 定义要下载的文件类型。
3. 定义字段。
4. 单击“Apply Changes”（应用更改）。

软件将被下载到设备。

注：要激活选定的映像文件，请重启动设备。有关重启动设备的信息，请参阅“在堆栈主装置之间切换”。

使用 CLI 命令下载文件

下表概括了用于设置“File Download from Server”（从服务器下载文件）页面中显示的字段的等效 CLI 命令。

表 6-55. 文件下载的 CLI 命令

CLI 命令	说明
copy 源 URL 目的地 URL	将文件从源复制到目的地。

以下是 CLI 命令的示例：

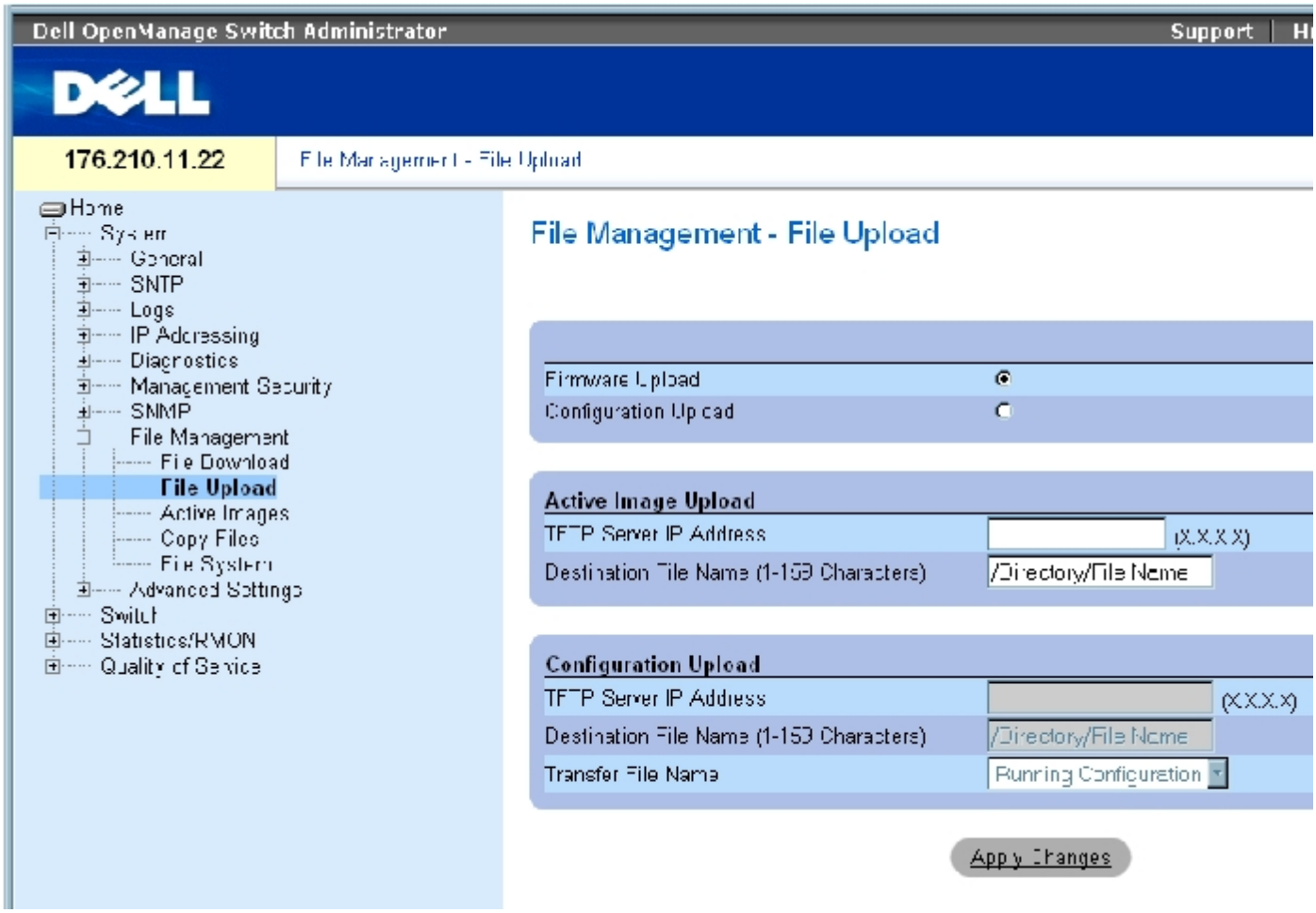
```
console# copy
tftp://10.6.6.64/pp.txt
startup-config


....!


Copy:575 bytes copied in
00:00:06 [hh:mm:ss]


01-Jan-2000 06:41:55
%COPY-W-TRAP:The copy
operation was completed
successfully
```

注：每个感叹号（!）表示已成功传输十个信息包。

加载文件

“File Upload to Server”（将文件加载至服务器）页面包含用于将软件从设备加载到 TFTP 服务器的字段。通过“File Upload to Server”（将文件加载至服务器）页面也可以加载映像文件。要打开“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 6-76. 将文件加载至服务器



“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）— 加载固件文件。如果选择了“Firmware Upload”（固件加载），“Configuration Upload”（配置加载）字段将不可用。

“Configuration Upload”（配置加载）— 加载配置文件。如果选择了“Configuration Upload”（配置加载），“Active Image Upload”（活动映像加载）字段将不可用。

“Active Image Upload”（活动映像加载）

“TFTP Server IP Address”（TFTP 服务器 IP 地址）— 软件映像要加载到的 TFTP 服务器 IP 地址。

“Destination File Name (1-159 Characters)”（目标文件名 [1 至 159 个字符]）— 表示文件要加载到的软件映像文件路径。

“Configuration Upload”（配置加载）

“TFTP Server IP Address”（TFTP 服务器 IP 地址）— 配置文件要加载到的 TFTP 服务器 IP 地址。

“Destination File Name (1-159 Characters)”（目标文件名 [1 至 159 个字符]）— 表示文件要加载到的配置文件路径。

“Transfer File Name”（传输文件名）— 配置要加载到的软件文件。可能的字段值包括：

“Running Configuration”（运行配置）— 加载运行配置文件。

“Startup Configuration”（启动配置）— 加载启动配置文件。

“List of User Defined Configuration Files”（用户定义的配置文件列表）— 加载用户定义的配置文件。

注：仅当用户创建了备份配置文件后，才会显示这一用户定义的配置文件列表。例如，如果用户将运行配置文件复制到名为 BACKUP-SITE-1 的用户定义的配置文件中，则此列表将显示在“File Upload to Server”（将文件加载至服务器）页面，并且 BACKUP-SITE-1 配置文件将显示在列表中。

加载文件

1. 打开“File Upload to Server”（将文件加载至服务器）页面。
2. 定义要加载的文件类型。
3. 定义字段。
4. 单击“Apply Changes”（应用更改）。

软件将被加载到 TFTP 服务器。

使用 CLI 命令加载文件

下表概括了用于设置“File Upload to Server”（将文件加载至服务器）页面中显示的字段的等效 CLI 命令。

表 6-56. 文件加载 CLI 命令

CLI 命令	说明
copy 源 URL 目的地 URL	将文件从源复制到目的地。

以下是 CLI 命令的示例：

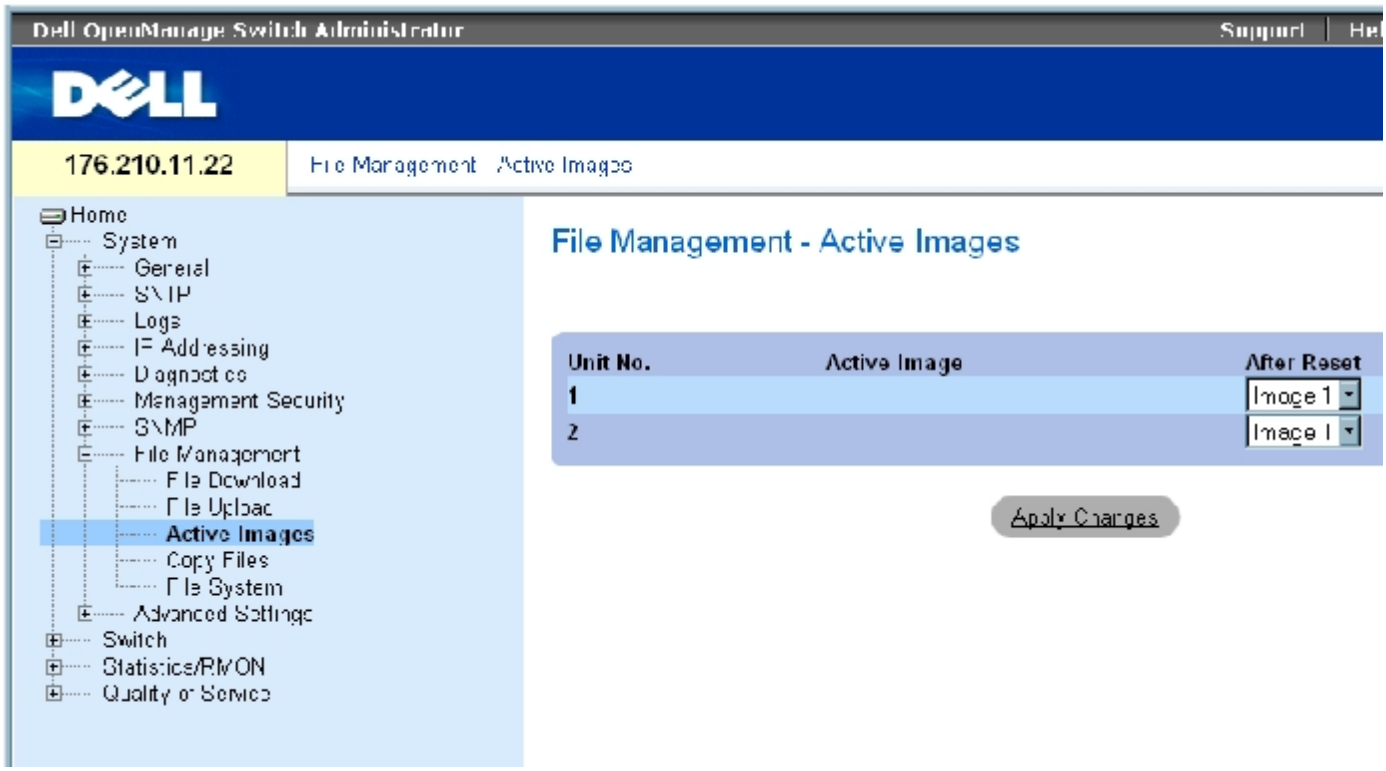
```
console# copy image tftp://10.6.6.64/uploaded.ros
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy:4234656 bytes copied in 00:00:33 [hh:mm:ss]

01-Jan-2000 07:30:42 %COPY-W-TRAP:The copy operation was
completed successfully
```

激活映像文件

“Active Images”（活动映像）页面使网络管理员可以选择和重设映像文件。可以分别为堆叠配置中的各个装置选择活动映像文件。要打开“Active Images”（活动映像）页面，请在树视图中单击“System”（系统）→“File Management”（文件管理）→“Active Images”（活动映像）。

图 6-77. 活动映像



“Active Images”（活动映像）页面包含以下字段：

“Unit No.”（装置号）— 为其选定了映像文件的装置号。

“Active Image”（活动映像）— 装置上当前处于活动状态的映像文件。

“After Reset”（重启动后）— 设备重启动后装置上处于活动状态的映像文件。可能的字段值包括：

“Image 1”（映像 1）— 设备重启动后激活映像文件 1。

“Image 2”（映像 2）— 设备重启动后激活映像文件 2。

选择映像文件

1. 打开“Active Images”（活动映像）页面。
2. 在“After Reset”（重启动后）字段中为某一特定装置选择映像文件。
3. 单击“Apply Changes”（应用更改）。

系统将选定映像文件。仅在下一次重启动后才重新加载映像文件。当前选定的映像文件将继续运行，直至下一次设备重启动。

使用 CLI 命令处理活动映像文件

下表概括了用于查看“Active Images”（活动映像）中显示的字段的等效 CLI 命令。

表 6-57. 文件加载 CLI 命令

CLI 命令	说明
boot system [unit | 装置] {image-1 | image-2}	表示设备启动时加载的系统映像。
show version [unit 装置]	显示系统版本信息

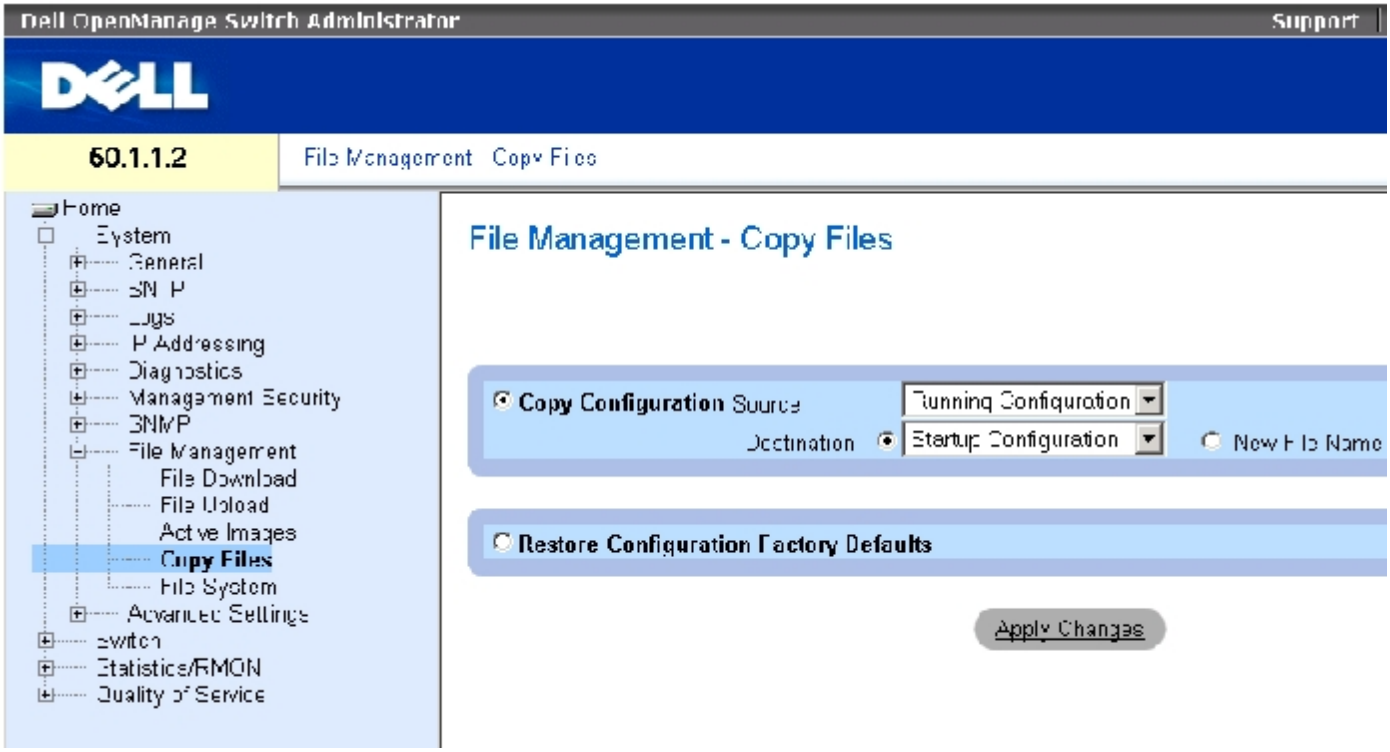
以下是 CLI 命令的示例：

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

复制文件

通过“Copy Files”（复制文件）页面可以复制和删除文件。要打开“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 Files”（复制文件）。

图 6-78. 复制文件



“Copy Files”（复制文件）页面包含以下字段：

“Copy Configuration”（复制配置）— 如果选择此字段，将把主文件的运行配置文件、启动配置文件或备份配置文件复制到目标文件中。

“Source”（源）— 表示要复制到目标文件的文件类型。请选择运行配置文件、启动配置文件或其中一个用户定义的备份配置文件。

“Destination”（目的地）— 表示要将源文件复制到的目标配置文件。不能将文件复制到备份主文件的备份文件中。仅当定义了备份文件后，“Destination Unit”（目标装置）字段中才会显示备份文件。选取“New File Name”（新文件名）复选框，表示要将源文件复制到的新备份配置文件的新文件名。

“New File Name”（新文件名）— 表示新创建的备份配置文件的名称。

“Restore Configuration Factory Defaults”（恢复出厂默认配置）— 如果选择此字段，则表示应将当前的配置设置更换为出厂默认配置设置。如果不选择此字段，则表示应保留当前配置设置。

复制文件

1. 打开“Copy Files”（复制文件）页面。
2. 定义“Source”（源）和“Destination”（目的地）字段。
3. 单击“Apply Changes”（应用更改）。

系统将复制文件，并更新设备。

恢复出厂默认设置

1. 打开“Copy Files”（复制文件）页面。
2. 单击“Restore Configuration Factory Defaults”（恢复出厂默认配置）。
3. 单击“Apply Changes”（应用更改）。

系统将恢复出厂默认设置，并更新设备。

使用 CLI 命令复制和删除文件

下表概括了用于设置“Copy Files”（复制文件）页面中显示的字段的等效 CLI 命令。

表 6-58. 复制文件的 CLI 命令

CLI 命令	说明
copy 源 URL 目的地 URL	将文件从源复制到目的地。
delete startup-config	删除启动配置文件。

以下是 CLI 命令的示例：

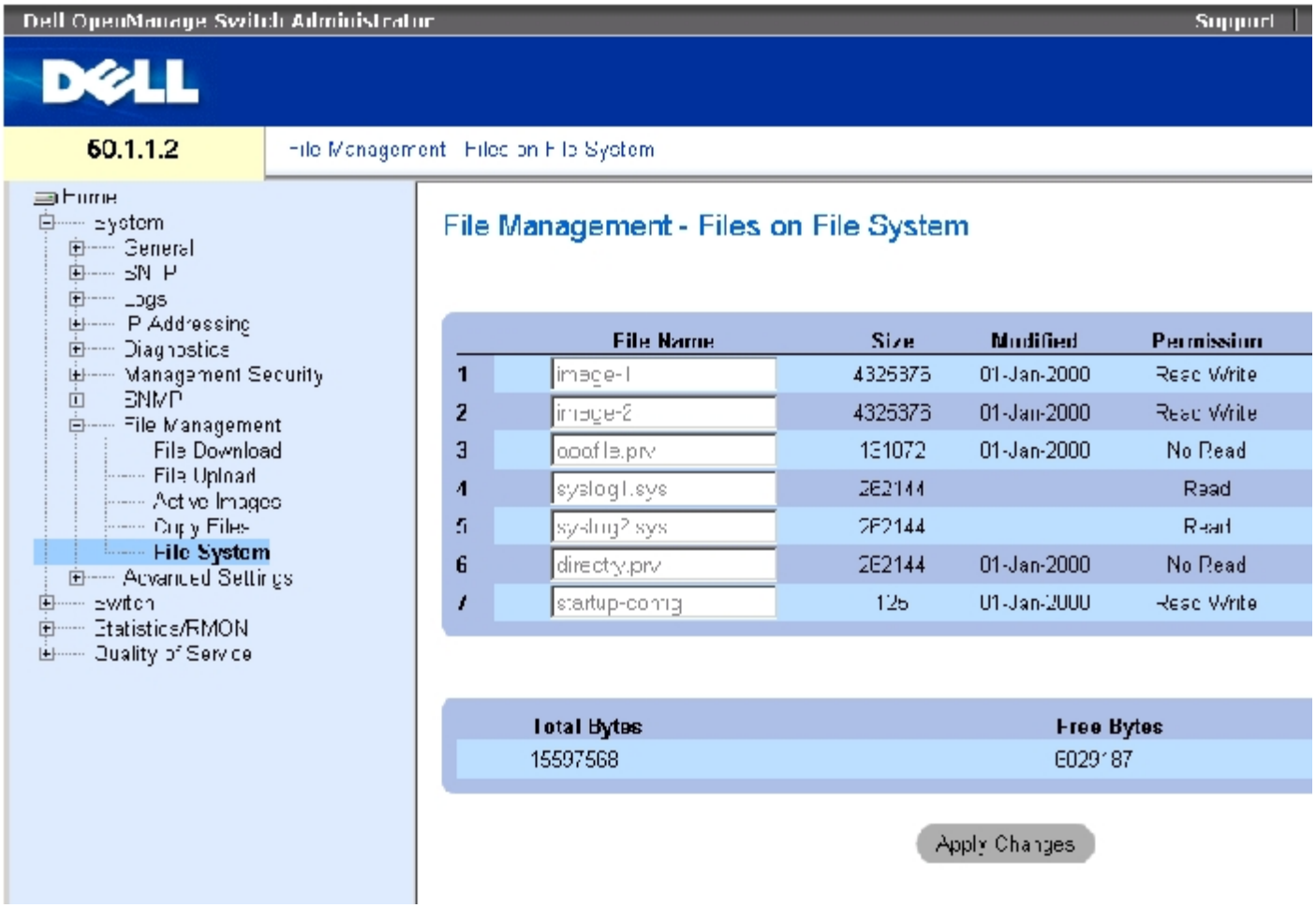
```
console# delete startup-
config

Startup file was deleted

console#

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

```
01-Jan-2000 06:55:32
%COPY-W-TRAP:The copy
operation was completed
successfully


Copy succeeded


console#
```

管理设备文件

“Files on File System”（文件系统上的文件）页面提供关于当前存储在系统上的文件的信息，包括文件名、文件大小、文件修改和文件权限。文件系统最多允许管理五个文件，总文件大小最多为 3 MB。要打开“Files on File System”（文件系统上的文件）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 6-79. 文件系统上的文件



“Files on File System”（文件系统上的文件）页面包含以下字段：

“File Name”（文件名）— 表示当前存储在文件管理系统中的文件。

“Size”（大小）— 表示文件大小。

“Modified”（修改时间）— 表示上次修改文件的日期。

“Permission”（权限）— 表示为文件设定的权限类型。可能的字段值包括：

“Read Only”（只读）— 表示只读文件。

“Read Write”（读写）— 表示读写文件。

“Remove”（删除）— 如果选取此字段，将删除文件。

“Rename”（重命名）— 允许重命名文件。在“File Name”（文件名）字段中重命名文件名。

“Total Bytes”（字节总数）— 表示当前使用的空间总量。

“Free Bytes”（可用字节）— 表示当前剩余的可用空间量。

使用 CLI 命令管理文件

下表概括了用于管理系统文件的等效 CLI 命令。

表 6-59. 复制文件的 CLI 命令

CLI 命令	说明
dir	显示快擦写文件系统上的文件列表

以下是 CLI 命令的示例：

```
console# dir

Directory of flash:

File Name    Permis-sion  Flash Size  Data Size  Modified
-----------  ------       ------      ------     ---------------
3.txt        rw           524288      523776     22-Feb-2005 18:49:27
```

setup	rw	524288	95	22-Feb-2005 15:58:19
setup2	rw	524288	95	22-Feb-2005 15:58:35
image-1	rw	4325376	4325376	06-Feb-2005 17:55:32
image-2	rw	4325376	4325376	06-Feb-2005 17:55:31
test.txt	rw	524288	95	22-Feb-2005 12:16:44
aaafile.prv	--	131072	--	06-Feb-2005 19:09:02
syslog1.sys	r-	262144	--	22-Feb-2005 18:49:27
syslog2.sys	r-	262144	--	22-Feb-2005 18:49:27
directory.prv	--	262144	--	06-Feb-2005 17:55:31
startup-config	rw	524288	347	22-Feb-2005 11:56:03
Total size of flash:16646144 bytes				
Free size of flash:4456448 bytes				

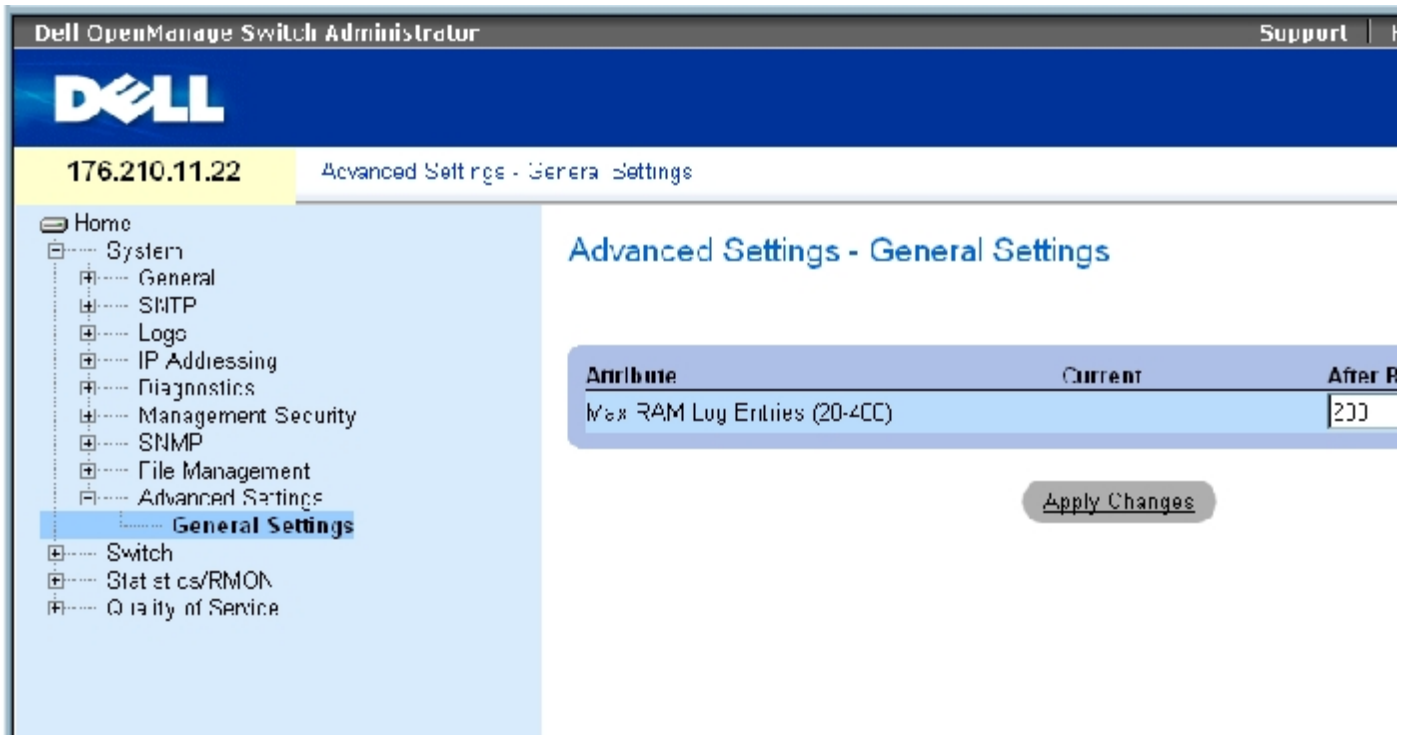
配置常规设置

使用“Advanced Settings”（高级设置）可以设置交换机的各种全局属性。只有在交换机重启动之后，才能应用对这些属性的更改。在树视图中单击“System”（系统）→“Advanced Settings”（高级设置）可以打开“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。

“General Settings”（常规设置）页面提供了用于定义常规设备参数的信息。要打开“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 6-80. 常规设置



"General Settings" (常规设置) 页面包含以下信息：

"Attribute" (属性) — 常规设置属性。

"Current" (当前) — 当前配置的值。

"After Reset" (重启动后) — 将来 (重启动后) 的值。通过在 "After Reset" (重启动后) 列中输入值，可以为字段表分配存储空间。

"Max RAM Log Entries (20-400)" (最大 RAM 日志条目 [20 至 400]) — 最大 RAM 日志条目数。如果日志条目已满，日志将被清除，并且日志文件将重新启动。

使用 CLI 命令查看 RAM 日志条目计数器

下表概括了用于设置 "General Settings" (常规设置) 页面中显示的字段的等效 CLI 命令。

表 6-60. 常规设置的 CLI 命令

CLI 命令	说明
logging buffered size 数目	设置存储在内部缓冲区 (RAM) 中的系统日志信息的数目。

以下是 CLI 命令的示例：

```
console(config)# logging
```

```
buffered size 300
```

返回目录页面

返回目录页面

配置交换机信息

Dell™ PowerConnect™ 34XX 系统用户指南

本节介绍了有关配置网络安全保护、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。

配置网络安全保护

使用“Network Security”（网络安全保护）页面可以通过访问控制列表和锁定端口设置网络安全保护。要打开“Network Security”（网络安全保护）页面，请选择“Switch”（交换机）→“Network Security”（网络安全保护）。

基于端口的验证

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。端口通过 RADIUS 服务器使用扩展验证协议（EAP）进行验证。端口验证包括：

- 验证方 — 指定允许系统访问之前要验证的设备端口。
- 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。
- 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），并指示申请方是否有权访问系统服务。

基于端口的验证将创建两种访问状态：

- 受控制的访问 — 如果申请方已经过授权，则允许该申请方和系统进行通信。
- 不受控制的访问 — 不管端口的状态如何，都允许不受控制的通信。

该设备目前通过 RADIUS 服务器支持基于端口的验证。

基于端口的高级验证

基于端口的高级验证：

- 允许多台主机连接至单个端口。
- 只需要授权一台主机，就可以使所有主机都具有系统访问权限。如果该端口未经授权，则将拒绝连接的所有主机对网络进行访问。
- 启用基于用户的验证。设备中的特定 VLAN 始终可用，即使连接至 VLAN 的特定端口未经授权。
    - 例如，通过 IP 传输语音不需要验证，而数据通信则需要验证。可以定义不需要授权的 VLAN。用户可以使用未经验证的 VLAN，即使连接至 VLAN 的端口被定义为授权。

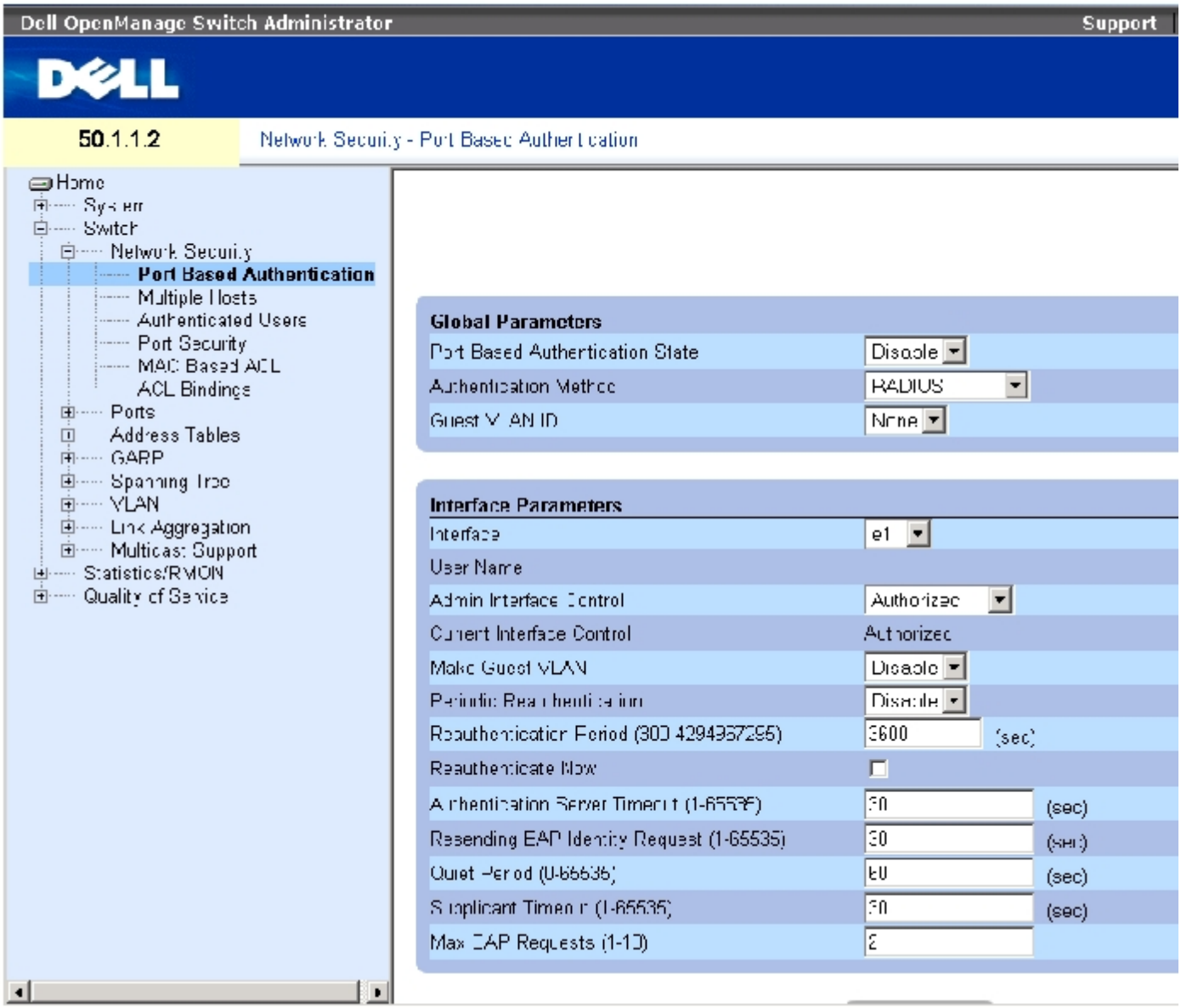
使用以下模式可以实现基于端口的高级验证：

- 单台主机模式 — 只有授权的主机才可以访问端口。
- 多台主机模式 — 可以将多台主机连接至单个端口。只须授权一台主机，就可以使所有主机都能访问网络。如果该主机验证失败或接收到一条 EAPOL 注销信息，则将拒绝连接的所有客户端对网络进行访问。
- 来宾 VLAN — 提供了授权给端口的有限网络访问。如果拒绝端口通过基于端口的授权对网络进行访问，但是启用了来宾 VLAN，则该端口可以收到有限网络访问。例如，网络管理员可以使用来宾 VLAN 拒绝通过基于端口的验证对网络进行访问，但是可以授予未经授权的用户 Internet 访问权限。

配置基于端口的验证

“Port Based Authentication”（基于端口的验证）页面使网络管理员可以配置基于端口的验证。要打开“Port Based Authentication”（基于端口的验证）页面，请单击“Switch”（交换机）→“Network Security”（网络安全保护）→“Port Based Authentication”（基于端口的验证）。

图 7-1. 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：

“Port Based Authentication State”（基于端口的验证的状态） — 在设备上允许进行基于端口的验证。可能的字段值包括：

“Enable”（启用） — 在设备上启用基于端口的验证。

“Disable”（禁用） — 在设备上禁用基于端口的验证。

“Authentication Method”（验证方法）— 表示使用的验证方法。可能的字段值包括：

“None”（无）— 表示没有用于验证端口的验证方法。

“RADIUS”— 表示通过 RADIUS 服务器执行端口验证。

“RADIUS, None”（RADIUS，无）— 表示首先通过 RADIUS 服务器执行端口验证。如果端口未经过验证，则没有验证方法可供使用，将允许会话。

“Guest VLAN”（来宾 VLAN）— 允许将来宾 VLAN 用于未经授权的端口。如果启用了来宾 VLAN，未经授权的端口将自动加入在“VLAN List”（VLAN 列表）字段中选择的 VLAN。字段默认值为“Disabled”（已禁用）。

“Interface”（接口）— 包含启用了基于端口的验证的接口列表。

“User Name”（用户名）— 表示申请方的用户名。

“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：

“Auto”（自动）— 在设备上启用基于端口的验证。根据设备和客户端之间的验证交换，接口在已授权状态和未授权状态之间转换。

“Authorized”（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重新发送和接收正常通信。

“Unauthorized”（未经授权）— 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。设备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）— 当前端口的授权状态。

“Make Guest VLAN”（使用来宾 VLAN）— 如果已启用，则表示连接至此接口的未经授权的用户可以访问来宾 VLAN。

“Periodic Reauthentication”（定期重新验证）— 允许立即重新验证端口。

“Reauthentication Period (300-4294967295)”（重新验证时段 [300-4294967295]）— 表明要重新验证选定端口的时间范围。字段值以秒为单位。字段默认值为 3600 秒。

“Reauthenticate Now”（立即重新验证）— 如果选取该选项，则会允许立即重新验证端口。

“Authentication Server Timeout (1-65535)”（验证服务器超时 [1-65535]）— 定义设备将请求重新发送到验证服务器之前经过的时间。字段值以秒为单位指定。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。字段默认值为 30 秒。

“Quiet Period (0-65535)” (无提示时段 [0-65535]) — 表示设备在验证交换失败之后处于无提示状态的秒数。可能的字段范围为 0 至 65535。字段默认值为 60 秒。

“Supplicant Timeout (1-65535)” (申请方超时 [1-65535]) — 表示 EAP 请求被重新发送到申请方之前经过的时间。字段值以秒为单位。字段默认值为 30 秒。

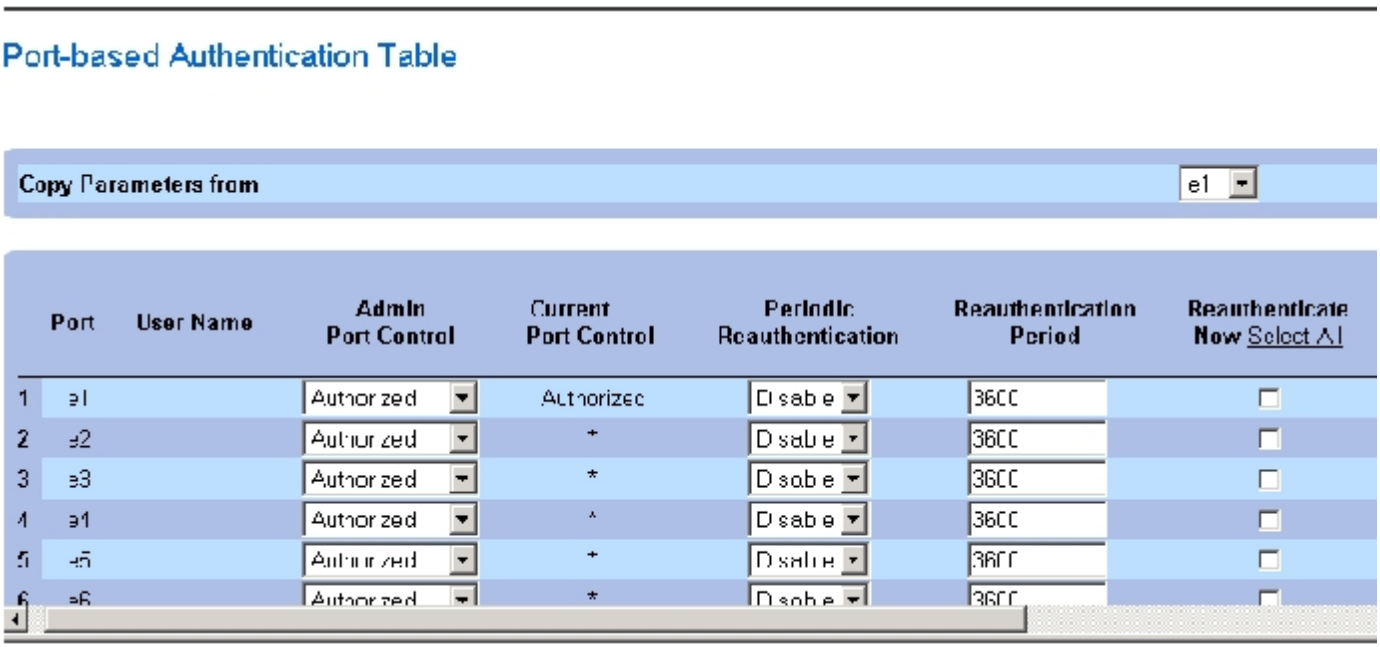
“Max EAP Requests (1-10)” (最大 EAP 请求 [1-10]) — 表示发送 EAP 请求的总次数。如果在定义的时段后未接收到响应，验证过程将重新启动。字段默认值为 2，即进行 2 次重试。

显示基于端口的验证表

1. 打开“Port Based Authentication” (基于端口的验证) 页面。
2. 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) ：

图 7-2. 基于端口的验证表



除了“Port Based Authentication” (基于端口的验证) 页面中的字段，“Port Based Authentication Table” (基于端口的验证表) 还显示了

以下字段：

“Unit No.”（装置号）— 选择堆栈成员。

“Copy Parameters from Port No.”（参数复制自端口号）— 从选定的端口复制参数。

复制“Port Based Authentication Table”（基于端口的验证表）中的参数

1. 打开该页面。
2. 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）。
3. 在“Copy Parameters from Port No.”（参数复制自端口号）字段中选择接口。
4. 在“Port Based Authentication Table”（基于端口的验证表）中选择一个接口。
5. 选取“Copy to”（复制到）复选框以定义基于端口的验证参数要复制到的接口。
6. 单击“Apply Changes”（应用更改）。

使用 CLI 命令启用基于端口的验证

下表概述了与“Port Based Authentication”（基于端口的验证）表中显示的用于启用基于端口的验证的选项等效的 CLI 命令。

表 7-61. 端口验证的 CLI 命令

CLI 命令	说明
aaa authentication dot1x default 方法 1 [方法 2.]	指定要在运行 IEEE 802.1X 的接口上使用的一种或多种验证、授权和计费 (AAA) 方法。
dot1x max-req 计数	设置设备在重新启动验证过程之前向客户端发送 EAP 的最大次数。
dot1x re-authenticate [ethernet 接口]	手动启动所有启用 802.1X 端口或指定的启用 802.1X 端口的重新验证。
dot1x re-authentication	启用客户端的定期重新验证。

dot1x timeout quiet-period 秒	设置设备在验证交换失败之后处于无提示状态的秒数。
dot1x timeout re-authperiod 秒	设置两次重新验证尝试之间的秒数。
dot1x timeout server-timeout 秒	设置将信息包重新传输到验证服务器的时间。
dot1x timeout supp-timeout 秒	设置将 EAP 请求帧重新传输到客户端的时间。
dot1x timeout tx-period 秒	设置设备重新发送请求之前等待客户端发出的对 EAP – 请求/标识帧的响应的秒数。
show dot1x [ethernet 接口]	显示设备或指定接口的 802.1X 状态。
show dot1x users [username username]	显示设备的 802.1X 用户。
dot1x guest-vlan enable	允许将来宾 VLAN 用于未经授权的端口。如果启用了来宾 VLAN，未经授权的端口将自动加入在“VLAN List”（VLAN 列表）字段中选择的 VLAN。字段默认值为“Disabled”（已禁用）。
dot1x guest-vlan	包含 VLAN 的列表。来宾 VLAN 是从“VLAN List”（VLAN 列表）中选择

以下是 CLI 命令的示例：

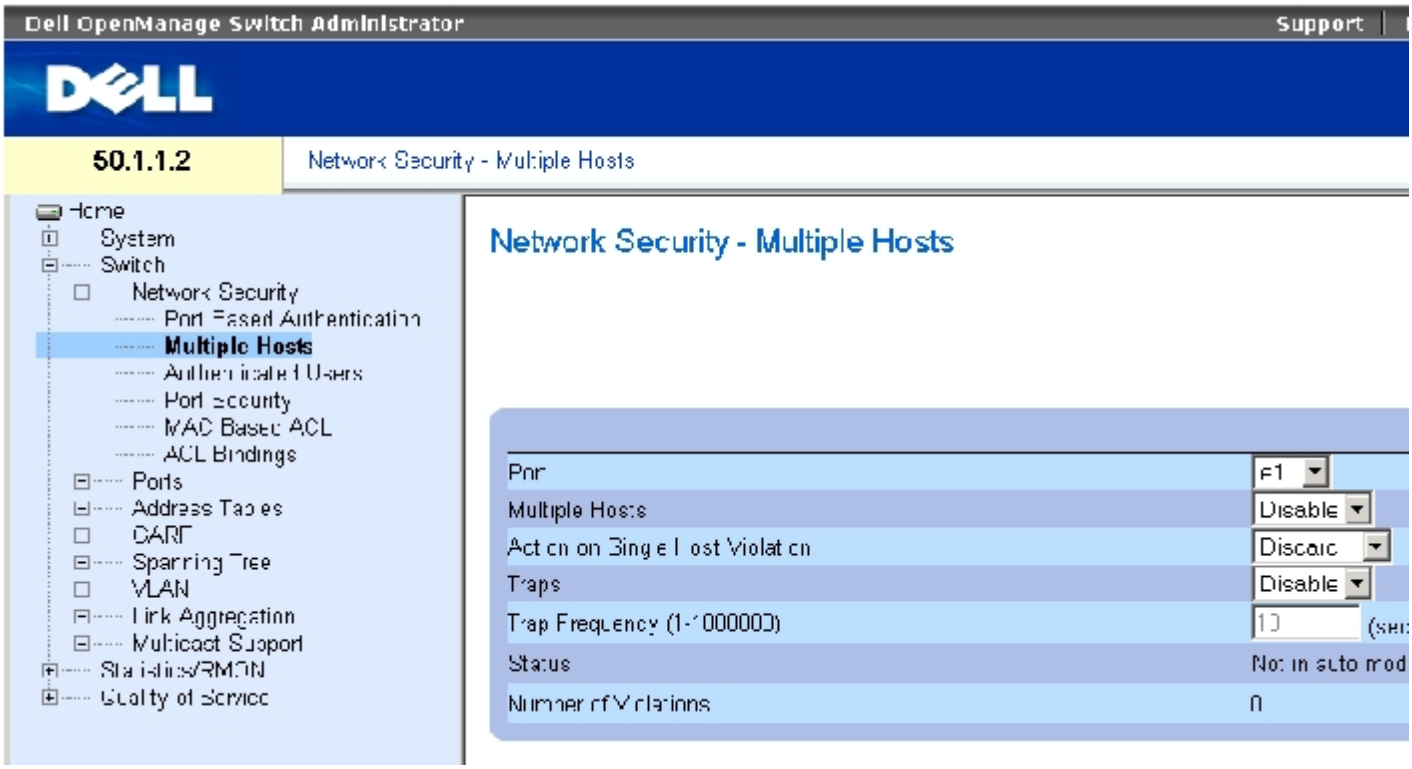
```
Console# show dot1x

Interface  Admin Mode  Oper Mode     Reauth Control  Reauth Period  Username
---------  ----------  ------------  --------------  -------------  --------
1/e1       Auto        Authorized    Ena             3600           Bob
1/e2       Auto        Authorized    Ena             3600           John
1/e3       Auto        Unauthorized  Ena             3600           Clark
1/e4       Force-auth  Authorized    Dis             3600           n/a
```

配置基于端口的高级验证

“Multiple Hosts”（多台主机）页面提供了关于为特定端口和 VLAN 定义基于端口的高级验证设置的信息。有关基于端口的高级验证的详细信

息，请参阅基于端口的高级验证。要打开“Multiple Hosts”（多个主机），请单击“Switch”（交换机）→“Network Security”（网络安全保护）→“Multiple Hosts”（多个主机）。

图 7-3. 多台主机



“Multiple Hosts”（多台主机）页面包含以下字段：

“Port”（端口）— 已启用了基于端口的高级验证的端口号。

“Multiple Hosts”（多个主机）— 允许或禁止一台主机可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器或使用锁定端口的安全保护。

“Action on Single Host Violation”（单个主机侵入时的措施）— 定义对以单个主机模式到达的信息包所采取的措施，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”（传输）— 传输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。

“Shutdown”（关闭）— 丢弃来自任何未记忆源的信息包，并关闭端口。在激活端口或重启动交换机之前，端口保持关闭状态。

“Traps”（陷阱）— 如果发生侵入，允许或禁止将陷阱发送到主机。

“Trap Frequency (1-1000000) (Sec)”（陷阱频率 [1-1000000] [秒]）— 定义将陷阱发送到主机的时间段。仅当“Multiple Hosts”（多台主机）字段定义为“Disable”（禁用）时，才能定义“Trap Frequency (1-1000000)”（陷阱频率 [1-1000000]）字段。默认值为 10 秒。

“Status”（状态）— 主机的状态。可能的字段值包括：

“Unauthorized”（未经授权）— 表示端口控制为“Force Unauthorized”（强制未授权），端口链路已断开或端口控制为“Auto”（自动），但尚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），并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）并且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）。

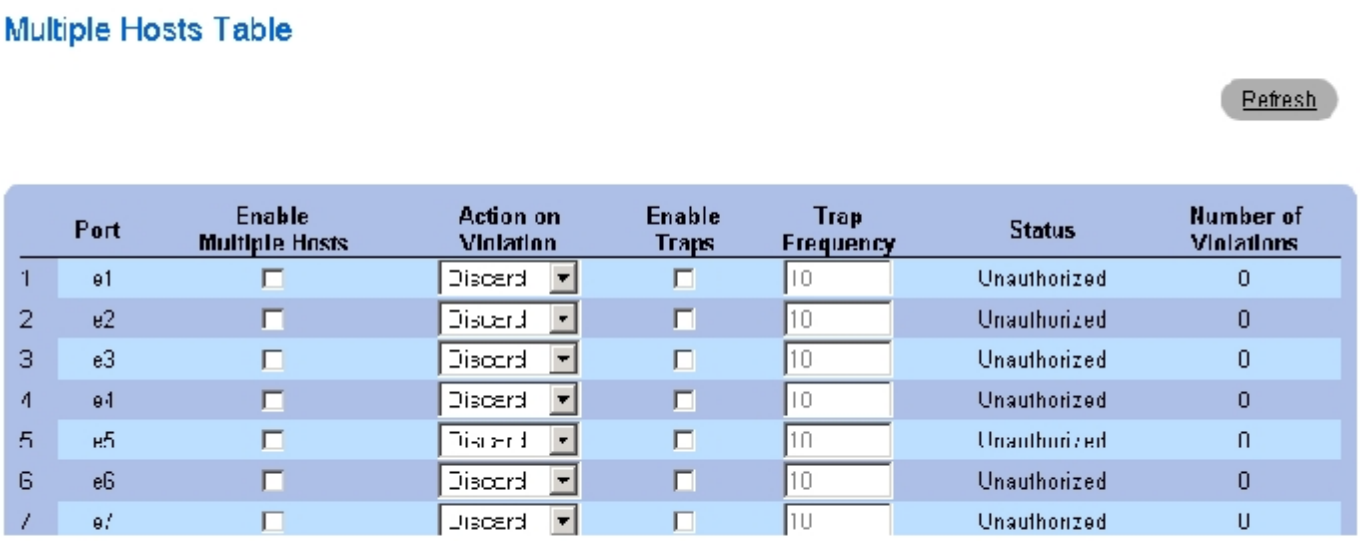
“Number of Violations”（侵入数目）— 以单个主机模式到达接口的信息包的数目，这些信息包来自其 MAC 地址不是客户端（申请方）MAC 地址的主机。

显示多台主机表

1. 打开“Multiple Hosts”（多台主机）页面。
2. 单击“Show All”（全部显示）。

系统将打开“Multiple Hosts Table”（多台主机表）。

图 7-4. 多台主机表



使用 CLI 命令启用多台主机

下表概述了与“Multiple Hosts”（多台主机）页面中显示的用于启用基于端口的高级验证的选项等效的 CLI 命令。

表 7-62. 多台主机的 CLI 命令

CLI 命令	说明
dot1x multiple-hosts	在具有 802.1X 授权的端口上允许多台主机（客户端），该端口将 dot1x 端口控制接口配置命令设置为自动。
dot1x single-host-violation {forward |discard |discard-shutdown}[trap seconds]	配置当其 MAC 地址不是客户端（申请方）MAC 地址的站点尝试访问接口时所采取的措施。

以下是 CLI 命令的示例。

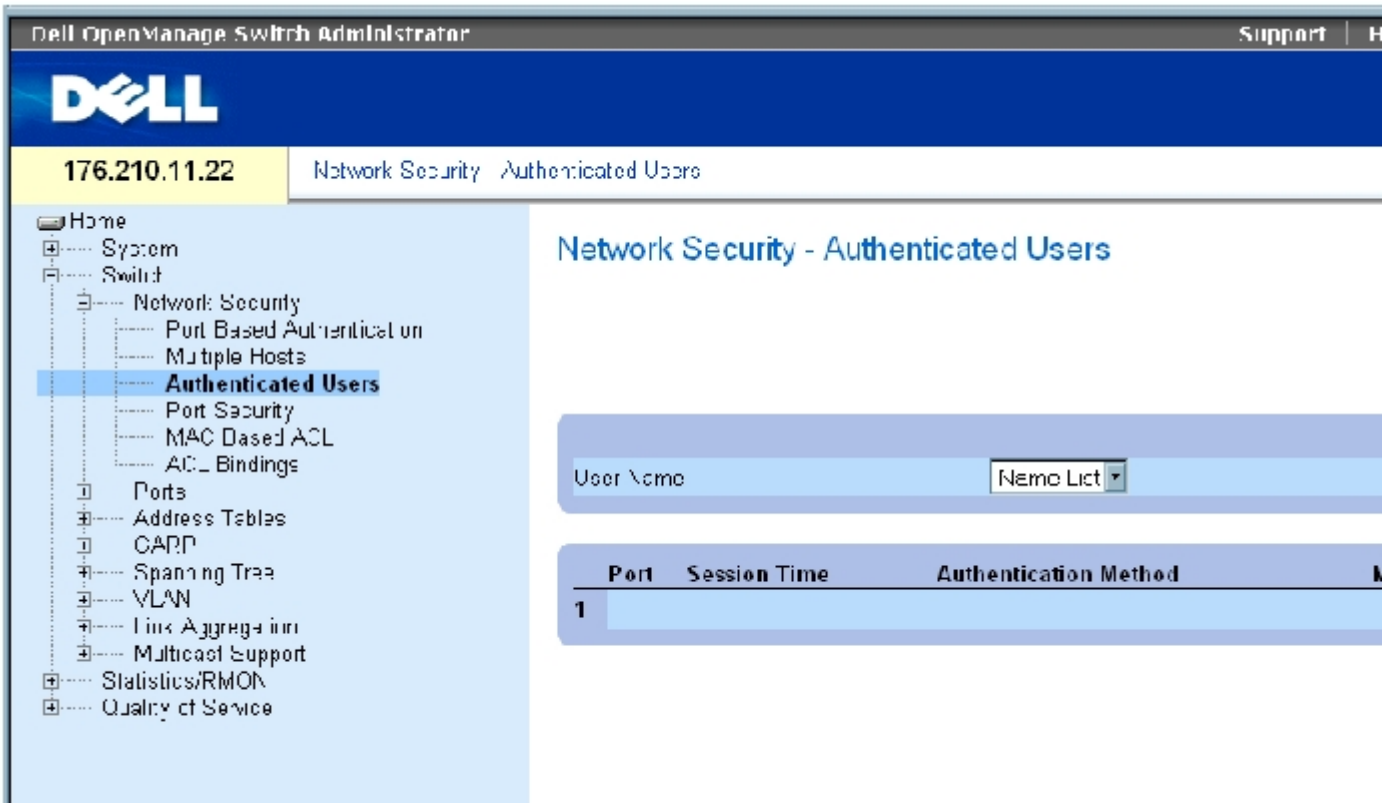
```
Console(config)# interface
ethernet 1/e1

Console(config-if)# dot1x
multiple-hosts
```

验证用户

“Authenticated Users”（经验证的用户）页面显示用户端口访问列表。“User Access Lists”（用户访问列表）在“Add User Name”（添加用户名）页面中作了定义。要打开“Authenticated Users”（经验证的用户）页面，请单击“Switch”（交换机）→“Network Security”（网

络安全保护）→“Authenticated Users”（经验证的用户）。

图 7-5. 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）— 通过 RADIUS 服务器授权的用户的列表。

“Port”（端口）— 用于验证的端口号，针对每个用户名。

“Session Time”（会话时间）— 用户登录到设备的时间。字段格式为天：小时：分钟：秒，例如，3 天：2 小时：4 分钟：39 秒。

“Authentication Method”（验证方法）— 验证上次会话时所使用的方法。可能的字段值包括：

“Remote”（远程）— 从远程服务器验证用户。

“None”（无）— 未验证用户。

“MAC Address”（MAC 地址）— 申请方 MAC 地址。

显示经验证的用户表

1. 打开“Authenticated Users”（经验证的用户）页面。

2. 单击“Show All”（全部显示）。

系统将打开“Authenticated Users Table”（经验证的用户表）：

图 7-6. 经验证的用户表

使用 CLI 命令验证用户

下表概括了与“Authenticated Users”（经验证的用户）页面中显示的用于验证用户的选项等效的 CLI 命令。

表 7-63. 添加用户名的 CLI 命令

CLI 命令	说明
show dot1x users [username username]	显示设备的 802.1X 用户。

以下是 CLI 命令的示例：

```
console# show dot1x users

Port Username Session Time Auth Method MAC Address

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

1/e11 gili 00:09:27 Remote 00:80:c8:b9:dc:1d
```

配置端口安全保护

通过将对特定端口的访问权限限制为只有具有特定 MAC 地址的用户可以访问，可以增强网络的安全性。根据以上需求，MAC 地址可以被动态记忆

或被静态配置。锁定端口安全保护监测在特定端口上接收的已接收到的信息包和已记忆的信息包。对锁定端口的访问仅限于具有特定 MAC 地址的用户。这些地址可以在端口上手动定义，也可以在锁定端口时在该端口上记忆。如果锁定端口接收到一个信息包，并且该信息包的源 MAC 地址没有与该端口关联（该 MAC 地址被记忆在其它端口上或系统不知道该地址），将调用保护机制，保护机制可以提供各种选项。未经授权的信息包到达锁定端口时保护机制提供的选项为：

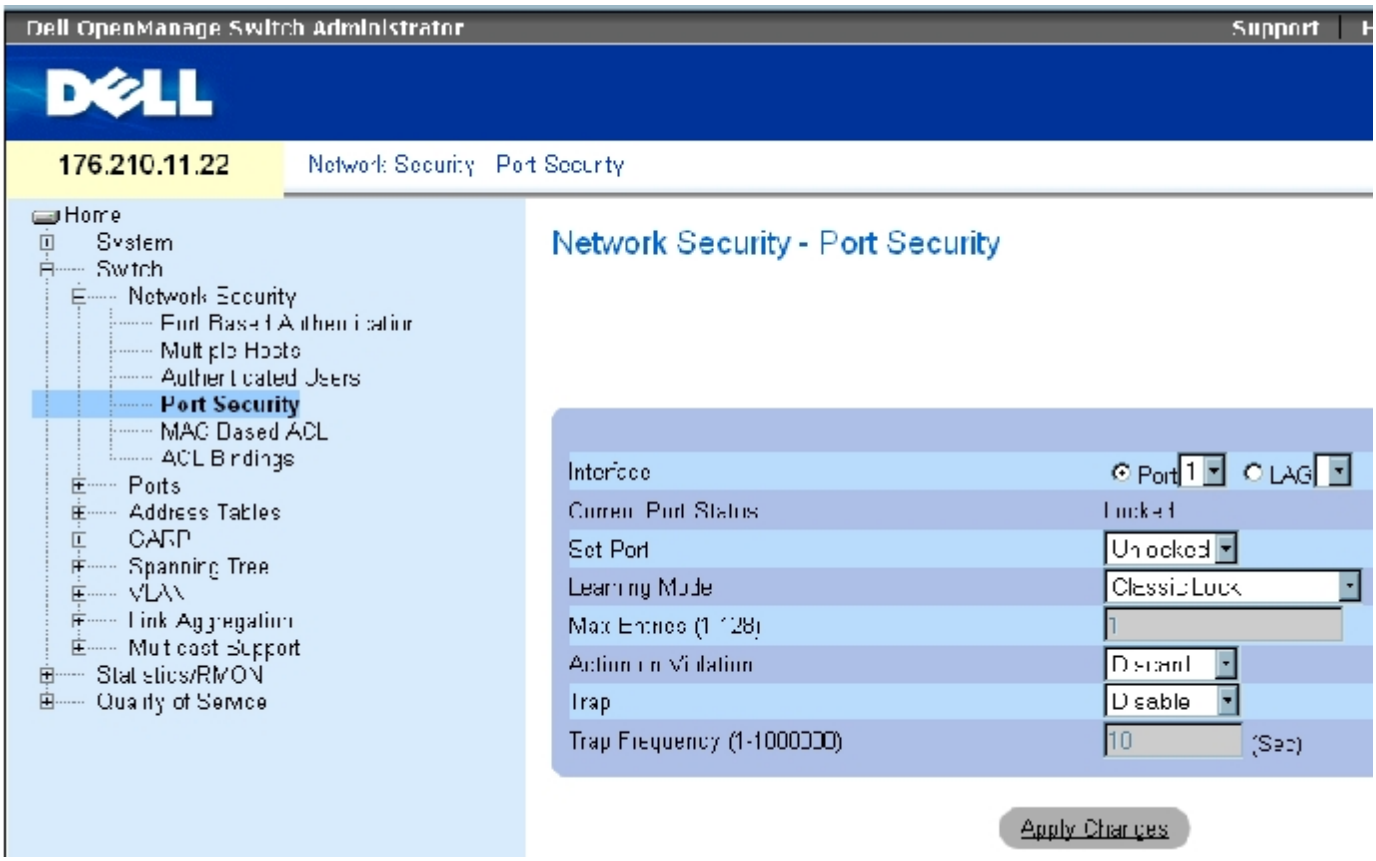
- 传输
- 不使用陷阱丢弃
- 使用陷阱丢弃
- 端口已关闭

锁定端口安全保护还可以在配置文件中存储 MAC 地址列表。重启动设备后，可以恢复 MAC 地址列表。

注：要启用端口安全保护，请在所需端口上启用“Multiple Hosts”（多台主机）功能。

通过“Port Security”（端口安全保护）页面可以激活已禁用的端口。“Ports”（端口）页面提供用于配置端口功能（包括风暴控制和端口镜像等高级功能）和执行虚拟端口测试的链路。要打开“Port Security”（端口安全保护）页面，请单击“Switch”（交换机）→“Network Security”（网络安全保护）→“Port Security”（端口安全保护）。

图 7-7. 端口安全保护



“Port Security”（端口安全保护）页面包含以下字段：

“Interface”（接口）— 要启用锁定端口的选定接口的类型。

“Port”（端口）— 选定的接口类型为端口。

“LAG”— 选定的接口类型为 LAG。

“Current Port Status”（当前端口状态）— 当前配置的端口状态。

“Set Port”（设置端口）— 端口已锁定或已解除锁定。可能的字段值包括：

“Unlocked”（已解除锁定）— 解除端口锁定。这是默认值。

“Locked”（已锁定）— 锁定端口。

“Learning Mode”（记忆模式）— 定义锁定端口类型。仅当选定“Set Port”（设置端口）字段中的“Locked”（已锁定）时，才能启用“Learning Mode”（记忆模式）字段。可能的字段值包括：

“Classic Lock”（经典锁定）— 使用经典锁定机制锁定端口。立即锁定端口，而不考虑已记忆的地址数。

“Limited Dynamic Lock”（限制动态锁定）— 通过删除与端口相关的当前动态 MAC 地址来锁定端口。端口最多记忆端口上允许的最大地址数。同时启用重新记忆的 MAC 地址和存在的 MAC 地址。

“Max Entries”（最大条目）— 指定端口上可以记忆的 MAC 地址数。仅当选定“Set Port”（设置端口）字段中的“Locked”（已锁定）时，才可以启用“Max Entries”（最大条目）字段。此外，还选择了“Limited Dynamic Lock”（限制动态锁定）模式。默认值为 1。

“Action on Violation”（侵入措施）— 对到达锁定端口的信息包所采取的措施。可能的字段值包括：

“Forward”（传输）— 传输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。

“Shutdown”（关闭）— 丢弃来自任何未记忆源的信息包，并关闭端口。在重新激活端口或重启动设备之前，端口保持关闭状态。

“Trap”（陷阱）— 当锁定端口接收到信息包时，允许发送陷阱。

“Trap Frequency (1-1000000)”（陷阱频率 [1-1000000]）— 两次陷阱之间的时间间隔（以秒为单位）。默认值为 10 秒。

定义锁定端口

1. 打开“Port Security”（端口安全保护）页面。
2. 选择接口类型和编号。
3. 定义字段。
4. 单击“Apply Changes”（应用更改）。

系统会将锁定端口添加至“Port Security Table”（端口安全保护表），并更新设备。

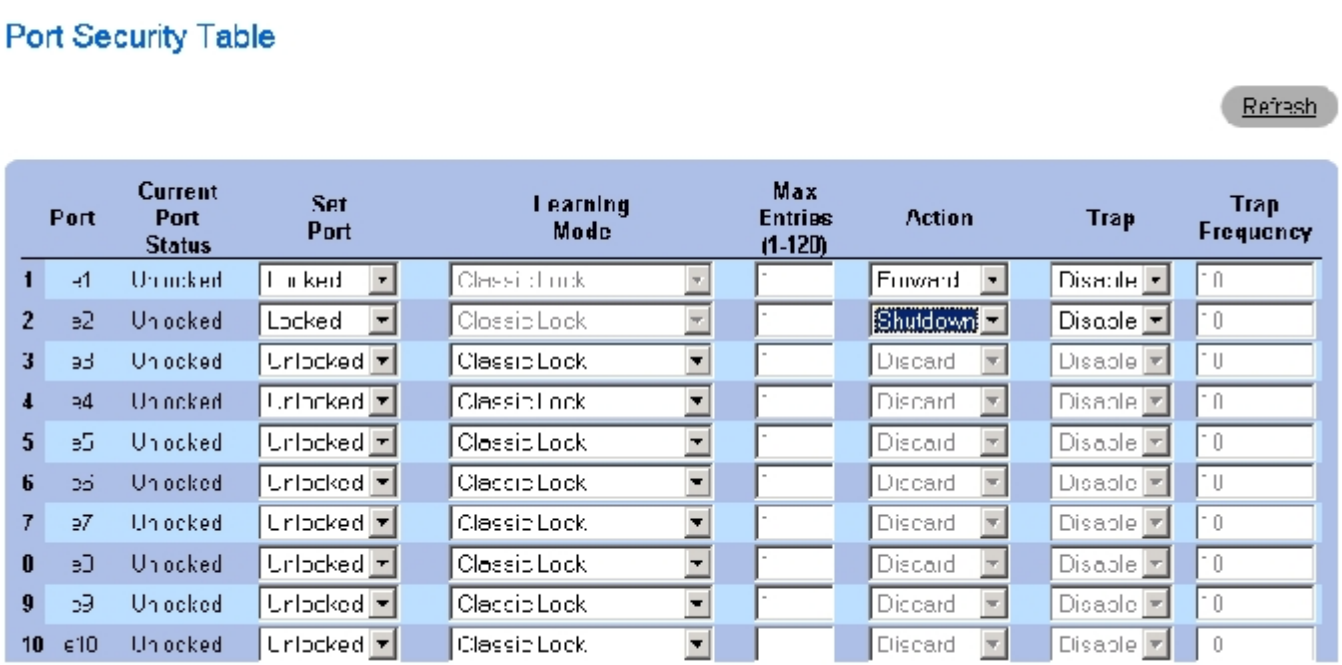
显示端口安全保护表

1. 打开“Port Security”（端口安全保护）页面。
2. 单击“Show All”（全部显示）。

系统将打开“Port Security Table”（端口安全保护表）：

注：锁定端口在“Port Security Table”（端口安全保护表）中进行定义。

图 7-8. 端口安全保护表



“Port Security Table”（端口安全保护表）还包含以下字段：

“Unit No.”（装置号）— 指定要显示锁定端口信息的堆栈装置。

“Copy Parameters from”（参数复制自）— 将参数复制到选定的装置号。

使用 CLI 命令配置锁定端口的安全保护

下表概括了与“Port Security”（端口安全保护）页面中显示的用于配置锁定端口安全保护的选项等效的 CLI 命令。

表 7-64. 端口安全保护的 CLI 命令

CLI 命令	说明
shutdown	禁用接口。
set interface active {ethernet 接口 | port-channel 端口信道号}	重新激活由于端口安全保护原因而关闭的接口。
port security learning {disabled | dynamic}	定义锁定端口类型。

port security max max-addr	指定端口上可以记忆的 MAC 地址数。
port security [forward | discard | discard-shutdown] [trap seconds]	锁定在接口上记忆新地址。
show ports security {ethernet 接口 | port-channel 端口信道号}	显示端口锁定状态。

以下是 CLI 命令的示例：

console # show ports security					
端口	Status	Action	Trap	Frequency	Counter
----	-------	-------	-------	---------	-------
1/e1	locked	Discard	Enable	100	88
1/e2	locked	Discard, Shutdown	Disable		
1/e3	Unlocked	-	-	-	-

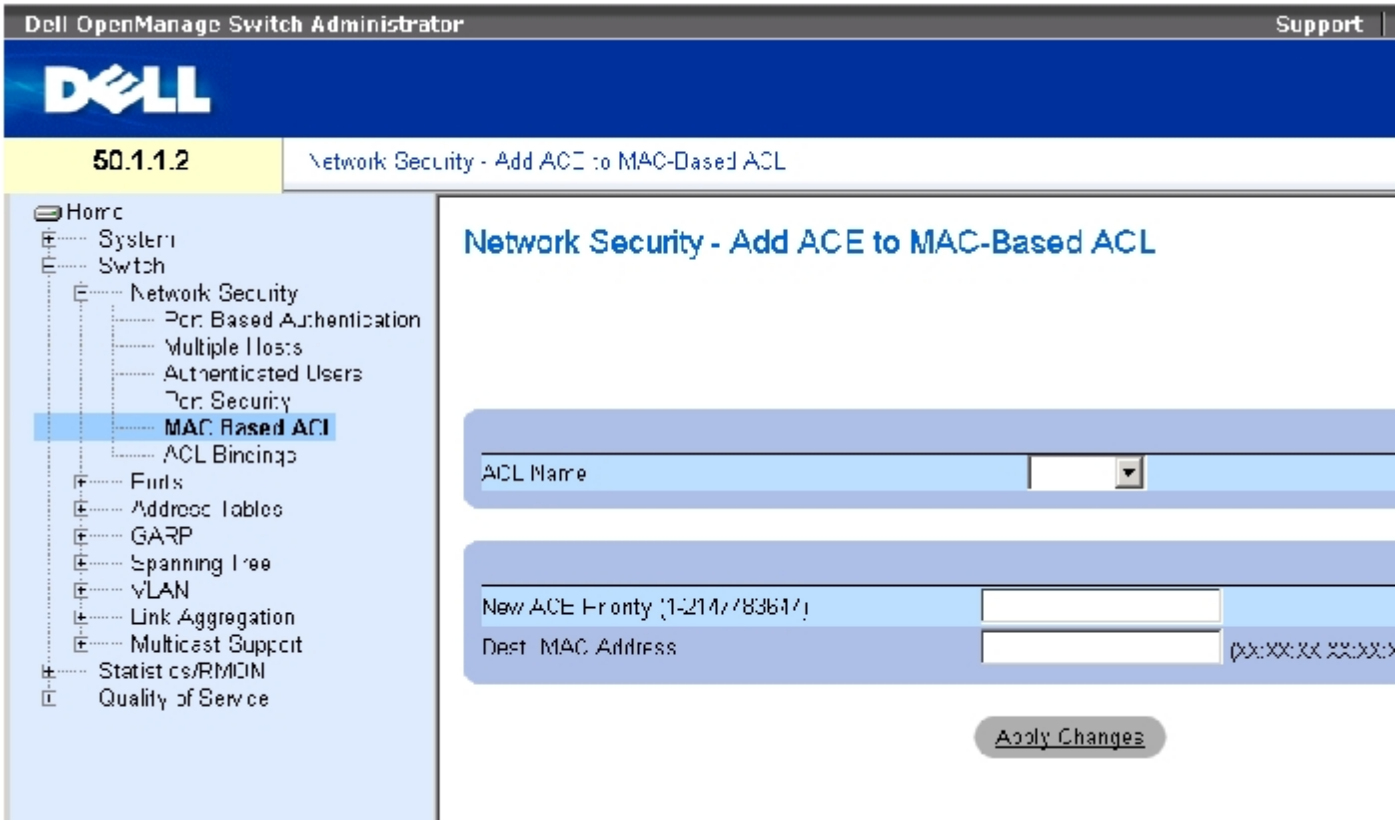
定义基于 MAC 的 ACL

访问控制列表 (ACL) 使网络管理员可以为特定入口端口定义分类操作和规则。ACL 包含多个分类规则和操作。每个分类规则和操作都被称为访问控制元素 (ACE)。ACE 是确定通信分类的筛选器。基于 MAC 的 ACL 适用于所有信息包，包括非 IP 信息包。分类字段仅基于 L2 字段。

“MAC Based ACL” (基于 MAC 的 ACL) 页面允许定义基于 MAC 的 ACL。有关 ACL 的说明，请参阅“定义基于 MAC 的 ACL”。

要打开“MAC Based ACL” (基于 MAC 的 ACL) 页面，请选择“Switch” (交换机) → “Network Security” (网络安全保护) → “MAC based ACL” (基于 MAC 的 ACL) 。

图 7-9. 基于 MAC 的 ACL



“MAC Based ACL”（基于 MAC 的 ACL）页面包含以下字段：

“ACL Name”（ACL 名称）— 用户定义的 ACL。

“New ACE Priority (1-2147483647)”（新 ACE 优先级 [1-2147483647]）—“ACL”字段中的 ACE 规则索引。

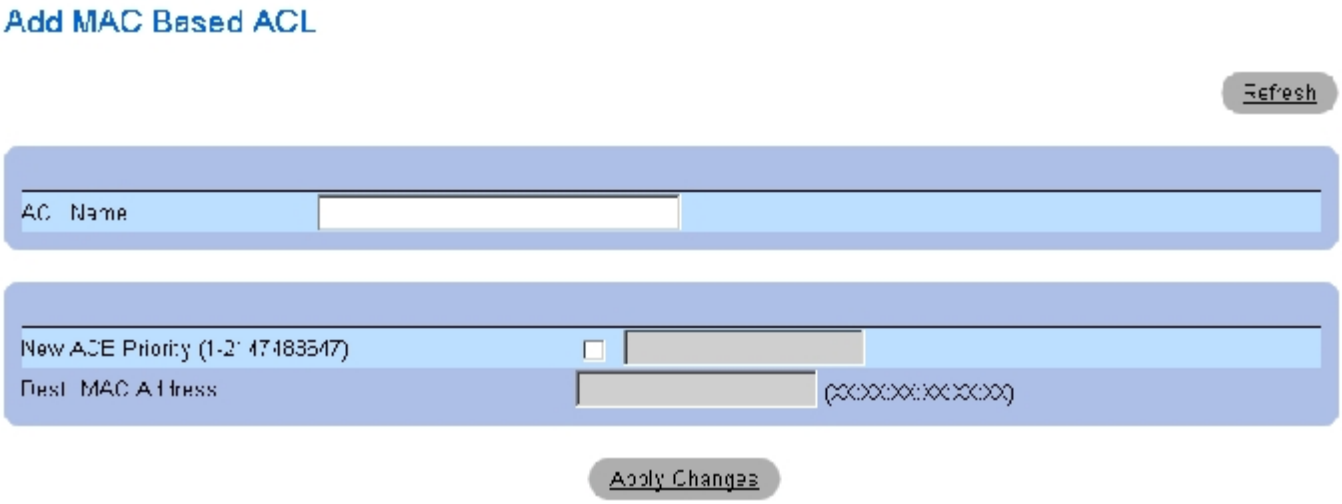
“Destination MAC Address”（目的地 MAC 地址）— 将信息包定址到的目的地 MAC 地址与 ACE 进行匹配。

添加基于 MAC 的 ACL：

1. 打开“MAC Based ACL”（基于 MAC 的 ACL）页面。
2. 单击“Add”（添加）。

   系统将打开“Add MAC Based ACLs”（添加基于 MAC 的 ACL）页面。

图 7-10. 添加基于 MAC 的 ACL



3. 定义字段。

4. 单击“Apply Changes”（应用更改）。

系统将定义基于 MAC 的 ACL，并更新设备。

显示特定 ACL 的 ACE

1. 打开“MAC Based ACL”（基于 MAC 的 ACL）页面。

2. 选择一个 ACL。

3. 单击“Show All”（全部显示）。

系统将打开“ACEs Associated with MAC ACL”（与 MAC ACL 相关联的 ACE）页面。

删除 ACL

1. 打开“MAC Based ACL”（基于 MAC 的 ACL）页面。

注：仅当 ACL 没有捆绑到接口时，才可以将其删除。

2. 选择一个 ACL。

3. 单击“Show All”（全部显示）。

系统将打开“ACEs Associated with MAC ACL”（与 MAC ACL 相关联的 ACE）页面。

4. 选取“Remove ACL”（删除 ACL）复选框。

使用 CLI 命令将基于 MAC 的 ACE 分配至 ACL

下表概括了与“MAC Based ACL”（基于 MAC 的 ACL）页面中显示的将基于 MAC 的 ACE 分配至 ACL 的选项等效的 CLI 命令。

表 7-65. 基于 MAC 的 ACE 的 CLI 命令

CLI 命令	说明
mac access-list 名称	创建第 2 层 MAC ACL，并进入 MAC 访问列表配置模式。
deny 目的地	如果与基于 MAC 的 ACL 中定义的条件相匹配，则拒绝通信。
show access-lists [名称]	显示设备上配置的访问控制列表。

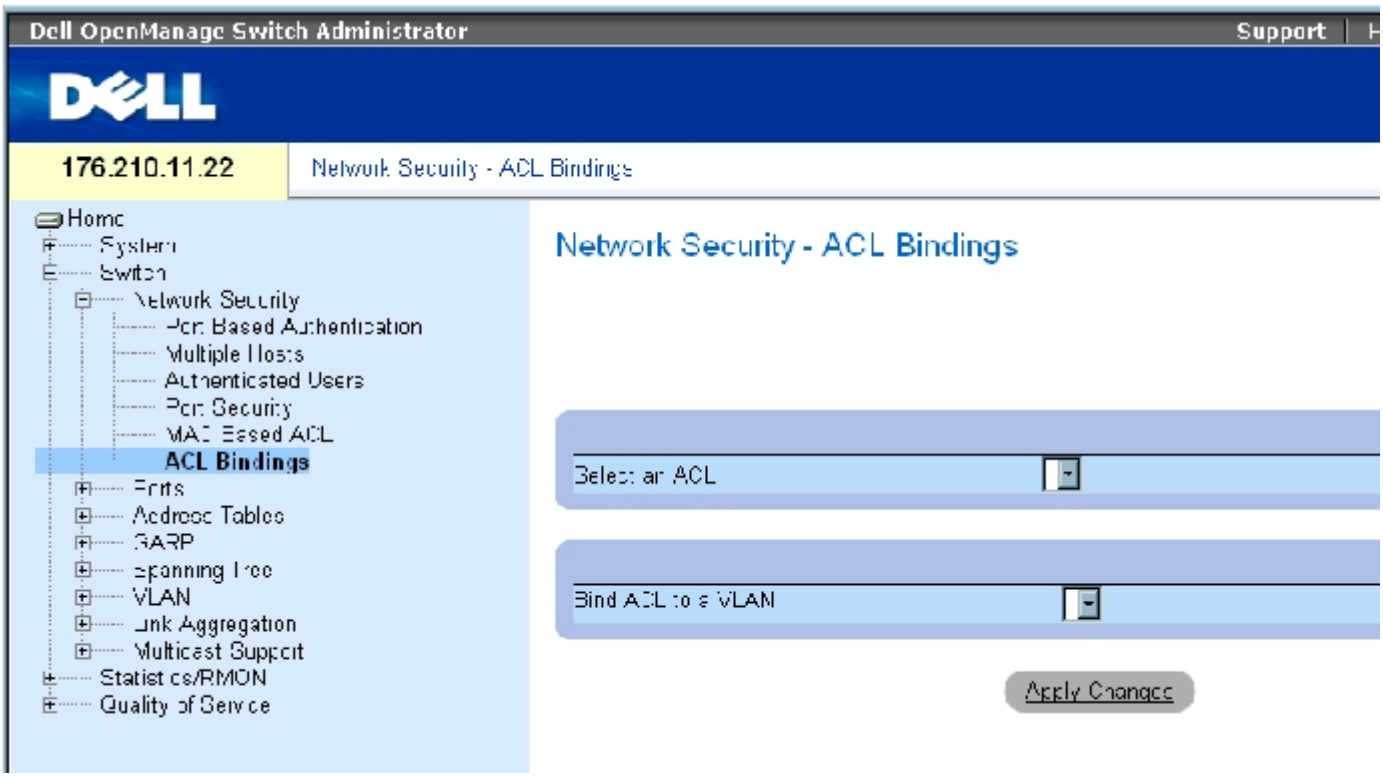
以下是 CLI 命令的示例：

```
console (config)# mac access-list dell
console (config-mac-al)# deny 00-10-B5-F4-00-01
```

配置 ACL 捆绑

当 ACL 与某接口捆绑时，此 ACL 将应用于该选定的接口。使用“ACL Bindings”（ACL 捆绑）页面将 ACL 列表分配至分类方法和接口。要打开“ACL Bindings”（ACL 捆绑）页面，请选择“Switch”（交换机）→“Network Security”（网络安全保护）→“ACL Binding”（ACL 捆绑）。

图 7-11. ACL 捆绑



"ACL Bindings" (ACL 捆绑) 页面包含以下字段：

"Select an ACL" (选择 ACL) — 与传入的信息包相匹配的 ACL 类型。

"Bind ACL to VLAN" (将 ACL 捆绑至 VLAN) — ACL 要连接的 VLAN。

将 ACL 分配至接口

1. 打开"ACL Bindings" (ACL 捆绑) 页面。
2. 在"Select an ACL" (选择 ACL) 字段中选择 ACL 类型。
3. 在"Bind ACL to an VLAN" (将 ACL 捆绑至 VLAN) 字段中选择 ACL 要连接的 VLAN。
4. 单击"Apply Changes" (应用更改) 。

ACL 将被连接至接口。

从 ACL 捆绑表中删除条目

1. 打开“ACL Bindings” (ACL 捆绑) 页面。
2. 单击“Show All” (全部显示) 。

   系统将打开“ACL Bindings Table” (ACL 捆绑表) 。
3. 为需要删除的条目选取“Remove” (删除) 复选框。
4. 单击“Apply Changes” (应用更改) 。

   系统将从表中删除选定的条目，并更新设备。

显示 ACL 捆绑表

1. 打开“ACL Bindings” (ACL 捆绑) 页面。
2. 单击“Show All” (全部显示) 以打开“ACL Bindings Table” (ACL 捆绑表) 。

   “ACL Bindings Table” (ACL 捆绑表) 中的字段与“ACL Bindings” (ACL 捆绑) 页面上的字段相同。

复制 ACL 捆绑表中的参数

1. 打开“ACL Bindings” (ACL 捆绑) 页面。
2. 单击“Show All” (全部显示) 。

   系统将打开“ACL Bindings Table” (ACL 捆绑表) 。
3. 在“Copy Parameters from” (参数复制自) 字段中选择一个接口。
4. 从“VLAN”下拉式菜单中选择一个 VLAN。

   此接口的定义将被复制到选定的目标端口/主干中。
5. 为要编辑的条目选取“Copy to” (复制到) 复选框，或为将定义复制到所有可用的端口/主干而选取该复选框。

6. 单击“Select All”（全部选定）。

7. 单击“Apply Changes”（应用更改）。

系统会将参数复制到“ACL Bindings Table”（ACL 捆绑表）中的目标端口/主干，并更新设备。

使用 CLI 命令分配 ACL 成员关系

下表概括了与“ACL Binding”（ACL 捆绑）页面中显示的分配 ACL 成员关系选项等效的 CLI 命令。

表 7-66. ACL 捆绑的 CLI 命令

CLI 命令	说明
service-acl {input acl 名称}	将访问列表应用于接口输入。

以下是 CLI 命令的示例：

```
console(config)# interface vlan 123

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

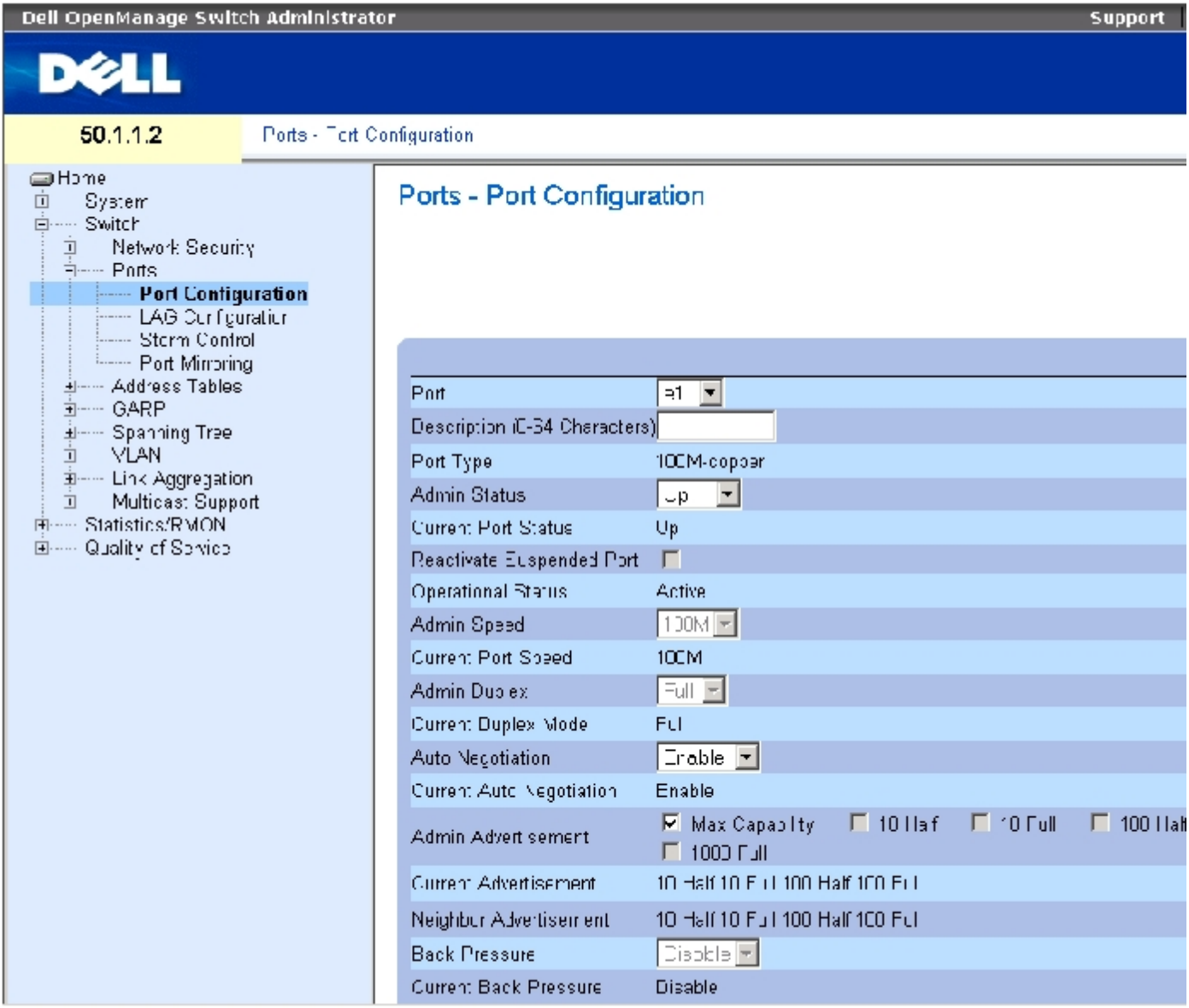
配置端口

“Ports”（端口）页面提供用于配置端口功能（包括风暴控制和端口镜像等高级功能）和执行虚拟端口测试的链路。要打开“Ports”（端口）页面，请选择“Switch”（交换机）→“Ports”（端口）。

定义端口配置

使用“Port Configuration”（端口配置）页面可以定义端口参数。如果在端口为 LAG 成员时修改了端口配置，则仅在从 LAG 中删除端口之后，配置更改才生效。要打开“Port Configuration”（端口配置）页面，请在树视图中单击“Switch”（交换机）→“Ports”（端口）→“Port Configuration”（端口配置）。

图 7-12. 端口配置



“Port Configuration”（端口配置）页面包含以下字段：

“Port”（端口）— 要为其定义端口参数的端口号。

“Description (0 - 64 Characters)”（说明 [0 至 64 个字符]）— 接口的简短说明，例如以太网。

“Port Type”（端口类型）— 端口的类型。

“Admin Status”（管理状态）— 允许或禁止通过端口传输通信。

“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。

“Reactivate Suspended Port”（重新激活暂挂的端口）— 重新激活已通过锁定端口安全保护选项禁用的端口。

“Operational Status”（运行状态）— 表示端口的运行状态。可能的字段值包括：

“Suspended”（暂挂）— 端口当前处于活动状态，并且未接收或传输通信。

“Active”（激活）— 端口当前处于活动状态，并且正在接收和传输通信。

“Disable”（禁用）— 端口当前处于禁用状态，并且未接收或传输通信。

“Admin Speed”（管理速率）— 端口的配置的速率。端口类型确定可以使用的速率设置选项。仅当端口被禁用时才可以指定管理速率。

“Current Port Speed”（当前端口速率）— 实际同步端口速率（以 bps 为单位）。

“Admin Duplex”（管理双工）— 端口的双工模式（以 bps 为单位）。“Full”（全双工）表示接口支持在设备和客户端之间同时进行双向传输。“Half”（半双工）表示接口仅支持在设备和客户端之间进行单向传输。

“Current Duplex Mode”（当前双工模式）— 同步端口的双工模式。

“Auto Negotiation”（自适应）— 在端口上启用自适应。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）— 当前的自适应设置。

“Admin Advertisement”（管理公告）— 定义端口公布的自适应设置。可能的字段值包括：

“Max Capability”（最大能力）— 表示接受所有的端口速率和双工模式设置。

“10 Half”（10 半双工）— 表示端口公布了 10 mbps 速率端口和半双工模式设置。

“10 Full”（10 全双工）— 表示端口公布了 10 mbps 速率端口和全双工模式设置。

“100 Half”（100 半双工）— 表示端口公布了 100 mbps 速率端口和半双工模式设置。

“100 Full”（100 全双工）— 表示端口公布了 100 mbps 速率端口和全双工模式设置。

“1000 Full”（1000 全双工）— 表示端口公布了 1000 mbps 速率端口和全双工模式设置。

“Current Advertisement”（当前公告）— 端口向其邻居端口公布其速率以启动适应进程。可能的字段值为在“Admin Advertisement”（管理公告）字段中指定的那些值。

“Neighbor Advertisement”（邻居公告）— 表示邻居端口的公告设置。其字段值与“Admin Advertisement”（管理公告）字段值相同。

“Back Pressure”（背压）— 在端口上启用背压模式。背压模式与半双工模式一起使用可以禁止端口接收信息。OOB 端口中不支持背压。

“Current Back Pressure”（当前背压）— 当前的背压设置。

“Flow Control”（流控制）— 启用或禁用端口上的流控制或启用流控制的自适应。

“Current Flow Control”（当前流控制）— 当前的流控制设置。

“MDI/MDIX”— 使设备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。如果禁用自适应，则自动 MDIX 不能在 FE 端口上运行。可能的字段值包括：

“Auto”（自动）— 用于自动检测电缆的类型。

“MDIX”— 用于集线器和交换机。

“MDI”— 用于终端站点。

“Current MDI/MDIX”（当前 MDI/MDIX）— 表示当前的设备 MDIX 设置。可能的字段值包括：

“MDI”— 当前的 MDI 设置为 MDI。

“MDIX”— 当前的 MDI 设置为 MDIX。

“LAG”— 指定端口是否为 LAG 的一部分。

注：如果在端口为 LAG 成员时修改了端口配置，则仅在从 LAG 中删除端口之后，配置更改才生效。

定义端口参数

1. 打开“Port Configuration”（端口配置）页面。
2. 在“Port”（端口）字段中选择一个端口。
3. 定义对话框中的可用字段。
4. 单击“Apply Changes”（应用更改）。

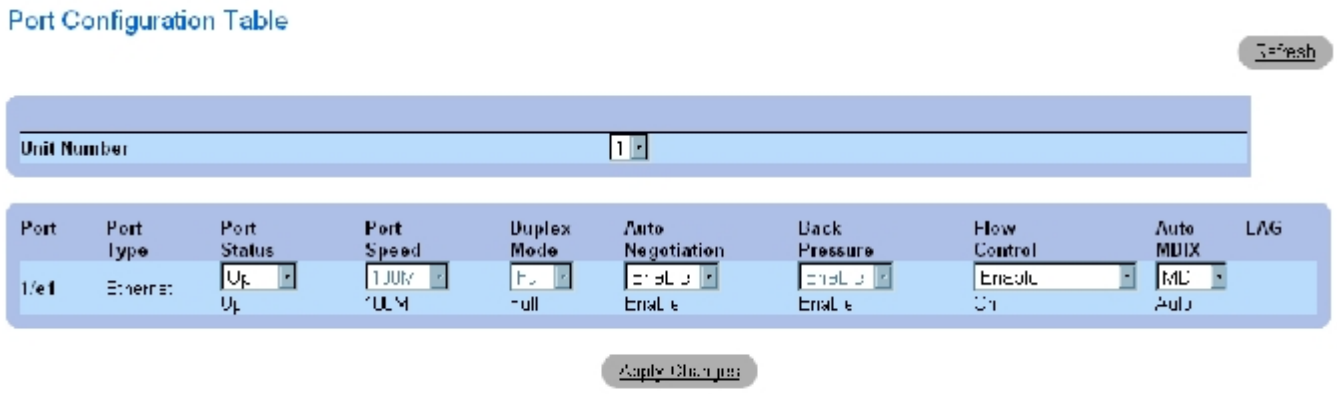
端口参数将被保存至设备。

显示端口表

1. 打开“Port Configuration”（端口配置）页面。
2. 单击“Show All”（全部显示）。

系统将打开“Port Configuration Table”（端口配置表）。

图 7-13. 端口配置表



使用 CLI 命令配置端口

下表概括了与“Port Configuration”（端口配置）页面中显示的配置端口的选项等效的 CLI 命令。

表 7-67. 端口配置的 CLI 命令

CLI 命令	说明
interface ethernet 接口	进入接口配置模式以配置以太网类型接口。
description 字符串	添加对接口配置的说明。
shutdown	禁用属于当前设置环境的接口。
set interface active {ethernet 接口 | port-channel 端口信道号}	重新激活由于安全保护原因而关闭的接口。

speed Mbps	配置在不使用自适应时给定以太网接口的速率。
duplex {half | full}	配置在不使用自适应时给定以太网接口的全/半双工操作。
negotiation [capability1 [capability2...capability5]	启用给定接口的速率和双工参数的自适应操作。
back-pressure	在给定接口上启用背压。
flowcontrol {auto | on | off}	在给定接口上配置流控制。
mdix {on | auto}	在给定接口或端口信道上启用自动绞接。
show interfaces configuration [ethernet 接口| port-channel 端口信道号]	显示所有已配置接口的配置。
show interface advertise	显示接口的适应公告设置。
show interfaces status [ethernet 接口 |port-channel 端口信道号]	显示所有已配置接口的状态。
show interfaces description [ethernet 接口 | port-channel 端口信道号]	显示所有已配置接口的说明。

以下是 CLI 命令的示例：

```
console(config)# interface ethernet 1/e3

console(config-if)# description "RD SW#3"

console(config-if)# shutdown

console(config-if)# no shutdown

console(config-if)# speed 100

console(config-if)# duplex full

console(config-if)# negotiation

console(config-if)# back-pressure

console(config-if)# flowcontrol on

console(config-if)# mdix auto

console(config-if)# end

console# show interfaces configuration ethernet 1/e3
```

Port	Type	Duplex	Speed	Neg	Flow Control	Admin State	Back Pressure	Mdix Mode
---	---	-----	----	----	------	-----	------	---
1/e3	100	Full	100	Enabled	On	Up	Enable	Auto

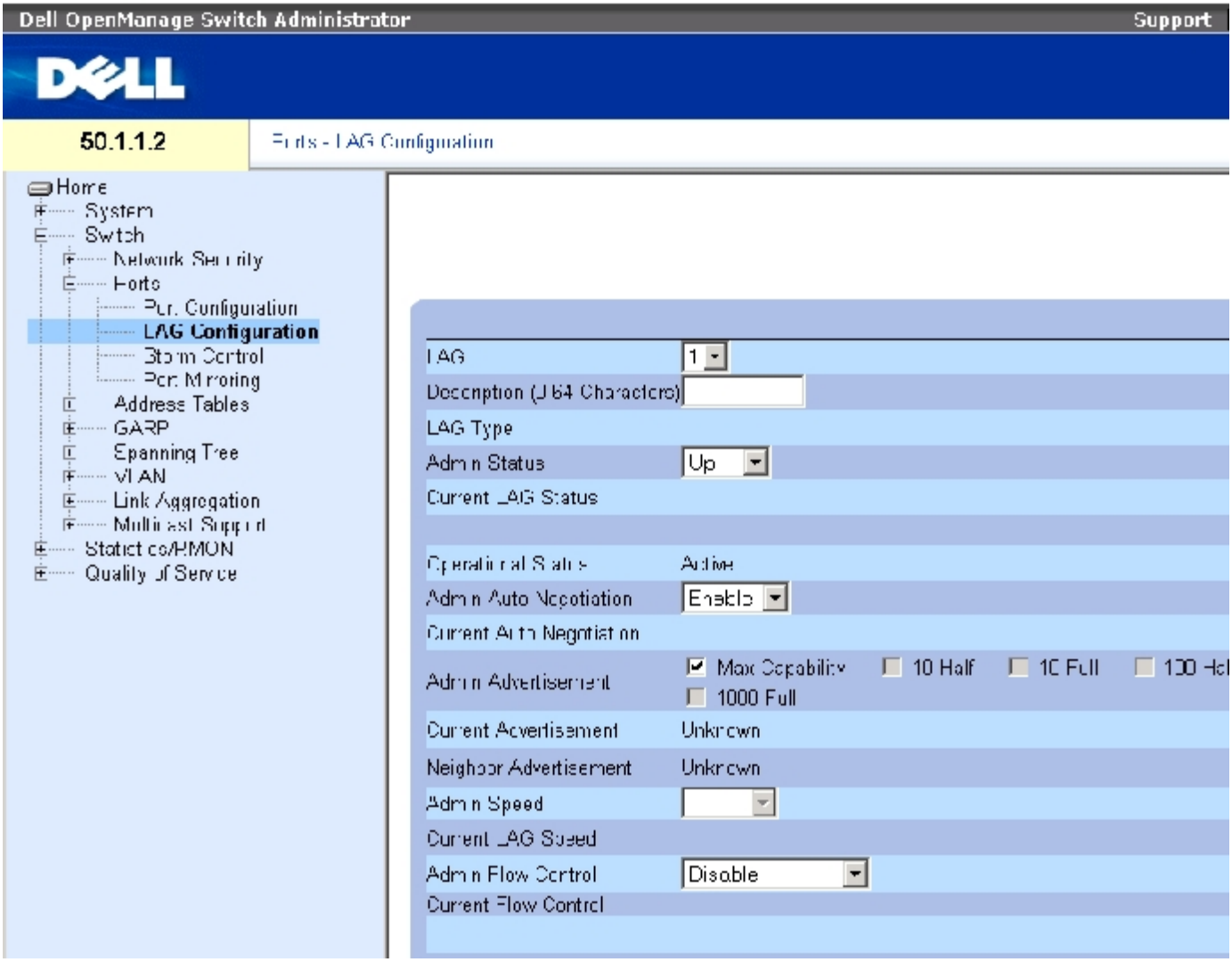
Console# **show interfaces status**								
Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Mode
----	----	------	-----	----	-------	------	-------	----
1/e3	100	Full	100	Auto	On	Up	Enable	On
1/e4	100	Full	1000	Off	Off	Up	Disable	On
Ch	Type	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State	
---	----	------	-----	------	-------	--------	-------	
1	1000	Full	1000	Off	Off	Disable	Up	

定义 LAG 参数

“LAG Configuration” (LAG 配置) 页面包含用于为已配置的 LAG 配置参数的字段。设备支持每个 LAG 最多八个端口，每个系统八个 LAG。有关链路聚合组 (LAG) 以及将端口分配至 LAG 的信息，请参阅“聚合端口”。

要打开“Port Configuration” (端口配置) 页面，请在树视图中单击“Switch” (交换机) → “Ports” (端口) → “LAG Configuration” (LAG 配置) 。

图 7-14. LAG 配置



“LAG Configuration” (LAG 配置) 页面包含以下字段：

“LAG” — LAG 号。

“Description (0 - 64 Characters)” (说明 [0 至 64 个字符]) — 提供已配置的 LAG 的用户定义的说明。

“LAG Type” (LAG 类型) — 组成 LAG 的端口类型。

“Admin Status” (管理状态) — 启用或禁用选定的 LAG。

“Current LAG Status” (当前 LAG 状态) — 表示 LAG 当前是否正在运行。

“Operational Status” (运行状态) — 允许或禁止通过选定的 LAG 传输通信。

“Admin Auto Negotiation” (管理自适应) — 在 LAG 上启用或禁用自适应。自适应是两个链接伙伴之间的协议，使一个 LAG 可以将其传输速率、双工模式和流控制（流控制的默认设置为已禁用）能力通知给伙伴端口。

“Current Auto Negotiation”（当前自适应）— 当前配置的自适应设置。

“Admin Advertisement”（管理公告）— 定义 LAG 公布的自适应设置。可能的字段值包括：

“Max Capability”（最大能力）— 表示接受所有的 LAG 速率和双工模式设置。

“10 Half”（10 半双工）— 表示 LAG 公布了 10 mbps 速率 LAG 和半双工模式设置。

“10 Full”（10 全双工）— 表示 LAG 公布了 10 mbps 速率 LAG 和全双工模式设置。

“100 Half”（100 半双工）— 表示 LAG 公布了 100 mbps 速率 LAG 和半双工模式设置。

“100 Full”（100 全双工）— 表示 LAG 公布了 100 mbps 速率 LAG 和全双工模式设置。

“1000 Full”（1000 全双工）— 表示 LAG 公布了 1000 mbps 速率 LAG 和全双工模式设置。

“Current Advertisement”（当前公告）— LAG 向其邻居 LAG 公布其速率以启动适应进程。可能的字段值为在“Admin Advertisement”（管理公告）字段中指定的那些值。

“Neighbor Advertisement”（邻居公告）— 表示邻居 LAG 的公告设置。其字段值与“Admin Advertisement”（管理公告）字段值相同。

“Admin Speed”（管理速率）— LAG 运行的速率。

“Current LAG Speed”（当前 LAG 速率）— 当前的 LAG 运行速率。

“Admin Flow Control”（管理流控制）— 启用/禁用流控制或启用 LAG 上流控制的自适应。流控制模式在 LAG 中以全双工模式运行的端口上有效。

“Current Flow Control”（当前流控制）— 用户指定的的流控制的设置。

定义 LAG 参数

1. 打开“LAG Configuration”（LAG 配置）页面。
2. 在“LAG”字段中选择一个 LAG。
3. 定义字段。

4. 单击“Apply Changes”（应用更改）。

LAG 参数将被保存至设备。

修改 LAG 参数

1. 打开“LAG Configuration”（LAG 配置）页面。
2. 在“LAG”字段中选择一个 LAG。
3. 修改字段。
4. 单击“Apply Changes”（应用更改）。

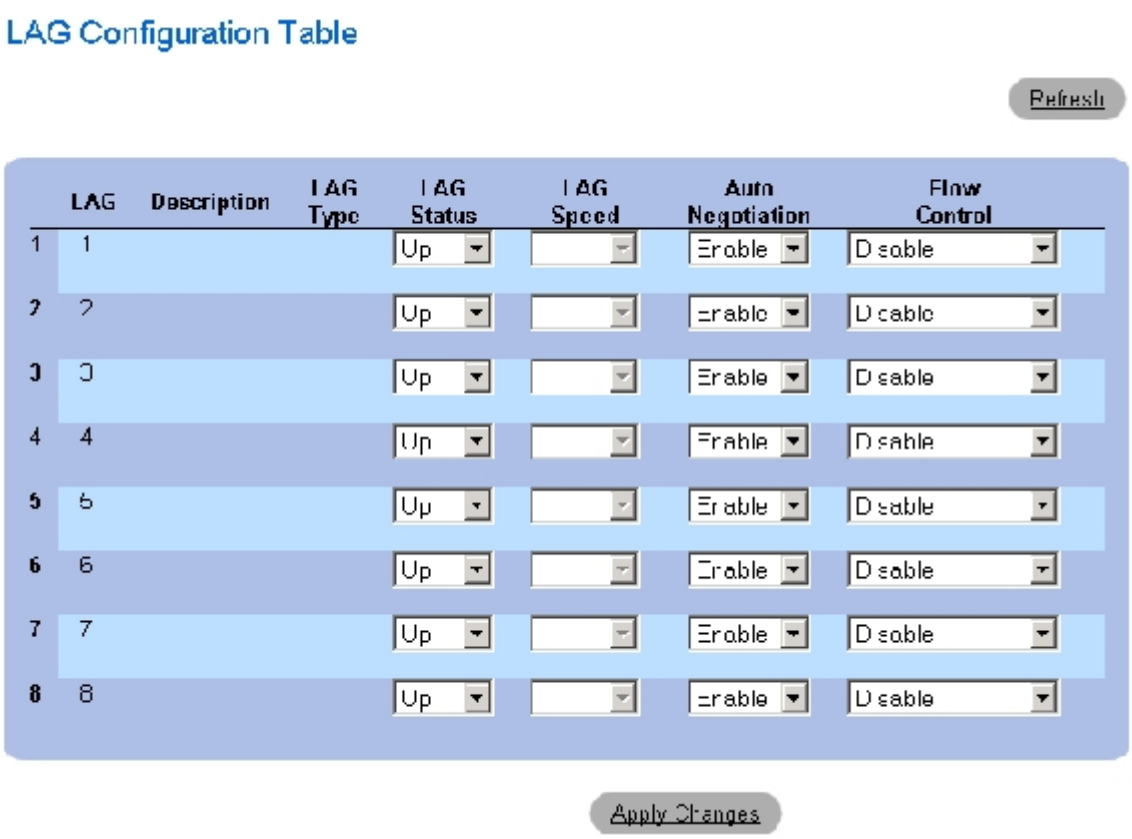
LAG 参数将被保存至设备。

要显示 LAG 配置表，请：

1. 打开“LAG Configuration”（LAG 配置）页面。
2. 单击“Show All”（全部显示）。

系统将打开“LAG Configuration Table”（LAG 配置表）：

图 7-15. LAG 配置表



使用 CLI 命令配置 LAG

下表概括了与“LAG Configuration” (LAG 配置) 页面中显示的用于配置 LAG 的选项等效的 CLI 命令。

表 7-68. LAG 配置的 CLI 命令

CLI 命令	说明
interface port-channel 端口信道号	进入特定端口信道的接口配置模式。
description 字符串	添加对接口配置的说明。
shutdown	禁用属于当前设置环境的接口。
speed bps	配置在不使用自适应时给定以太网接口的速率。
negotiation [capability1 [capability2...capability5]	启用接口速率自适应操作。
back-pressure	在给定接口上启用背压。
flowcontrol {auto | on | off}	在给定接口上配置流控制。
show interfaces configuration [ethernet 接口| port-channel 端口信道号]	显示所有已配置接口的配置。

show interfaces status [ethernet 接口 |port-channel 端口信道号]	显示所有已配置接口的状态。
show interfaces configuration [ethernet 接口| port-channel 端口信道号]	显示所有已配置接口的说明。
show interfaces port-channel [端口信道号]	显示端口信道信息（哪些端口是端口信道的成员，以及它们当前是否处于活动状态）。

以下是 CLI 命令的示例：

```
console(config)# interface port-channel 2

console(config-if)# no negotiation

console(config-if)# speed 100

console(config-if)# flowcontrol on

console(config-if)# exit

console(config)# interface port-channel 3

console(config-if)# shutdown

console(config-if)# exit

console(config)# interface port-channel 4

console(config-if)# back-pressure

console(config-if)# description p4

console(config-if)# end

console# show interfaces port-channel
```

Channel	Ports
---------	---------
ch1	Inactive:1/e(11-13)
ch2	Active:1/e14

启用风暴控制

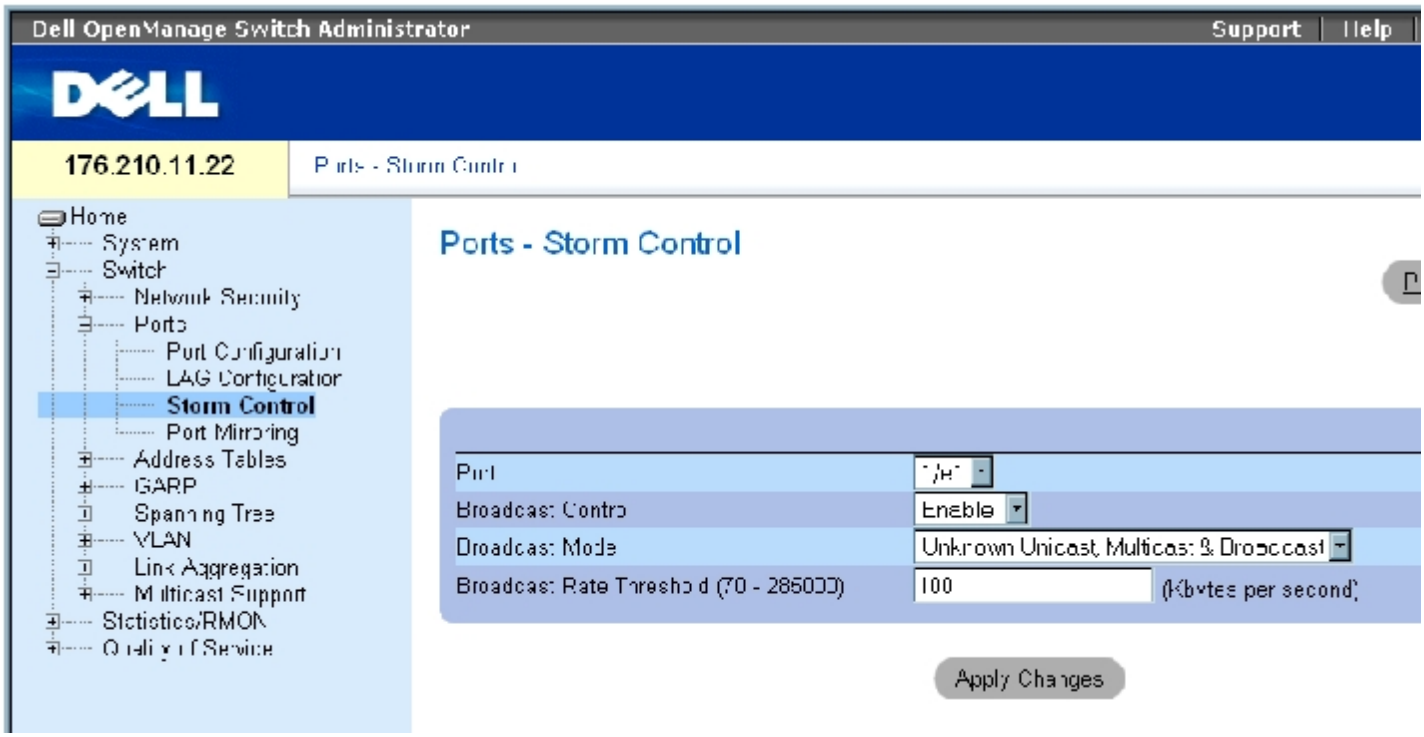
广播风暴是过多的广播信息同时通过单个端口在网络中传输的结果。已传输信息的响应被堆入网络，从而过多占用网络资源或导致网络超时。

通过定义信息包类型和信息包传输速率来针对每个端口启用风暴控制。

系统在各个端口上分别测量传入的广播、单点传送和多点传送帧速率，并在速率超出用户定义的速率时丢弃帧。

“Storm Control” （风暴控制）页面提供了用于启用和配置风暴控制的字段。要打开“Storm Control” （风暴控制）页面，请在树视图中单击“Switch” （交换机）→“Ports” （端口）→“Storm Control” （风暴控制）。

图 7-16. 风暴控制



“Storm Control” （风暴控制）页面包含以下字段：

“Port” （端口） — 要从其启用风暴控制的端口。

“Broadcast Control” （广播控制） — 在特定接口上启用或禁用传输广播信息包的类型。

“Broadcast Mode” （广播模式） — 指定当前在设备或堆栈上启用的广播模式。可能的字段值包括：

“Unknown Unicast, Multicast & Broadcast” （未知单点传送、多点传送和广播） — 计数单点传送、多点传送和广播通信。

“Multicast & Broadcast” （多点传送和广播） — 同时计数广播和多点传送通信。

“Broadcast Only” （仅广播） — 仅计数广播通信。

“Broadcast Rate Threshold (70-285000)” （广播速率阈值 [70-285000]） — 传输未知信息包的最大速率（千字节/秒）。字段范围为 70 至

285000 千字节/秒。

启用风暴控制

1. 打开“Storm Control”（风暴控制）页面。
2. 选择要在其上实现风暴控制的接口。
3. 定义字段。
4. 单击“Apply Changes”（应用更改）。

系统将启用风暴控制。

修改风暴控制端口参数

1. 打开“Storm Control”（风暴控制）页面。
2. 修改字段。
3. 单击“Apply Changes”（应用更改）

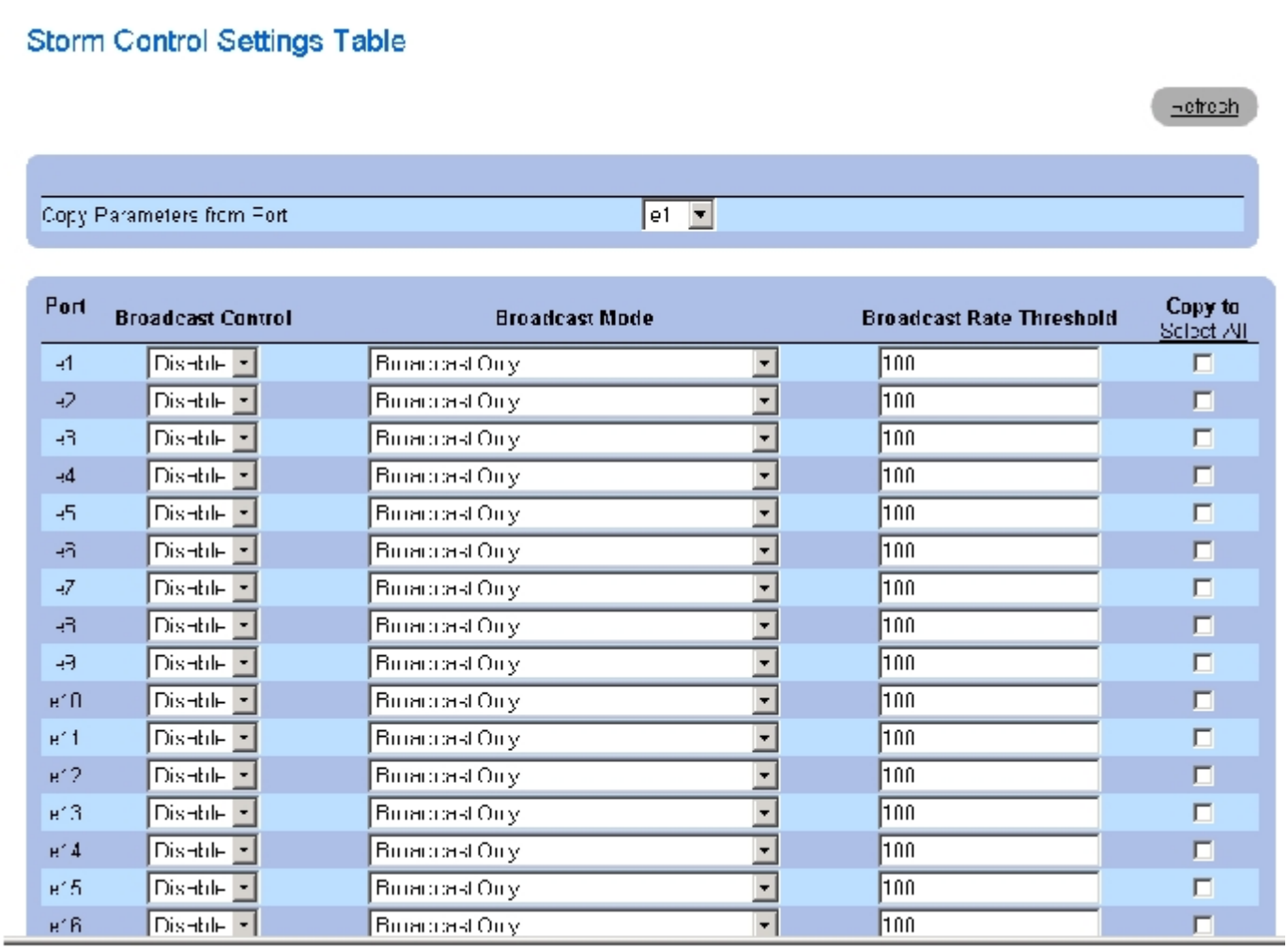
风暴控制端口参数将被保存至设备。

显示端口参数表

1. 打开“Storm Control”（风暴控制）页面。
2. 单击“Show All”（全部显示）。

系统将打开“Storm Control Settings Table”（风暴控制设置表）：

图 7-17. 风暴控制设置表



除了“Storm Control”（风暴控制）页面中的字段外，“Storm Control Settings Table”（风暴控制设置表）还包含以下字段：

“Copy Parameters from Port”（参数复制自端口）— 表示从中复制风暴控制参数的特定端口。

复制风暴控制设置表中的参数

1. 打开“Storm Control”（风暴控制）页面。
2. 单击“Show All”（全部显示）。

   系统将打开“Storm Control Settings Table”（风暴控制设置表）。
3. 从“Copy Parameters from Port”（参数复制自端口）字段中选择要从中复制设置的端口。
4. 选取“Copy to”（复制到）复选框以定义风暴控制定义要复制到的接口，或单击“Select All”（全部选定）以将定义复制到所有端口。
5. 单击“Apply Changes”（应用更改）。

系统会将参数复制到“Storm Control Settings Table”（风暴控制设置表）中选定的端口，并更新设备。

使用 CLI 命令配置风暴控制

下表概括了与“Storm Control”（风暴控制）页面中显示的配置风暴控制的选项等效的 CLI 命令。

表 7-69. 风暴控制的 CLI 命令

CLI 命令	说明
port storm-control include-multicast	允许设备将多点传送信息包、单点传送信息包和广播信息包一起计数。
port storm-control broadcast enable	启用广播风暴控制。
port storm-control broadcast rate	配置最大广播速率。
show ports storm-control 端口	显示风暴控制配置。

以下是 CLI 命令的示例：

```
console(config)# port storm-control include-multicast

console(config)# interface ethernet 1/e1

console(config-if)# port storm-control broadcast enable

console(config-if)# port storm-control broadcast rate 100000

console(config-if)# end

console# show ports storm-control
```

Port	Broadcast Storm control [kbyes/sec]
-----	----------
1/e1	8000

2/e1	Disabled
3/e2	Disabled

定义端口镜像会话

端口镜像：

- 通过将传入和传出信息包的副本从一个端口传输至监测端口，端口镜像可以监测和镜像网络通信。
- 可以用作诊断工具和/或调试功能。
- 启用设备性能和监测。

通过选择要复制所有信息包的特定端口以及要从中复制信息包的其它端口，即可配置端口镜像。

在配置端口镜像之前，请注意以下几点：

- 通过将传入和传出信息包的副本从被监测端口传输至监测端口，端口镜像可以监测和镜像网络通信。
- 被监测端口的运行速率不能高于监测端口的运行速率。
- 所有 RX/TX 信息包应在同一端口进行监测。

以下限制适用于要被配置为目的地端口的端口：

- 端口不能被配置为源端口。
- 端口不能为 LAG 成员。
- 未在端口上配置 IP 接口。
- 未在端口上启用 GVRP。
- 端口不是 VLAN 成员。
- 只能定义一个目的地端口。

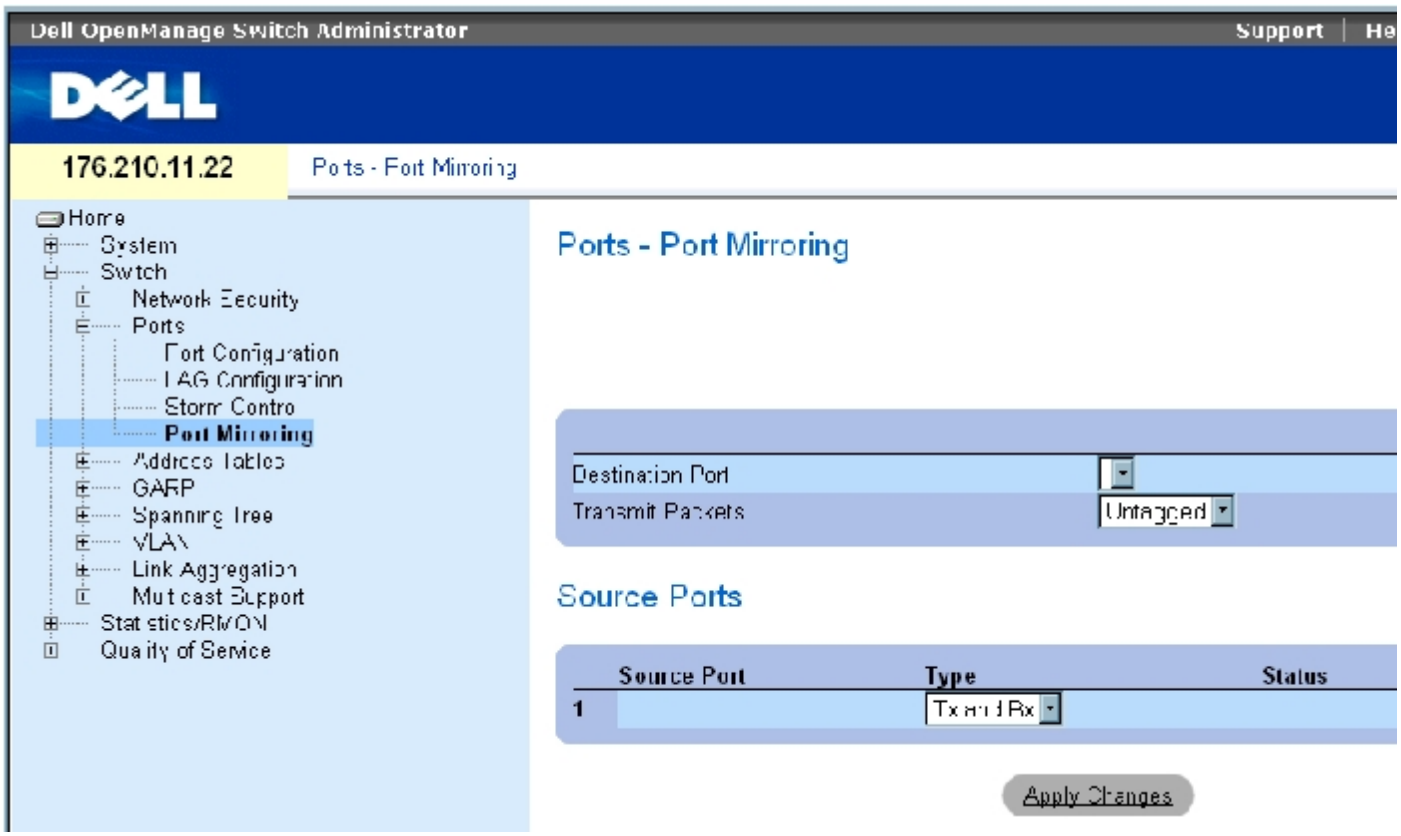
以下限制适用于要被配置为源端口的端口：

- 源端口不能为 LAG 成员。
- 端口不能被配置为目的地端口。
- 最多支持 8 个源端口。

要打开“Port Mirroring”（端口镜像）页面，请在树视图中单击“Switch”（交换机）→“Ports”（端口）→“Port Mirroring”（端口镜像）。

注：将端口设置为用于端口镜像会话的目标端口时，此端口上的所有正常操作均将被暂挂，包括生成树和 LACP。

图 7-18. 端口镜像



“Port Mirroring”（端口镜像）页面包含以下字段：

“Destination Port”（目的地端口）— 端口通信要复制到的端口号。

“Transmit Packets”（传输信息包）— 定义信息包的镜像方法。可能的字段值包括：

“Untagged”（未标记）— 将信息包镜像为未标记的 vlan 信息包。这是默认值。

“Tagged”（已标记）— 将信息包镜像为已标记的 vlan 信息包。

“Type”（类型）— 表示被镜像的信息包是否为 RX 或 TX 或者同时为 RX 和 TX。

“Status”（状态）— 表示端口当前处于被监测（“Active”[激活]）状态还是未被监测（“Ready”[就绪]）状态。

“Remove”（删除）— 如果选定该选项，将删除端口镜像会话。

添加端口镜像会话

1. 打开“Port Mirroring”（端口镜像）页面。
2. 单击“Add”（添加）。

   系统将打开“Add Source Port”（添加源端口）页面。
3. 定义“Source Port”（源端口）和“Type”（类型）字段。
4. 单击“Apply Changes”（应用更改）。
5. 从“Destination Port”（目的地端口）下拉式菜单中选择目的地端口。
6. 单击“Refresh”（刷新）按钮，打开“Port Mirroring”（端口镜像）页面。
7. 定义“Tagged Packets”（已标记信息包）字段。
8. 定义“Type”（类型）字段。
9. 单击“Apply Changes”（应用更改）。

   系统将定义新的源端口，并更新设备。

从端口镜像会话中删除副本端口

1. 打开“Port Mirroring”（端口镜像）页面。
2. 选取“Remove”（删除）复选框。
3. 单击“Apply Changes”（应用更改）。

系统将删除选定端口的镜像会话，并更新设备。

使用 CLI 命令配置端口镜像会话

下表概括了与“Port Mirroring”（端口镜像）页面中显示的配置端口镜像会话的选项等效的 CLI 命令。

表 7-70. 端口镜像的 CLI 命令

CLI 命令	说明
port monitor SRC 接口 [rx | tx]	启动端口监测会话。

以下是 CLI 命令的示例：

```
console(config)# interface ethernet 1/e1

console(config-if)# port monitor 1/e2

console(config-if)# end

console# show ports monitor
```

Source Port	Destination Port	Type	Status	VLAN Tagging
----------	----------	----------	----------	----------
1/e2	1/e1	RX, TX	Active	No

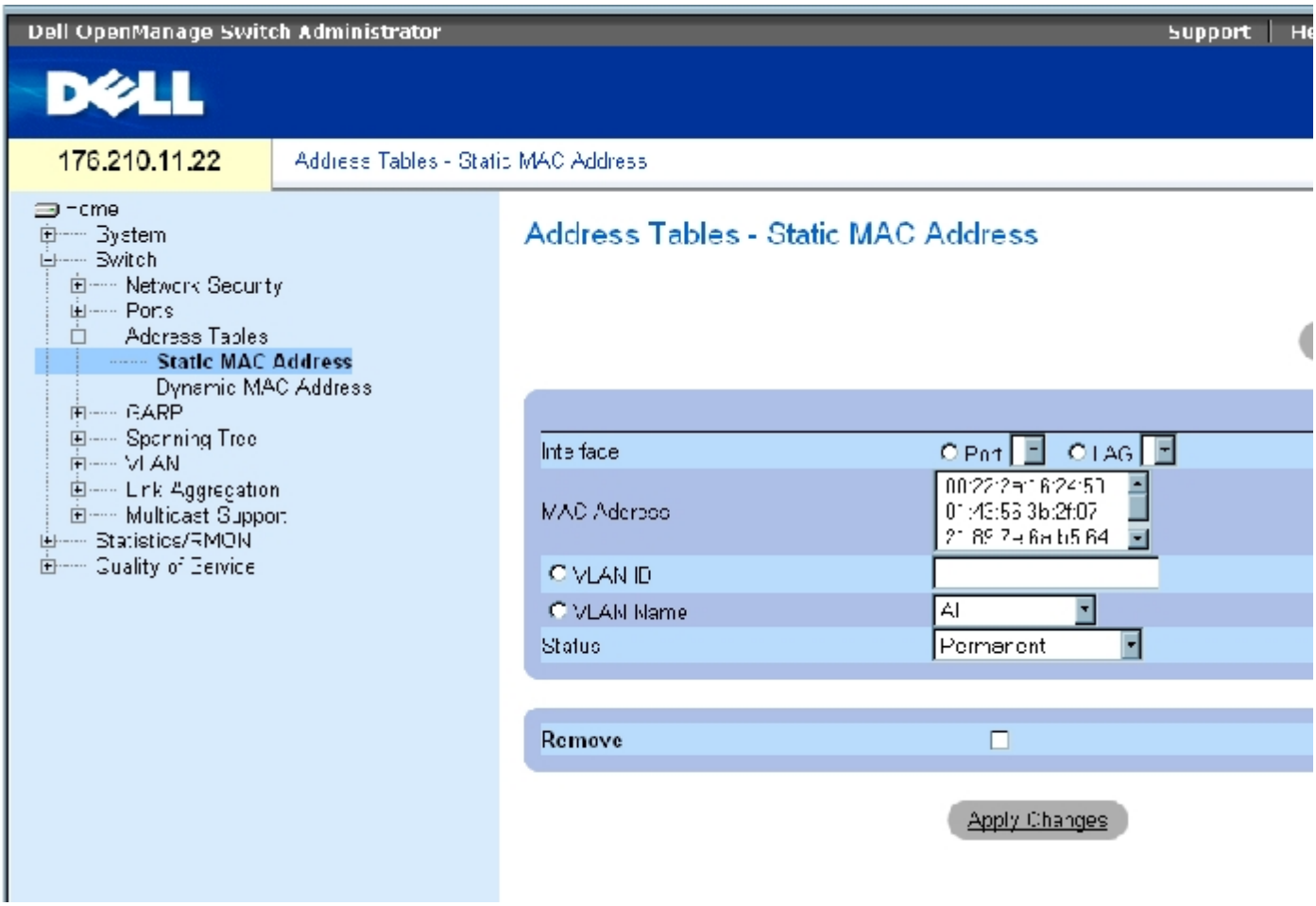
配置地址表

MAC 地址存储在静态地址或动态地址数据库中。定址到其中一个数据库存储的目的地的信息包将被立即传输至端口。动态地址表可以按接口、VLAN 和 MAC 地址进行排序。当信息包从源到达设备时，MAC 地址将被动态记忆。通过从帧的源地址学习端口，可以将地址与端口相关联。定址到与任一端口均不相关的目的地 MAC 地址的帧将被多路发送至相关 VLAN 的所有端口。可以手动配置静态地址。为防止桥接表溢出，在特定时间段内未进行任何通信的动态 MAC 地址将被删除。要打开“Address Tables”（地址表）页面，请在树视图中单击“Switch”（交换机）→“Address Tables”（地址表）。

定义静态地址

“Static MAC Address Table”（静态 MAC 地址表）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）页面中添加和删除静态地址。此外，也可以为单个端口定义若干个 MAC 地址。要打开“Static MAC Address Table”（静态 MAC 地址表）页面，请在树视图中单击“Switch”（交换机）→“Address Table”（地址表）→“Static Address Table”（静态地址表）。

图 7-19. 静态 MAC 地址表



“Static MAC Address Table”（静态 MAC 地址表）页面包含以下字段：

“Interface”（接口）— 要应用静态 MAC 地址的特定端口或 LAG。

“MAC Address”（MAC 地址）— 当前静态地址列表中列出的 MAC 地址。

“VLAN ID”— 附加至 MAC 的 VLAN ID。

“VLAN Name”（VLAN 名称）— 用户定义的 VLAN 名称。

“Status”（状态）— MAC 地址的状态。可能的值包括：

“Secure”（安全）— 用于定义锁定端口的静态 MAC 地址。

“Permanent”（永久）— MAC 地址是永久性的。

“Delete on Reset”（重设时删除）— 在重设设备时删除 MAC 地址。

“Delete on Timeout”（超时时删除）— 发生超时时删除 MAC 地址。

注：要防止在重启动以太网设备时删除静态 MAC 地址，请确保已锁定连接至 MAC 地址的端口。

“Remove”（删除）— 如果选定该选项，将从 MAC 地址表中删除选定的 MAC 地址。

添加静态 MAC 地址

1. 打开“Static MAC Address Table”（静态 MAC 地址表）页面。
2. 单击“Add”（添加）。

   系统将打开“Add Static MAC Address”（添加静态 MAC 地址）页面。
3. 完成字段。
4. 单击“Apply Changes”（应用更改）。

   系统会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设置

1. 打开“Static MAC Address Table”（静态 MAC 地址表）页面。

2. 选择接口。

3. 修改字段。

4. 单击“Apply Changes”（应用更改）。

系统将修改静态 MAC 地址，并更新设备。

从静态地址表中删除静态地址

1. 打开“Static MAC Address Table”（静态 MAC 地址表）页面。

2. 选择一个接口。

3. 单击“Show All”（全部显示）。

系统将打开“Static MAC Address Table”（静态 MAC 地址表）。

4. 选择一个表条目。

5. 选取“Remove”（删除）复选框。

6. 单击“Apply Changes”（应用更改）。

系统将删除选定的静态地址，并更新设备。

使用 CLI 命令配置静态地址参数

下表概括了与“Static MAC Address Table”（静态 MAC 地址表）页面中显示的配置静态地址参数的选项等效的 CLI 命令。

表 7-71. 静态地址的 CLI 命令

CLI 命令	说明
bridge address mac 地址 [permanent | delete-on-reset | delete-on-timeout | secure] {ethernet	将静态 MAC 层的站点源地址添加

interface | port-channel 端口信道号}	至网桥表中。
show bridge address-table [vlan VLAN] [ethernet 接口 | port-channel 端口信道号]	显示网桥传输数据库中的条目。

以下是 CLI 命令的示例。

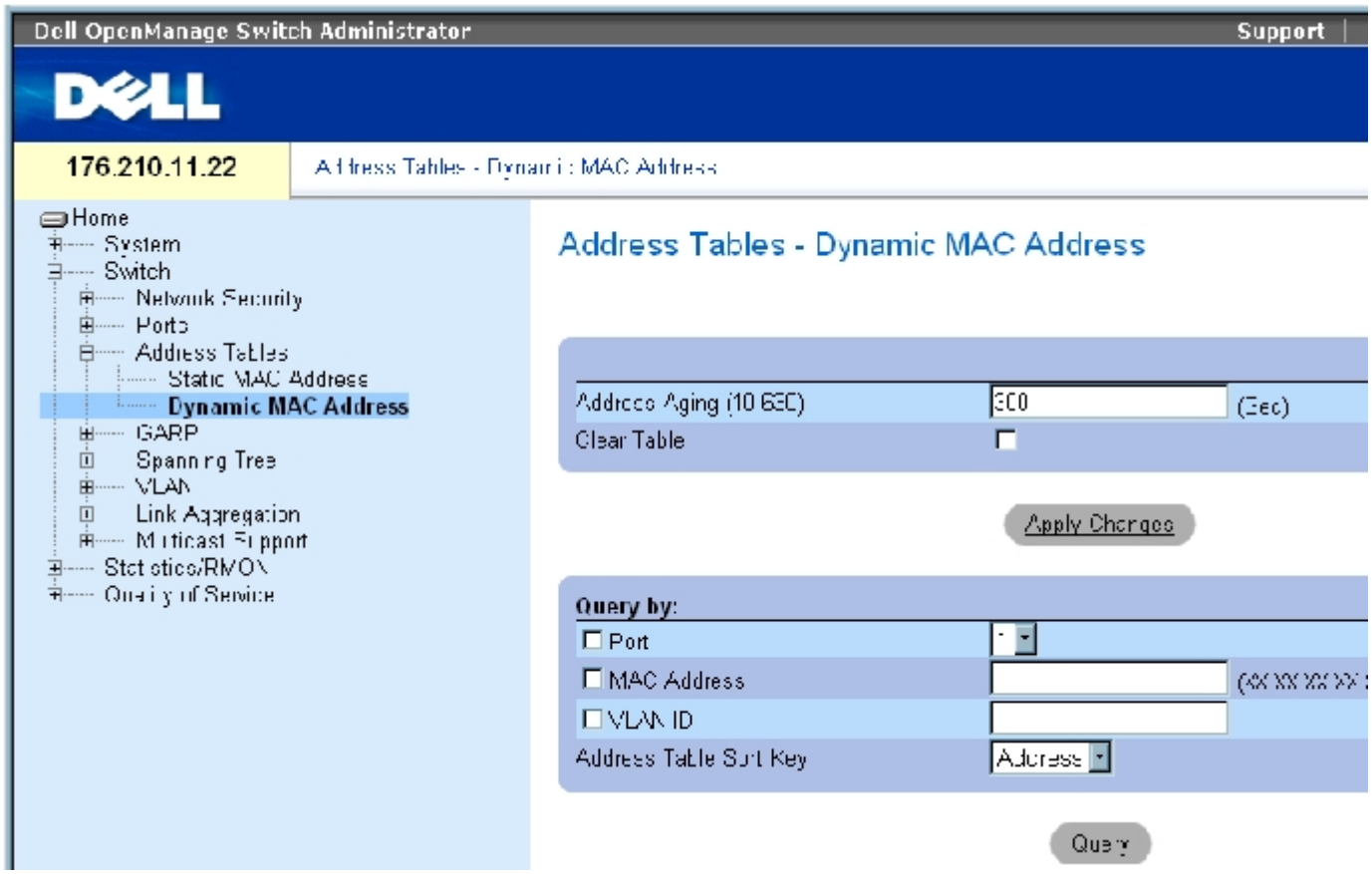
```
console(config-if)#bridge address 00:60:70:4C:73:FF permanent ethernet g8

console# show bridge address-table

Aging time is 300 sec

vlan    mac address         port    type
----    -----------         ----    --------
1       00:60:70:4C:73:FF   1/e8    dynamic
1       00:60:70:8C:73:FF   1/e8    dynamic
200     00:10:0D:48:37:FF   1/e9    static
```

查看动态地址

“Dynamic MAC Address”（动态 MAC 地址）包含用于查询动态地址表中的信息（包括接口类型、MAC 地址、VLAN 和表排序）的信息。传输至存储在地址表中的地址的信息包将被直接传输至那些端口。“Dynamic MAC Address”（动态 MAC 地址）页面还包含有关动态 MAC 地址被删除前存在时间的信息，并包括用于查询和查看动态地址列表的参数。当前地址表包含将信息包直接传输至那些端口所依据的动态地址参数。

要打开“Dynamic MAC Address”（动态 MAC 地址）页面，请在树视图中单击“Switch”（交换机）→“Address Tables”（地址表）→“Dynamic MAC Address”（动态 MAC 地址）。

图 7-20. 动态 MAC 地址



“Dynamic MAC Address” (动态 MAC 地址) 页面包含以下字段：

“Address Aging (10-630)” (地址存在时间 [10-630]) — 指定如果未检测到来自源的通信，在超时之前 MAC 地址在“Dynamic MAC Address” (动态 MAC 地址) 中保留的时间。默认值为 300 秒。

“Clear Table” (清除表) — 如果选取了此项，将清除动态地址表。

“Port” (端口) — 指定要为其查询表的接口。可以选择的端口类型有两种。

“MAC Address” (MAC 地址) — 指定要为其查询表的 MAC 地址。

“VLAN ID” — 要为其查询表的 VLAN ID。

“Address Table Sort Key” (地址表排序关键字) — 指定动态地址表的排序方法。地址表可以按地址、VLAN 或接口排序。

重新定义存在时间

1. 打开“Dynamic MAC Address” (动态 MAC 地址)。
2. 定义“Aging Time” (存在时间) 字段。

3. 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

1. 打开“Dynamic MAC Address”（动态 MAC 地址）。
2. 定义查询“Dynamic Address Table”（动态地址表）所依据的参数。

可以按照“Port”（端口）、“MAC Address”（MAC 地址）或“VLAN ID”查询条目。

3. 单击“Query”（查询）。

将查询“Dynamic MAC Address”（动态 MAC 地址）。

对动态地址表进行排序

1. 打开“Dynamic MAC Address”（动态 MAC 地址）。
2. 从“Address Table Sort Key”（地址表排序关键字）下拉式菜单中选择是按照地址、VLAN ID 还是按照接口对地址进行排序。
3. 单击“Query”（查询）。

将对“Dynamic MAC Address”（动态 MAC 地址）进行排序。

使用 CLI 命令查询并排序动态地址

下表概括了与“Dynamic MAC Address”（动态 MAC 地址）中显示的设置存在时间、查询和排序动态地址的选项等效的 CLI 命令。

表 7-72. 查询和排序的 CLI 命令

CLI 命令	说明

bridge aging-time 秒	设置地址表的存在时间。
show bridge address-table [vlan VLAN] [ethernet 接口 | port-channel 端口信道号]	显示在网桥传输数据库中动态创建的条目的分类。

以下是 CLI 命令的示例：

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

console (config)# end

console# show bridge address-table
```

Aging time is 250 sec

vlan	mac address	port	type
----	----------	----	----
1	00:60:70:4C:73:FF	1/e8	dynamic
1	00:60:70:8C:73:FF	1/e8	dynamic
200	00:10:0D:48:37:FF	1/e8	static

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）的设备。

配置 GARP 时，请确保满足以下要求：

- 离开时间必须大于或等于加入时间的三倍。
- 全部离开时间必须大于离开时间。
- 在第 2 层连接的所有设备上设置同一 GARP 计时器值。如果在第 2 层连接的设备上设置不同的 GARP 计时器，GARP 应用程序将不能成功运行。

要打开“GARP”页面，请在树视图中单击“Switch”（交换机）→“GARP”。

定义 GARP 计时器

“GARP Timers” (GARP 计时器) 页面包含用于在设备上启用 GARP 的字段。要打开“GARP Timers” (GARP 计时器) 页面，请在树视图中单击“Switch” (交换机) → “GARP” → “GARP Timers” (GARP 计时器) 。

图 7-21. GARP 计时器

“GARP Timers” (GARP 计时器) 页面包含以下字段：

“Interface” (接口) — 用于选择端口或 LAG 以编辑 GARP 计时器。

“GARP Join Timer (10 - 2147483640)” (GARP 加入计时器 [10 - 2147483640]) (以毫秒为单位) — 传输 PDU 的时间 (以毫秒为单位) 。默认值为 200 毫秒。

“GARP Leave Timer (10 - 2147483640)” (GARP 离开计时器 [10 - 2147483640]) (以毫秒为单位) — 设备离开其 GARP 状态之前等待的时间 (以毫秒为单位) 。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。即离开时间必须大于或等于加入时间的三倍，默认值为 600 毫秒。

“GARP Leave All Timer (10 - 2147483640)” (GARP 全部离开计时器 [10 - 2147483640]) (以毫秒为单位) — 所有设备离开 GARP 状态之前等待的时间 (以毫秒为单位) 。全部离开时间必须大于离开时间。默认值为 10000 毫秒。

定义 GARP 计时器

1. 打开“GARP Timers” (GARP 计时器) 页面。
2. 选择接口。
3. 完成字段。
4. 单击“Apply Changes” (应用更改) 。

GARP 参数将被保存至设备。

复制 GARP 计时器表中的参数

1. 打开“GARP Timers” (GARP 计时器) 页面。
2. 单击“Show All” (全部显示) 。

系统将打开“GARP Timers Table” (GARP 计时器表) 。

3. 在“Copy Parameters from” (参数复制自) 字段中选择接口类型。
4. 在“Port” (端口) 或“LAG”下拉式菜单中选择一个接口。

此接口的定义将被复制到选定的接口中。请参阅步骤 6。

5. 选取“Copy to” (复制到) 复选框以定义 GARP 计时器定义要复制到的接口，或单击“Select All” (全部选定) 以将定义复制到所有端口或 LAG。
6. 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。

使用 CLI 命令定义 GARP 计时器

下表概括了与“GARP Timers” (GARP 计时器) 页面中显示的用于定义 GARP 计时器的选项等效的 CLI 命令。

表 7-73. GARP 计时器的 CLI 命令

CLI 命令	说明
garp timer {join | leave | leaveall} 计时器值	调整 GARP 应用程序加入、离开和全部离开 GARP 计时器的值。

以下是 CLI 命令的示例：

```
console(config)# interface ethernet 1/e1

console(config-if)# garp timer leave 900

console(config-if)# end

console# show gvrp configuration ethernet 1/e11


GVRP Feature is currently Disabled on the device.

Maximum VLANs: 223
```

Port(s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
1/e11	Disabled	Normal	Enabled	200	900	10000

配置生成树协议

生成树协议 (STP) 提供了树拓扑，用于任意网桥排列。STP 通过在网络中的终端站点之间提供一条路径消除了环路。

主机之间存在备用路由时，将形成环路。扩展网络中的环路可能会造成网桥无限制地传输通信，从而导致通信量增加以及网络效率降低。

设备支持以下生成树版本：

- 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 的详细信息，请参阅定义 STP 全局设置。

- 快速 STP — 检测并使用提供快速生成树聚合的网络拓扑，且不会创建传输环路。如果设备上启用了 RSTP 而相邻设备上启用了 STP，则本地设备使用 STP。

  有关配置快速 STP 的详细信息，请参阅定义快速生成树。

- 多个 STP — 提供分配至任意 VLAN 的信息包的完整连接。多个 STP 基于 RSTP。此外，多个 STP 通过不同 MST 区域传输分配至不同 VLAN 的信息包。如果设备上启用了 MSTP，则 MST 区域将用作单个网桥。但是，如果相邻设备上启用了 RSTP 并且本地设备使用 STP、RSTP 和 MSTP，则这两个设备可以交互操作。

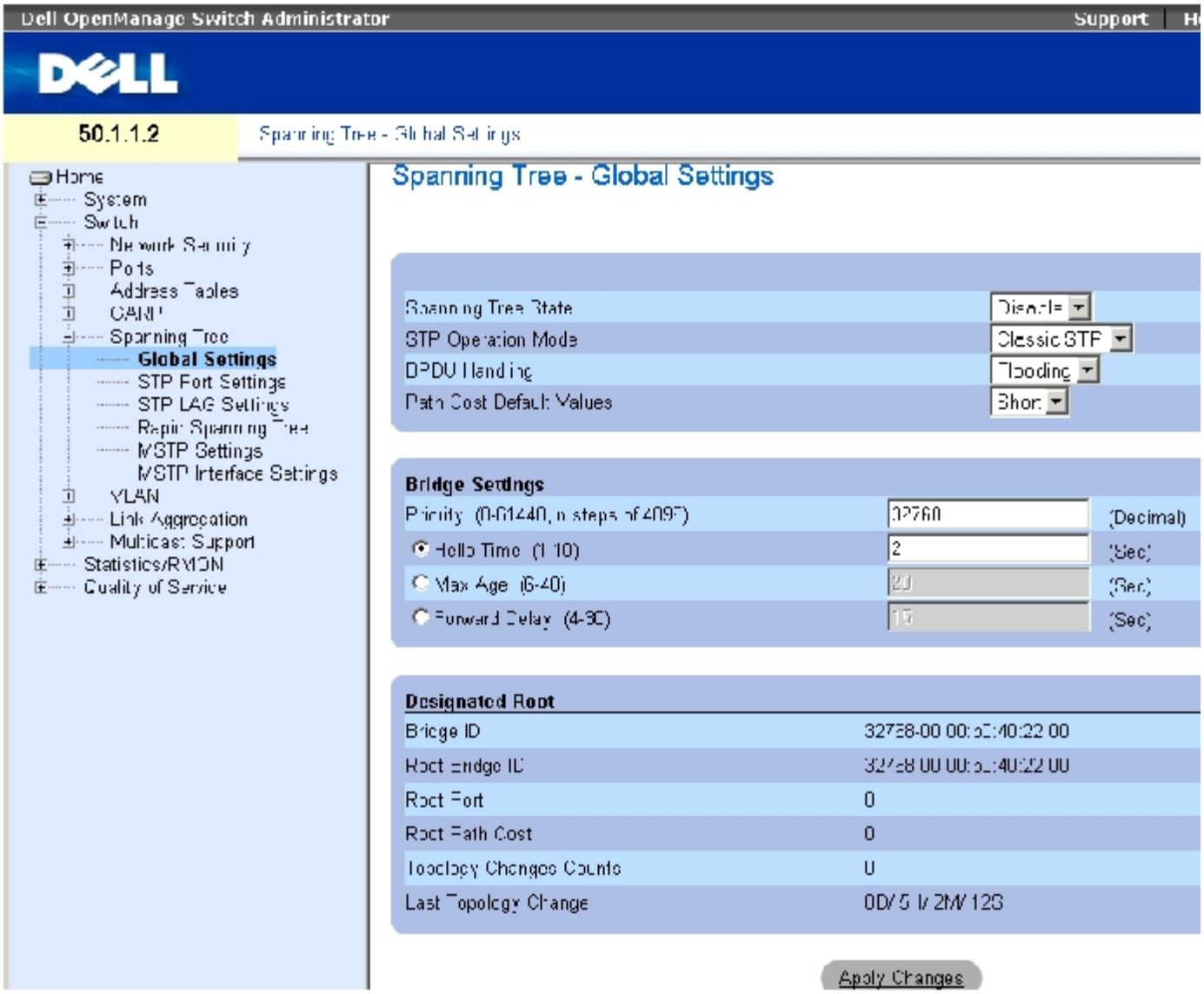
  有关配置多个 STP 的详细信息，请参阅配置多个生成树。

要打开“Spanning Tree”（生成树）页面，请在树视图中单击“Switch”（交换机）→“Spanning Tree”（生成树）。

定义 STP 全局设置

“Spanning Tree Global Settings”（生成树全局设置）页面包含用于在设备上启用 STP 的参数。要打开“Spanning Tree Global Settings”（生成树全局设置）页面，请在树视图中单击“Switch”（交换机）→“Spanning Tree”（生成树）→“Global Settings”（全局设置）。

图 7-22. 生成树全局设置



"Spanning Tree Global Settings" (生成树全局设置) 页面包含以下字段：

"Spanning Tree State" (生成树状态) — 在设备上启用或禁用 STP、快速 STP 或 MSTP。

"STP Operation Mode" (STP 运行模式) — 表示在设备上启用的 STP 的模式。可能的字段值包括：

"Classic STP" (经典 STP) — 在设备上启用经典 STP。这是默认值。

"Rapid STP" (快速 STP) — 在设备上启用快速 STP。

"Multiple STP" (多个 STP) — 在设备上启用多个 STP。

"BPDU Handling" (BPDU 处理) — 确定 STP 在端口/设备上被禁用时如何管理 BPDU 信息包。BPDU 用于传输生成树信息。可能的字段值包括：

"Filtering" (筛选) — 生成树在接口上被禁用时筛选 BPDU 信息包。这是默认值。

“Flooding”（多路发送）— 生成树在接口上被禁用时多路发送 BPDU 信息包。

“Path Cost Default Values”（路径成本默认值）— 指定给 STP 端口分配默认路径成本的方法。可能的字段值包括：

“Short”（短）— 指定端口路径成本为 1 至 65,535。这是默认值。

“Long”（长）— 指定端口路径成本为 1 至 200,000,000。

分配至接口的默认路径成本根据选定方法的不同而有所不同：

接口	长	短
LAG	20,000	4
1000 Mbps	20,000	4
100 Mbps	200,000	19
10 Mbps	2,000,000	100

“Priority (0-65535)”（优先级 [0-65535]）— 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，优先级值最低的设备将成为根网桥。默认值为 32768。以 4096 为增量提供端口优先级值。例如，4096、8192、12288 等。

“Hello Time (1-10)”（问候间隔 [1-10]）— 指定设备的问候间隔。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 秒。

“Max Age (6-40)”（最长存在时间 [6-40]）— 指定设备的最长存在时间。最长存在时间表示网桥在发送配置信息之前等待的时间（以秒为单位）。默认的最长存在时间为 20 秒。

“Forward Delay (4-30)”（传输延迟 [4-30]）— 指定设备的传输延迟时间。传输延迟时间表示在传输信息包之前网桥处于侦听和学习状态的时间（以秒为单位）。默认值为 10 秒。

“Bridge ID”（网桥 ID）— 标识网桥优先级和 MAC 地址。

“Root Bridge ID”（根网桥 ID）— 标识根网桥优先级和 MAC 地址。

“Root Port”（根端口）— 表示提供从此网桥至根网桥的最低成本路径的端口号。当网桥不是根网桥时，此选项非常重要。

“Root Path Cost”（根路径成本）— 从此网桥至根网桥的路径成本。

“Topology Changes Counts”（拓扑更改计数）— 指定发生的 STP 状态更改的总次数。

“Last Topology Change”（上次拓扑更改）— 表示自网桥初始化或重设以及上次拓扑更改以来经过的时间。时间以 D/H/M/S 格式显示，例如 2D/5H/10M/4S。

定义 STP 全局参数

1. 打开该页面。
2. 在“Spanning Tree State”（生成树状态）字段中选择“Enable”（启用）。
3. 在“STP Operation Mode”（STP 运行模式）字段中选择“STP”模式，并定义网桥设置。
4. 单击“Apply Changes”（应用更改）。

系统将在设备上启用 STP。

修改 STP 全局参数

1. 打开该页面。
2. 定义对话框中的字段。
3. 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

下表概括了与“Spanning Tree Global Settings”（生成树全局设置）页面中显示的用于定义 STP 全局参数的选项等效的 CLI 命令。

表 7-74. STP 全局参数的 CLI 命令

CLI 命令	说明
spanning-tree	启用生成树功能。
spanning-tree mode {**stp**| **rstp** | **mstp**}	配置生成树协议的模式。

spanning-tree priority 优先级	配置生成树优先级。
spanning-tree hello-time 秒	配置生成树网桥问候间隔，即设备向其它设备广播问候信息的频率。
spanning-tree max-age 秒	配置生成树网桥的最长存在时间。
spanning-tree forward-time 秒数	配置生成树网桥的传输时间，即端口在进入传输状态之前保持侦听和记忆状态的时间。
show spanning-tree [**ethernet** 接口 | **port-channel** 端口信道号] [**instance** 实例 **ID**]	显示生成树配置。
show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** 实例 **ID**]	显示有关活动或锁定端口的详细生成树信息。
show spanning-tree mst- configuration	显示生成树 MST 配置标识符。

以下是 CLI 命令的示例：

```
console(config)# spanning-tree

console(config)# spanning-tree mode rstp

console(config)# spanning-tree priority 12288

console(config)# spanning-tree hello-time 5

console(config)# spanning-tree max-age 12

console(config)# spanning-tree forward-time 25

console(config)#exit

console# show spanning-tree
```

Spanning tree enabled mode MSTP							
Default port cost method:short							
Gathering information							
###### MST 0 Vlans Mapped:		16-4094					
CST Root ID Priority 20480							
	Address	00:30:ab:00:00:08					
	Path Cost	4					
	Root Port	ch2					

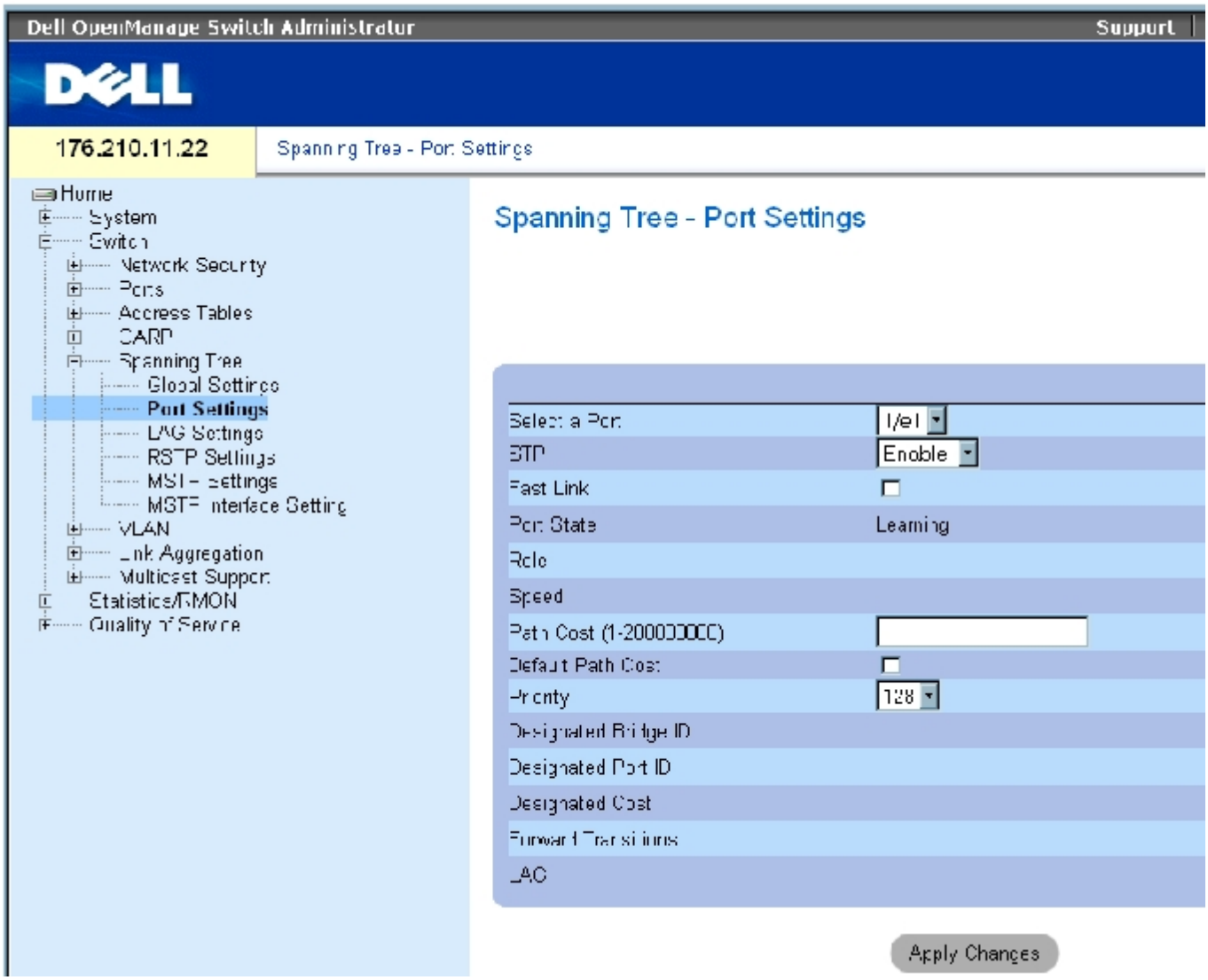
	This switch is the IST master						
	Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec						
Bridge ID Priority			32768				
	Address		00:00:00:16:00:64				
	Max hops		20				
Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
----	-----	-------	----	---	----	-------	----
1/e2	enabled	128.2	100	DSBL	Dsbl	No	P2p Intr
1/e3	enabled	128.3	100	DSBL	Dsbl	No	P2p Intr
1/e4	enabled	128.4	100	DSBL	Dsbl	No	P2p Intr
1/e5	enabled	128.5	19	FRW	Desg	Yes	P2p Intr
1/e6	enabled	128.6	100	DSBL	Dsbl	No	P2p Intr
1/e7	enabled	128.7	100	DSBL	Dsbl	No	P2p Intr
1/e8	enabled	128.8	100	DSBL	Dsbl	No	P2p Intr
1/e9	enabled	128.9	100	DSBL	Dsbl	No	P2p Intr
1/e10	enabled	128.10	100	DSBL	Dsbl	No	P2p Intr
1/e11	enabled	128.11	19	DSBL	Desg	Yes	P2p Intr
console# show spanning-tree active							
Spanning tree enabled mode MSTP							
Default port cost method:short							
Gathering information							
###### MST 0 Vlans Mapped: 16-4094							
CST Root ID Priority 20480							
	Address		00:30:ab:00:00:08				
	Path Cost		4				
	Root Port		ch2				
	This switch is the IST master						

	Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec						
Bridge ID Priority			32768				
	Address		00:00:00:16:00:64				
	Max hops		20				
Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
----	-----	-------	----	---	----	-------	----
1/e5	enabled	128.2	19	FRW	Desg	Yes	P2p Intr
1/e7	enabled	128.7	19	DSCR	Altn	No	P2p Bound (STP)
1/e11	enabled	128.11	19	FRW	Desg	Yes	P2p Intr
1/e15	enabled	128.15	19	FRW	Desg	No	P2p Intr
1/e22	enabled	128.22	19	FRW	Desg	Yes	P2p Intr

定义 STP 端口设置

使用“Spanning Tree Port Settings”（生成树端口设置）页面可以给各个端口设定 STP 属性。要打开“Spanning Tree Port Settings”（生成树端口设置）页面，请在树视图中单击“Switch”（交换机）→“Spanning Tree”（生成树）→“Port Settings”（端口设置）。

图 7-23. 生成树端口设置



“Spanning Tree Port Settings”（生成树端口设置）页面包含以下字段：

“Select a Port”（选择端口）— 指定将在其上修改 STP 设置的端口号。

“STP”— 在端口上启用或禁用 STP。

“Fast Link”（快速链路）— 如果选取此选项，将为端口启用快速链路模式。如果为端口启用了快速链路模式，则当端口链路良好时，“Port State”（端口状态）将自动被置入“Forwarding”（传输）状态。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）— 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传输操作。可能的端口状态包括：

“Disabled”（已禁用）— 当前已在端口上禁用 STP。端口在记忆 MAC 地址的同时传输通信。

“Blocking”（阻塞）— 端口当前已被阻塞，无法用于传输通信或记忆 MAC 地址。启用“Classic STP”（经典 STP）时，将显

示“Blocking”（阻塞）。

“Listening”（侦听）— 端口当前处于侦听模式。端口既不能传输通信，也不能记忆 MAC 地址。

“Learning”（记忆）— 端口当前处于记忆模式。端口不能传输通信，但可以学习新的 MAC 地址。

“Forwarding”（传输）— 端口当前处于传输模式。端口可以传输通信，也可以学习新的 MAC 地址。

“Role”（角色）— 表示由 STP 算法分配的提供 STP 路径的端口角色。可能的字段值包括：

“Root”（根）— 提供最低成本路径以将信息包传输给根交换机。

“Designated”（指定）— 表示指定的交换机连接至 LAN 所通过的端口。

“Alternate”（备用）— 通过根接口向根交换机提供备用路径。

“Backup”（备份）— 提供去往生成树树叶的指定的端口路径的备份路径。仅当两个端口通过点对点链路连接在一个环路中时，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）— 表示端口未加入生成树。

“Speed”（速率）— 端口运行的速率。

“Path Cost (1-200000000)”（路径成本 [1-200000000]）— 端口在根路径成本中所占的比例。可以将路径成本调整为较高或较低的值，并且在路径被重定路线时可以使用路径成本来传输通信。

“Default Path Cost”（默认路径成本）— 默认路径成本。长路径成本的默认值包括：

“Ethernet”（以太网）- 2,000,000

“Fast Ethernet”（快速以太网）- 200,000

“Gigabit Ethernet”（吉位以太网）- 20,000

短路径成本的默认值包括：

“Ethernet”（以太网）- 100

“Fast Ethernet”（快速以太网）- 19

“Gigabit Ethernet”（吉位以太网）- 4

“Priority (0-240, in steps of 16)”（优先级 [0-240，步进为 16]）— 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。优先级值介于 0 至 240 之间。以 16 为增量提供优先级值。

“Designated Bridge ID”（指定网桥 ID）— 指定网桥的网桥优先级和 MAC 地址。

“Designated Port ID”（指定端口 ID）— 指定端口的优先级和接口。

“Designated Cost”（指定成本）— 参与 STP 拓扑的端口的成本。如果 STP 检测到环路，则端口成本越低，被阻塞的可能性越小。

“Forward Transmission”（传输转换）— 端口从“Forwarding”（传输）状态变为“Blocking”（阻塞）状态的次数。

“LAG”— 端口所连接的 LAG。

在端口上启用 STP

1. 打开“Spanning Tree Port Settings”（生成树端口设置）页面。
2. 选择端口。
3. 在“STP”字段中选择“Enabled”（已启用）。
4. 定义“Fast Link”（快速链路）、“Path Cost”（路径成本）和“Priority”（优先级）字段。
5. 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

1. 打开“Spanning Tree Port Settings”（生成树端口设置）页面。
2. 选择端口。
3. 修改相关的字段。

4. 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

1. 打开“Spanning Tree Port Settings”（生成树端口设置）页面。
2. 单击“Show All”（全部显示）。

系统将打开“STP Port Table”（STP 端口表）。

使用 CLI 命令定义 STP 端口设置

下表概括了与“STP Port Settings”（STP 端口设置）页面中显示的用于定义 STP 端口参数的选项等效的 CLI 命令。

表 7-75. STP 端口设置的 CLI 命令

CLI 命令	说明
spanning-tree disable	禁用特定端口上的生成树。
spanning-tree cost 成本	配置端口的生成树成本比例。
spanning-tree port-priority 优先级	配置端口优先级。
show **spanning-tree** [**ethernet** 接口 **| port-channel** 端口信道号][**instance** 实例 **ID**]	显示生成树配置。
spanning-tree portfast	启用 PortFast 模式。
show spanning-tree [detail] [**active | blockedports**] [**instance** 实例 **ID**]	显示有关活动或锁定端口的详细生成树信息。
show spanning-tree mst- configuration	显示生成树 MST 配置标识符。

以下是 CLI 命令的示例：

```
console> enable

console# configure

Console(config)# interface ethernet 1/e1

Console(config-if)# spanning-tree disable

Console(config-if)# spanning-tree cost 35000

Console(config-if)# spanning-tree port-priority 96

Console(config-if)# spanning-tree portfast

Console(config-if)# exit

Console (config)# exit

Console# show spanning-tree ethernet 1/e15
```

Port 1/e15 enabled					
State:forwarding			Role:designated		
Port id: 128.15			Port cost: 19		
Type:P2p (configured:Auto) Internal Port Fast:No (configured:No)					
Designated bridge Priority : 32768			Address: 00:00:00:16:00:64		
Designated port id: 128.15			Designated path cost: 4		
Guard root:Disabled					
Number of transitions to forwarding state: 2					
BPDU:sent 483, received 1037					

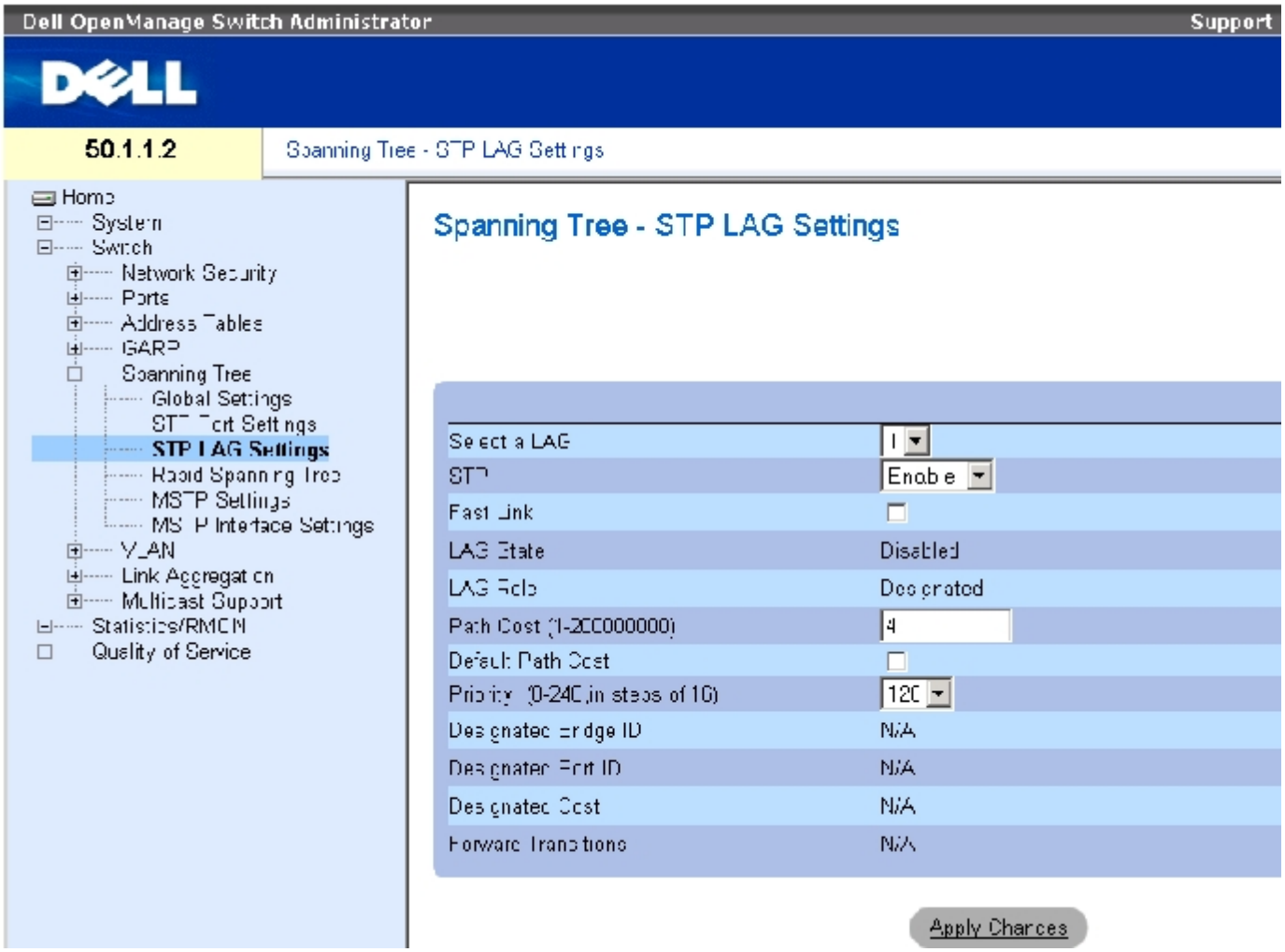
```
console# show spanning-tree ethernet 1/e15 instance 12
```

Port 1/e15 enabled					
State:discarding			Role:alternate		
Port id: 128.15			Port cost: 19		
Type:P2p (configured:Auto) Internal Port Fast:No (configured:No)					
Designated bridge Priority : 32768			Address:00:00:b0:07:07:49		
Designated port id: 128.11			Designated path cost: 0		
Guard root:Disabled					
Number of transitions to forwarding state: 3					
BPDU:sent 482, received 1035					

定义 STP LAG 设置

使用“Spanning Tree LAG Settings”（生成树 LAG 设置）页面可以设定 STP 聚合端口参数。要打开“Spanning Tree LAG Settings”（生成树 LAG 设置）页面，请在树视图中单击“Switch”（交换机）→“Spanning Tree”（生成树）→“LAG Settings”（LAG 设置）。

图 7-24. 生成树 LAG 设置



“Spanning Tree LAG Settings”（生成树 LAG 设置）页面包含以下字段：

“Select a LAG”（选择 LAG）— 要修改其 STP 设置的 LAG 号。

“STP”— 在 LAG 上启用或禁用 STP。

“Fast Link”（快速链路）— 为 LAG 启用快速链路模式。如果为 LAG 启用了快速链路模式，则当 LAG 良好时，“LAG State”（LAG 状态）将自动被置入“Forwarding”（传输）状态。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。

“LAG State”（LAG 状态）— LAG 的当前 STP 状态。如果已启用该选项，LAG 状态将确定对通信所采取的传输操作。如果网桥发现故障 LAG，该 LAG 将被置入“Broken”（断开）状态。可能的 LAG 状态包括：

“Disabled”（已禁用）— 当前已在 LAG 上禁用 STP。LAG 在记忆 MAC 地址的同时传输通信。

“Blocking”（阻塞）— LAG 已被阻塞，无法用于传输通信或记忆 MAC 地址。

“RSTP Discarding State”（RSTP 丢弃状态）— 在此状态下，端口不记忆 MAC 地址，也不传输帧。

此状态是阻塞状态和从 STP (802.1.D) 中引入的侦听状态的结合。

“Listening”（侦听）— LAG 处于侦听模式，无法传输通信或记忆 MAC 地址。

“Learning”（记忆）— LAG 处于记忆模式，无法传输通信，但可以记忆新的 MAC 地址。

“Forwarding”（传输）— LAG 当前处于传输模式，可以传输通信和记忆新的 MAC 地址。

“Broken”（断开）— LAG 当前出现故障，无法用于传输通信。

“LAG Role”（LAG 角色）— 表示由 STP 算法分配的提供 STP 路径的 LAG 角色。可能的字段值包括：

“Root”（根）— 提供最低成本路径以将信息包传输给根交换机。

“Designated”（指定）— 表示指定的交换机连接至 LAN 所通过的 LAG。

“Alternate”（备用）— 通过根接口向根交换机提供备用 LAG。

“Backup”（备份）— 提供去往生成树树叶的指定的端口路径的备份路径。仅当两个端口通过点对点链路连接在一个环路中时，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 LAG 未加入生成树。

“Path Cost (1-200000000)”（路径成本 [1-200000000]）— LAG 在根路径成本中所占的比例。可以将路径成本调整为较高或较低的值，并且在路径被重定路线时可以使用路径成本来传输通信。路径成本可以是 1 至 200000000 之间的值。

“Default Path Cost”（默认路径成本）— 表示是否使用默认路径成本。可能的 LAG 路径成本默认值包括：

“Long Method for LAG”（用于 LAG 的长方法）— 20,000

“Short Method for LAG”（用于 LAG 的短方法）— 4

“Priority (0-240, in steps of 16)”（优先级 [0-240，步进为 16]）— LAG 的优先级值。当网桥具有环路端口时，优先级值用于确定 LAG 的选择。优先级值介于 0 至 240 之间，步进为 16。

“Designated Bridge ID”（指定网桥 ID）— 指定网桥的优先级和 MAC 地址。

“Designated Port ID”（指定端口 ID）— 选定接口的 ID。

“Designated Cost”（指定成本）— 参与 STP 拓扑的端口的成本。如果 STP 检测到环路，则端口成本越低，被阻塞的可能性越小。

“Forward Transitions”（传输转换）—“LAG State”（LAG 状态）从“Forwarding”（传输）状态变为“Blocking”（阻塞）状态的次数。

修改 LAG STP 参数

1. 打开“Spanning Tree LAG Settings”（生成树 LAG 设置）页面。
2. 从“Select a LAG”（选择 LAG）下拉式菜单中选择一个 LAG。
3. 根据需要修改字段。
4. 单击“Apply Changes”（应用更改）。

系统将修改 STP LAG 参数，并更新设备。

使用 CLI 命令定义 STP LAG 设置

下表包含用于定义 STP LAG 设置的 CLI 命令。

表 7-76. STP LAG 设置的 CLI 命令

CLI 命令	说明
`spanning-tree`	启用生成树。
`spanning-tree disable`	禁用特定 LAG 上的生成树。
`spanning-tree cost` 成本	配置 LAG 的生成树成本比例。

`spanning-tree port-priority` 优先级	配置端口优先级。
`show spanning-tree [`**`ethernet`** 接口 `|` **`port-channel`** 端口信道号`][`**`instance`** 实例 **`ID`**`]`	显示生成树配置。
`show spanning-tree [detail] [active	blockedports] [`**`instance`** 实例 **`ID`**`]`	显示有关活动或锁定端口的详细生成树信息。

以下是 CLI 命令的示例：

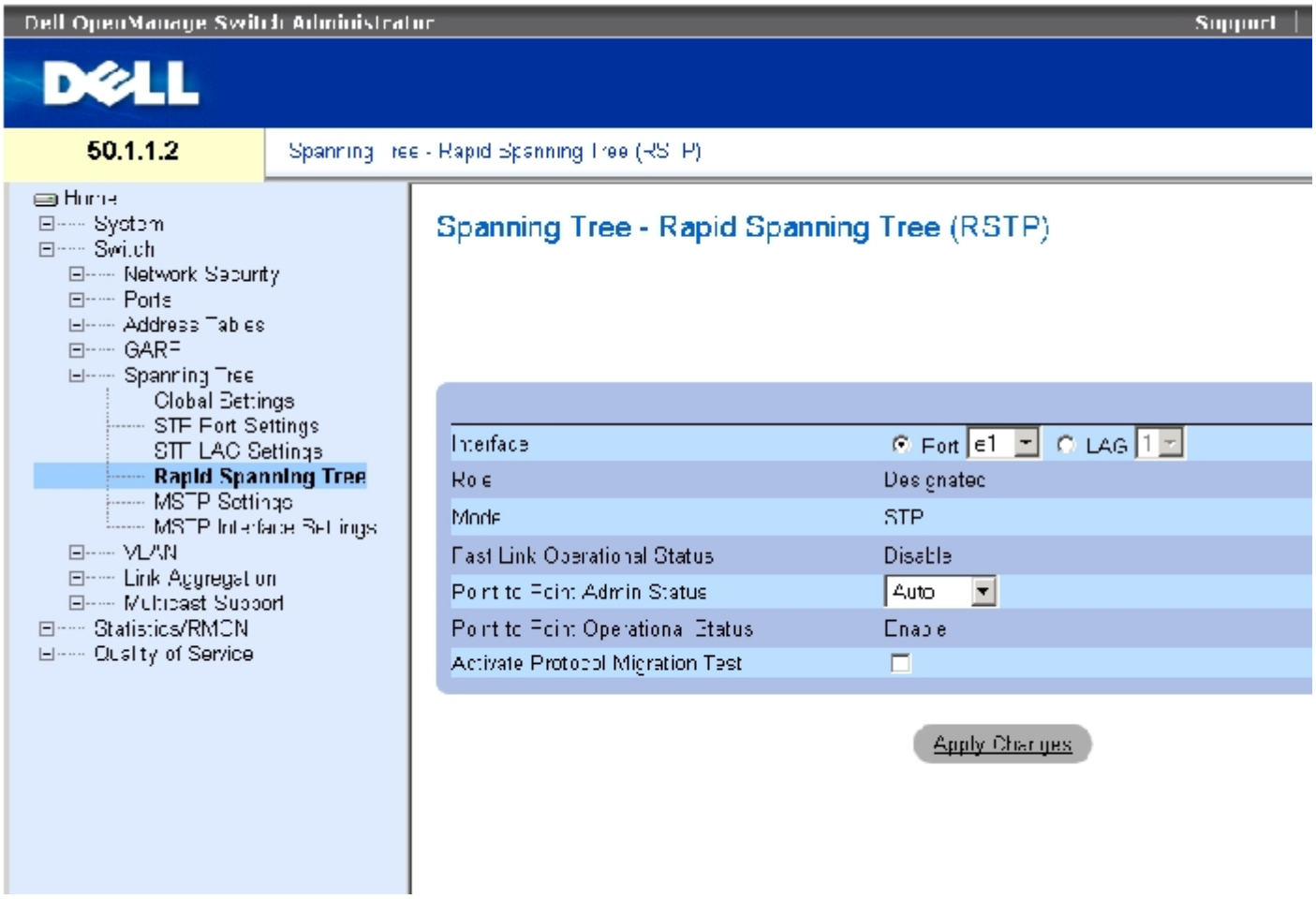
```
console(config)# interface
port-channel 1

console(config-if)#
spanning-tree disable

console(config-if)#
spanning-tree cost 35000

console(config-if)#
spanning-tree port-
priority 96

console(config-if)#
spanning-tree portfast
```

定义快速生成树

虽然经典生成树可以防止普通网络拓扑中出现第 2 层传输环路，但聚合需要花费 30 至 60 秒。该延迟将留出时间以检测可能存在的环路，并传播状态更改。

快速生成树协议 (RSTP) 可以检测并使用允许生成树快速聚合的网络拓扑，且不会创建传输环路。要打开“Rapid Spanning Tree (RSTP)”（快速生成树 [RSTP]）设置页面，请在树视图中单击“Switch”（交换机）→“Spanning Tree”（生成树）→“Rapid Spanning Tree”（快速生成树）。

图 7-25. 快速生成树 (RSTP) 设置



生成树 RSTP 页面包含以下字段：

“Interface”（接口）— 可以查看和编辑其 RSTP 设置的端口或 LAG。

“State”（状态）— 禁用选定接口的 RSTP 状态。

“Role”（角色）— 表示由 STP 算法分配的以便提供 STP 路径的端口角色。可能的字段值包括：

“Root”（根）— 提供最低成本路径以将信息包传输给根交换机。

“Designated”（指定）— 表示指定的交换机连接至 LAN 所通过的端口或 LAG。

“Alternate”（备用）— 通过根接口向根交换机提供备用路径。

“Backup”（备份）— 提供去往生成树树叶的指定的端口路径的备份路径。仅当两个端口通过点对点链路连接在一个环路中时，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）— 表示端口未加入生成树。

“Mode”（模式）— 表示当前的生成树模式。生成树模式在“Spanning Tree Global Settings”（生成树全局设置）页面中选择。可能的字段值包括：

“Classic STP”（经典 STP）— 表示在设备上启用经典 STP。

“Rapid STP”（快速 STP）— 表示在设备上启用快速 STP。

“Multiple STP”（多个 STP）— 表示在设备上启用多个 STP。

“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。如果为接口启用了快速链路，则接口将自动被置入传输状态。

“Point-to-Point Admin Status”（点对点管理状态）— 允许或禁止设备建立点对点链路，或为设备指定该选项以自动建立点对点链路。

要建立通过点对点链路的通信，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按照 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进行了配置，则可以通过链路发送来自每个网络层协议的信息包。在显式 LCP 或 NCP 信息包关闭链路或发生某个外部事件之前，链路保持配置为进行通信的状态。这是实际的交换机端口链路类型。它可能与管理状态不同。

“Point-to-Point Operational Status”（点对点运行状态）— 点对点运行状态。

“Activate Protocol Migrational”（激活协议迁移）— 如果选取该选项，将允许 PPP 发送链路控制协议（LCP）信息包配置和检测数据链路。

定义 RSTP 参数

1. 打开“Spanning Tree RSTP Settings”（生成树 RSTP 设置）页面。
2. 选择接口。
3. 定义字段。
4. 单击“Apply Changes”（应用更改）。

系统将定义 RSTP 参数，并更新设备。

显示快速生成树（RSTP）表

1. 打开“Rapid Spanning Tree (RSTP)”（快速生成树 [RSTP]）页面。

2. 单击“Show All”（全部显示）。

   系统将打开“Rapid Spanning Tree (RSTP) Table”（快速生成树 [RSTP] 表）。

使用 CLI 命令定义快速 STP 参数

下表概括了与“Rapid Spanning Tree (RSTP)”（快速生成树 [RSTP]）中显示的定义快速 STP 参数的选项等效的 CLI 命令。

表 7-77. RSTP 设置的 CLI 命令

CLI 命令	说明
spanning-tree link-type{point-to-point |shared}	代替默认链路类型设置。
spanning tree mode {stp | rstp | mstp}	配置当前运行的生成树协议。
clear spanning-tree detected-protocols [ethernet 接口 | port-channel 端口信道号]	重新启动协议迁移进程。
show spanning-tree [ethernet interface | port-channel port-channel-number]	显示生成树配置。

以下是 CLI 命令的示例：

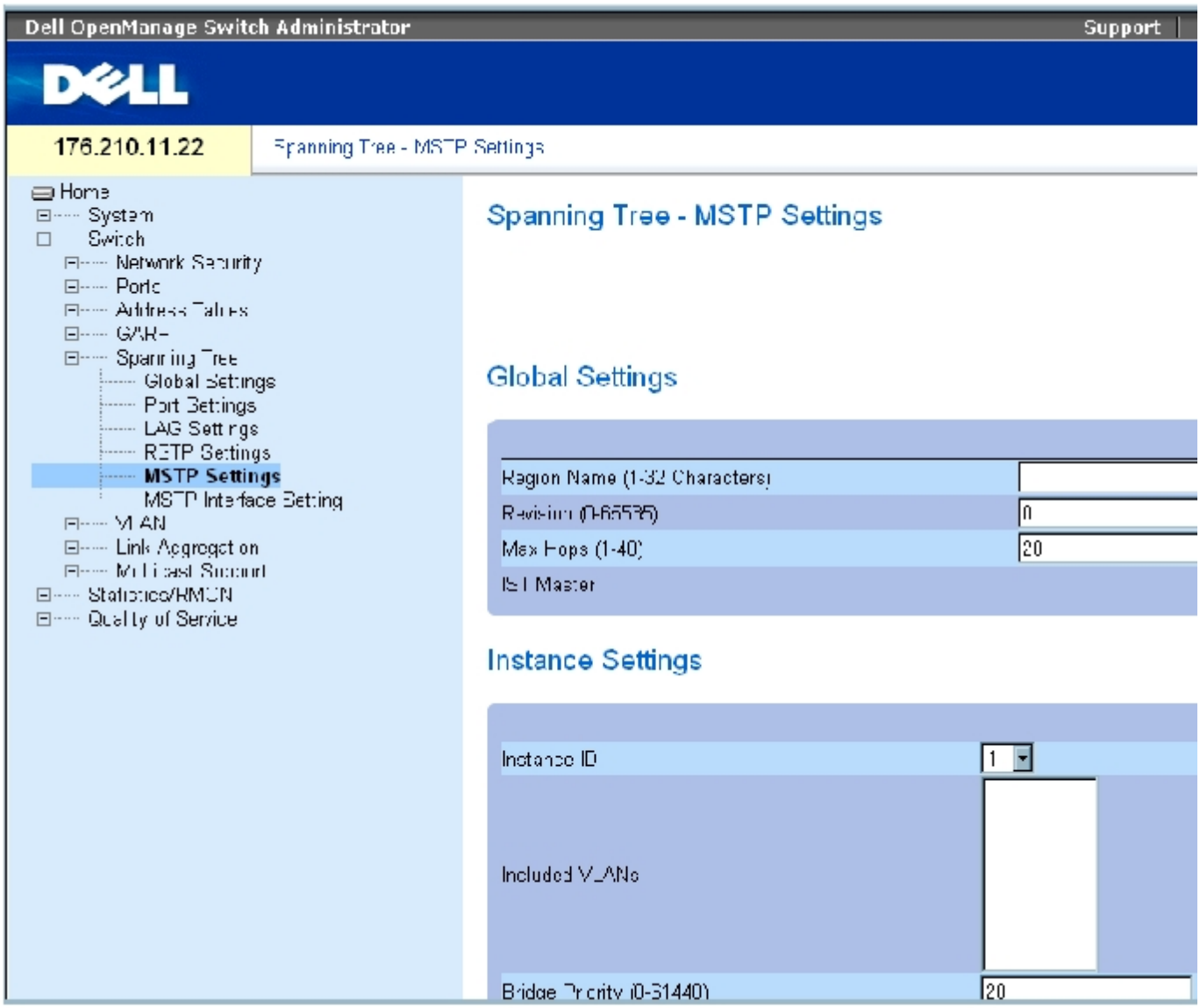
```
console(config)# interface ethernet 1/e5
console(config-if)# spanning-tree link-type shared
console(config-if)# spanning tree mode rstp
```

配置多个生成树

MSTP 操作将 VLAN 映射至 STP 实例中。多个生成树提供了不同的负载平衡方案。例如，一个 STP 实例中的端口 A 处于阻塞状态时，另一个 STP 实例中的相同端口将处于传输状态。

此外，分配至不同 VLAN 的信息包将在多个生成树区域（MST 区域）内部沿不同路径发送。区域为一个或多个可用于传输帧的多个生成树网桥。要打开“MSTP Settings”（MSTP 设置）页面，请在树视图中单击“Switch”（交换机）→“Spanning Tree”（生成树）→“MSTP Settings”（MSTP 设置）。

图 7-26. MSTP 设置



“MSTP Settings” (MSTP 设置) 页面包含以下字段：

“Region Name (1-32 Characters)” (区域名称 [1 至 32 个字符]) — 表示用户定义的 MSTP 区域名称。

“Revision (0-65535)” (版本 [0-65535]) — 定义标识当前 MST 配置版本的无符号 16 位数字。版本号是 MST 配置所需的一部分。可能的字段范围是 0 至 65535。

“Max Hops (1-40)” (最大路程段 [1-40]) — 定义在丢弃 BPDU 以前特定区域中所出现的路程段总数。丢弃 BPDU 后，端口信息将过期。可能的字段范围为 1 至 40。字段默认值为 20 个路程段。

“IST Master” (主 IST) — 表示内部生成树的主 ID。主 IST 为实例 0 的根。

“Instance ID” (实例 ID) — 定义 MSTP 实例。字段范围为 1 至 15。

“Included VLANs”（包括的 VLAN）— 显示映射至选定实例的 VLAN。每个 VLAN 属于一个实例。

“Bridge Priority (0-61440)”（网桥优先级 [0-61440]）— 指定选定的生成树实例设备优先级。字段范围为 0 至 61440，步进为 4096。

“Designated Root Bridge ID”（指定根网桥 ID）— 表示选定实例的根网桥的 ID。

“Root Port”（根端口）— 表示选定实例的根端口。

“Root Path Cost”（根路径成本）— 表示选定实例的路径成本。

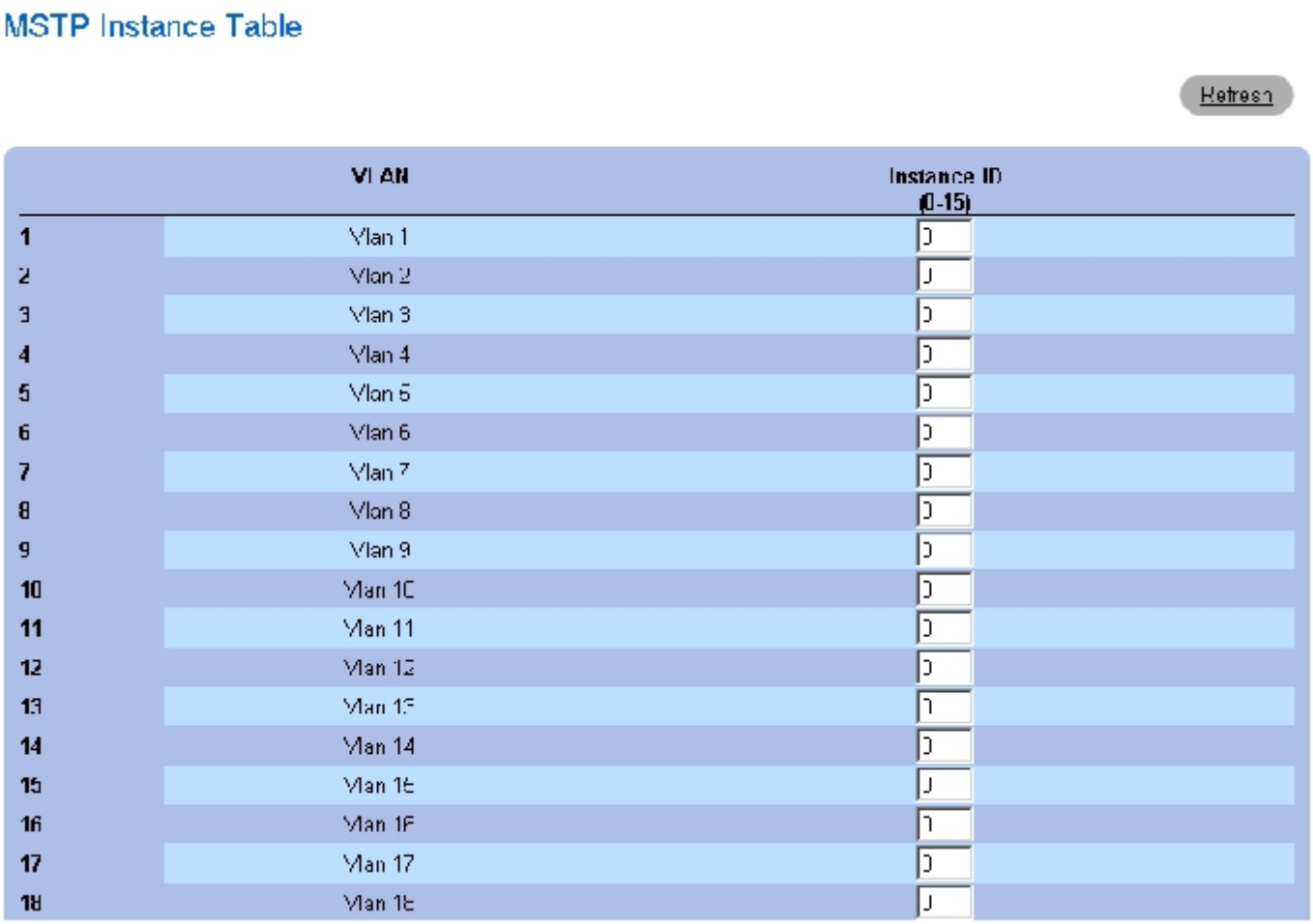
“Bridge ID”（网桥 ID）— 表示选定实例的网桥 ID。

“Remaining Hops”（剩余路程段）— 表示距下一个目的地的剩余路程段数。

显示“MSTP Instance Table”（MSTP 实例表）

1. 打开“Spanning Tree MSTP Settings”（生成树 MSTP 设置）页面。
2. 单击“Show All”（全部显示）以打开“MSTP Instance Table”（MSTP 实例表）。

图 7-27. MSTP 实例表



使用 CLI 命令定义 MST 实例

下表概括了与“Spanning Tree MSTP Settings” (生成树 MSTP 设置) 页面中显示的用于定义 MST 实例组的选项等效的 CLI 命令。

表 7-78. MSTP 实例的 CLI 命令

CLI 命令	说明
`spanning-tree mst configuration`	进入 MST 配置模式。
`instance instance-id {add | remove} vlan vlan-range`	将 VLAN 映射到 MST 实例。
`name string`	设置配置名称。
`revision value`	设置配置版本号
`spanning-tree mst instance-id port- priority priority`	设置端口的优先级。
`spanning-tree mst instance-id priority priority`	为指定的生成树实例设置设备优先级。
`spanning-tree mst max- hops hop-count`	设置丢弃 BPDU 且端口信息过期以前 MST 区域中的路程段数。

spanning-tree mst instance-id **cost** cost	为 MST 计算设置端口的路径成本
exit	退出 MST 区域配置模式并应用配置更改。
abort	退出 MST 区域配置模式而不应用配置更改。
show {current | pending}	显示当前或挂起的 MST 区域配置。

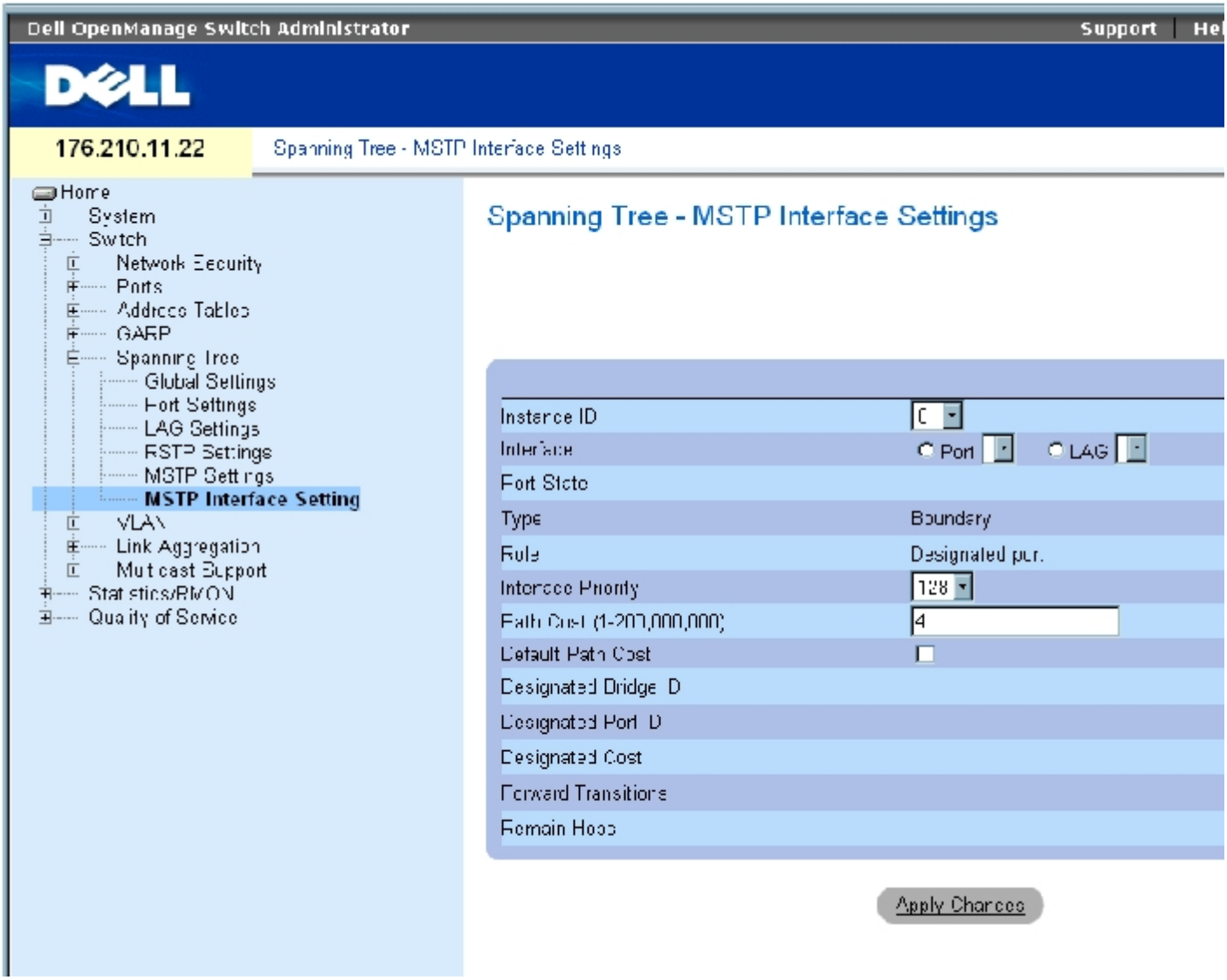
以下是 CLI 命令的示例：

```
console(config)# spanning-tree mst configuration
console(config-mst)# instance 1 add vlan 10-20
console(config-mst)# name region1
console(config-mst)# revision 1
console(config)# spanning-tree mst configuration
console(config-mst)# instance 2 add vlan 21-30
console(config-mst)# name region1
console(config-mst)# revision 1
console(config-mst)# show pending
Pending MST configuration
Name:Region1
Revision: 1
Instance Vlans Mapped
-------- ------------
0 1-9,31-4094
1 10-20
2 21-30
```

定义 MSTP 接口设置

“MSTP Interface Settings” (MSTP 接口设置) 页面包含用于将 MSTP 设置分配至特定接口的参数。要打开“MSTP Interface Settings” (MSTP 接口设置) 页面，请在树视图中单击“Switch” (交换机) → “Spanning Tree” (生成树) → “MSTP Interface Settings” (MSTP 接口设置) 。

图 7-28. 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) — 列出设备上配置的 MSTP 实例。可能的字段范围是 1 至 15。

“Interface” (接口) — 将端口或 LAG 分配至选定的 MSTP 实例。

“Port State” (端口状态) — 表示在特定实例中是启用还是禁用端口。

“Type” (类型) — 表示 MSTP 是将端口视为点对点端口还是视为连接至集线器的端口，以及端口是 MST 区域的内部端口还是边界端口。主端口提供从 MSTP 区域到远端 CIST 根的连接。边界端口将 MST 网桥连接至远端区域中的 LAN。如果端口为边界端口，它还可以表示链路另一端的设备是以 RSTP 模式还是以 STP 模式工作。

“Role” (角色) — 表示由 STP 算法分配的以便提供 STP 路径的端口角色。可能的字段值包括：

“Root”（根）— 提供最低成本路径以将信息包传输给根设备。

“Designated”（指定）— 表示指定的设备连接至 LAN 所通过的端口或 LAG。

“Alternate”（备用）— 通过根接口向根设备提供备用路径。

“Backup”（备份）— 提供去往生成树树叶的指定的端口路径的备份路径。仅当两个端口通过点对点链路连接在一个环路中时，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）— 表示端口未加入生成树。

“Interface Priority (0-240,in steps of 16)”（接口优先级 [0-240，步进为 16]）— 定义指定实例的接口优先级。默认值为 128。

“Path Cost”（路径成本）— 表示端口在生成树实例中所占的比例。范围应始终为 1 至 200,000,000。

“Default Path Cost”（默认路径成本）— 表示根据“Spanning Tree Global Settings”（生成树全局设置）页面上选择的方法分配默认路径成本。

“Designated Bridge ID”（指定网桥 ID）— 将链路或共享 LAN 连接至根的网桥 ID 号。

“Designated Port ID”（指定端口 ID）— 将链路或共享 LAN 连接至根的指定网桥上的端口 ID 号。

“Designated Cost”（指定成本）— 从链路或共享 LAN 至根的路径成本。

“Forward Transitions”（传输转换）— 端口变为“forwarding”（传输）状态的次数。

“Remain Hops”（剩余路程段）— 表示距下一个目的地的剩余路程段数。

定义 MSTP 接口设置

1. 打开“MSTP Interface Settings”（MSTP 接口设置）页面。
2. 选择接口。
3. 定义字段。
4. 单击“Apply Changes”（应用更改）。

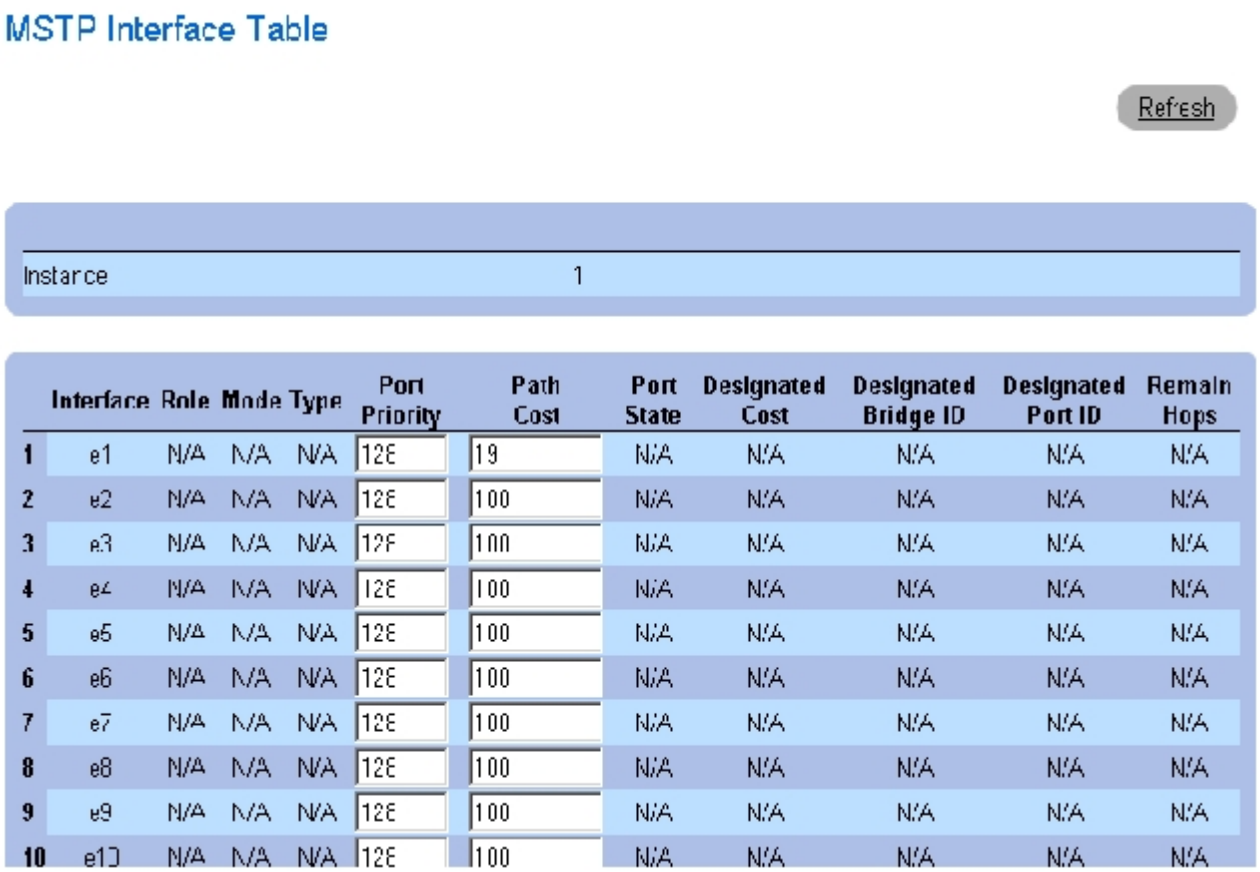
系统将定义 MSTP 参数，并更新设备。

查看 MSTP 接口表

1. 打开“MSTP Interface Settings” (MSTP 接口设置) 页面。
2. 单击“Show All” (全部显示) 。

系统将打开“MSTP Interface Table” (MSTP 接口表) 页面：

图 7-29. MSTP 接口表



使用 CLI 命令定义 MSTP 接口

下表概括了与“Spanning Tree MSTP Interface Settings” (生成树 MSTP 接口设置) 页面中显示的用于定义 MSTP 接口的选项等效的 CLI 命令。

表 7-79. MSTP 接口的 CLI 命令

CLI 命令	说明
spanning-tree mst instance-id cost cost	为 MST 计算设置端口的路径成本
spanning-tree mst instance-id priority priority	为指定的 ST 实例设置设备优先级。
show spanning-tree mst- configuration	显示 MST 配置。

以下是 CLI 命令的示例：

console# **show spanning-tree mst-configuration**		
Gathering information		
Current MST configuration		
Name:Gili		
Revision: 65000		
Instance	Vlans Mapped	State
---------	------------------------	----------
0	16-4094	enabled
1	1	enabled
2	2	enabled
3	3	enabled
4	4	enabled
5	5	enabled
6	6	enabled
7	7	enabled
8	8	enabled
9	9	enabled
10	10	enabled
11	11	enabled
12	12	enabled
13	13	enabled
14	14	enabled
15	15	enabled

配置 VLAN

VLAN 是 LAN 的逻辑子组，它是通过软件而不是通过定义硬件解决方案创建的。VLAN 将用户站点和网络设备组合为单个单元，而不考虑它们连接的物理 LAN 网段。VLAN 使网络通信在子组内的传输更加有效。通过软件管理的 VLAN 可减少执行网络更改、添加和移动所需的时间。

由于 VLAN 是基于软件，而不是通过物理属性进行定义的，因此 VLAN 可以拥有无限数量的端口，并且可以针对每个装置、设备、堆栈或任何其它逻辑连接组合进行创建。

VLAN 在第 2 层起作用。由于 VLAN 将通信隔离在 VLAN 内部，所以需要在第 3 层协议级别工作的路由器以允许通信在 VLAN 之间传输。第 3 层路由器使用 VLAN 标识网段和坐标。VLAN 是广播域和多点传送域。广播和多点传送通信仅在生成通信的 VLAN 中传输。

VLAN 标记提供了在 VLAN 组之间传输 VLAN 信息的方法。VLAN 标记可以将一个 4 字节标记附加至信息包标头。VLAN 标记表示信息包所属的 VLAN。VLAN 标记由终端站点或网络设备附加至 VLAN。VLAN 标记还可以包含 VLAN 网络优先级信息。

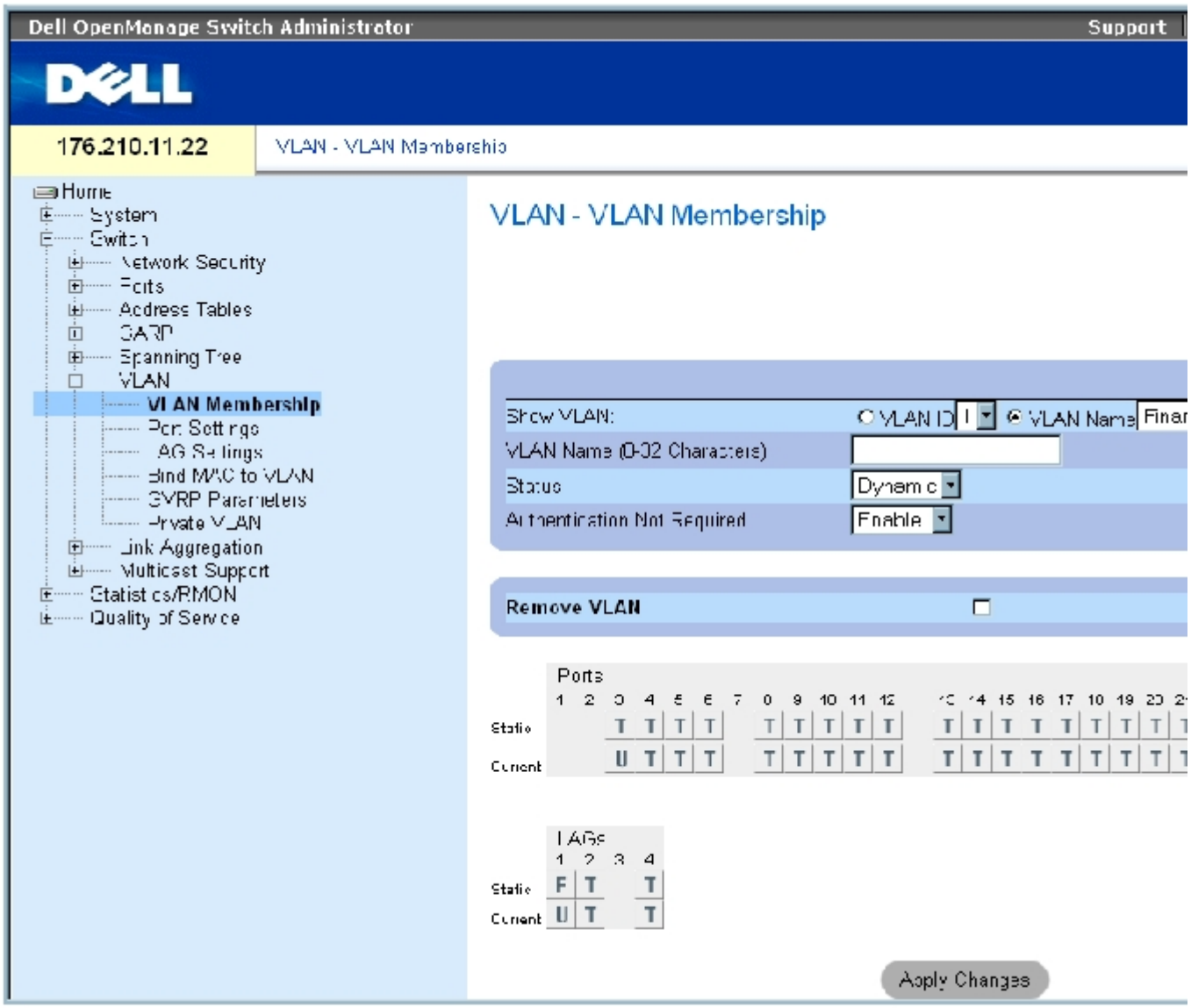
组合 VLAN 和 GVRP 使网络管理员可以将网络节点定义到广播域中。广播和多点传送通信被限制在发源组中。

要打开“VLAN”页面，请在树视图中单击“Switch”（交换机）→“VLAN”。

定义 VLAN 成员关系

“VLAN Membership”（VLAN 成员关系）页面包含用于定义 VLAN 组的字段。设备支持 4094 VLAN ID 至 256 VLAN 的映射。所有端口必须具有已定义的 PVID。如果未配置其它值，将使用默认的 VLAN PVID。VLAN ID 1 是默认的 VLAN，无法从系统中将其删除。要打开“VLAN Membership”（VLAN 成员关系）页面，请在树视图中单击“Switch”（交换机）→“VLAN”→“VLAN Membership”（VLAN 成员关系）。

图 7-30. VLAN 成员关系



“VLAN Membership” (VLAN 成员关系)页面包含以下字段：

“Show VLAN” (显示 VLAN) — 根据 VLAN ID 或 VLAN 名称列出并显示特定的 VLAN 信息。

“VLAN Name (0-32 Characters)” (VLAN 名称 [0 至 32 个字符]) — 用户定义的 VLAN 名称。

“Status” (状态) — VLAN 的类型。可能的值包括：

“Dynamic” (动态) — VLAN 是通过 GVRP 动态创建的。

“Static” (静态) — VLAN 是由用户定义的。

“Default” (默认) — VLAN 是默认的 VLAN。

“Authentication Not Required” (无需验证) — 允许或禁止未经授权的用户访问 VLAN。

“Remove VLAN”（删除 VLAN）— 如果选定此选项，将从 VLAN 成员关系表中删除 VLAN。

添加新 VLAN

1. 打开“VLAN Membership”（VLAN 成员关系）页面。
2. 单击“Add”（添加）。

   系统将打开“Create New VLAN”（创建新 VLAN）页面。
3. 输入 VLAN ID 和 VLAN 名称。
4. 单击“Apply Changes”（应用更改）。

   系统将添加新 VLAN，并更新设备。

修改 VLAN 成员关系组

1. 打开“VLAN Membership”（VLAN 成员关系）页面。
2. 从“Show VLAN”（显示 VLAN）下拉式菜单中选择一个 VLAN。
3. 根据需要修改字段。
4. 单击“Apply Changes”（应用更改）。

   系统将修改 VLAN 成员关系信息，并更新设备。

删除 VLAN

1. 打开“VLAN Membership”（VLAN 成员关系）页面。
2. 在“Show VLAN”（显示 VLAN）字段中选择一个 VLAN。

3. 选取“Remove VLAN”（删除 VLAN）复选框。

4. 单击“Apply Changes”（应用更改）。

系统将删除选定的 VLAN，并更新设备。

使用 CLI 命令定义 VLAN 成员关系组

下表概括了与“VLAN Membership”（VLAN 成员关系）页面中显示的用于定义 VLAN 成员关系组的选项等效的 CLI 命令。

表 7-80. VLAN 成员关系组的 CLI 命令

CLI 命令	说明
vlan database	进入 VLAN 配置模式。
vlan {VLAN 范围}	创建 VLAN。
name 字符串	为 VLAN 添加名称。

以下是 CLI 命令的示例：

```
console(config)#vlan
database

console(config-vlan)#
vlan 1972

console(config-vlan)# end

console(config)# interface
vlan 1972

console(config-if)# name
Marketing

console(config-if)# end
```

VLAN 端口成员关系表

“VLAN Port Membership Table”（VLAN 端口成员关系表）包含用于为 VLAN 分配端口的端口表。通过在“Port Control”（端口控制）设置之间进行切换，可以为 VLAN 分配端口。端口可以具有以下值：

表 7-81. VLAN 端口成员关系表

端口控制	定义
T	接口是 VLAN 的成员。通过接口传输的所有信息包均被标记。信息包包含 VLAN 信息。
U	接口是 VLAN 成员。通过接口传输的信息包均未标记。
F	否认接口是 VLAN 的成员。
空白	接口不是 VLAN 成员。将不会传输与接口相关联的信息包。

“VLAN Port Membership Table” (VLAN 端口成员关系表) 显示了端口和端口状态，以及 LAG。

为 VLAN 组分配端口

1. 打开“VLAN Membership” (VLAN 成员关系) 页面。
2. 单击“VLAN ID”或“VLAN Name” (VLAN 名称) 选项按钮并从下拉式菜单中选择一个 VLAN。
3. 在“Port Membership Table” (端口成员关系表) 中选择一个端口，并设定端口值。
4. 单击“Apply Changes” (应用更改) 。

系统会将端口分配至 VLAN 组，并更新设备。

删除 VLAN

1. 打开“VLAN Membership” (VLAN 成员关系) 页面。
2. 单击“VLAN ID”或“VLAN Name” (VLAN 名称) 选项按钮并从下拉式菜单中选择一个 VLAN。
3. 选取“Remove VLAN” (删除 VLAN) 复选框。
4. 单击“Apply Changes” (应用更改) 。

系统将删除选定的 VLAN，并更新设备。

使用 CLI 命令为 VLAN 组分配端口

下表概括了用于将端口分配至 VLAN 组的等效 CLI 命令。

表 7-82. 为 VLAN 组分配端口的 CLI 命令

CLI 命令	说明
switchport general acceptable-frame-types tagged-only	在入口丢弃未标记的帧。
switchport forbidden vlan {add VLAN 列表 | remove VLAN 列表}	禁止向端口添加特定的 VLAN。
switchport mode {access | trunk | general}	配置端口的 VLAN 成员关系模式。
switchport access vlan VLAN ID	在接口处于访问模式时配置 VLAN ID。
switchport trunk allowed vlan {add vlan-list | remove vlan-list}	在主干端口中添加或删除 VLAN。
switchport trunk native vlan vlan id	将端口定义为指定 VLAN 的成员，并将 VLAN ID 定义为端口默认 VLAN ID (PVID)。
switchport general allowed vlan add vlan-list [tagged | untagged]	为常规模式下的端口添加或删除 VLAN。
switchport general pvid vlan id	在接口处于常规模式时配置 PVID。

以下是 CLI 命令的示例：

```
console(config)#vlan
database

console(config-vlan)#
vlan 23-25

console(config-vlan)# end

console(config)# interface
vlan 23

console(config-if)# name
Marketing

console(config-if)# end

console(config)# interface
ethernet 1/e8

console(config-if)#
switchport mode access
```

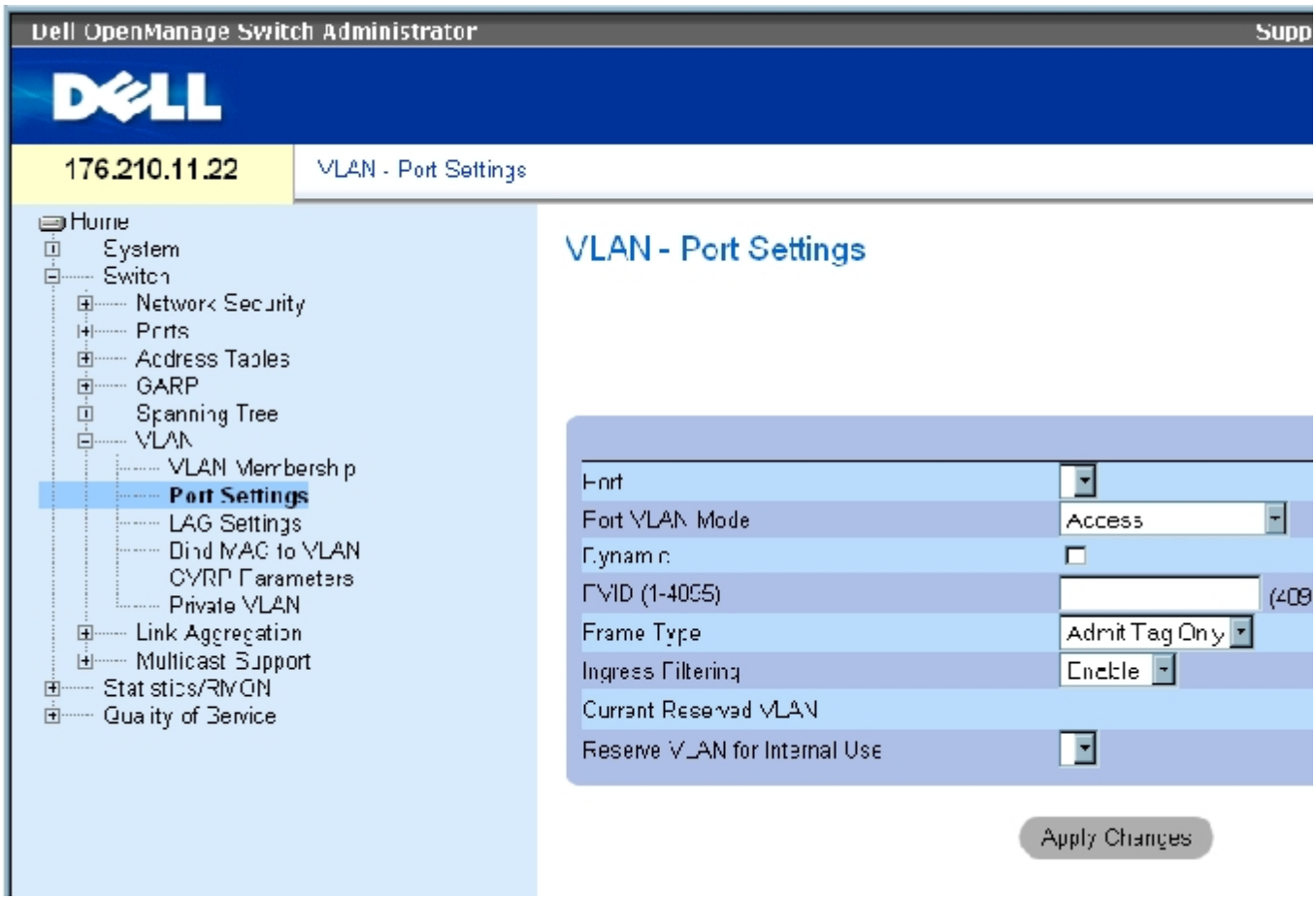
```
console(config-if)#
switchport access vlan 23


console(config-if)# end


console(config)# interface
ethernet 1/e9


console(config-if)#
switchport mode trunk


console(config-if)#
switchport mode trunk
allowed vlan add 23-25


console(config-if)# end


console(config)# interface
ethernet 1/e11


console(config-if)#
switchport mode general


console(config-if)#
switchport general
allowed vlan add 23,25
tagged


console(config-if)#
switchport general pvid
25
```

定义 VLAN 端口设置

“VLAN Port Settings” (VLAN 端口设置) 页面提供了用于管理属于 VLAN 的端口。“Port Default VLAN ID” (端口默认 VLAN ID) (PVID) 可在“VLAN Port Settings” (VLAN 端口设置) 页面中进行配置。所有到达设备的未标记信息包均通过端口 PVID 进行标记。

要打开“VLAN Port Settings” (VLAN 端口设置) 页面，请在树视图中单击“Switch” (交换机) → “VLAN” → “Port Settings” (端口设置) 。

图 7-31. VLAN 端口设置



"VLAN Port Settings" (VLAN 端口设置) 页面包含以下字段：

"Port" (端口) — VLAN 中包含的端口号。

"Port VLAN Mode" (端口 VLAN 模式) — 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。端口处于访问模式时，不能指定端口上接受的信息包类型。不能在访问端口上启用/禁用入口筛选。

"Trunk" (主干) — 端口属于其中所有端口 (可以不标记的那个端口除外) 均被标记的 VLAN。

"PVE Promiscuous" (PVE 混合) — 端口为 PVE 混合 VLAN 的一部分。

"PVE Community" (PVE 团体) — 端口为 PVE 团体 VLAN 的一部分。

"PVE Isolated" (PVE 隔离) — 端口为 PVE 隔离 VLAN 的一部分。

"Dynamic" (动态) — 基于连接至端口的主机源 MAC 地址将端口分配到 VLAN。

“PVID”— 为未标记信息包分配 VLAN ID。可能的值介于 1 至 4095 之间。VLAN 4095 按照标准和行业惯例被定义为丢弃的 VLAN。分类为丢弃的 VLAN 的信息包将被丢弃。

“Frame Type”（帧类型）— 端口上接受的信息包类型。可能的值包括：

“Admit Tag Only”（仅接受标记）— 端口仅接受已标记信息包。

“Admit All”（全部接受）— 端口既接受已标记信息包，也接受未标记信息包。

“Ingress Filtering”（入口筛选）— 在端口上启用或禁用入口筛选。入口筛选将丢弃预定给特定端口不是其组成部分的 VLAN 的信息包。

“Current Reserved VLAN”（当前保留 VLAN）— 当前由系统指定为保留 VLAN 的 VLAN。

“Reserve VLAN for Internal Use”（保留 VLAN 用于内部使用）— 如果系统未使用用户选定的 VLAN，它将作为保留 VLAN。

设定端口设置

1. 打开“VLAN Port Settings”（VLAN 端口设置）页面。
2. 从“Port”（端口）下拉式菜单中选择需要为其设定设置的端口。
3. 完成页面中的其余字段。
4. 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

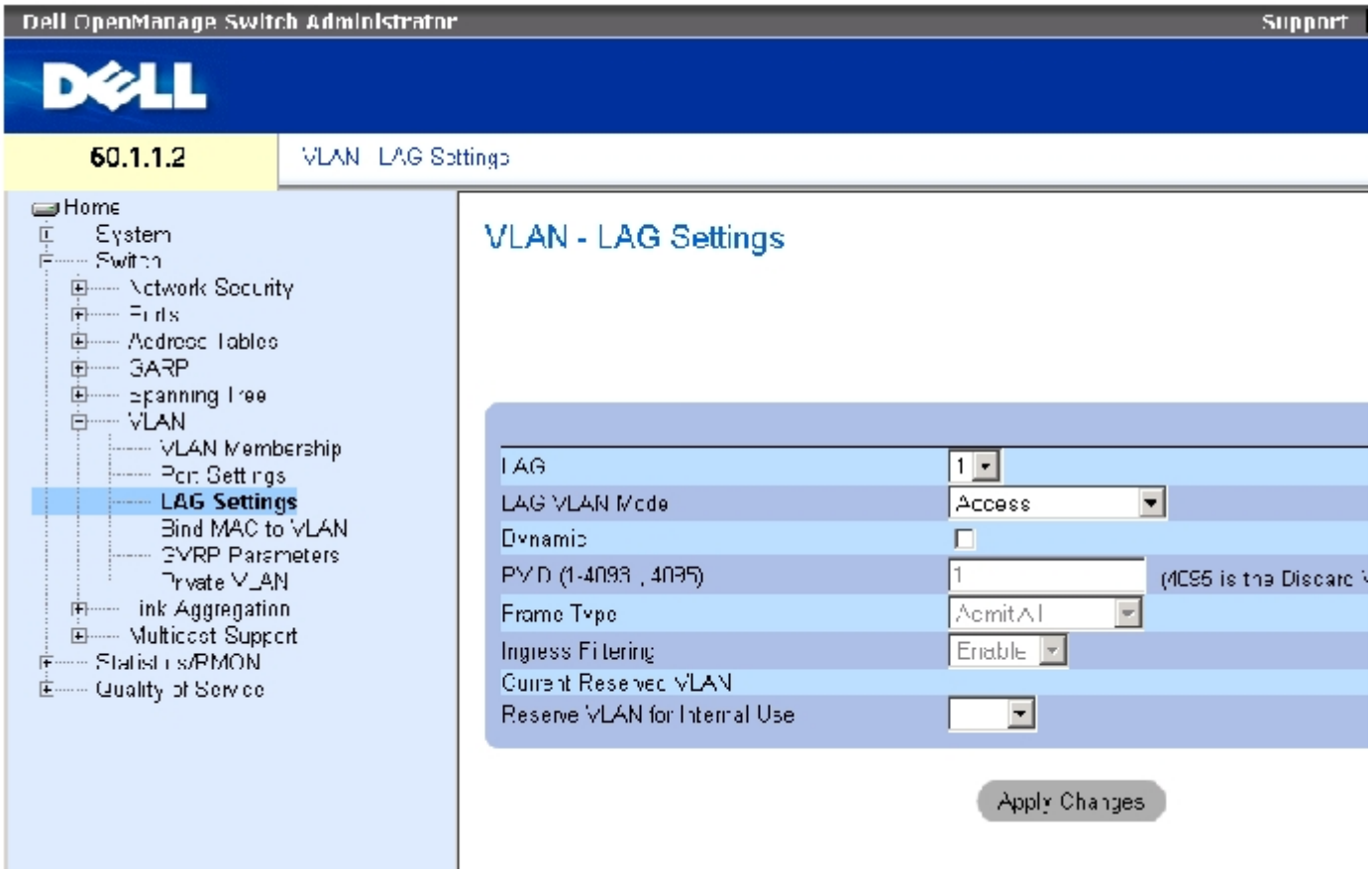
1. 打开“VLAN Port Settings”（VLAN 端口设置）页面。
2. 单击“Show All”（全部显示）。

系统将打开“VLAN Port Table”（VLAN 端口表）。

定义 VLAN LAG 设置

"VLAN LAG Settings" (VLAN LAG 设置) 页面提供了用于管理属于 VLAN 的 LAG 的参数。VLAN 可以由各个端口或 LAG 组成。进入设备的未标记信息包按照 PVID 指定的 LAG ID 进行标记。要打开"VLAN LAG Settings" (VLAN LAG 设置) 页面，请在树视图中单击"Switch" (交换机) → "VLAN" → "LAG Settings" (LAG 设置) 。

图 7-32. VLAN LAG 设置



"VLAN LAG Settings" (VLAN LAG 设置) 页面包含以下字段：

"LAG" — VLAN 中包含的 LAG 号。

"LAG VLAN Mode" (LAG VLAN 模式) — LAG 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 属于其中所有端口 (可以不标记的那个端口除外) 均被标记的 VLAN。

“PVE Promiscuous” (PVE 混合) — LAG 属于 PVE 混合 VLAN。

“PVE Community” (PVE 团体) — LAG 属于 PVE 团体 VLAN。

“PVE Isolated” (PVE 隔离) — LAG 属于 PVE 隔离 VLAN。

“Dynamic” (动态) — 基于连接至 LAG 的主机源 MAC 地址将 LAG 分配到 VLAN。

“PVID (1-4093 , 4095)” — 为未标记的信息包分配 VALN ID。可能的字段值介于 1 至 4095 之间。VLAN 4095 按照标准和行业惯例被定义为丢弃的 VLAN。分类为此 VLAN 的信息包将被丢弃。

“Frame Type” (帧类型) — LAG 接受的信息包类型。可能的值包括:

“Admit Tag Only” (仅接受标记) — LAG 仅接受已标记信息包。

“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) — 启用或禁用由 LAG 进行的入口筛选。入口筛选将丢弃预定给特定 LAG 不是其成员的 VLAN 的信息包。

“Current Reserve VLAN” (当前保留 VLAN) — 当前指定为保留 VLAN 的 VLAN。

“Reserve VLAN for Internal Use” (保留 VLAN 用于内部使用) — 重启动设备后指定为保留 VLAN 的 VLAN。

设定 VLAN LAG 设置:

1. 打开“VLAN LAG Settings” (VLAN LAG 设置) 页面。
2. 从“LAG”下拉式菜单中选择一个 LAG，并完成页面中的字段。
3. 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

1. 打开“VLAN LAG Settings” (VLAN LAG 设置) 页面。

2. 单击“Show All”（全部显示）。

系统将打开“VLAN LAG Table”（VLAN LAG 表）。

使用 CLI 命令为 VLAN 组分配 LAG

下表概括了与“VLAN LAG Settings”（VLAN LAG 设置）页面中显示的为 VLAN 组分配 LAG 的选项等效的 CLI 命令。

表 7-83. 为 VLAN 分配 LAG 的 CLI 命令

CLI 命令	说明
switchport mode {access | trunk | general}	配置 LAG VLAN 成员关系模式。
switchport trunk native vlan VLAN ID	将端口定义为指定 VLAN 的成员，并将 VLAN ID 定义为 LAG 默认 VLAN ID (PVID)。
switchport general pvid VLAN ID	在接口处于常规模式时配置 LAG VLAN ID (PVID)。
switchport general allowed vlan add VLAN 列表 [tagged | untagged]	在常规 LAG 中添加或删除 VLAN。
switchport general acceptable-frame-type tagged-only	在入口丢弃未标记的信息包。
switchport access vlan dynamic	将 MAC 地址捆绑至 VLAN。
switchport general ingress-filtering disable	禁用 LAG 入口筛选。

以下是 CLI 命令的示例：

```
console(config)# interface
port-channel 1

console(config-if)#
switchport mode access

console(config-if)#
switchport access vlan 2

console(config-if)# exit

console(config)# interface
port-channel 2

console(config-if)#
switchport mode general

console(config-if)#
```

```
switchport general
allowed vlan add 2-3
tagged


console(config-if)#
switchport general pvid 2


console(config-if)#
switchport general
acceptable-frame-type
tagged-only


console(config-if)#
switchport general
ingress-filtering disable


console(config-if)# exit


console(config)# interface
port-channel 3


console(config-if)#
switchport mode trunk


console(config-if)#
switchport trunk native
vlan 3


console(config-if)#
switchport trunk allowed
vlan add 2
```

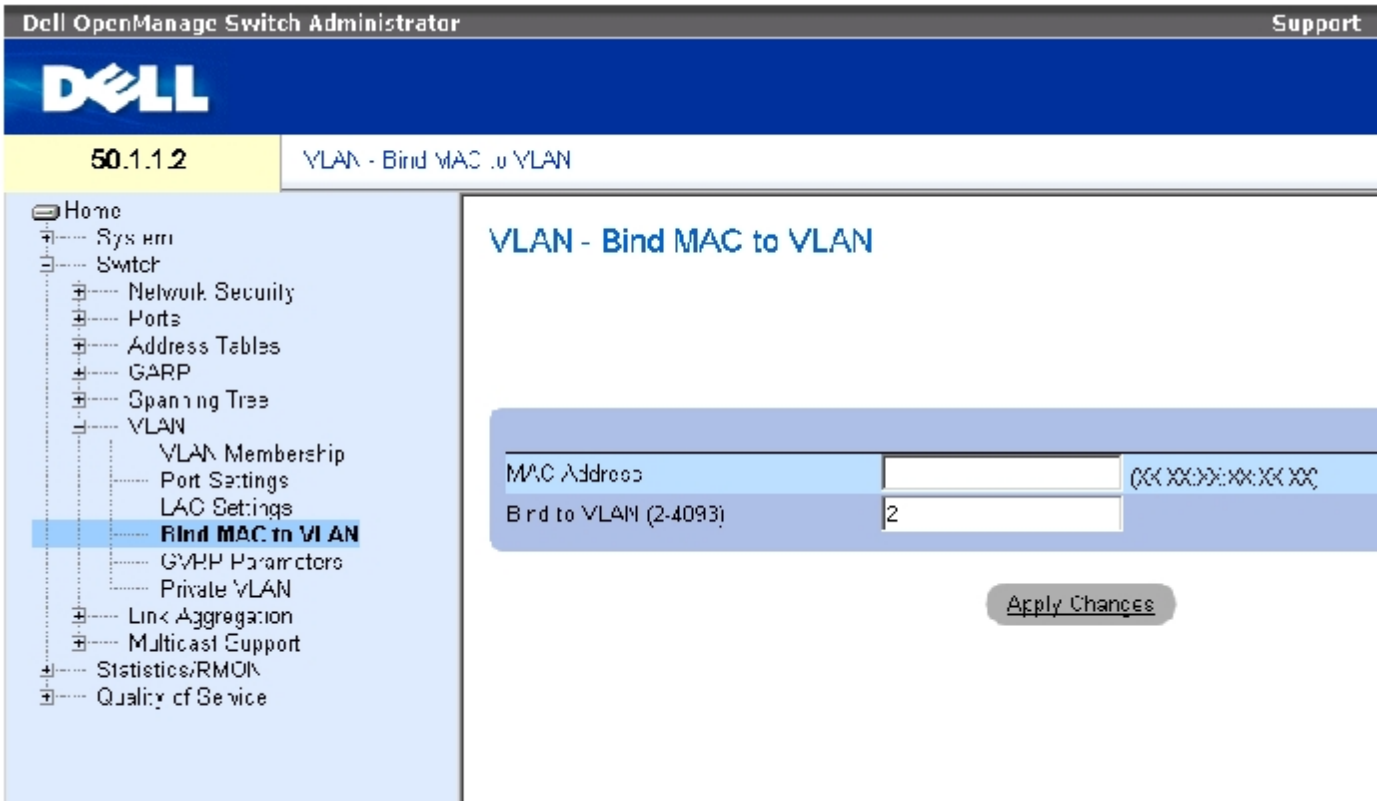
将 MAC 地址捆绑至 VLAN

将 MAC 地址捆绑至 VLAN 可以基于 MAC 地址为 VLAN 分配端口。为 VLAN 分配了 MAC 地址并且该 MAC 地址被记忆在某端口上，该端口将加入捆绑的 VLAN。MAC 地址过期后，端口将离开 VLAN。只有动态 VLAN 才可以与 MAC 地址相捆绑。

要将 MAC 地址捆绑至 VLAN，请确保 VLAN 端口为动态添加的，而非静态 VLAN 端口。

要打开“Bind MAC to VLAN” (将 MAC 捆绑至 VLAN)页面，请单击“Switch” (交换机) →“VLAN”→“Bind MAC to VLAN” (将 MAC 捆绑至 VLAN) 。

图 7-33. 将 MAC 捆绑至 VLAN



“Bind MAC to VLAN” (将 MAC 捆绑至 VLAN) 页面包含以下字段：

“MAC Address” (MAC 地址) — 表示捆绑至 VLAN 的 MAC 地址。

“Bind to VLAN (2-4093)” (捆绑至 VLAN [2-4093]) — 表示 MAC 地址捆绑至的 VLAN。

显示 MAC 至 VLAN 表：

1. 打开“Bind MAC to VLAN” (将 MAC 捆绑至 VLAN) 页面。
2. 单击“Show All” (全部显示) 。

   系统将打开“MAC to VLAN table” (MAC 至 VLAN 表) 。

使用 CLI 命令将 MAC 地址捆绑至 VLAN：

下表概括了用于将 MAC 地址捆绑至 VLAN 的等效 CLI 命令。

表 7-84. 将 MAC 地址捆绑至 VLAN 的 CLI 命令

CLI 命令	说明
mac-to-vlan mac-address vlan-id	将 MAC 地址捆绑至 VLAN。
switchport access vlan dynamic	配置专用 VLAN。
show mac-to-vlan	显示 MAC 至 VLAN 数据库
no mac-to-vlan mac-address	将 MAC 地址从 VLAN 解除捆绑。

以下是 CLI 命令的示例：

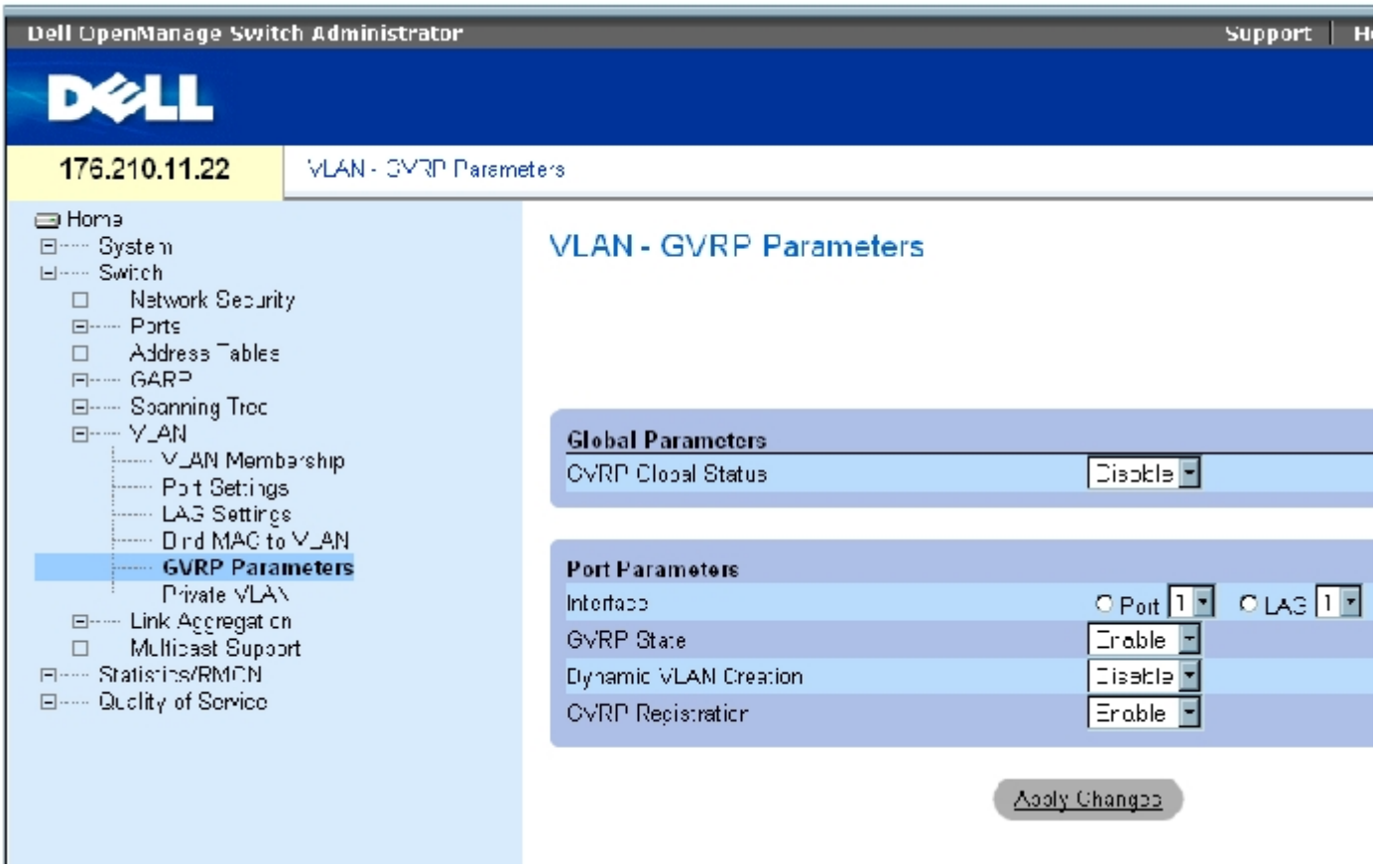
```
console(config-vlan)# mac-to-vlan 0060.704c.73ff 123

console(config-vlan)# exit

console(config)# exit

console# show vlan mac-to-vlan

MAC Address VLAN

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

0060.704c.73ff 123
```

配置 GVRP 参数

GARP VLAN 注册协议 (GVRP) 专用于在可识别 VLAN 的网桥之间自动分配 VLAN 成员关系信息。GVRP 使可识别 VLAN 的网桥能够自动记忆 VLAN 到网桥端口的映射，而无需逐个配置每个网桥并注册 VLAN 成员关系。

“GVRP Parameters” (GVRP 参数) 页面用于全局启用 GVRP。还可以针对每个接口启用 GVRP。要打开“GVRP Parameters” (GVRP 参数) 页面，请在树视图中单击“Switch” (交换机) → “VLAN” → “GVRP Parameters” (GVRP 参数) 。

图 7-34. GVRP 参数



"GVRP Parameters" (GVRP 参数) 页面包含以下字段:

"GVRP Global Status" (GVRP 全局状态) — 在设备上启用或禁用 GVRP。默认情况下，GVRP 处于禁用状态。

"Interface" (接口) — 指定端口或 LAG 以便编辑 GVRP 设置。

"GVRP State" (GVRP 状态) — 在接口上启用或禁用 GVRP。

"Dynamic VLAN Creation" (动态 VLAN 创建) — 允许或禁止在接口上通过 GVRP 创建 VLAN。

"GVRP Registration" (GVRP 注册) — 允许或禁止在接口上通过 GVRP 注册 VLAN。

在设备上启用 GVRP

1. 打开"GVRP Global Parameters" (GVRP 全局参数) 页面。
2. 在"GVRP Global Status" (GVRP 全局状态) 字段中选择"Enable" (启用) 。
3. 单击"Apply Changes" (应用更改) 。

系统将在设备上启用 GVRP。

通过 GVRP 启用 VLAN 注册

1. 打开“GVRP Global Parameters”（GVRP 全局参数）页面。
2. 在“GVRP Global Status”（GVRP 全局状态）中选择“Enable”（启用）。
3. 在“GVRP State”（GVRP 状态）字段中为所需的接口选择“Enable”（启用）。
4. 在“GVRP Registration”（GVRP 注册）字段中选择“Enable”（启用）。
5. 单击“Apply Changes”（应用更改）。

系统将在端口上启用 GVRP VLAN 注册，并更新设备。

使用 CLI 命令配置 GVRP

下表概括了与“GVRP Global Parameters”（GVRP 全局参数）页面中显示的配置 GVRP 的选项等效的 CLI 命令。

表 7-85. GVRP 全局参数的 CLI 命令

CLI 命令	说明
gvrp enable （全局）	全局启用 GVRP。
gvrp enable （接口）	在某个接口上启用 GVRP。
gvrp vlan-creation-forbid	启用或禁用动态 VLAN 创建。
gvrp registration-forbid	取消注册所有动态 VLAN，并禁止在端口上进行动态 VLAN 注册。
show gvrp configuration [ethernet 接口| port-channel 端口信道号]	显示 GVRP 配置信息，包括计时器值、是否已启用 GVRP 和动态 VLAN 创建，以及运行 GVRP 的端口。
show gvrp error-statistics [ethernet 接口| port-channel 端口信道号]	显示 GVRP 错误统计数据。
show gvrp statistics [ethernet 接口| port-channel 端口信道号]	显示 GVRP 统计数据。

clear gvrp statistics [ethernet 接口| port-channel 端口信道号]	清除所有 GVRP 统计数据信息。

以下是 CLI 命令的示例：

```
console(config)# gvrp enable

console(config)# interface ethernet 1/e1

console(config-if)# gvrp enable

console(config-if)# gvrp vlan-creation-forbid

console(config-if)# gvrp registration-forbid

console(config-if)# end

console# show gvrp configuration

GVRP Feature is currently Enabled on the device

Maximum VLANs: 223
```

Port(s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
------	------	----------	-------	----------	----	----
1/e11	Enabled	Forbidden	Disabled	200	900	10000
1/e12	Disabled	Normal	Enabled	200	600	10000

配置专用 VLAN

专用 VLAN (PVLAN) 通过将端口间的通信限制在一个 VLAN 内部，从而增强了网络安全性。专用 VLAN 在第 2 层限制网络通信。网络管理员定义主 VLAN。在主 VLAN 内部有隔离 VLAN 和团体 VLAN。专用 VLAN 端口可以具有以下状态：

- 混合 — 混合端口可以与 PVLAN 内部的所有端口通信。所有混合信息包都会自动分配给隔离 VLAN 和团体 VLAN。
- 隔离 — 隔离端口与同一 PVLAN 中的其它端口完全隔离。但是，隔离端口可以与混合端口通信。此外，通过 VLAN 的隔离端口的所有来往通信将被阻塞（除了来自混合端口的通信）。所有隔离端口都会自动分配给隔离 VLAN。
- 团体 — 团体端口可以与其它团体端口和混合端口通信。在同一 PVLAN 中，团体端口与其它团体或隔离端口中的所有其它接口是单独分开的。所有团体端口都会自动分配给团体 VLAN 和专用 VLAN。

注：如果端口为现有 VLAN 成员，则不能将其定义为混合端口或隔离端口。

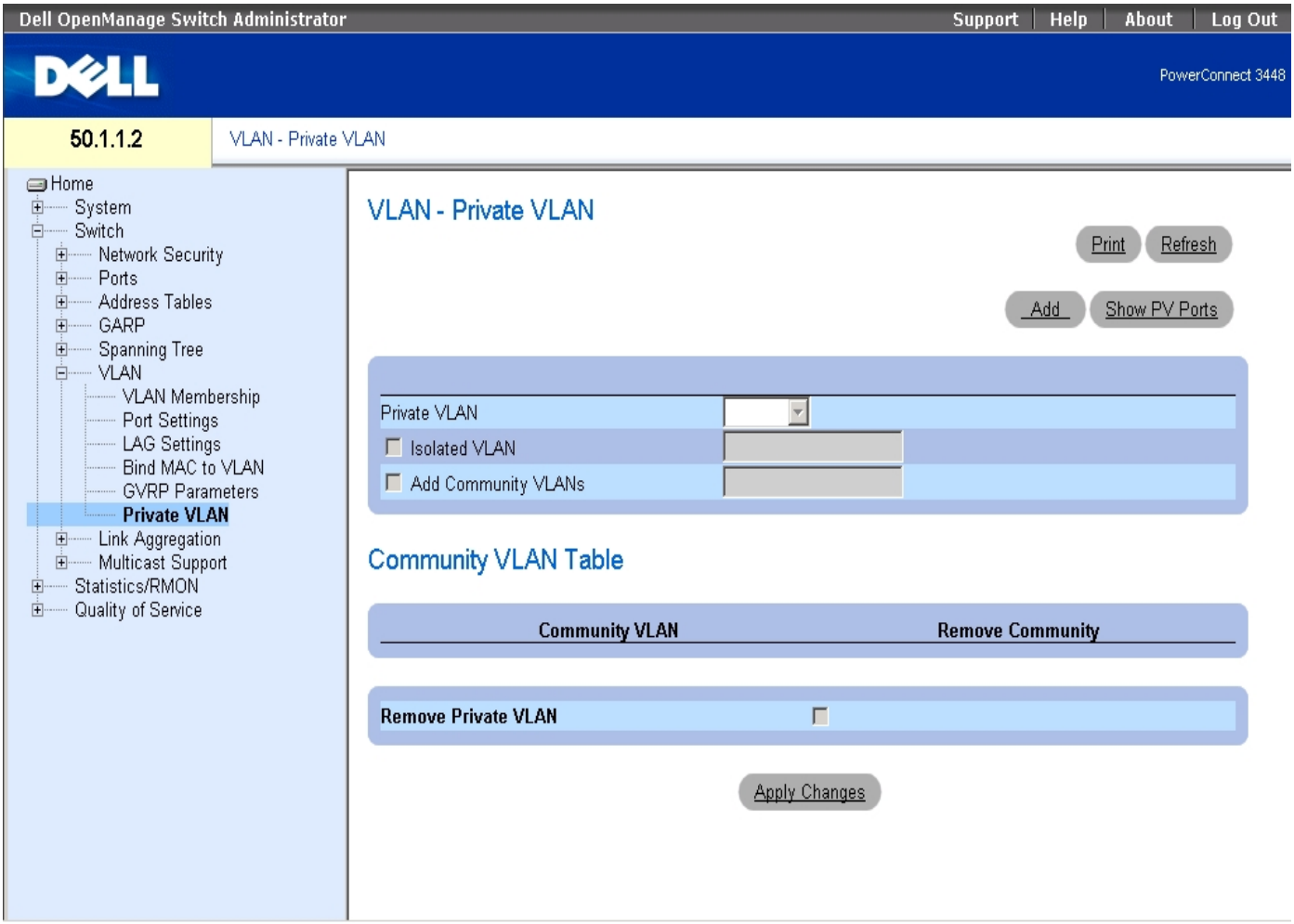
注：以前创建的 VLAN 不能配置为隔离 VLAN 或团体 VLAN。

注：隔离 VLAN 和团体 VLAN 包含在总 VLAN 计数中。

如果删除了主 VLAN，则隔离 VLAN 和团体 VALN 也将删除。此外，隔离 VLAN 和团体 VALN 只传输未标记的通信。

要打开“Private VLAN”（专用 VLAN）页面，请在树视图中单击“Switch”（交换机）→“VLAN”→“Private VLAN”（专用 VLAN）。

图 7-35. 专用 VLAN



“Private VLAN”（专用 VLAN）页面包含以下字段：

“Private VLAN”（专用 VLAN）— 包含用户定义的专用 VLAN 列表。专用 VLAN 在“Add Private VLAN”（添加专用 VLAN）页面中定义。

“Isolated VLAN”（隔离 VLAN）— 表示将隔离端口分配至哪一个 VLAN。

“Add Community VLANs”（添加团体 VLAN）— 添加向其分配了团体端口的团体 VLAN。

“Community VLAN”（团体 VLAN）— 显示团体 VLAN 的列表。

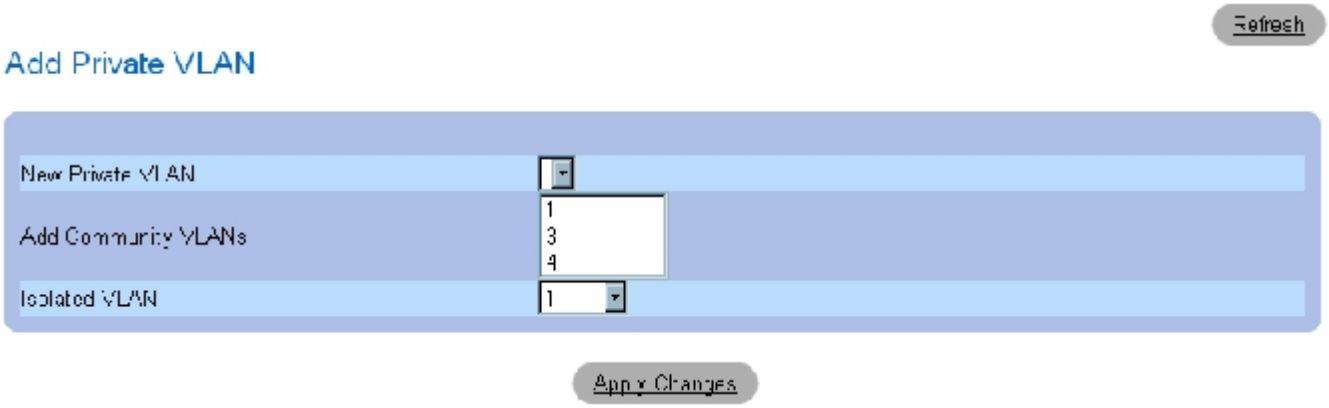
“Remove Community”（删除团体）— 如果选取该选项，将删除团体 VLAN。

“Remove Private VLAN”（删除专用 VLAN）— 如果选取该选项，将删除专用 VLAN。

添加专用 VLAN

1. 打开“Private VLAN”（专用 VLAN）页面。
2. 单击“Add”（添加）。系统将打开“Add Private VLAN”（添加专用 VLAN）页面：

图 7-36. 添加专用 VLAN



“Add Private VLAN”（添加专用 VLAN）页面还包含以下字段：

“New Private VLAN”（新专用 VLAN）— 包含专用 VLAN 的列表。团体 VLAN 被添加至专用 VLAN。

“Add Community VLANs”（添加团体 VLAN）— 向专用 VLAN 添加团体 VLAN。

“Isolated VLAN”（隔离 VLAN）— 向专用 VLAN 添加隔离 VLAN。

3. 定义字段。
4. 单击“Apply Changes”（应用更改）。

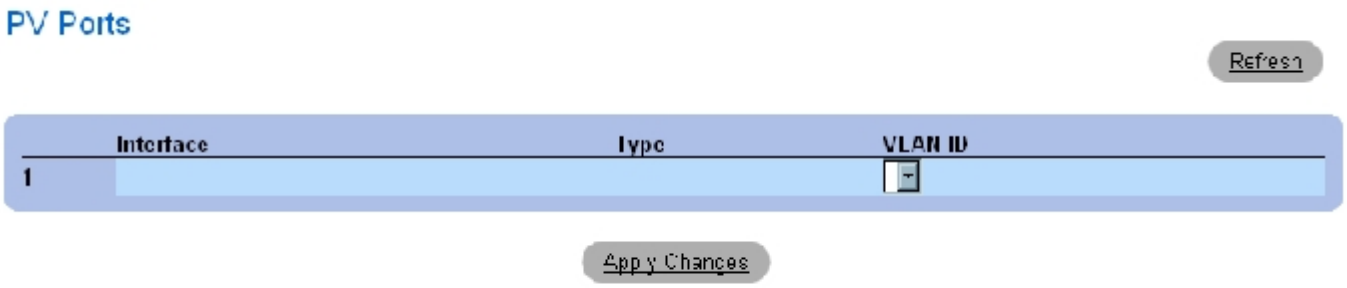
系统将定义专用 VLAN，并更新设备。

显示 PV 端口表

1. 打开“Private VLAN” (专用 VLAN) 页面。
2. 单击“Show PV Ports” (显示 PV 端口) 。

系统将打开“PV Ports Table” (PV 端口表) ：

图 7-37. PV 端口表



使用 CLI 命令配置 PVLAN

下表概括了与“Private VLAN” (专用 VLAN) 页面中显示的用于配置 PVLAN 的选项等效的 CLI 命令。

表 7-86. 专用 VLAN 的 CLI 命令

CLI 命令	说明
switchport mode private vlan promiscuous	将混合端口添加至混合 VLAN。
switchport mode private vlan community	将团体端口添加至团体 VLAN。
switchport mode private vlan isolated	将隔离端口添加至隔离 VLAN。
private-vlan primary	定义专用 VLAN。
private-vlan community {add community-vlan-list | remove community-vlan-list }	定义或删除主 VLAN 的团体 VLAN。
private-vlan isolated	定义主 VLAN 的隔离 VLAN。
switchport private-vlan pvlan [community cvlan]	定义专用 VLAN 端口。

show vlan private-vlan [primary vlan-id]	显示专用的主 VLAN。

以下是 CLI 命令的示例：

```
console(config)#vlan
database

console(config-vlan)#vlan
2

console(config-vlan)#exit

console(config)#interface
vlan 2

console(config-if)#
private-vlan primary

console(config)#interface
vlan 2

console(config-if)#
private-vlan isolated 10

console(config-if)#
private-vlan community
add 20

console# show vlan
private-vlan

console(config-if)# end
```

聚合端口

链路聚合通过将一组端口链接在一起形成单个 LAG（链路聚合组）来优化端口的使用。聚合端口可以使设备之间的带宽成倍增加、增强端口灵活性并提供链路冗余。

设备既支持静态 LAG，也支持链路聚合控制协议 (LACP) LAG。LACP LAG 与位于其它设备上的 LACP 端口协商聚合端口的链路。如果其它设备端口也是 LACP 端口，则设备将在设备之间建立 LAG。

聚合端口时应考虑以下因素：

- LAG 内的所有端口必须为相同的介质类型。
- 未在端口上配置 VLAN。
- 端口未分配至不同的 LAG。

- 端口上未配置自适应模式。
- 端口处于全双工模式。
- LAG 中的所有端口具有相同的入口筛选和标记模式。
- LAG 中的所有端口具有相同的背压和流控制模式。
- LAG 中的所有端口具有相同的优先级。
- LAG 中的所有端口具有相同的收发机类型。
- 设备最多支持八个 LAG，且每个 LAG 中有八个端口。
- 仅当端口不属于先前配置的 LAG 时，才可以将端口配置为 LACP 端口。

添加至 LAG 的端口将失去其各自的端口配置。将端口从 LAG 中删除时，原始端口配置将应用于端口。

设备使用哈希函数确定在聚合链路成员上传输的信息包。哈希函数以统计学方式在聚合链路成员之间平衡负载。设备将聚合链路看作单个逻辑端口。

定义 LACP 参数

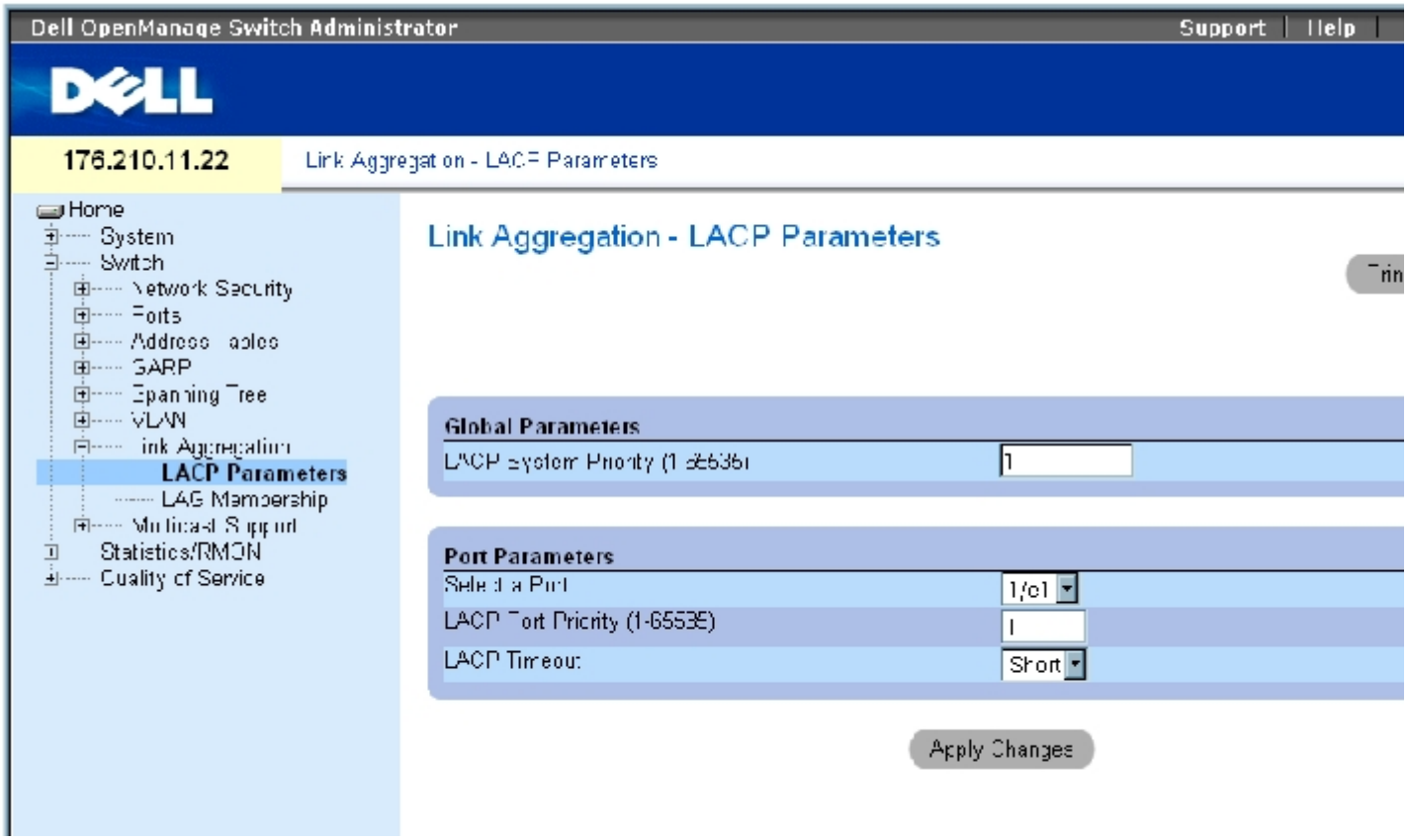
聚合端口可以被链接至链路聚合端口组。每个组都包含具有相同速率并被设置为全双工运行的端口。

链路聚合组 (LAG) 中的端口如果以同一速率运行，则可以包含不同的介质类型。通过在相关链路上启用链路聚合控制协议 (LACP)，可以手动配置或自动配置聚合链路。

定义 LACP 参数

“LACP Parameters” (LACP 参数) 页面包含用于配置 LACP LAG 的字段。聚合端口可以被链接至链路聚合端口组。每个组由具有相同速率的端口组成。通过在相关链路上启用链路聚合控制协议 (LACP)，可以手动设置或自动建立聚合链路。要打开“LACP Parameters” (LACP 参数) 页面，请在树视图中单击“Switch” (交换机) → “Link Aggregation” (链路聚合) → “LACP Parameters” (LACP 参数) 。

图 7-38. LACP 参数



“LACP Parameters” (LACP 参数) 页面包含以下字段：

“LACP System Priority (1-65535)” (LACP 系统优先级 [1-65535]) — 全局设置的 LACP 优先级值。可能范围为 1 至 65535。默认值为 1。

“Select a Port” (选择端口) — 要设定超时和优先级值的端口号。

“LACP Port Priority (1-65535)” (LACP 端口优先级 [1-65535]) — 端口的 LACP 优先级值。

“LACP Timeout” (LACP 超时) — 管理 LACP 超时。可能的字段值包括：

“Short” (短) — 指定短超时值。

“Long” (长) — 指定长超时值。

定义链路聚合全局参数

1. 打开“LACP Parameters” (LACP 参数) 页面。
2. 完成“LACP System Priority” (LACP 系统优先级) 字段。

3. 单击“Apply Changes”（应用更改）。

系统将定义参数，并更新设备。

定义链路聚合端口参数

1. 打开“LACP Parameters”（LACP 参数）页面。
2. 完成“Port Parameters”（端口参数）区域中的字段。
3. 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

1. 打开“LACP Parameters”（LACP 参数）页面。
2. 单击“Show All”（全部显示）。

系统将打开“LACP Parameters Table”（LACP 参数表）。

使用 CLI 命令配置 LACP 参数

下表概括了与“LACP Parameters”（LACP 参数）页面中显示的配置 LACP 参数的选项等效的 CLI 命令。

表 7-87. LACP 参数的 CLI 命令

CLI 命令	说明
lacp system-priority 值	配置系统优先级。
lacp port-priority 值	配置物理端口的优先级值。
lacp timeout {long | short}	设定管理 LACP 超时。
[| |]	

show lacp ethernet 接口	parameters	statistics	protocol-state	显示以太网端口的 LACP 信息。

以下是 CLI 命令的示例：

```
Console (config)# lacp
system-priority 120

Console (config)#
interface ethernet 1/e11

Console (config-if)# lacp
port-priority 247

Console (config-if)# lacp
timeout long

Console(config-if)# end

Console# show lacp
ethernet 1/e11 statistics

Port 1/e11 LACP
Statistics:

LACP PDUs sent:2

LACP PDUs received:2
```

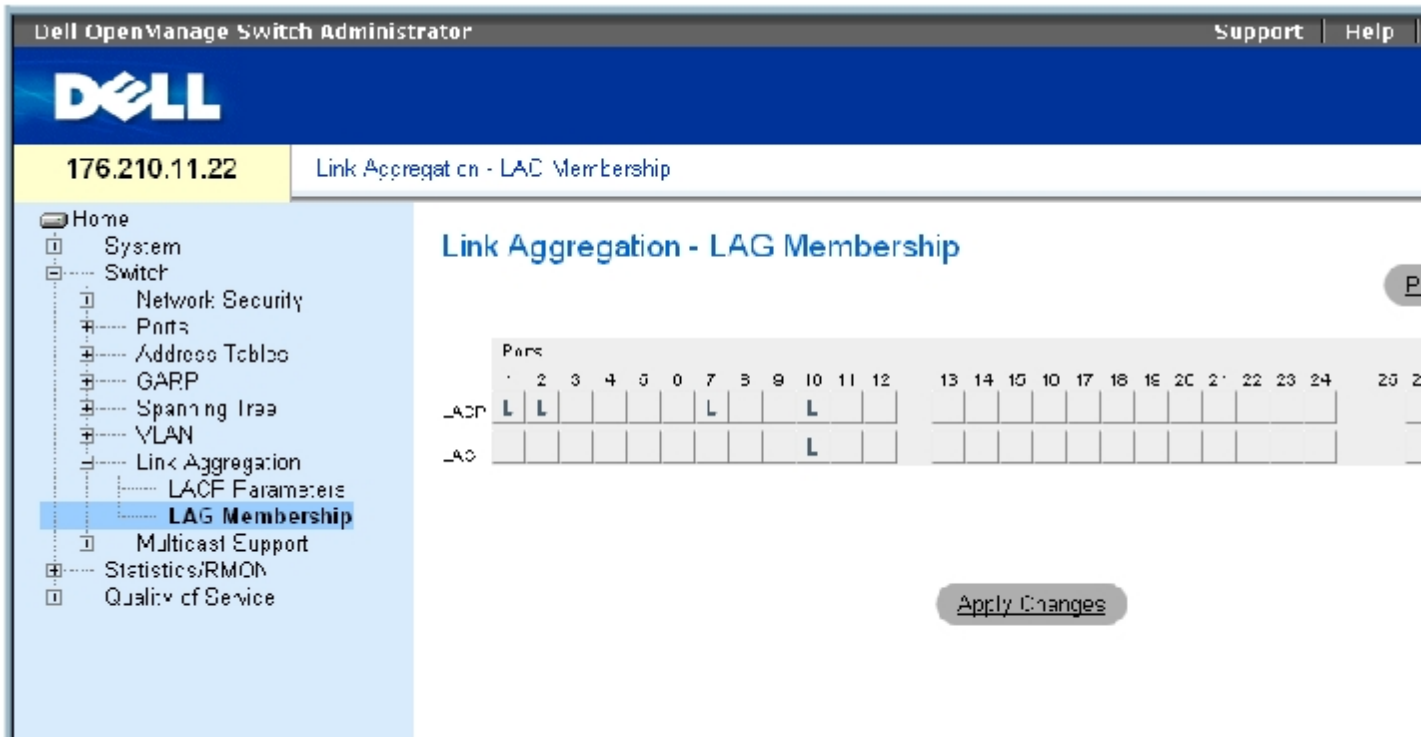
定义 LAG 成员关系

设备支持每个系统八个 LAG，每个 LAG 八个端口，无论设备为独立设备还是处于堆栈中。

如果向 LAG 添加了端口，则该端口将获取 LAG 的属性。如果无法将此端口配置为带有 LAG 的属性，则该端口将不会添加至 LAG。系统将生成错误信息。但是，如果无法使用 LAG 设置配置加入 LAG 的第一个端口，系统将使用端口的默认设置把该端口添加至 LAG。系统将生成错误信息。但是，由于此端口是 LAG 中的唯一端口，因此整个 LAG 将使用端口的设置（而不是 LAG 的定义设置）运行。

使用“LAG Membership” (LAG 成员关系) 页面将端口分配至 LAG。要打开“LAG Membership” (LACP 成员关系) 页面，请在树视图中单击“Switch” (交换机) → “Link Aggregation” (链路聚合) → “LAG Membership” (LAG 成员关系) 。

图 7-39. LAG 成员关系



“LAG Membership” (LAG 成员关系) 页面包含以下字段：

“LACP” — 使用 LACP 将端口聚合到 LAG。

“LAG” — 向 LAG 添加端口，并指示端口所属的特定 LAG。

向 LAG 或 LACP 添加端口

1. 打开“LAG Membership” (LAG 成员关系) 页面。
2. 在“LAG”行 (第二行) 中，将按钮切换至特定编号以将端口聚合到该 LAG 号或删除与 LAG 号对应的端口。
3. 在“LACP”行 (第一行) 中，切换端口号下相应的按钮以设定 LACP 或静态 LAG。
4. 单击“Apply Changes” (应用更改) 。

系统会将端口添加至 LAG 或 LACP，并更新设备。

使用 CLI 命令向 LAG 添加端口

下表概括了与“LAG Membership” (LAG 成员关系) 页面中显示的用于为 LAG 分配端口的选项等效的 CLI 命令。

表 7-88. LAG 成员关系的 CLI 命令

CLI 命令	说明
channel-group 端口信道号 mode {on | auto}	使端口与端口信道相关联。在此命令前加 no 将从接口删除信道组配置。
show interfaces port-channel [端口信道号]	显示端口信道信息。

以下是 CLI 命令的示例：

```
console(config)# interface
ethernet 1/e11

console(config-if)#
channel-group 1 mode on
```

多点传送支持

多点传送使单个信息包可以传输至多个目的地。第 2 层多点传送服务基于第 2 层设备，该设备接收定址到特定多点传送地址的单个信息包。多点传送可以创建信息包副本，然后将这些信息包传输至相关的端口。

“Registered Multicast traffic”（注册的多点传送通信）— 如果发现定址到注册多点传送组的通信，则该通信将通过多点传送筛选数据库中的条目处理，并且仅传输至注册的端口。

“Unregistered Multicast traffic”（未注册的多点传送通信）— 如果发现定址到未注册的多点传送组的通信，则该通信将通过多点传送筛选数据库中的特殊条目处理。此选项的默认设置为多路发送所有此类通信（未注册的多点传送组中的通信）。

设备支持以下信息包：

- “Forwarding L2 Multicast Packets”（传输 L2 多点传送信息包）— 传输第 2 层多点传送信息包。默认情况下，系统将启用第 2 层多点传送筛选，并且用户不可以对其进行配置。

注：系统支持 256 个多点传送组的多点传送筛选。

- “Filtering L2 Multicast Packets”（筛选 L2 多点传送信息包）— 向接口传输第 2 层信息包。如果禁用了多点传送筛选，则多点传送信息包将多路发送至所有相关的端口。

要打开“Multicast Support”（多点传送支持）页面，请在树视图中单击“Switch”（交换机）→“Multicast Support”（多点传送支持）。

定义多点传送全局参数

默认情况下，第 2 层交换机向所有相关 VLAN 端口传输多点传送信息包，即将信息包作为单个多点传送信息包进行管理。虽然多点传送通信传输很有效，但是由于不相关的端口也会接收到多点传送信息包，因此它并不是最佳的。超额信息包将导致网络通信增加。多点传送筛选器允许将第 2 层信息包传输到端口子集。

全局启用 IGMP 监测时，所有 IGMP 信息包将传输至 CPU。CPU 将分析传入的信息包，并确定：

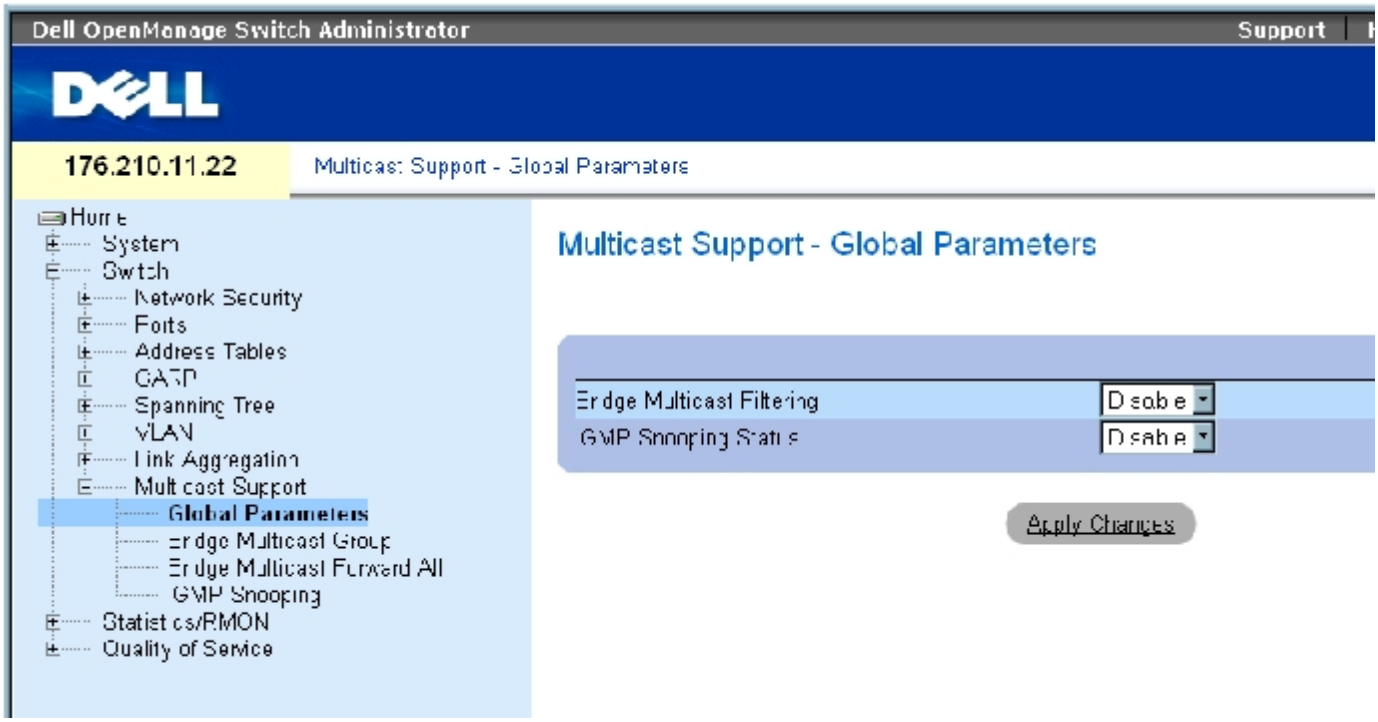
- 哪些端口要加入哪些多点传送组。
- 哪些端口具有生成 IGMP 查询的多点传送路由器。
- 哪些路由协议传输信息包和多点传送通信。

请求加入特定多点传送组的端口将发出 IGMP 报告，指明该多点传送组正在接受成员。这将导致创建多点传送筛选数据库。

要打开“Multicast Support”（多点传送支持）页面，请在树视图中单击“Switch”（交换机）→“Multicast Support”（多点传送支持）。

“Global Parameters”（全局参数）页面包含用于在设备上启用 IGMP 监测的字段。要打开“Global Parameters”（全局参数）页面，请在树视图中单击“Switch”（交换机）→“Multicast Support”（多点传送支持）→“Global Parameters”（全局参数）。

图 7-40. 全局参数



“Global Parameters”（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。默认值为已禁用。

“IGMP Snooping Status”（IGMP 监测状态）— 在设备上启用或禁用 IGMP 监测。默认值为已禁用。仅当启用“Global Parameters”（全局参数）时才能启用 IGMP 监测。

在设备上启用网桥多点传送筛选

1. 打开“Global Parameters”（全局参数）页面。
2. 在“Bridge Multicast Filtering”（网桥多点传送筛选）字段中选择“Enable”（启用）。
3. 单击“Apply Changes”（应用更改）。

系统将在设备上启用网桥多点传送筛选。

在设备上启用 IGMP 监测

1. 打开“Global Parameters”（全局参数）页面。
2. 在“IGMP Snooping Status”（IGMP 监测状态）字段中选择“Enable”（启用）。
3. 单击“Apply Changes”（应用更改）。

系统将在设备上启用 IGMP 监测。

使用 CLI 命令启用多点传送筛选和 IGMP 监测

下表概括了与**“Global Parameters”（全局参数）**页面中显示的用于启用多点传送筛选和 **IGMP** 监测的选项等效的 **CLI** 命令。

表 7-89. 多点传送筛选和监测的 CLI 命令

CLI 命令	说明
bridge multicast filtering	启用多点传送地址筛选。

ip igmp snooping	启用因特网组员资格协议（IGMP）监测。

以下是 CLI 命令的示例：

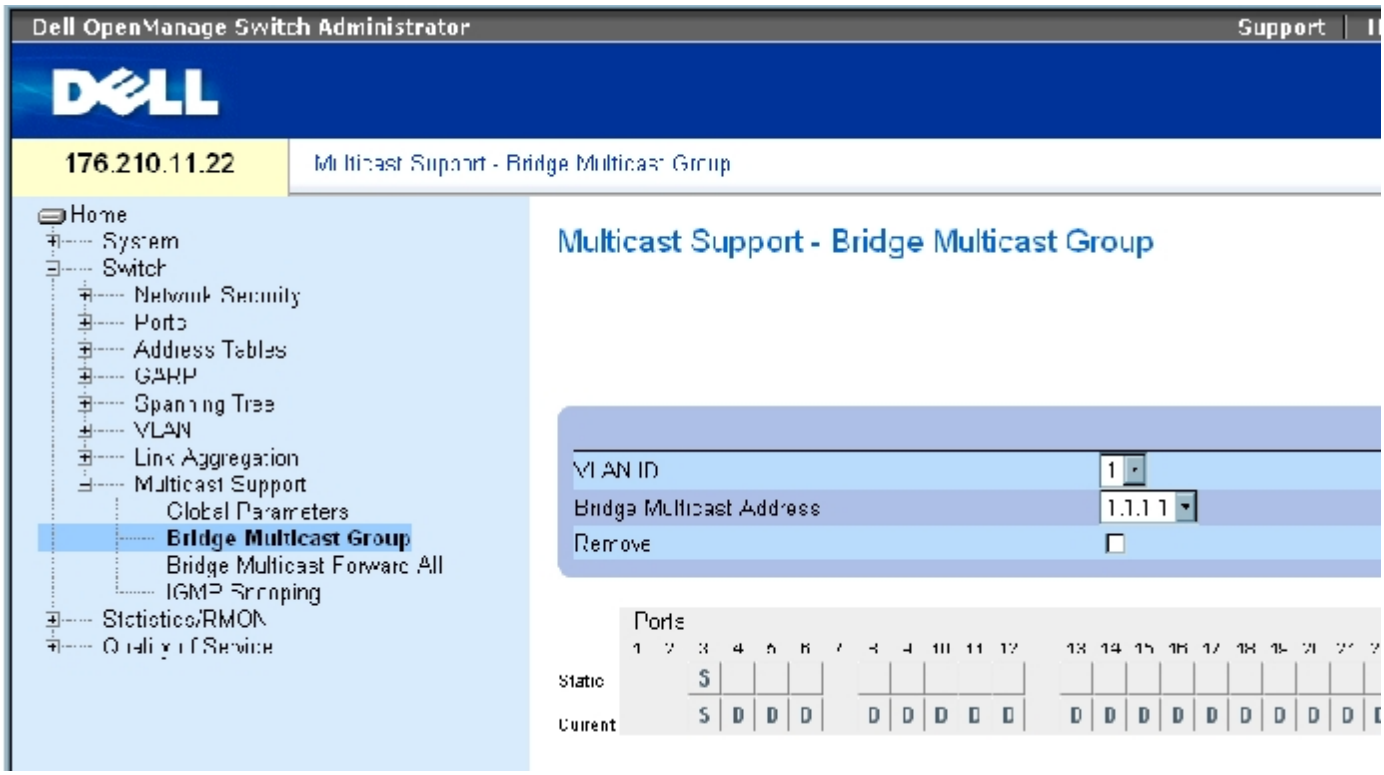
```
console(config)# bridge
multicast filtering

console(config)# ip igmp
snooping
```

添加网桥多点传送地址成员

“Bridge Multicast Group”（网桥多点传送组）页面在“Ports”（端口）和“LAG”表中显示连接至多点传送服务组的端口和 LAG。端口和 LAG 表还反映端口或 LAG 加入多点传送组的方式。可以将端口添加至现有组，也可以添加至新的多点传送服务组。在“Bridge Multicast Group”（网桥多点传送组）页面中，可以创建新的多点传送服务组。“Bridge Multicast Group”（网桥多点传送组）页面还可以为特定的多点传送服务地址组分配端口。

要打开“Bridge Multicast Group”（网桥多点传送组）页面，请在树视图中单击“Switch”（交换机）→“Multicast Support”（多点传送支持）→“Bridge Multicast Group”（网桥多点传送组）。

图 7-41. 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” — 标识 VLAN，并包含有关多点传送组地址的信息。

“Bridge Multicast Address”（网桥多点传送地址）— 标识多点传送组 MAC 地址/IP 地址。

“Remove”（删除）— 如果选定该选项，将删除网桥多点传送地址。

“Ports”（端口）— 可以添加至多点传送服务的端口。

“LAG” — 可以添加至多点传送服务的 LAG。

下表包含 IGMP 端口和 LAG 成员管理设置：

表 7-90. IGMP 端口/LAG 成员表控制设置

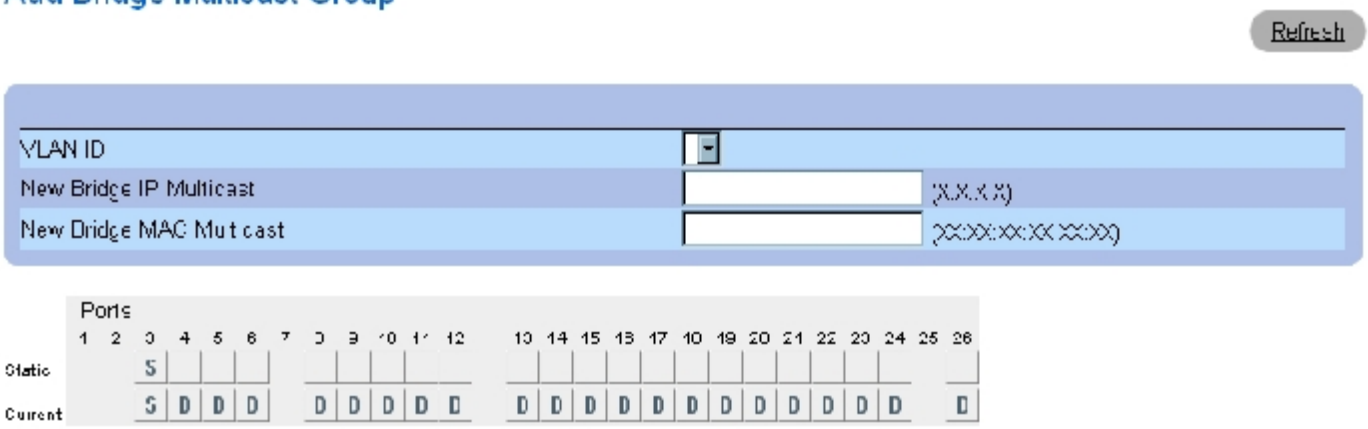
端口控制	定义
D	端口/LAG 已动态加入当前行中的多点传送组。
S	将端口作为静态行中的静态成员连接至多点传送组。 端口/LAG 已静态加入当前行中的多点传送组。
F	已禁止。
空白	端口未连接至多点传送组。

添加网桥多点传送地址

1. 打开“Bridge Multicast Group”（网桥多点传送组）页面。
2. 单击“Add”（添加）。

系统将打开“Add Bridge Multicast Group”（添加网桥多点传送组）页面：

图 7-42. 添加网桥多点传送组



3. 定义“VLAN ID”和“New Bridge Multicast Address”（新网桥多点传送地址）字段。

4. 将端口切换为“S”以将该端口加入到选定的多点传送组中。

5. 将端口切换为“F”以禁止将特定多点传送地址添加至特定端口。

6. 单击“Apply Changes”（应用更改）。

系统会将网桥多点传送地址分配至多点传送组，并更新设备。

定义端口以接收多点传送服务

1. 打开“Bridge Multicast Group”（网桥多点传送组）页面。

2. 定义“VLAN ID”和“Bridge Multicast Address”（网桥多点传送地址）字段。

3. 将端口切换为“S”以将该端口加入到选定的多点传送组。

4. 将端口切换为“F”以禁止将特定多点传送地址添加至特定端口。

5. 单击“Apply Changes”（应用更改）。

系统会将端口分配至多点传送组，并更新设备。

分配 LAG 以接收多点传送服务

1. 打开“Bridge Multicast Group”（网桥多点传送组）页面。
2. 定义“VLAN ID”和“Bridge Multicast Address”（网桥多点传送地址）字段。
3. 将 LAG 切换为“S”以将该 LAG 加入到选定的多点传送组中。
4. 将 LAG 切换为“F”以禁止将特定多点传送地址添加至特定 LAG。
5. 单击“Apply Changes”（应用更改）。

系统会将 LAG 分配至多点传送组，并更新设备。

使用 CLI 命令管理多点传送服务成员

下表概括了与“Bridge Multicast Group”（网桥多点传送组）页面中显示的用于管理多点传送服务成员的选项等效的 CLI 命令。

表 7-91. 多点传送服务成员的 CLI 命令

CLI 命令	说明
bridge multicast address {MAC 多点传送地址 | IP 多点传送地址}	将 MAC 层多点传送地址注册到网桥表，并将静态端口添加至组。
bridge multicast forbidden address {MAC 多点传送地址 | IP 多点传送地址}[add | remove] {ethernet 接口列表 | port-channel 端口信道号列表}	禁止将特定多点传送地址添加至特定端口。在此命令前加 no 将恢复默认设置。
show bridge multicast address-table [vlan VLAN **ID] [**address {MAC 多点传送地址 **|** IP 多点传送地址}**]** [format ip | mac]	显示多点传送 MAC 地址表信息。

以下是 CLI 命令的示例：

```
Console(config-if)# bridge multicast address 0100.5e02.0203
add ethernet 1/e11,1/e12
console(config-if)# end
console # show bridge multicast address-table
```

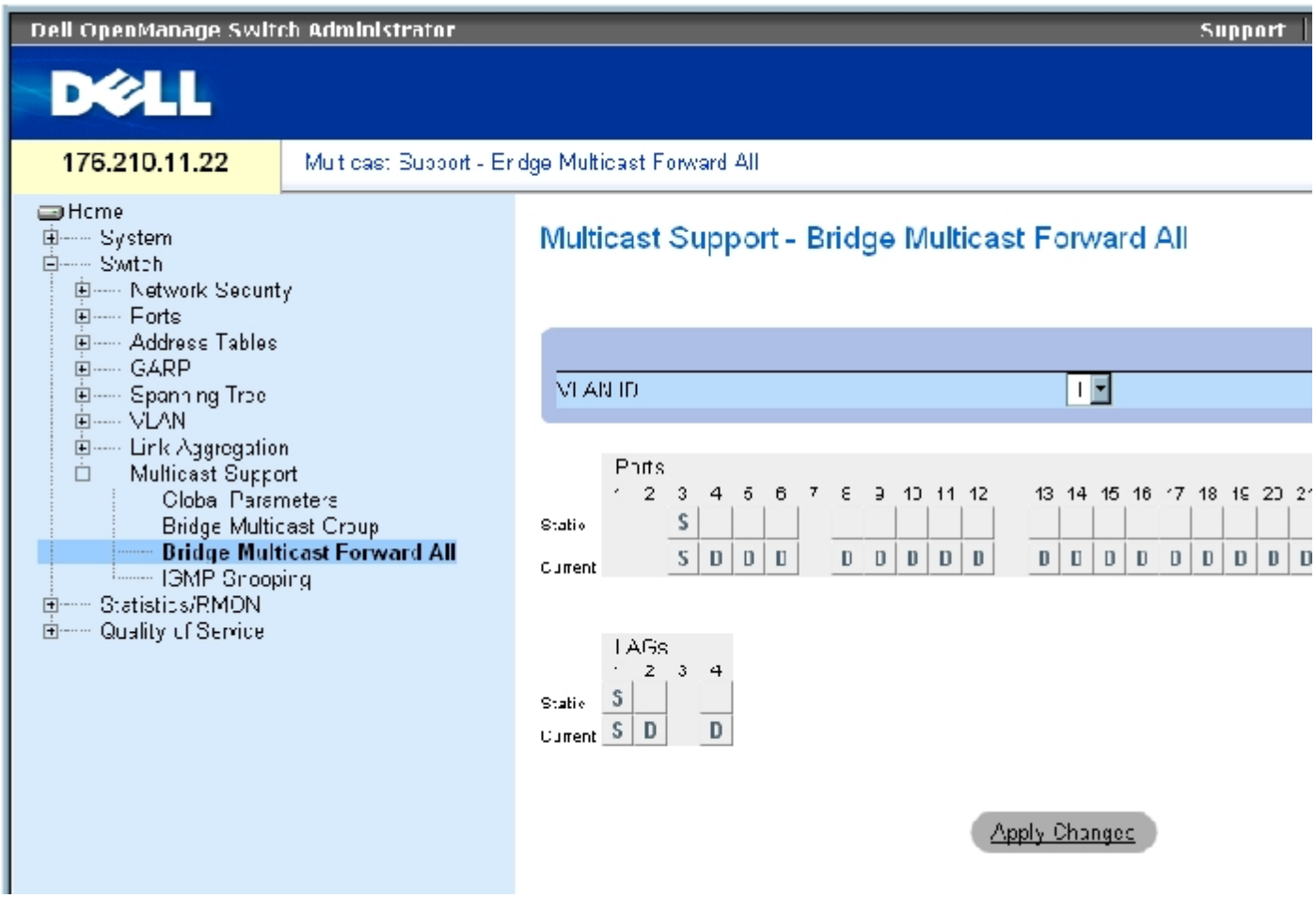

Vlan	MAC Address	Type	Ports
----	----------	-----	----------
1	0100.5e02.0203	static	1/e11, 1/e12
19	0100.5e02.0208	static	1/e11-16
19	0100.5e02.0208	dynamic	1/e11-12
Forbidden ports for multicast addresses:			
Vlan	MAC Address	Ports	
----	----------	----------	
1	0100.5e02.0203	1/e8	
19	0100.5e02.0208	1/e8	
console # **show bridge multicast address-table format ip**			
Vlan	IP Address	Type	Ports
----	----------	-----	----------
1	224-239.130|2.2.3	static	1/e11, 1/e12
19	224-239.130|2.2.8	static	1/e11-16
19	224-239.130|2.2.8	dynamic	1/e11-12
Forbidden ports for multicast addresses:			
Vlan	IP Address	Ports	
----	----------	----------	
1	224-239.130|2.2.3	1/e8	
19	224-239.130|2.2.8	1/e8	

设定全部多点传送参数

“Bridge Multicast Forward All”（网桥全部多点传送）页面包含用于将端口或 LAG 连接至相邻多点传送路由器/交换机所连接的设备的字段。启用 IGMP 监测后，多点传送信息包将被传输至相应的端口或 VLAN。

要打开“Bridge Multicast Forward All”（网桥全部多点传送）页面，请在树视图中单击“Switch”（交换机）→“Multicast Support”（多点传送支持）→“Bridge Multicast Forward All”（网桥全部多点传送）。

图 7-43. 网桥全部多点传送



“Bridge Multicast Forward All”（网桥全部多点传送）页面包含以下字段：

“VLAN ID” — 标识 VLAN。

“Ports”（端口） — 可以添加至多点传送服务的端口。

“LAG” — 可以添加至多点传送服务的 LAG。

网桥全部多点传送交换机/端口控制设置表包含用于管理路由器和端口设置的设置。

管理网桥全部多点传送交换机/端口控制设置表

下表介绍了用于设置端口控制的控制。

表 7-92. 网桥全部多点传送交换机/端口控制设置表

端口控制	定义
D	将端口作为动态端口连接至多点传送路由器或交换机。
S	将端口作为静态端口连接至多点传送路由器或交换机。
F	已禁止。
空白	端口未连接至多点传送路由器或交换机。

将端口连接至多点传送路由器或交换机

1. 打开“Bridge Multicast Forward All”（网桥全部多点传送）页面。
2. 定义“VLAN ID”字段。
3. 在“Port”（端口）表中选择一个端口，并设定端口值。
4. 单击“Apply Changes”（应用更改）。

该端口将被连接至多点传送路由器或交换机。

将 LAG 连接至多点传送路由器或交换机

1. 打开“Bridge Multicast Forward All”（网桥全部多点传送）页面。
2. 定义“VLAN ID”字段。
3. 在“LAG”表中选择一个端口，并设定 LAG 值。
4. 单击“Apply Changes”（应用更改）。

LAG 将被连接至多点传送路由器或交换机。

使用 CLI 命令管理连接至多点传送路由器的 LAG 和端口

下表概括了与“Bridge Multicast Forward All”（网桥全部多点传送）页面显示的用于管理连接至多点传送路由器的 LAG 和端口的选项等效的 CLI 命令。

表 7-93. 用于管理连接至多点传送路由器的 LAG 和端口的 CLI 命令

CLI 命令	说明
show bridge multicast filtering VLAN ID	显示多点传送筛选配置。
bridge multicast forward-all {add | remove} {ethernet 接口列表 | port-channel 端口信道号列表}	允许在端口上传输所有多点传送信息包。在此命令前加 no 将恢复默认设置。

以下是 CLI 命令的示例：

```
Console (config)# interface vlan 1

Console(config-if)# bridge multicast forward-all add ethernet1/e3

Console(config-if)# end

Console # show bridge multicast filtering 1
```

```
Filtering:Enabled
```

VLAN:	Forward-All	
Port	Static	Status
-------	------------------	------------
1/e11	Forbidden	Filter
1/e12	Forward	Forward(s)
1/e13	-	Forward(d)

IGMP 监测

“IGMP Snooping”（IGMP 监测）页面包含用于针对每个 VLAN 启用 IGMP 监测以及定义信息包存在时间的字段。要打开“IGMP Snooping”（IGMP 监测）页面，请在树视图中单击“Switch”（交换机）→“Multicast Support”（多点传送支持）→“IGMP Snooping”（IGMP 监测）。

图 7-44. IGMP 监测

“VLAN ID” — 指定 VLAN ID。

“IGMP Snooping Status” (IGMP 监测状态) — 在 VLAN 上启用或禁用 IGMP 监测。

“Auto Learn” (自动记忆) — 在以太网设备上启用或禁用自动记忆。

“Host Timeout (1-2147483647)” (主机超时 [1-2147483647]) — IGMP 监测条目过期前的时间。默认时间为 260 秒。

“Multicast Router Timeout (1-2147483647)” (多点传送路由器超时 [1-2147483647]) — 多点传送路由器条目过期前的时间。默认值为 300 秒。

“Leave TimeOut (0-2147483647)” (离开超时 [0-2147483647]) — 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) 。默认超时为 10 秒。

在设备上启用 IGMP 监测

1. 打开“IGMP Snooping” (IGMP 监测) 页面。

2. 为需要启用 IGMP 监测的设备选择 VLAN ID。

3. 在“IGMP Snooping Status”（IGMP 监测状态）字段中选择“Enable”（启用）。

4. 完成页面中的字段。

5. 单击“Apply Changes”（应用更改）。

系统将在设备上启用 IGMP 监测。

显示 IGMP 监测表

1. 打开“IGMP Snooping”（IGMP 监测）。

2. 单击“Show All”（全部显示）。

系统将打开“IGMP Snooping Table”（IGMP 监测表）。

使用 CLI 命令配置 IGMP 监测

下表概括了用于在设备上配置“IGMP Snooping”（IGMP 监测）的等效的 CLI 命令。

表 7-94. IGMP 监测的 CLI 命令

CLI 命令	说明
ip igmp snooping	启用因特网组员资格协议（IGMP）监测。
ip igmp snooping mrouter learn-pim-dvmrp	启用特定 VLAN 环境中多点传送路由器端口的自动记忆功能。
ip igmp snooping host-time-out 超时	配置主机超时。
ip igmp snooping mrouter-time-out 超时	配置多点传送路由器超时。
ip igmp snooping leave-time-out {超时 | 立即离开}	配置离开超时。
show ip igmp snooping groups [vlan VLAN ID] [address IP 多点传送地址]	显示由 IGMP 监测记忆的多点传送组。
show ip igmp snooping interface VLAN ID	显示 IGMP 监测配置。
show ip igmp snooping mrouter [interface vlan-id]	显示有关动态记忆的多点传送路由器接口的信息。

以下是 CLI 命令的示例：

```
console> enable

console# config

console(config)# ip igmp snooping

console(config)# interface vlan 1

console(config-if)# ip igmp
snooping mrouter learn-pim-dvmrp

console(config-if)# ip igmp
snooping host-time-out 300

Console(config-if)# ip igmp
snooping mrouter-time-out 200

console(config-if)# ip igmp
snooping leave-time-out 60

console(config-if)# end

console# show ip igmp snooping
groups
```

Vlan	IP Address	Querier	Ports
1	224-239.130|2.2.3	Yes	1/e11, 1/e12
19	224-239.130|2.2.8	Yes	1/e11-13

```
console# show ip igmp snooping
interface 1/e1

IGMP Snooping is globally enabled

IGMP Snooping is enabled on VLAN 1

IGMP host timeout is 300 sec

IGMP Immediate leave is
disabled.IGMP leave timeout is 60
sec

IGMP mrouter timeout is 200 sec

Automatic learning of multicast
router ports is enabled
```

```
console# show ip igmp snooping mrouter
```

VLAN	Ports		
----	------		
1	1/e11		

返回目录页面

返回目录页面

查看统计数据

Dell™ PowerConnect™ 34XX 系统用户指南

统计数据页面包含接口、GVRP、以太网类、RMON 和设备使用的设备信息。要打开统计数据页面，请在树视图中单击“Statistics”（统计数据）。

注：CLI 命令并非对所有统计数据页面均可用。

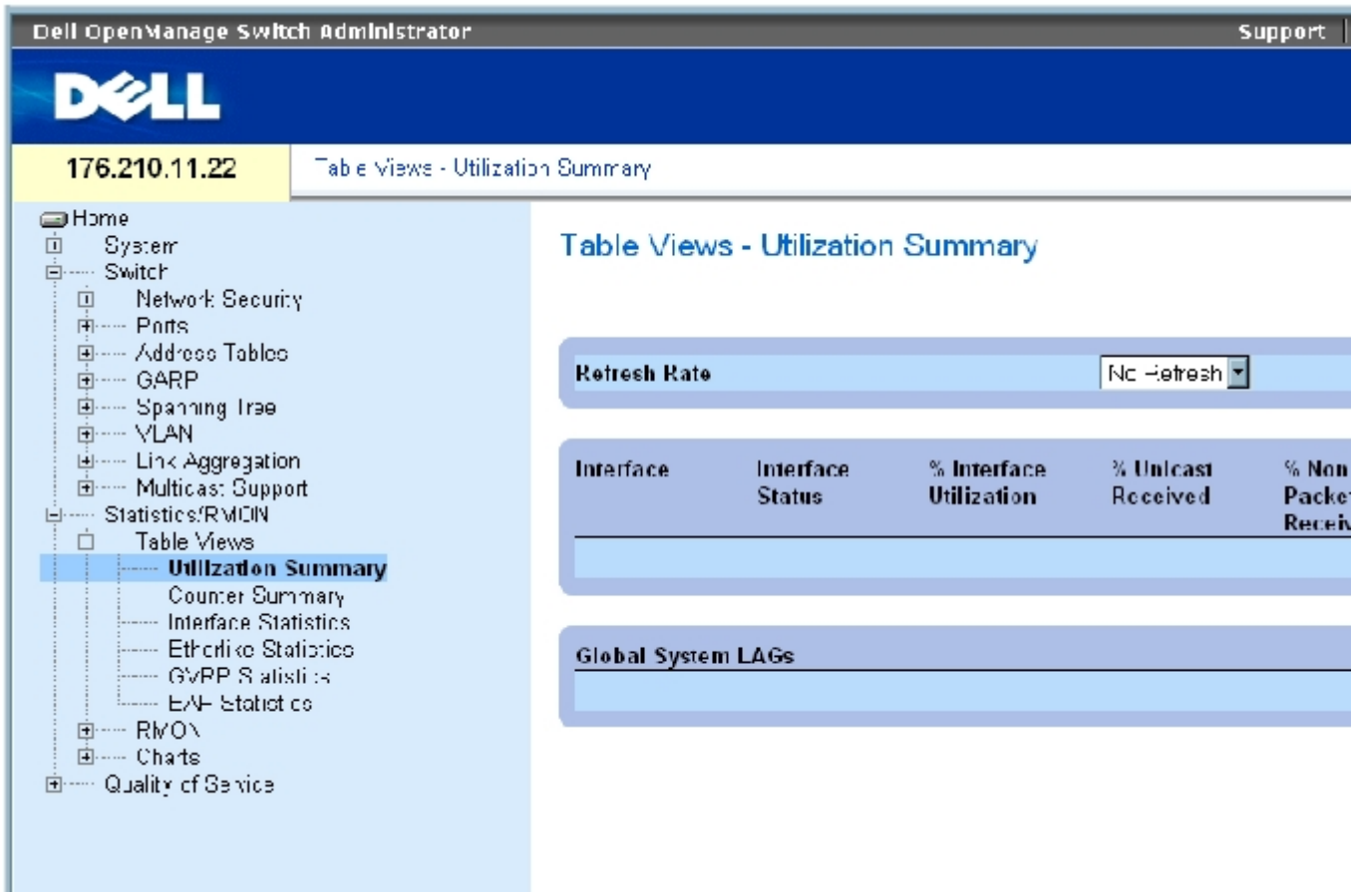
查看表

“Table View”（表视图）页面包含以表形式显示统计数据的链接。要打开此页面，请在树视图中单击“Statistics”（统计数据）→“Table”（表）。

查看使用摘要

“Utilization Summary”（使用摘要）页面包含接口使用的统计数据。要打开该页面，请在树视图中单击“Statistics”（统计数据）→“Table Views”（表视图）→“Utilization Summary”（使用摘要）。

图 8-1. 使用摘要



注：系统将定期刷新此屏幕，以降低对内存较低的计算机的影响。在此期间，可能会影响屏幕显示。

“Utilization Summary”（使用摘要）页面包含以下字段：

“Refresh Rate”（刷新率）— 表示刷新接口统计数据之前经过的时间。

“Interface”（接口）— 接口编号。

“Interface Status”（接口状态）— 接口的状态。

“% Interface Utilization”（接口使用百分比）— 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”（接收到的单点传送百分比）— 接口上接收到的单点传送信息包的百分比。

“% Non Unicast Packets Received”（接收到的非单点传送信息包百分比）— 接口上接收到的非单点传送信息包的百分比。

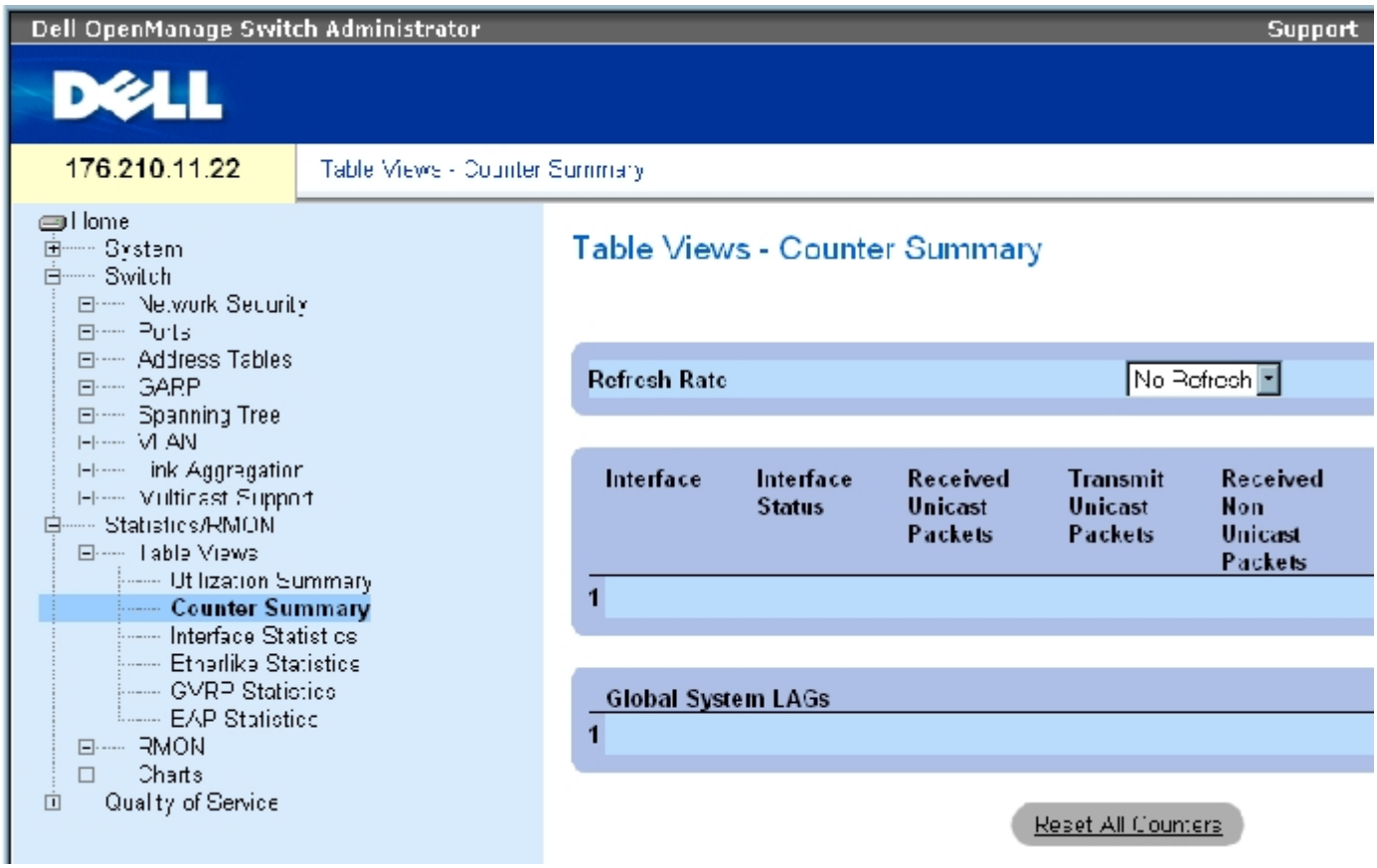
“% Error Packets Received”（接收到的错误信息包百分比）— 接口上接收到的错误信息包的百分比。

“Global System LAGs”（全局系统 LAG）— 表示当前全局 LAG 的使用情况。

查看计数器摘要

“Counter Summary” （计数器摘要）页面包含端口使用统计数据的数字总和，而不是百分比。要打开“Counter Summary” （计数器摘要）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 8-2. 计数器摘要



“Counter Summary” （计数器摘要）页面包含以下字段：

“Refresh Rate” （刷新率） — 表示刷新接口统计数据之前经过的时间。

“Interface” （接口） — 接口编号。

“Interface Status” （接口状态） — 接口的状态。

“Received Unicast Packets” （接收到的单点传送信息包） — 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） — 从接口发送的单点传送信息包的数量。

“Received Non Unicast Packets”（接收到的非单点传送信息包）— 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）— 从接口发送的非单点传送信息包的数量。

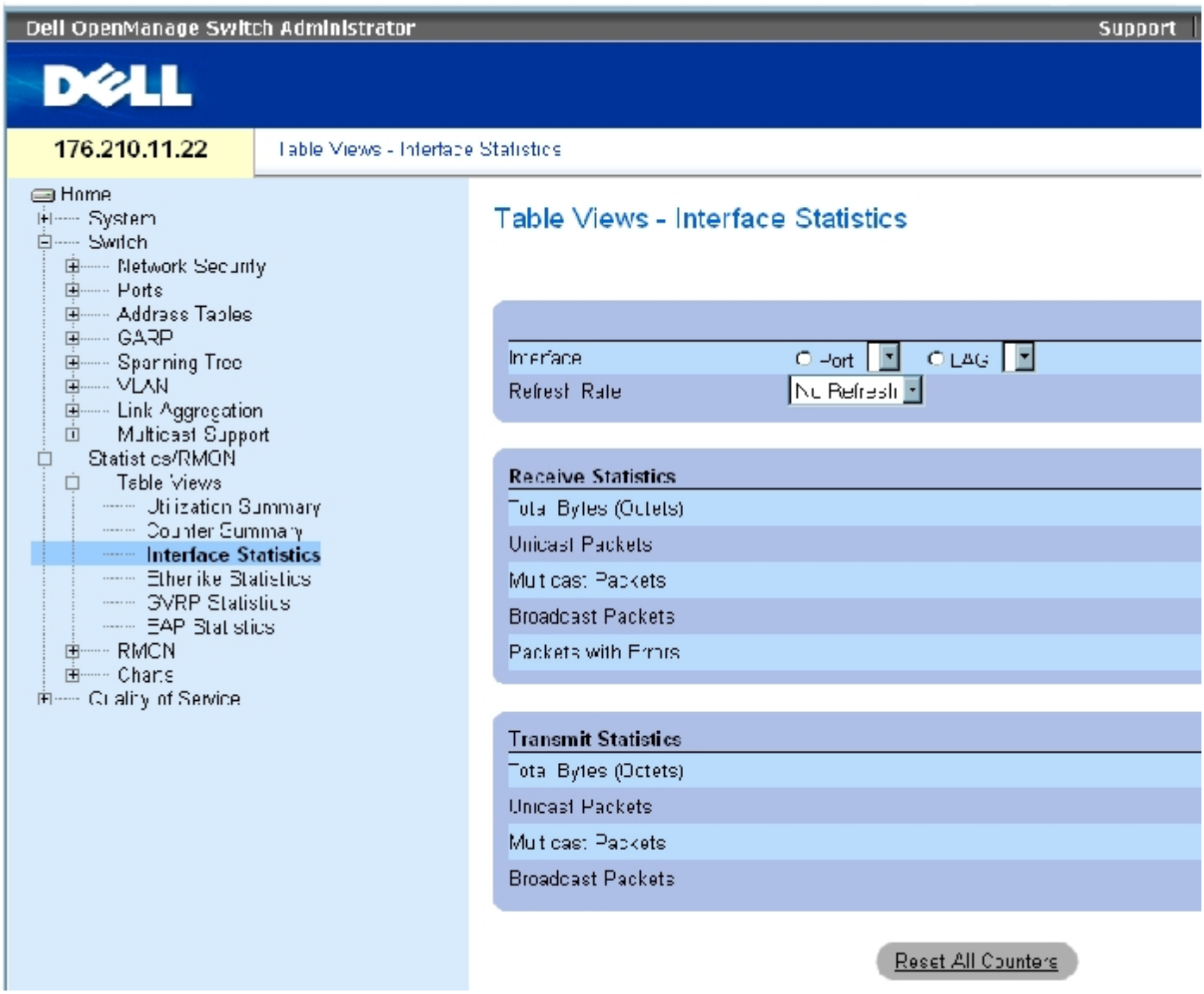
“Received Errors”（接收到的错误）— 接口上接收到的错误信息包的数量。

“Global System LAGs”（全局系统 LAG）— 提供用于全局系统 LAG 的计数器摘要。

查看接口统计数据

“Interface Statistics”（接口统计数据）页面包含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。要打开“Interface Statistics”（接口统计数据）页面，请在树视图中单击“Statistics/RMON”（统计数据/RMON）→“Table Views”（表视图）→“Interface Statistics”（接口统计数据）。

图 8-3. 接口统计数据



“Interface Statistics”（接口统计数据）页面包含以下字段：

“Interface”（接口）— 指定显示的是端口还是 LAG 的统计数据。

“Refresh Rate”（刷新率）— 刷新接口统计数据之前经过的时间。

接收统计数据

“Total Bytes (Octets)”（总字节数 [八位位组]）— 选定接口上接收到的八位位组的数量。

“Unicast Packets”（单点传送信息包）— 选定接口上接收到的单点传送信息包的数量。

“Multicast Packets”（多点传送信息包）— 选定接口上接收到的多点传送信息包的数量。

“Broadcast Packets”（广播信息包）— 选定接口上接收到的广播信息包的数量。

发送统计数据

“Total Bytes (Octets)”（总字节数 [八位位组]）— 选定接口上发送的八位位组的数量。

“Unicast Packets”（单点传送信息包）— 选定接口上发送的单点传送信息包的数量。

“Multicast Packets”（多点传送信息包）— 选定接口上发送的多点传送信息包的数量。

“Broadcast Packets”（广播信息包）— 选定接口上发送的广播信息包的数量。

显示接口统计数据

1. 打开“Interface Statistics”（接口统计数据）页面。
2. 在“Interface”（接口）字段中选择接口。

   系统将显示选定接口的接口统计数据。

重设接口统计数据计数器

1. 打开“Interface Statistics”（接口统计数据）页面。
2. 单击“Reset All Counters”（重设所有计数器）。

   系统将重设接口统计数据计数器。

使用 CLI 命令查看接口统计数据

下表包含用于查看接口统计数据的 CLI 命令。

表 8-95. 接口统计数据的 CLI 命令

CLI 命令	说明
show interfaces counters [**ethernet** 接口 | **port-channel** 端口信道号]	显示经由物理接口的通信。

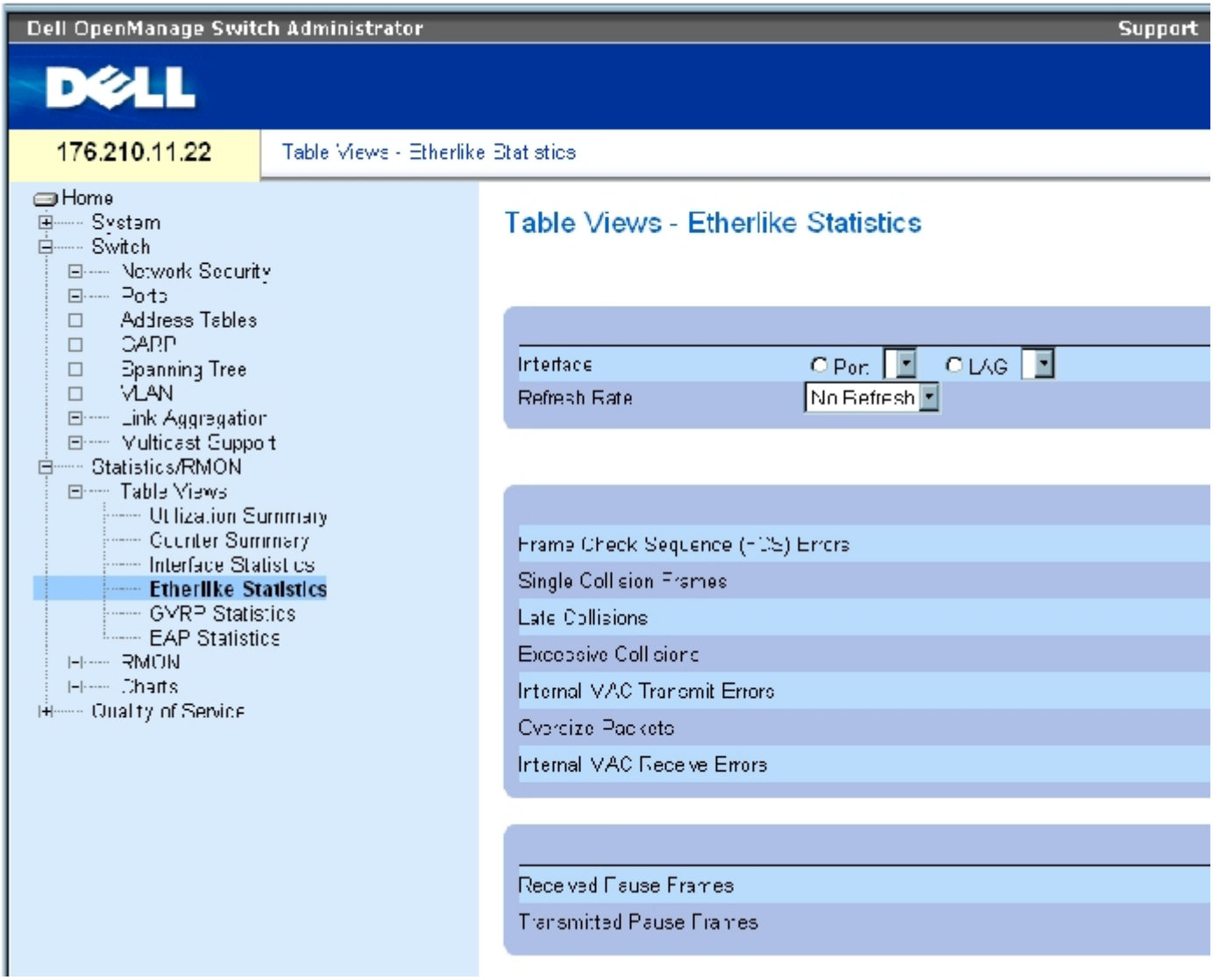
以下是 CLI 命令的示例。

```
console> enable

console# show interfaces counters

Port InOctets InUcastPkts InMcastPkts InBcastPkts

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

1/e1 0 0 0 0

1/e2 0 0 0 0

1/e3 0 0 0 0

1/e4 0 0 0 0

1/e5 0 0 0 0

1/ e6 0 0 0 0

1/e7 0 0 0 0

1/e8 0 0 0 0

1/e9 0 0 0 0

1/e10 0 0 0 0
```

查看以太网类统计数据

“Etherlike Statistics”（以太网类统计数据）页面包含接口错误统计数据。要打开“Etherlike Statistics”（以太网类统计数据）页面，请在树视图中单击“Statistics/RMON”（统计数据/RMON）→“Table Views”（表视图）→“Etherlike Statistics”（以太网类统计数据）。

图 8-4. 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）— 指定显示的是端口还是 LAG 的统计数据。

“Refresh Rate”（刷新率）— 刷新接口统计数据之前经过的时间。

“Frame Check Sequence (FCS) Errors”（帧检查顺序 [FCS] 错误）— 选定接口上接收到的 FCS 错误的数量。

“Single Collision Frames”（单冲突帧）— 选定接口上接收到的单冲突帧错误的数量。

“Late Collision”（推迟冲突）— 选定接口上接收到的推迟冲突的数量。

“Oversize Packets”（超大信息包）— 选定接口上超大信息包的数量。

“Internal MAC Transmit Errors”（内部 MAC 发送错误）— 选定接口上内部 MAC 发送错误的数量。

“Received Pause Frames”（接收到的暂停帧）— 选定接口上接收到的暂停错误的数量。

“Transmitted Pause Frames”（发送的暂停帧）— 选定接口发送的暂停错误的数量。

显示接口的以太网类统计数据

1. 打开“Etherlike Statistics”（以太网类统计数据）页面。
2. 在“Interface”（接口）字段中选择接口。

重设以太网类统计数据

1. 打开“Etherlike Statistics”（以太网类统计数据）页面。
2. 单击“Reset All Counters”（重设所有计数器）。

系统将重设“Etherlike Statistics”（以太网类统计数据）计数器。

使用 CLI 命令查看以太网类统计数据

下表包含用于查看以太网类统计数据的 CLI 命令。

表 8-96. 以太网类统计数据 CLI 命令

CLI 命令	说明
show interfaces counters [ethernet 接口 **| port-channel** 端口信道号**]**	显示经由物理接口的通信。

以下是 CLI 命令的示例。

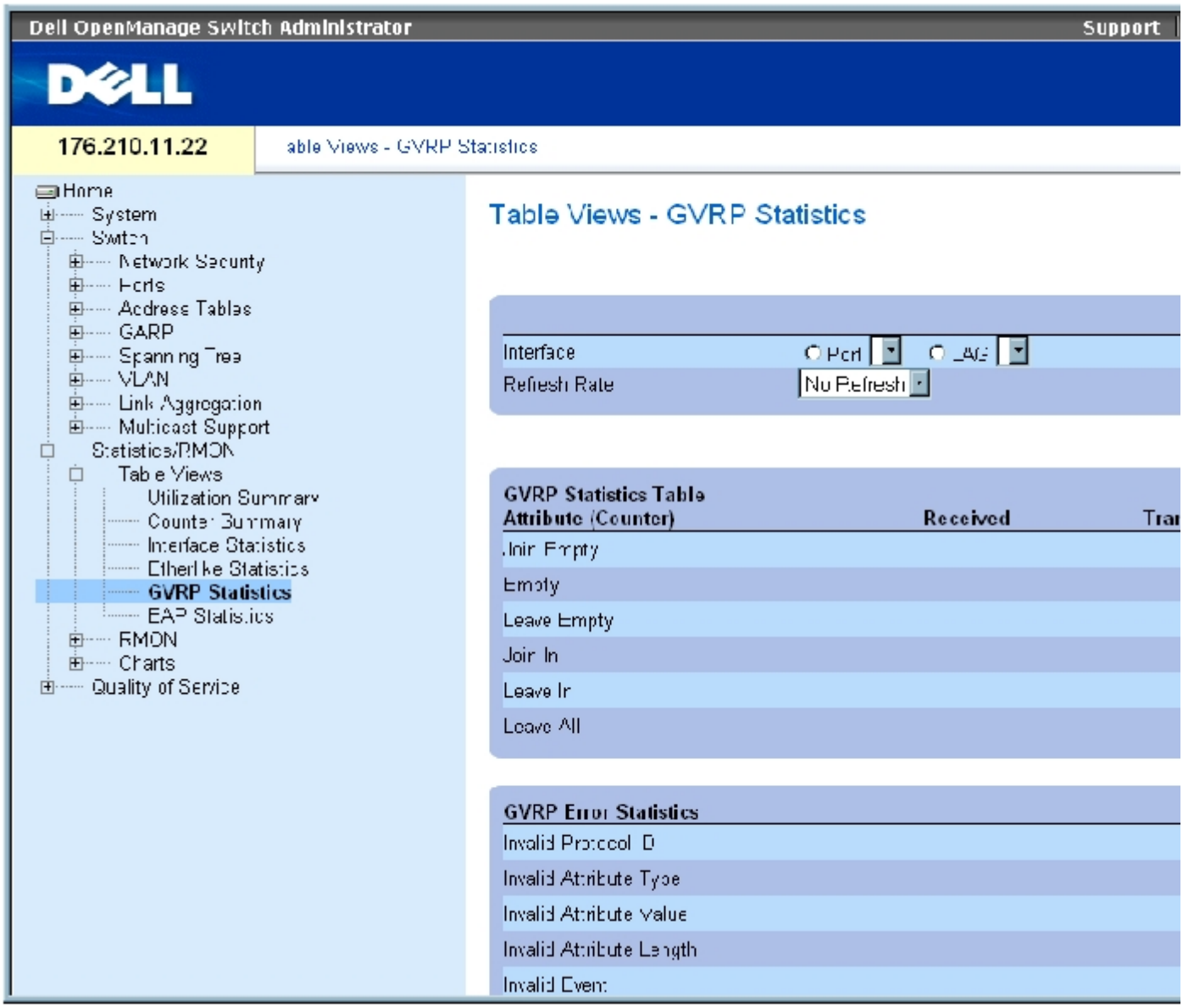
```
Console# show interfaces counters ethernet 1/1

Port    IN Octets    InUcastPkts    InMcastPkts    InBcastPkts
---     -------      -----------    -----------    -----------
```

-	--	-	-	-
1/e1	183892	1289	987	8
Port	OUT Octets	OutUcastPkts	OutMcastPkts	OutBcastPkts
---	----------	----------	----------	----------
1/e1	9188	9	8	0
FCS Errors: 8				
Single Collision Frames: 0				
Multiple Collision Frames: 0				
SQE Test Errors: 0				
Deferred Transmissions: 0				
Late Collisions: 0				
Excessive Collisions: 0				
Internal MAC Tx Errors: 0				
Carrier Sense Errors: 0				
Oversize Packets: 0				
Internal MAC Rx Errors: 0				
Received Pause Frames: 0				
Transmitted Pause Frames: 0				

查看 GVRP 统计数据

“GVRP Statistics” (GVRP 统计数据) 页面包含 GVRP 的设备统计数据。要打开该页面，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 8-5. GVRP 统计数据



“GVRP Statistics” (GVRP 统计数据) 页面包含以下字段：

“Interface” (接口) — 指定显示的是端口还是 LAG 的统计数据。

“Refresh Rate” (刷新率) — 刷新接口统计数据之前经过的时间。

“Join Empty” (加入空) — 设备的 GVRP 加入空统计数据。

“Leave Empty” (保留空) — 设备的 GVRP 保留空统计数据。

“Empty” (空) — 表示空 GVRP 统计数据的数量。

“Join In” (加入) — 设备的 GVRP 加入统计数据。

“Leave In”（保留）— 设备的 GVRP 保留统计数据。

“Leave All”（全部离开）— 设备的 GVRP 全部离开统计数据。

“Invalid Protocol ID”（无效协议 ID）— 设备的 GVRP 无效协议 ID 统计数据。

“Invalid Attribute Type”（无效属性类型）— 设备的 GVRP 无效属性 ID 统计数据。

“Invalid Attribute Value”（无效属性值）— 设备的 GVRP 无效属性值统计数据。

“Invalid Attribute Length”（无效属性长度）— 设备的 GVRP 无效属性长度统计数据。

“Invalid Events”（无效事件）— 设备的 GVRP 无效事件统计数据。

显示端口的 GVRP 统计数据

1. 打开“GVRP Statistics”（GVRP 统计数据）页面。
2. 在“Interface”（接口）字段中选择接口。

   系统将显示选定接口的 GVRP 统计数据。

重设 GVRP 统计数据

1. 打开“GVRP Statistics”（GVRP 统计数据）页面。
2. 单击“Reset All Counters”（重设所有计数器）。

   系统将重设 GVRP 统计数据计数器。

使用 CLI 命令查看 GVRP 统计数据

下表包含用于查看 GVRP 统计数据的 CLI 命令。

表 8-97. GVRP 统计数据 CLI 命令

CLI 命令	说明
show gvrp statistics [**ethernet** 接口| **port-channel** 端口信道号]	显示 GVRP 统计数据。
show gvrp error- statistics [**ethernet** 接口	**port-channel** 端口信道号]	显示 GVRP 错误统计数据。

以下是 CLI 命令的示例：

```
console# show gvrp statistics

GVRP statistics:

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

Legend:

rJE :Join Empty Received

rJIn :Join In Received

rEmp :Empty Received

rLIn :Leave In Received

rLE :Leave Empty Received

rLA :Leave All Received

sJE :Join Empty Sent

sJIn :Join In Sent

sEmp :Empty Sent

sLIn :Leave In Sent

sLE :Leave Empty Sent

sLA :Leave All Sent
```

```
Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn
sLE sLA

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

1/e1 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0
1/e3 0 0 0 0 0 0 0 0 0 0 00 0
```

```

```

```
Console# show gvrp error-statistics
```

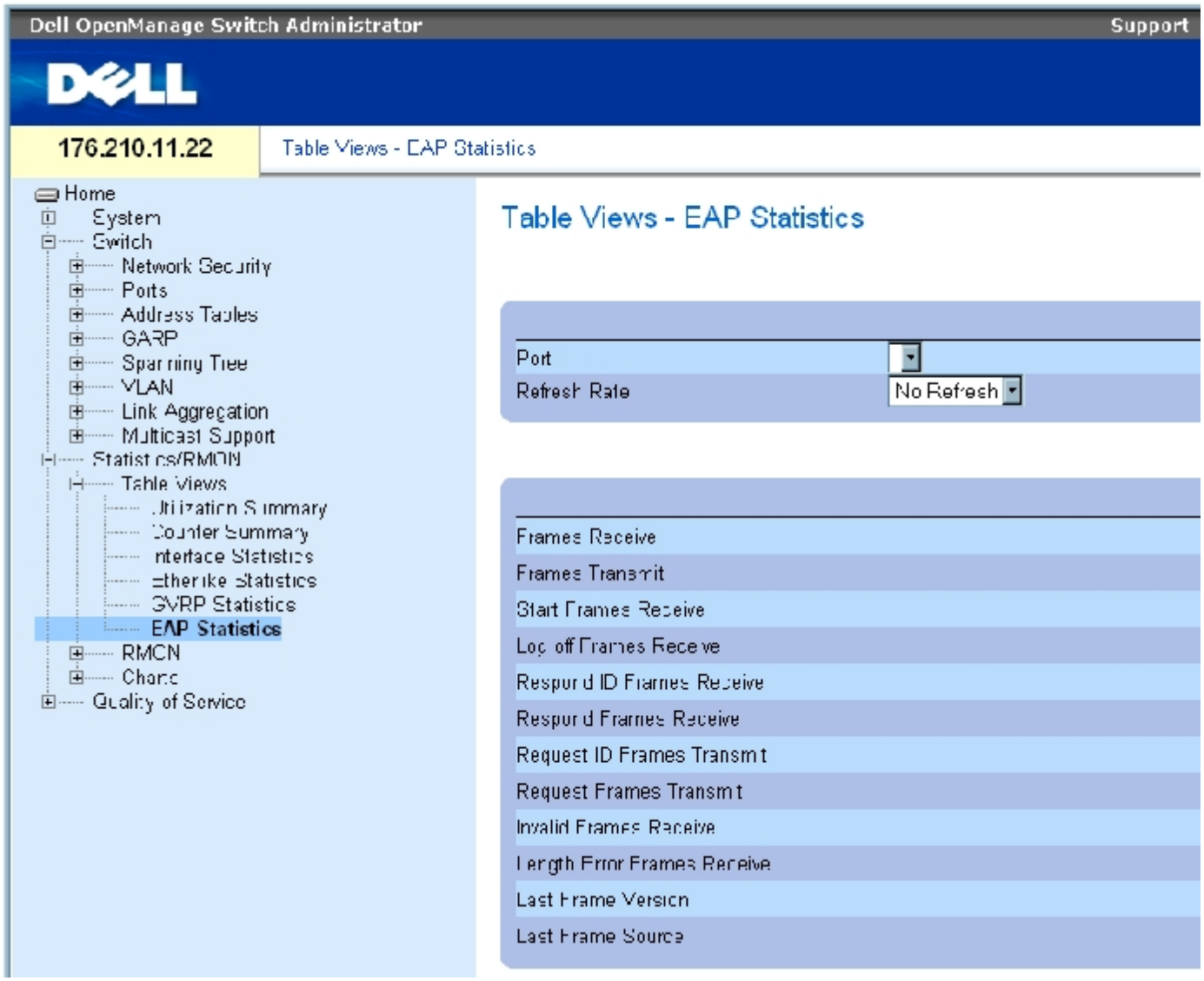
```
GVRP error statistics:

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

Legend:

INVPROT :Invalid Protocol Id

INVPLEN :Invalid PDU Length

INVATYP :Invalid Attribute Type

INVALEN :Invalid Attribute Length

INVAVAL :Invalid Attribute Value

INVEVENT :Invalid Event

Port INVPROT INVATYP INVAVAL INVPLEN INVALEN INVEVENT

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

1/e1 0 0 0 0 0 0

1/e2 0 0 0 0 0 0

1/e3 0 0 0 0 0 0

1/e4 0 0 0 0 0 0
```

```
sLE :Leave Empty Sent

sLA :Leave All Sent

Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn
sLE sLA

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

1/e1 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0 0 0 0 0 0

1/e5 0 0 0 0 0 0 0 0 0 0 0 0

1/e6 0 0 0 0 0 0 0 0 0 0 0 0

1/e7 0 0 0 0 0 0 0 0 0 0 0 0

1/e8 0 0 0 0 0 0 0 0 0 0 0 0
```

查看 EAP 统计数据

“EAP Statistics” (EAP 统计数据) 页面包含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“配置基于端口的验证”。要打开“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 8-6. EAP 统计数据



“EAP Statistics” (EAP 统计数据) 页面包含以下字段：

“Port” (端口) — 表示对其进行轮询以获得统计数据的端口。

“Refresh Rate” (刷新率) — 刷新接口统计数据之前经过的时间。

“Frames Receive”（接收到的帧）— 表示端口上接收到的有效 EAPOL 帧的数量。

“Frames Transmit”（发送的帧）— 表示通过端口发送的 EAPOL 帧的数量。

“Start Frames Receive”（接收到的启动帧）— 表示端口上接收到的 EAPOL 启动帧的数量。

“Log off Frames Receive”（接收到的注销帧）— 表示端口上接收到的 EAPOL 注销帧的数量。

“Respond ID Frames Receive”（接收到的响应 ID 帧）— 表示端口上接收到的 EAP 响应/ID 帧的数量。

“Respond Frames Receive”（接收到的响应帧）— 表示端口上接收到的有效 EAP 响应帧的数量。

“Request ID Frames Transmit”（发送的请求 ID 帧）— 表示端口发送的 EAP 请求/ID 帧的数量。

“Request Frames Transmit”（发送的请求帧）— 表示通过端口发送的 EAP 请求帧的数量。

“Invalid Frames Receive”（接收到的无效帧）— 表示端口上接收到的无法识别的 EAPOL 帧的数量。

“Length Error Frames Receive”（接收到的长度错误帧）— 表示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 Frame Version”（上一帧版本）— 表示与最近一次接收到的 EAPOL 帧相关的协议版本号。

“Last Frame Source”（上一帧的源）— 表示与最近一次接收到的 EAPOL 帧相关的源 MAC 地址。

显示端口的 EAP 统计数据

1. 打开“EAP Statistics”（EAP 统计数据）页面。
2. 在“Interface”（接口）字段中选择接口。

系统将显示接口 EAP 统计数据。

重设 EAP 统计数据

1. 打开“EAP Statistics”（EAP 统计数据）页面。
2. 单击“Reset All Counters”（重设所有计数器）。

系统将重设 EAP 统计数据计数器。

使用 CLI 命令查看 EAP 统计数据

下表概括了用于查看 EAP 统计数据的 CLI 命令。

表 8-98. EAP 统计数据 CLI 命令

CLI 命令	说明
show dot1x statistics	显示指定接口的 802.1X 统计数据。

以下是 CLI 命令的示例：

```
console# show dot1x statistics ethernet 1/e1

EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource:0008.3b79.8787
```

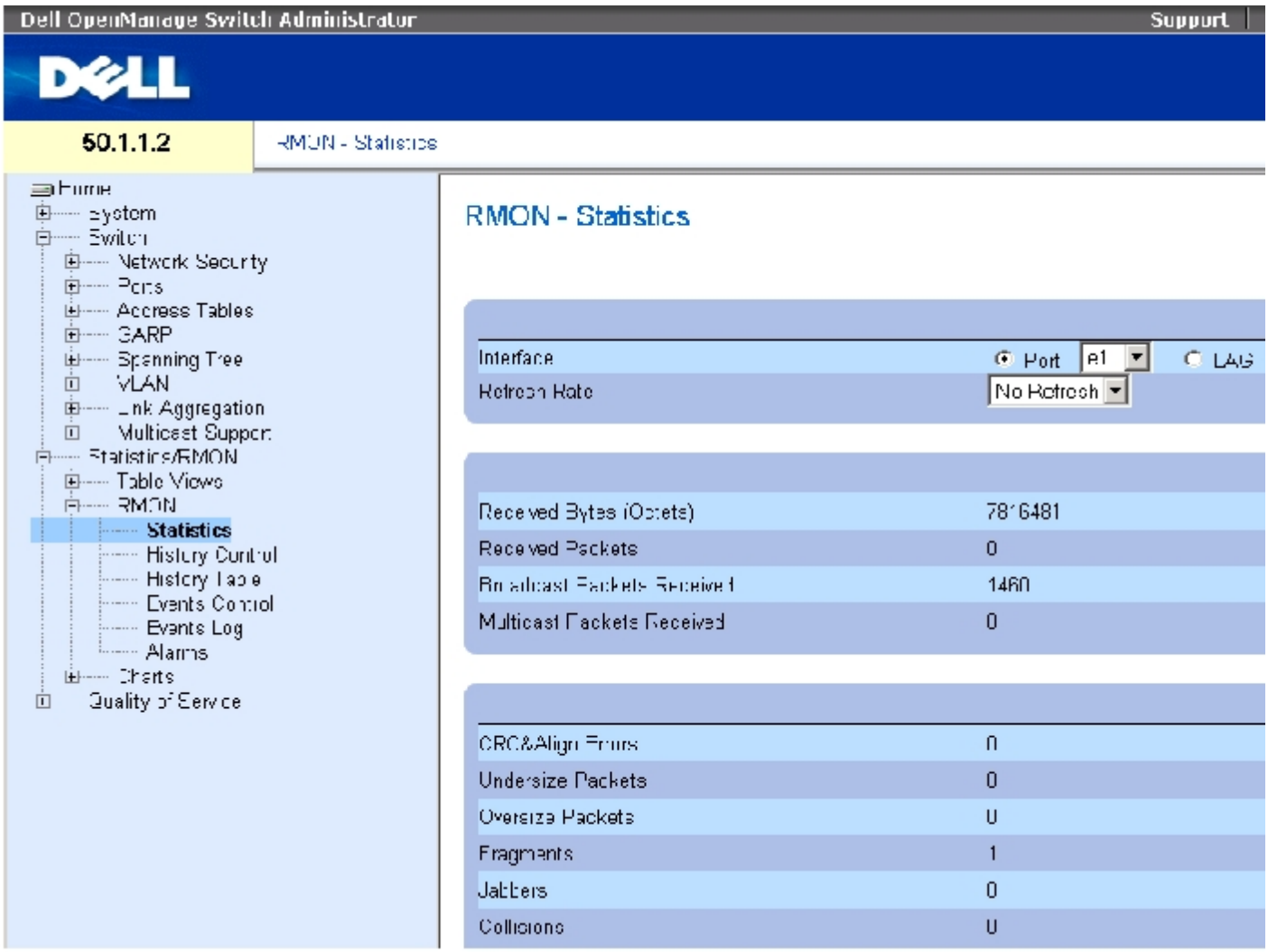
查看 RMON 统计数据

远程监测（RMON）使网络管理员可以从远程位置查看网络信息。要打开“RMON”页面，请在树视图中单击“Statistics/RMON”（统计数据/RMON）→“RMON”。

查看 RMON 统计数据组

使用“RMON Statistics”（RMON 统计数据）页面可以查看有关设备使用和设备上出现的错误的信息。要打开“RMON Statistics”（RMON 统计数据）页面，请在树视图中单击“Statistics/RMON”（统计数据/RMON）→“RMON”→“Statistics”（统计数据）。

图 8-7. RMON 统计数据



“RMON Statistics”（RMON 统计数据）页面包含以下字段：

“Interface”（接口）— 指定显示的是端口还是 LAG 的统计数据。

“Refresh Rate”（刷新率）— 刷新统计数据之前经过的时间。

“Received Bytes (Octets)”（接收到的字节 [八位位组]）— 选定接口上接收到的字节的数量。

“Received Packets”（接收到的信息包）— 选定接口上接收到的信息包的数量。

“Broadcast Packets Received”（接收到的广播信息包）— 自上一次刷新设备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”（接收到的多点传送信息包）— 自上一次刷新设备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）— 自上一次刷新设备以来接口上发生的 CRC 和校准错误的数量。

“Undersize Packets”（超小信息包）— 自上一次刷新设备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）— 自上一次刷新设备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）— 自上一次刷新设备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）— 自上一次刷新设备以来接口上接收到的无用信息（超过 1518 个八位位组的信息包）的数量。

“Collisions”（冲突）— 自上一次刷新设备以来接口上接收到的冲突的数量。

“Frames of xx Bytes”（xx 字节的帧）— 自上一次刷新设备以来接口上接收到的 xx 字节帧的数量。

查看接口统计数据

1. 打开“RMON Statistics”（RMON 统计数据）页面。
2. 在“Interface”（接口）字段中选择接口类型和编号。

   系统将显示接口统计数据。

使用 CLI 命令查看 RMON 统计数据

下表包含用于查看 RMON 统计数据的 CLI 命令。

表 8-99. RMON 统计数据 CLI 命令

CLI 命令	说明
show rmon statistics {ethernet 接口 **| port-channel** 端口信道号**}**	显示 RMON 以太网统计数据。

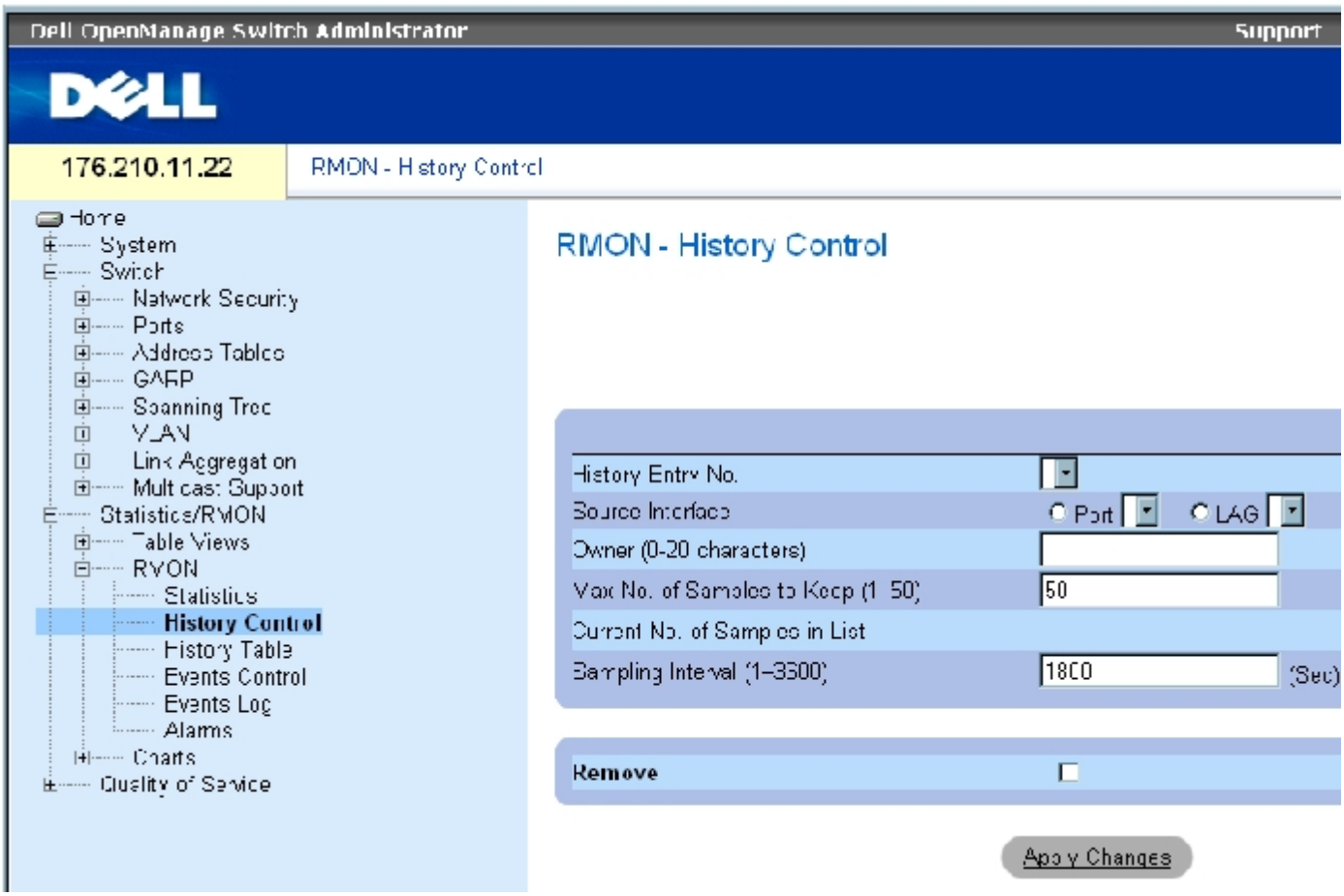
以下是 CLI 命令的示例：

```
console# show rmon statistics ethernet 1/e1

Port 1/e1

Dropped:8

Octets:878128 Packets:978

Broadcast:7 Multicast:1

CRC Align Errors:0 Collisions:0

Undersize Pkts:0 Oversize Pkts:0

Fragments:0 Jabbers:0

64 Octets:98 65 to 127 Octets:0

128 to 255 Octets:0 256 to 511 Octets:0

512 to 1023 Octets:491 1024 to 1518 Octets: 389
```

查看 RMON 历史记录控制统计数据

“RMON History Control” (RMON 历史记录控制) 包含有关从端口获取的数据样例的信息。例如，样例可能包含接口定义或轮询周期。要打开“RMON History Control” (RMON 历史记录控制) 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 8-8. 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 No.”（历史记录条目号） — “History Control”（历史记录控制）页面的条目号。

“Source Interface”（源接口） — 获取历史记录样例的端口或 LAG。

“Owner (0-20 characters)”（所有者 [0 至 20 个字符]） — 请求 RMON 信息的 RMON 站点或用户。

“Max No. of Samples to Keep (1-50)”（要保留的最大样例数 [1 至 50]） — 要保存的样例的数量。默认值为 50。

“Current No. of Samples in List”（当前列表中的样例数） — 表示当前获取的样例数。

“Sampling Interval (1-3600)”（取样间隔 [1 至 3600]） — 表示从端口取样的时间间隔（以秒为单位）。可能的值为 1 至 3600 秒。默认值为“1800”秒（30 分钟）。

“Remove”（删除） — 如果选取此字段，将删除“History Control Table”（历史记录控制表）条目。

添加历史记录控制条目

1. 打开“RMON History Control”（RMON 历史记录控制）页面。
2. 单击“Add”（添加）。

   系统将打开“Add History Entry”（添加历史记录条目）页面。
3. 完成对话框中的字段。
4. 单击“Apply Changes”（应用更改）。

   条目将被添加至历史记录控制表。

修改历史记录控制表条目

1. 打开“RMON History Control”（RMON 历史记录控制）页面。
2. 在“History Entry No.”（历史记录条目号）字段中选择一个条目。
3. 根据需要修改字段
4. 单击“Apply Changes”（应用更改）。

   系统将修改表条目，并更新设备。

删除历史记录控制表条目

1. 打开“RMON History Control”（RMON 历史记录控制）页面。
2. 在“History Entry No.”（历史记录条目号）字段中选择一个条目。
3. 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

下表包含用于查看 RMON 历史记录控制的 CLI 命令。

表 8-100. RMON 历史记录 CLI 命令

CLI 命令	说明
rmon collection history 索引 [**owner** 所有者名称 | **buckets** 存储区号] [**interval** 秒]	在接口上启用和配置 RMON。
show rmon collection history [**ethernet** 接口 | **port-channel** 端口信道号]	显示 RMON 收集历史纪录统计数据。

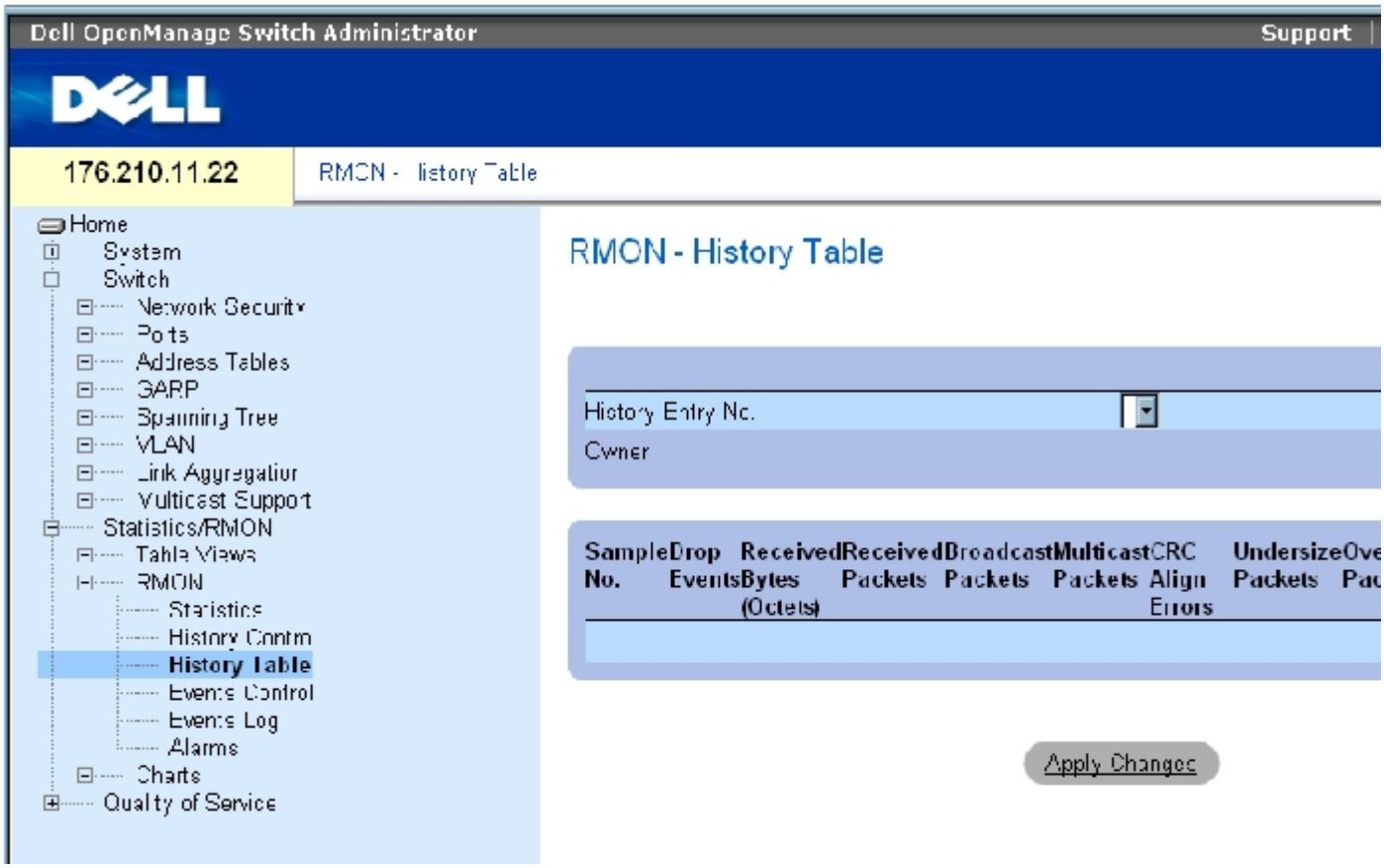
以下是 CLI 命令的示例：

```
console(config)# interface ethernet 1/e8

console(config-if)# rmon collection history 1
interval 2400
```

查看 RMON 历史记录表

“RMON History Table” (RMON 历史记录表) 包含接口特定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。要打开“RMON History Table” (RMON 历史记录表)，请在树视图中单击“Statistics/RMON” (统计数据/RMON) → “RMON” → “History Table” (历史记录表)。

图 8-9. RMON 历史记录表



“RMON History Table” (RMON 历史记录表) 页面包含以下字段：

注：并非所有字段都显示在 RMON 历史记录表中。

“History Entry No.” (历史记录条目号) —指定“History Control” (历史记录控制) 页面的条目号。

“Owner” (所有者) — 表示请求 RMON 信息的 RMON 站点或用户。

“Sample No.” (样例号) — 表示表中信息反映的特定样例的数量。

“Drop Events” (丢弃事件) — 在取样间隔期间由于缺少网络资源而导致被丢弃的信息包的数量。此字段可能并不表示丢弃的信息包的确切数量，而是检测到丢弃信息包的次数。

“Received Bytes (Octets)” (接收到的字节 [八位位组]) — 网络上接收到的数据八位位组 (包括坏信息包) 的数量。

“Received Packets” (接收到的信息包) — 取样间隔期间接收到的信息包的数量。

“Broadcast Packets” (广播信息包) — 在取样间隔期间接收到的完好广播信息包的数量。

“Multicast Packets” (多点传送信息包) — 取样间隔期间接收到的完好多点传送信息包的数量。

“CRC Align Errors”（CRC 校准错误）— 取样会话过程中接收到的长度为 64 至 1518 个八位位组的信息包的数量。但是，这些信息包带有包含整数个八位位组的坏信息包校验序列 (FCS)，或带有包含非整数个八位位组的坏 FCS。

“Undersized Packets”（超小信息包）— 取样会话期间接收到的长度小于 64 个八位位组的信息包的数量。

“Oversize Packets”（超大信息包）— 取样会话期间接收到的长度大于 1518 个八位位组的信息包的数量。

“Fragments”（碎片）— 取样会话期间接收到的长度小于 64 个八位位组并带有 FCS 的信息包的数量。

“Jabbers”（无用信息）— 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）— 估计在取样会话期间发生的信息包冲突的总数。当中继器端口检测到有两个或多个站点同时进行发送时，即检测到冲突。

“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

1. 打开“RMON History Table”（RMON 历史记录表）。
2. 在“History Entry No.”（历史记录条目号）字段中选择一个条目。

该条目的统计数据将显示在“RMON History Table”（RMON 历史记录表）中。

使用 CLI 命令查看 RMON 历史记录控制

下表包含用于查看 RMON 历史记录的 CLI 命令。

表 8-101. RMON 历史记录控制 CLI 命令

CLI 命令	说明
show rmon history 索引 {throughput | errors | other} [period 秒]	显示 RMON 以太网统计数据历史记录。

以下是用于显示索引 1 上的吞吐量的 RMON 以太网统计数据的 CLI 命令示例：

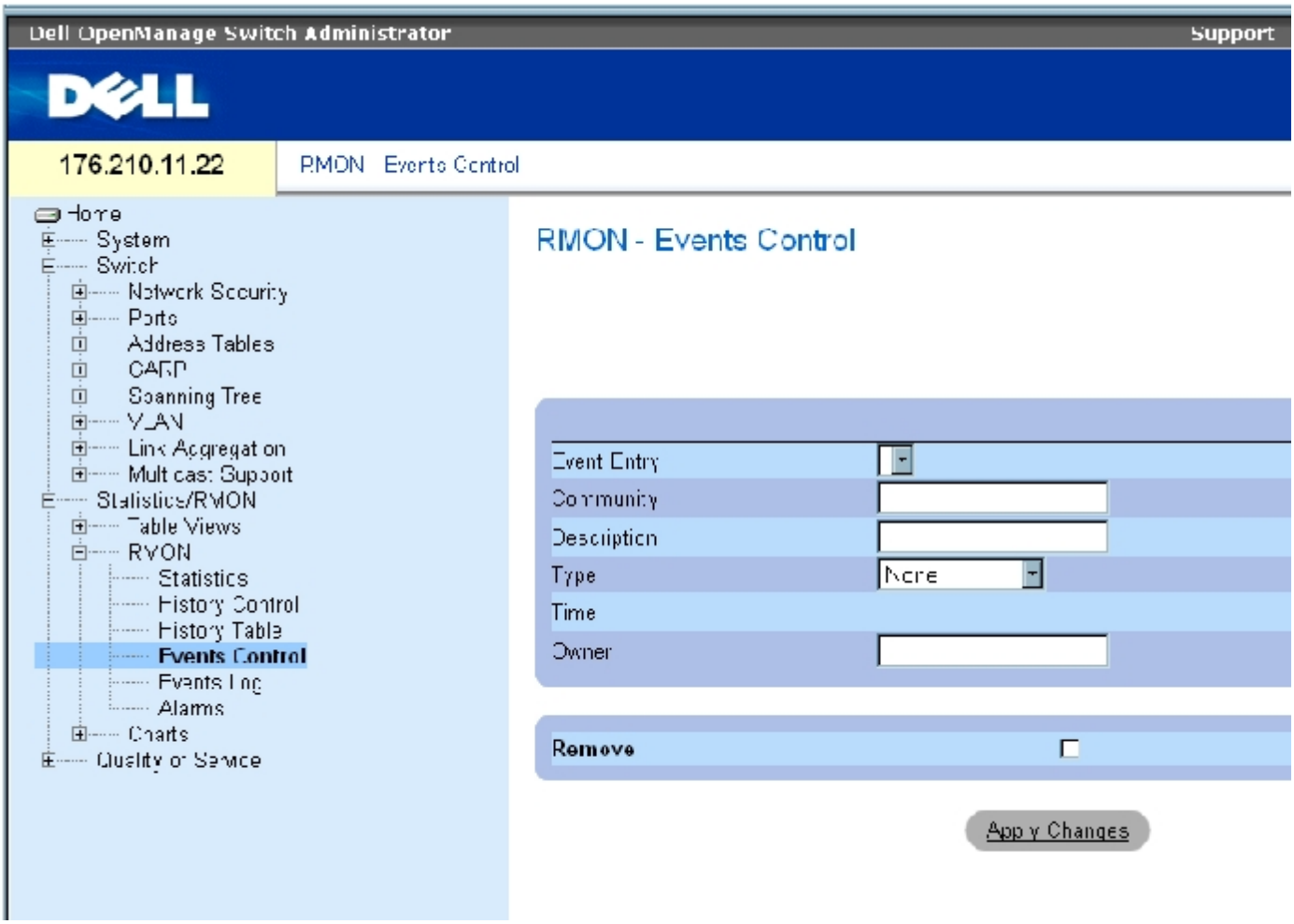
```
console> enable
```

```
console# show rmon history 1 throughput

Sample Set:5 Owner:cli

Interface:24 interval:10

Requested samples:50 Granted samples:50

Maximum table size:270

Time Octets Packets Broadcast Multicast %

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

09-Mar-2003 18:29:32 0 0 0 0 0

09-Mar-2003 18:29:42 0 0 0 0 0

09-Mar-2003 18:29:52 0 0 0 0 0

09-Mar-2003 18:30:02 0 0 0 0 0

09-Mar-2003 18:30:12 0 0 0 0 0

09-Mar-2003 18:30:22 0 0 0 0 0
```

定义设备 RMON 事件

使用“RMON Events Control” (RMON 事件控制) 页面可以定义 RMON 事件。要打开“RMON Events Control” (RMON 事件控制) 页面，请在树视图中单击“Statistics/RMON” (统计数据/RMON) → “RMON” → “Events Control” (事件控制) 。

图 8-10. RMON 事件控制



"RMON Events Control" (RMON 事件控制) 页面包含以下字段:

"Event Entry" (事件条目) — 表示事件。

"Community" (团体) — 事件所属的团体。

"Description" (说明) — 用户定义的事件说明。

"Type" (类型) — 说明事件的类型。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）— 事件发生的时间。

“Owner”（所有者）— 定义事件的设备或用户。

“Remove”（删除）— 如果选取此字段，将从“RMON Events Table”（RMON 事件表）中删除事件。

添加 RMON 事件

1. 打开“RMON Events Control”（RMON 事件控制）页面。
2. 单击“Add”（添加）。

   系统将打开“Add an Event Entry”（添加事件条目）页面。
3. 完成对话框中的信息并单击“Apply Changes”（应用更改）。

   系统将添加“Event Table”（事件表）条目，并更新设备。

修改 RMON 事件

1. 打开“RMON Events Control”（RMON 事件控制）页面。
2. 在“Event Table”（事件表）中选择一个条目。
3. 修改对话框中的字段并单击“Apply Changes”（应用更改）。

   系统将修改“Event Table”（事件表）条目，并更新设备。

删除 RMON 事件条目

1. 打开“RMON Events Control”（RMON 事件控制）页面。
2. 单击“Show All”（全部显示）。

系统将打开“RMON Events Table”（RMON 事件表）页面。

3. 对于需要删除的事件，选取“Remove”（删除）复选框，然后单击“Apply Changes”（应用更改）。

系统将删除表条目，并更新设备。

注：在“RMON Events Control”（RMON 事件控制）页面中，通过选取该页面上的“Remove”（删除）复选框可以删除单个事件条目。

使用 CLI 命令定义设备事件

下表包含用于定义设备事件的 CLI 命令。

表 8-102. 设备事件定义 CLI 命令

CLI 命令	说明
rmon event 索引类型 **[community** 文本] **[description** 文本] **[owner**名称]	配置 RMON 事件。
show rmon events	显示 RMON 事件表。

以下是 CLI 命令的示例：

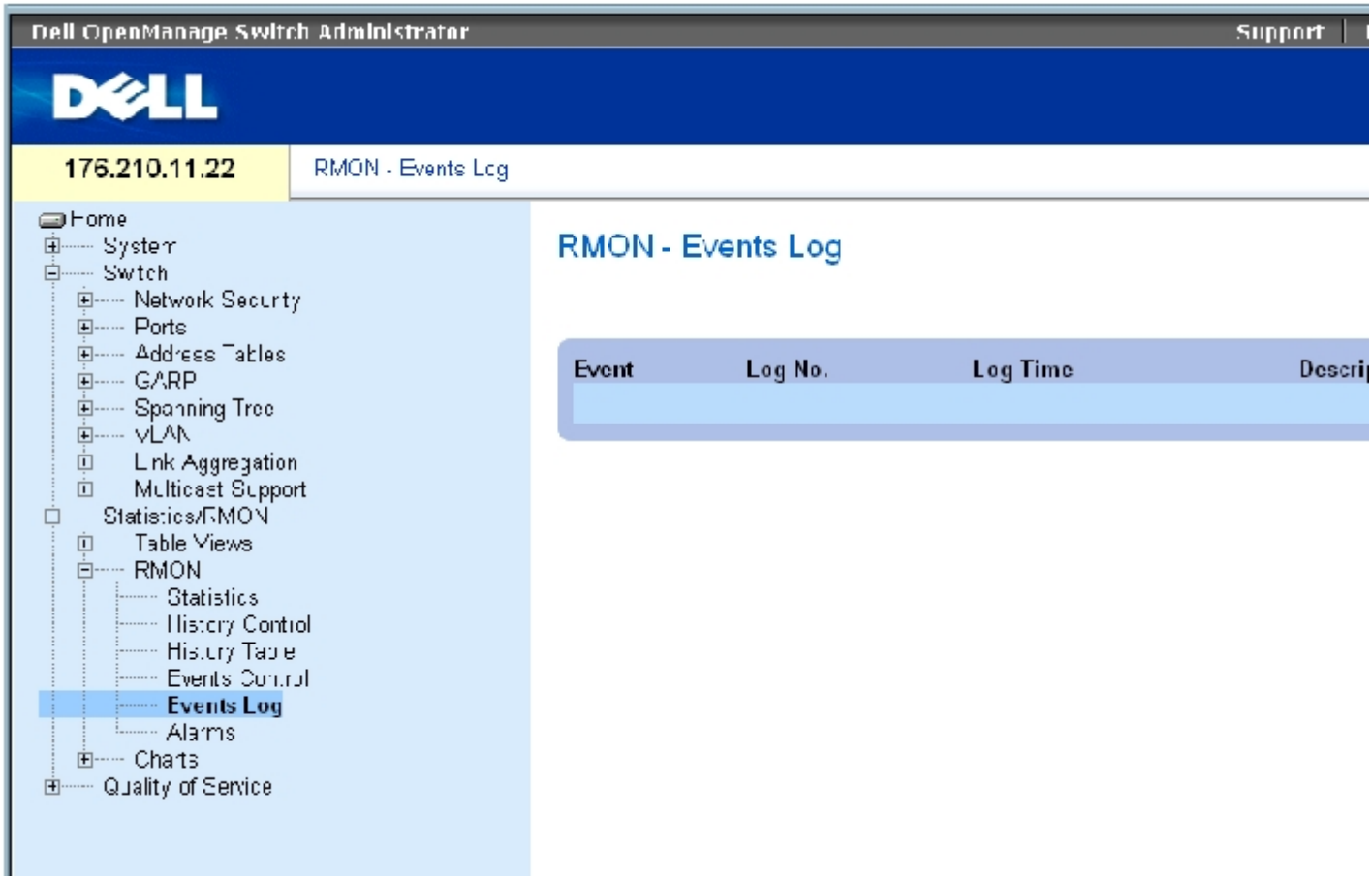
```
console (config)# rmon event 1 log

console(config)#exit

console# show rmon events

Index  Description  Type  Community  Owner  Last Time Sent
-----  -----------  ------  ---------  -------  ---------
1  Errors  Log    CLI  Jan 18 2002 23:58:17
2  High Broadcast  Log-Trap  router  Manager  Jan 18 2002 23:59:48
```

查看 RMON 事件日志

“RMON Events Log”（RMON 事件日志）页面包含 RMON 事件的列表。要打开“RMON Events Log”（RMON 事件日志）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 8-11. RMON 事件日志



“RMON Events Log”（RMON 事件日志）页面包含以下字段：

“Event”（事件）— RMON 事件日志条目号。

“Log No.”（日志号）— 日志编号。

“Log Time”（记录时间）— 输入日志条目的时间。

“Description”（说明）— 说明日志条目。

使用 CLI 命令定义设备事件

下表包含用于定义设备事件的 CLI 命令。

表 8-103. 设备事件定义 CLI 命令

CLI 命令	说明
show rmon log [事件]	显示 RMON 记录表。

以下是 CLI 命令的示例：

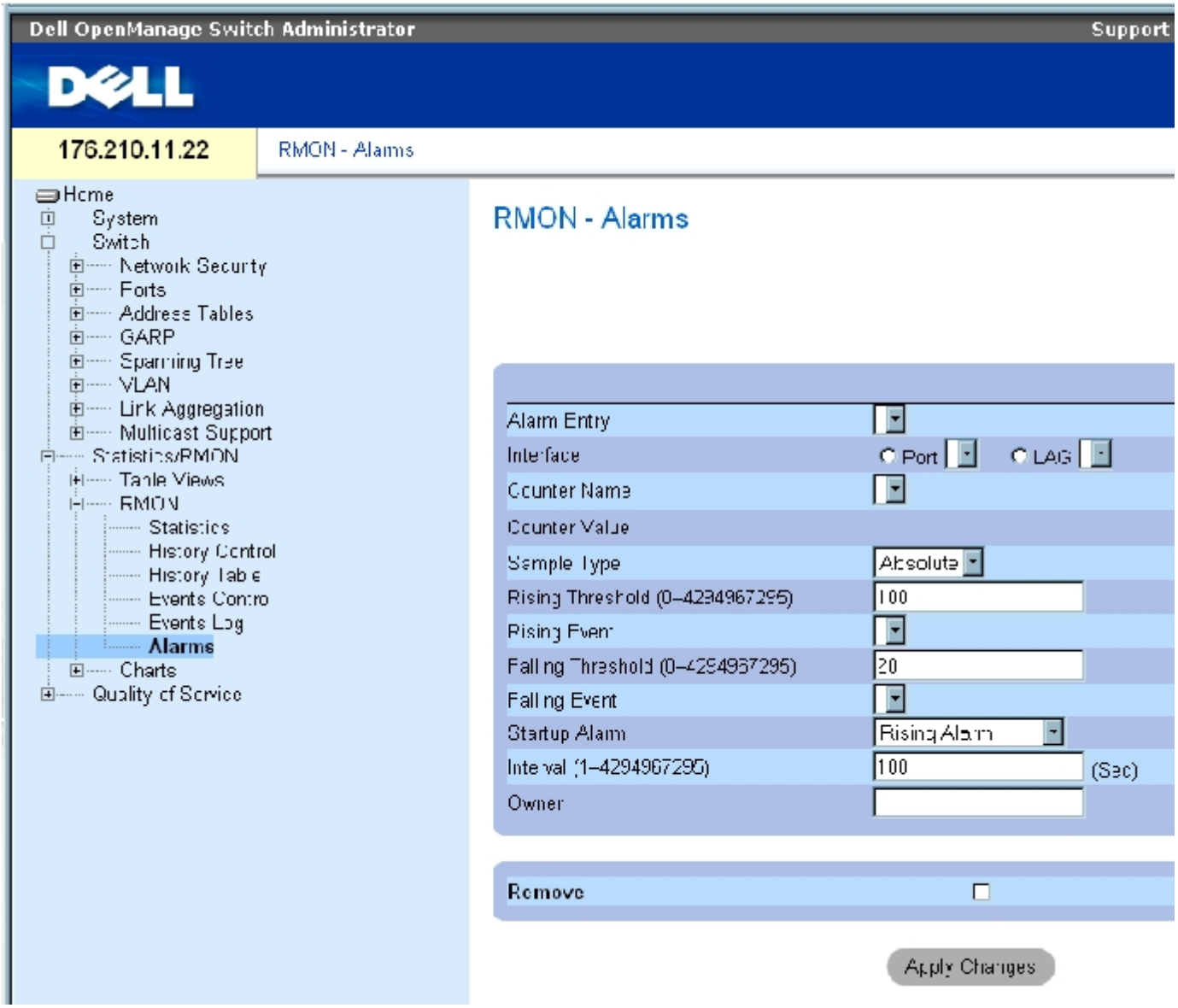
```
console (config)# rmon event 1 log

Console> show rmon log

Maximum table size:500

Event Description Time

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

1 Errors Jan 18 2002 23:58:17

2 High Broadcast Jan 18 2002 23:59:48
```

定义 RMON 设备警报

使用“RMON Alarms” (RMON 警报) 页面可以设置网络警报。当系统检测到网络问题或事件时就会发出网络警报。阈值上升和下降也会生成事件。有关事件的详细信息，请参阅“查看 RMON 事件日志”。

要打开“RMON Alarm” (RMON 警报) 页面，请在树视图中单击“Statistics/RMON” (统计数据/RMON) → “RMON” → “Alarms” (警报) 。

图 8-12. RMON 警报



“RMON Alarms” (RMON 警报) 页面包含以下字段：

“Alarm Entry” (警报条目) — 表示特定的警报。

“Interface” (接口) — 表示显示其 RMON 统计数据的接口。

“Counter Name” (计数器名称) — 表示选定的 MIB 变量。

“Counter Value” (计数器值) — 选定的 MIB 变量的值。

“Sample Type” (样例类型) — 指定选定变量的取样方法，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。

“Rising Threshold (0 - 4294967295)”（上升阈值 [0 至 4294967295]）— 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。字段默认值为 100 秒。

“Rising Event”（上升事件）— 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，则在设备或管理系统中均无保存机制。但是，如果不重启动设备，日志将保留在设备日志表中。如果选择陷阱，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 - 4294967295)”（下降阈值 [0 至 4294967295]）— 触发下降阈值警报的下降计数器值。下降阈值以图形方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。字段默认值为 20。

“Startup Alarm”（启动警报）— 用于激活警报生成的触发器。可以通过将阈值从较低阈值提升到较高阈值来定义上升。

“Interval (1 - 4294967295) (sec)”（时间间隔 [1 至 4294967295] [秒]）— 警报的间隔时间。字段默认值为 100 秒。

“Owner”（所有者）— 定义警报的设备或用户。

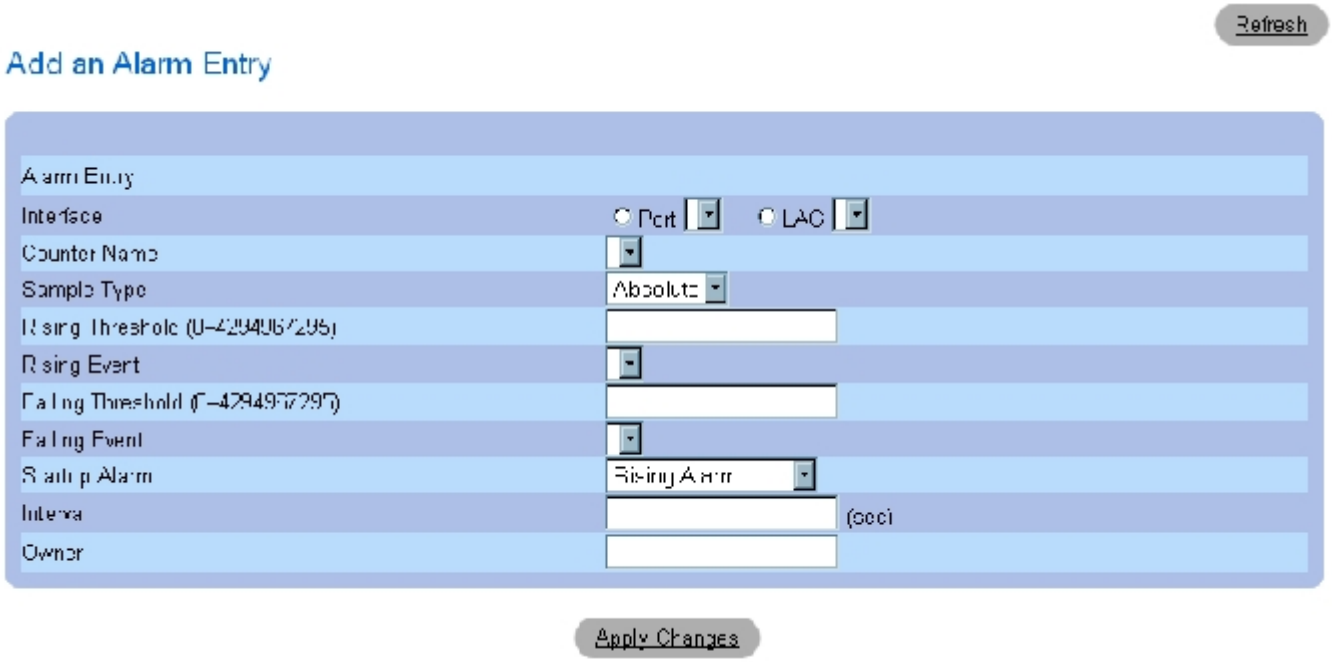
“Remove”（删除）— 如果选取此字段，将删除 RMON 警报。

添加警报表条目

1. 打开“RMON Alarms”（RMON 警报）页面。
2. 单击“Add”（添加）。

系统将打开“Add an Alarm Entry”（添加警报条目）页面：

图 8-13. “Add an Alarm Entry”（添加警报条目）页面



3. 选择接口。

4. 完成字段。

5. 单击“Apply Changes”（应用更改）。

系统将添加 RMON 警报，并更新设备。

修改警报表条目

1. 打开“RMON Alarms”（RMON 警报）页面。

2. 在“Alarm Entry”（警报条目）下拉式菜单中选择一个条目。

3. 修改字段。

4. 单击“Apply Changes”（应用更改）。

系统将修改条目，并更新设备。

显示警报表

1. 打开“RMON Alarms” (RMON 警报) 页面。
2. 单击“Show All” (全部显示) 。

   系统将打开“Alarm Table” (警报表) 。

删除警报表条目

1. 打开“RMON Alarms” (RMON 警报) 页面。
2. 在“Alarm Entry” (警报条目) 下拉式菜单中选择一个条目。
3. 选取“Remove” (删除) 复选框。
4. 单击“Apply Changes” (应用更改) 。

   系统将删除条目，并更新设备。

使用 CLI 命令定义设备警报

下表包含用于定义设备警报的 CLI 命令。

表 8-104. 设备警报 CLI 命令

CLI 命令	说明
rmon alarm 索引 **MIB_Object_ID** 时间间隔 上升阈值 下降阈值 上升事件 下降事件 **[type** 类型**] [startup** 方向**] [owner** 名称**]**	配置 RMON 警报条件。
show rmon alarm-table	显示警报表的摘要。
show rmon alarm	显示 RMON 警报配置。

以下是 CLI 命令的示例：

```
console(config)# rmon alarm 1000
1.3.6.1.2.1.2.2.1.10.1 360000 1000000 1000000 10 20

Console# show rmon alarm-table

Index OID Owner

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

1 1.3.6.1.2.1.2.2.1.10.1 CLI

2 1.3.6.1.2.1.2.2.1.10.1 Manager

3 1.3.6.1.2.1.2.2.1.10.9 CLI
```

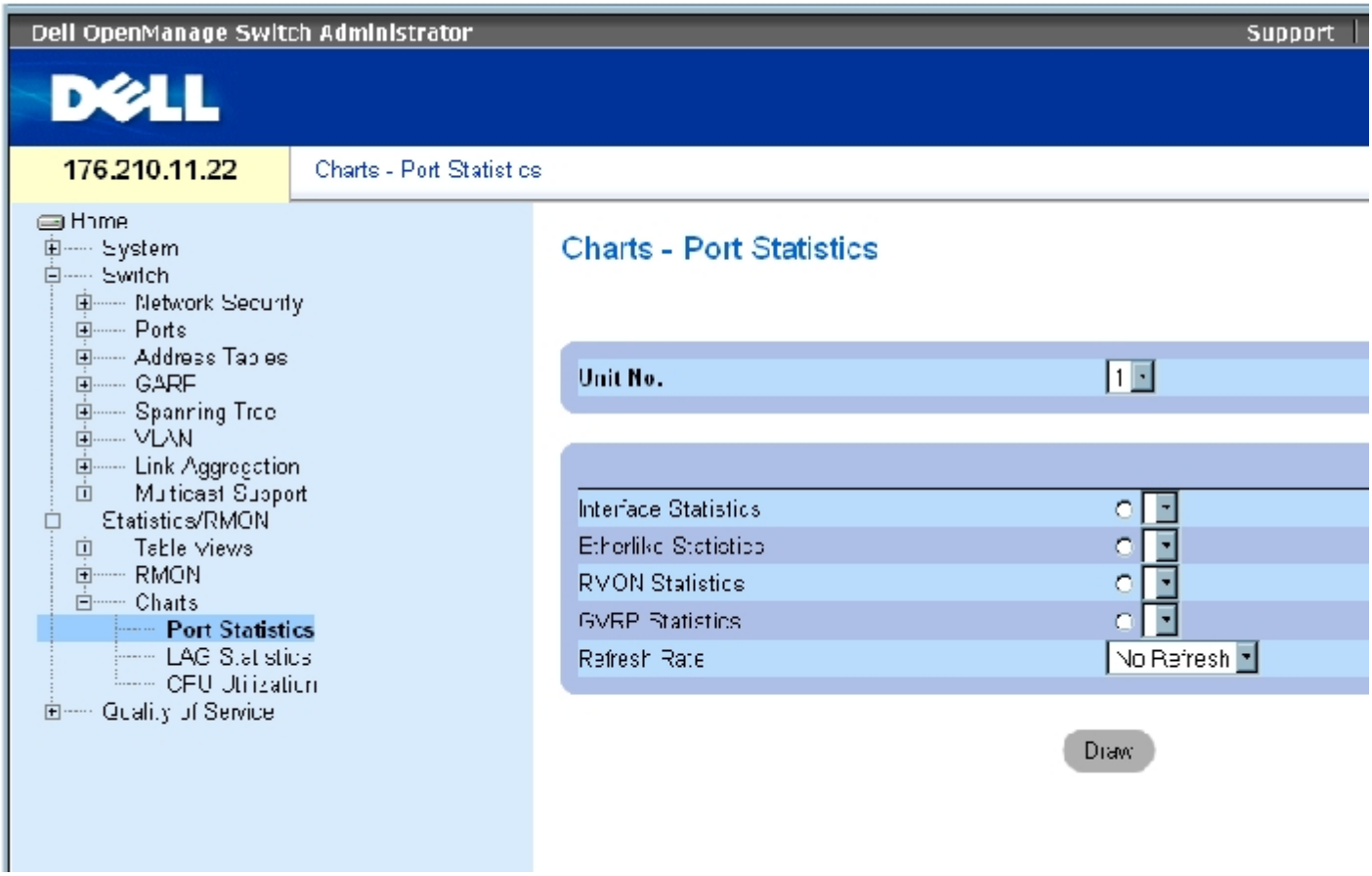
查看图表

“Chart”（图表）页面包含以图表格式显示统计数据的链接。要打开该页面，请在树视图中单击“Statistics”（统计数据）→“Charts”（图表）。

查看端口统计数据

使用“Port Statistics”（端口统计数据）页面可以以图表格式打开端口元素的统计数据。要打开“Port Statistics”（端口统计数据）页面，请在树视图中单击“Statistics/RMON”（统计数据/RMON）→“Charts”（图表）→“Ports Statistics”（端口统计数据）。

图 8-14. 端口统计数据



“Port Statistics”（端口统计数据）页面包含以下字段：

“Unit No.”（装置号）— 表示显示统计数据的堆栈装置。

“Interface Statistics”（接口统计数据）— 选择要显示的接口统计数据。

“Etherlike Statistics”（以太网类统计数据） 选择要显示的以太网类统计数据。

“RMON Statistics”（RMON 统计数据） 选择要显示的 RMON 统计数据。

“GVRP Statistics”（GVRP 统计数据）— 选择要显示的 GVRP 统计数据类型。

“Refresh Rate”（刷新率）— 刷新统计数据之前经过的时间。

显示端口统计数据

1. 打开“Port Statistics”（端口统计数据）页面。
2. 选择要打开的统计数据类型。

3. 从“Refresh Rate”（刷新率）下拉式菜单中选择所需的刷新率。

4. 单击“Draw”（绘制）。

系统将显示选定统计数据的图形。

使用 CLI 命令查看端口统计数据

下表包含用于查看端口统计数据的 CLI 命令。

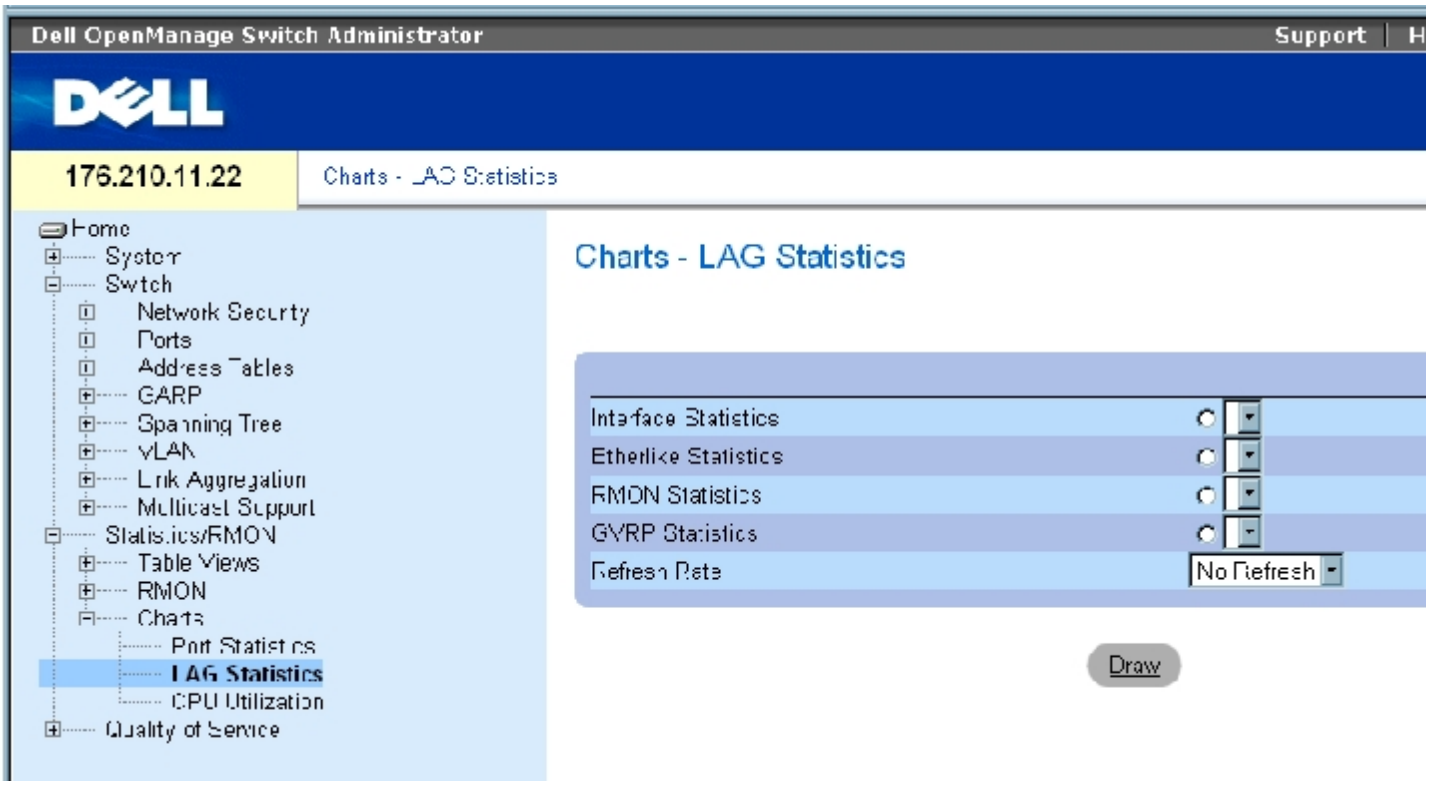
表 8-105. 端口统计数据 CLI 命令

CLI 命令	说明
show interfaces counters [ethernet 接口 **| port-channel** 端口信道号**]**	显示经由物理接口的通信。
show rmon statistics {ethernet 接口 **| port-channel** 端口信道号**}**	显示 RMON 以太网统计数据。
show gvrp statistics {ethernet 接口 **| port-channel** 端口信道号**}**	显示 GVRP 统计数据。
show gvrp-error statistics {ethernet 接口 **| port-channel** 端口信道号**}**	显示 GVRP 错误统计数据。

查看 LAG 统计数据

使用“LAG Statistics”（LAG 统计数据）页面可以以图表格式打开 LAG 的统计数据。要打开“LAG Statistics”（LAG 统计数据）页面，请在树视图中单击“Statistics/RMON”（统计数据/RMON）→“Charts”（图表）→“LAG Statistics”（LAG 统计数据）。

图 8-15. 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) — 选择要显示的接口统计数据。

“Etherlike Statistics” (以太网类统计数据) 选择要显示的以太网类统计数据。

“RMON Statistics” (RMON 统计数据) 选择要显示的 RMON 统计数据。

“GVRP Statistics” (GVRP 统计数据) — 选择要显示的 GVRP 统计数据类型。

“Refresh Rate” (刷新率) — 刷新统计数据之前经过的时间。

显示 LAG 统计数据

1. 打开“LAG Statistics” (LAG 统计数据) 页面。
2. 选择要打开的统计数据的类型。
3. 从“Refresh Rate” (刷新率) 下拉式菜单中选择所需的刷新率。
4. 单击“Draw” (绘制) 。

系统将显示选定统计数据的图形。

使用 CLI 命令查看 LAG 统计数据

下表包含用于查看 LAG 统计数据的 CLI 命令。

表 8-106. LAG 统计数据 CLI 命令

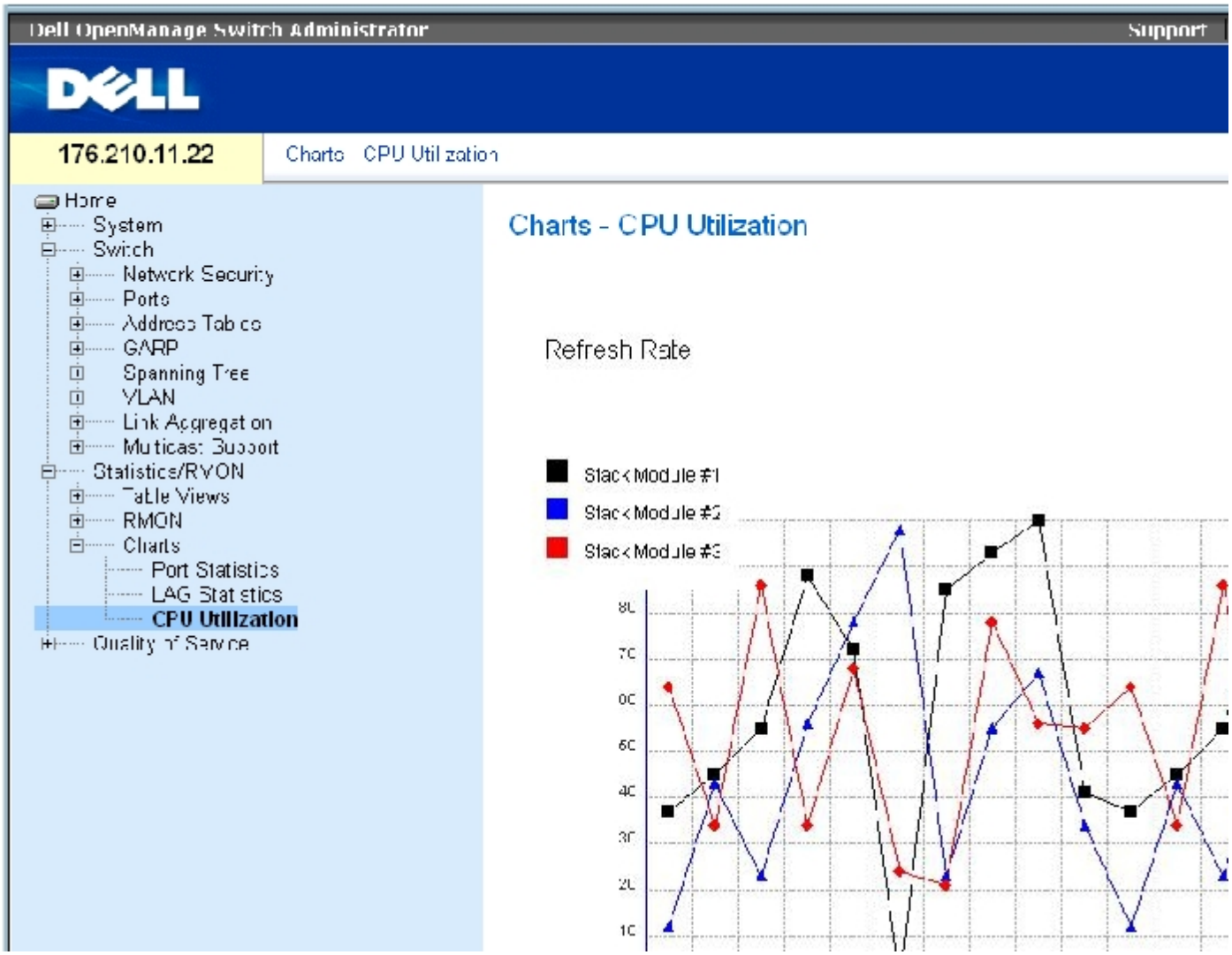
CLI 命令	说明
show interfaces counters [ethernet 接口 **| port-channel** 端口信道号**]**	显示经由物理接口的通信。
show rmon statistics {ethernet 接口 **| port-channel** 端口信道号**}**	显示 RMON 以太网统计数据。
show gvrp statistics {ethernet 接口 **| port-channel** 端口信道号**}**	显示 GVRP 统计数据。
show gvrp-error statistics {ethernet 接口 **| port-channel** 端口信道号**}**	显示 GVRP 错误统计数据。

查看 CPU 使用

“CPU Utilization” (CPU 使用) 页面包含有关系统的 CPU 使用和每个堆栈成员占用 CPU 资源的百分比的信息。图形中每个堆栈成员被指定一种颜色。

要打开“CPU Utilization” (CPU 使用) 页面，请在树视图中单击“Statistics/RMON” (统计数据/RMON) → “Charts” (图表) → “CPU Utilization” (CPU 使用) 。

图 8-16. CPU 使用



“CPU Utilization” (CPU 使用) 页面包含以下信息：

“Refresh Rate” (刷新率) — 刷新统计数据之前经过的时间。

返回目录页面

返回目录页面

配置服务质量

Dell™ PowerConnect™ 34XX 系统用户指南

本节提供了定义和配置服务质量（QoS）参数的信息。要打开“Quality of Service”（服务质量）页面，请在树视图中单击“Quality of Service”（服务质量）。

服务质量（QoS）概览

服务质量（QoS）提供了实现 QoS 和网络内部优先级排队的能力。

一个需要 QoS 的实现示例包含特定类型的、可以分配到高优先级队列的通信（例如语音通信、视频通信和实时通信），而其它通信则可以分配到较低优先级队列。这样做的结果是提高了高需求通信的通信流量。

QoS 由以下因素定义：

- “Classification”（分类）— 指定与特定值匹配的信息包字段。所有与用户定义的规格相匹配的信息包将被分为一类。
- 操作 — 定义通信管理，使信息包的传输基于信息包信息和信息包字段值（例如 VLAN 优先级标记 [VPT] 和 DSCP [DiffServ 代码点]）。

VPT 分类信息

VLAN 优先级标记用于通过将信息包映射到其中一个外出队列来对信息包进行分类。VLAN 优先级标记至队列的分配可以由用户定义。下表详细说明了 VPT 至队列的默认设置：

表 9-107. CoS 至队列映射表默认值

CoS 值	传输队列值
0	q1（最低优先级）

1	q1（最低优先级）
2	q1（最低优先级）
3	q1（最低优先级）
4	q2
5	q2
6	q3
7	q3

注：在堆叠配置中，队列 4 用于传输堆叠通信。因此，为队列 4 分配其它通信可能会影响通信传输。

到达的未标记信息包被分配了一个针对每个端口设置的默认 VPT 值。分配的 VPT 用于将信息包映射到外出队列。

可以将 DSCP 值映射到优先级队列。下表包含了映射到外出队列的默认 DSCP 值：

表 9-108. DSCP 至队列映射表默认值

DSCP 值	传输队列值
0-15	q1（最低优先级）
16-39	q2
40-63	q3

DSCP 映射是针对每个系统进行启用的。

CoS 服务

信息包被分配到特定外出队列后，可以为此队列设定 CoS 服务。可通过以下方法之一为外出队列配置安排方案：

- 严格优先级 — 确保始终传输与时间密切相关的应用程序。严格优先级（SP）使您可以排定任务关键、与时间密切相关的通信的优先级，使其高于与时间相关度较低的应用程序的优先级。
  例如，在严格优先级下，通过 IP 的语音通信会具有优先级，从而先于 FTP 或电子邮件（SMTP）通信进行传输。

- 加权轮流 — 确保单个应用程序不会控制设备的传输能力。加权轮流（WRR）以轮流方式传输全部队列。除了 SP 队列，所有队列均可参与 WRR。
  SP 队列将在 WRR 队列之前传输。如果通信流量非常小，并且 SP 队列未占用分配给端口的整个带宽，则 WRR 队列可以与 SP 队列共用带宽。确保剩余带宽是按照加权比进行分配的。如果选择 WRR，则将为队列分配以下加权： 1，2，4，8 。

定义 QoS 全局参数

“QoS Parameters”（QoS 参数）页面包含指向启用设置服务质量全局参数页面的链接。

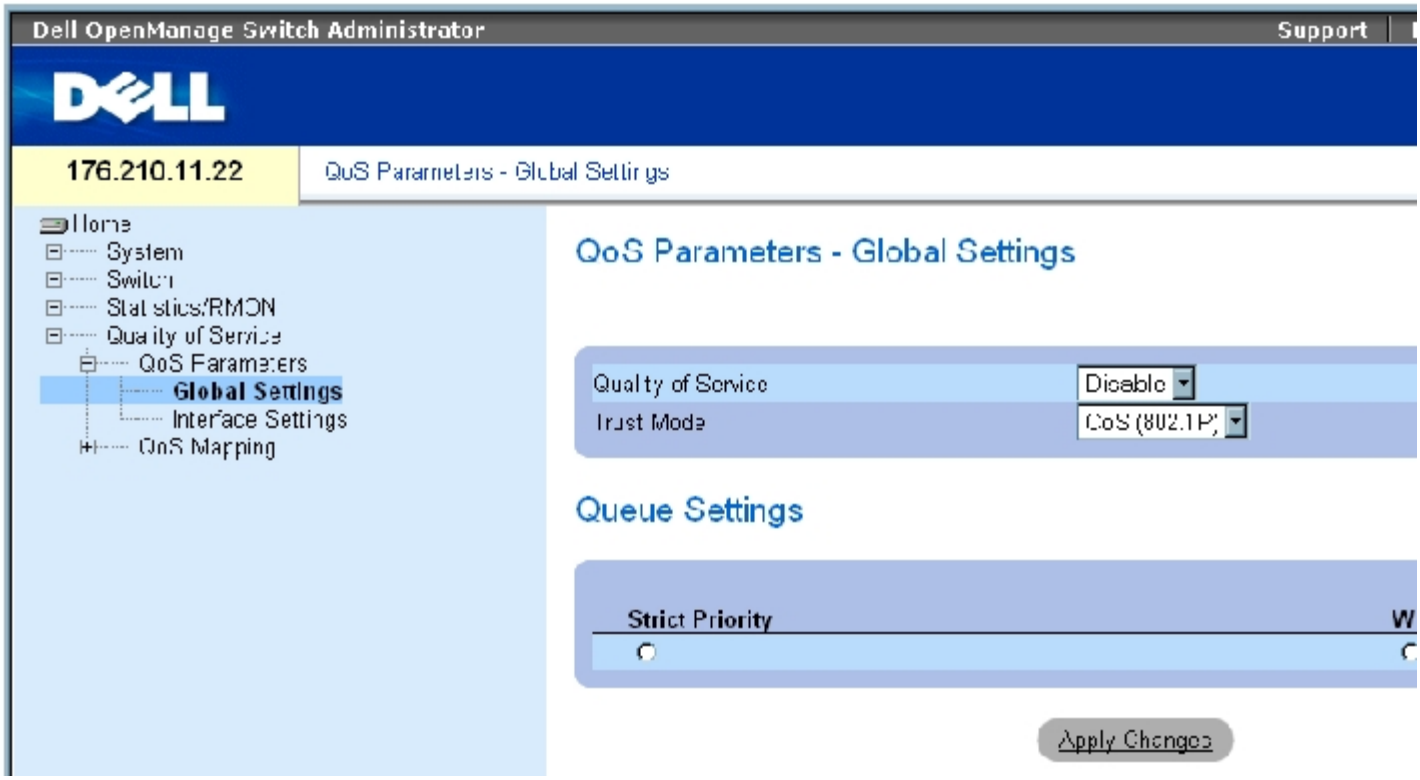
配置 QoS 全局设置

“Global Settings”（全局设置）页面包含用于启用或禁用 QoS 的字段。还包含用于选择信任模式的字段。信任模式根据信息包中预定义的字段来确定外出队列。

此外，使用“Global Settings”（全局设置）页面可以将队列定义为严格优先级（SP）或加权轮流（WRR）。

要打开“Global Settings”（全局设置）页面，请在树视图中单击“Quality of Service”（服务质量）→“QoS Parameters”（QoS 参数）→“Global Settings”（全局设置）。

图 9-1. 全局设置



“Global Settings”（全局设置）页面包含以下部分：

- QoS 设置

- 队列设置

QoS 设置

“Quality of Service”（服务质量）— 启用或禁用使用服务质量管理网络通信。

“Trust Mode”（信任模式）— 确定用于对进入设备的信息包进行分类的信息包字段。如果未定义规则，则将根据选定的信任模式映射包含预定义的 CoS 或 DSCP 信息包字段的通信。不包含预定义信息包字段的通信将被映射至最佳传输能力队列 (q2)。可能的“Trust Mode”（信任模式）字段值包括：

“CoS (802.1p)”— 外出队列的分配由 IEEE802.1p VLAN 优先级标记 (VPT) 或分配到端口的默认 VPT 确定。设备默认值为 IEEE802.1p。

“DSCP”— 外出队列的分配由 DSCP 字段确定。

注：接口“Trust”（信任）中的设置将代替全局“Trust”（信任）设置。

队列设置

“Strict Priority”（严格优先级）— 如果选择此选项，则表示系统队列为 SP 队列。

“WRR”— 如果选择此选项，则表示系统队列为 WRR 队列。

启用服务质量：

1. 打开“Global Settings”（全局设置）页面。
2. 在“Quality of Service”（服务质量）字段中选择“Enable”（启用）。
3. 单击“Apply Changes”（应用更改）。

设备上将启用“Class of Service”（服务级别）。

启用信任模式：

1. 打开“Global Settings”（全局设置）页面。
2. 定义“Trust Mode”（信任模式）字段。
3. 单击“Apply Changes”（应用更改）。

设备上将启用信任模式。

使用 CLI 命令启用信任

下表概括了用于配置“Global Settings”（全局设置）页面中字段的等效 CLI 命令。

表 9-109. QoS 设置 CLI 命令

CLI 命令	说明
qos trust [cos | dscp]	将系统配置为信任模式。
no qos trust	恢复为非信任状态。

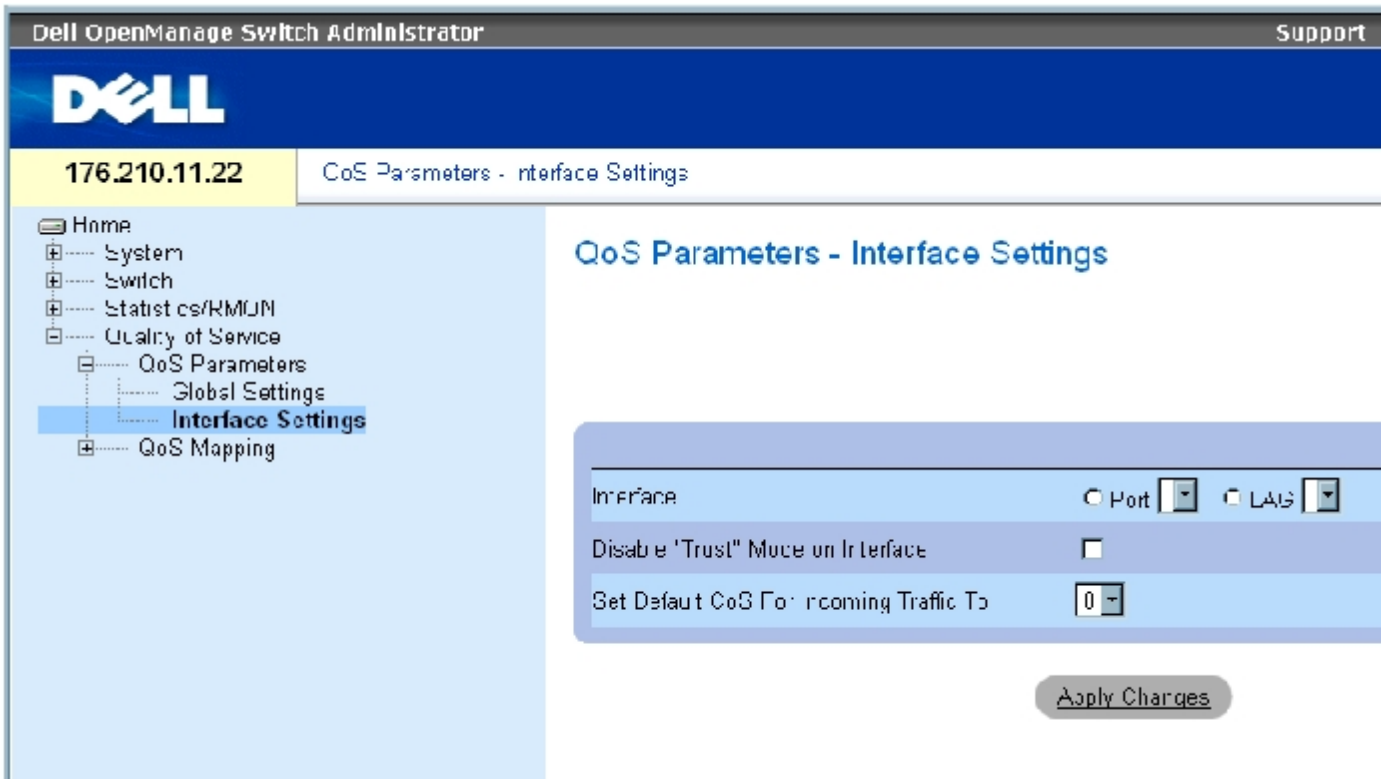
以下是 CLI 命令的示例：

```
console(config)# qos trust
dscp
```

定义 QoS 接口设置

“Interface Settings”（接口设置）页面包括用于取消激活信任模式和对传入的未标记信息包设置默认 CoS 值的字段。要打开“Interface Settings”（接口设置）页面，请在树视图中单击“Quality of Service”（服务质量）→“QoS Parameters”（QoS 参数）→“Interface Settings”（接口设置）。

图 9-2. 接口设置



“Interface Settings”（接口设置）页面包含以下字段：

“Interface”（接口）— 要配置的特定端口或 LAG。

“Disable 'Trust' Mode on Interface”（在接口上禁用“信任”模式）— 在指定接口上禁用信任模式。此设置将代替设备上全局配置的“Trust”（信任）模式。

“Set Default CoS For Incoming Traffic To”（将传入通信的默认 CoS 设置为）— 设置未标记信息包的默认 CoS 标记值。CoS 标记值为 0 至 7。默认值为 0。

为接口设定 QoS 设置：

1. 打开“Interface Settings”（接口设置）页面。
2. 在“Interface”（接口）字段中选择接口。
3. 定义字段。
4. 单击“Apply Changes”（应用更改）。

将为接口设定 CoS 设置。

显示 QoS/CoS 设置：

1. 打开“Interface Settings”（接口设置）页面。
2. 单击“Show All”（全部显示）。

将显示“Interface Table”（接口表）。

使用 CLI 命令设定 QoS 接口

下表概括了用于配置“Interface Settings”（接口设置）页面中的字段的等效 CLI 命令。

表 9-110. QoS 接口 CLI 命令

CLI 命令	说明
qos trust	启用信任模式。
no qos trust	在每个端口上禁用信任状态。

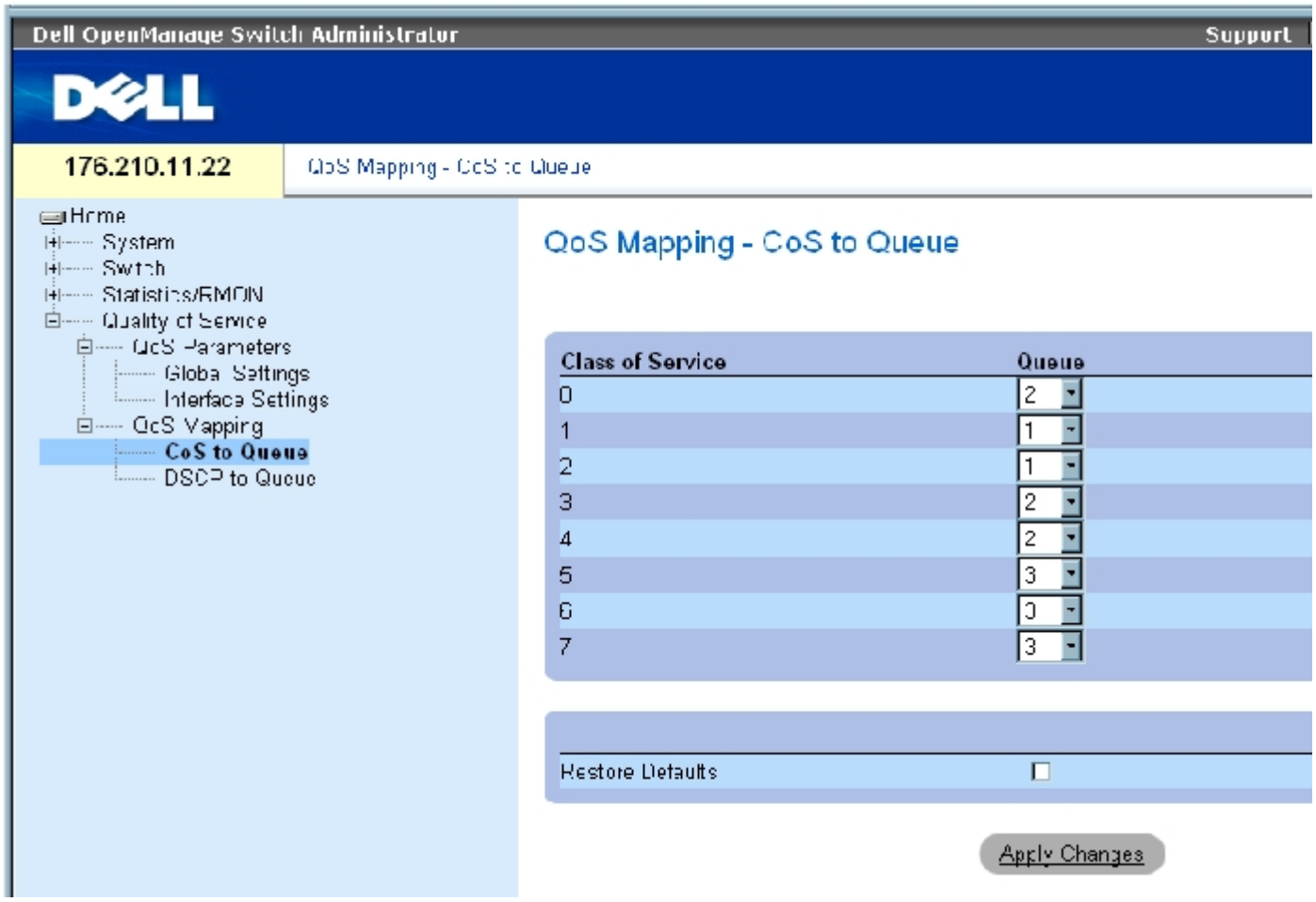
以下是 CLI 命令的示例：

```
console(config)# interface
ethernet 1/e15

console(config-if)# qos
trust
```

将 CoS 值映射到队列

“CoS to Queue”（CoS 至队列）页面包含用于将 CoS 设置分类到通信队列的字段。要打开“CoS to Queue”（CoS 至队列）页面，请在树视图中单击“Quality of Service”（服务质量）→“QoS Mapping”（QoS 映射）→“CoS to Queue”（CoS 至队列）。

图 9-3. CoS 至队列



"CoS to Queue" (CoS 至队列) 页面包含以下字段：

"Class of Service" (服务级别) — 指定 CoS 优先级标记值，其中零为最低值，7 为最高值。

"Queue" (队列) — CoS 优先级要映射到的队列。支持四个通信优先级队列。

"Restore Defaults" (恢复默认设置) — 恢复将 CoS 值映射到外出队列的设备出厂默认设置。

将 CoS 值映射到队列

1. 打开"CoS to Queue" (CoS 至队列) 页面。
2. 选择 CoS 条目。
3. 在"Queue" (队列) 字段中定义队列号。
4. 单击"Apply Changes" (应用更改) 。

CoS 值将被映射到外出队列，并更新设备。

使用 CLI 命令为队列设定 CoS 值

下表概括了用于配置“CoS to Queue” (CoS 至队列) 页面中字段的等效 CLI 命令。

表 9-111. CoS 至队列设置 CLI 命令

CLI 命令	说明
wrr-queue cos-map queue-id cos0.cos7	将设定的 CoS 值映射到外出队列。

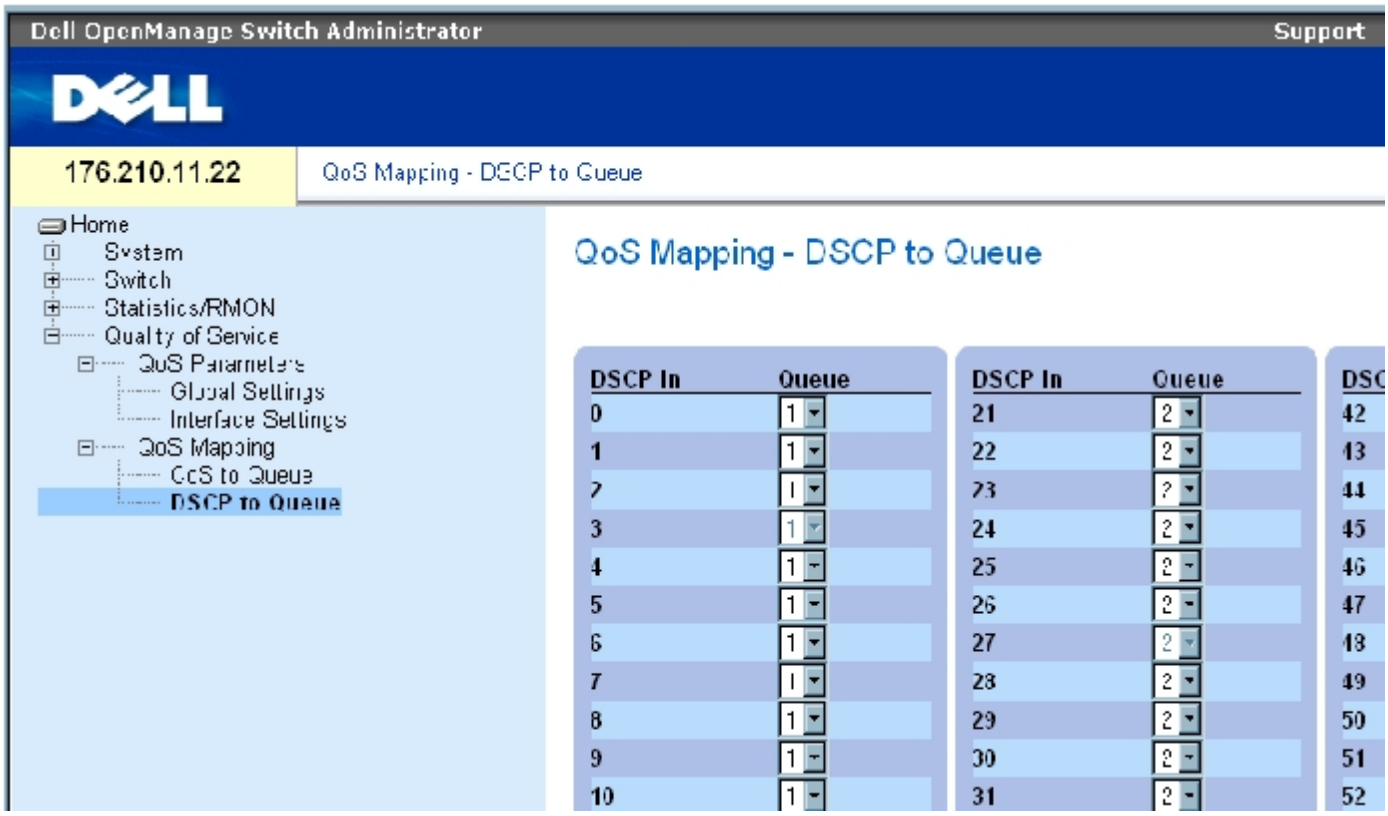
以下是 CLI 命令的示例：

```
console(config)# wrr-queue cos-
map 4 7
```

将 DSCP 值映射到队列

“DSCP to Queue” (DSCP 至队列) 页面提供了用于将外出队列定义至特定 DSCP 字段的字段。要打开“DSCP to Queue” (DSCP 至队列) 页面，请在树视图中单击“Quality of Service” (服务质量) → “QoS Mapping” (QoS 映射) → “DSCP to Queue” (DSCP 至队列) 。

图 9-4. DSCP 至队列



“DSCP to Queue” (DSCP 至队列) 页面包含以下字段：

“DSCP In” (DSCP 位于) — 传入信息包中 DSCP 字段的值。

“Queue” (队列) — 具有特定 DSCP 值的信息包将要分配到的队列。值包括 1 至 4，其中 1 为最低值，4 为最高值。

要映射 DSCP 值和分配优先级队列，请：

1. 打开“DSCP to Queue” (DSCP 至队列) 页面。
2. 在“DSCP In” (DSCP 位于) 列中选择一个值。
3. 定义“Queue” (队列) 字段。
4. 单击“Apply Changes” (应用更改) 。

DSCP 将被覆盖，但会为其值分配一个外出队列。

使用 CLI 命令设定 DSCP 值

下表概括了用于配置“DSCP to Queue” (DSCP 至队列) 页面中字段的等效 CLI 命令。

表 9-112. DSCP 值至队列 CLI 命令

CLI 命令	说明
qos map dscp-queue dscp-list to queue-id	修改 DSCP 至队列映射。

以下是 CLI 命令的示例：

```
console(config)# qos map
dscp-queue 33 40 41 to 1
```

返回目录页面

返回目录页面

设备特性交互作用信息

Dell™ PowerConnect™ 34XX 系统用户指南

下表包含了有关特性交互作用的信息

特性	特性说明
802.1x 未经验证的 VLAN	802.1x 未经验证的 VLAN 与以下特性交互时，其功能将受到限制： • 802.1X 访客 VLAN • 专用 VLAN • 隔离 VLAN • 团体 VLAN • 特定 VLAN
802.1x 未经验证的 VLAN 端口	802.1x 未经验证的 VLAN 端口与以下特性交互时，其功能将受到限制： • 隔离端口 • 团体端口 • 混合端口 • 基于 MAC 的 VLAN 端口 • 入口过滤
ACL	ACL 与以下特性交互时，其功能将受到限制： • 基于 MAC 的 ACL • 特定 VLAN
自适应	无特性交互作用限制。
背压支持	
桥接多点传送过滤	无特性交互作用限制。
电缆检测	无特性交互作用限制。
团体端口	团体端口与锁定端口交互时，其功能受到限制。

团体 VLAN	团体 VLAN 与以下特性交互时，其功能将受到限制： • 静态 MAC 地址 • ACL • GVRP • IGMP 监测 • 特定 VLAN
DNS	无限制。
双工模式	
流控制	无特性交互作用限制。
GARP	无特性交互作用限制。
访客 VLAN	访客 VLAN 无法与以下特性交互： • 专用 VLAN • 隔离 VLAN • 团体 VLAN • 基于 MAC 的 VLAN • 特定 VLAN
GVRP	无特性交互作用限制。
IGMP 监测	无特性交互作用限制。
入口过滤	无特性交互作用限制。
隔离端口	隔离端口无法与以下特性交互： • 团体端口 • 混合端口 • 锁定端口 • GVRP • 基于 MAC 的 ACL • 入口过滤
隔离 VLAN	隔离 VLAN 无法与以下特性交互： • 团体 VLAN • 静态 MAC 地址 • ACL • GVRP • IGMP 监测

	• 特定 VLAN
LAG 统计数据	无特性交互作用限制。
链路聚合	无特性交互作用限制。但是，此特性有一些用于配置链路聚合的原则。有关此特性所有原则的信息，请参阅“定义 LAG 参数”。
锁定端口	锁定端口与以下特性交互时，其功能将受到限制： • 基于 MAC 的 ACL • 入口过滤
日志记录	无特性交互作用限制。
MAC 地址支持	无特性交互作用限制。
MDI/MDIX 检测	无特性交互作用限制。
多点传送过滤	无特性交互作用限制。
多台主机	802.1X 标准（多台主机）无法与以下特性交互： • 隔离端口 • 基于 MAC 的 VLAN 端口
多个生成树	多个生成树无法与以下特性交互： • 隔离端口 • 入口过滤
基于端口的验证	基于端口的验证与以下特性交互时，其功能将受到限制： • 802.1 单个端口 • 隔离端口 • 锁定端口 • 基于 MAC 的 VLAN • 入口端口
端口镜像	无特性交互作用限制。但是，此特性有一些用于配置风暴控制的原则。有关此特性所有原则的信息，请参阅“定义端口镜像会话”。
端口统计数据	无特性交互作用限制

专用 VLAN	专用 VLAN 无法与以下特性交互： • 隔离端口 • 团体端口 • GVRP • IGMP 监测 • 特定 VLAN
专用 VLAN	专用 VLAN 与以下特性交互时，其功能将受到限制： • 隔离 VLAN • GVRP • IGMP 监测 • 特定 VLAN
混合端口	混合端口无法与以下特性交互： • 锁定端口 • GVRP • 基于 MAC 的 VLAN 端口
服务质量	无特性交互作用限制。
RMON 统计数据	无特性交互作用限制。
SNMP 验证通知	无特性交互作用限制。
SNMP 通知	无特性交互作用限制。
SNTP 验证	无特性交互作用限制。
生成树	无特性交互作用限制。
特定 VLAN	无特性交互作用限制
静态 MAC	无特性交互作用限制
风暴控制	无特性交互作用限制
系统日志	无特性交互作用限制
系统时间同步	无特性交互作用限制。
未经验证的 VLAN 端口	未经验证的 VLAN 端口与以下特性交互时，其功能将受到限制： • 隔离端口 • 团体端口

	• 混合端口 • GVRP • 基于 MAC 的 VLAN 端口 • 入口过滤

返回目录页面

返回目录页面

词汇表

Dell™ PowerConnect™ 34XX 系统用户指南

此词汇表包含有用的关键技术词汇。

英文 | B | C | D | F | G | I | L | O | R | S | T | W | X | Y | Z

英文

ARP

地址解析协议。一种协议，用于将 IP 地址转换为物理地址。

ASIC

应用程序特定集成电路。一种专用于特定应用程序的自定义芯片。

BootP

Bootstrap 协议。使工作站可以发现其 IP 地址、网络上的 BootP 服务器的 IP 地址或载入到交换机模块引导的配置文件。

BPDU

桥接协议数据装置。以信息格式提供桥接信息。BPDU 随生成树配置内的交换机模块信息一起发送。BPDU 信息包包含有关端口、地址、优先级和传输成本的信息。

CDB

配置数据库。一个包含设备的配置信息的文件。

CLI

命令行界面。用于配置系统的一组行命令。有关使用 CLI 的详细信息，请参阅“使用 CLI”。

CPU

中央处理器。处理信息的计算机部件。CPU 由控制单元和 ALU 组成。

DHCP 客户端

使用 DHCP 获得配置参数（例如网络地址）的设备。

DRAC/MC

DRAC/MC。提供对 Dell 模块化服务器系统组件的单点控制。

DSCP

DiffServe 代码点 (DSCP)。DSCP 提供了为 IP 信息包标记 QoS 优先级信息的方法。

EWS

嵌入式 Web 服务器。通过标准 Web 浏览器提供设备管理。除 CLI 或 NMS 外，还可以使用嵌入式 Web 服务器；也可以使用嵌入式 Web 服务器替代 CLI 或 NMS。

FFT

快速传输表。提供有关传输路由的信息。如果信息包到达具有已知路由的设备，则此信息包将通过 FFT 中已列出的路由进行传输。如果没有已知路由，CPU 将传输信息包并更新 FFT。

FIFO

先进先出。一种排队处理，其中队列中的第一个信息包为出自信息包的第一个信息包。

GARP

通用属性注册协议。将客户端站点注册至多点传送域。

GVRP

GARP VLAN 注册协议。将客户端站点注册至 VLAN。

HOL

队列头。信息包被排队。先传输队列头的信息包，然后再传输队列尾的信息包。

HTTP

超文本传输协议。在 Internet 上的服务器和客户端之间传输 HTML 文档。

IC

集成电路。集成电路是由半导体材料构成的小型电子设备。

ICMP

Internet 信报控制协议。使网关或目的地主机可以与源主机进行通信，例如报告正在处理的错误。

IEEE

美国电气及电子工程师学会。制订通信和网络标准的工程师行业组织。

IEEE 802.1d

用于生成树协议，IEEE 802.1d 支持 MAC 桥接从而避免了网络环路。

IEEE 802.1p

可以排定数据链路/MAC 子层的网络通信的优先级。

IEEE 802.1Q

定义 VLAN 网桥的操作，VLAN 网桥允许定义、操作和管理桥接 LAN 基础设施内的 VLAN。

IP

网际协议。指定信息包的格式和定址方法。IP 选定信息包地址，并将信息包传输至正确的端口。

IP 地址

网际协议地址。分配给两个或多个互连 LAN 或 WAN 的网络设备的唯一的地址。

LAG

链路聚合组。将端口或 VLAN 聚合到一个虚拟端口或 VLAN。

有关 LAG 的详细信息，请参阅“定义 LAG 成员关系”。

LAN

局域网。包含在一个房间、建筑、校园或其它有限的地理区域内的网络。

MAC 层

数据链路控制 (DTL) 层的一个子层。

MAC 地址

介质访问控制地址。MAC 地址是标识各个网络节点的硬件特定地址。

MAC 地址记忆

MAC 地址记忆具有记忆网桥的特征，其中记录了信息包的源 MAC 地址。指定传输到该地址的信息包将仅被传输至该地址所在的网桥接口。定址到未知地址的信息包将被传输至每个网桥接口。MAC 地址记忆使连接的 LAN 上的通信达到最小。

MD5

报文摘要 5。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。

MDI

介质相关接口。一种用于终端站点的电缆。

MDIX

带有绞接电缆的介质相关接口 (MDIX)。一种用于集线器和交换机的电缆。

MIB

管理信息库。MIB 包含了对网络组件的特定方面进行说明的信息。

NMS

网络管理系统。一种提供了管理系统的方式的接口。

OID

对象标识符。SNMP 使用对象标识符标识管理型对象。在 SNMP 管理器/代理网络管理范例中，每个管理型对象必须有一个 OID 用于标识该对象。

PDU

协议数据装置。一种在分层协议中指定的数据装置，它包括协议控制信息和层用户数据。

PING

因特网信息包搜索协议。验证特定 IP 地址是否可用。将信息包发送到另一个 IP 地址并等待回复。

QoS

服务质量。QoS 使网络管理员可以根据优先级、应用程序类型以及源地址和目的地地址确定如何传输网络通信以及传输哪些网络通信。

RADIUS

远程认证拨入用户服务。一种用于验证系统用户并记录连接时间的方式。

RMON

远程监测。提供要从单个工作站收集的网络信息。

RSTP

快速生成树协议。可以检测并使用网络拓扑，网络拓扑使生成树可以快速聚合，而不会创建传输环路。

SNMP

简单网络管理协议。管理 LAN。基于 SNMP 的软件通过嵌入式 SNMP 代理与网络设备进行通信。SNMP 代理收集网络活动信息和设备状态信息，并将信息发送回工作站。

SNTP

简单网络计时协议。SNTP 确保网络交换机时钟时间同步准确，最多可准确到毫秒。

SoC

芯片上的系统。一种包含整个系统的 ASIC。例如，通信 SoC 应用程序可能包含微处理器、数字信号处理器、RAM 和 ROM。

SSH

安全命令解释程序。允许通过网络登录到另一台计算机、执行远程计算机上的命令以及将文件从一台计算机上移动到另一台计算机。安全命令解释程序为不安全通道提供了强大的验证和安全通信方法。

TCP/IP

传输控制协议。使两台主机可以相互通信和交换数据流。TCP 保证信息包的传送，并保证信息包以其发送时的顺序被传输和接收。

Telnet

终端仿真协议。使系统用户可以登录远程网络并使用远程网络上的资源。

TFTP

小型文件传输协议。使用不带安全保护功能的用户数据协议 (UDP) 传输文件。

Trap

由 SNMP 发送的信息，表示发生了系统事件。

UDP

用户数据协议。传输信息包，但并不保证其发送。

VLAN

虚拟局域网。局域网 (LAN) 的逻辑子组，它是通过软件而不是通过定义硬件解决方案创建的。

WAN

广域网。覆盖大面积地理区域的网络。

B

背板

交换机模块中传输信息的主总线。

备份配置文件

包含交换机模块配置的备份副本。将运行配置文件或启动配置文件复制到备份文件时，备份文件将发生更改。

背压

半双工模式使用的一种机制，使端口无法接收信息。

波特

每秒中传输的信号元素的数量。

C

查询

从数据库中抽取信息并显示要使用的信息。

超长帧

可以在较少的帧内传输相同的数据。超长帧减少了额外开销、缩短了处理时间并确保中断较少。

出口端口

从中传输网络通信的端口。

D

带宽

带宽指定了在固定时间段内可以传输的数据量。对于数字交换机模块，带宽以每秒位数（bps）或每秒字节数定义。

带宽分配

分配给特定应用程序、用户或接口的带宽量。

单点传送

将一个信息包传输给一个用户的路由形式。

第 2 层

数据链路层或 MAC 层。包含客户端站点或服务器站点的物理地址。由于要处理的信息较少，因此第 2 层处理要快于第 3 层处理。

第 4 层

建立一个连接，并确保所有数据均到达其目的地。对第 4 层上检查到的信息包进行分析，并基于其应用程序进行传输判断。

端口

提供了使微处理器可以与外围设备进行通信的连接组件的物理端口。

端口镜像

通过将传入和传出信息包的副本从一个端口传输至监测端口，端口镜像可以监测和镜像网络通信。

有关端口镜像的详细信息，请参阅“定义端口镜像会话”。

端口速率

表明端口的端口速率。端口速率包括：

- 以太网 10 Mbps
- 高速以太网 100Mbps
- 吉位以太网 1000 Mbps

多点传送

将一个信息包的副本传输至多个端口。

F

访问模式

指定向用户授予访问系统的权限的方法。

访问配置文件

使网络管理员可以定义用于访问交换机模块的配置文件和规则。对管理功能的访问可以限制在用户组内，它由以下条件定义：

- 入口接口
- 源 IP 地址或源 IP 子网

分段

将 LAN 分为单独的 LAN 网段，用于桥接。分段消除了 LAN 带宽限制。

封盖

当接口状态不断更改时，会出现封盖。例如，STP 端口从侦听到了解再到传输不断进行更改。这可能导致通信丢失。

服务级别

服务级别 (CoS)。服务级别是指 802.1p 优先级方案。CoS 提供了为信息包标记优先级信息的方法。CoS 值介于 0 至 7 之间，该值被添加到信息包的第 II 层标头，其中，零为最低优先级，七为最高优先级。

重叠传送两个或多个相冲突的信息包。传输的数据无法使用，会话将重新启动。

服务器

一种为网络中的其它计算机提供服务的中央计算机。服务可能包括文件存储和访问应用程序。

负载平衡

使数据或处理信息包在可用的网络资源上平均分配。例如，负载平衡可能将传入信息包平均地分配给所有服务器，或者将信息包重定向至下一个可用服务器。

G

广播

一种将信息包传输至网络上的所有端口的方式。

广播风暴

过多的广播信息同时通过单个端口在网络中传输。已传输信息的响应被堆入网络，从而使网络资源过载或导致网络超时。

有关广播风暴的详细信息，请参阅“定义 LAG 参数”。

广播域

设备组，用于接收源自一个指定组内的任何设备的广播帧。路由器捆绑广播域，因为路由器不传输广播帧。

J

吉位以太网

吉位以太网以 1000 Mbps 进行传输，并与现有 10/100 Mbps 以太网标准兼容。

交换机

在 LAN 网段之间筛选和传输信息包。交换机支持任何信息包协议类型。

节点

一个网络连接端点或一个用于多条网络线路的公共交叉点。节点包括：

- 处理器
- 控制器
- 工作站

聚合 VLAN

将若干 VLAN 组成一个聚合 VLAN。聚合 VLAN 使路由器可以响应对位于不同子 VLAN（属于同一个超级 VLAN）上的节点的 ARP 请求。路由器以其

MAC 地址进行响应。

L

流控制

使低速设备可以与高速设备进行通信，即高速设备阻止发送信息包。

路由器

一种连接到单个网络的设备。路由器在两个或多个网络之间传输信息包。路由器在第 3 层上运行。

Q

启动配置

在交换机模块断电或重新引导时维护完整的交换机模块配置。

R

入口端口

接收网络通信的端口。

S

生成树协议

防止网络通信中的环路。生成树协议 (STP) 提供了树拓扑用于任意排列网桥。STP 在网络中的终端站点之间提供了一条路径，消除了环路。

双工模式

允许同时传输和接收数据。有两种不同的双工模式：

- 全双工模式 — 允许进行双同步通信，例如电话。双方可以同时传输信息。

- 半双工模式 — 允许进行异步通信，例如手提对讲机。一次只有其中一方可以传输信息。

碎片

小于 576 位的以太网信息包。

T

通配符掩码

指定要使用的 IP 地址位以及要忽略的 IP 地址位。通配符交换机模块掩码 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。

例如，如果目的地 IP 地址为 149.36.184.198，通配符掩码为 255.36.184.00，则表示使用 IP 地址的前两位，忽略最后两位。

团体

指定具有相同系统访问权限的一组用户。

W

网桥

一种连接两个网络的设备。网桥是针对硬件而言的，与协议无关。网桥在第 1 层和第 2 层上运行。

X

协议

控制设备如何在网络中交换信息的一组规则。

信息包

用于在信息包交换系统中传输的信息块。

Y

掩码

包括或排除某些值（例如部分 IP 地址）的筛选器。

例如，装置 2 被插入一个十分钟周期的第一分钟，装置 1 被插入同一周期的第五分钟，则认为这两个装置处于同一时间。

验证配置文件

规则集，使您可以登录及验证用户和应用程序。

以太网

以太网按照 IEEE 802.3 被标准化。以太网是最常用的执行的 LAN 标准。支持以 Mbps 为单位的数据传输速率，支持 10 Mbps、100 Mbps 或 1000 Mbps。

引导版本

引导版本。

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）的闪存扇区中。活动映像存储活动副本，另一个映像存储次副本。

域

以共同的规则和步骤组合起来的网络中的一组计算机和设备。

运行配置文件

包含所有启动配置文件命令以及在当前会话过程中输入的所有命令。交换机模块断电或重新引导后，所有存储在运行配置文件中的命令均会丢失。

Z

帧

包含物理介质所需的标头和报尾信息的信息包。

终端系统

网络上的终端用户设备。

主干聚合

链路聚合。通过将一组端口链接在一起形成一条主干（聚合组）来优化端口的使用。

主机

用作其它计算机的信息源或服务源的计算机。

资产标签

指定用户定义的交换机模块参考。

子网

子网。子网是网络的组成部分，它们共用一个公用地址组件。在 TCP/IP 网络上，共用一个前缀的设备是同一子网的一部分。例如，具有前缀 157.100.100.100 的所有设备均为同一子网的一部分。

子网掩码

用于屏蔽子网地址中所使用的全部或部分 IP 地址。

自适应

可以建立 10/100 Mpbs 或 10/100/1000 Mbps 以太网端口，使其具有以下功能：

- 双工/半双工模式
- 流控制
- 速率

最佳传输能力

将通信量分配给优先级最低的队列，并且不保证信息包传送。

返回目录页面