Dell™ PowerConnect™ 3324/3348 用户指南

注：注表示可以帮助您更好地使用设备的重要信息。

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。

2003 年 11 月 Rev. A01

返回目录页面

配置 PowerConnect 3324/3348 交换机

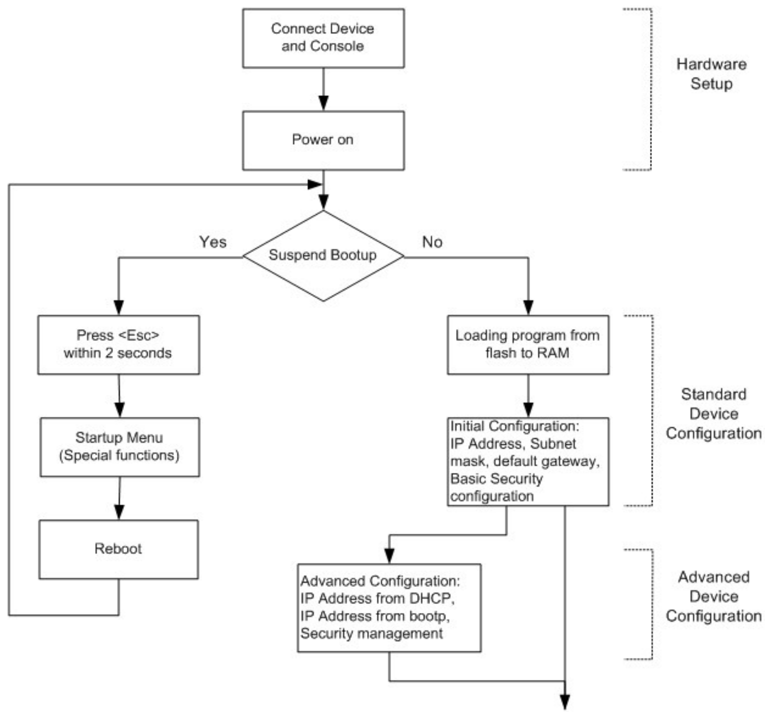
Dell™ PowerConnect™ 3324/3348 用户指南

配置概览

本节介绍初始设备配置，包括：

- 初始设备引导
- 前期配置要求
- 配置堆叠

在所有的设备外部连接均已就位之后，必须将终端连接至设备，以监视引导过程和其它过程。
以下流程图说明了安装和配置过程的顺序：



前面的章节已介绍了如何安装设备和硬件。 初次安装时会执行标准设备安装。 您还可以执行其它特殊功能，但会暂停安装过程，并需要重新引导系统。 本节稍后将对此选项进行说明。

一般配置信息

Dell™PowerConnect™ 3324/3348 提供了预定义的执行功能和安装配置。

自动协商

通过自动协商功能，设备可以通告操作模式，并与另一与之共享点对点链路网段的设备共享信息。 在自动协商模式下，会自动配置两个设备，以最大限度地利用其各自的功能。

链路初始化过程中在物理层内即可完全执行自动协商，而不会对 MAC 或更高的协议层产生额外开销。 自动协商允许端口执行以下功能：

- 通告其功能。
- 确认收到并了解两个设备共享的通用操作模式。
- 拒绝使用两个设备未共享的操作模式。
- 为每个端口配置两个端口均支持的最高级别的操作模式。

如果交换机端口所连接的工作站或服务器的网络接口控制器 (NIC) 不支持自动协商或未设置为自动协商，则必须使用 Web 浏览器界面或 CLI 命令手动将交换端口和 NIC 设置为相同的速率和双工模式。

注意： 如果链路另一端的站点尝试与手动配置为全双工模式的端口自动协商，则自动协商将导致此站点尝试以半双工模式运行。 产生的不匹配可能会导致严重的帧丢失。 这是自动协商标准所固有的。

交换端口默认设置

下表说明了端口的默认设置。

功能	默认设置
端口速率和模式	10/100M 铜质端口： 自动协商 1000M 自动协商
端口传输状态	已启用
端口标记	无标记
防止线端 (HOL) 阻塞	打开（已启用）
流控制	关闭
背压	关闭

端口默认设置

以下是使用 CLI 命令更改端口 1/e5 速率的实例：

```
console> enable

console# configure

Console (config)# interface ethernet 1/e5

Console (config-if)# speed 9600
```

以下是使用 CLI 命令在端口 1/e5 上启用流控制的实例：

```
console> enable

console# configure

Console (config)# interface ethernet 1/e5

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

以下是使用 CLI 命令在端口 1/e5 上启用背压的实例：

```
console> enable

console# configure
```

```
Console (config)# interface ethernet 1/e5

Console (config-if)# back-pressure
```

波特率

可以将波特率手动更改为以下任一值：

- 2400
- 4800
- 9600
- 19,200
- 38,400
- 57,600
- 115,200

注： 默认波特率为 9600。

注： 关闭设备不会返回默认的波特率。 必须进行专门配置。

注： 要进入配置模式，您必须具备 15 级管理权限。

以下是使用 CLI 命令更改默认波特率的配置实例：

```
console> enable

console# configure

console(config)# line console

console(config-line)# speed 9600

console(config-if)# exit

console(config)# exit
```

终端连接配置

PowerConnect 3324/3348 需要配置以下终端连接参数：

- 无奇偶校验
- 1 个停止位
- 8 个数据位

其它配置要求

以下是下载嵌入式软件和配置设备的要求：

- ASCII 终端（或仿真）连接至装置背面的串行端口。
- 为 PowerConnect 3324/3348 分配 IP 地址，以使用 Telnet、SSH 等进行设备远程控制。

注： 配置进程仅定义一个端口。

引导设备

连接好本地终端，接通电源之后，设备即会进行 POST（开机自测）。 每次初始化设备时都会运行此内置开机自测。 在 POST 过程中，系统将检查硬件组件，确定设备在完成引导之前运转完全正常。

如果检测到严重错误，程序流程即会停止。 如果成功通过 POST，则代码会解压缩到 RAM 内存中。

POST 信息会显示在终端上，表示测试成功或失败。

要引导设备，请：

1. 确保 ASCII 电缆已连接至终端。
2. 将电源设备连接至设备。设备将开始进行引导。 引导检测会首先计算设备内存可用性，然后再继续引导。 以下屏幕信息是一个 POST 测试的显示实例：

```
------ Performing the Power-On Self Test (POST) ------



UART Channel Loopback Test......PASS

Testing the System Cache.......PASS

Testing the System SDRAM.......PASS

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

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

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

Testing CPU PCI Bus Device Configuration...PASS


BOOT Software Version 1.30.11 Built 27-JAN-2003 10:06:03

Processor: MPC8245 Rev 0.12, 250 MHz (Bus: 100MHz), 32 MByte SDRAM.

I-Cache 16 KB, linesize 32.D-Cache 16 KB, linesize 32.

Cache Enabled.

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

POST 结束后显示的自动引导信息（最后数行）表示在引导过程中未遇到问题。

如果需运行可以从“Startup”（启动）菜单调用的特殊程序，可以在此时进行用户输入，获取此菜单。 要进入“Startup”（启动）菜单，必须在显示自动引导信息后的前两秒钟内按 **<Esc>** 键或 **<Enter>** 键。 有关“Startup”（启动）菜单的详细信息，请参阅“启动菜单功能”。

如果未进行用户输入，系统会将代码解压缩到 RAM 中，继续操作。 然后开始从 RAM 中运行代码，此时即会显示可用端口号及其状态（良好或断开）列表。

注： 以下屏幕信息是一个配置实例。 每个设备所显示的项目（例如地址、版本和日期）可能会有所不同。

```
Preparing to decompress.

Decompressing SW from RSCOD_2

85e000

OK

Running from RAM.

******************************************************Running SW Ver. 3.30 Date 03-Feb-2003 Time 10:10:37
******************************************************
```

```
HW version is X.X

Base Mac address is: 00:01:02:03:04:05

Dram size is: 32M bytes

Dram first block size is: 20M bytes

Dram first PTR is: 0xB70000

Flash size is: 8M


STAND ALONE

The BCM5625_A1 0 initiate successfully

The BCM5625_A1 1 initiate successfully

02-Jan-2000 01:01:11%SSHD-W-NOHOSTKEY: SSHG_init: The SSH daemon cannot listen

for incoming connections, because a host key has not been generated.

The service will start automatically when a host key is generated.

01-Jan-2000 01:01:11 %INIT-I-InitCompleted: Initialization task is completed


console> 01-Jan-2000 01:01:12 %PS-I-PSUP: Power Supply #1 is up

01-Jan-2000 01:01:12%PS-W-PSDOWN: Power Supply #2 is down

01-Jan-2000 01:01:12%LINK-W-Up: 1/e1

01-Jan-2000 01:01:12%LINK-W-UP: 1/e2

01-Jan-2000 01:01:12%LINK-W-Up: 1/e3
```

```
01-Jan-2000 01:01:12%LINK-W-UP: 1/e4

01-Jan-2000 01:01:12%LINK-W-Up: 1/e5

01-Jan-2000 01:01:13%LINK-W-Up: 1/e9
```

成功引导设备之后，屏幕将显示系统提示 (console>)，此时即可启动配置过程。 可以使用本地终端进行配置。

设备配置简介

配置分两种类型或级别。 初始配置包括基本的配置功能以及基本的安全考虑。 高级配置包括动态 IP 配置以及更高级的安全考虑。

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

console> **enable**

console# **copy running-config startup-config**

初始配置

成功引导设备后，即会启动初始配置。 设备初始配置范围包括：

- 静态 IP 地址和子网掩码
- 默认网关
- 必须配置用户名和权限级别，以进行远程管理。

如果要从基于 SNMP 的管理站管理设备，则还必须配置 SNMP 团体字符串。

静态 IP 地址和子网掩码

在 PowerConnect 3324/3348 设备中，可以在每个端口上配置 IP 接口，其数量不受限制。 建议您在输入配置命令后，输入 show ip interface 命令，检查端口是否配置了 IP 地址。

注意： 只能为一个 VLAN 分配 IP 地址。 如果您将某个 IP 地址分配给其它任何 VLAN，新地址将覆盖原始 IP 地址。

要在 VLAN 上配置接口，请在系统提示符后输入命令，如以下配置实例所示：

console> **enable**

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address 100.1.1.1 /8
console(config-if)# exit
console(config)# exit
console# show ip interface

Gateway IP Address Activity status
---------------------- ----------------------

IP Address I/F
---------------------- ---------------------
100.1.1.1/8 vlan 1

console#
```

要在端口上配置接口，请在系统提示符后输入命令，如以下配置实例所示：

```
console> enable
console# configure
console(config)# interface ethernet 1/e1
console(config-if)# ip address 10.1.1.1 255.0.0.0
```

```
console(config-if)# exit

console(config)# exit

console# show ip interface


Gateway IP Address Activity status

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



IP Address I/F

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

10.1.1.1/8 1/e1



console#
```

默认网关

要通过远程网络管理 PowerConnect 3324/3348 设备，必须配置默认网关，即未指定特定网关时设备使用的网关。 所配置的网关 IP 地址必须与其中的一个设备 IP 接口属于同一子网。

要配置默认网关，请在系统提示符后输入命令，如以下配置实例所示：

```
console> enable

console# configure

console(config)# ip default-gateway 100.1.1.100

console(config)# exit
```

用户名、密码和权限级别

切记： 要通过远程终端或 Web 管理界面管理设备，必须输入用户名、密码和最高权限级别 (15)。 （最高权限级别提供对 CLI 配置环境的访问权限。） 有关权限级别的详细信息，请参阅 CLI 参考指南。

输入所配置的用户名作为远程管理会话的登录名。 要配置用户名和权限级别，请在系统提示符后输入命令，如以下配置实例所示：

```
console> enable

console# configure

console(config)# username admin password admin level 15

console(config)# exit
```

SNMP 团体字符串

简单网络管理协议 (SNMP) 提供了一种管理网络设备的方法。 支持 SNMP 的设备运行本地软件（代理）。 SNMP 代理维护用于管理设备的变量列表。 这些变量在管理信息库 (MIB) 中定义。 MIB 提供了由代理控制的变量。 SNMP 代理定义了 MIB 规格格式以及用于通过网络访问信息的格式。 对 SNMP 代理的访问权限由访问字符串和 SNMP 团体字符串控制。

此设备与 SNMP 兼容。 其包含支持一组标准和私有 MIB 变量的 SNMP 代理。 管理站的开发人员需要 MIB 树的精确结构并获取完整的私有 MIB 信息，才能管理 MIB。

除了 SNMP 管理站 IP 地址和团体（团体名称和访问权限）之外，所有参数均可以通过任何 SNMP 管理平台进行管理。 如果不存在团体字符串，则会禁用对设备的 SNMP 管理访问。
设备交付时未配置团体字符串。

以下屏幕信息显示默认设备配置：

```
console# enable

console# show snmp

Community-String Community-Access IP address

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

Traps are enabled.
```

```
Authentication-failure trap is enabled.
```

在初始配置过程中，可以通过本地终端设置团体字符串、团体访问权限和 IP 地址。

SNMP 配置选项如下：

- 团体字符串
- 访问权限选项： ro（只读）、rw（读写）或 su（超级）。
- 是否配置 IP 地址的选项： 如果不配置 IP 地址，则所有具有相同团体名称的团体成员均被授予相同的访问权限。

通常对设备使用两个团体字符串：一个（public 团体）具有只读权限，另一个（private 团体）具有读写权限：

- Public — 允许经授权的管理站检索 MIB 对象。
- Private — 允许经授权的管理站检索和修改 MIB 对象。

建议您在初始配置过程中，根据网络管理员的要求配置设备，以便于使用基于 SNMP 的管理站。

要配置 SNMP 站点 IP 地址和团体字符串，请：

1. 在控制台提示符后键入 **Enable**。 提示符将显示为 #。
2. 键入 configure，然后按 **<Enter >**键。
3. 在配置模式下，键入 SNMP 配置命令以及团体名称 (private)、团体访问权限（读写）和 IP 地址等参数，如以下实例所示：

```
console> enable

config# configure

config(config)# snmp-server community private rw 11.1.1.2

config(config)# exit

config# show snmp

Community-String Community-Access IP address

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

private readWrite 11.1.1.2

Traps are enabled.
```

```
Authentication-failure trap is enabled.

Trap-Rec-Address Trap-Rec-Community Version

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

System Contact:

System Location:
```

通过本地终端对设备进行初始配置即告完成。 通过所配置的参数可以从远程位置对设备进行进一步的配置。

高级配置

本节介绍基于 AAA（验证、授权和计费）机制的 IP 地址动态分配和安全保护管理。
本节包括以下主题：

- 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不但包括 IP 地址，
还可能会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。

要从 DHCP 服务器检索 IP 地址，请：

1. 选择任一端口并将其连接至 DHCP 服务器或包含 DHCP 服务器的子网，
以便检索 IP 地址。
2. 输入以下命令，以使用选定端口检索 IP 地址，如以下实例所示：

```
console> enable

console# configure

console(config)# interface vlan 1
```

```
console(config-if)# ip address dhcp hostname <string>

console(config-if)# exit

console(config)# exit
```

3. 设备将自动获取 IP 地址。

要验证 IP 地址，请：

1. 在系统提示符后，键入 **show ip interface**。 请参阅以下显示实例。

```
console> enable

console# show ip interface



Gateway IP Address Activity status

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



IP Address I/F

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

10.1.1.1/8 vlan1



console#
```

注： 检索 DHCP 服务器的 IP 地址时无需删除设备配置。

从 BOOTP 服务器获取 IP 地址

此设备支持标准 BOOTP 协议，可以从 Internet 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 BOOTP 服务器的子网，

以便检索 IP 地址。

2. 在系统提示符后键入删除启动配置命令，从快闪内存中删除启动配置。 设备将在没有配置的情况下重新引导，并在 60 秒内开始发送 BOOTP 请求。
3. 设备将自动获取 IP 地址。

注： 一旦开始执行“删除启动配置”命令，使用 ASCII 终端或键盘输入任何内容均会自动终止配置过程，而且设备不会从 BOOTP 获取 IP 地址。

以下实例说明了该步骤：

```
console> enable

console# delete startup-config
```

要验证 IP 地址，请参阅以下显示实例：

```
console> enable

console# show ip interface



Gateway IP Address Activity status

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



IP Address I/F

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

10.1.1.1/8 vlan1



console#
```

现在设备即已配置了 IP 地址。

要从 BOOTP 服务器检索 IP 地址，必须删除设备配置。

安全保护管理和密码配置

系统安全保护通过 AAA（验证、授权和计费）机制进行处理，该机制管理用户访问权限、权限和管理方法。 AAA 使用本地和远程用户数据库。 通过 SSH 机制进行数据加密。

系统交付时未配置默认用户名或密码—所有用户名和密码均由用户定义。 如果用户定义的密码丢失，则可以从“Startup”（启动）菜单调用密码恢复程序。 该程序仅适用于本地终端，允许不输入密码从本地终端访问一次设备。

注： 请确保您在输入用户名和密码时始终包括管理权限级别 15。

配置 安全保护密码

可以为以下服务配置安全保护密码：

- 控制台
- 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，即用户拥有访问权限，但没有配置权限。 必须特别设置为优先级 15 才能启用对设备的访问和配置权限。

有关密码限制的详细信息，请参阅“配置网络安全保护”。

配置初始控制台密码

要配置初始控制台密码，请输入以下命令：

```
console> enable

console# configure

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 console

console(config-line)# exit

console(config)# exit
```

- 通过控制台会话首次登录设备时，请在密码提示符后输入 console。
- 将设备模式更改为“启用”时，请在密码提示符后输入 console。

配置初始 Telnet 密码

要配置初始 Telnet 密码，请输入以下命令：

```
console> enable

console# configure

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 admin

console(config-line)# exit

console(config)# exit
```

- 通过 Telnet 会话首次登录设备时，请输入 admin。
- 将设备模式更改为“启用”时，请输入 admin。

配置初始 SSH 密码

要配置初始 SSH 密码，请输入以下命令：

```
console> enable
console# configure
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 admin
console(config-line)# exit
console(config)# exit
```

- 通过 SSH 会话首次登录设备时，请输入 admin 作为密码。
- 将设备模式更改为“启用”时，请输入 admin 作为密码。

配置初始 HTTP 密码

要配置初始 HTTP 密码，请输入以下命令：

```
console> enable
console# configure
console(config)# ip http authentication local
console(config)# username admin password admin level 15
```

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

配置初始 HTTPS 密码

要配置初始 HTTPS 密码，请输入以下命令：

```
console> enable

console# configure

console(config)# ip https authentication local

console(config)# username admin password admin level 15

console(config)# exit
```

配置控制台、Telnet 或 SSH 会话时只需输入一次以下命令，以便使用 HTTPS 会话。

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

```
console> enable

console# configure

console(config)# crypto certificate generate key-generate

console(config)# ip https server

console(config)# exit
```

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 服务要求 15 级访问权限，并直接连接至配置级别的访问权限。

配置过程实例

本节旨在说明与 PowerConnect 3324/3348 设备建立远程网络管理连接所需的基本步骤， 对设备上可用的各种配置或相关命令不做解释。

本节介绍在设备出厂配置和定义仍未改变时对设备的首次访问。 如果以前输入的配置有问题，
则应删除启动配置文件（打开设备电源时的配置）并重新引导设备。请参阅
"设备默认设置"。

设备安装要求

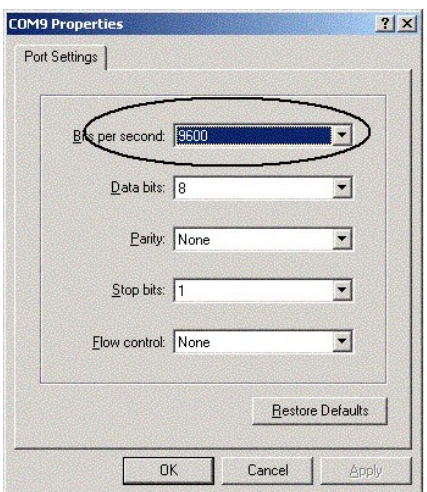
本实例需要以下组件：

- PowerConnect 3324/3348 设备
- 安装了以下软硬件的 PC 工作站：
  - NIC（网络适配器）卡
  - ASCII 终端应用程序（例如，Microsoft® Windows® MS Hyper Terminal 或 Procomm Plus Terminal）
  - 浏览器应用程序
- 一根虚拟调制解调器 F2F 电缆
- 直通或绞接 UTP (cat 5) 电缆

初始连接

初始连接如下所示：

1. 将 PowerConnect 3324/3348 设备连接至作为 ASCII 终端的计算机的 RS232 接口。
2. 使用以下设置设置 ASCII 终端，并选择相应的 COM 端口（在本实例中，使用 Windows Hyper Terminal 应用程序）



注： 9600 是新设备的默认波特率。 如果使用 9600 波特率不能查看设备终端，则尝试使用其它波特率设置（可以设置不同的设备波特率）。

3. 使用 F2F 虚拟调制解调器电缆，将运行 ASCII 终端应用程序的 PC 连接至设备。
4. 将设备电源线连接至电源插座，打开设备电源。 此时即会显示以下屏幕信息：

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

```
***************** SYSTEM RESET *****************

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


Booting...



------ Performing the Power-On Self Test (POST) ------

UART Channel Loopback Test........................PASS

Testing the System Cache..........................PASS

Testing the System SDRAM..........................PASS

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

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

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

Testing CPU PCI Bus Device Configuration..........PASS


BOOT Software Version 1.0.0.13 Built 11-May-2003 14:58:20

Processor: MPC8245 Rev 0.14, 250 MHz (Bus: 100MHz), 32 MByte SDRAM.

I-Cache 16 KB, linesize 32.D-Cache 16 KB, linesize 32.

Cache Enabled.


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

Preparing to decompress...
```

解压缩映像文件后，将显示以下屏幕信息，包括设备信息、SW/HW 版本和所有现有接口的状态（良好/断开）：

```
Decompressing SW from image-2

8cc000

OK

Running from RAM...


Update Host params for stand-alone


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

*** Running SW Ver. 1.0.0.52 Date 29-Jun-2003 Time 19:04:06 ***

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


HW version is 00.00.01

Base Mac address is: 00:06:5b:ff:59:4d

Dram size is : 32M bytes

Dram first block size is : 20M bytes

Dram first PTR is : 0xB20000

Flash size is: 8M


STAND ALONE

The BCM5615_A1 0 initiate successfully
```

```
01-Jan-2000 01:01:10 %SSHD-W-NOHOSTKEY: SSH has been enabled but an encryption key was not found.

For key generation use the 'crypto key generate' commands. The service will start automatically when a host
key is generated.

01-Jan-2000 01:01:11 %INIT-I-InitCompleted: Initialization task is completed

console> 01-Jan-2000 01:01:11 %BOX-I-PSUP: Power Supply #1 is up

01-Jan-2000 01:01:11 %BOX-W-PSNOTPRES: Power Supply #2 is not present

01-Jan-2000 01:01:11 %LINK-W-Down: 1/e1

01-Jan-2000 01:01:11 %LINK-W-Down: 1/e2

01-Jan-2000 01:01:11 %LINK-W-Down: 1/e3

.....

.....

Jan-2000 01:01:13 %LINK-W-Down: 1/e22

01-Jan-2000 01:01:13 %LINK-W-Down: 1/e23

01-Jan-2000 01:01:13 %LINK-W-Down: 1/e24

01-Jan-2000 01:01:13 %LINK-W-Down: 1/g1

01-Jan-2000 01:01:13 %LINK-W-Down: 1/g2

01-Jan-2000 01:01:14 %LINK-I-Up: Vlan 1

01-Jan-2000 01:01:14 %LINK-I-Up: 1/e1

console>
```

设备准备就绪，可以进行配置。

设备默认设置

要返回设备默认设置，请在优先模式提示符 (#) 后输入 **delete startup-config** 命令，并重新引导设备。 设备重新加载后，即会使用默认设置。

```
console>

console> enable

console# delete startup-config

Startup file was deleted

console# reload

This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n] ?

y


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

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

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

.

.

.

.
```

远程管理访问

要进行远程设备管理（Telnet、Web 等），请执行以下操作：

1. 在控制台输入命令 **enable**，进入优先执行屏幕模式，如下所示：

```
console>enable

console#
```

2. 使用 CAT5 电缆，通过其中一个以太网端口（本实例中为端口 e1）或通过与设备相连的网络，将管理站 (PC) 连接至设备。 请确保（在 ASCII 终端上）接口状态更改为“良好”，且在 30 秒之后 STP 状态为“传输”：

```
console>enable

Console#

01-Jan-2000 01:43:03 %LINK-I-Up: Vlan 1

01-Jan-2000 01:43:03 %LINK-I-Up: 1/e1

01-Jan-2000 01:43:34 %STP-I-PORTSTATUS: Port 1/e1: STP status Forwarding
```

3. 在控制台输入命令 **configure**，进入配置屏幕模式，如下所示：

```
console> enable

console# configure

console(config)#
```

4. 在控制台输入命令 **interface ethernet**，通过 VLAN1 进入设备配置屏幕模式，如下所示：

```
console> enable

console# configure

console(config)# interface vlan 1

console (config)# exit
```

5. 通过为管理站所连接的接口分配 IP 地址来定义 IP 地址（本实例中为 50.1.1.1）。 如果管理站直接连接至接口，则接口上的 IP 地址必须与管理站属于同一子网。

```
console> enable

console# configure

console(config)#

console(config-if)# ip address 50.1.1.2 /8

01-Jan-2000 01:48:37 %LINK-W-Down: Vlan 1

console(config-if)# exit

console(config)# exit
```

6. 如果管理站未直接连接至接口（即远程网络的成员），则定义设备上的默认网关。 网关所配置的 IP 地址即是连接至设备的路由器接口 IP。

```
console> enable

console# configure

console(config-if)#

console(config-if)# exit

console(config)# ip default-gateway 50.1.1.100

console(config)# exit
```

7. 通过设备对管理站执行 ping 命令，确保实现连接（在此之前等待 30 秒，直至端口处于 STP 传输状态）。 在本实例中，管理站 IP 为 50.1.1.3：

```
console> enable

console# configure

console(config)#

console(config)# exit
```

```
console# ping 50.1.1.2

64 bytes from 50.1.1.2: icmp_seq=1. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=2. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=3. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=4. time=0 ms


----50.1.1.2 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

console#
```

8. 定义用户名和密码，以允许远程用户（telnet、Web 服务器等）对设备进行完全（权限级别 15）访问。 在本实例中，用户名和密码均为 Dell。

```
console#

console# configure

console(config)# username Dell password Dell level 15

console(config)#
```

9. 配置控制台、Telnet、SSH、HTTP 和HTTPS 安全保护密码：

```
console> enable

console# configure

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** admin

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

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** admin

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

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** admin

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

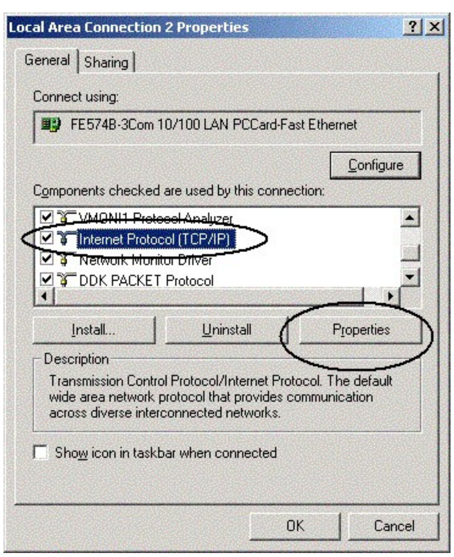
```
console(config)# ip http authentication local

console(config)# username admin password admin 15

console(config)# ip https authentication local

console(config)# username admin password admin 15

console(config)# crypto certificate generate key-generate

console(config)# ip https server

console(config)# exit

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

设备现已配置就绪，可以运行 Web 管理界面。

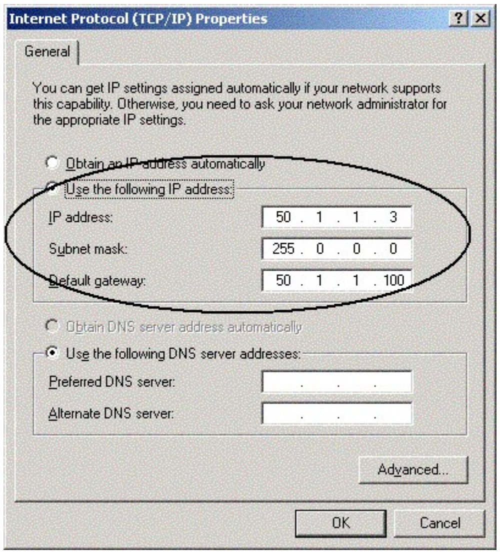
开始运行管理站

要开始运行设备，请执行以下操作：

1. 为要用作远程管理站的 PC 定义 IP 地址。 在 Windows 开始菜单中，单击 **“Start”（开始）>“Settings”（设置）>“Network and Dial-up Connections”（网络和拨号连接）**。
2. 右击用于管理的网络连接。 屏幕将显示连接属性窗口。



3. 选择配置 Internet 协议 (TCP/IP) 的选项，然后单击 **“Properties”（属性）**。
屏幕将显示 Internet 协议 (TCP/IP) 属性窗口。



4. 选择 **“Use the following IP address”（使用下面的 IP 地址）**选项。

5. 在 Internet 协议 (TCP/IP) 属性窗口中，静态（不通过 DHCP）定义 PC 的 IP 地址、掩码和默认网关。

注： 如果 PC 连接至路由器但未直接连接至 PowerConnect 3324/3348 设备，则必须将默认网关配置为 PC 所连接的路由器接口（直接连接至 PowerConnect 设备）的 IP 地址。

Telnet 访问

使用 Windows/DOS 命令行或 Telnet 应用程序，通过 Telnet 访问设备。 切记输入相应的密码。
通过设备上定义的 IP 地址进行连接。

一旦授予访问权限，对命令的使用与直接进行设备管理时相同：

1. 在 Windows 下单击 **“Start”（开始）>“Run”（运行）**，然后输入命令 cmd。 屏幕将显示标准 Windows 命令行界面。

2. 输入命令 **Telnet** 和设备 IP 地址。

```
Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-2000 Microsoft Corp.

C:\>telnet 50.1.1.2

01-Jan-2000 02:40:23 %MSCM-I-NEWTERM: New TELNET connection from 50.1.1.2
```

```
User Name:Dell

Password:****


console# show ip interface


Gateway IP Address Activity status

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

50.1.1.100 inactive


IP Address I/F

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

50.1.1.1/8 vlan 1


console#
```

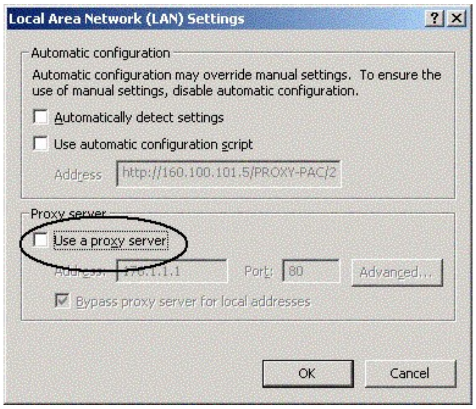
请注意，设备会提示（在 ASCII 终端中）Telnet 会话状态：

```
console> 01-Jan-2000 02:39:04 %MSCM-I-NEWTERM: New TELNET connection from 50.1.1.3

01Jan-2000 02:39:11 %MSCM-I-TERMTERMINATED: TELNET connection from 50.1.1.3 terminated
```

Web 访问（HTTP 服务器）

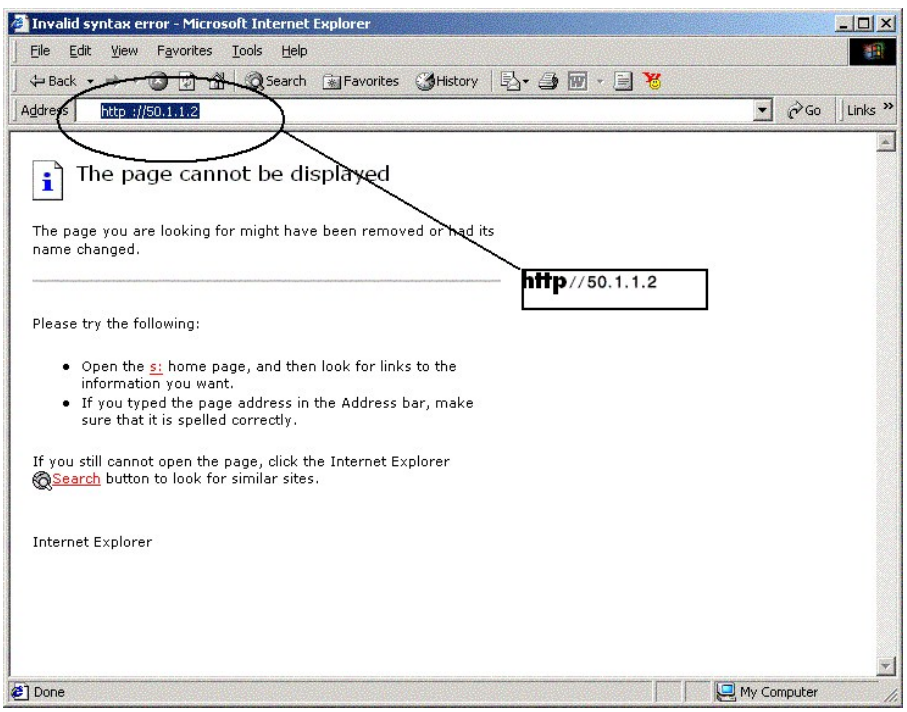
要对设备进行 Web 访问，请执行以下操作：

1. 为避免使用 HTTP 代理服务器时出现某些问题，请禁用（不选中）浏览器上的代理设置（Microsoft Internet 浏览器>"Tools"（工具）>"Internet Options"（Internet 选项）>"Connections"（连接）>"LAN settings"（局域网设置））：



禁用代理窗口

2. 在浏览器窗口中，键入以前在设备上配置的 IP（带或不带 http:// 前缀均可）：

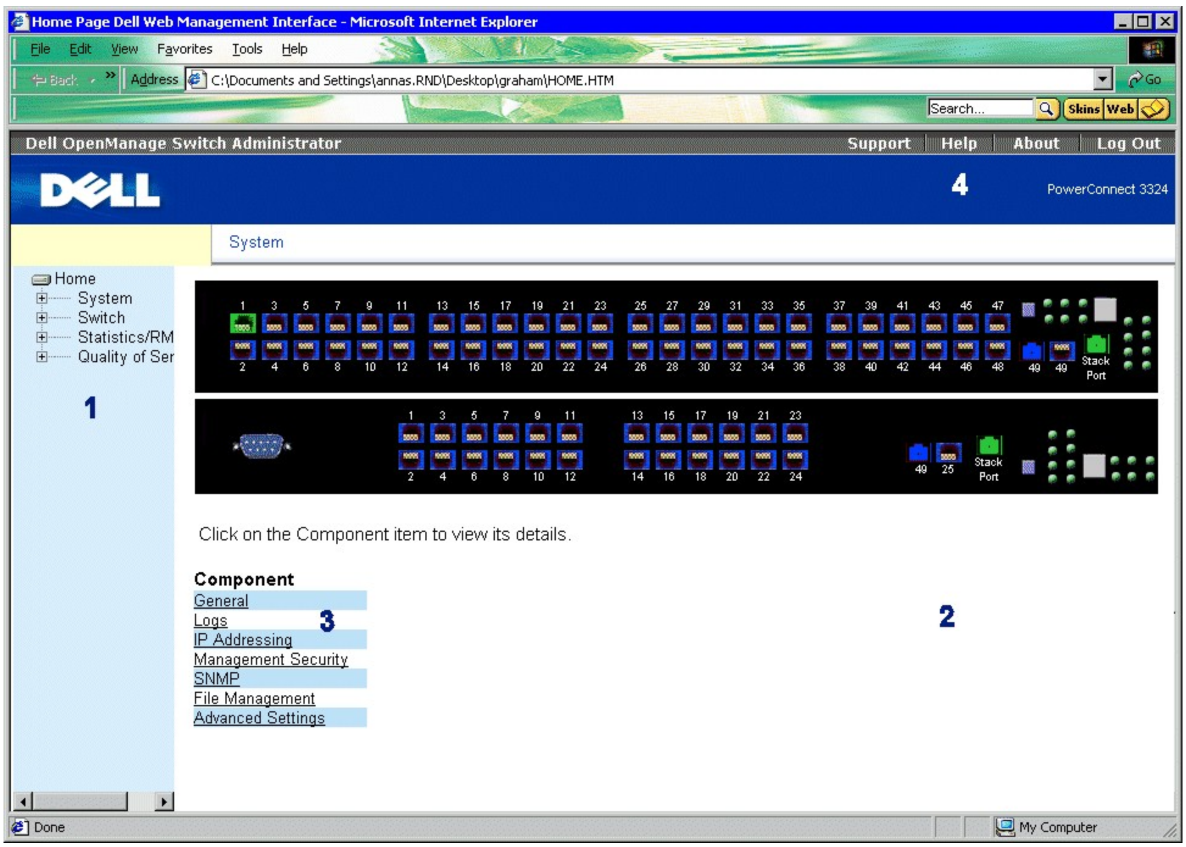


登录界面

3. 显示验证窗口时，输入用户名和密码：

密码提示

屏幕将显示设备 Web 管理界面。



PowerConnect 3324/3348 Web 管理界面

PowerConnect 3324/3348 Interface Components Table（PowerConnect 3324/3348 界面组件表）列出了界面组件及其相应的编号：

配置堆叠

堆叠简介

堆叠的 PowerConnect 3324/3348 装置可以用作单个系统。 每个堆叠有一个主装置和最多五个成员装置。 主装置将：

- 管理所有成员设备设置。
- 配置成员端口。
- 管理在成员环境中发生的事件。

所有堆叠装置的事件日志由选定的主装置管理和报告。 需通过主装置访问成员装置，但是每个装置都可以通过其 ASCII 终端（RS-232 端口）进行访问。

堆叠要求

建立堆叠之前，请执行以下堆叠要求：

- 确保每个装置均已插入堆叠链接模块。
- 确保所有电缆均已正确连接。
- 所有装置均已通电。 几秒钟后，装置 ID LED 将闪烁。
- 每个成员装置都有装置 ID。有关选择装置 ID 的详细信息，请参阅“堆叠 ID 按钮”。

配置堆叠

本节包含配置堆叠的说明。 要配置堆叠，请：

注： 必须在 15 秒钟内选择堆叠装置 ID。

1. 插入选定的主装置。 设备将开始进行引导。
2. 使用**堆叠 ID**按钮选择装置 1，直至选定堆叠 LED 1。 如果选定的装置是堆叠主装置，LED 将在 15 秒钟内停止闪烁。

注： 如果堆叠 LED 继续闪烁，则主装置尚未加入组。

3. 插入选定的成员装置。 设备将开始进行引导。
4. 使用**堆叠 ID**按钮在 15 秒钟内选择装置 2。
5. 对所有堆叠成员重复步骤 3 和 4。

注： 请按照各自的装置 ID 堆叠装置。例如，先堆叠主装置，并将装置 2 直接放在主装置下。

扩展堆叠

本节包含添加堆叠成员的说明。 要扩展堆叠，请：

注： 必须在 15 秒钟内选择堆叠装置 ID。

1. 确保堆叠运行正常。
2. 将下部堆叠连接器连接至附加堆叠成员装置。
3. 插入新的堆叠装置。 设备将开始进行引导。

4. 使用**堆叠 ID**按钮在 15 秒钟内选择装置编号。
5. 对于每个新成员，请打开现有的链路环并连接新成员的堆叠电缆。

有关更换堆叠成员和重新分配装置 ID 的信息，请参阅“更换堆叠成员”。

重新引导设备

注： 重新引导设备之前，请保存设备配置。 重启动设备后，所有未保存的配置更改都将丢失。

1. 进入 CLI 模式。 系统将显示以下提示：

```
Console > enable
```

2. 输入 Reload。 系统将显示以下信息：

```
>reload

This command will restart the whole system and disconnect your current session. Do you want to continue?
```

3. 输入 Y。 设备将重新引导。

启动菜单功能

在“Startup”（启动）菜单中，可以执行其它设备配置功能。 “Startup”（启动）菜单会显示以下配置功能：

- 下载软件
- 删除 FLASH 文件
- 删除 FLASH 扇区

以下屏幕信息示例了“Startup”（启动）菜单：

```
[1] Download Software

[2] Erase Flash File

[3] Erase Flash Sectors

[4] Password Recovery Procedure

[5] Enter Diagnostic Mode
```

```
[6] Back（返回）

Enter your choice or press 'ESC' to exit: Startup Menu
```

下载软件

使用“Startup”（启动）菜单

通过在引导进程中访问“Startup”（启动）菜单可以下载设备软件。

从 CLI 模式开始下载软件：

1. 进入 CLI 模式。 系统将显示以下提示：

```
console>
```

2. 键入 reload。 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]?
```

3. 键入 Y。 设备将重新引导。
4. 在 2 秒钟内按 <Return> 键或 <Esc> 键。 系统将显示 **“Startup”（启动）**菜单。

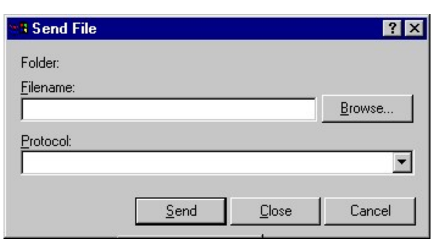
注： 必须在 2 秒钟内按 <Return> 键或 <Esc> 键，才能显示 **“Startup”（启动）**菜单。

注： 如果未在 35 秒钟内作出任何选择，设备将超时。 使用 CLI 可以重设超时时段。

5. 键入 1。 系统将显示以下提示：

```
Downloading code using XMODEM.
```

6. 使用任一 VT100 仿真程序，选择下载文件选项。 系统将显示 **“Send File”（发送文件）**窗口。 单击 **“Send”（发送）** 按钮。



发送文件窗口

7. 输入配置文件的文件路径。
8. 确保协议定义为 Xmodem。
9. 单击**“Send”（发送）**。 软件将被下载。

设备将自动重新引导。

注： 开始下载软件之前，必须先配置 TFTP 服务器。

删除 FLASH 文件

使用 ASCII 终端可以删除设备配置。 如果配置被删除，则必须重新配置所有 IP 主机参数以及通过 CLI、Web 管理界面或 SNMP 配置的参数。

要删除设备配置，请：

1. 验证 ASCII 终端已连接至设备。
2. 连接电源电缆。 设备将引导，并显示**“Startup”（启动）**菜单。 设备将开始进行引导。
3. 在两秒钟内按 <Esc> 键退出或按 <Enter> 键。 系统将显示**“Startup”（启动）** 菜单。
4. 键入表明您的选择的数字或按 <Esc> 键退出。 在两秒钟内键入 2。 系统将会显示以下信息：

```
Warning! About to erase the file from flash Are you sure (Y/N)?
```

5. 键入 Y。系统将显示以下信息。

```
? Flash file name (8 characters, Enter for none.)
```

6. 输入 `config` 作为 FLASH 文件名。 配置被删除，交换机将重新引导。
   在“设备配置简介”中介绍了如何首次配置 IP 参数配置。

删除 FLASH 扇区

FLASH 存储器存储了可执行映像、CDB（MIB 文件）、日志文件和其它文件。

注意： 如果删除了 FLASH，则必须再次下载并安装所有软件文件。

1. 验证 ASCII 终端已连接至设备。
2. 连接电源电缆。 设备将引导，并显示“Startup”(启动)菜单。
3. 输入您的选择或按 <Esc> 键退出。 在两秒钟内键入 3。 系统将显示以下信息：

```
Warning! About to erase Flash Memory! FLASH size = 16252928. blocks = 64 Are you sure (Y/N)?
```

4. 键入 Y 确认。 系统将显示以下信息：

```
Enter First flash block (1 - 64):
```

5. 输入第一个要被删除的 FLASH 块，并按 <Enter> 键。 值的范围是 1 到 64。

系统将显示以下信息：

```
Enter Last flash block (1 - 64):
```

6. 输入最后一个要被删除的 FLASH 块，并按 <Enter> 键。 系统将显示以下信息：

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

7. 键入 Y 确认。 系统将显示以下信息：

```
Erasing flash blocks 1 - 1: Done.
```

密码恢复

要恢复访问方式密码，请：

1. 引导或重新引导设备，并在 2 秒钟内按 <Enter> 键。 屏幕将显示“Startup”（启动）菜单。 下图显示了“Startup”（启动）菜单：

```
Startup menu

[1] Download sw

[2] Erase from flash

[3] Erase Flash

[4] Password Recovery Procedure
```

2. 键入 4 并按 <Enter> 键。 系统将重设访问方式。

注： 要确保设备安全，请重新定义控制台访问方式密码。

有关配置用户密码的信息，请参阅 *CLI 用户指南*。

运行诊断程序

使用此选项之前，请与 Dell 技术支持部门联系。 请参阅“与 Dell 联系”。

将软件下载到堆叠装置

通过以下方法之一，将软件从 TFTP 服务器下载到所有堆叠装置：

- 顺序使用 CLI
- 单独使用 CLI
- 通过 Dell OpenManage™ Switch Administrator

顺序使用 CLI 下载软件

1. 确保将 IP 地址至少分配给主装置的一个端口。
2. 输入 `console# show version` 以验证每个装置上当前运行的软件版本。 以下是一个信息显示实例：

```
Unit SW version Boot version HW version

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

1 1.0.0.52 1.0.0.13 00.00.01

2 1.0.0.52 1.0.0.13 00.00.01
```

   系统将显示每个装置的软件版本、引导版本和硬件版本。 在上例中，装置的引导版本和硬件版本不同，但是软件版本相同。

3. 输入 `console# show bootvar` 以验证装置上处于激活状态的映像版本。
   以下是一个信息显示实例：

```
Unit Active image Selected for next boot

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

1 image-2 image-2

2 image-1 image-1
```

   系统将显示所有装置的激活的映像文件以及在设备重启动后激活的映像文件。

4. 输入 `console# copy tftp://{tftp 地址}/{文件名} image`，以将软件复制到主装置。 文件将被复制，但是只有在设备重启动后将文件选定为激活映像文件，
   该文件才能被激活。 以下是一个信息显示实例：

```
console# copy tftp://176.215.31.3/332448-10018.dos image

Erasing file image-1...done.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

注： 每个 ！表示已成功传输十个信息包。

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

5. 输入 console# copy tftp://50.1.1.2/332448-10018.dos unit://2/image。 设备软件被复制到堆叠成员 2。unit: the //2/image
表示软件将被复制到的堆叠成员装置 ID。 以下是一个信息显示实例：

```
..................Unit 2: Erased image-1

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

Copy: 2744590 bytes copied in 00:01:41 [hh:mm:ss]

console# 01-Jan-2000 01:01:55 %COPY-W-TRAP: The copy operation was completed successfully
```

6. 对每个堆叠成员重复步骤 5。 确保将软件复制到正确的堆叠成员装置 ID。
7. 输入 console# boot system image-2 以设置重启动设备后要使用的映像文件。
8. 输入 console# boot system unit 2 image-1。 这表示设备在重新引导后将从映像 1 进行引导。
9. 输入 console# reload。 系统将显示以下信息：

```
This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n]?
```

10. 输入 Y。 设备将重新引导。
11. 重复步骤 2 和 3 以验证处于激活状态的映像文件。

单独使用 CLI 下载软件

本节包含将设备软件分别下载到每个堆叠成员的说明：

- 从 TFTP 服务器到主装置
- 从主装置到成员装置

1. 确保将 IP 地址至少分配给主装置的一个端口。
2. 输入 console# show version 以验证每个装置上当前运行的软件版本。 以下是一个信息显示实例：

```
Unit SW version Boot version HW version

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

1 1.0.0.52 1.0.0.13 00.00.01
```

```
2 1.0.0.52 1.0.0.13 00.00.01
```

系统将显示每个装置的软件版本、引导版本和硬件版本。 在上例中，装置的引导版本和硬件版本均不同，但是软件版本相同。

3. 输入 console# show bootvar 以验证装置上当前处于激活状态的映像版本。
以下是一个信息显示实例：

```
Unit Active image Selected for next boot

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

1 image-2 image-2

2 image-1 image-1
```

系统将显示所有装置的激活的映像文件以及在设备重启动后激活的映像文件。

4. 输入 console# copy tftp://{tftp 地址}/{文件名} image，以将软件复制到主装置。 文件将被复制，但是只有在设备重启动后将文件选定为激活映像文件，
该文件才能被激活。 以下是一个信息显示实例：

```
console# copy tftp://176.215.31.3/332448-10018.dos image

Erasing file image-1...done.

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

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

5. 输入 console# boot system image-1 以设置重启动设备后要使用的映像文件。
6. 输入 console# reload。 系统将显示以下信息：

```
This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n] ?
```

7. 输入 Y。 设备将重新引导。
8. 重复步骤 3 以验证处于激活状态的映像文件。
9. 输入 console# copy image unit://2/image。 以下是一个信息显示实例：

```
console# copy image unit://2/image

...................Unit 2: Erased image-2
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

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

Copy: 2883576 bytes copied in 00:01:35 [hh:mm:ss]

console# 01-Jan-2000 01:08:59 %COPY-W-TRAP: The copy operation was completed successfully
```

10. 输入 console# boot system unit {装置编号} image-{文件名}。
11. 对每个堆叠装置重复步骤 9。
12. 输入 console# reload。 系统将显示以下信息：

```
This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n] ?
```

13. 输入 Y。 设备将重新引导。
14. 重复步骤 2 和 3 以确保正确的映像文件处于激活状态。

通过 PowerConnect 3324/3348 Dell OpenManage Switch Administrator 下载软件

有关通过 Dell OpenManage Switch Administrator 下载软件的说明，请参阅“管理文件”。

定义 SNMP 设置

简单网络管理协议 (SNMP) 提供了一种管理网络设备的方法。 支持 SNMP 的设备运行本地软件（代理）。

SNMP 代理维护用于管理设备的变量列表。 这些变量在管理信息库 (MIB) 中定义。 MIB 提供了由代理控制的变量。 SNMP 代理定义了 MIB 规范格式，以及通过网络访问信息的格式。

对 SNMP 代理的访问权限由访问字符串控制。 为与设备进行通信，嵌入式 Web 服务器将提交有效的团体字符串以供验证。

PowerConnect 设备的默认团体字符串是：

- Public — 允许经授权的管理站检索 MIB 对象。
- Private — 允许经授权的管理站检索和修改 MIB 对象。

如果未使用 SNMP，请：

- 更改默认团体字符串以防止未经授权擅自访问 PowerConnect 设备。
- 删除这两个默认团体字符串。 如果不存在团体字符串，则会禁用对 PowerConnect 设备的 SNMP 管理访问。

要删除字符串，请：

注： 要使用配置环境，必须为用户分配权限级别 15。

1. 键入 Enable。 提示符将显示 “#”符号。
2. 如果未启用优先执行级别的全局配置环境，请键入 configure 并按 <Enter> 键。
3. 键入 no snmp-server community private 并按 <Enter> 键，删除 **private** 团体字符串。
4. 键入 no snmp-server community public 并按 <Enter>键，删除 **public 团体字符串。**
5. 键入 exit。 退出配置环境。
6. 键入 copy running-config startup-config 并按 <Enter> 键，保存配置更改。

连接设备

为 PowerConnect 设备分配 IP 地址后，将设备连接至 PowerConnect 前面板上的 RJ-45 连接器。

注意： 如果禁用 RJ-45 端口的自动协商，则 auto-MDI/MDI-X 插针信号配置也将被禁用。

要将设备连接至 SFP 收发器端口，请：

1. 按照布线要求选择相应的 SFP 收发器类型：
2. 将 SFP 收发器（单独出售）插入 SFP 收发器插槽。
3. 使用相应的网络电缆，将设备连接至 SFP 收发器上的连接器。

注意： SFP 收发器链路形成后，相关联的集成 10/100/1000BASE-T 端口将被禁用。

要关闭所有设备，请从电源插座中拔下电源设备电缆。 电源插座应位于设备附近并应易于触及。

保护标记 B 表明此设备符合 PN-93/T-42107 和 PN-EN 55022: 1996 标准中的保护使用要求。

返回目录页面

[返回目录页面]

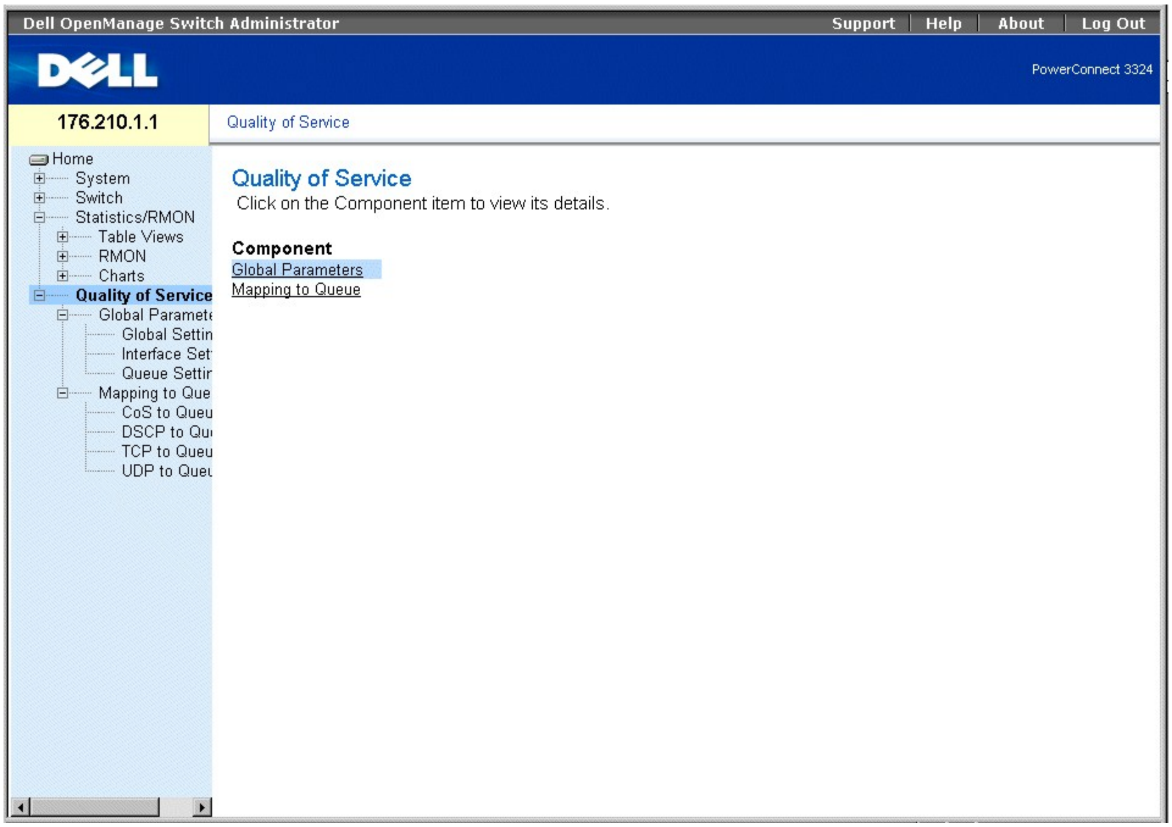
配置服务质量

Dell™ PowerConnect™ 3324/3348 用户指南

- 服务质量 (QoS) 概览
- 定义 QoS 全局参数
- 映射到队列

本节提供了定义和配置服务质量 (QoS) 参数的信息。

- 在树视图中单击 **"Quality of Service"（服务质量）**。 系统将打开 **"Quality of Service"（服务质量）**页面。



服务质量页面

本节包括以下主题：

- 服务质量 (QoS) 概览
- 定义 QoS 全局参数
- 映射到队列

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。 QoS 基于规则、帧计数器和环境来提高网络通信流量。

QoS 包含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：

- 分类 － 指定应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 [VPT] 和 DSCP [DiffServ 代码点]）。
- 排定优先级 － 为通信分配优先级并在相应的队列中排队以进行传输。

服务级别 (CoS) 信息

可以将八个 CoS 值映射到四个传输队列（队列 1 至 4）中的一个。 每个队列具有不同的优先级。 第一个队列的传输优先级最低，而第四个队列的传输优先级最高且在默认情况下不被映射。

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堆叠控制。

包括的三个映射表为：

- CoS 至队列映射表。
- DSCP 至队列映射表。
- TCP/UDP 至队列映射表。 默认情况下，TCP/UDP 表为空。

Cos 至队列映射表包含 CoS 与传输队列映射关系的默认值：

CoS 值	传输队列值
0	q2
1	q1（最低优先级 = 最佳传输能力）
2	q1（最低优先级 = 最佳传输能力）
3	q2
4	q2
5	q3
6	q3
7	q3

CoS 至队列映射表默认值

CoS 映射是针对每个系统进行启用的。 CoS 值的顺序为从 0 至 7，其中 0 表示最低优先级，
7 表示最高优先级。

可以将 DSCP 值映射到优先级队列。 **DSCP 至队列映射表默认值表**包含 DSCP 与传输队列映射关系的默认值：

DSCP 值	传输队列值

0-7	q1（最低优先级）
8-15	q1
16-23	q2
24-31	q2
32-39	q2
40-47	q3
48-55	q3
55-63	q3（最高优先级）

DSCP 至队列映射表默认值

DSCP 映射是针对每个系统进行启用的。

QoS 服务

信息包被分配到特定队列后，可以为此队列设定 QoS 服务。 可通过以下方法之一为输出队列配置安排方案：

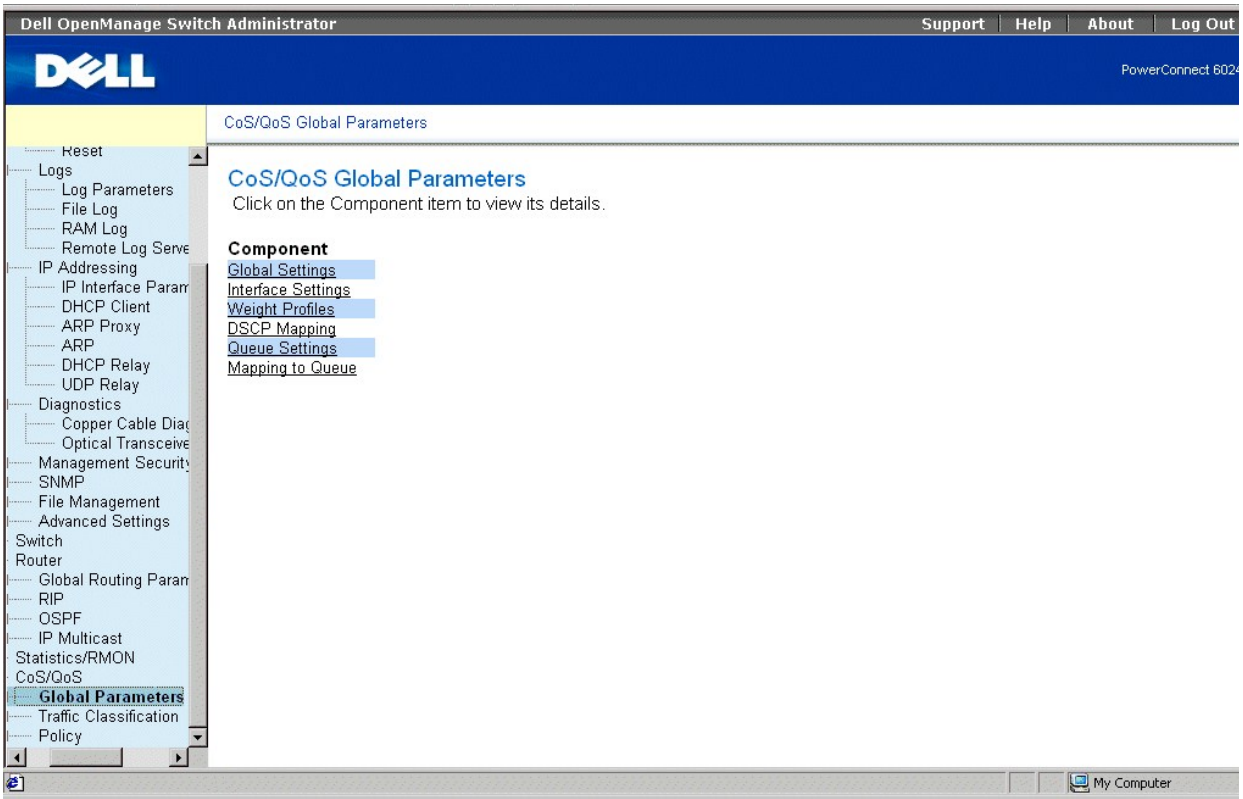
- 严格优先级 — 确保与时间密切相关的应用程序总是通过最快的路径传输。 严格优先级使网络管理员可以排定任务关键、与时间密切相关的通信的优先级，使其高于与时间相关度较低的应用程序的优先级。 例如，在严格优先级下，通过 IP 的语音通信会先于 FTP 或电子邮件 (SMTP) 通信进行传输。 只有严格优先级队列中的通信传输完毕后才会传输其余队列中的通信。
- 加权轮流 — 确保单个应用程序不会控制 PowerConnect 3324/3348 的传输能力。加权轮流 (WRR) 以轮流方式传输全部队列。 队列的优先级由队列长度定义。 队列长度越长，队列的传输优先级就越高。 例如，如果四个队列的队列加权分别为 1、2、3 和 4，则传输优先级最高的信息包将被分配到队列 4，传输优先级最低的信息包将被分配到队列 1。通过为队列 4 提供最高传输优先级，加权轮流将处理具有较高优先级的通信，同时确保适时传输具有低优先级的通信。

安排方案是针对整个系统进行启用的。 指定了严格优先级规则的队列将自动被分配到最高优先级队列。 默认情况下，所有的值均被设定为严格优先级。 更改为 WRR 模式时，默认的加权值为一。 使用 WRR 可以将队列加权值设定为任何顺序。 WRR 值可以针对每个系统进行设定。 最佳通信能力始终分配给第一个队列。 必须设定 WRR 值以使队列 1 保持最佳通信能力。

定义 QoS 全局参数

在 QoS 全局参数页面中可以设置服务质量全局参数。 要打开**“QoS Global Parameters”（QoS 全局参数）**页面，请：

- 在树视图中选择**“Quality of Service”（服务质量）**>**“Global Parameters”（全局参数）**。 系统将打开**“QoS Global Parameters”（QoS 全局参数）**页面。



QoS 全局参数页面

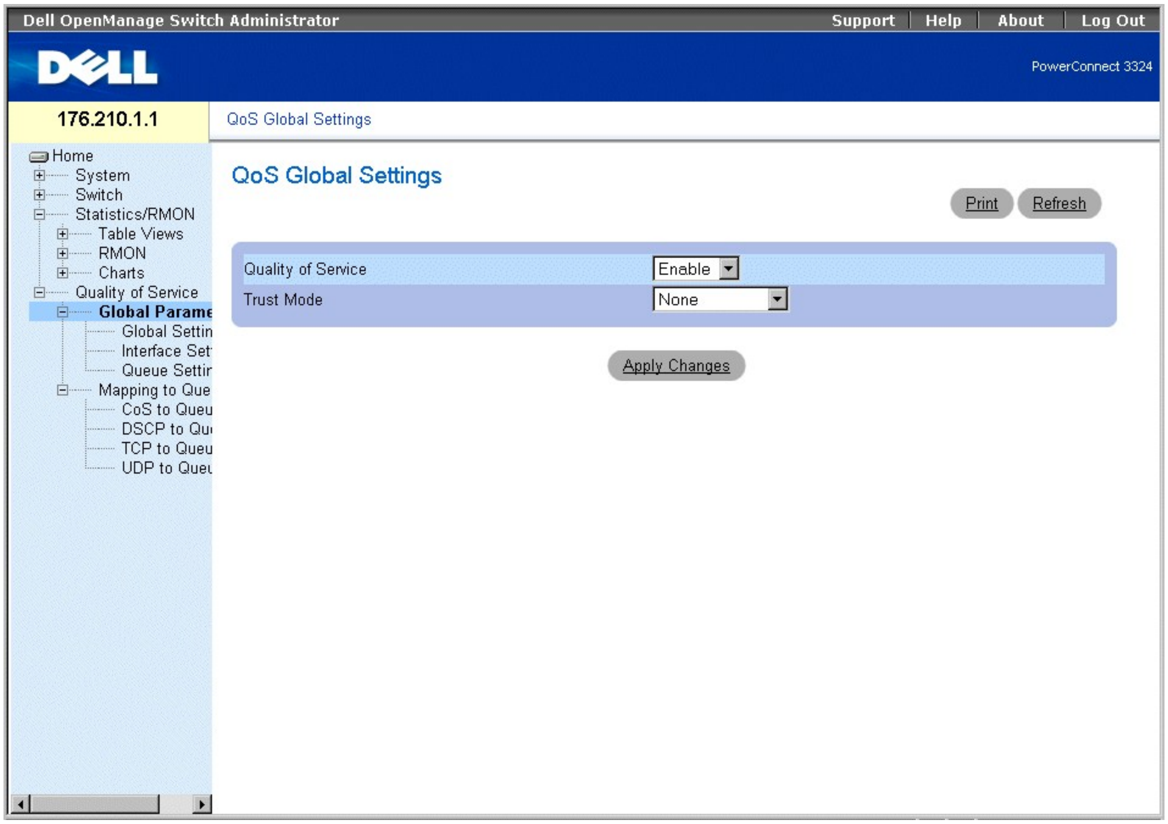
“QoS Global Parameters”（QoS 全局参数）页面包含以下链接：

- 配置全局 QoS 设置
- 定义 QoS 接口设置
- 定义队列设置

配置全局 QoS 设置

“QoS Global Parameters”（QoS 全局参数）页面使用户可以启用或禁用 QoS。 此外，用户还可以选择**“Trust”（信任）**模式。 此模式根据信息包中预定义的字段来确定输出队列，从而确定信息包的服务。 要打开**“QoS Global Settings”（QoS 全局设置）**页面，请：

- 在树视图中选择**“Quality of Service”（服务质量）>“Global Parameters”（全局参数）>“Global Settings”（全局设置）**。 系统将打开**“QoS Global Settings”（QoS 全局设置）**页面。



QoS 全局设置页面

"QoS Global Settings"(QoS 全局设置)页面包含以下字段:

- **"Quality of Service"(服务质量)**— 允许使用 QoS 管理网络通信。 字段值选项包括:
  - **"Enable"(启用)**— 在设备上启用 QoS。
  - **"Disable"(禁用)**— 在设备上禁用 QoS。
- **"Trust Mode"(信任模式)**— 确定用于对进入交换机的信息包进行分类的信息包字段。 如果未定义规则,则将根据相关的信任模式表映射包含预定义信息包字段(CoS、DSCP 或 TCP/UDP 端口)的通信。 不包含预定义信息包字段的通信将被映射为最佳能力传输。 可能的信任模式字段值包括:
  - **"CoS"**— 表示输出队列的分配由 IEEE802.1p VLAN 优先级标记 (VPT) 或分配到端口的默认 VPT 确定。
  - **"DSCP"**— 表示输出队列的分配由 DSCP 字段确定。
  - **"TCP/UDP"**— 表示输出队列的分配由 TCP/UDP 端口确定。

注: 接口**"Trust"(信任)**设置将代替全局**"Trust"(信任)**设置。

启用服务质量

1. 打开**"QoS Global Settings"(QoS 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)**。 系统将在设备上启用**"Quality of Service"(服务质量)**。

启用信任:

1. 打开**"QoS Global Settings"(QoS 全局设置)**页面。

2. 在**“Trust Mode”（模式）** 字段中选择信任设置。

3. 单击**“Apply Changes”（应用更改）**。 系统将在设备上启用/禁用信任。

使用 CLI 命令启用信任

下表概括了用于配置**“QoS Global Settings”（QoS 全局设置）**页面中字段的等效 CLI 命令。

CLI 命令	**说明**
qos trust [cos | dscp | tcp-udp-port]	将系统配置为基本模式和信任状态。
qos	在设备上启用 QoS。
no qos trust	恢复为非信任状态。

以下是 CLI 命令实例：

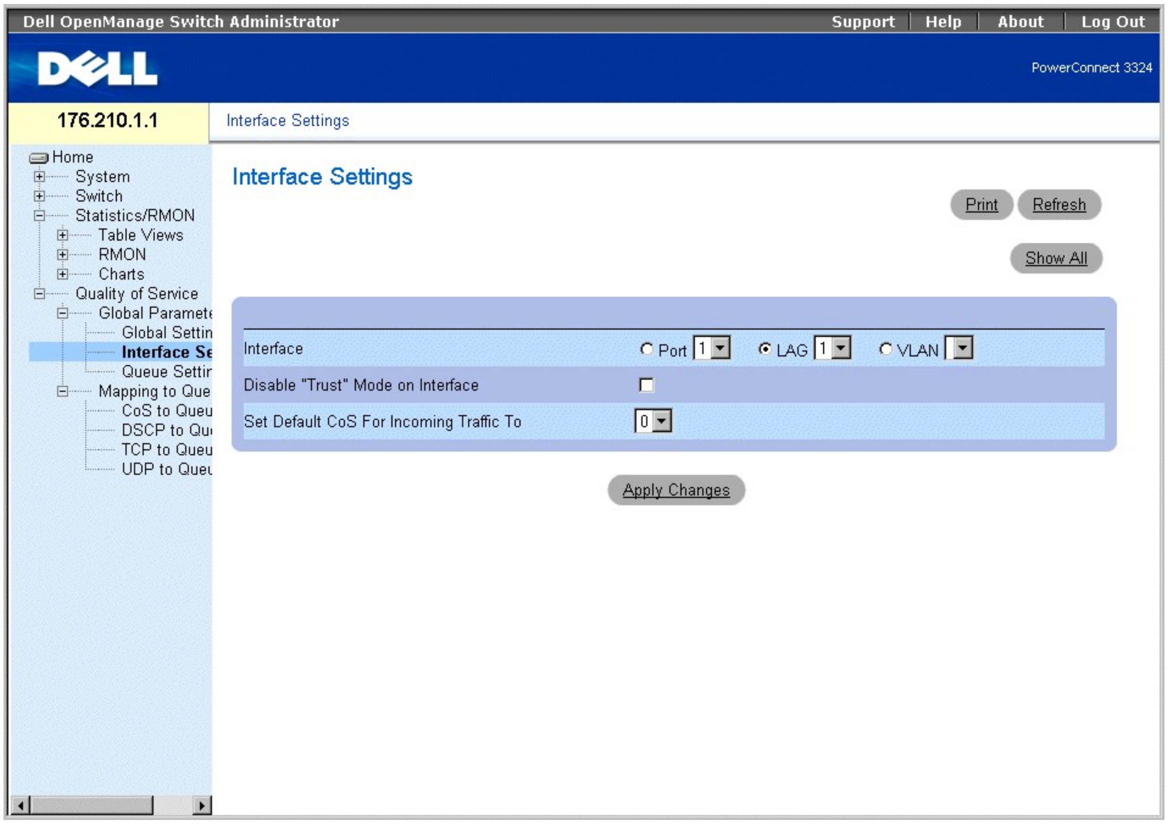
```
Console (config)# qos
```

```
Console (config)# qos trust dscp
```

定义 QoS 接口设置

“QoS Interface Settings”（QoS 接口设置）页面使用户可以针对每个接口定义是否要激活选定的信任模式。 在**“QoS Interface Settings”（QoS 接口设置）**页面中还可以选择传入的未标记信息包的默认优先级。 要打开**“QoS Interface Settings”（QoS 接口设置）**页面，请：

- 在树视图中单击**“Quality of Service”（服务质量）>“Global Parameters”（全局参数）>“Interface Settings”（接口设置）**。 系统将打开**“QoS Interface Settings”（QoS 接口设置）**页面。



接口设置页面

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

- **“Interface”（接口）**— 表示要应用信任模式的特定接口。 信任模式将应用到：
  - **“Port”（端口）**— 表示端口号。
  - **“LAG”**— 表示 LAG 号。
  - **“VLAN”**— 表示 VLAN 号。
- **“Disable "Trust" Mode on Interface”（在接口上禁用“信任”模式）**— 在设备上禁用信任值。 有关信任设置的详细信息，请参阅“配置全局 QoS 设置”。
- **“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/CoS 设置：

1. 打开**“QoS Interface Settings”（QoS 接口设置）**页面。
2. 在**“Interface”（接口）**字段中选择接口。
3. 如果要禁用特定接口上的信任模式，请选取**“Disable "Trust" Mode on Interface”（在接口上禁用“信任”模式）**复选框。
4. 将**“Set Default CoS For Incoming Traffic To”（将传入通信的默认 CoS 设置为）**设置为所需值。
5. 单击**“Apply Changes”（应用更改）**。 系统将为接口设定 QoS/CoS 设置。

使用 CLI 命令设定 QoS/CoS 接口

下表概括了用于配置 **“QoS Interface Settings”（QoS 接口设置）**页面中字段的等效 CLI 命令。

CLI 命令	**说明**
qos trust	为每个接口启用信任状态。
qos cos 默认 CoS	配置默认的端口 CoS 值。
no qos trust	在每个端口上禁用信任状态。

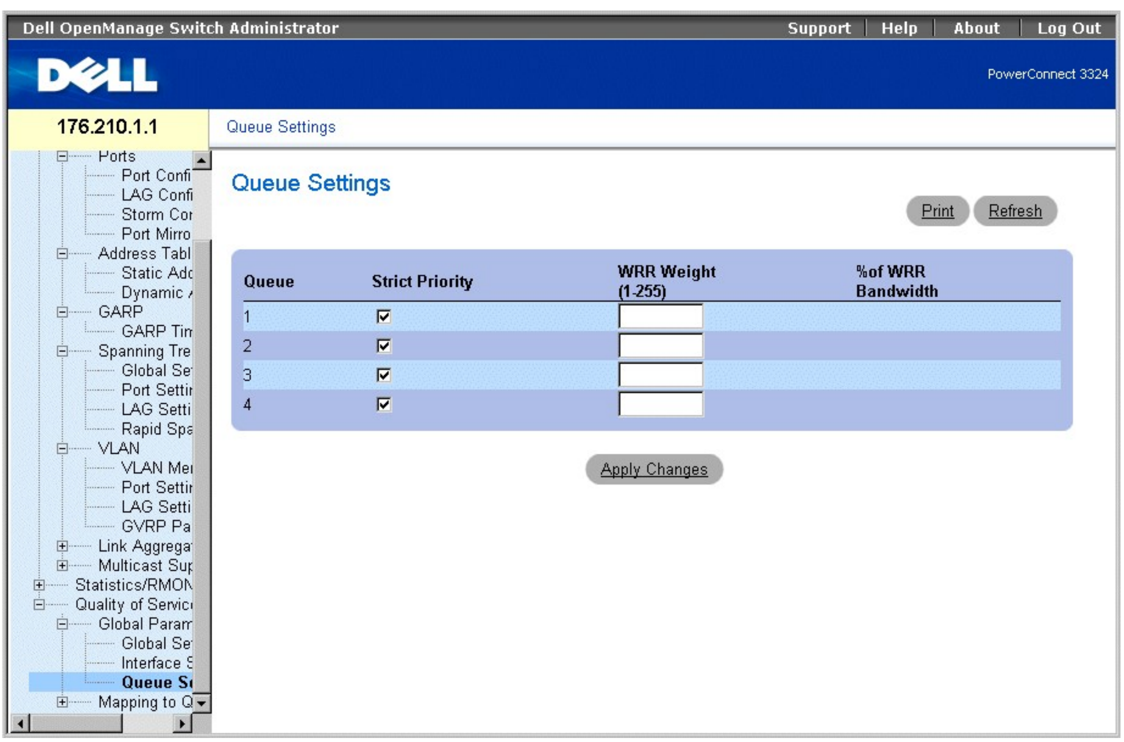
以下是 CLI 命令实例：

```
Console (config)# interface ethernet 1/e5

Console (config-if)# qos trust

Console (config-if)# qos cos 3
```

定义队列设置

“Queue Settings”（队列设置）页面使网络管理员可以配置加权轮流 (WRR) 并为队列分配带宽值。 每个队列均配置了不同的 WRR 和加权随机早期检测 (WRED) 值。 要打开 **“Queue Settings”（队列设置）**页面，请：

- 在树视图中选择 **“Quality of Service”（服务质量）>“Global Parameters”（全局参数）>“Queue Settings”（队列设置）**。 系统将打开 **“Queue Settings”（队列设置）**页面。



队列设置页面

“Queue Settings”（队列设置）页面包含以下字段：

- **“Queues”（队列）**— 指定队列号。

注： 队列过载可能会导致网络堵塞。

- **“Strict Priority”（严格优先级）**— 指定是否严格基于队列优先级安排通信。默认设置为已启用。
- **“WRR”**— 指定是否基于 WRR 方案安排队列通信。
- **“WRR Weight”（WRR 加权）**— 为外出队列分配 WRR 加权。 可能的字段值为 1 至 255，其中 1 为最低值，255 为最高值。
- **“% of WRR Bandwidth”（WRR 带宽百分比）**— 表示为 WRR 分配的带宽量。

定义队列设置：

1. 打开**“Queue Settings”（队列设置）**页面。
2. 定义**“Scheduling”（安排）**、**“WRR Weight”（WRR 加权）**和 **“Bandwidth”（带宽）**字段。
3. 单击**“Apply Changes”（应用更改）**。 系统将更新**“Queue Settings”（队列设置）**页面和设备。

使用 CLI 命令指定队列设置

下表概括了用于配置**“Queue Settings”（队列设置）**页面中字段的等效 CLI 命令。

CLI 命令	说明
wrr-queue bandwidth 加权 1 加权 2 **.** 加权 n	为外出队列分配加权轮流 (WRR) 加权。
show qos interface [接口 ID**] [queuing]**	显示接口 QoS 数据。

以下是 CLI 命令实例：

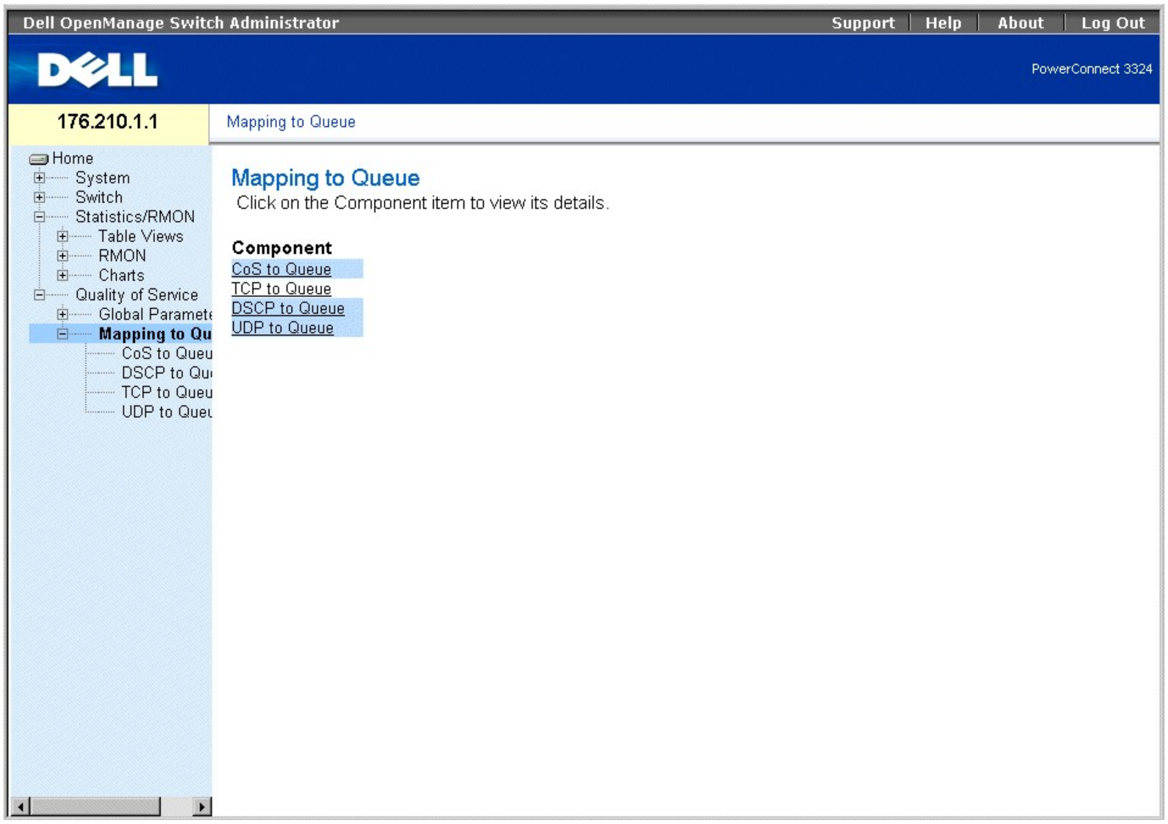
```
Console (config)# wrr-queue bandwidth 10 20 30 40

Console (config)# exit

Console # exit

Console> show qos interface ethernet 1/e3 queueing

Ethernet 1/e3

wrr bandwidth weights and EF priority:

qid-weights Ef - Priority
```

```
1 — 10 dis- N/A

2 — 20 dis- N/A

3 — 30 dis- N/A

4 — 1 dis- N/A

Cos-queue map:

cos-qid

0 - 2

1 - 1

2 - 1

3 - 2

4 - 2

5 - 3

6 - 3

7 - 3
```

映射到队列

“Mapping to Queue”（映射到队列）页面中包含指向将 CoS 和 DSCP 值以及 TCP 和 UDP 端口映射到 QoS 队列的页面的链接。 要打开**“Mapping to Queue”（映射到队列）**页面，请：

- 选择 **“Quality of Service”（服务质量）>“Mapping to Queue”（映射到队列）**。 系统将打开**“Mapping to Queue”（映射到队列）**页面。



映射到队列页面

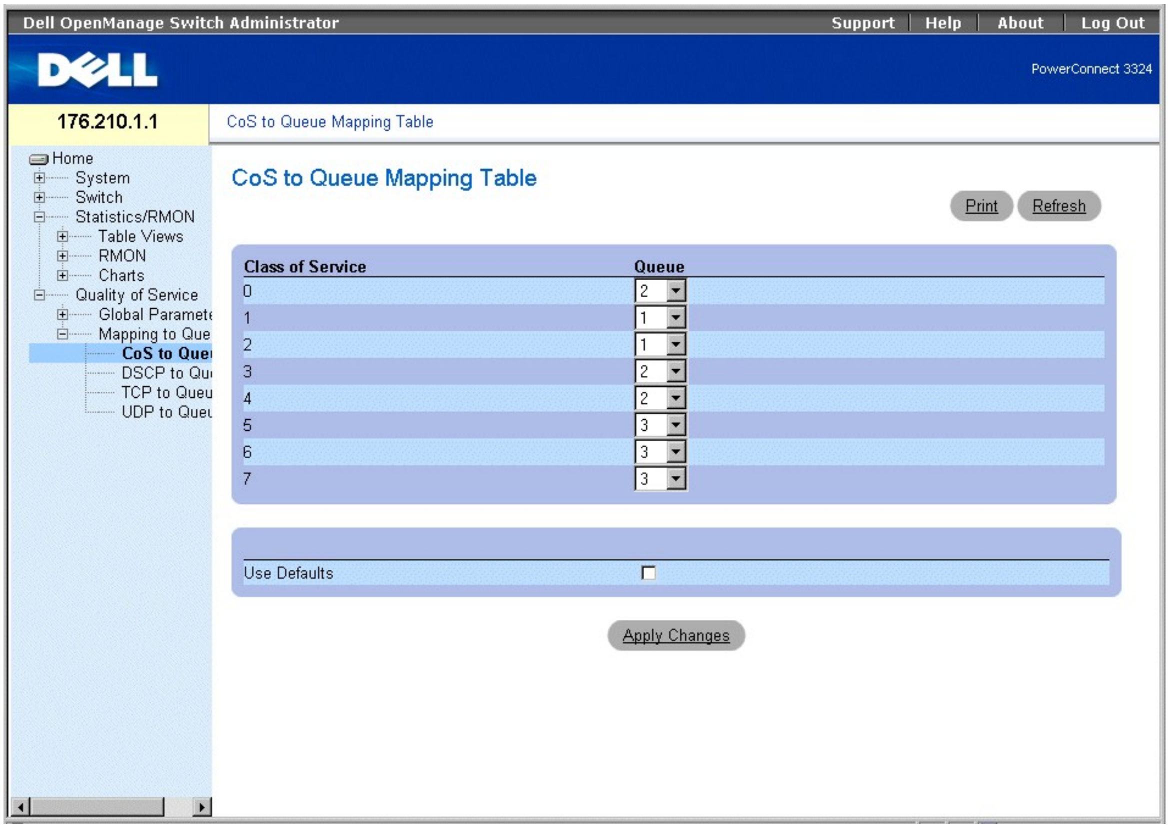
“Mapping to Queue”（映射到队列）页面包含指向以下主题的链接：

- 将 CoS 值映射到队列
- 将 TCP 端口值映射到队列
- 将 DSCP 值映射到队列
- 将 UDP 端口值映射到队列

将 CoS 值映射到队列

“CoS to Queue”（CoS 至队列）页面使网络管理员可以将 CoS 设置分类到通信队列。
要打开**“CoS to Queue Mapping Table”（CoS 至队列映射表）**页面，请：

- 在树视图中选择 **“Quality of Service”（服务质量）>“Mapping to Queue”（映射到队列）>“CoS to Queue”（CoS 至队列）**。
系统将打开
“CoS to Queue Mapping Table”（CoS 至队列映射表）页面。



CoS 至队列映射表页面

"CoS to Queue Mapping Table"（CoS 至队列映射表）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，七为最高值。
- **"Queue"（队列）**— 表示 CoS 优先级要映射到的通信传输队列。 支持四个通信优先级队列。

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堆叠控制。

- **"Use Defaults"（使用默认值）**— 使用将 CoS 值映射到传输队列的设备默认值。

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**"Mapping CoS Values to Queues Table"（将 CoS 值映射到队列表）**中字段的等效 CLI 命令。

CLI 命令	**说明**
wrr-queue cos-map 队列 ID **cos1.cosn**	将设定的 CoS 值映射到外出队列。

以下是 CLI 命令实例：

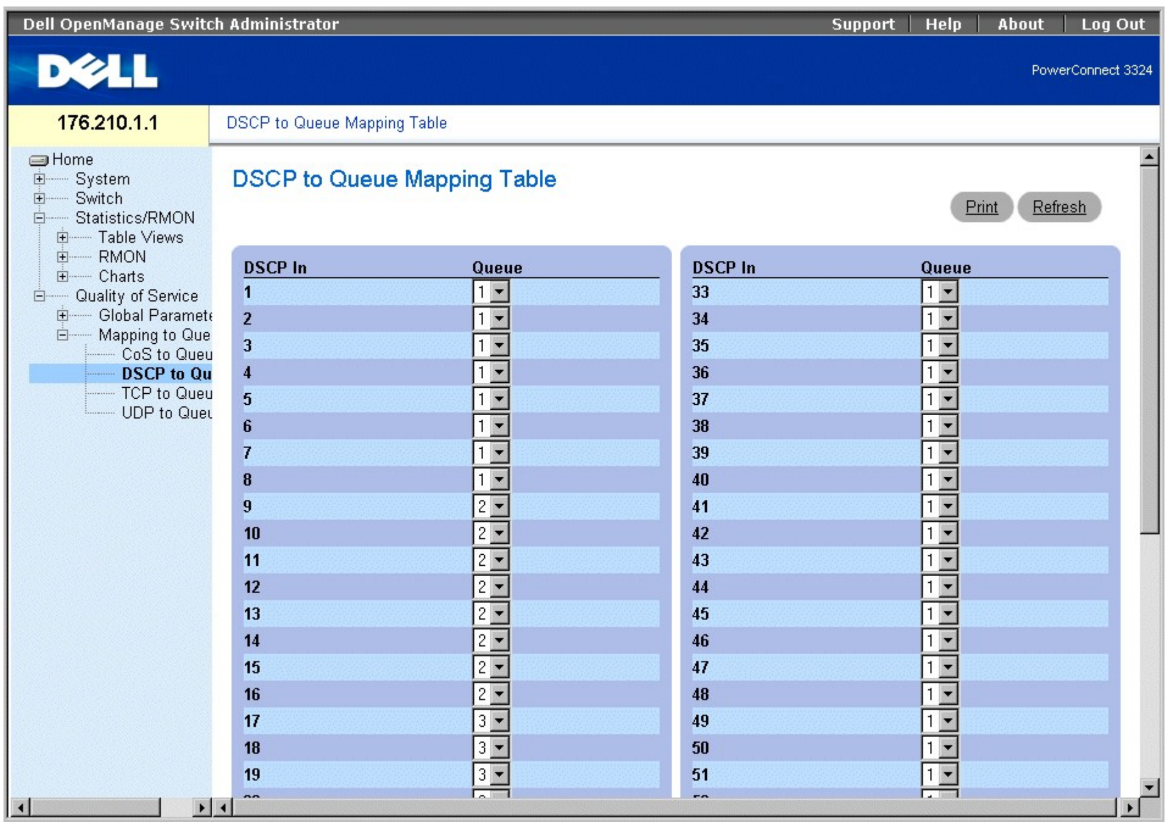
```
Console (config)# wrr queue cos-map 4 7
```

将 DSCP 值映射到队列

“DSCP Mapping”（DSCP 映射）页面使网络管理员可以确定为每个特定 DSCP 字段分配的输出队列。 要打开**“DSCP Mapping”（DSCP 映射）**页面，请：

注： 有关 DSCP 默认队列设置的列表，请参阅**“ DSCP 至队列映射表默认值”**。

- 在树视图中选择 **“Quality of Service”（服务质量）>“Global Parameters”（全局参数）>“Global Settings”（全局设置）>“DSCP Mapping”（DSCP 映射）**。 系统将打开**“DSCP Mapping”（DSCP 映射）**页面。



DSCP 映射页面

DSCP 默认队列设置列表包含以下字段：

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堆叠控制。

- **"DSCP In"(DSCP 位于）**－ 表示传入信息包中 DSCP 字段的值。
- **"Queue"（队列）**－ 表示具有特定 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。

映射 DSCP 值和分配优先级队列：

1. 打开 **"DSCP Mapping"（DSCP 映射）**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 不会被覆盖，但会为其值分配一个传输队列。

使用 CLI 命令设定 DSCP 值

下表概括了用于配置 **"DSCP Mapping"（DSCP 映射）**页面中字段的等效 CLI 命令。

CLI 命令	**说明**
qos map dscp-queue DSCP 列表 to 队列 ID	修改 DSCP 至队列映射。

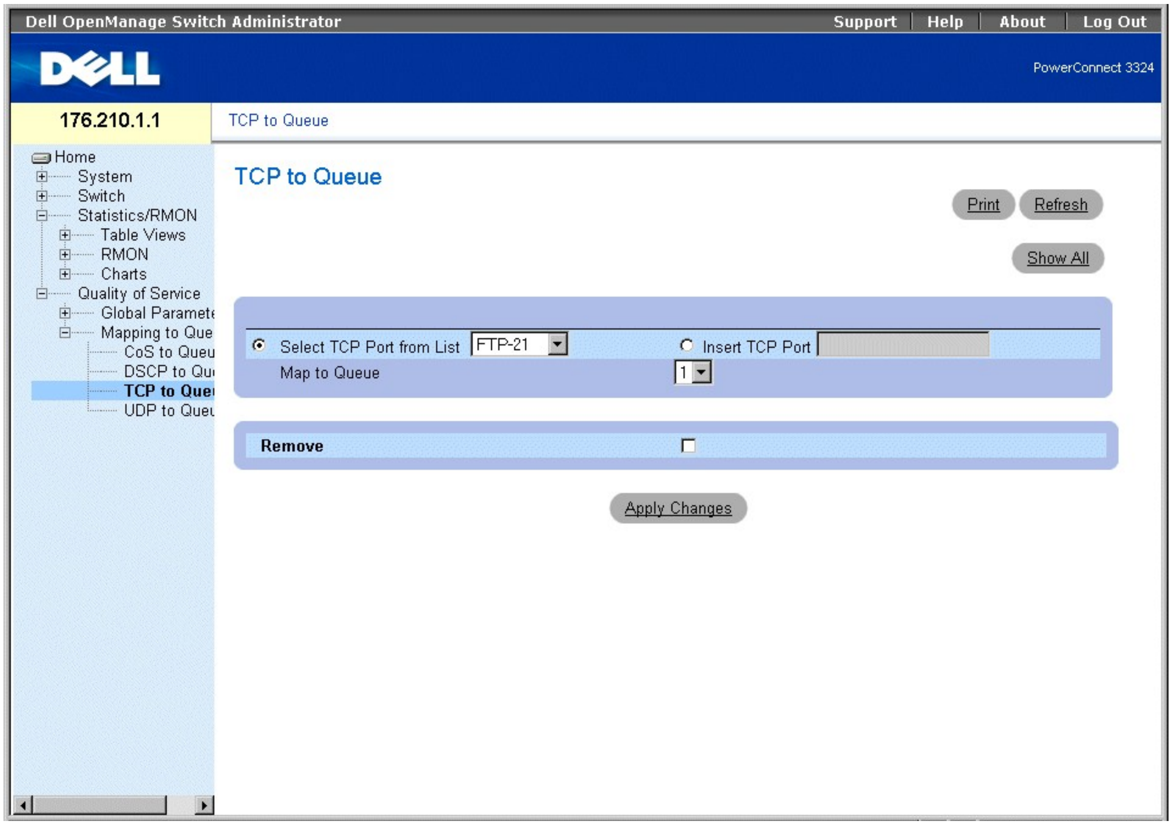
以下是 CLI 命令实例：

```
Console (config)# qos map dscp-queue 33 40 41 to 1
```

将 TCP 端口值映射到队列

"TCP to Queue"（TCP 至队列）页面页面使网络管理员可以将特定的 TCP 目的地端口通信分类到队列。 要打开 **"TCP to Queue"（TCP 至队列）**页面，请：

- 在树视图中选择 **"Quality of Service"（服务质量）>"Mapping to Queue"（映射到队列）>"TCP to Queue"（TCP 至队列）**。
  系统将打开 **"TCP to Queue"（TCP 至队列）**页面。



TCP 至队列页面

"TCP to Queue"（TCP 至队列）页面包含以下信息：

- **"Select TCP Port from List"（从列表中选择 TCP 端口）**— 提供了预定义的常用 TCP 端口的下拉列表。
- **"Insert TCP Port"（插入 TCP 端口）**— 允许定义新的 TCP 端口。
- **"Map to Queue"（映射到队列）**— 表示 TCP 端口将要分配到的通信队列。

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堆叠控制。

- **"Remove"（删除）**— 删除 TCP 端口映射。
  - **已选取** — 删除特定 TCP 端口映射。
  - **未选取** — 保留 TCP 端口映射。

将 TCP 端口分配至通信队列：

1. 打开**"TCP to Queue"（TCP 至队列）**页面。
2. 在**"TCP Port List"（TCP 端口列表）**中选择一个端口。

   或

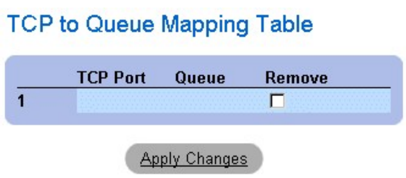
   选取**"Insert TCP Port"（插入 TCP 端口）**复选框。 将启用**"New TCP Port"（新 TCP 端口）**字段。 定义新的 TCP 端口。
3. 在**"Map to Queue"（映射到队列）**下拉列表中选择一个队列号。
4. 单击**"Apply Changes"（应用更改）**。 TCP 端口将被分配一个传输队列。

修改 TCP 端口至通信队列设置：

1. 打开**“TCP to Queue”（TCP 至队列）**页面。
2. 在**“TCP Port List”（TCP 端口列表）**下拉列表中选择一个端口。 为端口分配的队列将显示在**“Map to Queue”（映射到队列）**下拉列表中。
3. 在**“Map to Queue”（映射到队列）**下拉列表中选择新的通信队列。
4. 单击**“Apply Changes”（应用更改）**。 TCP 端口将被重新分配至不同的通信队列。

显示 TCP 至队列映射表：

1. 打开**“TCP to Queue”（TCP 至队列）**页面。
2. 单击**“Show All”（全部显示）**。 The 系统将打开**“TCP to Queue Mapping Table”（TCP 至队列映射表）**。



TCP 至队列映射表

从**“TCP to Queue Mapping Table”（TCP 至队列映射表）**中删除 TCP 端口映射：

1. 打开**“TCP to Queue”（TCP 至队列）**页面。
2. 单击**“Show All”（全部显示）**。 系统将打开**“TCP to Queue Mapping Table”（TCP 至队列映射表）**。
3. 在**“TCP Port List”（TCP 端口列表）**下拉列表中选择一个端口。 为端口分配的队列将显示在**“Map to Queue”（映射到队列）**下拉列表中。
4. 选取**“Remove”（删除）**复选框。
5. 单击**“Apply Changes”（应用更改）**。 系统将从通信队列中删除 TCP 端口。

使用 CLI 命令将 TCP 端口分配至队列

下表概括了用于配置**“TCP to Queue”（TCP 至队列）**页面中字段的等效 CLI 命令。

CLI 命令	**说明**
qos map tcp-port-queue 端口 1.端口 8 to 队列 ID	修改 TCP 端口至队列设置。
show qos map tcp-port-queue	显示 TCP 端口至队列设置。
no qos map tcp-port-queue	从队列中删除 TCP 端口。

以下是 CLI 命令实例：

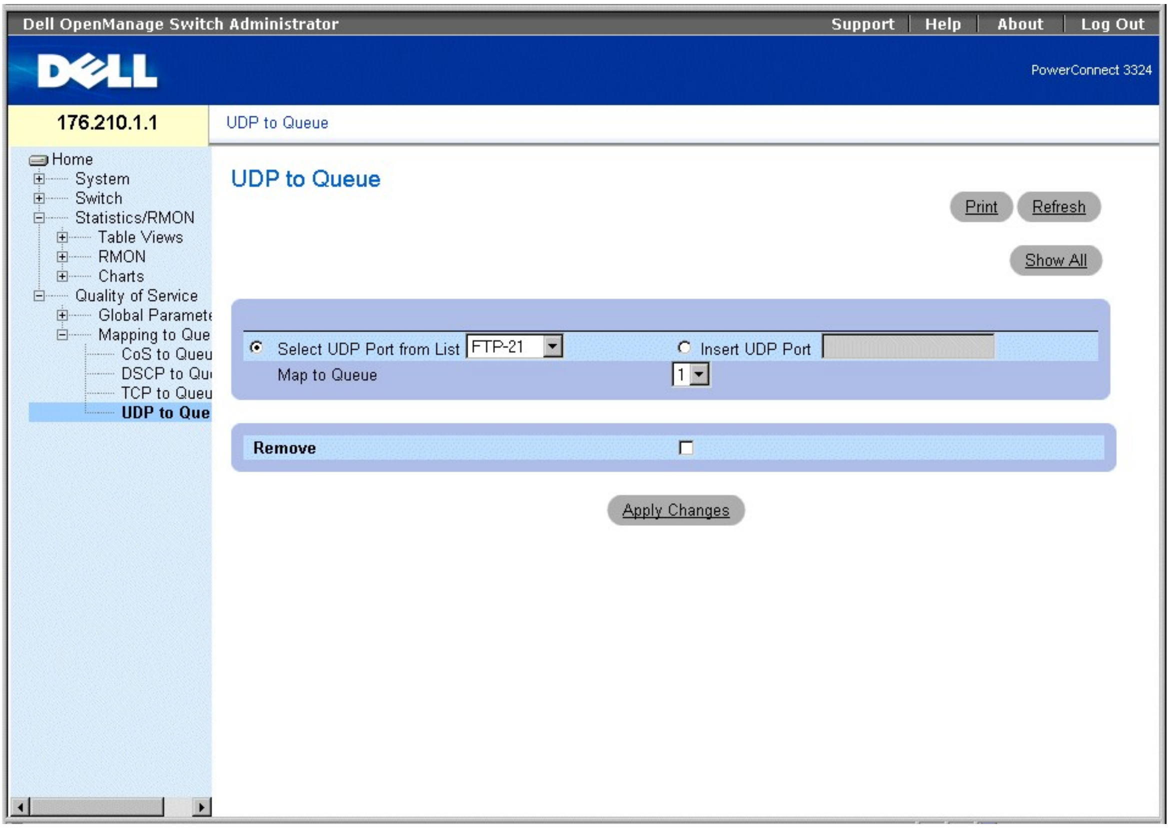
```
Console (config)# qos map tcp-port-queue 6001 to 2
```

```
Console (config)# exit

Console # exit

Console (config)# show qos map tcp-port-queue

Tcp port-queue map:

Port queue

----- ------

6000 1

6001 2

6002 3
```

将 UDP 端口值映射到队列

“UDP to Queue”（UDP 至队列）页面使网络管理员可以将特定的 UDP 端口通信分类到队列。 要打开**“UDP to Queue”（UDP 至队列）**页面，请：

- 在树视图中选择**“Quality of Service”（服务质量）>“Mapping to Queue”（映射到队列）>“UDP to Queue”（UDP 至队列）**。 系统将打开**“UDP to Queue”（UDP 至队列）**页面。



UDP 至队列页面

“UDP to Queue”（UDP 至队列）页面包含以下信息：

- **“Select UDP from the List”（从列表中选择 UDP）** — 提供了预定义的常用 UDP 端口的下拉列表。
- **“Insert UDP Port”（插入 UDP 端口）** — 允许定义新的 UDP 端口。
- **“Map to Queue”（映射到队列）** — 表示 UDP 端口将要分配到的通信队列。

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堆叠控制。

- **“Remove”（删除）** — 删除 UDP 端口映射。
  - **已选取** — 删除 UDP 端口映射。
  - **未选取** — 保留 UDP 端口映射。

将 UDP 端口分配到通信队列：

1. 打开**“UDP to Queue”（UDP 至队列）**页面。
2. 在**“UDP Port List”（UDP 端口列表）**中选择一个端口。

   或

   选取**“Insert UDP Port”（插入 UDP 端口）**复选框。 将启用**“New UDP Port”（新 UDP 端口）**字段。

   定义新的 UDP 端口。
3. 在**“Map to Queue”（映射到队列）**下拉列表中选择一个队列号。
4. 单击**“Apply Changes”（应用更改）**。 UDP 端口将被分配一个传输队列。

修改 UDP 端口至通信队列设置：

1. 打开**“UDP to Queue”（UDP 至队列）**页面。
2. 在**“UDP Port List”（UDP 端口列表）**下拉列表中选择端口映射。 为端口分配的队列将显示在**“Map to Queue”（映射到队列）**下拉列表中。
3. 在**“Map to Queue”（映射到队列）**下拉列表中选择新的通信队列。
4. 单击**“Apply Changes”（应用更改）**。 UDP 映射将被重新分配至不同的通信队列。

从 UDP 至通信映射表中删除 UDP 端口映射：

1. 打开**“UDP to Queue”（UDP 至队列）**页面。
2. 在**“UDP Port List”（UDP 端口列表）**下拉列表中选择端口映射。 为端口分配的队列将显示在**“Map to Queue”（映射到队列）**下拉列表中。
3. 选取**“Remove”（删除）**复选框。
4. 单击**“Apply Changes”（应用更改）**。 系统将从 UDP 至通信映射表中删除 UDP 端口映射。

使用 CLI 命令将 UDP 端口分配至队列

下表概括了用于配置**“UDP to Queue”（UDP 至队列）**页面中字段的等效 CLI 命令。

CLI 命令	**说明**
qos map udp-port-queue 端口 1.端口 8 to 队列 ID	修改 UDP 端口至队列设置。
show qos map udp-port-queue	显示 UDP 端口至队列设置。
no qos map udp-port-queue	从队列中删除 UDP 端口。

以下是 CLI 命令实例：

```
Console (config)# qos map udp-port-queue 2000 80 to 2

Console (config)# show qos map udp-port-queue
```

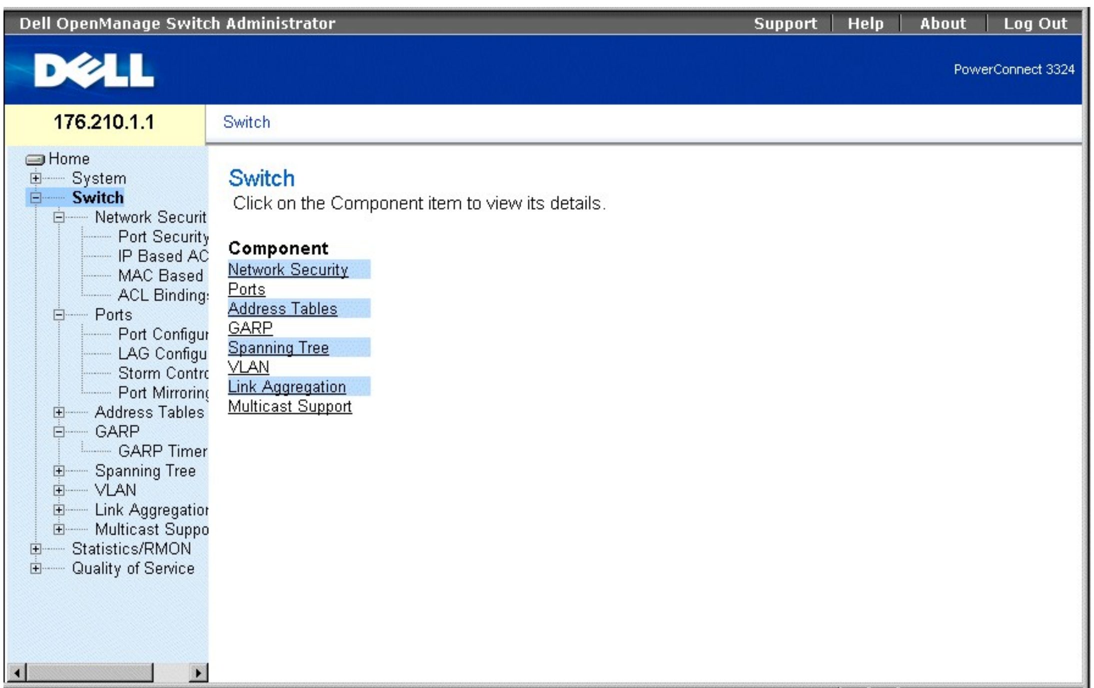
返回目录页面

[返回目录页面](#)

配置交换机信息

Dell™ PowerConnect™ 3324/3348 用户指南

本节提供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。



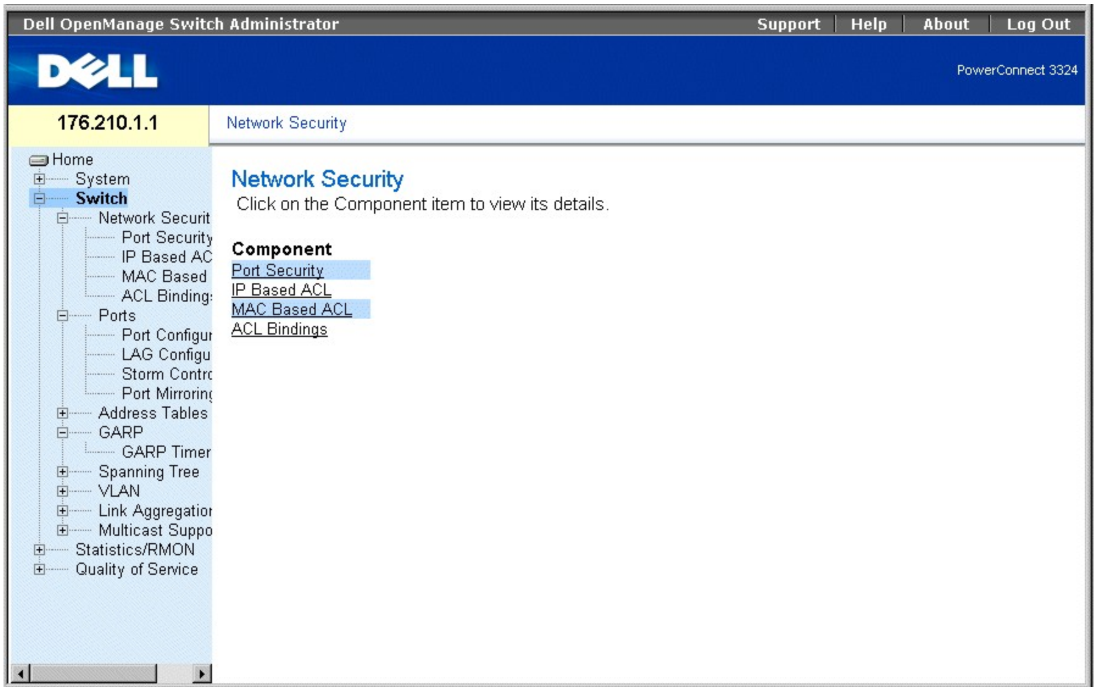
交换机页面

配置网络安全保护

Dell™ PowerConnect™ 3324/3348 使网络管理员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）**。 系统将打开 **"Network Security"（网络安全保护）**页面。



网络安全保护页面

"Network Security"（网络安全保护） 页面包含指向以下主题的链接：

- 网络安全保护概览
- 配置端口安全保护
- 定义基于 IP 的 ACL
- 定义基于 MAC 的 ACL
- 捆绑 ACL

网络安全保护概览

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是一个访问控制元素 (ACE)。 ACE 是确定通信分类的筛选器。 信息包需匹配以下 ACE：

- 协议
- 目的地端口
- 源 IP 地址
- 目的地 IP 地址
- 通配符掩码
- 匹配 DSCP
- 匹配 IP 优先级
- 源 MAC 地址
- 目的地 MAC 地址
- VLAN ID

例如，网络管理员可以定义以下 ACL 规则：端口号为 20 的端口可以接收 TCP 信息包；但是，如果接收到 UDP 信息包，则此信息包将被丢弃。

单个 ACL 可以包含多个 ACE。 ACL 中的 ACE 按照第一适用的方式进行应用。 从第一个 ACE 开始顺序处理 ACE。 当信息包与某个 ACE 分类相匹配时，将采取该 ACE 操作，ACL 进程将停止。 如果未找到匹配项，将执行默认操作将该信息包丢弃。 如果要处理几个 ACL，则仅在处理了所有 ACL 之后才应用默认操作。 默认丢弃操作会将所有允许的通信传输到交换机，包括 Telnet、HTTP 或 SNMP 等管理通信。

网络管理员可以定义两种类型的 ACL：

- IP ACL － 仅适用于 IP 信息包。 所有分类字段都与 IP 信息包有关。
- MAC 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。

进入具有活动 ACL 的入口端口的信息包将被：

- 传输。
- 丢弃并发送陷阱。
- 丢弃并发送陷阱，而且入口端口将被禁用。

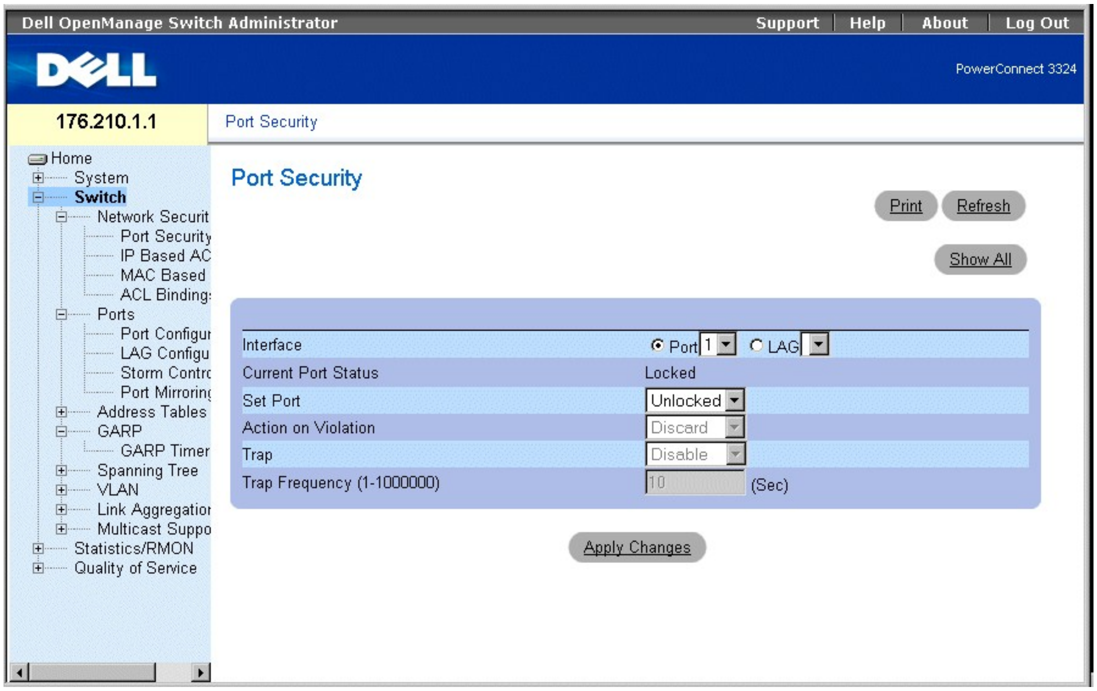
PowerConnect 3324/3348 最多支持 128 个 ACL。 PowerConnect 3324/3348 支持每个 FE 端口最多定义 248 个 ACE，每个 GE 端口最多定义 120 个 ACE。

配置端口安全保护

使用端口锁定可以将网络用户限制为仅能访问特定的端口或 LAG。 具有特定 MAC 地址的用户才可以使用锁定端口。 只能在静态 MAC 地址上启用锁定端口。 此外，通过锁定端口安全保护选项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。 可以动态学习或静态学习 MAC 地址。

到达锁定端口的信息包会被传输、丢弃，或被丢弃、发送陷阱，并禁用入口端口。 通过**“Port Parameters”（端口参数）**页面可以激活已禁用的端口。 请参阅“定义端口参数”。 要打开 **“Port Security”（端口安全保护）**页面，请：

- 选择**“Switch”（交换机）>“Network Security”（网络安全保护）>“Port Security”（端口安全保护）**。 系统将打开**“Port Security”（端口安全保护）**页面。



端口安全保护页面

"Port Security"（端口安全保护）页面包含以下字段：

- **"Interface"（接口）**— 表示要启用锁定端口的选定接口的类型。
  - **"Port"（端口）**— 表示选定的接口类型为端口。
  - **LAG** 表示选定的接口类型为堆叠成员。
- **"Current Port Status"（当前端口状态）**— 表示当前端口状态。
- **"Set Port"（设置端口）**— 表示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。 此为默认值。
  - **"Locked"（已锁定）**— 锁定端口。
- **"Action on Violation"（侵入措施）**— 表示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，不学习 MAC 地址。
  - **"Discard"（丢弃）**— 丢弃来自任何未学习其 MAC 地址的源的信息包。 此为默认值。
  - **"Shutdown"（关闭）**— 丢弃来自任何未学习其 MAC 地址的源的信息包，并锁定端口。 在激活端口或重启动设备之前，端口保持锁定状态。
- **"Trap"（陷阱）**— 允许发送陷阱。 可能的字段值包括：
  - **"Enable"（启用）**— 当锁定端口上接收到信息包时，允许发送陷阱。
  - **"Disable"（禁用）**— 当锁定端口上接收到信息包时，禁止发送陷阱。 此为默认值。
- **"Trap Frequency (1-1000000)"（陷阱频率 [1-1000000]）**— 表示两次陷阱之间的时间间隔（以秒为单位）。 此字段仅适用于锁定端口。 默认值为 10 秒。

要定义锁定端口，请：

1. 打开 **"Port Security"（端口安全保护）**页面。

2. 选择接口类型和编号。

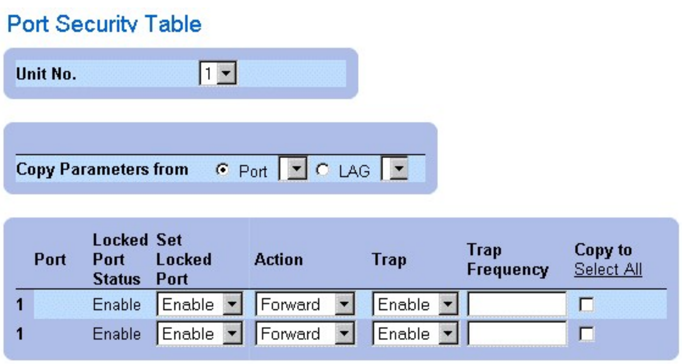
3. 定义 **“Set Port”（设置端口）**、 **“Action on Violation”（侵入措施）**和 **“Trap”（陷阱）**字段。

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。

要显示锁定端口表，请：

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）**页面。 **“Port Security Table”（端口安全保护表）**中的字段与 **“Port Security”（端口安全保护）**页面中的字段相同。 可以通过 **“Locked Ports Table”（锁定端口表）** 和 **“Port Security”（端口安全保护）**页面定义锁定端口。



端口安全保护表页面

除了 “端口安全保护页面” 中显示的字段外， **“Port Security Table”（端口安全保护表）**页面还包含以下字段：

- **“Unit No.”（装置号）**— 表示要显示端口安全保护信息的装置号。

使用 CLI 命令配置锁定端口的安全保护

下表概括了与“端口安全保护页面” 中显示的配置锁定端口安全保护的选项等效的 CLI 命令。

CLI 命令	说明
shutdown	禁用接口。
set interface active {ethernet 接口 **| port-channel** 端口通道号**}**	重新激活由于端口安全保护原因而关闭的接口。
port security<选项**>**陷阱频率	锁定在接口上学习新地址。
show ports security	显示端口锁定状态。

以下是 CLI 命令实例：

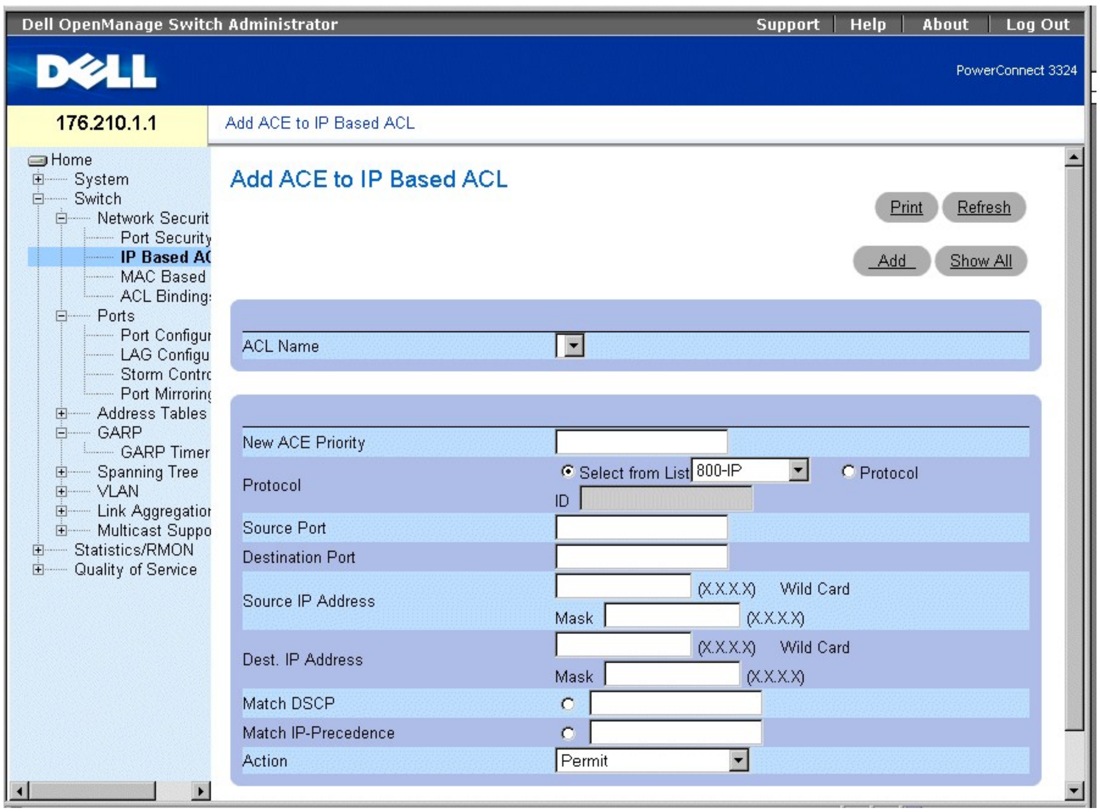
```
From 18.1.16 Console # show ports security

Port Action Trap Frequency Counter
```

```
---------------------------------------------

5/7 Discard Enable 100 88

7/8 Discard Disable
```

定义基于 IP 的 ACL

"Add ACE to IP Based ACL"（将 ACE 添加至基于 IP 的 ACL）页面使网络管理员可以定义基于 IP 的访问控制列表 (ACL) 和访问控制项 (ACE)。 ACE 用作筛选器以将信息包与传输条件进行匹配。 要打开**"Add ACE to IP Based ACL"（将 ACE 添加至基于 IP 的 ACL）**页面，请：

- 选择**"Switch"（交换机）>"Network Security"（网络安全保护）>"IP based ACL"（基于 IP 的 ACL）**。 系统将打开**"Add ACE to IP Based ACL"**
（将 ACE 添加至基于 IP 的 ACL）页面。



将 ACE 添加至基于 IP 的 ACL 页面

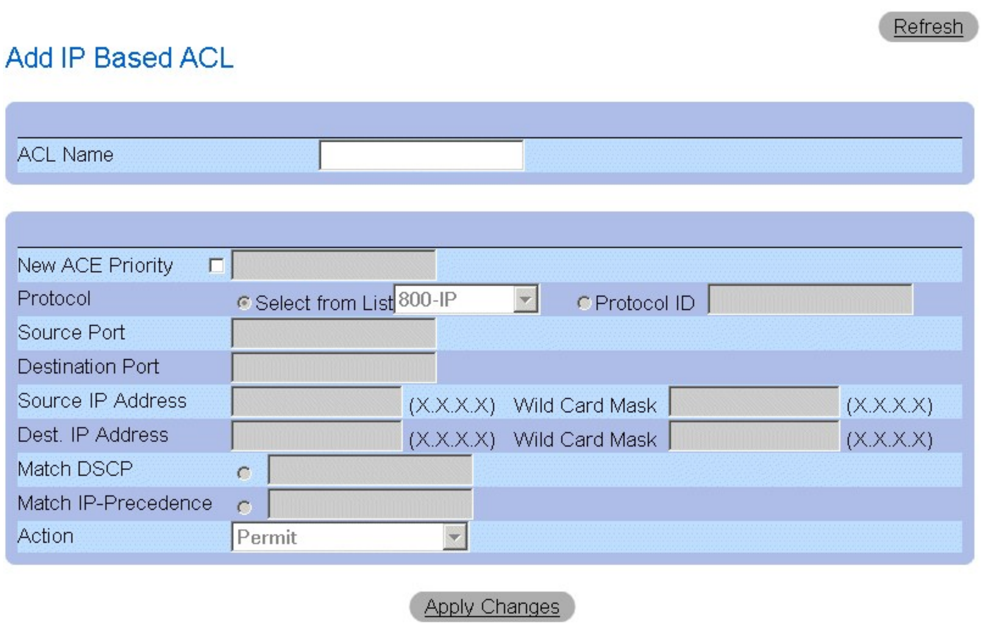
"Add ACE to IP Based ACL"（将 ACE 添加至基于 IP 的 ACL）页面包含以下字段：

- **"ACL Name"（ACL 名称）** — 包含用户定义的 ACL 的列表。
- **"New ACE Priority"（新 ACE 优先级）** — 定义 ACE 的优先级。 根据第一适用原则检查 ACE。 ACE 优先级定义了 ACL 列表中的 ACE 顺序。
- **"Protocol"（协议）** — 允许基于特定协议创建 ACE。

- **"Source Port"（源端口）** — 表示匹配信息包的源端口。 仅在协议列表中选定了 TCP 或 UDP 时，才启用此字段。
- **"Destination Port"（目的地端口）** — 表示匹配信息包的目的地端口。 仅在协议列表中选定了 TCP 或 UDP 时，才启用此字段。
- **"Source IP Address"（源 IP 地址）** — 将信息包定址到的源 IP 地址与 ACE 进行匹配。
- **"Wild Card Mask"（通配符掩码）** — 表示源 IP 地址的通配符掩码。 通配符用于屏蔽所有或部分源 IP 地址。 通配符掩码将指定要使用的位以及要忽略的位。 通配符掩码 255.255.255.255 表示所有位都不重要。 通配符 00.00.00.00 表示所有位都重要。 例如，如果源 IP 地址为 149.36.184.198，通配符掩码为 255.36.184.00，则表示忽略 IP 地址的前两位，使用最后两位。
- **"Dest. IP Address"（目的地 IP 地址）** — 将信息包定址到的目的地 IP 地址与 ACE 进行匹配。
- **"Wild Card Mask"（通配符掩码）** — 表示目的地 IP 地址的通配符掩码。 通配符用于屏蔽所有或部分目的地 IP 地址。 通配符掩码将指定要使用的位以及要忽略的位。 通配符掩码 255.255.255.255 表示所有位都不重要。 通配符 00.00.00.00 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。
- **"Match DSCP"（匹配 DSCP）** — 将信息包 DSCP 值与 ACE 进行匹配。 将使用 DSCP 值或 IP 优先级值将信息包与 ACE 进行匹配。
- **"Match IP-Precedence"（匹配 IP 优先级）** — 将信息包 IP 优先级值与 ACE 进行匹配。 将使用 DSCP 值或 IP 优先级值将信息包与 ACE 进行匹配。
- **"Action"（操作）** — 表示 ACE 的传输操作。 可能的字段值包括：
  - **"Permit"（允许）** — 传输符合 ACE 条件的信息包。
  - **"Deny"（拒绝）** — 丢弃符合 ACE 条件的信息包。
  - **"Deny and Disable Port"（拒绝并禁用端口）** — 丢弃符合 ACE 条件的信息包，并禁用信息包定址到的端口。 通过端口配置可以重新激活端口；请参阅"定义端口参数"。

要添加基于 IP 的 ACL，请：

1. 打开 **"Add ACE to IP Based ACL"（将 ACE 添加至基于 IP 的 ACL）**页面。
2. 单击 **"Add"（添加）**。 系统将打开 **""（将 ACE 添加至基于 IP 的 ACL）**页面。



添加基于 IP 的 ACL 页面

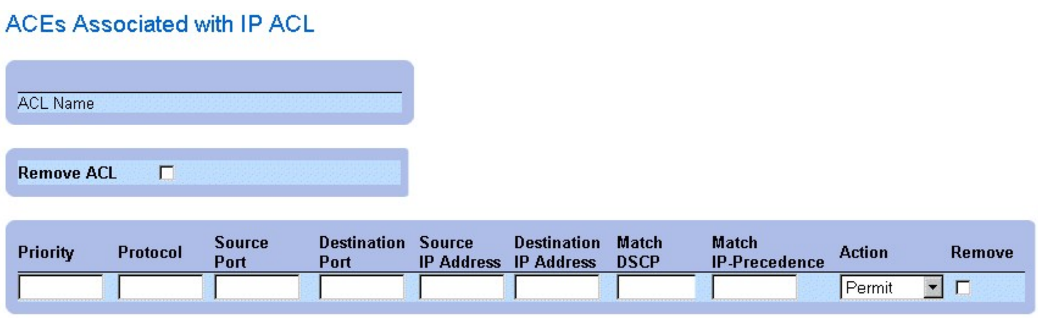
3. 定义 **"ACL Name"（ACL 名称）**、**"New Ace Priority"（新 Ace 优先级）**、**"Protocol"（协议）**、**"Source Port"（源端口）**、**"Destination Port"（目的地端口）**、**"Source IP Address"（源 IP 地址）**、**"Destination IP Address"（目的地 IP 地址）**、**"Match DSCP"（匹配 DSCP）**或 **"Match IP Precedence"（匹配 IP 优先级）**以及 **"Action"（操作）**字段。
4. 单击 **"Apply Changes"（应用更改）**。 系统将定义基于 IP 的 ACL。 如果定义了新 ACE 优先级，它会被添加到新的 ACL。

要将 ACE 分配至基于 IP 的 ACL，请：

1. 打开**“Add ACE to IP Based ACL”（将 ACE 添加至基于 IP 的 ACL）**页面。
2. 在**“ACL Name”（ACL 名称）**下拉列表中选择一个 ACL。
3. 定义**“New ACE Priority”（新 ACE 优先级）**字段。
4. 定义**“ACE No.”（ACE 编号）**、**“Protocol”（协议）**、**“Source Port”（源端口）**、**“Destination Port”（目的地端口）**、**“Source IP Address”（源 IP 地址）**、**“Destination IP Address”（目的地 IP 地址）**、**“Match DSCP”（匹配 DSCP）**或**“Match IP Precedence”（匹配 IP 优先级）**和/或**“Action”（操作）**字段。
5. 单击**“Apply Changes”（应用更改）**。 ACE 将被分配至基于 IP 的 ACL。

要显示特定 ACL 的 ACE，请：

1. 打开**“Add ACE to IP Based ACL”（将 ACE 添加至基于 IP 的 ACL）**页面。
2. 单击**“Show All”（全部显示）**。 系统将打开**“ACEs Associated with IP-ACL”（与 IP-ACL 相关联的 ACE）**页面。



与 IP-ACL 相关联的 ACE

要修改基于 IP 的 ACE，请：

1. 打开**“Add ACE to IP Based ACL”（将 ACE 添加至基于 IP 的 ACL）**页面。
2. 单击“Show All”（全部显示）。系统将打开**“ACEs Associated with IP-ACL”（与 IP-ACL 相关联的 ACE）**页面。
3. 修改**“ACL Name”（ACL 名称）**、**“New Ace Priority”（新 Ace 优先级）**、**“Protocol”（协议）**、**“Source Port”（源端口）**、**“Destination Port”（目的地端口）****'Source IP Address”（源 IP 地址）**、**“Destination IP Address”（目的地 IP 地址）**、**“Match DSCP”（匹配 DSCP）**或**“Match IP Precedence”（匹配 IP 优先级）**以及**“Action”（操作）**字段。
4. 单击**“Apply Changes”（应用更改）**。 系统将修改基于 IP 的 ACE，并更新设备。

要删除 ACL，请：

1. 打开**“Add ACE to IP Based ACL”（将 ACE 添加至基于 IP 的 ACL）**页面。
2. 单击**“Show All”（全部显示）**。系统将打开**“ACEs Associated with IP-ACL”（与 IP-ACL 相关联的 ACE）**页面。
3. 选择一个 ACL。
4. 选取**“Remove ACL”（删除 ACL）**复选框。
5. 单击**“Apply Changes”（应用更改）**。 系统将删除基于 IP 的 ACL，并更新设备。

要删除 ACE，请：

1. 打开**“Add ACE to IP Based ACL”（将 ACE 添加至基于 IP 的 ACL）**页面。
2. 单击**“Show All”（全部显示）**。系统将打开**“ACEs Associated with IP-ACL”（与 IP-ACL 相关联的 ACE）**页面。
3. 选择一个 ACE。
4. 选取**“Remove”（删除）**复选框。
5. 单击**“Apply Changes”（应用更改）**。 系统将删除基于 IP 的 ACE，并更新设备。

使用 CLI 命令将基于 IP 的 ACE 分配至 ACL

下表概括了与**“Add ACE to IP Based ACL”（将 ACE 添加至基于 IP 的 ACL）**页面中显示的将基于 IP 的 ACE 分配至 ACL 的选项等效的 CLI 命令。

CLI 命令	说明
ip access-list 名称	进入 IP 访问列表配置模式。
permit {any | 协议**} {any | {**源 源通配符**}} {any | {**目的地 目的地通配符**}} [dscp** DSCP 号 **| ip-precedence** IP 优先级**]**	如果与 permit 语句中定义的条件相匹配，则允许通信。
deny [disable-port] {any| 协议**} {any | {**源 源通配符**}} {any | {**目的地 目的地通配符**}} [dscp** DSCP 号**| ip-precedence** IP 优先级**]**	如果与 deny 语句中定义的条件相匹配，则拒绝通信。

以下是 CLI 命令实例：

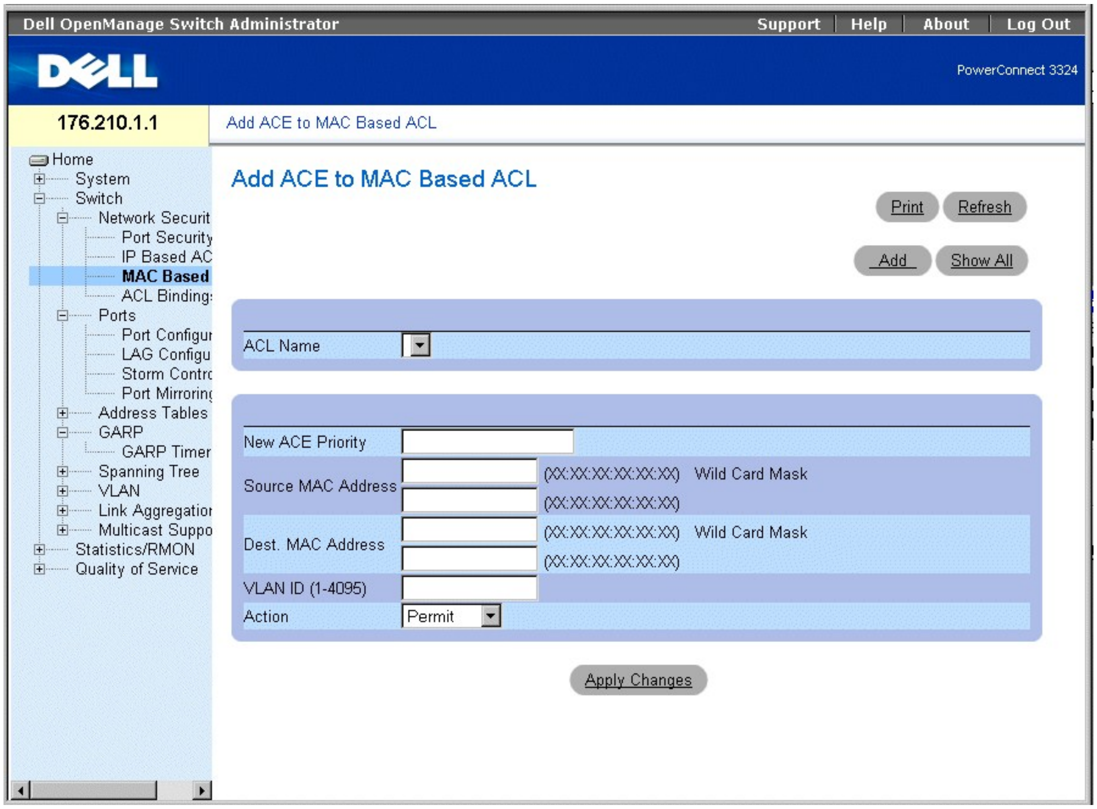
```
Permit 00:00:bo:11:11:11 0:0:0:0:0:0 any VLAN 4
```

```
deny 00:00:bo:11:11:11 0:0:0:0:0:0 any VLAN 4
```

定义基于 MAC 的 ACL

“Add ACE to MAC Based ACL”（将 ACE 添加至基于 MAC 的 ACL）页面使网络管理员可以定义基于 MAC 的**访问控制项** (ACE) 和**访问控制列表**(ACL)。 ACE 用作筛选器以将信息包与传输条件进行匹配。 要打开**“Add ACE to MAC Based ACL”（将 ACE 添加至基于 MAC 的 ACL）**，请：

- 选择**“Switch”（交换机）>“Network Security”（网络安全保护）>“MAC based ACL”（基于 MAC 的 ACL）**。 系统将打开**“Add ACE to MAC Based ACL”（将 ACE 添加至基于 MAC 的 ACL）**页面。



将 ACE 添加至基于 MAC 的 ACL 页面

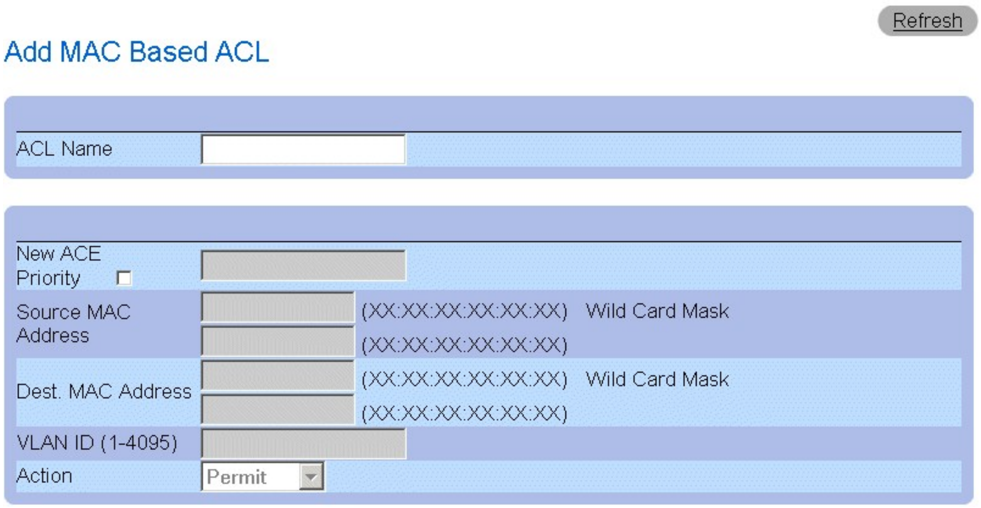
"Add ACE to MAC Based ACL"（将 ACE 添加至基于 MAC 的 ACL）页面包含以下字段：

- **"ACL Name"（ACL 名称）** — 包含用户定义的 ACL 的列表。
- **"New ACE Priority"（新 ACE 优先级）** — 允许创建新的 ACE，并表明 ACE 的优先级。
- **"Source MAC Address"（源 MAC 地址）** — 将信息包定址到的源 MAC 地址与 ACE 进行匹配。
- **"Wild Card Mask"（通配符掩码）** — 表示源 MAC 地址的通配符掩码。 通配符用于屏蔽所有或部分源 MAC 地址。 通配符掩码将指定要使用的位以及要忽略的位。 通配符掩码 FF:FF:FF:FF:FF:FF 表示所有位都不重要。 通配符 00.00.00.00.00.00.00 表示所有位都重要。 例如，如果源 MAC 地址为 E0:3B:4A:C2:CA:E2，通配符掩码为 00:3B:4A:C2:CA:FF，则表示使用 MAC 的前两位，忽略最后两位。
- **"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。
- **"Wild Card Mask"（通配符掩码）** — 表示目的地 MAC 地址的通配符掩码。 通配符用于屏蔽所有或部分目的地 MAC 地址。 通配符掩码将指定要使用的位以及要忽略的位。 通配符掩码 FF:FF:FF:FF:FF:FF 表示所有位都不重要。 通配符掩码 00.00.00.00.00.00 表示所有位都重要。 例如，如果目的地 MAC 地址为 E0:3B:4A:C2:CA:E2，通配符掩码为 00:3B:4A:C2:CA:FF，则表示使用 MAC 的前两位，忽略最后两位。
- **VLAN ID**— 将信息包的 VLAN ID 与 ACE 进行匹配。
- **"Action"（操作）** — 表示 ACE 的传输操作。 可能的字段值包括：
  - **"Permit"（允许）** — 传输符合 ACE 条件的信息包。
  - **"Deny"（拒绝）** — 丢弃符合 ACE 条件的信息包。
  - **"Shutdown"（关闭）** — 丢弃符合 ACE 条件的信息包，并禁用信息包定址到的端口。 通过端口配置可以重新激活端口，请参阅"定义端口参数"。

要添加基于 MAC 的 ACL，请：

1. 打开**"Add ACE to MAC Based ACL"（将 ACE 添加至基于 MAC 的 ACL）**页面。

2. 单击**“Add”（添加）**。 系统将打开**“Add MAC Based ACL”（添加基于 MAC 的 ACL）**页面。



与基于 MAC 的 ACL 相关联的 ACE

3. 定义**“ACL Name”（ACL 名称）**、**“Source Address”（源地址）**、**“Destination Address”（目的地地址）**和**“Action”（操作）**字段。

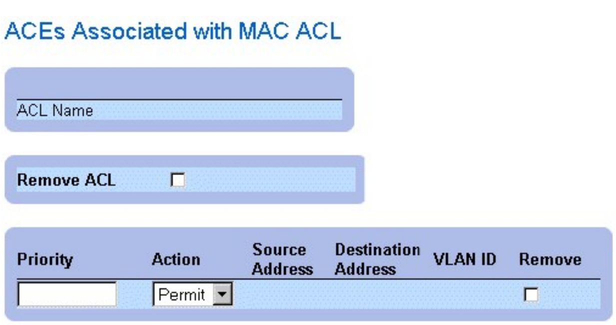
4. 单击**“Apply Changes”（应用更改）**。 系统将定义基于 MAC 的 ACL，并更新设备。

要将 ACE 分配至基于 MAC 的 ACL，请：

1. 打开**“Add ACE to MAC Based ACL”（将 ACE 添加至基于 MAC 的 ACL）**页面。
2. 在**“ACL Name”（ACL 名称）**下拉列表中选择一个 ACL。
3. 定义**“New ACE Priority”（新 ACE 优先级）**字段。
4. 定义**“ACL Name”（ACL 名称）**、**“VLAN ID”**、**“Source Address”（源地址）**、**“Destination Address”（目的地地址）**和**“Action”（操作）**字段。
5. 单击**“Apply Changes”（应用更改）**。 ACE 将被分配至基于 MAC 的 ACL。

要显示特定 ACL 的 ACE，请：

1. 打开**“Add ACE to MAC Based ACL”（将 ACE 添加至基于 MAC 的 ACL）**页面。
2. 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。



与 MAC ACL 相关联的 ACE

要修改基于 MAC 的 ACE，请：

1. 打开**“Add ACE to MAC Based ACL”（将 ACE 添加至基于 MAC 的 ACL**）页面。
2. 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。
3. 修改**“ACL Name”（ACL 名称）**、**“Source Address”（源地址）**、**“Destination Address”（目的地地址）**和**“Action”（操作）**字段。
4. 单击**“Apply Changes”（应用更改）**。 系统将修改基于 MAC 的 ACE，并更新设备。

要删除 ACL，请：

1. 打开**“Add ACE to MAC Based ACL”（将 ACE 添加至基于 MAC 的 ACL**）页面。
2. 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。
3. 选择一个 ACL。
4. 选取**“Remove ACL”（删除 ACL**）复选框。
5. 单击**“Apply Changes”（应用更改）**。 系统将删除基于 MAC 的 ACL，并更新设备。

要删除 ACE，请：

1. 打开**“Add ACE to MAC Based ACL”（将 ACE 添加至基于 MAC 的 ACL**）页面。
2. 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。
3. 选择一个 ACE。
4. 选取**“Remove”（删除）**复选框。
5. 单击**“Apply Changes”（应用更改）**。 系统将删除基于 MAC 的 ACE，并更新设备。

使用 CLI 命令将基于 MAC 的 ACE 分配至 ACL

以下是一个实例。 站点 A 已连接至端口 5，站点 B 已连接至端口 9。站点 A 的 MAC 地址为 00-0B-CD-35-6A-00（IP 地址：10.0.0.1 255.255.255.0）。 站点 B 的 MAC 地址为 00-06-6B-C7-A1-D8（IP 地址：10.0.0.2 255.255.255.0）。

要在端口 5 上实现将所有通信从站点 A 移至站点 B 的 MAC ACL，请输入以下 CLI 命令

```
permit source mac address destination mac address
```

```
permit 00-0B-CD-35-6A-00 0.0.0.0.0.0 00-06-6B-C7-A1-D8 0.0.0.0.0.0
```

所有与 ACL 相匹配的通信均将通过，而所有其它通信均将被拒绝。 （在 ACL 的末尾输入了不进行区分的附加命令 `deny all`。）

对于上述实例，站点 A 尝试将 ICMP ECHO 发送至站点 B。尽管 MAC ACL 允许发送 ICMP，但是操作失败。 问题在于站点 A 尝试将 ICMP ECHO 发送至站点 B，但是它在 ARP 表中没有条目。 通过 ARP 请求（即广播帧，具有站点 A 的源 MAC [00-0B-CD-35-6A-00] 和目的地广播 [FF.FF.FF.FF.FF.FF]），站点 A 尝试获取站点 B 的 MAC 地址。 此帧将被无提示丢弃，因为它与在端口 5 上设置的 MAC ACL 不匹配。

要解决此问题，用户必须输入允许使用广播帧的附加 `permit` 行：

```
permit 00-0B-CD-35-6A-00 0.0.0.0.0.0 FF.FF.FF.FF.FF.FF 0.0.0.0.0.0
```

注： 尽管用户希望能够在 MAC 地址 A 与 MAC 地址 B 之间进行通信，但是无法成功进行像 ICMP 这样的简单通信，因为未考虑附加广播。

下表概括了与 **"Add ACE to MAC Based ACL"（将 ACE 添加至基于 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。

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。
permit {any | {host 源 源通配符**} any | {**目的地 目的地通配符**}}[vlan** VLAN ID**]**	如果与 permit 语句中定义的条件相匹配，则允许通信。
deny [disable-port] {any | {源 源通配符**} any | {**目的地 目的地通配符**}}[vlan** VLAN ID**]**	如果与 permit 语句中定义的条件相匹配，则允许通信。

以下是 CLI 命令实例：

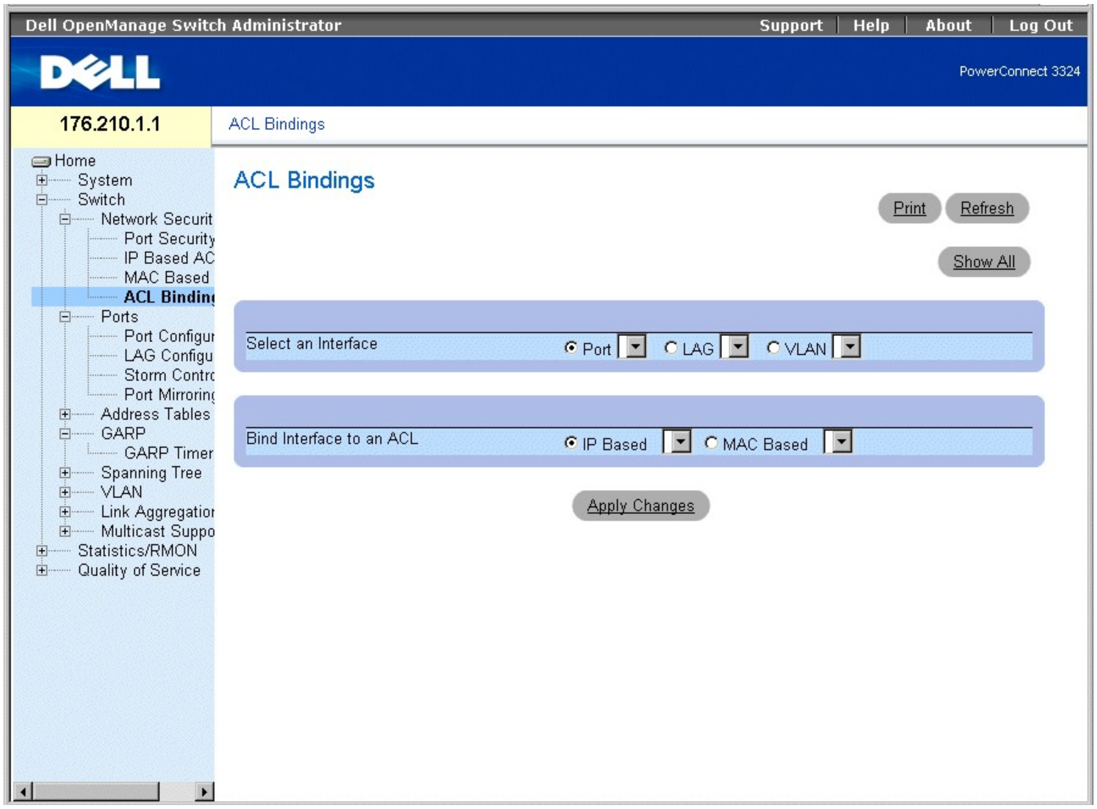
```
Console (config)# mac access-list dell

Console (config-mac-al)# permit 6.6.6.6.6.6 0.0.0.0.0.0 any vlan 4

Console (config-mac-al)# deny 6.6.6.6.6.6 0.0.255.255.255.255
```

捆绑 ACL

"ACL Bindings"（ACL 捆绑）页面使网络管理员可以将 ACL 列表分配至接口。 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 Bindings"（ACL 捆绑）**。 系统将打开 **"ACL Bindings"（ACL 捆绑）**页面。

注： ACL 只有连接至接口才起作用。



ACL 捆绑页面

"ACL Bindings"（ACL 捆绑）页面包含以下字段：

- **"Select an Interface"（选择接口）**— 表示 ACL 要连接的接口及接口类型。 可能的字段值包括：
  - **"Port"（端口）**— 表示 ACL 要连接的端口号。
  - **LAG**— 表示 ACL 要连接的 LAG。
  - **VLAN**— 表示 ACL 要连接的 VLAN。
- **"Bind Interface to ACL"（将接口捆绑至 ACL)**— 表示传入信息包要匹配的 ACL 名称。 信息包可以与基于 IP 的 ACL 或基于 MAC 地址的 ACL 进行匹配。 可能的字段值包括：
  - **"IP Based"（基于 IP）**— 表示将传入的信息包与基于 IP 的 ACL 进行匹配。
  - **"MAC Based"（基于 MAC）**— 表示将传入的信息包与基于 MAC 的 ACL 进行匹配。

要将 ACL 分配至接口，请：

1. 打开**"ACL Bindings"（ACL 捆绑）**页面。
2. 在**"Select ACL"（选择 ACL）**字段中选择 ACL 类型。
3. 在**"Attach ACL to an Interface"（将 ACL 连接至接口）**字段中定义 ACL 要连接的接口。
4. 单击**"Apply Changes"（应用更改）**。 ACL 将被连接至接口。

使用 CLI 命令分配 ACL 成员关系

下表概括了与**"ACL Bindings"（ACL 捆绑）**页面中显示的分配 ACL 成员关系选项等效的 CLI 命令。

CLI 命令	说明
class-map 分类映射名称 **[match-all | match-any]**	创建分类映射，并进入分类映射配置模式。
match access-group ACL 名称	定义分类通信的匹配条件。
show class-map [分类映射名称**]**	显示设备上配置的所有分类映射。

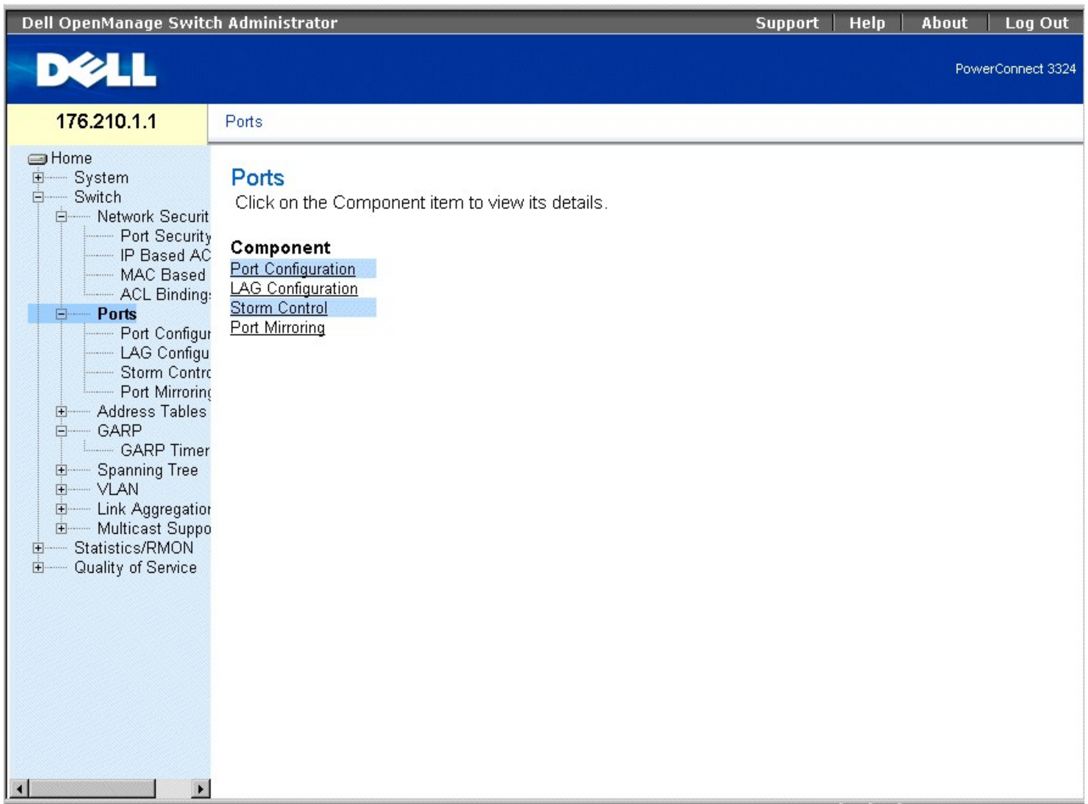
以下是 CLI 命令实例：

```
Console (config)# class-map class1 match-any

Console (config-cmap)# match access-group dell

Console (config-cmap)# exit

Console (config)# exit

Console # exit

Console> show class-map class1

Class Map match-any class1 (id4)
```

配置端口

本节提供了有关配置端口功能（包括风暴控制和端口镜像等高级功能）的解释和说明。 要打开 **“Ports”（端口）**页面，请：

- 选择 **“Switch”（交换机）>“Ports”（端口）**。 系统将打开 **“Ports”（端口）**页面。



端口页面

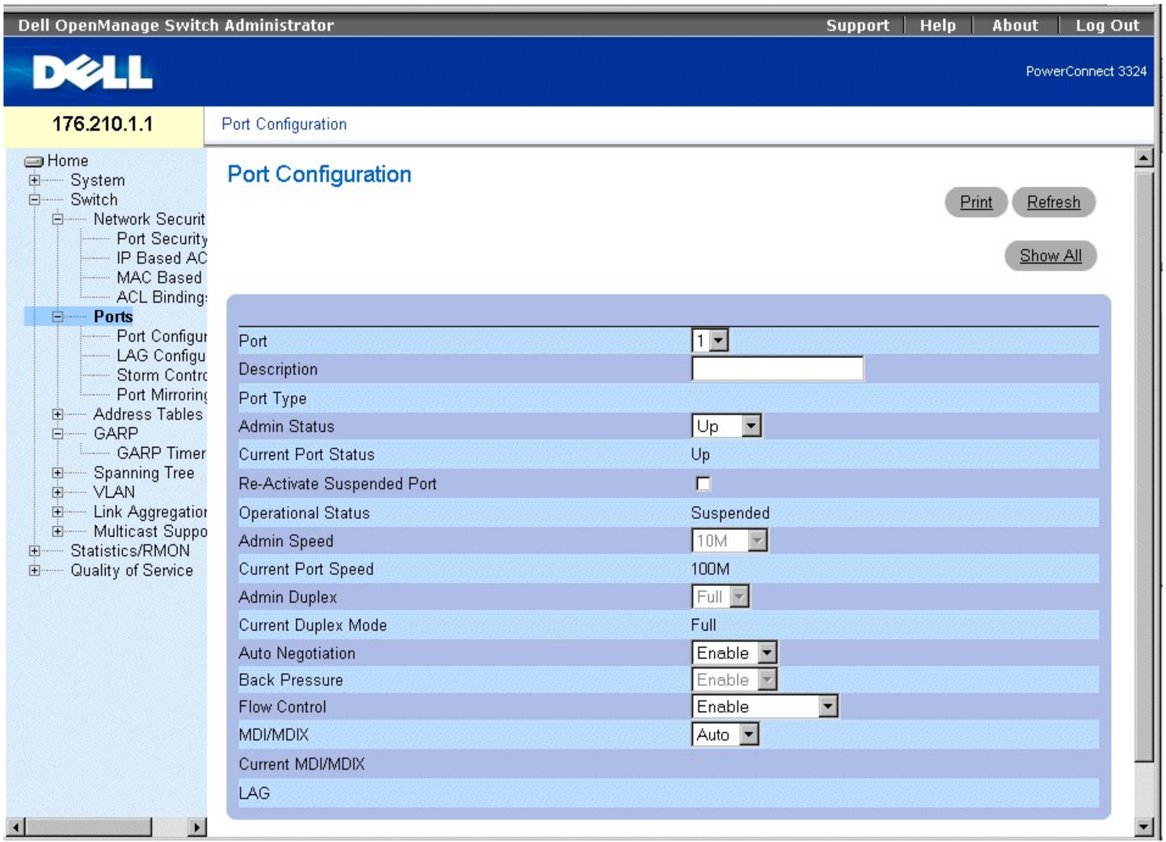
本节包括以下主题：

- 定义端口参数
- 定义 LAG 参数
- 启用风暴控制
- 定义端口镜像会话

定义端口参数

"Port Configuration"（端口配置）页面使网络管理员可以定义端口参数。 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）**。 系统将打开**"Port Configuration"（端口配置）**页面。



端口配置

"Port Configuration"（端口配置）页面包含以下字段：

- **"Port"（端口）** — 指定端口号。
- **"Description"（说明）** — 提供接口的简短说明，例如以太网。
- **"Port Type"（端口类型）** — 表示端口的类型。 可能的字段值包括：
  - "Ethernet"（以太网）
  - "Fast Ethernet"（快速以太网）
  - "GE"
- **"Admin Status"（管理状态）** — 控制选定端口的通信。 默认情况下，此参数设置为 **"Enable"（启用）**。 可能的字段值包括：
  - **"Up"（良好）** — 允许通过端口传输通信。
  - **"Down"（断开）** — 禁止通过端口传输通信。
- **"Current Port Status"（当前端口状态）** — 指定端口的运行状态。 可能的字段值包括：
  - **"Up"（良好）** — 表示端口当前正在运行。
  - **"Down"（断开）** — 表示端口当前未运行。
- **"Re-Activate Suspended Port"（重新激活暂挂的端口）** — 重新激活已通过 **"Locked Port"（锁定端口）**或 **"ACL"**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。
- **"Admin Speed"（管理速率）** — 指定端口运行的速率。 仅当端口被禁用时才能指定此值。 可能的字段值包括：
  - "10M"

- “100M”
- “1000M”

- **“Current Port Speed”（当前端口速率）**－ 指定同步端口的速率（以 bps 为单位）。 可能的字段值包括：
  - **“10M”**
  - **“100M”**
  - **“1000M”**
- **“Admin Duplex”（管理双工）**－ 指定同步端口的双工模式（以 bps 为单位）。 当“Admin Duplex”（管理双工）设置为全双工时，队列阻塞可以在选定端口上运行。 可能的字段值包括：
  - **“Full”（全）**－ 接口支持在设备和客户端之间同时进行双向传输。 此为默认值。
  - **“Half”（半）**－ 接口仅支持在设备和客户端之间进行单向传输。
- **“CurrentDuplex Mode”（当前双工模式）**－ 指定同步端口的双工模式。 可能的字段值包括：
  - **“Full”（全）**
  - **“Half”（半）**
- **“Auto Negotiation”（自动协商）**－ 在设备上启用自动协商。 自动协商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。 可能的字段值包括：
  - **“Enable”（启用）**－ 在端口上启用自动协商。
  - **“Disable”（禁用）**－ 在端口上禁用自动协商。 此为默认值。
  - **“Current Auto Negotiation”（当前自动协商）**－ 表示自动协商的运行状态。
- **“Back Pressure”（背压）**－ 在设备上启用背压模式。 背压模式与半双工模式一起使用可以禁止端口接收信息。 启用背压后，即使将队列阻塞设置为禁用，它也无法运行。
- 可能的字段值包括：
  - **“Enable”（启用）**－ 在端口上启用背压。
  - **“Disable”（禁用）**－ 在端口上禁用背压。 此为默认值。
  - **“Current Back Pressure”（当前背压）**－ 表示背压的运行状态。
- **“Flow Control”（流控制）**－ 表示是否在端口上启用流控制。 如果设备处于双工模式，将启用流控制。 此外，当流控制处于启用状态时，选定端口上将禁用队列。 启用流控制后，即使将队列阻塞设置为启用，它也无法运行。 可能的字段值包括：
  - **“Enable”（启用）**－ 表示在设备上启用流控制。
  - **“Disable”（禁用）**－ 表示在设备上禁用流控制。 此为默认值。
  - **“Current Flow Control”（当前流控制）**－ 表示流控制的运行状态。
  - **“Auto-negotiation”（自动协商）**－ 在端口上启用流控制的自动协商。
  - **“Tx Only”（仅 Tx）**－ 为出口端口启用自动协商。
  - **“Rx Only”（仅 Rx）**－ 为入口端口启用自动协商。
- **“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。 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。 标准的电缆布线包括：
  - 对于集线器和交换机，应使用带有绞接电缆的介质相关接口 (MDIX)
  - 对于终端站点，应使用介质相关接口 (MDI)

注： 禁用自动协商时，自动 MDIX 不能在 FE 端口上运行。

下表介绍了配置端口所需的参数组合设置。 这些设置可以确保保持配置功能。

	自动协商	
	已启用	已禁用

自动	合法	**非法**
MDI	合法	合法
MDIX	合法	合法

- **"Current MDI/MDIX"（当前 MDI/MDIX）**— 表示 MDIX 的运行状态。 可能的字段值包括：
  - **"MDI"**
  - **"MDIX"**
  - **"Auto"（自动）**— 表示自动设置值。
- **"LAG"**— 指定端口是否为 LAG 的一部分。

要定义端口参数，请：

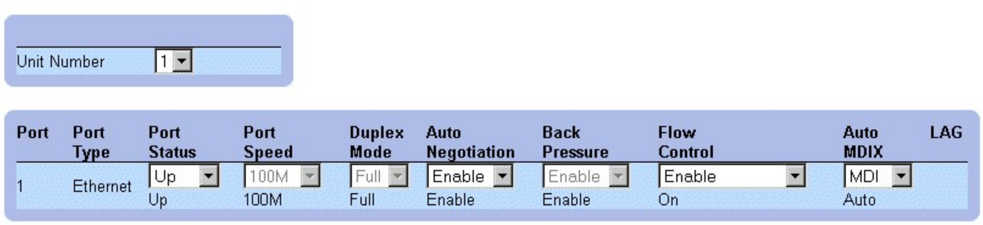
1. 打开**"Port Configuration"（端口配置）**页面。
2. 在**"Port"（端口）**字段中选择一个端口。
3. 定义**"Description"（说明）**、**"Admin Status"（管理状态）**、**"Admin Speed"（管理速率）**、**"Admin Duplex"（管理双工）**、**"Auto Negotiation"（自动协商）**、**"Back Pressure"（背压）**、**"Admin Auto MDIX"（管理自动 MDIX）**和/或**"Admin Flow Control"（管理流控制）**字段。
4. 单击**"Apply Changes"（应用更改）**。 端口参数将被保存至设备。

要修改端口参数，请：

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. 修改**"Description"（说明）**、**"Admin Status"（管理状态）**、**"Admin Speed"（管理速率）**、**"Admin Duplex"（管理双工）**、**"Auto Negotiation"（自动协商）**、**"Back Pressure"（背压）**、**"Admin Auto MDIX"（管理自动 MDIX）**和/或**"Admin Flow Control"（管理流控制）**字段。
4. 单击**"Apply Changes"（应用更改）**。 端口参数将被保存至设备。

要显示端口配置表，请：

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）**。



端口配置表

除了**"Port Configuration"（端口配置）**页面中的字段外，**P"Port Configuration Table"（端口配置表）**还显示以下字段：

- **"Unit Number"（装置号）**— 表示要显示端口信息的堆叠装置号。

使用 CLI 命令配置端口

以下实例说明了如何将端口设置为 MDIX 模式或 MDI 模式。 要将端口设置为 MDIX 模式，
请在系统提示符后输入以下信息：

```
console(config-if)# mdix on
```

系统将显示以下信息：

```
console # show inter config ethernet 1/e1

Flow Admin Back Mdix
Port Type Duplex Speed Neg Control State Pressure Mode

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

1/e1 100M-Copper Enabled Off Up Disabled On
```

要将端口设置为 MDI 模式，请在系统提示符后输入以下信息：

```
console(config)# inter eth 1/e1

console(config-if)# no mdix
```

系统将显示以下信息：

```
console # show inter config ethernet 1/e1

Flow Admin Back Mdix
Port Type Duplex Speed Neg Control State Pressure Mode

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

1/e1 100M-Copper Enabled Off Up Disabled Off
```

下表概括了与**“Port Configuration”（端口配置）**中显示的配置端口的选项等效的 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** 端口通道号**}**	重新激活由于安全保护原因而关闭的接口。
speed {10 | 100 | 1000}	配置在未使用自动协商时给定以太网接口的速率。
duplex {half | full}	配置在未使用自动协商时给定以太网接口的全/半双工操作。
negotiation	启用给定接口的速率和双工参数的自动协商操作。
back-pressure	在给定接口上启用背压。
flowcontrol {auto | on | off | rx | tx}	在给定接口上配置流控制。
mdix {on | auto}	在给定接口或端口通道上启用自动绞接。
show interfaces configuration [ethernet 接口 **| port-channel** 端口通道号**]**	显示所有已配置接口的配置。
show interfaces status [ethernet 接口 **| port-channel** 端口通道号**]**	显示所有已配置接口的状态。
show interfaces description [ethernet 接口 | port-channel 端口通道号**]**	显示所有已配置接口的说明。

以下是 CLI 命令实例：

```
Console (config)# interface ethernet 1/e5

Console (config-if)#

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)# exit

Console (config)# exit
```

Console# **show interfaces configuration**

```
Port Type Duplex Speed Neg Flow Back MDIX Admin

Cont Pres Mode State

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

1/e1 1g-combo-c Full 1000 Auto On Enable Auto Up

2/e1 100-copper Full 1000 Off Off Disable off Up

2/e2 1g-Fiber Full 1000 Off Off Disable on Up


Neg : Negotiation

Flow Cont: Flow Control

Back Pres: Back Pressure
```

Console# **show interfaces status**

```
Port Port Duplex Speed Neg Flow Back MDI Link

Cont Pres Mode State

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

2/e1 100-copper Full 1000 off Off Disable Off Down*


Legend

Neg : Negotiation

Flow Cont: Flow Control
```

```
Back Pres: Back Pressure

*: The interface was suspended by the system.

Router# show interfaces description


Port Description

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

1/e1 Port that should be used for management only

2/e1

2/e2


Port Channel Description

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

1 dell

2 projects
```

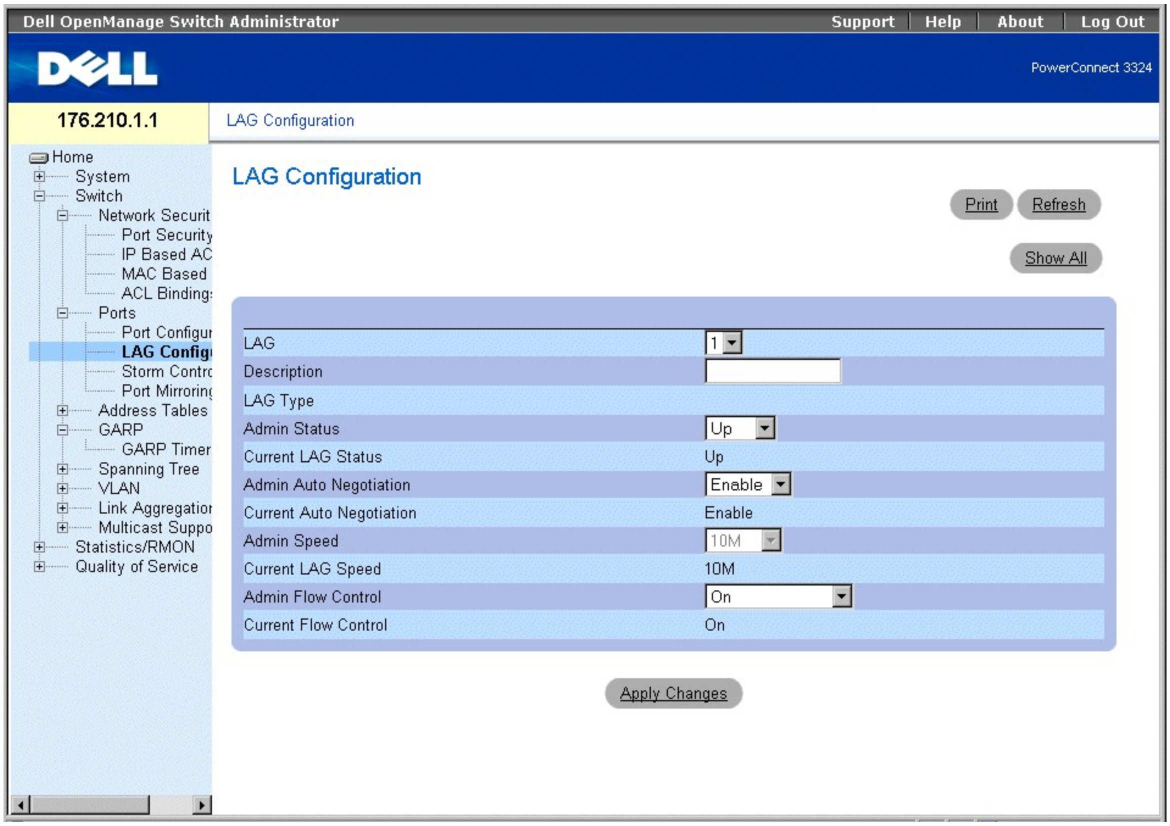
定义 LAG 参数

"LAG Configuration"（LAG 配置）页面使网络管理员可以为已配置的 LAG 配置参数。 PowerConnect 3324/3348 支持每个 LAG 最多 8 个端口，每个系统 6 个 LAG。 系统提供了 6 个永久性 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 **"LAG Configuration"（LAG 配置）**页面，请：

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。

- 在树视图中单击**"Switch"（交换机）>"Ports"（端口）>"LAG Configuration"（LAG 配置）**。 系统将显示**"LAG Configuration"（LAG 配置）**页面。



LAG 配置页面

"LAG Configuration"（LAG 配置）页面包含以下字段：

- **"LAG"**— 表示 LAG 号。
- **"Description"（说明）**— 提供用户定义的 LAG 说明。
- **"LAG Type"（LAG 类型）**— 表示 LAG 的最大速率容量。
- **"Admin Status"（管理状态）**— 控制来自选定 LAG 的通信。 默认情况下，此参数被设置为 **"Up"（良好）**。 可能的字段值包括：
  - **"Up"（良好）**— 允许通过 LAG 传输通信。
  - **"Down"（断开）**— 禁止通过 LAG 传输通信。
- **"Current LAG Status"（当前 LAG 状态）**— 指定 LAG 的状态。 可能的字段值包括：
  - **"Up"（良好）**— 表示 LAG 当前正在运行。
  - **"Down"（断开）**— 表示 LAG 当前未运行。
- **"AdminAuto Negotiation"（管理自动协商）**— 在 LAG 上启用自动协商。 自动协商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。 可能的字段值包括：
  - **"Enable"（启用）**— 在 LAG 上启用自动协商。
  - **"Disable"（禁用）**— 在 LAG 上禁用自动协商。
- **"Current Auto Negotiation"（当前自动协商）**— 表示当前的自动协商设置。 可能的字段值包括：
  - **"Enable"（启用）**
  - **"Disable"（禁用）**
- **"Admin Speed"（管理速率）**— 表示 LAG 运行的速率。 仅在禁用 LAG 时才可以输入此值。 可能的字段值包括：

- **"10M"**
- **"100M"**
- **"1000M"**

- **"Current LAG Speed"（当前 LAG 速率）**－ 指定同步 LAG 的速率（以 bps 为单位）。 可能的字段值包括：
  - **"10M"**
  - **"100M"**
  - **"1000M"**
- **"Current Duplex Mode"（当前双工模式）**－ 指定 LAG 的对话类型。 当前的字段值包括：
  - **"Full"（全）**－ 接口支持在设备和客户端之间同时进行双向传输。
  - **"Half"（半）**－ 接口仅支持在设备和客户端之间进行单向传输。
- **"Admin Current Duplex Mode"（管理当前双工模式）**－ 指定 LAG 的对话类型。 当前的字段值包括：
  - **"Full"（全）**－ 接口支持在设备和客户端之间同时进行双向传输。
  - **"Half"（半）**－ 接口仅支持在设备和客户端之间进行单向传输。
- **"Flow Control"（流控制）**－ 表示是否在 LAG 上启用流控制。 可能的值包括：
  - **"Off"（关）**－ 在 LAG 上禁用流控制。 此为默认值。
  - **"On"（开）**－ 在 LAG 上启用流控制。
  - **"Auto-negotiation"（自动协商）**－ 在 LAG 上启用流控制的自动协商。
- **"Current Flow Control"（当前流控制）**－ 表示当前流控制的设置。 可能的值包括：
  - **"Off"（关）**
  - **"On"（开）**
  - **"Auto-negotiation"（自动协商）**

要定义 LAG 参数，请：

1. 打开**"LAG Configuration"（LAG 配置）**页面。
2. 在**"LAG"**字段中选择一个 LAG。
3. 定义**"Description"（说明）**、**"Admin Status"（管理状态）**、**"Port Speed"（端口速率）**、**"Admin Auto Negotiation"（管理自动协商）**、**"Admin Speed"（管理速率）**和/或**"Admin Flow Control"（管理流控制）**字段。
4. 单击**"Apply Changes"（应用更改）**。 LAG 参数将被保存至设备。

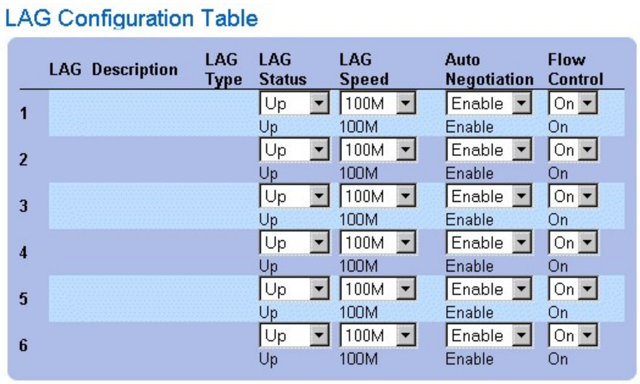
要修改 LAG 参数，请：

1. 打开**"LAG Configuration"（LAG 配置）**页面。
2. 在**"LAG"**字段中选择一个 LAG。
3. 修改**"Description"（说明）**、**"Admin Status"（管理状态）**、**"Port Speed"（端口速率）**、**"Admin Auto Negotiation"（管理自动协商）**、**"Admin Speed"（管理速率）**和/或**"Admin Flow Control"（管理流控制）**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**）。



LAG Configuration Table

LAG	Description	LAG Type	LAG Status	LAG Speed	Auto Negotiation	Flow Control
1			Up Up	100M 100M	Enable Enable	On On
2			Up Up	100M 100M	Enable Enable	On On
3			Up Up	100M 100M	Enable Enable	On On
4			Up Up	100M 100M	Enable Enable	On On
5			Up Up	100M 100M	Enable Enable	On On
6			Up Up	100M 100M	Enable Enable	On On

LAG 配置表

使用 CLI 命令配置 LAG

以下为如何将 LAG 设置为禁用自动协商、速率 100M、全双工的实例。

在系统提示符后，输入以下信息以设置静态链路聚合：

```
console> en

console# config

console(config)# interface port-channel 1

console(config-if)# no neg

console(config-if)# speed 100

console(config-if)# exit

console(config)# interface range ethernet 1/e23-24

console(config-if)# no mdix

console(config-if)# no neg

console(config-if)# speed 100
```

```
console(config-if)# duplex full

console(config-if)# channel-group 1 mode on

console(config-if)# end
```

系统将显示以下信息：

```
console# sh interfaces status port-channel 1

Flow Link Back
ch Type Duplex Speed Neg Control State Pressure

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

ch1 100M Full 100 Disabled Off Up Disabled
```

下表概括了与 **“LAG Configuration”**（**LAG 配置**）页面中显示的配置 LAG 的选项等效的 CLI 命令。

CLI 命令	说明
interface port-channel 端口通道号	创建端口通道，并进入端口通道配置模式。
channel-group 端口通道号 **mode {on | auto}**	使端口与端口通道相关联。
show interfaces port-channel [端口通道号**]**	显示端口通道信息（哪些端口是端口通道的成员，以及它们当前是否处于激活状态）。

以下是 CLI 命令实例：

```
Console (config)# interface ethernet 1/e5

Console (config-if)# channel-group 1 mode on

Console (config-if)# exit

Console (config-if)# exit

Console # show interfaces port-channel

Channel Port
```

```
------------ ----------------------------------

1 Active 1/e5, 2/e2 Inactive 3/e3

2 Active 1/e2

3 Inactive 3/e8
```

启用风暴控制

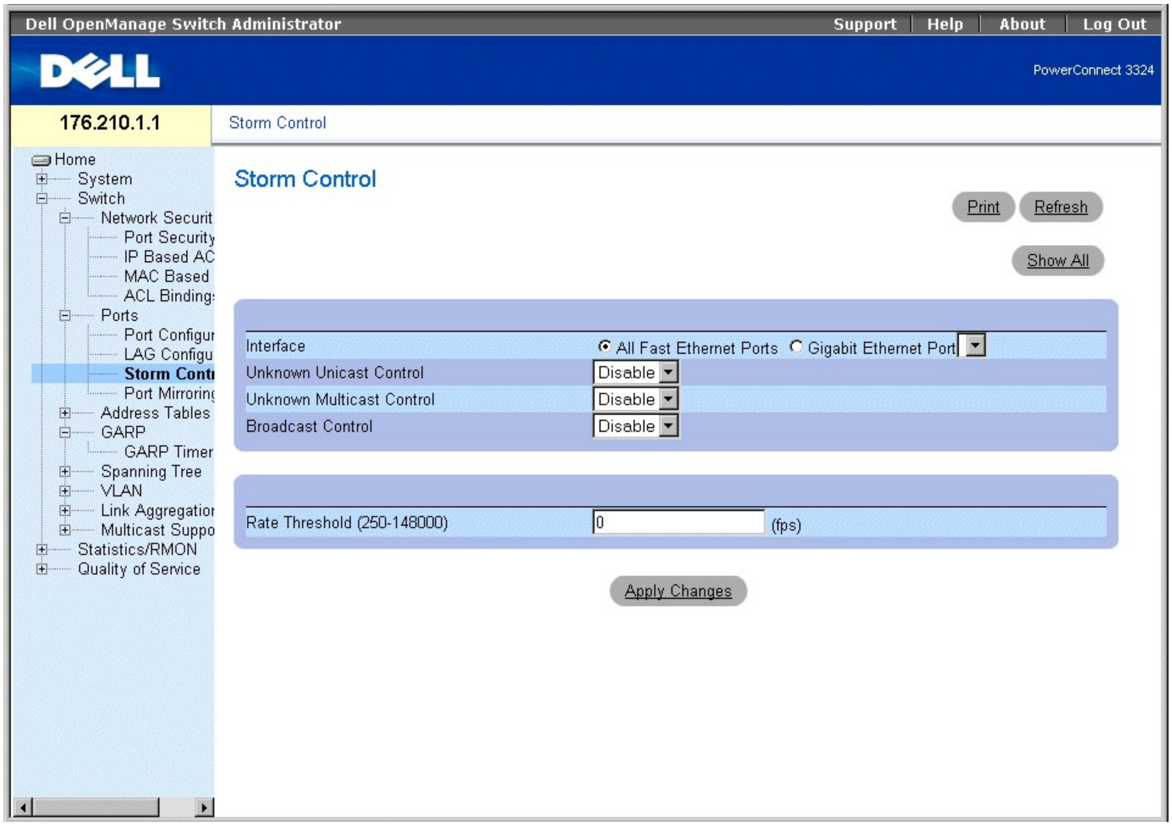
广播风暴是过多的广播信息同时通过单个端口在网络中传输的结果。 已传输信息的响应被载入网络，从而过多占用网络资源或导致网络超时。

通过定义信息包类型和信息包传输的速率，可以为所有高速以太网端口或吉位端口启用风暴控制。 也可以将端口分组，以便为整个组提供风暴保护。

系统在各个端口上分别测量传入的广播、多点传送和未知帧速率，并在速率超出用户定义的速率时丢弃帧。

"Storm Control"（风暴控制）页面使网络管理员可以启用和配置风暴控制。 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）**，打开**"Storm Control"（风暴控制）**页面。



风暴控制页面

"Storm Control"（风暴控制）页面包含以下字段：

- **"Interface"（接口）** — 表示要在其上配置风暴控制的接口。
  - **"All Fast Ethernet Ports"（所有高速以太网端口）** — 表示为所有 FE 端口启用风暴控制。 可以将风暴控制单独应用于 GE 端口。
  - **"Gigabit Ethernet Port"（吉位以太网端口）** — 表示为选定的吉位以太网端口启用风暴控制。 可以为所有 FE 端口启用或禁用风暴控制。
- **"Unknown Unicast Control"（未知单点传送控制）** — 允许调节设备上的未知单点传送信息包。 可能的字段值包括：
  - **"Enable"（启用）** — 允许调节设备上的未知单点传送信息包。
  - **"Disable"（禁用）** — 禁止调节设备上的未知单点传送信息包。
- **"Unknown Multicast Control"（未知多点传送控制）** — 允许调节设备上的未知多点传送信息包。 可能的字段值包括：
  - **"Enable"（启用）** — 允许调节设备上的未知多点传送信息包。
  - **"Disable"（禁用）** — 禁止调节设备上的未知多点传送信息包。
- **"Broadcast Control"（广播控制）** — 允许调节未知广播信息包。 可能的字段值包括：
  - **"Enable"（启用）** — 允许调节广播信息包。
  - **"Disable"（禁用）** — 禁止调节广播信息包。
- **"Rate Threshold (250-148000)"（速率阈值 250-148000）** — 设置风暴控制的广播信息包速率限制。 对于 FE 端口，范围为 250 至 148,000。对于 GE 端口，范围为 250 至 262,143 个信息包。 对于 FE 端口，默认值为 148000，对于 GE 端口，默认值为 262,143。

要在设备上启用风暴控制，请：

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 **“Unknown Unicast Control”（未知单点传送控制）**、**“Unknown Multicast Control”（未知多点传送控制）**、**“Broadcast Control”（广播控制）**和
“Rate Threshold (250-148000)”（速率阈值 50-148000]）字段。

4. 单击 **“Apply Changes”（应用更改）**。 系统将在设备上启用风暴控制。

要修改风暴控制端口参数，请：

1. 打开 **“Storm Control”（风暴控制）**页面。

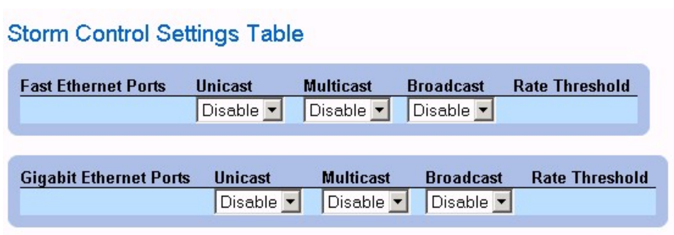
2. 修改 **“Unknown Unicast Control”（未知单点传送控制）**、**“Unknown Multicast Control”（未知多点传送控制）**、**“Broadcast Control”（广播控制）**和
“Rate Threshold (250-148000)”（速率阈值 50-148000]）字段。

3. 单击 **“Apply Changes”（应用更改）**。 风暴控制端口参数将被保存至设备。

要显示端口参数表，请：

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）**。



风暴控制设置表

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。

CLI 命令	**说明**
port storm-control enable {unknown | broadcast | multicast} {fastethernet | gigaethernet 接口**}**	为单点传送、多点传送和广播信息包启用广播风暴控制。
port storm-control rate gigaethernet 接口速率	配置最大广播速率。
show ports storm-control	显示风暴控制配置。

以下是 CLI 命令实例：

```
Console(config)# port storm-control rate fastethernet 300
```

```
Console(config)# port storm-control enable fastethernet
```

```
Console# show ports storm-control

Port Unknown Broadcast Multicast Rate

[Packets/sec]

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

Gigaethernet 1 Enabled Disabled Enabled 2000

Gigaethernet 2 Enabled Enabled Enabled 2000

FastEthernet Enabled Enabled Enabled 1000
```

定义端口镜像会话

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。 可以将端口镜像用作诊断工具和/或调试功能。 端口镜像还可以监测交换机性能。

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，网络管理员即可配置端口镜像。 在配置端口镜像之前，请注意以下几点：

- 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。
- PowerConnect 3348 可以在同一装置中的 1 至 24 端口与 25 至 48 端口之间进行镜像。 也可以在 25 至 48 端口与其它 PowerConnect 3348 的 25 至 48 端口（或任意 PowerConnect 3324 的端口）之间进行镜像。
- 只要源端口不是 G2 端口，PowerConnect 3348 可以镜像至任意 PowerConnect 3324 装置。 只要端口是 PowerConnect 25 至 48 端口中的端口，PowerConnect 3348 就可以与其它 PowerConnect 3348 装置进行镜像。

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。
- 从目的地端口传输的所有信息包均被标记。

以下限制适用于已被配置为源端口的端口：

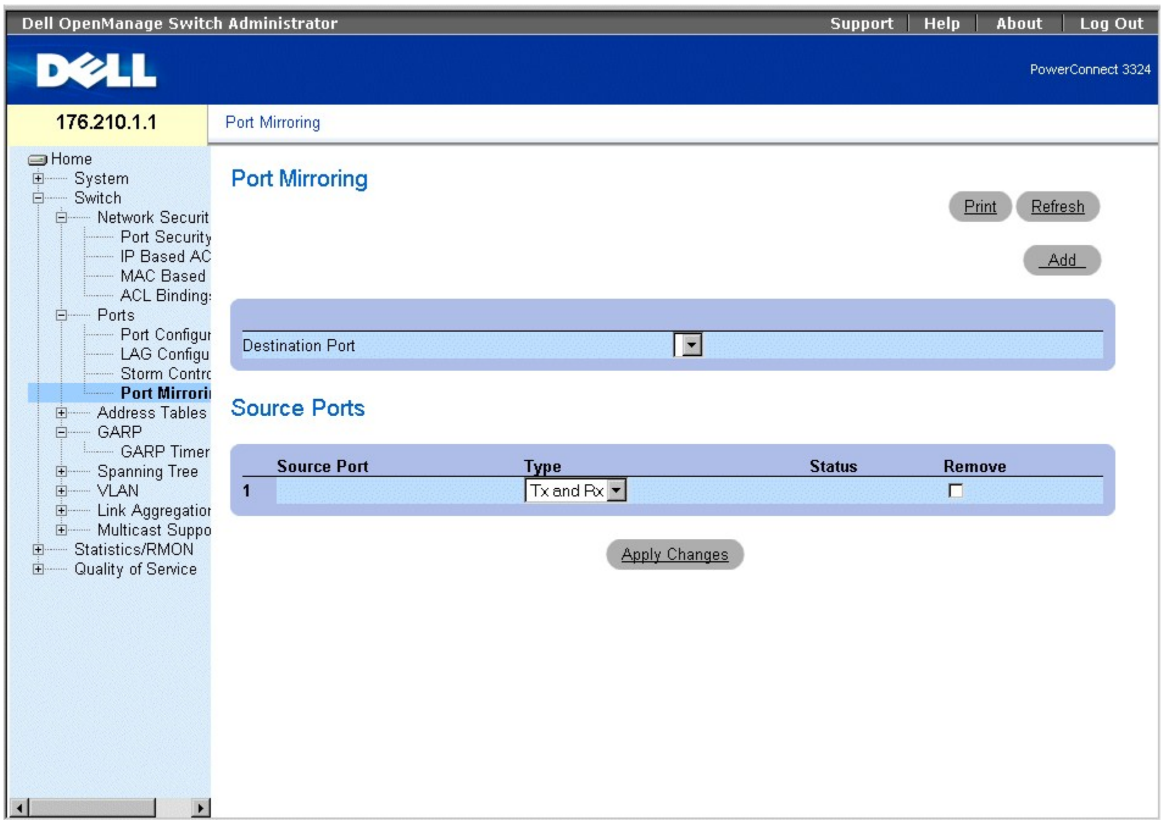
- 如果在源端口上接收到的信息包未被标记，则在该信息包被发送至端口镜像目的地端口时，将被标以源端口的默认 PVID。

所有 RX/TX 信息包应在同一端口进行监测。

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）**。 系统将打开**“Port Mirroring”（端口镜像）**页面。

注： 将某一端口设置为端口镜像会话的目标端口时，此端口上的所有常规操作均将被暂挂。 这些操作包括生成树和 LACP。



端口镜像页面

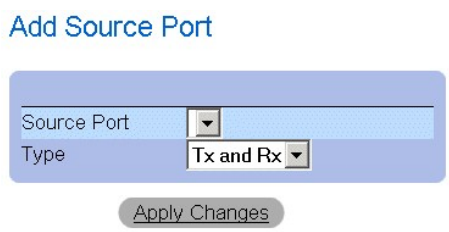
- **“Destination Port”（目的地端口）**— 定义端口通信要镜像到的端口号。 副本端口不能进行自我镜像，不能成为源端口 VLAN 以外的 VLAN 成员，并且不能使用 IP 接口进行配置。 源端口上的所有通信均将被标记。
- **“Source Port”（源端口）**— 定义要复制其端口通信的端口号。 最多可以将 8 个端口镜像至一个镜像端口。
- **“Type”（类型）**— 指定要镜像的端口通信类型。 可能的字段值包括：
  - **“RX”**— 表示传入通信被镜像。
  - **“TX”**— 表示传出通信被镜像。
  - **“Both”（二者兼有）**— 表示传入和传出通信均被镜像。
- **“Status”（状态）**— 表示端口的状态。 可能的字段值包括：
  - **“Active”（激活）**— 表示端口被启用，正在接收/传输网络通信。

- **“Not Active”（未激活）**— 表示端口被禁用，不能接收/传输网络通信。

- **“Remove”（删除）**— 删除端口镜像会话。 可能的字段值包括：
  - **已选取** — 删除端口镜像会话。
  - **未选取** — 保留端口镜像会话。

要添加端口镜像会话，请：

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。



添加源端口

3. 定义 **“Source Port”（源端口）**和 **“Type”（类型）**字段。
4. 单击 **“Apply Changes”（应用更改）**。 系统将定义新的源端口，并更新设备。

要从端口镜像会话删除副本端口，请：

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）**。 系统将删除端口镜像会话，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。

CLI 命令	**说明**
port monitor src 接口 **[rx | tx]**	显示端口副本的状态。
show ports monitor	启动端口监测会话。

以下是 CLI 命令实例：

```
Console(config)# interface ethernet 1/e1

Console(config-if)# port monitor 1/e8
```

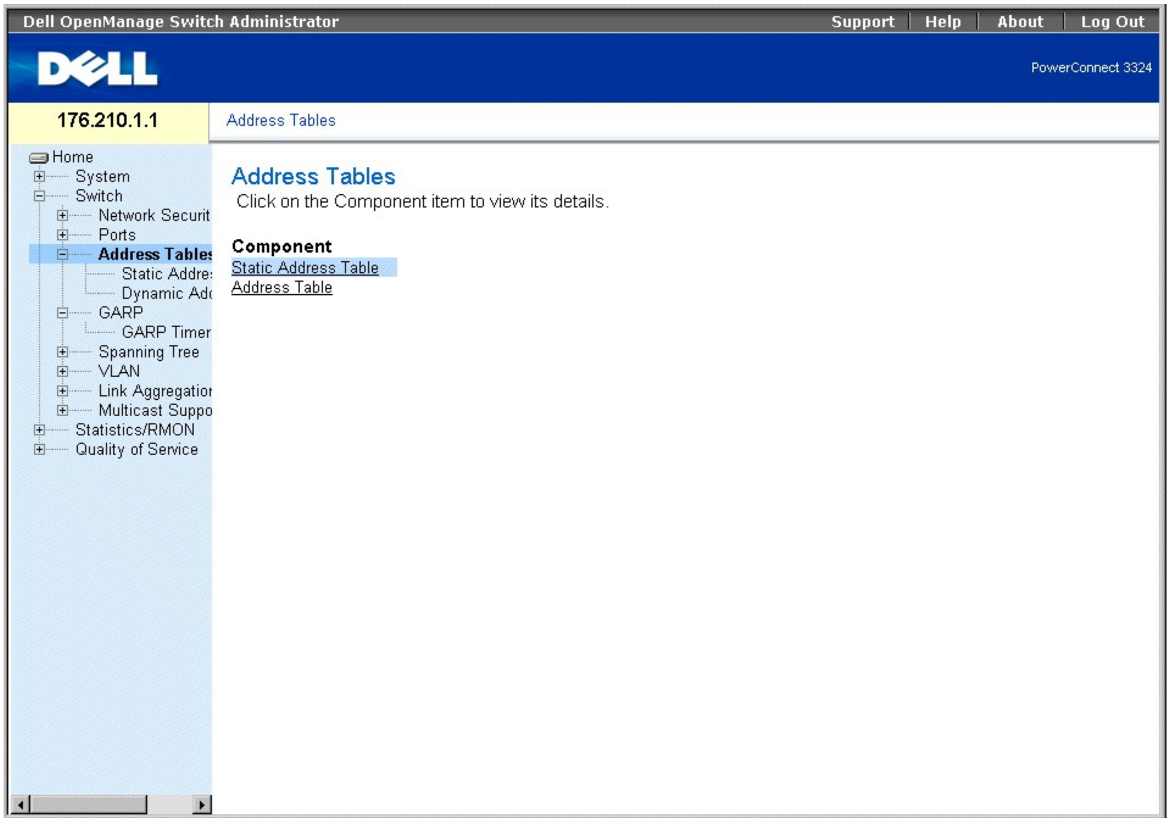
```
Console# show ports monitor

Source port Destination Port Type Status

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

1/e1 1/e8 RX, TX Active

1/e2 1/e8 RX Active
```

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。 静态和动态地址表可以按接口、VLAN 和接口类型进行排序。 当信息包从源到达交换机时，MAC 地址将被动态学习。 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。 静态地址需要用户手动进行配置。 如果动态 MAC 地址在特定时间段后未进行任何通信，
这些地址将被删除，以防止桥接表溢出。

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）**。
  系统将打开 **"Address Tables"（地址表）**页面。



地址表页面

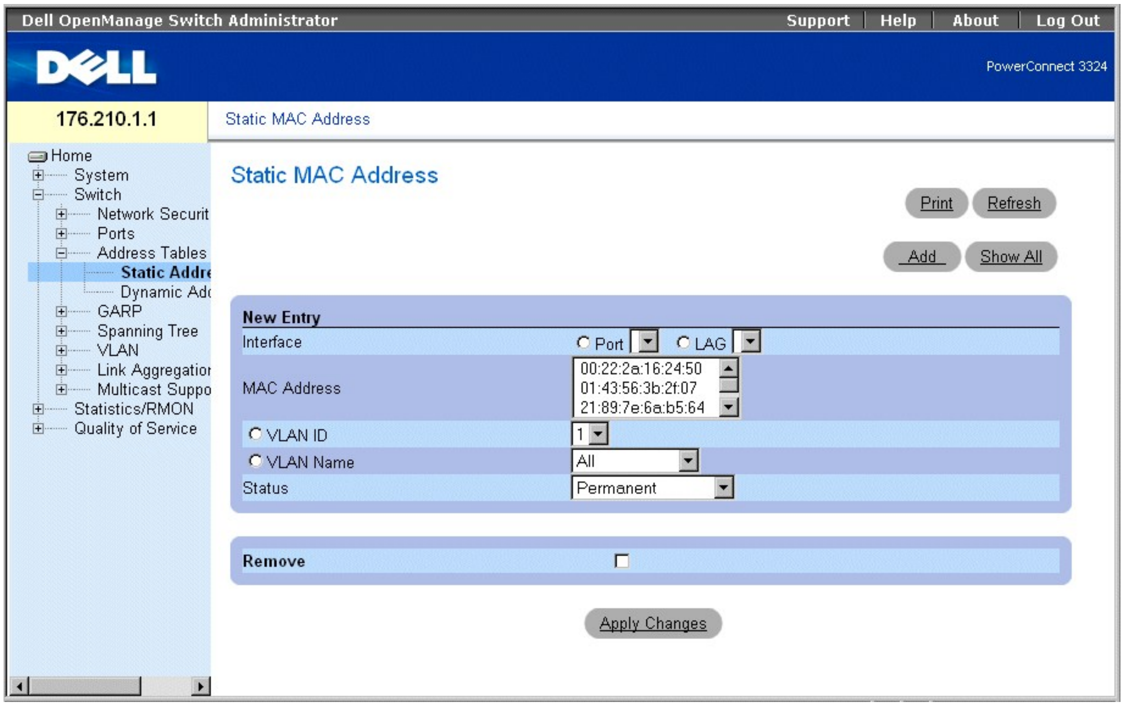
"Address Tables"（地址表）页面包含指向以下内容的链接：

- 定义静态地址
- 查看动态地址

定义静态地址

"Static MAC Address"（静态 MAC 地址）页面包含静态 MAC 地址的列表。 可以在**"Static MAC Address"（静态 MAC 地址）**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"（静态 MAC 地址）**页面，请：

- 在树视图中单击**"Switch"（交换机）>"Address Tables"（地址表）> "Static Address"（静态地址）**。 系统将打开**"Add Static MAC Address"（添加静态 MAC 地址）**页面。



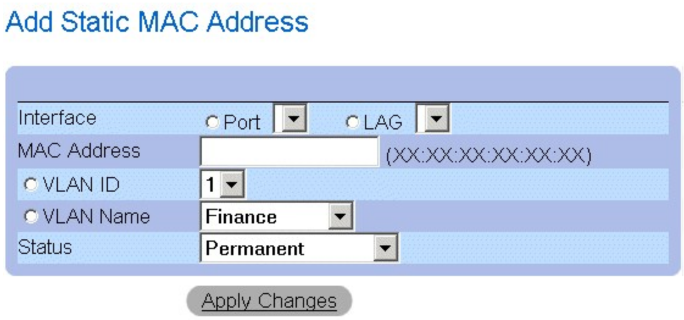
添加静态 MAC 地址页面

"AddStatic MAC Address"（添加静态 MAC 地址）页面包含以下字段：

- **"Interface"（接口）**— 表示要添加静态 MAC 地址的特定接口。 可能的字段值包括：
  - **"Port"（端口）**— 表示要添加 MAC 地址的特定端口。
  - **"LAG"**— 表示要添加 MAC 地址的特定 LAG。
- **"MAC Address"（MAC 地址）**— 指定**"Current Static Address List"（当前静态地址列表）**中列出的 MAC 地址。
- **"VLAN ID"**— 表示连接至 MAC 地址的 VLAN ID 的值。
- **"VLAN Name"（VLAN 名称）**— 表示用户定义的 VLAN 名称。
- **"Status"（状态）**— 定义静态 MAC 地址的状态。 可能的字段值包括：
  - **"Permanent"（永久）**— 表示 MAC 地址是永久性的。
  - **"Delete on Reset"（重设时删除）**— 表示在重设设备时删除 MAC 地址。
  - **"Timeout"（超时）**— 表示在设备超时时删除 MAC 地址。
  - **"Secure"（安全）**— 保证锁定端口的 MAC 地址不被删除。 安全 MAC 地址可通过"端口安全保护页面"删除。

要将静态地址添加至静态地址表中，请：

1. 打开**"Static Address Table"（静态地址表）**。
2. 单击**"Add"（添加）**。 系统将打开**"AddStatic MAC Address"（添加静态 MAC 地址）**页面。



添加静态 MAC 地址页面

3. 定义 **"Interface"（接口）**、**"MAC Address"（MAC 地址）**、**"VLAN ID"** 或 **"VLAN Name"（VLAN 名称）**以及 **"Status"（状态）**字段。

4. 单击 **"Apply Changes"（应用更改）**。 系统会将新的静态地址添加至静态地址表中，并更新设备。

要修改静态地址表中的静态地址，请：

1. 打开 **"Static Address Table"（静态地址表）**。

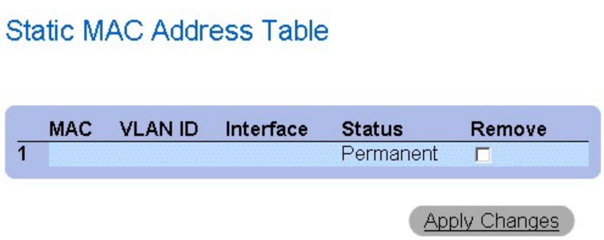
2. 修改 **"Port"（端口）**、**"MAC Address"（MAC 地址）**和 **"VLAN"**字段。

3. 单击 **"Apply Changes"（应用更改）**。 系统将修改静态地址，并更新设备。

要显示静态 MAC 地址表，请：

1. 打开 **"Static Address Table"（静态地址表）**。

2. 单击 **"Show All"（全部显示）**。 系统将打开 **"Static MAC Address Table"（静态 MAC 地址表）**。



静态 MAC 地址表

要删除静态地址表中的静态地址，请：

1. 打开 **"Static Address Table"（静态地址表）**。

2. 单击 **"Show All"（全部显示）**，打开 **"Static MAC Address Table"（静态 MAC 地址表）**。

3. 选择单个或多个表条目。

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 **“Add Static MAC Address”（添加静态 MAC 地址）**页面中显示的配置静态地址参数的选项等效的 CLI 命令。

CLI 命令	说明
bridge address MAC 地址 **{ethernet** 接口 **| port-channel** 端口通道号**} [permanent | delete-on-reset | delete-on-timeout| secure]**	将静态 MAC 层的站点源地址添加至网桥表中。
show bridge address-table static [vlan VLAN**] [ethernet** 接口 **| port-channel** 端口通道号**]**	显示在网桥传输数据库中静态输入的条目的分类。

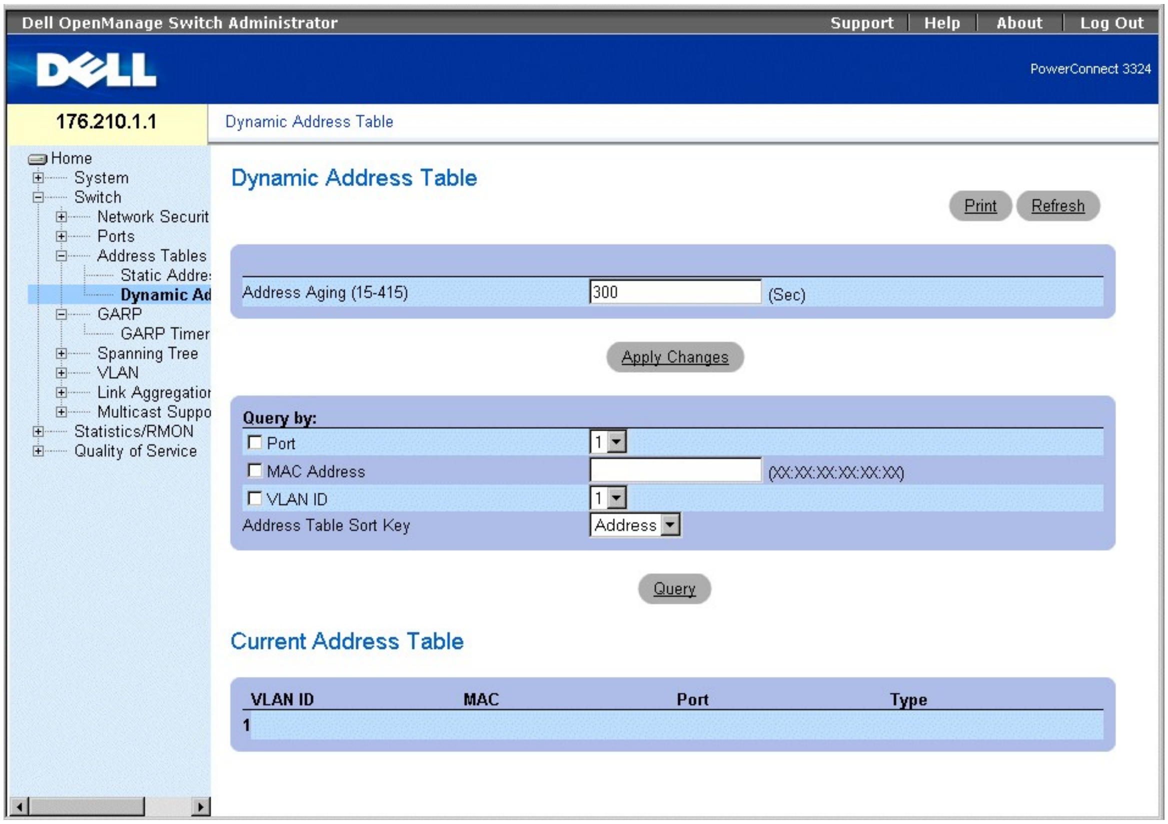
以下是 CLI 命令实例：

```
Console (config-vlan)# bridge address 168.210.0.10 ethernet 1/e8 permanent

Console# show bridge address table static

Aging time is 300 sec

vlan mac address port type

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

200 0010.0D48.37FF 5/9 delete-on-reset
```

查看动态地址

“Dynamic Address”（动态地址）页面包含有关查询 **“Dynamic Address Table”（动态地址表）**的信息，包括接口类型、MAC 地址、VLAN 和表排序。 传输至存储在地址表中的地址的信息包将被直接发送至那些端口。 要打开 **“Dynamic Address”（动态地址）**页面，请：

- 在树视图中单击 **“Switch”（交换机）>“Address Tables”（地址表）>“Dynamic Address”（动态地址）**。 系统将打开 **“Dynamic Address Table”（动态地址表）**页面。



动态地址表页面

"Dynamic Address"（动态地址）页面包含以下字段：

- **"Address Aging"（地址存在时间）**— 指定如果未检测到来自源的通信，在超时之前 MAC 地址在 **"Dynamic Address Table"（动态地址表）**中保留的时间。
  默认值为 300 秒。
- **"Port"（端口）**— 指定要为其查询表的端口号。
- **"MAC Address"（MAC 地址）**— 指定要为其查询表的 MAC 地址。
- **"VLAN ID"**— 表示要为其查询表的 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。 可能的字段值包括：
  - **"Address"（地址）**— 排序指定 MAC 地址的查询结果。
  - **"VLAN"**— 按照 VLAN ID 排序查询结果。
  - **"Interface"（接口）**— 按照接口排序查询结果，并显示在指定端口上学习的所有 MAC 地址。

"Query Results Table"（查询结果表）包含以下列：

- **"VLAN ID"**— 表示 VLAN 标记值。
- **"MAC"**— 表示 MAC 地址。
- **"Port"（端口）**— 表示连接至动态 MAC 地址的端口。
- **"Type"（类型）**— 表示 MAC 地址的类型。

要重新定义存在时间，请：

1. 打开**“Dynamic Address Table”（动态地址表）**。
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。

要查询动态地址表，请：

1. 打开**“Dynamic Address Table”（动态地址表）**。
2. 定义查询**“Dynamic Address Table”（动态地址表）**所依据的参数。 可以按照接口、MAC 地址或 VLAN 查询**“Dynamic Address Table”（动态地址表）**条目。
3. 单击**“Query”（查询）**。 将查询**“Dynamic Address Table”（动态地址表）**。 查询结果将按照选定的**“Address Table Sort Key”（地址表排序关键字）**字段值进行排序。

使用 CLI 命令查询并排序动态地址

下表概括了与**“Dynamic Address Table”（动态地址表）**页面中显示的查询和排序动态地址的选项等效的 CLI 命令。

CLI 命令	说明
bridge aging-time 秒	设置地址表存在时间。
show bridge address-table [vlan VLAN**] [ethernet** 接口 **| port-channel** 端口通道号**]**	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 命令实例：

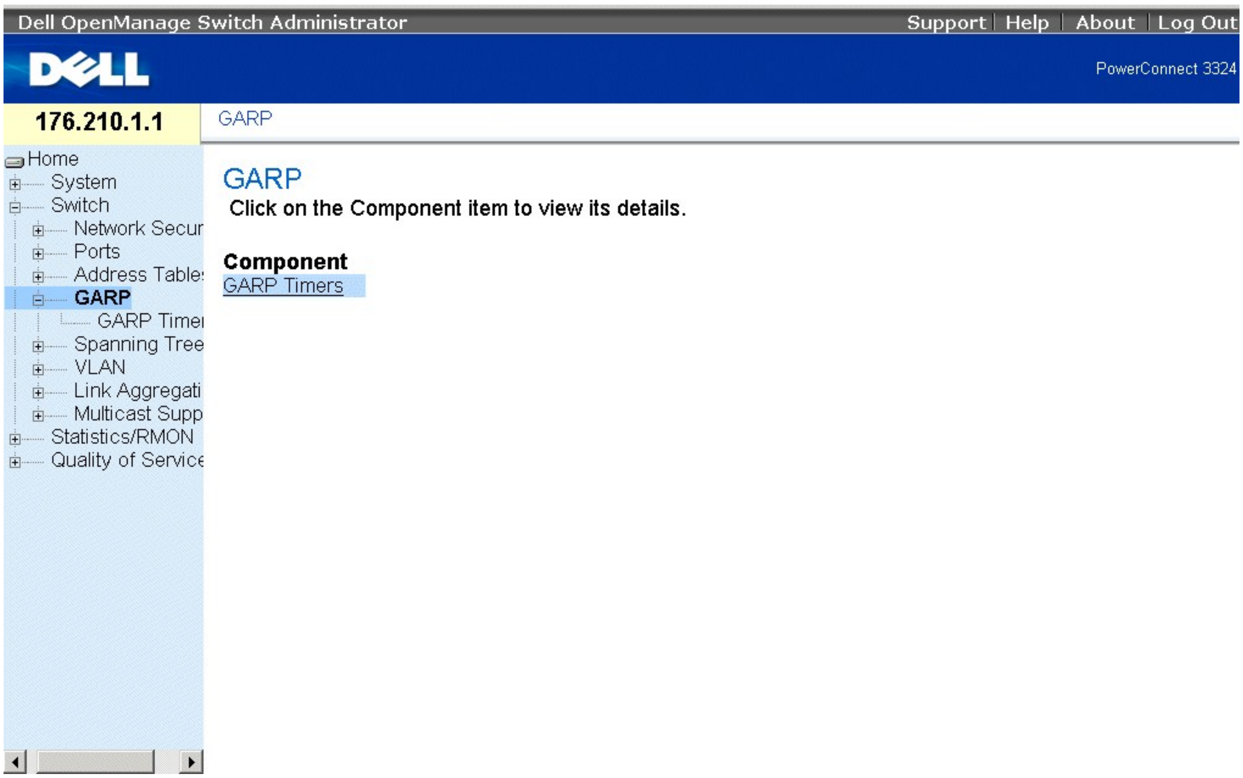
```
Console (config)# bridge aging-time 250

Console (config)# exit

Console# show bridge address table


Aging time is 250 sec


vlan mac address port type

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

1 0060.704C.73FF 5/e8 dynamic

1 0060.708C.73FF 5/e8 dynamic
```

200 0010.0D48.37FF 5/e9 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。 要打开 **"GARP"**页面，请：

- 在树视图中单击 **"Switch"（交换机）>"GARP"**。 系统将打开 **"GARP"**页面。



GARP 页面

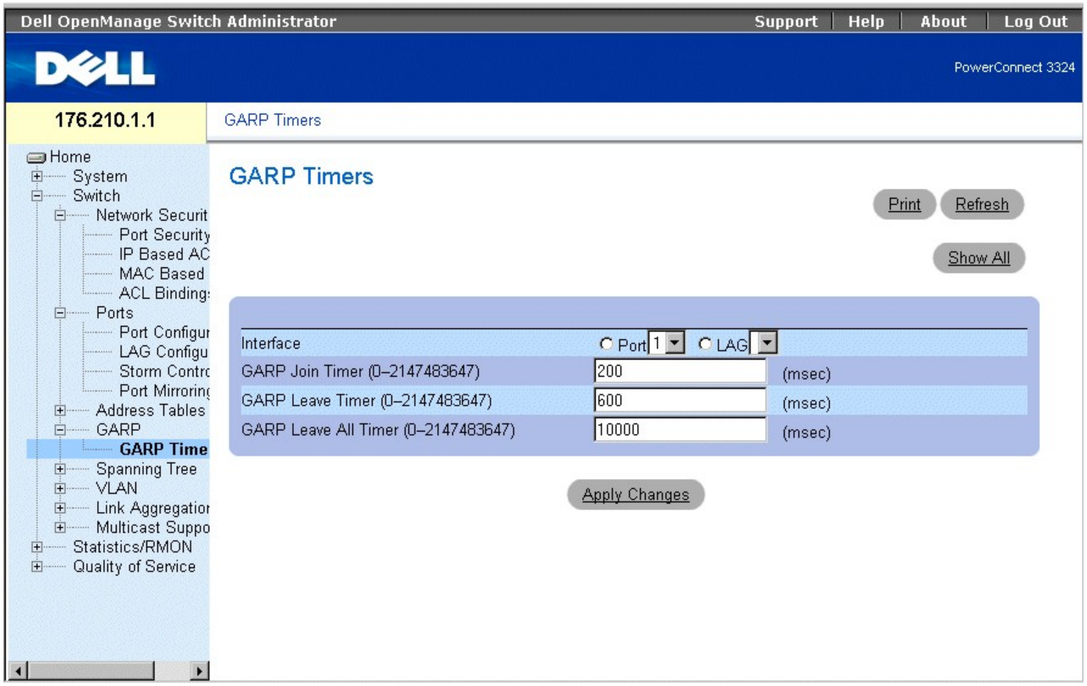
本节包括以下主题：

- [定义 GARP 计时器]

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 的参数。 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）**。 系统将打开 **"GARP Timers"（GARP 计时器）**页面。



GARP 计时器页面

"GARP Timers"（GARP 计时器）页面包含以下字段：

- **"Interface"（接口）** — 表示要在其上显示 GARP 计时器的接口的类型。
  可能的字段值包括：
  - **"Port"（端口）** — 表示要显示 GARP 计时器的端口。
  - **LAG** — 表示要显示 GARP 计时器的 LAG。
- **"GARP Join Timer (10-2147483647)"（GARP 加入计时器 [10-2147483647]）** — 表示传输 PDU 的时间（以毫秒为单位）。
- **"GARP Leave Timer (10-2147483647)"（GARP 离开计时器 [10-2147483647]）** — 表示设备离开其 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 **"Leave Time"（离开时间）**，接收到的 **"Join"（加入）**信息可以取消 **"Leave Time"（离开时间）**。 默认值为 600 毫秒。
- **"GARP Leave All Timer (10-2147483647)"（GARP 全部离开计时器 [10-2147483647]）** — 用于确认 VLAN 内部的端口。 发送信息之间的时间以毫秒为单位。 默认值为 10000 毫秒。

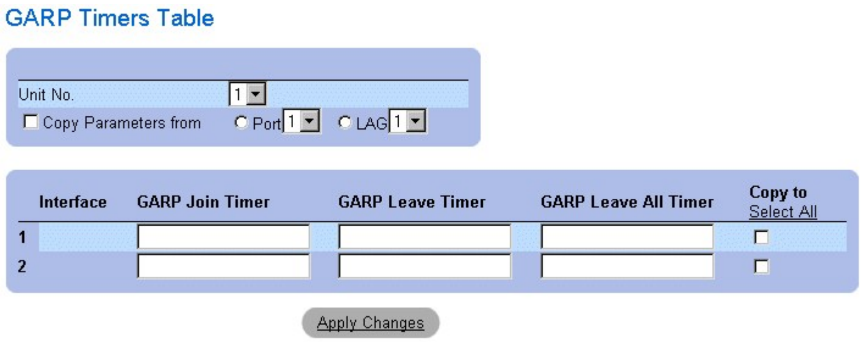
注： 各个计时器值之间必须保持以下关系： 即离开时间必须大于或等于加入时间的三倍， 全部离开时间必须大于离开时间。

要定义 GARP 计时器，请：

1. 打开 **"GARP Timers"（GARP 计时器）**页面。
2. 定义 **"Interface"（接口）**、**"GARP Join Timer"（GARP 加入计时器）**、**"GARP Leave Timer"（GARP 离开计时器）**和 **"GARP Leave All Timer"（GARP 全部离开计时器）**。
3. 单击 **"Apply Changes"（应用更改）**。 GARP 参数将被保存至设备。

要显示 GARP 计时器表，请：

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）**。



GARP 计时器表

除了**“GARP Timers”（GARP 计时器）**页面中的字段外，**“GARP Timers Table”（GARP 计时器表）**页面还显示以下字段：

- **"Unit No."（装置号）**— 表示堆叠装置号。
- **"Copy From"（复制自）**— 将端口 GVRP 参数复制到**“Copy to”（复制到）**字段中指定的接口。
- **"Copy to"（复制到）**— 表示 GVRP 计时器要复制到的接口。

要复制 GARP 信息，请：

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）**字段中选择一个接口。
4. 在**“Copy to”（复制到）**字段中选择 GARP 计时器信息要复制到的接口。

使用 CLI 命令定义 GARP 计时器

下表概括了与**“GARP Timers”（GARP 计时器）**页面中显示的定义 GARP 计时器的选项等效的 CLI 命令。

CLI 命令	说明
garp timer {join | leave | leaveall} 计时器值	设置 GARP 应用程序加入、离开和全部离开 GARP 计时器的值。

以下是 CLI 命令实例：

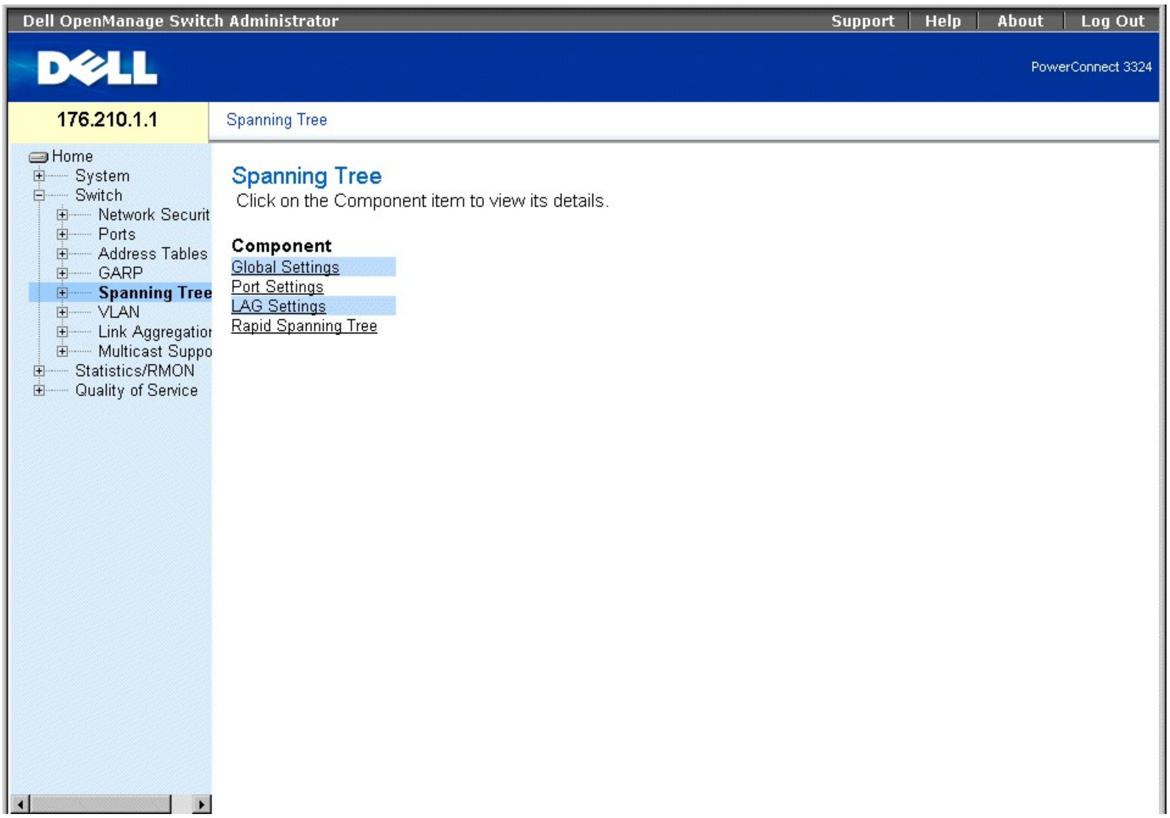
```
Console (config)# interface ethernet 1/e8

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

配置生成树协议

生成树协议 (STP) 可以提供第 2 层网络上终端站点之间的单一路径，从而消除了环路。

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性能降低。 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）**。 系统将打开 **"Spanning Tree"（生成树）**页面。



生成树页面

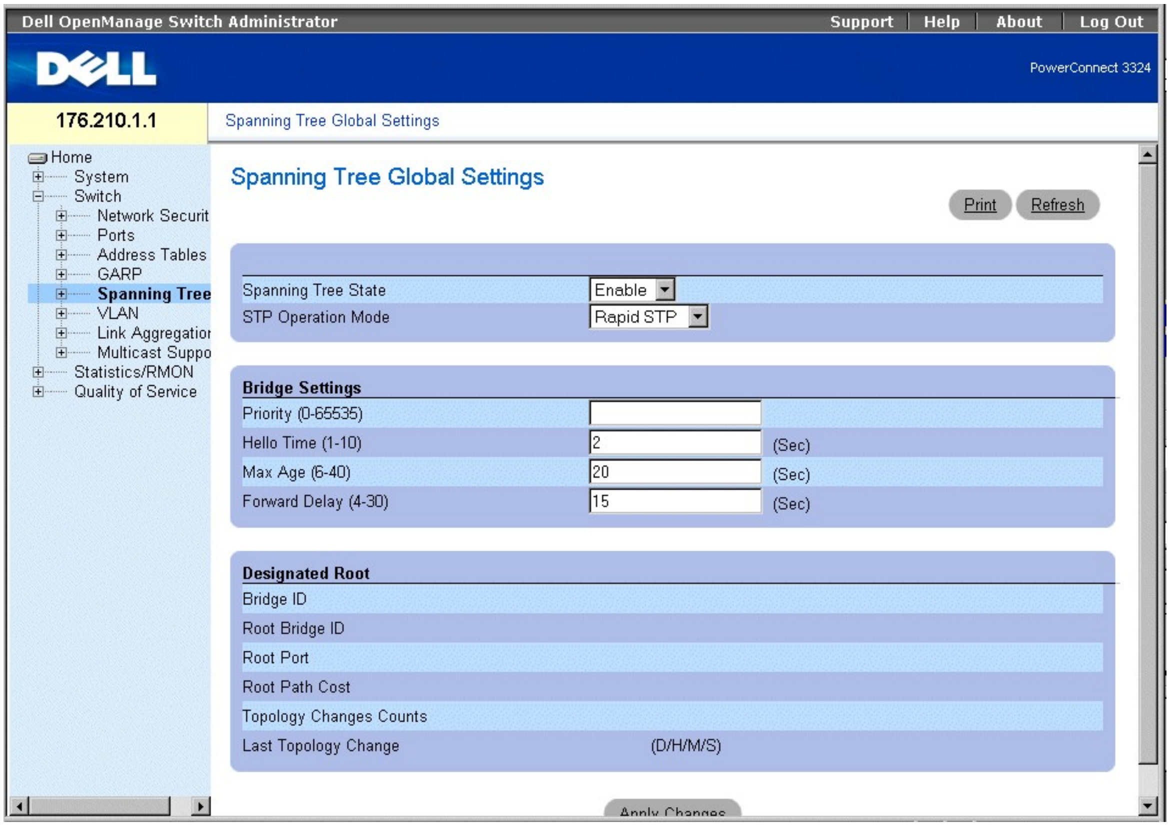
本节包含以下主题：

- 定义 STP 全局设置
- 定义 STP 端口设置
- 定义 STP LAG 设置
- 配置快速生成树

定义 STP 全局设置

"Spanning Tree Global Parameters"（生成树全局参数）页面包含用于在设备上启用和配置 STP 操作的参数。 要打开 **"Spanning Tree Global Parameters"（生成树全局参数）**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）**。 系统将打开 **"Spanning Tree Global Parameters"（生成树全局参数）**页面。



生成树全局设置页面

"Spanning Tree Global Parameters"（生成树全局参数）页面包含以下字段：

- **"Spanning Tree State"（生成树状态）** — 在设备上启用 STP。 可能的字段值包括：
  - **"Enable"（启用）** — 在设备上启用 STP。
  - **"Disable"（禁用）** — 在设备上禁用 STP。
- **"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 (IEEE 802.1D)。
  - **"Rapid STP"（快速 STP）** — 在设备上启用快速 STP (IEEE 802.1w)。
    有关快速 STP 的详细信息，请参阅"配置快速生成树"。
- **"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，优先级值最低的交换机将成为根网桥。 默认值为 32768。端口优先级值以 16 的倍数为增量递增，例如 16、32、64 和 80 等。
- **"Hello Time (1-10)"（问候间隔 [1-10]）** — 指定交换机的问候间隔。 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]）** — 指定交换机的最长存在时间。 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]）** — 指定交换机的传输延迟时间。 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 15 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。 默认值为 0。
- **"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。 时间以日、小时、分钟、秒钟的格式显示，例如，
  2 天 5 小时 10 分钟 4 秒。

要定义 STP 全局参数，请：

1. 打开**"Spanning Tree Global Parameters"（生成树全局参数）**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**"Classic STP"（经典 STP）**。
4. 单击**"Apply Changes"（应用更改）**。 系统将在设备上启用 STP。

要修改 STP 全局参数，请：

1. 打开**"Spanning Tree Global Parameters"（生成树全局参数）**页面。
2. 定义**"STP Operation Mode"（STP 运行模式）**、**"Bridge Priority"（网桥优先级）**、**"Hello Time (Sec)"（问候间隔 [秒]）**、**"Max Age (Sec)"（最长存在时间 [秒]）**和**"Forward Delay (Sec)"（传输延迟 [秒]）**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）**页面中显示的定义 STP 全局参数的选项等效的 CLI 命令。

CLI 命令	**说明**
spanning-tree	启用生成树功能。
spanning-tree mode {stp | rstp}	配置当前运行的生成树协议。
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，即交换机向其它交换机广播问候信息的频率。
spanning-tree max-age 秒	配置生成树网桥最长存在时间，即确定交换机存储端口接收的协议信息的时间。
spanning-tree forward-time seconds	配置生成树网桥传输时间，即进入传输状态之前端口保持侦听和学习状态的时间。
show spanning-tree [ethernet 接口 **| port-channel** 端口通道号**]**	显示生成树配置。

以下是 CLI 命令实例：

```
Console(config)# spanning-tree

Console(config)# spanning-tree mode rstp

Console(config)# spanning-tree priority 12288

Console(config)# spanning-tree hello-time 5
```

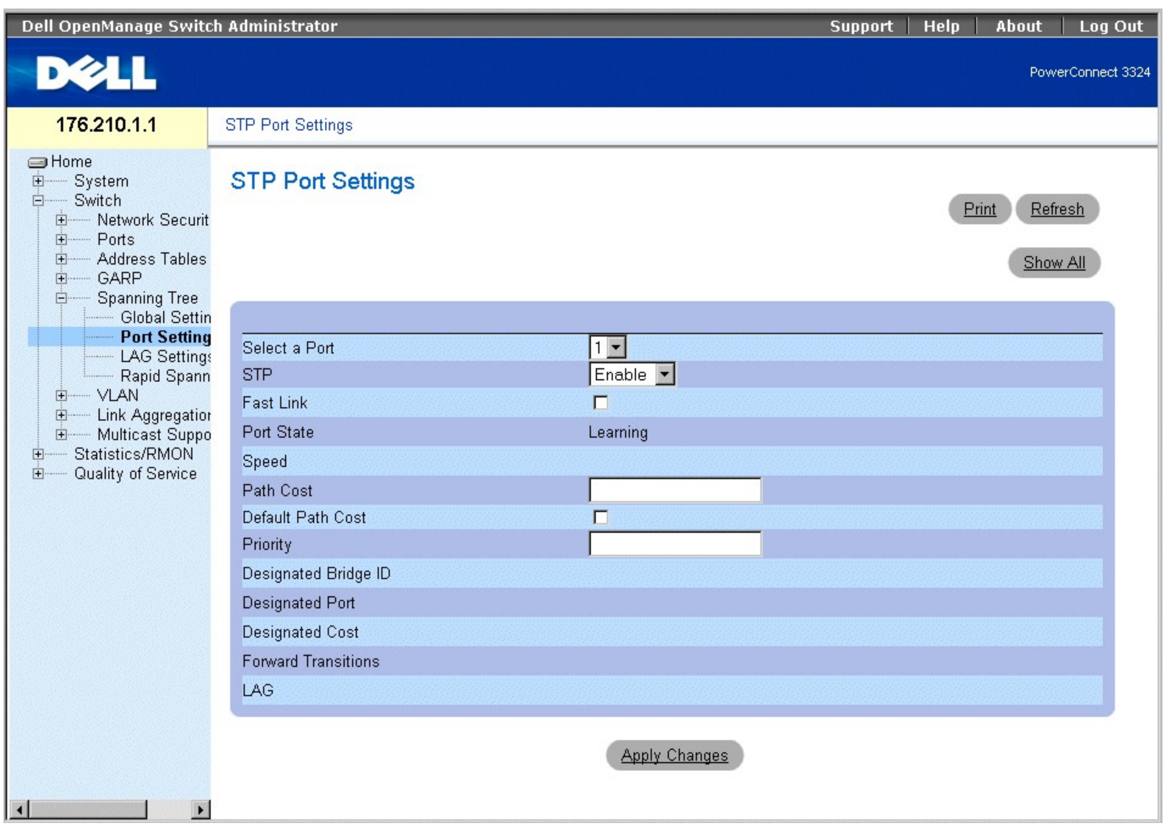
```
Console(config)# spanning-tree max-age 10

Console(config)# spanning-tree forward-time 25

Console(config)# exit

Console# show spanning-tree

Spanning tree enabled mode RSTP

Root ID Priority 32768

Address X.X.X.X.X.X

Cost 57

Port 1/e1

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769

Address X.X.X.X.X.X

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Number of topology changes 2 last change occurred 00:23:56 ago

Times: hold 1, topology change 35, notification 2

hello 2, max age 20, forward delay 15


Interface Port ID Designated Port ID

Name Prio Cost Sts Cost Bridge ID Prio.Nbr
```

```
-------- ------ --- --- -------------------- ------

1/e1 128 19 FWD 38 8000 00:30:94:41:62c1 80 001

1/e2 128 19 FWD 57 8000 00:02:4b:29:7a:00 80 002

ch1 128 19 FWD 57 8000 00:02:4b:29:7a:00 80 003
```

定义 STP 端口设置

"STP Port Settings"（STP 端口设置）页面使网络管理员可以为各个端口设定 STP 属性。
要打开**"STP Port Settings"（STP 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）**。 系统将打开**"STP Port Settings"（STP 端口设置）**页面。



STP 端口设置页面

"STP Port Settings"（STP 端口设置）页面包含以下字段：

- **"Select a Port"（选择端口）**— 表示要显示 STP 统计数据的端口。
- **"STP"**— 在端口上启用 STP。 可能的字段值包括：

- **"Enable"（启用）**－ 在端口上启用 STP。
- **"Disable"（禁用）**－ 在端口上禁用 STP。

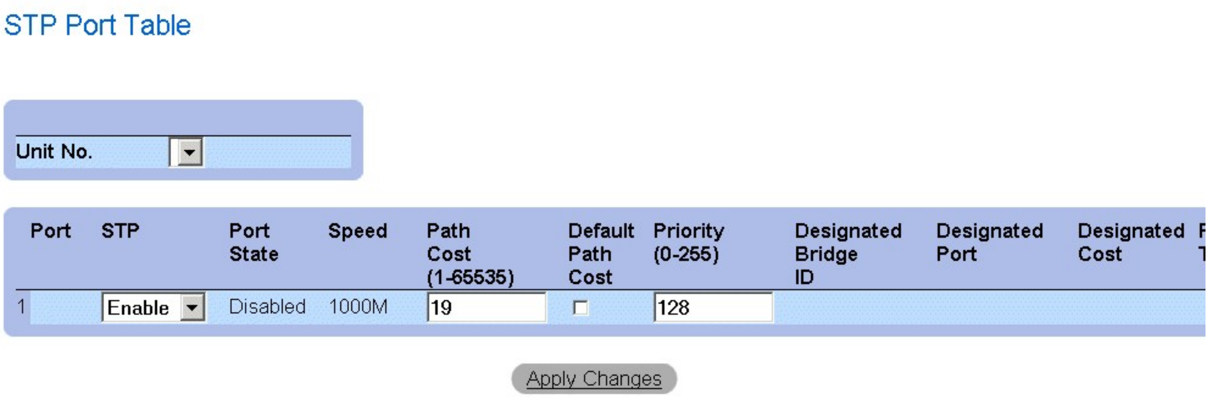
- **"Fast Link"（快速链路）**－ 为端口启用快速链路模式。 如果为端口启用了快速链路，则端口链路良好时端口将被自动置入**"Forwarding State"（传输状态）**。 快速链路模式可以优化 STP 协议进行聚合所需的时间（在大型网络中，STP 聚合可能需要 30 至 60 秒）。
- **"Port State"（端口状态）**－ 表示端口的当前 STP 状态。 如果已启用该选项，端口状态将确定对通信所采取的传输操作。 可能的字段值包括：
  - **"Disabled"（已禁用）**－ 表示端口链路当前已断开。
  - **"Blocking"（阻塞）**－ 端口当前已被阻塞，无法用于传输通信或学习 MAC 地址。
  - **"Listening"（侦听）**－ 端口当前处于侦听模式。 端口既不能传输通信，也不能学习 MAC 地址。
  - **"Learning"（学习）**－ 端口当前处于学习模式。 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。
- **"Speed"（速率）**－ 表示端口速率。 可能的字段值包括：
  - **"10M"**
  - **"100M"**
  - **"1000M"**
- "Path Cost"（路径成本）－ 表示此端口在根路径成本中所占的比例。 路径成本可以调整为较高或较低的值，可以将通信传输至重定路线的路径或从重定路线的路径传输通信。 路径成本可以是 1 至 65,535 之间的值。
- **"Default Path Cost"（默认路径成本）**－ 指定默认路径成本。
- **"Priority"（优先级）**－ 表示端口的优先级值。 当网桥有两个端口连接在同一 LAN 的环路中时，优先级值可用于确定端口的选择。 优先级值介于 0 至 255 之间。
- **"Designated Bridge ID"（指定网桥 ID）**－ 表示指定网桥的优先级和 MAC 地址。
- **"Designated Port"（指定端口）**－ 表示指定网桥上选定端口的优先级和 MAC 地址。
- **"Designated Cost"（指定成本）**－ 表示参与 STP 拓扑的指定端口的成本。
- **"Forward Transitions"（传输转换）** 表示端口从**"blocking"（阻塞）**状态变为**"forwarding"（传输）**状态的次数。
- **"LAG"**－ 指定端口要连接的 LAG。

要在端口上启用 STP，请：

1. 打开**"STP Port Settings"（STP 端口设置）**页面。
2. 在"STP"字段中选择**"Enabled"（启用）**。
3. 定义**"Priority"（优先级）**、**"Path Cost"（路径成本）**、**"Default Path Cost"（默认路径成本）**和**"Fast Link"（快速链路）**字段。
4. 单击**"Apply Changes"（应用更改）**。 系统将在端口上启用 STP。

要修改 STP 端口属性，请：

1. 打开**"STP Port Settings"（STP 端口设置）**页面。
2. 修改**"Priority"（优先级）**、**"Path Cost"（路径成本）**、**"Default Path Cost"（默认路径成本）**和**"Fast Link"（快速链路）**字段。
3. 单击**"Apply Changes"（应用更改）**。 系统将修改 STP 端口参数，并更新设备。



STP 端口表页面

使用 CLI 命令定义 STP 端口参数

下表概括了与 **“STP Port Settings”（STP 端口设置）**页面中显示的定义 STP 端口参数的选项等效的 CLI 命令。

CLI 命令	**说明**
spanning-tree disable	禁用指定端口上的生成树。
spanning-tree cost 成本	配置端口的生成树端口成本。
spanning-tree port-priority 优先级	配置端口优先级。
show spanning-tree [ethernet 接口 **| port-channel** 端口通道号**]**	显示生成树配置。
spanning-tree portfast	启用 PortFast 模式。

以下是 CLI 命令实例：

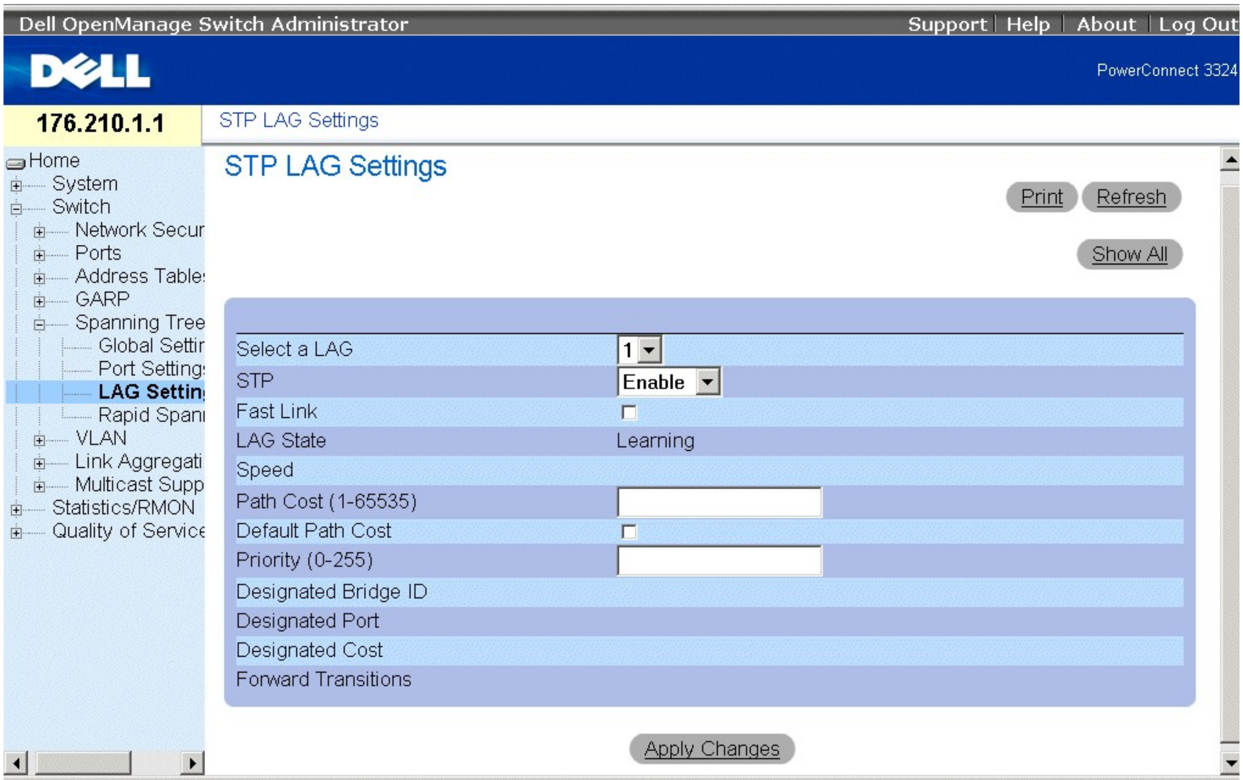
```
Console(config)# interface ethernet 1/e5

Console(config-if)# spanning-tree disable

Console(config-if)# spanning-tree cost 35000

Console(config-if)# spanning-tree port-priority 96

Console(config-if)# exit

Console(config)# exit

Console# show spanning-tree ethernet 1/e5
```

```
Console# show spanning-tree ethernet 1/e5

Interface Port ID Designated Port ID

Name Prio Sts Enb Cost Cost Bridge ID Prio.Nbr

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

1/e5 128 DSBL True 100 0 8000 xx.xx.xx.xx.xx.xx 80 001

Spanning tree enabled

Port Fast: no (configured: no)

Type: point-to-point (configured: auto)

Number of transitions to forwarding state: 1

BPDU: sent 2, received 120638
```

定义 STP LAG 设置

"STP LAG Settings"（STP LAG 设置）页面使网络管理员可以为 LAG 设定 STP 参数。
打开**"STP LAG Settings"（STP 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）**。系统将打开**"STP LAG Settings"（STP LAG 设置）**页面。



STP LAG 设置页面

"STP LAG Settings"（STP LAG 设置）页面包含以下字段：

- **"Select a LAG"（选择 LAG）**— 表示用户定义的 LAG。 有关定义 LAG 的详细信息，请参阅"定义 LAG 成员关系"。
- **"STP"**— 在 LAG 上启用 STP。 可能的字段值包括：
  - **"Enable"（启用）**— 在 LAG 上启用 STP。
  - **"Disable"（禁用）**— 在 LAG 上禁用 STP。
- **"Fast Link"（快速链路）**— 为 LAG 启用快速链路。 如果为 LAG 启用了快速链路，则 LAG 将被自动置入**"Forwarding State"（传输状态）**。 快速链路可以优化 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）。

注： 请仅在适合的情况下使用**"Fast Link"（快速链路）**选项；例如，当设备是终端站点 STP 网络拓扑中的叶设备时。

- **"LAG State"（LAG 状态）**— 表示 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，LAG 将被置入**"Disabled"（禁用）**状态。 可能的字段值包括：
  - **"Disabled"（禁用）**— 链路当前已断开。
  - **"Blocking"（阻塞）**— LAG 当前已被阻塞，无法用于传输通信或学习 MAC 地址。
  - **"Listening"（侦听）**— LAG 当前处于侦听模式。 LAG 不能传输通信，也不能学习 MAC 地址。
  - **"Learning"（学习）**— LAG 当前处于学习模式。 LAG 不能传输通信，但可以学习新的 MAC 地址。
  - **"Forwarding"（传输）**— LAG 当前处于传输模式。 LAG 可以传输通信，也可以学习新的 MAC 地址。
- **"Speed"（速率）**— 组成 LAG 的端口的速率。
- **"Path Cost (1-65535)"（路径成本 [1-65535]）**— 表示此 LAG 在根路径成本中所占的比例。 路径成本可以调整为较高或较低的值，可以将通信传输至重定路线的路径或从重定路线的路径传输通信。 路径成本可以是 1 至 65,535 之间的值。

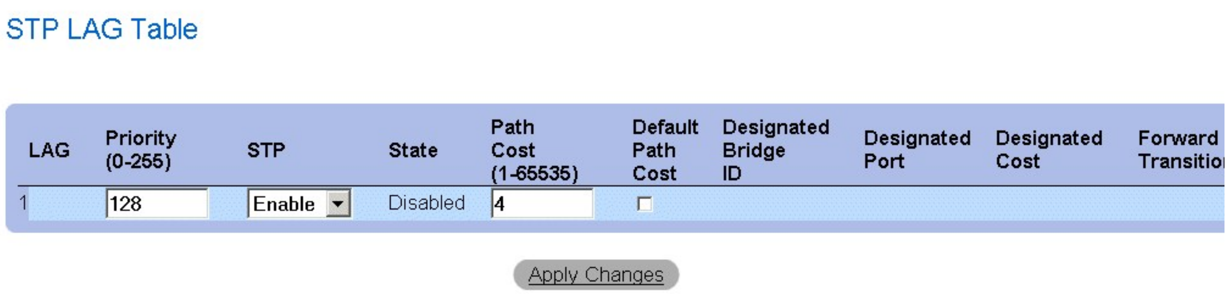
- **"Default Path Cost"（默认路径成本）**— 指定默认路径成本。 LAG 的默认路径成本为 4。
- **"Priority (0-255)"（优先级 [0-255]）**— 表示 LAG 的优先级值。 当网桥有两个环路端口在同一 LAN 中时，优先级值可用于确定 LAG 的选择。 优先级值介于 0 至 255 之间。
- **"Designated Bridge ID"（指定网桥 ID）**— 表示指定网桥的优先级和 MAC 地址。
- **"Designated Port"（指定端口）**— 表示选定端口的优先级和 MAC 地址。
- **"Designated Cost"（指定成本）**— 表示指定的成本。
- **"Forward Transitions"（传输转换）**— 表示端口从 **"blocking"（阻塞）** 状态变为 **"forwarding"（传输）** 状态的次数。

要在 LAG 上启用 STP，请：

1. 打开 **"STP LAG Settings"（STP LAG 设置）** 页面。
2. 在 "STP"字段中选择 **"Enable"（启用）**。
3. 定义 **"Priority"（优先级）**、**"Path Cost"（路径成本）** 和 **"Fast Link"（快速链路）** 字段。
4. 单击 **"Apply Changes"（应用更改）**。 系统将在 LAG 上启用 STP，并更新设备。

要修改 LAG STP 参数，请：

1. 打开 **"STP LAG Settings"（STP LAG 设置）** 页面。
2. 修改 **"Priority"（优先级）**、**"Path Cost"（路径成本）** 和 **"Fast Link"（快速链路）** 字段。
3. 单击 **"Apply Changes"（应用更改）**。 系统将修改 STP LAG 参数，并更新设备。



STP LAG 表页面

使用 CLI 命令定义 STP LAG 参数

下表概括了与 **"STP LAG Settings"（STP LAG 设置）** 页面中显示的定义 STP LAG 参数的选项等效的 CLI 命令。

CLI 命令	说明
interface port-channel 端口通道号	进入端口通道配置模式。
spanning-tree port-priority 优先级	

	配置 LAG 优先级。

以下是 CLI 命令实例：

```
console(config)# interface port-channel 1
```

```
console(config-if)# spanning-tree port-priority 16
```

配置快速生成树

经典生成树可以防止普通网络拓扑中的 L2 传输环路。 但是，聚合最多需要 30 至 60 秒。 对于许多应用程序来说，聚合时间太长。 如果网络拓扑允许，可以进行更快的聚合。 快速生成树协议 (RSTP) 可以检测并使用提供生成树快速聚合的网络拓扑，且不会创建传输环路。

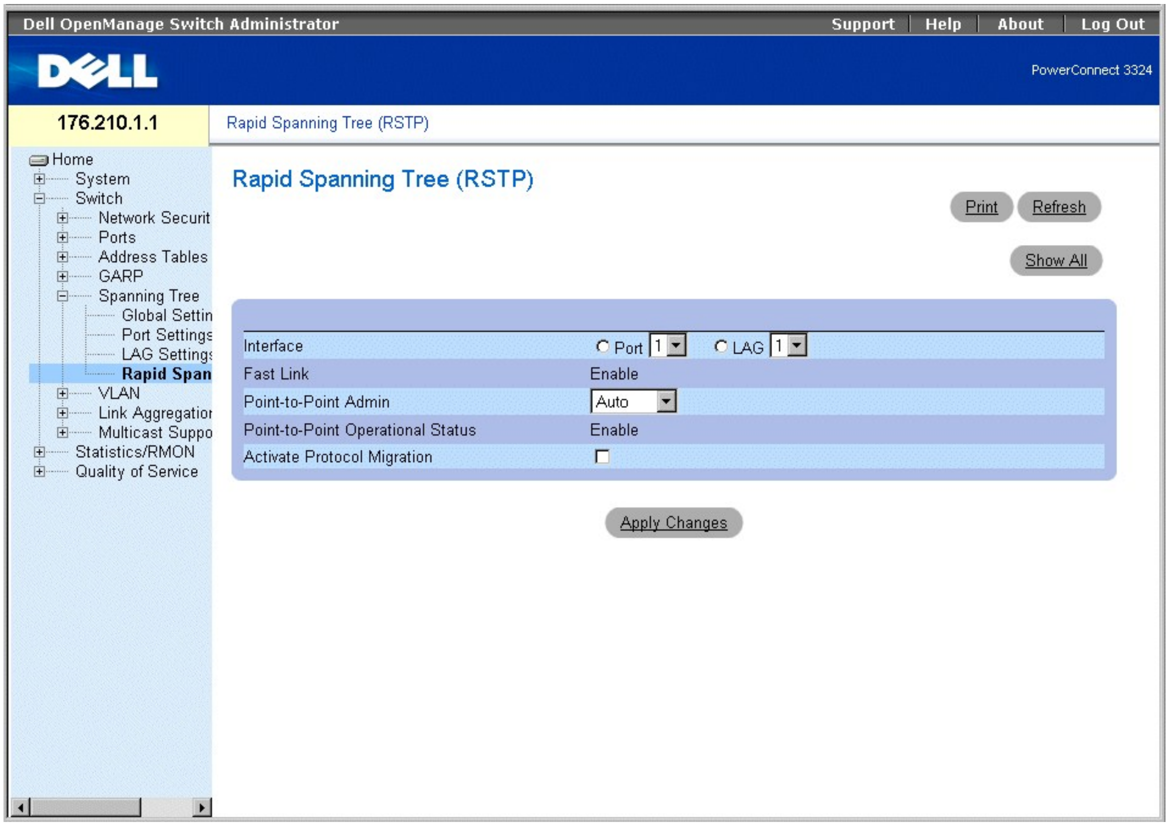
STP 具有以下几种端口状态：

- "Listening"（侦听）
- "Learning"（学习）
- "Blocking"（阻塞）
- "Forwarding"（传输）

侦听端口是指定端口或根端口，并处于转至传输状态的进程中。 但是，当端口处于传输状态后，将无法确定该端口是根端口还是指定端口。 RSTP 通过取消端口角色及其状态的耦合来解决此问题。 使用**"Spanning Tree Global Settings"（生成树全局设置）**页面可以启用 RSTP。

要打开**"Rapid Spanning Tree (RSTP)"（快速生成树 [RSTP]）**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）**。 系统将打开**"Rapid Spanning Tree (RSTP)"（快速生成树 [RSTP]）**页面。



快速生成树 (RSTP) 页面

"Rapid Spanning Tree (RSTP)"(快速生成树 [RSTP])页面包含以下字段:

- **"Interface"(接口)** — 表示启用 RSTP 的接口编号。
- **"Fast Link"(快速链路)** — 表示是否启用快速链路。

注: 快速链路可以在**"STP Port Settings"(STP 端口设置)**页面或**"STP LAG Settings"(STP LAG 设置)**页面中启用。 有关启用快速链路的详细信息,请参阅"定义 STP 端口设置"或"定义 STP LAG 设置"。

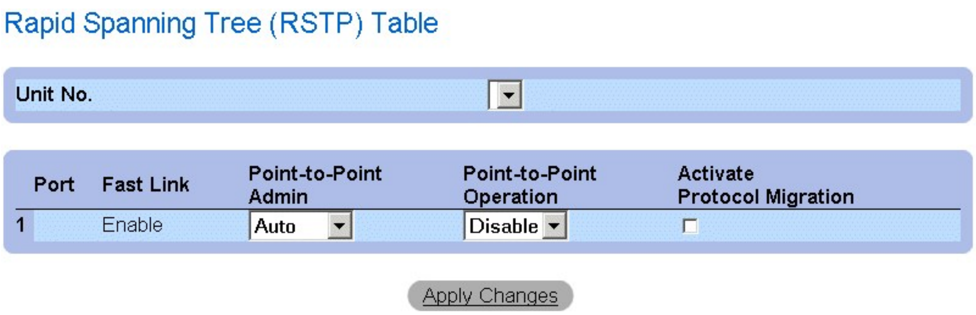
- **"Point-to-Point Admin"(点对点管理)** — 指定端口链路类型为点对点。
  可能的字段值包括:
  - **"Auto"(自动)** — 允许设备自动检测点对点链路。
  - **"Enable"(启用)** — 允许建立点对点链路。
  - **"Disable"(禁用)** — 禁止建立点对点链路。
- **"Point-to-Point Operational Status"(点对点运行状态)** — 表示点对点运行状态。
- **"Activate Protocol Migration"(激活协议迁移)** — 激活协议迁移。 协议迁移使协议可以通过检测端口来与相邻的交换机重新协商,以查看协议是否可以迁移至 RSTP。 可能的字段值包括:
  - **已选取** — 激活协议迁移。
  - **未选取** — 禁用协议迁移。

要启用快速 STP,请:

1. 打开**"Rapid Spanning Tree (RSTP)"(快速生成树 [RSTP])**页面。
2. 定义**"Point-to-Point Admin"(点对点管理)**、**"Protocol Operation"**

（协议运行）和 **“Activate Protocol Migration”（激活协议迁移）**字段。

3. 单击 **“Apply Changes”（应用更改）**。 系统将启用 RSTP，并更新设备。



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]）**页面中显示的定义 RSTP 参数的选项等效的 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（此操作由端口双工模式确定），并使快速生成树协议 (RSTP) 转为传输状态。
spanning tree mode {stp |rstp}	配置当前运行的 RSTP。
clear spanning-tree detected-protocols	重新启动协议迁移进程。
show spanning-tree [ethernet interface | port-channel port-channel-number]	显示 RSTP 配置。

以下是 CLI 命令实例：

```
Console(config)# interface ethernet 1/e5
```

```
Console(config-if)# spanning-tree link-type shared
```

配置 VLAN

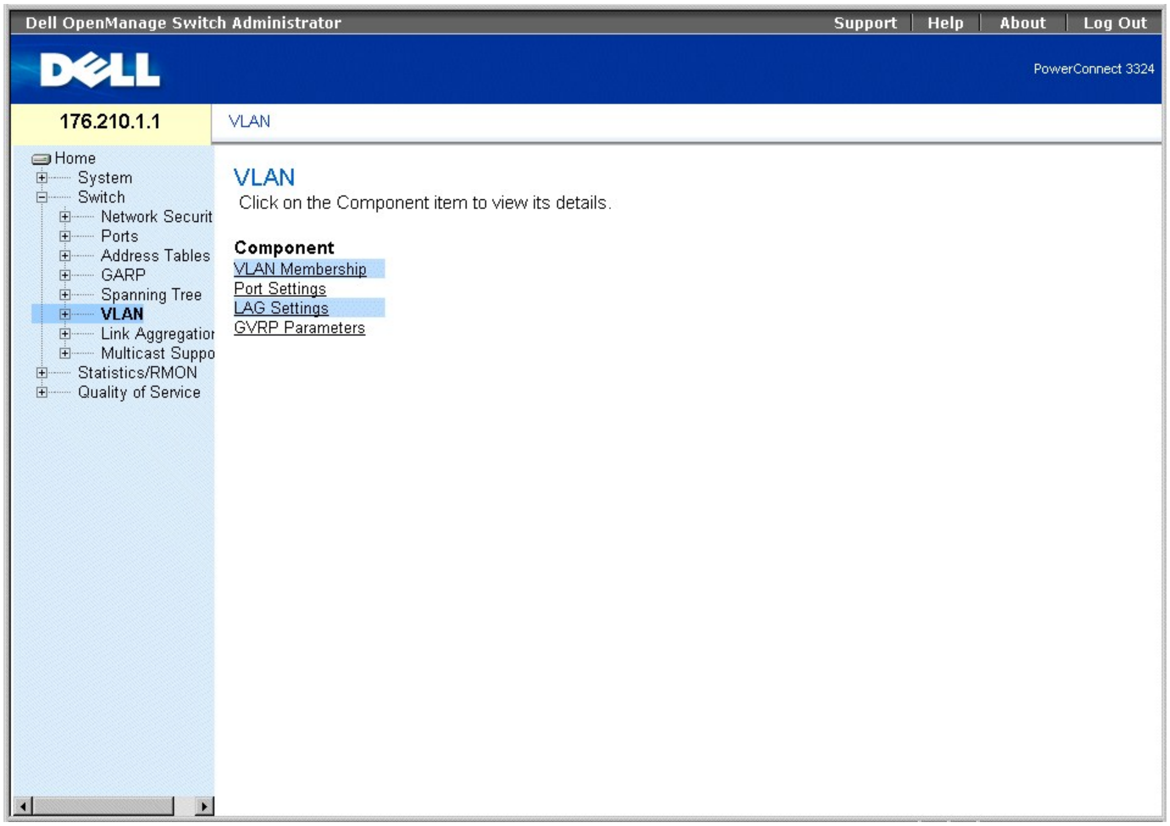
VLAN 是局域网 (LAN) 的逻辑子组，它是通过软件而不是通过定义硬件解决方案创建的。 VLAN 将用户站点和网络设备组合为单个域，而不考虑它们连接的物理 LAN 网段。 VLAN 使网络通信在子组内的传输更加有效。 通过软件管理的 VLAN 可减少执行网络更改所需的时间。

VLAN 基于软件，不是通过物理属性进行定义。 因此，VLAN 可以拥有无限数量的端口，
并且可以针对每个装置、每个设备、每个堆叠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 层安装可正常运行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 标记可以将一个四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信息包。 VLAN 标记还可以包含 VLAN 网络优先级信息。 组合 VLAN 和 GVRP 使网络管理员可以自动分散 VLAN 信息。要显示 **"VLAN"**页面，请：

- 在树视图中单击 **"Switch"（交换机）>"VLAN"**。 系统将打开 **"VLAN"**页面。



VLAN 页面

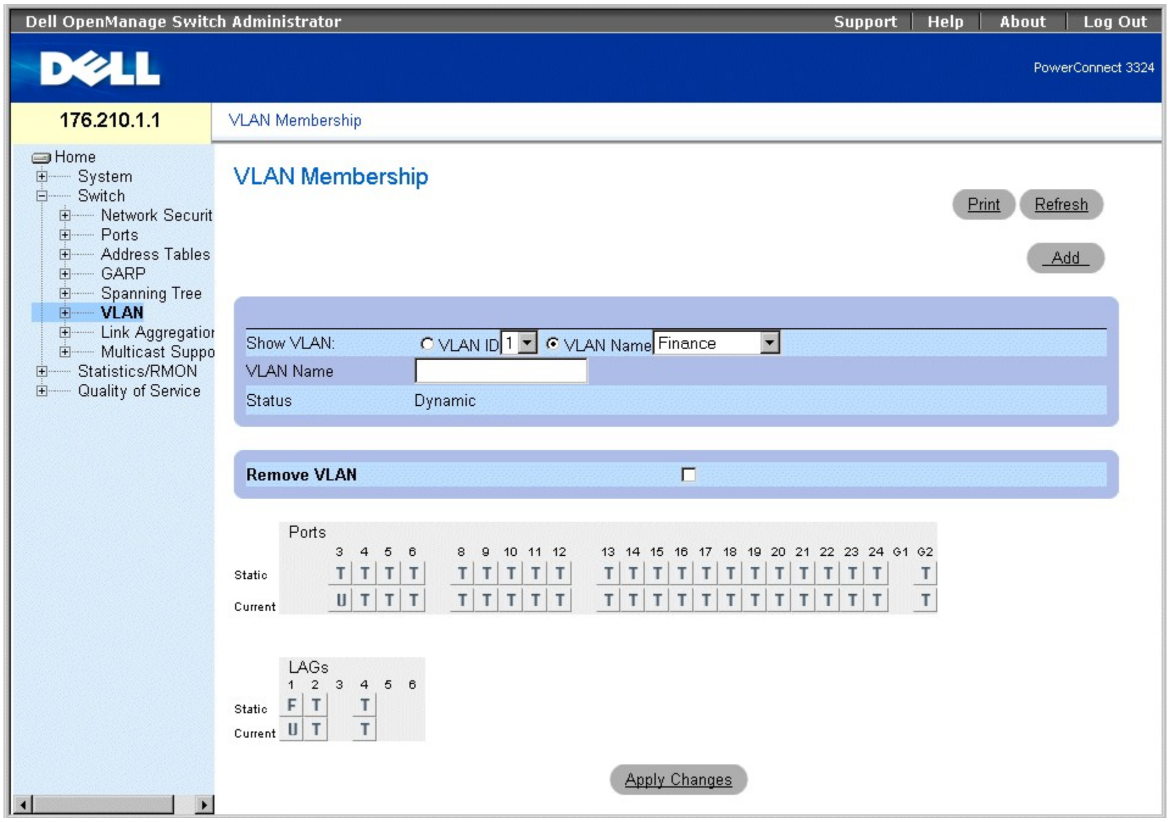
"VLAN"页面包含定义以下信息的链接：

- 定义 VLAN 成员
- 定义 VLAN 端口设置
- 定义 VLAN LAG 设置
- 配置 GVRP

定义 VLAN 成员

"VLAN Membership"（VLAN 成员关系） 页面使网络管理员可以定义 VLAN 组。 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）**。 系统将打开 **"VLAN Membership"（VLAN 成员关系）** 页面。



VLAN 成员关系页面

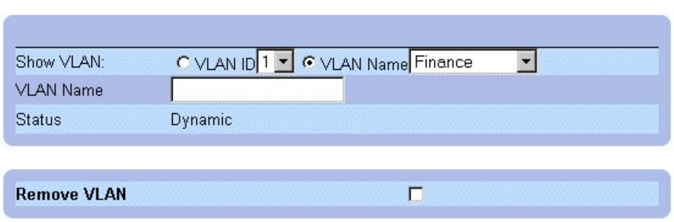
"VLAN Membership"（VLAN 成员关系）页面分为以下几个部分：

- VLAN 成员关系部分
- VLAN 端口成员关系表
- 定义 VLAN LAG 设置

VLAN 成员关系部分

VLAN 成员关系部分包含用于为端口分配 VLAN 成员关系的参数。 PowerConnect 3324/3348 最多支持 256 个 VLAN。

注： 所有端口必须具有已定义的 PVID。 如果未配置其它值，请使用默认的 VLAN PVID。



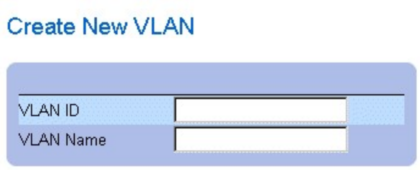
VLAN 成员关系部分

"VLAN Membership Section"（VLAN 成员关系部分）包含以下字段：

- **“Show VLAN”（显示 VLAN）**— 根据以下条件列出并显示特定 VLAN 信息：
  - **“VLAN ID”**— 按 VLAN ID 显示 VLAN。VLAN 的默认 ID 为 1。如果 VLAN 的 ID 是当前端口的端口默认 VLAN ID (PVID)，并且此 ID 已从端口删除，则端口 PVID 将被设置为 1。VLAN 编号 1 无法从系统中删除。 VLAN 的范围是 1 至 4095。VLAN 4095 是丢弃的 VLAN。
  - **“VLAN Name”（VLAN 名称）**— 根据 VLAN 名称显示 VLAN。
- **“VLAN Name”（VLAN 名称）**— 显示或定义 VLAN 的用户名。
- **“Status”（状态）**— 表示 VLAN 类型。 VLAN 可以由用户定义（永久），可以通过 GVRP 创建，也可以是默认的 VLAN。 可能的字段值包括：
  - **“Dynamic”（动态）**— 表示 VLAN 是通过 GVRP 动态创建的。
  - **“Static”（静态）**— 表示 VLAN 是由用户定义的。
  - **“Default”（默认）**— 表示 VLAN 是默认的 VLAN。
- **“Remove”（删除）**— 从 **“VLAN Membership Table”（VLAN 成员关系表）** 中删除 VLAN。 可能的字段值包括：
  - **已选取** — 从“VLAN Membership Table”（VLAN 成员关系表）中删除 VLAN 组。
  - **未选取** — 保留“VLAN Membership Table”（VLAN 成员关系表）中的 VLAN 组。

要添加新 VLAN，请：

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：



创建新 VLAN 页面

3. 定义 **“VLAN ID”** 和 **“VLAN Name”（VLAN 名称）** 字段。
4. 单击 **“Apply Changes”（应用更改）**。 系统将添加新 VLAN，并更新设备。

要修改 VLAN 名称组，请：

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. 修改 **“VLAN Name”（VLAN 名称）** 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。

要删除 VLAN，请：

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”（删除）** 复选框。

4. 单击**“Apply Changes”（应用更改）**。 系统将删除 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）**页面中显示的定义 VLAN 成员关系组的选项等效的 CLI 命令。

CLI 命令	**说明**
vlan database	进入接口配置 (VLAN) 模式。
vlan {VLAN 范围**}**	创建 VLAN。
name 字符串	为 VLAN 添加名称。

以下是 CLI 命令实例：

```
Console # vlan database

Console (config-switch)#

Console (config-switch)# vlan 1972

Console (config-switch)# exit

Console (config)# interface vlan 19

Console (config-if)# name Marketing
```

VLAN 端口成员关系表

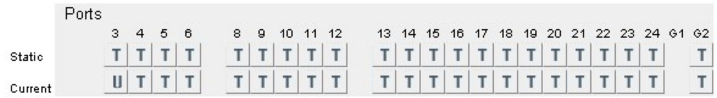
“VLAN Port Membership Table”（VLAN 端口成员关系表）包含用于为 VLAN 分配端口的端口表。 通过在端口控制设置之间进行切换可以为端口分配 VLAN 成员关系。 端口可以具有以下值：

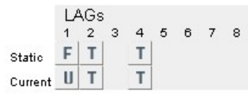
VLAN 端口成员关系控制设置

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	接口是此成员的成员。 通过接口传输的信息包均未标记。
F	通过 GVRP 否认接口是 VLAN 的成员。
空白	接口不是此 VLAN 的成员。 与 VLAN 相关联的信息包不被传输。

注： 属于 LAG 成员的端口不在“VLAN Port Membership Table”（VLAN 端口成员关系表）中显示。

“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。





VLAN 端口成员关系表

要为 VLAN 组分配端口，请：

1. 打开**“VLAN Membership”（VLAN 成员关系）**页面。
2. 从**“Show VLAN”（显示 VLAN）**下拉列表中选择 VLAN。
3. 在**“Port Membership Table”（端口成员关系表）**中选择端口，并指定端口值（**“v”**、**“t”**、**“f”**或**“b”**）。
4. 单击**“Apply Changes”（应用更改）**。 系统会将端口分配给 VLAN 组，并更新设备。

要删除 VLAN，请：

1. 打开**“VLAN Membership”（VLAN 成员关系）**页面。
2. 从**“Show VLAN”（显示 VLAN）**下拉列表中选择 VLAN。
3. 选取**“Remove”（删除）**复选框。
4. 单击**“Apply Changes”（应用更改）**。 系统将删除 VLAN 组，并更新设备。

使用 CLI 命令为 VLAN 组分配端口

下表概括了与**“VLAN Membership”（VLAN 成员关系）**页面中显示的为 VLAN 组分配端口的选项等效的 CLI 命令。

CLI 命令	**说明**
vlan database	进入接口配置 (VLAN) 模式。
vlan {VLAN 范围**}**	创建或删除 VLAN。
interface vlan VLAN ID	进入接口配置 (VLAN) 模式以配置现有 VLAN。
name 字符串	为 VLAN 添加名称。
interface range ethernet {端口范围 **| all}**	允许在多个端口同时执行命令。
switchport forbidden vlan {add vlan-list | remove vlan-list}	禁止向端口添加特定 VLAN

以下是 CLI 命令实例：

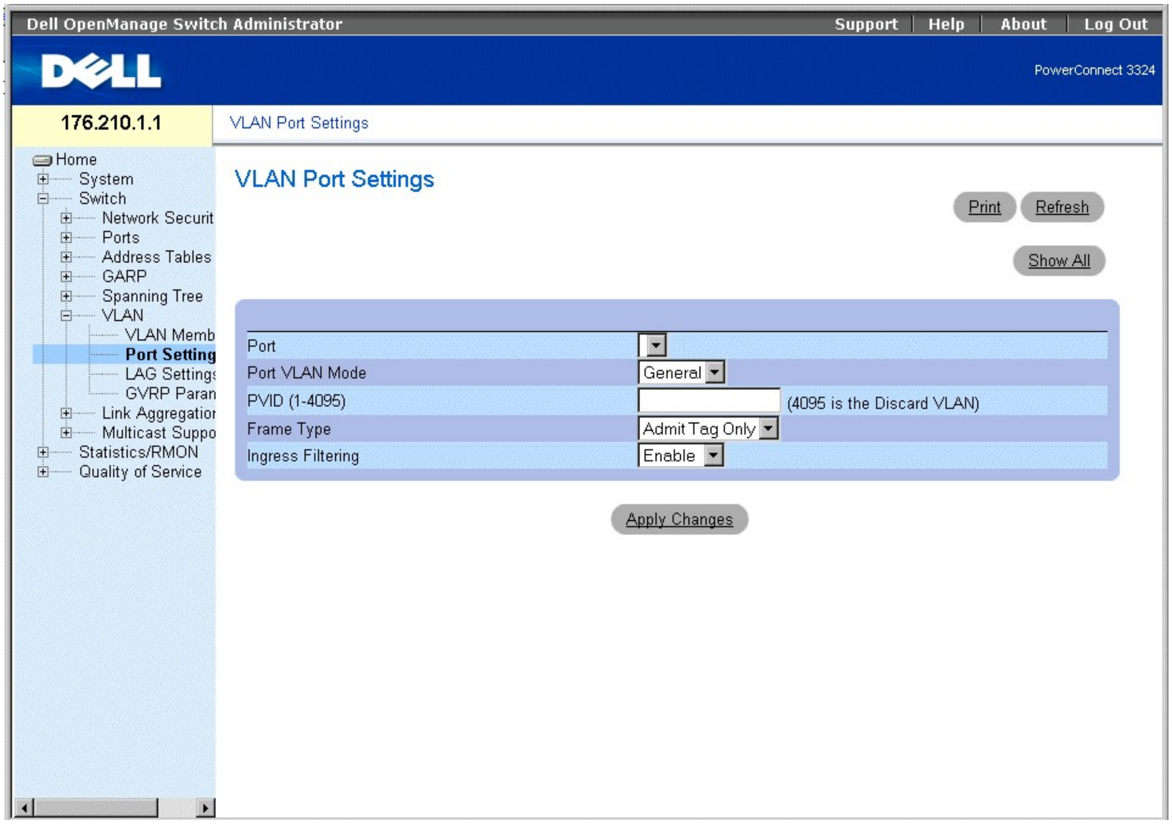
```
Console # vlan database

Console (config-vlan)# vlan 1972

Console (config-vlan)# exit

Console (config)# interface vlan 1972

Console (config-if)# name Marketing

Console (config-if)# exit

Console (config)# interface range ethernet 1/e18 - e20
```

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 的端口的参数。

"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）**。 系统将打开**"VLAN Port Settings"（VLAN 端口设置）**页面。



VLAN 端口设置页面

"VLAN Port Settings"（VLAN 端口设置）页面包含以下字段：

- **"Port"（端口）**— 表示 VLAN 中包含的端口号。
- **"Port VLAN Mode"（端口 VLAN 模式）**— 指定端口 LAN 模式。可能的字段值包括：
  - **"General"（常规）**— 表示端口属于一个或多个 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）。 只能在常规模式端口中禁用入口筛选。
  - **"Access"（访问）**— 表示端口属于单个未标记 VLAN。 将端口 VLAN 模式定义为访问表示端口接受所有未标记帧，以及所有使用当前设置为端口 PVID 的 VID 标记的帧。 访问模式端口旨在将终端站点连接至系统，特别是在终端站点不能生成 VLAN 标记时。 入口筛选已启用。
  - **"Trunk"（主干）**— 表示端口属于所有帧均将被标记的 VLAN。 在主干模式端口上可以启用入口筛选。
- **"PVID (1-4095)"**— 为未标记的信息包分配 VLAN ID。 只能为常规模式端口执行此操作。 可能的字段值范围是 1 至 4095。

注： VLAN 4095 是丢弃的 VLAN。

- **"Frame Type"（帧类型）**— 表示端口上接受的信息包类型。 可能的字段值包括：
  - **"Admit Tag Only"（仅接受标记）**— 表示端口仅接受已标记信息包。
  - **"Admit All"（全部接受）**— 表示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）**— 在端口上启用入口筛选。 入口筛选将丢弃与不包含入口端口的 VLAN 相关联的信息包。 可能的字段值包括：
  - **"Enable"（启用）**— 在端口上启用入口筛选。
  - **"Disable"（禁用）**— 在端口上禁用入口筛选。

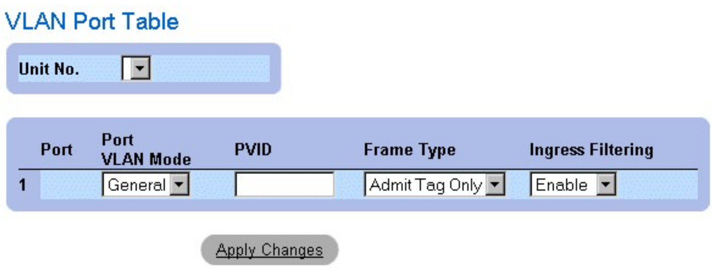
要设定端口设置，请：

注： 只能在设置为常规 VLAN 模式的端口上禁用入口筛选。

1. 打开 **“VLAN Port Settings”（VLAN 端口设置）** 页面。
2. 定义 **“Port Mode”（端口模式）**、**“PVID”**、**“Frame Type”（帧类型）** 和 **“Ingress Filtering”（入口筛选）** 字段。
3. 单击 **“Apply Changes”（应用更改）**。 系统将定义 VLAN 端口参数，并更新设备。

要显示 VLAN 端口表，请：

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）**。



VLAN 端口表

除了 **“VLAN Port Settings”（VLAN 端口设置）** 页面中的字段外， **“VLAN Port Table”（VLAN 端口表）** 页面还显示以下字段：

- **“Unit”（装置）** — 表示要显示 VLAN 端口信息的堆叠装置号。

使用 CLI 命令为 VLAN 组分配端口

下表概括了与 **“VLAN Port Settings”（VLAN 端口设置）** 页面中显示的为 VLAN 组分配端口的选项等效的 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。
switchport mode {access | trunk | general}	配置端口 VLAN 成员关系模式。
switchport general pvid VLAN ID	在接口处于常规模式时配置端口 VLAN ID (PVID)。
switchport general allowed vlan add VLAN 列表 **[tagged | untagged]**	向常规端口添加 VLAN。
switchport general allowed vlan remove VLAN 列表	从常规端口删除 VLAN。
switchport general ingress-filtering disable	

	禁用端口入口筛选。

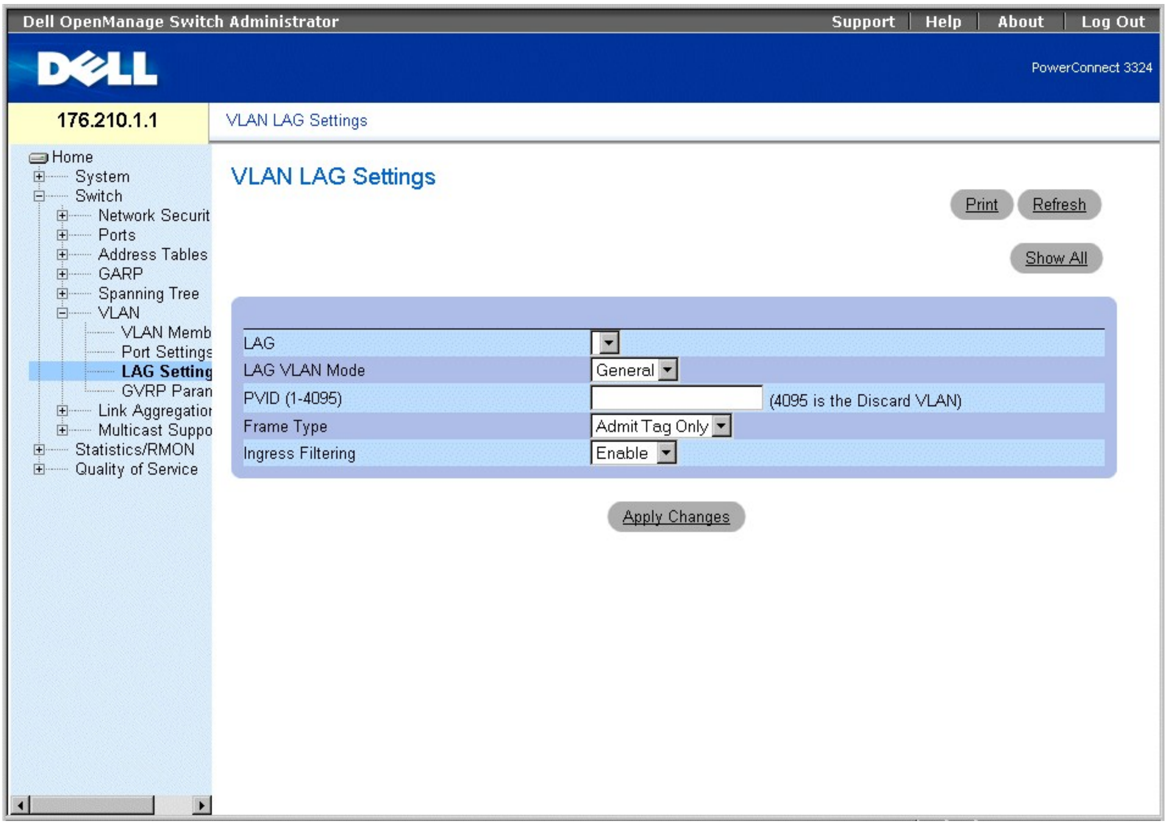
以下是 CLI 命令实例：

```
Console (config)# interface range ethernet 1/e18 - e20

Console (config-if)# switchport mode access

Console (config-if)# switchport general pvid 234

Console (config-if)# switchport general allowed vlan add 1,2,5,6 tagged

Console (config-if)# switchport general ingress-filtering disable
```

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 由各个端口或 LAG 组成。 进入 LAG 上交换机的未标记信息包按照 LAG 的 PVID 的指定进行标记。 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）**。 系统将打开**VLAN LAG Settings"（VLAN LAG 设置）**页面。



VLAN LAG 设置页面

"VLAN LACP Parameters"（VLAN LACP 设置）页面包含以下字段：

- **"LAG"**— 表示 VLAN 中包含的 LAG 号。
- **"Port Mode"（端口模式）**— 表示端口的模式。 可能的字段值包括：
  - **"General"（常规）**— 表示 LAG 属于一个或多个 VLAN，并且每个 VLAN 均由用户定义为已标记或未标记（完全兼容 802.1Q）。
  - **"Access"（访问）**— 表示 LAG 属于单个未标记 VLAN。
  - **"Trunk"（主干）**— 表示 LAG 属于所有帧都将被标记的 VLAN（可选单个固有 VLAN 除外）。
- **"PVID"**— 为未标记信息包分配 VLAN ID。 为了使 LAG 可以分配 PVID，必须在 **"VLAN Port Membership Table"（VLAN 端口成员关系表）**中将 LAG 定义为未标记。
- **"Frame Type"（帧类型）**— 表示 LAG 接受的信息包类型。 可能的字段值包括：
  - **"Admit Tag Only"（仅接受标记）**— 表示 LAG 仅接受已标记信息包。
  - **"Admit All"（全部接受）**— 表示 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）**— 按 LAG 启用入口筛选。 入口筛选将丢弃不包含入口端口的信息包。 可能的字段值包括：
  - **"Enable"（启用）**— 按 LAG 启用入口筛选。
  - **"Disable"（禁用）**— 按 LAG 禁用入口筛选。

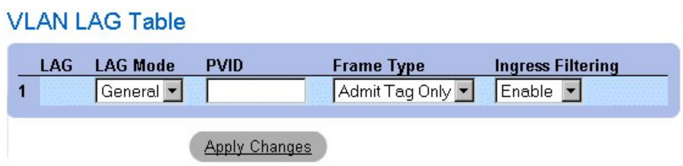
要设定 LAG 设置，请：

1. 打开 **"VLAN LAG Settings"（VLAN LAG 设置）**页面。
2. 定义 **"Port Mode"（端口模式）**、**"PVID"**、**"Frame Type"（帧类型）**和 **"Ingress Filtering"（入口筛选）**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。

要显示 VLAN LAG 表，请：

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）**。



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。

CLI 命令	**说明**
switchport mode {access | LAG | general}	配置端口 VLAN 成员关系模式。
switchport LAG native vlan VLAN ID	将 LAG 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 pvid VLAN ID	在接口处于常规模式时配置端口 VLAN ID (PVID)。
switchport general allowed vlan add VLAN 列表**[tagged | untagged]**	向常规端口添加 VLAN。
switchport general allowed vlan remove VLAN 列表**[tagged | untagged]**	从常规端口删除 VLAN。
switchport general acceptable-frame-types tagged-only	在入口丢弃未标记的帧。
switchport general ingress-filtering off	禁用端口入口筛选。

以下是 CLI 命令实例：

```
Console (config)# interface port channel 1 1/e8

Console (config-if)# switchport mode access

console (config-if)# switchport LAG native vlan 123

Console (config-if)# switchport general pvid 234

Console (config-if)# switchport general allowed vlan add 1,2,5,6 tagged
```

```
Console (config-if)# switchport general acceptable-frame-types tagged-only
```

```
Console (config-if)# switchport general ingress-filtering disable
```

配置 GVRP

GARP VLAN 注册协议 (GVRP) 协议专用于在可识别 VLAN 的网桥之间自动分配 VLAN 成员关系信息。 GVRP 使可识别 VLAN 的网桥能够自动学习 VLAN 与网桥端口的映射（而无需逐个配置每个网桥）并注册 VLAN 成员关系。

要使运行 GVRP 协议时的内存需求最小，需要将两个专用调节变量添加至标准变量：

- **"Maximum number of GVRP VLANs"（GVRP VLAN 的最大数目）**— 显示允许参与 GVRP 运行的 GVRP VLAN 的数目。
- **"Maximum number of GVRP VLANs after Reset"（重设后 GVRP VLAN 的最大数目）**— 为 GVRP VLAN 设置另一个值，并用于调节。 此值仅在重启动后才有效。

GVRP VLAN 的最大数目包括所有参与 GVRP 运行的 VLAN，无论其是静态还是动态。

通过设置重设后 GVRP VLAN 的最大数目来指定参与 GVRP 的 VLAN 的最大数目时，应考虑以下因素：

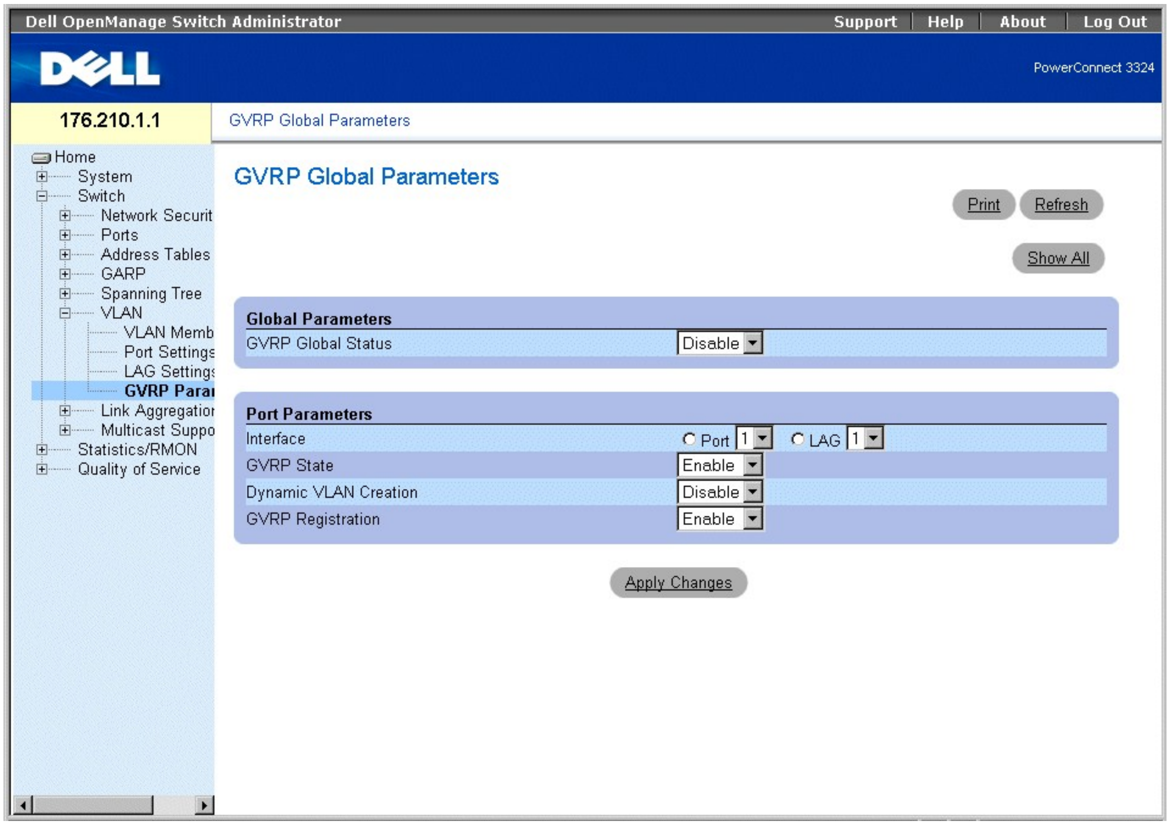
- 由于内存限制，默认的 GVRP VLAN 最大数目为 128。
- VLAN 的最大数目（通过最大 VLAN MIB 变量进行管理）会限制 GVRP VLAN 的最大数目。

为确保 GVRP 协议能够正常运行，建议用户将 GVRP VLAN 的最大数目设置为大大超出以下各值总和的值：

- 所有当前已配置和要配置的静态 VLAN 的数目。
- 所有当前已配置（动态 GVRP VLAN 的初始数目为 128）和要配置的、参与 GVRP 的动态 VLAN 的数目。

将 GVRP VLAN 的最大数目值增加到超出上述各值的总和时，用户便可以运行 GVRP，并且无需重设设备以接收更大数量的 GVRP VLAN。 例如，如果现在有三个 VLAN，并且要配置另外两个 VLAN（VLAN 静态或动态注册的结果），请将重设后 GVRP VLAN 的最大数目设置为 10。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）**。 系统将打开 **"GVRP Parameters"（GVRP 参数）**页面。



GVRP 参数页面

"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 GVRP。 可能的字段值包括：
  - **"Enabled"（已启用）**— 表示已在设备上启用 GVRP。
  - **"Disabled"（已禁用）**— 表示已在设备上禁用 GVRP。 此字段值为默认值。
- **"Interface"（接口）**— 表示要启用 GVRP 的特定接口。 可能的字段值包括：
  - **"Port"（端口）**— 表示要启用 GVRP 的特定端口。
  - **"LAG"**— 表示要启用 GVRP 的特定 LAG。
- **"GVRP State"（GVRP 状态）**— 表示端口上是否已启用 GVRP。 可能的字段值包括：
  - **"Enable"（启用）**— 在接口上启用 GVRP。
  - **"Disable"（禁用）**— 在接口上禁用 GVRP。 此为默认值。
- **"Dynamic VLAN Creation"（动态 VLAN 创建）**— 允许通过 GVRP 创建 VLAN。 可能的字段值包括：
  - **"Enable"（启用）**— 允许通过 GVRP 创建 VLAN。
  - **"Disable"（禁用）**— 禁止通过 GVRP 创建 VLAN。
- **"GVRP Registration"（GVRP 注册）**— 启用 GVRP 注册状态。 可能的字段值包括：
  - **"Enable"（启用）**— 允许通过 GVRP 注册 VLAN。
  - **"Disable"（禁用）**— 禁止通过 GVRP 注册 VLAN。

要在设备上启用 GVRP，请：

1. 打开**“GVRP Parameters”（GVRP 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。

要定义 GVRP 端口，请：

1. 打开**“GVRP Parameters”（GVRP 参数）**页面。

2. 单击**“Show All”（全部显示）**。 系统将打开**“GVRP Parameters”（GVRP 参数）**页面。 **“GVRP Port Parameters”（GVRP 端口参数）**包含用于在端口上启用 GVRP 的参数，以及允许端口通过 GVRP 参与 VLAN 注册的参数。 此外， **“GVRP Port Parameters Table”（GVRP 端口参数表）**还包含有关 VLAN 注册模式的信息。 还可以阻止特定端口进行注册或在 VLAN 中的使用。

3. 选择端口。

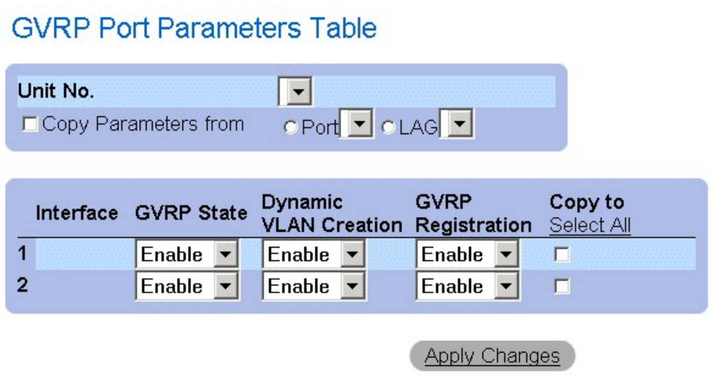
4. 定义**“GVRP State”（GVRP 状态）**、**“Dynamic VLAN Creation”（动态 VLAN 创建）**、**“VLAN Registration”（VLAN 注册）**和**“GVRP Registration”（GVRP 注册）**字段。

5. 单击**“Apply Changes”（应用更改）**。 系统将在端口上启用 GVRP，定义参数，并更新设备。

要显示 GVRP 端口参数表，请：

1. 打开**“GVRP Parameters”（GVRP 参数）**页面。

2. 单击**“Show All”（全部显示）**。 系统将打开**“GVRP Port Parameters Table”（GVRP 端口参数表）**。



GVRP 端口参数表

除了**“GVRP Parameters”（GVRP 参数）**页面中显示的字段外， **“GVRP Port Parameters Table”（GVRP 端口参数表）**页面还显示以下字段：

- **“Unit”（装置）**— 表示要显示 GVRP 信息的堆叠装置号。
- **“Copy Parameters From”（复制参数自）**— 表示从中复制 GVRP 参数的特定接口。
- **“Copy To”（复制到）**— 表示 GVRP 参数要复制到的端口。

使用 CLI 命令配置 GVRP

下表概括了与**“GVRP Parameters”（GVRP 参数）**页面中显示的配置 GVRP 的选项等效的 CLI 命令。

CLI 命令	说明

gvrp enable	全局启用 GVRP。
gvrp enable	在接口上启用 GVRP。
gvrp vlan-creation-forbid	启用或禁用动态 VLAN 创建。
gvrp registration-forbid	取消注册所有 VLAN，并禁止端口上的动态 VLAN 创建或注册。
show gvrp configuration [ethernet 接口| port-channel 端口通道号]	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。
gvrp max-vlan number	配置启用 GVRP 时 VLAN 的最大数目。

以下是 CLI 命令实例：

```
Console (config)# gvrp enable

Console (config)# interface ethernet 1/e8

Console (config-if)# gvrp enable

Console (config-if)# gvrp-vlan-creation-forbid

Console (config-if)# gvrp registration-forbid

Console# show interfaces configuration

GVRP Feature is currently enabled on the switch.

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

Port(s)Status Registration Dynamic VLAN Timers (milliseconds)

Creation Join Leave Leave All

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

2/1 Enabled Normal Enabled 200 600 10000

4/4 Enabled Normal Enabled 200 600 10000
```

聚合端口

端口聚合通过将一组端口链接在一起形成单个链路聚合组 (LAG) 来优化端口的使用。 端口聚合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。 PowerConnect 3324 和 PowerConnect 3348 最多支持六个 LAG，并支持每个 LAG、每个堆叠或独立装置八个端口。

每个 LAG 由具有相同速率的端口组成，并被设置为全双工运行。 LAG 中的端口可以是各种介质类型（UTP/光纤或其它光纤类型），只要它们都以相同速率运行。

通过在相关链路上启用链路聚合控制协议 (LACP)，可以手动分配或自动分配聚合链路。 PowerConnect 3324/3348 根据源 MAC 地址和目的地 MAC 地址提供 LAG 负载平衡。

系统将聚合链路用作单个逻辑端口。 需要特别注意的是，聚合链路具有与非聚合端口类似的端口属性，包括自动协商、速率和双工设置等。

PowerConnect 3324/3348 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。

对于独立配置或堆叠配置，在向 LAG 添加端口时，请遵循以下原则：

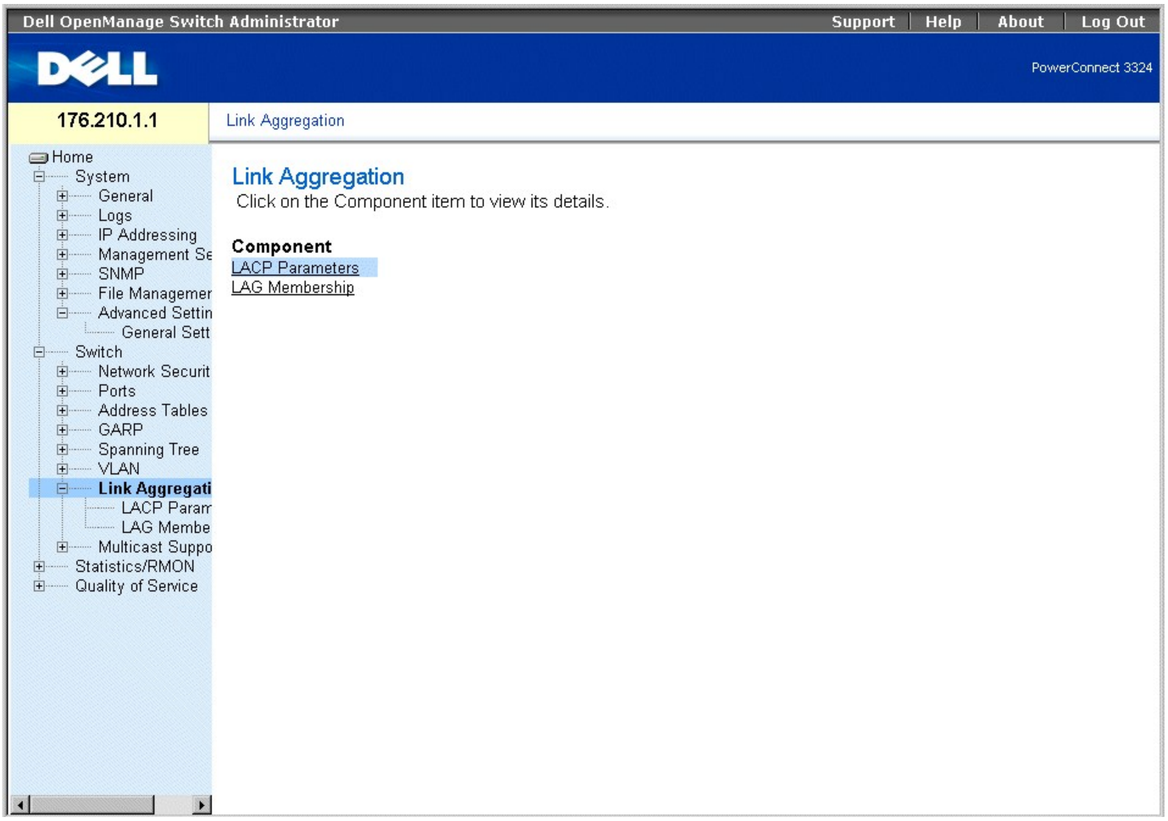
- 端口上未定义第 3 层接口。
- 端口不属于任何 VLAN。
- 端口不属于任何其它 LAG。
- 端口不是镜像端口。
- 端口的 802.1p 优先级等于 LAG 的 802.1p 优先级。
- 端口上未定义 ACL。
- 端口上未禁用 QoS 信任。
- 未启用 GVRP。

注： 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。

PowerConnect 3324/3348 使用哈希函数确定在聚合链路成员上传输的帧。 哈希函数以统计学方式在聚合链路成员之间平衡负载。 PowerConnect 3324/3348 将聚合链路看作单个逻辑端口。

每个聚合链路具有一个聚合链路端口类型，包括吉位以太网端口和高速以太网端口。 仅当端口具有相同的端口类型时，才能将其添加至聚合链路。 将端口从聚合链路删除时，端口将恢复为原始端口设置。 要打开 **“Link Aggregation”（链路聚合）**页面，请：

- 在树视图中单击 **“Switch”（交换机）>"Link Aggregation"（链路聚合）**。
  系统将打开 **“Link Aggregation”（链路聚合）**页面。



链路聚合页面

本节包括以下主题：

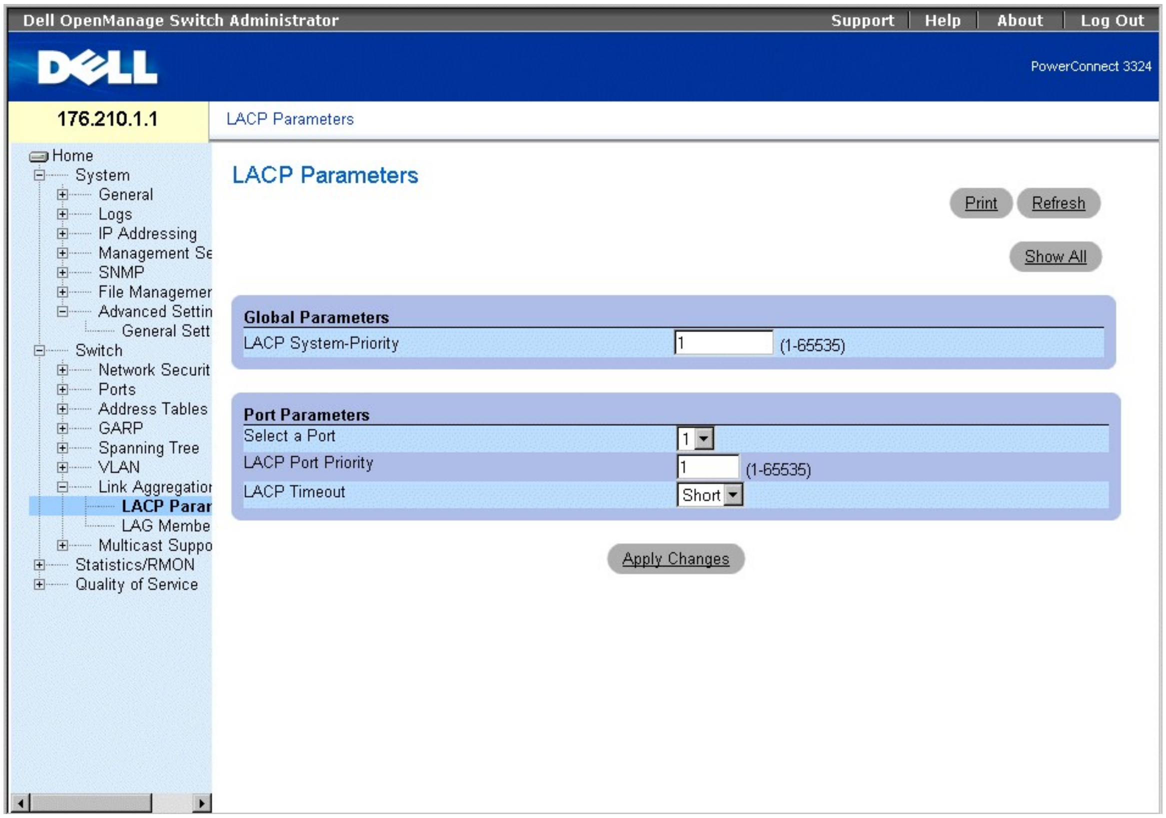
- 定义 LACP 参数
- 定义 LAG 成员关系

定义 LACP 参数

"LACP Parameters"（LACP 参数）页面包含用于配置 LACP LAG 的信息。 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）**。 系统将打开 **"LACP Parameters"（LACP 参数）**页面。



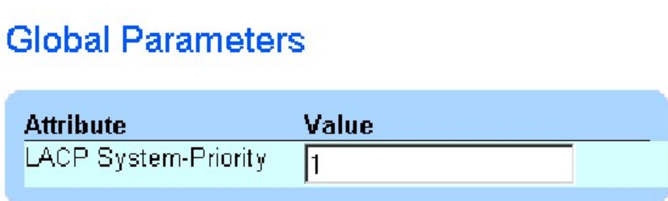
LACP 参数页面

"LACP Parameters"（LACP 参数）页面包含以下部分：

- 全局参数
- 端口参数表

全局参数

"Global Parameters"（全局参数）包含用于分配 LACP 优先级的信息。 聚合端口可以被链接至链路聚合端口组。 LAG 可以通过用户明确设定进行分配手动设置，也可以通过在相关 LAG 上启用链路聚合控制协议 (LACP) 自动设置。



全局参数

"Global Parameters"（全局参数）部分包含以下字段：

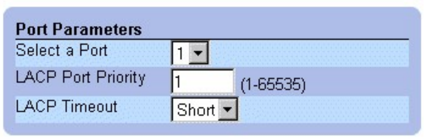
- **"LACP System Priority"（LACP 系统优先级）**— 表示 LACP 的优先级值。
  可能范围为 1 至 65535。默认值为 1。

要定义全局参数，请：

1. 打开**“LACP Parameters”（LACP 参数）**页面。
2. 滚动浏览至**“Global Parameters”（全局参数）**部分。
3. 定义**“LACP System Priority”（LACP 系统优先级）**和**“LACP Timeout”（LACP 超时）**字段。
4. 单击**“Apply Changes”（应用更改）**。 系统将定义全局参数，并更新设备。

端口参数表

“Port Parameters”（端口参数）包含用于向端口分配 LACP 优先级和超时值的信息：



端口参数表

“Port Parameters”（端口参数）表包含以下字段：

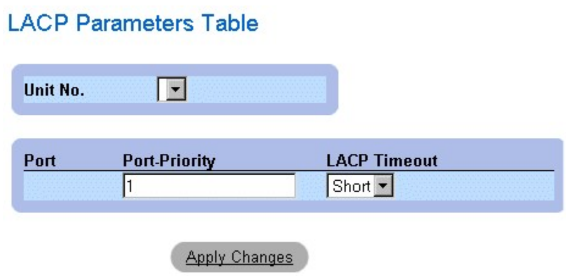
- **“Select Port”（选择端口）**— 表示端口号。
- **“LACP Port Priority”（LACP 端口优先级）**— 表示 LACP 端口优先级值。 默认值为 1。
- **“LACP Timeout”（LACP 超时）**— 设定管理性 LACP 超时。可能的字段值包括：
  - **“Short”（短）**— 指定短超时值。
  - **“Long”（长）**— 指定长超时值。

要定义端口参数，请：

1. 打开**“LACP Parameters”（LACP 参数）**页面。
2. 滚动浏览至**“Link Aggregation Port Parameters Table”（链路聚合端口参数表）**。
3. 定义**“LACP System Priority”（LACP 系统优先级）**和**“LACP Timeout”（LACP 超时）**字段。
4. 单击**“Apply Changes”（应用更改）**。 系统将定义链路聚合全局参数，并更新设备。

要显示 LACP 参数表，请：

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）**。



LACP 参数表

除了**“LACP Parameters”（LACP 参数）**页面中的字段外，**“LACP Parameters Table”（LACP 参数表）**页面还显示以下字段：

- **“Unit”（装置）**— 表示要显示 LACP 信息的堆叠装置号。

使用 CLI 命令配置 LACP 参数

下表概括了与**“Link Aggregation”（链路聚合）**页面中显示的配置 LACP 参数的选项等效的 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。
show lacp port-channel **[port_channel_number]**	显示端口通道的 LACP 信息。

以下是 CLI 命令实例：

```
Console (config)# lacp system-priority 120

Console (config)# interface ethernet 1/e8

Console (config-if)# lacp port-priority 247

Console (config-if)# lacp timeout long

Console (config-if)# exit

Console# show lacp ethernet 1/e1 statistics

Port 1/e1 LACP Statistics:
```

LACP PDUs sent:2

LACP PDUs received:2

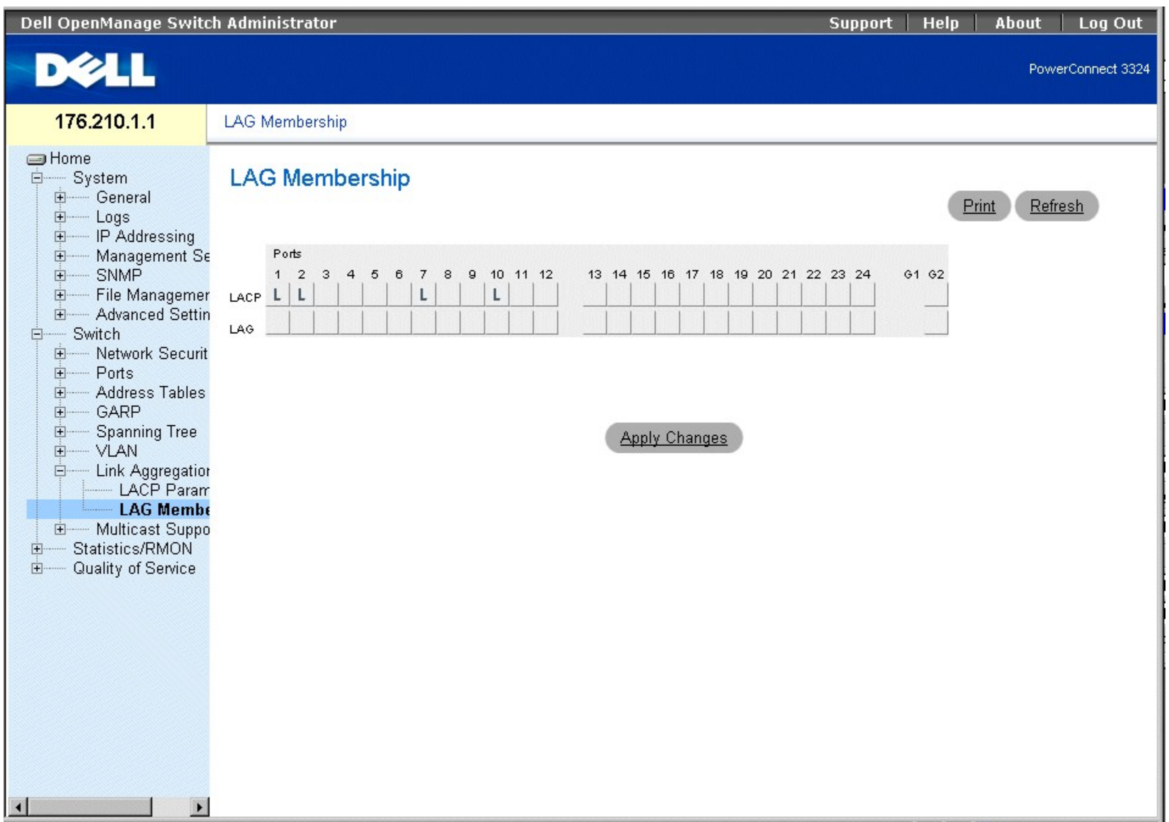
定义 LAG 成员关系

"LAG Membership"（LAG 成员关系）页面使网络管理员可以为 LAG 分配端口。 LAG 最多可以包含 8 个端口。 无论设备是独立设备还是位于堆叠中，PowerConnect 3324/3348 目前可支持每个系统 6 个 LAG。 **"LAG Membership Table"（LAG 成员关系表）**包含以下行：

- **"LACP"**— 通过允许端口成为 LAG 成员来表示端口是否为动态端口。
- **"LAG"** 向 LAG 添加端口，并表示端口所属的特定 LAG。

要打开**"LAG Membership"（LAG 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）选项卡。 系统将打开**"LAG Membership"（LAG 成员关系）**页面。



LAG 成员关系页面

要向 LAG 添加端口，请：

1. 打开**"LAG Membership"（LAG 成员关系）**页面。

2. 在端口号下进行切换以分配 LAG 设置和编号。
3. 单击 **“Apply Changes”（应用更改）**。 系统会将端口添加至 LAG，并更新设备。

使用 CLI 命令向 LAG 分配端口

下表概括了与 **“LAG Membership”（LAG 成员关系）**页面中显示的为 LAG 分配端口的选项等效的 CLI 命令。

CLI 命令	说明
channel-group port-channel-number mode {on | auto}	将端口配置为端口通道。
show interface port_channel	显示连接至 LAG 的接口。

以下是 CLI 命令实例：

```
Console# channel-group port-channel-number mode on auto 1

Port-Channel 1:Port Type 1000 Ethernet

Actor

System Priority:1

MAC Address: 000285:0E1C00

Admin Key: 29

Oper Key: 29

Partner

System Priority:0

MAC Address: 000000:000000

Oper Key: 14
```

多点传送支持

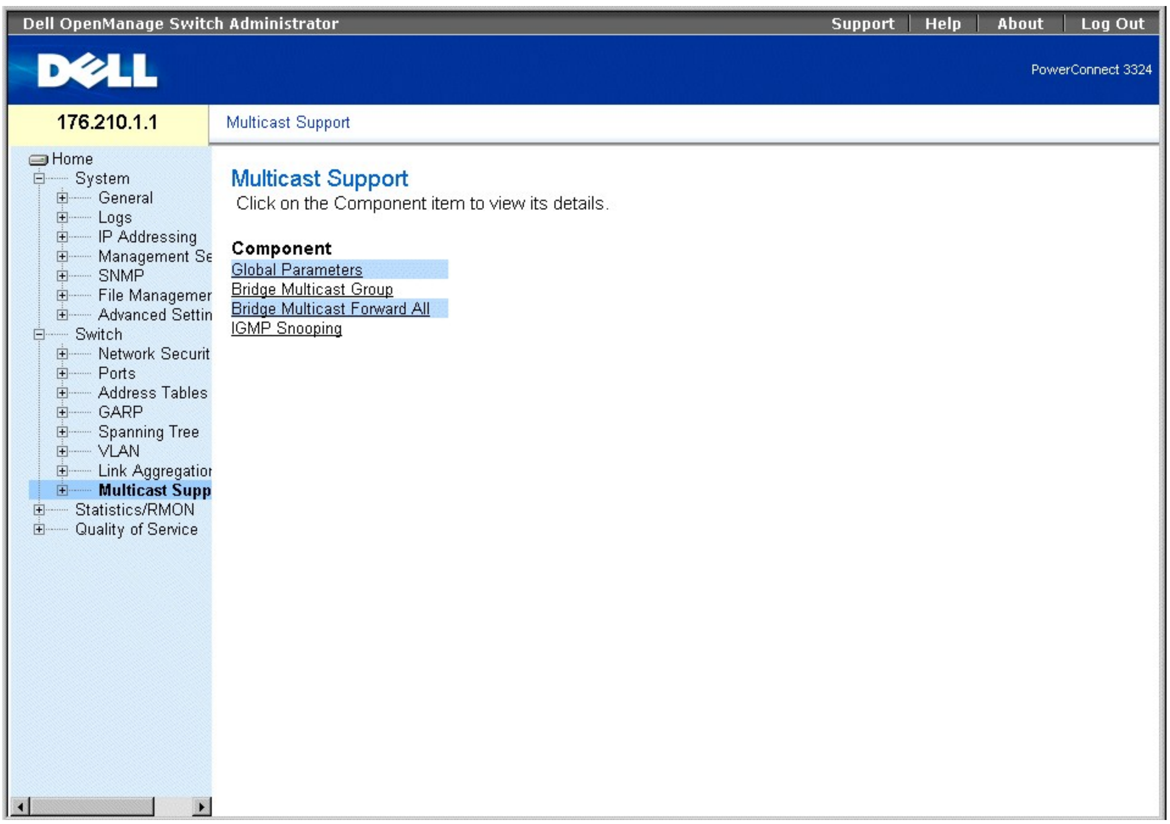
多点传送使单个信息包可以传输至多个目的地。 L2 多点传送服务基于接收定址到特定多点传送地址的单个信息包的 L2 交换机。 多点传送可以创建信息包副本，然后将这些信息包传输至相关的端口。

PowerConnect 3324/3348 支持：

- **"Forwarding L2 Multicast Packets"（传输 L2 多点传送信息包）**— 默认情况下处于启用状态。
- **"Filtering L2 Multicast Packets"（筛选 L2 多点传送信息包）**— 允许向端口 VLAN 传输 L2 信息包。 如果禁用了多点传送筛选，则多点传送信息包将传输至所有相关的 VLAN 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）**。 系统将打开**"Multicast Support"（多点传送支持）**页面。



多点传送支持页面

"Multicast Support"（多点传送支持）页面包括指向以下主题的链接：

- 定义 IGMP 监测设置
- 添加网桥多点传送组成员
- 设定全部多点传送参数
- 启用 IGMP 监测

定义 IGMP 监测设置

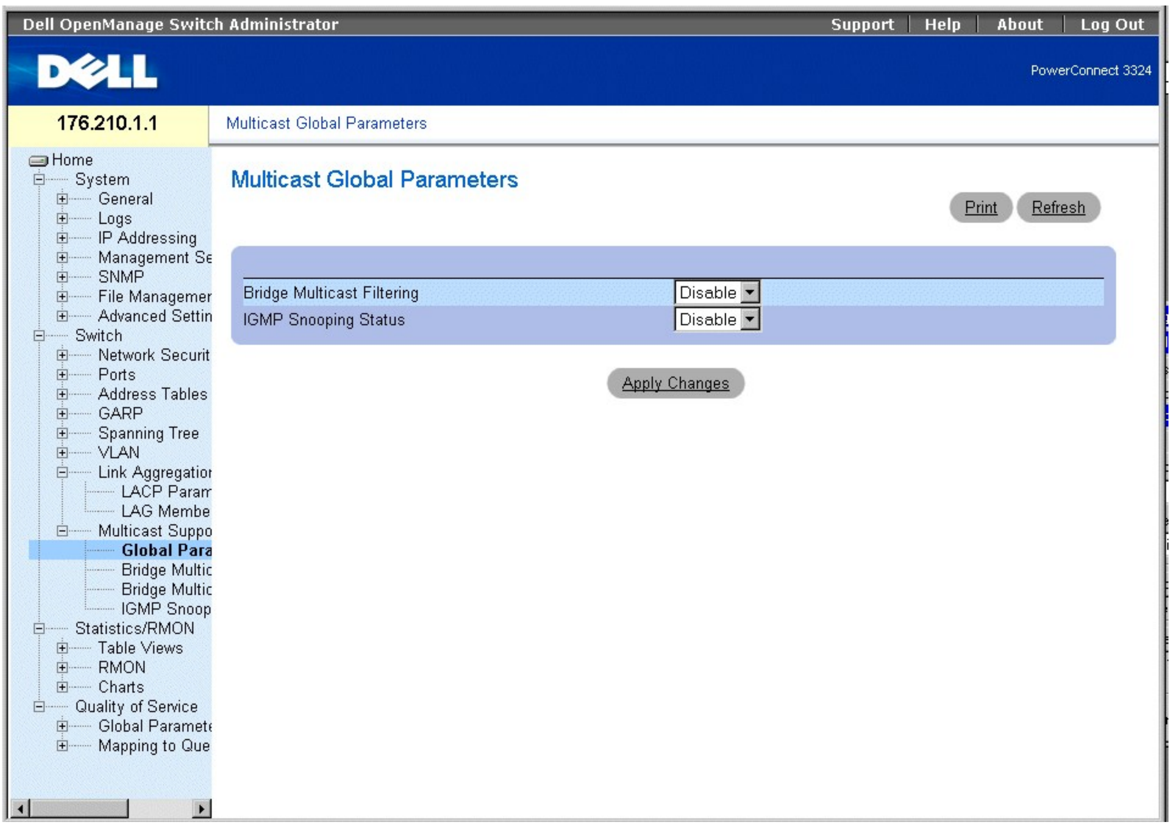
默认情况下，第 2 层交换机向所有相关 VLAN 端口传输多点传送信息包，即将信息包作为多点传送信息包处理。 此类通信传输可以正常进行，但是不相关的端口也会收到多点传送通信，
从而导致网络通信量增加。

通过在 IGMP 帧从站点传输至多点传送路由器时检查 IGMP 帧，IGMP 监测可以消除不必要的多点传送通信。

全局启用 IGMP 监测时，交换 ASIC 将被设置为向 CPU 传输所有 IGMP 帧。 CPU 将分析传入的帧，并确定要加入多点传送组的端口、具有生成 IGMP 查询的多点传送路由器的端口，以及传输信息包和多点传送通信的路由协议。 要加入特定多点传送组的端口将发出 IGMP 报告，以指明该多点传送组。

"Multicast Global Parameters"（多点传送全局参数）页面使网络管理员可以在设备上全局启用 IGMP 监测和多点传送筛选。 要打开**"Multicast Global Parameters"（多点传送全局参数）**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）**。 系统将打开**"Multicast Global Parameters"（多点传送全局参数）**页面。



多点传送全局参数页面

Multicast Global Parameters（多点传送全局参数）页面包含以下字段：

- **"Bridge Multicast Filtering"（网桥多点传送筛选）**－ 表示是否在设备上启用网桥多点传送筛选。 可能的字段值包括：
  - **"Enabled"（已启用）**－ 在设备上启用网桥多点传送筛选。
  - **"Disabled"（已禁用）**－ 在设备上禁用网桥多点传送筛选。 此为默认值。
- **"IGMP Snooping Status"（IGMP 监测状态）**－ 表示是否在设备上启用 IGMP 监测。 可能的字段值包括：

- **"Enabled"（已启用）**— 在特定 VLAN 上启用 IGMP 监测。
- **"Disabled"（已禁用）**— 在特定 VLAN 上禁用 IGMP 监测。 此为默认值。

要在设备上启用网桥多点传送筛选，请：

1. 打开**"Multicast Global Parameters"（多点传送全局参数）**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 **"Bridge Multicast"（网桥多点传送）**。

要在设备上启用 IGMP 监测，请：

1. 打开**"Multicast Global Parameters"（多点传送全局参数）**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 命令启用多点传送和 IGMP 监测

下表概括了与**"Multicast Support"（多点传送支持）**页面中显示的启用多点传送和 IGMP 监测的选项等效的 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 Internet 成组管理协议 (IGMP) 监测。

以下是 CLI 命令实例：

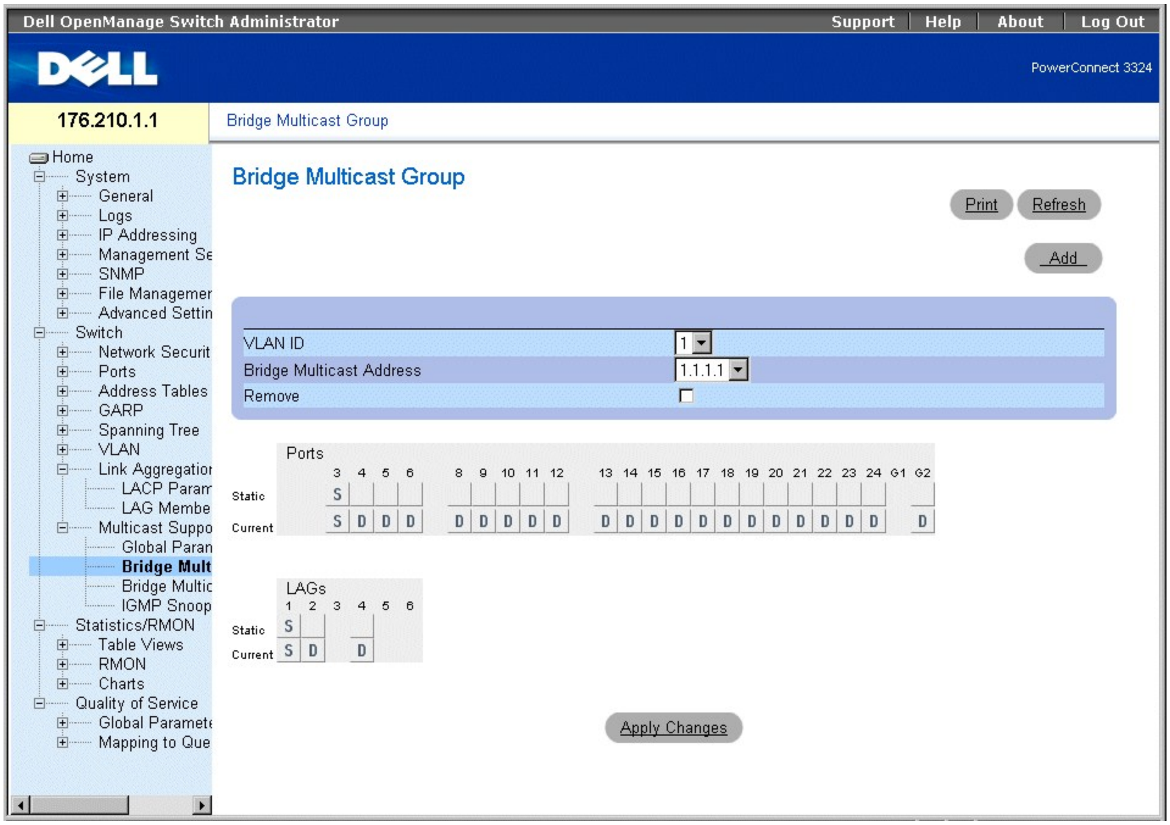
```
Console (config)# bridge multicast filtering
```

```
Console (config)# ip igmp snooping
```

添加网桥多点传送组成员

"Bridge Multicast Group"（网桥多点传送组）页面在**"Port"（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 表也可以反映端口或 LAG 加入多点传送组的方式。 端口可以添加至现有组，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）**页面还可以向特定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）**。 系统将打开**"Bridge Multicast Group"（网桥多点传送组）**页面。

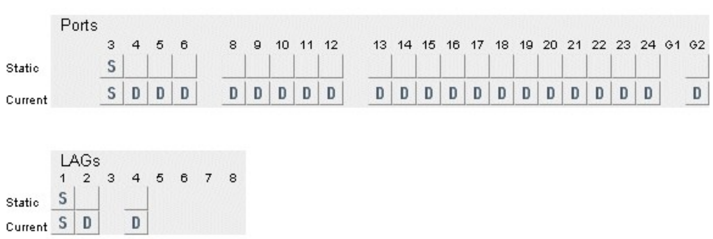


网桥多点传送组页面

"Bridge Multicast Group"（网桥多点传送组）页面包含以下字段：

- **"VLAN ID"**— 标识 VLAN。
- **"Bridge Multicast Address"（网桥多点传送地址）**— 标识多点传送组 IP 地址。
- **"Remove"（删除）**— 删除按地址指定的网桥多点传送组。
  - **已选取** — 删除网桥多点传送地址。
  - **未选取** — 保留网桥多点传送地址。
- **"Ports Table"（端口表）**— 列出可以添加至多点传送服务的端口。
- **"LAGs Table"（LAG 表）**— 列出可以添加至多点传送服务的 LAG。

The **"IGMP Port Members Table"（IGMP 端口成员表）/"IGMP LAG Members Table"（IGMP LAG 成员表）**图显示了 IGMP 端口/LAG 成员状态。



IGMP 端口/LAG 成员表

IGMP 端口/LAG 成员表控制设置表包含用于管理 IGMP 端口和 LAG 成员的设置。

端口控制	定义
D	表示端口/LAG 已动态加入 **“Current”（当前）**行中的多点传送组。
S	将端口作为 **“Static”（静态）**行中的静态成员连接至多点传送组。 表示端口/LAG 已静态加入 **“Current”（当前）**行中的多点传送组。
F	表示禁止端口加入此多点传送组。
空白	表示端口未连接至多点传送组。

IGMP 端口/LAG 成员表控制设置

要定义端口以接收多点传送服务，请：

1. 打开 **“Bridge Multicast”（网桥多点传送）**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”** 以使端口加入选定的多点传送组，或将端口切换为 **“F”**以禁止端口加入该多点传送组。
4. 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。

要分配 LAG 以接收多点传送服务，请：

1. 打开 **“Bridge Multicast”（网桥多点传送）**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”**以使 LAG 加入选定的多点传送组，或将端口切换为 **“F”**以禁止端口加入多点传送组。
4. 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）**页面中显示的管理多点传送服务成员的选项等效的 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**} {add | remove} {ethernet** 接口列表 **| port-channel** 端口通道号列表**}**	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。
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 命令实例：

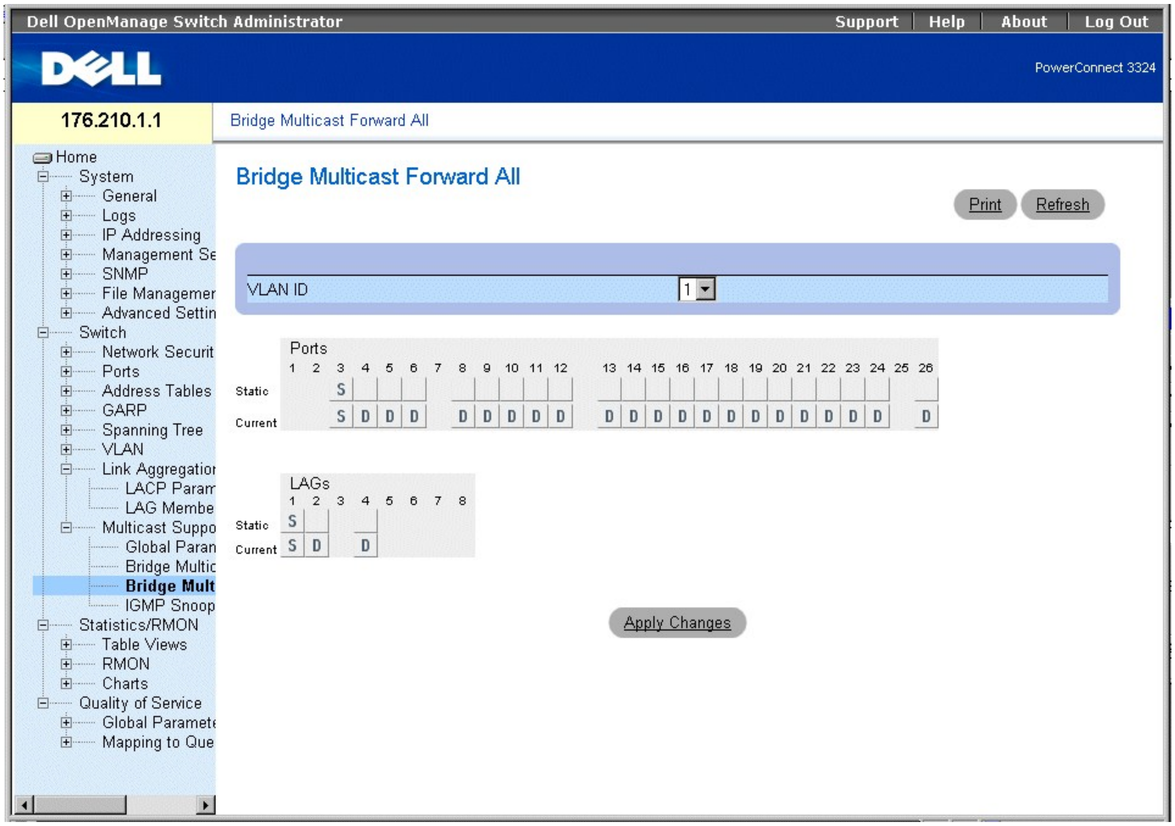
```
Console (config)# interface vlan 8

bridge multicast address 0100.5e02.0203

bridge multicast address 0100.5e02.0203 add ethernet 1/e1, 2/e2
```

```
Console (config-if)# Exit

Console # show bridge multicast address-table


Vlan MAC Address type Ports

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

1 0100.5e02.0203 static 1/e1, 2/e2

19 0100.5e02.0208 static 1/e1-8

19 0100.5e02.0208 dynamic 1/e9-11


Forbidden ports for multicast addresses:

Vlan MAC Address Ports

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

1 0100.5e02.0203 2/e8

19 0100.5e02.0208 2/e8
```

设定全部多点传送参数

"Bridge Multicast Forward All"（网桥全部多点传送）页面使网络管理员可以将端口或 LAG 连接至相邻多点传送路由器/交换机所连接的交换机。 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。

- 在树视图中单击**"Switch"（交换机）>"Multicast Support"（多点传送支持）>"Bridge Multicast"（网桥多点传送）>"Bridge Multicast Forward All"（网桥全部多点传送）**选项卡。 系统将打开**"Bridge Multicast Forward All"（网桥全部多点传送）**页面。



网桥全部多点传送页面

"Bridge Multicast Forward All"（网桥全部多点传送）页面包含以下字段：

- **"VLAN ID"**— 标识帧 VLAN，并包含有关多点传送组地址的信息。
- **"Ports Table"（端口表）**— 列出可以添加至多点传送服务的端口。
- **"LAGs Table"（LAG 表）**— 列出可以添加至多点传送服务的 LAG。

"Bridge Multicast Forward All"（网桥全部多点传送）页面包含用于管理交换机和端口设置的设置。

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	表示禁止端口加入多点传送组。
空白	表示端口未连接至多点传送路由器或交换机。

网桥全部多点传送路由器/端口控制设置

要将端口连接至多点传送路由器或交换机，请：

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**"Multicast Router Port Table"（多点传送路由器端口表）**中选择一个端口，并设定端口值。
4. 单击**"Apply Changes"（应用更改）**。 系统将更新连接至多点传送路由器或组的端口。

要将 LAG 连接至多点传送路由器或交换机，请：

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 **“Multicast Router Port Table”（多点传送路由器端口表）**中选择一个 LAG，并设定 LAG 的值。
4. 单击 **“Apply Changes”（应用更改）**。 系统将更新连接至多点传送路由器或组的 LAG。

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。

CLI 命令	说明
show bridge multicast filtering *VLAN ID*	显示多点传送配置。
bridge multicast forbidden forward-all	禁止在端口上传输多点传送信息包。
bridge multicast forward-all {add | remove} {ethernet interface-list | port-channel port-channel-number-list}	允许在端口上传输所有多点传送信息包。

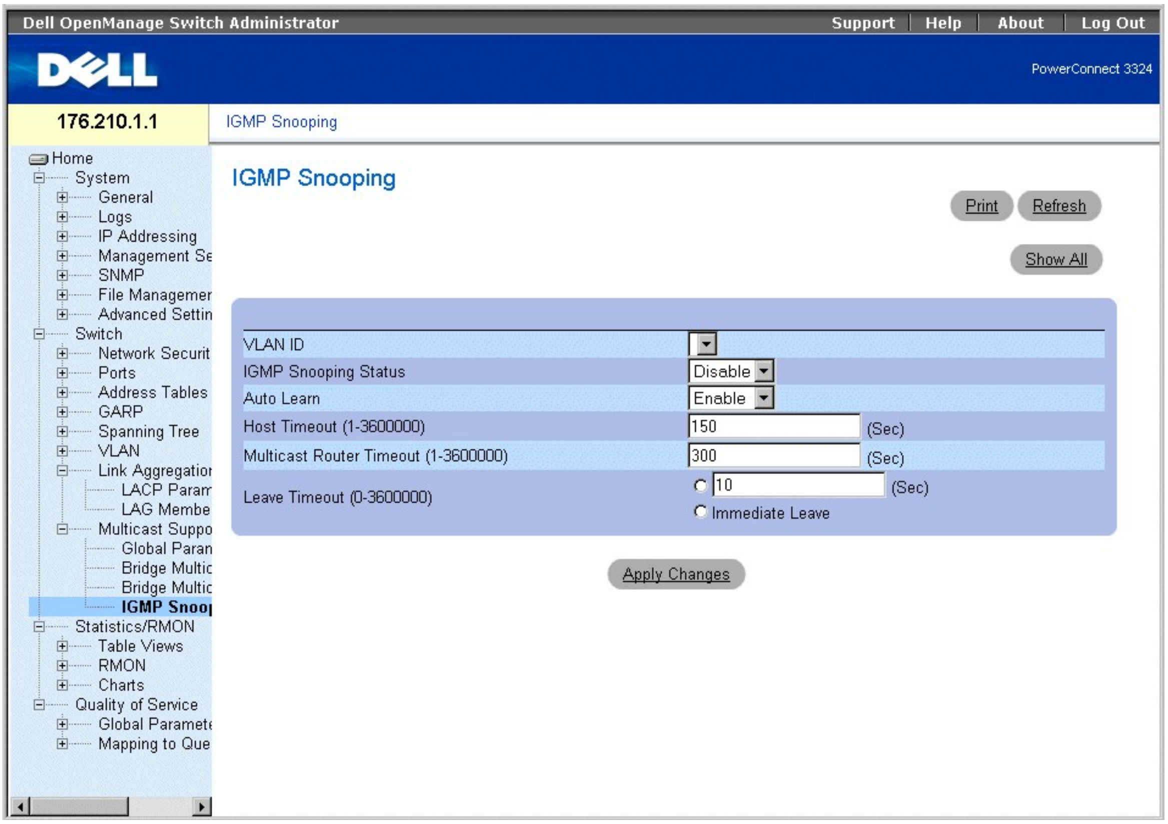
以下是 CLI 命令实例：

```
Console # show bridge multicast filtering

Filtering: Enabled

VLAN: 1

Port Forward-All

Static Status

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

1/e1 Forbidden Filter

1/e2 Forward Forward(s)

1/e3 - Forward(s)
```

启用 IGMP 监测

"IGMP Snooping"（IGMP 监测）页面使网络管理员可以添加 IGMP 成员。 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）**。 系统将打开 **"IGMP Snooping"（IGMP 监测）**页面。



IGMP 监测页面

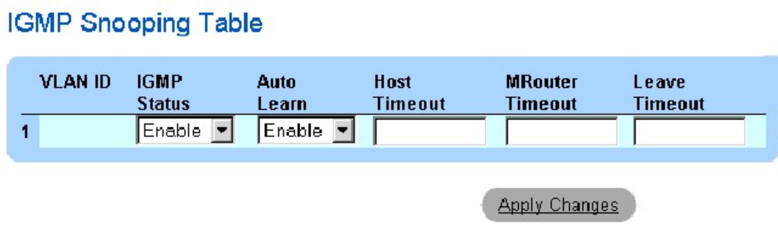
"IGMP Snooping"（IGMP 监测）页面包含以下信息：

- **"VLAN ID"**— 指定 VLAN ID。
- **"IGMP Snooping Status"（IGMP 监测状态）**— 在设备上启用 IGMP 监测。 可能的字段值包括：
  - **"Enable"（启用）**— 在设备上启用 IGMP 监测。
  - **"Disable"（禁用）**— 在设备上禁用 IGMP 监测。
- **"Auto Learn"（自动学习）**— 允许自动学习新多点传送组成员。 可能的字段值包括：
  - **"Enable"（启用）**— 允许自动学习新多点传送组成员。
  - **"Disable"（禁用）**— 禁止自动学习新多点传送组成员。
- **"Host Timeout (1-3600000)"（主机超时 [1-3600000]）**— 表示 IGMP 监测条目过期前的时间。 默认时间为 **"150"**秒。
- **"Multicast Router Timeout (1-3600000)"（多点传送路由器超时 [1-3600000]）**— 表示多点传送路由器条目过期前的时间。 默认值为 **"300"**秒。
- **"Leave Time Out (1-3600000)"（离开超时 [1-3600000]）**— 指定在收到端口离开信息之后、条目过期之前的时间（以秒为单位）。 可能的字段值包括：
  - **"User-Defined"（用户定义）**— 表示用户定义的离开超时时段。

- **“Immediate Leave”（立即离开）**— 指定立即离开超时时段。

要显示 IGMP 监测表，请：

1. 打开 **“IGMP Snooping”（IGMP 监测）**页面。
2. 单击 **“Show All”（全部显示）**。 系统将打开 **“IGMP Snooping Table”（IGMP 监测表）**。



IGMP 监测表

使用 CLI 命令配置 IGMP 监测

下表概括了与 **“IGMP Snooping”（IGMP 监测）**页面显示的配置 IGMP 监测的选项等效的 CLI 命令。

CLI 命令	说明
ip igmp snooping	使用 Internet 成组管理协议（IGMP) 监测特定 VLAN。
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学习功能。
ip igmp snooping host-time-out *¨þ±*	配置主机超时。
ip igmp snooping mrouter-time-out *¨þ±*	配置多点传送路由器超时。
ip igmp snooping leave-time-out { *¨þ±* **| immediate-leave}**	配置离开超时。
show ip igmp snooping mrouter [interface *VLAN ID***]**	显示有关动态学习的多点传送路由器接口的信息。

以下是 CLI 命令实例：

```
Console (config)# interface vlan 2

Console (config-if)# ip igmp snooping

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 300

Console (config-if)# exit
```

```
Console (config)# interface vlan 2

Console (config-if)# ip igmp snooping leave-time-out 60

Console (config-if)# exit

Console (config)# exit

Console # show igmp snooping mrouter interface 1000

VLAN Ports

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

200 1/e1, 2/e1
```

返回目录页面

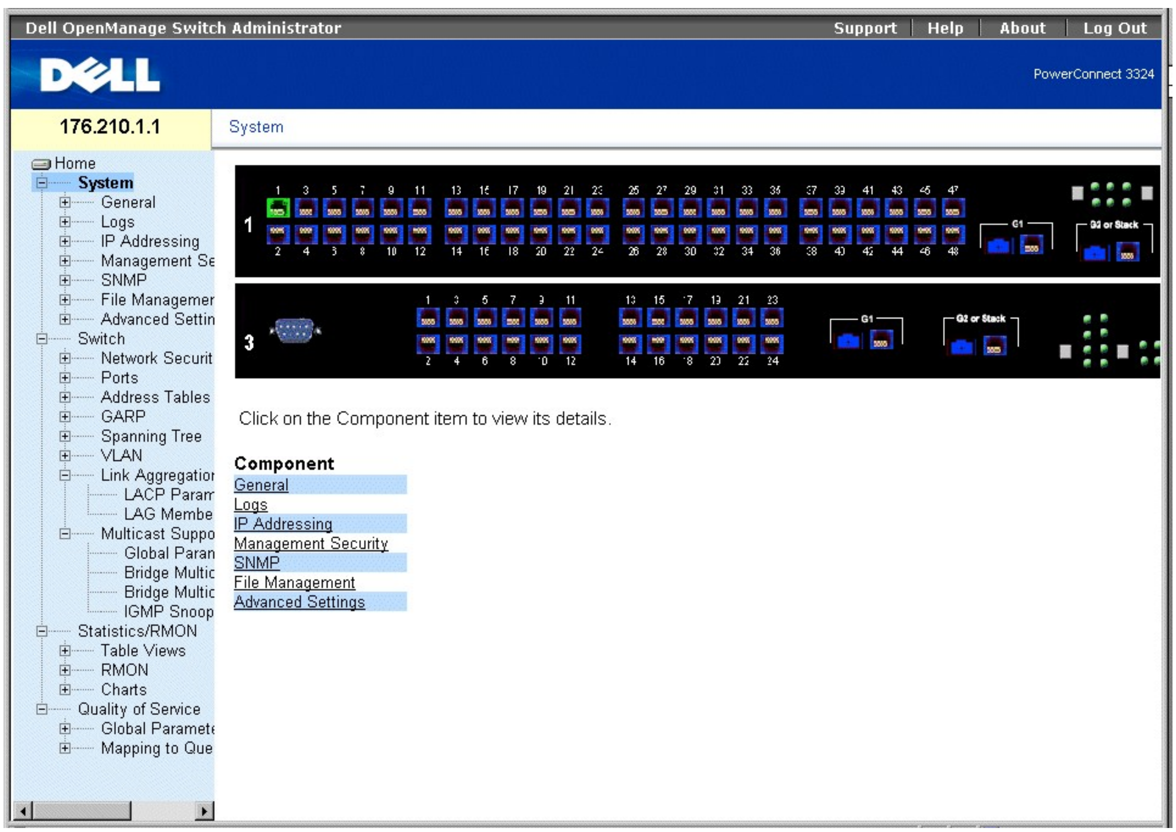
返回目录页面

配置系统信息

Dell™ PowerConnect™ 3324/3348 用户指南

本节提供了有关定义系统参数（包括安全保护功能）、下载设备软件以及重启动设备的信息。
要打开 **“System”（系统）**页面，请：

- 在树视图中单击 **“System”（系统）**。 系统将打开 **“System”（系统）**页面。

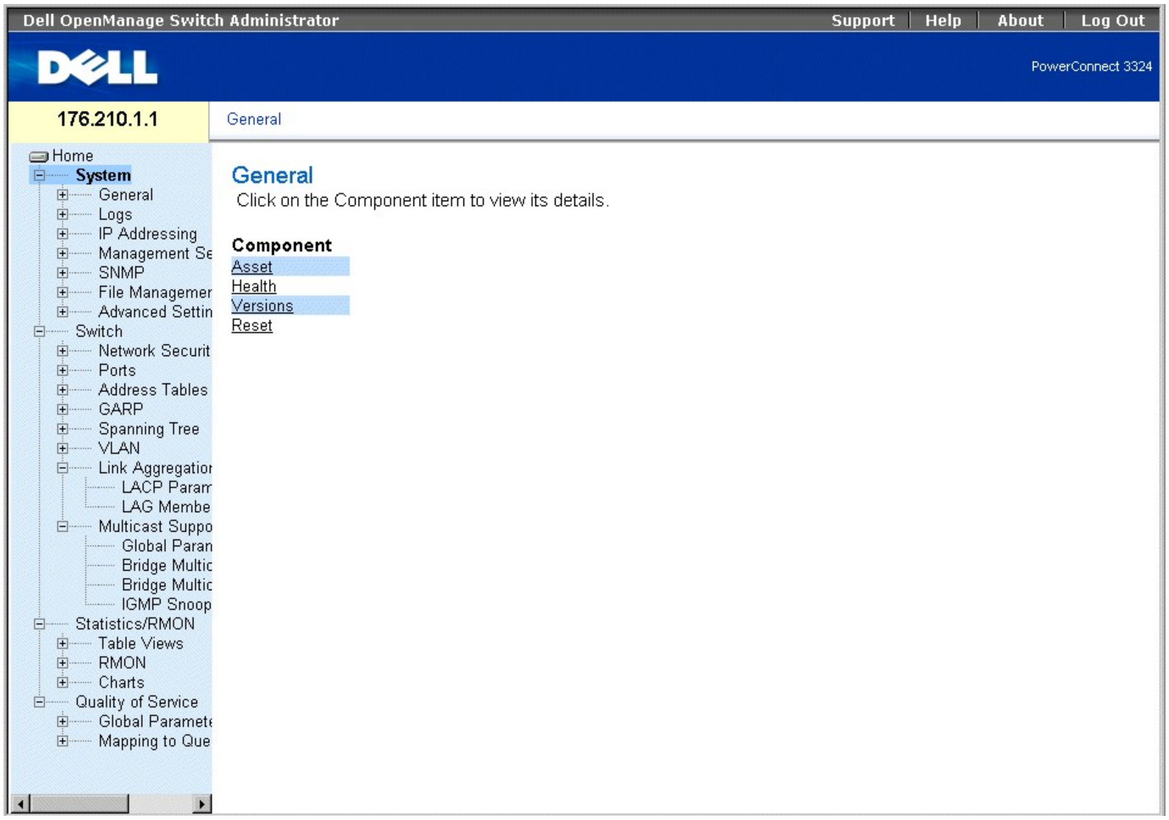


系统页面

定义一般设备信息

“General”（一般）页面包含指向网络管理员可以配置设备参数的页面的链接，包括：

- 查看资产页面
- 查看系统运行状况信息
- 查看版本页面
- 重启动设备

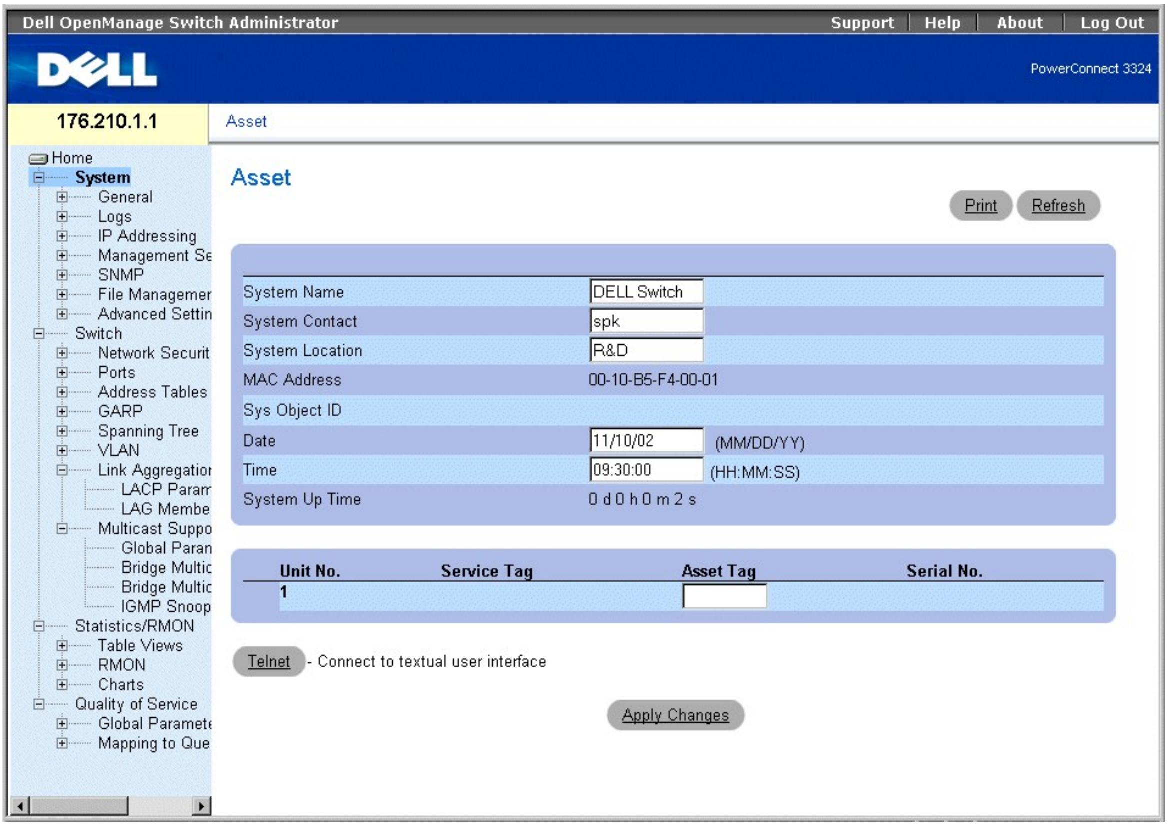


一般页面

查看资产页面

"Asset"（资产）页面包含用于配置一般设备信息的参数，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"（一般）>"Asset"（资产）**。 系统将打开 **"Asset"（资产）**页面。



资产页面

"Asset"（资产）页面包含以下字段：

- **"System Name"（系统名称）** — 定义用户定义的设备名称。
- **"System Contact"（系统联系人）** — 指定联系人的姓名。
- **"System Location"（系统位置）** — 表示系统当前运行的位置。
- **"MAC Address"（MAC 地址）** — 指定交换机的 MAC 地址。
- **"Sys Object ID"（系统对象 ID）** — 标识 MIB 的 OID。
- **"Date (MM/DD/YY)"（日期 [MM/DD/YY]）** — 表示当前日期。 日期格式为月、日、年；例如，11/10/02 表示 2002 年 11 月 10 日。
- **"Time (HH:MM:SS)"（时间 [HH:MM:SS]）** — 指定时间。 时间格式为小时、分钟、秒；例如，20:12:03 表示二十点十二分零三秒。
- **"System Up Time"（系统重设后运行时间）** — 显示自上次设备重设后的时间。 系统时间的显示格式为： 天、小时、分钟和秒。 例如，41 天 2 小时 22 分 15 秒。
- **"Unit No."（装置号）** — 表示堆叠装置号。
- **"Service Tag"（服务标签）** — 表示维修设备时使用的服务参考号码。
- **"Asset Tag"（资产标签）** — 指定用户定义的设备参考。
- **"Serial No."（序列号）** — 表示设备的序列号。

要定义系统信息，请：

1. 打开 **"Asset"（资产）**页面。
2. 定义 **"System Name"（系统名称）**、**"System Contact"（系统联系人）**、**"System Location"（系统位置）**、**"Date"（日**

期）、“Asset Tag”（资产标签）和**“Time”（时间）**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。

要启动 Telnet 会话，请：

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**“Asset”（资产）**页面中显示的字段的等效 CLI 命令。

CLI 命令	说明
hostname *名称*	指定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 *时:分:秒 日 月 年*	手动设置系统时钟和日期。 请注意日期格式不同。
show clock	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	显示设备资产标签。

以下是 CLI 命令实例：

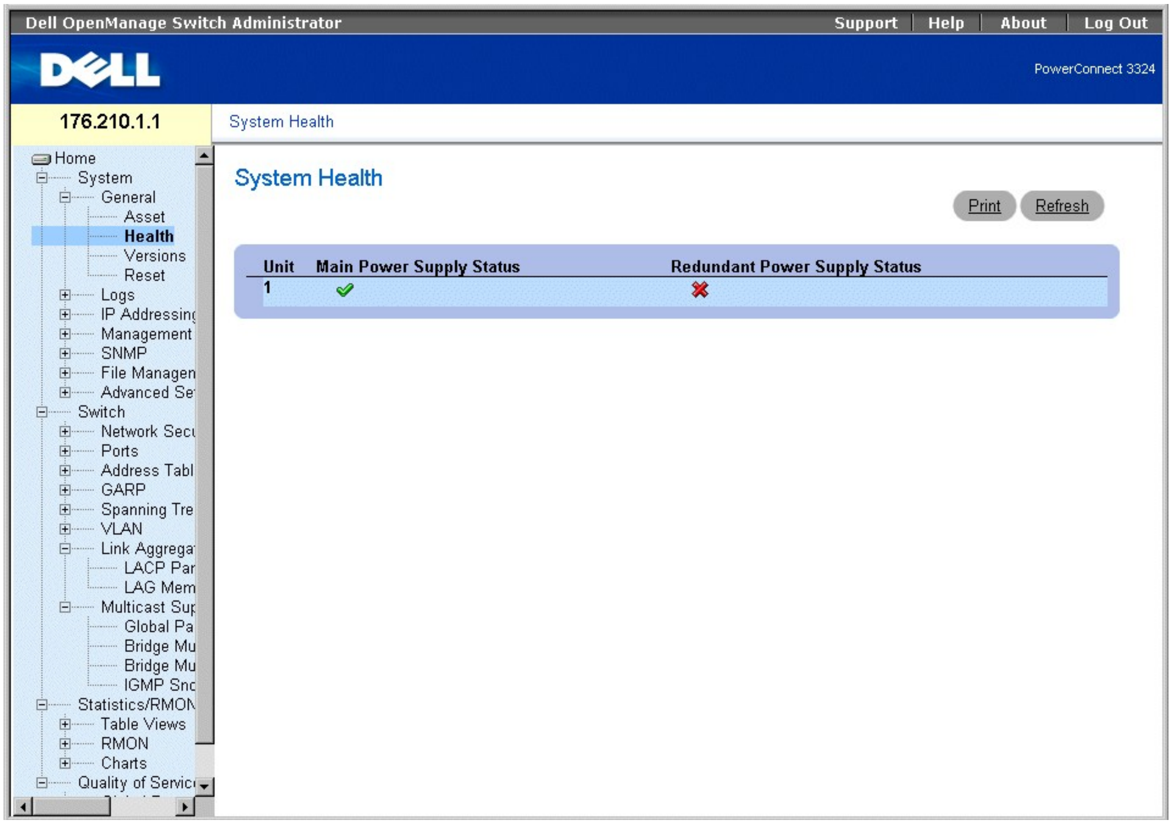
```
Console (config)# hostname dell

Console (config)# snmp-server contact Dell_Tech_Supp

Console (config)# snmp-server location New_York

Console (config)# exit

Console # exit

Console (config)# asset-tag lqwepot

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

Console> show clock
```

```
13:32:00 7 Mar 2002

console# show system

System Description: Ethernet Stackable Switching System

System Up Time (days,hour:min:sec): 0,00:30:58

System Contact: Dell_Tech_Supp

System Name: dell

System Location: New_York

MAC Address: 00:00:b0:22:33:44

Sys Object ID: 1.3.6.1.4.1.674.10895.3004

Power supply Source Status

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

Internal Power Supply Internal redundant OK unit1

External Power Supply External OK unit1

Internal PowerSupply Internal redundant OK unit2

External PowerSupply External OK unit2

Internal PowerSupply Internal redundant OK unit3

External PowerSupply External OK unit3

Internal PowerSupply Internal redundant OK unit6

External PowerSupply External OK unit6
```

查看系统运行状况信息

"System Health"（系统运行状况）页面包含物理设备硬件信息。 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"（一般）>"Health"（运行状况）**。 系统将打开**"System Health"（系统运行状况）**页面。



系统运行状况页面

"System Health"（系统运行状况）页面包含以下字段：

- **"Unit"（装置）** — 表示堆叠装置号。
- **"Main Power Supply Status"（主电源设备状态）** — 表示主电源设备的状态。 可能的字段值包括：
  -  — 表示指定装置的主电源设备运行正常。
  -  — 表示指定装置的主电源设备运行不正常。
  - **"Not Present"（不存在）** — 表示指定装置没有电源设备。
- **"Redundant Power Supply Status"（冗余电源设备状态）** — 表示冗余电源设备的状态。 可能的字段值包括：
  -  — 表示指定装置的冗余电源设备运行正常。
  -  — 表示指定装置的冗余电源设备运行不正常。
  - **"Not Present"（不存在）** — 表示指定装置没有电源设备。

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。

CLI 命令	说明
show system	显示系统信息。

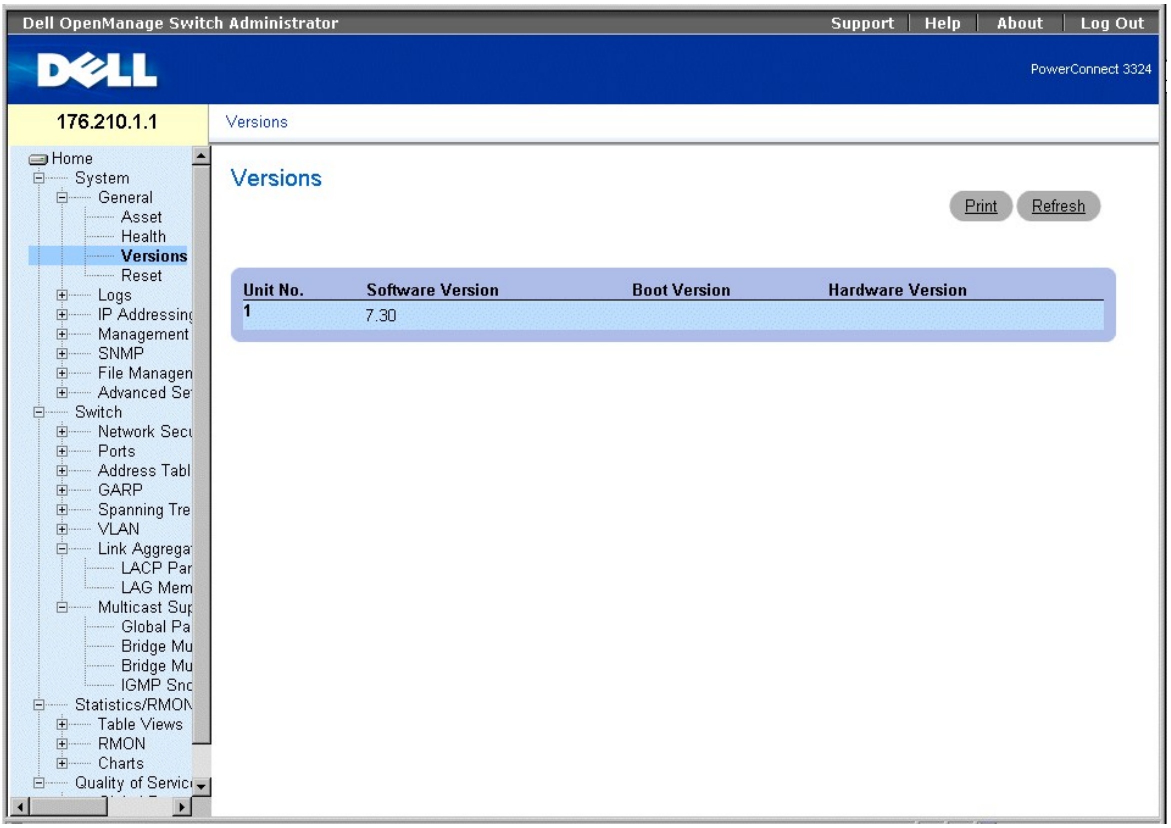
以下是 CLI 命令实例：

```
Console> show system

System Description: Ethernet Stackable Switching System

System Up Time (days,hour:min:sec): 0,00:08:56

System Contact: Dell_Tech_Supp

System Name: dell

System Location: New_York
```

查看版本页面

“Versions”（版本）页面包含有关当前运行硬件和软件的版本的信息。 要打开**“Versions”（版本）**页面，请：

- 在树视图中单击**“System”（系统）>“General”（一般）>“Versions”（版本）**。 系统将打开**“Versions”（版本）**页面。



版本页面

"Versions"（版本）页面包含以下信息：

- **"Unit No."（装置号）**— 表示堆叠装置号。
- **"Software Version"（软件版本）**— 显示特定堆叠装置上当前运行的软件的版本。
- **"Boot Version"（引导版本）**— 显示特定堆叠装置上当前运行的引导版本。
- **"Hardware Version"（硬件版本）**— 显示特定堆叠装置上当前运行的硬件的版本。

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。

CLI 命令	说明
show version	显示系统版本信息。

以下是 CLI 命令实例：

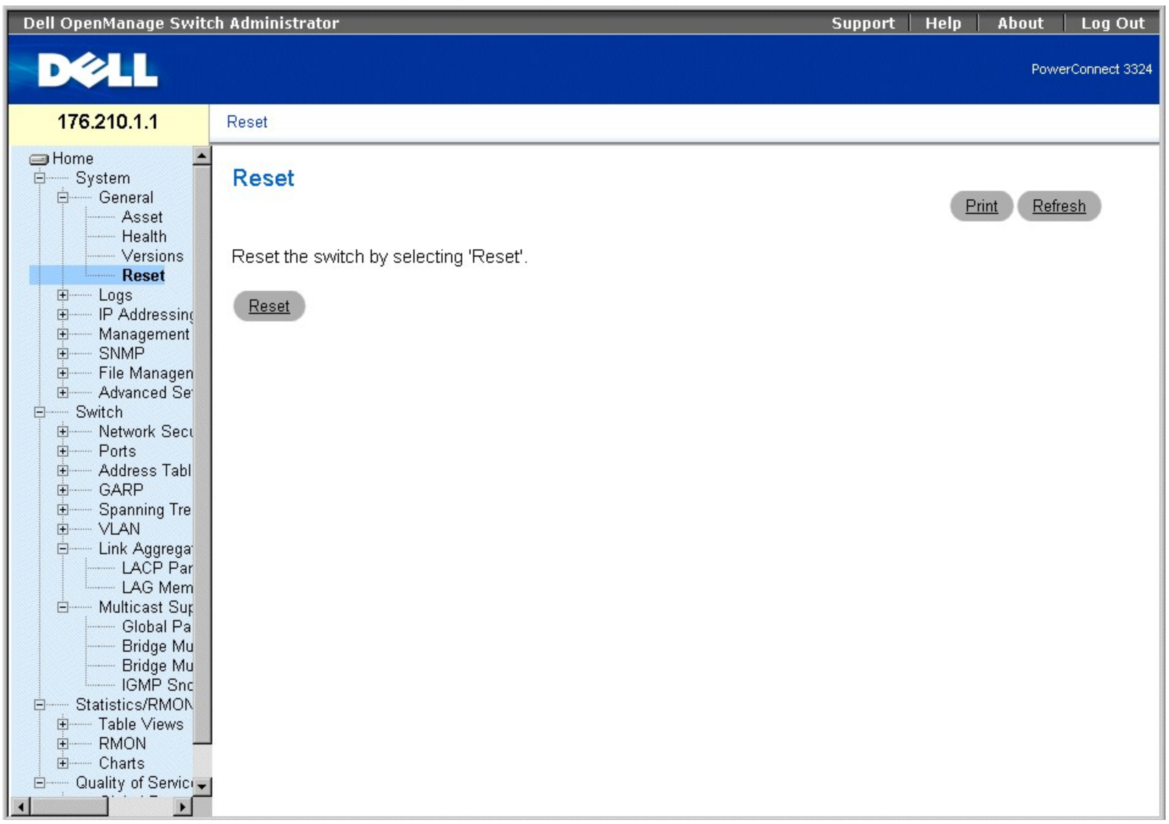
```
Console> show version

SW version 1.0.0.01 (date 14-Feb-2003 time 14:42:16 )
```

```
Boot version 1.30.11 ( date 27-Jan-2003 time 10:06:02 )

HW version 01.01.01
```

重启动设备

"Reset"（重启动）页面使用户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"（一般）>"Reset"（重启动）**。 系统将打开 **"Reset"（重启动）**页面。

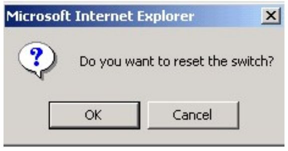


重启动页面

注： 重启动设备之前，请保存对**正在运行的配置**文件所作的所有更改，以免丢失当前的设备配置。 有关保存配置文件的详细信息，请参阅"管理文件"。

要重启动设备，请：

1. 打开 **"Reset"（重启动）**页面。
2. 单击 **"Reset"（重启动）**。 系统将显示确认信息：



设备重启动确认信息

3. 单击 **“OK”（确定）**。 设备将重启动。 重启动设备后，系统将提示用户输入用户名和密码。

使用 CLI 重启动设备

下表概括了用于查看 **“Reset ”（重启动）**页面中显示的字段的等效 CLI 命令。

CLI 命令	说明
reload	重新加载操作系统。

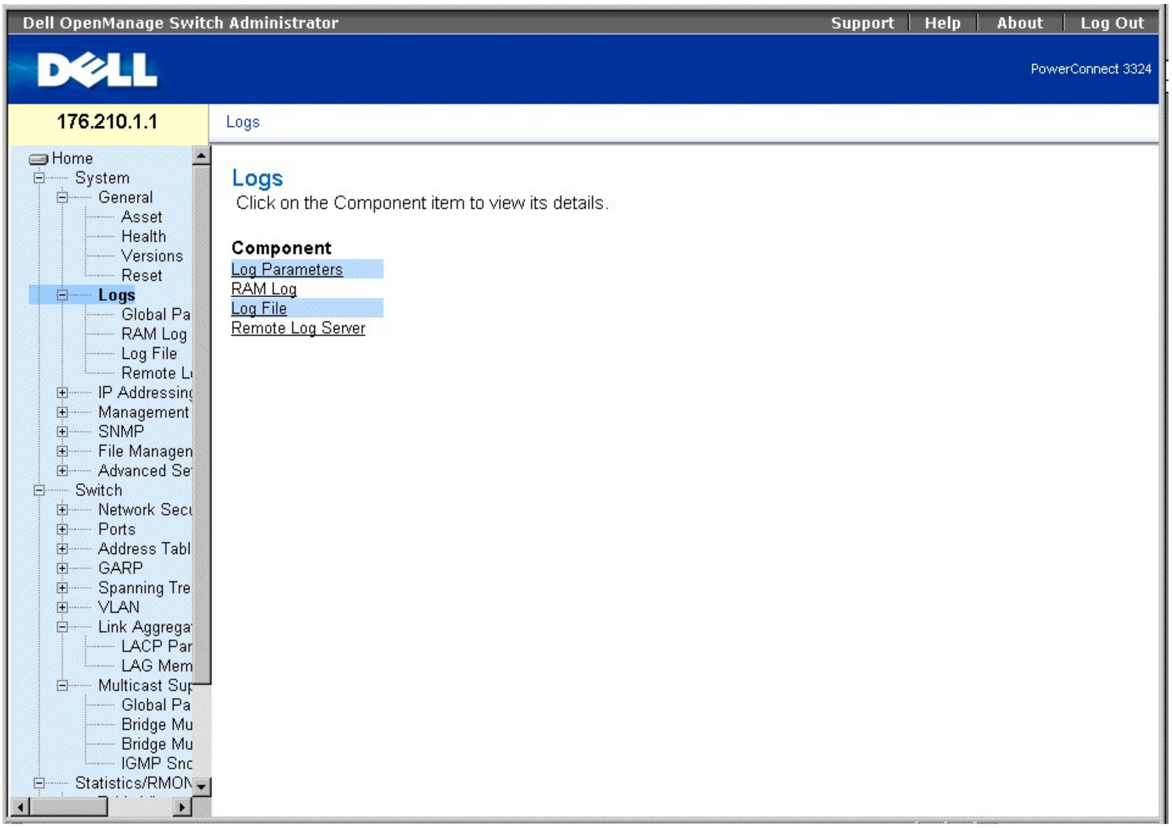
以下是 CLI 命令实例：

```
Console >reload

This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n] ?
```

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）**。 系统将打开 **“Logs”（日志）**页面。



日志页面

"Logs"（日志）页面包含指向以下页面的链接：

- 定义全局日志参数
- 显示 RAM 日志表
- 显示日志文件表
- 查看远程日志服务器设置页面

定义全局日志参数

系统日志使您可以实时查看重要的事件，并记录这些事件以便将来使用。 此功能可用于记录和管理事件以及报告错误。

事件信息具有唯一的格式，即按照 SYSLOG RFC 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。 信息将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。 信息按照其紧急性或相关性进行筛选。 每则信息的严重性决定了每个事件记录设备的信息将被发送到的事件记录设备集。 下表包含日志严重性级别：

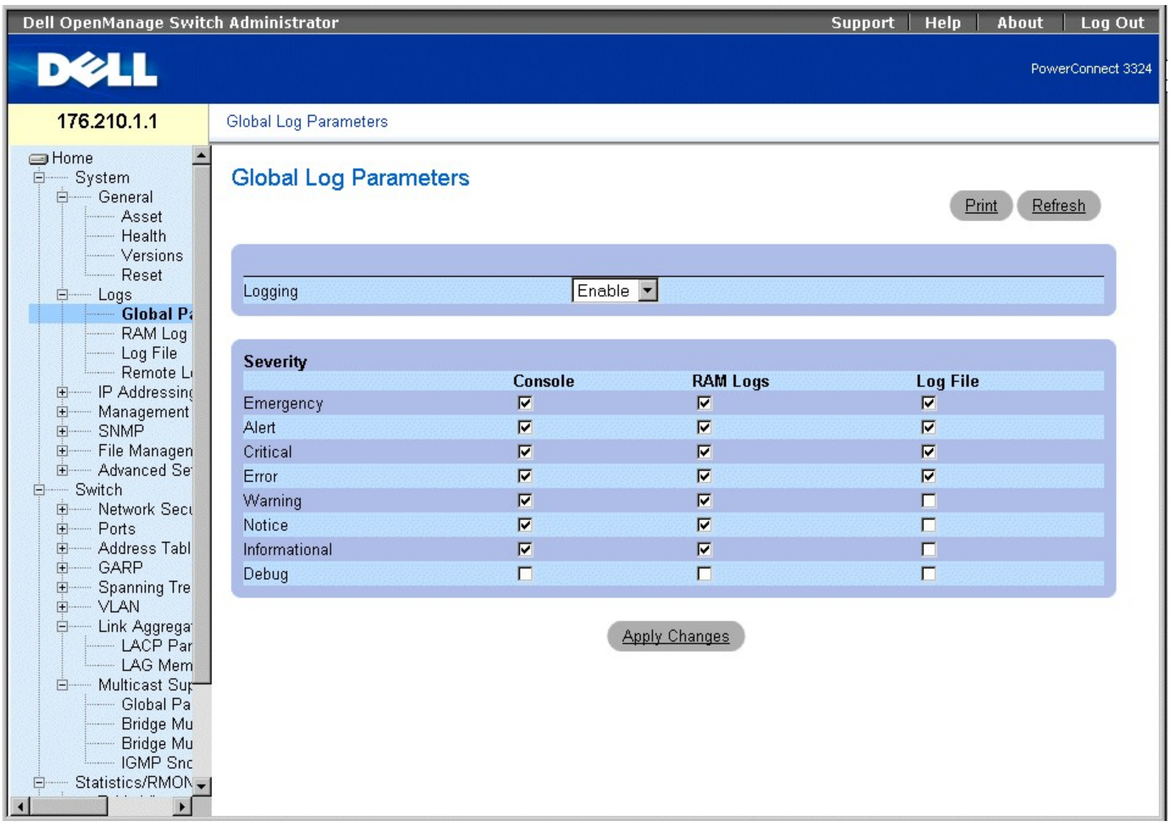
严重性类型	**严重性级别**	**说明**
紧急	0	表示系统无法运行。
警报	1	表示系统需要立即引起注意。
严重	2	表示系统处于严重状态。
错误	3	表示出现了系统错误。
警告	4	表示出现了系统警告。
注意	5	表示系统运行正常，但出现系统注意信息。

信息	6	提供设备信息。
调试	7	提供关于日志的详细信息。

日志严重性级别

"Global Log Parameters"（全局日志参数）页面使您可以定义将哪些事件记录到哪些日志。 该页面包含用于全局性启用日志的字段以及用于定义日志参数的参数。 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）**。 系统将打开**"Global Log Parameters"（全局日志参数）**页面。



全局日志参数页面

"Global Log Parameters"（全局日志参数）页面包含以下字段：

- **"Logging"（记录）**— 为高速缓存、文件和服务器日志启用设备全局日志。 默认情况下，控制台日志处于启用状态，并且不能被禁用。 可能的字段值包括：
  - **"Enable"（启用）**— 允许在高速缓存 (RAM)、文件 (FLASH) 和外部服务器中保存日志。
  - **"Disable"（禁用）**— 禁止保存日志。 不能禁用控制台日志。
- **"Severity"（严重性）**— 以下为可用的严重性日志：
  - **"Emergency"（紧急）**— 表示最高级警告。 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）**— 表示第二级警告。 如果设备出现严重故障，将保存警报日志；例如，如果所有设备功能停止运行。
  - **"Critical"（严重）**— 表示第三级警告。 如果设备出现严重故障，将保存严重日志；例如，其中两个设备端口无法运行，而其余设备端口可以运行。
  - **"Error"（错误）**— 表示出现设备错误；例如，单个端口脱机。

- **"Warning"（警告）**— 表示最低级设备警告。 设备可以工作，但出现运行问题。
- **"Notice"（注意）**— 为网络管理员提供设备信息。
- **"Informational"（信息）**— 提供设备信息。
- **"Debug"（调试）**— 提供有关日志的详细信息。 如果出现调试错误，请与 Dell 在线技术支持（**www.support.ap.dell.com / china.com**）联系。

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记录系统的复选框：

- **"Console"（控制台）**— 表示发送到控制台的日志的最低严重性级别。
- **"RAM Logs"（RAM 日志）**— 表示发送到 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）**— 表示发送到 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"（记录）**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

下表概括了用于查看**"Global Log Parameters"（全局日志参数）**页面中显示的字段的等效 CLI 命令。

CLI 命令	说明
logging on	启用错误信息记录。
logging IP 地址[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。 有关严重性级别列表的信息，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。

以下是 CLI 命令实例：

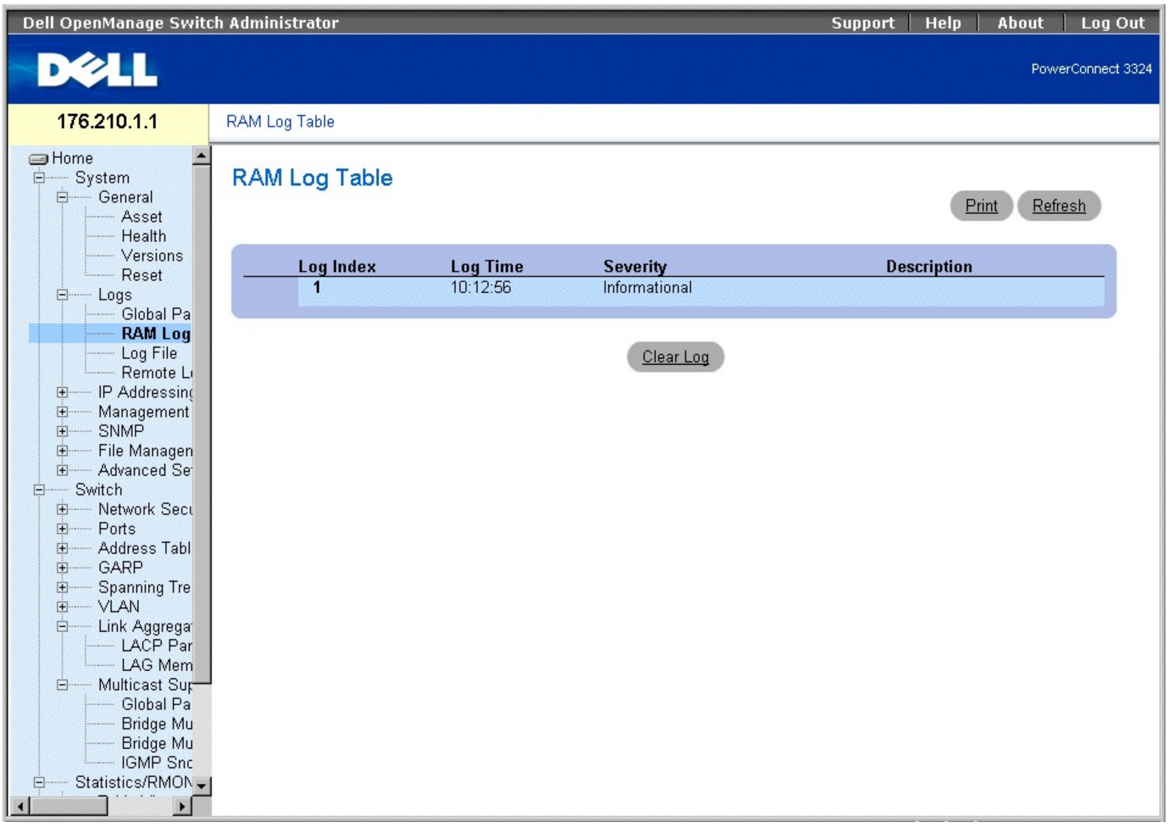
```
Console (config)# logging on

Console (config)# logging console errors

Console (config)# logging buffered debugging

Console (config)# logging file alerts
```

```
Console (config)# clear logging
```

显示 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）**页面，请：

- 在树视图中单击 **"System"（系统）>"Logs"（日志）>"RAM Log"（RAM 日志）**。 系统将打开 **"RAM Log Table"（RAM 日志表）**页面。



RAM 日志表页面

"RAM Log Table"（RAM 日志表）页面包含以下字段：

- **"Log Index"（日志索引）**— 表示 **"RAM Log Table"（RAM 日志表）**中的日志编号。
- **"Log Time"（记录时间）**— 说明日志输入 **RAM 日志表**的时间。
- **"Severity"（严重性）**— 说明日志严重性。
- **"Description"（说明）**— 显示用户定义的日志说明。

要删除日志信息，请：

1. 打开 **"RAM Log Table"（RAM 日志表）**页面。
2. 单击 **"Clear Log"（清除日志）**。 系统将从 **"RAM Log Table"（RAM 日志表）/"Log File Table"（日志文件表）**中删除日志信息，并更新设备。

使用 CLI 命令查看 RAM 日志表

下表概括了用于查看**“RAM Log Table”（RAM 日志表）**页面中显示的字段的等效 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 命令实例：

```
Console # show logging

Console logging: level debugging. Console Messages: 0 Dropped (severity).

Buffer logging: level debugging. Buffer Messages: 11 Logged,
200 Max.

File logging: level notifications. File Messages: 0 Dropped (severity).

Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped (severity).

Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped (severity).

2 messages were not logged (resources)

Buffer log:

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e0, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e1, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e2, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e3, changed state to up
```

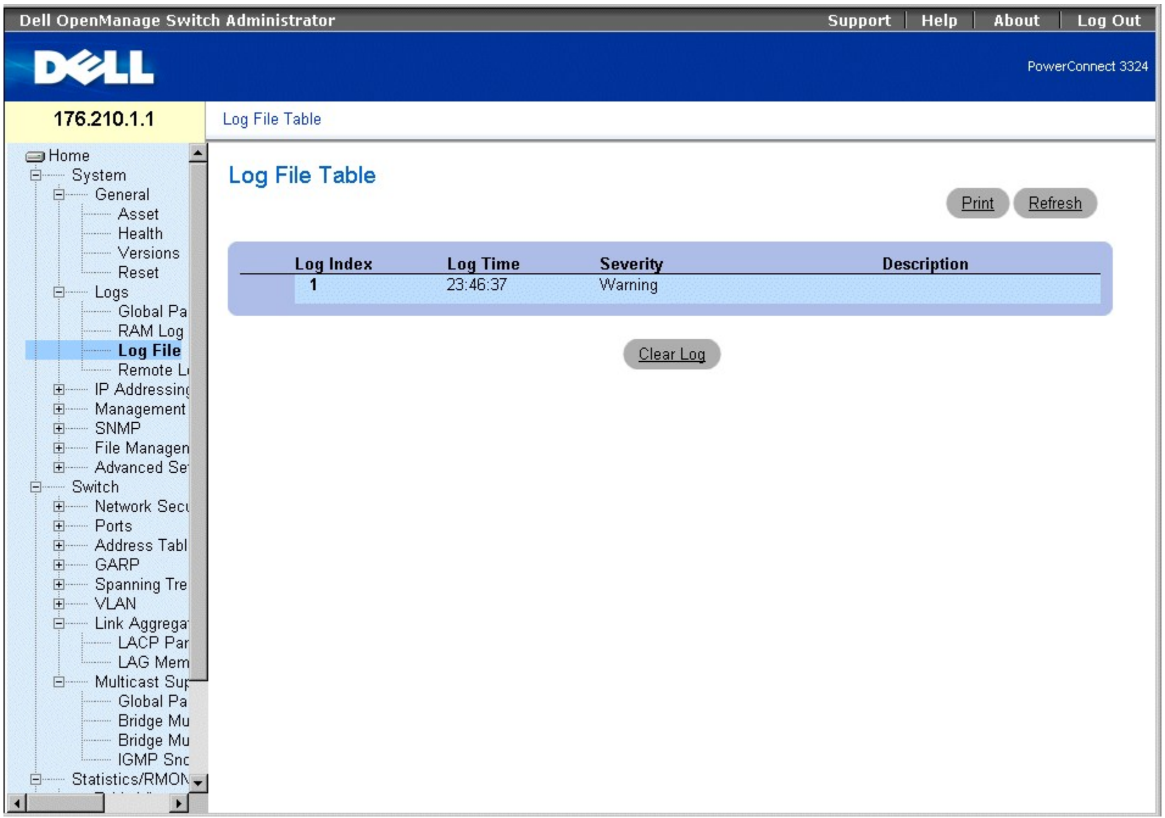
```
11-Aug-2002 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e0, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e1, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e2, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e3, changed state to down

Console # clear logging

clear logging buffer [confirm]

Console #
```

```
Console # clear logging file

clear logging buffer [confirm]

Console #
```

显示日志文件表

"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）**页面，请：

- 在树视图中单击**"System"（系统）>"Logs"（日志）>"Log File"（日志文件）**。 系统将打开**"Log File Table"（日志文件表）**页面。



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）** — 表示 **"Log File Table"（日志文件表）**中的日志编号。
- **"Log Time"（记录时间）** — 说明日志输入 **"Log File Table"（日志文件表）**的时间。
- **"Severity"（严重性）** — 说明日志严重性。
- **"Description"（说明）** — 显示日志信息文本。

使用 CLI 命令显示日志文件表

下表概括了用于查看 **"Log File Table"（日志文件表）**页面中显示的字段的等效 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	清除所有日志文件。

以下是 CLI 命令实例：

```
Console # show logging file
```

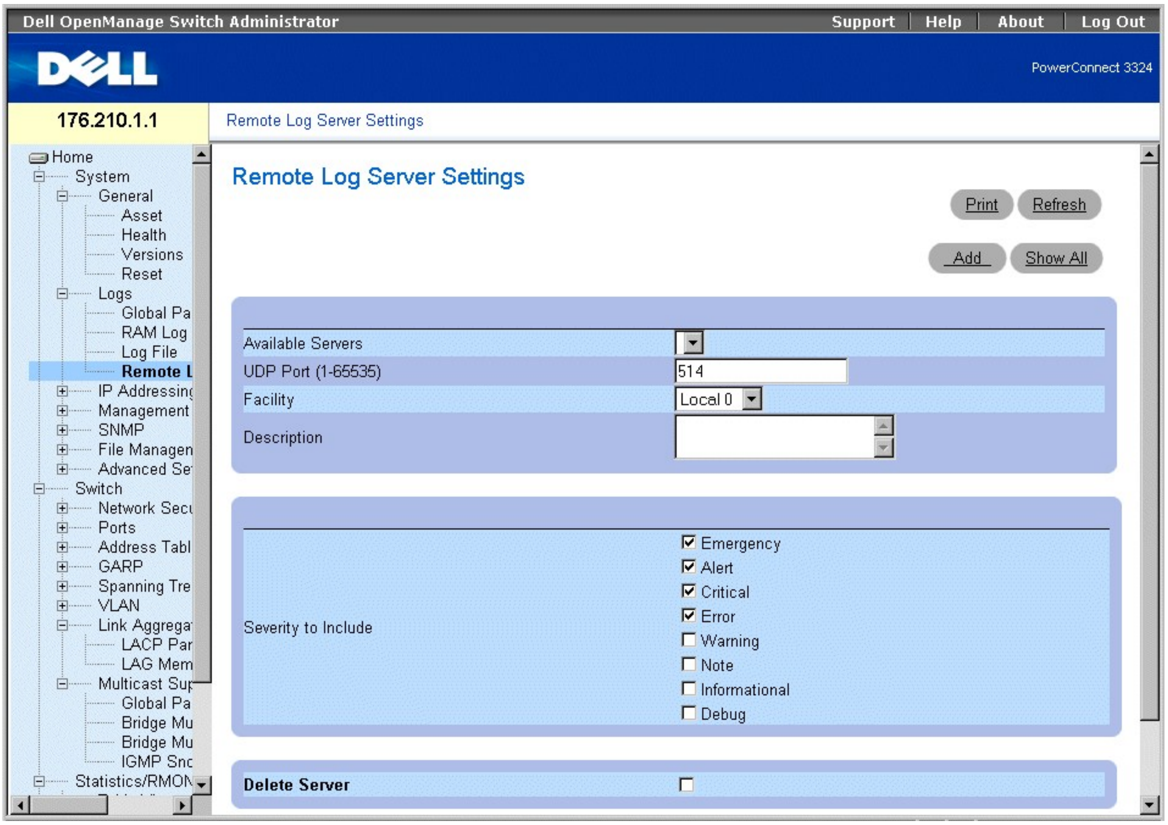
查看远程日志服务器设置页面

```
Console logging: level debugging. Console Messages: 0 Dropped (severity).

Buffer logging: level debugging. Buffer Messages: 11 Logged,
200 Max.

File logging: level notifications. File Messages: 0 Dropped (severity).

Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped (severity).

Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped (severity).

2 messages were not logged (resources)

File log:

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e0, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e1, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e2, changed state to up

11-Aug-2002 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/e3, changed state to up

11-Aug-2002 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e0, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e1, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e2, changed state to down

11-Aug-2002 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/e3, changed state to down
```

查看远程日志服务器设置页面

"Remote Log Server Settings"（远程日志服务器设置）页面包含用于查看可用日志服务器的字段。 此外，还可以定义新的日志服务器并为每个服务器发送日志严重性。 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 Log Server"（远程日志服务器）**。 系统将打开**"Remote Log Server Settings"（远程日志服务器设置）**页面。



远程日志服务器设置页面

"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 [1-65535]）** — 表示为选定服务器发送日志的 UDP 端口。 可能范围为 1 至 65,535，默认值为 514。
- **"Facility"（设备）** — 表示选定服务器的设备映射级别。 默认值为"Local 0"（本地 0）。可能的值包括：
  - **"Local 0"（本地 0）至"Local 7"（本地 7）。**
  - **"No Map"（不映射）。**
- **"Description"（说明）** — 显示用户定义的服务器说明。
- **"Delete Server"（删除服务器）** — 从**"Available Servers"（可用服务器）**列表中删除当前选定的服务器。 可能的字段值包括：
  - **已选取** — 从**"Available Servers"（可用服务器）**列表中删除服务器。
  - **未选取** — 保留**"Available Servers"（可用服务器）**列表中的服务器。

"Remote Logs 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"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 Logs 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**“UDP Port”（UDP 端口）**、**“Facility”（设备）**和**“Description”（说明）**字段。

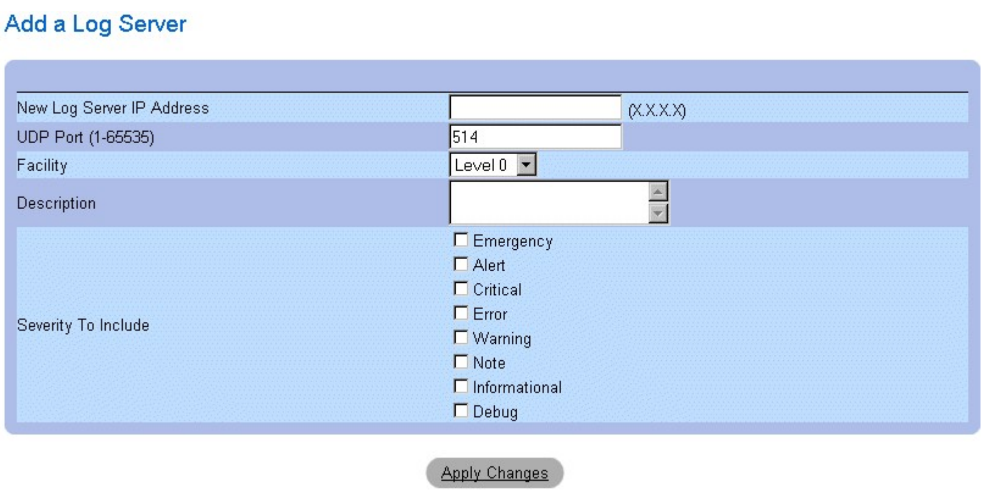
4. 在**“Severity to Include”（要包含的严重性）**复选框中选择日志严重性。

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 Logs 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。



添加日志服务器页面

除了**“Remote Logs Server Settings”（远程日志服务器设置）**页面中的字段外，**“Add a Log Server”（添加日志服务器）**页面还包含以下字段：

- **"New Log Server IP Address"（新日志服务器 IP 地址）**— 指定新日志服务器的 IP 地址。

要添加日志服务器，请：

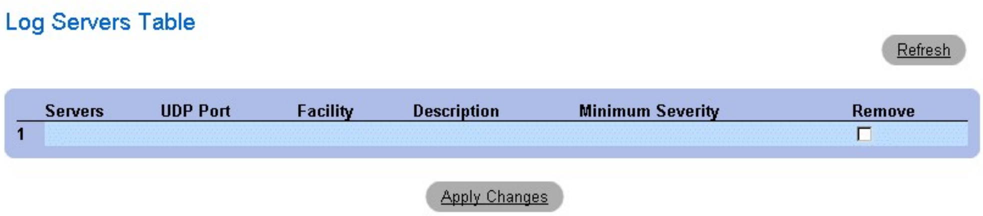
1. 定义**“New Log Server IP Address"（新日志服务器 IP 地址）**、**“UDP Port”（UDP 端口）**、**“Facility”（设备）**和**"Description”（说明）**字段，并选择**“Severity to Include”（要包含的严重性）**复选框。

2. 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。

要显示日志服务器表，请：

1. 打开**“Remote Logs 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。



日志服务器表页面

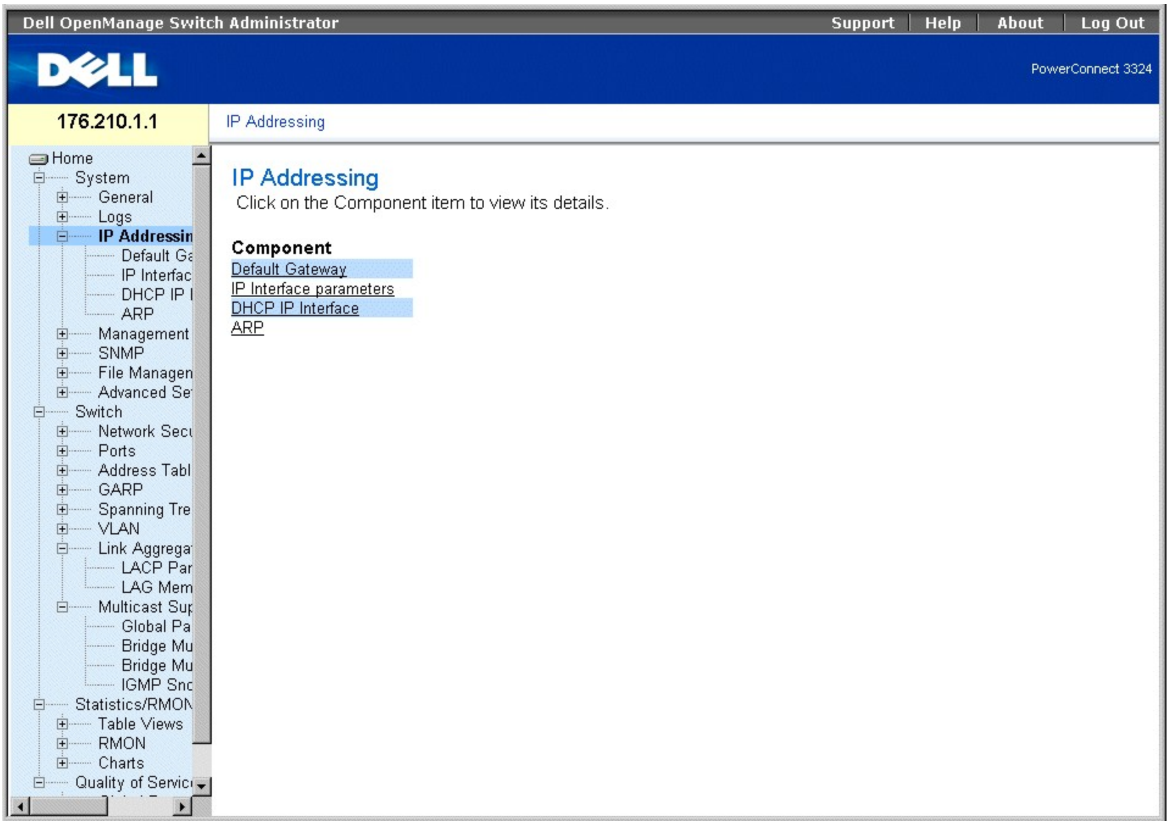
要从**“Log Servers Table”（日志服务器表）**页面中删除日志服务器，请：

1. 打开**“Remote Logs 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。

定义设备 IP 地址

“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）**。 系统将打开**“IP Addressing”（IP 定址）**页面。



IP 定址页面

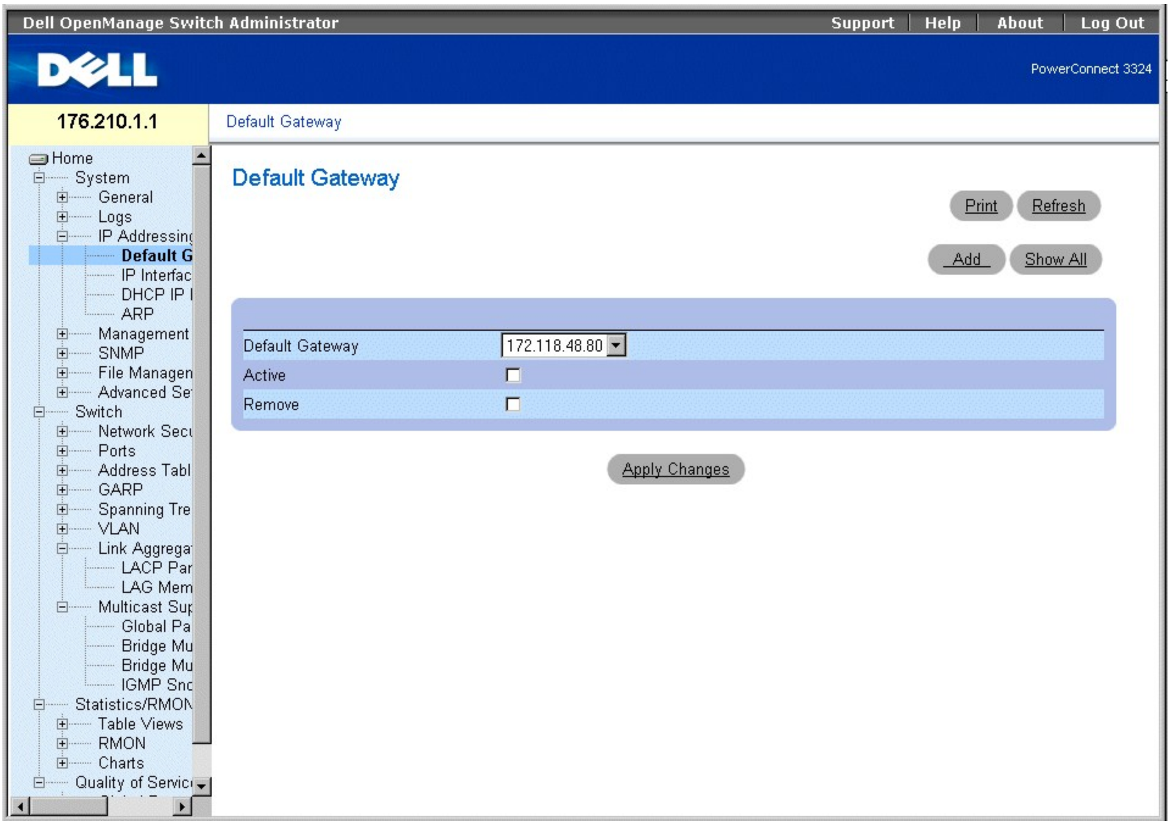
"IP Addressing"（IP 定址）页面包含指向以下页面的链接：

- 定义默认网关
- 定义 IP 接口
- 定义 DHCP IP 接口
- 配置 ARP

定义默认网关

"Default Gateway"（默认网关）页面使网络管理员可以分配网关设备。 将帧发送到远程网络时，信息包便被传输到默认的 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）**。 系统将打开**"Default Gateway"（默认网关）**页面。



默认网关页面

"Default Gateway"（默认网关）页面包含以下字段：

- **"Default Gateway"（默认网关）** — 表示网关设备 IP 地址。
- **"Active"（活动）** — 表示 **"Default Gateway"（默认网关）**下拉列表中指定的默认网关设备当前是否处于活动状态。 可能的字段值包括：
  - **已选取** — 表示网关设备当前处于活动状态。
  - **未选取** — 表示网关设备当前未处于活动状态。
- **"Remove"（删除）** — 从 **"Default Gateway"（默认网关）**下拉列表中删除网关设备。
  - **已选取** — 从 **"Default Gateway"（默认网关）**下拉列表中删除选定的网关设备。
  - **未选取** — 保留 **"Default Gateway"（默认网关）**下拉列表中的网关设备。

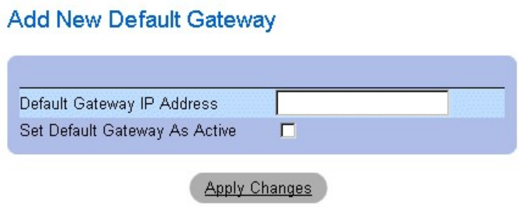
要选择网关设备，请：

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）**。 系统将选定网关设备，并且其状态显示在 **"Active"（活动）**字段中。

要添加网关设备，请：

1. 打开 **"Default Gateway"（默认网关）**页面。
2. 单击 **"Add"（添加）**。 系统将打开 **"Add New Default Gateway"**

（**添加新的默认网关**）页面。



添加新的默认网关

3. 定义 **“Default Gateway IP Address”**（**默认网关 IP 地址**）字段。

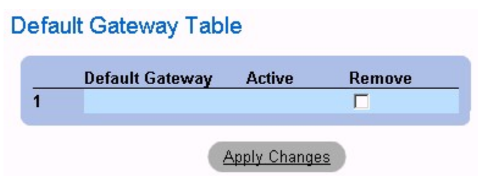
   或

   通过选取复选框将新的网关设置为活动状态。

4. 单击 **“Apply Changes”**（**应用更改**）。 系统将定义新的默认网关设备，并更新设备。

要显示默认网关表，请：

1. 打开 **“Default Gateway”**（**默认网关**）页面。
2. 单击 **“Show All”**（**全部显示**）。 系统将打开 **“Default Gateway Table”**（**默认网关表**）页面。



默认网关表页面

要删除默认网关设备，请：

1. 打开 **“Default Gateway”**（**默认网关**）页面。
2. 单击 **“Show All”**（**全部显示**）。 系统将打开 **“Default Gateway Table”**（**默认网关表**）页面。
3. 选择一个 **“Default Gateway Table”**（**默认网关表**）条目。
4. 选取 **“Remove”**（**删除**）复选框以删除默认网关。
5. 单击 **“Apply Changes”**（**应用更改**）。 系统将删除默认网关表条目，并更新设备。

使用 CLI 命令定义网关设备

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

CLI 命令	**说明**
ip default-gateway IP 地址 1 [IP 地址 2.]	定义默认网关。

no ip default-gateway [IP 地址]	删除默认网关。

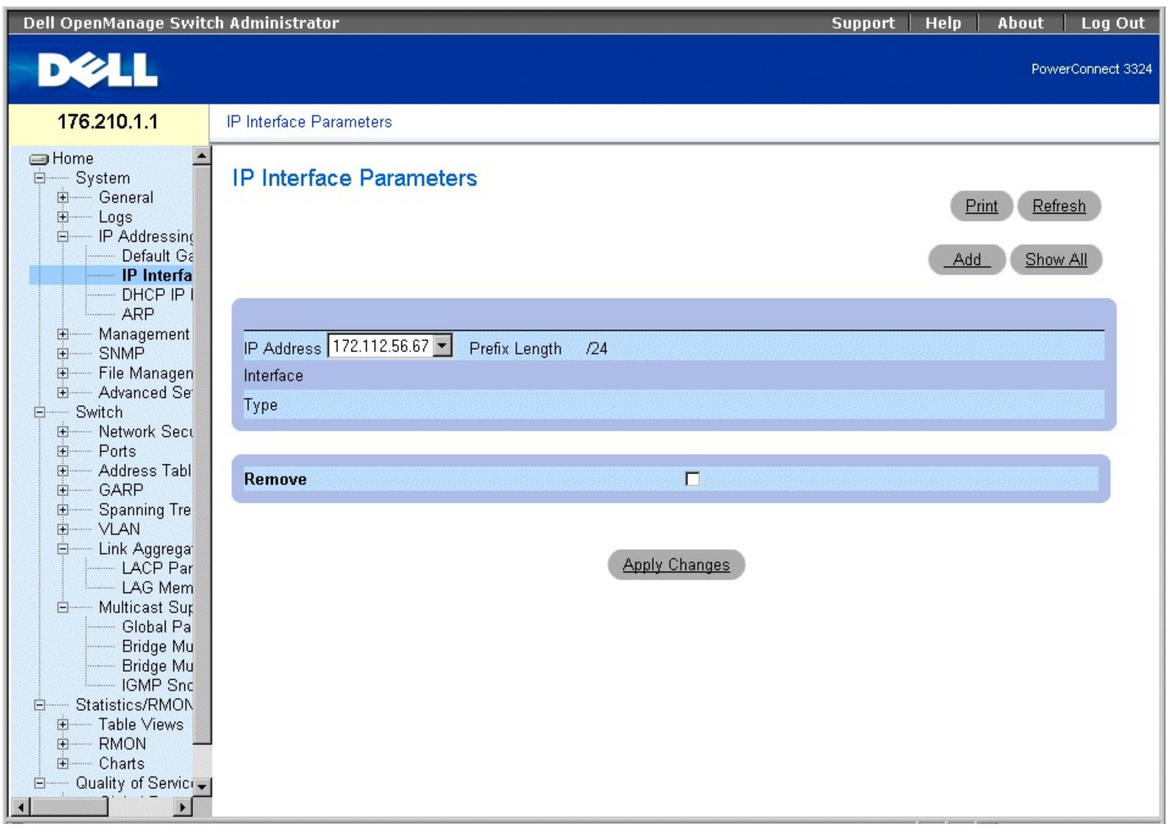
以下是 CLI 命令实例：

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

Console (config)# no ip default-gateway 196.210.10.1
```

定义 IP 接口

"IP Interface Parameters"（IP 接口参数）页面包含用于为接口分配 IP 地址的参数。 要打开 **"IP Interface 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）**。 系统将打开 **"IP Interface Parameters"（IP 接口参数）**页面。



IP 接口参数页面

"IP Interface Parameters"（IP 接口参数）页面包含以下字段：

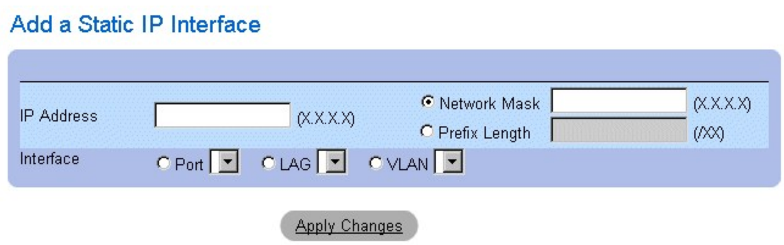
- **"IP Address"（IP 地址）**— 表示接口 IP 地址的列表。
- **"Interface"（接口）**— 指定定义了选定 IP 地址的接口的类型。
  可能的字段值包括：

- **“Port”（端口）**— 表示 IP 地址已分配至端口。
- **“LAG”**— 表示 IP 地址已分配至链路聚合组 (LAG)。
- **“VLAN”**— 表示 IP 地址已分配至 VLAN。

- **“Type”（类型）**— 表示 IP 地址是手动定义为静态 IP 地址，还是通过 DHCP 自动定义。
- **“Remove”（删除）**— 从 **“IP Address”（IP 地址）**下拉列表中删除选定的接口。
  - **已选取** — 从 **“IP Address”（IP 地址）**下拉列表中删除接口。
  - **未选取** — 保留 **“IP Address”（IP 地址）**下拉列表中的接口。

要添加 IP 接口，请：

1. 打开 **“IP Interface 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：

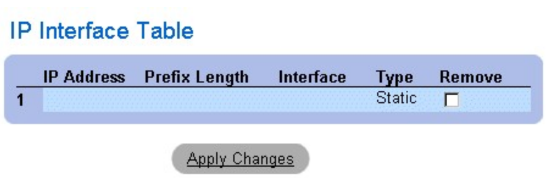


添加静态 IP 接口页面

3. 定义 **“IP Address”（IP 地址）**、**“Interface”（接口）**、**“Network Mask”（网络掩码）**或 **“Prefix Length”（前缀长度）**字段。
4. 选择要为其分配 IP 接口的接口。
5. 单击 **“Apply Changes”（应用更改）**。 系统将添加新接口，并更新设备。

要显示 IP 接口表，请：

1. 打开 **“IP Interface Parameters”（IP 接口参数）**页面。
2. 单击 **“Show All”（全部显示）**。 系统将打开 **“IP Interface Table”（IP 接口表）**页面。 **“IP Interface Table”（IP 接口表）**包含的字段与“[定义 IP 接口](#)”中的字段相同。



IP 接口表页面

要删除 IP 地址，请：

1. 打开 **“IP Interface”（IP 接口）**页面。
2. 单击 **“Show All”（全部显示）**。 系统将打开 **“IP Interface Table”（IP 接口表）**页面。

3. 在**“IP Interface Table”（IP 接口表）**中选择一个条目。
4. 选取**“Remove”（删除）**复选框以删除 IP 地址。
5. 单击**“Apply Changes”（应用更改）**。 系统将删除 IP 地址，并更新设备。

使用 CLI 命令定义 IP 接口

下表概括了用于查看**“IP Interface Parameters”（IP 接口参数）**页面中显示的字段的等效 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 的接口的使用状态。

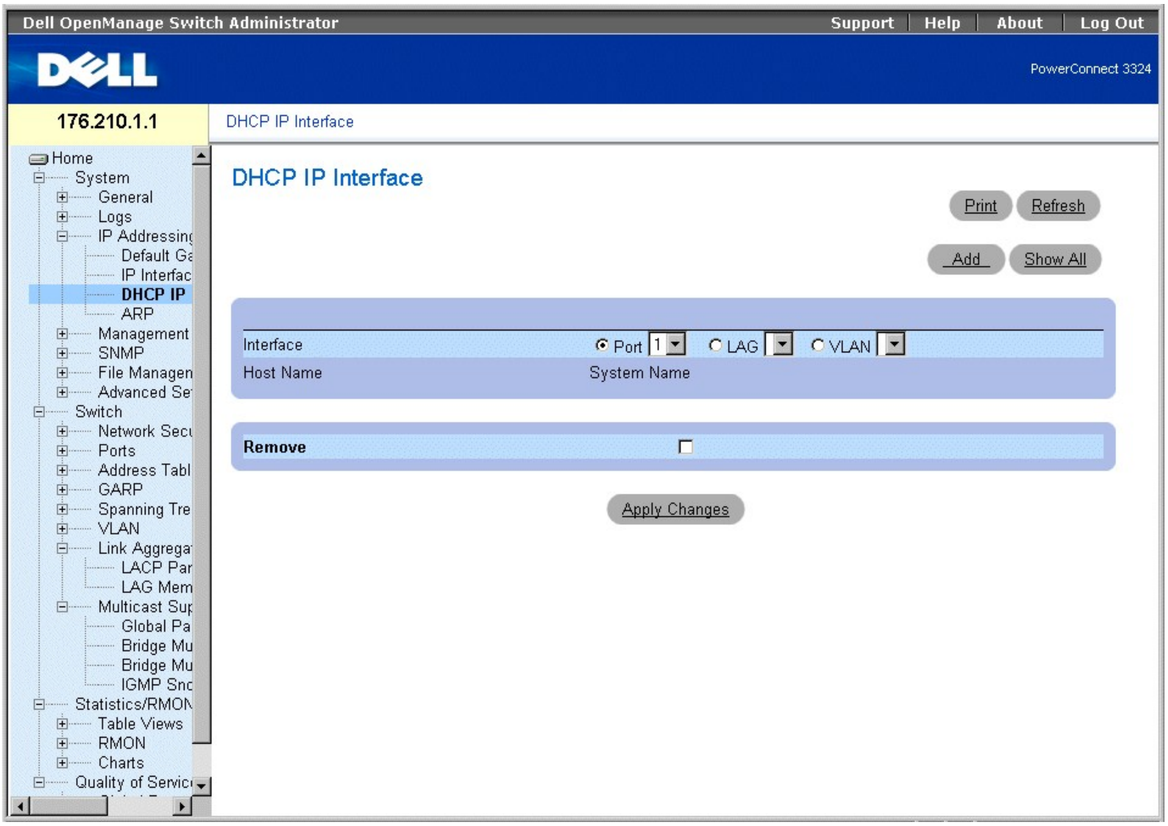
以下是 CLI 命令实例：

```
Console (config)# interface vlan 1

Console (config-if)# ip address 131.108.1.27 255.255.255.0

Console (config-if)# no ip address 131.108.1.27

Console (config-if)# exit

Console# show ip interface vlan 1

Internet address is 10.7.1.192/24

console# show ip interface vlan 204


IP Address Directed Broadcast

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

146.1.0.132/29 disable


console#
```

定义 DHCP IP 接口

"DHCP IP Interface"（DHCP IP 接口）页面用于针对接口指定设备的 DHCP 客户端设置。

- 在树视图中单击**"System"（系统）>"IP Addressing"（IP 定址）>"DHCP IP Interface"（DHCP IP 接口）**。 系统将打开**"DHCP IP Interface"（DHCP IP 接口）**页面。



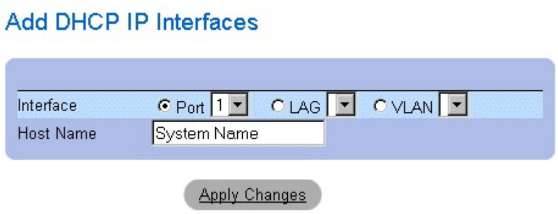
DHCP IP 接口页面

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

- "Inerface"（接口）— 选择设备的接口。
  - **"Port"（端口）**— 指定接口类型为端口，并指定显示 DHCP 客户端设置的特定端口号。
  - **"LAG"**— 指定接口类型为 LAG，并指定显示 DHCP 客户端设置的特定 LAG 号。
  - **"VLAN"**— 指定接口类型为 VLAN，并指定显示 DHCP 客户端设置的特定 VLAN 号。
- **"Host Name"（主机名称）**— 表示系统名称。
- **"Remove"（删除）**— 从**"DHCP IP Interfaces Table"（DHCP IP 接口表）**中删除选定接口的 DHCP 客户端实例。
  - **已选取** — 从**"DHCP IP Interfaces Table"（DHCP IP 接口表）**中删除接口。
  - **未选取** — 保留**"DHCP IP Interfaces Table"（DHCP IP 接口表）**中的接口。

要添加 DHCP IP 接口，请：

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 Interfaces”**
（添加 DHCP IP 接口）页面。



添加 DHCP IP 接口

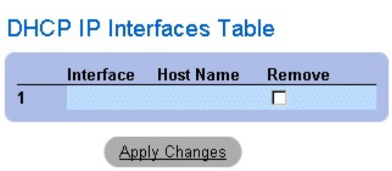
3. 选择**“Interface”（接口）**，并定义**“Host Name”（主机名称）**。
4. 单击**“Apply Changes”（应用更改）**。 系统将添加新的 DHCP IP 接口，并更新设备。

要修改 DHCP IP 接口，请：

1. 打开**“DHCP IP Interface”（DHCP IP 接口）**页面。
2. 修改**“Interface”（接口）**字段。
3. 单击**“Apply Changes”（应用更改）**。 系统将修改条目，并更新设备。

要显示 DHCP IP 接口表，请：

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 IP Interfaces Table”（DHCP IP 接口表）**页面。



DHCP IP 接口表页面

要删除 DHCP IP 接口，请：

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 IP Interfaces Table”（DHCP IP 接口表）**。
3. 选择 DHCP 客户端条目。
4. 选取**“Remove”（删除）**复选框以删除 DHCP 客户端条目。
5. 单击**“Apply Changes”（应用更改）**。 系统将删除**“DHCP IP Interfaces Table”（DHCP IP 接口表）**条目，并更新设备。

使用 CLI 命令定义 DHCP 客户端

下表概括了用于查看**“DHCP IP Interface”（DHCP IP 接口）**页面中显示的字段的等效 CLI 命令。

CLI 命令	说明
ip address-dhcp [hostname 主机名称**]**	通过 DHCP 获取以太网接口的 IP 地址。

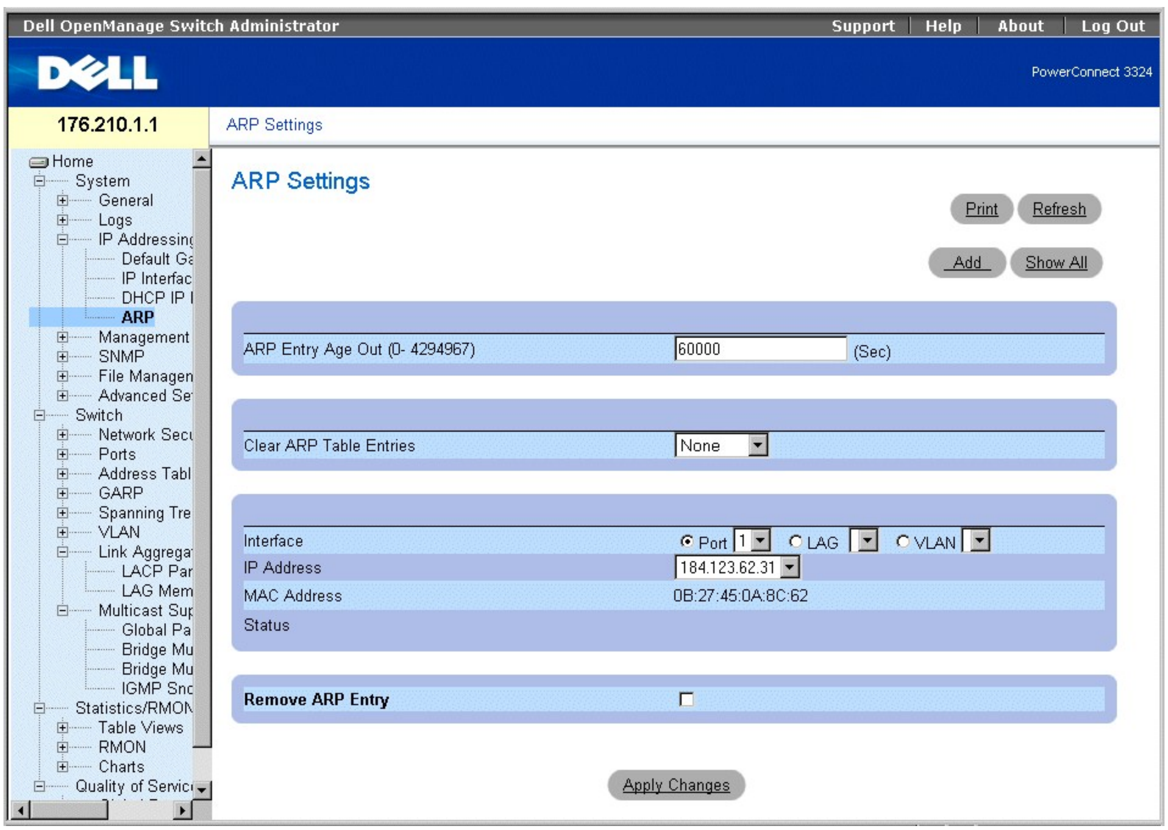
以下是 CLI 命令实例：

```
Console (config)# interface ethernet 1/e8

Console (config-if)# ip address-dhcp hostname marketing
```

配置 ARP

地址解析协议 (ARP) 是一种 TCP/IP 协议，用于将 IP 地址转换为物理地址。 可以在 ARP 表中定义静态条目。 定义静态条目时，将输入一个永久性条目，以用于将 IP 地址转换为 MAC 地址。 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"**。 系统将打开 **"ARP Settings"（ARP 设置）**页面。



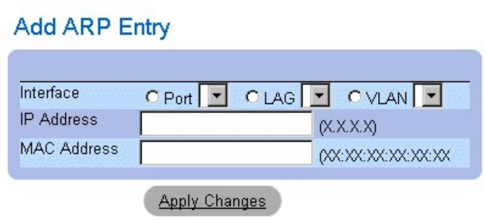
ARP 设置页面

"ARP Settings"（ARP 设置）页面包含以下字段：

- **"ARP Entry Age Out (0-4000000)"（ARP 条目超时 [0-4000000]）**— 表示 ARP 条目超时之前存在的时间（以秒为单位）。 在此时间段之后，该条目将从表中删除。 默认值为 60,000 秒。
- **"Clear ARP Table Entries"（清除 ARP 表条目）**— 表示清除的 ARP 条目的类型。 可能的字段值包括：
  - **"None"（无）**— 表示不清除 ARP 条目。
  - **"All"（所有）**— 表示清除所有 ARP 条目。
  - **"Static"（静态）**— 表示只清除静态 ARP 条目。
  - **"Dynamic"（动态）**— 表示只清除动态 ARP 条目。
- **"Interface"（接口）**— 选择接口类型和特定接口号。 可能的字段值包括：
  - **"Port"（端口）**— 包含可定义 ARP 的端口列表。
  - **"LAG"**— 包含可定义 ARP 的 LAG 列表。
  - **"VLAN"**— 包含可定义 ARP 的 VLAN 列表。
- **"IP Address"（IP 地址）**— 选择与指定接口相关联的 IP 地址。
- **"MAC Address"（MAC 地址）**— 指定相关联的 MAC 地址。
- **"Status"（状态）**— 指定 **"ARP Table"（ARP 表）**条目的状态。 可能的字段值包括：
  - **"Other"（其它）**— 表示 ARP 条目既不是通过动态学习获得的，也不是静态条目。
  - **"Invalid"（无效）**— 表示 ARP 条目无效。
  - **"Dynamic"（动态）**— 表示 ARP 条目是通过动态学习获得的。
  - **"Static"（静态）**— 表示 ARP 条目是静态条目。
- "Remove ARP Entry"（删除 ARP 条目）— 从 **"ARP Table"（ARP 表）**中删除 ARP 条目。
  - **已选取** — 删除特定 ARP 条目。
  - **未选取** — 保留 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。



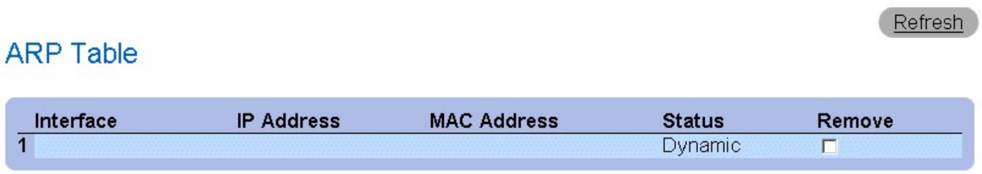
添加 ARP 条目页面

3. 选择一个 **"Interface"（接口）**，并定义其 **"IP Address"（IP 地址）**和 **"MAC address"（MAC 地址）**字段。
4. 单击 **"Apply Changes"（应用更改）**。 系统将添加 **"ARP Table"（ARP 表）**条目，并更新设备。

要显示 ARP 表，请：

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。



ARP 表页面

要删除 ARP 表条目，请：

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**“ARP Table”（ARP 表）**条目，并更新设备。

使用 CLI 命令配置 ARP

下表概括了用于查看**“ARP Settings”（ARP 设置）**页面中显示的字段的等效 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。
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 命令实例：

```
console(config)# arp 146.1.0.131 00-00-55-66-77-00 ethernet 1/e1

Console (config)# exit

Console# arp timeout 12000

Console# show arp

Interface IP address HW address Status

---- ---------- ----------------- -------
```

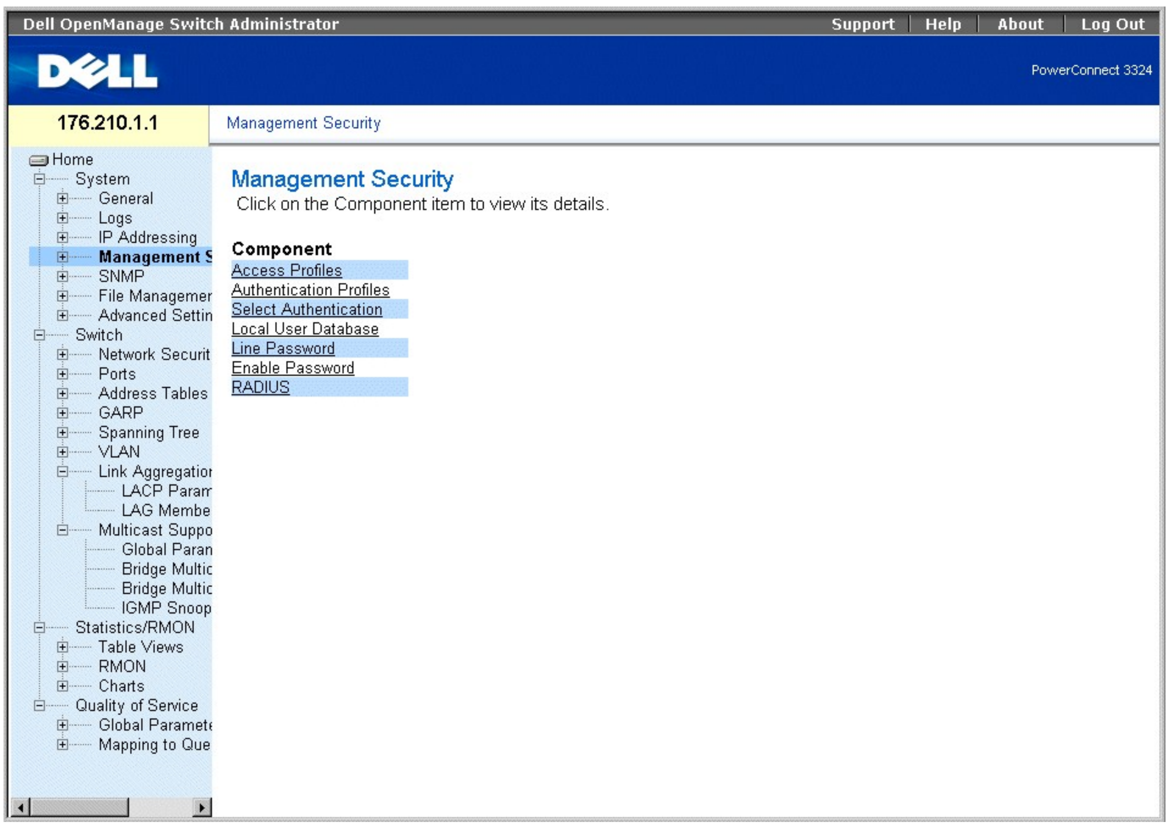
1/e1 10.7.1.102 00:10:B5:04:DB:4B Dynamic

2/e2 10.7.1.135 00:50:22:00:2A:A4 Static

管理设备安全保护

通过**“Management Security”（管理安全保护）**页面可以访问安全保护页面，使网络管理员可以设置端口、设备管理方法、用户和服务器安全保护的安全保护参数。 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）**。 系统将打开**“Management Security”（管理安全保护）**页面。



管理安全保护页面

本节包括以下主题：

- 定义访问配置文件
- 定义验证配置文件
- 分配验证配置文件
- 定义本地用户数据库
- 定义线路密码

- [定义启用密码]
- [配置 RADIUS 全局参数]

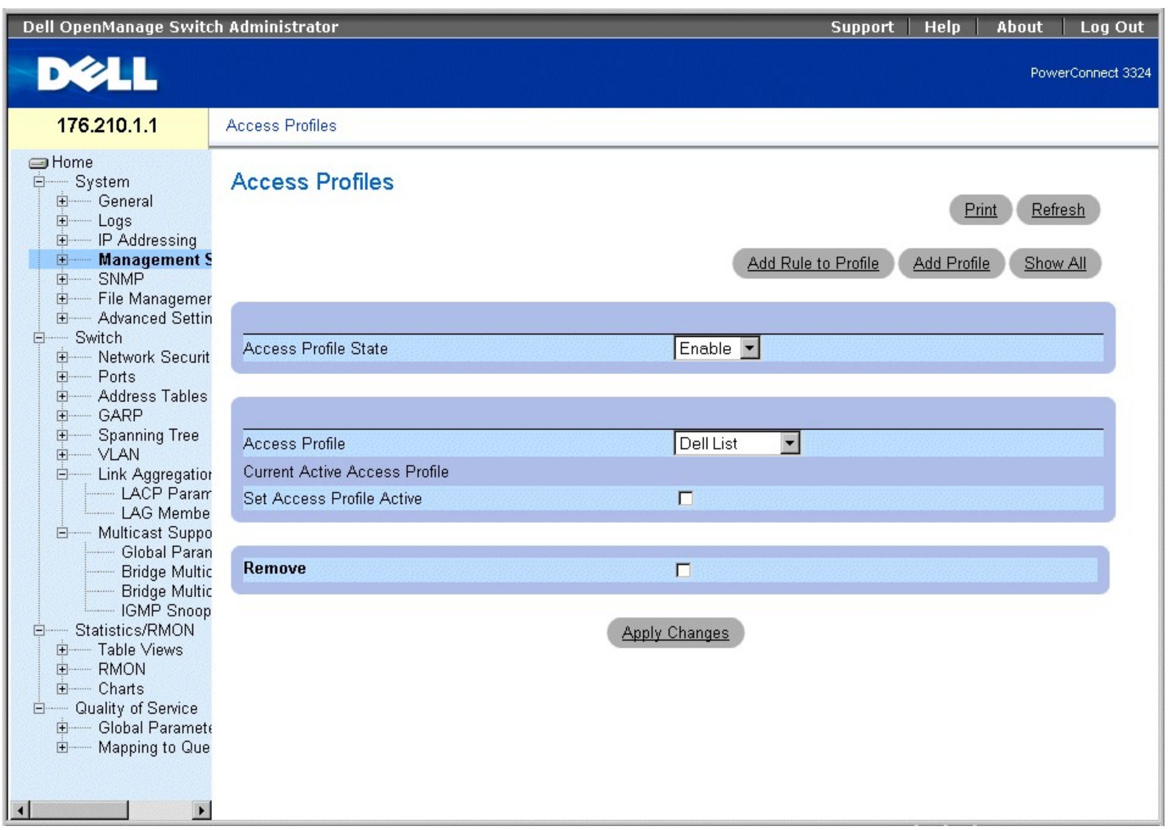
定义访问配置文件

"Access Profiles"（访问配置文件）页面使网络管理员可以定义用于访问设备的配置文件和规则。 通过入口端口、源 IP 地址和/或子网掩码，可以将管理方法访问限制在特定用户组内。
可以为以下各项分别定义管理访问方法：

- Web 访问 (HTTP)
- 安全 Web 访问 (HTTPS)
- Telnet
- SNMP
- 以上全部

访问一个管理服务的用户可能不同于管理另一个管理服务的用户。 管理访问列表包含的的规则用于确定设备管理方式和管理者。 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）**。 系统将打开**"Access Profiles"（访问配置文件）**页面。



访问配置文件页面

"Access Profiles"（访问配置文件）页面包含以下字段：

- **"Access Profile State"（访问配置文件状态）** — 在设备上启用访问配置文件。
  可能的字段值包括：
  - **"Enable"（启用）** — 在设备上启用访问配置文件安全保护管理。
  - **"Disable"（禁用）** — 在设备上禁用访问配置文件安全保护管理。 如果禁用了访问配置文件安全保护管理，则所有站点均可访问该设备。
- **"Access Profiles"（访问配置文件）** — 包含一系列用户定义的**访问配置文件列表**。 **"Access Profile"（访问配置文件）**列表包含以下默认值：
  - **"Console Only"（仅控制台）** — 仅允许通过控制台访问。 选择"Console Only"（仅控制台）将断开 HTTP 和 Telnet 会话的连接。 此为默认值，并且不能被删除。
- **"Current Active Access Profile"（当前活动的访问配置文件）** — 显示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）** — 激活选定的访问配置文件。
- **"Remove"（删除）** — 从**"Access Profile Names"（访问配置文件名称）**中删除选定的访问配置文件。
  - **已选取** — 删除访问配置文件。
  - **未选取** — 保留访问配置文件。

注： 不能删除处于活动状态的配置文件。

要激活配置文件，请：

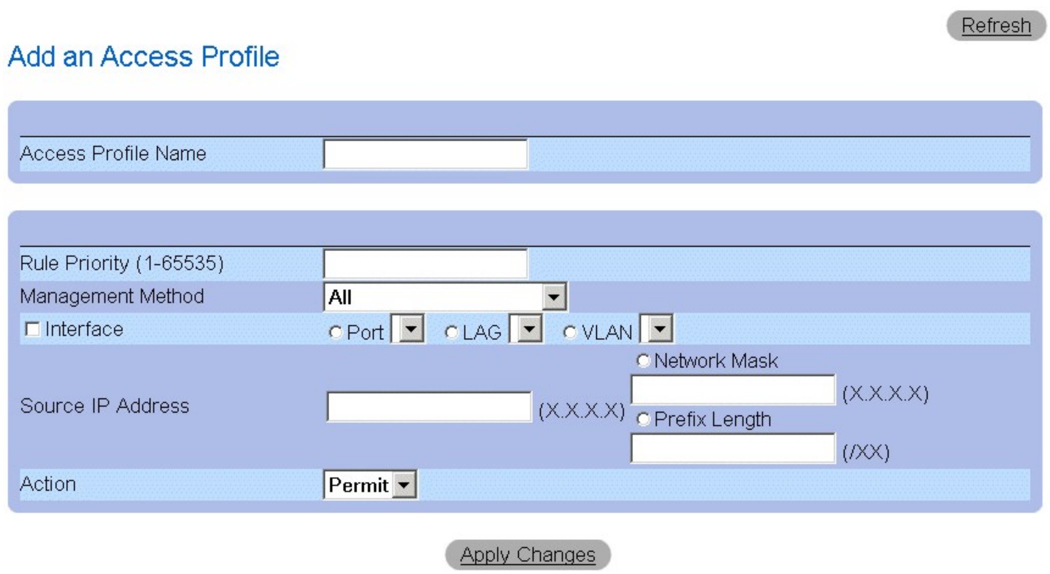
1. 打开**"Access Profiles"（访问配置文件）**页面。
2. 在**"Access Profiles"（访问配置文件）**字段中选择一个访问配置文件。
3. 选取**"Set Access Profile Active"（将访问配置文件设置为活动状态）**复选框。
4. 单击**"Apply Changes"（应用更改）**。 系统将激活访问配置文件。

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。 规则优先级设置了配置文件中规则的应用顺序。

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。



添加访问配置文件页面

“Add An Access Profile”（添加访问配置文件）页面包含以下字段：

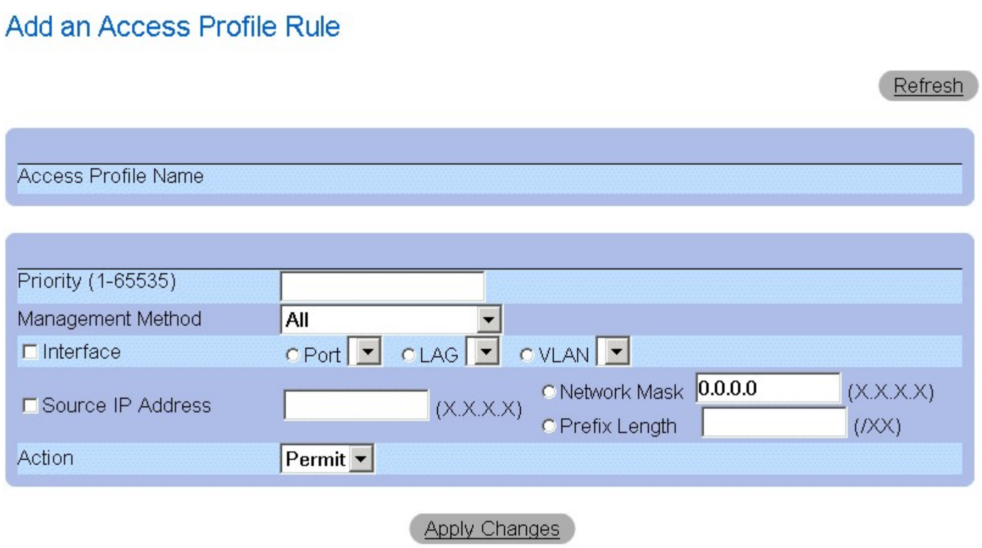
- **“Access Profiles Name”（访问配置文件名称）**— 指定为其定义了规则的访问配置文件。
- **“Rule Priority (1-65535)”（规则优先级 [1-65535]）**— 表示规则优先级（要包含在新配置文件中的可选的第一条规则）。
- **“Management Method”（管理方法）**— 指定为其定义了访问配置文件的管理方法。 可能的字段值包括：
  - **“All”（所有）**— 表示将所有管理方法分配至访问配置文件。
  - **“Telnet”**— 表示将所有 Telnet 会话分配至访问配置文件。
  - **“Secure Telnet”（安全 Telnet）**— 表示将安全 Telnet 会话分配至访问配置文件。
  - **“HTTP”**— 表示将 HTTP 会话分配至访问配置文件。
  - **“Secure HTTP”（安全 HTTP）**— 表示将安全 HTTP 会话分配至访问配置文件。
  - **“SNMP”**— 表示将 SNMP 会话分配至访问配置文件。
- **“Interface”（接口）**— 指定要应用规则的接口。 可能的字段值包括：
  - **“Port”（端口）**— 表示接口为端口，并且是为其定义了访问配置文件的特定端口。
  - **“LAG”**— 表示接口为 LAG，并且是为其定义了访问配置文件的特定 LAG。
  - **“VLAN”**— 表示接口为 VLAN，并且是为其定义了访问配置文件的特定 VLAN。
- **“Source IP Address”（源 IP 地址）**— 表示信息包应匹配的接口源 IP 地址。
- **“Network Mask”（网络掩码）**— 表示信息包应匹配的接口网络掩码。
- **“Prefix Length”（前缀长度）**— 表示信息包应匹配的前缀长度。
- **“Action”（操作）**— 定义管理安全保护规则操作。 可能的字段值包括：
  - **“Permit”（允许）**— 允许对定义的接口进行管理访问。
  - **“Deny”（拒绝）**— 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 **“Rule Priority”（规则优先级）**、**“Management Method”（管理方法）**、**“Interface”（接口）**、**“Source IP”（源 IP）**、**“Network Mask”（网络掩码）**、**“Prefix Length”（前缀长度）**和 **“Action”（操作）**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。

要将规则添加至访问配置文件，请：

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。



添加访问配置文件规则页面

"Add An Access Profile Rule"（添加访问配置文件规则）页面包含以下字段：

- **"Access Profile Name"（访问配置文件名称）** — 表示访问配置文件的名称。
- **"Rule Priority (1-65535)"（规则优先级 [1-65535]）** — 表示规则的优先级。
- **"Management Method"（管理方法）** — 指定为其定义了访问配置文件的管理方法。 可能的字段值包括：
  - **"All"（所有）** — 表示将所有管理方法分配至访问配置文件。 具有此访问配置文件的用户可以使用所有管理方法访问设备。
  - **"Telnet"** — 表示将所有 Telnet 会话分配至访问配置文件。 具有此访问配置文件的用户可以使用 Telnet 管理方法访问设备。
  - **"Secure Telnet"（安全 Telnet）** — 表示将安全 Telnet 会话分配至访问配置文件。 具有此访问配置文件的用户可以使用安全 Telnet 管理方法访问设备。
  - **"HTTP"** — 表示将 HTTP 会话分配至访问配置文件。 具有此访问配置文件的用户可以使用 HTTP 管理方法访问设备。
  - **"Secure HTTP"（安全 HTTP）** — 表示将安全 HTTP 会话分配至访问配置文件。 具有此访问配置文件的用户可以使用安全 HTTP 管理方法访问设备。
  - **"SNMP"** — 表示将 SNMP 会话分配至访问配置文件。 具有此访问配置文件的用户可以使用 SNMP 管理方法访问设备。
- **"Interface"（接口）** — 指定要应用规则的接口。 可能的字段值包括：
  - **"Port"（端口）** — 表示接口为端口，并且是为其定义了访问配置文件的特定端口。
  - **"LAG"** — 表示接口为 LAG，并且是为其定义了访问配置文件的特定 LAG。
  - **"VLAN"** — 表示接口为 VLAN，并且是为其定义了访问配置文件的特定 VLAN。
- **"Source IP Address"（源 IP 地址）** — 表示信息包应匹配的接口源 IP 地址。
- **"Network Mask"（网络掩码）** — 表示信息包应匹配的接口网络掩码。

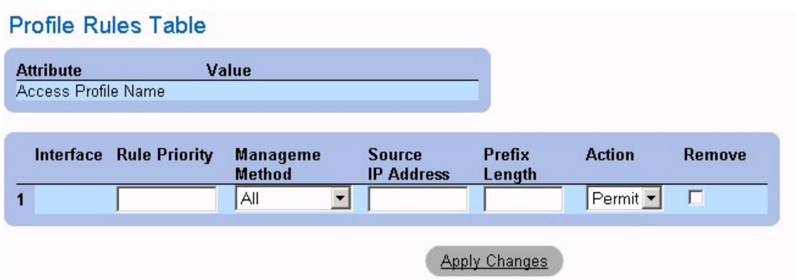
- **"Prefix Length"（前缀长度）**— 表示信息包应匹配的前缀长度。
- **"Action"（操作）**— 定义管理安全保护规则操作。 可能的字段值包括：
  - **"Permit"（允许）**— 允许对定义的接口进行管理访问。
  - **"Deny"（拒绝）**— 拒绝对定义的接口进行管理访问。

3. 定义 **"Access Profile Name"（访问配置文件名称）**字段。
4. 定义 **"Rule Priority"（规则优先级）**、**"Management Method"（管理方法）**、**"Interface"（接口）**、**"Source IP"（源 IP）**、**"Network Mask"（网络掩码）**、**"Prefix Length"（前缀长度）**和 **"Action"（操作）**字段。
5. 单击 **"Apply Changes"（应用更改）**。 系统将添加规则，并更新设备。

要查看配置文件规则表，请：

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。



配置文件规则表页面

3. 单击 **"Apply Changes"（应用更改）**。

要删除规则，请：

注： 如果删除了规则，则配置文件名称也将被删除。

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. 在 **"Profile Rules Table"（配置文件规则表）**页面中选择一条规则。
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

下表概括了用于查看 **"Access Profiles"（访问配置文件）**页面中显示的字段的等效 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 命令实例：

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

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

Console (config-macl)# permit ethernet 2/e9

Console (config-macl)# deny ethernet 1/e2

Console (config-macl)# deny ethernet 2/e10

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 2/e9
```

```
! (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）页面使网络管理员可以选择设备上的用户验证方法。 用户验证可通过以下方式进行：

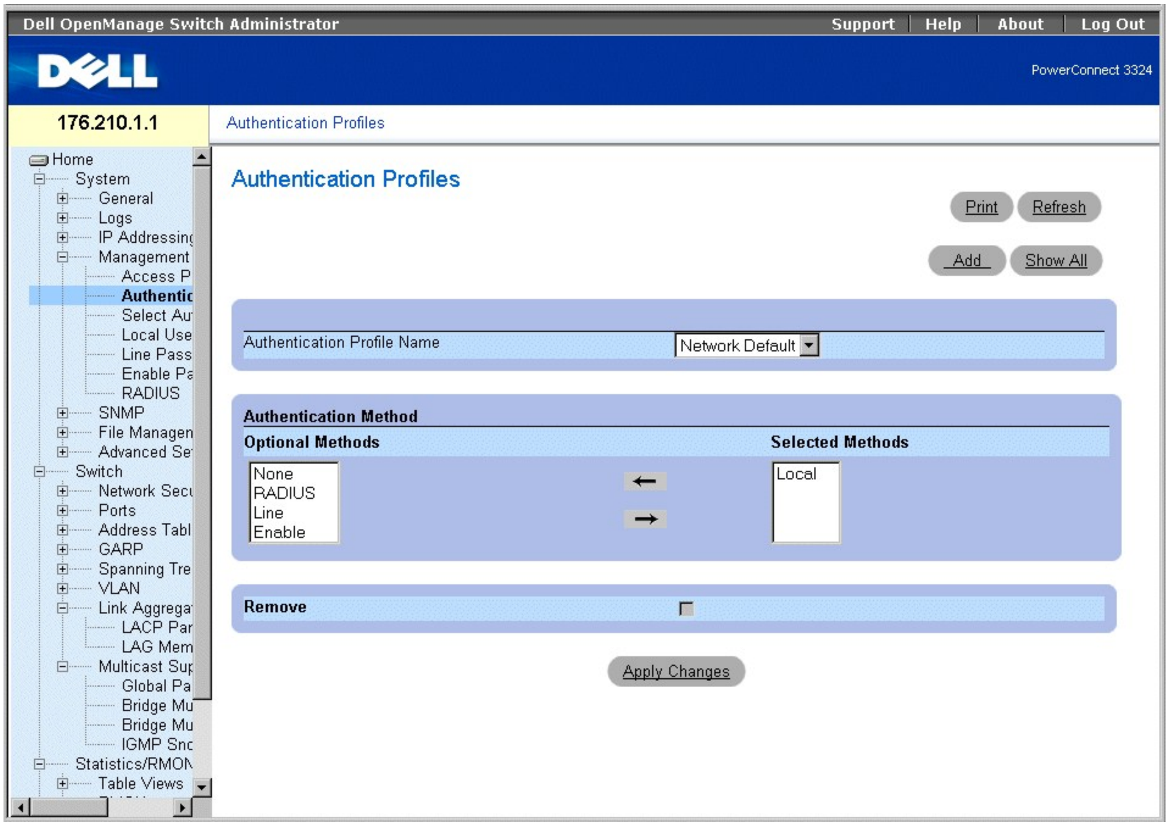
- 本地
- 通过外部服务器

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**"Local"（本地）**和**"RADIUS"**选项均被选定，则先在本地进行用户验证。 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）**。 系统将打开**"Authentication Profiles"（验证配置文件）**页面。



验证配置文件页面

"Authentication Profiles"（验证配置文件）页面包含以下选项列表：

- **"Authentication Profile Name"（验证配置文件名称）** — 显示用户定义的验证方法列表，包括以下值：
  - **"Network Default"（网络默认值）**
  - **"Console Default"（控制台默认值）**
- **"Optional Methods"（可选方法）** — 列出了用户验证方法。 可能的选项包括：
  - **"Local"（本地）** — 表示在本地进行验证。 设备将检查用户名和密码以进行验证。
  - **"None"（无）** — 表示不进行用户验证。
  - **"RADIUS"**— 表示在 RADIUS 服务器上进行用户验证。
  - **"Line"（线路）** — 表示使用线路密码进行验证。
  - **"Enable"（启用）** — 表示使用启用密码进行验证。
- **"Selected Methods"（选定方法）** — 表示选定的验证方法及其顺序。
- **"Remove"（删除）**—从 **"Authentication Profile Name"（验证配置文件名称）**列表中删除选定的验证配置文件。
  - **已选取** — 删除验证配置文件。
  - **未选取** — 保留验证配置文件。

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。

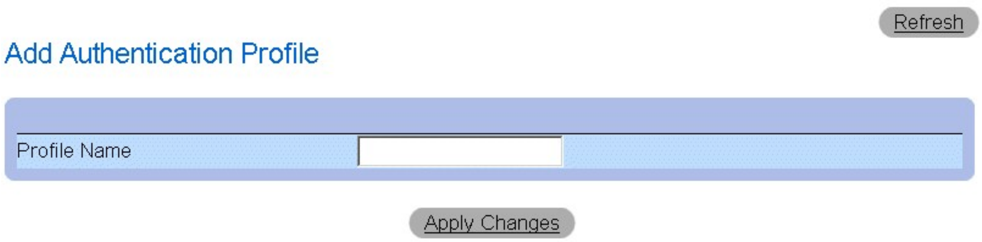
3. 使用箭头图标选择验证方法。

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**添加验证方法配置文件名称**页面。

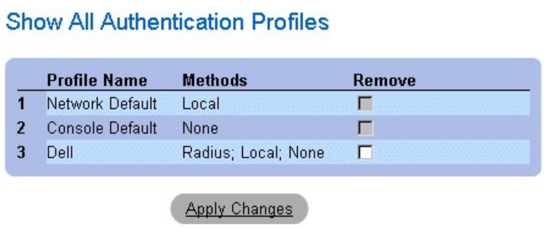


添加验证配置文件页面

打开显示所有验证配置文件页面：

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**“Open the Authentication Profile”（打开验证配置文件）**页面：



验证配置文件页面

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**“Open the Authentication Profile”（打开验证配置文件）**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

下表概括了用于查看**“Authentication Profiles”（验证配置文件）**页面中显示的字段的等效 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 命令实例：

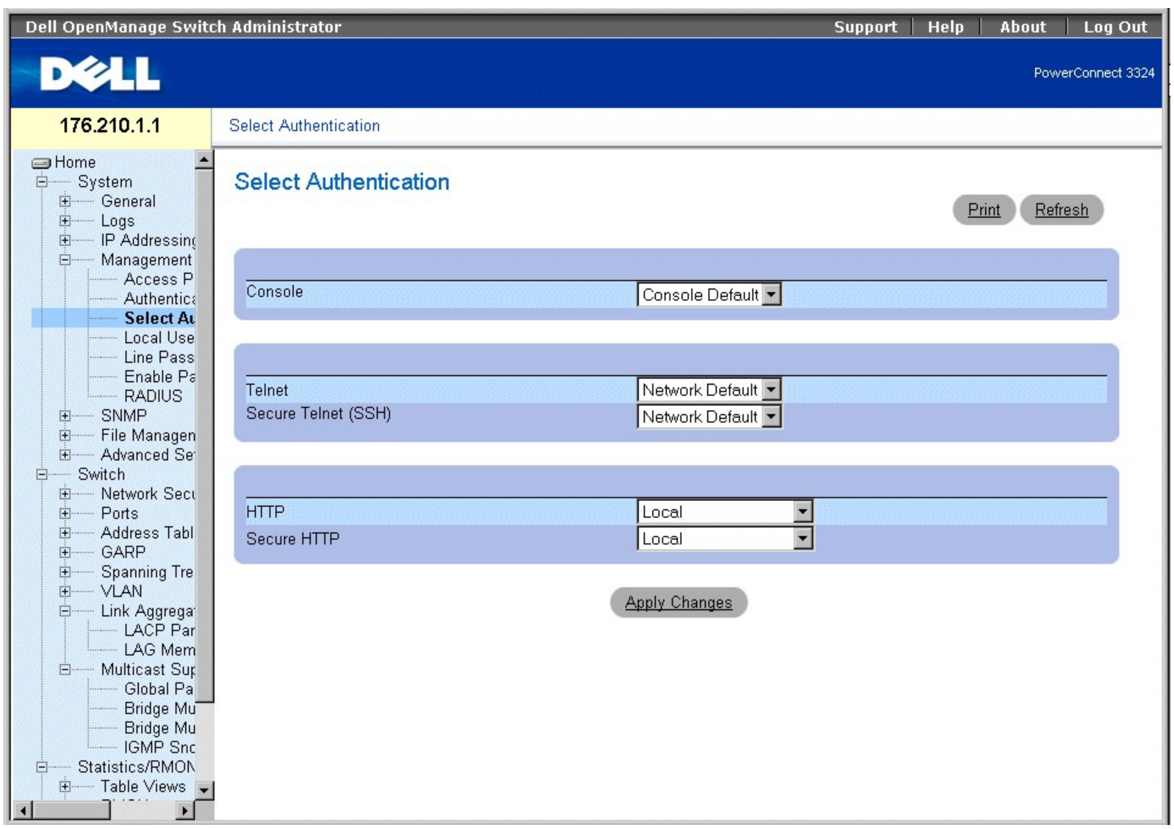
```
Console (config)# aaa authentication login default radius local enable none
```

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

分配验证配置文件

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 **"Management Authentication"（管理验证）**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）**。 系统将打开 **"Select Authentication"（选择验证）**页面。



选择验证页面

"Select Authentication"（选择验证）页面包含以下字段：

- **"Console"（控制台）**— 显示用于验证控制台用户的验证配置文件。 在"分配验证配置文件"中介绍了验证配置文件的分配。 有两个可以向

其添加其它验证配置文件的预定义字段值。 但不能删除这两个预定义的值。 预定义的字段值包括：

- **“Network Default”（网络默认值）**
- **“Console Default”（控制台默认值）**

- **“Telnet”**— 显示用于验证 Telnet 用户的验证配置文件。 在 “分配验证配置文件”中介绍了验证配置文件的分配。 有两个可以向其添加其它验证配置文件的预定义字段值。 但不能删除这两个预定义的值。 预定义的字段值包括：
  - **“Network Default”（网络默认值）**
  - **“Console Default”（控制台默认值）**
- **“Secure Telnet (SSH)”（安全 Telnet [SSH]）**— 显示用于验证 SSH 用户的验证配置文件。 安全命令解释程序 (SSH) 提供了与设备的安全远程连接。 SSH 使 SSH 客户端可以建立与设备的安全加密连接。 在“分配验证配置文件”中介绍了验证方法列表的分配。
- **“HTTP”**— 显示用于 HTTP 访问的验证方法。 可能的字段值包括：
  - **“None”（无）**— 表示没有用于 HTTP 访问的验证配置文件。
  - **“Local”（本地）**— 表示在本地进行 HTTP 验证。
  - **“Radius”**— 表示在 RADIUS 服务器上进行 HTTP 验证，并且允许 HTTP 访问。
  - **“Local, None”（本地, 无）**— 表示先在本地进行 HTTP 验证。 如果未使用验证方法，则本地用户数据库为空，并且允许 HTTP 访问。
  - **“Radius, None”（Radius, 无）**— 表示先在 RADIUS 服务器上进行 HTTP 验证。 如果未使用验证方法，则不能访问 RADIUS 服务器。
  - **“Local, Radius”（本地, Radius）**— 表示先在本地进行 HTTP 验证。 如果由 RADIUS 服务器验证用户，则本地用户数据库为空。 如果 RADIUS 服务器不能验证管理方法，则 HTTP 会话将被禁止。
  - **“Radius, Local”（Radius, 本地）**ó 表示先在 RADIUS 服务器上进行 HTTP 验证。 如果不能访问 RADIUS 服务器，HTTP 会话将在本地进行验证。 如果 HTTP 会话不能在本地验证，则 HTTP 会话将被禁止。
  - **“Local, Radius, None”（本地, Radius, 无）**— 表示先在本地进行 HTTP 验证。 如果本地数据库为空，则 RADIUS 服务器将验证管理方法。 如果不能访问 RADIUS 服务器，则允许进行 HTTP 会话。
  - **“Radius, Local, None”（Radius, 本地, 无）**— 表示先在 RADIUS 服务器上进行 HTTP 验证。 如果不能访问 RADIUS 服务器，HTTP 会话将在本地进行验证。 如果本地数据库为空，则允许进行 HTTP 会话。
- **“Secure HTTP”（安全 HTTP）**— 指定用于安全 HTTP 访问的验证配置文件。 可能的字段值包括：
  - “None”（无）— 表示没有用于安全 HTTP 访问的验证配置文件。
  - “Local”（本地）— 表示在本地进行安全 HTTP 验证。
  - “Radius”— 表示在 RADIUS 服务器上进行安全 HTTP 验证。
  - “Local, None”（本地, 无）— 表示先在本地进行安全 HTTP 验证。 如果本地数据库为空，则未使用验证方法，并允许进行安全 HTTP 访问。
  - “Radius, None”（Radius, 无）— 表示先在 RADIUS 服务器上进行安全 HTTP 验证。 如果不能访问 RADIUS 服务器，则未使用验证方法，并允许进行安全 HTTP 访问。
  - “Local, Radius”（本地, Radius）— 表示先在本地进行安全 HTTP 验证。 如果本地数据库为空，则由 RADIUS 服务器验证用户。 如果 RADIUS 服务器不能验证管理方法，则安全 HTTP 会话将被禁止。
  - “Radius, Local”（Radius, 本地）— 表示先在 RADIUS 服务器上进行安全 HTTP 验证。 如果不能访问 RADIUS 服务器，将在本地验证安全 HTTP 会话。 如果安全 HTTP 会话不能在本地验证，则安全 HTTP 会话将被禁止。
  - “Local, Radius, None”（本地, Radius, 无）— 表示先在本地进行安全 HTTP 验证。 如果本地数据库为空，则 RADIUS 服务器将验证管理方法。 如果 RADIUS 服务器不能访问数据库，则允许进行安全 HTTP 会话。
  - “Radius, Local, None”（Radius, 本地, 无）— 表示先在 RADIUS 服务器上进行安全 HTTP 验证。 如果不能访问 RADIUS 服务器，将在本地验证安全 HTTP 会话。 如果本地数据库为空，则允许进行安全 HTTP 会话。

要将验证列表应用于控制台会话，请：

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。

要将验证配置文件应用于 Telnet 会话，请：

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。

要将验证配置文件应用于安全 Telnet (SSH) 会话，请：

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。

要为 HTTP 会话分配验证顺序，请：

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。

要为安全 HTTP 会话分配验证顺序，请：

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

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

CLI 命令	**说明**
enable authentication [default | 列表名称**]**	指定从远程 Telnet 或控制台访问更高权限级别时的验证方法列表。
login authentication [default | 列表名称**]**	指定远程 Telnet 或控制台的登录验证方法列表。
ip http authentication 方法 1 **[**方法 2.**]**	指定 HTTP 服务器的验证方法。
ip https authentication 方法 1 **[**方法 2.**]**	指定 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 命令实例：

```
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

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

Default: Radius, Local, Line

Console_Login: Line, None


Enable Authentication Method Lists

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

Default: Radius, Enable

console> enable: Enable, None


Line Login Method List Enable Method List

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

Console Console_Login Console_Enable

Telnet Default Default
```

SSH Default Default

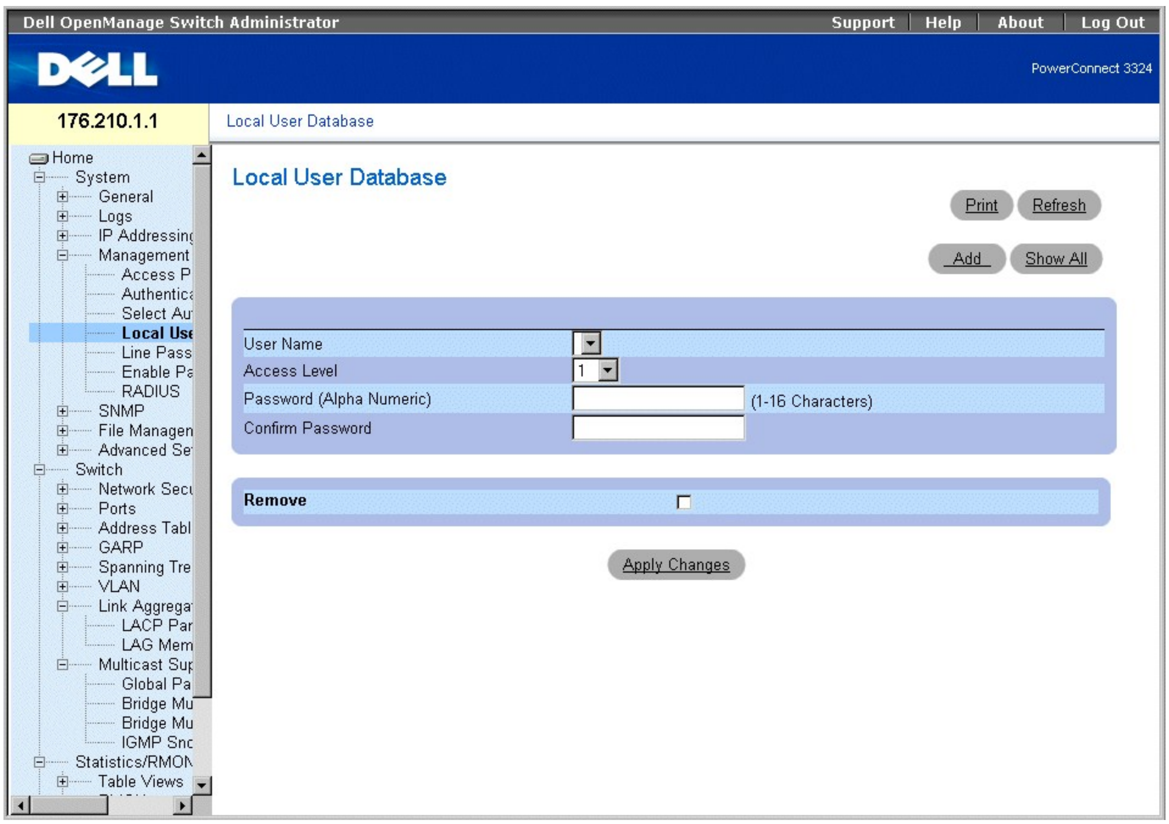
HTTP: Radius, local

HTTPS: Radius, local

定义本地用户数据库

"Local User Database"（本地用户数据库）页面使网络管理员可以定义用户、密码和访问级别。 密码最多可包含 16 个字符。 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）**。 系统将打开 **"Local User Database"（本地用户数据库）**页面。



本地用户数据库页面

"Local User Database"（本地用户数据库）页面包含以下字段：

- **"User Name"（用户名）**— 包含用户的列表。
- **"Access Level"（访问级别）**— 确定用户的访问级别。 可能的值包括：
  - **1 至 15** — 表示用户的访问级别。 **"1"**表示最低的用户访问级别。
- **"Password (Alpha Numeric)"（密码 [字母数字]）**— 指定用户密码。 密码显示为 *******。

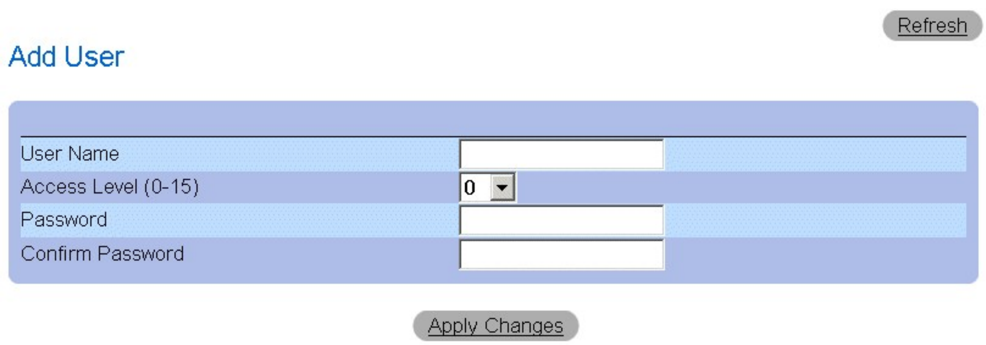
- **"Confirm Password"（确认密码）** — 确认用户定义的密码。 确认密码显示为 *******。
- **"Remove"（删除）** — 从 **"User Name"（用户名）**列表中删除用户。
  - **已选取** — 从 **"Local User Database"（本地用户数据库）**中删除特定用户。
  - 未选取 — 保留"Local User Database"（本地用户数据库）中的用户。

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 **"Access Level"（访问级别）**和 **"Password"（密码）**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：

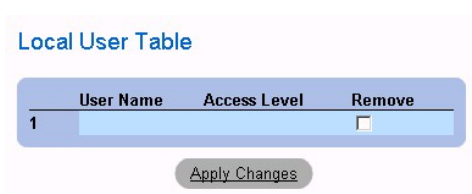


添加用户页面

3. 定义 **"User Name"（用户名）**、**"Access Level (1-15)"（访问级别 [1-15]）**、**"Password"（密码）**和 **"Confirm Password"（确认密码）**字段，以定义一个新用户。
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）**页面。



本地用户表页面

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）**页面。
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）**。 系统将删除用户，并更新设备。

使用 CLI 命令设定用户

下表概括了用于查看**“Local User Database”（本地用户数据库）**页面中显示的字段的等效 CLI 命令。

CLI 命令	说明
username 名称 **[password** 密码**] [privilege** 级别**] [encrypted]**	建立基于用户名的验证系统。

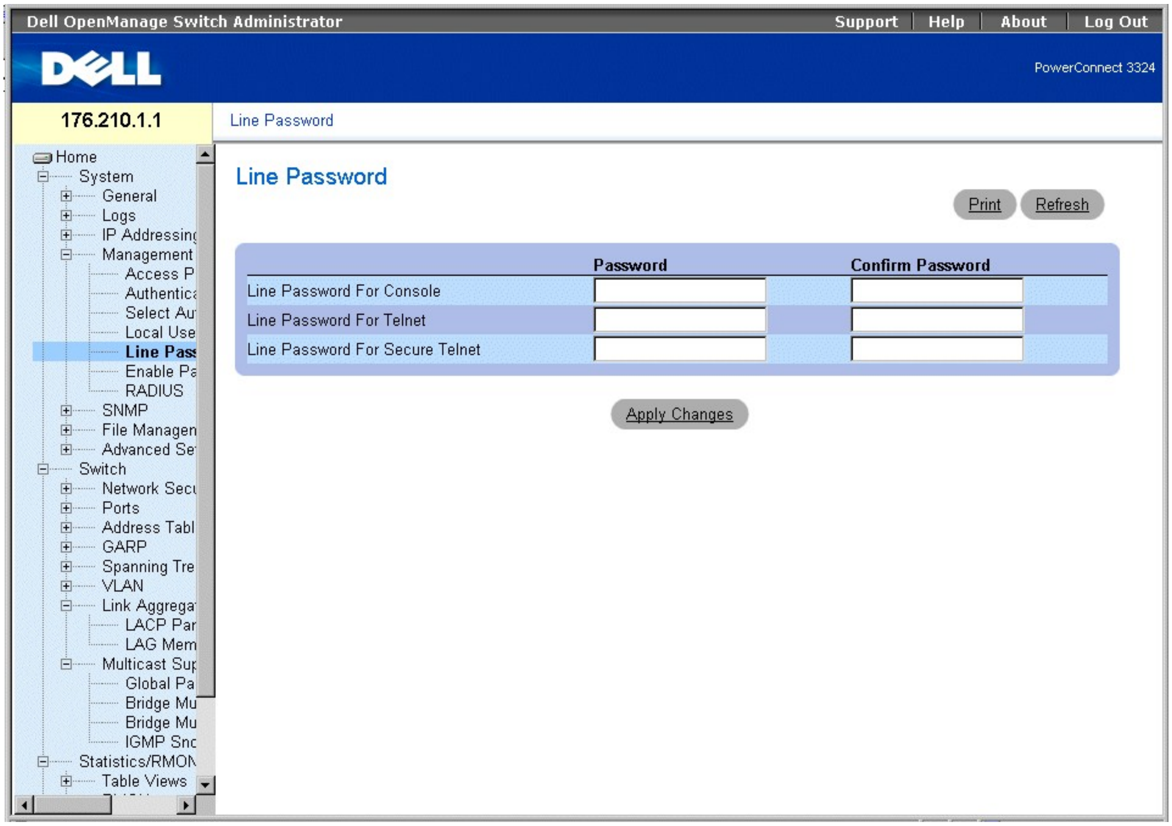
以下是 CLI 命令实例：

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

定义线路密码

“Line Passwords”（线路密码）页面使网络管理员可以定义管理方法的线路密码。 密码最多可包含 16 个字符。 要打开**“Line Passwords”（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）**。 系统将打开**“Line Passwords”（线路密码）**页面。



线路密码页面

"Line Passwords"（线路密码）页面包含以下字段：

- **"Line Password For Console"（控制台的线路密码）**— 指定通过控制台会话访问设备的线路密码。 密码显示为 *******。
- **"Line Password For Telnet"（Telnet 的线路密码）**— 指定通过 Telnet 会话访问设备的线路密码。密码显示为 *******。
- **"Line Password For Secure Telnet"（安全 Telnet 的线路密码）**— 指定通过安全 Telnet 会话访问设备的线路密码。 密码显示为 *******。

要定义控制台会话的线路密码，请：

1. 打开**"Line Password"（线路密码）**页面。
2. 定义**"Line Password For Console"（控制台的线路密码）**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。

要定义 Telnet 会话的线路密码，请：

1. 打开**"Line Password"（线路密码）**页面。
2. 定义**"Line Password For Telnet"（Telnet 的线路密码）**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。

要定义安全 Telnet 会话的线路密码，请：

1. 打开**"Line Password"（线路密码）**页面。

2. 定义 **“Line Password for Secure Telnet”（安全 Telnet 的线路密码）**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

下表概括了用于查看 **“Line Password”（线路密码）**页面中显示的字段的等效 CLI 命令。

CLI 命令	**说明**
password 密码 **[encrypted]**	指定线路上的密码。

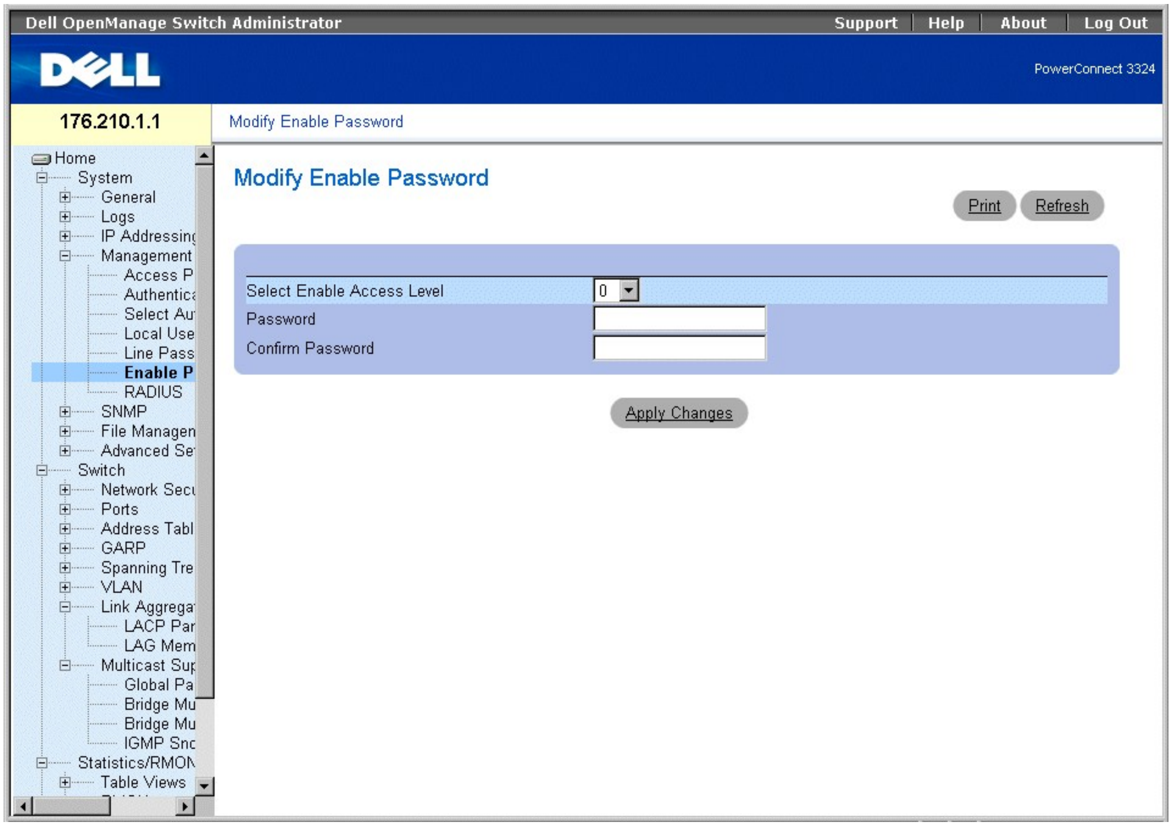
以下是 CLI 命令实例：

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

定义启用密码

“Modify Enable Password”（修改启用密码）页面可以设置本地密码，以控制对普通、优先和全局配置的访问。 要打开 **“Modify Enable Password”（修改启用密码）**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）**。 系统将打开 **“Modify Enable Password”（修改启用密码）**页面。



修改启用密码页面

"Modify Enable Password"（修改启用密码）页面包含以下字段：

- **"Select Enable Access Level"（选择启用访问级别）** — 指定与启用密码相关联的访问级别。
- **"Password"（密码）** — 表示启用密码。密码显示为 *******。
- **"Confirm Password"（确认密码）** — 确认新的启用密码。 确认密码显示为 *******。

要定义新的启用密码，请：

1. 打开**"Modify Enable Password"（修改启用密码）**页面。
2. 定义**"Select Enable Access Level"（选择启用访问级别）**、**"Password"（密码）**和**"Confirm Password"（确认密码）**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

下表概括了用于查看**"Modify Enable Password"（修改启用密码）**页面中显示的字段的等效 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。
show users accounts	显示有关本地用户数据库的信息。

以下是 CLI 命令实例：

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

Console# show users accounts



Username Privilege

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

Bob 15

Robert 15
```

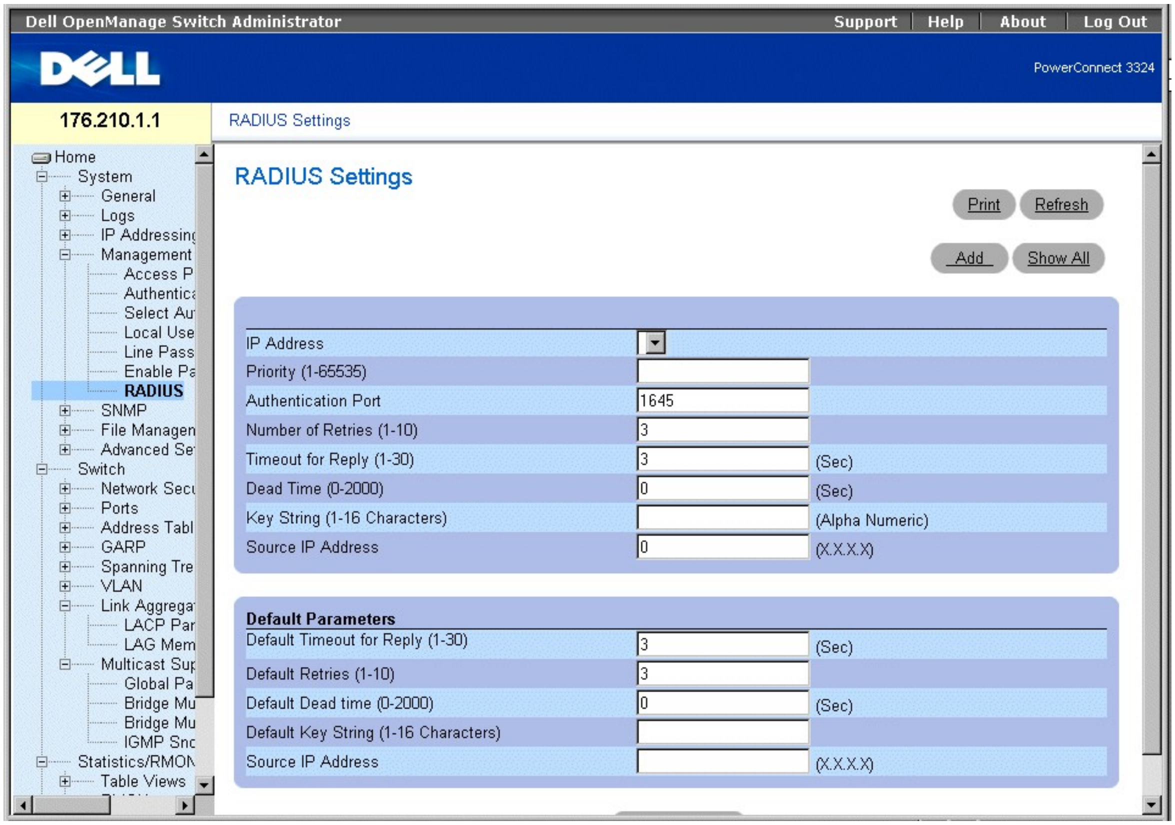
配置 RADIUS 全局参数

远程认证拨入用户服务 (RADIUS) 服务器为网络提供了附加安全保护。 RADIUS 服务器为以下操作提供了集中式的验证方法：

- Telnet 访问
- Web 访问
- 控制台对交换机的访问

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"**。 系统将打开 **"RADIUS Settings"（RADIUS 设置）**页面。



RADIUS 设置页面

"RADIUS Settings"（RADIUS 设置）页面包含以下字段：

- **"IP Address"（IP 地址）**— 表示验证服务器 IP 地址的列表。
- **"Priority (1-65535)"（优先级 [1-65535]）**— 表示服务器的优先级。 可能的值为 1 至 65535，其中 1 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 [1-10]）**— 指定在失败前发送至 RADIUS 服务器的请求被传输的次数。 可能的字段值为 1 至 10，默认值为 3。
- **"Timeout for Reply (1-30)"（回复超时 [1-30]）**— 指定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，默认值为 3。
- **"Dead Time (0-2000)"（停用时间）**— 指定不经过 RADIUS 服务器进行服务请求的时间（以秒为单位）。 范围为 0 至 2000。
- **"Key String (1-16 Characters)"（关键字字符串 [1-16 个字符]）**— 表示用于验证和加密设备与 RADIUS 服务器之间所有 RADIUS 通信的关键字字符串。 此关键字已被加密。
- **"Source IP Address"（源 IP 地址）**— 表示设备访问 RADIUS 服务器时要使用的 IP 地址。

以下字段设置了 RADIUS 的默认值：

- **"Default Timeout for Reply (1-30)"（默认回复超时 [1-30]）**— 指定超时之前设备等待 RADIUS 服务器回复的默认时间（以秒为单位）。

注： 如果未指定**"Host Specific Timeouts"（主机特定超时）**、**"Retransmit"（重新发送）**、**"Dead Time"（停用时间）**或**"Deny"（拒绝）**的值，则全局值将应用到每个主机。

- **"Default Retries (1-10)"（默认重试次数 [1-10]）**— 指定在失败前发送至 RADIUS 服务器的请求被传输的默认次数。

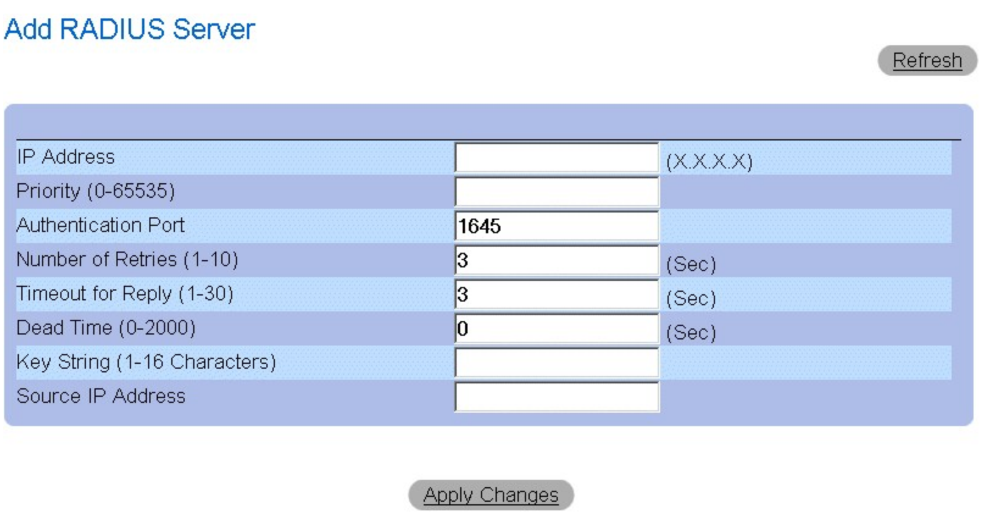
- **"Default Dead time (0-2000)"（默认停用时间 [0-2000]）**— 指定不经过 RADIUS 服务器进行服务请求的默认时间（以秒为单位）。 范围为 0 至 2000。
- **"Default Key String (1-16 Characters)"（默认关键字字符串 [1-16 个字符]）**— 表示用于验证和加密设备与 RADIUS 服务器之间所有 RADIUS 通信的默认关键字字符串。 此关键字已被加密。
- **"Source IP Address"（源 IP 地址）**— 表示设备访问 RADIUS 服务器时要使用的默认 IP 地址。

要定义 RADIUS 参数，请：

1. 打开**"RADIUS Settings"（RADIUS 设置）**页面。
2. 定义**"Default Timeout for Reply"（默认回复超时）**、**"Default Retries"（默认重试次数）**、**"Default Dead Time"（默认停用时间）**和**"Default Key Strings"（默认关键字字符串）**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 Settings"（添加 RADIUS 设置）**页面：



添加 RADIUS 服务器页面

3. 定义**"IP Address"（IP 地址）**、**"Priority"（优先级）**、**"Authentication Port"（验证端口）**、**"Number of Retries"（重试次数）**、**"Timeout for Reply"（回复超时）**、**"Dead Time"（停用时间）**、**"Key String"（关键字字符串）**和**"Source IP Address"（源 IP 地址）**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）**页面。

	IP Address	Authentication Port	Number of Retries	Timeout for Reply	Dead Time	Priority	Remove
1							☐

RADIUS 服务器列表页面

要修改 RADIUS 服务器设置，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）**页面。
3. 修改**“Priority”（优先级）**、**“Number of Retries”（重试次数）**、**“Timeout for Reply”（回复超时）**或**“Dead Time”（停用时间）**字段。
4. 单击**“Apply Changes”（应用更改）**。 系统将修改 RADIUS 服务器设置，并更新设备。

要删除 RADIUS 服务器列表中的 RADIUS 服务器，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）**页面。
3. 在**“RADIUS Servers List”（RADIUS 服务器列表）**中选择一个 RADIUS 服务器。
4. 选取**“Remove”（删除）**复选框。 系统将从**“RADIUS Servers List”（RADIUS 服务器列表）**中删除 RADIUS 服务器。

使用 CLI 命令定义 RADIUS 服务器

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

CLI 命令	说明
radius-server timeout 超时	设置设备等待服务器主机回复的默认时间间隔。
radius-server retransmit 重试次数	指定软件搜索 RADIUS 服务器主机列表的默认次数。
radius-server deadtime 停用时间	配置要被忽略的不可用默认服务器。
radius-server key 关键字字符串	为设备与 RADIUS 环境之间的所有 RADIUS 通信设置默认的验证和加密关键字。
radius-server host IP 地址 **[auth-port** 验证端口号**] [timeout** 超时**] [retransmit** 重试次数**] [deadtime** 停用时间**] [key** 关键字字符串**] [source** 源**] [priority** 优先级**]**	指定 RADIUS 服务器主机和所有非默认设置。
show radius-servers	显示 RADIUS 服务器设置。

以下是 CLI 命令实例：

```
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 1645 timeout 20

Console# show radius-servers

Port

IP address Auth Acct TimeOut Retransmit deadtime Priority

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

172.16.1.1 1645 1646 3 3 0 1

172.16.1.2 1645 1646 11 8 0 2
```

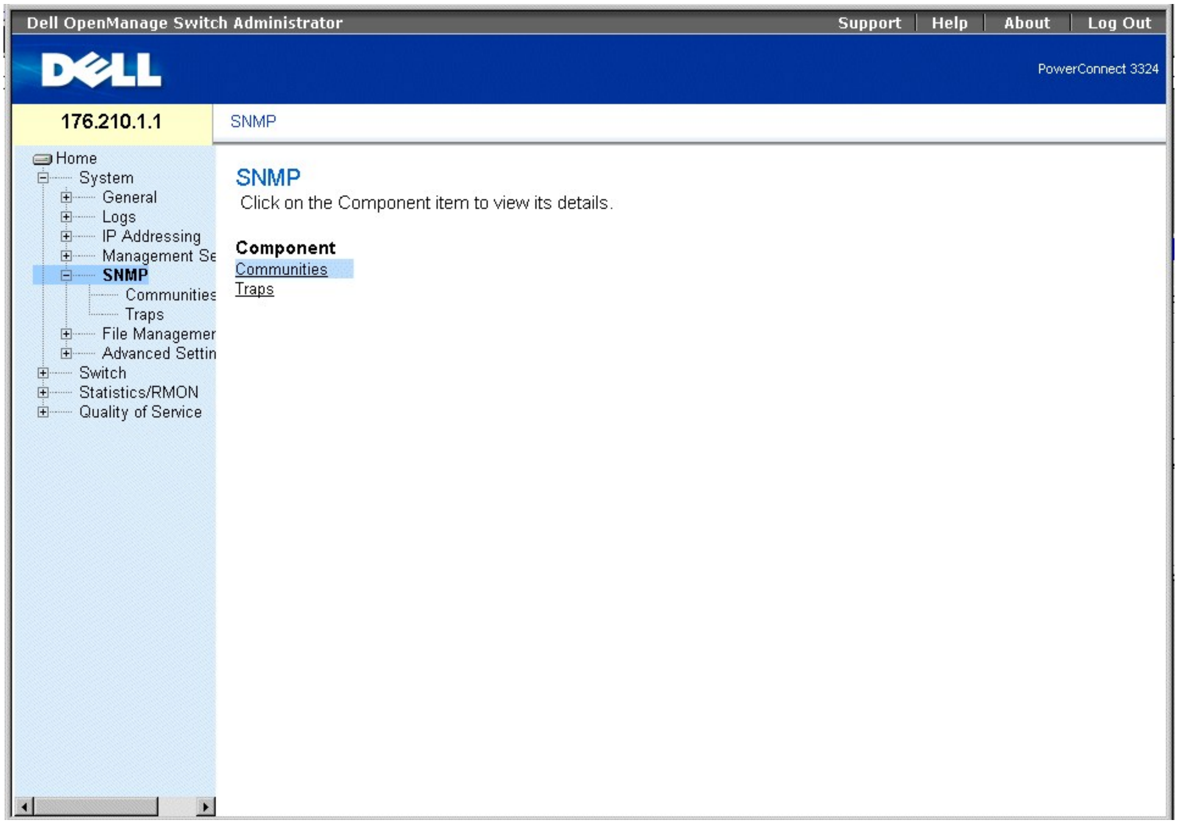
定义 SNMP 参数

简单网络管理协议 (SNMP) 提供了一种管理网络设备的方法。 支持 SNMP 的设备运行本地软件（代理）。

SNMP 代理维护用于管理设备的变量列表。 这些变量在管理信息库 (MIB) 中定义。 MIB 提供了由代理控制的变量。 SNMP 协议定义了 MIB 规格的格式以及用于通过网络访问信息的格式。

对 SNMP 代理的访问权限由访问字符串控制。 为与设备进行通信，嵌入式 Web 服务器将提交有效的团体字符串以供验证。 要打开“SNMP”页面，请：

- 在树视图中单击 **“System”（系统）>“SNMP”**。 系统将打开 **“SNMP”**页面。



SNMP 页面

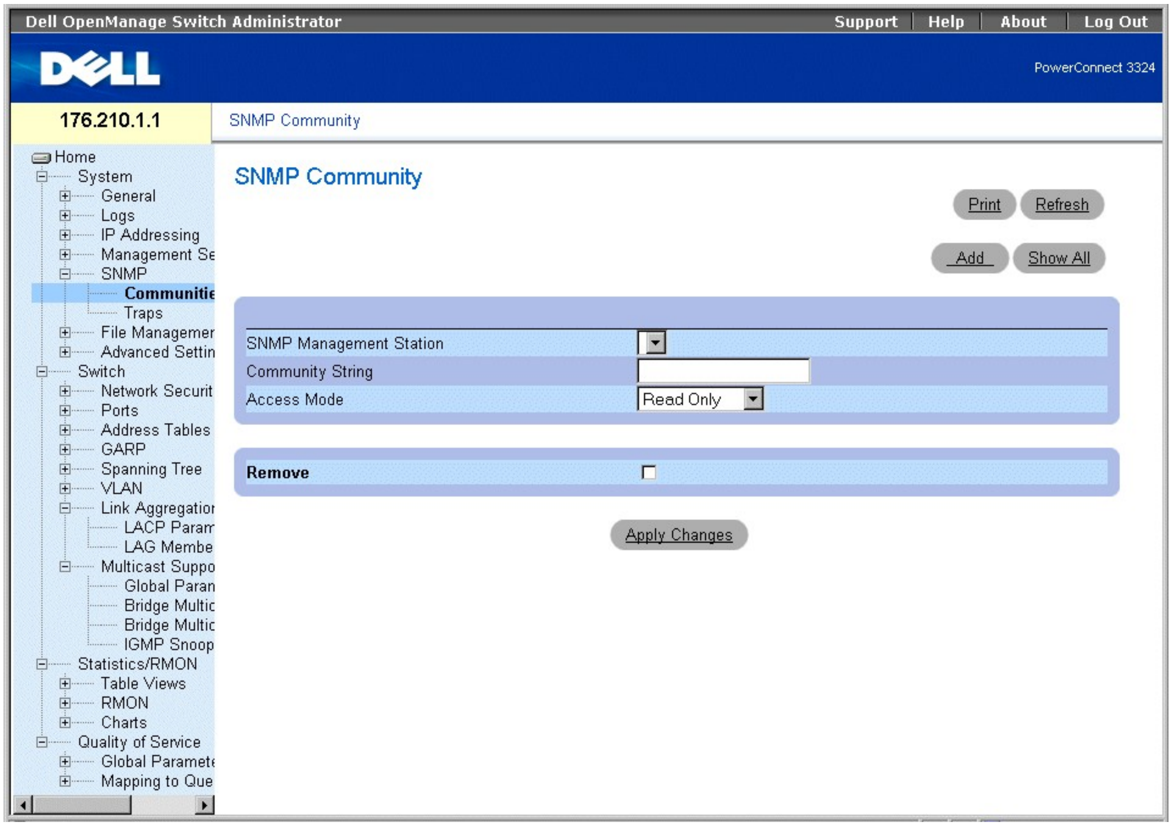
本节包含用于管理 SNMP 配置的信息，并包括以下主题：

- 定义团体
- 定义陷阱

定义团体

系统管理员通过在团体表中定义团体来管理访问权限（读写和只读等等）。 更改团体名称时，
访问权限也随之更改。 要打开**“SNMP Community”（SNMP 团体）**页面，请：

- 在树视图中单击**“System”（系统）>“SNMP”>“Communities”（团体）**。 系统将打开**“SNMP Community”（SNMP 团体）**页面。



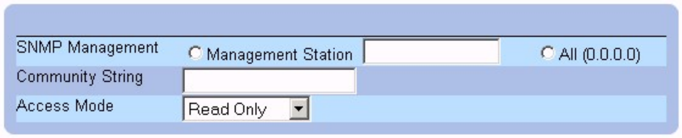
SNMP 团体页面

"SNMP Community"（SNMP 团体）页面包含以下字段：

- **"SNMP Management Station"（SNMP 管理站点）** — 显示管理站点 IP 地址的列表。
- **"Community String"（团体字符串）** — 相当于密码，用于验证连接至设备的选定管理站点。
- **"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）** — 表示管理访问被限制为只读，不能对团体进行更改。
  - **"Read Write"（读写）** — 表示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）** — 表示用户具有访问所有设备配置选项以及修改团体的权限。
- **"Remove"（删除）** — 删除团体。 可能的字段值包括：
  - **已选取** — 删除团体。
  - **未选取** — 保留团体。

要定义新团体，请：

1. 打开**"SNMP Community"（SNMP 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。



添加 SNMP 团体页面

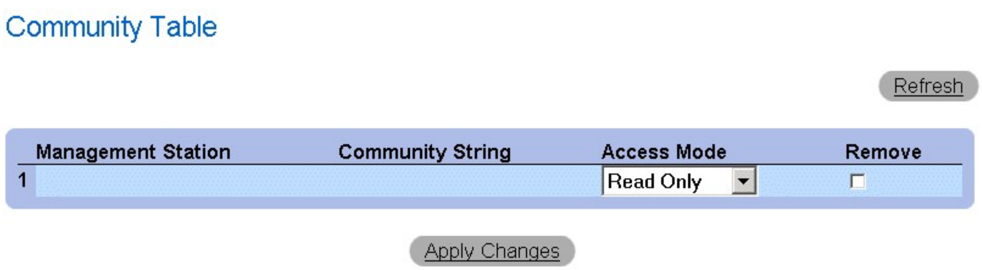
除了 **"SNMP Community"(SNMP 团体)**页面中的字段外，**"Add SNMP Community"
(添加 SNMP 团体)**页面还包含以下字段:

- **"SNMP Management"(SNMP 管理)**— 表示 SNMP 团体的定义是针对特定管理站点，还是针对所有管理站点。 可能的字段值包括:
  - **"Management Station"(管理站点)**— 表示管理站点 IP 地址。 值 0.0.0.0 将指定所有管理站点。
  - "All"(所有)— 表示针对所有管理站点定义 SNMP 团体。

3. 定义 **"SNMP Management"(SNMP 管理)**、**"Management Station"(管理站点)**、**"Community String"(团体字符串)**和 **"Access Mode"(访问模式)**字段。
4. 单击 **"Apply Changes"(应用更改)**。 系统将保存新团体，并更新设备。

要显示所有团体，请

1. 打开 **"SNMP Community"(SNMP 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。



团体表页面

要删除团体，请:

1. 打开 **"SNMP Community"(SNMP 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. 在 **"Community Table"(团体表)**中选择一个团体。
4. 选取 **"Remove"(删除)**复选框。
5. 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 **"SNMP Community"(SNMP 团体)**页面中显示的字段的等效 CLI 命令。

CLI 命令	**说明**
snmp-server community 字符串 **[ro | rw | su] [**IP 地址**]**	设置团体访问字符串以允许对 SNMP 协议进行访问。

show snmp	查看 SNMP 通信的状态。

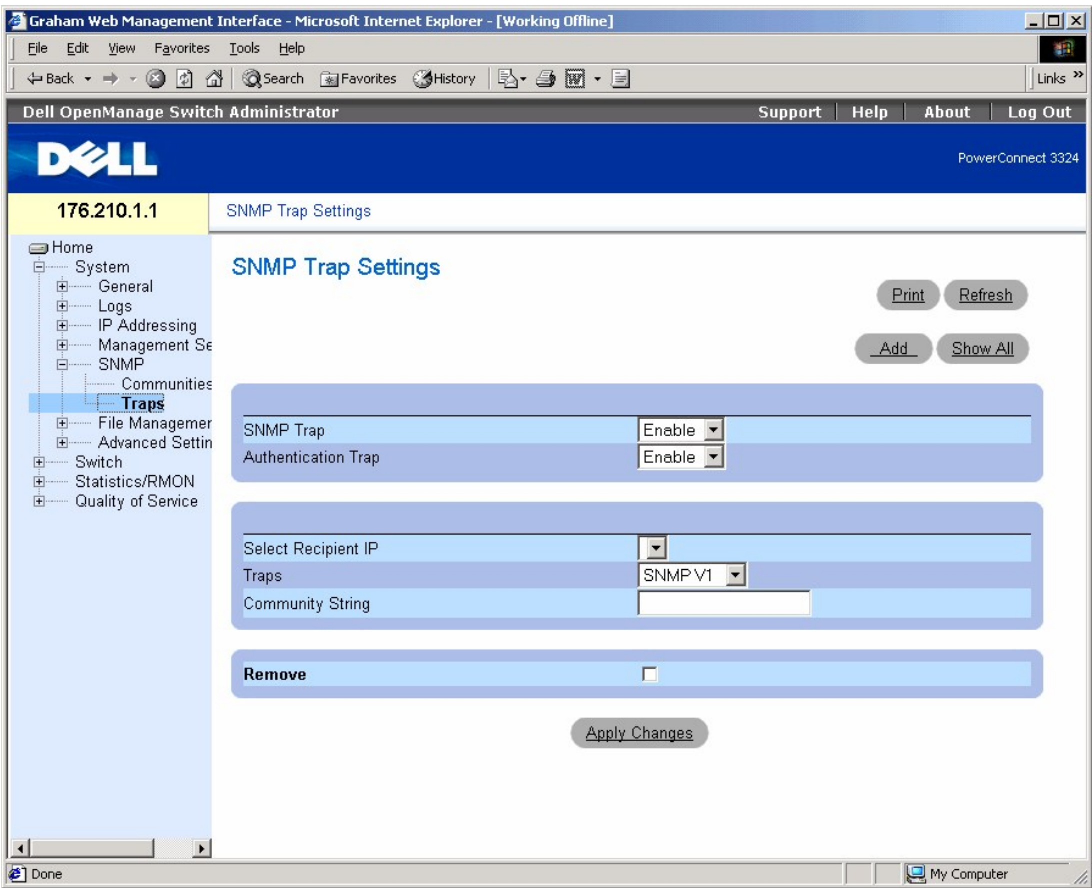
以下是 CLI 命令实例：

```
Console (config)# snmp-server community public su 0.0.0.0
```

定义陷阱

在 **“SNMP Trap Settings”（SNMP 陷阱设置）**页面中，用户可以启用或禁用设备发送 SNMP 陷阱或通知的功能。 要打开 **“SNMP Trap Settings”（SNMP 陷阱设置）**页面，请：

- 在树视图中单击 **“System”（系统）>“SNMP”>“Traps”（陷阱）**。 系统将打开 **“SNMP Trap Settings”（SNMP 陷阱设置）**页面。



SNMP 陷阱设置页面

“SNMP Trap Settings”（SNMP 陷阱设置）页面包含以下字段：

- **“SNMP Trap”（SNMP 陷阱）**— 启用将 SNMP 陷阱或 SNMP 通知从交换机发送到已定义的陷阱接收设备。 可能的字段值包括：
  - “Enable”（启用）— 允许发送 SNMP 陷阱或 SNMP 通知。
  - “Disable”（禁用）— 停止发送所有 SNMP 陷阱。
- **“Authentication Trap”（验证陷阱）**— 启用在验证失败时将 SNMP 陷阱发送到已定义的接收设备。 可能的字段值包括：

  - “Enable”（启用）－ 允许在验证失败时发送 SNMP 陷阱。
  - “Disable”（禁用）－ 禁止在验证失败时发送 SNMP 陷阱。
- **“Select Recipient IP”（选择接收设备 IP）**－ 指定陷阱发送到的 IP 地址。
- **“Traps”（陷阱）**－ 确定发送到选定接收设备的陷阱类型。 可能的字段值包括：
  - **“SNMP V1”**－ 表示发送 SNMP 版本 1 陷阱。
  - **“SNMP V2c”**－ 表示发送 SNMP 版本 2 陷阱。
  - **“Disable”（禁用）**－ 禁止将陷阱发送到接收设备。
- **“Community String”（团体字符串）**－ 标识陷阱管理器的团体字符串。
- **“Remove”（删除）**－ 删除 **“Trap Manager Table”（陷阱管理器表）**的条目。
  - **已选取** － 删除 **“Trap Manager Table”（陷阱管理器表）**条目。
  - **未选取** － 保留 **“Trap Manager Table”（陷阱管理器表）**条目。

要在设备上启用 SNMP 陷阱，请：

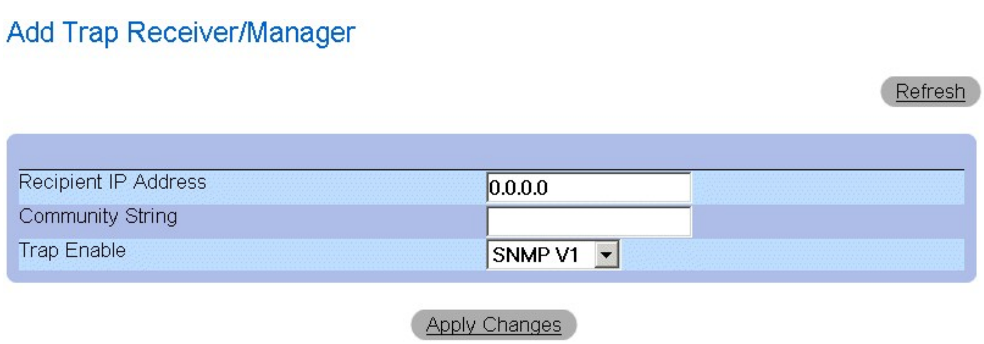
1. 打开 **“SNMP Trap Settings”（SNMP 陷阱设置）**页面。
2. 在 **“SNMP Trap”（SNMP 陷阱）**下拉列表中选择 **“Enable”（启用）**。
3. 定义 **“Select Recipient IP”（选择接收设备 IP）**、**“Traps”（陷阱）**和 **“Community String”（团体字符串）**字段。
4. 单击 **“Apply Changes”（应用更改）**。 系统将在设备上启用 SNMP 陷阱。

要在设备上启用验证陷阱，请：

1. 打开 **“SNMP Trap Settings”（SNMP 陷阱设置）**页面。
2. 在 **“Authentication Trap”（验证陷阱）**下拉列表中选择 **“Enable”（启用）**。
3. 定义 **“Select Recipient IP”（选择接收设备 IP）**、**“Traps”（陷阱）**和 **“Community String”（团体字符串）**字段。
4. 单击 **“Apply Changes”（应用更改）**。 系统将在设备上启用验证陷阱。

要添加新的陷阱接收设备，请：

1. 打开 **“SNMP Trap Settings”（SNMP 陷阱设置）**页面。
2. 单击 **“Add”（添加）**。 系统将打开 **“Add Trap Receiver/Manager”（添加陷阱接收设备/管理器）**页面。



添加陷阱接收设备/管理器页面

3. 定义**“Recipient IP Address”（接收设备 IP 地址）**、**“Community String”（团体字符串）**和**“Trap Enable”（陷阱启用）**字段。（请注意 0.0.0.0 表示“所有”，并广播陷阱。）

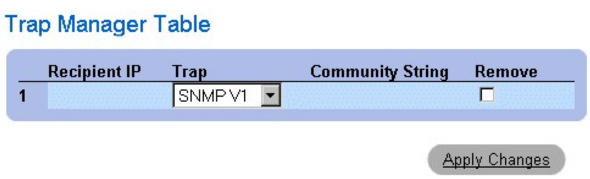
4. 单击**“Apply Changes”（应用更改）**。系统将添加陷阱接收设备/管理器，并更新设备。

要显示陷阱管理器表，请：

“Trap Managers Table”（陷阱管理器表）包含用于配置陷阱类型的字段。

1. 打开**“Traps”（陷阱）**页面。

2. 单击**“Show All”（全部显示）**。 系统将打开**“Trap Managers Table”（陷阱管理器表）**页面。



陷阱管理器表页面

要删除陷阱管理器表条目，请：

1. 打开**“SNMP Trap Settings”（SNMP 陷阱设置）**页面。

2. 单击**“Show All”（全部显示）**。 系统将打开**“Trap Managers Table”（陷阱管理器表）**页面。

3. 选择**“Trap Managers Table”（陷阱管理器表）**条目。

4. 选取**“Remove”（删除）**复选框。

5. 单击**“Apply Changes”（应用更改）**。 系统将删除陷阱管理器，并更新设备。

使用 CLI 命令配置陷阱

下表概括了用于查看**“SNMP Trap Settings”（SNMP 陷阱设置）**页面中显示的字段的等效 CLI 命令。

CLI 命令	**说明**
snmp-server enable traps	允许交换机发送 SNMP 陷阱或 SNMP 通知。
snmp-server trap authentication	允许交换机在验证失败时发送 SNMP 陷阱。
snmp-server host 主机地址 团体字符串 [1 | 2]	确定发送到选定接收设备的陷阱类型。
show snmp	显示 SNMP 通信状态。

以下是 CLI 命令实例：

```
Console (config)# snmp-server enable traps
```

```
Console (config)# snmp-server trap authentication

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

Console (config)# exit

Console# show snmp


Community-String Community-Access IP address

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

public read only All

private read write 172.16.1.1

private read write 172.17.1.1


Traps are enabled.

Authentication trap is enabled.


Trap-Rec-Address Trap-Rec-Community Version

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

192.122.173.42 public 2


System Contact: Robert

System Location: Marketing
```

管理文件

"File Management"（文件管理）页面使网络管理员可以管理设备软件、映像文件和配置文件。 文件可从 TFTP 服务器下载。

文件管理概览

配置文件由以下文件构成：

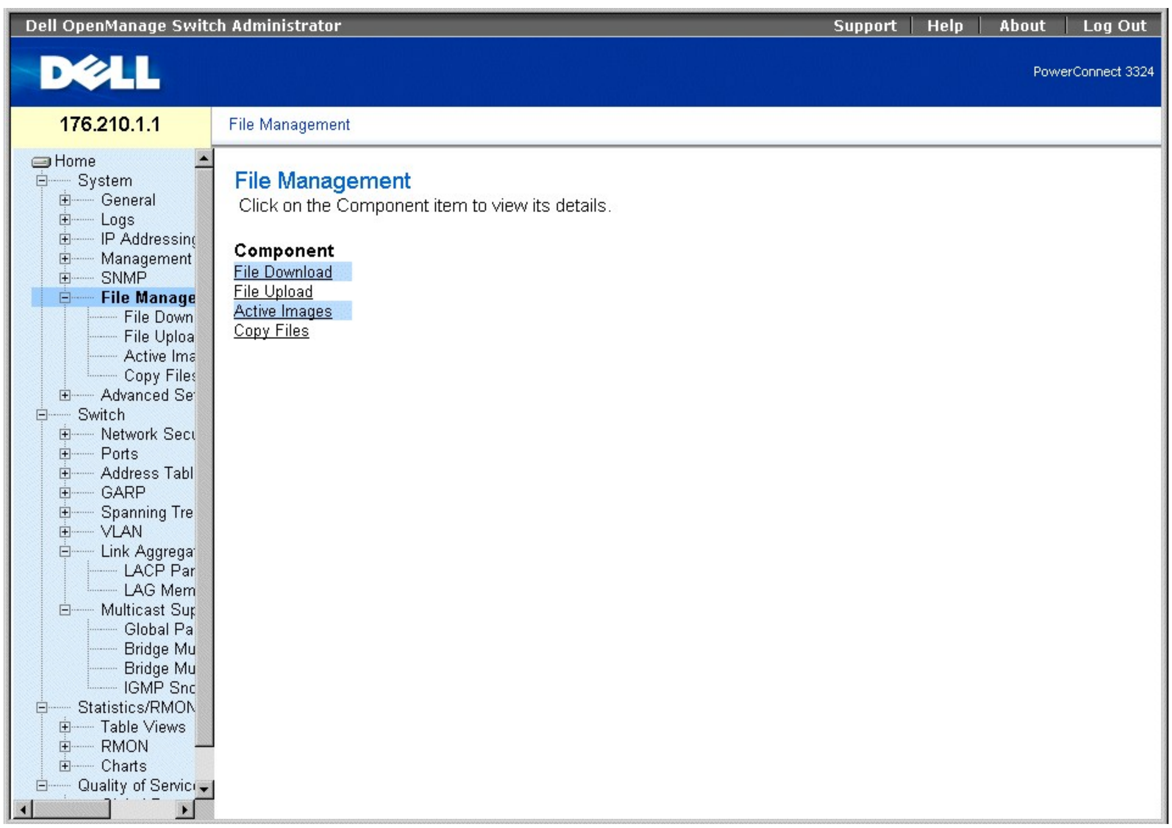
- 启动配置文件 — 在设备断电或重新引导时维护完整的设备配置。 启动文件可以维护配置命令，并且正在运行的配置文件中的配置命令可以保存到启动文件。
- 正在运行的配置文件 — 包含所有启动文件命令以及在当前会话过程中输入的所有命令。 设备断电或重新引导后，所有存储在正在运行的配置文件中的命令均会丢失。 启动期间，启动文件中的所有命令将被复制到正在运行的配置文件中，并应用于设备。 会话期间，输入的所有新命令将被添加到正在运行的配置文件中存在的命令中。 命令不会被覆盖。 要更新启动文件，必须先将正在运行的配置文件复制到启动配置文件中，然后再断开设备的电源连接。 下次重新启动设备时，这些命令将从启动配置文件复制回正在运行的配置文件中。

注： 配置命令将与正在运行的配置文件合并，并立即应用于设备。

- 备份配置文件 — 包含设备配置的备份副本。 正在运行的配置文件或启动文件被复制到备份文件时，备份文件将发生更改。 复制到备份文件的命令将替换备份文件中保存的现有命令。 可以将备份文件的内容复制到正在运行的配置文件或启动配置文件中。
- 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 FLASH 文件中。 活动映像存储活动副本，另一个映像存储次副本。 设备从活动映像进行引导并运行。 如果活动映像损坏，系统将自动从非活动映像进行引导。 这种安全功能可用于防止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）**。
  系统将打开**"File Management"（文件管理）**页面。



文件管理页面

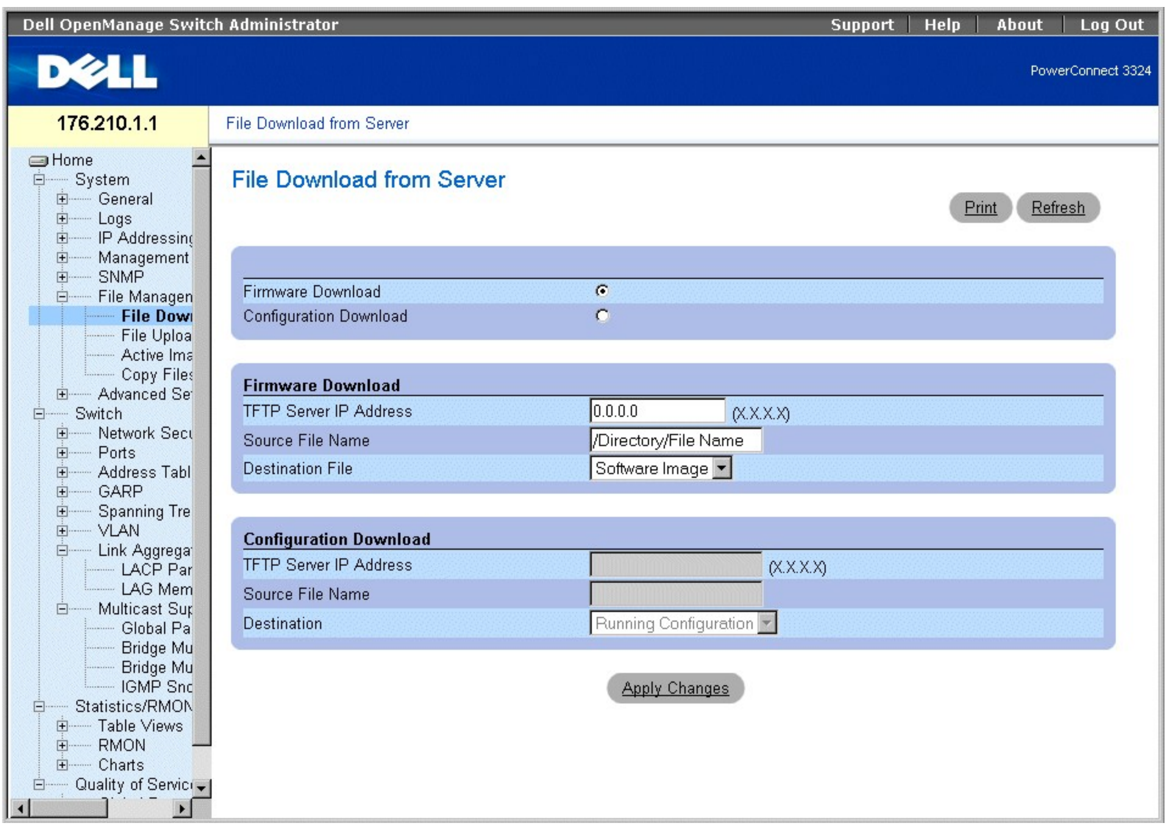
"File Management"（文件管理）页面包含指向以下内容的链接：

- 下载文件
- 加载文件
- 重设活动映像
- 复制和删除文件

下载文件

"File Download from Server"（从服务器下载文件）页面包含用于将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）**。 系统将打开**"File Download from Server"（从服务器下载文件）**页面。



从服务器下载文件页面

"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）**— 表示下载固件文件。 如果选定了**"Firmware Download"（固件下载）**，则**"Configuration Download"（配置下载）**字段将呈灰色。
- **"Configuration Download"（配置下载）**— 表示下载配置文件。 如果选定了**"Configuration Download"（配置下载）**，则**"Firmware Download"（固件下载）**字段将呈灰色。

- **“Firmware Download TFTP Server IP Address”（固件下载 TFTP 服务器 IP 地址）**— 表示下载文件所在的 TFTP 服务器 IP 地址。
- **“Firmware Download Source File Name”（固件下载源文件名）**— 指定要下载的文件。
- **“Firmware Download Destination File”（固件下载目标文件）**— 表示文件下载到的目标文件的类型。 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 File TFTP Server IP Address”（配置下载文件 TFTP 服务器 IP 地址）**— 表示下载配置文件所使用的 TFTP 服务器 IP 地址。
- **“Configuration Download File Source File Name”（配置下载文件源文件名）**— 指定要下载的配置文件。
- **“Configuration Download File Destination”（配置下载文件目的地）**— 表示配置文件下载到的目标文件。 可能的字段值包括：
  - **“Running Configuration”（正在运行的配置）**— 将命令下载到正在运行的配置文件中。
  - **“Startup Configuration”（启动配置）**— 下载启动配置文件并将其覆盖。
  - **“Backup Configuration”（备份配置）**— 下载备份配置文件并将其覆盖。

要下载文件，请：

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**“TFTP Server IP Address”（TFTP 服务器 IP 地址）**、**“Source File Name”（源文件名）**和**“Destination File”（目标文件）**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“重启动设备”。

使用 CLI 命令下载文件

下表概括了用于查看**“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。

CLI 命令	说明
copy 源 URL 目的地 URL **[snmp]**	将文件从源复制到目的地。

以下是 CLI 命令实例：

```
console# copy running-config tftp://11.1.1.2/pp.txt
```

注： 每个 ! 表示已成功传输十个信息包。

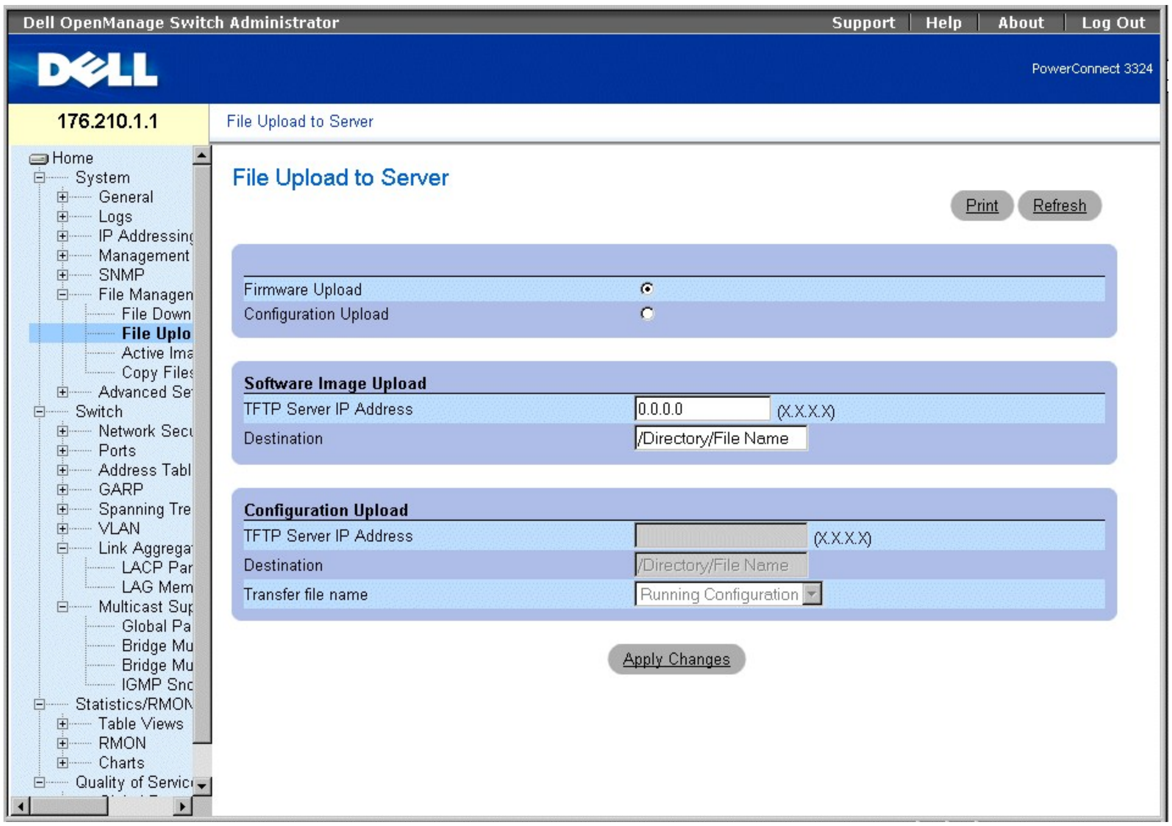
```
Accessing file 'file1' on 172.16.101.101.

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

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

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

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 TFTP 服务器加载到设备的字段。 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）**。 系统将打开**"File Upload to Server"（将文件加载至服务器）**页面：



将文件加载至服务器页面

"File Upload to Server"（将文件加载至服务器）页面包含以下字段：

- "Firmware Upload"（固件加载）— 表示加载固件文件。 如果选定了**"Firmware Upload"（固件加载）**，则**"Configuration Upload"（配置加载）**字段将呈灰色。
- **"Configuration Upload"（配置加载）**— 表示加载配置文件。 如果选定了**"Configuration Upload"（配置加载）**，则**"Software Image Upload"（软件映像加载）**字段将呈灰色。
- **"Software Image Upload TFTP Server IP Address"（软件映像加载 TFTP 服务器 IP 地址）**— 表示软件映像要加载到的 TFTP 服务器 IP 地址。
- **"Software Image Upload Destination"（软件映像加载目的地）**— 指定文件要加载到的软件映像文件路径。

- **"Configuration Upload TFTP Server IP Address"（配置加载 TFTP 服务器 IP 地址）**— 表示配置文件要加载到的 TFTP 服务器 IP 地址。
- **"Configuration Upload Destination"（配置加载目的地）**— 指定加载文件使用的配置文件路径。
- **° × Configuration Upload Transfer file name"（配置加载传输文件名）**— 表示配置要加载到的软件文件。 可能的字段值包括：
  - **"Running Configuration"（正在运行的配置）**— 加载正在运行的配置文件。
  - **"Startup Configuration"（启动配置）**— 加载启动配置文件。
  - **"Backup Configuration"（备份配置）**— 加载备份文件。

要加载文件，请：

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 **"TFTP Server IP Address"（TFTP 服务器 IP 地址）**、**"Destination"（目的地）**和 **"Transfer file name"（传输文件名）**字段。
4. 单击 **"Apply Changes"（应用更改）**。 软件将被加载到设备。

使用 CLI 命令加载文件

下表概括了用于查看 **"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。

CLI 命令	说明
copy 源 URL 目的地 URL [snmp]	将文件从源复制到目的地。

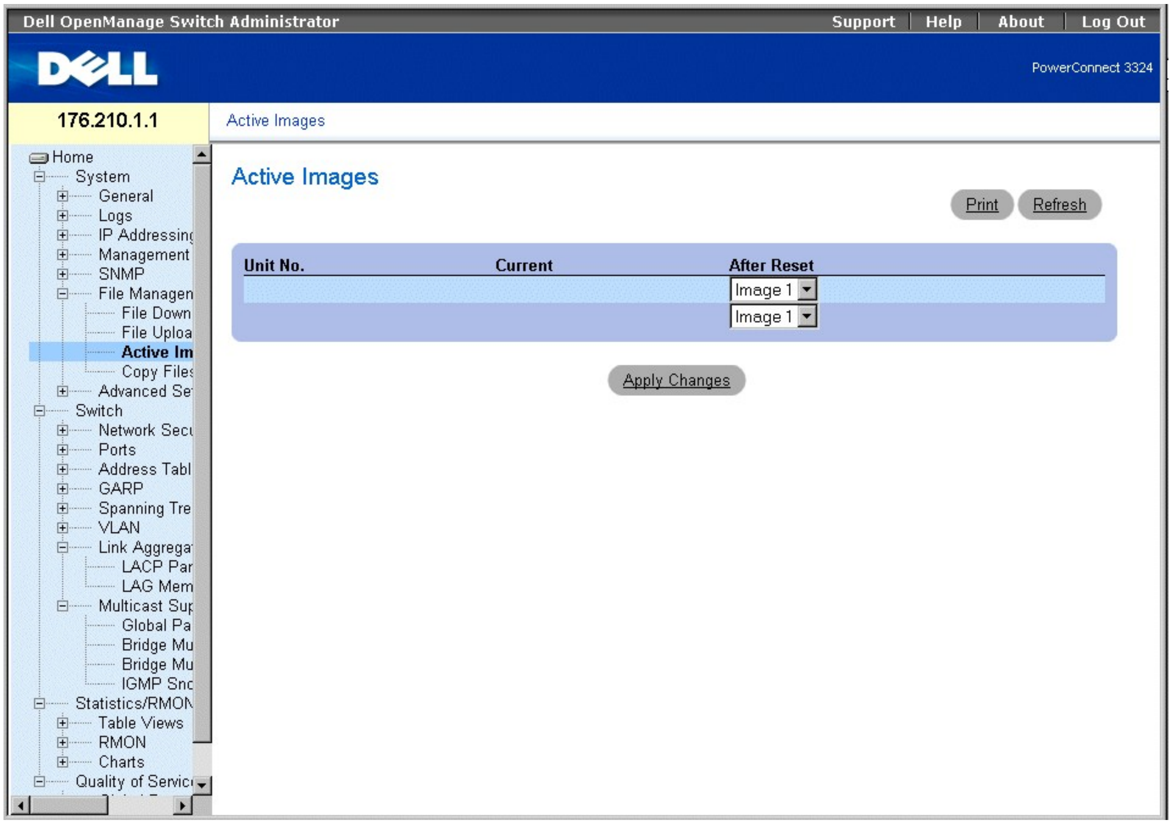
以下是 CLI 命令实例：

```
-----------------------------------------------------

console# copy tftp://16.1.1.200/file1 image

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
2883576 bytes copied in 00:00:10 [hh:mm:ss]
```

重设活动映像

"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）**。 系统将打开 **"Active Images"（活动映像）**页面。



活动映像页面

"Active Images"（活动映像）页面包含以下字段：

- **"Unit No."（装置号）**— 显示为其选定了映像文件的装置号。
- **"Current"（当前）**— 显示装置上当前处于活动状态的映像文件。
- **"After Reset"（重启动后）**— 表示设备重启动后装置上处于活动状态的映像文件。

要选择映像文件，请：

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。 有关重启动设备的说明，请参阅"重启动设备"。

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）**页面中显示的字段的等效 CLI 命令。

CLI 命令	说明
boot system [unit | unit] {image-1 | image-2}	指定设备启动时加载的系统映像。

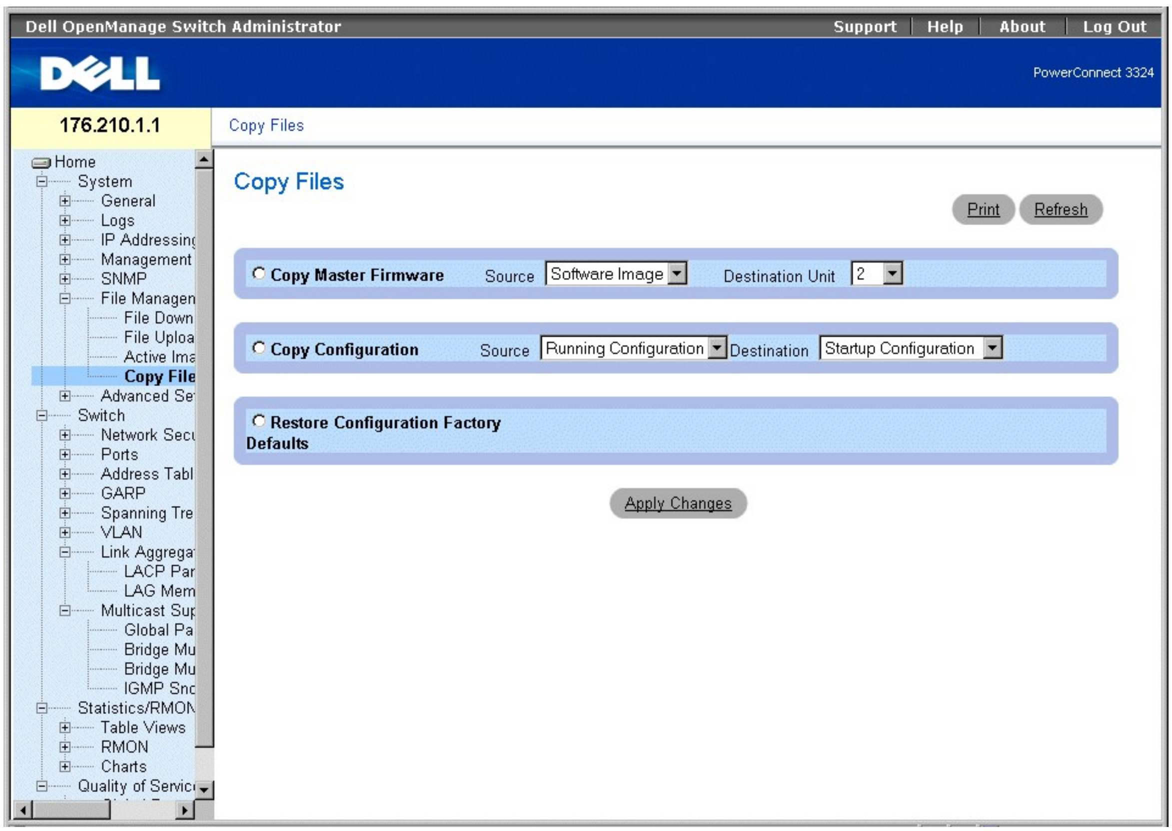
以下是 CLI 命令实例：

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

复制和删除文件

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）**。 系统将打开**“Copy Files”（复制文件）**页面。



复制文件页面

“Copy Files”（复制文件）页面包含以下字段：

- **“Copy Master Firmware”（复制主固件）**— 将软件映像和/或引导代码从主装置复制到选定堆叠装置。
  - **“Source”（源）**— 将软件映像文件或引导代码文件复制到选定堆叠装置。
  - **“Destination Unit”（目标装置）**— 表示软件映像或引导代码要复制到的堆叠装置。
- **“Copy Configuration”（复制配置）**— 将正在运行的配置文件、启动配置文件或备份配置文件复制到启动配置文件或备份配置文件。
  - **“Source”（源）**— 表示要复制到选定堆叠装置的正在运行的配置文件、启动配置文件或备份配置文件。
  - **“Destination”（目的地）**— 表示要覆盖的配置（启动配置或备份配置）。
- “Restore Configuration Factory Defaults”（恢复出厂默认配置）— 通过删除启动配置文件，恢复出厂默认配置文件。 请注意，备份配置文

件未被删除。 可能的字段值包括：

- **已选取** — 恢复出厂默认配置。
- **未选取** — 保留当前的配置设置。

要复制文件，请：

1. 打开 **"Copy Files"（复制文件）**页面。
2. 选择 **"Copy Configuration"（复制配置）**或 **"Copy Master Firmware"（复制主固件）**字段。
3. 为文件定义 **"Source"（源）**和 **"Destination"（目的地）**字段。
4. 单击 **"Apply Changes"（应用更改）**。 系统将复制文件，并更新设备。

要恢复出厂默认设置，请：

1. 打开 **"Copy Files"（复制文件）**页面。
2. 选择 **"Restore Company Factory Defaults"（恢复出厂默认设置）**字段。
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

下表概括了用于查看 **"Copy Files"（复制文件）**页面中显示的字段的等效 CLI 命令。

CLI 命令	说明
delete 启动配置	删除启动配置文件。
copy 源 URL 目的地 URL [SNMP]	将文件从源复制到目的地。

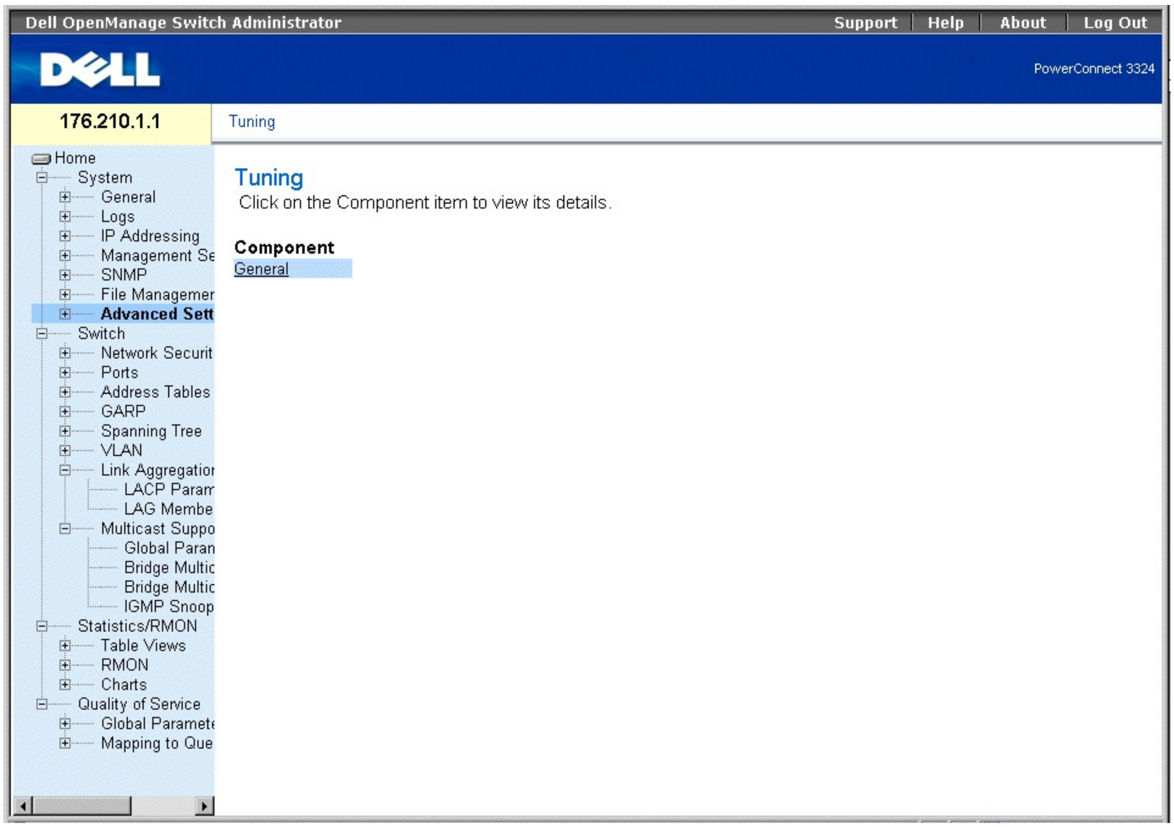
以下是 CLI 命令实例：

```
Console# delete startup-config

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

Console # copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101.

Loading file1 from
172.16.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!
[OK]

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

定义高级设置

设备调节功能可用于确定所列出的各种表中允许的最大条目数。 仅在重启动设备后才能实现更改。 要打开**“Tuning”（调节）**页面，请：

- 在树视图中单击**“System”（系统）**>**“Advanced Settings”（高级设置）**。
  系统将打开**“Tuning”（调节）**页面。



调节页面

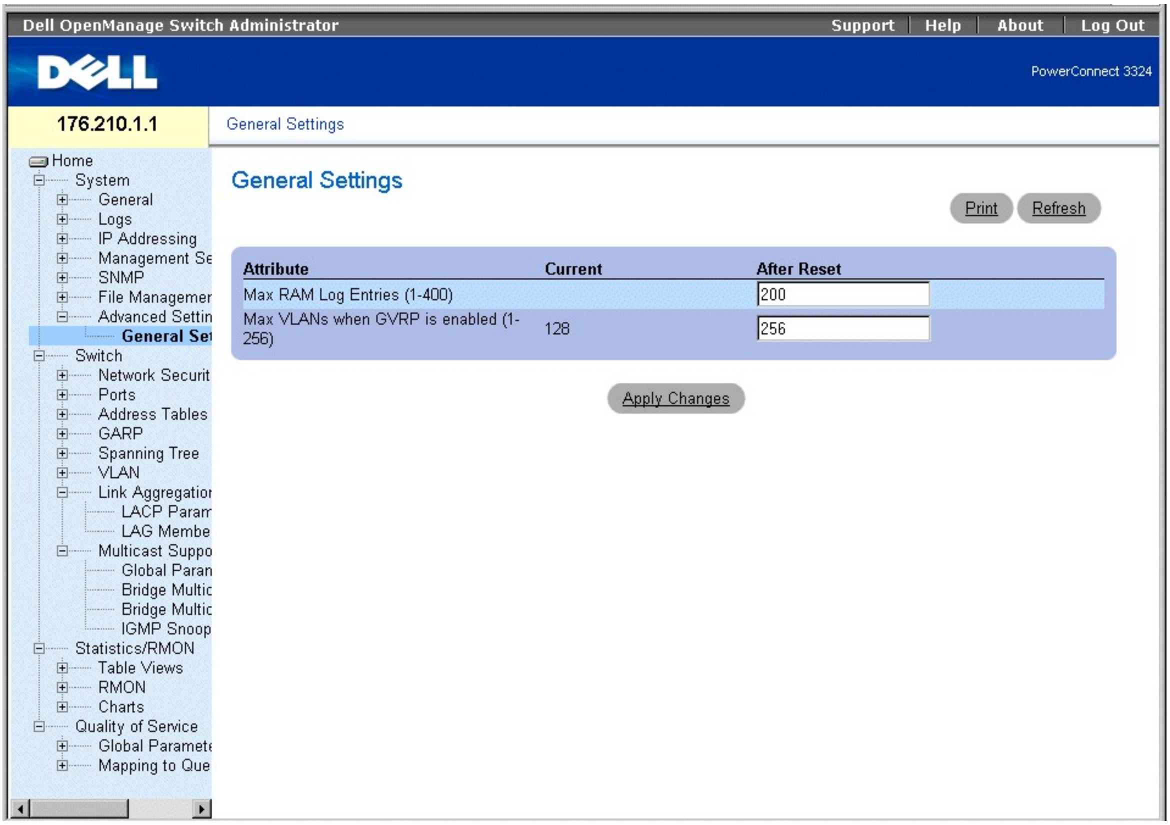
“Tuning”（调节）页面包含以下链接：

- 配置设备的常规调节参数

配置设备的常规调节参数

“General Settings”（常规设置）页面使网络管理员可以定义设备的常规参数。 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”（常规）**。 系统将打开**“General Settings”（常规设置）**页面。



常规设置页面

"General Settings"（常规设置）页面包含以下列：

- **"Attribute"（属性）**— 常规设置属性。
- **"Current"（当前）**— 当前值。
- **"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器。

常规调节页面包含以下字段：

- **"Max RAM Log Entries (1-400)"（最大 RAM 日志条目 [1-400]）**— 表示最大 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。
- **"Max VLANs when GVRP is enabled (1-256)"（启用 GVRP 时的最大 VLAN 数目）**— 定义启用 GVRP 时 VLAN 的总数。

注： GVRP VLAN 的最大数目包括所有参与 GVRP 运行的 VLAN，无论它们是静态 VLAN 还是动态 VLAN。

使用 CLI 命令查看 RAM 日志条目计数器

下表概括了用于查看**"General Settings"（常规设置）**页面中显示的字段的等效 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。
gvrp max vlan	配置启用 GVRP 时 VLAN 的最大数目。

以下是 CLI 命令实例：

```
Console (config)# logging buffered size 300
```

返回目录页面

返回目录页面

获得帮助

Dell™ PowerConnect™ 3324/3348 用户指南

技术帮助

如果您遇到技术问题需要帮助，请使用 Dell 支持（位于 **support.dell.com**）上的多种 Dell 在线服务以获得有关安装和故障排除过程的帮助。

有关详情，请参阅“在线服务”。

如果仍未能解决问题，请致电 Dell 寻求技术帮助。

注： 致电技术支持时，请使用计算机旁边的电话，以便完成技术支持要求的所有必要步骤。

注： 并非在所有国家/地区均可使用 Dell 的快速服务代码系统。

Dell 自动电话系统提示时，输入您的快速服务代码，从而将电话直接转至相应的技术支持人员。 如果您没有快速服务代码，请打开 **“Dell Accessories”（Dell 附件）**文件夹，双击 **“Express Service Code”（快速服务代码）**图标，然后按照提示进行操作。

有关使用技术支持服务的说明，请参阅“技术支持服务”和“致电之前”。

注： 以下部分服务并非在美国本土以外的所有地区都能使用。有关其可用性的信息，请致电当地的 Dell 代表。

在线服务

您可以访问位于 **support.dell.com** 的 Dell 支持。 请在 **“WELCOME TO DELL SUPPORT”（欢迎访问 DELL SUPPORT）**页面上选择您所在的地区，并填写所需的详细信息以查看帮助工具和信息。

您可以使用以下地址与 Dell 进行电子联络：

- World Wide Web

www.dell.com/

www.dell.com/ap/（仅限于亚太国家和地区）

www.euro.dell.com （仅限于欧洲）

www.dell.com/la （仅限于拉丁美洲国家和地区）

www.dell.ca（仅限于加拿大）

- 匿名文件传输协议 (FTP)

ftp.dell.com/

使用用户名 anonymous 登录，并将您的电子邮件地址用作密码。

- 电子邮件支持服务

support@us.dell.com

apsupport@dell.com（仅限于亚太国家和地区）

support.euro.dell.com（仅限于欧洲）

- 电子邮件报价服务

sales@dell.com

apmarketing@dell.com（仅限于亚太国家和地区）

sales_canada@dell.com（仅限于加拿大）

- 电子邮件信息服务

info@dell.com

AutoTech 服务

Dell 的自动技术支持服务 AutoTech 针对 Dell 客户经常询问的便携式和台式计算机系统问题，
提供了预先录制的解答。

致电 AutoTech 时，请使用按键式电话选择与您的问题相对应的主题。

自动技术支持每天 24 小时、每周 7 天提供服务。 ##您也可以通过技术支持服务中心访问此服务。 请参阅适用于您所在地区的联络信息。

订单状态自动查询服务

您可以访问 **support.dell.com**，或致电订单状态自动查询服务，查询您订购的任何 Dell™ 产品的情况。 电话录音将提示您输入用于查找和介绍订单的信息。 请参阅适用于您所在地区的联络信息。

技术支持服务

Dell 技术支持服务可以每天 24 小时、每周 7 天答复有关 Dell 硬件的问题。 我们的技术支持人员使用基于计算机的诊断程序，可以快速准确地解答您的问题。

要与 Dell 的技术支持服务部门联系，请首先参阅“致电之前”，然后参阅适用于您所在地区的联系信息。

Dell 企业培训和认证

Dell 可以提供企业培训与认证；有关详情，请访问 **www.dell.com/training**。 并非所有地区均提供此服务。

订单问题

如果您的订购出现问题，例如缺少或装错部件或帐单错误，请与 Dell 联络寻求客户帮助。
致电时，请准备好发票或装箱单。 请参阅适用于您所在地区的联络信息。

产品信息

如果您需要有关 Dell 提供的其它产品的信息，或者想要订购产品，请访问 Dell Web 站点 **www.dell.com**。 要获得致电销售人员所需的电话号码，请参阅适用于您所在地区的联络信息。

退回部件以要求保修或退款

无论您是要求保修还是退款，请按以下说明准备好所有要退回的部件：

1. 致电 Dell 获得退回材料授权号，并在包装箱外侧的显著位置清楚地注明此号码。

   要获得致电所需的电话号码，请参阅适用于您所在地区的联系信息。

2. 附上发票复印件和一封说明退回原因的信函。
3. 附上诊断信息的复印件，其中应填写您运行过的检测程序和系统诊断程序报告的所有错误信息。
4. 如果您要求退款，请附上退回产品的所有附件（例如电源电缆、介质 [如 CD 和软盘] 及指南）。
5. 使用原来的（或相当的）包装材料包装退回的设备。

您必须支付运费， 同时还应为退回的所有产品投保，并承担产品在运送至 Dell 公司途中丢失的风险。 本公司不接受以货到付款 (C.O.D.) 方式寄送的包裹。

如果退回的物品不符合上述任何要求，本公司的接收部门将会拒绝接收并将其退回给您。

致电之前

注： 致电之前，请准备好您的快速服务代码。 此代码可以帮助 Dell 的自动支持电话系统快速转接您的电话。

如果有可能，请在致电 Dell 获得技术帮助之前打开系统，同时使用靠近计算机的电话。 技术人员可能要求您在键盘上键入一些命令，转述操作细节；或者尝试执行只能在系统上进行的其它故障排除步骤。 确保可以获得系统说明文件。

警告： 在维修计算机内部任何组件之前，请参阅您的《*系统信息指南*》以获得重要的安全信息。

与 Dell 联系

要与 Dell 进行电子联系，您可以访问以下 Web 站点：

- **www.dell.com**
- **support.dell.com**（技术支持）
- **premiersupport.dell.com**（对教育部门、政府、医疗机构和中型/大型企业客户的技术支持，包括首要客户、铂金客户和黄金客户）

有关您所在国家或地区的特定 Web 地址，请在下表中查找相应的国家或地区部分。

注： 免费电话号码仅可在列出的国家内使用。

需要与 Dell 联系时，请使用下表中提供的电子地址、电话号码和代码。 如果您无法确定应该使用的代码，请与本地或国际电话营运商联系。

国家/地区（城市） 国际拨号代码 国家/地区代码 城市代码	部门名称或服务区域、 Web 站点和电子邮件地址	区号、 当地电话号码和 免费电话号码
安圭拉岛	一般支持	免费：800-335-0031
安提瓜和巴布达	一般支持	1-800-805-5924
阿根廷（布宜诺斯艾利斯）	Web 站点： **www.dell.com.ar**	
国际访问代码： **00**	技术支持和客户服务	免费：0-800-444-0733
	销售	0-810-444-3355
国家/地区代码： **54**	技术支持传真	11 4515 7139
城市代码： **11**	客户服务传真	11 4515 7138
阿鲁巴	一般支持	免费：800-1578
澳大利亚（悉尼）	电子邮件（澳大利亚）： au_tech_support@dell.com	
国际访问代码：**0011**	电子邮件（新西兰）： nz_tech_support@dell.com	
	家庭和小型企业	1-300-65-55-33

国家/地区代码： **61** 城市代码： **2**	政府和企业	免费：1-800-633-559
	重要客户部（PAD)	免费：1-800-060-889
	客户服务	免费：1-800-819-339
	公司客户销售	免费：1-800-808-385
	合同销售	免费：1-800-808-312
	传真	免费：1-800-818-341
澳大利亚（悉尼） 国际访问代码： **900** 国家/地区代码： **43** 城市代码： **1**	Web 站点： **support.euro.dell.com**	
	电子邮件： tech_support_central_europe@dell.com	
	家庭/小型企业客户销售	0820 240 530 00
	家庭/小型企业客户传真	0820 240 530 49
	家庭/小型企业客户服务	0820 240 530 14
	重要客户/公司客户服务	0820 240 530 16
	家庭/小型企业客户技术支持	0820 240 530 14
	重要客户/公司客户技术支持	0660 8779
	总机	0820 240 530 00
巴哈马	一般支持	免费：1-866-278-6818
巴巴多斯	一般支持	1-800-534-3066
比利时（布鲁塞尔） 国际访问代码： **00** 国家/地区代码： **32** 城市代码： **2**	Web 站点： **support.euro.dell.com**	
	电子邮件： tech_be@dell.com	
	电子邮件（使用法语的客户）： **support.euro.dell.com/be/fr/emaildell/**	
	技术支持	02 481 92 88
	客户服务	02 481 91 19
	公司客户销售	02 481 91 00
	传真	02 481 92 99
	总机	02 481 91 00
百慕大群岛	一般支持	1-800-342-0671
玻利维亚	一般支持	免费：800-10-0238
巴西 国际访问代码： **00** 国家/地区代码： **55** 城市代码： **51**	Web 站点： **www.dell.com/br**	
	客户支持和技术支持	0800 90 3355
	技术支持传真	51 481 5470
	客户服务传真	51 481 5480
	销售	0800 90 3390
英属维尔京群岛	一般支持	免费：1-866-278-6820
文莱 国家/地区代码： **673**	客户技术支持（马来西亚，槟城）	604 633 4966
	客户服务（马来西亚，槟城）	604 633 4949
	合同销售（马来西亚，槟城）	604 633 4955
加拿大（安大略省，北约克） 国际访问代码： **011**	在线订单状态： **www.dell.ca/ostatus**	
	AutoTech（自动技术支持）	免费：1-800-247-9362
	技术传真	免费：1-800-950-1329
	客户服务（家庭/小型企业客户）	免费：1-800-847-4096
	客户服务（中型/大型企业客户和政府部门）	免费：1-800-326-9463
	技术支持（家庭/小型企业客户）	免费：1-800-847-4096
	技术支持（中型/大型企业客户和政府部门）	免费：1-800-387-5757
	销售（家庭/小型企业客户）	免费：1-800-387-5752
	销售（中型/大型企业客户和政府部门）	免费：1-800-387-5755
	备用部件销售和扩展服务销售	1 866 440 3355
开曼群岛	一般支持	1-800-805-7541
智利（圣地亚哥）	销售、客户支持和技术支持	免费：1230-020-4823

国家/地区代码： **56** 城市代码： **2**		
中国（厦门） 国家/地区代码： **86** 城市代码： **592**	技术支持 Web 站点： **support.ap.dell.com/china**	
	技术支持电子邮件： cn_support@dell.com	
	技术支持传真	818 1350
	家庭和小型企业客户技术支持	免费：800 858 2437
	公司客户技术支持	免费：800,8582333
	客户体验	免费：800 858 2060
	家庭和小型企业	免费：800 858 2222
	重要客户部	免费：800 858 2557
	大公司客户 (GCP)	免费：800 858 2055
	大公司客户（重要客户）	免费：800 858 2628
	大公司客户（北部地区）	免费：800 858 2999
	大公司客户（北部地区政府和教育部门）	免费：800 858 2955
	大公司客户（东部地区）	免费：800 858 2020
	大公司客户（东部地区政府和教育部门）	免费：800 858 2669
	大公司客户 (Queue Team)	免费：800 858 2222
	大公司客户（南部地区）	免费：800 858 2355
	大公司客户（西部地区）	免费：800 858 2811
	大公司客户（备用部件）	免费：800 858 2621
哥伦比亚	一般支持	980-9-15-3978
哥斯达黎加	一般支持	0800-012-0435
捷克共和国（布拉格） 国际访问代码： **00** 国家/地区代码： **420** 城市代码： **2**	Web 站点： **support.euro.dell.com**	
	电子邮件： czech_dell@dell.com	
	技术支持	02 2186 27 27
	客户服务	02 2186 27 11
	传真	02 2186 27 14
	技术传真	02 2186 27 28
	总机	02 2186 27 11
丹麦（哥本哈根） 国际访问代码： **00** 国家/地区代码： **45**	Web 站点： **support.euro.dell.com**	
	电子邮件支持（便携式计算机）： den_nbk_support@dell.com	
	电子邮件支持（台式计算机）： den_support@dell.com	
	电子邮件支持（服务器）： Nordic_server_support@dell.com	
	技术支持	7023 0182
	客户服务 (Relational)	7023 0184
	家庭/小型企业客户服务	3287 5505
	总机 (Relational)	3287 1200
	传真总机 (Relational)	3287 1201
	总机（家庭/小型企业）	3287 5000
	传真总机（家庭/小型企业）	3287 5001
多米尼加	一般支持	免费：1-866-278-6821
多米尼加共和国	一般支持	1-800-148-0530
厄瓜多尔	一般支持	免费：999-119
萨尔瓦多	一般支持	01-899-753-0777
芬兰（赫尔辛基） 国际访问代码： **990** 国家/地区代码：	Web 站点： **support.euro.dell.com**	
	电子邮件： fin_support@dell.com	
	电子邮件支持（服务器）： Nordic_support@dell.com	
	技术支持	09 253 313 60

358 城市代码： **9**	技术支持传真	09 253 313 81
	关系客户服务	09 253 313 38
	家庭/小型企业客户服务	09 693 791 94
	传真	09 253 313 99
	总机	09 253 313 00
法国（巴黎）（蒙彼利埃） 国际访问代码： **00** 国家/地区代码： **33** 城市代码： **(1) (4)**	Web 站点： **support.euro.dell.com**	
	电子邮件： **support.euro.dell.com/fr/fr/emaildell/**	
	家庭和小型企业	
	技术支持	0825 387 270
	客户服务	0825 823 833
	总机	0825 004 700
	总机（从法国以外地区拨打）	04 99 75 40 00
	销售	0825 004 700
	传真	0825 004 701
	传真（从法国以外地区拨打）	04 99 75 40 01
	公司	
	技术支持	0825 004 719
	客户服务	0825 338 339
	总机	01 55 94 71 00
	销售	01 55 94 71 00
	传真	01 55 94 71 01
德国（郎根） 国际访问代码： **00** 国家/地区代码： **49** 城市代码： **6103**	Web 站点： **support.euro.dell.com**	
	电子邮件： tech_support_central_europe@dell.com	
	技术支持	06103 766-7200
	家庭/小型企业客户服务	0180-5-224400
	区域客户服务	06103 766-9570
	重要客户服务	06103 766-9420
	大客户服务	06103 766-9560
	一般客户服务	06103 766-9555
	总机	06103 766-7000
希腊 国际访问代码： 00 国家/地区代码： 30	Web 站点： **support.euro.dell.com**	
	电子邮件： support.euro.dell.com/gr/en/emaildell/	
	技术支持	080044149518
	黄金客户技术支持	08844140083
	总机	2108129800
	销售	2108129800
	传真	2108129812
格林纳达	一般支持	免费：1-866-540-3355
危地马拉	一般支持	1-800-999-0136
圭亚那	一般支持	免费：1-877-270-4609
香港 国际访问代码： **001** 国家/地区代码： **852**	Web 站点： **support.ap.dell.com**	
	电子邮件： ap_support@dell.com	
	技术支持(Dimension™ 和 Inspiron™)	2969 3189
	技术支持(OptiPlex™, Latitude™, 和 Dell Precision™)	2969 3191
	技术支持（(PowerApp™, PowerEdge™, PowerConnect™, 和 PowerVault™)	2969 3196
	金服务 EEC 热线	2969 3187
	客户促进	3416 0910

	大公司客户	3416 0907
	全球客户计划	3416 0908
	中型企业部	3416 0912
	家庭和小型企业部	2969 3105
印度	技术支持	1600 33 8045
	销售	1600 33 8044
爱尔兰（切里伍德） 国际访问代码： **16** 国家/地区代码： **353** 城市代码： **1**	Web 站点： **support.euro.dell.com**	
	电子邮件： dell_direct_support@dell.com	
	技术支持	1850 543 543
	技术支持（英国）（仅限于英国境内拨打）	0870 908 0800
	家庭用户服务	01 204 4014
	小型企业客户服务	01 204 4014
	客户服务（英国）（仅限于英国境内拨打）	0870 906 0010
	公司客户服务	1850 200 982
	公司客户服务（仅限于英国境内拨打）	0870 907 4499
	销售（爱尔兰）	01 204 4444
	销售（英国）（仅限于英国境内拨打）	0870 907 4000
	传真/销售传真	01 204 0103
	总机	01 204 4444
意大利（米兰） 国际访问代码： **00** 国家/地区代码： **39** 城市代码： **02**	Web 站点： **support.euro.dell.com**	
	电子邮件： **support.euro.dell.com/it/it/emaildell/**	
	家庭和小型企业	
	技术支持	02 577 826 90
	客户服务	02 696 821 14
	传真	02 696 821 13
	总机	02 696 821 12
	公司	
	技术支持	02 577 826 90
	客户服务	02 577 825 55
	传真	02 575 035 30
	总机	02 577 821
牙买加	一般支持（仅限于牙买加境内拨打）	1-800-682-3639
日本（川崎） 国际访问代码： **001** 国家/地区代码： **81** 城市代码： **44**	Web 站点： **support.jp.dell.com**	
	技术支持（服务器）	免费： 0120-198-498
	日本以外地区技术支持（服务器）	81-44-556-4162
	技术支持(Dimension™ 和 Inspiron™)	免费： 0120-198-226
	日本以外地区技术支持 （Dimension 和 Inspiron）	81-44-520-1435
	技术支持（(Dell Precision™, OptiPlex™, and Latitude™)	免费：0120-198-433
	日本以外地区技术支持 (Dell Precision, OptiPlex, 和 Latitude)	81-44-556-3894
	技术支持 (Axim™)	免费： 0120-981-690
	日本以外地区技术支持 (Axim)	81-44-556-3468
	传真信箱服务	044-556-3490
	24 小时订单状态自动查询服务	044-556-3801
	客户服务	044-556-4240
	企业客户销售部（400 名以下员工）	044-556-1465
	重要客户部销售（400 名以上员工）	044-556-3433
	大公司客户销售（3500 名以上员工）	044-556-3430

	公共部门销售 （政府机构、教育部门和医疗机构）	044-556-1469
	全球分区（日本）	044-556-3469
	个人用户	044-556-1760
	总机	044-556-4300
韩国（汉城） 国际访问代码：**001** 国家/地区代码：**82** 城市代码：**2**	技术支持	免费：080-200-3800
	销售	免费：080-200-3600
	客户服务（韩国，汉城）	免费： 080-200-3800
	客户服务（马来西亚，槟城）	604 633 4949
	传真	2194-6202
	总机	2194-6000
拉丁美洲	客户技术支持（美国，得克萨斯州，奥斯汀）	512 728-4093
	客户服务（美国，德克萨斯州，奥斯汀）	512 728-3619
	技术支持和客户服务传真（美国，得克萨斯州，奥斯汀）	512 728-3883
	销售（美国，德克萨斯州，奥斯汀）	512 728-4397
	销售传真（美国，德克萨斯州，奥斯汀）	512 728-4600 或 512 728-3772
卢森堡 国际访问代码：**00** 国家/地区代码：**352**	Web 站点：**support.euro.dell.com**	
	电子邮件：tech_be@dell.com	
	技术支持（比利时，布鲁塞尔）	3420808075
	家庭/小型企业客户销售（比利时，布鲁塞尔）	免费：080016884
	公司销售（比利时，布鲁塞尔）	02 481 91 00
	客户服务（比利时，布鲁塞尔）	02 481 91 19
	传真（比利时，布鲁塞尔）	02 481 92 99
	总机（比利时，布鲁塞尔）	02 481 91 00
澳门特区 国家/地区代码：**853**	技术支持	免费：0800 582
	客户服务（马来西亚，槟城）	604 633 4949
	合同销售	免费：0800 581
马来西亚（槟城） 国际访问代码：**00** 国家/地区代码：**60** 城市代码：**4**	技术支持	免费：1 800 888 298
	客户服务	04 633 4949
	合同销售	免费：1 800 888 202
	公司客户销售	免费：1 800 888 213
墨西哥 国际访问代码：**00** 国家/地区代码：**52**	客户技术支持	001-877-384-8979 或 001-877-269-3383
	销售	50-81-8800 或 01-800-888-3355
	客户服务	001-877-384-8979 或 001-877-269-3383
	主要客户	50-81-8800 或 01-800-888-3355
蒙塞拉特岛	一般支持	免费：1-866-278-6822
荷属安的列斯群岛	一般支持	001-800-882-1519
荷兰（阿姆斯特丹） 国际访问代码：**00** 国家/地区代码：**31** 城市代码：**20**	Web 站点：**support.euro.dell.com** 电子邮件（技术支持）： （企业）：nl_server_support@dell.com (Latitude)：nl_latitude_support@dell.com	

	(Inspiron)： nl_inspiron_support@dell.com (Dimension)： nl_dimension_support@dell.com (OptiPlex)： nl_optiplex_support@dell.com (Dell Precision)： nl_workstation_support@dell.com	
	技术支持	020 674 45 00
	技术支持传真	020 674 47 66
	家庭/小型企业客户服务	020 674 42 00
	客户服务 (Relational)	020 674 4325
	家庭/小型企业客户销售	020 674 55 00
	销售 (Relational)	020 674 50 00
	家庭/小型企业客户销售传真	020 674 47 75
	销售传真 (Relational)	020 674 47 50
	总机	020 674 50 00
	总机传真	020 674 47 50
新西兰 国际访问代码： **00** 国家/地区代码： **64**	电子邮件（新西兰）： nz_tech_support@dell.com	
	电子邮件（澳大利亚）： au_tech_support@dell.com	
	家庭和小型企业	0800 446 255
	政府和企业	0800 444 617
	销售	0800 441 567
	传真	0800 441 566
尼加拉瓜	一般支持	001-800-220-1006
挪威（利萨克） 国际访问代码： **00** 国家/地区代码： **47**	Web 站点： **support.euro.dell.com**	
	电子邮件支持（便携式计算机）： nor_nbk_support@dell.com	
	电子邮件支持（台式计算机）： nor_support@dell.com	
	电子邮件支持（服务器）： nordic_server_support@dell.com	
	技术支持	671 16882
	客户服务 (Relational)	671 17514
	家庭/小型企业客户服务	23162298
	总机	671 16800
	传真总机	671 16865
巴拿马	一般支持	001-800-507-0962
秘鲁	一般支持	0800-50-669
波兰（华沙） 国际访问代码： **011** 国家/地区代码： **48** 城市代码： **22**	Web 站点： **support.euro.dell.com**	
	电子邮件： pl_support_tech@dell.com	
	客户服务电话	57 95 700
	客户服务	57 95 999
	销售	57 95 999
	客户服务传真	57 95 806
	接待处传真	57 95 998
	总机	57 95 999
葡萄牙 国际访问代码： **00**	Web 站点： **support.euro.dell.com**	
	电子邮件： **support.euro.dell.com/pt/en/emaildell/**	

国家/地区代码：**351**	技术支持	707200149
	客户服务	800 300 413
	销售	800 300 410 或 800 300 411 或 800 300 412 或 21 422 07 10
	传真	21 424 01 12
波多黎各	一般支持	1-800-805-7545
圣基茨和尼维斯	一般支持	免费：1-877-441-4731
圣卢西亚	一般支持	1-800-882-1521
圣文森特和格林纳丁斯	一般支持	免费：1-877-270-4609
新加坡（新加坡） 国际访问代码：**005** 国家/地区代码：**65**	技术支持	免费：800 6011 051
	客户服务（马来西亚，槟城）	604 633 4949
	合同销售	免费：800 6011 054
	公司客户销售	免费：800 6011 053
南非（约翰内斯堡） 国际访问代码：**09/091** 国家/地区代码：**27** 城市代码：**11**	Web 站点：**support.euro.dell.com**	
	电子邮件：dell_za_support@dell.com	
	技术支持	011 709 7710
	客户服务	011 709 7707
	销售	011 709 7700
	传真	011 706 0495
	总机	011 709 7700
东南亚及太平洋国家/地区	客户技术支持、客户服务和销售（马来西亚，槟城）	604 633 4810
西班牙（马德里） 国际访问代码：**00** 国家/地区代码：**34** 城市代码：**91**	Web 站点：**support.euro.dell.com**	
	电子邮件：**support.euro.dell.com/es/es/emaildell/**	
	家庭和小型企业	
	技术支持	902 100 130
	客户服务	902 118 540
	销售	902 118 541
	总机	902 118 541
	传真	902 118 539
	公司	
	技术支持	902 100 130
	客户服务	902 118 546
	总机	91 722 92 00
	传真	91 722 95 83
瑞典（乌普兰斯韦斯比） 国际访问代码：**00** 国家/地区代码：**46** 城市代码：**8**	Web 站点：**support.euro.dell.com**	
	电子邮件：swe_support@dell.com	
	Latitude 和 Inspiron 电子邮件支持：Swe-nbk_kats@dell.com	
	OptiPlex 电子邮件支持：Swe_kats@dell.com	
	服务器电子邮件支持：Nordic_server_support@dell.com	
	技术支持	08 590 05 199
	客户服务 (Relational)	08 590 05 642
	家庭/小型企业客户服务	08 587 70 527
	员工购买计划 (EPP) 支持	20 140 14 44
	传真技术支持	08 590 05 594
	销售	08 590 05 185
瑞士（日内瓦） 国际访问代码：**00**	Web 站点：**support.euro.dell.com**	
	电子邮件：swisstech@dell.com	

国家/地区代码： **41** 城市代码： **22**	电子邮件（使用法语的 HSB 和公司客户）：**support.euro.dell.com/ch/fr/emaildell/**	
	技术支持（家庭和小型企业）	0844 811 411
	技术支持（公司）	0844 822 844
	客户服务（家庭和小型企业）	0848 802 202
	客户服务（公司）	0848 821 721
	传真	022 799 01 90
	总机	022 799 01 01
台湾 国际访问代码：**002** 国家/地区代码：**886**	技术支持（便携式和台式计算机）	免费：00801 86 1011
	技术支持（服务器）	免费：0080 60 1256
	合同销售	免费：0080 651 228
	公司客户销售	免费：0080 651 227
泰国 国际访问代码：**001** 国家/地区代码： **66**	技术支持	免费：0880 060 07
	客户服务（马来西亚，槟城）	604 633 4949
	销售	免费：0880 060 09
特立尼达和多巴哥	一般支持	1-800-805-8035
特克斯群岛和凯科斯群岛	一般支持	免费：1-866-540-3355
英国（布莱克内尔） 国际访问代码： **00** 国家/地区代码： **44** 城市代码： **1344**	Web 站点： **support.euro.dell.com**	
	客户服务 Web 站点： **support.euro.dell.com/uk/en/ECare/Form/Home.asp**	
	电子邮件： dell_direct_support@dell.com	
	技术支持（公司/重要客户/PAD [1000 名以上员工]）	0870 908 0500
	技术支持（直接/PAD 和一般客户）	0870 908 0800
	全球客户服务	01344 373 186
	家庭和小型企业客户服务	0870 906 0010
	公司客户服务	01344 373 185
	重要客户（500-5000 名员工）服务	0870 906 0010
	中央政府客户服务	01344 373 193
	地方政府和教育部门客户服务	01344 373 199
	医疗机构客户服务	01344 373 194
	家庭和小型企业客户销售	0870 907 4000
	公司/公共部门客户销售	01344 860 456
	家庭和小型企业传真	0870 907 4006
乌拉圭	一般支持	免费：000-413-598-2521
美国（德克萨斯州，奥斯汀） 国际访问代码：**011** 国家/地区代码： **1**	订单状态自动查询服务	免费：1-800-433-9014
	自动技术支持（便携式和台式计算机）	免费：1-800-247-9362
	个人用户（家庭和家庭办公室）	
	技术支持	免费：1-800-624-9896
	客户服务	免费：1-800-624-9897
	DellNet 服务和支持	免费：1-877-Dellnet (1-877-335-5638)
	员工购买计划 (EPP) 客户	免费：1-800-695-8133
	财务服务 Web 站点： **www.dellfinancialservices.com**	
	财务服务（租赁/贷款）	免费：1-877-577-3355
	财务服务（Dell 重要客户 [DPA]）	免费：1-800-283-2210
	企业	

	客户服务和技术支持	免费：1-800-822-8965
	员工购买计划 (EPP) 客户	免费：1-800-695-8133
	投影机技术支持	免费：1-877-459-7298
	公共部门（政府部门、教育部门和医疗机构）	
	客户服务和技术支持	免费：1-800-456-3355
	员工购买计划 (EPP) 客户	免费：1-800-234-1490
	Dell 销售）	免费：1-800-289-3355 或免费：1-800-879-3355
	Dell Outlet Store（Dell 翻新计算机）	免费：1-888-798-7561
	软件和外围设备销售	免费：1-800-671-3355
	备用部件销售	免费：1-800-357-3355
	扩展服务和保修销售	免费：1-800-247-4618
	传真	免费：1-800-727-8320
	Dell 为失聪人士、听力有困难或有语言障碍人士提供的服务	免费：1-877-DELLTTY (1-877-335-5889)
美属维尔京群岛	一般支持	1-877-673-3355
委内瑞拉	一般支持	8001-3605

返回目录页面

[返回目录页面]

使用入门

Dell™ PowerConnect™ 3324/3348 用户指南

启动 Switch Administrator

通过任一带有 Web 浏览器的 PC 可以访问 Dell™ PowerConnect™ 3324/3348 OpenManage™ Switch Administrator。 要启动 Switch Administrator，请：

1. 打开 Web 浏览器。
2. 在地址栏中输入设备 IP 地址/home.htm，并按 <Enter> 键。 系统将显示登录窗口。

PowerConnect 3324/3348 密码页面

3. 输入用户名和密码。

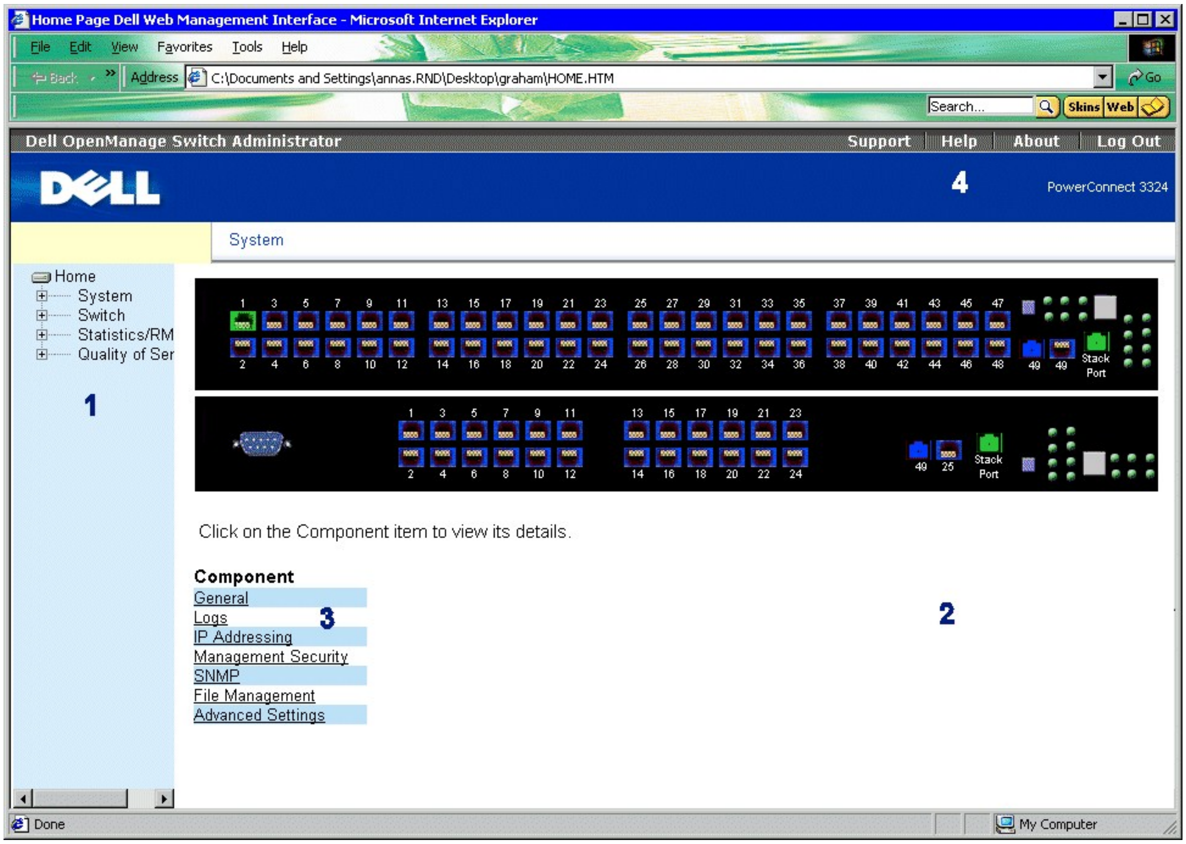
注： 不输入密码也可以配置 PowerConnect 3324/3348。 密码区分大小写，并且只能为字母数字。

4. 单击 **"OK"（确定）**。 系统将显示 **"Switch Administrator"**主页。

了解界面

"Switch Administrator"主页包含以下视图：

- 树视图 — 位于 **"Switch Administrator"**主页左侧的树视图提供了功能及其组件（组件列表）的可展开树视图。
- 设备视图 — 位于 **"Switch Administrator"**主页右侧的设备视图提供了设备视图、信息或表区域以及配置说明。



PowerConnect 3324 / 3348 Web 管理界面

“**PowerConnect 3324 / 3348 Interface Components Table**”（**PowerConnect 3324 / 3348 界面组件表**）列出了界面组件及其相应的编号：

组件	名称
1	树视图。 树视图包含各种设备功能的列表。 有关树视图的详细信息，请参阅“树视图”。
2	设备视图。 设备视图提供了有关设备端口、表信息和功能组件的信息。 有关设备视图的详细信息，请参阅“设备视图”。
3	组件列表。 组件列表包含功能组件的列表。 有关使用组件列表的详细信息，请参阅“组件列表”。
4	信息按钮。 使用信息按钮可以查看 PowerConnect 设备信息和 Dell 服务。 有关信息按钮的详细信息，请参阅“使用 Switch Administrator 按钮”。

PowerConnect 3324 / 3348 界面组件表

树视图

树视图包含可以配置的各种功能（包括交换功能、端口、生成树、VLAN、服务级别、链路聚合 [LAG]、多点传送支持和统计数据）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。

设备视图

以下小节介绍了设备视图的各个方面。 设备提供了有关 PowerConnect 3324/3348 交换机的信息。 设备视图包含以下组件：

- [组件列表]
- [设备图示]
- [工作台]

组件列表

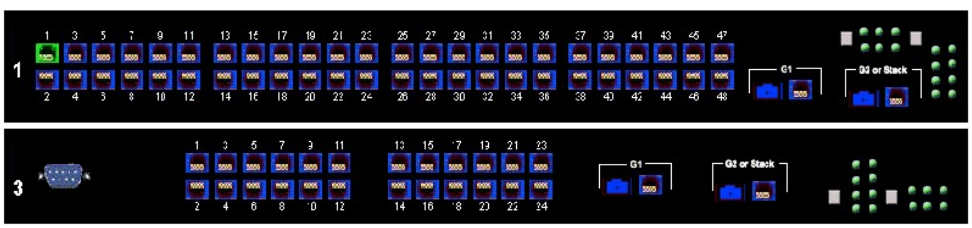
"Switch Administrator"主页显示了包含配置菜单选项的组件列表。 要显示组件的配置，请：

- 单击某个组件列表项目。 系统将打开特定的组件页面。 例如，在树视图中单击**"Switch"（交换机）**， 将打开以下页面：

组件列表

设备图示

"Switch Administrator"主页包含 PowerConnect 3324/3348 前面板的图示。



PowerConnect 3348

端口颜色表明特定端口当前是否处于活动状态。 端口状态的颜色表示如下：

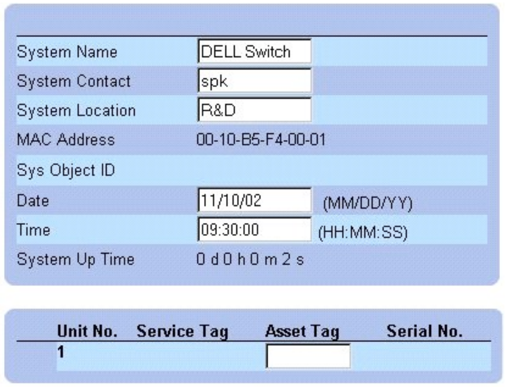
组件	名称
绿色	表示端口已连接。
蓝色	表示端口由于安全保护功能而暂停。
红色	表示端口已断开连接。

PowerConnect 3324/3348 端口指示灯

注： Switch Administrator 中的 PowerConnect 3324/3348 前面板上未反映 LED。 只能通过查看实际设备建立 LED 状态。 有关 LED 定义的详细信息，请参阅"LED 定义"。

工作台

设备视图中的工作台提供了包含设备表、一般设备信息和可配置设备参数的工作区域。
下图显示了一个选定后可能显示的表的实例：



工作台信息实例

使用 **Switch Administrator** 按钮

本节包含了有关界面提供的各个Dell OpenManage *Switch Administrator* 按钮的信息。
Switch Administrator 提供了以下按钮：

- 信息按钮 — 使用此按钮可以访问信息服务（包括技术支持、联机帮助、有关设备的信息以及关闭 *Switch Administrator*）。
- 关于 PageDevice 管理按钮 — 提供了用于管理 *Switch Administrator* 的管理按钮（包括添加按钮、删除按钮、查询按钮和应用更改按钮）的说明。

信息按钮

“Switch Administrator”主页包含以下信息按钮：

按钮	**说明**
Support	打开 Dell 支持页面。 Dell 技术支持页面的 URL 是 **www.support.ap.dell.com/china.com**
Help	打开联机帮助。
About	打开 **“About”（关于）**页面。
Log Out	退出 Switch Administrator。

信息按钮

支持按钮

“Support”（支持）页面包含访问 Dell 技术支持页面所需的信息。

1. 单击 **“Support”（支持）**。 系统将打开 **“Dell Technical Support”（Dell 技术支持）**页面：

Dell 技术支持页面

2. 选择区域，以显示所需支持。 系统将显示相应的支持页面。

3. 输入用户名和密码。

4. 单击**“Login”（登录）**并阅读说明。

注： 根据所需技术支持类型的不同，可能需要输入用户名和密码。

帮助按钮

“Online Help”（联机帮助）页面包含可帮助您配置和管理交换机的信息。

1. 单击**“Help”（帮助）**。 系统将打开**“Online Help”（联机帮助）**页面。

2. 选择帮助主题。 系统将打开选定的帮助主题页面。

注： 每个屏幕均包含一个简要的帮助页面。 要查看帮助，请单击 Switch Administrator "趁嫔系**“Help”（帮助）**。

关于按钮

“About”（关于）按钮可以打开**“About”（关于）**页面。 **“About”（关于）**页面包含设备名称、软件版本号和 Dell 版权信息。要访问**“About”（关于）**页面，请：

- 单击**“About”（关于）**。 系统将打开**“About”（关于）**页面：

关于 PageDevice 管理按钮

Switch Administrator 管理按钮使网络管理员能够在远程位置轻松地配置 PowerConnect。
Switch Administrator 包含以下管理按钮：

按钮	说明
Apply Changes	将设置更改应用于设备。
Add	将信息添加至表或信息窗口。
Telnet	启动 Telnet 会话。
Reset All Counters	查询表。
Show All	显示设备表。
Transfer to Server	将固件文件从设备传输至服务器。
← →	在列表之间移动信息。
Refresh	刷新设备信息。
Show Log File	打开 **“Log File Table”（日志文件表）**页面。
Show Log RAM	打开 **“Log Ram Table”（日志 Ram 表）**页面。

Restart DHCP	重新启动 DHCP 客户端连接。
Add ACE to ACL	将 ACE 添加至 ACL。
Add ACL	添加 ACL。
Add List Name	添加新列表。
Attach to Interface	将分类的列表附加到界面上。
Reset All Counters	重设统计计数器。
Print	打印**“Network Management System”（网络管理系统）**页面和/或表信息。
Sort	排序表信息。
Show Neighbors List	通过**“Neighbors Table”（邻居表）**页面显示邻居列表。
Restore Defaults	恢复设备的默认设置。
Draw	迅速创建统计图表。

设备管理按钮

使用 CLI

本节介绍命令行界面 (CLI)。

命令模式

CLI 分为几种命令模式。 每种命令模式均有其特定的命令集。 在系统提示符（控制台提示符）后输入问号 ? 将显示特定命令模式的可用命令列表。

每种模式均有一个特定的命令，用于从一种命令模式切换到另一种命令模式。 访问模式的标准如下所示：

- 用户执行模式
- 优先执行模式
- 全局配置模式
- 接口配置模式

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设备配置的任务，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。

优先执行模式可提供对设备一般配置的访问。 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。

全局配置模式以全局级别管理设备配置。 要进行特定配置，请进入下一个级别，即接口配置模式。 不需要密码。

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

用户执行模式

登录到设备后，用户执行命令模式处于启用状态。 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，请输入命令 ?。

用户级提示符由主机名后跟尖括号 (>) 组成。

```
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。

优先执行模式

此模式可确保优先访问受密码保护，以防止未经授权的使用。 密码在屏幕上显示为 *****，
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，输入命令 enable 并按 <Enter> 键。 系统将显示密码提示。
2. 输入密码并按 <Enter> 键。 密码显示为 *。 系统将显示优先执行模式提示符。
   优先执行模式提示符由设备主机名后跟井号 (#) 组成。

```
console#
```

- 要列出优先执行命令，请输入命令 ?。

要从优先执行模式返回用户执行模式，请使用：

- enable
- disable
- exit/end
- Ctrl+Z 组合键

以下实例说明了如何进入优先执行模式并返回用户执行模式：

```
console>enable
```

```
Enter Password: ******

console#

console#disable

console>
```

exit 命令用于从任一模式返回上一级别模式，例如，从接口配置模式返回全局配置模式，
然后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。 优先执行模式命令 configure 用于进入全局配置模式。

要查看并列出全局配置模式命令，请：

- 在优先执行模式提示符后输入 configure 并按 <Enter> 键。 系统将显示全局配置模式提示符。 全局配置模式提示符由设备主机名后跟井号 # 和 (config) 组成。

```
console(config)#
```

- 要列出全局配置命令，请输入命令 ?。

要从全局配置模式返回优先执行模式，请使用以下命令之一：

- exit
- Ctrl+Z 组合键

以下实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#
```

接口配置模式

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

- VLAN — 包含创建 VLAN 并将其配置为一个整体的命令，例如，创建一个 VLAN 并将 IP 地址应用于该 VLAN。
- 端口通道 — 包含配置单个端口的命令，例如，将端口分配给 LAG。
- 线接口 — 包含配置管理连接的命令。 其中包括线速和超时设置等命令。
- IP 访问列表 — 包含管理访问列表的命令。 这些命令用于创建和维护列表。
- 以太网 — 包含管理端口配置的命令。
- 管理访问列表 — 包含定义访问列表以进行管理的命令。 访问列表用于管理访问授权和用户验证。
- MAC 列表 — 配置允许基于 MAC 地址进行通信所需的条件。

启动 CLI

通过与控制台端口的直接连接或 Telnet 连接可以管理 PowerConnect 3324/3348， 这是通过在命令提示符后键入命令关键字和参数来实现的。 使用 CLI 类似于在 UNIX 系统中输入命令。

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

有关配置初始 IP 地址的详细信息，请参阅“初始配置”。

控制台连接

启动 CLI：

1. 启动设备并等待，直至系统显示启动提示符 `Console>`。
2. 配置设备并输入必要的命令以完成所需的任务。
3. 任务完成后，通过输入 `quit` 或 `exit` 退出会话。

要注销当前用户并以新用户登录，请在优先执行命令模式中键入 login 命令。

注： 闲置时间超过用户指定的时间段后，Telnet 会话将自动断开连接。

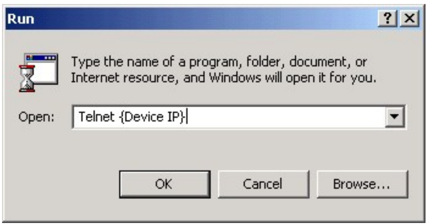
Telnet 连接

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

PowerConnect 3324/3348 同时最多支持四个 Telnet 会话。 可以通过 Telnet 会话使用所有 CLI 命令。

启动 Telnet 会话：

1. 选择 **“Start”（开始）**>**“Run”（运行）**。 系统将打开 **“Run”（运行）**窗口。



运行窗口

2. 在 **“Open”（打开）**字段中键入 Telnet 和设备 IP 地址。

3. 单击 **“OK”（确定）**。 Telnet 会话将启动。

Telnet 窗口

[返回目录页面](#)

[返回目录页面]

硬件说明

Dell™ PowerConnect™ 3324/3348 用户指南

- [PowerConnect 3324/3348 说明]
- [端口说明]
- [LED 定义]

PowerConnect 3324/3348 说明

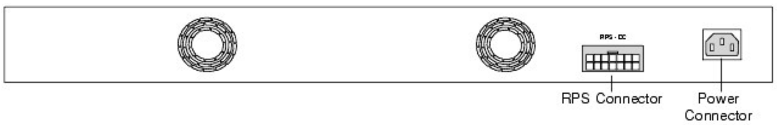
PowerConnect 3324/3348 尺寸

此设备的尺寸如下所示：

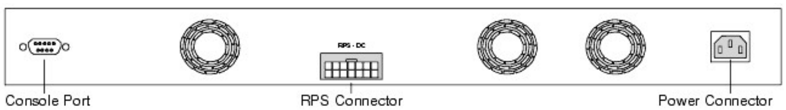
- 宽度 — 19"
- 高度 — 1U

PowerConnect 3324/3348 背面板

Dell™ PowerConnect™ 3324/3348 的背面板如下图所示：



PowerConnect 3324 背面板



PowerConnect 3348 背面板

PowerConnect 3324/3348 组件

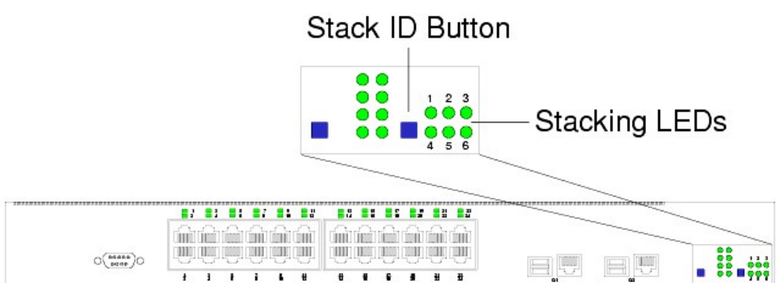
本节介绍各种 PowerConnect 3324/3348 硬件组件，并包括以下主题：

- [一般设备组件]
- [模式按钮]
- [堆叠 ID 按钮]

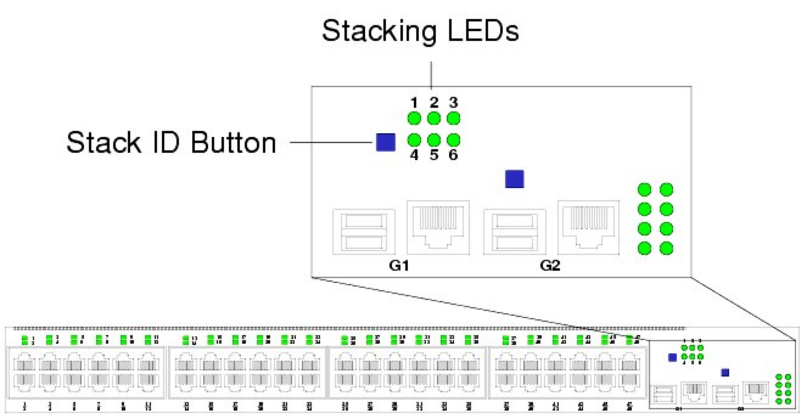
一般设备组件

PowerConnect 3324/3348 包括以下硬件组件：

- CPU —基于 Motorola 的 MPC 8245。
- FLASH — 8 MB FLASH 存储器。
- SDRAM — 包含 32 MB。



PowerConnect 3324 前面板



PowerConnect 3348 前面板

模式按钮

模式按钮用于在端口活动和端口双工设置之间进行切换。

堆叠 ID 按钮

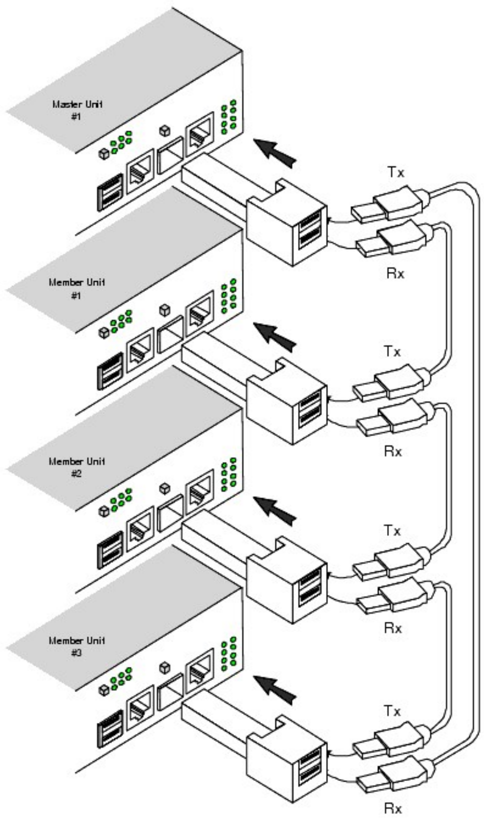
PowerConnect 3324/3348 前面板包含一个**堆叠 ID** 按钮，网络管理员可以使用此按钮手动选择堆叠主装置和堆叠成员。

注： 必须在设备引导后 15 秒内选择堆叠主装置和堆叠成员。 如果未在 15 秒内选择堆叠主装置，则必须重启动设备以选择装置 ID。

一旦选定了堆叠主装置，则其余设备均被定义为堆叠成员。 主装置获取的装置 ID 为 1，堆叠成员将获取不同的装置 ID（2 到 6）。 例如，如果堆叠中有 4 个装置，则主装置的 ID 为 1，第二个堆叠成员的 ID 为 2，第三个堆叠成员的 ID 为 3，第四个堆叠成员的 ID 为 4。

堆叠模块和连接器

PowerConnect 3324/3348 堆叠模块将连接到端口 G2。 堆叠模块为小型 GBIC 模块，带有两个堆叠连接器： RX 和 TX。 其中 RX 为低位连接点，TX 为高位连接点。 此模块使用堆叠电缆连接至其它堆叠装置。 顶部装置的 RX 将连接到较低装置的 TX。 这就构成了环形拓扑。 堆叠连接图说明了环形拓扑。



堆叠连接

有关连接堆叠电缆的详细信息，请参阅“连接堆叠电缆”。

端口说明

以太网端口说明

每个 PowerConnect 3324 装置配有 24 个 FE 10BaseT/100BaseTX UTP 铜质 RJ45 端口以及 2 个组合端口。 每个 PowerConnect 3348 装置配有 48 个 FE 10BaseT/100BaseTX UTP 铜质 RJ45 端口以及 2 个组合端口。 每个组合端口均为单个逻辑端口，具有以下两个物理接口：

- 1000Base-T 连接器。
- 小型 GBIC (SFP) 连接器。

每次只能使用组合端口的两个物理连接中的一个。

如果启用了自动 MDIX，PowerConnect 3324/3348 将自动检测并更正所有端口上绞接电缆和直通电缆之间的差异。

PowerConnect 3324/3348 支持速率为 10/100 Mbps 的铜质端口的半双工和全双工模式。

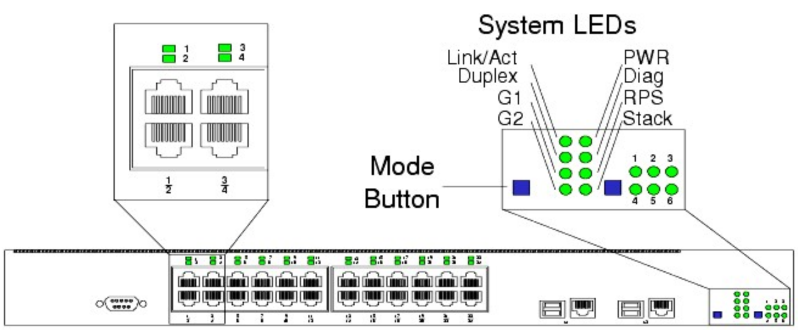
控制台端口说明

控制台端口接口支持八个数据位、一个停止位以及无奇偶校验的同步数据。 支持所有 RS232 插针（9 插针），可支持调制解调器。

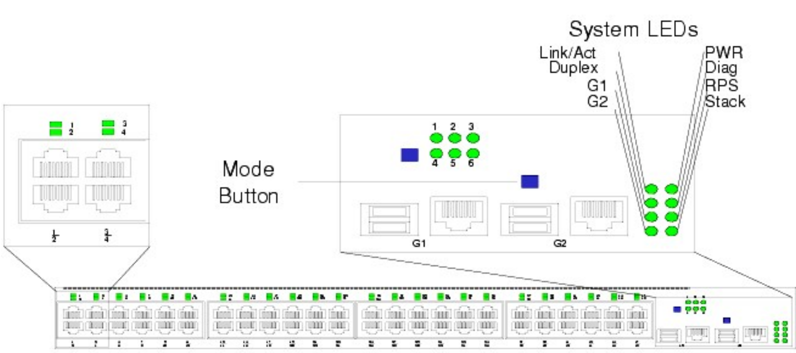
LED 定义

下图中的前面板 LED 表明了端口链路的状态和模式、电源设备状态、堆叠状态以及系统诊断程序。 LED 的类型如下所示：

- 端口 LED
- 系统 LED
- 堆叠 LED



前面板 LED： 24 个端口



前面板 LED： 48 个端口

端口 LED

每个端口的上方均有一个相应的 LED。 LED 将显示链路活动或双工模式，这取决于端口 LED 的显示模式。 有关设置 LED 显示模式的详细信息，请参阅“系统 LED”。

颜色	活动	定义
绿色	静态	端口链路良好。 端口运行速率为 100 Mbps。
绿色	闪烁	端口链路良好并且有活动。 端口运行速率为 100 Mbps。
红色	静态	端口链路良好。 端口运行速率为 10 Mbps。
红色	闪烁	端口链路良好并且有活动。 端口运行速率为 10 Mbps。
不亮	不亮	端口链路断开。

端口链路活动

颜色	活动	定义
绿色	静态	端口全双工。
不亮	不亮	端口链路断开或半双工。

端口双工模式

系统 LED

八个系统 LED 表明了设备各个方面的状态：

- 如在本节开始处的前面板图中所示，左上方的两个系统 LED 表示链路活动和双工。 这些 LED 表明端口 LED 显示的是链路活动还是双工状态。

- 图中左下方的两个 LED 显示了吉位端口 1 和 2 的链路活动状态，如下所示：

颜色	活动	定义
绿色	静态	端口链路良好。 端口运行速率为 1000 Mbps。
绿色	闪烁	端口链路良好并且有活动。 端口运行速率为 1000 Mbps。
红色	静态	端口链路良好。 端口运行速率为 10/100 Mbps。
红色	闪烁	端口链路良好并且有活动。 端口运行速率为 10/100 Mbps。
不亮	不亮	端口链路断开。

吉位端口链路活动状态

- 系统 LED 旁边的Mode（**模式**）按钮用于在两种显示模式之间进行切换。 有关任何一种模式下的端口 LED 的说明，请参阅“端口 LED”。

电源设备出现故障时，系统将生成错误信息和若干陷阱。 每个电源设备的状态由前面板上的 LED 表明。

- 右侧的四个 LED 显示了电源设备、诊断模式和堆叠模式的状态，如下所示：

LED	颜色	活动	定义
PWR	绿色	静态	电源设备可以运行。

	琥珀色	静态	电源设备出现故障。
RPS	绿色	静态	冗余电源设备可以运行。
	琥珀色	静态	冗余电源设备出现故障。
	不亮	不亮	无冗余电源设备。
诊断	绿色	闪烁	系统当前处于诊断模式。
堆叠	绿色	静态	堆叠已成功完成。
	不亮	不亮	独立状态。

电源、诊断和堆叠 LED

堆叠 LED

堆叠 LED 表明了装置在堆叠中所处的位置。 如在本节开始处的前面板图例中所示，堆叠 LED 的编号为 1 到 6。堆叠中的每个装置均有一个亮起的堆叠 LED，用于表明其在堆叠中的位置。 当堆叠 LED 1 亮起时，表明该装置为主装置。 当编号为 2 到 6 的堆叠 LED 中的一个 LED 亮起时，表明该装置为相应的堆叠成员装置。

返回目录页面

[返回目录页面]

安装 PowerConnect 3324/3348 交换机

Dell™ PowerConnect™ 3324/3348 用户指南

安装注意事项

警告： 放置交换机的机架或机柜应足够稳固，以防止交换机不稳固和/或跌落。

警告： 请确保电源电路正确接地。

警告： 仔细阅读并遵循维修标记上的说明。 除非系统说明文件中已有说明，否则请勿维修任何产品。 打开或卸下标有带闪电标记的三角符号的护盖可能会导致触电。 只有经过培训的维修技术人员才能对这些组件进行维修。

警告： 请确保电源电缆、延长电缆和/或插头未损坏。

警告： 请确保产品未被水沾湿。

警告： 请勿将其它物品塞入设备，否则可能会导致火灾或触电。

警告： 待产品冷却后再卸下护盖或触摸内部设备。

警告： 请确保交换机的电源电路、电缆和过电流保护未过载。 要确定供电电路过载的可能性，请将与该交换机安装在同一电路中的所有交换机的额定安培值相加。 将总值与电路的额定限制值相比较。 最大额定安培值通常印在交换机上靠近交流电源连接器的地方。

注意： 请确保设备未暴露在有暖气片和/或热源的地方。

注意： 请确保冷却通风孔未被堵塞。

注意： 仅将设备与许可的设备配合使用。

注意： 请勿将交换机安装在运行环境温度可能超过 40℃ (122®H) 的环境中。

注意： 请确保交换机的正面、侧面和背面通风良好。

现场要求

Dell™ PowerConnect™ 3324/3348 系列设备可以安装在标准 19 英寸设备机架中，也可以放置在桌面上。 在安装装置之前，请验证所选的安装位置符合如下所述的现场要求。

- 一般要求 — 确保电源设备已正确安装。
- 电源要求 — 在距可方便插拔的接地插座（100 - 250 VAC，50 - 60 Hz）1.5 m
（5 英尺）的范围内安装装置。 最好提供两个单独的电源设备，例如一个 UPS 和一个单独相位电源设备。
- 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 到 40℃（32 到 122®H），相对湿度最大为 95%，非冷凝。 请确保水或湿气无法进入装置外壳。

打开包装并安装

包装内容

打开 PowerConnect 3324/3348 的包装时，请确保包含以下项目：

- PowerConnect 3324/3348 设备。
- 一根交流电源电缆。
- 虚拟调制解调器电缆。
- 自粘橡皮垫。
- 用于机架安装的机架安装套件。
- 说明文件 CD。

打开包装

注： 打开 PowerConnect 3324/3348 交换机的包装之前，请检查包装，如有损坏，请立即报告。

1. 通过戴上 ESD 腕带并将 ESD 固定夹连接到金属表面来导去身上的静电。
2. 将包装箱放在清洁的平面上，然后剪断所有捆扎包装箱的带子。
3. 打开包装箱或取下包装箱顶盖。
4. 从包装箱中小心取出装置，并将其放置在稳固清洁的表面上。
5. 取下所有包装材料。
6. 检查产品是否有损坏。 如有任何损坏，请立即报告。 有关与 Dell 联系的信息，请参阅“获得帮助”。

设备机架安装

警告： 在机架或机柜中安装 PowerConnect 3324/3348 交换机之前，请从装置上断开所有电缆的连接。

要安装 PowerConnect 3324/3348，请：

1. 通过戴上 ESD 腕带并将 ESD 固定夹连接到金属表面来导去身上的静电。
2. 将 PowerConnect 3324/3348 交换机放置在稳固的平面上。
3. 将附带的机架固定支架放在 PowerConnect 3324/3348 的一侧。确保 PowerConnect 3324/3348 上的安装孔与机架固定支架上的安装孔对齐。
4. 将附带的螺钉插入机架安装孔，并用梅花槽螺丝刀将其拧紧。
5. 重复此过程，以安装 PowerConnect 3324/3348 另一侧的机架固定支架。
6. 将装置放入 19 英寸机架中，并用机架螺钉（PowerConnect 3324/3348 供应商不提供）将装置固定到机架中。 固定时先拧紧下部的一对螺钉，然后再拧紧上部的一对螺钉，以确保装置的重量在安装过程中均匀分布。 请确保通风孔未被堵塞。

不使用机架安装交换机

如果 PowerConnect 3324/3348 不安装在机架中，则必须安装在平面上。 该平面必须能够承受设备以及设备电缆的重量。

1. 将 PowerConnect 3324/3348 放置在平面上，在两侧各留出 2 英寸的空间，并在背面留出 5 英寸的空间。
2. 确保设备通风良好。
3. 将橡皮支脚连接至设备底部以防止设备滑动。

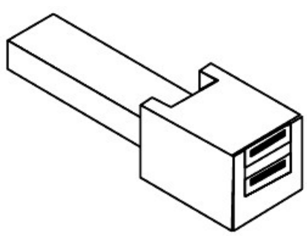
堆叠 PowerConnect 3324/3348

PowerConnect 3324/3348 最多可支持堆叠六个 PowerConnect 3324/3348 设备，或者最多 192 个高速以太网端口和六个吉位端口。 每个 PowerConnect 3324/3348 堆叠均包含一个主装置，其余装置则作为堆叠成员。 所有管理均通过主装置执行。 24 端口设备和 48 端口设备均可以包括在堆叠中。

要启用堆叠，必须使用连接至 SFP 插槽中的 G2 端口的堆叠模块堆叠装置。

连接堆叠电缆

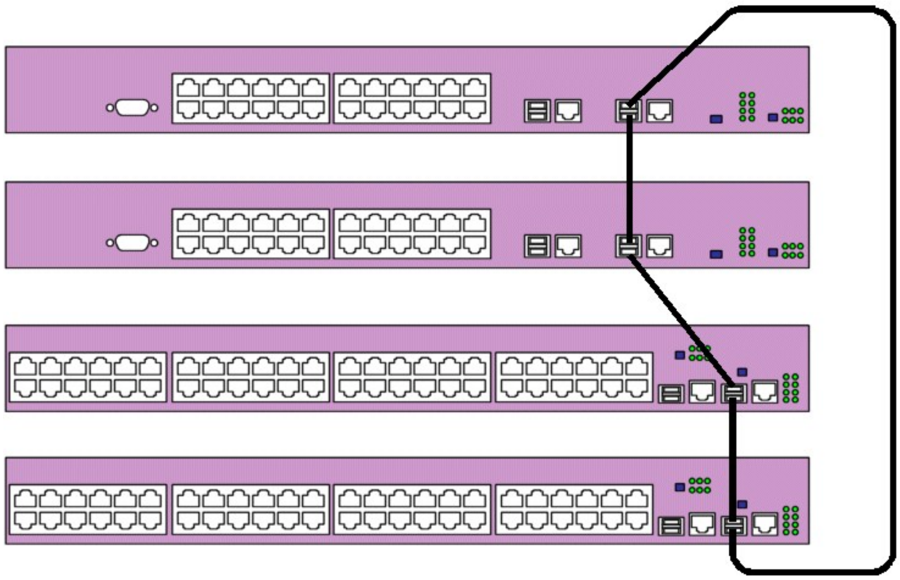
1. 将所有设备放置在机架中或平面上。
2. 在每个 G2 端口中插入一个堆叠连接器。



USB 连接器

3. 将主装置的下部 RX 堆叠连接器连接至选定成员的上部 TX 端口。
4. 以堆叠环形拓扑的方式连接堆叠，即将堆叠电缆从下部 RX 堆叠连接器连接至上部 TX 堆叠连接器。
5. 确保上部和下部的堆叠成员均通过堆叠电缆进行连接。 下图示意了正确连接的堆叠：

注： 如果未构成堆叠环，则堆叠将不起作用。



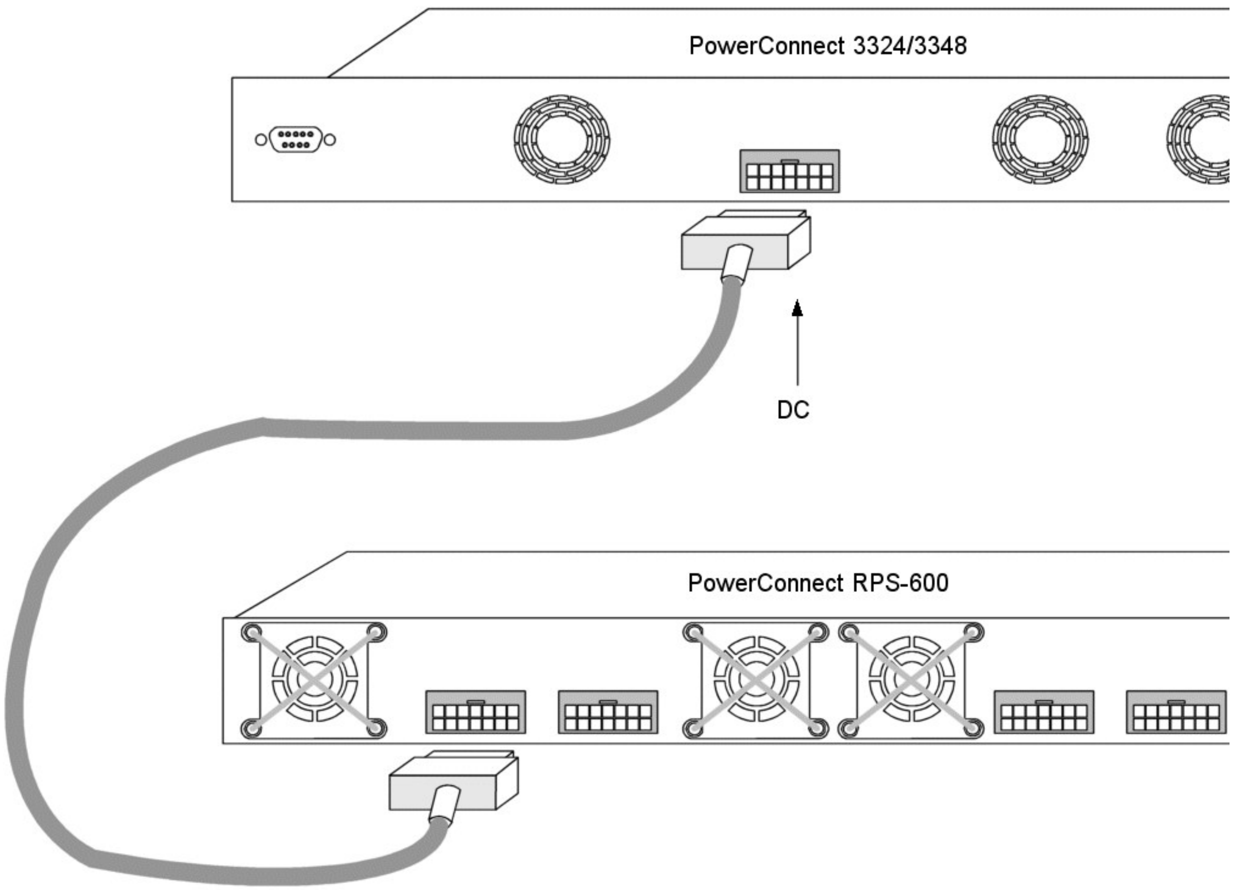
已连接的堆叠

有关配置堆叠的详细信息，请参阅“配置堆叠”。

将 PowerConnect 3324/3348 连接至电源设备

下节包含了将 PowerConnect 3324/3348 连接至交流电源连接的说明。 PowerConnect 3324/3348 通过以下方式获得电源：

- 交流电源。
- 可选的 PowerConnect RPS-600 冗余电源设备。
- 交流电源和直流电源。



将 PowerConnect 3324/3348 连接至电源设备

- 将 PowerConnect 3324/3348 连接至以上列出的电源之一。

交流电源连接

应该使用已安全接地的 1.5 m（5 英尺）标准电源电缆为装置提供交流电源。

要将电源连接至 PowerConnect 3324/3348，请：

1. 将电源电缆连接至背面板上的交流电源主插槽。 如果有冗余电源模块，请将此冗余电源模块的电缆连接至单独的电源设备。
2. 将电源电缆连接至接地的交流电源插座。
3. 通过检查前面板上的 LED 来确定设备已正确连接并且运行正常。 有关 LED 的详细信息，请参阅“LED 定义”。

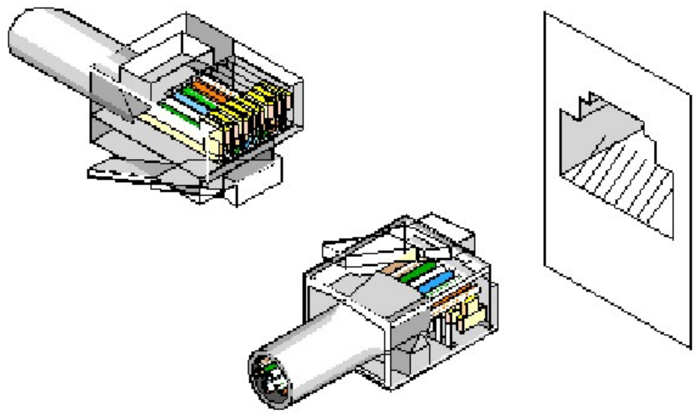
电缆、端口和插针输出信息

本节介绍 PowerConnect 3324/3348 的物理接口，并提供有关电缆连接的信息。 站点是通过前面板上的物理接口连接至 PowerConnect 3324/3348 端口的。 对于每个站点，将设置相应的模式
（半/全双工和自动）。

端口连接

这些端口都是标准的 RJ45 以太网端口。 使用直通电缆可以将交换端口连接至以标准 RJ45 以太网站点模式布线的站点。 传输设备使用绞接电缆相互连接。

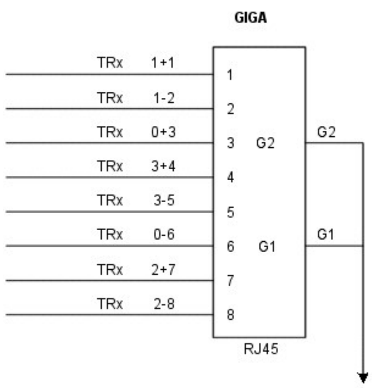
下图说明了 10/100M 端口的 RJ45 插针编号的分配情况。



RJ45 插针编号分配

插针	使用情况
1	RX +
2	RX -
3	TX +
4	
5	--
6	TX -
7	-
8	-

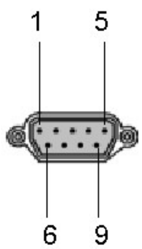
下图说明了吉位端口连接器：



吉位端口连接器

PowerConnect 3324/3348 通过串行电缆连接至终端以进行初始设置和配置。
（也可以使用运行终端仿真软件的 PC）。 串行电缆为内孔至内孔的 DB-9 绞接电缆。

下图说明了 DB-9 连接器。



DB-9 串行电缆

插针	使用情况
1	未使用
2	TXD
3	RXD
4	未使用
5	GND
6	未使用
7	CTS
8	RTS
9	未使用

DB-9 插针编号分配

电缆连接

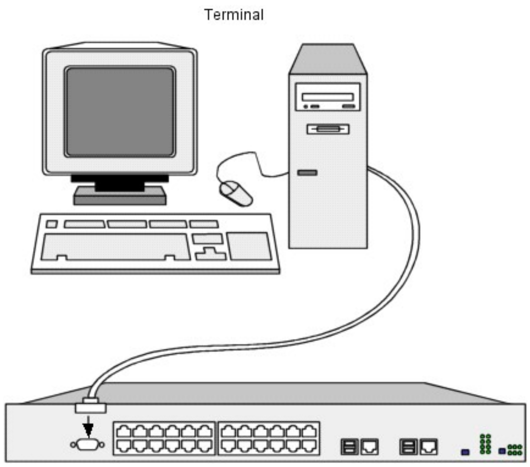
本小节介绍如何将各种电缆连接至 PowerConnect 3324/3348 设备。

ASCII 终端（串行）连接

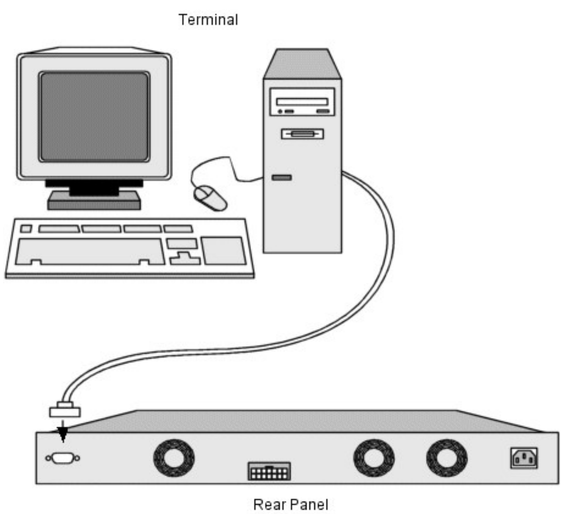
串行端口连接器是 DB-9 型连接器。 需要附带的接口电缆来连接设备。

要连接设备，请：

1. 将接口绞接电缆连接至终端 ASCII DTE RS-232 连接。
2. 将接口绞接电缆连接至设备串行连接。



PowerConnect 3324 终端连接



PowerConnect 3348 终端连接

返回目录页面

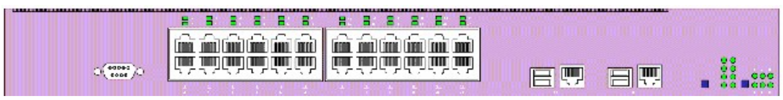
返回目录页面

概览

Dell™ PowerConnect™ 3324/3348 用户指南

系统说明

Dell™ PowerConnect™ 3324 和 3348 设备是高级的、第 2 层交换机，它们即可独立使用也可堆叠使用。 PowerConnect 3324 和 PowerConnect 3348 还可用作独立的第 2 层交换系统。 使用带内管理（通过远程网络站点）或通过控制台均可管理 PowerConnect 3324/3348 设备。



PowerConnect 3324

作为堆叠成员运行时，每个 PowerConnect 3324 装置可提供 24 个 10 BaseT/100BaseTX 高速以太网端口、一个吉位以太网组合端口（10/100/1000 BaseT 或小型 GBIC 连接器）和一个吉位以太网堆叠端口。

PowerConnect 3348

作为堆叠成员运行时，每个 PowerConnect 3348 装置可提供 48 个 10 BaseT/100BaseTX 高速以太网端口、一个吉位以太网组合端口（10/100/1000 BaseT 或小型 GBIC 连接器）和一个吉位以太网堆叠端口。

作为独立装置运行时，PowerConnect 3324/3348 堆叠端口可以用作吉位以太网端口。

PowerConnect 3324/3348 堆叠概览

PowerConnect 3324/3348 堆叠提供了通过单点进行的多设备管理，就好像所有堆叠成员是一个装置。 通过一个 IP 地址（用于 SNMP 管理）和控制台/Telnet 会话（通过其管理整个堆叠）可以访问所有成员。

对于每个堆叠，PowerConnect 3324/3348 最多可支持堆叠六个装置，或者最多 192 个 FE 和六个吉位以太网端口。 PowerConnect 3324/3348 也可以作为独立装置运行。

在堆叠设置过程中，网络管理员将选择一个设备作为堆叠主装置，选择所有其它设备作为堆叠成员，并为它们分配唯一的装置 ID。

PowerConnect 3324/3348 堆叠可提供跨堆叠的第 2 层功能，包括：

- 交换
- 主干聚合
- 端口镜像
- VLAN

例如，可以从属于不同堆叠成员的端口配置 VLAN，或者配置第二个堆叠成员到第三个堆叠成员的端口镜像。 在堆叠配置中运行的应用程序是集中运行的。 例如，整个堆叠的生成树协议在主装置上运行。 设备软件则是针对每个堆叠成员单独下载的。

PowerConnect 3324/3348 堆叠体系结构提供了堆叠拓扑的动态学习功能，在发生以下事件时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
- 装置间链路丢失
- 插入装置
- 卸下堆叠装置

堆叠成员和装置 ID

堆叠运行模式在引导过程中确定。

PowerConnect 3324/3348 装置出厂时默认装置 ID 为 1。 对于堆叠配置，装置 ID 非常重要。 如果堆叠成员在没有堆叠模块的情况下重新引导，则设备将作为独立装置运行，直至设备重启动。 如果 PowerConnect 3324/3348 装置作为独立装置运行，则所有堆叠 LED 都不亮。 如果将装置重新连接至堆叠，装置 ID 不会被删除，并仍将有效。

注： 必须将堆叠模块插入端口 G2，堆叠才能运行。 如果将堆叠模块插入端口 G1，控制台上将显示警告信息。

主装置引导时或者插入或卸下堆叠成员时，主装置将启动堆叠查找进程。 如果发现两个成员具有相同的装置 ID，或者未找到主装置，则整个堆叠将无法运行。 堆叠 LED 将呈红色稳定亮起。

配置操作

在可运行的 PowerConnect 3324/3348 堆叠中，由堆叠主装置负责堆叠配置。 每个堆叠成员没有单独的配置文件。 堆叠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 PowerConnect 3324/3348 堆叠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： 即使堆叠被重设和/或端口不再存在，所有已配置端口的堆叠配置仍会保存。

只能通过明确的用户配置更改配置文件。 此外，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。
- 装置在堆叠模式和独立模式之间进行切换。

每次系统重新引导时，已存储的配置都会写入启动配置文件。

如果从堆叠中卸下 PowerConnect 3324/3348 堆叠成员，然后由其它装置代替，
并使用相同的装置 ID，则新的堆叠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 Dell OpenManage™ Switch Administrator 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。

重新排列堆叠

可以通过卸下堆叠成员或重新排列堆叠电缆来更改堆叠顺序。 堆叠成员的排列顺序不是根据堆叠成员的物理顺序建立，而是根据装置 ID 的分配建立。 更改堆叠顺序后，
堆叠配置将存储在堆叠主装置中，然后堆叠将重启动。

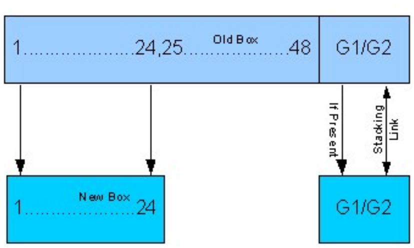
如果堆叠中的 PowerConnect 3324/3348 装置被卸下或替换，堆叠将按以下方式恢复断开的连接：

- 如果堆叠断开连接超过两分钟，则整个堆叠将不再传输网络通信。 每个堆叠成员将重新引导并等待，直至重新连接堆叠。 如果装置未被替换，主装置将不断轮询堆叠。
- 如果堆叠在两分钟之内重新连接，则所有装置将保持堆叠状态，并在五秒钟内重新获得与其它装置的连接。 新的堆叠成员将连接至主装置，并根据主装置的配置进行初始化。 如果未存储配置，设备将使用默认配置进行配置。

更换堆叠成员

如果使用新的设备替换堆叠成员，将选定所需的设备 ID。 此外，先前的设备配置将应用于插入的堆叠成员。 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叠成员。 例如：

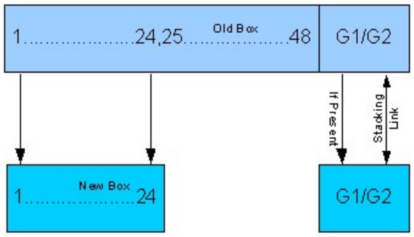
- 如果用 PowerConnect 3324 替换 PowerConnect 3324，则新的 24 个 10/100 BaseT 端口将获取先前的 24 个 10/100 BaseT 端口的配置。 端口 G1 和 G2 将获取先前设备的 G1 和 G2 端口配置。
- 如果用 PowerConnect 3324 替换 PowerConnect 3348，则 10/100 BaseT 端口 1 到 24 将获取先前设备端口 1 到 24 的配置。端口 G1 和 G2 将获取先前设备的 G1 和 G2 端口配置。



用 PowerConnect 3324 替换 PowerConnect 3348

- 如果用 PowerConnect 3348 替换 PowerConnect 3348，则新的 48 个 10/100 BaseT 端口将获取先前的 48 个 10/100 BaseT 端口的配置。 端口 G1 和 G2 将获取先前设备的 G1 和 G2 端口配置。
- 如果用 PowerConnect 3348 替换 PowerConnect 3324，则 10/100 BaseT 端口 1 到 24 将获取先前设备端口 1 到 24 的配置。

- 端口 25 到 48 将获取出厂时的默认端口配置。 端口 G1 和 G2 将获取先前设备的 G1 和 G2 端口配置。



用 PowerConnect 3348 替换 PowerConnect 3324

PowerConnect 用户指南概览

PowerConnect 用户指南分为两部分：

- 关于安装 PowerConnect 3324/3348 交换机
- 使用 Dell OpenManage Switch Administrator

安装 PowerConnect 3324/3348 交换机

本节包含以下有关打开包装、安装和配置 PowerConnect 3324/3348 的小节：

- 硬件说明 — 包含有关 PowerConnect 3324/3348 硬件的信息，包括端口和 LED 类型的说明。
- 安装 PowerConnect 3324/3348 交换机 — 包含有关在机架中或平面上安装 PowerConnect 3324/3348 的说明。 此外，本节还包含安装注意事项以及连接器和电缆说明。
- 配置 PowerConnect 3324/3348 交换机 — 包含有关设备初始配置的说明，包括下载设备软件、设备引导屏幕和可选的配置功能。

使用 Dell OpenManage Switch Administrator

本节包含以下有关使用 Web 管理系统和命令行界面 (CLI) 设备管理系统配置设备的信息：

- 使用入门 — 包含有关初始使用 Web 管理系统界面的信息，包括管理和信息图标、组件列表以及设备视图和树视图的说明。
- 配置系统信息 — 包含有关配置一般系统信息的信息，包括定义系统信息、配置默认 IP 地址、定义设备安全保护和 SNMP 团体、下载设备软件以及定义高级设置。
- 配置交换机信息 — 包含有关配置端口和 VLAN、定义静态和动态地址表、配置 GARP 和 GVRP、定义生成树参数、聚合端口以及配置多点传送支持的信息。
- 查看统计数据 — 包含有关查看端口、GVRP、以太网类、RMON 及接口统计数据的表和图表统计数据的信息。
- 配置服务质量 — 包含有关配置设备服务级别的信息。
- 获得帮助 — 包含有关技术帮助、订购问题、退回部件以要求保修或退款以及如何与 Dell 联系的信息。

PowerConnect 3324/3348 CLI 说明文件

除 *PowerConnect 3324/3348 用户指南*之外，Dell 还提供了 *PowerConnect 3324/3348 CLI 参考指南*。 *PowerConnect 3324/3348 CLI 参考指南*提供了有关用于配置 PowerConnect 3324/3348 的 CLI 命令的信息。

[返回目录页面]

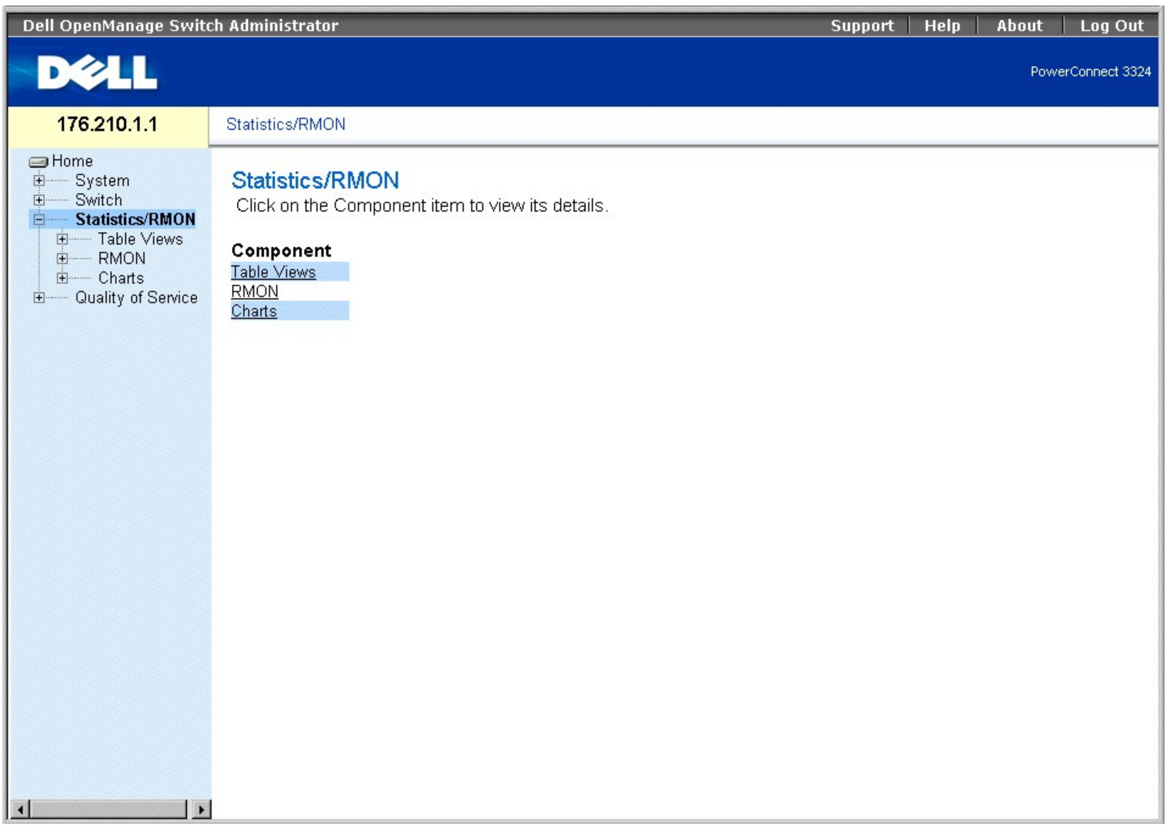
[返回目录页面]

查看统计数据

Dell™ PowerConnect™ 3324/3348 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**“Statistics/RMON”（统计数据/RMON）**页面，请：

- 在树视图中单击**“Statistics/RMON”（统计数据/RMON）**。
  系统将打开**“Statistics/RMON”（统计数据/RMON）**页面。



统计数据/RMON 页面

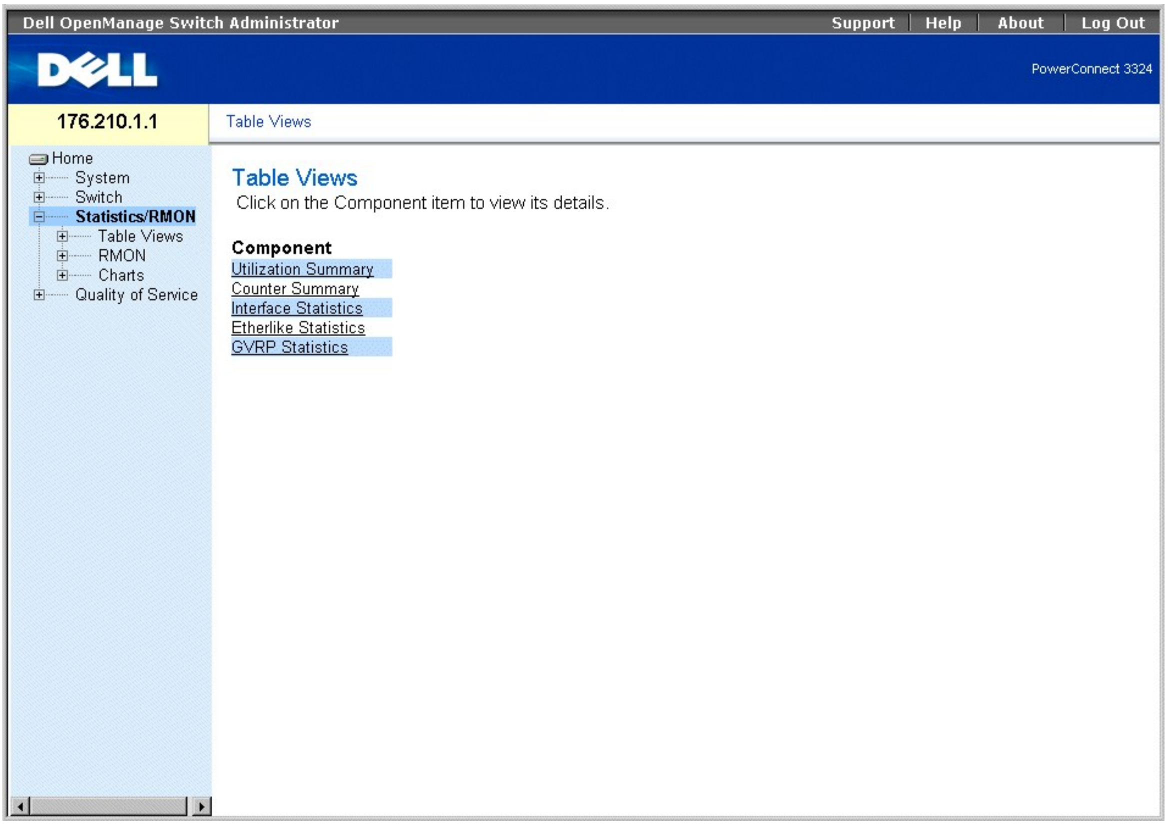
本节包含以下主题：

- 查看表
- 查看 RMON 信息
- 查看图表

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**"Table View"**
（表视图）页面，请：

- 在树视图中单击**"Statistics"（统计数据）>"Table"（表）**。 系统将打开**"Table View"（表视图）**页面。



表视图页面

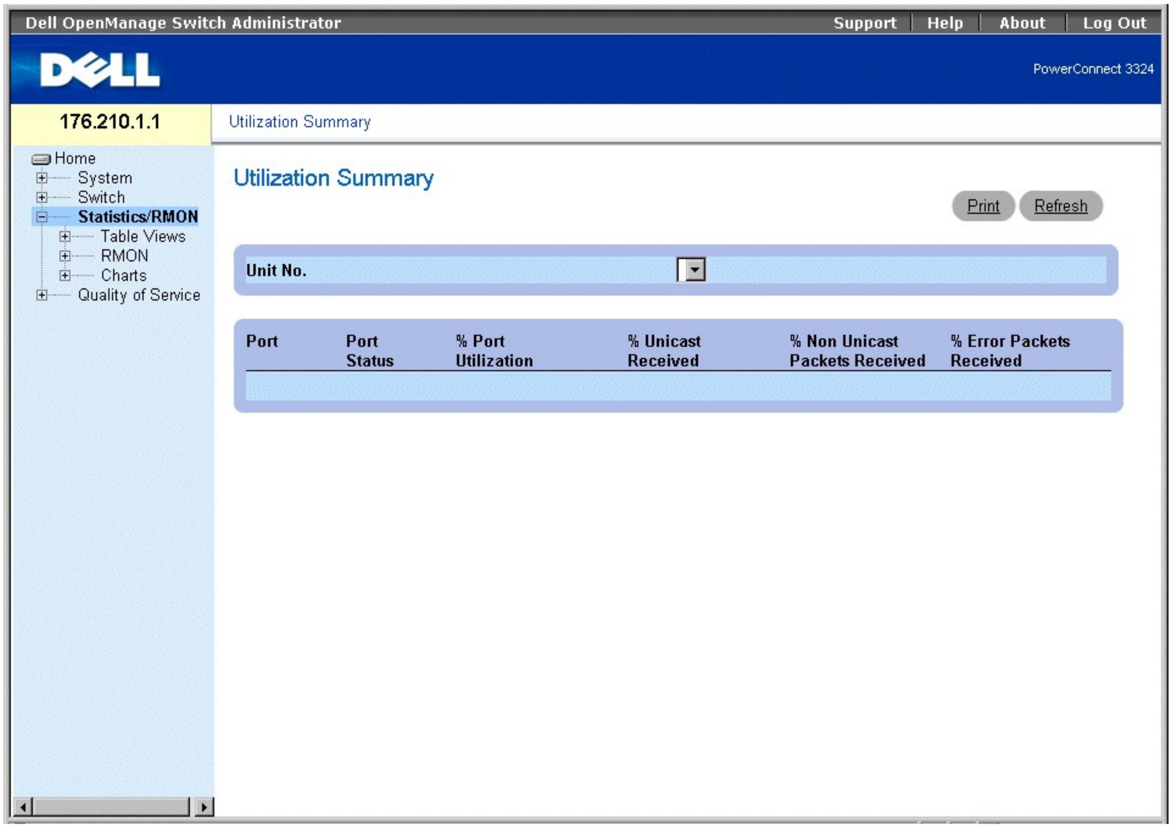
"Table View"（表视图）页面包含以下链接：

- 查看使用摘要
- 查看计数器摘要
- 查看接口统计数据
- 查看以太网类统计数据
- 查看 GVRP 统计数据

查看使用摘要

"Utilization Summary"（使用摘要）页面包含端口使用的统计数据。 要打开
"Utilization Summary"（使用摘要）页面，请：

- 在树视图中单击**"Statistics"（统计数据）>"Table View"（表视图）>"Utilization Summary"（使用摘要）**。 系统将打开**"Utilization Summary"（使用摘要）**页面：



使用摘要页面

"Utilization Summary"（使用摘要）页面包含以下字段：

- **"Unit No."（装置号）**— 表示显示端口统计数据的装置号。
- **"Port"（端口）**— 表示端口号。
- **"Port Status"（端口状态）**— 表示端口的状态。
- **"% Port Utilization"（% 端口使用）**— 表示端口的使用。
- **"% Unicast Received"（% 接收到的单点传送）**— 表示端口上接收到的单点传送信息包的百分比。
- **"% Non Unicast Received"（% 接收到的非单点传送）**— 表示端口上接收到的坏信息包的数量。
- **"% Error Packets Received"（% 接收到的错误信息包）**— 表示端口上接收到的包含错误的信息包的数量。

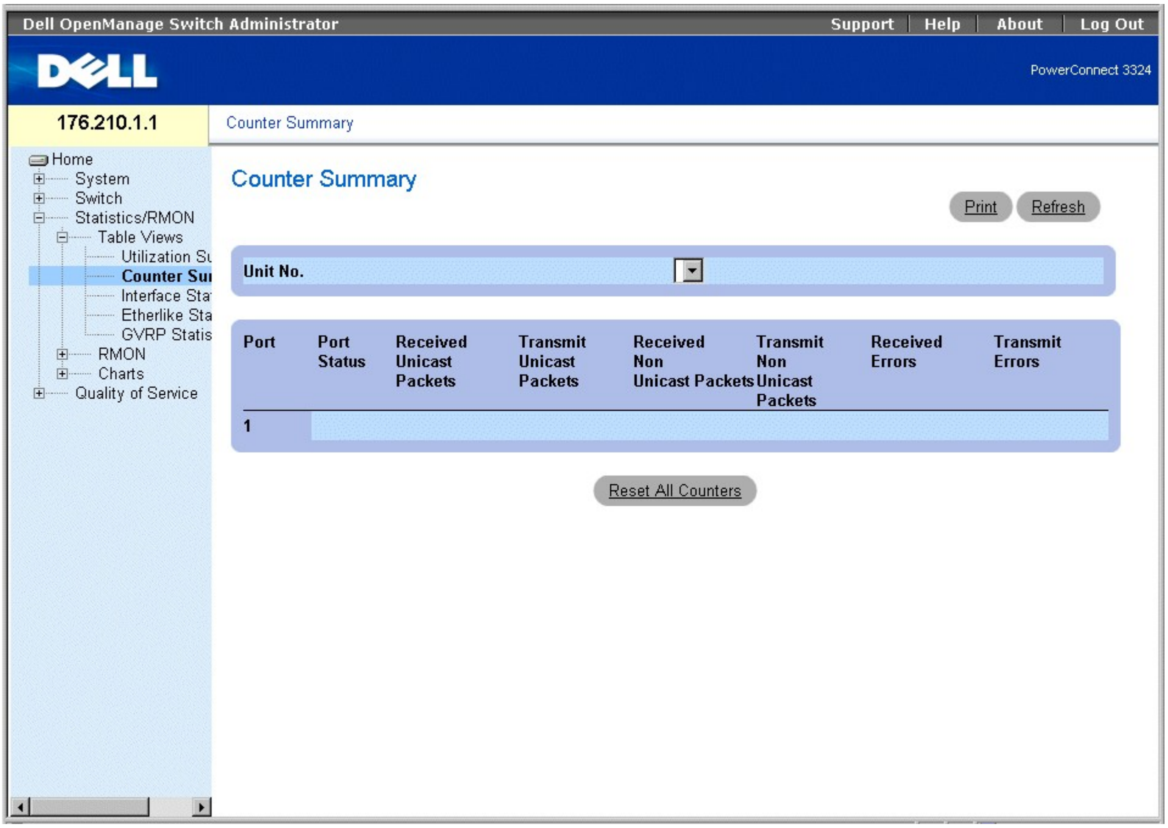
要查看使用统计数据，请：

1. 打开**"Utilization Summary"（使用摘要）**页面。
2. 在**"Unit"（装置）**字段中选择一个装置。 系统将显示选定装置的使用统计数据。

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）**。系统将打开 **“Counter Summary”（计数器摘要）**页面：



计数器摘要页面

“Counter Summary”（计数器摘要）页面包含以下字段：

- **“Unit No.”（装置号）** — 表示显示端口统计数据的装置号。
- **“Port”（端口）** — 表示端口号。
- **“Port Status”（端口状态）** — 表示端口的状态。
- **“Received Unicast Packets”（接收到的单点传送信息包）** — 表示端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）** — 表示从端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）** — 表示端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）** — 表示从端口发送的非单点传送信息包的数量。
- **“Received Errors”（接收到的错误）** — 表示端口上接收到的错误的数量。
- **“Transmit Errors”（发送的错误）** — 表示从端口发送的错误的数量。

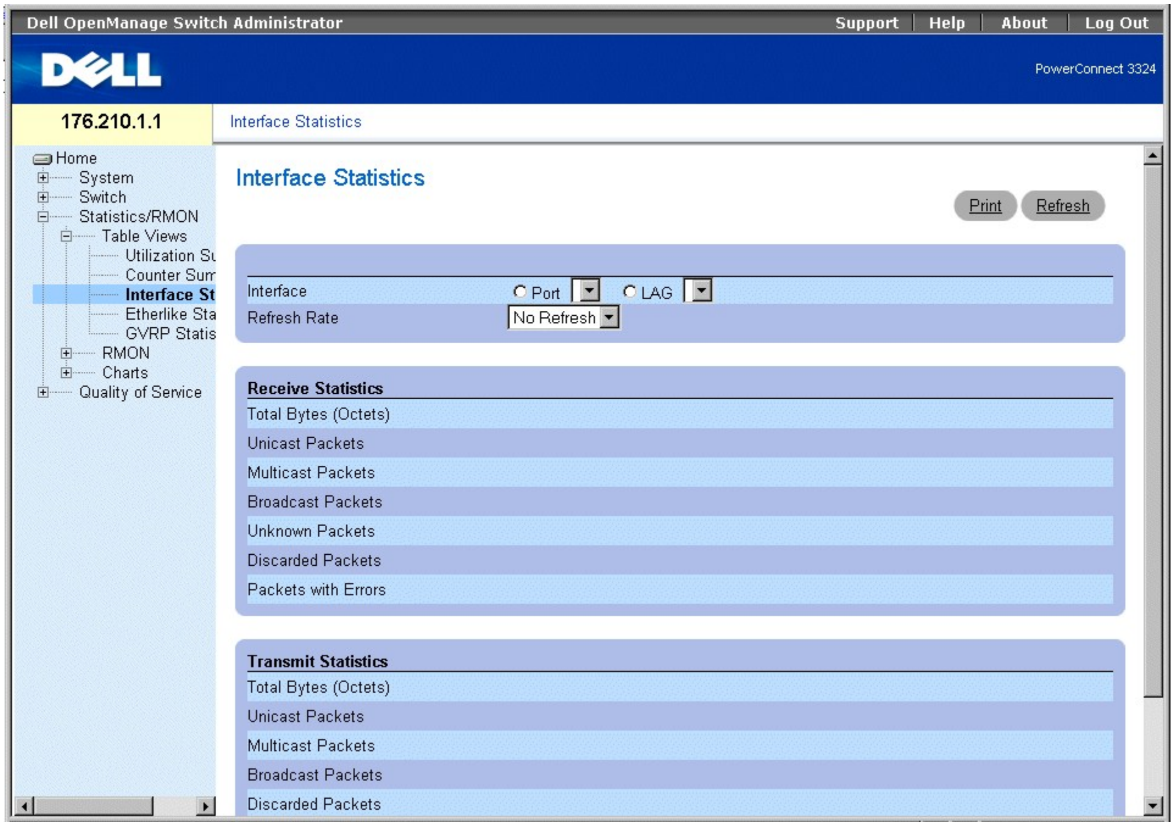
要查看计数器摘要统计数据，请：

1. 打开 **“Counter Summary”（计数器摘要）**页面。
2. 在 **“Unit”（装置）**字段中选择一个装置。 系统将显示选定装置的计数器摘要统计数据。

查看接口统计数据

"Interface Statistics"（接口统计数据）页面包含接口的统计数据。 要打开 **"Interface Statistics"（接口统计数据）**页面：

- 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）**。 系统将打开 **"Interface Statistics"（接口统计数据）**页面。



接口统计数据页面

I"Interface Statistics"（接口统计数据）页面包含以下字段：

- **"Interface"（接口）**— 指定要显示统计数据的接口（类型和编号）。
  - **"Port"（端口）**— 表示显示端口统计数据。
  - **"LAG"**— 表示显示 LAG 统计数据。
- **"Refresh Rate"（刷新率）**— 表示刷新接口统计数据之前经过的时间。 可能的字段值包括：
  - **"15 Sec"（15 秒）**— 表示接口统计数据每 15 秒钟刷新一次。
  - **"30 Sec"（30 秒）**— 表示接口统计数据每 30 秒钟刷新一次。
  - **"60 Sec"（60 秒）**— 表示接口统计数据每 60 秒钟刷新一次。
  - **"No Refresh"（不刷新）**— 表示不自动刷新接口统计数据。
- **"Total Bytes (Octets) Received"（接收到的字节 [八位位组] 总数）**— 显示选定接口上接收到的字节数。
- **"Received Unicast Packets"（接收到的单点传送信息包）**— 显示选定接口上接收到的单点传送信息包的数量。

- **“Received Multicast Packets”（接收到的多点传送信息包）**— 显示选定接口上接收到的多点传送信息包的数量。
- **“Received Broadcast Packets”（接收到的广播信息包）**— 显示选定接口上接收到的广播信息包的数量。
- **“Received Unknown Packets”（接收到的未知信息包）**— 显示选定接口上接收到的未知信息包的数量。
- **“Received Discarded Packets”（接收到的丢弃信息包）**— 显示选定接口在接收过程中丢弃的信息包的数量。
- **“Received Packets with Errors”（接收到的包含错误的信息包）**— 显示在选定接口上接收到的包含错误的信息包的数量。
- **“Total Bytes (Octets) Transmitted”（发送的字节 [八位位组] 总数）**— 显示从选定接口发送的字节数。
- **“Transmitted Unicast Packets”（发送的单点传送信息包）**— 显示从选定接口发送的单点传送信息包的数量。
- **“Transmitted Multicast Packets”（发送的多点传送信息包）**— 显示从选定接口发送的多点传送信息包的数量。
- **“Transmitted Broadcast Packets”（发送的广播信息包）**— 显示从选定接口发送的广播信息包的数量。
- **“Transmitted Unknown Packets”（发送的未知信息包）**— 显示从选定接口发送的未知信息包的数量。
- **“Transmitted Discarded Packets”（发送的丢弃信息包）**— 显示选定接口在发送过程中丢弃的信息包的数量。
- **“Transmitted Packets with Errors”（发送的包含错误的信息包）**— 显示在选定接口发送过程中发现的包含错误的信息包的数量。

要显示端口的接口统计数据，请：

1. 打开 **“Interface Statistics”（接口统计数据）**页面。
2. 在 **“Interface”（接口）**字段中选择 **“Port”（端口）**。
3. 单击 **“Reset All Counters”（重设所有计数器）**。 系统将显示端口的接口统计数据。

要显示 LAG 的接口统计数据，请：

1. 打开 **“Interface Statistics”（接口统计数据）**页面。
2. 在 **“Interface”（接口）**字段中选择 **“LAG”**。
3. 单击 **“Reset All Counters”（重设所有计数器）**。 系统将显示 LAG 的接口统计数据。

使用 CLI 命令查看接口统计数据

本节包含用于查看接口统计数据的 CLI 命令。

CLI 命令	说明
show interfaces counters [ethernet *interface* | port-channel *port-channel-number*]	显示经由物理接口的通信。

以下是 CLI 命令实例：

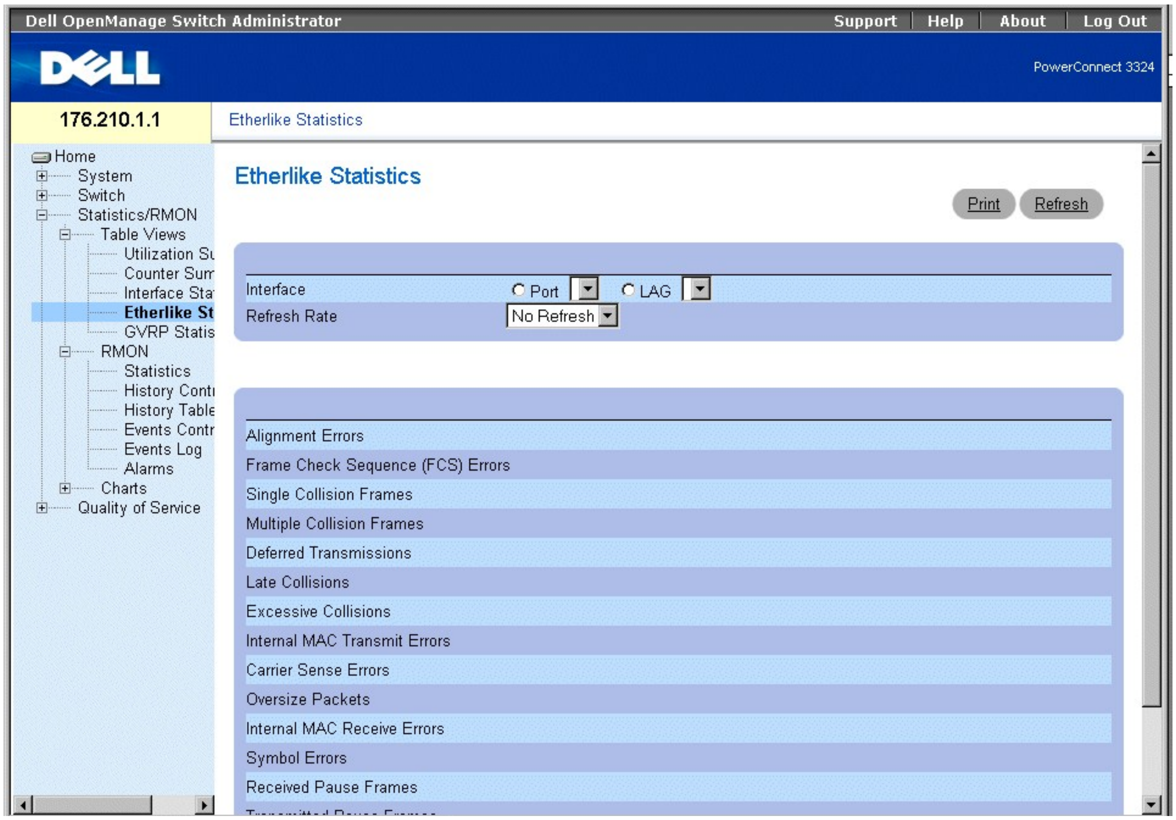
```
console# show interfaces counters ethernet 1/e1

Port InOctets InUcastPkts InMcastPkts InBcastPkts

---- ---------- ----------- ----------- -----------
```

```
1/e1 1717 0 326 26

Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts
--- ---------- ------------ ------------ ------------
1/e1 21845 0 326 26

Alignment Errors: 0
FCS Errors: 0
Single Collision Frames: 0
Multiple Collision Frames: 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
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 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）**。 系统将打开**"Etherlike Statistics"（以太网类统计数据）**页面。



以太网类统计数据页面

"Etherlike Statistics"（以太网类统计数据）页面包含以下字段：

- **"Interface"（接口）**— 指定要显示统计数据的接口类型。
  - **"Port"（端口）**— 表示显示端口统计数据。
  - **"LAG"**— 表示显示 LAG 统计数据。
- **"Refresh Rate"（刷新率）**— 表示刷新接口统计数据之前经过的时间。可能的字段值包括：
  - **"15 Sec"（15 秒）**— 表示以太网类统计数据每 15 秒钟刷新一次。
  - **"30 Sec"（30 秒）**— 表示以太网类统计数据每 30 秒钟刷新一次。
  - **"60 Sec"（60 秒）**— 表示以太网类统计数据每 60 秒钟刷新一次。
  - **"No Refresh"（不刷新）**— 表示不自动刷新以太网类统计数据。
- **"Alignment Errors"（校准错误）**— 显示选定接口上接收到的校准错误的数量。

- **"Frame Check Sequence (FCS) Errors"（帧检查顺序 [FCS] 错误）**— 显示选定接口上接收到的帧检查顺序错误的数量。
- **"Single Collision Frames"（单冲突帧）**— 显示选定接口上接收到的单冲突帧错误的数量。
- **"Multiple Collision Frames"（多冲突帧）**— 显示选定接口上接收到的多冲突帧错误的数量。
- **"Deferred Transmissions"（延迟的传输）**— 显示选定接口上延迟传输的数量。
- **"Late Collision"（推迟冲突）**— 显示选定接口上接收到的推迟冲突的数量。
- **"Excessive Collisions"（严重冲突）**— 显示选定接口上接收到的严重冲突的数量。
- **"Internal MAC Transmit Errors"（内部 MAC 发送错误）**— 显示选定接口上内部 MAC 发送错误的数量。
- **"Carrier Sense Errors"（载波侦听错误）**— 显示选定接口上载波侦听错误的数量。
- **"Oversize Packets"（超大信息包）**— 显示选定接口上过长帧错误的数量。
- **"Internal MAC Receive Errors"（内部 MAC 接收错误）**— 显示选定接口上内部 MAC 接收错误的数量。
- **"Symbol Errors"（符号错误）**— 显示选定接口上符号错误的数量。
- **"Received Pause Frames"（接收到的暂停帧）**— 显示选定接口 (IEEE 802.3X) 上接收到的暂停帧的数量。
- **"Transmitted Pause Frames"（发送的暂停帧）**— 显示选定接口 (IEEE 802.3X) 上发送的暂停帧的数量。

要显示端口的以太网类统计数据，请：

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**"Port"（端口）**。
3. 单击**"Query"（查询）**。系统将显示端口的以太网类统计数据。

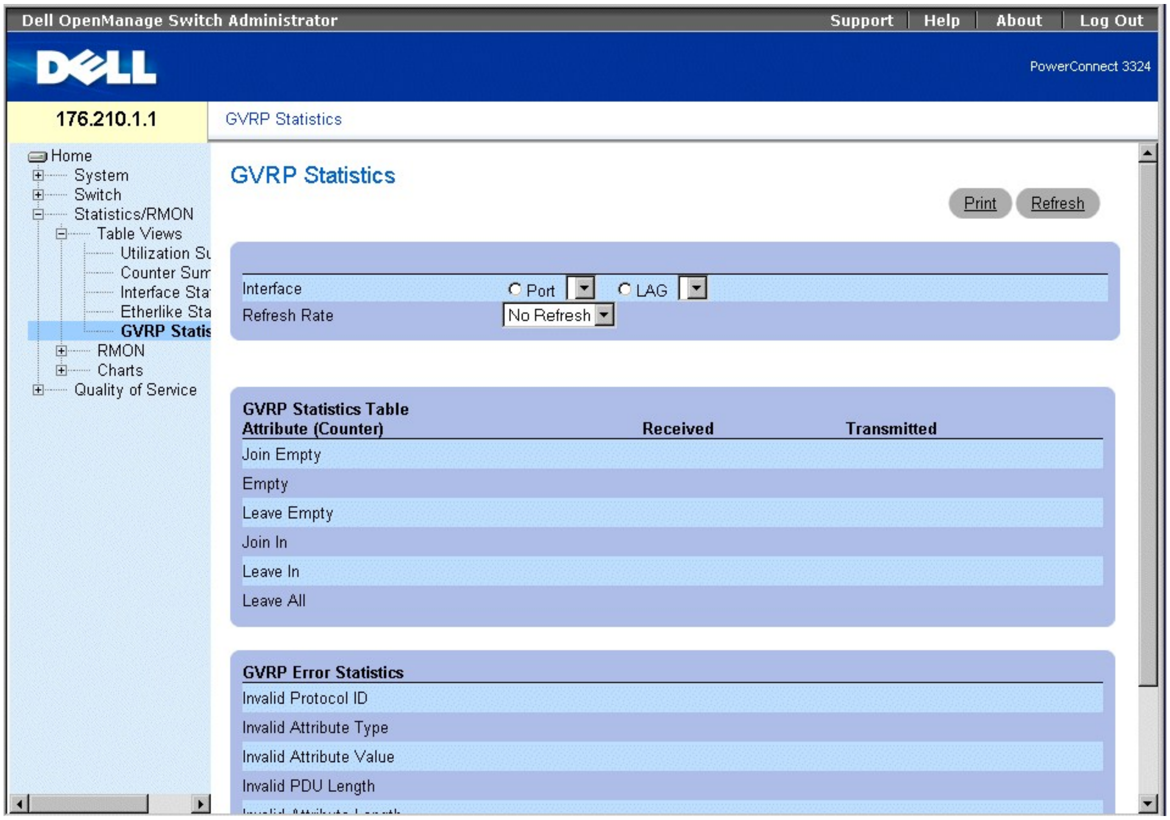
要显示 LAG 的以太网类统计数据，请：

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**"LAG"**。
3. 单击**"Query"（查询）**。系统将显示 LAG 的以太网类统计数据。

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**"GVRP Statistics"（GVRP 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）**>**"GVRP"**。系统将打开**"GVRP Statistics"（GVRP 统计数据）**页面：



GVRP 统计数据页面

"GVRP Statistics"（GVRP 统计数据）页面包含以下字段：

- **"Interface"（接口）**— 指定要显示统计数据的接口类型。
  - **"Port"（端口）**— 表示显示端口统计数据。
  - **"LAG"**— 表示显示 LAG 统计数据。
- **"Refresh Rate"（刷新率）**— 表示刷新 GVRP 统计数据之前经过的时间。
  可能的字段值包括：
  - **"15 Sec"（15 秒）**— 表示 GVRP 统计数据每 15 秒钟刷新一次。
  - **"30 Sec"（30 秒）**— 表示 GVRP 统计数据每 30 秒钟刷新一次。
  - **"60 Sec"（60 秒）**— 表示 GVRP 统计数据每 60 秒钟刷新一次。
  - **"No Refresh"（不刷新）**— 表示不自动刷新 GVRP 统计数据。
- **"Join Empty"（加入空）**— 显示设备的 GVRP 加入空统计数据。
- **"Empty"（空）**— 显示设备的 GVRP 空统计数据。
- **"Leave Empty"（保留空）**— 显示设备的 GVRP 保留空统计数据。
- **"Join In"（加入）**— 显示设备的 GVRP 加入统计数据。
- **"Leave In"（保留）**— 显示设备的 GVRP 保留统计数据。
- **"Invalid Protocol ID"（无效协议 ID）**— 显示设备的 GVRP 无效协议 ID 统计数据。
- **"Invalid Attribute Type"（无效属性类型）**— 显示设备的 GVRP 无效属性 ID 统计数据。
- **"Invalid Attribute Value"（无效属性值）**— 显示设备的 GVRP 无效属性值统计数据。
- **"Invalid PDU Length"（无效 PDU 长度）**— 显示设备的 GVRP 无效 PDU 长度统计数据。

- **"Invalid Attribute Length"（无效属性长度）**— 显示设备的 GVRP 无效属性长度统计数据。
- **"Invalid Events"（无效事件）**— 显示设备的 GVRP 无效事件统计数据。

要显示端口的 GVRP 统计数据，请：

1. 打开 **"GVRP Statistics"（GVRP 统计数据）**页面。
2. 在 **"Interface"（接口）**字段中选择 **"Port"（端口）**。
3. 单击 **"Query"（查询）**。 系统将显示端口的 GVRP 统计数据。

要显示 LAG 的 GVRP 统计数据，请：

1. 打开 **"GVRP Statistics"（GVRP 统计数据）**页面。
2. 在 **"Interface"（接口）**字段中选择 **"LAG"**。
3. 单击 **"Query"（查询）**。 系统将显示 LAG GVRP 统计数据。

使用 CLI 命令查看 GVRP 统计数据

有关以每个端口为基础查看 GVRP 说明的信息，请参阅 **"Port Statistics"（端口统计数据）**页面。 下表说明了 CLI 命令。

CLI 命令	**说明**
show gvrp statistics [**ethernet** 接口 | **port-channel** 端口通道号]	显示 GVRP 统计数据。
show gvrp error-statistics [**ethernet** *接口*| **port-channel** *端口通道号*]	显示 GVRP 错误统计数据。

以下是 CLI 命令的实例：

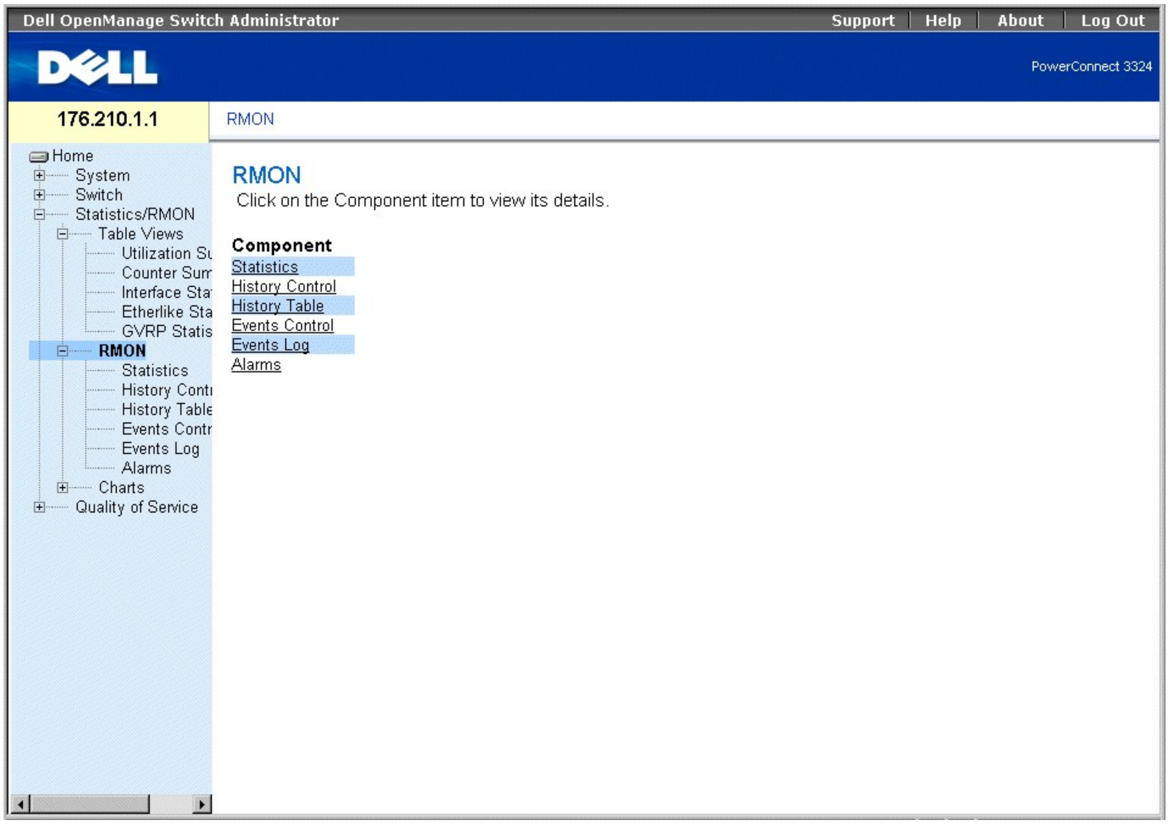
```
Console# show gvrp statistics



GVRP statistics:

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

Legend:

rJE: Join Empty Received . : 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 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 RMON 信息

远程监测 (RMON) 使网络管理员可以从远程位置查看网络通信量信息。 要打开**“RMON”**页面，请：

- 在树视图中单击**“Statistics/RMON”**（**统计数据/RMON**）>**“RMON”**。
  系统将打开**“RMON”**页面。



RMON 页面

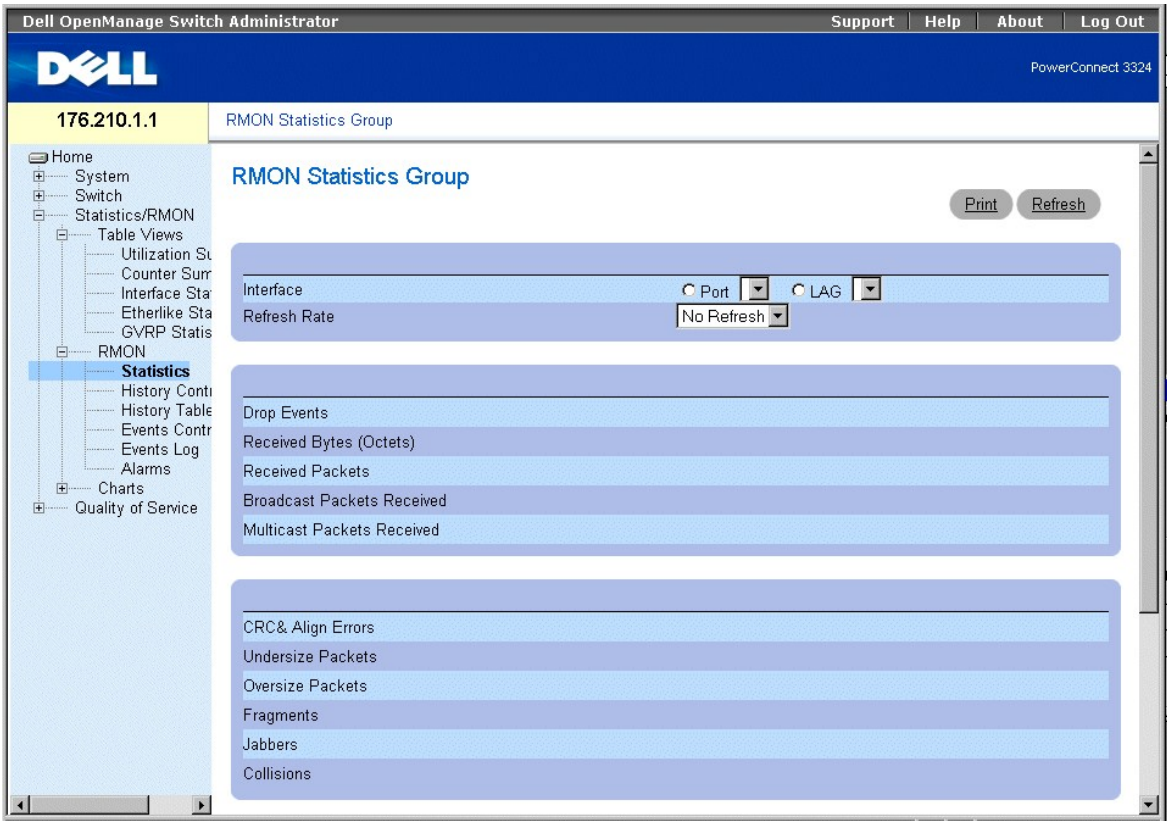
本节包含以下主题：

- 查看 RMON 统计数据
- 查看历史记录控制统计数据
- 查看 RMON 历史记录表
- 定义设备事件
- 查看事件日志
- 定义设备警报

查看 RMON 统计数据

"RMON Statistics Group"（RMON 统计数据组）页面使网络管理员可以显示接口的 RMON 统计数据。 接口统计数据提供了有关设备使用以及设备上出现的错误的信息。 要打开**"RMON Statistics Group"（RMON 统计数据组）**页面，请：

- 在树视图中单击**"Statistics/RMON"（统计数据/RMON）>"RMON">"Statistics"（统计数据）**。 系统将打开**"RMON Statistics Group"（RMON 统计数据组）**页面。



RMON 统计数据组页面

"RMON Statistics Group"（RMON 统计数据组）页面包含以下信息：

- **"Interface"（接口）**— 表示要显示统计数据的接口类型和编号。 可能的字段值包括：
  - **"Port"（端口）**— 表示显示端口的特定统计数据。
  - **"LAG"**— 表示显示 LAG 的特定统计数据。
- **"Refresh Rate"（刷新率）**— 表示刷新 RMON 统计数据之前经过的时间。
  可能的字段值包括：
  - **"15 Sec"（15 秒）**— 表示 RMON 统计数据每 15 秒钟刷新一次。
  - **"30 Sec"（30 秒）**— 表示 RMON 统计数据每 30 秒钟刷新一次。
  - **"60 Sec"（60 秒）**— 表示 RMON 统计数据每 60 秒钟刷新一次。
  - **"No Refresh"（不刷新）**— 表示不自动刷新 RMON 统计数据。
- **"Drop Events"（丢弃事件）**— 表示自上一次清除计数器以来接口上发生的丢弃事件的数量。
- **"Received Octets"（接收到的八位位组）**— 表示自上一次清除计数器以来接口上接收到的八位位组的数量。
- **"Received Packets"（接收到的信息包）**— 表示自上一次清除计数器以来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）**— 表示自上一次清除计数器以来接口上接收到的广播信息包的数量。
- **"Multicast Packets Received"（接收到的多点传送信息包）**— 表示自上一次清除计数器以来接口上接收到的多点传送信息包的数量。
- **"CRC& Align Errors"（CRC 和校准错误）**— 表示自上一次清除计数器以来接口上发生的 CRC 和校准错误的数量。
- **"Undersize Packets"（超小信息包）**— 表示自上一次清除计数器以来接口上接收到的超小信息包的数量。
- **"Oversize Packets"（超大信息包）**— 表示自上一次清除计数器以来接口上接收到的超大信息包的数量。
- **"Fragments"（碎片）**— 表示自上一次清除计数器以来接口上接收到的碎片的数量。

- **"Jabbers"（无用信息）**— 表示自上一次清除计数器以来接口上接收到的无用信息的数量。
- **"Collisions"（冲突）**— 表示自上一次清除计数器以来接口上接收到的冲突的数量。
- **"Frames of 64 Bytes"（64 字节的帧）**— 表示自上一次清除计数器以来接口上接收到的 64 字节信息包的数量。
- **"Frames of 65-127 Bytes"（65 至 127 字节的帧）**— 表示自上一次清除计数器以来接口上接收到的 65 至 127 字节的信息包的数量。
- **"Frames of 128-255 Bytes"（128 至 255 字节的帧）**— 表示自上一次清除计数器以来接口上接收到的 128 至 255 字节的信息包的数量。
- **"Frames of 256-511 Bytes"（256 至 511 字节的帧）**— 表示自上一次清除计数器以来接口上接收到的 256 至 511 字节的信息包的数量。
- **"Frames of 512-1023 Bytes"（512 至 1023 字节的帧）**— 表示自上一次清除计数器以来接口上接收到的 512 至 1023 字节的信息包的数量。
- **"Frames of 1024-1518 Bytes"（1024 至 1518 字节的帧）**— 表示自上一次清除计数器以来接口上接收到的 1024 至 1518 字节的信息包的数量。

要查看接口统计数据，请：

1. 打开**"RMON Statistics Group"（RMON 统计数据组）**页面。
2. 在**"Interface"（接口）**字段中选择接口类型和编号。 在**"RMON Statistics"（RMON 统计数据）**区段中将显示接口统计数据。

使用 CLI 命令查看 RMON 统计数据

下表概括了用于查看**"RMON Statistics Group"（RMON 统计数据组）**页面中显示的字段的等效 CLI 命令。

CLI 命令	说明
show rmon statistics [**ethernet** 接口 | **port-channel** 端口通道号]	显示 RMON 以太网统计数据。

以下是 CLI 命令的示例：

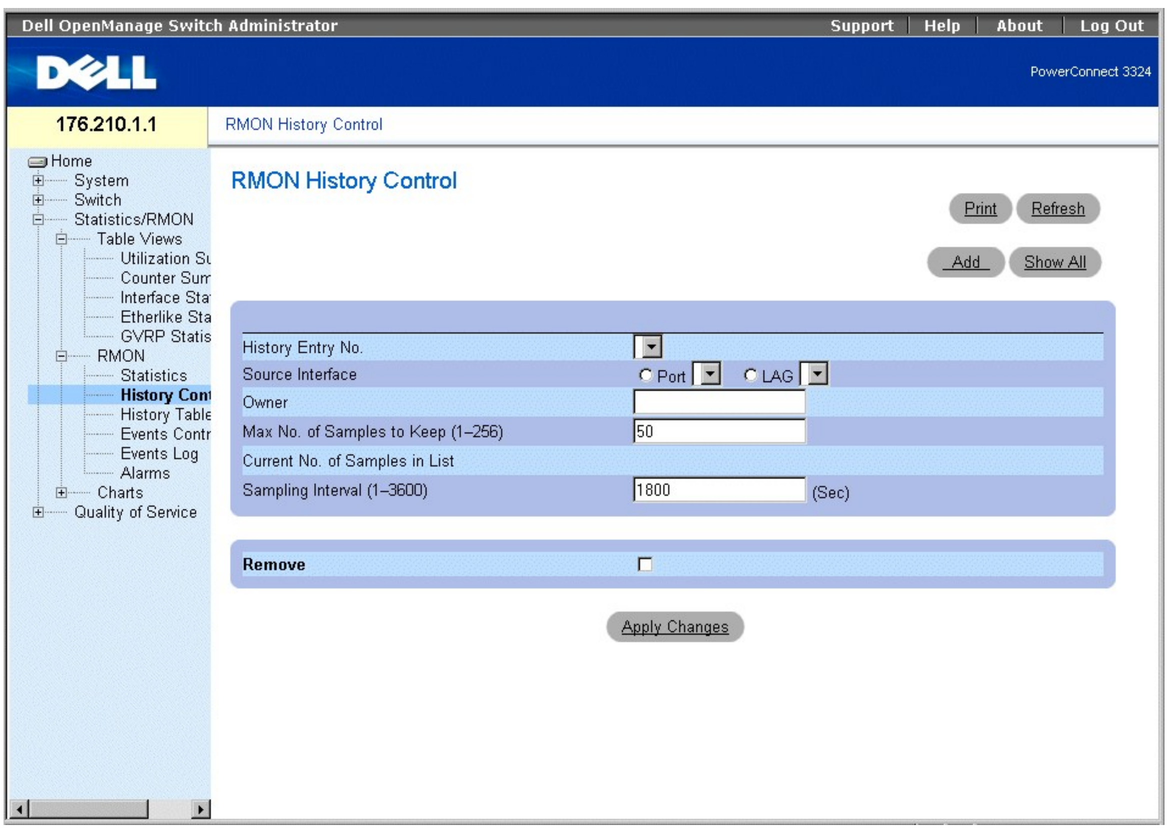
```
Console# show rmon statistics ethernet 1/e1

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
```

查看历史记录控制统计数据

"RMON History Control"（RMON 历史记录控制）页面包含有关从端口获取的 RMON 数据样例的信息。 **"RMON History Control"（RMON 历史记录控制）**页面用于控制这些样例的收集。

- 在树视图中单击**"Statistics/RMON"（统计数据/RMON）> "History Control"（历史记录控制）**。 系统将打开**"History Control"（历史记录控制）**页面。



RMON 历史记录控制页面

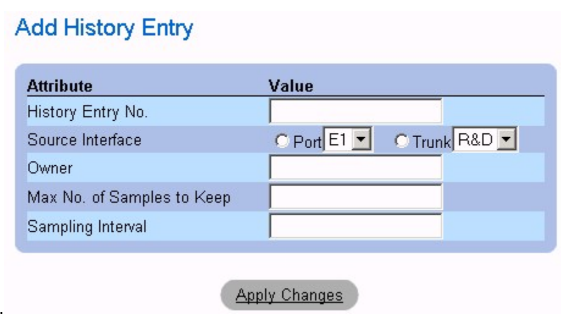
"History Control"（历史记录控制）页面包含以下信息：

- **"History Entry No."（历史记录条目号）** — 指定**"History Control Table"（历史记录控制表）**条目。

- **“Source Interface”（源接口）** — 表示获取历史记录样例的源。 可能的字段值包括：
  - **“Port”（端口）** — 表示从端口获取历史记录样例。
  - **“LAG”**— 表示从 LAG 获取历史记录样例。
- **“Owner”（所有者）** — 表示请求 RMON 信息的 RMON 站点或用户。
- **“Max Number of Samples to Keep”（要保留的最大样例数）** — 表示要保存的样例的数量。 默认值为**50**。
- **“Current Number of Samples”（当前样例数）** — 表示当前获取的样例的数量。
- **“Sampling Interval”（取样间隔）** — 表示从端口取样的时间（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）** — 删除**“History Control Table”（历史记录控制表）**条目。
  - **已选取** — 删除**“History Control Table”（历史记录控制表）**条目。
  - **未选取** — 保留**“History Control Table”（历史记录控制表）**条目。

要添加历史记录控制条目，请：

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。



.

添加历史记录条目

3. 定义**“History Entry No.”（历史记录条目号）**、**“Source Interface”（源接口）**、**“Owner”（所有者）**、**“Max No. of Samples to Keep”（要保留的最大样例数）**
   和**“Sampling Interval”（取样间隔）**字段。
4. 单击**“Apply Changes”（应用更改）**。 系统将添加**“History Control Entry”**
   （历史记录控制条目）。

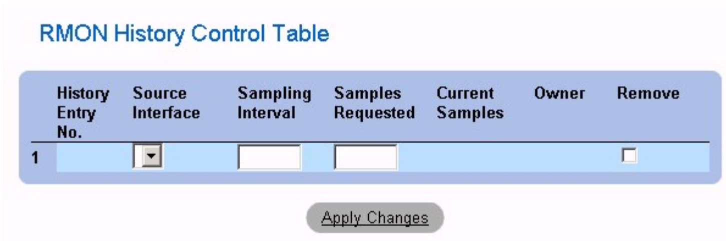
要修改历史记录控制表条目，请：

1. 打开**“RMON History Control”（RMON 历史记录控制）**页面。
2. 在**“History Index”（历史记录索引）**字段中选择**“RMON History Control Table”（RMON 历史记录控制表）**条目。
3. 修改**“Source Interface”（源接口）**、**“Owner”（所有者）**、**“Max Number of Samples to Keep”（要保留的最大样例数）**、**“Number of Current Samples”**
   （当前样例数）和/或**“Sampling Interval”（取样间隔）**字段。
4. 单击**“Apply Changes”（应用更改）**。 系统将修改**“RMON History Control Table”（RMON 历史记录控制表）**条目，并更新设备。

要显示历史记录控制表，请：

1. 打开**“RMON History Control”（RMON 历史记录控制）**页面。

2. 单击**“Show All”（全部显示）**。 系统将打开**“History Control Table”（历史记录控制表）**。



历史记录控制表

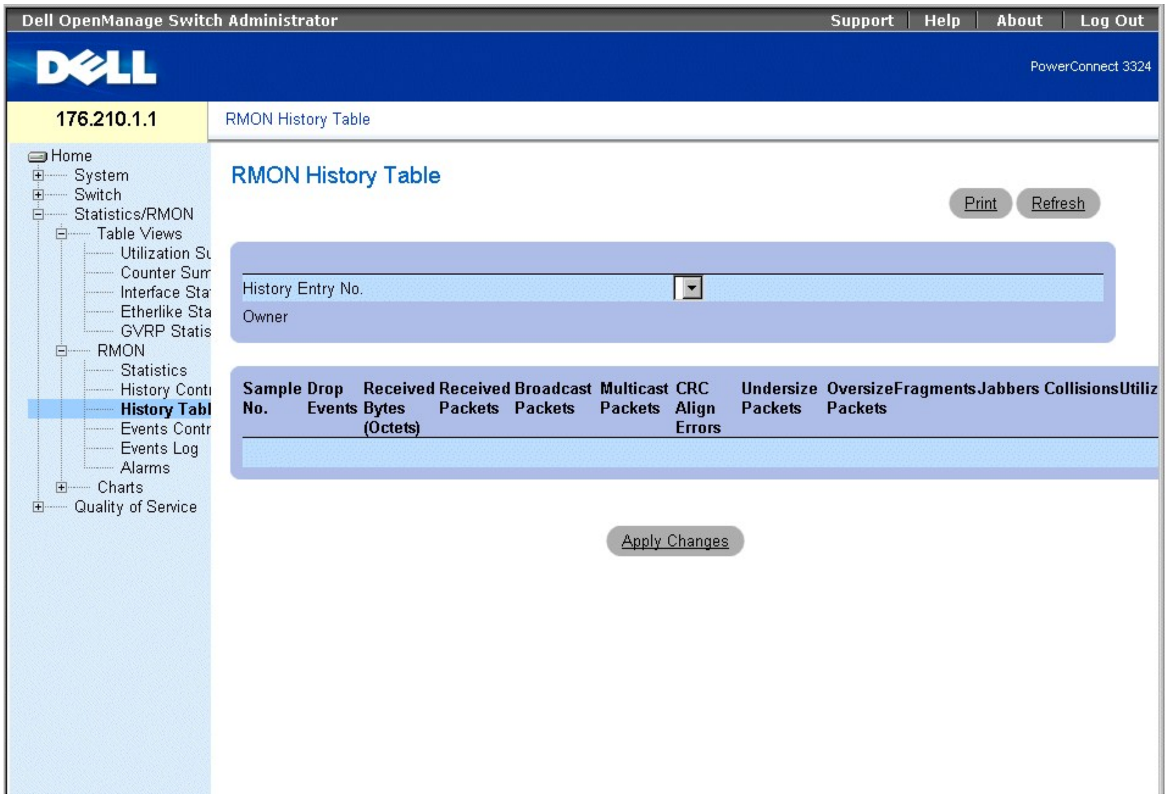
要删除历史记录控制表条目，请：

1. 打开**“RMON History Control”（RMON 历史记录控制）**页面。
2. 在**“History Index”（历史记录索引）**字段选择**“History Control Table”（历史记录控制表）**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**“RMON History Control Table”（RMON 历史记录控制表）**条目，并更新设备。

查看 RMON 历史记录表

“RMON History Table”（RMON 历史记录表）包含特定接口的 RMON 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”（RMON 历史记录）>“History Table”（历史记录表）**。



RMON 历史记录表

注： 并非所有字段都显示在 RMON 历史记录表中。

"RMON History Table"（RMON 历史记录表）包含以下字段：

- **"Sample No."（样例号）**— 表示表中信息反映的特定样例。
- **"Drop Events"（丢弃事件）**— 表示在取样间隔期间由于缺少网络资源而导致的被丢弃信息包的数量。 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]）**— 表示在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）**— 表示在取样间隔期间接收到的信息包的数量。
- **"Broadcast Packets"（广播信息包）**— 表示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）**— 表示在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）**— 表示在取样会话过程中接收到的长度为 64 至 1518 个八位位组、包含整数个或非整数个八位位组的坏帧检查顺序 (FCS) 的信息包的数量。
- **"Undersized Packets"（超小信息包）**— 表示在取样会话过程中接收到的长度小于 64 个八位位组的信息包的数量。
- **"Oversized Packets"（超大信息包）**— 表示在取样会话过程中接收到的长度大于 1518 个八位位组的信息包的数量。
- **"Fragments"（碎片）**— 表示在取样会话过程中接收到的长度小于 64 个八位位组并带有 FCS 的信息包的数量。
- **"Jabbers"（无用信息）**— 表示在取样会话过程中接收到的长度大于 1518 个八位位组并带有 FCS 的信息包的数量。
- **"Collisions"（冲突）**— 估计在取样会话过程中发生冲突的信息包的总数。 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）**— 估计在取样会话过程中接口上的主物理层网络说明。 此值用带两个小数位的百分比表示。

要查看特定历史记录条目的统计数据，请：

1. 打开**“RMON History Table”**（**RMON 历史记录表**）页面。

2. 在**“History Table No.”**（**历史记录表编号**）字段中选择一个历史记录条目。
   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 历史记录统计数据

下表包含用于查看 RMON 历史记录统计数据的 CLI 命令。

CLI 命令	**说明**
rmon table-size history 条目	配置历史记录表条目的最大数量。
rmon collection history 索引 [owner 所有者名称] [**buckets** 存储区号] [**interval** 秒]	允许在接口上远程监测 (RMON) MIB 历史记录统计数据组。
show rmon history 索引 {**throughput** | **errors** | **other**} [**period** *hh:mm:ss*]	显示 RMON 以太网统计数据历史记录。

以下是 CLI 命令实例：

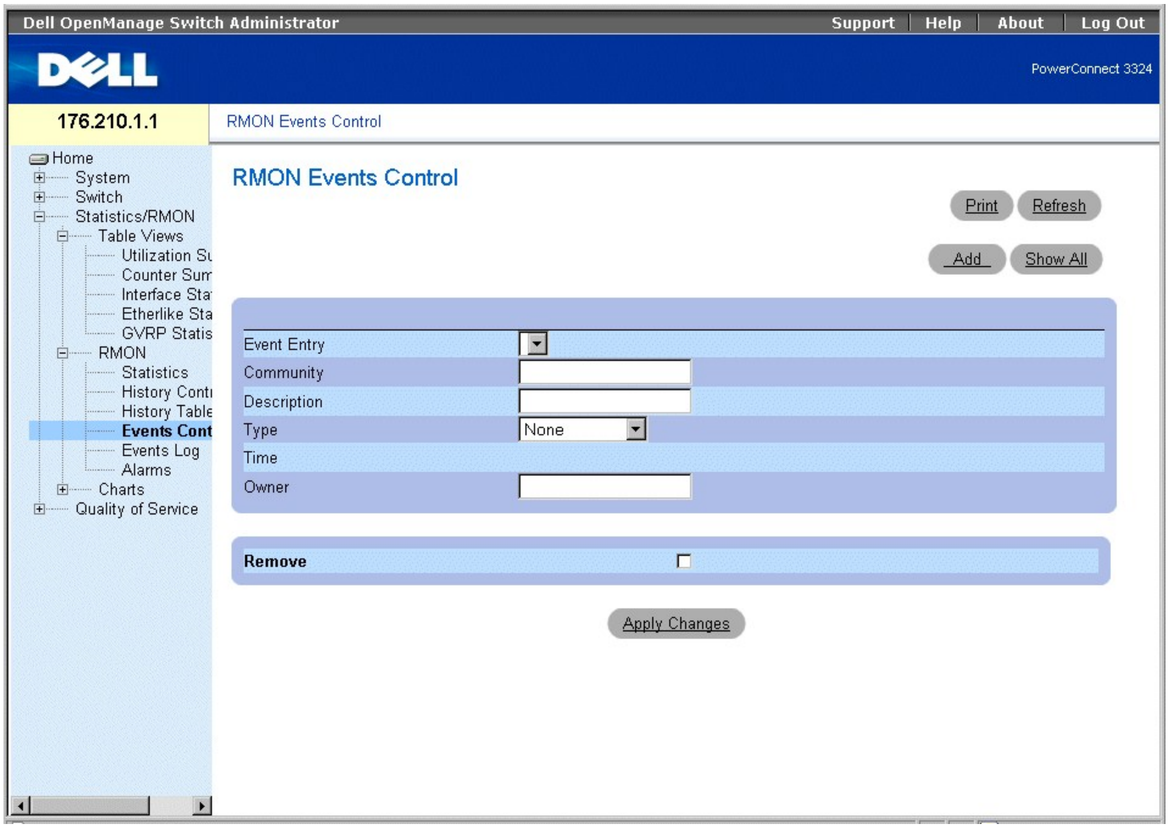
```
Console (config)# rmon table-size history 1000

Console (config)# interface ethernet 1/e8

Console (config-if)# rmon collection history 1 interval 2400

Console# show rmon history 1 throughput

Sample set: 1 Owner: CLI

Interface: 1/e1 Interval: 1800

Requested samples: 50 Granted samples: 50



Maximum table size: 500



Day: Jan 18 2002

Time Octets Packets Broadcast Multicast Utilization

-------- ------- ------- --------- --------- ----------
```

```
23:58:30 878128 878 7 1 20.87%

23:59:00 75898768 91892 932 1723 19.27%

23:59:30 171797536 193784 1817 3289 19.82%


Day: Jan 19 2002

Time Octets Packets Broadcast Multicast Utilization

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

00:00:00 287696304 275686 2789 5878 20.17%

00:00:30 303595962 357568 3289 7287 19.98%
```

定义设备事件

"RMON Events Control"（RMON 事件控制）页面使网络管理员可以查看 RMON 事件。 可以通过**"RMON Events Control"（RMON 事件控制）**表打开 **"RMON Events"（RMON 事件）**表。 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"（事件）**。 系统将打开**"RMON Events Control"（RMON 事件控制）**页面。



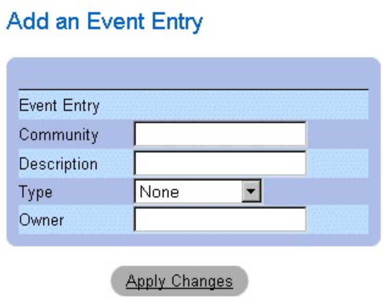
RMON 事件控制页面

"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）** — 指定事件所属的 SNMP 团体。
- **"Description"（说明）** — 提供用户定义的事件说明。
- **"Type"（类型）** — 说明事件的类型。 可能的字段值包括：
  - **"Log"（日志）** — 表示事件类型为日志条目。
  - **"Trap"（陷阱）** — 表示事件类型为陷阱。
  - **"Log** and **Trap"（日志和陷阱）** — 表示事件类型既是日志条目，又是陷阱。
- **"Time"（时间）** — 表示事件发生的时间。
- **"Owner"（所有者）** — 表示定义事件的设备或用户。
- **"Remove"（删除）** — 从 **"Events Table"（事件表）**中删除事件。
  - **已选取** — 从 **"Events Table"（事件表）**中删除事件。
  - **未选取** — 保留 **"Events Table"（事件表）**中的事件。

要添加 RMON 事件，请：

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 New RMON Event"（添加新 RMON 事件）**页面。



添加新 RMON 事件

3. 定义 **“New Event Index”（新事件索引）**、**“Community”（团体）**、**“Description”（说明）**、**“Type”（类型）**和 **“Owner”（所有者）**字段。

4. 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。

要修改 RMON 事件，请：

1. 打开 **“RMON Events Control”（RMON 事件控制）**页面。

2. 在 **“Event Entry‟（事件条目）**字段中选择一个 **“Event Table”（事件表）**条目。

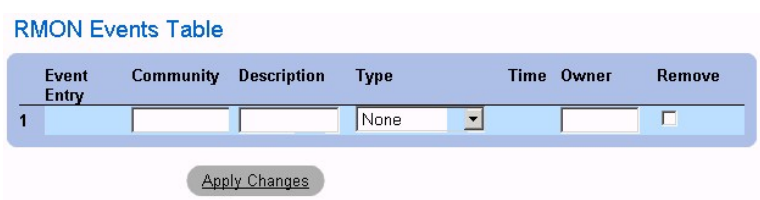
3. 修改 **“Community”（团体）**、**“Description”（说明）**、**“Type”（类型）**和/或 **“Owner”（所有者）**字段。

4. 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。

要显示 RMON 事件表，请：

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 **“Event Table”（事件表）**。



RMON 事件表

要删除多个 RMON 事件条目，请：

1. 打开 **“RMON Events Control”（RMON 事件控制）**页面。

2. 在 **“Event Index‟（事件索引）**字段中选择一个 **“Event Table”（事件表）**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 **“Event Table”（事件表）**条目，并更新设备。

注： 使用 **“Remove”（删除）**复选框，可以从 **“RMON Events”（RMON 事件）**页面中删除单个 **“Event”（事件）**条目。

使用 CLI 命令定义和显示 RMON 事件控制

下表概括了用于配置和显示**"RMON Events Control"**（**RMON 事件控制**）页面中的字段的等效 CLI 命令。

CLI 命令	**说明**
rmon event 索引类型[**community** 文本] [**description** 文本] [所有者名称]	配置 RMON 事件。
show rmon events	显示 RMON 事件表。

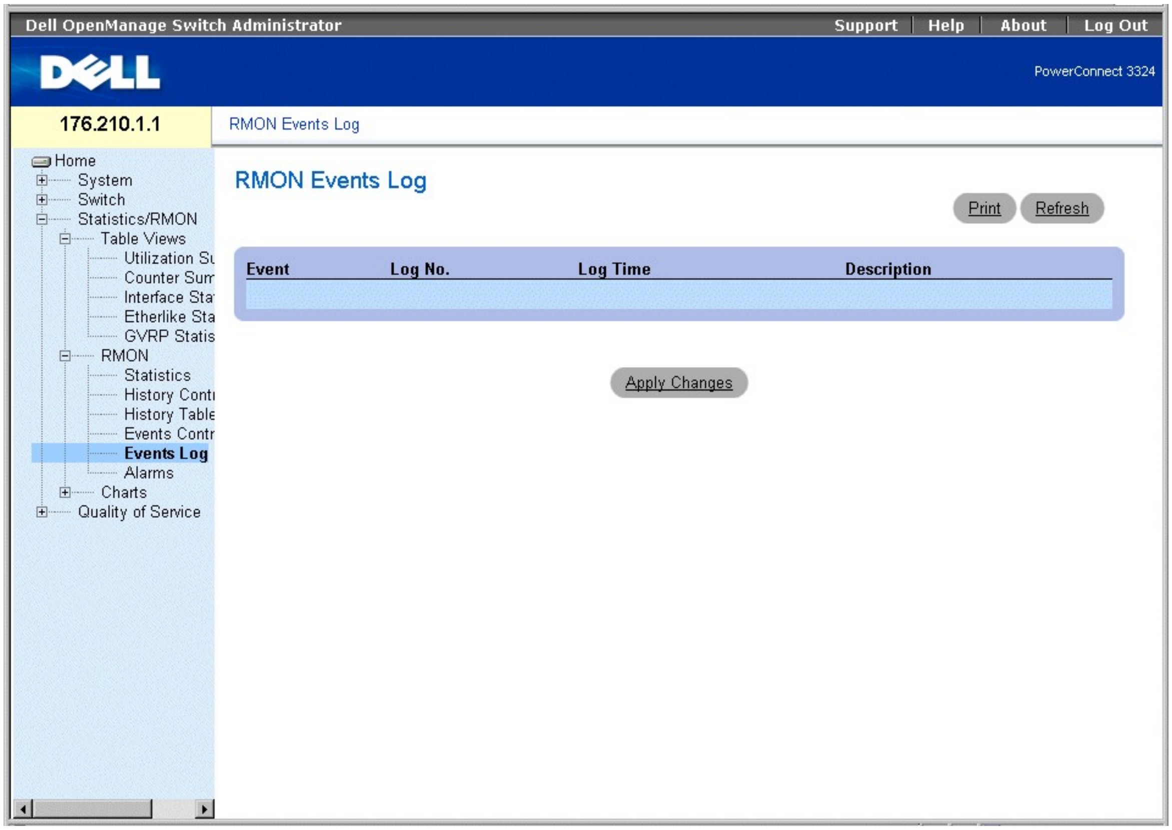
以下是 CLI 命令实例：

```
Console (config)# rmon event 10 log

Config (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 device Manager Jan 18 2002 23:59:48
```

查看事件日志

"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**），请：

- 在树视图中单击**"Statistics/RMON"**（**统计数据/RMON**）>**"RMON"**>**"Events"**（**事件**）。 系统将打开**"RMON Events Log"**（**RMON 事件日志**）页面。



RMON 事件日志页面

"RMON Events Log"（RMON 事件日志）页面包含以下字段：

- **"Event"（事件）**— 标识**"RMON Events Log"（RMON 事件日志）**条目号。
- **"Log No"（日志号）**— 表示日志编号。
- **"Log Time"（日志时间）**— 指定输入日志条目的时间。
- **"Description"（说明）**— 说明日志条目。

使用 CLI 命令查看 RMON 事件日志

下表概括了用于查看**"RMON Events Log"（RMON 事件日志）**页面中显示的字段的等效 CLI 命令。

CLI 命令	说明
rmon table-size log 条目	配置日志表条目的最大数量。
show rmon log [事件]	显示 RMON 记录表。

以下是 CLI 命令实例：

```
Console (config)# rmon table-size log 500
```

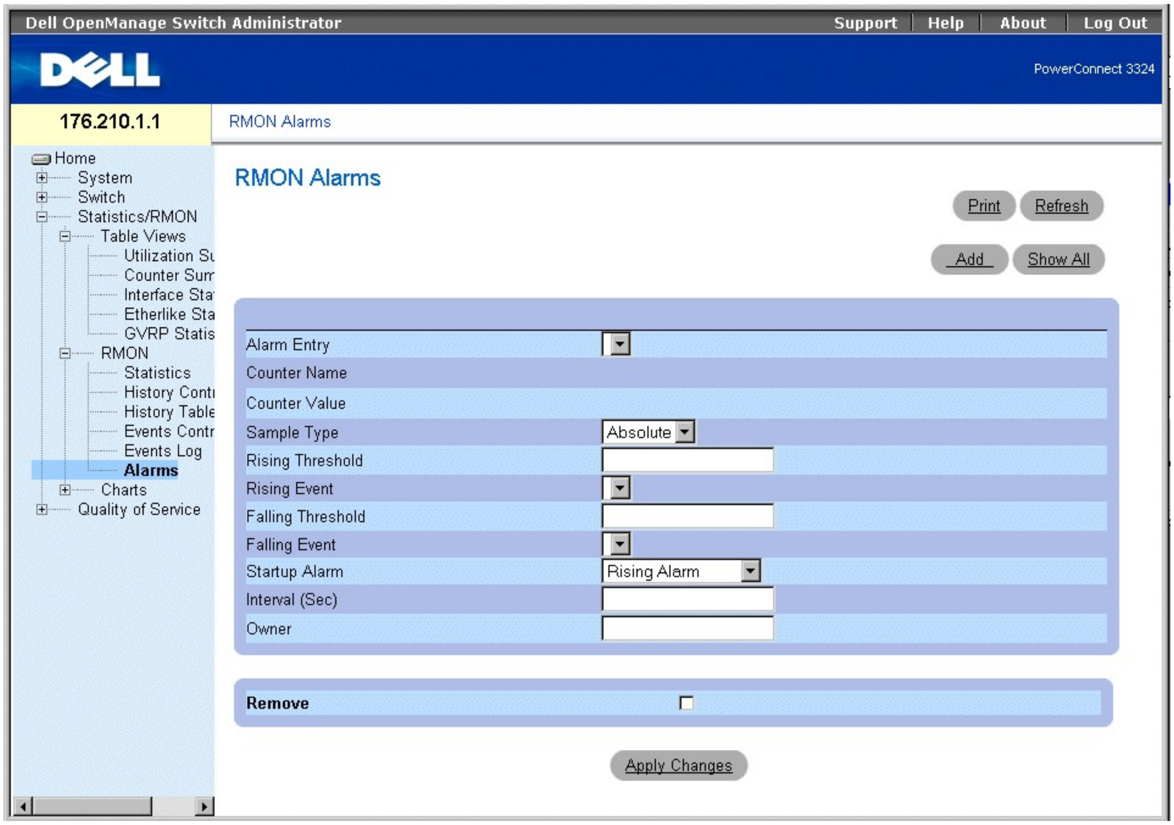
```
Console# show rmon log

Maximum table size: 500

Event Description Time

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

1 Errors Jan 18 2002 23:48:19

1 Errors Jan 18 2002 23:58:17

2 High Broadcast Jan 18 2002 23:59:48
```

```
Console# show rmon log

Maximum table size: 500 (800 after reset)

Event Description Time

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

1 Errors Jan 18 2002 23:48:19

1 Errors Jan 18 2002 23:58:17

2 High Broadcast Jan 18 2002 23:59:48
```

定义设备警报

"RMON Alarm"（RMON 警报）页面使网络管理员可以设置网络警报。 当系统检测到网络问题时就会发出网络警报。 阈值上升和下降也会生成警报。 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）**。 系统将打开**"RMON Alarm"（RMON 警报）**页面。



RMON 警报页面

"RMON Alarm"（RMON 警报）页面包含以下字段：

- **"Alarm Entry"（警报条目）** — 表示特定的警报。
- **"Counter Name"（计数器名称）** — 表示选定的 RMON 计数器。
- **"Counter Value"（计数器值）** — 表示 RMON 计数器的值。
- **"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"（上升阈值）** — 触发上升阈值警报的上升计数器值。
- **"Rising/Falling Event"（上升/下降事件）** — 报告警报的机制， 即日志或陷阱或者二者的组合。 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，则将生成通过 SNMP 的陷阱，并通过陷阱的一般机制进行报告。 可以使用同一机制保存陷阱。
- **"Falling Threshold"（下降阈值）** — 触发下降阈值警报的下降计数器值。

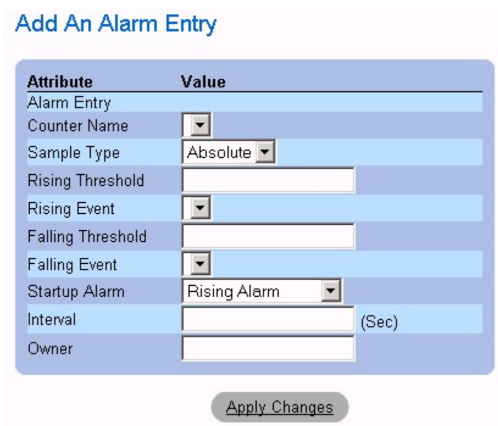
注： 上升和下降阈值将以图形形式显示在图形栏顶部。 每个被监测的变量均有一种指定的颜色。

- **"Startup Alarm"（启动警报）** — 用于激活警报的触发器。 可以通过将阈值从较低阈值提升到较高阈值来定义上升。 可能的字段值包括：
  - **"Rising Alarm"（上升警报）**
  - **"Falling Alarm"（下降警报）**
  - **"Rising and Falling Alarm"（上升和下降警报）**
- **"Interval"（时间间隔）** — 表示警报的间隔时间。

- **"Owner"（所有者）** — 表示定义警报的设备或用户。
- **"Remove"（删除）** — 删除 RMON 警报。
  - **已选取** — 删除 **"Alarm Table"（警报表）** 条目。
  - **未选取** — 保留 **"Alarm Table"（警报表）** 条目。

要添加警报表条目，请：

1. 打开 **"RMON Alarm"（RMON 警报）** 页面。
2. 单击 **"Add"（添加）**。 系统将打开 **"New Alarm Entry"（新建警报条目）** 页面。



新建警报条目

3. 定义 **"New Alarm Index"（新警报索引）**、**"Sample Variable"（样例变量）**、**"Sample Type"（样例类型）**、**"Rising Threshold"（上升阈值）**、**"Rising Event"（上升事件）**、**"Falling Threshold"（下降阈值）**、**"Falling Event"（下降事件）**、**"Startup Alarm"（启动警报）**、**"Interval"（时间间隔）** 和 **"Owner"（所有者）** 字段。
4. 单击 **"Apply Changes"（应用更改）**。 系统将添加 RMON 警报，并更新设备。

要修改警报表条目，请：

1. 打开 **"RMON Alarm"（RMON 警报）** 页面。
2. 在 **"Alarm Entry"（警报条目）** 下拉框中选择一个 **"RMON Alarm Table"（RMON 警报表）** 条目。
3. 修改 **"Sample Type"（样例类型）**、**"Rising Threshold"（上升阈值）**、**"Rising Event"（上升事件）**、**"Falling Threshold"（下降阈值）**、**"Falling Event"（下降事件）**、**"Startup Alarm"（启动警报）**、**"Interval"（时间间隔）** 和/或 **"Owner"（所有者）** 字段。
4. 单击 **"Apply Changes"（应用更改）**。 系统将修改 **"RMON Alarm Table"（RMON 警报表）** 条目，并更新设备。

要显示警报表，请：

1. 打开 **"RMON Alarm Table"（RMON 警报表）**，
2. 单击 **"Show All"（全部显示）**。 系统将打开 **"RMON Alarm Table"（RMON 警报表）**。

RMON 警报表

要删除警报表条目，请：

1. 打开**“RMON Alarm”（RMON 警报）**页面。
2. 在**“Alarm Entry”（警报条目）**下拉框中选择一个**“RMON Alarm”（RMON 警报）**。
3. 选取**“Remove”（删除）**复选框。
4. 单击**“Apply Changes”（应用更改）**。 系统将删除**“RMON Alarm Table”（RMON 警报表）**条目，并更新设备。

使用 CLI 命令定义和显示设备警报

下表概括了用于配置和显示**“RMON Alarm”（RMON 警报）**页面中的字段的等效 CLI 命令。

CLI 命令	说明
rmon alarm 索引 变量 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]	配置警报条件。
show rmon alarm-table	显示警报摘要表。
show rmon alarm 编号	显示警报配置。

以下是 CLI 命令的示例：

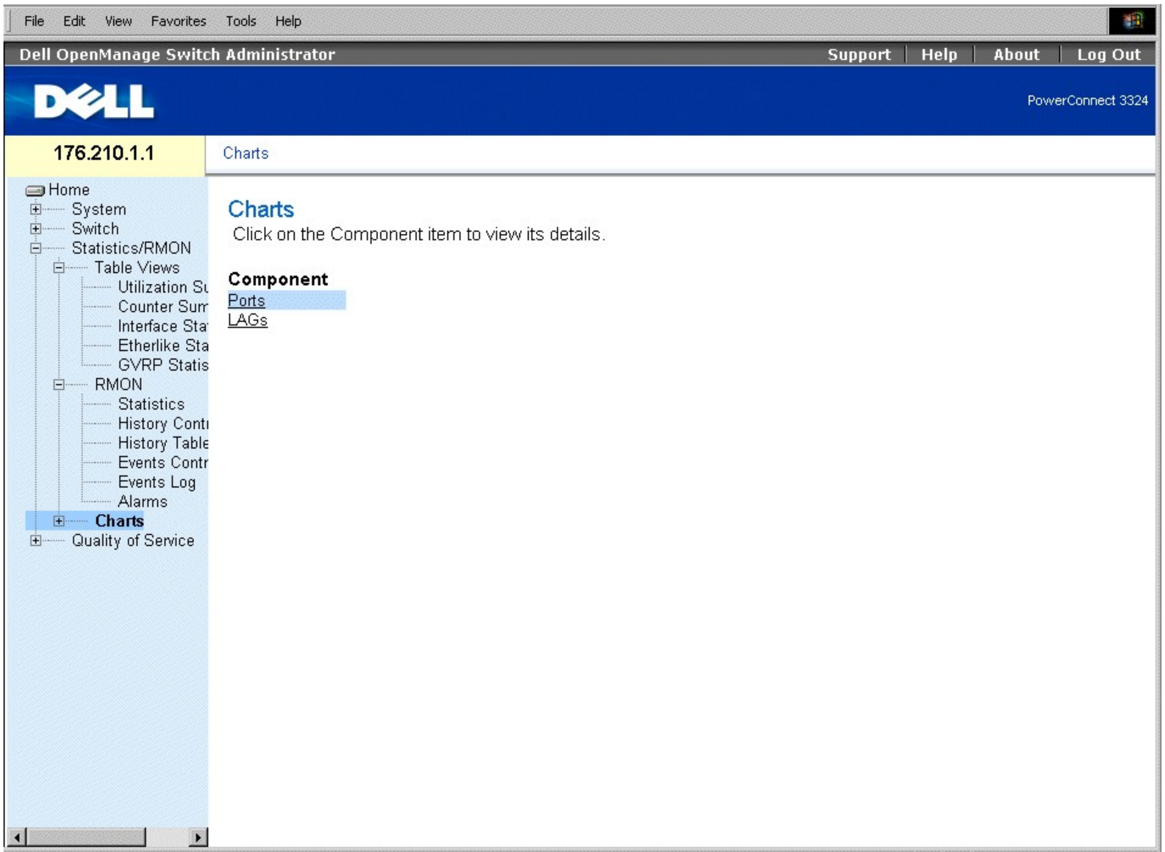
```
Console (config)# rmon alarm 1.3.6.1.2.1.2.2.1.10 1000000 10 20

Console (config)# exit

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

Console# show rmon alarm 1

Alarm 1
```

```
-------

OID: 1.3.6.1.2.1.2.2.1.10.1

Last sample Value: 878128

Interval: 30

Sample Type: delta

Startup Alarm: rising

Rising Threshold: 8700000

Falling Threshold: 78

Rising Event: 1

Falling Event: 1

Owner: CLI
```

查看图表

"Charts"（图表）页面包含以图表格式显示统计数据的链接。 要打开**"Charts"（图表）**页面，请：

- 在树视图中单击**"Statistics"（统计数据）>"Charts"（图表）**。 系统将打开**"Charts"（图表）**页面。



图表页面

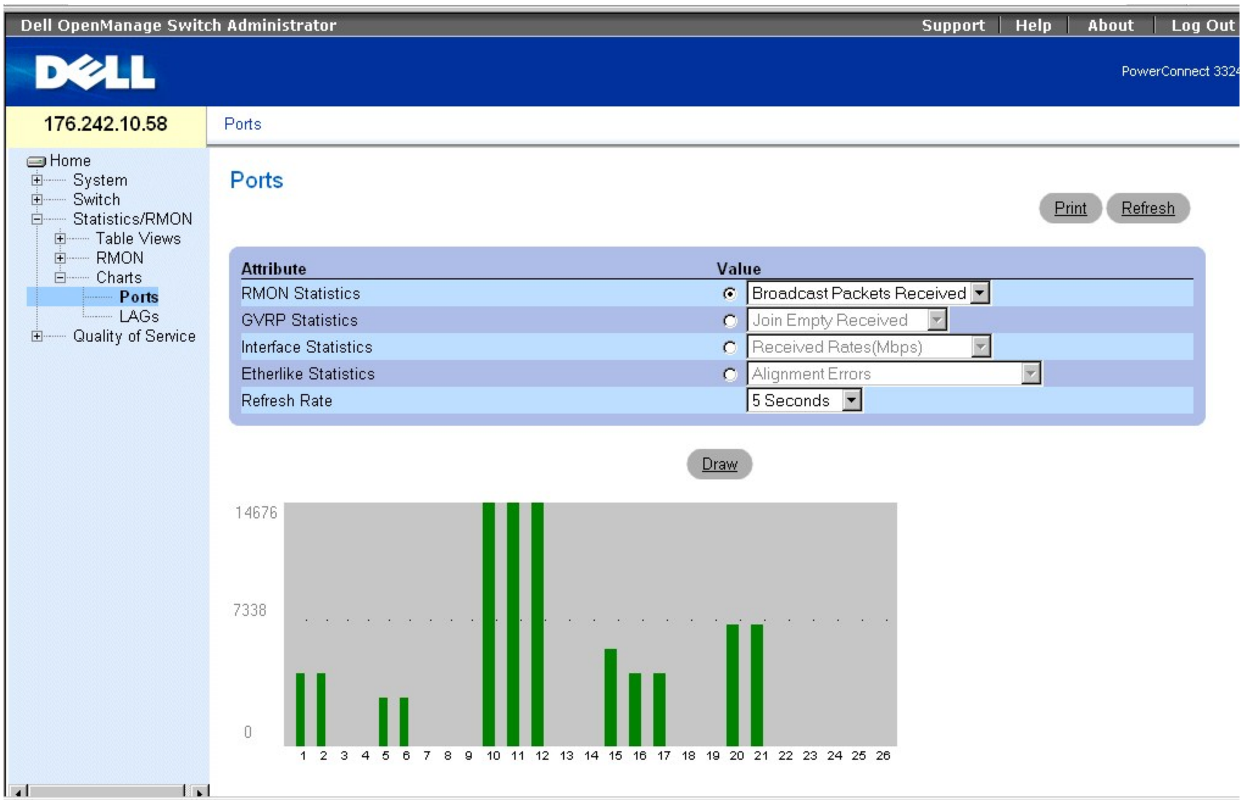
"Charts"（图表）页面包含以下链接：

- [查看端口统计数据]
- [查看 LAG 统计数据]

查看端口统计数据

"Ports"（端口）页面以图表格式显示选定端口的统计数据。 要打开"Port **Statistics"（端口统计数据）**页面：

- 在树视图中单击**"Statistics"（统计数据）>"Charts"（图表）>"Ports"（端口）**。 系统将打开"Port **Statistics"（端口统计数据）**页面。



端口统计数据页面

"Port Statistics"(端口统计数据)页面包含以下字段:

- **"Interface Statistics"(接口统计数据)**— 提供选定装置的接口统计数据。
- **"Etherlike Statistics"(以太网类统计数据)**— 提供选定装置的以太网类统计数据。
- **"RMON Statistics"(RMON 统计数据)**— 提供选定装置的 RMON 统计数据。
- **"GVRP Statistics"(GVRP 统计数据)**— 提供选定装置的 GVRP 统计数据。
- **"Refresh Rate"(刷新率)**— 指定刷新设备之前经过的时间。 可能的字段值包括:
  - **"15 Sec"(15 秒)**— 表示端口统计数据每 15 秒钟刷新一次。
  - **"30 Sec"(30 秒)**— 表示端口统计数据每 30 秒钟刷新一次。
  - **"60 Sec"(60 秒)**— 表示端口统计数据每 60 秒钟刷新一次。
  - **"No Refresh"(不刷新)**— 表示不自动刷新端口统计数据。

要显示特定端口统计数据,请

1. 打开"Port **Statistics"(端口统计数据)**页面。
2. 选择统计数据类别和端口。
3. 单击**"Draw"(绘制)**。 系统将显示选定接口的统计数据。

使用 CLI 命令查看端口统计数据

下表概括了用于查看“Port **Statistics”（端口统计数据**）页面中显示的字段的等效 CLI 命令。

CLI 命令	**说明**
clear counters [ethernet 接口 | **port-channel** 端口通道号]	清除接口上的统计数据。
show rmon statistics [ethernet 接口 | **port-channel** 端口通道号]	显示 RMON 以太网统计数据。
clear gvrp statistics [**ethernet** 接口 | **port-channel** 端口通道号]	清除所有 GVRP 统计数据信息。
show gvrp statistics [ethernet 接口 | **port-channel** 端口通道号]	显示 GVRP 统计数据。
show gvrp error-statistics [**ethernet** 接口 | **port-channel** 端口通道号]	显示 GVRP 错误统计数据。

以下是 CLI 命令实例：

```
Console# clear counters ethernet 1/e1

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

Console # configure

Console (config)# clear gvrp statistics ethernet 1/e8
```

```
Console (config)# exit

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 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
```

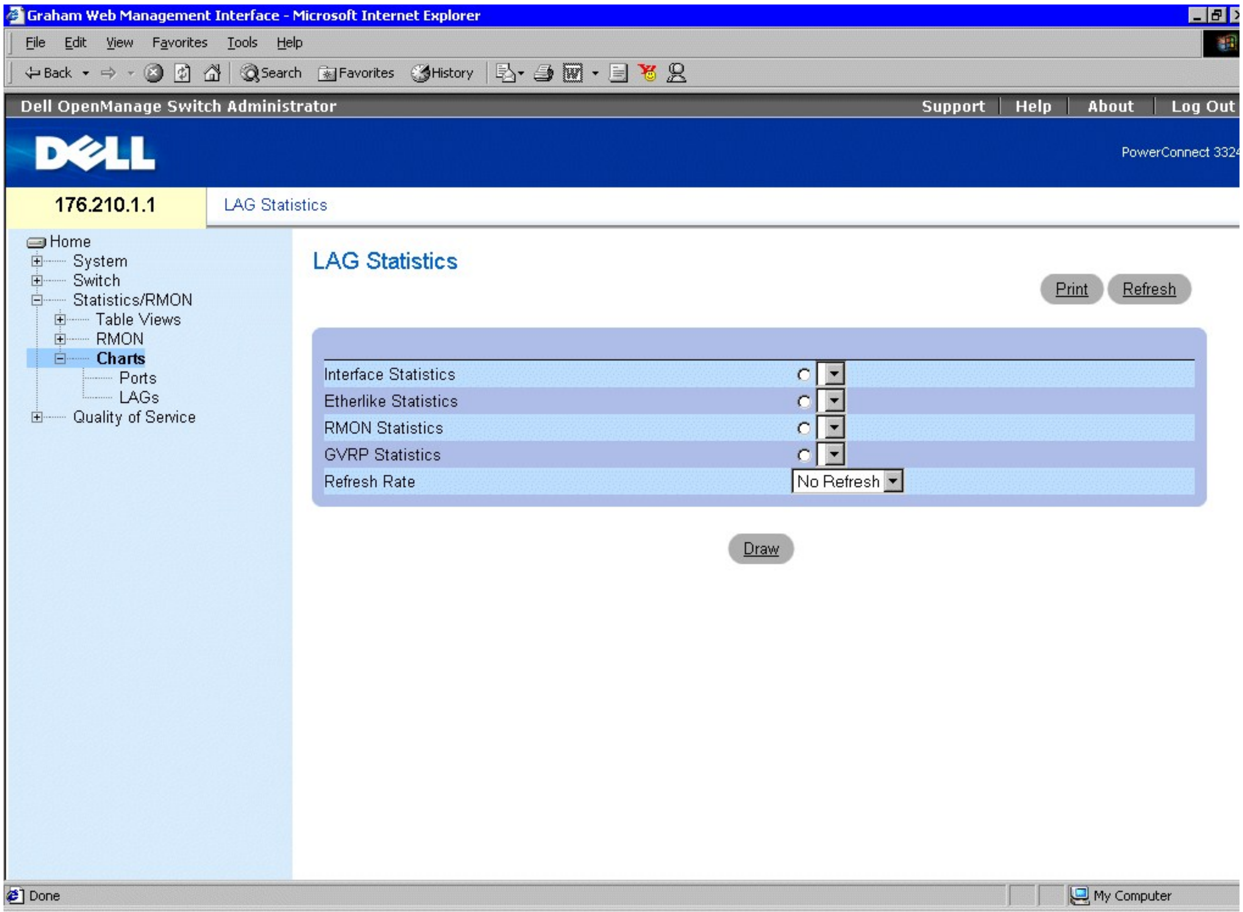
```
1/e7 0 0 0 0 0 0 0 0 0 0 0 0

1/e8 0 0 0 0 0 0 0 0 0 0 0 0


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

1/e5 0 0 0 0 0 0

1/e6 0 0 0 0 0 0

1/e7 0 0 0 0 0 0
```

1/e8 0 0 0 0 0 0

查看 LAG 统计数据

"LAG Statistics"（LAG 统计数据）页面以图表格式显示端口元素的统计数据。 要打开
"LAG Statistics"（LAG 统计数据）页面，请：

- 在树视图中单击 **"Statistics"（统计数据）>"Charts"（图表） >"LAGs"**。 系统将打开 **"LAG Statistics"（LAG 统计数据）**页面。



LAG 统计数据页面

"LAG Statistics"（LAG 统计数据）页面包含以下字段：

- **"Interface Statistics"（接口统计数据）** — 提供主干的接口统计数据。
- **"Etherlike Statistics"（以太网类统计数据）** — 提供主干的以太网类统计数据。
- **"RMON Statistics"（RMON 统计数据）** — 提供主干的 RMON 统计数据。
- **"GVRP Statistics"（GVRP 统计数据）** — 提供主干的 GVRP 统计数据。
- **"Refresh Rate"（刷新率）** — 指定刷新设备之前经过的时间。 可能的字段值包括：
  - **"15 Sec"（15 秒）** — 表示 LAG 统计数据每 15 秒钟刷新一次。
  - **"30 Sec"（30 秒）** — 表示 LAG 统计数据每 30 秒钟刷新一次。

- **"60 Sec"（60 秒）**— 表示 LAG 统计数据每 60 秒钟刷新一次。
- **"No Refresh"（不刷新）**— 表示不刷新 LAG 统计数据。

要显示端口的特定统计数据，请：

1. 打开**"Port Statistics"（端口统计数据）**页面。
2. 选择接口类型。
3. 单击**"Draw"（绘制）**。 系统将显示选定接口的统计数据。

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。

CLI 命令	**说明**
show interfaces counters [**ethernet** 接口 | **port-channel** 端口通道号]	显示物理接口的统计数据。

以下是 CLI 命令实例：

```
Console# show interfaces counters

Port InOctets InUcastPkts InMcastPkts InBcastPkts

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

1/e1 183892 1289 987 8

2/e1 0 0 0 0

3/e1 123899 1788 373 19

Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

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

1/e1 9188 9 8 0

2/e1 0 0 0 0
```

```
3/e1 8789 27 8 0

Ch InOctets InUcastPkts InMcastPkts InBcastPkts

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

1 27889 928 0 78

Ch OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

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

1 23739 882 0 122


Console# show interfaces counters ethernet 1/e1

Port InOctets InUcastPkts InMcastPkts InBcastPkts

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

1/e1 183892 1289 987 8

Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

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

1/e1 9188 9 8 0

Alignment Errors: 17

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

    Symbol Errors: 0

    Received Pause Frames: 0

    Transmitted Pause Frames: 0

---------------------------------------------------------------------
```

返回目录页面

返回目录页面

Dell™ PowerConnect™ 3324/3348 用户指南

- 注、注意和警告

型号：PowerConnect 3324/3348

注、注意和警告

注：注表示可以帮助您更好地使用设备的重要信息。

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。

2003 年 11 月 Rev. A01

返回目录页面