Dell™ PowerConnect™ 5324 系统用户指南

注、注意和警告

注：注表示可以帮助您更好地使用计算机的重要信息。

注意：注意表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。

警告：警告表示可能会导致财产损失、人身伤害甚至死亡。

2007 年 5 月

返回目录页面

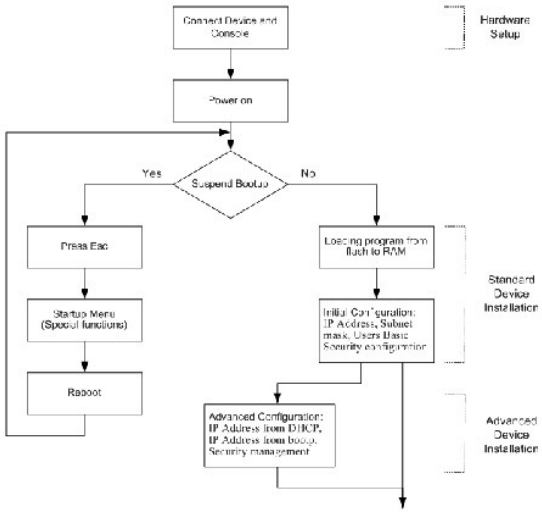
启动和配置设备

Dell™ PowerConnect™ 5324 系统用户指南

完成所有外部连接之后，请将终端连接至设备，以配置设备及继续其它过程。要获得初始配置，请执行标准的设备配置。

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

图 4-12. 安装和配置流程



配置终端

要配置设备，则终端必须运行终端仿真软件。

请确保按照以下步骤设置终端仿真软件：

1. 选择相应的串行端口（串行端口 1 或串行端口 2），以连接至控制台。
2. 将数据速率设置为 9600 波特。
3. 将数据格式设置为 8 个数据位、1 个停止位以及无奇偶校验。
4. 将流控制设置为“**none**”（无）。

5. 在“**Properties**”（**属性**）下，选择“**VT100 for Emulation**”（**VT100 仿真**）模式。
6. 选择“**Terminal keys**”（**终端键**）作为“**Function, Arrow, and Ctrl keys**”（**功能键、箭头键和 Ctrl 键用作**）的设置。确保此设置为“**Terminal keys**”（**终端键**）（而不是“**Windows keys**”[**Windows 键**]）。

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

引导设备

注：假定的引导信息如下所示：

- 设备出厂时为默认配置。
- 设备未配置为使用默认用户名和密码。

要引导设备，请执行以下操作：

1. 确保将设备串行端口连接至 ASCII 终端或运行终端仿真软件的台式机系统的串行连接器。
2. 找到交流电源插座。
3. 切断交流电源插座的电源。
4. 将设备连接至交流电源插座。请参阅“将设备连接至电源设备”。
5. 接通交流电源插座的电源。

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

1. 确保 ASCII 电缆已连接至终端，并确保 SW 仿真上的参数已正确配置。
2. 将电源设备连接至设备。
3. 接通设备电源。
4. 当设备进行引导时，引导检测将首先计算设备内存的可用性，然后再继续进行引导。以下屏幕信息是一个显示的 POST 的示例：

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

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

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

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

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

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



BOOT Software Version 1.0.0.20 Built 22-Jan-2004 15:09:28

Processor: FireFox 88E6218 ARM946E-S , 64 MByte SDRAM.

I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.
```

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


Preparing to decompress...
```

此引导进程大约运行 90 秒钟。

显示在 POST 末尾（请参见最后一行）的自动引导信息表明在引导期间没有遇到问题。

在引导期间，可以使用**“Startup”（启动）**菜单运行特殊程序。要进入**“Startup”（启动）**菜单，请在显示自动引导信息之后的前两秒钟内按 <Esc> 键或 <Enter> 键。

如果没有按下 <Esc> 键或 <Enter> 键来中断系统引导进程，则该进程将继续将代码解压缩并载入到 RAM 中。代码将开始从 RAM 运行，并且系统将显示已编号的系统端口及其状态（良好或断开）的列表。

以下屏幕信息是一个配置示例。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。

```
Decompressing SW from image-2


78c000


OK


Running from RAM...



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


*** Running SW Ver.1.0.0.15 Date 03-Mar-2004 Time 10:41:14 ***


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



HW version is 00.01.07


Base Mac address is: 00:00:07:77:77:77


Dram size is :64M bytes


Dram first block size is :40960K bytes


Dram first PTR is : 0x1800000
```

```
Flash size is: 16M

Device configuration:

Prestera based system

Slot 1 - Neyland24 HW Rev. 0.1

Tapi Version: v1.2.9

Core Version: v1.2.9

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



console> 01-Jan-2000 01:01:35 %LINK-W-Down: g1

01-Jan-2000 01:01:35 %LINK-W-Down: g2

01-Jan-2000 01:01:35 %LINK-W-Down: g3

01-Jan-2000 01:01:35 %LINK-W-Down: g4

01-Jan-2000 01:01:35 %LINK-W-Down: g5

01-Jan-2000 01:01:35 %LINK-W-Down: g6

01-Jan-2000 01:01:35 %LINK-W-Down: g7

01-Jan-2000 01:01:35 %LINK-W-Down: g8

01-Jan-2000 01:01:35 %LINK-W-Down: g9

01-Jan-2000 01:01:35 %LINK-W-Down: g10

01-Jan-2000 01:01:35 %LINK-W-Down: g11

01-Jan-2000 01:01:35 %LINK-W-Down: g12

01-Jan-2000 01:01:35 %LINK-W-Down: g13
```

01-Jan-2000 01:01:36 %LINK-W-Down: g14

01-Jan-2000 01:01:36 %LINK-W-Down: g15

01-Jan-2000 01:01:36 %LINK-W-Down: g16

01-Jan-2000 01:01:36 %LINK-W-Down: g17

01-Jan-2000 01:01:36 %LINK-W-Down: g18

01-Jan-2000 01:01:36 %LINK-W-Down: g19

01-Jan-2000 01:01:36 %LINK-W-Down: g20

01-Jan-2000 01:01:36 %LINK-W-Down: g21

01-Jan-2000 01:01:36 %LINK-W-Down: g22

01-Jan-2000 01:01:36 %LINK-I-Up: Vlan 3000

01-Jan-2000 01:01:36 %LINK-I-Up: Vlan 1

01-Jan-2000 01:01:36 %LINK-I-Up: g1

01-Jan-2000 01:01:36 %LINK-I-Up: g13

01-Jan-2000 01:01:36 %LINK-I-Up: g14

01-Jan-2000 01:01:36 %LINK-I-Up: g19

01-Jan-2000 01:01:36 %LINK-I-Up: g20

01-Jan-2000 01:01:36 %LINK-I-Up: g21

01-Jan-2000 01:01:36 %LINK-W-Down: g23

01-Jan-2000 01:01:36 %LINK-W-Down: g24

01-Jan-2000 01:01:36 %LINK-W-Down: ch1

01-Jan-2000 01:01:36 %LINK-I-Up: Vlan 1000

```
01-Jan-2000 01:01:36 %TRUNK-I-PORTADDED: Port g24 added to ch1

01-Jan-2000 01:01:36 %LINK-I-Up: g22

01-Jan-2000 01:01:36 %LINK-I-Up: g23

01-Jan-2000 01:01:36 %LINK-I-Up: g24

01-Jan-2000 01:01:36 %LINK-I-Up: ch1

01-Jan-2000 01:01:36 %LINK-W-Down: g1

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


console>
```

设备成功引导之后，将显示系统提示符 (console>)，它用于配置设备。但是，在配置设备之前，请确保设备上已安装了最新的软件版本。如果此版本不是最新的版本，请下载并安装最新的版本。有关下载最新版本的详细信息，请参阅“软件下载”。

配置概览

为设备分配静态 IP 地址之前，请获取以下信息：

- 分配给设备以便对设备进行配置的特定 IP 地址。
- 默认路由。
- 网络的网络掩码。

有以下两种配置类型：

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

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

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

初始配置

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

注：初始简单配置需要满足以下假设条件：

- PowerConnect 设备以前从未进行配置，其状态与收到该设备时的状态相同。
- PowerConnect 设备已成功引导。
- 串行连接已建立，并且控制台提示符已显示在 VT100 终端设备的屏幕上。（按下 <Enter> 键若干次，以验证提示符是否正确显示。）

- 设备未配置为使用默认用户名和密码。

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

初始配置包括以下内容：

- 将用户名设置为“admin”，将密码设置为“dell”，使最高权限级别为 15。
- 配置静态 IP 地址和默认网关。
- 配置 SNMP 读/写团体字符串。
- 分配由 DHCP 服务器分配的 IP 地址。

对 PowerConnect 设备应用初始配置过程之前，必须从网络管理员处获取以下信息：

- 要分配给 VLAN 的 IP 地址，设备通过该 VLAN 进行管理。
- 网络的 IP 子网掩码。
- 默认网关 IP 地址。
- SNMP 团体。

静态 IP 地址和子网掩码

IP 地址可以在任何接口上配置，包括 VLAN、LAG 和物理端口。输入配置命令之后，建议您通过输入 **show ip interface** 命令来检查是否有某个端口已配置了该 IP 地址。

重要提示：如果已在 LAG 或物理端口（例如 g10）上配置了 IP 地址，则该接口将从 VLAN 1 中删除。

静态路由配置

要从远程网络对设备进行管理，则必须配置一个静态路由，该路由是一个 IP 地址，在设备表中未找到任何条目的情况下，信息包将被发往该 IP 地址。所配置的 IP 地址必须与其中一个设备 IP 接口属于同一子网。

要配置静态路由，请按如下配置示例所示，在系统提示符后输入命令。其中，100.1.1.1（掩码 24）是特定管理站点，100.1.1.10 是用作默认网关的静态路由。

在带内接口上分配静态 IP 地址

注：此示例需要满足以下假设条件：

- 要分配给 PowerConnect VLAN 接口的 IP 地址为 192.168.1.123
- 网络的 IP 子网掩码为 255.255.255.0
- 默认路由的 IP 地址为 192.168.1.1
- 读/写 SNMP 团体字符串为“private”

```
console> enable

console# configure

console(config)# username admin password dell level 15

console(config)# interface VLAN 1
```

```
console (config-if) # ip address 192.168.1.123 /24

console (config-if) # exit

console (config) # ip default-gateway 192.168.1.1

console (config) # snmp-server community private rw

console(config)# exit

console#
```

验证 IP 地址和默认网关地址

通过执行以下命令并检查其输出，请确保 IP 地址和默认网关已正确分配：

命令

```
console# show ip interface vlan 1
```

输出

Gateway IP Address	Activity status	
---	---	
192.168.1.1	Active	
IP address	Interface	Type
---	---	---
192.168.1.123 /24	VLAN 1	Static

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

用户名

要远程管理设备（例如通过 SSH、Telnet 或 Web 界面），则必须配置用户名。要获得对设备的完全的管理控制，必须指定设备的最高权限 (15)。

注：仅允许具有最高权限级别 (15) 的管理员（超级用户）通过 Web 浏览器界面对设备进行管理。

有关权限级别的详细信息，请参阅“CLI 参考指南”。

将配置的用户名作为登录名输入，以远程管理会话。要配置用户名和权限级别，请按如下配置示例所示，在系统提示符后输入命令：

```
console> enable

console# configure

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

SNMP 团体字符串

简单网络管理协议 (SNMP) 提供了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。变量在管理信息库 (MIB) 中进行定义。MIB 提供了代理控制的变量。SNMP 代理定义了 MIB 规范格式，以及通过网络访问信息的格式。访问 SNMP 代理的权限由访问字符串和 SNMP 团体字符串控制。

此设备是 SNMP 兼容的，它包含支持一组标准和专用 MIB 变量的 SNMP 代理。管理站点的开发人员需要准确的 MIB 树结构并在接收到完整的专用 MIB 信息之后，才能管理 MIB。

除 SNMP 管理站点 IP 地址、团体名称和访问权限之外的所有参数均可以从任何 SNMP 管理平台进行管理。如果团体字符串不存在，则会禁止对设备进行 SNMP 管理访问。

注：设备出厂时未配置团体字符串。此设备支持 SNMPv1 和 SNMPv2。本节介绍了 SNMPv1/v2 配置参数。

以下屏幕信息显示了默认的设备配置：

Console# **show snmp**

Community- String	Community-Access	IP address
---------------	----------------	-----------------------------

Traps are enabled.
Authentication trap is enabled.

Trap-Rec- Address	Trap-Rec- Community	Version

System Contact:
System Location:

在初始配置期间，团体字符串、团体访问和 IP 地址可以通过本地终端进行设置。

SNMP 配置选项包括：

- 团体字符串。
  - **“Read Only”（只读）**— 表明团体成员可以查看配置信息，但不能更改任何信息。
  - **“Read/Write”（读/写）**— 表明团体成员可以查看和修改配置信息。
  - **“Super”（高级）**— 表明团体成员具有管理访问权限。
- 可配置的 IP 地址。如果未配置 IP 地址，则具有相同团体名称的所有团体成员均被授予相同的访问权限。

通常的做法是对设备使用两个团体字符串 — 一个（public 团体）具有只读访问权限，另一个（private 团体）具有读写访问权限。public 字符串允许经授权的管理站点检索 MIB 对象，而 private 字符串允许经授权的管理站点检索和修改 MIB 对象。

初始配置期间，建议您根据网络管理要求配置设备，并与使用基于 SNMP 的管理站点保持一致。

配置 SNMP

要为一般设备路由器表配置 SNMP 站点 IP 地址和团体字符串，请执行以下步骤。

1. 在控制台提示符后，输入命令 **Enable**。提示符显示为 **#**。
2. 输入命令 **configure** 并按 <Enter> 键。
3. 在配置模式中，输入带有包含团体名称 (private)、团体访问权限（读和写）和 IP 地址等参数的 SNMP 配置命令，如以下示例所示：

```
console# configure

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

查看 SNMP 团体表

要查看 SNMP 站点 IP 地址和团体表，请：

1. 在控制台提示符后，输入命令 **exit**。提示符显示为 **#**。
2. 在优先执行模式下，输入如以下示例所示的显示命令：

配置完参数后才能从任何远程位置进行进一步的设备配置。

Console# **show snmp**		
Community- String	Community-Access	IP address
---	---	---
private	read write	11.1.1.2

Traps are enabled.		
Authentication trap is enabled.		
Trap-Rec- Address	Trap-Rec- Community	Version
System Contact:		
System Location:		

高级配置

本节介绍了有关 IP 地址的动态分配和基于验证、授权和计费 (AAA) 机制的安全保护管理的信息，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包括 IP 地址，并可能包括子网掩码和默认网关。

从 DHCP 服务器检索 IP 地址

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

1. 选择并连接 DHCP 服务器的任何端口或具有 DHCP 服务器的子网的任何端口，以便检索 IP 地址。
2. 输入以下命令，以使用选定的端口来获取 IP 地址。在以下示例中，命令基于配置中使用的端口类型。

- 分配动态 IP 地址：

```
console# configure

console(config)# interface ethernet g1

console(config-if)# ip address dhcp hostname device

console(config-if)# exit

console(config)#
```

- 分配动态 IP 地址（在 VLAN 上）：

```
console# configure
```

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

console(config-if)# ip address dhcp hostname device

console(config-if)# exit

console(config)#
```

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

```
Console# show ip interface

                                                                    

Gateway IP Address                Activity status

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

10.7.1.1                          Active

                                                                    

                                                                    

IP address                        Interface                 Type

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

10.7.1.192/24                     VLAN 1                    Static

10.7.2.192/24                     VLAN 2                    DHCP
```

注：要从 DHCP 服务器检索 IP 地址，没有必要删除设备配置。

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

从 BOOTP 服务器获取 IP 地址

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

要从 BOOTP 服务器检索 IP 地址，请：

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

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

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

以下示例说明了此过程：

```
console> enable

console# delete startup-config

Startup file was deleted

console# reload

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

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

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

/* the switch reboots */
```

要验证此 IP 地址，请输入 **show ip interface** 命令。

此设备现已配置了 IP 地址。

安全保护管理和密码配置

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

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

配置安全保护密码

您可以为以下服务配置安全保护密码：

- 终端
- Telnet
- SSH
- HTTP
- HTTPS

注：密码由用户定义。

注：创建用户名时，默认的优先级为“1”，即允许访问权限但不允许配置权限。必须设置为优先级 15 才能启用对设备的访问权限和配置权限。虽然可以为用户名分配优先级 15（不使用密码），但建议您始终指定密码。如果没有指定的密码，则具有权限的用户可以使用任何密码访问 Web 界面。

配置初始终端密码

要配置初始终端密码，请输入以下命令：

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

console(config)# aaa authentication enable default line

console(config)# line console

console(config-line)# login authentication default

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

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

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

配置初始 Telnet 密码

要配置初始 Telnet 密码，请输入以下命令：

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

console(config)# aaa authentication enable default line

console(config)# line telnet

console(config-line)# login authentication default

console(config-line)# enable authentication default

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

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

配置初始 SSH 密码

要配置初始 SSH 密码，请输入以下命令：

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

console(config)# aaa authentication enable default line

console(config)# line ssh

console(config-line)# login authentication default

console(config-line)# enable authentication default

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

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

配置初始 HTTP 密码

要配置初始 HTTP 密码，请输入以下命令：

```
console(config)# ip http authentication local
console(config)# username admin password user1 level 15
```

配置初始 HTTPS 密码

要配置初始 HTTPS 密码，请输入以下命令：

```
console(config)# ip https authentication local
console(config)# username admin password user1 level 15
```

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

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

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

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

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

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

启动程序

“Startup”（启动）菜单程序

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

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

要进入**“Startup”（启动）**菜单，请：

1. 打开电源并等待自动引导信息。

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

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

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

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


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

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

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

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

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



BOOT Software Version 1.0.0.20 Built 22-Jan-2004 15:09:28

Processor: FireFox 88E6218 ARM946E-S , 64 MByte SDRAM.

I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.


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

Preparing to decompress...
```

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

```
[1] Download Software

[2] Erase Flash File

[3] Password Recovery Procedure

[4] Enter Diagnostic Mode

[5] Set Terminal Baud-Rate

[6] Back

Enter your choice or press 'ESC' to exit
```

以下各节介绍了可用的**“Startup”（启动）**菜单选项。

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

软件下载

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

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

```
Downloading code using XMODEM
```

2. 使用超级终端时，单击超级终端菜单栏上的**“Transfer”（传输）**。
3. 在**“Filename”（文件名）**字段中，输入要下载的文件的文件路径。
4. 确保在**“Protocol”（协议）**字段中已选择 Xmodem 协议。
5. 按**“Send”（发送）**。软件将被下载。

注：软件下载之后，设备将自动重新启动。

注：下载时间的长短因使用的工具的不同而有所差异。

删除快擦写文件

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

删除设备配置

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

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

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

2. 按 Y。系统将显示以下信息。

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

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

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

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

密码恢复

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

要仅为本地终端恢复丢失的密码，请：

1. 在**“Startup”（启动）**菜单中，键入 3 并按 <Enter> 键。

密码被删除。

注：要确保设备安全，请重新配置适用的管理方法的密码。

通过 TFTP 服务器下载软件

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

系统映像下载

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

除非选择其它映像，否则，下次引导时，设备将解压缩并运行当前的活动系统映像。

要通过 TFTP 服务器下载系统映像，请：

1. 确保已在其中一个设备端口上配置 IP 地址，并且可以将 ping 发送至 TFTP 服务器。
2. 确保要下载的文件已保存在 TFTP 服务器上（ros 文件）。
3. 输入 show version 以验证设备上当前运行的是哪个软件版本。以下是一个信息显示示例：

```
console# show version

SW version 1.0.0.42 (date 22-Jul-2004 time 13:42:41)

Boot version 1.0.0.18 (date 01-Jun-2004 time 15:12:20)

HW version
```

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

```
console# sh bootvar

Images currently available on the Flash

Image-1 active (selected for next boot)

Image-2 not active

console#
```

5. 输入 copy tftp://{tftp address}/{file name} image，以将新的系统映像复制到设备。下载新的映像之后，该映像将保存在分配给另一个系统映像副本的区域中（image-2，如示例中所示）。以下是一个信息显示示例：

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

Accessing file `file1' on 176.215.31.3Ö

Loading file1 from 176.215.31.3:

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

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

感叹号表示复制过程正在进行。每个符号 (!) 对应于已成功传输 512 个字节。句号表示复制过程已超时。一行中的多个句号表示复制过程失败。

6. 通过输入引导系统命令来为下一个引导选择映像。然后，输入 show bootvar，以验证表示为引导系统命令中的参数的副本已选择为下一个引导。

以下是一个屏幕上显示的信息示例。

```
console# boot system image-2

console# sh boot
```

```
Images currently available on the Flash

Image-1 active

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

如果未通过输入 boot system 命令选择下一个引导的映像，则系统将从当前活动映像进行引导。

7. 输入 reload 命令。系统将显示以下信息：

```
console# reload

This command will reset the whole system and disconnect your current

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

8. 输入 y。设备将重新引导。

引导映像下载

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

1. 确保已在其中一个设备端口上配置 IP 地址，并且可以将 ping 发送至 TFTP 服务器。
2. 确保要下载的文件已保存在 TFTP 服务器上（rfb 文件）。
3. 输入 show version 以验证设备上当前运行的是哪个软件版本。以下是一个信息显示示例：

```
console# sh ver

SW version 1.0.0.42 (date 22-Jul-2004 time 13:42:41)

Boot version 1.0.0.18 (date 01-Jun-2004 time 15:12:20)

HW version 00.00.01 (date 01-May-2004 time 12:12:20)
```

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

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

Erasing file..done.

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

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

5. 输入 reload 命令。系统将显示以下信息：

```
console# reload

This command will reset the whole system and disconnect your current

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

6. 输入 y。

设备将重新引导。

返回目录页面

返回目录页面

词汇表

Dell™ PowerConnect™ 5324 系统用户指南

英文 B C D F G J L Q R S T W X Y Z

此词汇表包含重要的关键技术词汇。

B C D F G J L Q R S T W X Y Z

英文

ARP

地址解析协议。一种 TCP/IP 协议，用于将 IP 地址转换为物理地址。

ASIC

应用程序特定集成电路。一种专用于特定应用程序的自定义芯片。

BootP

Bootstrap 协议。使工作站可以发现其 IP 地址、网络上的 BootP 服务器的 IP 地址或载入到设备引导的配置文件。

BPDU

桥接协议数据装置。以信息格式提供桥接信息。BPDU 随生成树配置内的设备信息一起发送。BPDU 信息包包含有关端口、地址、优先级和传输成本的信息。

CDB

配置数据库。一个包含设备的配置信息的文件。

CLI

命令行界面。用于配置系统的一组行命令。有关使用 CLI 的详细信息，请参阅“使用 CLI”。

CPU

中央处理器。处理信息的计算机部件。CPU 由控制单元和 ALU 组成。

DHCP 客户端

使用 DHCP 获得配置参数（例如网络地址）的 Internet 主机。

DSCP

DiffServe 代码点 (DSCP)。DSCP 提供了为 IP 信息包标记 QoS 优先级信息的方法。

EWS

嵌入式 Web 服务器。通过标准 Web 浏览器提供设备管理。嵌入式 Web 服务器用于附加或替代 CLI 或 NMS。

FFT

快速传输表。提供有关传输路由的信息。如果信息包到达具有已知路由的设备，则此信息包将通过 FFT 中列出的路由进行传输。如果没有已知路由，CPU 将传输信息包并更新 FFT。

FIFO

先进先出。一种排队处理，其中队列中的第一个信息包为出自信息包的第一个信息包。

GARP

通用属性注册协议。将客户端站点注册至多点传送域。

GVRP

GARP VLAN 注册协议。将客户端站点注册至 VLAN。

HOL

队列。信息包被排队。队列首的信息包先传输，然后列尾的信息包再传输。

HTTP

超文本传输协议。在 Internet 上的服务器和客户端之间传输 HTML 文档。

IC

集成电路。集成电路是由半导体材料构成的小型电子设备。

ICMP

Internet 信报控制协议。使网关或目的地主机可以与源主机进行通信，例如报告正在处理的错误。

IEEE

美国电气及电子工程师学会。制订通信和网络标准的工程师行业组织。

IEEE 802.1d

用于生成树协议，IEEE 802.1d 支持 MAC 桥接从而避免了网络环路。

IEEE 802.1p

可以排定数据链路/MAC 子层的网络通信的优先级。

IEEE 802.1Q

定义 VLAN 网桥的操作，VLAN 网桥允许定义、操作和管理桥接 LAN 基础设施内的 VLAN。

IP

网际协议。指定信息包的格式和定址方法。IP 选定信息包地址，并将信息包传输至正确的端口。

IP 地址

网际协议地址。分配给两个或多个互连 LAN 或 WAN 的网络设备的唯一的地址。

IPX

互联网信息包交换。传输无连接通信。

LAG

链路聚合组。将端口或 VLAN 聚合到一个虚拟端口或 VLAN。

有关 LAG 的详细信息，请参阅“**定义 LAG 成员关系**”。

LAN

局域网。包含在一个房间、建筑、校园或其它有限的地理区域内的网络。

MAC 层

数据链路控制 (DTL) 层的一个子层。

MAC 地址

介质访问控制地址。MAC 地址是标识各个网络节点的硬件特定地址。

MAC 地址学习

MAC 地址学习具有一个学习网桥的特征，在该网桥中记录了信息包的源 MAC 地址。指定传输到该地址的信息包将仅被传输至该地址所在的网桥接口。定址到未知地址的信息包将被传输至每个网桥接口。MAC 地址学习使连接的 LAN 上的通信达到最小。

MD5

报文摘要 5。一种生成 128 位散列的算法。MD5 是 MD4 的一种变体，它增强了 MD4 的安全性。MD5 验证通信是否完整并验证通信的起点。

MDI

介质相关接口。一种用于终端站点的电缆。

MDIX

带有绞接电缆的介质相关接口 (MDIX)。一种用于集线器和交换机的电缆。

MIB

管理信息库。MIB 包含了对网络组件的特定方面进行说明的信息。

NMS

网络管理系统。一种提供了管理系统的方式的接口。

OID

对象标识符。SNMP 使用对象标识符标识管理型对象。在 SNMP 管理器/代理网络管理范例中，每个管理型对象必须有一个 OID 用于标识该对象。

PDU

协议数据装置。一种在分层协议中指定的数据装置，它包括协议控制信息和层用户数据。

PING

因特网信息包搜索协议。验证特定 IP 地址是否可用。发送到另一个 IP 地址并等待回复的信息包。

QoS

服务质量。QoS 使网络管理员可以根据优先级、应用程序类型以及源地址和目的地地址确定如何传输网络通信和传输哪些网络通信。

RADIUS

远程认证拨入用户服务。一种用于验证系统用户并记录连接时间的方式。

RMON

远程监测。提供了可以从单个工作站收集的网络信息。

RSTP

快速生成树协议。可以检测并使用网络拓扑，网络拓扑使生成树可以快速聚合，而不会创建传输环路。

SNMP

简单网络管理协议。管理 LAN。基于 SNMP 的软件通过嵌入式 SNMP 代理与网络设备进行通信。SNMP 代理收集网络活动信息和设备状态信息，并将信息发送回工作站。

SNTP

简单网络计时协议。SNTP 确保网络交换机时钟时间同步准确，最多准确到毫秒。

SoC

芯片上的系统。一种包含整个系统的 ASIC。例如，通信 SoC 应用程序可能包含微处理器、数字信号处理器、RAM 和 ROM。

SSH

安全命令解释程序。通过网络登录到远程计算机、执行命令并将文件从一台计算机传输到另一台计算机。

TCP/IP

传输控制协议。使两台主机可以相互通信和交换数据流。TCP 保证信息包的传送，并保证信息包以其发送的顺序被传输和接收。

Telnet

终端仿真协议。使系统用户可以登录远程网络并使用远程网络上的资源。

TFTP

小型文件传输协议。使用不带安全保护功能的用户数据协议 (UDP) 传输文件。

UDP

用户数据协议。传输信息包，但并不保证其发送。

VLAN

虚拟局域网。局域网 (LAN) 的逻辑子组，它是通过软件而不是通过定义硬件解决方案创建的。

WAN

广域网。覆盖大面积地理区域的网络。

B

背板

设备中传输信息的主总线。

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。

背压

半双工模式使用的一种机制，使端口无法接收信息。

波特

每秒中传输的信号元素的数量。

C

查询

从数据库中抽取信息并显示要使用的信息。

超长帧

可以在较少的帧内传输相同的数据。超长帧减少了额外开销、缩短了处理时间并确保中断较少。

出口端口

从中传输网络通信的端口。

D

带宽

带宽指定了在固定时间段内可以传输的数据量。对于数字设备，带宽以每秒位数 (bps) 或每秒字节数定义。

带宽分配

分配给特定应用程序、用户和/或接口的带宽量。

单点传送

将一个信息包传输给一个用户的路由形式。

第 2 层

数据链路层或 MAC 层。包含客户端站点或服务器站点的物理地址。由于要处理的信息较少，因此第 2 层理要快于第 3 层处理。

第 4 层

建立一个连接，并确保所有数据均到达其目的地。对第 4 层上检查到的信息包进行分析，并基于其应用程序进行传输判断。

端口

提供了使微处理器可以与外围设备进行通信的连接组件的物理端口。

端口镜像

通过将传入和传出信息包的副本从一个端口传输至监测端口，端口镜像可以监测和镜像网络通信。

有关端口镜像的详细信息，请参阅“**定义端口镜像会话**”。

端口速率

表明端口的端口速率。端口速率包括：

- 以太网 10 Mbps
- 高速以太网 100Mbps
- 吉位以太网 1000 Mbps

多点传送

将一个信息包的副本传输至多个端口。

F

访问模式

指定了向用户授予访问系统权限的方法。

访问配置文件

使网络管理员可以定义配置文件和用于访问设备的规则。对管理功能的访问可以限制在用户组内，它由以下条件定义：

- 入口接口
- 源 IP 地址和/或源 IP 子网

分段

将 LAN 分为单独的 LAN 网段，用于桥接和路由。分段消除了 LAN 带宽限制。

封盖

当接口状态不断更改时，会出现封盖。例如，STP 端口从侦听到了解、到传输不断进行更改。这可能导致通信丢失。

服务级别

服务级别为 802.1p 优先级方案。CoS 提供了为信息包标记优先级信息的方法。CoS 值介于 0 至 7 之间，该值被添加到信息包的第 II 层标头，其中，零为最低优先级，七为最高优先级。

服务器

一种为网络中的其它计算机提供服务的中央计算机。服务可能包括文件存储和访问应用程序。

负载平衡

使数据和/或处理信息包在可用的网络资源上平均分配。例如，负载平衡可能将传入信息包平均地分配给所有服务器，或者将信息包重定向至下一个可用服务器。

G

广播

一种将信息包传输至网络上的所有端口的方式。

广播风暴

过多的广播信息同时通过单个端口在网络中传输。已传输信息的响应被堆入网络，从而使网络资源过载或导致网络超时。

有关广播风暴的详细信息，请参阅“定义 LAG 参数”。

广播域

设备组，用于接收源自一个指定组内的任何设备的广播帧。路由器捆绑广播域，由于路由器不传输广播帧。

J

吉位以太网

吉位以太网以 1000 Mbps 进行传输，并与现有 10/100 Mbps 以太网标准兼容。

交换机

在 LAN 网端之间筛选和传输信息包。交换机支持任何信息包协议类型。

节点

一个网络连接端点或一个用于多条网络线路的公共交叉点。节点包括：

- 处理器
- 控制器
- 工作站

聚合 VLAN

将若干 VLAN 组成一个聚合 VLAN。聚合 VLAN 使路由器可以响应对位于不同子 VLAN（属于同一个超级 VLAN）上的节点的 ARP 请求。路由器以其 MAC 地址进行响应。

L

流控制

使低速设备可以与高速设备进行通信，即高速设备阻止发送信息包。

路由器

一种连接到单个网络的设备。路由器在两个或多个网络之间传输信息包。路由器在第 3 层上运行。

Q

启动配置

在设备断电或重新引导时维护完整的设备配置。

R

入口端口

接收网络通信的端口。

S

生成树协议

防止网络通信中的环路。生成树协议 (STP) 提供了树拓扑用于任意排列网桥。STP 在网络中的终端站点之间提供了一条路径，消除了环路。

双工模式

允许同时传输和接收数据。有两种不同的双工模式：

- **全双工模式** — 允许进行双同步通信，例如电话。双方可以同时传输信息。
- **半双工模式** — 允许进行异步通信，例如手提对讲机。一次仅其中一方可以传输信息。

碎片

小于 576 位的以太网信息包。

T

通配符掩码

指定要使用的 IP 地址位以及要忽略的 IP 地址位。通配符掩码 255.255.255.255 表示所有位都不重要。通配符 0.0.0.0 表示所有位都重要。

例如，如果目的地 IP 地址为 149.36.184.198，通配符掩码为 255.36.184.00，则表示使用 IP 地址的前两位，忽略最后两位。

团体

指定具有相同系统访问权限的一组用户。

W

网桥

一种连接两个网络的设备。网桥是硬件特定的，与协议无关。网桥在第 1 层和第 2 层上运行。

X

陷阱

由 SNMP 发送的信息，表示发生了系统事件。

协议

控制设备如何在网络中交换信息的一组规则。

信息包

用于在信息包交换系统中传输的信息块。

Y

验证配置文件

若干组规则，使您可以登录及验证用户和应用程序。

以太网

以太网按照 IEEE 802.3 被标准化。以太网是最常用的执行的 LAN 标准。支持以 Mbps 为单位的数据传输速率，支持 10 Mbps、100 Mbps 或 1000 Mbps。

引导版本

引导版本。

映像文件

系统映像被保存到两个称为映像（映像 1 和映像 2）的闪存扇区中。活动映像存储活动副本，另个映像存储次副本。

域

以共同的规则和步骤组合起来的网络中的一组计算机和设备。

Z

帧

包含物理介质所需的标头和报尾信息的信息包。

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。

终端系统

网络上的终端用户设备。

主干聚合

链路聚合。通过将一组端口链接在一起形成一条主干（聚合组）来优化端口的使用。

主机

用作其它计算机的信息源或服务源的计算机。

资产标签

指定用户定义的设备参考。

子网

子网。子网是网络的组成部分，它共用一个公用地址组件。在 TCP/IP 网络上，共用一个前缀的设备是同一子网的一部分。例如，具有前缀 157.100.100.100 的所有设备均为同一子网的一部分。

子网掩码

用于屏蔽子网地址中所使用的全部或部分 IP 地址。

自适应

可以建立 10/100 Mpbs 或 10/100/1000 Mbps 以太网端口，使其具有以下功能：

- 双工/半双工模式
- 流控制
- 速率

组合端口

具有两个物理连接的单个逻辑端口，包括一个 RJ-45 连接和一个 SFP 连接。

最佳传输能力

通信能力分配给最低优先级队列，不保证信息包传送。

返回目录页面

返回目录页面

硬件说明

Dell™ PowerConnect™ 5324 系统用户指南

设备端口配置

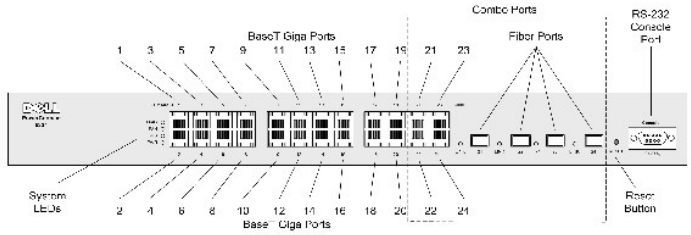
PowerConnect 5324 前面板端口说明

PowerConnect 5324 设备配置了以下端口：

- **24 个铜质端口** — 指定为 10/100/1000 BaseT 吉位以太网端口的 RJ-45 端口
- **4 个光纤端口** — 指定为吉位端口
- **终端端口** — 基于 RS-232 控制台的端口

下图说明了 PowerConnect 5324 前面板。

图 2-3. PowerConnect 5324 前面板



前面板包含端口 1 至 24（为铜质的基于 RJ-45 的端口），这些端口被指定为 10/100/1000 Mbps 并支持半双工和全双工模式。共有四个 SFP 光纤端口，它们被指定为组合端口 21 至 24。组合端口是具有两个物理连接的单个逻辑端口。一次仅有一个物理连接可以处于活动状态，因此，或者是铜质端口可以处于活动状态，或者是等效的光纤端口 21 至 24 可以处于活动状态，但两者无法同时处于活动状态。上面一排端口用奇数 1 至 23 进行标记，下面一排端口用偶数 2 至 24 进行标记。

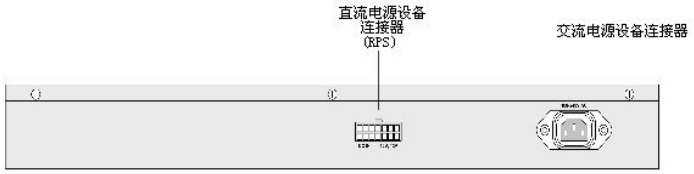
前面板上有一个 RS-232 控制台端口、所有设备 LED 以及一个用于手动重启动设备的重启动按钮。

设备将自动检测连接到 RJ-45 端口的电缆是绞接电缆还是直通电缆，并以哪种方式运行。

PowerConnect 背面板端口说明

设备背面板带有电源连接器，如图 2-4 所示。

图 2-4. 设备背面板



设备背面板上有两个电源设备连接器。有一个交流电源设备连接器可连接到 110V 或 220V 电源设备，可用于常规使用。

直流电源设备连接器用于连接冗余电源设备 (RPS)，在交流电源设备断电时该 RPS 会自动激活。

设备端口

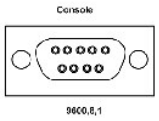
SFP 端口

超小型可插入式 (SFP) 端口是一个可热交换的光模块化收发机，它提供了高速率和高压缩性。此端口被指定为 1000Base-SX 或 LX。

RS-232 控制台端口

一个 DB-9 连接器，用于串行终端连接，它可用于调试、软件下载等等。默认波特率为 9600 bps。可以将波特率配置为 2400 bps 到最大为 38400 bps。

图 2-5. 控制台端口



组合端口

组合端口是具有两个物理连接的单个逻辑端口：

- RJ-45，用于连接双绞线铜质电缆
- SFP，用于连接各种基于光纤的模块

每次只能使用组合端口的两个物理连接中的一个。端口配置和可用的端口控件由所使用的物理连接所确定。

系统将自动检测组合端口上使用的介质，并将在所有操作和控制接口中使用此信息。

如果 RJ-45 和 SFP 同时存在，并且 SFP 端口中已插入一个连接器，SFP 端口就处于活动状态，除非插入了相同数量的 Base-T 端口的铜质连接器并形成了链路。

系统无须重新引导或重启动即可从 RJ-45 切换至 SFP（反之亦然）。

物理尺寸

此设备的物理尺寸如下所示：

- 高度 — 44 mm（1.73 英寸）
- 宽度 — 440 mm（17.32 英寸）
- 厚度 — 255 mm（10.03 英寸）

LED 定义

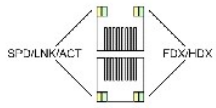
前面板上有发光二极管 (LED)，这些发光二极管表明链路状态、电源设备状态、风扇状态以及系统诊断程序的状态。

端口 LED

10/100/1000 Base-T 端口 LED

每个 10/100/1000 Base-T 端口均具有两个 LED。左侧 LED 表明速率/链路/活动，右侧 LED 表明双工模式。

图 2-6. 基于 RJ-45 的铜质的 10/100/1000 BaseT LED



下表说明了 RJ-45 LED 指示灯的信息：

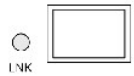
表 2-1. 基于 RJ-45 的铜质的 10/100/1000BaseT LED 指示灯

LED	颜色	说明
左侧 LED	呈绿色稳定亮起	端口以 1000 Mbps 链接。
	呈绿色闪烁	端口正在以 1000 Mbps 发送或接收数据。
	呈橙色稳定亮起	端口以 10 Mbps 或 100 Mbps 链接。
	呈橙色闪烁	端口正在以 10 Mbps 或 100 Mbps 发送或接收数据。
	不亮	端口正在以半双工模式运行。

SFP LED

每个 SFP 端口均具有一个标记为 LNK 的 LED。

图 2-7. SFP 端口 LED



下表说明了 SFP 端口 LED 指示灯的信息：

表 2-2. SFP 端口 LED 提示灯

LED	颜色	说明
SFP	呈绿色稳定亮起	端口当前已打开。
	呈绿色闪烁	端口当前正在发送或接收数据。
	不亮	端口当前已关闭。

连接了 SFP 端口后，相应的铜质组合端口上的双 LED 将呈绿色亮起。

系统 LED

系统 LED 位于前面板的左侧，它提供了有关电源设备、风扇、温度条件和诊断程序的信息。图 2-8 对系统 LED 进行了说明。

图 2-8. 系统 LED

下表说明了系统 LED 指示灯。

表 2-3. 系统 LED 指示灯

LED	颜色	说明
诊断程序 (DIAG)	呈绿色闪烁	系统当前正在运行诊断检测程序。
	呈绿色稳定亮起	系统已通过诊断程序的检测。
	呈红色稳定亮起	系统未通过诊断程序的检测。
风扇 (FAN)	呈绿色稳定亮起	设备风扇运行正常。
	呈红色稳定亮起	一个或多个风扇未运行。
冗余电源设备 (RPS)	呈绿色稳定亮起	冗余电源设备当前正在运行。
	呈红色稳定亮起	冗余电源设备未运行。
	不亮	冗余电源设备当前未运行。
主电源设备 (PWR)	呈绿色稳定亮起	主电源设备当前运行正常。
	不亮	主电源设备当前未运行。
	呈红色亮起	主电源设备出现故障

硬件组件

电源设备

该设备具有一个内部电源装置（交流装置），并带有一个连接器，可以将该设备连接至外部电源装置（直流装置）。外部装置提供冗余，被称为 RPS 装置。要使设备通电，仅需要一个电源设备。使用两个电源装置的运行通过负载共享进行调节。

负载共享就是在需要设备电源的位置在两个电源设备之间分配电源。如果一个电源设备断电，第二个电源设备将自动继续为整个设备供电。

电源设备 LED 表明电源设备的状态。有关 LED 的详细信息，请参阅“LED 定义”。

交流电源装置

交流电源装置将标准的 220/110V、50/60 Hz 交流电转换为 5V、5A 或 12V、3A 的直流电。该装置将自动侦听可用的电压额定值（110 或 220V），不需要设置。

交流电源装置使用标准的 AC220/110V 连接器。LED 指示灯位于前面板上，它可以表明交流装置是否已连接。

直流电源装置

外部直流电源装置用作冗余电源装置。仅通过该装置供电，设备就可运行。使用 RPS600 连接器类型。不需要进行配置。LED 指示灯位于前面板上，它可以表明直流装置是否已连接。

如果设备连接至不同的电源，则电源断电导致出现故障的可能性将会下降。

重启动按钮

重启动按钮位于前面板上，可用其手动重新启动设备。

通风系统

该设备使用风扇系统进行冷却。风扇运行状态可以通过观察 LED 来验证，它可以表明风扇是否出现故障。有关信息，请参阅“LED 定义”。

返回目录页面

返回目录页面

安装 PowerConnect 设备

Dell™ PowerConnect™ 5324 系统用户指南

本节包含了有关设备打开包装、定位、安装和电缆连接的信息。

安装注意事项

警告 在执行以下任何步骤之前，请阅读并遵循 Dell 说明文件中包含的《系统信息指南》中的安全说明。

警告 在执行本节中的步骤之前，请遵守以下几点措施：

- 请确保放置设备的机架或机柜足够稳固，以防止设备不稳固和/或跌落。
- 请确保电源电路正确接地。
- 仔细查看并遵守维修标记。请勿维修任何设备，除非系统说明文件另有说明。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。
- 请确保电源电缆、延长电缆和/或插头未损坏。
- 请确保设备未被水沾湿。
- 请确保设备未暴露在有暖气片和/或热源的地方。
- 请确保冷却通风孔未被堵塞。
- 请勿将其它物品塞入设备，否则可能会导致火灾或触电。
- 仅将设备与许可的设备配合使用。
- 待设备冷却后再卸下护盖或触摸内部设备。
- 请确保设备的电源电路、电缆和过电流保护未过载。要确定供电电路过载的可能性，请将与该设备安装在同一电路中的所有交换机的额定安培值相加。将该总值与电路的额定限制值相比较。
- 请勿将设备安装在周围运行温度可能超过 40ºC (122ºF) 的环境中。
- 请确保设备的正面、侧面和背面通风良好。

现场要求

设备可以安装在标准的 19 英寸机架中或放置在桌面上。在安装设备之前，请验证所选的安装位置符合现场要求。

- 一般要求 — 确保电源设备已正确安装。
- 电源要求 — 在距可方便插拔的电源插座（220/110 VAC，50/60 Hz）1.5 m（5 英尺）的范围内安装设备。
- 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 40ºC（32 到 104ºF），相对湿度为 10% 到 90%，非冷凝。请验证水或湿气无法进入装置外壳。

打开包装

套件内容

打开设备的包装时，请确保包含以下项目：

- 设备
- 交流电源电缆
- RS-232 绞接电缆
- 自粘橡皮垫
- 用于机架安装的机架安装套件
- 说明文件 CD

打开设备的包装

要打开设备的包装，请：

注：打开设备的包装之前，请检查包装，如有损坏立即报告。

注：未提供 ESD 腕带，但是建议您在执行以下步骤时戴上腕带。

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

安装设备

概览

设备的电源连接器位于背面板上。连接直流冗余电源设备 (UPS) 为可选操作，但是建议您执行此操作。UPS 直流连接器位于设备的背面板上。

安装系统

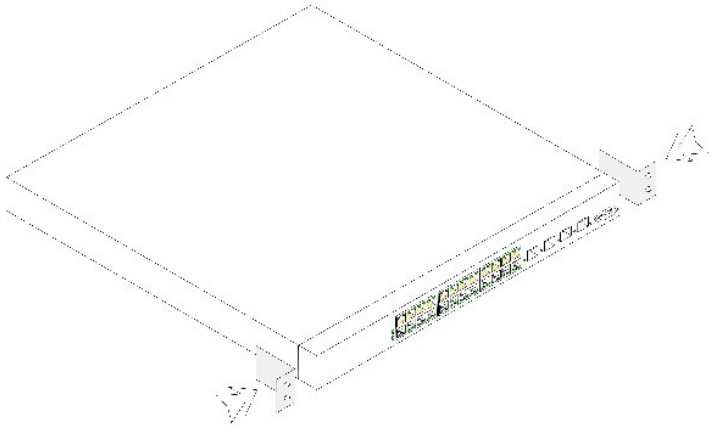
设备机架安装

警告：在机架或机柜中安装设备之前，请从装置上断开所有电缆的连接。

警告：将多个设备安装在机架中时，请按照从下到上的顺序安装设备。

1. 将附带的机架固定支架放在设备的一侧，确保设备上的安装孔与机架固定支架上的安装孔对齐。图 3-9 说明了安装支架的位置。

图 3-9. 连接机架固定支架



2. 将附带的螺钉插入机架安装孔，并用螺丝刀拧紧。
3. 重复此过程，以安装设备另一侧的机架固定支架。
4. 将装置放入 19 英寸机架中，确保设备上的机架安装孔与机架上的安装孔对齐。
5. 用机架螺钉（未提供）将装置固定到机架中。先拧紧下部的一对螺钉，然后再拧紧上部的一对螺钉。这可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。

不使用机架安装设备

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

1. 安装随设备提供的橡皮支脚。
2. 将设备放置在平面上，在两侧各留出 2 英寸 (5.08 cm) 的空间，并在背面留出 5 英寸 (12.7 cm) 的空间。
3. 确保设备能够正常通风。

连接设备

要配置设备，必须将设备连接至终端。

将设备连接至终端

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

要使用控制台端口，需要满足以下要求：

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

要将终端连接至设备控制台端口，请执行以下操作：

1. 将 RS-232 绞接电缆连接至运行 VT100 终端仿真软件的终端。
2. 请确保按照以下步骤设置终端仿真软件：
   a. 选择相应的串行端口（串行端口 1 或串行端口 2），以连接至控制台。
   b. 将数据速率设置为 9600 波特。
   c. 将数据格式设置为 8 个数据位、1 个停止位以及无奇偶校验。
   d. 将流控制设置为无。
   e. 在“**Properties**”（**属性**）下，选择“**VT100 for Emulation**”（**VT100 仿真**）模式。

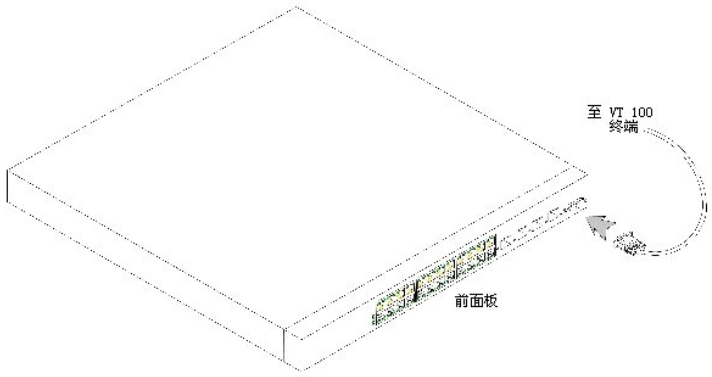
f. 选择“**Terminal keys**”（**终端键**）作为“**Function, Arrow, and Ctrl keys**”（**功能键、箭头键和 Ctrl 键用作**）的设置。确保此设置为“**Terminal keys**”（**终端键**）（而不是“**Windows keys**”[**Windows 键**]）。

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

3. 将 RS-232 绞接电缆的内孔连接器直接连接至设备控制台端口，并拧紧固定螺钉。

设备控制台端口位于前面板上。

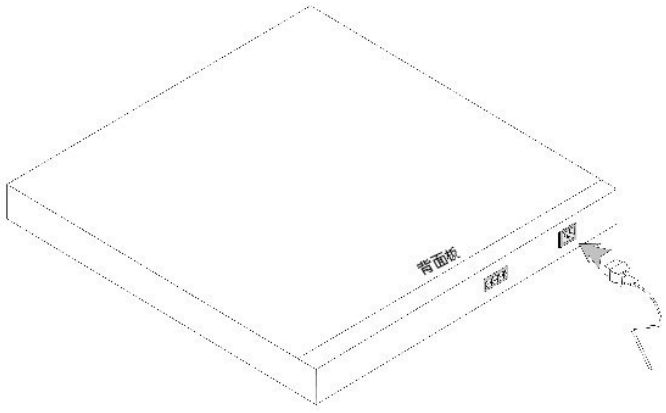
图 3-10. 连接至 PowerConnect 5324 控制台端口



将设备连接至电源设备

1. 使用已安全接地的 5 英尺 (1.5 m) 标准电源电缆，将电源电缆连接至位于背面板上的交流电源连接器。
2. 将电源电缆连接至接地的交流电源插座。

图 3-11. 连接至设备电源连接器



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。

端口连接、电缆和插针输出信息

本节说明了设备的物理接口，并提供了有关端口连接的信息。连接器类型、端口和电缆在“端口、连接器和电缆”中进行了概括。支持铜质电缆和光收发机诊断程序。

用于连接 10/100/1000BaseT 端口的 RJ-45

10/100/1000BaseT 端口是铜质双绞线端口。

要为双绞线端口建立链接，必须将电缆一端的 Tx 对与另一端的 Rx 对相连接，反之亦然。如果布线的方式为将一端的 Tx 连接至另一端的 Tx，并且将 Rx 连接至 Rx，则未建立链接。

选择使用电缆将设备端口连接至其网络同级时，必须使用直通电缆将设备连接至工作站，并且必须使用绞接电缆将一个传输设备（交换机或集线器）连接至另一个传输设备。直通电缆和绞接电缆均为 5 类电缆。

连接了端口后，其链路 LED 指示灯将亮起。

表 3-4. 端口、连接器和电缆

连接器	端口/接口	电缆
RJ-45	10/100/1000BaseT 端口	5 类

10/100/1000BaseT 端口的 RJ-45 插针编号的分配情况列在下表中。

表 3-5. 10/100/1000BaseT 以太网端口的 RJ-45 插针编号的分配情况

插针编号	功能
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx 3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

端口默认设置

配置设备端口的一般信息包括对自适应机制的简短说明和交换端口的默认设置。

自适应

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

自适应是两个链接伙伴之间建立的机制，使一个端口可以将其传输速率、双工模式和流控制（默认情况下，流控制被禁用）能力通知给伙伴端口。然后两个端口以二者之间的最高共同标准运行。

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

如果链路另一端的站点尝试与配置为全双工的设备 10/100/1000BaseT 端口自适应，则自适应将导致此站点尝试以半双工运行。

MDI/MDIX

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

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

流控制

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

背压

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

交换端口默认设置

下表介绍了端口的默认设置。

表 3-6. 端口默认设置

功能	默认设置
端口速率和模式	10/100/1000BaseT 铜质端口：自适应 100 全双工
端口传输状态	已启用
端口标记	无标记
流控制	关闭（在入口被禁用）
背压	关闭（在入口被禁用）

返回目录页面

返回目录页面

简介

Dell™ PowerConnect™ 5324 系统用户指南

注意：首先，请阅读本产品的版本注释。您可以从 support.dell.com 下载版本注释。

本用户指南介绍有关安装、配置和维护 PowerConnect 设备的信息。

PowerConnect 5324

PowerConnect 5324 具有 24 吉位以太网端口。另外，还有四个 SFP 光纤端口，可以指定作为代替以太网端口 21-24 的组合端口。启用一个物理连接时，另一个将被禁用。

图 1-1 和图 1-2 分别说明了 PowerConnect 5324 的前面板和背面板。

图 1-1. PowerConnect 5324 前面板

图 1-2. PowerConnect 5324 背面板

功能

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

一般功能

队列头阻塞

队列头 (HOL) 阻塞会导致由于通信竞争同一出口端口资源而引起的通信延迟和帧丢失。HOL 阻塞会对信息包进行排队，队列头部的信息包将在队列尾部的信息包之前被传输。

虚拟电缆测试 (VCT)

VCT 用于检测和报告铜质链接线路中的故障（例如断路和短路）。

超长帧支持

超长帧可以使传输相同的数据所需的帧数少一些。从而减少开销、处理时间和中断。

有关启用超长帧的信息，请参阅“定义一般设备信息”。

MDI/MDIX 支持

设备支持绞接电缆和直通电缆之间的自动检测。

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

有关为端口或链路聚合组(LAG)配置 MDI/MDIX 的信息，请参阅“定义端口参数”或“定义 LAG 参数”。

流控制支持 (IEEE 802.3X)

流控制通过请求高速设备抑制发送信息包，从而使低速设备可以与高速设备进行通信。传输会暂时中止，以防止缓冲区溢出。

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

背压支持

在半双工链路中，接收端口通过占用链路以使其不能用于其它通信来防止缓冲区溢出。

有关为端口或 LAG 配置背压的信息，请参阅“定义端口参数”或“定义 LAG 参数”。

支持 MAC 地址的功能

MAC 地址容量支持

设备最多支持八千个 MAC 地址。设备保留了供系统使用的特定 MAC 地址。

自学习 MAC 地址

设备允许从传入信息包自动学习 MAC 地址。MAC 地址存储在桥接表中。

自动管理 MAC 地址的存在时间

在给定时间段内没有接收到其通信的 MAC 地址将会过期。这会防止桥接表溢出。

有关配置 MAC 地址过期时间的详细信息，请参阅“配置地址表”。

静态 MAC 条目

用户定义的静态 MAC 条目存储在**桥接表**中。

有关详情，请参阅“配置地址表”。

可识别 VLAN 的基于 MAC 的交换

来自未知源地址的信息包将被发送至微处理器，在微处理器中源地址会被添加至硬件表。从而通过硬件表使发往或来自该地址的信息包能够更有效地传输。

MAC 多点传送支持

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

有关详情，请参阅“多点传送支持”。

第 2 层功能

IGMP 监测

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

有关详情，请参阅“IGMP 监测”。

端口镜像

通过将传入和传出信息包的副本从一个被监测端口传输至监测端口，端口镜像可以监测和镜像网络通信。用户可以指定由哪个目标端口接收经由指定源端口所有通信的副本。

有关详情，请参阅“定义端口镜像会话”。

广播风暴控制

风暴控制用于限制设备接收和传输的多点传送帧和广播帧的数量。

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

有关详情，请参阅“启用风暴控制”。

支持 VLAN 的功能

VLAN 支持

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

有关详情，请参阅“配置 VLAN”。

基于端口的虚拟 LAN (VLAN)

基于端口的 VLAN 根据传入信息包的入口端口将其分类至不同 VLAN。

有关详情，请参阅“定义 VLAN 端口设置”。

基于 IEEE802.1V 协议的虚拟 LAN (VLAN)

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

有关详情，请参阅“定义 VLAN 协议组”。

完全兼容 802.1Q VLAN 标记

IEEE 802.1Q 定义了虚拟桥接 LAN 的体系结构、VLAN 中提供的服务以及提供这些服务所涉及的协议和算法。此标准中包含的一项重要要求是能够用所需的服务级别 (CoS) 标记值 (0-7) 标记帧。

GVRP 支持

GARP VLAN 注册协议 (GVRP) 支持在 802.1Q 主干端口上删减 IEEE 802.1Q 兼容 VLAN 和动态创建 VLAN。启用 GVRP 后，设备将在属于处于活动状态的基础**“生成树协议功能”**拓扑的所有端口上注册和传播 VLAN 成员关系。

有关详情，请参阅“配置 GVRP”。

生成树协议功能

生成树协议 (STP)

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

有关详情，请参阅“配置生成树协议”。

快速链路

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

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

IEEE 802.1w 快速生成树

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

有关详情，请参阅“配置快速生成树”。

链路聚合

有关详情，请参阅“聚合端口”。

链路聚合

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

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

LAG 由具有相同速率并被设置为全双工运行的端口组成。

有关详情，请参阅“定义 LAG 成员关系”。

链路聚合和 LACP

在不中断的基础上，LACP 在链路中使用同级交换以确定不同链路的聚合功能，并不断在给定的一对系统之间提供可以获得的最高级别的聚合功能。LACP 自动确定、配置、捆绑和监测系统内捆绑至聚合器的端口。

有关详情，请参阅“定义 LACP 参数”。

第 3 层功能

地址解析协议 (ARP)

ARP 是一个用于将 IP 地址转换为物理地址的 TCP/IP 协议。ARP 自动确定系统（包括直接连接的终端系统）的设备下一跳级 MAC 地址。用户可以通过定义其它 ARP 表条目来代替和补充此设置。

有关详情，请参阅“映射域主机”。

TCP

传输控制协议 (TCP) 连接通过初始同步交换在 2 个端口之间进行定义。TCP 端口由一个 IP 地址和一个 16 位端口号来标识。八位位组流将被分成多个 TCP 信息包，每个信息包带有一个序列号。

BootP 和 DHCP 客户端

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

有关 DHCP 的详细信息，请参阅“定义 DHCP IP 接口参数”。

服务质量功能

服务级别 802.1p 支持

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

有关详情，请参阅“配置服务质量”。

设备管理功能

SNMP 警报和陷阱日志

系统用严重性代码和时间戳来记录事件。事件将作为简单网络管理协议 (SNMP) 陷阱被发送至陷阱接收列表。

有关 SNMP 警报和陷阱的详细信息，请参阅“定义 SNMP 参数”。

SNMP 版本 1 和版本 2

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

基于 Web 的管理

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

配置文件下载和加载

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

有关详情，请参阅“管理文件”。

小型文件传输协议 (TFTP)

设备支持通过 TFTP 加载/下载引导映像、软件和配置。

远程监测

远程监测 (RMON) 是对 SNMP 的扩展，它使网络通信监测功能更加全面（相对于允许网络设备管理和监测的 SNMP）。RMON 是一种标准的 MIB，它定义了当前和历史 MAC 层统计数据和控制对象，使得可以从整个网络中捕获实时信息。

有关详情，请参阅“查看 RMON 统计数据”。

命令行界面

命令行界面 (CLI) 的语法和语义尽可能地符合业界惯例。CLI 由必要元素和可选元素组成。CLI 解释器提供命令和关键字自动完成功能，可以帮助用户并减少输入量。

系统日志

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

有关系统日志的详细信息，请参阅“管理日志”。

SNTP

简单网络时间协议 (SNTP) 可以确保精确到毫秒的网络设备时钟时间同步。时间同步由网络 SNTP 服务器来执行。时间源通过时间服务器来建立。时间服务器定义与参考时钟的时间差。时间服务器越高（最高为零），时钟越准确。

有关详情，请参阅“配置 SNTP 设置”。

Traceroute

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

安全保护功能

SSL

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

基于端口的验证 (802.1x)

基于端口的验证启用通过外部服务器针对各个端口验证系统用户。只有经过验证和许可的系统用户才可以传输和接收数据。使用可扩展验证协议 (EAP)，通过远程验证拨入用户服务 (RADIUS) 服务器来验证端口。

有关详情，请参阅“配置基于端口的验证”。

锁定端口支持

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

有关详情，请参阅“配置端口安全保护”。

RADIUS 客户端

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

有关详情，请参阅“配置 RADIUS 全局参数”。

SSH

安全命令解释程序 (SSH) 是一个提供了到设备的安全远程连接的协议。SSH 版本 1 为当前可用版本。SSH 服务器特性使 SSH 客户端可以建立与设备的安全加密连接。此连接所提供的功能类似于入站的 Telnet 连接。SSH 使用 RSA 公用密钥加密法进行设备连接和验证。

TACACS+

TACACS+ 为访问设备的用户的验证提供了集中式的安全保护。TACACS+ 提供了集中式的用户管理系统，同时还保持了与 RADIUS 和其它验证过程的一致性。

有关详情，请参阅“定义 TACACS+ 设置”。

附加 CLI 说明文件

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

返回目录页面

返回目录页面

配置服务质量

Dell™ PowerConnect™ 5324 系统用户指南

本节介绍了定义和配置服务质量 (QoS) 参数的信息。要打开“Quality of Service”（服务质量）页面，请单击“Home”（主页）→“Quality of Service”（服务质量）。

服务质量 (QoS) 概览

服务质量 (QoS) 提供了实现 QoS 和网络内部优先级排队的能力。QoS 基于规则、帧计数器和环境来提高网络通信流量。

一个实现示例需要 QoS 包含某些类型的、可以分配到高优先级队列的通信（例如语音通信、视频通信和实时通信），而其它通信则可以分配到较低优先级队列。这样做的结果是提高了高需求通信的通信流量。

QoS 由以下因素定义：

- 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]）。

VPT 标记分类信息

VLAN 优先级标记用于通过将信息包映射到其中一个输出队列来对信息包进行分类。VLAN 优先级标记至队列的分配也可以由用户定义。下表详细说明了 VPT 至队列的默认设置：

表 9-92. CoS 至队列映射表默认值

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	q3
5	q3
6	q4（最高优先级）
7	q4（最高优先级）

到达的未标记信息包被分配了一个针对每个端口设置的默认 VPT。分配的 VPT 用于将信息包映射至输出队列并用作外出 VPT。

可以将 DSCP 值映射到优先级队列。下表包含了映射至传输队列的 DSCP 默认值：

表 9-93. DSCP 至队列映射表默认值

DSCP 值	传输队列值
0-7	q2（最低优先级）
8-15	q1
16-23	q1
24-31	q2
32-39	q3

40-47	q3
48-55	q4
55-63	q4（最高优先级）

DSCP 映射是针对每个系统进行启用的。

CoS 服务

信息包被分配到特定队列后，可以为此队列设定 CoS 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。严格优先级使您可以排定任务关键、与时间密切相关的通信的优先级，使其高于与时间相关度较低的应用程序的优先级。
  例如，在严格优先级下，通过 IP 的语音通信会先于 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。
- 加权轮循 — 确保单个应用程序不会控制设备的传输能力。加权轮循 (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。
  通过为长度 4 队列提供最高传输优先级，加权轮循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 值可以针对整个系统进行设定。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。

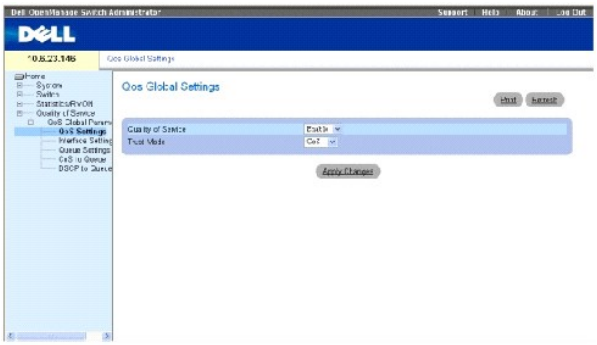
定义 CoS 全局参数

在**“CoS Global Parameter”（CoS 全局参数）**页面中可以设置服务级别全局参数。

配置 QoS 全局设置

“QoS Global Settings”（QoS 全局设置）页面包含用于启用或禁用 QoS 的字段。此外，您还可以选择“Trust”（信任）模式。信任模式根据信息包中预定义的字段来确定输出队列。要打开**“QoS Settings”（QoS 设置）**页面，请在树视图中单击**“Quality of Service”（服务质量）→“CoS Global Parameters”（CoS 全局参数）→“CoS Settings”（CoS 设置）**。

图 9-130. QoS 设置



“Quality of Service”（服务质量）— 启用或禁用使用服务质量管理网络通信。

“Trust Mode”（信任模式）— 确定用于对进入设备的信息包进行分类的信息包字段。如果未定义规则，则将根据相关的信任模式表映射包含预定义信息包字段（CoS 或 DSCP）的通信。不包含预定义信息包字段的通信将被映射为最佳传输能力。可能的**“Trust Mode”（信任模式）**字段值包括：

“CoS”— 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” — 输出队列的分配由 DSCP 字段确定。

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 Settings”（QoS 设置）**页面。
2. 在**“CoS Mode”（CoS 模式）**字段中选择**“Enable”（启用）**。
3. 单击**“Apply Changes”（应用更改）**。

设备上将启用**“Class of Service”（服务级别）**。

启用信任：

1. 打开**“QoS Settings”（QoS 设置）**页面。
2. 在**“Trust Mode”（信任模式）**字段中选择**“Trust”（信任）**。
3. 单击**“Apply Changes”（应用更改）**。

设备上将启用信任。

使用 CLI 命令启用信任

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

表 9-94. CoS 设置 CLI 命令

CLI 命令	说明
qos trust [**cos** | **dscp**]	将系统配置为基本模式和“信任”状态。
no cos trust	恢复为非信任状态。

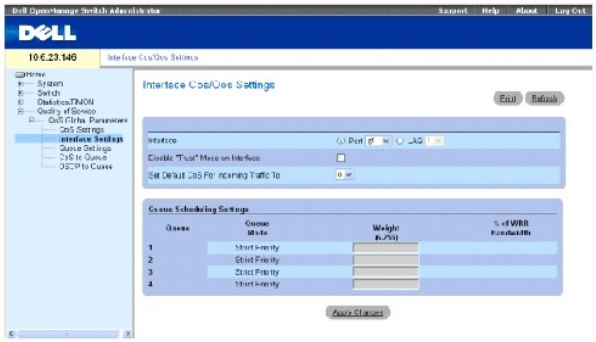
以下是 CLI 命令的示例：

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

定义 QoS 接口设置

“Interface Cos/QoS Settings”（接口 Cos/QoS 设置）页面包含用于针对每个接口定义是否要激活选定的信任模式的字段。在**“Interface Cos/QoS Settings”（接口 Cos/QoS 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，请在树视图中单击**“Quality of Service”（服务质量）→“CoS Global Parameters”（CoS 全局参数）→“Interface Settings”（接口设置）**。

图 9-131. 接口 Cos/QoS 设置



“Interface”（接口）— 要配置的特定端口或 LAG：

“Disable 'Trust' Mode on Interface”（在接口上禁用“信任”模式）— 在指定接口上禁用信任模式。此设置将代替设备上全局配置的“Trust”（信任）模式。

“Set Default CoS For Incoming Traffic To”（将传入通信的默认 CoS 设置为）— 设置未标记信息包的默认 CoS 标记值。CoS 标记值为 0 至 7。默认值为 0。

“Queues”（队列）— 队列号。

“Queue Mode”（队列模式）— 表明队列是**“Strict Priority”（严格优先级）**还是“WRR”。在**“Queue Settings”（队列设置）**屏幕中定义了该模式。

- 可以在所有队列 1 至 4 上配置 SP。
- 可以在所有队列 1 至 4 上配置 WRR。
- 可以在队列 1 至 2 上配置 SP 模式，在队列 3 至 4 上配置 WRR。
- 可以在队列 1 至 2 上配置 WRR 模式，在队列 3 至 4 上配置 SP。

“Weight (6-255)”（加权 [6-255]）— 为队列分配 WRR 加权。仅对处于 WRR 队列模式的队列启用此字段。

“% of WRR Bandwidth”（WRR 带宽百分比）— 将“Weight **(6-255)**”（加权 **[6-255]**）字段中定义的加权进行转换的百分比。

为接口设定 QoS/CoS 设置：

1. 打开**“Interface Cos/QoS Settings”（接口 Cos/QoS 设置）**页面。
2. 在**“Interface”（接口）**字段中选择接口。
3. 定义字段。
4. 单击**“Apply Changes”（应用更改）**。

接口将设定 CoS 设置。

使用 CLI 命令设定 CoS 接口

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

表 9-95. CoS 接口 CLI 命令

CLI 命令	说明
qos trust	为每个端口启用信任状态。

qos cos default-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。

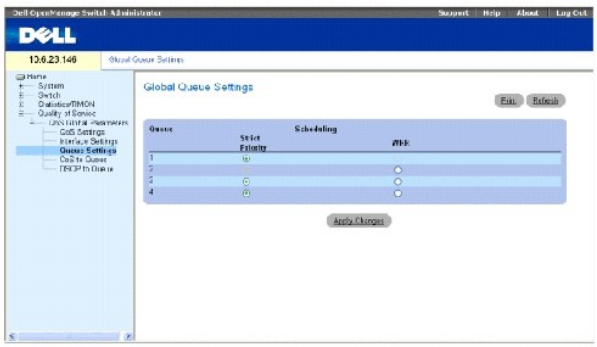
以下是 CLI 命令的示例：

```
Console (config)# interface ethernet g5

Console (config-if)# qos trust

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

定义队列设置

“Global Queue Setting”（全局队列设置）页面包含用于配置维护队列的安排方法的字段。要打开“Global Queue Setting”（全局队列设置）页面，请在树视图中单击“Quality of Service”（服务质量）→“CoS Global Parameters”（CoS 全局参数）→“Queue Settings”（队列设置）。

图 9-132. 全局队列设置



“Queues”（队列）— 队列号。

“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” — 指定是否基于加权轮循 (WRR) 加权为外出队列安排通信。

定义队列设置

1. 打开“Global Queue Setting”（全局队列设置）页面。
2. 定义字段。
3. 单击**“Apply Changes”（应用更改）**。

队列设置将被定义，并更新设备。

使用 CLI 命令指定队列设置

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

表 9-96. 队列设置 CLI 命令

CLI 命令	说明
wrr-queue bandwidth weight1 weight2 . weight_n	为外出队列分配加权轮循 (WRR) 加权。
show qos interface [**ethernet 接口号**] [queuing]	显示接口 QoS 数据。

以下是 CLI 命令的示例：

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


Console (config)# exit


Console # exit


Console> show qos
interface ethernet g1
queueing


Ethernet g1


wrr bandwidth weights and
EF priority:
```

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


Console (config)# exit


Console # exit


Console> show qos
interface ethernet g1
queueing


Ethernet g1


wrr bandwidth weights
and EF priority:
```

qid	weights	Ef	Priority
1	125	Disable	N/A
2	125	Disable	N/A
3	125	Disable	N/A
4	125	Disable	N/A

Cos queue map:

Cos qid

0 2

1 1

2 1

3 2

4 3

5 3

6 4

7 4

将 CoS 值映射到队列

“CoS to Queue Mapping Table”（CoS 至队列映射表）页面包含用于将 CoS 设置分类到通信队列的字段。要打开“CoS to Queue Mapping Table”（CoS 至队列映射表）页面，请在树视图中单击“Quality of Service”（服务质量）→“CoS Global Parameters”（CoS 全局参数）→“CoS to Queue”（CoS 至队列）。

图 9-133. CoS 至队列映射表

“Class of Service”（服务级别）— 指定 CoS 优先级标记值，其中零为最低值，7 为最高值。

“Queue”（队列）— CoS 优先级要映射到的通信传输队列。支持四个通信优先级队列。

“Restore Defaults”（恢复默认设置）— 恢复将 CoS 值映射到传输队列的设备出厂默认设置。

将 CoS 值映射到队列

1. 打开**“CoS to Queue Mapping Table”（CoS 至队列映射表）**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**“CoS to Queue Mapping Table”（CoS 至队列映射表）**页面中字段的等效 CLI 命令。

表 9-97. CoS 至队列设置 CLI 命令

CLI 命令	说明
wrr-queue cos-map queue-id cos1..cos8	将设定的 CoS 值映射到外出队列。

以下是 CLI 命令的示例：

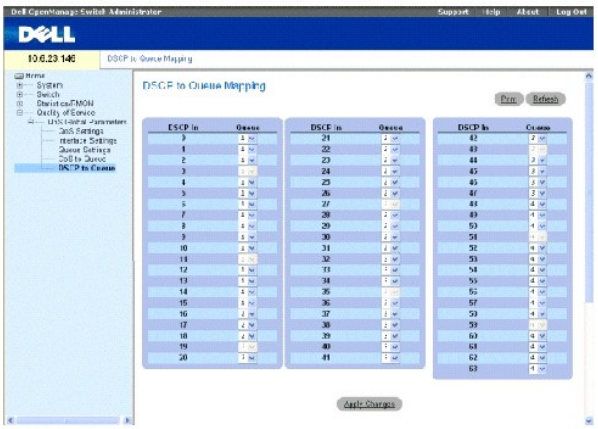
```
Console (config)# wrr-queue
cos-map 4 7
```

将 DSCP 值映射到队列

“DSCP Mapping”（DSCP 映射）页面提供了用于将输出队列定义至特定 DSCP 字段的字段。要打开**“DSCP Mapping”（DSCP 映射）**页面，请在树视图中单击**“Quality of Service”（服务质量）→“CoS Global Parameters”（CoS 全局参数）→“DSCP Mapping”（DSCP 映射）**。

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”。

图 9-134. DSCP 映射



“DSCP In”（DSCP 位于）— 传入信息包中 DSCP 字段的值。

“Queue”（队列）— 具有特定 DSCP 值的信息包将要分配到的队列。值包括 1 至 4，其中 1 为最低值，4 为最高值。

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 将被覆盖，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。

表 9-98. 队列 CLI 命令的 DSCP 值

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

以下是 CLI 命令的示例：

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

返回目录页面

返回目录页面

设备规格

Dell™ PowerConnect™ 5324 系统用户指南

本附录包含运行设备所需的信息。

端口和电缆规格

本节介绍了端口规格。

端口规格

下表介绍了设备端口类型及端口类型的说明。

表 10-99. 端口规格

设备	规格
PowerConnect 5324	• 24 个 GE 端口 • 4 个 SFP 端口 • RS-232 控制台端口
端口类型	
RJ-45	• 10 Base-T • 100 Base-T • 1000 Base-T
SFP	支持标准超小型 吉位插入式收发机
端口设置	
	• 速率、双工模式和流控制自适应 • 背压 • 队列阻塞 • 自动 MDI/MDIX • 端口镜像 • 广播风暴控制

运行条件

本节详细介绍了包含运行时的温度和湿度的运行条件。

表 10-100. 运行条件

特性	规格
运行时的温度	0 至 40 C（32 至 104 F）
运行时的湿度	10% 至 90%（非冷凝）

设备物理规格

本节详细介绍了包含运行时的温度和湿度的运行条件。

表 10-101. 设备物理规格

特性	规格
装置大小	• 宽度为 19" • 高度为 1U
通风	每个装置配备两个风扇。

设备存储器规格

本节详细介绍了设备存储器规格。

表 10-102. 设备存储器规格

存储器类型	容量
CPU DRAM	64MB
快擦写存储器	16MB
信息包缓冲区存储器	2Mb

功能规范

VLAN

- 按照 IEEE 802.1Q 基于标记和端口的 VLAN 支持
- 最多支持 4094 个 VLAN
- 供内部系统使用的保留 VLAN
- 具有 GVRP 支持的动态 VLAN
- 基于协议的 VLAN

服务质量

- 第 2 层信任模式（IEEE 802.1p 标记）
- 第 3 层信任模式 (DSCP)
- 可调整加权轮循 (WRR)
- 可调整严格队列安排

第 2 层多点传送

- 动态多点传送支持 — IGMP 监测或静态多点传送时最多支持 256 个多点传送组

设备安全保护

- 交换机访问密码保护
- 基于端口的 MAC 地址警报和锁定
- 用于交换机管理访问的 RADIUS 远程验证
- TACACS+
- 通过管理访问配置文件进行管理访问筛选

- SSH/SSL 管理加密

附加的交换功能

- 链路聚合，每台设备最多支持 8 个聚合链路，每个聚合链路 (IEEE 802.3ad) 最多支持 8 个端口
- LACP 支持
- 支持超长帧（最大 10K）
- 广播风暴控制
- 端口镜像

设备管理

- 基于 Web 的管理界面
- 通过 Telnet 可以访问 CLI
- 支持 SNMPv1 和 SNMP v2
- 支持 4 个 RMON 组
- 固件和配置文件的 TFTP 传输
- 机载双固件映像
- 支持多个配置文件的加载/下载
- 错误监测和性能优化统计数据
- 支持 BootP/DHCP IP 地址管理
- 系统日志远程记录功能
- SNTP 支持
- 第 3 层 Traceroute
- Telnet 客户端
- DNS 客户端

返回目录页面

返回目录页面

配置设备信息

Dell™ PowerConnect™ 5324 系统用户指南

本节介绍了有关配置网络安全保护、端口、地址表、GARP、VLAN、生成树、端口聚合和多点传送支持的所有系统操作和一般信息。

配置网络安全保护

该设备通过存取控制表和锁定端口启用网络安全保护。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**）。

网络安全保护概览

本节介绍了网络安全保护功能。

基于端口的验证 (802.1x)

基于端口的验证可以通过外部服务器针对每个端口验证系统用户。只有经验证和经批准的系统用户才可以传输和接收数据。端口通过 RADIUS 服务器使用扩展验证协议 (EAP) 进行验证。端口验证包括：

- 验证方 — 指定允许系统访问之前要验证的端口。
- 申请方 — 指定连接至请求访问系统服务的经验证端口的主机。
- 验证服务器 — 指定外部服务器（例如，代表验证方执行验证的 RADIUS 服务器），并表明是否已授权用户可以访问系统服务。

基于端口的验证将创建两种访问状态：

- 受控制的访问 — 如果用户已经过授权，则允许该用户和系统之间进行通信。
- 不受控制的访问 — 不管端口的状态如何，都允许不受控制的通信。

该设备目前通过 RADIUS 服务器支持基于端口的验证。

基于端口的高级验证

基于端口的高级验证使多台主机可以连接至单个端口。基于端口的高级验证只需要授权一台主机，就可以使所有主机都具有系统访问权限。如果该端口未经授权，则将会拒绝连接的所有主机对网络进行访问。

基于端口的高级验证还启用基于用户的验证。设备中的特定 VLAN 始终可用，即使连接至 VLAN 的特定端口未经授权。例如，通过 IP 传输语音不需要验证，而数据通信需要验证。可以定义不需要授权的 VLAN。用户可以使用未经验证的 VLAN，即使连接至 VLAN 的端口被定义为授权。

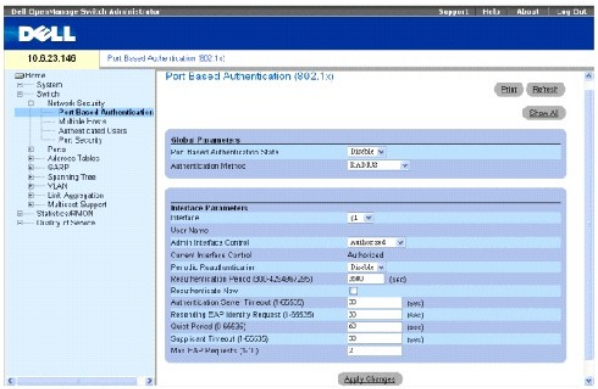
使用以下模式可以实现基于端口的高级验证：

- **一台主机模式** — 只允许授权的主机访问端口。
- **多台主机模式** — 允许多台主机连接至单个端口。必须只授权一台主机，就可以使所有主机都访问网络。如果该主机验证失败或接收到一条 EAPOL 注销信息，则将会拒绝连接的所有客户端对网络进行访问。

配置基于端口的验证

“Port Based Authentication”（基于端口的验证）页面包含用于配置基于端口的验证的字段。要打开**“Port Based Authentication”（基于端口的验证）**页面，请单击**“Switch”（交换机）→“Network Security”（网络安全保护）→“Port Based Authentication”（基于端口的验证）**。

图 7-80. 基于端口的验证



“Port Based Authentication State”（基于端口的验证的状态） — 在设备上允许进行基于端口的验证。可能的字段值包括：

“Enable”（启用）— 在设备上启用基于端口的验证。

“Disable”（禁用）— 在设备上禁用基于端口的验证。

“Authentication Method”（验证方法）— 使用的验证方法。可能的字段值包括：

“None”（无）— 没有用于验证端口的验证方法。

“RADIUS”— 使用 RADIUS 服务器执行端口验证。

“RADIUS, None”（RADIUS，无）— 首先使用 RADIUS 服务器执行端口验证。如果端口未经过验证，则没有验证方法可供使用，将允许会话。

“Interface”（接口）— 包含一个接口列表。

“User Name”（用户名）— 在 RADIUS 服务器中配置的用户名。

“Admin Interface Control”（管理接口控制）— 定义端口授权状态。可能的字段值包括：

“Authorized”（授权）— 将接口状态设置为授权（允许通信）。

“Unauthorized”（未经授权）— 将接口状态设置为未经授权（拒绝通信）。

“Auto”（自动）— 授权状态由授权方法设置。

“Current Interface Control”（当前接口控制）— 当前配置的端口的授权状态。

“Periodic Reauthentication”（定期重新验证）— 如果启用，则会定期重新验证选定端口。重新验证时段在**“Reauthentication Period (300-4294967295)”（重新验证时段 [300-4294967295]）**字段中作了定义。

“Reauthentication Period (300-4294967295)”（重新验证时段 [300-4294967295]）— 表明要重新验证选定端口的时间范围。字段值以秒为单位。字段默认值为 3600 秒。

“Reauthenticate Now”（立即重新验证）— 如果选定该选项，则会允许立即重新验证端口。

“Authentication Server Timeout (1-65535)”（验证服务器超时 [1-65535]）— 定义设备将请求重新发送到验证服务器之前经过的时间。字段值以秒为单位。字段默认值为 30 秒。

“Resending EAP Identity Request (1-65535)”（重新发送 EAP 标识请求 [1-65535]）— 定义重新发送 EAP 请求之前经过的时间。字段默认值为 30 秒。

“Quiet Period (0-65535)”（无提示时段 [0-65535]）— 设备在验证交换失败之后处于无提示状态的秒数。可能的字段范围为 0 至 65535。字段默认值为 60 秒。

“Supplicant Timeout (1-65535)”（申请方超时 [1-65535]）— EAP 请求被重新发送到用户之前经过的时间。字段值以秒为单位。字段默认值为 30 秒。

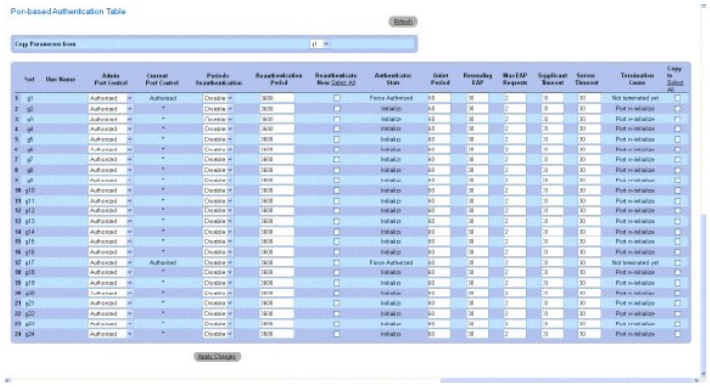
“Max EAP Requests (1-10)”（最大 EAP 请求 [1-10]）— 发送 EAP 请求的总次数。如果在定义的时段后未接收到响应，则验证过程将重新启动。字段默认值为 2，即进行 2 次重试。

显示基于端口的验证表

1. 显示**“Port Based Authentication”（基于端口的验证）**页面。
2. 单击**“Show All”（全部显示）**。

系统将打开**“Port Based Authentication Table”（基于端口的验证表）**：

图 7-81. 基于端口的验证表



“Termination Cause”（终止原因）— 端口验证被终止的原因。

“Copy To”（复制到）复选框 — 将端口参数从一个端口复制到选定的端口。

“Select All”（全部选定）— 选定**“Port Based Authentication Table”（基于端口的验证表）**中的所有端口。

复制**“Port Based Authentication Table”（基于端口的验证表）**中的参数

1. 打开**“Port Based Authentication”（基于端口的验证）**页面。
2. 单击**“Show All”（全部显示）**。

   系统将打开**“Port Based Authentication Table”（基于端口的验证表）**。
3. 在**“Copy Parameters from”（参数复制自）**字段中选择接口。
4. 在**“Port Based Authentication Table”（基于端口的验证表）**中选择一个接口。
5. 选取**“Copy to”（复制到）**复选框以定义基于端口的验证参数要复制到的接口。
6. 单击**“Apply Changes”（应用更改）**。

   系统会将参数复制到**“Port Based Authentication Table”（基于端口的验证表）**中的选定端口，并更新设备。

使用 CLI 命令启用基于端口的验证

下表概述了与**“Port Based Authentication”（基于端口的验证）**页面中显示的用于启用基于端口的验证的选项等效的 CLI 命令。

表 7-49. 端口验证的 CLI 命令

CLI 命令	说明
aaa authentication dot1x default 方法 1 [方法 2]	指定要在运行 IEEE 802.1X 的接口上使用的一种或多种验证、授权和计费 (AAA) 方法。
dot1x max-req 计数	设置设备在重新启动验证过程之前向客户端发送 EAP 的最大次数。
dot1x re-authenticate [ethernet 接口]	手动启动所有启用 802.1X 端口或指定的启用 802.1X 端口的重新验证。
dot1x re-authentication	启用客户端的定期重新验证。
dot1x timeout quiet-period 秒	设置设备在验证交换失败之后处于无提示状态的秒数。
dot1x timeout re-authperiod 秒	设置两次重新验证尝试之间的秒数。
dot1x timeout server-timeout 秒	设置将信息包重新传输到验证服务器的时间。
dot1x timeout supp-timeout 秒	设置将 EAP 请求帧重新传输到客户端的时间。
dot1x timeout tx-period 秒	设置设备重新发送请求之前等待客户端发出的对 EAP - 请求/标识帧的响应的秒数。

show dot1x [ethernet 接口]	显示设备或指定接口的 802.1X 状态。
show dot1x users [username 用户名]	显示设备的 802.1X 用户。

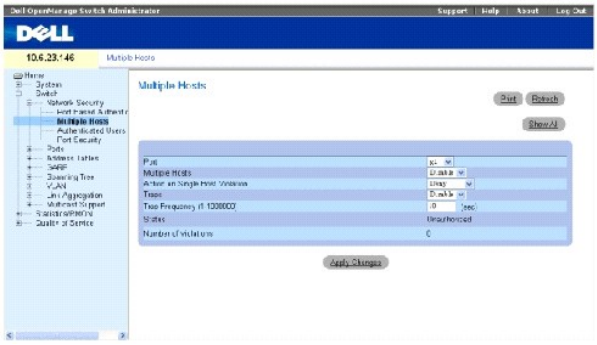
以下是 CLI 命令的示例：

```
console> enable

Console# show dot1x

Interface  Admin Mode  Oper Mode   Reauth Control  Reauth Period  Username
---------  ----------  ----------  --------------  -------------  --------
g1         Auto        Authorized  Ena             3600           Bob
g2         Auto        Authorized  Ena             3600           John
g3         Auto        Unauthorized Ena            3600           Clark
g4         Force-auth  Authorized  Dis             3600           n/a
```

配置基于端口的高级验证

"Multiple Hosts"（多个主机）页面提供了关于为特定端口定义基于端口的高级验证设置的信息。要打开**"Multiple Hosts"（多个主机）**，请单击**"Switch"（交换机）→"Network Security"（网络安全保护）→"Multiple Hosts"（多个主机）**。

图 7-82. 多个主机



"Port"（端口）— 已启用了基于端口的高级验证的端口号。

"Multiple Hosts"（多个主机）— 允许或禁止一台主机可以授权多台主机进行系统访问。必须启用此设置，以便在选定的端口上禁用入口筛选器或使用锁定端口的安全保护。

“Action on Single Host Violation”（单个主机侵入时的措施）— 定义对以单个主机模式到达的信息包所采取的措施，这些信息包来自其 MAC 地址不是客户端（申请方）MAC 地址的主机。仅当**“Multiple Hosts”（多个主机）**字段定义为**“Disable”（禁用）**时，才能定义**“Action on Single Host Violation”（单个主机侵入时的措施）**字段。可能的字段值包括：

“Permit”（允许）— 传输来自未知源的信息包；但是，不记忆 MAC 地址。

“Deny”（拒绝）— 丢弃来自任何未记忆源的信息包。此为默认值。

“Shutdown”（关闭）— 丢弃来自任何未记忆源的信息包，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。

“Traps”（陷阱）— 如果发生侵入，允许或禁止将陷阱发送到主机。

“Trap Frequency (1-1000000) (Sec)”（陷阱频率 [1-1000000] [秒]）— 定义将陷阱发送到主机的时间段。**“Trap Frequency (1-1000000)”（陷阱频率 [1-1000000]）**仅当**“Multiple Hosts”（多个主机）**字段定义为**“Disable”（禁用）**时，才能定义此字段。默认值为 10 秒。

“Status”（状态）— 主机的状态。可能的字段值包括：

“Unauthorized”（未经授权）— 客户端（申请方）有完全端口访问权限。

“Authorized”（授权）— 客户端（申请方）具有有限的端口访问权限。

“No single-host”（非单个主机）—**“Multiple Hosts”（多个主机）**已启用。

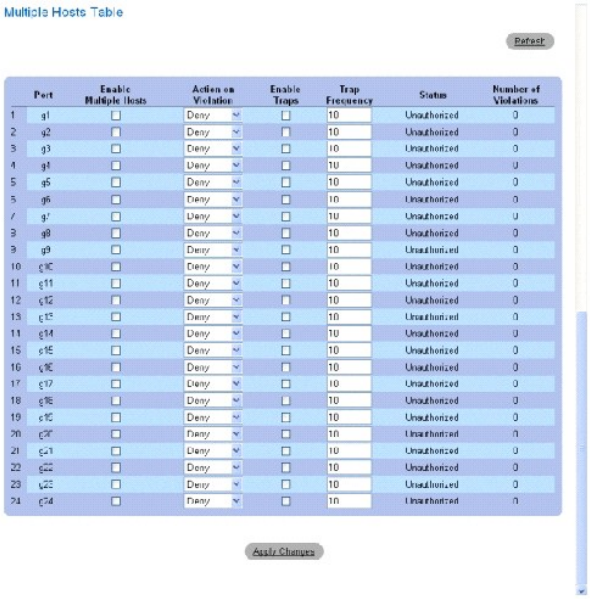
“Number of Violations”（侵入数目）— 以单个主机模式到达接口的信息包的数目，这些信息包来自其 MAC 地址不是客户端（申请方）MAC 地址的主机。

显示多个主机表

1. 打开**“Multiple Hosts”（多个主机）**页面。
2. 单击**“Show All”（全部显示）**。

系统将打开**“Multiple Hosts Table”（多个主机表）**：

图 7-83. 多个主机表



使用 CLI 命令启用多台主机

下表概述了与**“Multiple Hosts”（多个主机）**页面中显示的用于启用基于端口的高级验证的选项等效的 CLI 命令。

表 7-50. 多台主机的 CLI 命令

CLI 命令	说明
dot1x multiple-hosts	在授权 802.1X 的端口上允许多台主机（客户端），该端口将 dot1x 端口控制接口配置命令设置为自动。
dot1x single-host-violation {forward |discard |discard-shutdown}[trap seconds]	如果其 MAC 地址不是客户端（申请方）MAC 地址的站点尝试访问接口时，配置要采取的措施。

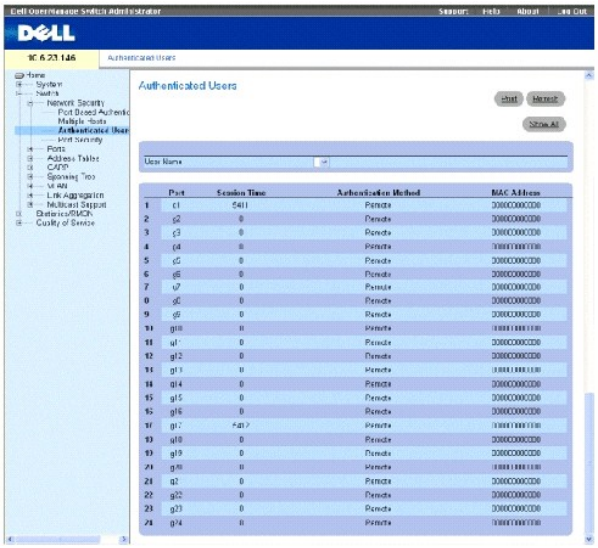
以下是 CLI 命令的示例。

```
Neyland# configure

Neyland(config)# interface
ethernet g1

Neyland(config-if)# dot1x
multiple-hosts
```

验证用户

“Authenticated Users”（经验证的用户）页面显示用户端口访问列表。**“User Access Lists”（用户访问列表）**在**“Add User Name”（添加用户名）**页面中作了定义。要打开**“Authenticated Users”（经验证的用户）**页面，请单击**“Switch”（交换机）→“Network Security”（网络安全保护）→“Authenticated Users”（经验证的用户）**。

图 7-84. 经验证的用户



“User Name”（用户名）— 通过 RADIUS 服务器授权的用户的列表。

“Port”（端口）— 用于验证的端口号 - 针对每个用户名。

“Session Time”（会话时间）— 用户登录到设备的时间。字段格式为**日:小时:分钟:秒**，例如，3 天:2 小时:4 分钟:39 秒。

“Last Authentication”（上次验证）— 用户上次被验证以来经过的时间。字段格式为**日:小时:分钟:秒**，例如，3 天:2 小时:4 分钟:39 秒。

“Authentication Method”（验证方法）— 验证上次会话使用的方法。可能的字段值包括：

“Remote”（远程）— 从远程服务器验证用户。

“None”（无）— 未验证用户。

“MAC Address”（MAC 地址）— 客户端（申请方）MAC 地址。

显示经验证的用户表

1. 打开**“Add User Name”（添加用户名）**页面。
2. 单击**“Show All”（全部显示）**。

系统将打开**“Authenticated Users Table”（经验证的用户表）**：

图 7-85. 经验证的用户表

使用 CLI 命令验证用户

下表概括了与**“Add User Name”（添加用户名）**页面中显示的验证用户选项等效的 CLI 命令。

表 7-51. 添加用户名的 CLI 命令

CLI 命令	说明
show dot1x users [username 用户名]	显示设备的 802.1X 用户。

以下是 CLI 命令的示例：

```
console# show dot1x users

Username   Session Time   Last Auth   Auth Method   MAC Address         Interface
--------   ------------   ---------   -----------   -----------------   ---------
Bob        1d3h           58m         Remote        00:08:3b:79:87:87   g1
John       8h19m          2m          None          00:08:3b:89:31:27   g2
```

配置端口安全保护

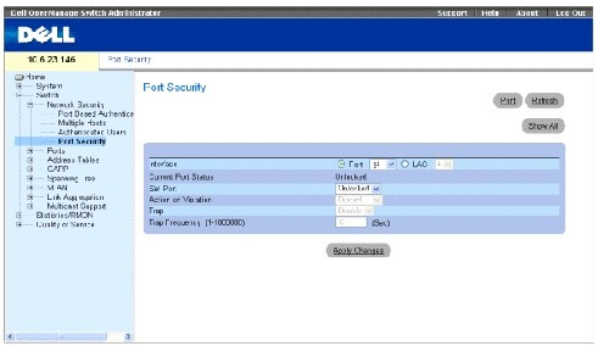
通过将对特定端口的访问权限限制为只有具有特定 MAC 地址的用户可以访问，可以增强网络安全保护。根据以上需求，MAC 地址可以被动态记忆或被静态配置。锁定端口安全保护监测在特定端口上接收的已接收到的信息包和已记忆的信息包。对锁定端口的访问仅限于具有特定 MAC 地址的用户。这些地址可以在端口上手动定义或在锁定端口时在一定程度上在该端口上记忆。如果锁定端口接收到一个信息包，并且该信息包的源 MAC 地址没有与该端口关联（该 MAC 地址被记忆在其它端口上或系统未知此地址），保护机制将被调用，并且保护机制还可以提供各种选项。未经授权的信息包到达锁定端口时保护机制提供的选项为：

- 传输
- 不使用陷阱丢弃
- 使用陷阱丢弃
- 入口端口被禁用

锁定端口安全保护还可以在配置文件中存储 MAC 地址的列表。重启动设备后，可以恢复 MAC 地址列表。

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，请单击**“Switch”（交换机）→“Network Security”（网络安全保护）→“Port Security”（端口安全保护）**。

图 7-86. 端口安全保护



“Interface”（接口）— 要启用锁定端口的选定接口的类型。

“Port”（端口）— 选定的接口类型为端口。

“LAG”— 选定的接口类型为 LAG。

“Current Port Status”（当前端口状态）— 当前配置的端口状态。

“Set Port”（设置端口）— 端口已锁定或已解除锁定。可能的字段值包括：

“Unlocked”（已解除锁定）— 解除端口锁定。此为默认值。

“Locked”（已锁定）— 锁定端口。

“Action on Violation”（侵入措施）— 对到达锁定端口的信息包所采取的措施。可能的字段值包括：

“Forward”（传输）— 传输来自未知源的信息包；但是，不记忆 MAC 地址。

“Discard”（丢弃）— 丢弃来自任何未记忆源的信息包。此为默认值。

“Shutdown”（关闭）— 丢弃来自任何未记忆源的信息包，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）— 当锁定端口接收到信息包时，允许发送陷阱。

“Trap Frequency (1-1000000)”（陷阱频率 [1-1000000]）— 两次陷阱之间的时间间隔（以秒为单位）。此字段仅适用于锁定端口。默认值为 10 秒。

定义锁定端口

1. 打开**“Port Security”（端口安全保护）**页面。
2. 选择接口类型和编号。
3. 定义字段。
4. 单击**“Apply Changes”（应用更改）**。

系统会将锁定端口添加至**“Port Security Table”（端口安全保护表）**，并更新设备。

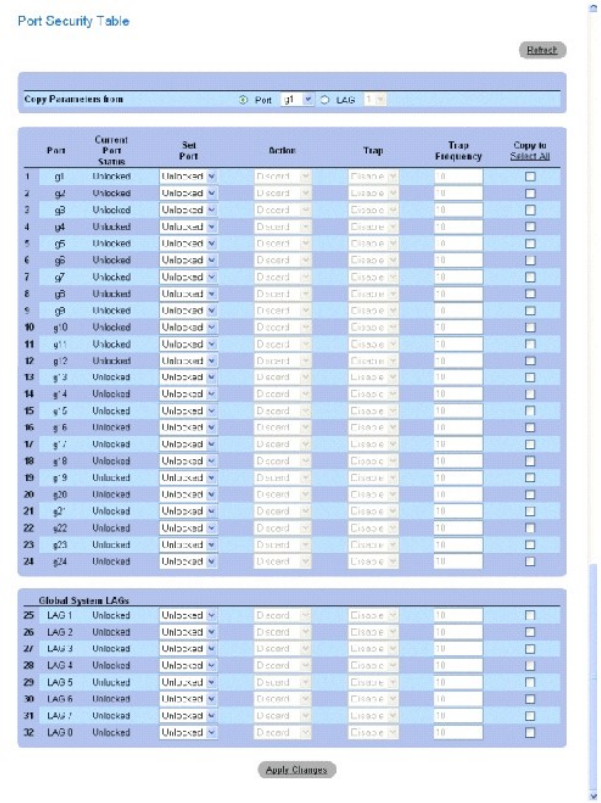
显示锁定端口表

1. 打开**“Port Security”（端口安全保护）**页面。
2. 单击**“Show All”（全部显示）**。

系统将打开**“Port Security Table”（端口安全保护表）**：

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。

图 7-87. 端口安全保护表



使用 CLI 命令配置锁定端口的安全保护

下表概括了与**“Port Security”（端口安全保护）**页面中显示的配置锁定端口安全保护选项等效的 CLI 命令。

表 7-52. 端口安全保护的 CLI 命令

CLI 命令	说明
shutdown	禁用接口。
set interface active {ethernet 接口 | port-channel 端口信道号}	重新激活由于端口安全保护原因而关闭的接口。
port security [**forward** | **discard** | **discard-shutdown**] [**trap** 秒]	锁定在接口上记忆新地址。
show ports security {**ethernet** 接口 | **port-channel** 端口信道号}	显示端口锁定状态。

以下是 CLI 命令的示例：

Console # **show ports security**					
Port	Status	Action	Trap	Frequency	Counter
----	-------	-------	-------	---------	-------
g7	Unlocked	Discard	Enable	100	88
g8	Unlocked	Discard, Shutdown	Disable		
g3	Unlocked	-	-	-	-

配置端口

“Ports”（端口）页面包含至端口功能（包括风暴控制和端口镜像等高级功能）页面的链接。要打开**“Ports”（端口）**页面，请单击**“Switch”（交换机）→“Ports”（端口）**。

定义端口参数

“Port Configuration”（端口配置）页面包含用于定义端口参数的字段。要打开**“Port Configuration”（端口配置）**页面，请在树视图中单击**“Switch”（交换机）→“Ports”（端口）→“Port Configuration”（端口配置）**。

图 7-88. 端口配置

“Port”（端口）— 要定义端口参数的端口号。

“Description”（说明）（0-64 个字符）— 接口的简短说明，例如以太网。

“Port Type”（端口类型）— 端口的类型。

“Admin Status”（管理状态）— 允许或禁止通过端口传输通信。新的端口状态将显示在**“Current Port Status”（当前端口状态）**字段中。

“Current Port Status”（当前端口状态）— 指定端口当前是正在运行还是未运行。

“Re-Activate Port”（重新激活端口）— 重新激活已通过锁定端口安全保护选项禁用的端口。

“Operational Status”（运行状态）— 端口的运行状态。可能的字段值包括：

“Suspended”（暂挂）— 端口当前处于活动状态，并且当前未接收或传输通信。

“Active”（激活）— 端口当前处于活动状态，并且当前正在接收和传输通信。

“Disable”（禁用）— 端口当前被禁用，并且当前未接收或传输通信。

“Admin Speed”（管理速率）— 端口的配置的速率。端口类型确定可以使用的速率设置选项。只有在已配置的端口上禁用了自适应，才可以指定管理速率。

“Current Port Speed”（当前端口速率）— 当前配置端口的实际速率（以 bps 为单位）。

“Admin Duplex”（管理双工）— 端口的双工模式可以为**“Full”（全双工）**或**“Half”（半双工）**。**“Full”（全双工）**表示接口支持在设备及其链接伙伴之间同时进行双向传输。**“Half”（半双工）**表示接口仅支持在设备和客户端之间进行单向传输。

“Current Duplex Mode”（当前双工模式）— 当前配置端口的双工模式。

“Auto Negotiation”（自适应）— 在端口上启用自适应。自适应是两个链接伙伴之间的协议，使一个端口可以将其传输速率、双工模式和流控制能力通知给伙伴端口。

“Current Auto Negotiation”（当前自适应）— 当前配置的自适应设置。

“Back Pressure”（背压）— 在端口上启用背压模式。背压模式与半双工模式一起使用可以禁止端口接收信息。

“Current Back Pressure”（当前背压）— 当前配置的背压设置。

“Flow Control”（流控制）— 启用或禁用端口上的流控制或启用流控制的自适应。端口处于**“Full”（全双工）**双工模式时运行。

“Current Flow Control”（当前流控制）— 当前配置的流控制的设置。

“MDI/MDIX”— 使设备可以辨认绞接电缆和非绞接电缆。

应专门使集线器和交换机布线方式与终端站点布线方式完全相反，以便在将集线器或交换机连接至终端站点时，可以使用直通以太网电缆，并且能够正确匹配成对电缆。将两台集线器/交换机

互相连接或将两个终端站点互相连接时，使用绞接电缆可以确保正确成对连接。可能的字段值包括：

“Auto”（自动） — 用于自动检测电缆的类型。

“MDI (Media Dependent Interface)”（MDI [介质相关接口]） — 用于终端站点。

“MDIX (Media Dependent Interface with Crossover)”（MDIX [带有绞接电缆的介质相关接口]） — 用于集线器和交换机。

“Current MDI/MDIX”（当前 MDI/MDIX） — 当前配置设备的 MDI/MDIX 设置。

“LAG”— 指定端口是否为 LAG 的一部分。

定义端口参数

1. 打开**“Port Configuration”（端口配置）**页面。
2. 在**“Port”（端口）**字段中选择一个端口。
3. 定义其余字段。
4. 单击**“Apply Changes”（应用更改）**。

端口参数将被保存至设备。

修改端口参数

1. 打开**“Port Configuration”（端口配置）**页面。
2. 在**“Port”（端口）**字段中选择一个端口。
3. 修改其余字段。
4. 单击**“Apply Changes”（应用更改）**。

端口参数将被保存至设备。

显示端口配置表：

1. 打开**“Port Configuration”（端口配置）**页面。
2. 单击**“Show All”（全部显示）**。

系统将打开**“Port Configuration Table”（端口配置表）**：

图 7-89. 端口配置表

使用 CLI 命令配置端口

下表概括了与 **“Ports Configuration Table”（端口配置表）** 页面中显示的配置端口的选项等效的 CLI 命令。

表 7-53. 端口配置的 CLI 命令

CLI 命令	说明
interface ethernet 接口	进入接口配置模式以配置以太网类型接口。
description 字符串	添加对接口配置的说明。
shutdown	禁用属于当前设置环境的接口。
set interface active {ethernet 接口 | port-channel 端口信道号}	重新激活由于安全保护原因而关闭的接口。
speed bps	配置在不使用自适应时给定以太网接口的速率。
autobaud	为自动波特率检测设置线路。
duplex {half | full}	配置在不使用自适应时给定以太网接口的全/半双工操作。
negotiation	启用给定接口的速率和双工参数的自适应操作。
back-pressure	在给定接口上启用背压。
flowcontrol {auto | on | off | rx | tx}	在给定接口上配置流控制。
mdix {on | auto}	在给定接口或端口信道上启用自动绞接。
show interfaces description [ethernet 接口 | port-channel 端口信道号]	显示所有已配置接口的配置。
show interfaces status [ethernet 接口 | port-channel 端口信道号]	显示所有已配置接口的状态。
show interfaces description [ethernet 接口 | port-channel 端口信道号]	显示所有已配置接口的说明。

以下是 CLI 命令的示例：

```
Console (config)# interface ethernet g5

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 ethernet g5
```

Port	Type	Duplex	Speed	Neg	Flow Control	Admin State	Back Pressure	Mdix Mode
----	----	------	-----	----	------	-----	------	----
g5	1G	Full	100	Enabled	On	Up	Enable	Auto

```
console#

console# show interfaces status ethernet g5
```

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Mode
----	----	------	-----	----	------	-----	------	----
g5	1G	Full	100	Enabled	On	Up	Disabled	on

```
console#
```

```
Console# show interfaces status
```

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Mode
----	----	------	-----	----	------	-----	------	----
g1	1G	Full	100	Auto	On	Up	Enable	On
g1	100	Full	100	Off	Off	Down	Disable	Off
g2	100	Full	1000	Off	Off	Up	Disable	On
Ch	Type	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State	
---	----	-----	---	----	-------	-------	------	
1	1000	Full	1000	Off	Off	Disable	Up	

定义 LAG 参数

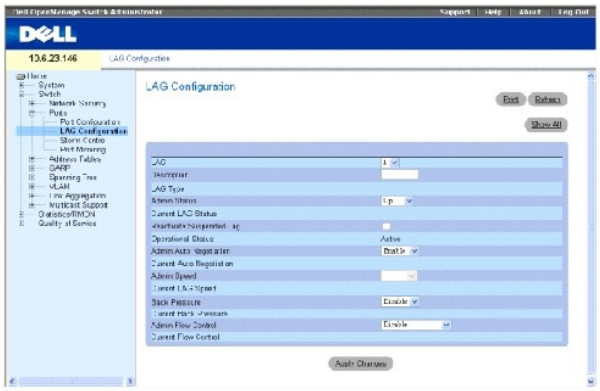
“LAG Configuration”（LAG 配置）页面包含用于为已配置的 LAG 配置参数的字段。设备支持每个 LAG 最多八个端口，每个系统八个 LAG。

有关链路聚合组 (LAG) 以及将端口分配至 LAG 的信息，请参阅“**聚合端口**”。

要打开**“LAG Configuration”（LAG 配置）**页面，请在树视图中单击**“Switch”（交换机）→“Ports”（端口）→“LAG Configuration”（LAG 配置）**。

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。

图 7-90. LAG 配置



"LAG"— LAG 号。

"Description"（说明）（0-64 个字符）— 提供已配置的 LAG 的用户定义的说明。

"LAG Type"（LAG 类型）— 组成 LAG 的端口类型。

"Admin Status"（管理状态）— 允许或禁止通过选定的 LAG 传输通信。

"Current LAG Status"（当前 LAG 状态）— 表示 LAG 当前是否正在运行。

"Re-Activate Suspended LAG"（重新激活暂挂的 LAG）— 重新激活暂挂的 LAG。

"Operational Status"（运行状态）— LAG 的运行状态。

"Admin Auto Negotiation"（管理自适应）— 在 LAG 上启用或禁用自适应。自适应是两个链接伙伴之间的协议，使一个 LAG 可以将其传输速率、双工模式和流控制（流控制的默认设置为已禁用）能力通知给伙伴端口。

"Current Auto Negotiation"（当前自适应）— 当前配置的自适应设置。

"Admin Speed"（管理速率）— LAG 运行的速率。

"Current LAG Speed"（当前 LAG 速率）— 当前配置的 LAG 运行的速率。

"Admin Back Pressure"（管理背压）— 在 LAG 上启用或禁用背压模式。背压模式在 LAG 中以半双工模式运行的端口上有效。

"Current Back Pressure"（当前背压）— 当前配置的背压设置。

"Admin Flow Control"（管理流控制）— 启用/禁用流控制或启用 LAG 上流控制的自适应。流控制模式在 LAG 中以全双工模式运行的端口上有效。

"Current Flow Control"（当前流控制）— 用户指定的的流控制的设置。

定义 LAG 参数

1. 打开**“LAG Configuration”（LAG 配置）**页面。
2. 在**“LAG”**字段中选择一个 LAG。
3. 定义字段。
4. 单击**“Apply Changes”（应用更改）**。

LAG 参数将被保存至设备。

修改 LAG 参数

1. 打开**“LAG Configuration”（LAG 配置）**页面。
2. 在**“LAG”**字段中选择一个 LAG。
3. 修改字段。
4. 单击**“Apply Changes”（应用更改）**。

LAG 参数将被保存至设备。

显示 LAG 配置表：

1. 打开**“LAG Configuration”（LAG 配置）**页面。
2. 单击**“Show All”（全部显示）**。

系统将打开**“LAG Configuration Table”（LAG 配置表）**：

图 7-91. LAG 配置表

使用 CLI 命令配置 LAG

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

表 7-54. LAG 配置的 CLI 命令

CLI 命令	说明
interface port-channel 端口信道号	进入特定端口信道的接口配置模式。
description 字符串	添加对接口配置的说明。
shutdown	禁用属于当前设置环境的接口。
speed bps	配置在不使用自适应时给定以太网接口的速率。

autobaud	为自动波特率检测设置线路。
negotiation	启用给定接口的速率和双工参数的自适应操作。
back-pressure	在给定接口上启用背压。
flowcontrol {auto | on | off | rx | tx}	在给定接口上配置流控制。
show interfaces description［ethernet 接口| port-channel 端口信道号]	显示所有已配置接口的配置。
show interfaces status［ethernet 接口 |port-channel 端口信道号]	显示所有已配置接口的状态。
show interfaces description［ethernet 接口| port-channel 端口信道号]	显示所有已配置接口的说明。
show interfaces port-channel［端口信道号]	显示端口信道信息（哪些端口是端口信道的成员，以及它们当前是否处于活动状态）。

以下是 CLI 命令的示例：

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

console(config-if)# exit

console(config)# interface range e g21-24

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

console(config-if)# ex

console(config)# interface ethernet g5

console(config-if)# channel-group 2 mode on

console(config-if)# exit

console(config)#exit
```

```
console# show interfaces port-channel
```

Channel	Ports
---------	---------
ch1	Inactive: g(21-24)
ch2	Active: g5
ch3	
ch4	

ch5	
ch6	
ch7	
ch8	
console#	

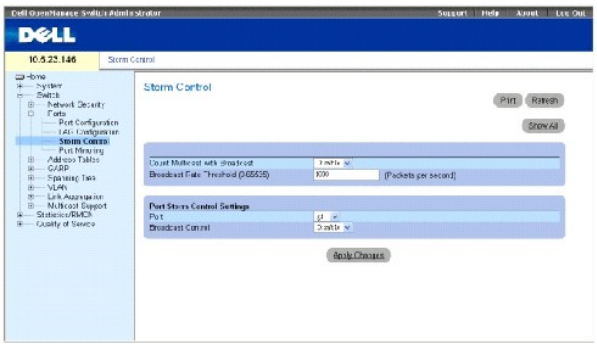
启用风暴控制

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

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

“Storm Control”（风暴控制）页面提供了用于启用和配置风暴控制的字段。要打开“Storm Control”（风暴控制）页面，请在树视图中单击 **“Switch”（交换机）→“Ports”（端口）→“Storm Control”（风暴控制）**。

图 7-92. 风暴控制



“Count Multicast with Broadcast”（计数多点传送和广播）— 计数广播和多点传送通信。可能的字段值包括：

- **“Enable”（启用）**— 计数广播和多点传送通信。
- **“Disable”（禁用）**— 仅计数广播通信。

“Broadcast Rate Threshold (1-1000000)”（广播速率阈值 [1-1000000]）— 传输未知信息包的最大速率（信息包/秒）。范围为 0 至 1000000。默认值为 0。所有值均舍入到最接近 64 Kbps。如果字段值小于 64 Kbps，该值将向上舍入到 64 Kbps，0 值是个例外。

“Port”（端口）— 要从其启用风暴控制的端口。

“Broadcast Control”（广播控制）— 在设备上启用或禁用传输广播信息包的类型。

在设备上启用风暴控制

1. 打开**“Storm Control”（风暴控制）**页面。
2. 选择一个要在其上实现风暴控制的接口。
3. 定义字段。
4. 单击**“Show All”（全部显示）**。

系统将在设备上启用风暴控制。

修改风暴控制端口参数

1. 打开**“Storm Control”（风暴控制）**页面。
2. 修改字段。
3. 单击**“Show All”（全部显示）**。

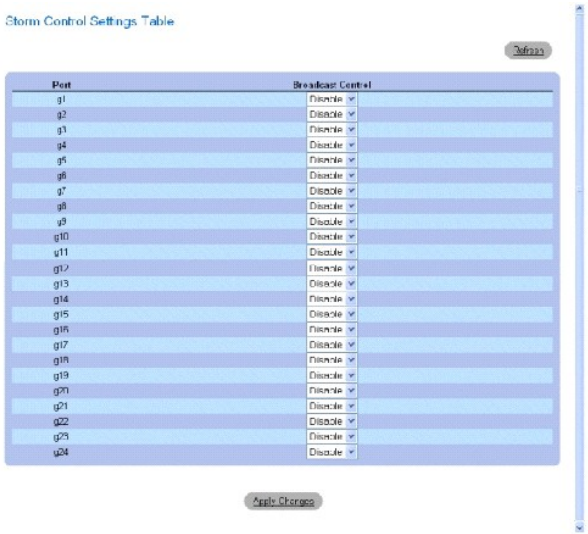
风暴控制端口参数将被保存至设备。

显示端口参数表

1. 打开**“Storm Control”（风暴控制）**页面。
2. 单击**“Show All”（全部显示）**。

系统将打开**“Storm Control Settings Table”（风暴控制设置表）**：

图 7-93. 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。

表 7-55. 风暴控制的 CLI 命令

CLI 命令	说明

port storm-control include-multicast	允许设备计数多点传送信息包和广播信息包。
port storm-control broadcast enable	启用广播风暴控制。
port storm-control broadcast rate 速率	配置最大广播速率。
show ports storm-control [ethernet 接口]	显示风暴控制配置。

以下是 CLI 命令的示例：

```
console> enable

console# configure

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

Console(config)# port storm-control broadcast rate 8000

Console(config)# interface ethernet g1

Console(config-if)# port storm-control broadcast enable

Console(config-if)# end

Console# show ports storm-control
```

Port	Broadcast Storm control [Packets/sec]
----	----------
g1	8000
g2	Disabled
g4	Disabled

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。

通过选择要复制所有信息包的特定端口以及要从中复制信息包的其它端口，即可配置端口镜像。在配置端口镜像之前，请注意以下几点：

- 被监测端口的运行速率不能高于监测端口的运行速率。
- 所有 RX/TX 信息包应在同一端口进行监测。

以下限制适用于要被配置为目的地端口的端口：

- 端口不能被配置为源端口。
- 端口不能为 LAG 成员。
- 未在端口上配置 IP 接口。
- 未在端口上启用 GVRP。
- 端口不是 VLAN 成员。
- 只能定义一个目的地端口。

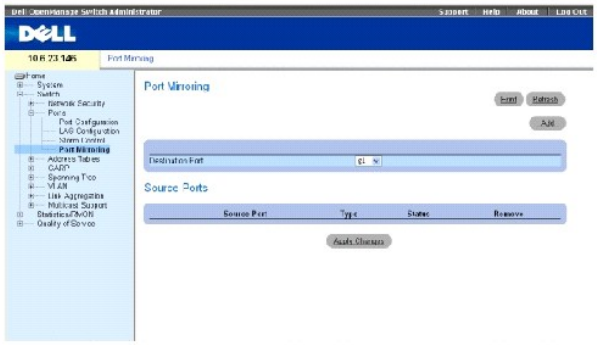
以下限制适用于要被配置为源端口的端口：

- 源端口不能为 LAG 成员。
- 端口不能被配置为目的地端口。
- 所有被传输的信息包都将标记为来自目的地端口。
- 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）**。

注：将端口设置为用于端口镜像会话的目标端口时，此端口上的所有常规操作均将被暂挂，包括生成树和 LACP。

图 7-94. 端口镜像



“Destination Port”（目的地端口）— 端口通信要复制到的端口号。

“Source Port”（源端口）— 定义要镜像其端口通信的端口号。

“Type”（类型）— 表示源端口是否为 RX 或 TX 或者同时为 RX 和 TX。

“Status”（状态）— 表示端口当前是否被监测（**“Active”[激活]**）或未被监测（**“Ready”[就绪]**）。

“Remove”（删除）— 如果选定该选项，将删除端口镜像会话。

添加端口镜像会话

1. 打开**“Port Mirroring”（端口镜像）**页面。
2. 单击**“Add”（添加）**。

   系统将打开**“Add Source Port”（添加源端口）**页面。
3. 从**“Destination Port”（目的地端口）**下拉式菜单中选择目的地端口。
4. 从**“Source Port”（源端口）**下拉式菜单中选择源端口。
5. 定义**“Type”（类型）**字段。
6. 单击**“Apply Changes”（应用更改）**。

   系统将定义新的源端口，并更新设备。

从端口镜像会话中删除副本端口

1. 打开**“Port Mirroring”（端口镜像）**页面。
2. 选定**“Remove”（删除）**复选框。
3. 单击**“Apply Changes”（应用更改）**。

   系统将删除选定端口的镜像会话，并更新设备。

使用 CLI 命令配置端口镜像会话

下表概括了与**“Port Mirroring”（端口镜像）**页面中显示的配置端口镜像会话的选项等效的 CLI 命令。

表 7-56. 端口镜像的 CLI 命令

CLI 命令	说明
port monitor SRC 接口 [**rx** | **tx**]	启动端口监测会话。

以下是 CLI 命令的示例：

```
Console(config)# interface ethernet g1

Console(config-if)# port monitor g8

Console# show ports monitor
```

Source Port	Destination Port	Type	Status	VLAN Tagging
----------	----------	----------	-------	----------
g8	g1	RX, TX	Active	No

g2	g8	RX, TX	Active	No
g18	g8	Rx	Active	No

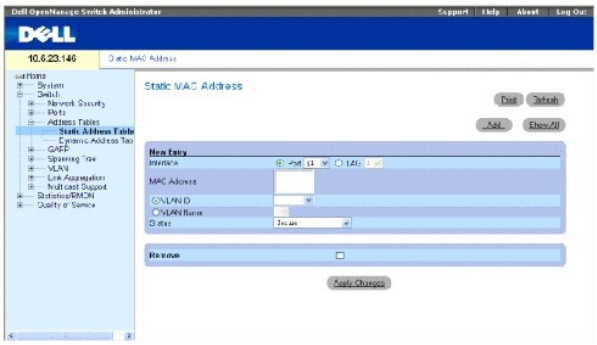
配置地址表

MAC 地址存储在静态地址数据库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。当信息包从源到达设备时，MAC 地址将被动态记忆。通过从帧的源地址记忆端口，可以将地址与端口相关联。定址到与任一端口均不相关联的目的地 MAC 地址的帧将被多路发送至相关 VLAN 的所有端口。可以手动配置静态地址。为防止桥接表溢出，在特定时间段内未进行任何通信的动态 MAC 地址将被删除。要打开**“Address Tables”（地址表）**页面，请在树视图中单击 **“Switch”（交换机）→“Address Table”（地址表）**。

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 Table”（地址表）→“Static Address”（静态地址）**。

图 7-95. 静态 MAC 地址



“Interface”（接口）— 静态 MAC 地址被应用于的特定端口或 LAG。

“MAC Address”（MAC 地址）— 当前静态地址列表中列出的 MAC 地址。

“VLAN ID”— 连接至 MAC 地址的 VLAN ID。

“VLAN Name”（VLAN 名称）— 用户定义的 VLAN 名称。

“Status”（状态）— MAC 地址的状态。可能的值包括：

“Secure”（安全）— 保证锁定端口的 MAC 地址不被删除。

“Permanent”（永久）— MAC 地址是永久性的。

“Delete on Reset”（重设时删除）— 在重设设备时删除 MAC 地址。

“Delete on Timeout”（超时时删除）— 发生超时时删除 MAC 地址。

“Remove”（删除）— 如果选定该选项，将从 MAC 地址表中删除 MAC 地址。

添加静态 MAC 地址

1. 打开**“Static MAC Address”（静态 MAC 地址）**页面。
2. 单击**“Add”（添加）**。

   系统将打开**“Add Static MAC Address”（添加静态 MAC 地址）**页面。
3. 完成字段。
4. 单击**“Apply Changes”（应用更改）**。

   系统会将新的静态地址添加至**“Static MAC Address Table”（静态 MAC 地址表）**中，并更新设备。

修改静态 MAC 地址表中的静态地址

1. 打开**“Static MAC Address”（静态 MAC 地址）**页面。
2. 修改字段。
3. 单击**“Apply Changes”（应用更改）**。

   系统将修改静态 MAC 地址，并更新设备。

从静态地址表中删除静态地址

1. 打开**“Static MAC Address”（静态 MAC 地址）**页面。
2. 单击**“Show All”（全部显示）**。

   系统将打开**“Static MAC Address Table”（静态 MAC 地址表）**。
3. 选择一个表条目。
4. 选定**“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**“Static MAC Address”（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。

表 7-57. 静态地址 CLI 命令

CLI 命令	说明
bridge address MAC 地址 {**ethernet 接口** | **port-channel 端口信道号**} [**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 [**vlan VLAN**] [**ethernet 接口** | **port-channel 端口信道号**]	显示网桥传输数据库中的条目。

以下是 CLI 命令的示例：

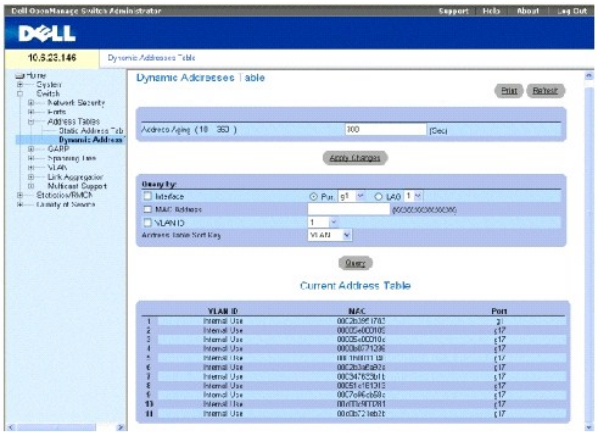
```
Console# show bridge address-table

Aging time is 300 sec

vlan  mac address       port  type
----  ------------      ----  --------
1     00:60:70:4C:73:FF g8    dynamic
1     00:60:70:8C:73:FF g8    dynamic
200    00:10:0D:48:37:FF g9    static
g8    00:10:0D:98:37:88 g8    dynamic
```

查看动态地址

动态地址表包含用于查询动态地址表中的信息（包括接口类型、MAC 地址、VLAN 和表排序）的字段。传输至存储在地址表中的地址的信息包将被直接传输至那些端口。动态地址表还包含有关动态 MAC 地址被删除前存在时间的信息，并包括用于查询和查看动态地址列表的参数。当前地址表包含将信息包直接传输至那些端口所依据的动态地址参数。

要打开**“Dynamic Address Table”（动态地址表）**，请在树视图中单击**“Switch”（交换机）→“Address Table”（地址表）→“Dynamic Addresses Table”（动态地址表）**。

图 7-96. 动态地址表



“Address Aging (10-360)”（地址存在时间 [10-360]）— 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。

“Interface”（接口）— 指定要为其查询表的接口。可以选择的端口类型有两种。

“Port”（端口）— 指定要为其查询表的端口号。

“LAG”— 指定要为其查询表的 LAG。

“MAC Address”（MAC 地址）— 指定要为其查询表的 MAC 地址。

“VLAN ID”— 要为其查询表的 VLAN ID。

“Address Table Sort Key”（地址表排序关键字）— 指定动态地址表的排序方法。

重新定义存在时间

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。

查询动态地址表

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**“Port”（端口）**、**“MAC Address”（MAC 地址）**或**“VLAN ID”**查询条目。
3. 单击**“Query”（查询）**。

   将查询**“Dynamic Address Table”（动态地址表）**。

对动态地址表进行排序

1. 打开**“Dynamic Address Table”（动态地址表）**。
2. 从**“Address Table Sort Key”（地址表排序关键字）**下拉式菜单中选择是否按照地址、VLAN ID 或接口对地址进行排序。
3. 单击**“Query”（查询）**。

   将对动态地址表进行排序。

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）**中显示的查询和排序动态地址的选项等效的 CLI 命令。

表 7-58. 查询和排序的 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 端口信道号]	显示在网桥传输数据库中动态创建的条目的分类。

以下是 CLI 命令的示例：

```
```

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


Console (config)# exit


Console# show bridge address-table
```

Aging time is 250 sec

vlan	mac address	port	type
----	-----------	----	----
1	00:60:70:4C:73:FF	g8	dynamic
1	00:60:70:8C:73:FF	g8	dynamic
200	00:10:0D:48:37:FF	g8	static

配置 GARP

通用属性注册协议 (GARP) 是一个通用协议，用于注册所有网络连接信息或成员关系类型信息。GARP 定义了一组关注给定网络属性（例如 VLAN 或多点传送地址）的设备。

配置 GARP 时，请确保满足以下要求：

- 离开时间必须大于或等于加入时间的三倍。
- 全部离开时间必须大于离开时间。

在第 2 层连接的所有设备上设置同一 GARP 计时器值。如果在第 2 层连接的设备上设置不同的 GARP 计时器，GARP 应用程序将不能成功运行。

要打开 **“GARP”**页面，请在树视图中单击 **“Switch”（交换机）→“GARP”**。

定义 GARP 计时器

“GARP Timers”（GARP 计时器）页面包含用于在设备上启用 GARP 的字段。要打开 **“GARP Timers”（GARP 计时器）**页面，请在树视图中单击 **“Switch”（交换机）→“GARP”→“GARP Timers”（GARP 计时器）**。

图 7-97. GARP 计时器

“Interface”（接口）— 确定是在端口上还是在 LAG 上启用。

“GARP Join Timer (10 - 2147483640)”（GARP 加入计时器 [10 - 2147483640]）— 传输 PDU 的时间（以毫秒为单位）。可能的字段值为 10 至 2147483640。默认值为 200 毫秒。

“GARP Leave Timer (10 - 2147483640)”（GARP 离开计时器 [10 - 2147483640]）— 设备离开其 GARP 状态之前等待的时间（以毫秒为单位）。发送/接收到的“Leave All Time”（全部离开时间）信息可以激活离开时间，接收到的“Join”（加入）信息可以取消离开时间。离开时间必须大于或等于加入时间的三倍。可能的字段值为 0 至 2147483640。默认值为 600 毫秒。

“GARP Leave All Timer (10 - 2147483640)”（GARP 全部离开计时器 [10 - 2147483640]）— 所有设备离开 GARP 状态之前等待的时间（以毫秒为单位）。全部离开时间必须大于离开时间。可能的字段值为 0 至 2147483640。默认值为 10000 毫秒。

定义 GARP 计时器

1. 打开**“GARP Timers”（GARP 计时器）**页面。
2. 完成字段。
3. 单击**“Apply Changes”（应用更改）**。

GARP 参数将被保存至设备。

复制 GARP 计时器表中的参数

1. 打开**“GARP Timers”（GARP 计时器）**页面。
2. 单击**“Show All”（全部显示）**。

系统将打开**“GARP Timers Table”（GARP 计时器表）**。

3. 在**“Copy Parameters from”（参数复制自）**字段中选择接口类型。
4. 在**“Port”（端口）**或**“LAG”**下拉式菜单中选择一个接口。
5. 此接口的定义将被复制到选定的接口中。请参阅步骤 6。
6. 选定**“Copy to”（复制到）**复选框以定义 GARP 计时器定义要复制到的接口，或单击**“Select All”（全部选定）**以将此定义复制到所有端口或 LAG。
7. 单击**“Apply Changes”（应用更改）**。

系统会将参数复制到**“GARP Timers Table”（GARP 计时器表）**中的选定端口或 LAG，并更新设备。

使用 CLI 命令定义 GARP 计时器

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

表 7-59. GARP 计时器的 CLI 命令

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

以下是 CLI 命令的示例：

```
console(config)# interface ethernet g1

console(config-if)# garp timer leave 900

console(config-if)# end

console# show gvrp configuration ethernet g1



GVRP Feature is currently Disabled on the device.

Maximum VLANs: 223
```

Port (s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
g1	Disabled	Normal	Enabled	200	900	10000

```
console#
```

配置生成树协议

生成树协议 (STP) 提供了树拓扑，用于任意排列网桥。STP 还在网络中的终端站点之间提供了一条路径，消除了环路。

主机之间存在备用路径时，将形成环路。扩展网络中的环路可能会造成网桥无限制地传输通信，从而导致通信量增加以及网络效率降低。

设备支持以下生成树协议：

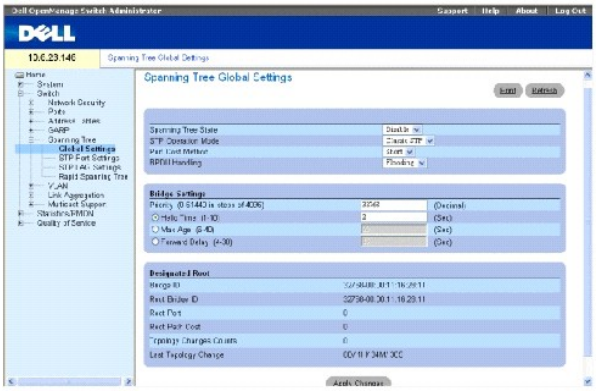
- “Classic STP”（经典 STP）— 在终端站点之间提供单一路径，避免并消除环路。有关配置经典 STP 的详细信息，请参阅“定义 STP 全局设置”。
- “Rapid STP”（快速 STP）— 检测并使用提供快速生成树聚合的网络拓扑，且不会创建传输环路。有关配置快速 STP 的详细信息，请参阅“配置快速生成树”。

要打开**“Spanning Tree”（生成树）**页面，请在树视图中单击**“Switch”（交换机）→“Spanning Tree”（生成树）**。

定义 STP 全局设置

“STP Global Settings”（STP 全局设置）页面包含用于在设备上启用和配置 STP 操作的参数。要打开“STP Global Settings”（STP 全局设置）页面，请在树视图中单击 **“Switch”（交换机）→“Spanning Tree”（生成树）→“Global Settings”（全局设置）**。

图 7-98. STP 全局设置



“Spanning Tree State”（生成树状态）— 在设备上启用或禁用生成树。可能的字段值包括：

- **“Enable”（启用）**— 启用生成树
- **“Disable”（禁用）**— 禁用生成树

“STP Operation Mode”（STP 运行模式）— 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。此为默认值。

“Rapid STP”（快速 STP）— 在设备上启用快速 STP。

“Port Cost Method”（端口成本方法）— 确定生成树默认路径的成本方法。可能的字段值包括：

“Short”（短）— 指定端口路径成本为 1 至 65535。此为默认值。

“Long”（长）— 指定端口路径成本为 1 至 200000000。

“BPDU Handling”（BPDU 处理）— 确定 STP 在端口/设备上被禁用时如何管理 BPDU 信息包。BPDU 用于传输生成树信息。可能的字段值包括：

“Filtering”（筛选）— 生成树在接口上被禁用时筛选 BPDU 信息包。

“Flooding”（多路发送）— 生成树在接口上被禁用时多路发送 BPDU 信息包。此为默认值。

“Priority (0-61440, in steps of 4096)”（优先级 [0-61440，步进为 4096]）— 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。以 4096（增量为 4K）为增量提供网桥优先级值。例如，0、4096、8192 等。

“Hello Time (1-10)”（问候间隔 [1-10]）— 指定设备的问候间隔。问候间隔表示根网桥在配置信息之间等待的时间（以秒为单位）。默认值为 2 秒。

“Max Age (6-40)”（最长持续时间 [6-40]）— 指定设备的最长存在时间。最长存在时间表示网桥在发送配置信息之前等待的时间（以秒为单位）。默认的最长存在时间为 20 秒。

“Forward Delay (4-30)”（传输延迟 [4-30]）— 指定设备的传输延迟时间。传输延迟时间表示在传输信息包之前网桥处于侦听和记忆状态的时间（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）— 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）— 指定自上次重新引导以来发生的 STP 状态更改的总次数。

“Last Topology Change”（上次拓扑更改）— 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、秒的格式显示，例如，0 天 1 小时 34 分钟 38 秒。

定义 STP 全局参数

1. 打开**“STP Global Settings”（STP 全局设置）**页面。
2. 从**“Select a Port”（选择端口）**下拉式菜单中选择需要启用的端口。
3. 在**“Spanning Tree State”（生成树状态）**字段中选择**“Enable”（启用）**。
4. 在**“STP Operation Mode”（STP 运行模式）**字段中选择**“STP”**模式，并定义网桥设置。
5. 单击**“Apply Changes”（应用更改）**。

系统将在设备上启用 STP。

修改 STP 全局参数

1. 打开**“STP Global Settings”（STP 全局设置）**页面。
2. 定义对话框中的字段。
3. 单击**“Apply Changes”（应用更改）**。

系统将修改 STP 参数，并更新设备。

使用 CLI 命令定义 STP 全局参数

下表概括了与**“STP Global Settings”（STP 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。

表 7-60. STP 全局参数的 CLI 命令

CLI 命令	说明
spanning-tree	启用生成树功能。

spanning-tree mode {stp | rstp}	配置生成树协议。
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，即设备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。
spanning-tree forward-time 秒	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记忆状态的时间。
show spanning-tree [ethernet 接口 | port-channel 端口信道号]	显示生成树配置标识符。
show spanning-tree [detail] [active | blockedports]	显示生成树配置信息 - 详细信息或者活动端口或锁定端口。

以下是 CLI 命令的示例：

```
console(config)# spanning-tree

console(config)# spanning-tree mode rstp

console(config)# spanning-tree priority 12288

console(config)# spanning-tree hello-time 5

console(config)# spanning-tree max-age 15

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

console(config)#exit

console# show spanning-tree


Spanning tree enabled mode RSTP

Default port cost method: short

Root ID     Priority    12288
            Address     00:e8:00:b4:c0:00
            This switch is the root
            Hello Time 5 sec Max Age 15 sec Forward Delay 25 sec

Number of topology changes 5 last change occurred 00:05:28 ago
```

Times: hold 1, topology change 40, notification 5

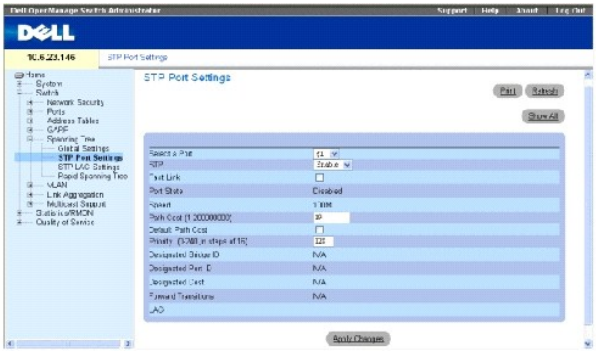
hello 5, max age 15, forward delay 25

Interfaces							
Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
-----	------	-----	----	------	------	---------	------
g1	enabled	128.1	100	DSBL	Dsbl	No	P2p (STP)
g2	enabled	128.2	100	DSBL	Dsbl	No	P2p (STP)
g3	enabled	128.3	100	DSBL	Dsbl	No	P2p (STP)

定义 STP 端口设置

"STP Port Settings"（STP 端口设置）页面包含用于为各个端口设定 STP 属性的字段。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）**。

图 7-99. STP 端口设置



"Select a Port"（选择端口）— 要在其上启用 STP 的端口。

"STP"— 在端口上启用或禁用 STP。

"Fast Link"（快速链路）— 如果选定该选项，将为端口启用快速链路模式。如果为端口启用了快速链路模式，则端口链路良好时**"Port State"（端口状态）**将被自动置入**"Forwarding"（传输）**状态。快速链路模式可以优化 STP 协议进行聚合所需的时间。在大型网络中，STP 聚合可能需要 30 至 60 秒。

"Port State"（端口状态）— 当前端口的 STP 状态。如果已启用该选项，端口状态将确定对通信所采取的传输操作。可能的端口状态包括：

“Disabled”（已禁用）— 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记忆 MAC 地址。启用“Classic STP”（经典 STP）时将显示“Blocking”（阻塞）。

“Listening”（侦听）— 端口当前处于侦听模式。端口既不能传输通信，也不能记忆 MAC 地址。

“Learning”（记忆）— 端口当前处于记忆模式。端口不能传输通信，但可以记忆新的 MAC 地址。

“Forwarding”（传输）— 端口当前处于传输模式。端口可以传输通信，也可以记忆新的 MAC 地址。

“Speed”（速率）— 端口运行的速率。

“Path Cost (1-200000000)”（路径成本 [1-200000000]）— 端口在根路径成本中所占的比例。路径成本可以调整为较高或较低的值，路径被重定路线时路径成本用于传输通信。

“Default Path Cost”（默认路径成本）— 端口的默认路径成本由端口速率和默认路径成本方法自动设置。

长路径成本的默认值包括：

“Ethernet”（以太网）- 2000000

“Fast Ethernet”（快速以太网）- 200000

“Gigabit Ethernet”（吉位以太网）- 20000

短路径成本的默认值（默认设置为短路径成本）包括：

“Ethernet”（以太网）- 100

“Fast Ethernet”（快速以太网）- 19

“Gigabit Ethernet”（吉位以太网）- 4

“Priority (0-240, in steps of 16)”（优先级 [0-240，步进为 16]）— 端口的优先级值。当网桥有两个端口连接在一个环路中时，优先级值用于确定端口的选择。优先级值介于 0 至 240 之间。以 16 为增量提供优先级值。

“Designated Bridge ID”（指定网桥 ID）— 指定网桥的网桥优先级和 MAC 地址。

“Designated Port ID”（指定端口 ID）— 选定端口的优先级和接口。

“Designated Cost”（指定成本）— 参与 STP 拓扑的端口的成本。如果 STP 检测到环路，则端口成本越低，被阻塞的可能性越小。

“Forward Transitions”（传输转换） — 端口从**“Blocking”（阻塞）**状态变为**“Forwarding”（传输）状态**的次数。

“LAG”— 端口要连接的 LAG。

在端口上启用 STP

1. 打开**“STP Port Settings”（STP 端口设置）**页面。
2. 在**“STP Port Status”（STP 端口状态）**字段中选择**“Enabled”（已启用）**。
3. 定义**“Fast Link”（快速链路）**、**“Path Cost”（路径成本）**和**“Priority”（优先级）**字段。
4. 单击**“Apply Changes”（应用更改）**。

系统将在端口上启用 STP。

修改 STP 端口属性

1. 打开**“STP Port Settings”（STP 端口设置）**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 端口参数，并更新设备。

显示 STP 端口表

1. 打开**“STP Port Settings”（STP 端口设置）**页面。
2. 单击**“Show All”（全部显示）**。

系统将打开**“STP Port Table”（STP 端口表）**。

使用 CLI 命令定义 STP 端口设置

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

表 7-61. STP 端口设置的 CLI 命令

CLI 命令	说明
spanning-tree disable	禁用特定端口上的生成树。
spanning-tree cost 成本	配置端口的生成树成本比例。
spanning-tree port-priority 优先级	配置端口优先级。
spanning-tree portfast	启用 PortFast 模式。
show spanning-tree [ethernet 接口 **| port-channel** 端口信道号**]**	显示生成树配置。

以下是 CLI 命令的示例：

```
console(config)# interface ethernet g5
```

```
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 g5
```

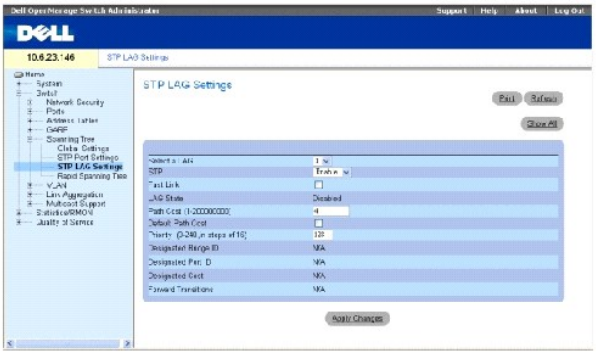
```
Port g5 disabled

State:disabled

Port id: 96.5

Type:P2p (configured:Auto) STP

Designated bridge Priority : 32768

Designated port id: 96.5

Number of transitions to forwarding
state: 0

BPDU:sent 0, received 0

console#
```

```
Role:disabled

Port cost: 35000

Port Fast: No (configured:No)

Address: 00:e8:00:b4:c0:00

Designated path cost: 19
```

定义 STP LAG 设置

“STP LAG Settings”（STP LAG 设置）页面包含用于设定 STP 聚合端口参数的字段。要打开“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）。

图 7-100. STP LAG 设置



“Select a LAG”（选择 LAG）— 用户定义的 LAG。有关详情，请参阅“定义 LAG 成员关系”。

“STP”— 在 LAG 上启用或禁用 STP。

“Fast Link”（快速链路）— 为 LAG 启用快速链路模式。如果为 LAG 启用了快速链路模式，则 LAG 良好时**“LAG State”（LAG 状态）**将被自动置入**“Forwarding”（传输）**状态。快速链路模式可以优化 STP 协议进行聚合所需的时间。在大型网络中，STP 聚合可能需要 30 至 60 秒。

“LAG State”（LAG 状态）— LAG 的当前 STP 状态。如果已启用该选项，LAG 状态将确定对通信所采取的传输操作。如果网桥发现故障 LAG，LAG 将被置入**“Broken”（断开）**状态。可能的 LAG 状态包括：

“Disabled”（已禁用）— LAG 链路当前已断开。

“Blocking”（阻塞）— LAG 已被阻塞，无法用于传输通信或记忆 MAC 地址。

“Listening”（侦听）— LAG 处于侦听模式，无法传输通信或记忆 MAC 地址。

“Learning”（记忆）— LAG 处于记忆模式，无法传输通信，但可以记忆新的 MAC 地址。

“Forwarding”（传输）— LAG 当前处于传输模式，可以传输通信和记忆新的 MAC 地址。

“Broken”（断开）— LAG 当前出现故障，无法用于传输通信。

“Path Cost (1-200000000)”（路径成本 [1-200000000]）— 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，路径被重定路线时路径成本用于传输通信。路径成本的值为 1 至 200000000。如果路径成本方法为“短”，则 LAG 成本默认值为 4。如果路径成本方法为“长”，则 LAG 成本默认值为 20000。

“Default Path Cost”（默认路径成本）— 如果选定该选项，LAG 路径成本将恢复其默认值。

“Priority (0-240, in steps of 16)”（优先级 [0-240，步进为 16]）— LAG 的优先级值。当网桥有两个环路端口时，优先级值用于确定 LAG 的选择。优先级值介于 0 至 240 之间，以 16 为增量。

“Designated Bridge ID”（指定网桥 ID）— 指定网桥的网桥优先级和 MAC 地址。

“Designated Port ID”（指定端口 ID）— 指定端口的端口优先级和接口数目。

“Designated Cost”（指定成本）— 指定网桥的成本。

“Forward Transitions”（传输转换）— **“LAG State”（LAG 状态）**从**“Blocking”（阻塞）**状态变为**“Forwarding”（传输）**状态的次数。

修改 LAG STP 参数

1. 打开**“STP LAG Settings”（STP LAG 设置）**页面。
2. 从**“Select a LAG”（选择 LAG）**下拉式菜单中选择一个 LAG。
3. 根据需要修改字段。
4. 单击**“Apply Changes”（应用更改）**。

系统将修改 STP LAG 参数，并更新设备。

使用 CLI 命令定义 STP LAG 设置

下表概括了用于定义 STP LAG 设置选项等效的 CLI 命令。

表 7-62. STP LAG 设置的 CLI 命令

CLI 命令	说明
spanning-tree	启用生成树。
spanning-tree disable	禁用特定 LAG 上的生成树。
spanning-tree cost 成本	配置 LAG 的生成树成本比例。
spanning-tree port-priority 优先级	配置端口优先级。
show spanning-tree [ethernet 接口 | port-channel 端口信道号]	显示生成树配置。
show spanning-tree [detail] [active | blockedports]	显示有关活动或锁定端口的详细生成树信息。

以下是 CLI 命令的示例：

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


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

配置快速生成树

由于经典生成树可以确保防止普通网络拓扑中的 L2 传输环路，因此聚合最多需要 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。

RSTP 具有以下几种端口状态：

- “Disabled”（已禁用）
- “Learning”（记忆）
- “Discarding”（丢弃）
- “Forwarding”（传输）

可以在“STP Global Settings”（STP 全局设置）页面中启用快速生成树。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）。

图 7-101. 快速生成树(RSTP)

“Interface”（接口）— 要在其上启用快速 STP 的端口或 LAG。

“Role”（角色）— 由 STP 算法分配的以便提供给 STP 路径的端口角色。可能的字段值包括：

“Root”（根）— 提供最低成本路径以将信息包传输给根设备。

“Designated”（指定）— 指定的设备通过其连接到 LAN 的端口或 LAG。

“Alternate”（备用）— 通过根接口向根设备提供备用路径。

“Backup”（备份）— 生成树离开时向指定端口路径提供备份路径。只有当两个端口连接在一个环路中时，才会出现备份端口。当 LAN 有两个或多个连接已连接到一个共享网段时，也会出现备份端口。

“Disabled”（已禁用）— 端口未加入生成树（端口的链路已断开）。

“Fast Link Operational Status”（快速链路运行状态）— 表示是否为端口或 LAG 启用或禁用快速链路。如果为端口启用了快速链路，则端口将被自动置入传输状态。

“Point-to-Point Admin Status”（点对点管理状态）— 允许或禁止设备建立点对点链路，或为设备指定该选项以自动建立点对点链路。

为通过点对点链路建立通信，起始 PPP 首先发送链路控制协议 (LCP) 信息包以配置和检测数据链路。建立了链路并根据需要按照 LCP 协商了可选设备之后，起始 PPP 将发送网络控制协议 (NCP) 信息包以选择和配置一个或多个网络层协议。如果每个选定的网络层协议均已进行了配置，则可以通过链路发送来自每个网络层协议的信息包。在明确的 LCP 或 NCP 信息包关闭链路或发生某些外部事件之前，链路保持配置为进行通信的状态。这是实际的设备端口链路类型。它可能与管理状态不同。

“Point-to-Point Operational Status”（点对点运行状态）— 点对点运行状态。

“Activate Protocol Migrational Test”（激活协议迁移检测）— 如果选定该选项，将允许 PPP 发送链路控制协议 (LCP) 信息包以配置和检测数据链路。

启用 RSTP

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）**、**“Point-to-Point Oper”（点对点运行）**和**“Activate Protocol Migration”（激活协议迁移）**字段。
3. 单击**“Apply Changes”（应用更改）**。

系统将启用快速 STP，并更新设备。

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]）**页面中显示的定义快速 STP 参数的选项等效的 CLI 命令。

表 7-63. RSTP 设置的 CLI 命令

CLI 命令	说明
spanning-tree link-type {**point-to-point** | **shared**}	代替默认链路类型设置。
spanning tree mode {**stp** | **rstp**}	配置当前运行的生成树协议。
clear spanning-tree detected-protocols [**ethernet 接口** | **port-channel 端口信道号**]	重新启动协议迁移进程。
show spanning-tree [**ethernet 接口** | **port-channel 端口信道号**]	显示生成树配置。

以下是 CLI 命令的示例：

```
Console(config)# interface
ethernet g5


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。

由于 VLAN 是基于软件，而不是通过物理属性进行定义的，因此 VLAN 可以拥有无限数量的端口，并且可以针对每个设备或任何其它逻辑连接组合进行创建。

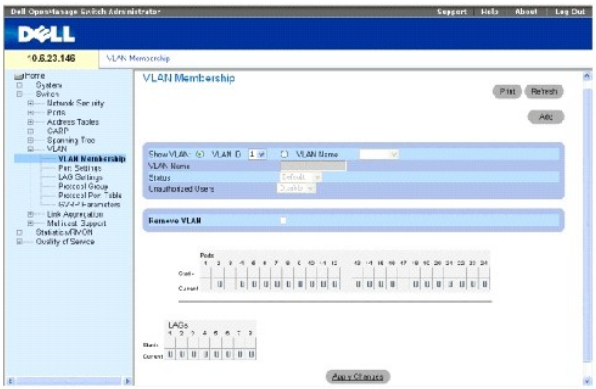
VLAN 在第 2 层起作用。由于 VLAN 将通信隔离在 VLAN 内部，因此需要在第 3 层安装可正常运行的路由器以允许通信在 VLAN 之间传输。第 3 层路由器使用 VLAN 标识网段和坐标。VLAN 是广播域和多点传送域。广播和多点传送通信仅在生成通信的 VLAN 中传输。

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 可以自动分散 VLAN 信息。要打开**“VLAN”**页面，请在树视图中单击**“Switch”（交换机）→“VLAN”**。

定义 VLAN 成员

“VLAN Membership”（VLAN 成员关系）页面包含用于定义 VLAN 组的字段。设备支持 4094 VLAN ID 至 256 VLAN 的映射。所有端口必须具有已定义的 PVID。如果未配置其它值，请使用默认的 VLAN PVID。VLAN 编号 1 是默认的 VLAN，无法从系统中将其删除。要打开“VLAN Membership”（VLAN 成员关系）页面，请在树视图中单击**“Switch”（交换机）→“VLAN”→“VLAN Membership”（VLAN 成员关系）**。

图 7-102. VLAN 成员关系页面



"Show VLAN"（显示 VLAN）— 根据 VLAN ID 或 VLAN 名称列出并显示特定的 VLAN 信息。

"VLAN Name"（VLAN 名称）— 用户定义的 VLAN 名称。

"Status"（状态）— VLAN 的类型。可能的值包括：

"Dynamic"（动态）— VLAN 是通过 GVRP 动态创建的。

"Static"（静态）— VLAN 是由用户定义的。

"Default"（默认）— VLAN 是默认的 VLAN。

"Unauthorized Users"（未经授权的用户）— 允许或禁止未经授权的用户访问 VLAN。

"Remove VLAN"（删除 VLAN）— 如果选定此选项，将从 VLAN 成员关系表中删除 VLAN。

添加新 VLAN

1. 打开**"VLAN Membership"（VLAN 成员关系）**页面。
2. 单击**"Add"（添加）**。

   系统将打开**"Create New VLAN"（创建新 VLAN）**页面。
3. 输入 VLAN ID 和 VLAN 名称。
4. 单击**"Apply Changes"（应用更改）**。

   系统将添加新 VLAN，并更新设备。

修改 VLAN 成员关系组

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

2. 从“**Show VLAN**”（**显示 VLAN**）下拉式菜单中选择一个 VLAN。
3. 根据需要修改字段。
4. 单击“**Apply Changes**”（**应用更改**）。

系统将修改 VLAN 成员关系信息，并更新设备。

删除 VLAN 成员关系组

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. 选定“**Remove VLAN**”（**删除 VLAN**）复选框。
4. 单击“**Apply Changes**”（**应用更改**）。

系统将删除选定的 VLAN，并更新设备。

使用 CLI 命令定义 VLAN 成员关系组

下表概括了与“**VLAN Membership**”（**VLAN 成员关系**）页面中显示的定义 VLAN 成员关系组的选项等效的 CLI 命令。

表 7-64. VLAN 成员关系组的 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 命令的示例：

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

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：

表 7-65. VLAN 端口成员关系表

端口控制	定义
T	接口是 VLAN 的成员。通过接口传输的所有信息包均被标记。信息包包含 VLAN 信息。
U	接口是 VLAN 成员。通过接口传输的信息包均未标记。
F	否认接口是 VLAN 的成员。
空白	接口不是 VLAN 成员。与接口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。

为 VLAN 组分配端口

1. 打开**“VLAN Membership”（VLAN 成员关系）**页面。
2. 单击**“VLAN ID”**或**“VLAN Name”（VLAN 名称）**选项按钮并从下拉式菜单中选择一个 VLAN。
3. 在**“Port Membership Table”（端口成员关系表）**中选择一个端口，并设定端口值。
4. 单击**“Apply Changes”（应用更改）**。

系统会将端口分配至 VLAN 组，并更新设备。

删除 VLAN

1. 打开**“VLAN Membership”（VLAN 成员关系）**页面。
2. 单击**“VLAN ID”**或**“VLAN Name”（VLAN 名称）**选项按钮并从下拉式菜单中选择一个 VLAN。
3. 选定**“Remove VLAN”（删除 VLAN）**复选框。
4. 单击**“Apply Changes”（应用更改）**。

系统将删除选定的 VLAN，并更新设备。

使用 CLI 命令为 VLAN 组分配端口

下表概括了用于将端口分配至 VLAN 组等效的 CLI 命令。

表 7-66. 端口至 VLAN 组分配的 CLI 命令

CLI 命令	说明
switchport general acceptable-frame-types tagged-only	在入口丢弃未标记的帧。
switchport forbidden vlan {add vlan-list | remove vlan-list}	禁止向端口添加特定的 VLAN。
switchport mode {access | trunk | general}	配置端口的 VLAN 成员关系模式。
switchport access vlan vlan id	在接口处于访问模式时配置 VLAN ID。

switchport trunk allowed vlan {add vlan-list | remove vlan-list}	在主干端口中添加或删除 VLAN。
switchport trunk native vlan vlan id	将端口定义为指定 VLAN 的成员，并将 VLAN ID 定义为“端口默认 VLAN ID (PVID)”。
switchport general allowed vlan add vlan-list [tagged | untagged]	在常规端口中添加或删除 VLAN。
switchport general pvid vlan id	在接口处于常规模式时配置 PVID。

以下是 CLI 命令的示例：

```
Console (config)#
vlan database

Console (config-vlan)
# vlan 23-25

Console (config-vlan)
# exit

Console (config)#
interface vlan 23

Console (config-if)#
name Marketing

Console(config-if)#
exit

Console (config)#
interface ethernet g8

Console (config-if)#
switchport mode
access

Console (config-if)#
switchport access
vlan 23

Console(config-if)#
exit

Console (config)#
interface ethernet g9

Console (config-if)#
switchport mode trunk

Console (config-if)#
swithport mode trunk
allowed vlan add 23-
25
```

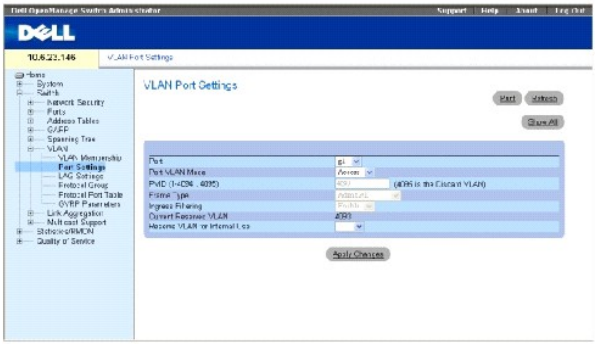
```
Console(config-if)#
exit


Console (config)#
interface ethernet
g10


Console (config-if)#
switchport mode
general


Console (config-if)#
switchport general
allowed vlan add
23,25 tagged


Console (config-if)#
switchport general
pvid 25
```

定义 VLAN 端口设置

“VLAN Port Settings”（VLAN 端口设置）页面中的字段用于管理属于 VLAN 的端口。**“Port Default VLAN ID”（端口默认 VLAN ID）**(PVID) 可在**“VLAN Port Settings”（VLAN 端口设置）**页面中进行配置。所有到达设备的未标记信息包均通过端口 PVID 进行标记。

要打开**“VLAN Port Settings”（VLAN 端口设置）**页面，请在树视图中单击**“Switch”（交换机）→“VLAN”→“Port Settings”（端口设置）**。

图 7-103. VLAN 端口设置



“Port”（端口）— VLAN 中包含的端口号。

“Port VLAN Mode”（端口 VLAN 模式）— 端口的模式。可能的值包括：

“General”（常规）— 端口属于 VLAN，并且每个 VLAN 均由用户定义为已标记或未标记（完全 802.1Q 模式）。

“Access”（访问）— 端口属于单个未标记 VLAN。端口处于访问模式时，不能指定端口上接受的信息包类型。不能在访问端口上启用/禁用入口筛选。

“Trunk”（主干）— 端口属于其中所有端口均将被标记的 VLAN（未标记的端口除外）。

“PVID”— 为未标记信息包分配 VLAN ID。可能的值介于 1 至 4094 之间。VLAN 4095 按照标准和行业惯例被定义为丢弃的 VLAN。分类为丢弃的 VLAN 的信息包将被丢弃。

“Frame Type”（帧类型）— 端口上接受的信息包类型。可能的值包括：

“Admit Tag Only”（仅接受标记）— 端口仅接受已标记信息包。

“Admit All”（全部接受）— 端口既接受已标记信息包，也接受未标记信息包。

“Ingress Filtering”（入口筛选）— 在端口上启用或禁用入口筛选。入口筛选将丢弃预定给特定 LAG 不属于的 VLAN 的信息包。

“Current Reserve VLAN”（当前保留 VLAN）— 当前由系统指定为保留 VLAN 的 VLAN。

“Reserve VLAN for Internal Use”（保留 VLAN 用于内部使用）— 如果系统未使用用户选定的 VLAN，它将作为保留 VLAN。

设定端口设置

1. 打开**“VLAN Port Settings”（VLAN 端口设置）**页面。
2. 从**“Port”（端口）**下拉式菜单中选择需要设定设置的端口。
3. 完成页面中的其余字段。
4. 单击**“Apply Changes”（应用更改）**。

系统将定义 VLAN 端口设置，并更新设备。

显示 VLAN 端口表

1. 打开**“VLAN Port Settings”（VLAN 端口设置）**页面。
2. 单击**“Show All”（全部显示）**。

系统将打开**“VLAN Port Table”（VLAN 端口表）**。

使用 CLI 命令为 VLAN 组分配端口

下表概括了将端口分配至 VLAN 组的选项等效的 CLI 命令。

表 7-67. VLAN 端口的 CLI 命令

CLI 命令	说明
switchport mode {access | trunk | general}	配置端口 VLAN 成员关系模式。
switchport trunk native vlan VLAN ID	将端口定义为指定 VLAN 的成员，并将 VLAN ID 定义为“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]	在常规端口中添加或删除 VLAN。
switchport general acceptable-frame-types tagged-only	在入口丢弃未标记的信息包。
switchport general ingress-filtering disable	禁用端口入口筛选。

shutdown	禁用接口。
set interface active {ethernet 接口 | port-channel 端口信道号 }	重新激活由于安全保护原因而关闭的接口。

以下是 CLI 命令的示例：

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


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 可以由各个端口或 LAG 组成。进入设备的未标记信息包按照 PVID 指定的 LAG ID 进行标记。要打开**"VLAN LAG Settings"（VLAN LAG 设置）**页面，请在树视图中单击**"Switch"（交换机）→"VLAN"→"LAG Settings"（LAG 设置）**。

图 7-104. VLAN LAG 设置

"LAG"— VLAN 中包含的 LAG 号。

"LAG VLAN Mode"（LAG VLAN 模式）— LAG VLAN 模式。可能的值包括：

"General"（常规）— LAG 属于 VLAN，并且每个 VLAN 均由用户定义为已标记或未标记（完全 802.1Q 模式）。

“Access”（访问）— LAG 属于单个未标记 VLAN。

“Trunk”（主干）— LAG 属于其中所有端口均将被标记的 VLAN（可选的单个固有 VLAN 除外）。

“PVID”— 为未标记信息包分配 VLAN ID。可能的字段值介于 1 至 4095 之间。VLAN 4095 按照标准和行业惯例被定义为丢弃的 VLAN。分类为此 VLAN 的信息包将被丢弃。

“Frame Type”（帧类型）— LAG 接受的信息包类型。可能的值包括：

“Admit Tag Only”（仅接受标记）— LAG 仅接受已标记的信息包。

“Admit All”（全部接受）— LAG 既接受已标记信息包，也接受未标记信息包。

“Ingress Filtering”（入口筛选）— 由 LAG 启用或禁用入口筛选。入口筛选将丢弃预定给特定端口不属于的 VLAN 的信息包。

“Current Reserve VLAN”（当前保留 VLAN）— 当前指定为保留 VLAN 的 VLAN。

“Reserve VLAN for Internal Use”（保留 VLAN 用于内部使用）— 重启动设备后指定为保留 VLAN 的 VLAN。

设定 VLAN LAG 设置：

1. 打开**“VLAN LAG Settings”（VLAN LAG 设置）**页面。
2. 从**“LAG”**下拉式菜单中选择一个 LAG，并完成页面中的字段。
3. 单击**“Apply Changes”（应用更改）**。

系统将定义 VLAN LAG 参数，并更新设备。

显示 VLAN LAG 表

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

系统将打开**“VLAN LAG Table”（VLAN LAG 表）**。

使用 CLI 命令为 VLAN 组分配 LAG

下表概括了与**“VLAN LAG Settings”（VLAN LAG 设置）**页面中显示的为 VLAN 组分配 LAG 的选项等效的 CLI 命令。

表 7-68. LAG VLAN 分配的 CLI 命令

CLI 命令	说明
switchport mode {access | trunk | general}	配置端口 VLAN 成员关系模式。
switchport trunk native vlan VLAN ID	将端口定义为指定 VLAN 的成员，并将 VLAN ID 定义为端口默认 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]	在常规端口中添加或删除 VLAN。
switchport general acceptable-frame-type tagged-only	在入口丢弃未标记的信息包。

switchport general ingress-filtering disable	禁用端口入口筛选。

以下是 CLI 命令的示例：

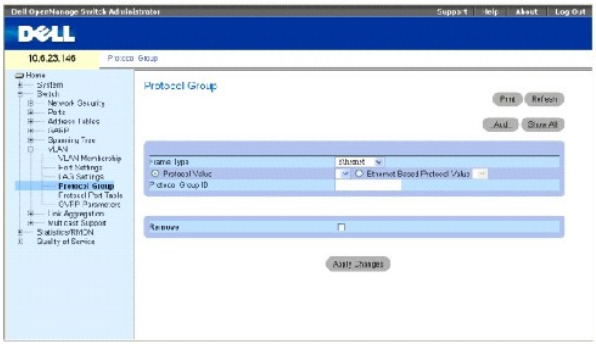
```
console(config)# interface
port-channel 1

console(config-if)#
switchport mode access

console(config-if)#
switchport access vlan 2

console(config-if)# exit

console(config)# interface
port-channel 2

console(config-if)#
switchport mode general

console(config-if)#
switchport general allowed
vlan add 2-3 tagged

console(config-if)#
switchport general pvid 2

console(config-if)#
switchport general
acceptable-frame-type
tagged-only

console(config-if)#
switchport general
ingress-filtering disable

console(config-if)# exit

console(config)# interface
port-channel 3

console(config-if)#
switchport mode trunk

console(config-if)#
switchport trunk native
vlan 3
```

```
console(config-if)#
switchport trunk allowed
vlan add 2


console(config-if)# exit
```

定义 VLAN 协议组

"Protocol Group"（协议组）页面提供用于将帧类型配置到特定协议组的参数。要打开**"Protocol Group"（协议组）**页面，请在树视图中单击**"Switch"（交换机）→"VLAN"→"Protocol Group"（协议组）**。

图 7-105. 协议组



"Frame Type"（帧类型）— 信息包类型。可能的字段值包括**"Ethernet"（以太网）**、**"RFC1042"**和**"LLC Other"（LLC 等其它）**。

"Protocol Value"（协议值）— 用户定义的协议名称。

"Ethernet-Based Protocol Value"（基于以太网的协议值）— 以太网协议组类型。可能的字段值包括"IP"、"IPX"和**"IPV6"**。

"Protocol Group ID"（协议组 ID）— VLAN 组 ID 号。

"Remove"（删除）— 在选定该选项时，如果要删除的协议组未配置于此协议端口上，则会删除帧到协议组的映射。

添加协议组

1. 打开**"Protocol Group"（协议组）**页面。
2. 单击**"Add"（添加）**。

   系统将打开**"Add Protocol to Group"（向组添加协议）**页面。
3. 完成页面中的字段。
4. 单击**"Apply Changes"（应用更改）**。

   系统将设定协议组，并更新设备。

设定 VLAN 协议组设置

1. 打开**“Protocol Group”（协议组）**页面。
2. 完成页面中的字段。
3. 单击**“Apply Changes”（应用更改）**。

系统将定义 VLAN 协议组参数，并更新设备。

从协议组表中删除协议

1. 打开**“Protocol Group”（协议组）**页面。
2. 单击**“Show All”（全部显示）**。

系统将打开**“Protocol Group Table”（协议组表）**。

3. 为需要删除的协议组选择**“Remove”（删除）**。
4. 单击**“Apply Changes”（应用更改）**。

系统将删除协议，并更新设备。

使用 CLI 命令定义 VLAN 协议组

下表概括了用于配置协议组的等效的 CLI 命令。

表 7-69. VLAN 协议组的 CLI 命令

CLI 命令	说明
map protocol 协议 [封装] protocols-group 组	将协议映射至协议组。协议组用于基于协议的 VLAN 分配。

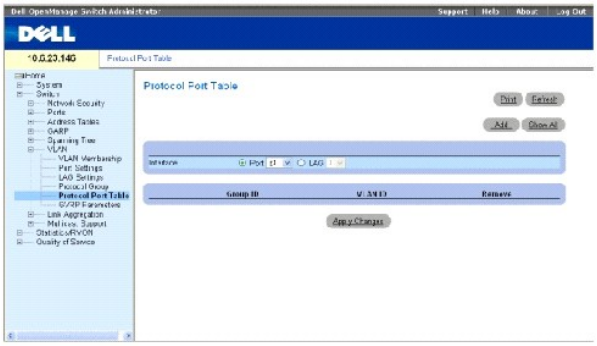
以下示例将 ip-arp 协议映射至组“213”：

```
Console (config)# vlan database

Console (config-vlan)# map protocol ip-arp protocols-group 213
```

添加协议端口

“Protocol Port”（协议端口）页面可以将接口添加至协议组。要打开**“Protocol Port”（协议端口）**页面，请在树视图中单击**“Switch”（交换机）→“VLAN”→“Protocol Port”（协议端口）**。

图 7-106. 协议端口



"Interface"（接口）— 要添加至协议组的端口或 LAG 号。

"Group ID"（组 ID）— 要添加接口的协议组的 ID。协议组 ID 在协议组表中作了定义。

"VLAN ID (1-4095)"（VLAN ID [1-4095]）— 将接口连接至用户定义的 VLAN ID。VLAN ID 在**"Create a New VLAN"（创建新 VLAN）**页面中作了定义。协议端口可以连接至 VLAN ID 或 VLAN 名称。

注：VLAN 4095 是丢弃的 VLAN。

添加新协议端口

注：协议端口只能在**"VLAN Port Settings"（VLAN 端口设置）**页面中被定义为"General"（常规）的端口上进行定义。

1. 打开**"Protocol Port"（协议端口）**页面。
2. 单击**"Add"（添加）**。

   系统将打开**"Add Protocol Port"（添加协议端口）**页面。
3. 完成对话框中的字段。
4. 单击**"Apply Changes"（应用更改）**。

   系统会将新 VLAN 协议组添加至**"Protocol Port Table"（协议端口表）**，并更新设备。

使用 CLI 命令定义协议端口

下表概括了用于定义协议端口的等效的 CLI 命令。

表 7-70. 协议端口的 CLI 命令

CLI 命令	说明
switchport general map protocols-group group vlan VLAN ID	设置基于协议的分类规则。

以下示例将协议组 1 的基于协议的分类规则设置为 VLAN 8：

```
Console (config-if)#
switchport general map protocols-
group 1 vlan 8
```

配置 GVRP

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

为确保 GVRP 协议能够正常运行，建议您将 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。

“GVRP Global Parameters”（GVRP 全局参数）页面用于全局启用 GVRP。GVRP 还可以针对每个接口启用。要打开**“GVRP Parameters”（GVRP 参数）**页面，请在树视图中单击 **“Switch”（交换机）→“VLAN”→“GVRP Parameters”（GVRP 参数）**。

图 7-107. GVRP 参数

“GVRP Global Status”（GVRP 全局状态） — 在设备上启用或禁用 GVRP。默认情况下，GVRP 被禁用。

“Interface”（接口） — 要启用 GVRP 的接口或 LAG。

“GVRP State”（GVRP 状态） — 在接口上启用或禁用 GVRP。

“Dynamic VLAN Creation”（动态 VLAN 创建） — 允许或禁止通过 GVRP 创建 VLAN。

“GVRP Registration”（GVRP 注册） — GVRP 注册状态。

在设备上启用 GVRP

1. 打开**“GVRP Global Parameters”（GVRP 全局参数）**页面。
2. 在**“GVRP Global Status”（GVRP 全局状态）**字段中选择**“Enable”（启用）**。
3. 单击**“Apply Changes”（应用更改）**。

系统将在设备上启用 GVRP。

通过 GVRP 启用 VLAN 注册

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

2. 在“**GVRP Global Status**”（**GVRP 全局状态**）字段中为所需的接口选择“**Enable**”（**启用**）。
3. 在“**GVRP Registration**”（**GVRP 注册**）字段中选择“**Enable**”（**启用**）。
4. 单击“**Apply Changes**”（**应用更改**）。

系统将在端口上启用 GVRP VLAN 注册，并更新设备。

使用 CLI 命令配置 GVRP

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

表 7-71. GVRP 全局参数的 CLI 命令

CLI 命令	说明
gvrp enable（全局）	全局启用 GVRP。
gvrp enable（接口）	在接口上启用 GVRP。
gvrp vlan-creation-forbid	启用或禁用动态 VLAN 创建。
gvrp registration-forbid	取消注册所有动态 VLAN，并禁止端口上的动态 VLAN 注册。
show gvrp configuration [**ethernet 接口**| **port-channel 端口信道号**]	显示 GVRP 配置信息，包括计时器值、是否已启用 GVRP 和动态 VLAN 创建，以及运行 GVRP 的端口。
show gvrp error-statistics [**ethernet 接口**| **port-channel 端口信道号**]	显示 GVRP 错误统计数据。
show gvrp statistics [**ethernet 接口**| **port-channel 端口信道号**]	显示 GVRP 统计数据。
clear gvrp statistics [**ethernet 接口**| **port-channel 端口信道号**]	清除所有 GVRP 统计数据信息。

以下是 CLI 命令的示例：

```
console(config)# gvrp enable

console(config)# interface ethernet g1

console(config-if)# gvrp enable

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

console(config-if)# gvrp registration-forbid

console(config-if)# end

console# show gvrp configuration



GVRP Feature is currently Enabled on the device.
```

Maximum VLANs: 223

Port(s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
g1	Enabled	Forbidden	Disabled	200	900	10000
g2	Disabled	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。设备支持每个系统最多八个 LAG，每个设备的每个 LAG 最多八个端口。

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)，可以手动或自动分配聚合链路。设备根据源 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，包括自适应、速率和双工设置等。

设备既支持静态 LAG，也支持链路聚合控制协议 (LACP) LAG。LACP LAG 与位于其它设备上的 LACP 端口协商聚合端口链路。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。

在向 LAG 添加端口时，应遵循以下原则：

- 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。

设备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。设备将聚合链路看作单个逻辑端口。

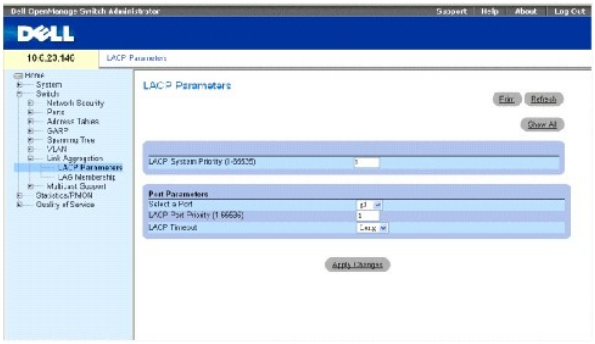
每个聚合链路具有一个聚合链路端口类型，包括吉位以太网端口。仅当端口具有相同的端口类型时，才能将其添加至聚合链路。将端口从聚合链路删除时，端口将恢复为原始端口设置。要打开**“Link Aggregation”（链路聚合）**页面，请在树视图中单击**“Switch”（交换机）→“Link Aggregation”（链路聚合）**。

定义 LACP 参数

“LACP Parameters”（LACP 参数）页面包含用于配置 LACP LAG 的字段。聚合端口可以被链接至链路聚合端口组。每个组由具有相同速率的端口组成。

通过在相关链路上启用链路聚合控制协议 (LACP)，可以手动设置或自动建立聚合链路。要打开**“LACP Parameters”（LACP 参数）**页面，请在树视图中单击**“Switch”（交换机）→“Link Aggregation”（链路聚合）→“LACP Parameters”（LACP 参数）**。

图 7-108. LACP 参数



“LACP System Priority (1-65535)”（LACP 系统优先级 [1-65535]）— 全局设置的 LACP 优先级值。可能值范围为 1 至 65535。默认值为 1。

“Select a Port”（选择端口）— 要设定超时和优先级值的端口号。

“LACP Port Priority (1-65535)”（LACP 端口优先级 [1-65535]）— 端口的 LACP 优先级值。

“LACP Timeout”（LACP 超时）— 管理 LACP 超时。可能的字段值包括：

“Short”（短）— 指定短超时值。

“Long”（长）— 指定长超时值。

定义链路聚合全局参数

1. 打开**“LACP Parameters”（LACP 参数）**页面。
2. 完成**“LACP System Priority”（LACP 系统优先级）**字段。
3. 单击**“Apply Changes”（应用更改）**。

系统将定义参数，并更新设备。

定义链路聚合端口参数

1. 打开**“LACP Parameters”（LACP 参数）**页面。
2. 完成**“Port Parameters”（端口参数）**区域中的字段。
3. 单击**“Apply Changes”（应用更改）**。

系统将定义参数，并更新设备。

显示 LACP 参数表

1. 打开**“LACP Parameters”（LACP 参数）**页面。
2. 单击**“Show All”（全部显示）**。

系统将打开**“LACP Parameters Table”（LACP 参数表）**。

使用 CLI 命令配置 LACP 参数

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

表 7-72. LACP 参数的 CLI 命令

CLI 命令	说明
lacp system-priority 值	配置系统优先级。
lacp port-priority 值	配置物理端口的优先级值。
lacp timeout {long | short}	设定管理 LACP 超时。
show lacp ethernet 接口 [parameters | statistics | protocol-state]	显示以太网端口的 LACP 信息。

以下是 CLI 命令的示例：

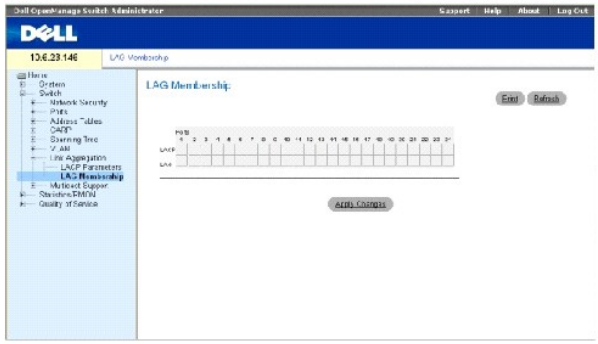
```
Console (config)# lacp
system-priority 120


Console (config)#
interface ethernet g1


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


Console (config-if)# lacp
timeout long


Console (config-if)# end


Console# show lacp
ethernet g1 statistics


Port g1 LACP Statistics:


LACP PDUs sent:2


LACP PDUs received:2
```

定义 LAG 成员关系

“LAG Membership”（LAG 成员关系）页面包含用于向 LAG 分配端口的字段。LAG 最多可以包括 8 个端口。将端口添加到 LAG 时，该端口将获取 LAG 的属性。如果该端口无法配置 LAG 属性，将生成陷阱，并且该端口将使用其默认设置运行。

“LAG Membership”（LAG 成员关系）页面包含用于向 LAG 分配端口的字段。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）**。

图 7-109. LAG 成员关系



“LACP”— 使用 LACP 将端口聚合到 LAG。

“LAG”— 向 LAG 添加端口，并表示端口所属的特定 LAG。

将端口配置为 LAG 或 LACP

1. 打开**“LAG Membership”（LAG 成员关系）**页面。
2. 在“LAG”行（第二行）中，将按钮切换至特定号以将端口聚合到该 LAG 号或在该 LAG 号中删除端口。
3. 在“LACP”行（第一行）中，切换端口号下相应的按钮以设定 LACP 或静态 LAG。
4. 单击**“Apply Changes”（应用更改）**。

系统会将端口添加至 LAG 或 LACP，并更新设备。

使用 CLI 命令向 LAG 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。

表 7-73. LAG 成员关系的 CLI 命令

CLI 命令	说明
interface port-channel 端口信道号	进入特定端口信道的接口配置模式。
channel-group 端口信道号 mode {on | auto}	使端口与端口信道相关联。在此命令前加 no 将从接口删除信道组配置。
show interfaces port-channel [端口信道号]	显示端口信道信息。

以下是 CLI 命令的示例：

```
console# config
console(config)# interface
ethernet g1
console(config-if)#
channel-group 1 mode on
console(config-if)# 01-
Jan-2000 01:47:18 %LINK-W-
Down: ch1



console(config-if)#
```

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。

设备支持以下信息包：

- **“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，并且不可配置。

注：系统支持 63 个多点传送组的多点传送筛选。

- **“Filtering L2 Multicast Packets”（筛选 L2 多点传送信息包）**— 允许向接口传输 第 2 层信息包。如果禁用了多点传送筛选，则多点传送信息包将多路发送至所有相关的端口。

要打开**“Multicast Support”（多点传送支持）**页面，请在树视图中单击**“Switch”（交换机）→“Multicast Support”（多点传送支持）**。

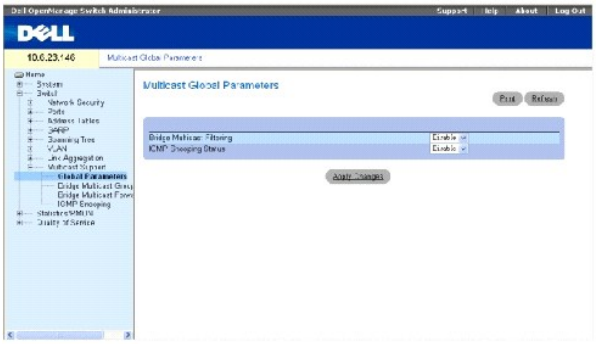
定义多点传送全局参数

默认情况下，第 2 层交换机向所有相关 VLAN 端口传输多点传送信息包，即将信息包作为多点传送信息包进行传输。正常运行时，在此意义上所有相关的端口/节点将接收帧的副本，当端口/节点可能接收到只有该 VLAN 的端口的子集才需要的不相关的帧时，这可能是一种浪费。多点传送筛选器允许将第 2 层信息包传输到在多点传送筛选器数据库中定义的端口子集。

全局启用 IGMP 监测时，交换 ASIC 将被设置为向 CPU 传输所有 IGMP 信息包。CPU 将分析传入的信息包，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。请求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。这将导致创建多点传送筛选数据库。

“Multicast Global Parameters”（多点传送全局参数）页面包含用于在设备上启用 IGMP 监测的字段。要打开**“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）**。

图 7-110. 多点传送全局参数



“Bridge Multicast Filtering”（网桥多点传送筛选） — 启用或禁用网桥多点传送筛选。默认值为已禁用。仅当启用了网桥多点传送过滤时才能启用 IGMP 监测。

“IGMP Snooping Status”（IGMP 监测状态） — 在设备上启用或禁用 IGMP 监测。默认值为已禁用。

在设备上启用网桥多点传送筛选

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）。

在设备上启用 IGMP 监测

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 Global Parameters”（多点传送全局参数）**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。

表 7-74. 多点传送和监测的 CLI 命令

CLI 命令	说明
bridge multicast filtering	启用多点传送地址筛选。
ip igmp snooping	启用因特网组员资格协议 (IGMP) 监测。

以下是 CLI 命令的示例：

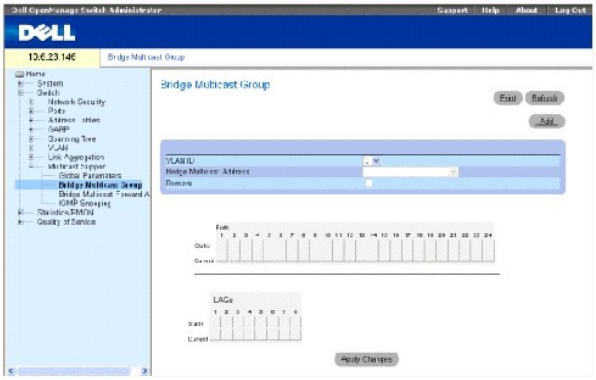
```
Console (config)# bridge
multicast filtering

Console (config)# ip igmp
snooping
```

添加网桥多点传送地址成员

“Bridge Multicast Group”（网桥多点传送组）页面在“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）页面还可以为特定多点传送服务地址组分配端口。

要打开“Bridge Multicast Support”（网桥多点传送支持）页面，请在树视图中单击“Switch”（交换机）→“Multicast Support”（多点传送支持）→“Bridge Multicast Address”（网桥多点传送地址）。

图 7-111. 网桥多点传送组



“VLAN ID”— 标识 VLAN，并包含有关多点传送组地址的信息。

“Bridge Multicast Address”（网桥多点传送地址）— 标识多点传送组 MAC 地址/IP 地址。

“Remove”（删除）— 如果选定该选项，将删除网桥多点传送地址。

“Ports”（端口）— 可以添加至多点传送服务的端口。

“LAG”— 可以添加至多点传送服务的 LAG。

下表包含 IGMP 端口和 LAG 成员管理设置：

表 7-75. IGMP 端口/LAG 成员表控制设置

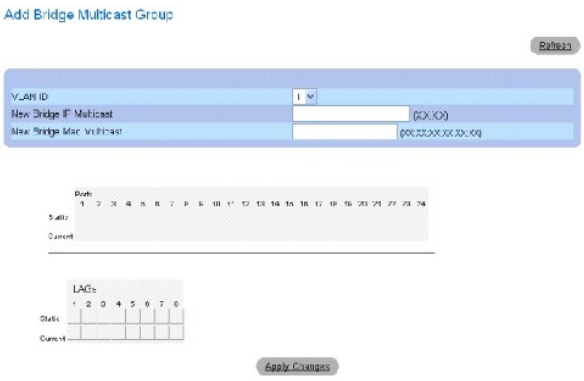
端口控制	定义
D	端口/LAG 已动态加入“Current”（当前）行中的多点传送组。
S	将端口作为“Static”（静态）行中的静态成员连接至多点传送组。 端口/LAG 已静态加入“Current”（当前）行中的多点传送组。
F	已禁止。
空白	端口未连接至多点传送组。

添加网桥多点传送地址

1. 打开“Bridge Multicast Group”（网桥多点传送组）页面。
2. 单击“Add”（添加）。

系统将打开“Add Bridge Multicast Group”（添加网桥多点传送组）页面：

图 7-112. 添加网桥多点传送组



3. 定义“VLAN ID”和“New Bridge Multicast Address”（新网桥多点传送地址）字段。
4. 将端口切换为“S”以将该端口加入到选定的多点传送组中。
5. 将端口切换为“F”以禁止将特定多点传送地址添加至特定端口。
6. 单击“Apply Changes”（应用更改）。

系统会将网桥多点传送地址分配至多点传送组，并更新设备。

定义端口以接收多点传送服务

1. 打开“Bridge Multicast Group”（网桥多点传送组）页面。
2. 定义“VLAN ID”和“Bridge Multicast Address”（网桥多点传送地址）字段。
3. 将端口切换为“S”以将该端口加入到选定的多点传送组。
4. 将端口切换为“F”以禁止将特定多点传送地址添加至特定端口。
5. 单击“Apply Changes”（应用更改）。

系统会将端口分配至多点传送组，并更新设备。

分配 LAG 以接收多点传送服务

1. 打开“Bridge Multicast Group”（网桥多点传送组）页面。
2. 定义“VLAN ID”和“Bridge Multicast Address”（网桥多点传送地址）字段。
3. 将 LAG 切换为“S”以将该 LAG 加入到选定的多点传送组中。
4. 将 LAG 切换为“F”以禁止将特定多点传送地址添加至特定 LAG。
5. 单击“Apply Changes”（应用更改）。

系统会将 LAG 分配至多点传送组，并更新设备。

使用 CLI 命令管理多点传送服务成员

下表概括了与“Bridge Multicast Group”（网桥多点传送组）页面中显示的管理多点传送服务成员的选项等效的 CLI 命令。

表 7-76. 多点传送服务成员的 CLI 命令

CLI 命令	说明
bridge multicast address {**MAC 多点传送地址** | **IP 多点传送地址**}	将 MAC 层多点传送地址注册到网桥表，并将静态端口添加至组。
bridge multicast forbidden address {**MAC 多点传送地址** | **IP 多点传送地址**}[**add** | **remove**] {**ethernet 接口列表** | **port-channel 端口信道号列表**}	禁止将特定多点传送地址添加至特定端口。在此命令前加 no 将恢复默认设置。
show bridge multicast address-table [**vlan VLAN** ID] [**address MAC 多点传送地址** | **IP 多点传送地址**] [**format ip** | **mac**]	显示多点传送 MAC 地址表信息。

以下是 CLI 命令的示例：

```
Console> enable

Console# config

console(config)#vlan database

console(config-if)#vlan 8

console(config-if)#exit

console(config)#interface range ethernet g1-9

console(config-if)# switchport mode general

console(config-if)# switchport general allow vlan add 8

console(config)#interface vlan 8

console (config-if)# exit

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

add ethernet g1,g2

Console(config-if)# exit

Console(config)# exit
```

```
Console # show bridge multicast address-table

Vlan    MAC Address          Type        Ports
----    -----------          -----       ----------
1       0100.5e02.0203       static      g1, g2
19      0100.5e02.0208       static      g1-8
19      0100.5e02.0208       dynamic     g9-11

Forbidden ports for multicast addresses:

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

Console # show bridge multicast address-table format ip

Vlan    IP Address           Type        Ports
----    -----------          -----       ----------
1       224-239.130|2.2.3    static      g1, g2
19      224-239.130|2.2.8    static      g1-8
19      224-239.130|2.2.8    dynamic     g9-11

Forbidden ports for multicast addresses:

Vlan    IP Address           Ports
```

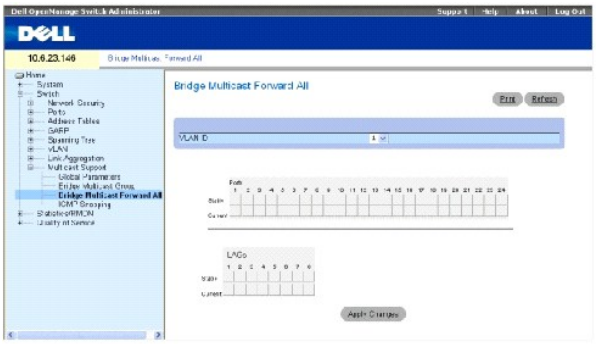
----	----------	----------	
1	224-239.130|2.2.3	g8	
19	224-239.130|2.2.8	g8	

设定全部多点传送参数

“Bridge Multicast Forward All”（网桥全部多点传送）页面包含用于将端口或 LAG 连接至相邻多点传送路由器/交换机所连接的设备的字段。启用 IGMP 监测后，多点传送信息包将被传输至相应的端口或 VLAN。

要打开**“Bridge Multicast Forward All”（网桥全部多点传送）**页面，请在树视图中单击**“Switch”（交换机）→“Multicast Support”（多点传送支持）→“Bridge Multicast”（网桥多点传送）→“Bridge Multicast Forward All”（网桥全部多点传送）**页面。

图 7-113. 网桥全部多点传送



“VLAN ID”— 标识 VLAN。

“Ports”（端口）— 可以添加至多点传送服务的端口。

“LAG”— 可以添加至多点传送服务的 LAG。

网桥全部多点传送路由器/端口控制设置表包含用于管理路由器和端口设置的设置。

表 7-77. 网桥全部多点传送路由器/端口控制设置表

端口控制	定义
D	将端口作为动态端口连接至多点传送路由器或交换机。
S	将端口作为静态端口连接至多点传送路由器或交换机。
F	已禁止。
空白	端口未连接至多点传送路由器或交换机。

将端口连接至多点传送路由器或交换机

1. 打开**“Bridge Multicast Forward All”（网桥全部多点传送）**页面。
2. 定义**“VLAN ID”**字段。

3. 在“**Port**”（**端口**）表中选择一个端口，并设定端口值。
4. 单击“**Apply Changes**”（**应用更改**）。

该端口将被连接至多点传送路由器或交换机。

将 LAG 连接至多点传送路由器或交换机

1. 打开“**Bridge Multicast Forward All**”（**网桥全部多点传送**）页面。
2. 定义“**VLAN ID**”字段。
3. 在“**LAG**”表中选择一个端口，并设定 LAG 值。
4. 单击“**Apply Changes**”（**应用更改**）。

LAG 将被连接至多点传送路由器或交换机。

使用 CLI 命令管理连接至多点传送路由器的 LAG 和端口

下表概括了与“**Bridge Multicast Forward All**”（**网桥全部多点传送**）页面显示的管理连接至多点传送路由器的 LAG 和端口的选项等效的 CLI 命令。

表 7-78. 用于管理连接至多点传送路由器的 LAG 和端口的 CLI 命令

CLI 命令	说明
show bridge multicast filtering VLAN ID	显示多点传送筛选配置。
no 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 接口列表 | port-channel 端口信道号列表}	允许在端口上传输所有多点传送信息包。在此命令前加 no 将恢复默认设置。

以下是 CLI 命令的示例：

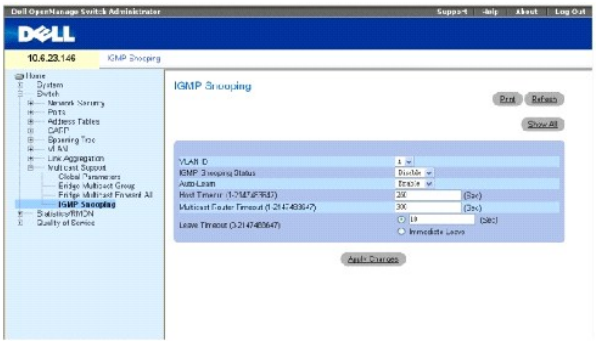
```
console(config)#vlan database

console(config-if)#vlan 8

console(config-vlan)#exit

console(config)#interface range ethernet g1-9

console(config-if)# switchport mode general

console(config-if)# switchport general allow vlan add 8

Console(config-if)# exit

console(config)#interface vlan 8
```

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

add ethernet g1-9

Console(config-if)# exit

Console (config)# interface VLAN 1

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

Console(config-if)# end

Console # show bridge multicast filtering 1

Filtering: Enabled

VLAN:   Forward-All

        Port    Static          Status
        -------  -----------------  -----------
        g1      Forbidden       Filter
        g2      Forward         Forward(s)
        g3      -               Forward(d)
```

IGMP 监测

"IGMP Snooping"（IGMP 监测）页面包含用于添加 IGMP 成员的字段。要打开"IGMP Snooping"（IGMP 监测）页面，请在树视图中单击**"Switch"（交换机）→"Multicast Support"（多点传送支持）→"IGMP Snooping"（IGMP 监测）**。

图 7-114. IGMP 监测



“VLAN ID”— 指定 VLAN ID。

“IGMP Snooping Status”（IGMP 监测状态）— 在 VLAN 上启用或禁用 IGMP 监测。

“Auto Learn”（自动记忆）— 在设备上启用或禁用自动记忆。

“Host Timeout (1-2147483647)”（主机超时 [1-2147483647]）— IGMP 监测条目过期前的时间。默认时间为 260 秒。

“Multicast Router Timeout (1-2147483647)”（多点传送路由器超时 [1-2147483647]）— 多点传送路由器条目过期前的时间。默认值为 300 秒。

“Leave TimeOut (0-2147483647)”（离开超时 [0-2147483647]）— 在接收到端口离开信息之后、条目过期之前的时间（以秒为单位）。**“User-defined”（用户定义）**允许用户定义的超时时段，**“Immediate Leave”（立即离开）**指定立即离开超时时段。默认超时为 10 秒。

在设备上启用 IGMP 监测

1. 打开**“IGMP Snooping”（IGMP 监测）**页面。
2. 为需要启用 IGMP 监测的设备选择 VLAN ID。
3. 在**“IGMP Snooping Status”（IGMP 监测状态）**字段中选择**“Enable”（启用）**。
4. 完成页面中的字段。
5. 单击**“Apply Changes”（应用更改）**。

系统将在设备上启用 IGMP 监测。

显示 IGMP 监测表

1. 打开**“IGMP Snooping”（IGMP 监测）**。
2. 单击**“Show All”（全部显示）**。

系统将打开**“IGMP Snooping Table”（IGMP 监测表）**。

使用 CLI 命令配置 IGMP 监测

下表概括了用于在设备上配置**“IGMP Snooping”（IGMP 监测）**的等效的 CLI 命令。

表 7-79. IGMP 监测的 CLI 命令

CLI 命令	说明
ip igmp snooping	启用因特网组员资格协议 (IGMP) 监测。
ip igmp snooping mrouter learn-pim-dvmrp	启用特定 VLAN 环境中多点传送路由器端口的自动记忆功能。
ip igmp snooping host-time-out 超时	配置主机超时。
ip igmp snooping mrouter-time-out 超时	配置多点传送路由器超时。
ip igmp snooping leave-time-out {**超时** | **立即离开**}	配置离开超时。
`show ip igmp snooping groups [vlan` **VLAN ID**`] [address` **IP 多点传送地址**`]`	显示由 IGMP 监测记忆的多点传送组。
show ip igmp snooping interface VLAN ID	显示 IGMP 监测配置。
show ip igmp snooping mrouter [**interface VLAN ID**]	显示有关动态记忆的多点传送路由器接口的信息。

以下是 `CLI` 命令的示例：

```
Console> enable

Console# config

Console (config)# ip igmp
snooping

Console(config)# interface
vlan 1

Console (config-if)# ip
igmp snooping mrouter
learn-pim-dvmrp

Console (config-if)# ip
igmp snooping host-time-
out 300

Console (config-if)# ip
igmp snooping mrouter-
time-out 200

Console(config-if)# exit

Console(config)# interface
vlan 1

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

Console(config-if)# exit

Console (config)# exit

Console # show ip igmp
snooping groups
```

```
Vlan IP Address Querier
Ports


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


1 224-239.130|2.2.3 Yes
g1, g2


19 224-239.130|2.2.8 Yes
g9-11




Console # show ip igmp
snooping interface 1


IGMP Snooping is globally
enabled


IGMP Snooping is enabled
on VLAN 1


IGMP host timeout is 300
sec


IGMP Immediate leave is
disabled.IGMP leave
timeout is 60 sec


IGMP mrouter timeout is
200 sec


Automatic learning of
multicast router ports is
enabled




Console # show ip igmp
snooping mrouter
```

VLAN	Ports
----	------
1	g1

返回目录页面

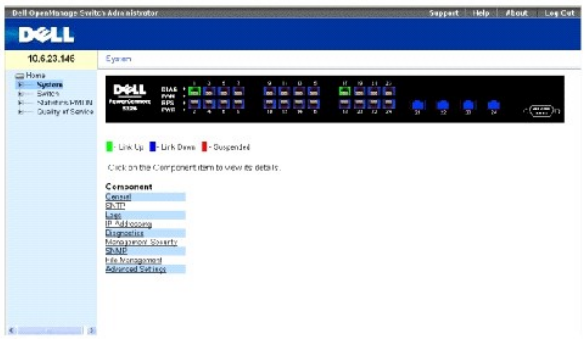
返回目录页面

配置系统信息

Dell™ PowerConnect™ 5324 系统用户指南

本节介绍了用于定义系统参数（包括安全保护功能）、下载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）**。

图 6-15. 系统



定义一般设备信息

“General”（一般）页面包含指向配置设备参数页面的链接。

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）**。

图 6-16. 资产

“System Name (0-160 Characters)”（系统名称 [0 至 160 个字符]）— 定义用户定义的设备名称。

“System Contact (0-160 Characters)”（系统联系人 [0 至 160 个字符]）— 指定联系人的姓名。

“System Location (0-160 Characters)”（系统位置 [0 至 160 个字符]）— 指定系统当前运行的位置。

“MAC Address”（MAC 地址）— 指定设备 MAC 地址。

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

“Service Tag”（服务标签）— 指定维修设备时使用的服务参考号码。

“Asset Tag (0-16 Characters)”（资产标签 [0 至 16 个字符]）— 指定用户定义的设备参考。

“Serial No.”（序列号）— 指定设备序列号。

“Date (DD/MM/YY)”（日期 [DD/MM/YY]）— 指定当前日期。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 表示晚上八点十二分零三秒。

“System Up Time”（系统重设后运行时间）— 指定自上次设备重启动后的时间。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。

要定义系统信息，请：

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

系统将定义系统参数，并更新设备。

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和设置“Asset”（资产）页面中显示的字段的等效 CLI 命令。

表 6-11. 资产 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。
show clock [**detail**]	显示系统时钟的时间和日期。
show system id	显示服务标签信息。
show system	显示系统信息。
asset-tag	设置设备资产标签。

以下是 CLI 命令的示例：

```
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 1qwepot


Console> clock set
13:32:00 7 Dec 2004


Console> show clock


13:32:00 (UTC+0) Dec 7
2004


No time source
```

DELL Switch# **show system**		
System Description:		Ethernet Routing Switch
System Up Time (days,hour:min:sec):		0,00:04:17
System Contact:		spk
System Name:		DELL Switch
System Location:		R&D
System MAC Address:		00:10:b5:f4:00:01
Sys Object ID:		1.3.6.1.4.1.674.10895.3000
Type: PowerConnect 5324		
Power Supply	Status	
------------	--------	
Main	OK	
Redundant	OK	
FAN	Status	
------------	--------	
1	OK	
2	OK	
DELL Switch#		

定义系统时间设置

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

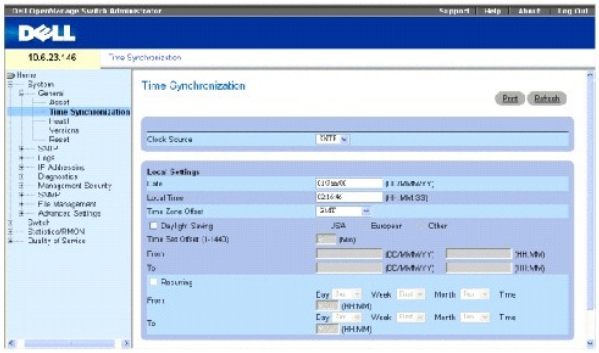
- 阿尔巴尼亚 — 3 月的最后一个周末至 10 月的最后一个周末。
- 澳大利亚 — 从 10 月底至 3 月底。
- 澳大利亚 - 塔斯马尼亚 — 从 10 月初至 3 月底。
- 亚美尼亚 — 3 月的最后一个周末至 10 月的最后一个周末。
- 奥地利 — 3 月的最后一个周末至 10 月的最后一个周末。
- 巴哈马 — 从 4 月至 10 月，与美国夏令时一致。
- 白俄罗斯 — 3 月的最后一个周末至 10 月的最后一个周末。
- 比利时 — 3 月的最后一个周末至 10 月的最后一个周末。
- 巴西 — 从 10 月的第三个星期日至 3 月的第三个星期六。在夏令时期间，巴西东南部大部分地区的时钟向前拨一个小时。
- 智利 — 复活节岛 3 月 9 日至 10 月 12 日。3 月的第一个星期日或 3 月 9 日以后。
- 中国 — 中国不实行夏令时。
- 加拿大 — 从 4 月的第一个星期日至 10 月的最后一个星期日。夏令时通常由省政府和地方政府规定。某些自治区可能存在例外。
- 古巴 — 从 3 月的最后一个星期日至 10 月的最后一个星期日。
- 塞浦路斯 — 3 月的最后一个周末至 10 月的最后一个周末。
- 丹麦 — 3 月的最后一个周末至 10 月的最后一个周末。
- 埃及 — 4 月的最后一个星期五至 9 月的最后一个星期四。
- 爱沙尼亚 — 3 月的最后一个周末至 10 月的最后一个周末。
- 芬兰 — 3 月的最后一个周末至 10 月的最后一个周末。
- 法国 — 3 月的最后一个周末至 10 月的最后一个周末。
- 德国 — 3 月的最后一个周末至 10 月的最后一个周末。
- 希腊 — 3 月的最后一个周末至 10 月的最后一个周末。
- 匈牙利 — 3 月的最后一个周末至 10 月的最后一个周末。
- 印度 — 印度不实行夏令时。
- 伊朗 — 从 3 月 1 日至 9 月 1 日。
- 伊拉克 — 从 4 月 1 日至 10 月 1 日。
- 爱尔兰 — 3 月的最后一个周末至 10 月的最后一个周末。
- 以色列 — 根据年份不同而有所变化。
- 意大利 — 3 月的最后一个周末至 10 月的最后一个周末。
- 日本 — 日本不实行夏令时。
- 约旦 — 3 月的最后一个周末至 10 月的最后一个周末。
- 拉脱维亚 — 3 月的最后一个周末至 10 月的最后一个周末。
- 黎巴嫩 — 3 月的最后一个周末至 10 月的最后一个周末。
- 立陶宛 — 3 月的最后一个周末至 10 月的最后一个周末。
- 卢森堡 — 3 月的最后一个周末至 10 月的最后一个周末。
- 马其顿 — 3 月的最后一个周末至 10 月的最后一个周末。
- 墨西哥 — 从 4 月第一个星期日 02:00 至 10 月最后一个星期日 02:00。
- 摩尔多瓦 — 3 月的最后一个周末至 10 月的最后一个周末。
- 黑山 — 3 月的最后一个周末至 10 月的最后一个周末。
- 荷兰 — 3 月的最后一个周末至 10 月的最后一个周末。
- 新西兰 — 从 10 月的第一个星期日至 3 月的第一个星期日或 3 月 15 日以后。
- 挪威 — 3 月的最后一个周末至 10 月的最后一个周末。
- 巴拉圭 — 从 4 月 6 日至 9 月 7 日。
- 波兰 — 3 月的最后一个周末至 10 月的最后一个周末。
- 葡萄牙 — 3 月的最后一个周末至 10 月的最后一个周末。
- 罗马尼亚 — 3 月的最后一个周末至 10 月的最后一个周末。
- 俄罗斯 — 从 3 月 29 日至 10 月 25 日。

- 塞尔维亚 — 3 月的最后一个周末至 10 月的最后一个周末。
- 斯洛伐克共和国 — 3 月的最后一个周末至 10 月的最后一个周末。
- 南非 — 南非不实行夏令时。
- 西班牙 — 3 月的最后一个周末至 10 月的最后一个周末。
- 瑞典 — 3 月的最后一个周末至 10 月的最后一个周末。
- 瑞士 — 3 月的最后一个周末至 10 月的最后一个周末。
- 叙利亚 — 从 3 月 31 日至 10 月 30 日。
- 台湾地区 — 台湾地区不实行夏令时。
- 土耳其 — 3 月的最后一个周末至 10 月的最后一个周末。
- 英国 — 3 月的最后一个周末至 10 月的最后一个周末。
- 美国 — 从 4 月第一个星期日 02:00 至 10 月最后一个星期日 02:00。

有关 SNTP 的详细信息，请参阅“**配置 SNTP 设置**”。

要打开**“Time Synchronization”（时间同步）**页面，请在**树视图**中单击**“System”（系统）→“General”（一般）→“Time Synchronization”（时间同步）**。

图 6-17. 时间同步



时钟源

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

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

“None”（无）— 指定不通过外部源设置系统时间。

本地设置

“Date”（日期）— 定义系统日期。日期字段格式为日、月、年；例如，04 May 2050。

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

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

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

“Recurring”（常年定期）区域。

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

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

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

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

“From”（从）— 定义美国或欧洲以外国家/地区的 DST 开始时间；格式为：日月年占用一个字段，时间占用另一个字段。例如，DST 开始于 2007 年 10 月 25 日 5:00 am，则这两个字段分别为 25Oct07 和 5:00。可能的字段值包括：

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

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

“Year”（年份）— 配置的 DST 开始的年份。

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

“To”（至）— 定义美国或欧洲以外国家/地区的 DST 结束时间；格式为：日月年占用一个字段，时间占用另一个字段。例如，DST 结束于 2008 年 3 月 23 日 12:00 am，则这两个字段分别为 23Mar08 和 12:00。可能的字段值包括：

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

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

“Year”（年份）— 配置的 DST 结束的年份。

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

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

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

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

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

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

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

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

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

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

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

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

选择时钟源

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

系统将选定时钟源，并更新设备。

定义本地时钟设置

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

系统将应用本地时钟设置。

定义外部 SNTP 时钟设置

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

系统将应用外部时钟设置。

使用 CLI 命令定义时钟设置

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

表 6-12. 时钟设置 CLI 命令

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

clock summer-time date 日 月 年 hh:mm 日 月 年 hh:mm [offset 偏移] [zone 缩写]	将系统配置为在特定时期自动切换至夏季时间（夏令时）- 日/月/年格式。

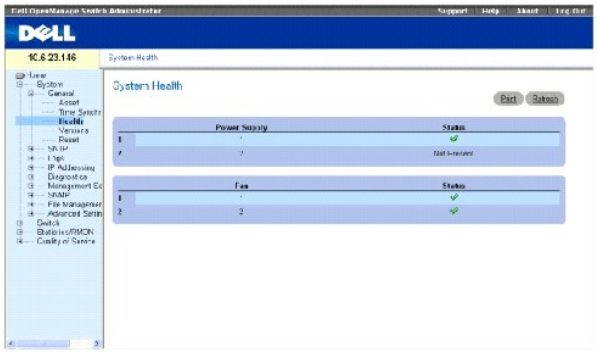
以下是 CLI 命令的示例：

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


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

查看系统运行状况信息

"System Health"（系统运行状况）页面显示物理设备硬件信息。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）**。

图 6-18. 系统运行状况



"Power Supply Status"（电源设备状态）— 主电源设备的状态。可能的字段值包括：

— 指定装置的主电源设备运行正常。

— 指定装置的主电源设备运行不正常。

"Not Present"（不存在）— 指定装置没有电源设备。

"Fan"（风扇）— 设备风扇的状态。可能的字段值包括：

— 指定装置的风扇运行正常。

— 指定装置的风扇运行不正常。

"Not Present"（不存在）— 指定装置没有风扇。

使用 CLI 命令查看系统运行状况信息

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

表 6-13. 系统运行状况 CLI 命令

CLI 命令	说明
show system	显示系统信息。

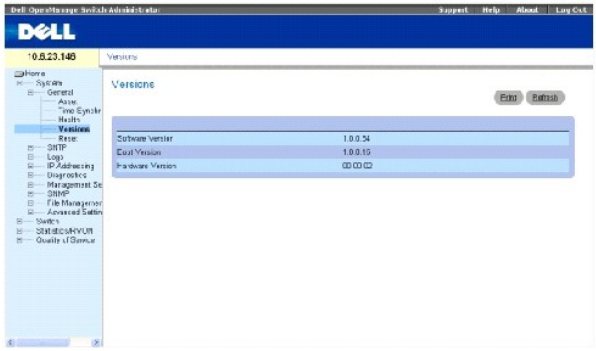
```
DELL Switch# show system

System Description:                      Ethernet Routing Switch

System Up Time (days,hour:min:sec):      0,00:04:17

System Contact:                          spk

System Name:                             DELL Switch

System Location:                         R&D

System MAC Address:                      00:10:b5:f4:00:01

Sys Object ID:                           1.3.6.1.4.1.674.10895.3000

Type: PowerConnect 5324

Power Supply                 Status
-------------                --------
Main                         OK
Redundant                    OK

FAN                          Status
-------------                --------
1                            OK
2                            OK
```

DELL Switch#		

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）。

图 6-19. 版本



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

“Boot Version”（引导版本）— 设备上当前运行的引导版本。

“Hardware Version”（硬件版本）— 设备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。

表 6-14. 版本 CLI 命令

CLI 命令	说明
show version	显示系统版本信息。

以下是 CLI 命令的示例：

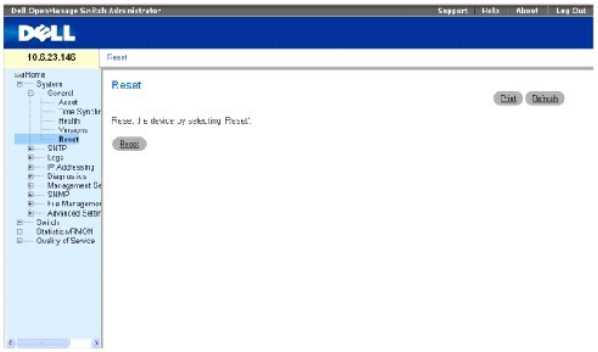
```
Console> show version

SW version x.xxx (date 23-Jul-xxxx time 17:34:19)
```

```
Boot version x.xxx (date 17-Jan-xxxx time 11:48:21)


HW version x.x.x
```

重启动设备

“Reset”（重启动）页面使您可以远程重启动设备。要打开**“Reset”（重启动）**页面，请在树视图中单击**“System”（系统）→“General”（一般）→“Reset”（重启动）**。

图 6-20. 重启动



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

重启动设备

1. 打开**“Reset”（重启动）**页面
2. 单击**“Reset”（重启动）**。

   系统将显示一条确认信息。
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。
4. 输入用户名和密码以重新连接至 Web 界面。

使用 CLI 重启动设备

下表概括了用于通过 CLI 执行设备重启动的等效 CLI 命令。

表 6-15. 重启动 CLI 命令

CLI 命令	说明
reload	重新加载操作系统。

以下是 CLI 命令的示例：

```
```

```
Console >reload



This command will reset
the whole system and
disconnect your current



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

配置 SNTP 设置

设备支持简单网络时间协议 (SNTP)。SNTP 可以确保精确到毫秒的网络设备时钟时间同步。时间同步由网络 SNTP 服务器来执行。本设备仅作为 SNTP 客户端运行，而无法为其它系统提供时间服务。

设备可以向以下服务器类型轮询服务器时间：

- 单点传送
- 任意点传送
- 广播

时间源通过时间服务器来建立。时间服务器定义参考时钟的精度。时间服务器越高（最高为零），时钟越准确。设备从 1 层和更高层接收时间。

以下是层的示例：

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

系统将根据时间级别和服务器类型对从 SNTP 服务器接收到的信息进行评估。

通过以下时间级别来评定和确定 SNTP 时间定义：

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

轮询单点传送时间信息

轮询单点传送信息用于轮询 IP 地址已知的服务器。T1 至 T4 用于确定服务器时间。这是同步交换机时间的首选方法。

轮询任意点传送时间信息

服务器 IP 地址未知时，可以使用轮询任意点传送信息。返回响应的第一个任意点传送服务器用于设置时间值。时间级别 T3 和 T4 用于确定服务器时间。对于同步交换机时间，使用任意点传送时间信息比使用广播时间信息更好。

广播时间信息

服务器 IP 地址未知时，可以使用广播信息。SNTP 服务器发送广播信息时，SNTP 客户端侦听响应。SNTP 客户端既不发送时间信息请求，也不接收广播服务器的响应。

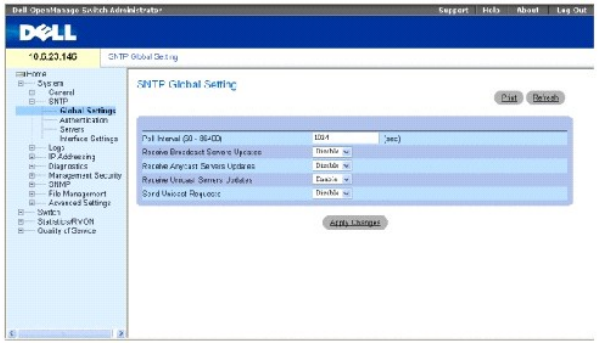
MD5 (Message Digest 5) 验证可以维护到 SNTP 服务器的交换机同步路径的安全。MD5 是一种生成 128 位散列的算法。MD5 由 MD4 演变而来，并且安全保护性能比 MD4 更强。MD5 验证通信的完整性，并验证通信的起点。

在树视图中单击**“System”（系统）→“SNTP”**可以打开**“SNTP”**页面。

定义 SNTP 全局参数

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

图 6-21. SNTP 全局设置



“Poll Interval (60-86400)”（轮询间隔 [60 至 86400]）— 定义向 SNTP 服务器轮询单点传送信息的时间间隔（以秒为单位）。

“Receive Broadcast Servers Updates”（接收广播服务器更新）— 向 SNTP 服务器轮询选定接口上的广播服务器时间信息。

“Receive Anycast Servers Updates”（接收任意点传送服务器更新）— 向 SNTP 服务器轮询任意点传送服务器时间信息（启用时）。如果同时启用**“Receive Anycast Servers Update”（接收任意点传送服务器更新）**和**“Receive Broadcast Servers Update”（接收广播服务器更新）**字段，则依据任意点传送服务器时间信息设置系统时间。

“Receive Unicast Servers Updates”（接收单点传送服务器更新）— 向 SNTP 服务器轮询单点传送服务器时间信息（启用时）。如果同时启用**“Receive Broadcast Servers Updates”（接收广播服务器更新）**、**“Receive Anycast Servers Updates”（接收任意点传送服务器更新）**和**“Receive Unicast Servers Updates”（接收单点传送服务器更新）**字段，则依据单点传送服务器时间信息设置系统时间。

“Poll Unicast Servers”（轮询单点传送服务器）— 向 SNTP 服务器发送 SNTP 单点传送传输信息（启用时）。

使用 CLI 命令定义 SNTP 全局参数

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

表 6-16. SNTP 全局参数 CLI 命令

CLI 命令	说明
sntp broadcast client enable	启用 SNTP 广播客户端

sntp unicast client enable	启用 SNTP 预定义的单点传送客户端

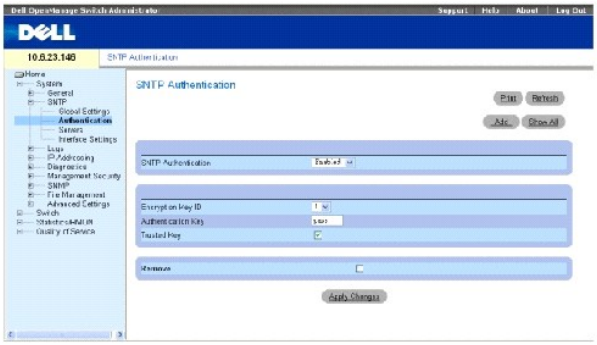
以下是 CLI 命令的示例：

```
console> enable

console# configure

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

定义 SNTP 验证方法

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

图 6-22. SNTP 验证



“SNTP Authentication”（SNTP 验证）— 启用（该选项）时，将启用在设备和 SNTP 服务器之间的 SNTP 会话的验证。

“Encryption Key ID”（密钥 ID）— 定义用于验证 SNTP 服务器和设备的关键字标识。该字段值最多可以为 4294967295 个字符。

“Authentication Key”（验证关键字）（1 至 8 个字符）— 指定用于验证的关键字。

“Trusted Key”（信任关键字）— 指定用于验证 SNTP 服务器的密钥。

“Remove”（删除）— 选取该字段时，将删除选定的关键字。

添加 SNTP 验证关键字

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

   系统将打开**“Add Authentication Key”（添加验证关键字）**页面。

图 6-23. 添加验证关键字

3. 定义各字段。
4. 单击**“Apply Changes”（应用更改）**。

系统将添加 SNTP 验证关键字，并更新设备。

显示验证关键字表

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

系统将打开**“Authentication Key Table”（验证关键字表）**。

图 6-24. 验证关键字表

删除验证关键字

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

系统将打开**“Authentication Key Table”（验证关键字表）**。

3. 选择一个**“Authentication Key Table”（验证关键字表）**条目。
4. 选取**“Remove”（删除）**复选框。
5. 单击**“Apply Changes”（应用更改）**。

系统将删除条目，并更新设备。

使用 CLI 命令定义 SNTP 验证设置

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

表 6-17. SNTP 验证 CLI 命令

CLI 命令	说明
sntp authenticate	定义从服务器接收到的网络时间协议通信的验证。
sntp authentication-key 数字 md5 值	定义 SNTP 的验证关键字。

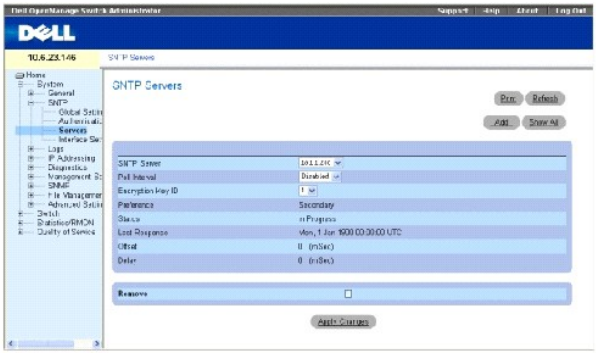
以下是 CLI 命令的示例：

```
console> enable

console# configure

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

Console(config)# sntp
trusted-key 8

Console(config)# sntp
authenticate
```

定义 SNTP 服务器

“SNTP Servers”（SNTP 服务器）页面包含用于启用 SNTP 服务器以及添加新的 SNTP 服务器的信息。此外，“SNTP Servers”（SNTP 服务器）页面使设备可以从服务器请求和接受 SNTP 通信。**要打开**“SNTP Servers”（SNTP 服务器）页面，请在**树视图**中单击“**System**”（**系统**）→“**SNTP**”→“**SNTP Servers**”（**SNTP 服务器**）。

图 6-25. SNTP 服务器



“SNTP Server”（SNTP 服务器）— 输入用户定义的 SNTP 服务器 IP 地址或主机名。最多可以定义八个 SNTP 服务器。该字段可以包含 1 至 158 个字符。

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

“Encryption Key ID”（密钥 ID）— 指定用于 SNTP 服务器和设备之间通信的关键字标识。范围是 1 至 4294967295。

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

“Primary”（主）— 主服务器提供 SNTP 信息。

“Secondary”（次）— 备份服务器提供 SNTP 信息。

“Status Up”（运行状态） — SNTP 服务器的运行状态。可能的字段值包括：

“Up”（良好） — SNTP 服务器当前运行正常。

“Down”（断开） — SNTP 服务器当前运行不正常。

“Unknown”（未知） — SNTP 服务器状态当前未知。

“Last Response”（上一次响应） — 上一次接收到 SNTP 服务器响应的时间。

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

“Delay”（延迟） — 到达 SNTP 服务器所需的时间。

“Remove”（删除） — 如果选择该选项，将从**“SNTP Server”（SNTP 服务器）**列表中删除特定的 SNTP 服务器。

添加 SNTP 服务器

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

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

图 6-26. 添加 SNTP 服务器

3. 定义各字段。
4. 单击**“Apply Changes”（应用更改）**。

   系统将添加 SNTP 服务器，并更新设备。

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

表 6-18. SNTP 服务器 CLI 命令

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

以下是 CLI 命令的示例：

```
console> enable
```

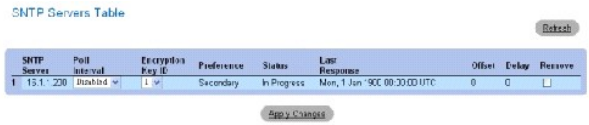
```
console# configure


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

显示 SNTP 服务器表

1. 打开**“SNTP Servers”（SNTP 服务器）**页面。
2. 单击**“Show All”（全部显示）**。

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

图 6-27. SNTP 服务器表



修改 SNTP 服务器

1. 打开**“SNTP Servers”（SNTP 服务器）**页面。
2. 单击**“Show All”（全部显示）**。

   系统将打开**“SNTP Servers Table”（SNTP 服务器表）**。
3. 选择一个 SNTP 服务器条目。
4. 修改相关的字段。
5. 单击**“Apply Changes”（应用更改）**。

   系统将更新 SNTP 服务器信息。

删除 SNTP 服务器

1. 打开**“SNTP Servers”（SNTP 服务器）**页面。
2. 单击**“Show All”（全部显示）**。

   系统将打开**“SNTP Servers Table”（SNTP 服务器表）**。
3. 选择一个 **SNTP 服务器**条目。
4. 选取**“Remove”（删除）**复选框。
5. 单击**“Apply Changes”（应用更改）**。

   系统将删除条目，并更新设备。

使用 CLI 命令定义 SNTP 服务器设置

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

表 6-19. SNTP 服务器 CLI 命令

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

以下是 CLI 命令的示例：

```
console> enable

console# configure

Console(config)# sntp server 100.1.1.1 poll key 10

Console# show sntp status

Clock is synchronized, stratum 4, reference is 176.1.1.8

Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)

Unicast servers:
```

Server	Preference	Status	Last response	Offset [mSec]	Delay [mSec]
---------	----------	-------	---------------	------	------
176.1.1.8	Primary	Up	AFE252C1.6DBDDFF2	7.33	117.79
176.1.8.179	Secondary	Unknown	AFE21789.643287C9	8.98	189.19

```
Anycast server:
```

Server	Preference	Status	Last response	Offset [mSec]	Delay [mSec]
-------	----------	-------	--------------	-----	------
VLAN 119	Secondary	Up	19:53:21.789 PDT Feb 19 2002	7.19	119.89

Broadcast:		
Interface	IP address	Last response
----------	----------	----------
176.1.1.8	Primary	AFE252C1.6DBDDFF2
176.1.8.179	Secondary	AFE21789.643287C9

定义 SNTP 接口

“SNTP Broadcast Interface Table”（SNTP 广播接口表）包含用于设置不同接口上的 SNTP 的字段。要打开**“SNTP Broadcast Interface Table”（SNTP 广播接口表）**，请单击**“System”（系统）→“SNTP”→“Interfaces Settings”（接口设置）**。

“SNTP Broadcast Interface Table”（SNTP 广播接口表）包含以下字段：

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

“Receive Server Updates”（接收服务器更新）— 启用或禁用特定接口。

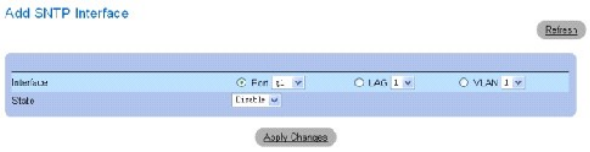
“Remove”（删除）— 如果选择该选项，将从特定接口删除 SNTP。

添加 SNTP 接口

1. 打开**“SNTP Broadcast Interface Table”（SNTP 广播接口表）**页面。
2. 单击**“Add”（添加）**。

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

图 6-28. “Add SNTP Interface”（添加 SNTP 接口）页面



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

   系统将添加 SNTP 接口，并更新设备。

使用 CLI 命令定义 SNTP 接口设置

下表概括了用于设置**“SNTP Broadcast Interface Table”（SNTP 广播接口表）**页面中显示的字段的等效 CLI 命令。

表 6-20. SNTP 广播 CLI 命令

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

以下是 CLI 命令的示例：

```
Console# show sntp configuration

Polling interval: 7200 seconds.

MD5 Authentication keys: 8, 9

Authentication is required for synchronization.

Trusted Keys: 8,9

Unicast Clients Polling:Enabled.

Server                          Polling     Encryption Key
------------                    --------    -----------------
176.1.1.8                       Enabled     9
176.1.8.179                     Disabled    Disabled

Broadcast Clients: Enabled

Broadcast Clients Poll: Enabled

Broadcast Interfaces: g1, g3
```

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）**。

“Logs”（日志）页面包含指向各种日志页面的链接。

定义全局日志参数

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

事件信息具有唯一的格式，即按照 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会被分配一个严重性代码，并包含一个信息助记符，用于标识生成信息的源应用程序。允许按照紧急性或相关性筛选信息。每条信息的严重性决定了每个事件记录发送的事件记录设备集。

下表包含日志严重性级别：

表 6-21. 日志严重性级别

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

“Global Log Parameters”（全局日志参数）页面包含用于定义将哪些事件记录到哪些日志的字段。该页面包含用于全局启用日志的字段，以及用于定义日志参数的参数。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）**。

图 6-29. 全局日志参数

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

“Severity”（严重性）— 以下为可用的严重性日志：

“Emergency”（紧急）— 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）— 第二级警告。如果设备出现严重故障（例如，所有设备功能停止运行），系统将保存警报日志。

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

“Error”（错误）— 出现设备错误；例如，单个端口脱机。

“Warning”（警告）— 最低级设备警告。设备可以工作，但出现运行问题。

“Notice”（注意）— 提供设备信息。

“Informational”（信息）— 提供设备信息。

“Debug”（调试）— 提供调试信息。

注：选定严重性级别后，所有高于此级别的严重性级别都将被自动选定。

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

“Console”（控制台）— 发送到控制台的日志的最低严重性级别。

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

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

要启用日志，请：

1. 打开**“Global Log Parameters”（全局日志参数）页面**。
2. 在**“Logging”（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

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

表 6-22. 全局日志参数 CLI 命令

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

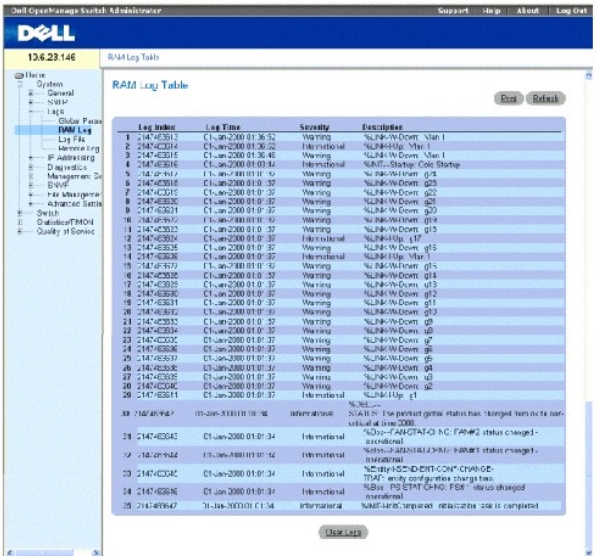
以下是 CLI 命令的示例：

```
Console (config)# logging
on


Console (config)# logging
console errors


Console (config)# logging
buffered debugging


Console (config)# logging
file alerts


Console (config)# clear
logging


Console (config)# exit


Console# clear logging
file


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

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）**，请在树视图中单击**"System"（系统）→"Logs"（日志）→"RAM Log"（RAM 日志）**。

图 6-30. RAM 日志表



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

“Log Time”（记录时间）— 说明日志输入**“RAM Log Table”（RAM 日志表）**的时间。

“Severity”（严重性）— 说明日志严重性。

“Description”（说明）— 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）**。
2. 单击**“Clear Log”（清除日志）**。

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

使用 CLI 命令查看和清除 RAM 日志表中的字段

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

表 6-23. RAM 日志表 CLI 命令

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

以下是 CLI 命令的示例：

```
console# show logging

Logging is enabled.

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

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

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

1 messages were not logged

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

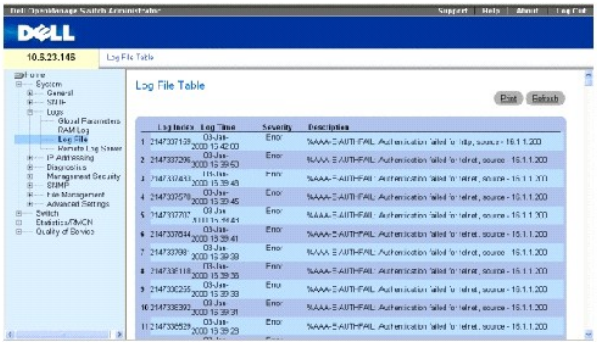
```
01-Jan-2000 01:01:36 :%
LINK-W-Down: g24


01-Jan-2000 01:01:36 :%
LINK-W-Down: g23


01-Jan-2000 01:01:36 :%
LINK-W-Down: g22


01-Jan-2000 01:01:36 :%
LINK-W-Down: g21


01-Jan-2000 01:01:36 :%
LINK-W-Down: g20


01-Jan-2000 01:01:36 :%
LINK-W-Down: g19


01-Jan-2000 01:01:36 :%
LINK-W-Down: g18


01-Jan-2000 01:01:36 :%
LINK-W-Down: g17


01-Jan-2000 01:01:36 :%
LINK-W-Down: g13


1-Jan-2000 01:01:36 :%
LINK-W-Down: g2


01-Jan-2000 01:01:36 :%
LINK-W-Down: g1




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




Console # clear logging


clear logging buffer
[y/n]?


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），请在树

视图中单击“System”（系统）→“Logs”（日志）→“Log File”（日志文件）。

图 6-31. 日志文件表



“Log Index”（日志索引）— **“Log File Table”（日志文件表）**中的日志编号。

“Log Time”（记录时间）— 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）— 日志信息文本。

使用 CLI 命令显示日志文件表

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

表 6-24. 日志文件表 CLI 命令

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

以下是 CLI 命令的示例：

```
Console # show
logging file


Logging is enabled.


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


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

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

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

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

1 messages were not logged

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

01-Jan-2000 01:11:49 :%LINK-I-Up: g21

01-Jan-2000 01:11:49 :%2SWPHY-I-CHNGCOMBOMEDIA: Media changed from copper media

to fiber media (1000BASE-SX) on port g21.

01-Jan-2000 01:11:48 :%2SWPHY-I-CHNGCOMBOMEDIA:Media changed from fiber media to copper media on port g21.

01-Jan-2000 01:11:48 :%LINK-W-Down: g21

01-Jan-2000 01:11:46 :%LINK-I-Up: g19

01-Jan-2000 01:11:42 :%LINK-W-Down: g14

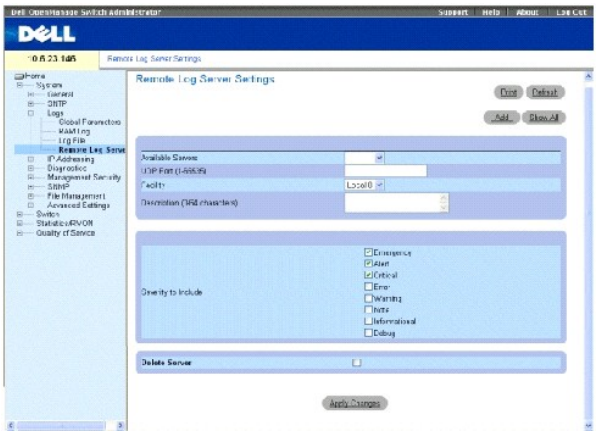
01-Jan-2000 01:11:41 :%LINK-I-Up: g14

```
01-Jan-2000
01:11:36 :%LINK-W-
Down: g9



01-Jan-2000
01:11:35 :%LINK-I-Up:
g1



01-Jan-2000
01:11:34 :%LINK-W-
Down: g1



console#
```

配置“Remote Log Server Settings”（远程日志服务器设置）页面

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

图 6-32. 远程日志服务器设置



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

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

“Facility”（设施）— 定义从其向远程服务器发送系统日志的用户定义的应用程序。只能将一个设备分配至单个服务器。如果分配了第二级设备，则第一级设备将被代替。为设施定义的所有应用程序在服务器上使用同一设备。可能的字段值包括：

“Local 0”（本地 0）至“Local 7”（本地 7）。

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

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

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

要将日志发送至服务器，请：

1. 打开"Remote Log Server Settings"（远程日志服务器设置）页面。
2. 在"Available Servers"（可用服务器）下拉列表中选择服务器。
3. 定义各字段。
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）。

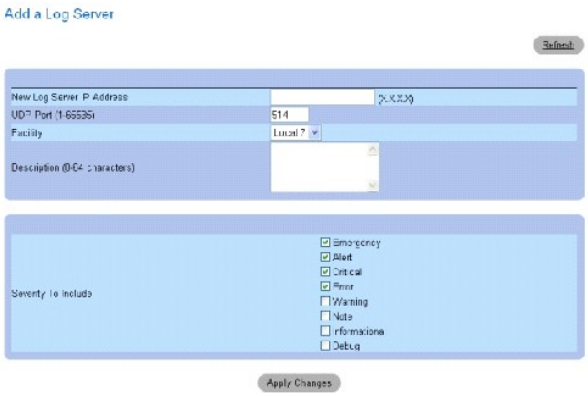
系统将保存日志设置，并更新设备。

要定义新服务器，请：

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

系统将打开"Add a Log Server"（添加日志服务器）页面。

图 6-33. 添加日志服务器



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

3. 定义各字段。
4. 单击"Apply Changes"（应用更改）。

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

要显示远程日志服务器表，请：

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

系统将打开"Remote Log Servers Table"（远程日志服务器表）页面。

图 6-34. 远程日志服务器表

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

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

   系统将打开**“Remote Log Servers Table”（远程日志服务器表）**页面。
3. 选择一个**“Remote Log Servers Table”（远程日志服务器表）**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**“Remote Log Servers Table”（远程日志服务器表）**条目，并更新设备。

使用 CLI 命令处理远程服务器日志

下表概括了用于处理远程服务器日志的等效 CLI 命令。

表 6-25. 远程日志服务器 CLI 命令

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

以下是 CLI 命令的示例：

```
console> enable

console# configure

console (config) # logging
10.1.1.1 severity critical

Console# show logging

Logging is enabled.

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

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



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



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



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



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



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



1 messages were not logged



03-Mar-2004 12:02:03 :%
LINK-I-Up: g1



03-Mar-2004 12:02:01 :%
LINK-W-Down: g2



03-Mar-2004 12:02:01 :%
LINK-I-Up: g3
```

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）**。

定义默认网关

“Default Gateway”（默认网关）页面包含用于分配网关设备的字段。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）**。

“Default Gateway”（默认网关）页面包含以下字段：

“Default Gateway”（默认网关）— 网关设备 IP 地址。

“Remove”（删除）— 如果选择该选项，将从**“Default Gateway”（默认网关）**下拉列表中删除网关设备。

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，并更新设备。

要删除默认网关设备，请：

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

系统将删除默认网关条目，并更新设备。

使用 CLI 命令定义网关设备

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

表 6-26. 默认网关 CLI 命令

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

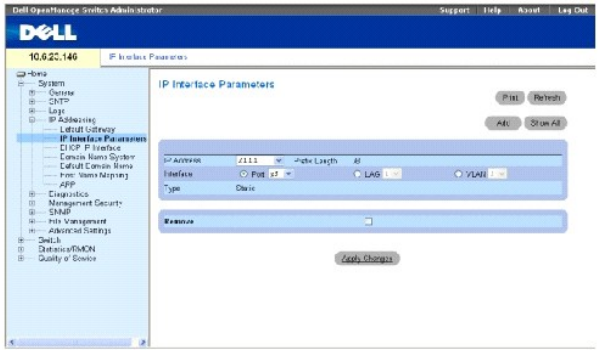
以下是 CLI 命令的示例：

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



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

定义 IP 接口

“IP Interface Parameters”（IP 接口参数）页面包含用于为接口分配 IP 参数的字段。要打开**“IP 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）→“Interface Parameters”（接口参数）**。

图 6-35. IP 接口参数



"IP Address"（IP 地址）— 接口 IP 地址。

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

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

有关详情，请参阅 "配置 VLAN"。

"Type"（类型）— 表示是否静态配置 IP 地址。

"Forward Directed IP Broadcasts"（传输定向 IP 广播）— 启用定向广播到物理广播的转换。禁用则丢弃 IP 定向广播并且不对其进行传输。

"Broadcast Type"（广播类型）— 定义接口广播地址。

"One Fill"（全填充）— 接口广播地址为全填充 (255.255.255.255)。

"Zero Fill"（零填充）— 接口广播地址为零填充 (0.0.0.0)。

"Remove"（删除）— 如果选择该选项，将从**"IP Address"（IP 地址）**下拉式菜单中删除接口。

添加 IP 接口

1. 打开**"IP Interface Parameters"（IP 接口参数）**页面。
2. 单击**"Add"（添加）**。

系统将打开**"Add a Static Interface"（添加静态接口）**页面。

图 6-36. 添加静态接口

3. 完成页面中的字段。

   “Network Mask”（网络掩码）用于指定源 IP 地址的子网掩码。

4. 单击**“Apply Changes”（应用更改）**。

   系统将添加新接口，并更新设备。

修改 IP 地址参数

1. 打开**“IP Interface Parameters”（IP 接口参数）**页面。
2. 在**“IP Address”（IP 地址）**下拉式菜单中选择一个 IP 地址。
3. 修改所需的字段。
4. 单击**“Apply Changes”（应用更改）**。

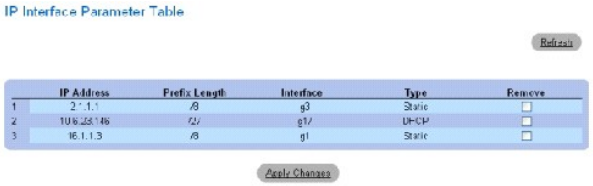
   系统将修改参数，并更新设备。

删除 IP 地址

1. 打开**“IP Interface Parameters”（IP 接口参数）**页面。
2. 单击**“Show All”（全部显示）**。

   系统将打开**“Interface Parameters Table”（接口参数表）**。

图 6-37. IP 接口参数表



3. 选择一个 IP 地址并选取**“Remove”（删除）**复选框。
4. 单击**“Apply Changes”（应用更改）**。

   系统将删除选定的 IP 地址，并更新设备。

使用 CLI 命令定义 IP 接口

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

表 6-27. IP 接口参数 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 命令的示例：

```
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)#
exitconsole# show ip
interface vlan 1

Output

Gateway IP Address Activity status

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

192.168.1.1 Active

IP address Interface Type

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

192.168.1.123 /24 VLAN 1 Static
```

定义 DHCP IP 接口参数

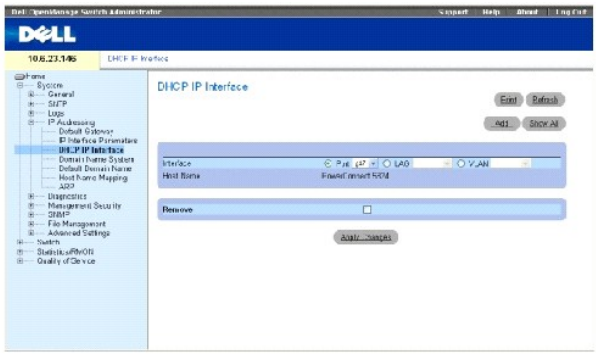
```
console# show ip interface vlan 1
```

输出

Gateway IP Address	Activity status	
----------	----------	
192.168.1.1	Active	
IP address	Interface	Type
----------	----------	----------
192.168.1.123 /24	VLAN 1	Static

"DHCP IP Interface"（DHCP IP 接口）页面包含用于指定连接至设备的 DHCP 客户端的字段。请在树视图中单击**"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**。

图 6-38. DHCP IP 接口



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

"Host Name"（主机名称）— 系统名称。该字段最多可以包含 20 个字符。

“Remove”（删除） — 如果选择该选项，将删除 DHCP 客户端。

添加 DHCP 客户端

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

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

   系统将添加 DHCP 接口，并更新设备。

修改 DHCP IP 接口

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

   系统将修改条目，并更新设备。

删除 DHCP IP 接口

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

   系统将打开**“DHCP Client Table”（DHCP 客户端表）**。
3. 选择 DHCP 客户端条目。
4. 选取**“Remove”（删除）**复选框。
5. 单击**“Apply Changes”（应用更改）**。

   系统将删除选定的条目，并更新设备。

使用 CLI 命令定义 DHCP IP 接口

下表概括了用于定义 DHCP 客户端的等效 CLI 命令。

表 6-28. DHCP IP 接口 CLI 命令

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

以下是 CLI 命令的示例：

```
```

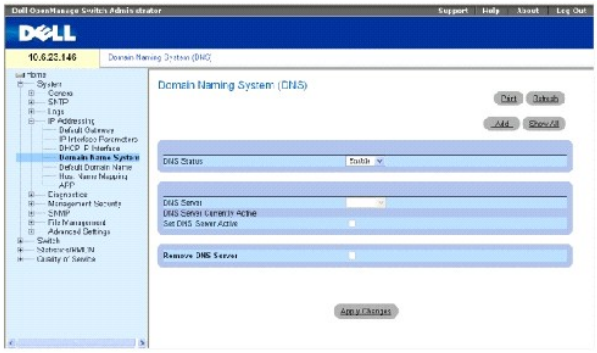
```
console> enable



console# config



console (config#)
interface ethernet g1



console (config-if)# ip
address dhcp 10.0.0.1 /8
```

配置域名系统

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

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

图 6-39. 域命名系统 (DNS)



“DNS Status”（DNS 状态）— 启用或禁用将 DNS 域名转换为 IP 地址。

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

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

“Set DNS Server Active”（将 DNS 服务器设置为活动状态）— 激活在**“DNS Server”（DNS 服务器）**字段中选定的 DNS 服务器。

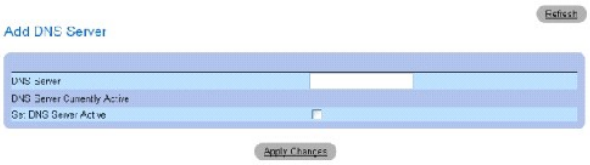
“Remove DNS Server”（删除 DNS 服务器）— 如果选择该选项，将删除 DNS 服务器。

添加 DNS 服务器

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

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

图 6-40. 添加 DNS 服务器



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

系统将定义新的 DNS 服务器，并更新设备。

显示 DNS 服务器表

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

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

图 6-41. DNS 服务器表

删除 DNS 服务器

1. 打开“**Domain Naming System (DNS)**”（**域命名系统 [DNS]**）页面。
2. 单击“**Show All**”（**全部显示**）。
3. 系统将打开“**DNS Server Table**”（**DNS 服务器表**）。
4. 选择一个“**DNS Server Table**”（**DNS 服务器表**）**条目**。
5. 选取“**Remove**”（**删除**）复选框。
6. 单击“**Apply Changes**”（**应用更改**）。

系统将删除选定的 DNS 服务器，并更新设备。

使用 CLI 命令配置 DNS 服务器

下表概括了用于配置设备系统信息的 CLI 命令。

表 6-29. DNS 服务器 CLI 命令

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

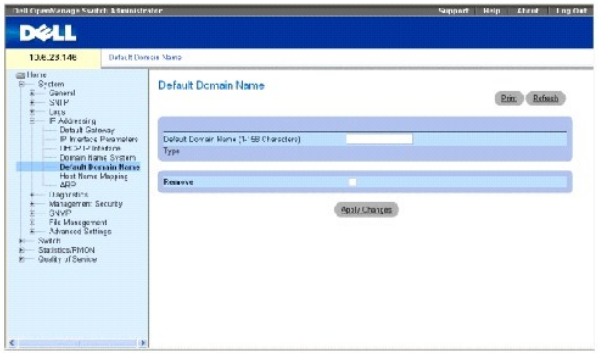
以下是 CLI 命令的示例：

```
console> enable


Console# configure


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

定义默认域

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

图 6-42. 默认域名



“Default Domain Name (1-158 characters)”（默认域名 [1 至 158 个字符]）— 包含用户定义的 DNS 域名服务器。如果选择该选项，则 DNS 域名为默认域。

“Type”（类型）— 域类型，静态还是动态创建域。

“Remove”（删除）— 如果选择该选项，将删除选定的域。

使用 CLI 命令定义 DNS 域名

下表概括了用于配置 DNS 域名的 CLI 命令。

表 6-30. DNS 域名 CLI 命令

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

以下是 CLI 命令的示例：

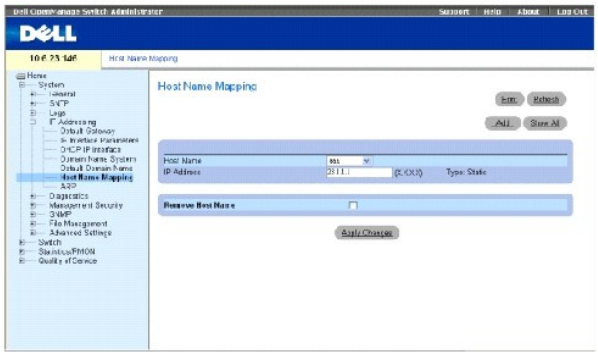
```
console> enable


console# configure
```

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

映射域主机

“Host Name Mapping”（主机名称映射）页面提供用于分配静态主机名称 IP 地址的参数。**“Host Name Mapping”（主机名称映射）**页面可以为每个主机最多提供八个 IP 地址。要打开**“Host Name Mapping”（主机名称映射）**页面，请单击**“System”（系统）→“IP Addressing”（IP 定址）→“Host Name Mapping”（主机名称映射）**。

图 6-43. 主机名称映射



“Host Name”（主机名称）— 包含主机名称列表。主机名称在**“Add Host Name Mapping”（添加主机名称映射）**页面中定义。每个主机最多提供八个 IP 地址。**“Host Name”（主机名称）**字段的字段值包括：

“IP Address”（IP 地址）(X.X.X.X) — 最多提供八个分配给指定的主机名称的 IP 地址。

“Type”（类型）— IP 地址类型。可能的字段值包括：

“Dynamic”（动态）— 动态创建 IP 地址。

“Static”（静态）— IP 地址是静态 IP 地址。

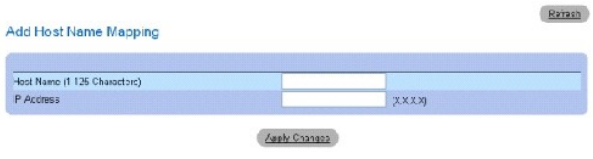
“Remove Host Name Mapping”（删除主机名称映射）— 如果选取该选项，将删除 DNS 主机映射。

添加主机域名

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

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

图 6-44. 添加主机名称映射



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

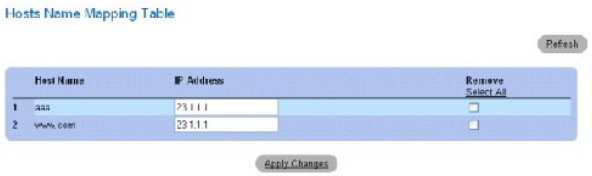
系统将把 IP 地址映射至主机名称，并更新设备。

显示主机名称映射表

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

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

图 6-45. 主机名称映射表



从 IP 地址映射中删除主机名称

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

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

使用 CLI 命令将 IP 地址映射至域主机名称

下表概括了用于将域主机名称映射至 IP 地址的等效 CLI 命令。

表 6-31. 域主机名称 CLI 命令

CLI 命令	说明
ip host name 地址 1 [地址 2 ... 地址 8]	在主机高速缓存中定义静态主机名称到地址映射
no ip host name	删除名称到地址映射。
clear host {名称 | *}	从主机名称到地址高速缓存中删除条目。
show hosts [名称]	显示默认域名、名称服务器主机的列表、主机名称和地址的静态和高速缓存的列表。

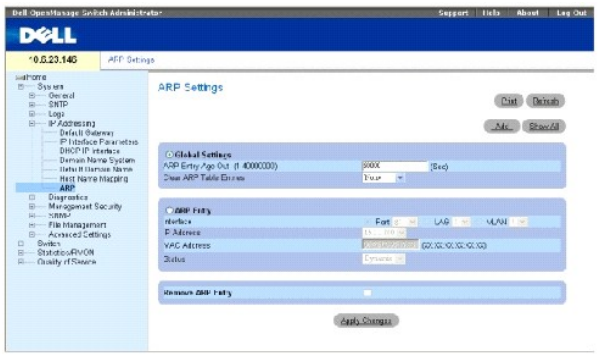
以下是 CLI 命令的示例：

```
console# enable

console# configure

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

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 Table**”（**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，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**”。

图 6-46. ARP 设置



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

“ARP Entry Age Out (1-40000000)”（ARP 条目超时 [1 至 40000000]）— 对于所有设备，关于 ARP 表条目的 ARP 请求之间经过的时间（秒）。在此时间段之后，该条目将从表中删除。范围是 1 至 4000000，其中零表示不从高速缓存中清除条目。默认值为 60000 秒。

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

“None”（无）— 不清除 ARP 条目。

“All”（全部）— 清除所有 ARP 条目。

“Dynamic”（动态）— 仅清除动态 ARP 条目。

“Static”（静态）— 仅清除静态 ARP 条目。

“ARP Entry”（ARP 条目）— 选择此选项可以在单个设备上激活用于 ARP 设置的字段。

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

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

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

“Status”（状态）— ARP 表条目状态。可能的字段值包括：

“Dynamic”（动态）— 动态学习 ARP 条目。

“Static”（静态）— ARP 条目是静态条目。

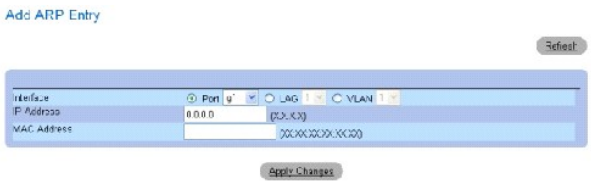
“Remove ARP Entry”（删除 ARP 条目）— 如果选择该选项，将删除 ARP 条目。

要添加静态 ARP 表条目，请：

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

系统将打开**“Add ARP Entry”（添加 ARP 条目）**页面。

图 6-47. “Add ARP Entry”（添加 ARP 条目）页面



3. 选择接口。
4. 定义各字段。
5. 单击**“Apply Changes”（应用更改）**。

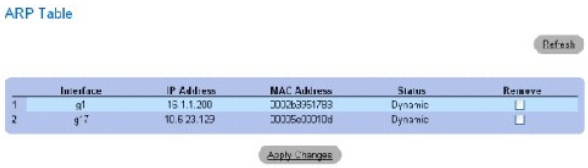
系统将添加**“ARP Table”（ARP 表）**条目，并更新设备。

显示 ARP 表

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

系统将打开**“ARP Table”（ARP 表）**。

图 6-48. “ARP Table”（ARP 表）页面



删除 ARP 表条目

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

系统将打开**“ARP Table”（ARP 表）**页面。

3. 选择一个表条目。

4. 选取“**Remove**”（**删除**）复选框。
5. 单击“**Apply Changes**”（**应用更改**）。

系统将删除选定的“**ARP Table**”（**ARP 表**）条目，并更新设备。

使用 CLI 命令配置 ARP

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

表 6-32. ARP 设置 CLI 命令

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

以下是 CLI 命令的示例：

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

Console (config)# exit

Console# arp timeout 12000

Console# show arp

ARP timeout: 80000 Seconds
```

Interface	IP address	HW address	Status
---------	----------	----------	------
g1	10.7.1.102	00:10:B5:04:DB:4B	Dynamic
g2	10.7.1.135	00:50:22:00:2A:A4	Static

运行电缆诊断程序

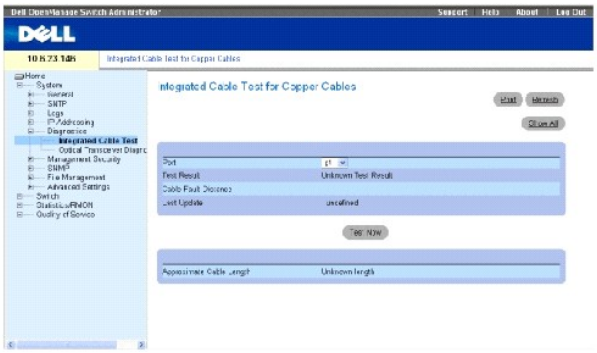
“**Diagnostics**”（**诊断程序**）页面包含指向用于对铜质和光纤电缆执行虚拟电缆检测的页面的链接。要打开“**Diagnostics**”（**诊断程序**）页面，请在树视图中单击“**System**”（**系统**）→“**Diagnostics**”（**诊断程序**）。

查看铜质电缆诊断程序

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

要打开“Integrated Cable Test for Copper Cables”（用于铜质电缆的集成电缆检测）页面，请在树视图中单击“System”（系统）→“Diagnostics”（诊断程序）→“Integrated Cable Test”（集成电缆检测）。

图 6-49. 用于铜质电缆的集成电缆检测



“Port”（端口）— 电缆连接的端口。

“Test Result”（检测结果）— 电缆检测结果。可能的值包括：

“No Cable”（没有电缆）— 没有电缆连接至端口。

“Open Cable”（电缆断路）— 电缆仅有一端连接。

“Short Cable”（电缆短路）— 电缆出现短路。

“OK”（通过）— 电缆通过检测。

“Fiber Cable”（光纤电缆）— 光纤电缆连接至端口。

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

“Last Update”（上一次更新）— 上一次检测端口的时间。

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

执行电缆检测

1. 请确保铜质电缆的两端均连接至设备。
2. 打开“Integrated Cable Test for Copper Cables”（用于铜质电缆的集成电缆检测）页面。
3. 单击“Test Now”（开始检测）。

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

显示虚拟电缆检测结果表

1. 打开“Integrated Cable Test for Copper Cables”（用于铜质电缆的集成电缆检测）页面。
2. 单击“Show All”（全部显示）。

系统将打开“Virtual Cable Test Results Table”（虚拟电缆检测结果表）。

使用 CLI 命令执行铜质电缆检测

下表概括了用于执行铜质电缆检测的等效 CLI 命令。

表 6-33. 铜质电缆检测 CLI 命令

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

以下是 CLI 命令的示例：

```
console> enable

Console# test copper-port tdr g3

Cable is open at 100 meters.

Console> show copper-ports tdr
```

Port	Result	Length [meters]	Date
----	------	---------------	----
g1	OK		
g2	Short	50	13:32:00 15 January 2004
g3	Test has not been performed		
g4	Open	64	13:32:00 15 January 2004
g5	Fiber	-	-

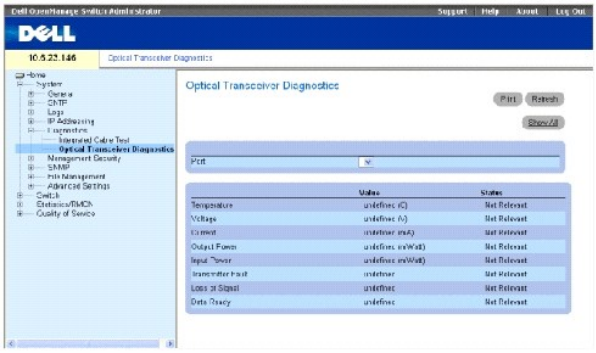
注：返回的电缆长度是一个近似值，它的范围为不超过 50 米、50 至 80 米、80 至 110 米、110 至 120 米或大于 120 米。偏差最大可达 20 米。

查看光收发机诊断程序

“Optical Transceiver Diagnostics”（光收发机诊断程序）页面包含用于对光纤电缆执行检测的字段。要打开“Optical Transceiver Diagnostics”（光收发机诊断程序）页面，请在树视图中单击“System”（系统）→“Diagnostics”（诊断程序）→“Optical Transceiver Diagnostics”（光收发机诊断程序）。

注：仅当链路存在时才能执行光收发机诊断程序。

图 6-50. 光收发机诊断程序



“Port”（端口）— 光纤电缆连接的端口。

“Temperature”（温度）— 电缆运行时的温度（以摄氏为单位）。

“Voltage”（电压）— 电缆运行时的电压。

“Current”（电流）— 电缆运行时的电流。

“Output Power”（输出功率）— 输出功率的传输速率。

“Input Power”（输入功率）— 输入功率的传输速率。

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

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

“Data Ready”（数据就绪）— 收发机已通电并且数据已就绪。

显示光收发机诊断程序检测结果表

1. 打开**“Optical Transceiver Diagnostics”（光收发机诊断程序）**页面。
2. 单击**“Show All”（全部显示）**。

系统将运行检测程序并打开**“Virtual Cable Test Results Table”（虚拟电缆检测结果表）**。

使用 CLI 命令执行光纤电缆检测

下表概括了用于执行光纤电缆检测的等效 CLI 命令。

表 6-34. 光纤电缆检测 CLI 命令

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

以下是 CLI 命令的示例：

```
console> enable

Console# show fiber-ports optical-transceiver
```

				Power			
Port	Temp (C)	Voltage (Volt)	Current (mA)	Output (mWatt)	Input (mWatt)	TX Fault	LOS
g1	W	OK	E	OK	OK	OK	OK
g2	OK	OK	OK	OK	OK	E	OK
g3	Copper						

```
Temp – Internally measured transceiver temperature.

Voltage - Internally measured supply voltage.

Current – Measured TX bias current.

Output Power – Measured TX output power.

Input Power – Measured RX received power.

Tx Fault – Transmitter fault

LOS – Loss of signal
```

“Optical Transceiver Diagnostics Table”（光收发机诊断程序表）包含以下列：

- **“Temp”（温度）**— 内部测量的收发机温度。
- **“Voltage”（电压）**— 内部测量的电源电压。
- **“Current”（电流）**— 测量的 TX 偏流。
- **“Output Power”（输出功率）**— 测量的 TX 输出功率（以毫瓦为单位）。
- **“Input Power”（输入功率）**— 测量的 RX 接收功率（以毫瓦为单位）。
- **“TX Fault”（TX 故障）**— 发送器出现故障。

注：Finisair 收发机不支持发送器故障诊断测试。

- **“LOS”（丢失）**— 信号丢失。
- **“Data Ready”（数据就绪）**— 收发机已通电并且数据已就绪。
- **N/A** — 不可用；**N/S** — 不支持；**W** — 警告；**E** — 错误。

注：光纤分析功能只能对支持数字诊断标准 SFF- 4872 的 SFP 使用。

管理设备安全保护

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

定义访问配置文件

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

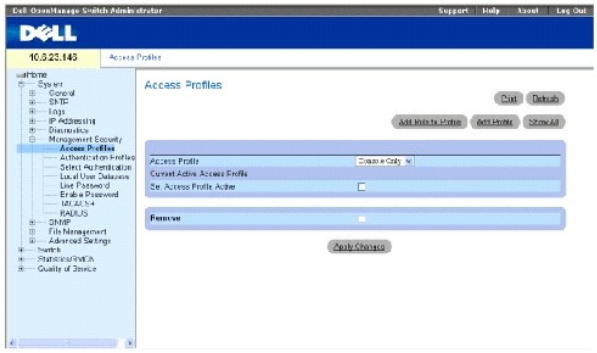
可以针对 Web (HTTP)、安全 Web (HTTPS)、Telnet、安全 Telnet 和 SNMP 等各种类型的管理访问方法分别定义管理访问。

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

管理访问列表包含用于确定哪些用户可以通过哪些方法管理设备的规则。还可以禁止用户访问设备。

“Access Profiles”（访问配置文件）页面包含用于配置管理列表并将其应用于特定接口的字段。要打开**“Access Profiles”（访问配置文件）**页面，请在树视图中单击**“System”（系统）→“Management Security”（管理安全保护）→“Access Profiles”（访问配置文件）**。

图 6-51. 访问配置文件



“Access Profile”（访问配置文件）— 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**“Console List”（控制台列表）**的默认值，用户定义的访问配置文件将添加至该处。如果选择**“Console Only”（仅控制台）**作为**“Access Profile”（访问配置文件）**名称，将断开会话并且仅通过控制台访问设备。

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

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

“Remove”（删除）— 如果选择该选项，将从**“Access Profile Name”（访问配置文件名称）**列表中删除访问配置文件。

激活配置文件

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

系统将激活访问配置文件。

添加访问配置文件

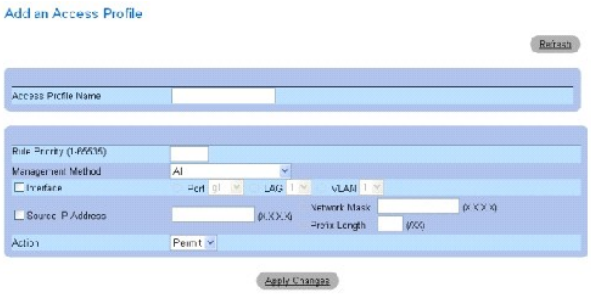
规则用作筛选器，用于确定规则优先级、设备管理方法、接口类型、源 IP 地址和网络掩码以及设备管理访问操作。可以禁止或允许用户进行管理访问。规则优先级设置了配置文件中规则的应用顺序。

要定义访问配置文件规则，请：

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

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

图 6-52. “Add An Access Profile”（添加访问配置文件）页面



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

“Rule Priority (1-65535)”（规则优先级 [1 至 65535]）— 规则优先级。信息包与规则进行匹配时，用户组会被允许或拒绝进行设备管理访问。通过在**“Profile Rules Table”（配置文件规则表）**中定义规则编号来设置规则顺序。由于根据第一适用原则对信息包进行匹配，所以在将信息包与规则进行匹配时，规则编号非常重要。在**“Profile Rules Table”（配置文件规则表）**中设定规则优先级。

“Management Method”（管理方法）— 为其定义了访问配置文件的管理方法。具有此访问配置文件的用户可以使用选定的管理方法访问设备。

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

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

“Source IP Address”（源 IP 地址）— 为其应用规则的接口源 IP 地址。这是一个可选字段，它表示规则对于子网有效。

“Network Mask”（网络掩码）— IP 子网掩码。

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

“Action”（操作）— 定义是允许还是拒绝对定义的接口进行管理访问。

3. 定义**“Access Profile Name”（访问配置文件名称）**字段。
4. 定义相关的字段。
5. 单击**“Apply Changes”（应用更改）**。

系统将添加新的访问配置文件，并更新设备。

将规则添加至访问配置文件

注：必须定义第一条规则才能开始通信与访问配置文件的匹配。

1. 打开**“Access Profiles”（访问配置文件）**页面。
2. 单击**“Add Profile to Rule”（将配置文件添加至规则）**。

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

图 6-53. 添加访问配置文件规则

3. 完成各字段。
4. 单击**“Apply Changes”（应用更改）**。

系统将把规则添加至访问配置文件，并更新设备。

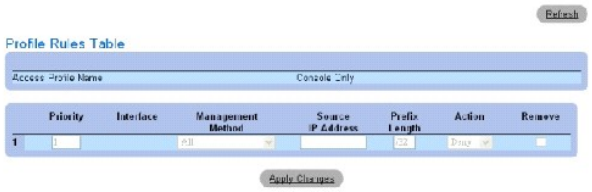
要查看配置文件规则表，请：

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。

图 6-54. “Profile Rules Table”（配置文件规则表）页面



删除规则

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

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

3. 选择一条规则。
4. 选取“**Remove**”（**删除**）复选框。
5. 单击“**Apply Changes**”（**应用更改**）。

系统将删除选定的规则，并更新设备。

使用 CLI 命令定义访问配置文件

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

表 6-35. 访问配置文件 CLI 命令

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

以下是 CLI 命令的示例：

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



Console (config-macl)#
permit ethernet g1



Console (config-macl)#
permit ethernet g9
```

```
Console (config-macl)#
deny ethernet g2


Console (config-macl)#
deny ethernet g10


Console (config-macl)#
exit


Console (config)#
management access-class
mlist


Console (config)# exit


Console# show management
access-list


mlist


-----


permit ethernet g1


permit ethernet g9


! (Note: all other access
implicitly denied)


Console> show management
access-class


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

定义验证配置文件

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

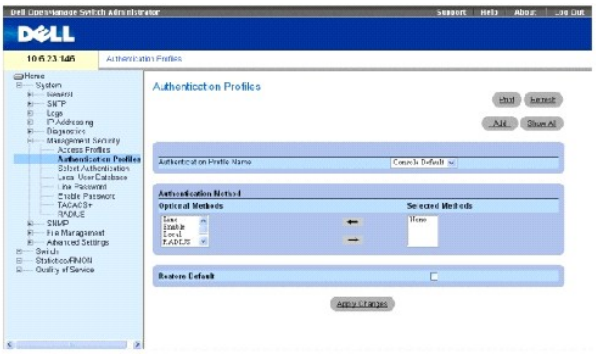
- 本地
- 通过外部服务器

也可以将用户验证设置为“None”（无）。

用户验证按照方法选择顺序进行。例如，如果同时选择“Local”（本地）和“RADIUS”选项，则首先在本地验证用户。如果本地用户数据库为空，则再通过 RADIUS 服务器进行用户验证。

如果在验证过程中出现错误，将使用下一个选定方法。要打开**“Authentication Profiles”（验证配置文件）**页面，请在树视图中单击**“System”（系统）→“Management Security”（管理安全保护）→“Authentication Profiles”（验证配置文件）**。

图 6-55. 验证配置文件



“Authentication Profile Name”（验证配置文件名称）— 可以向其中添加用户定义的验证配置文件的用户定义的验证配置文件列表。默认为**“Network Default”（网络默认值）**和**“Console Default”（控制台默认值）**。

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

“None”（无）— 不进行用户验证。

“Local”（本地）— 在设备级别进行用户验证。设备将检查用户名和密码以进行验证。

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

“Line”（线路）— 使用线路密码进行用户验证。

“Enable”（启用）— 使用启用密码进行验证。

“TACACS+”— 在 TACACS+ 服务器进行用户验证。

“Restore Default”（恢复默认设置）— 恢复设备上的默认用户验证方法。

要选择验证配置文件，请：

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

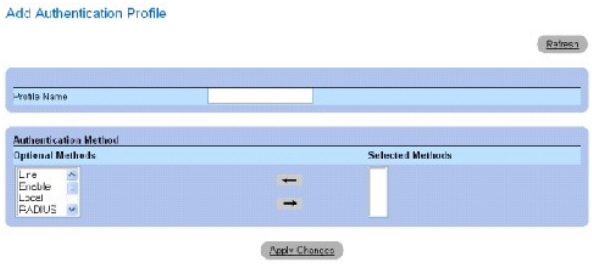
用户验证配置文件将被更新到设备。

要添加验证配置文件，请：

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

   系统将打开“Add Authentication Method Profile Name”（添加验证方法配置文件名称）页面。

图 6-56. “Add Authentication Profile”（添加验证配置文件）页面



3. 配置该配置文件。
4. 单击“Apply Changes”（应用更改）。

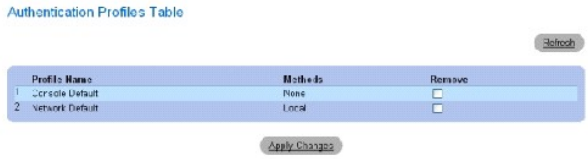
   验证配置文件将被更新到设备。

要显示“Show All Authentication Profiles”（显示所有验证配置文件）页面，请：

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

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

图 6-57. 验证配置文件



要删除验证配置文件，请：

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

   系统将打开“Authentication Profile”（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）。

   系统将删除选定的验证配置文件。

使用 CLI 命令配置验证配置文件

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

表 6-36. 验证配置文件 CLI 命令

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

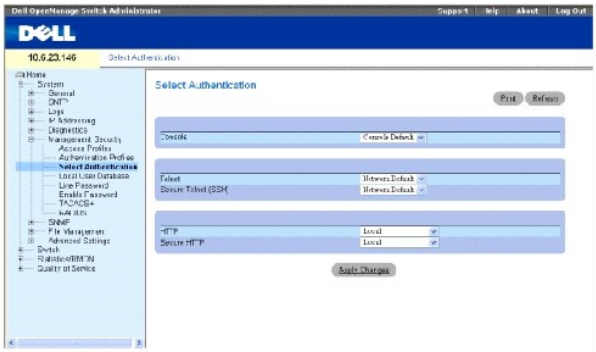
以下是 CLI 命令的示例：

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


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

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 **“Select Authentication”（选择验证）** 页面，请在树视图中单击 **“System”（系统）→“Management Security”（管理安全保护）→“Select Authentication”（选择验证）**。

图 6-58. 选择验证



“Console”（控制台） — 用于验证控制台用户的验证配置文件。

“Telnet”— 用于验证 Telnet 用户的验证配置文件。

“Secure Telnet (SSH)”（安全 Telnet [SSH]） — 用于验证安全命令解释程序 (SSH) 用户的验证配置文件。SSH 使客户端可以与设备建立安全和加密的远程连接。

“HTTP”和 **“Secure HTTP”（安全 HTTP）** — 分别用于 HTTP 访问和安全 HTTP 访问的验证方法。可能的字段值包括：

“None”（无） — 对于访问不使用任何验证方法。

“Local”（本地）— 在本地进行验证。

“RADIUS”— 在 RADIUS 服务器进行验证。

“TACACS+”— 在 TACACS+ 服务器进行验证。

将验证列表应用于控制台会话

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

控制台会话将被分配一个验证列表。

将验证配置文件应用于 Telnet 会话

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

Telnet 会话将被分配一个验证列表。

将验证配置文件应用于安全 Telnet (SSH) 会话

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

安全 Telnet (SSH) 会话将被分配一个验证配置文件。

为 HTTP 会话分配验证顺序

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

HTTP 会话将被分配一个验证顺序。

为安全 HTTP 会话分配验证顺序

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

安全 HTTP 会话将被分配一个验证顺序。

使用 CLI 命令分配访问验证配置文件或验证顺序

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

表 6-37. 选择验证 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 命令的示例：

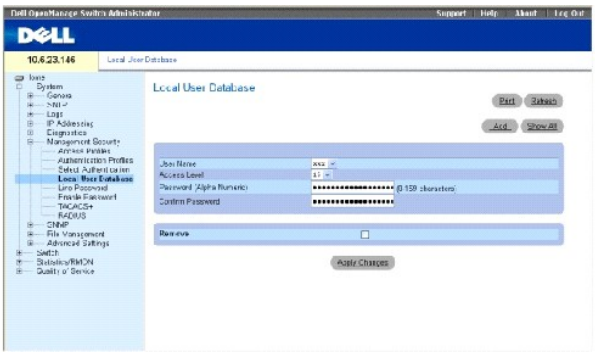
```
Console (config-line)
# enable
authentication
default

Console (config-line)
# login
authentication
default

Console (config-line)
# exit

Console (config)# ip
http authentication
radius local

Console (config)# ip
https authentication
radius local

Console (config)#
exit

Console# show
authentication
methods

Login Authentication
Method Lists

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

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


Dot1x: Radius
```

定义本地用户数据库

"Local User Database"（本地用户数据库）页面包含用于定义用户、密码和访问级别的字段。要打开"Local User Database"（本地用户数据库）页面，请在树视图中单击**"System"（系统）>"Management Security"（管理安全保护）>"Local User Database"（本地用户数据库）**。

图 6-59. 本地用户数据库



"User Name"（用户名）— 用户的列表。

"Access Level"（访问级别）— 用户访问级别。最低的用户访问级别为 **1**，最高的用户访问级别为 **15**。

"Password"（密码）（0 至 159 个字符）— 用户定义的密码。本地用户数据库密码最多可以有 159 个字符。

"Confirm Password"（确认密码）— 确认用户定义的密码。

"Remove"（删除）— 如果选择该选项，将从**"User Name"（用户名）**列表中删除用户。

要为用户分配访问权限，请：

1. 打开**"Local User Database"（本地用户数据库）**页面。
2. 在**"User Name"（用户名）**字段中选择一个用户。
3. 定义各字段。
4. 单击**"Apply Changes"（应用更改）**。

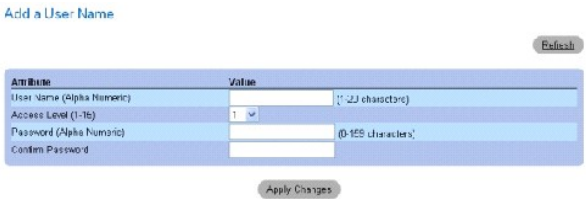
   系统将定义用户访问权限和密码，并更新设备。

要定义新用户，请：

1. 打开**"Local User Database"（本地用户数据库）**页面。
2. 单击**"Add"（添加）**。

   系统将打开**"Add User"（添加用户）**页面。

图 6-60. 添加用户



3. 定义各字段。

4. 单击“**Apply Changes**”（**应用更改**）。

   系统将定义新用户，并更新设备。

要显示本地用户表，请：

1. 打开“**Local User Database**”（**本地用户数据库**）页面。
2. 单击“**Show All**”（**全部显示**）。

   系统将打开“**Local User Table**”（**本地用户表**）。

图 6-61. “Local User Table”（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**）。

3. 选择一个**用户名**。
4. 选取“**Remove**”（**删除**）复选框。
5. 单击“**Apply Changes**”（**应用更改**）。

   系统将删除选定的用户，并更新设备。

使用 CLI 命令设定用户

下表概括了用于设置“**Local User Database**”（**本地用户数据库**）页面中显示的字段的等效 CLI 命令。

表 6-38. 本地用户数据库 CLI 命令

CLI 命令	说明
username 名称 [password 密码] [level 级别] [encrypted]	建立基于用户名的验证系统。

以下是 CLI 命令的示例：

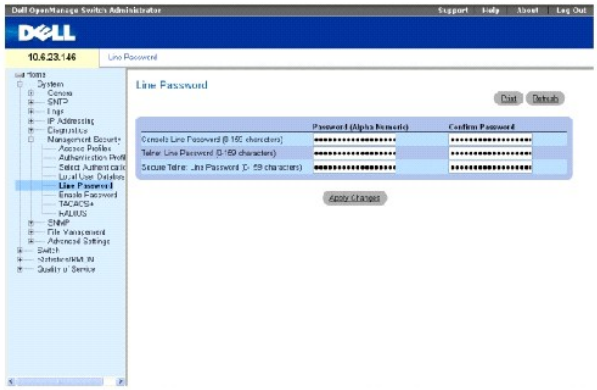
```
Console (config)# username bob
password lee level 15
```

定义线路密码

“**Line Password**”（**线路密码**）页面包含用于定义管理方法的线路密码的字段。要打开“**Line Password**”（**线路密码**）页面，请在树视图中单击“**System**”（**系统**）→“**Management**

Security”（管理安全保护）→“Line Passwords”（线路密码）。

图 6-62. 线路密码



“Line Password for Console (0-159 Characters)”（控制台的线路密码 [0 至 159 个字符]）/“Line Password for Telnet (0-159 Characters)”（Telnet 的线路密码 [0 至 159 个字符]）/“Line Password for Secure Telnet (0-159 Characters)”（安全 Telnet 的线路密码 [0 至 159 个字符]）— 通过控制台、Telnet 或安全 Telnet 会话访问设备的线路密码。密码最多可以包含 159 个字符。

“Confirm Password”（确认密码）— 确认新的线路密码。密码将以 ***** 形式显示。

定义控制台会话的线路密码

1. 打开**“Line Password”（线路密码）**页面。
2. 定义**“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。

定义 Telnet 会话的线路密码

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。

定义安全 Telnet 会话的线路密码

1. 打开**“Line Password”（线路密码）**页面。
2. 定义**“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

下表概括了用于设置“Line Password”（线路密码）页面中显示的字段的等效 CLI 命令。

表 6-39. 线路密码 CLI 命令

CLI 命令	说明
password 密码 [encrypted]	指定线路上的密码。

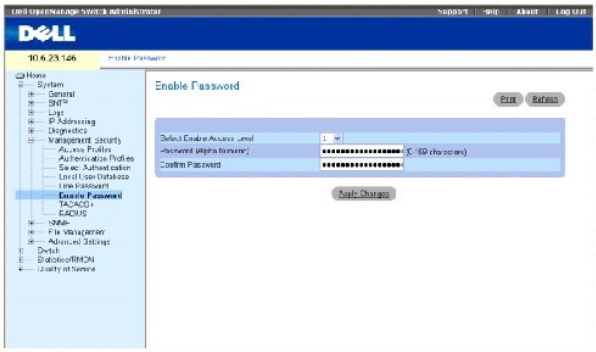
以下是 CLI 命令的示例：

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

定义启用密码

“Modify Enable Password”（修改启用密码）页面用于设置本地密码，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）。

图 6-63. 修改启用密码



“Select Enable Access Level”（选择启用访问级别）— 与启用密码相关的访问级别。可能的字段值为 1 至 15。

“Password”（密码）（0 至 159 个字符）— 当前配置的启用密码。启用密码最多可以包含 159 个字符。

“Confirm Password”（确认密码）— 确认新的启用密码。密码将以 ***** 形式显示。

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

系统将定义新的启用密码，并更新设备。

使用 CLI 命令设定启用密码

下表概括了用于设置**“Modify Enable Password”（修改启用密码）**页面中显示的字段的等效 CLI 命令。

表 6-40. 修改启用密码 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 命令的示例：

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


Console# show users
accounts


Username Privilege


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


secret 15
```

定义 TACACS+ 设置

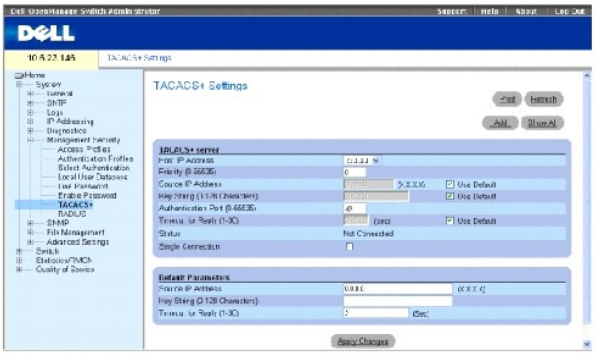
设备提供对终端访问控制器访问控制系统 (TACACS+) 客户端的支持。TACACS+ 为访问设备的用户的验证提供了集中式的安全保护。

TACACS+ 提供了集中式的用户管理系统，同时还保持了与 RADIUS 和其它验证过程的一致性。TACACS+ 提供以下服务：

- 验证 — 登录时验证用户名和用户定义的密码。
- 授权 — 登录时执行。完成验证会话后，将使用通过验证的用户名开始授权会话。TACACS 服务器将检查用户权限。

TACACS+ 协议通过设备与 TACACS+ 服务器之间加密的协议交换确保网络完整性。要打开**“TACACS+ Settings”（TACACS+ 设置）页面**，请在树视图中单击**“System”（系统）→“Management Security”（管理安全保护）→“TACACS+”**。

图 6-64. TACACS+ 设置



“Host IP Address”（主机 IP 地址）— 指定 TACACS+ 服务器 IP 地址。

“Priority (0-65535)”（优先级 [0 至 65535]）— 指定使用 TACACS+ 服务器的顺序。默认值为 0。

“Source IP Address”（源 IP 地址）— 用于设备与 TACACS+ 服务器之间的 TACACS+ 会话的设备源 IP 地址。

“Key String (0-128 Characters)”（关键字字符串 [0 至 128 个字符]）— 定义设备与 TACACS+ 服务器之间的 TACACS+ 通信的验证和加密关键字。此关键字必须与 TACACS+ 服务器上使用的加密匹配。

“Authentication Port (0-65535)”（验证端口 [0 至 65535]）— 通过其进行 TACACS+ 会话的端口号。默认端口号为 49。

“Reply Timeout (1-30)”（回复超时 [1 至 30]）（秒）— 设备与 TACACS+ 服务器之间连接超时之前所经过的时间。字段范围是 1 至 30 秒。

“Status”（状态）— 设备与 TACACS+ 服务器之间的连接状态。可能的字段值包括：

“Connected”（已连接）— 当前设备与 TACACS+ 服务器之间有连接。

“Not Connected”（未连接）— 当前设备与 TACACS+ 服务器之间无连接。

“Single Connection”（单一连接）— 如果选择该选项，将在设备与 TACACS+ 服务器之间维护单一打开的连接。

TACACS+ 默认参数是用户定义的默认值。默认设置将应用于新定义的 TACACS+ 服务器。如果未定义默认值，则将系统默认值应用于新的 TACACS+ 服务器。以下是 TACACS+ 默认值：

“Source IP Address”（源 IP 地址）— 用于设备和 TACACS+ 服务器之间的 TACACS+ 会话的默认设备源 IP 地址。

“Key String(0-128 Characters)”（关键字字符串 [0 至 128 个字符]）— 设备与 TACACS+ 服务器之间的 TACACS+ 通信的默认验证和加密关键字。

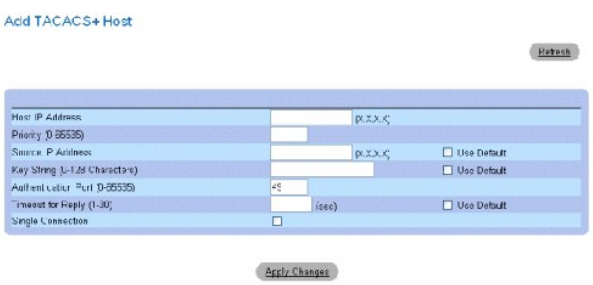
“Timeout for Reply (1-30)”（回复超时 [1 至 30]）— 设备与 TACACS+ 连接超时之前所经过的默认时间。

添加 TACACS+ 服务器

1. 打开**“TACACS+ Settings”（TACACS+ 设置）页面**。
2. 单击**“Add”（添加）**。

系统将打开**“Add TACACS+ Host”（添加 TACACS+ 主机）页面**。

图 6-65. 添加 TACACS+ 主机



3. 定义各字段。
4. 单击“**Apply Changes**”（应用更改）。

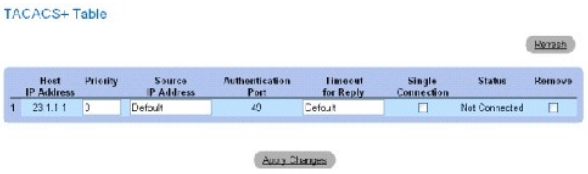
系统将添加 TACACS+ 服务器，并更新设备。

显示 TACACS+ 表

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

系统将打开“**TACACS+ Table**”（**TACACS+ 表**）。

图 6-66. TACACS+ 表



删除 TACACS+ 服务器

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

系统将打开“**TACACS+ Table**”（**TACACS+ 表**）。

3. 选择一个“**TACACS+ Table**”（**TACACS+ 表**）条目。
4. 选取“**Remove**”（**删除**）复选框。
5. 单击“**Apply Changes**”（**应用更改**）。

系统将删除 TACACS+ 服务器，并更新设备。

使用 CLI 命令定义 TACACS+ 设置

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

表 6-41. TACACS+ CLI 命令

CLI 命令	**说明**
TACACS-server host (IP 地址 | 主机名) [single-connection] [port 端口号] [timeout 超时] [key 关键字字符串] [source 源] [priority 优先级]	指定 TACACS+ 主机。
no TACACS-server host (IP 地址 | 主机名)	删除 TACACS+ 主机。
tacacs-server key 关键字字符串	指定设备与 TACACS+ 服务器之间所有 TACACS+ 通信的验证和加密关键字。此关键字必须与 TACACS+ 守护程序中使用的加密匹配。（范围为 0 至 128 个字符。）
tacacs-server timeout 超时	指定超时值（以秒为单位）。（范围为 1 至 30。）
tacacs-server source-ip 源	指定源 IP 地址。（范围为有效的 IP 地址。）
show TACACS [IP 地址]	显示 TACACS+ 服务器的配置和统计数据。

以下是 CLI 命令的示例：

Console# **show tacacs**						
Router Configuration						
----------	---------	----	----------	---------	--------	--------
IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority
----------	---------	----	----------	---------	--------	--------
12.1.1.2	Not Connected	49	Yes	1	12.1.1.1	1
Global values						

TimeOut : 5						
Router Configuration ----------						
Source IP : 0.0.0.0						
console#						

配置 RADIUS 全局参数

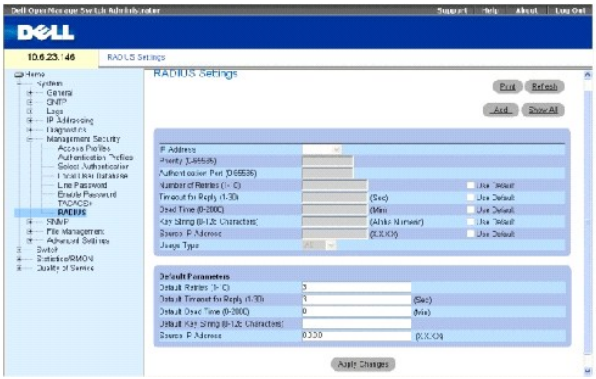
远程认证拨入用户服务 (RADIUS) 服务器为网络提供了附加安全保护。RADIUS 服务器为以下操作提供了集中式的验证方法：

- Telnet 访问

- Web 访问
- 从控制台对设备的访问

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”。

图 6-67. RADIUS 设置



“IP Address”（IP 地址）— 验证服务器 IP 地址的列表。

“Priority (1-65535)”（优先级 [1 至 65535]）— 指定服务器的优先级。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 至 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 至 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 [0 至 2000]）— 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 (1-128 Characters)”（关键字字符串 [1 至 128 个字符]）— 指定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）— 指定用于与 RADIUS 服务器进行通信的源 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 至 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：如果未指定主机特定超时、重试次数或停用时间值，则全局值（默认值）将应用于各主机。

“Default Retries (1-10)”（默认重试次数 [1 至 10]）— 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 至 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 (1-128 Characters)”（默认关键字字符串 [1 至 128 个字符]）— 指定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）— 指定用于与 RADIUS 服务器进行通信的源 IP 地址。

“Usage Type”（使用类型）— 指定服务器的使用类型。它可以是以下值之一：“login”（登录）、“802.1x”或“all”（全部）。如果未指定，则默认为“all”（全部）。

要定义 RADIUS 参数，请：

1. 打开**“RADIUS Settings”（RADIUS 设置）**页面。
2. 定义各字段。
3. 单击**“Apply Changes”（应用更改）**。

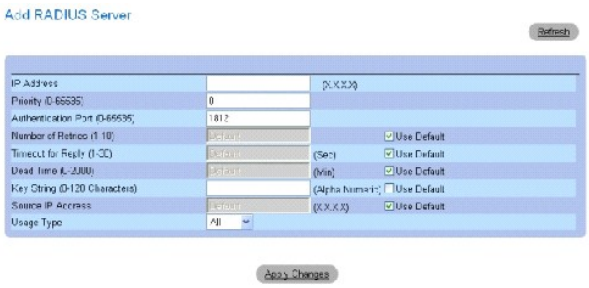
RADIUS 设置将被更新到设备。

要添加 RADIUS 服务器，请：

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

系统将打开**“Add RADIUS Server”（添加 RADIUS 服务器）**页面。

图 6-68. “Add RADIUS Server”（添加 RADIUS 服务器）页面



3. 定义各字段。
4. 单击**“Apply Changes”（应用更改）**。

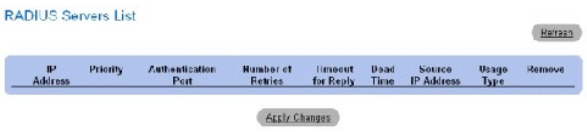
系统将添加新的 RADIUS 服务器，并更新设备。

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**“Show all RADIUS Servers”（显示所有 RADIUS 服务器）**页面。

图 6-69. 显示所有 RADIUS 服务器



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. 修改相关的字段。
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。
5. 单击**“Apply Changes”（应用更改）**。

   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

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

表 6-42. RADIUS 设置 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 | 主机名} [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] [usage 类型]	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 命令的示例：

```
Console (config)# radius-
server timeout 5
```

```
Console (config)# radius-
server retransmit 5


Console (config)# radius-
server deadtime 10


Console (config)# radius-
server key dell-server


Console (config)# radius-
server host 196.210.100.1
auth-port 1645 timeout 20
```

```
Console# show radius-servers
```

	Port							
IP address	Auth	Acct	TimeOut	Retransmit	Deadtime	Source IP	Priority	Usage
---------	----	----	-------	----------	-------	-----	-------	-----
33.1.1.1	1812	1813	6	4	10	0.0.0.0	0	All
172.16.1.2	1645	1646	11	8	Global	Global	2	All

```
     Global values


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


     TimeOut: 5


     Retransmit: 5


     Deadtime: 10


     Source IP: 0.0.0.0
```

定义 SNMP 参数

简单网络管理协议 (SNMP) 提供了管理网络设备的方法。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。变量在管理信息库 (MIB) 中进行定义。MIB 包含代理控制的变量。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。

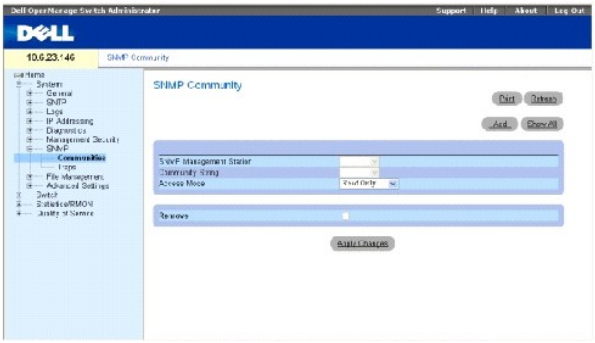
访问 SNMP 代理的权限由访问字符串控制。要与设备进行通信，嵌入式 Web 服务器需要提交有效的团体字符串以进行验证。要打开“SNMP”页面，请在树视图中单击**“System”（系统）→“SNMP”**。

本节包含用于管理 SNMP 配置的信息。

定义团体

访问权限是通过在**“Community Table”（团体表）**中定义团体来管理的。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）**。

图 6-70. SNMP 团体



“SNMP Management Station”（SNMP 管理站点）— 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）— 对于所有 MIB（团体表除外，不能对其进行访问），管理访问被限制为只读。

“Read Write”（读写）— 对于所有 MIB（团体表除外，不能对其进行访问），管理访问为读写模式。

“SNMP Admin”（SNMP 管理）— 对于所有 MIB（包括团体表），管理访问为读写模式。

“Remove”（删除）— 如果选择该选项，将删除团体。

定义新团体

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。

图 6-71. 添加 SNMP 团体

3. 选择以下选项之一：

“Management Station”（管理站点）— 为特定管理站点定义 SNMP 团体。（值 0.0.0.0 指定所有管理站点。）

“All”（全部）— 为所有管理站点定义 SNMP 团体。

4. 定义其余字段。
5. 单击“**Apply Changes**”（**应用更改**）。

系统将保存新团体，并更新设备。

显示所有团体

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**）。

图 6-72. 团体表

删除团体

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**）。

3. 从“**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**）。

系统将删除选定的团体条目，并更新设备。

使用 CLI 命令配置团体

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

表 6-43. SNMP 团体 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。
snmp-server host {IP 地址 | 主机名} 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	查看 SNMP 通信状态。

以下是 CLI 命令的示例：

```
console(config)# snmp-server community public_1 su 1.1.1.1
console(config)# snmp-server community public_2 rw 2.2.2.2
console(config)# snmp-server community public_3 ro 3.3.3.3
console(config)# snmp-server host 1.1.1.1 public_1 1
console(config)# snmp-server host 2.2.2.2 public_2 2
console(config)#
```

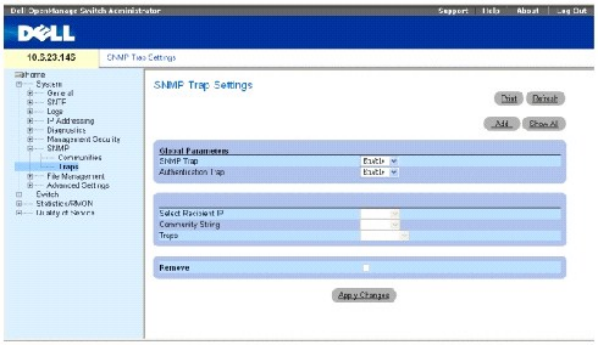
```
console# show snmp

Community-String  Community-Access  IP address
----------------  ----------------  -------
public_1          super             1.1.1.1
public_2          readwrite         2.2.2.2
public_3          readonly          3.3.3.3

Traps are enabled.

Authentication-failure trap is enabled.
```

Trap-Rec-Address	Trap-Rec-Community	Version
----------	----------	-------
1.1.1.1	public_1	1
2.2.2.2	public_2	2
System Contact: 3456789		
System Location: 1234 5678		
console#		

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）**。

图 6-73. SNMP 陷阱设置



“SNMP Trap”（SNMP 陷阱）— 启用将 SNMP 陷阱或 SNMP 通知从设备发送到已定义的陷阱接收设备。

“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。

“Select Recipient IP”（选择接收设备 IP）— 指定陷阱发送到的 IP 地址。

“Community String”（团体字符串）— 标识陷阱管理器的团体字符串。

“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”— 发送 SNMP 版本 1 陷阱

“SNMP V2c”— 发送 SNMP 版本 2 陷阱

“Remove”（删除）— 如果选择该选项，将删除**“Trap Manager Table”（陷阱管理器表）**条目。

在设备上启用 SNMP 陷阱

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. 定义各字段。
4. 单击**“Apply Changes”（应用更改）**。

系统将在设备上启用 SNMP 陷阱。

在设备上启用验证陷阱

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. 定义各字段。
4. 单击**“Apply Changes”（应用更改）**。

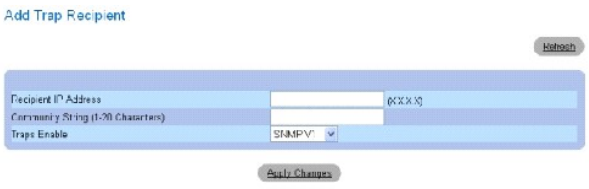
系统将在设备上启用验证陷阱。

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。

图 6-74. 添加陷阱接收设备/管理器



3. 定义各字段。配置 0.0.0.0 表示“全部”，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。

显示陷阱管理器表

“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**“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。

图 6-75. 陷阱管理器表

删除“Trap Manager Table”（陷阱管理器表）条目

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）**。

系统将删除选定的陷阱管理器，并更新设备。

使用 CLI 命令配置陷阱

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

表 6-44. SNMP 陷阱设置 CLI 命令

CLI 命令	说明
snmp-server enable traps	允许设备发送 SNMP 陷阱或 SNMP 通知。
snmp-server trap authentication	允许设备在验证失败时发送 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 命令的示例：

```
console(config)# snmp-
server community public_1
su 1.1.1.1
```

```
console(config)# snmp-
server community public_2
rw 2.2.2.2
```

```
console(config)# snmp-server community public_3 ro 3.3.3.3
console(config)# snmp-server host 1.1.1.1 public_1 1
console(config)# snmp-server host 2.2.2.2 public_2 2
console(config)# snmp-server enable traps
console(config)# snmp-server trap authentication
console(config)#
```

```
console# show snmp

Community-String  Community-Access  IP address
----------------  ----------------  ----------
public_1          super             1.1.1.1
public_2          readwrite         2.2.2.2
public_3          readonly          3.3.3.3

Traps are enabled.

Authentication-failure trap is enabled.

Trap-Rec-Address  Trap-Rec-Community  Version
----------------  ------------------  -------
1.1.1.1           public_1            1
2.2.2.2           public_2            2
```

System Contact: 345 6789		
System Location: 1234 5678		
console#		

管理文件

“File Management”（文件管理）页面包含用于管理设备软件、映像文件和配置文件的字段。文件可从 TFTP 服务器下载。

文件管理概览

配置文件结构由以下配置文件组成：

- 启动配置文件 — 包含在设备断电或重新引导时将设备重新配置为相同设置所必需的命令。启动文件是通过从正在运行的配置文件或备份配置文件中复制配置命令来创建的。
- 正在运行的配置文件 — 包含所有启动文件命令以及在当前会话过程中输入的所有命令。设备断电或重新引导后，所有存储在正在运行的配置文件中的命令均会丢失。启动期间，启动文件中的所有命令将被复制到正在运行的配置文件中，并应用于设备。会话期间，输入的所有新命令将被添加到正在运行的配置文件中存在的命令中。命令不会被覆盖。要更新启动文件，必须先将正在运行的配置文件复制到启动配置文件中，然后再断开设备的电源连接。下次重新启动设备时，这些命令将从启动配置文件复制回正在运行的配置文件中。
- 备份配置文件 — 包含设备配置的备份副本。正在运行的配置文件或启动文件被复制到备份文件时，将生成备份文件。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 — 系统文件映像保存在两个称为映像（映像 1 和映像 2）的快擦写文件中。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。

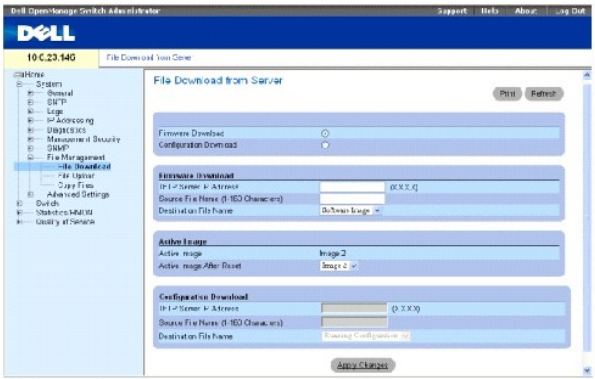
要打开**“File Management”（文件管理）**页面，请在树视图中单击**“System”（系统）→“File Management”（文件管理）**。**“File Management”（文件管理）**页面包含指向以下内容的链接：

- 文件下载
- 文件加载
- 复制文件

下载文件

“File Download From Server”（从服务器下载文件）页面包含用于将系统映像和配置文件从 TFTP 服务器下载到设备的字段。要打开**“File Download From Server”（从服务器下载文件）**页面，请在树视图中单击**“System”（系统）→“File Management”（文件管理）→“File Download”（文件下载）**。

图 6-76. 从服务器下载文件



“Firmware Download”（固件下载）— 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）— 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）— 要下载的文件所在的 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）— 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。

“Active Image”（活动映像）— 当前处于活动状态的映像文件。

“Active Image After Reset”（重启动后的活动映像）— 设备重启动后处于活动状态的映像文件。

“Configuration Download File TFTP Server IP Address”（配置下载文件 TFTP 服务器 IP 地址）— 要下载的配置文件所在的 TFTP 服务器 IP 地址。

“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）— 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. 定义各字段。
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

下表概括了用于设置**“File Download From Server”（从服务器下载文件）**页面中显示的字段的等效 CLI 命令。

表 6-45. 文件下载 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 命令的示例：

```
console# copy running-config tftp://11.1.1.2/pp.txt
```

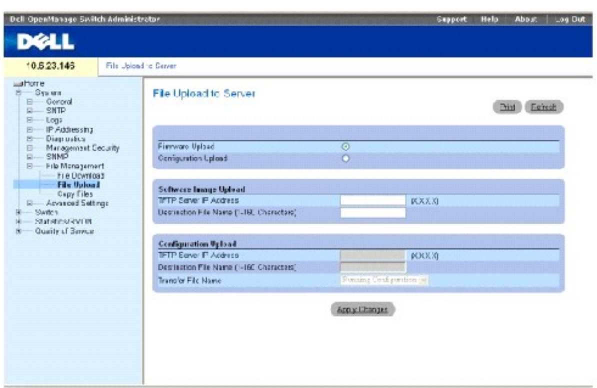
NOTE: Each "!" indicates that ten packets were successfully transferred.

```
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）**。

图 6-77. 将文件加载至服务器



“Firmware Upload”（固件加载）— 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）— 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）— 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）— 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）— 指定文件要加载到的配置文件路径。

“Configuration Upload Transfer file name”（配置加载传输文件名）— 配置要加载到的软件文件。可能的字段值包括：

“Running Configuration”（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）— 加载备份配置文件

加载文件

1. 打开**“File Upload to Server”（将文件加载至服务器）**页面。
2. 定义要加载的文件类型。
3. 定义各字段。
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

下表概括了用于设置**“File Upload to Server”（将文件加载至服务器）**页面中显示的字段的等效 CLI 命令。

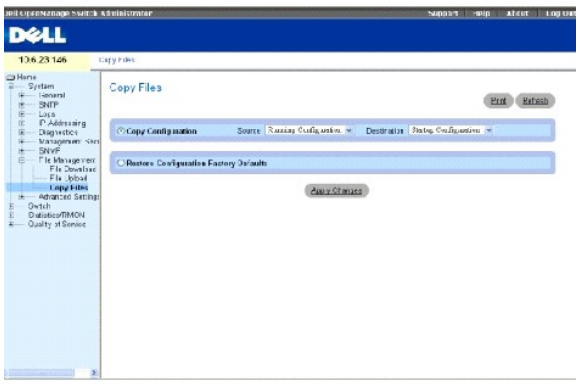
表 6-46. 文件加载 CLI 命令

CLI 命令	说明
copy 源 URL 目的地 URL [snmp]	将文件从源复制到目的地。

复制文件

通过**“Copy Files”（复制文件）**页面可以复制和删除文件。要打开**“Copy Files”（复制文件）**页面，请在树视图中单击**“System”（系统）→“File Management”（文件管理）→“Copy Files”（复制文件）**。

图 6-78. 复制文件



"Copy Configuration"（复制配置）— 如果选择该选项，将复制正在运行的配置文件、启动配置文件或备份配置文件。可能的字段值包括：

"Source"（源）— 复制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）— 要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的文件。

"Restore Configuration Factory Defaults"（恢复出厂默认配置）— 如果选择该选项，请指定要重设的出厂默认配置文件。如果未选择该选项，将维持当前配置设置。

复制文件

1. 打开**"Copy Files"（复制文件）**页面。
2. 定义**"Source"（源）**和**"Destination"（目的地）**字段。
3. 单击**"Apply Changes"（应用更改）**。

系统将复制文件，并更新设备。

恢复出厂默认设置

1. 打开**"Copy Files"（复制文件）**页面。
2. 单击**"Restore Company Factory Defaults"（恢复出厂默认设置）**。
3. 单击**"Apply Changes"（应用更改）**。

系统将恢复出厂默认设置，并更新设备。

使用 CLI 命令复制和删除文件

下表概括了用于设置**"Copy Files"（复制文件）**页面中显示的字段的等效 CLI 命令。

表 6-47. 复制文件 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。
delete startup-config	删除启动配置文件。

以下是 CLI 命令的示例：

```
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]

Console# delete startup-config

Console# copy running-config startup-config

01-Jan-2000 01:55:03 %COPY-W-TRAP: The copy operation was completed successfully

Copy succeeded
```

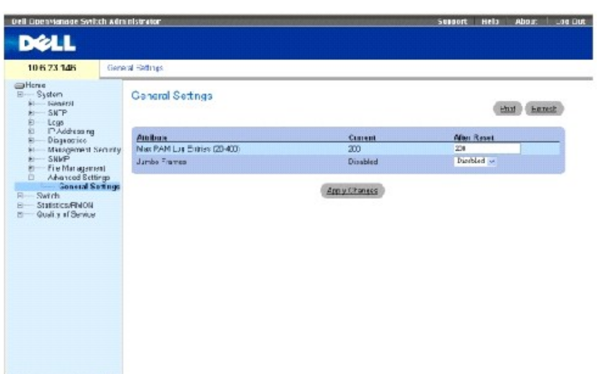
定义高级设置

“Advanced Settings”（高级设置）页面包含用于配置常规设置的链接。使用“Advanced Settings”（高级设置）可以设置设备的各种全局属性。只有在设备重启动之后，才能应用对这些属性的更改。要打开**“Advanced Settings”（高级设置）**页面，请在树视图中单击**“System”（系统）→“Advanced Settings”（高级设置）**。

配置设备的常规调节参数

“General Settings”（常规设置）页面提供了用于定义常规设备参数的信息。要打开**“General Settings”（常规设置）**页面，请在树视图中单击**“System”（系统）→“Advanced Settings”（高级设置）→“General”（常规）**。

图 6-79. 常规设置



“Attribute”（属性）— 常规设置属性。

“Current”（当前）— 当前配置的值。

“After Reset”（重启动后）— 将来（重启动后）的值。通过在**“After Reset”（重启动后）**列中输入值，可以为字段表分配存储器。

“Max RAM Log Entries (20-400)”（最大 RAM 日志条目 [20 至 400]）— 最大 RAM 日志条目数。如果日志条目已满，日志将被清除，并且日志文件将重新启动。

“Jumbo Frames”（超长帧）— 启用或禁用超长帧功能。超长帧可以使传输相同的数据所需的帧数减少。从而减少开销、处理时间和中断。

使用 CLI 命令查看 RAM 日志条目计数器

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

表 6-48. 常规设置 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。
port jumbo-frame	为设备启用超长帧。

以下是 CLI 命令的示例：

```
Console (config)# logging buffered size
300
```

返回目录页面

返回目录页面

Dell™ PowerConnect™ 5324 系统用户指南

注：注表示可以帮助您更好地使用计算机的重要信息。

注意：注意表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。

警告：警告表示可能会导致财产损失、人身伤害甚至死亡。

2004 年 4 月 Rev. A00

返回目录页面

返回目录页面

使用 Dell OpenManage Switch Administrator

Dell™ PowerConnect™ 5324 系统用户指南

本节介绍了用户界面。

了解界面

主页包含以下视图：

- 树视图 — 位于主页左侧，提供了功能及其组件的可展开视图。
- 设备视图 — 位于主页右侧，提供了设备视图、信息或表区域和配置说明。

图 5-13. Switch Administrator 组件

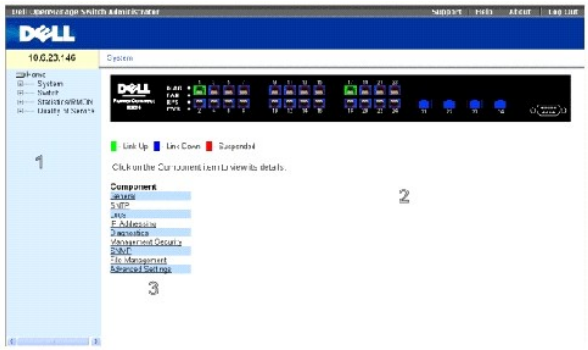


表 5-7 列出了界面组件及其相应的编号。

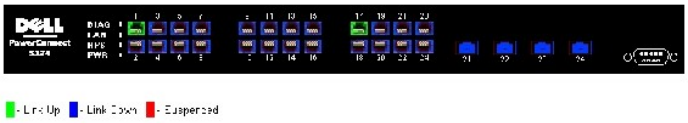
表 5-7. 界面组件

组件	名称
1	树视图包含各种设备功能的列表。可以展开树视图中的分支以查看特定功能下的所有组件，也可以折叠分支以隐藏功能组件。向右拖动垂直条，可以扩展树区域以显示组件的全名。
2	设备视图提供了有关设备端口、当前配置和状态、表信息和功能组件的信息。 根据选定的选项，设备视图底部的区域可以显示其它设备信息和/或配置参数的对话框。
3	组件列表包含功能组件的列表。也可以通过在树视图中展开功能来查看组件。
4	信息按钮使您可以访问有关设备的信息和 Dell 支持。有关详情，请参阅“信息按钮”。

设备图示

PowerConnect 主页包含设备前面板的图示。

图 5-14. 端口 LED 指示灯



端口颜色表明特定端口当前是否处于活动状态。端口可以具有以下颜色：

表 5-8. Led 指示灯

组件	名称
端口指示灯	
绿色	端口当前已启用。
红色	端口上出现了错误。
蓝色	端口当前已禁用。

注： PowerConnect OpenManage Switch Administrator 中的 PowerConnect 前面板上未反映端口 LED。只能通过查看实际设备确定 LED 状态。有关 LED 的详细信息，请参阅“LED 定义”。

使用 Switch Administrator 按钮

本节介绍了 OpenManage Switch Administrator 界面上的按钮。

信息按钮

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

表 5-9. 信息按钮

按钮	说明
“Support”（支持）	打开位于 **support.dell.com** 的 Dell 支持页面。
“Help”（帮助）	联机帮助包含可帮助您配置和管理设备的信息。联机帮助页面直接链接至当前打开的页面。例如，如果打开的是**“IP Addressing”（IP 定址）**页面，则单击**“Help”（帮助）**将打开该页面的帮助主题。
“About”（关于）	包含版本号和 Dell 版权信息。
“Log Out”（退出）	退出应用程序并关闭浏览器窗口。

设备管理按钮

设备管理按钮为配置设备信息提供了一种简单方法，其中包括以下按钮：

表 5-10. 设备管理按钮

按钮	说明
“Apply Changes”（应用更改）	将更改应用于设备。
“Add”（添加）	将信息添加至表或对话框。
“Telnet”	启动 Telnet 会话。
“Query”（查询）	查询表。
“Show All”（全部显示）	显示设备表。

左箭头/右箭头	在列表之间移动信息。
“Refresh”（刷新）	刷新设备信息。
“Reset All Counters”（重设所有计数器）	清除统计计数器。
“Print”（打印）	打印**“Network Management System”（网络管理系统）**页面和/或表信息。
“Show Neighbors Info”（显示邻居信息）	通过**“Neighbors Table”（邻居表）**页面显示**邻居列表**。
“Draw”（绘制）	迅速创建统计图表。

启动应用程序

1. 打开 Web 浏览器。
2. 在地址栏中输入设备的 IP 地址（如 CLI 中所定义）并按 <Enter> 键。

   有关为设备分配 IP 地址的信息，请参阅“静态 IP 地址和子网掩码”。
3. **“Enter Network Password”（输入网络密码）**窗口打开时，输入用户名和密码。

注：设备未配置默认密码，并且可以配置为无需输入密码。有关恢复丢失密码的信息，请参阅“密码恢复”。

注：密码区分大小写，并且只能为字母数字。

4. 单击**“OK”（确定）**。

   系统将打开**“Dell PowerConnect OpenManage™ Switch Administrator”**主页。

通过 CLI 访问设备

可以通过与控制台端口的直接连接或 Telnet 连接来管理设备。使用 CLI 类似于在 Linux 系统中输入命令。如果是通过 Telnet 连接进行访问，请确保在开始使用 CLI 命令之前设备具有已定义的 IP 地址，并且用于访问设备的工作站已连接至设备。

有关配置初始 IP 地址的信息，请参阅“静态 IP 地址和子网掩码”。

注：使用 CLI 之前，请确保已载入客户端。

控制台连接

1. 接通设备电源并等待，直至启动完成。
2. 系统显示 `Console>` 提示符时，键入 `enable`，并按 <Enter> 键。
3. 配置设备并输入必要的命令以完成所需的任务。
4. 任务完成后，使用 `quit` 或 `exit` 命令退出会话。

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

Telnet 连接

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

设备最多同时支持四个 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。

2. 在“Run”（运行）窗口的“Open”（打开）字段中键入 Telnet <IP 地址>。
3. 单击“OK”（确定）以开始 Telnet 会话。

使用 CLI

本节介绍了使用 CLI 的信息。

命令模式概览

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

每种模式均有一个特定的命令，用于从一种命令模式切换到另一种命令模式。

在 CLI 会话初始化过程中，CLI 模式为用户执行模式。在用户执行模式中只能使用有限的命令子集。此模式级别专用于不更改控制台配置的任务，还用于访问配置子系统（例如 CLI）。要进入下一个级别，即优先执行模式，需要密码（如果已配置）。

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

全局配置模式在全局级别管理设备配置。

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

用户执行模式

登录至设备后，执行命令模式处于启用状态。用户级提示符由主机名后跟尖括号 (>) 组成。例如：

```
console>
```

注：如果未在初始配置过程中修改主机名，则默认的主机名为 console。

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

要列出用户执行命令，请在命令提示符后输入问号。

优先执行模式

保护优先访问可以防止未经授权的访问并确保运行参数。密码在屏幕上显示为 ***** 形式，并区分大小写。

要查看并列出优先执行模式命令，请：

1. 在提示符后，键入 enable，并按 <Enter> 键。
2. 当系统显示密码提示符时，输入密码并按 <Enter> 键。

优先执行模式提示符显示为设备主机名后跟 #。例如：

```
console#
```

要列出优先执行命令，请在命令提示符后键入问号并按 <Enter> 键。

要从优先执行模式返回用户执行模式，请使用以下任一命令：disable、exit/end 或 <Ctrl><Z>。

以下示例说明了访问优先执行模式，然后再返回用户执行模式。

```
console>enable

Enter Password: ******

console#

console#disable

console>
```

使用 **exit** 命令可以返回先前模式。例如，从接口配置模式返回全局配置模式，和从全局配置模式返回优先执行模式。

全局配置模式

全局配置命令适用于系统配置，而不是特定的协议或接口。

要访问全局配置模式，请在优先执行模式提示符后键入 configure 并按 <Enter> 键。全局配置模式提示符显示为设备主机名后跟 (config) 和井号 #。

```
console(config)#
```

要列出全局配置命令，请在命令提示符后输入问号。

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

以下示例说明了如何访问全局配置模式并返回优先执行模式：

```
console#

console#configure
```

```
console(config)#exit

console#
```

接口配置模式

接口配置命令用于修改特定的 IP 接口设置（包括网桥组和说明等）。

VLAN 数据库模式

VLAN 模式包含用于从整体上创建和配置 VLAN 的命令，例如，创建一个 VLAN 并将 IP 地址应用于该 VLAN。以下是 VLAN 模式提示符的示例：

```
Console # vlan database

Console (config-vlan)#
```

端口通道模式

端口通道模式包含用于配置链路聚合组 (LAG) 的命令。以下是端口通道模式提示符的示例：

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

Console (config-if)#
```

接口模式

接口模式包含配置接口的命令。可以使用全局配置模式命令 `interface ethernet` 进入接口配置模式。以下是接口模式提示符的示例：

```
console> enable

console# configure

console(config)# interface ethernet g18

console(config-if)#
```

管理访问列表

管理访问列表模式包含用于定义管理访问列表的命令。可以使用全局配置模式命令 `management access-list` 进入管理访问列表配置模式。

以下示例说明了如何创建名为“mlist”的访问列表，配置两个管理接口 ethernet g1 和 ethernet g9，并激活该访问列表。

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

Console (config-macl)# permit ethernet g1

Console (config-macl)# permit ethernet g9

Console (config-macl)# exit

Console (config)# management access-class mlist
```

SSH 公用密钥

SSH 公用密钥模式包含用于手动指定其它设备 SSH 公用密钥的命令。

可以使用全局配置模式命令 `crypto key pubkey-chain ssh` 进入 SSH 公用密钥链配置模式。

以下是进入 SSH 公用密钥链配置模式的示例：

```
Console(config)# crypto key pubkey-chain ssh

Console(config-pubkey-chain)#
```

CLI 示例

提供的 CLI 命令作为配置示例。有关 CLI 命令的完整说明（包括示例），请参阅说明文件 CD 中的“CLI 参考指南”。

返回目录页面

返回目录页面

查看统计数据

Dell™ PowerConnect™ 5324 系统用户指南

统计数据页面包含接口、GVRP、以太网类、RMON 和设备使用的设备信息。要打开**统计数据**页面，请在树视图中单击**“Statistics”（统计数据）**。

注：CLI 命令并非对所有统计数据页面均可用。

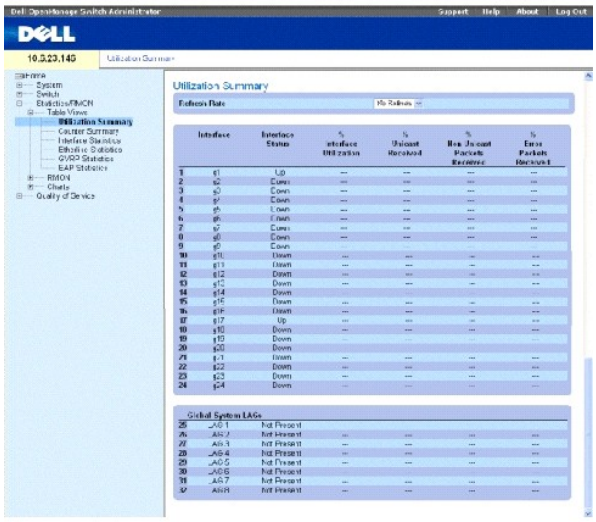
查看表

“Table Views”（表视图）页面包含以图表形式显示统计数据的链接。要打开该页面，请在树视图中单击**“Statistics”（统计数据）→“Table”（表）**。

查看使用摘要

“Utilization Summary”（使用摘要）页面包含接口使用的统计数据。要打开该页面，请在树视图中单击**“Statistics”（统计数据）→“Table Views”（表视图）→“Utilization Summary”（使用摘要）**。

图 8-115. 使用摘要



“Refresh Rate”（刷新率）— 刷新接口统计数据之前经过的时间。

“Interface”（接口）— 接口编号。

“Interface Status”（接口状态）— 接口的状态。

“% Interface Utilization”（% 接口使用）— 基于接口的双工模式的网络接口使用百分比。该读数的范围为 0 至 200%。最大读数 200%（全双工连接）表示通过接口的通信使用了传入和传出连接的 100% 带宽。对于半双工连接，最大读数为 100%。

“% Unicast Received”（% 接收到的单点传送）— 接口上接收到的单点传送信息包的百分比。

“% Non Unicast Packets Received”（% 接收到的非单点传送信息包）— 接口上接收到的非单点传送信息包的百分比。

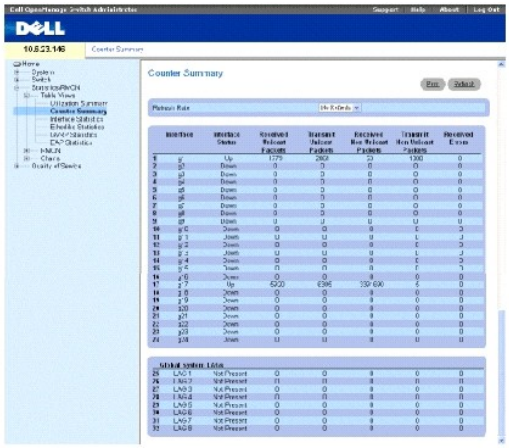
“% Error Packets Received”（% 接收到的错误信息包）— 接口上接收到的包含错误的信息包的数量。

“Global System LAG”（全局系统 LAG）— 当前 LAG/主干性能。

查看计数器摘要

“Counter Summary”（计数器摘要）页面包含端口使用统计数据的数字总和，而不是百分比。要打开**“Counter Summary”（计数器摘要）**页面，请在树视图中单击 **“Statistics/RMON”（统计数据/RMON）→“Table Views”（表视图）→“Counter Summary”（计数器摘要）**。

图 8-116. 计数器摘要



“Refresh Rate”（刷新率）— 刷新接口统计数据之前经过的时间。

“Interface”（接口）— 接口编号。

“Interface Status”（接口状态）— 接口的状态。

“Received Unicast Packets”（接收到的单点传送信息包）— 接口上接收到的单点传送信息包的数量。

“Received Non Unicast Packets”（接收到的非单点传送信息包）— 接口上接收到的非单点传送信息包的数量。

“Transmit Unicast Packets”（发送的单点传送信息包）— 从接口发送的单点传送信息包的数量。

“Transmit Non Unicast Packets”（发送的非单点传送信息包）— 从接口发送的非单点传送信息包的数量。

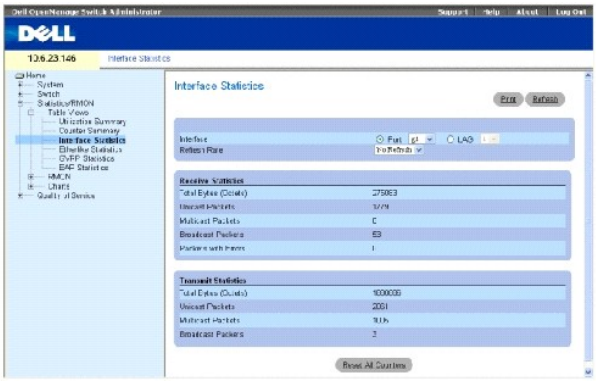
“Received Errors”（接收到的错误）— 接口上接收到的错误信息包的数量。

“Global System LAG”（全局系统 LAG）— 当前 LAG/主干性能。

查看接口统计数据

“Interface Statistics”（接口统计数据）页面包含接收和发送的信息包的统计数据。接收和发送的信息包的字段是相同的。要打开“Interface Statistics”（接口统计数据）页面，请在树视图中单击“Statistics/RMON”（统计数据/RMON）→“Table Views”（表视图）→“Interface Statistics”（接口统计数据）。

图 8-117. 接口统计数据



“Interface”（接口）— 指定显示的是端口还是 LAG 的统计数据。

“Refresh Rate”（刷新率）— 刷新接口统计数据之前经过的时间。

接收统计数据

“Total Bytes (Octets)”（字节 [八位位组] 总数）— 选定接口上接收到的八位位组的数量。

“Unicast Packets”（单点传送信息包）— 选定接口上接收到的单点传送信息包的数量。

“Multicast Packets”（多点传送信息包）— 选定接口上接收到的多点传送信息包的数量。

“Broadcast Packets”（广播信息包）— 选定接口上接收到的广播信息包的数量。

“Packets with Errors”（包含错误的信息包）— 从选定接口接收到的错误信息包的数量。

发送统计数据

“Total Bytes (Octets)”（字节 [八位位组] 总数）— 选定接口上发送的八位位组的数量。

“Unicast Packets”（单点传送信息包）— 选定接口上发送的单点传送信息包的数量。

“Multicast Packets”（多点传送信息包）— 选定接口上发送的多点传送信息包的数量。

“Broadcast Packets”（广播信息包）— 选定接口上发送的广播信息包的数量。

“Packets with Errors”（包含错误的信息包）— 从选定接口发送的错误信息包的数量。

显示接口统计数据

1. 打开**“Interface Statistics”（接口统计数据）**页面。
2. 在**“Interface”（接口）**字段中选择接口。

系统将显示接口统计数据。

重设接口统计数据计数器

1. 打开**“Interface Statistics”（接口统计数据）**页面。
2. 单击**“Reset All Counters”（重设所有计数器）**。

系统将重设接口统计数据计数器。

使用 CLI 命令查看接口统计数据

下表概括了用于查看接口统计数据的等效 CLI 命令。

表 8-80. 接口统计数据 CLI 命令

CLI 命令	说明
show interfaces counters [**ethernet 接口	port-channel 端口信道号**]	显示经由物理接口的通信。

以下是 CLI 命令的示例：

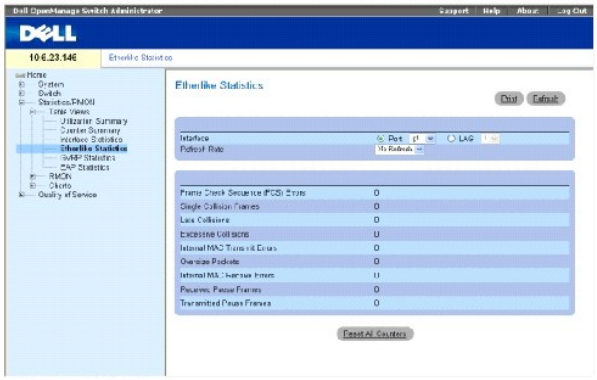
```
Console> enable

Console# show interfaces counters

Port      InOctets      InUcastPkts      InMcastPkts      InBcastPkts
--------  ------------  ---------------  ---------------  ------------
g1        183892        1289             987              8
```

g2	0	0	0	0
g3	123899	1788	373	19
Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
----	----------	----------	----------	----------
g4	9188	9	8	0
g5	0	0	0	0
g6	8789	27	8	0
Ch	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
----	----------	----------	----------	----------
1	27889	928	0	78
Ch	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
----	----------	----------	----------	----------
1	23739	882	0	122

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）**。

图 8-118. 以太网类统计数据



“Interface”（接口）— 指定显示的是端口还是 LAG 的统计数据。

“Refresh Rate”（刷新率）— 刷新接口统计数据之前经过的时间。

“Frame Check Sequence (FCS) Errors”（帧检查顺序 [FCS] 错误）— 选定接口上接收到的 FCS 错误的数量。

“Single Collision Frames”（单冲突帧）— 选定接口上接收到的单冲突帧的数量。

“Multiple Collision Frames”（多冲突帧）— 选定接口上接收到的多冲突帧的数量。

“Single Quality Error (SQE) Test Errors”（单质量错误 [SQE] 检测错误）— 选定接口上接收到的 SQE 检测错误的数量。

“Deferred Transmissions”（延迟的传输）— 选定接口上延迟传输的数量。

“Late Collision”（推迟冲突）— 选定接口上接收到的推迟冲突帧的数量。**“Excessive Collisions”（严重冲突）** 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）— 选定接口上内部 MAC 发送错误的数量。

“Carrier Sense Errors”（载波侦听错误）— 选定接口上载波侦听错误的数量。

“Oversize Packets”（超大信息包）— 选定接口上超大信息包错误的数量。

“Internal MAC Receive Errors”（内部 MAC 接收错误）— 选定接口上内部 MAC 接收错误的数量。

“Single Quality Errors (SQE) Test Errors”（单质量错误 [SQE] 检测错误）— 选定接口上接收到的 SQE 检测错误的数量。

“Receive Pause Frames”（接收到的暂停帧）— 选定接口上接收到的暂停帧的数量。

“Transmitted Pause Frames”（发送的暂停帧）— 从选定接口发送的暂停帧的数量。

显示接口的以太网类统计数据

1. 打开**“Etherlike Statistics”（以太网类统计数据）**页面。
2. 在**“Interface”（接口）**字段中选择接口。

   系统将显示接口的以太网类统计数据。

重设以太网类统计数据

1. 打开**“Etherlike Statistics”（以太网类统计数据）**页面。
2. 单击**“Reset All Counters”（重设所有计数器）**。

   系统将重设以太网类统计数据。

使用 CLI 命令查看以太网类统计数据

下表概括了用于查看以太网类统计数据的等效 CLI 命令。

表 8-81. 以太网类统计数据 CLI 命令

CLI 命令	说明
show interfaces counters [ethernet 接口 **| port-channel 端口信道号]**	显示经由物理接口的通信。

以下是 CLI 命令的示例：

```
Console> enable

Console# show interfaces counters ethernet g1

Port    InOctets    InUcastPkts    InMcastPkts    InBcastPkts
------  ----------  -------------  -------------  ------------
g1      183892      1289           987            8

Port    OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
------  ----------  -------------  -------------  ------------
g1      9188        9              8              0

FCS Errors: 8

Single Collision Frames: 0
```

```
Multiple Collision Frames: 0

SQE Test Errors: 0

Deferred Transmissions: 0

Late Collisions: 0

Excessive Collisions: 0

Internal MAC Tx Errors: 0

Carrier Sense Errors: 0

Oversize Packets: 0

Internal MAC Rx Errors: 0

Received Pause Frames: 0

Transmitted Pause Frames: 0
```

查看 GVRP 统计数据

"GVRP Statistics"（GVRP 统计数据）页面包含 GVRP 的设备统计数据。要打开该页面，请在树视图中单击 **"Statistics/RMON"（统计数据/RMON）→"Table Views"（表视图）→"GVRP Statistics"（GVRP 统计数据）**。

图 8-119. GVRP 统计数据

"Interface"（接口）— 指定显示的是端口还是 LAG 的统计数据。

“Refresh Rate”（刷新率）— 刷新接口统计数据之前经过的时间。

“Join Empty”（加入空）— 设备的 GVRP 加入空统计数据。

“Empty”（空）— 设备的 GVRP 空统计数据。

“Leave Empty”（保留空）— 设备的 GVRP 保留空统计数据。

“Join In”（加入）— 设备的 GVRP 加入统计数据。

“Leave In”（保留）— 设备的 GVRP 保留统计数据。

“Leave All”（全部离开）— 设备的 GVRP 全部离开统计数据。

“Invalid Protocol ID”（无效协议 ID）— 设备的 GVRP 无效协议 ID 统计数据。

“Invalid Attribute Type”（无效属性类型）— 设备的 GVRP 无效属性 ID 统计数据。

“Invalid Attribute Value”（无效属性值）— 设备的 GVRP 无效属性值统计数据。

“Invalid Attribute Length”（无效属性长度）— 设备的 GVRP 无效属性长度统计数据。

“Invalid Events”（无效事件）— 设备的 GVRP 无效事件统计数据。

显示端口的 GVRP 统计数据

1. 打开**“GVRP Statistics”（GVRP 统计数据）**页面。
2. 在**“Interface”（接口）**字段中选择接口。

系统显示接口的 GVRP 统计数据。

重设 GVRP 统计数据

1. 打开**“GVRP Statistics”（GVRP 统计数据）**页面。
2. 单击**“Reset All Counters”（重设所有计数器）**。

系统将重设 GVRP 计数器。

使用 CLI 命令查看 GVRP 统计数据

下表概括了用于查看 GVRP 统计数据的等效 CLI 命令。

表 8-82. GVRP 统计数据 CLI 命令

CLI 命令	说明
show gvrp statistics [ethernet 接口 | port-channel 端口信道号]	显示 GVRP 统计数据。
show gvrp error-statistics [ethernet 接口 | port-channel 端口信道号]	显示 GVRP 错误统计数据。

以下是 CLI 命令的示例：

```
Console# show gvrp statistics

GVRP statistics:

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

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

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

g8	0	0	0	0	0	0	0	0	0	0	0	0

```
Console# show gvrp error-statistics

GVRP error statistics:

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

Legend:
```

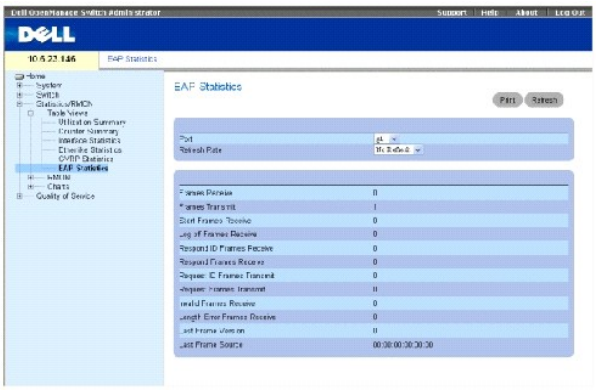
INVPROT : Invalid Protocol Id	INVPLEN : Invalid PDU Length
INVATYP : Invalid Attribute Type	INVALEN : Invalid Attribute Length
INVAVAL : Invalid Attribute Value	INVEVENT : Invalid Event

Port	INVPROT	INVATYP	INVAVAL	INVALEN	INVEVENT
----	-------	-------	-------	-------	--------
g1	0	0	0	0	0
g2	0	0	0	0	0
g3	0	0	0	0	0
g4	0	0	0	0	0
g5	0	0	0	0	0
g6	0	0	0	0	0
g7	0	0	0	0	0
g8	0	0	0	0	0

查看 EAP 统计数据

“EAP Statistics”（EAP 统计数据）页面包含有关特定端口上接收到的 EAP 信息包的信息。有关 EAP 的详细信息，请参阅“基于端口的验证（802.1x）”。要打开**“EAP Statistics”（EAP 统计数据）**页面，请在树视图中单击**“Statistics/RMON”（统计数据/RMON）>“Table Views”（表视图）>“EAP Statistics”（EAP 统计数据）**。

图 8-120. EAP 统计数据



“Port”（端口）— 对其进行轮询以获得统计数据的端口。

“Refresh Rate”（刷新率）— 刷新接口统计数据之前经过的时间。

“Frames Receive”（接收到的帧）— 端口上接收到的有效 EAPOL 帧的数量。

“Frames Receive”（发送的帧）— 通过端口发送的 EAPOL 帧的数量。

“Start Frames Receive”（接收到的启动帧）— 端口上接收到的 EAPOL 启动帧的数量。

“Log off Frames Receive”（接收到的注销帧）— 端口上接收到的 EAPOL 注销帧的数量。

“Respond ID Frames Receive”（接收到的响应 ID 帧）— 端口上接收到的 EAP 响应/ID 帧的数量。

“Respond Frames Receive”（接收到的响应帧）— 端口上接收到的有效 EAP 响应帧的数量。

“Request ID Frames Transmit”（发送的请求 ID 帧）— 通过端口发送的 EAP 请求 ID 帧的数量。

“Request Frames Transmit”（发送的请求帧）— 通过端口发送的 EAP 请求帧的数量。

“Invalid Frames Receive”（接收到的无效帧）— 该端口上接收到的无法识别的 EAPOL 帧的数量。

“Length Error Frames Receive”（接收到的长度错误帧）— 该端口上接收到的具有无效信息包正文长度的 EAPOL 帧的数量。

“Last Frame Version”（上一帧版本）— 与最近一次接收到的 EAPOL 帧相关的协议版本号。

“Last Frame Source”（上一帧的源）— 与最近一次接收到的 EAPOL 帧相关的源 MAC 地址。

显示端口的 EAP 统计数据

1. 打开**“EAP Statistics”（EAP 统计数据）**页面。
2. 在**“Interface”（接口）**字段中选择接口。

系统将显示接口 EAP 统计数据。

重设 EAP 统计数据

1. 打开**“EAP Statistics”（EAP 统计数据）**页面。
2. 单击**“Reset All Counters”（重设所有计数器）**以重设计数器。

系统将重设 EAP 统计数据。

使用 CLI 命令查看 EAP 统计数据

下表概括了用于查看 EAP 统计数据的 CLI 命令。

表 8-83. GVRP 统计数据 CLI 命令

CLI 命令	说明
show dot1x statistics ethernet 接口	显示指定接口的 802.1X 统计数据。

以下是 CLI 命令的示例：

```
Switch# show dot1x statistics ethernet g1

EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0
```

```
EapLengthErrorFramesRx: 0


LastEapolFrameVersion: 1


LastEapolFrameSource: 0008.3b79.8787
```

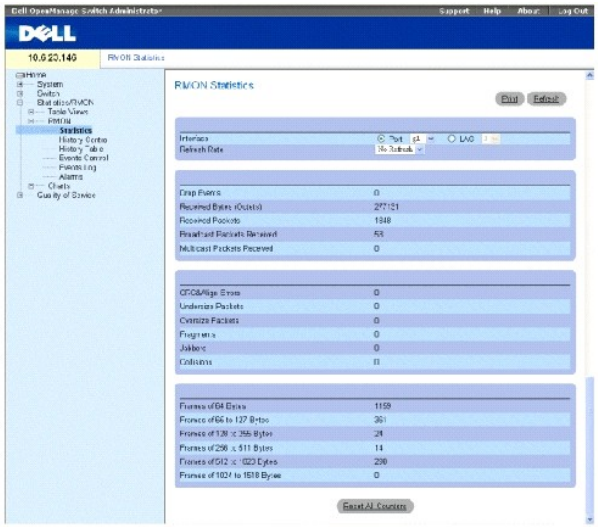
查看 RMON 统计数据

远程监测 (RMON) 包含用于从远程位置查看网络信息的链接。要打开**“RMON”**页面，请在树视图中单击**“Statistics/RMON”（统计数据/RMON）→“RMON”**。

查看 RMON 统计数据组

“RMON Statistics”（RMON 统计数据）页面包含用于查看有关设备使用和设备上出现的错误的信息的字段。要打开**“RMON Statistics”（RMON 统计数据）**页面，请在树视图中单击**“Statistics/RMON”（统计数据/RMON）→“RMON”→“Statistics”（统计数据）**。

图 8-121. RMON 统计数据



“Interface”（接口）— 指定显示的是端口还是 LAG 的统计数据。

“Refresh Rate”（刷新率）— 刷新统计数据之前经过的时间。

“Drop Events”（丢弃事件）— 自上一次刷新设备以来接口上发生的丢弃事件的数量。

“Received Bytes (Octets)”（接收到的字节 [八位位组]）— 自上一次刷新设备以来接口上接收到的八位位组的数量。该数量包括坏信息包和 FCS 八位位组，但不包括成帧位。

“Received Packets”（接收到的信息包）— 自上一次刷新设备以来接口上接收到的信息包的数量，包括坏信息包、多点传送信息包和广播信息包。

“Broadcast Packets Received”（接收到的广播信息包）— 自上一次刷新设备以来接口上接收到的完好广播信息包的数量。该数量不包括多点传送信息包。

“Multicast Packets Received”（接收到的多点传送信息包）— 自上一次刷新设备以来接口上接收到的完好多点传送信息包的数量。

“CRC & Align Errors”（CRC 和校准错误）— 自上一次刷新设备以来接口上发生的 CRC 和校准错误的数量。

“Undersize Packets”（超小信息包）— 自上一次刷新设备以来接口上接收到的超小信息包（少于 64 个八位位组）的数量。

“Oversize Packets”（超大信息包）— 自上一次刷新设备以来接口上接收到的超大信息包（超过 1518 个八位位组）的数量。

“Fragments”（碎片）— 自上一次刷新设备以来接口上接收到的碎片（少于 64 个八位位组的信息包，不包括成帧位，但包括 FCS 八位位组）的数量。

“Jabbers”（无用信息）— 自上一次刷新设备以来接口上接收到的无用信息（超过 1518 个八位位组的信息包）的数量。

“Collisions”（冲突）— 自上一次刷新设备以来接口上接收到的冲突的数量。

“Frames of xx Bytes”（xx 字节的帧）— 自上一次刷新设备以来接口上接收到的 **xx** 字节帧的数量。

查看接口统计数据

1. 打开**“RMON Statistics”（RMON 统计数据）**页面。
2. 在**“Interface”（接口）**字段中选择接口类型和编号。

系统将显示接口统计数据。

使用 CLI 命令查看 RMON 统计数据

下表概括了用于查看 RMON 统计数据的等效 CLI 命令。

表 8-84. RMON 统计数据 CLI 命令

CLI 命令	说明
show rmon statistics {ethernet 接口 | port-channel 端口信道号}	显示 RMON 以太网统计数据。

以下是 CLI 命令的示例：

```
console> enable
```

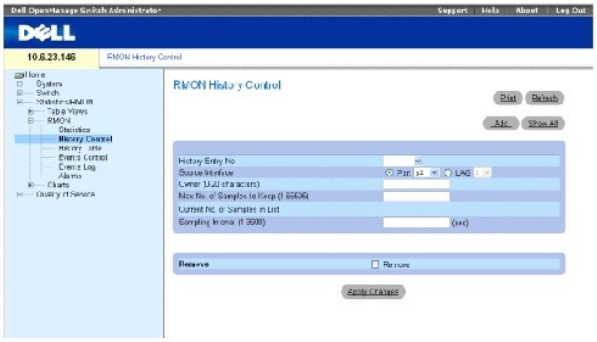
```
console> enable
```

```
Console# show rmon statistics ethernet g1

Port g1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0

Fragments: 0 Jabbers: 0

64 Octets: 98 65 to 127 Octets: 0

128 to 255 Octets: 0 256 to 511 Octets: 0

512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

查看 RMON 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数据样例的信息。例如，样例可能包含接口定义或轮询周期。要打开**"RMON History Control"（RMON 历史记录控制）**页面，请在树视图中单击**"Statistics/RMON"（统计数据/RMON）→"History Control"（历史记录控制）**。

图 8-122. RMON 历史记录控制



"History Entry No."（历史记录条目号） —**"History Control Table"（历史记录控制表）**页面的条目号。

"Source Interface"（源接口）— 是从端口还是 LAG 获取历史记录样例。

“Owner (0-20 characters)”（所有者 [0 至 20 个字符]） — 请求 RMON 信息的 RMON 站点或用户。

“Max No. of Samples to Keep (1-65535)”（要保留的最大样例数 [1 至 65535]） — 要保存的样例的数量。默认值为“50”。

“Current No. of Samples in List”（当前列表中的样例数） — 当前获取的样例数。

“Sampling Interval (1-3600)”（取样间隔 [1 至 3600]） — 表示从端口取样的时间（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） — 选择该选项时，将删除**“History Control Table”（历史记录控制表）**条目。

添加历史记录控制条目

1. 打开**“RMON History Control”（RMON 历史记录控制）**页面。
2. 单击**“Add”（添加）**。

   系统将打开**“Add History Entry”（添加历史记录条目）**页面。
3. 完成对话框中的字段。
4. 单击**“Apply Changes”（应用更改）**。

   条目将被添加至**“History Control Table”（历史记录控制表）**。

修改历史记录控制表条目

1. 打开**“RMON History Control”（RMON 历史记录控制）**页面。
2. 在**“History Entry No.”（历史记录条目号）**字段中选择一个条目。
3. 根据需要修改字段。
4. 单击**“Apply Changes”（应用更改）**。

   系统将修改表条目，并更新设备。

删除历史记录控制表条目

1. 打开**“RMON History Control”（RMON 历史记录控制）**页面。
2. 在**“History Entry No.”（历史记录条目号）**字段中选择一个条目。
3. 单击**“Remove”（删除）**。
4. 单击**“Apply Changes”（应用更改）**。

   系统将删除选定的表条目，并更新设备。

使用 CLI 命令查看 RMON 历史记录控制

下表概括了用于查看 GVRP 统计数据的等效 CLI 命令。

表 8-85. RMON 历史记录 CLI 命令

CLI 命令	说明
rmon collection history 索引 [owner 所有者名称 | buckets 存储区号] [interval 秒]	启用和配置接口上的 RMON。
show rmon collection history [ethernet 接口 | port-channel 端口信道号]	显示 RMON 收集历史纪录统计数据。

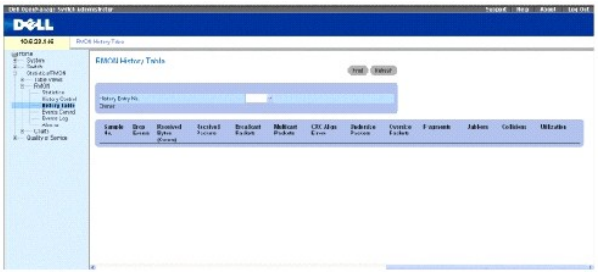
以下是 CLI 命令的示例：

```
Console (config)#
interface ethernet g8


Console (config-if)# rmon
collection history 1
interval 2400


Console(config-if)# exit


Console (config)# exit
```

查看 RMON 历史记录表

"RMON History Table"（RMON 历史记录表）包含特定接口的网络取样统计信息。每个表条目表示在单个取样过程中编译的所有计数器值。要打开**"RMON History Table"（RMON 历史记录表）**，请在树视图中单击**"Statistics/RMON"（统计数据/RMON）→"RMON"→"History Table"（历史记录表）**。

图 8-123. RMON 历史记录表



"Sample No."（样例号）— 表中信息反映的特定样例。

"Drop Events"（丢弃事件）— 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。该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]）— 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）— 在取样间隔期间接收到的信息包的数量。

"Broadcast Packets"（广播信息包）— 在取样间隔期间接收到的完好广播信息包的数量。

"Multicast Packets"（多点传送信息包）— 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）— 在取样会话过程中接收到的长度为 64 至 1518 个八位位组、坏帧检查顺序 (FCS)、整数个八位位组或包含非整数个 FCS 的信息包的数量。

“Undersized Packets”（超小信息包）— 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。

“Oversize Packets”（超大信息包）— 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）— 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）— 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使用情况。该值用百分比表示。

查看特定历史记录条目的统计数据

1. 打开**“RMON History Table”（RMON 历史记录表）**。
2. 在**“History Table No.”（历史记录表编号）**字段中选择一个条目。

该条目的统计数据将显示在“RMON History Table”（RMON 历史记录表）中。

使用 CLI 命令查看 RMON 历史记录控制

下表概括了用于查看 RMON 历史记录的等效 CLI 命令。

表 8-86. RMON 历史记录控制 CLI 命令

CLI 命令	说明
show rmon history 索引 {throughput | errors | other} [period 秒]	显示 RMON 以太网统计数据历史记录。

以下是用于显示 RMON 以太网统计数据（索引 1 上的吞吐量）的 CLI 命令的示例：

```
console> enable

Console# show rmon history 1 throughput
```

Sample Set: 1	Owner: CLI
Interface: g1	Interval: 1800
Requested samples: 50	Granted samples: 50

Maximum table size: 500					
Time	Octets	Packets	Broadcast	Multicast	%
----------	----------	----------	----------	----------	----------
Jan 18 2004 21:57:00	303595962	357568	3289	7287	19.98%
Jan 18 2004 21:57:30	287696304	275686	2789	2789	20.17%

定义设备 RMON 事件

"RMON Events Control"（RMON 事件控制）页面包含用于定义 RMON 事件的字段。要打开**"RMON Events Control"（RMON 事件控制）**页面，请在树视图中单击 **"Statistics/RMON"（统计数据/RMON）→"RMON"→"Events Control"（事件控制）**。

图 8-124. RMON 事件控制

"Event Entry"（事件条目）— 表示事件。

"Community"（团体）— 事件所属的团体。

"Description"（说明）— 用户定义的事件说明。

"Type"（类型）— 说明事件的类型。可能的值包括：

"Log"（日志）— 事件类型为日志条目。

"Trap"（陷阱）— 事件类型为陷阱。

"Log and Trap"（日志和陷阱）— 事件类型既是日志条目，又是陷阱。

"None"（无）— 无事件。

“Time”（时间）— 事件发生的时间（例如，2004 年 3 月 29 日上午 11 点将显示为 29/03/2004 11:00:00）。

“Owner”（所有者）— 定义事件的设备或用户。

“Remove”（删除）— 选择该选项时，将从“RMON Events Table”（RMON 事件表）中删除事件。

添加 RMON 事件

1. 打开**“RMON Events Control”（RMON 事件控制）**页面。
2. 单击**“Add”（添加）**。

   系统将打开**“Add an Event Entry”（添加事件条目）**页面。
3. 完成对话框中的信息并单击**“Apply Changes”（应用更改）**。

   系统将添加**“Event Table”（事件表）**条目，并更新设备。

修改 RMON 事件

1. 打开**“RMON Events Control”（RMON 事件控制）**页面。
2. 在**“Event Table”（事件表）**中选择一个条目。
3. 修改对话框中的字段并单击**“Apply Changes”（应用更改）**。

   系统将修改**“Event Table”（事件表）**条目，并更新设备。

删除 RMON 事件条目

1. 打开**“RMON Events Control”（RMON 事件控制）**页面。
2. 单击**“Show All”（全部显示）**。

   系统将打开**“Events Table”（事件表）**页面。
3. 对于需要删除的事件，选择**“Remove”（删除）**，然后单击**“Apply Changes”（应用更改）**。

   系统将删除选定的表条目，并更新设备。

注：在**“RMON Events Control”（RMON 事件控制）**页面中，通过选取该页面上的**“Remove”（删除）**复选框可以删除单个事件条目。

使用 CLI 命令定义设备事件

下表概括了用于定义设备事件的等效 CLI 命令。

表 8-87. 设备事件定义 CLI 命令

CLI 命令	说明
rmon event 索引类型 [community 文本] [description 文本] [owner 名称]	配置 RMON 事件。
show rmon events	显示 RMON 事件表。

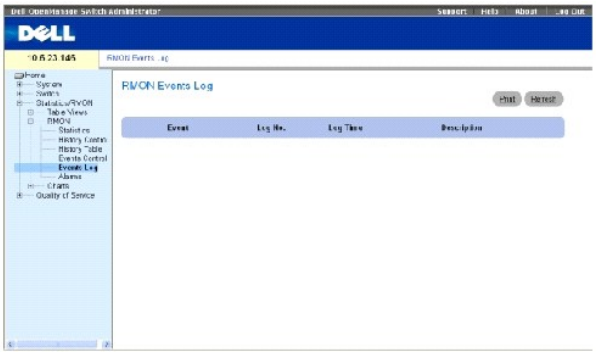
以下是 CLI 命令的示例：

```
console> enable

console# config

console (config)# rmon event 1 log

console(config)#exit

Console# show rmon events

Index   Description   Type    Community   Owner   Last time sent
-----   -----------   -------- ---------  -------  --------------------
1       Errors        Log                 CLI     Jan 18 2002 23:58:17
2       High Broadcast Log-Trap router    Manager Jan 18 2002 23:59:48
```

查看 RMON 事件日志

"RMON Events Log"（RMON 事件日志）页面包含 RMON 事件的列表。要打开**"RMON Events Log"（RMON 事件日志）**页面，请在树视图中单击**"Statistics/RMON"（统计数据/RMON）→"RMON"→"Events"（事件）**。

图 8-125. RMON 事件日志



"Event"（事件）— RMON 事件日志条目号。

"Log No."（日志号）— 日志编号。

“Log Time”（记录时间）— 输入日志条目的时间。

“Description”（说明）— 说明日志条目。

使用 CLI 命令定义设备事件

下表概括了用于定义设备事件的等效 CLI 命令。

表 8-88. 设备事件定义 CLI 命令

CLI 命令	说明
show rmon log [**事件**]	显示 RMON 记录表。

以下是 CLI 命令的示例：

```
console> enable

console# config

console (config)# rmon event 1 log

console(config)#exit

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
```

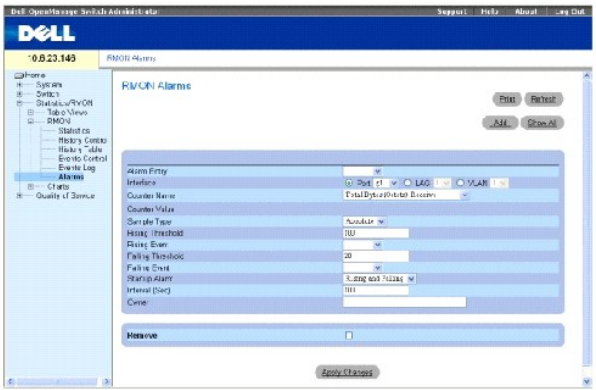
Maximum table size: 500 (800 after reset)

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 RMON 设备警报

“RMON Alarm”（RMON 警报）页面包含用于设置网络警报的字段。当系统检测到网络问题或事件时就会发出网络警报。阈值上升和下降也会生成事件。要打开**“RMON Alarm”（RMON 警报）**页面，请在树视图中单击**“Statistics/RMON”（统计数据/RMON）→“RMON”→“Alarms”（警报）**。

图 8-126. RMON 警报



“Alarm Entry”（警报条目）— 表示特定的警报。

“Interface”（接口）— 显示其 RMON 统计数据的接口。

“Counter Name”（计数器名称）— 选定的 MIB 变量。

“Counter Value”（计数器值）— 选定的 MIB 变量的值。

“Sample Type”（样例类型）— 指定选定变量的取样方法，并将其值与阈值进行比较。可能的字段值包括：

“Delta”（增量）— 从当前值中减去上一次取样值。将差值与阈值进行比较。

“Absolute”（绝对）— 在取样间隔结束时将值直接与阈值进行比较。

“Rising Threshold”（上升阈值）— 触发上升阈值警报的上升计数器值。上升阈值显示在图形栏顶部。每个被监测的变量均被指定一种颜色。

“Rising/Falling Event”（上升/下降事件）— 报告警报的机制 — 日志、陷阱或二者的结合。如果选择日志，则在设备或管理系统中均无保存机制。但是，如果不重启动设备，日志将保留在设备日志表中。如果选择陷阱，将通过陷阱的一般机制生成和报告 SNMP 陷阱。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。下降阈值以图形形式显示在图形栏底部。每个被监测的变量均被指定一种颜色。

“Startup Alarm”（启动警报）— 用于激活警报生成的触发器。可以通过将阈值从较低阈值提升到较高阈值来定义上升。

“Interval (sec)”（时间间隔 [秒]）— 警报的间隔时间。

“Owner”（所有者）— 定义警报的设备或用户。

“Remove”（删除）— 选择该选项时，将删除 RMON 警报。

添加警报表条目

1. 打开**“RMON Alarms”（RMON 警报）**页面。
2. 单击**“Add”（添加）**。

   系统将打开**“Add an Alarm Entry”（添加警报条目）**页面。

图 8-127. “Add an Alarm Entry”（添加警报条目）页面

3. 选择接口。
4. 完成对话框中的字段。
5. 单击**“Apply Changes”（应用更改）**。

   系统将添加 RMON 警报，并更新设备。

修改警报表条目

1. 打开“RMON Alarms”（RMON 警报）页面。
2. 在“Alarm Entry”（警报条目）下拉式菜单中选择一个条目。
3. 根据需要修改对话框中的字段。
4. 单击“Apply Changes”（应用更改）。

系统将修改条目，并更新设备。

显示警报表

1. 打开“RMON Alarms”（RMON 警报）页面。
2. 单击“Show All”（全部显示）。

系统将打开“Alarm Table”（警报表）页面。

删除警报表条目

1. 打开“RMON Alarms”（RMON 警报）页面。
2. 在“Alarm Entry”（警报条目）下拉式菜单中选择一个条目。
3. 选取“Remove”（删除）复选框。
4. 单击“Apply Changes”（应用更改）。

系统将删除选定的条目，并更新设备。

使用 CLI 命令定义设备警报

下表概括了用于定义设备警报的等效 CLI 命令。

表 8-89. 设备警报 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 RMON 警报条件。
show rmon alarm-table	显示警报表的摘要。
show rmon alarm	显示 RMON 警报配置。

以下是 CLI 命令的示例：

```
console> enable

console# config

Console (config)# rmon alarm 1000 dell 360000 1000000 1000000 10 20

Console# show rmon alarm-table
```


Index	OID	Owner
------	-------------------	--------------
1	1.3.6.1.2.1.2.2.1.1 0.1	CLI
2	1.3.6.1.2.1.2.2.1.1 0.1	Manager
3	1.3.6.1.2.1.2.2.1.1 0.9	CLI

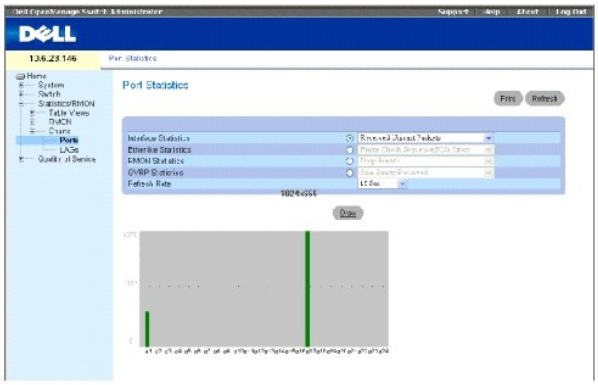
查看图表

“Chart”（图表）页面包含以图表格式显示统计数据的链接。要打开该页面，请在树视图中单击**“Statistics”（统计数据）→“Charts”（图表）**。

查看端口统计数据

“Port Statistics”（端口统计数据）页面包含以图表格式显示端口元素统计数据的字段。要打开**“Port Statistics”（端口统计数据）**页面，请在树视图中单击**“Statistics”（统计数据）→“Charts”（图表）→“Ports”（端口）**。

图 8-128. 端口统计数据



“Interface Statistics”（接口统计数据）— 选择要打开的接口统计数据的类型。

“Etherlike Statistics”（以太网类统计数据）— 选择要打开的以太网类统计数据的类型。

“RMON Statistics”（RMON 统计数据）— 选择要打开的 RMON 统计数据的类型。

“GVRP Statistics”（GVRP 统计数据）— 选择要打开的 GVRP 统计数据的类型。

“Refresh Rate”（刷新率）— 刷新统计数据之前经过的时间。

显示端口统计数据

1. 打开**“Port Statistics”（端口统计数据）**页面。
2. 选择要打开的统计数据的类型。
3. 从**“Refresh Rate”（刷新率）**下拉式菜单中选择所需的刷新率。
4. 单击**“Draw”（绘制）**。

系统将显示选定统计数据的图形。

使用 CLI 命令查看端口统计数据

下表概括了用于查看端口统计数据的等效 CLI 命令。

表 8-90. 端口统计数据 CLI 命令

CLI 命令	说明
show interfaces counters [**ethernet** 接口 | **port-channel 端口信道号**]	显示经由物理接口的通信。
show rmon statistics {**ethernet 接口 | port-channel 端口信道号**}	显示 RMON 以太网统计数据。
show gvrp statistics {**ethernet 接口 | port-channel 端口信道号**}	显示 GVRP 统计数据。
show gvrp error-statistics {**ethernet 接口 | port-channel 端口信道号**}	显示 GVRP 错误统计数据。

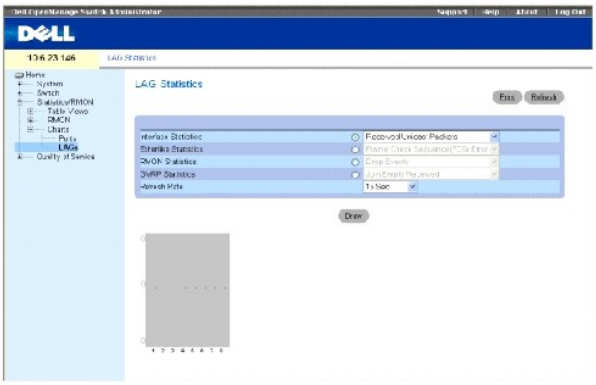
Console# **show interfaces description ethernet g1**

Port	Description
----	----------
g1	Management_port
g2	R&D_port
g3	Finance_port
Ch	Description
----	----------
1	Output

查看 LAG 统计数据

“LAG Statistics”（LAG 统计数据）页面包含以图表格式显示 LAG 统计数据的字段。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）→“LAG”**。

图 8-129. LAG 统计数据



“Interface Statistics”（接口统计数据）— 选择要打开的接口统计数据的类型。

“Etherlike Statistics”（以太网类统计数据）— 选择要打开的以太网类统计数据的类型。

“RMON Statistics”（RMON 统计数据）— 选择要打开的 RMON 统计数据的类型。

“GVRP Statistics”（GVRP 统计数据）— 选择要打开的 GVRP 统计数据的类型。

“Refresh Rate”（刷新率）— 刷新统计数据之前经过的时间。

显示 LAG 统计数据

1. 打开**“LAG Statistics”（LAG 统计数据）**页面。
2. 选择要打开的统计数据的类型。
3. 从**“Refresh Rate”（刷新率）**下拉式菜单中选择所需的刷新率。
4. 单击**“Draw”（绘制）**。

系统将显示选定统计数据的图形。

使用 CLI 命令查看 LAG 统计数据

下表概括了用于查看 LAG 统计数据的等效 CLI 命令。

表 8-91. LAG 统计数据 CLI 命令

CLI 命令	说明
show interfaces counters [**ethernet 接口	port-channel 端口信道号**]	显示经由物理接口的通信。
show rmon statistics {**ethernet 接口	port-channel 端口信道号**}	显示 RMON 以太网统计数据。
show gvrp statistics {**ethernet 接口	port-channel 端口信道号**}	显示 GVRP 统计数据。
show gvrp error-statistics {**ethernet 接口	port-channel 端口信道号**}	显示 GVRP 错误统计数据。

```
Console# show gvrp statistics
```

GVRP statistics:

---

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

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

返回目录页面