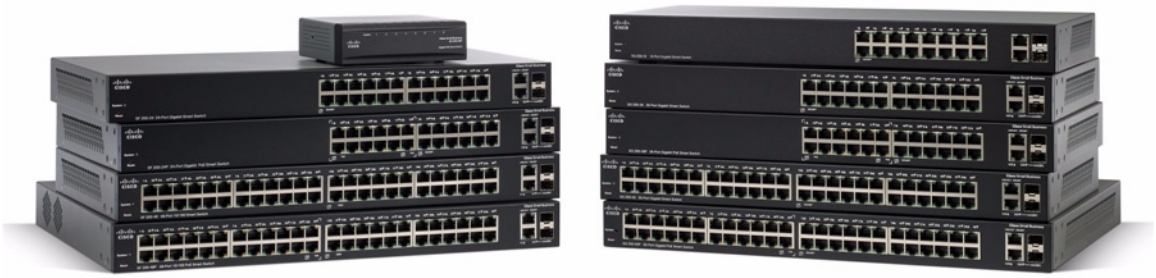

管理指南

思科 200 系列智能型交换机管理指南

目录

1

使用入门

本节介绍了基于 Web 的配置实用程序，具体包括以下主题：

- **启动基于 Web 的交换机配置实用程序**
- **交换机配置快速入门**
- **接口命名约定**
- **窗口导航**

启动基于 Web 的交换机配置实用程序

本节介绍了如何导航基于 Web 的交换机配置实用程序。

如果您使用了弹出窗口拦截器，请确保已将其禁用。

浏览器具有如下限制：

- 如果使用的是旧版 Internet Explorer，将无法直接使用 IPv6 地址访问交换机。但是，可以使用 DNS （域名系统）服务器创建包含 IPv6 地址的域名，然后在地址栏中使用该域名代替 IPv6 地址。
- 如果管理站上有多个 IPv6 接口，则可以使用 IPv6 全局地址代替 IPv6 链路本地地址，而从浏览器访问交换机。

启动配置实用程序

打开基于 Web 的配置实用程序的步骤：

步骤 1 打开任一 Web 浏览器。

步骤 2 在浏览器地址栏中输入要配置的交换机的 IP 地址，然后按 **Enter**。此时将显示*登录*页面。

注 当交换机使用出厂默认 IP 地址 192.168.1.254 时，其电源 LED 将持续闪烁。当交换机使用 DHCP 分配的 IP 地址或管理员配置的静态 IP 地址时，电源 LED 将持续亮起。

登录

默认用户名为 **cisco**，默认密码为 **cisco**。第一次使用默认用户名和密码登录时，您需要输入新密码。

注 如果您之前没有为 GUI 选择语言，则登录页面的语言将由浏览器所请求的语言以及交换机上配置的语言决定。例如，如果浏览器请求使用中文，且中文已加载到交换机中，则登录页面将自动显示为中文。如果中文尚未加载到交换机中，登录页面将显示为英文。

加载到交换机中的语言具有一个语言和国家 / 地区代码 （en-US、 en-GB 等）。若要使登录页面自动以特定语言显示，根据浏览器请求，浏览器的语言和国家 / 地区代码请求必须与交换机上所加载语言的代码相匹配。如果浏览器请求仅包含语言代码，而不包含国家 / 地区代码 （例如：fr），系统将会采用第一个具有匹配语言代码 （而没有匹配国家 / 地区代码，例如：fr_CA）的嵌入式语言。

登录到设备配置实用程序的步骤：

步骤 1 输入用户名 / 密码。该密码最多可以包含 64 个 ASCII 字符。在 “**配置安全性**” 一章中的 “**设置密码复杂性规则**” 一节中介绍了密码复杂性规则。

步骤 2 如果不使用英文，可以从*语言*下拉菜单中选择所需的语言。要为交换机添加新语言或更新当前语言，请参阅 “*升级 / 备份固件 / 语言*” 一节。

步骤 3 如果这是首次使用默认用户 ID (**cisco**) 和默认密码 (**cisco**) 登录，或者密码已过期，将会打开*更改密码*页面。有关其他信息，请参阅 “*密码过期*”。

步骤 4 选择是否选择**禁用密码复杂性规则**。有关密码复杂性的详情，请参阅 “*设置密码复杂性规则*” 一节。

步骤 5 输入新密码并单击**应用**。

如果登录尝试成功，将会打开*使用入门*页面。

如果输入了错误的用户名或密码，将显示错误消息，而窗口上会继续显示*登录*页面。

选择**启动时不显示此页面**，可防止每次登录系统时都显示*使用入门*页面。如果选择了该选项，系统将打开*系统摘要*页面，而不是*使用入门*页面。

HTTP/HTTPS

您可以单击**登录**以打开 HTTP 会话 （不安全），也可以单击**安全浏览 (HTTPS)** 打开 HTTP 会话 （安全）。系统会要求您使用默认的 RSA 密钥进行合法登录，然后将打开一个 HTTPS 会话。

有关如何配置 HTTPS 的信息，请参阅 **SSL 服务器验证设置**。

密码过期

此时将显示*新密码*页面：

- 首次使用默认用户名 **cisco** 和密码 **cisco** 访问交换机时，此页面会强制您替换出厂默认密码。
- 当密码过期时，此页面会强制您选择新密码。

注销

默认情况下，如果应用程序在十分钟内无活动，将会注销。您可以按 “**一般管理信息和操作**”一章中的 “**定义闲置会话超时**”一节中所述更改此默认值。

注意 除非将当前配置复制到启动配置，否则重启交换机时，将会删除自上次保存文件以来所做的所有更改。在注销前请先将当前配置保存到启动配置，以便保留在该会话期间所做的一切更改。

保存应用程序链接左侧的闪烁的红色 X 图标，表明尚未将当前配置更改保存到启动配置文件。在**复制 / 保存配置**页面上单击**禁用保存图标闪烁**按钮，可禁止图标闪烁。

交换机自动发现一台设备 （例如 IP 电话，请参阅**第 10 章，“什么是智能端口”**）时，会为该设备相应地配置端口。这些配置命令将写入当前配置文件中。这将导致您在登录时即使没有更改任何配置，“保存”图标也会开始闪烁。

单击**保存**时，将显示*复制 / 保存配置*页面。通过将当前配置文件复制到启动配置文件来保存该文件。保存后，将不再显示红色 X 图标和 “保存”应用程序链接。

要注销，只需单击任意页面右上角的**退出**。系统便会注销交换机。

如果发生超时，或者您主动注销系统，系统会显示一则消息并打开*登录*页面，同时弹出一则消息，说明应用程序处于已注销状态。登录后，应用程序会返回到初始页面。

初始页面的内容取决于是否在*使用入门*页面中选择 “启动时不显示此页面”选项。如果未选择该选项，则初始页面为*使用入门*页面。如果选择了该选项，则初始页面为*系统摘要*页面。

交换机配置快速入门

为通过快速导航简化交换机配置，*使用入门*页面提供了最常用页面的链接。

“使用入门”页面上的链接

类别	链接名称 （在页面上）	链接的页面
	更改管理应用和服务	*TCP/UDP 服务*页面
	更改设备 IP 地址	*IPv4 接口*页面
	创建 VLAN	*创建 VLAN*页面
	配置端口设置	*端口设置*页面
设备状态	系统摘要	*系统摘要*页面
	端口统计信息	*接口*页面
	RMON 统计信息	*统计信息*页面
	查看日志	*RAM*页面
快速访问	更改设备密码	*用户帐户*页面
	升级设备软件	*升级 / 备份固件 / 语言*页面
	备份设备配置	*下载 / 备份配置 / 日志*页面
	配置 QoS	*QoS 属性*页面
	配置端口镜像	*端口和 VLAN 镜像*页面

在 “使用入门”页面上有两个热链接，可将您带入思科 Web 页面了解详情。单击**支持**链接，您将可以访问交换机产品支持页面，而单击**论坛**链接，您将可以访问 “思科精睿支持社区”页面。

接口命名约定

在 GUI 内，可结合以下元素表示接口：

- **接口类型**：以下类型的接口在各种类型的设备上均有提供：
  - **快速以太网 （10/100 位）** - 这种类型的接口显示为 **FE**。
  - **千兆以太网端口 （10/100/1000 位）** - 这种类型的接口显示为 **GE**。
  - **LAG （端口通道）** - 这种类型的接口显示为 **LAG**。
  - **VLAN** - 这种类型的接口显示为 **VLAN**。
  - **隧道** - 这种类型的接口显示为 **隧道**。
- **接口编号**：**端口、 LAG、隧道或 VLAN ID**

窗口导航

本节介绍了基于 Web 的交换机配置实用程序的功能。

应用报头

应用报头显示在每个页面上。可以提供以下应用程序链接：

应用程序链接

应用程序链接名称	说明
	显示在**保存**应用程序链接左侧的闪烁的红色 X 图标表明对当前配置进行了更改，但尚未将更改保存到启动配置文件。您可以在 “复制 / 保存配置”页面上禁止红色 X 闪烁。 单击**保存**显示*复制 / 保存配置*页面。在交换机上，通过将当前配置文件复制到启动配置文件来保存该文件。保存后，将不再显示红色 X 图标和 “保存”应用程序链接。交换机重启时，会将启动配置文件类型复制到当前配置，并根据当前配置中的数据设置交换机参数。
用户名	显示登录到交换机的用户名。默认的用户名为 **cisco**。（默认密码是 **cisco**。）

应用程序链接 （续）

应用程序链接名称	说明
语言菜单	此菜单提供了以下选项： ▪ **选择语言**：从菜单所显示的语言中选择一种语言。此语言将作为基于 Web 的配置实用程序的语言。 ▪ **下载语言**：将一种新语言添加到交换机。 ▪ **删除语言**：删除交换机上的第二种语言。第一种语言（英文）无法删除。 ▪ **调试**：用来进行转换。如果选择此选项，所有基于 Web 的配置实用程序标签将消失，其原来的位置上将显示与语言文件中的 ID 对应的字符串 ID。 注 要升级语言文件，请使用*升级 / 备份固件 / 语言*页面。
退出	单击该按钮可注销基于 Web 的交换机配置实用程序。
关于	单击该链接会显示交换机名称和交换机版本号。
帮助	单击该按钮会显示在线帮助。
	如果记录了严重性级别高于*严重*的系统日志消息，则会显示“系统日志警报状态”图标。单击该图标将打开 *RAM 内存*页面。访问该页面后，将不会再显示 “系统日志警报状态”图标。要在没有活动的系统日志消息的情况下显示该页面，请单击**状态和统计信息** > **查看日志** > **RAM**。

管理按钮

下表介绍了系统中各页面上显示的常用按钮。

管理按钮

按钮名称	说明
	使用此下拉菜单可配置每个页面的条目数。
	表示必填字段。
添加	单击该按钮会显示相关的*添加*页面并在表格中添加一个条目。输入信息并单击**应用**，可将该更改保存到当前配置中。单击**关闭**可返回主页面。单击**保存**会显示*复制 / 保存配置*页面，并在交换机上将当前配置保存到启动配置文件类型。
应用	单击该按钮会将更改应用到交换机上的当前配置。除非将当前配置保存到启动配置文件类型或其他文件类型，否则当交换机重启时，当前配置会丢失。单击**保存**会显示*复制 / 保存配置*页面，并在交换机上将当前配置保存到启动配置文件类型。
取消	单击该按钮会重置对页面所做的更改。
清除所有接口的计数器	单击该按钮会将所有接口的统计计数器清零。
清除接口计数器	单击该按钮会将所选接口的统计计数器清零。
清除日志	清除日志文件。
清除表	清除表格条目。
关闭	返回主页面。如果所有更改均未应用到当前配置，将显示一条消息。
复制设置	表格通常包含一个或多个包含配置设置的条目。无需单独修改每个条目，而是可以先修改一个条目，然后再将所选条目复制到多个条目，方法如下： 1. 选择要复制的条目。单击**复制设置**以显示弹出式窗口。 2. 在**至**字段中输入目的条目编号。 3. 单击**应用**保存更改，然后单击**关闭**返回主页面。

管理按钮 （续）

按钮名称	说明
删除	在表中选中一个条目后，单击**删除**以删除该条目。
详情	单击该按钮可显示所选条目的相关详情。
编辑	选择条目，然后单击**编辑**。此时将打开*编辑*页面，并且可以对条目进行修改。 1. 单击**应用**可将更改保存到当前配置中。 2. 单击**关闭**可返回主页面。
转至	输入查询过滤条件并单击 **转至**。查询结果便会显示在页面上。
测试	单击**测试**可执行相关测试。

2

查看统计信息

本节介绍如何查看交换机统计信息。

其中包含以下主题：

- **查看以太网接口**
- **查看 Etherlike 统计信息**
- **查看 802.1X EAP 统计信息**
- **管理 RMON**

查看以太网接口

*接口*页面会显示每个端口的流量统计信息。该信息的刷新速率是可以选择的。

该页面对于分析发送和接收的流量数量及其传播方式 （单播、组播和广播）非常有用。

显示以太网统计信息和 / 或设置刷新率的步骤：

步骤 1 单击**状态和统计信息** > **接口**。此时将显示*接口*页面。

步骤 2 输入参数。

- **接口** - 选择接口类型以及要显示其以太网统计信息的具体接口。
- **刷新速率** - 选择刷新接口以太网统计信息的间隔时间。可用选项有：
  - *无刷新* - 不刷新统计信息。
  - *15 秒* - 每隔 15 秒刷新统计信息。
  - *30 秒* - 每隔 30 秒刷新统计信息。
  - *60 秒* - 每隔 60 秒刷新统计信息。

接收统计信息区域显示关于传入数据包的信息。

- **字节总数 (八位字节)** - 接收的八位字节数，包括坏数据包和 FCS 八位字节数，但不包括帧位。
- **单播数据包数** - 接收到的正常单播数据包数。
- **组播数据包数** - 接收到的正常组播数据包数。
- **广播数据包数** - 接收到的正常广播数据包数。
- **带有错误的数据包数** - 接收到的有错误的数据包数。

传输数据统计区域显示关于传出数据包的信息。

- **字节总数 (八位字节)** - 传输的八位字节数，包括坏数据包和 FCS 八位字节数，但不包括帧位。
- **单播数据包数** - 传输的正常单播数据包数。
- **组播数据包数** - 传输的正常组播数据包数。
- **广播数据包数** - 传输的正常广播数据包数。

清除统计信息计数器的步骤：

- 单击**清除接口计数器**清除显示的接口的计数器。
- 单击**清除所有接口计数器**清除所有接口的计数器。

查看 Etherlike 统计信息

Etherlike 页面根据 Etherlike MIB 标准定义显示每个端口的统计信息。该信息的刷新速率是可以选择的。该页面提供关于物理层 （第 1 层）中错误 （可能中断流量）的更为详细的信息。

查看 Etherlike 统计信息和 / 或设置刷新速率的步骤：

步骤 1 单击**状态和统计信息** > **Etherlike**。此时将显示 *Etherlike* 页面。

步骤 2 输入参数。

- **接口** - 选择接口类型以及要显示其以太网统计信息的具体接口。
- **刷新速率** - 选择刷新 Etherlike 统计信息的间隔时间。

将针对选定接口显示以下字段。

- **帧校验序列 (FCS) 错误数** - 接收到的未能通过 CRC （循环冗余校验）的帧。
- **信号冲突帧数** - 出现单个冲突，但成功传输的帧。
- **滞后冲突** - 在数据的前 512 位后检测到的冲突。
- **过量冲突** - 由于过量冲突而被拒绝的传输数。
- **过大数据包数** - 接收到的大于 2000 八位字节的数据包数。
- **内部 MAC 接收错误** - 由于接收器错误而被拒绝的帧数。
- **已接收的暂停帧数** - 接收到的流控制暂停帧数。
- **已发送的暂停帧数** - 从选定接口传输的流控制暂停帧数。

清除统计信息计数器的步骤：

- 单击**清除接口计数器**清除选定接口的计数器。
- 单击**清除所有接口计数器**清除所有接口的计数器。

查看 802.1X EAP 统计信息

802.1x EAP 页面会显示关于发送或接收的 EAP （扩展认证协议）帧的详细信息。要配置 802.1X 功能，请参阅 *802.1X 属性*页面。

查看 EAP 统计信息和 / 或设置刷新速率的步骤：

步骤 1 单击**状态和统计信息** > **802.1x EAP**。此时将显示 *802.1x EAP* 页面。

步骤 2 选择需要轮询统计信息的**接口**。

步骤 3 选择刷新 EAP 统计信息的间隔时间 （**刷新速率**）。

将针对选定接口显示以下值。

- **已接收的 EAPOL 帧数** - 在该端口上接收的有效 EAPOL 帧数。
- **已发送的 EAPOL 帧数** - 在该端口上传输的有效 EAPOL 帧数。
- **已接收的 EAPOL 开始帧数** - 在该端口上接收的 EAPOL 开始帧数。
- **已接收的 EAPOL 注销帧数** - 在该端口上接收的 EAPOL 注销帧数。

- **已接收的 EAP 响应 /ID 帧数** - 在该端口上接收的 EAP Resp/ID 帧数。
- **已接收的 EAP 响应帧数** - 端口接收的 EAP 响应帧数 （除 Resp/ID 帧外）。
- **已发送的 EAP 请求 /ID 帧数** - 在该端口上传输的 EAP Req/ID 帧数。
- **已发送的 EAP 请求帧数** - 该端口传输的 EAP 请求帧数。
- **已接收的无效 EAPOL 帧数** - 在该端口接收的不可识别的 EAPOL 帧数。
- **已接收的 EAP 长度错误帧数** - 此端口上接收的具有无效数据包正文长度的 EAPOL 帧数。
- **最新 EAPOL 帧版本** - 最新收到的 EAPOL 帧上附加的协议版本号。
- **最新 EAPOL 帧源** - 最新收到的 EAPOL 帧上附加的源 MAC 地址。

清除统计信息计数器的步骤：

- 单击**清除接口计数器**清除选定接口的计数器。
- 单击**清除所有接口计数器**清除所有接口的计数器。

管理 RMON

RMON （远程网络监控）使交换机能够在指定时间段内前瞻性地监控流量统计信息。通过此功能，您可以查看当前的统计信息 （因为计数器值已清除）。

查看 RMON 统计信息

*统计信息*页面显示关于数据包大小的详细信息和关于物理层错误的信息。显示的信息基于 RMON 标准。过大的数据包定义为满足以下条件的以太网帧：

- 数据包长度大于 MRU 字节大小。
- 尚未检测冲突事件。
- 尚未检测延时冲突事件。
- 尚未检测 Rx 错误事件。
- 数据包具有有效的 CRC。

查看 RMON 统计信息和 / 或设置刷新速率的步骤：

步骤 1 单击**状态和统计信息 > RMON > 统计信息**。此时将显示*统计信息*页面。

步骤 2 选择要显示以太网统计信息的**接口**。

步骤 3 选择**刷新速率**，即刷新接口统计信息的间隔时间。

将针对选定接口显示以下统计信息。

- **已接收的字节数** - 接收的八位字节数，包括坏数据包和 FCS 八位字节数，但不包括帧位。
- **丢弃事件** - 丢弃的数据包数。
- **已接收的数据包** - 接收的好数据包数，包括组播数据包和广播数据包。
- **已接收的广播数据包数** - 接收到的正常广播数据包数。该数量不包括组播数据包。
- **已接收的组播数据包数** - 接收到的正常组播数据包数。
- **CRC 和 Align 错误数** - 发生的 CRC 和 Align 错误数。
- **过小数据包数** - 接收的大小不足 （小于 64 八位字节）的数据包数。
- **过大数据包数** - 接收的大小过大 （大于 2000 八位字节）的数据包数。
- **分片** - 接收的片段 （小于 64 八位字节的数据包，不包括帧位，但包括 FCS 八位字节）数。
- **超时发送帧数** - 接收的大于 1632 八位字节的数据包总数。该数量不包括帧位，但包括具有整数数量八位字节 （FCS 错误）的坏 FCS （帧校验序列）或具有非整数八位字节 （校正误差）的坏 FCS 的 FCS 八位字节数。超时发送帧数据包定义为满足以下条件的以太网帧：
  - 数据包数据长度大于 MRU。
  - 数据包具有无效的 CRC。
  - 尚未检测 Rx 错误事件。
- **冲突数** - 接收的冲突数。如果启用了巨型帧，超时发送帧的阈值将提升为巨型帧的最大大小。
- **64 字节的帧数** - 接收的包含 64 字节的帧数。
- **65 至 127 字节的帧数** - 接收的包含 65-127 字节的帧数。
- **128 至 255 字节的帧数** - 接收的包含 128-255 字节的帧数。

- **256 至 511 字节的帧数** - 接收的包含 256-511 字节的帧数。
- **512 至 1023 字节的帧数** - 接收的包含 512-1023 字节的帧数。
- **超过 1024 字节的帧数** - 接收的包含 1024-2000 字节的帧和巨型帧的数量。

清除统计信息计数器的步骤：

- 单击**清除接口计数器**清除选定接口的计数器。
- 单击**清除所有接口计数器**清除所有接口的计数器。

3

管理系统日志

本节介绍系统日志功能，使用此功能，交换机可以生成若干独立的日志。每个日志是一组描述系统事件的消息。

交换机可生成以下本地日志：

- 将日志发送至 Console 接口。
- 写入到 RAM 中的记录事件循环列表中的日志，重启交换机会将其擦除。
- 写入到保存至闪存的循环日志文件的日志，重启不会将其擦除。

此外，还可以通过系统日志消息的形式将消息发送到远程系统日志服务器上。

本节包含以下小节：

- **设置系统日志设置**
- **设置远程记录设置**
- **查看内存日志**

设置系统日志设置

在*日志设置*页面*上*，您可以启用或禁用记录，及选择是否汇总日志消息。

可以按严重性级别选择事件。系统以在严重性级别首字母两侧加上破折号 (-) 的方式标记每则日志消息的严重性级别 （*紧急*除外，其以字母 F 表示）。例如，日志消息 "%INIT-I-InitCompleted:… " 的严重性级别为 **I**，表示*报告*。

下面按照从高到低的顺序列出了事件的严重性级别：

- *紧急* - 系统无法使用。
- *警报* - 需要采取措施。
- *严重* - 系统处于高危状态。
- *错误* - 系统出错。

- *警告* - 系统已发出警告。
- *注意* - 系统能够正常工作，但系统已发出通知。
- *报告* - 设备信息。
- *调试* - 提供关于事件的详情。

可以为 RAM 日志和闪存日志选择不同的严重性级别。这些日志将分别在 *RAM 内存*页面和*闪存*页面中显示。

选择要存储在日志中的严重性级别后，此级别以上的所有事件都会自动存储在日志中。而此级别以下的事件则不会存储在日志中。

例如，如果选择了**警告**，则会将严重性级别为**警告**及更高 （即严重性级别为 “紧急”、“警报”、“严重”、“错误”和 “警告”）的所有事件存储在日志中。但是不会存储严重性级别低于**警告** （即严重性级别为 “注意”、“报告”和 “调试”）的事件。

设置全局日志参数的步骤：

步骤 1 单击**管理** > **系统日志** > **日志设置**。将打开 *日志设置*页面。

步骤 2 输入参数。

- **记录** - 选择该选项将启用消息记录。
- **系统日志聚合** - 选择该选项可启用系统日志消息和 Trap 汇总。如果启用了该选项，将会汇总最大聚合时间内的相同和相邻的系统日志消息及 Trap，并会通过一则消息将汇总后的结果发出。将按照消息的到达顺序发送汇总后的消息。每则消息都会注明已汇总的次数。
- **最大聚合时间** - 输入汇总系统日志消息的时间间隔。
- **RAM 内存记录** - 选择要记录到 RAM 中的消息的严重性级别。
- **闪存记录** - 选择要记录到闪存中的消息的严重性级别。

步骤 3 单击**应用**。将更新当前配置文件。

设置远程记录设置

使用*远程日志服务器*页面可定义向其发送日志消息 （使用系统日志协议）的远程系统日志服务器。可以为每个服务器配置其所接收消息的严重性级别。

定义系统日志服务器的步骤：

步骤 1 单击**管理** > **系统日志** > **远程日志服务器**。将打开*远程日志服务器*页面。

该页面会显示远程日志服务器的列表。

步骤 2 单击**添加**。将打开*添加远程日志服务器*页面。

步骤 3 输入参数。

- **服务器定义** - 选择是按照 IP 地址还是名称来识别远程日志服务器。
- **IP 版本** - 选择支持的 IP 格式。
- **IPv6 地址类型** - 选择 IPv6 地址类型 （如果使用 IPv6）。选项如下：
  - *链路本地* - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
  - *全局* - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。
- **链路本地接口** - 从列表中选择链路本地接口 （如果选择的 IPv6 地址类型为“链路本地”）。
- **日志服务器 IP 地址 / 名称** - 输入日志服务器的 IP 地址或域名。
- **UDP 端口** - 输入要向其发送日志消息的 UDP 端口。
- **设备** - 选择从其将系统日志发送给远程服务器的设备值。只能为服务器指定一个设备值。如果指定第二个设备代码，其将覆盖第一个设备值。
- **说明** - 输入服务器说明。
- **最低严重程度** - 选择要发送到服务器的系统日志消息的最低严重性级别。

步骤 4 单击**应用**，将会关闭*添加远程日志服务器*页面，添加系统日志服务器，并更新当前配置文件。

查看内存日志

交换机可以写入以下日志：

- RAM 中的日志 （在重启过程中被清除）。
- 闪存中的日志 （只能由用户使用指令来清除）。

您可以按严重性配置写入到每个日志的消息，而一则消息可以被写入到多个日志，包括存放在外部系统日志服务器上的日志。

RAM 内存

*RAM 内存*页面会按时间先后顺序显示保存到 RAM （缓存）中的所有消息。系统会根据 *日志设置*页面中的配置将这些条目存储到 RAM 日志中。

要查看日志条目，请单击**状态和统计信息** > **查看日志** > **RAM 内存**。将打开 *RAM 内存*页面。

页面顶部有一个按钮，您可以使用该按钮禁用警报图标闪烁。单击该按钮可在禁用和启用间进行切换。

此页面显示以下字段：

- **日志索引** - 日志条目编号。
- **日志时间** - 消息生成的时间。
- **严重程度** - 事件严重性。
- **说明** - 描述事件的消息文本。

若要清除日志消息，请单击**清除日志**。消息即被清除。

闪存

*闪存*页面会按时间先后顺序显示存储在闪存中的消息。所记录事件的最低严重性级别在*日志设置*页面中配置。交换机重启时，闪存日志会保留在闪存中。您可以手动清除这些日志。

要查看闪存日志，请单击**状态和统计信息** > **查看日志** > **闪存**。将打开*闪存*页面。

此页面显示以下字段：

- **日志索引** - 日志条目编号。
- **日志时间** - 消息生成的时间。
- **严重程度** - 事件严重性。
- **说明** - 描述事件的消息文本。

若要清除消息，请单击**清除日志**。消息即被清除。

4

管理系统文件

本节介绍系统文件的管理方式。

其中包括以下主题：

- **系统文件类型**
- **升级 / 备份固件 / 语言**
- **下载或备份配置或日志**
- **查看配置文件属性**
- **复制配置文件**
- **DHCP 自动配置**

系统文件类型

系统文件是指包含配置信息、固件映像或引导代码的文件。

通过这些文件可进行各种操作，例如：选择用于交换机引导的固件文件，在交换机内部复制不同类型的配置文件，或在交换机和外部设备 （例如外部服务器）之间复制文件。

可用的文件传输方法有以下几种：

- 内部复制。
- 使用浏览器提供的工具的 HTTP/HTTPS。
- TFTP 客户端 （需要 TFTP 服务器）。

交换机上的配置文件由其*类型*定义，文件中包含设备的设置和参数值。

在交换机上参考配置时，会依据其*配置文件类型 （例如：启动配置或当前配置）*而非可由用户修改的文件名进行参考。

可以将内容从一种配置文件类型复制到另一种配置文件类型，但用户无法更改文件类型名称。

设备上的其他文件包括固件、引导代码和日志文件，这些文件称为*工作文件*。

配置文件是文本文件，将其复制到外部设备 （例如 PC）后，可在文本编辑器 （例如记事本）中对其进行编辑。

文件和文件类型

在交换机上可以找到以下类型的配置和工作文件：

- **当前配置** - 包含当前交换机工作所使用的参数。当您在设备上更改参数值时只会修改这种类型的文件。

  如果重启交换机，当前配置将会丢失。存储在闪存中的启动配置将覆盖存储在 RAM 中的当前配置。

  要保留对交换机所做的任何更改，您必须将当前配置保存到启动配置或其他文件类型。

- **启动配置** - 通过将其他配置 （通常为当前配置）复制到启动配置而保存的参数值。

  启动配置保留在闪存中，并且在交换机重启后会保留。这时，系统会将启动配置复制到 RAM 中并将其标识为当前配置。

- **镜像配置** - 在下述情况下，由交换机创建的启动配置副本：

  - 交换机已连续工作 24 小时。
  - 在过去的 24 小时内没有对当前配置进行任何配置更改。
  - 启动配置与当前配置一致。

  只有系统能够将启动配置复制到镜像配置。但是，可以将镜像配置复制到其他文件类型或其他设备。

  可在*配置文件属性*页面禁用自动将当前配置复制到镜像配置的选项。

- **备份配置** - 用于系统关机保护或特定工作状态维护的配置文件手动副本。可以将镜像配置、启动配置或当前配置复制到备份配置文件。备份配置存放在闪存中，并且当设备重启时会保留。

- **固件** - 可控制交换机的操作和功能的程序。更多时候被称为*映像*。

- **Boot 代码** - 控制基本系统启动及启动固件映像。

- **语言文件** - 能够使基于 Web 的配置实用程序窗口以选定语言显示的字典。

- **闪存日志** - 存储在闪存中的系统日志消息。

文件操作

可以执行以下操作来管理固件和配置文件：

- 按**升级 / 备份固件 / 语言**一节中所述升级固件或引导代码，或者更换第二语言。
- 按**下载或备份配置或日志**一节中所述将交换机上的配置文件保存到其他设备上的位置。
- 按**查看配置文件属性**一节中所述清除启动配置或备份配置文件类型。
- 按**复制配置文件**一节中所述将一种配置文件类型复制到另一种配置文件类型。
- 按 **DHCP 自动配置**一节中所述启用将配置文件从 DHCP 服务器自动上传到交换机的功能。

本节包含以下主题：

升级 / 备份固件 / 语言

升级 / 备份固件 / 语言流程可用于：

- 升级或备份固件映像。
- 升级或备份引导代码。
- 导入或升级第二语言文件。

支持以下文件传输方法：

- 使用浏览器提供的工具的 HTTP/HTTPS
- TFTP （需要 TFTP 服务器）

如果将新语言文件加载到了交换机上，便可以从下拉菜单中选择这种新语言。（无需重启交换机）。

交换机上将存储一个单独的固件映像。将新固件成功载入到交换机之后，在此新固件生效之前需要重启设备。*摘要*页面在重启之前将继续显示上一映像。

升级 / 备份固件或语言文件

升级或备份软件映像或语言文件的步骤：

步骤 1 单击**管理** > **文件管理** > **升级 / 备份固件 / 语言**。将打开*升级／备份固件／语言*页面。

步骤 2 单击 “传输方法”。按以下步骤进行：

- 如果选择了 **TFTP**，则转至**步骤 3**。
- 如果选择了**通过 HTTP/HTTPS**，则转至**步骤 4**。

步骤 3 如果选择了**通过 TFTP**，请按本步骤中所述输入参数。否则，请跳至**步骤 4**。

请选择以下其中一种操作：

- **升级保存操作** - 指定将使用 TFTP 服务器上新版本的文件类型替换交换机上的该文件类型。
- **备份保存操作** - 指定将文件类型副本保存至另一台设备上的文件。

输入以下字段：

- **文件类型** - 选择目的文件类型。只会显示有效的文件类型。（这些文件类型在**文件和文件类型**一节中做了说明）。
- **TFTP 服务器定义** - 选择是按照 IP 地址还是域名来指定 TFTP 服务器。
- **IP 版本** - 选择使用 IPv4 还是 IPv6 地址。
- **IPv6 地址类型** - 选择 IPv6 地址类型 （如果使用 IPv6）。选项如下：
  - **链路本地** - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 FE80，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
  - **全局** - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。
- **链路本地接口** - 从列表中选择链路本地接口 （如果使用 IPv6）。
- **TFTP 服务器 IP 地址 / 名称** - 输入 TFTP 服务器的 IP 地址或域名。
- **（用于升级）源文件名** - 输入源文件的名称。
- **（用于备份）目的** - 输入备份文件的名称。

步骤 4 如果选择了**通过 HTTP/HTTPS**，则只能进行**升级**。按照本步骤中所述输入参数。

- **文件类型** - 选择配置文件类型。只能选择有效的文件类型。（这些文件类型在**文件和文件类型**一节中做了说明）。可升级以下文件类型：
  - *固件映像* - 选择它可升级固件映像。
  - *语言* - 选择它可升级语言文件。
- **文件名** - 单击**浏览**选择文件或输入要在传输中使用的路径和源文件名。

步骤 5 单击**应用**或**完成**。将升级或备份该文件。

下载或备份配置或日志

通过 *下载 / 备份配置 / 日志*页面，可实现以下操作：

- 将配置文件或日志从交换机备份到外部设备中。
- 将配置文件从外部设备还原到交换机中。

注

将配置文件还原至当前配置时，导入的文件会*添加*旧文件中不存在的任何配置命令，并*覆盖*现有配置命令中的所有参数值。

将配置文件还原至启动配置或备份配置文件时，新文件会*替换*旧文件。

还原至启动配置时，必须重启交换机，才能将还原的启动配置作为当前配置使用。可以使用**重启交换机**一节中介绍的流程重启交换机。

备份或还原系统配置文件的步骤：

步骤 1 单击**管理** > **文件管理** > **下载 / 备份配置 / 日志**。将打开 *下载 / 备份配置 / 日志*页面。

步骤 2 选择**传输方法**。

步骤 3 如果选择了**通过 TFTP**，请输入参数。否则，请跳至**步骤 4**。

选择下载或备份**保存操作**。

下载保存操作 - 指定将使用其他设备上的文件替换交换机上的文件类型。输入以下字段：

a. **服务器定义** - 选择是按照 IP 地址还是域名来指定 TFTP 服务器。

b. **IP 版本** - 选择使用 IPv4 还是 IPv6 地址。

> **注** 如果在 “服务器定义”中按照名称选择了服务器，则无需选择与 IP 版本相关的选项。

c. **IPv6 地址类型** - 选择 IPv6 地址类型 （如果使用 IPv6）。选项如下：

- *链路本地* - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
- *全局* - IPv6 地址为全局单播 IPv6 类型，可从其他网络查看和访问。

d. **链路本地接口** - 从列表中选择链路本地接口。

e. **TFTP 服务器** - 输入 TFTP 服务器的 IP 地址。

f. **源文件名** - 输入源文件名。文件名不能包含斜线 （\ 或 /），不能以句点 (.) 开头，且包含的字符数必须在 1 到 160 之间。（有效字符为：A-Z、 a-z、 0-9、 "."、 "-"、 "_"）。

g. **目的文件类型** - 输入目的配置文件类型。只会显示有效的文件类型。（这些文件类型在**文件和文件类型**一节中做了说明）。

备份保存操作 - 指定将将要复制的文件类型保存至另一台设备上的文件。输入以下字段：

a. **服务器定义** - 选择是按照 IP 地址还是域名来指定 TFTP 服务器。

b. **IP 版本** - 选择使用 IPv4 还是 IPv6 地址。

c. **IPv6 地址类型** - 选择 IPv6 地址类型 （如果使用 IPv6）。选项如下：

- *链路本地* - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
- *全局* - IPv6 地址为全局单播 IPv6 类型，可从其他网络查看和访问。

d. **链路本地接口** - 从列表中选择链路本地接口。

e. **TFTP 服务器 IP 地址 / 名称** - 输入 TFTP 服务器的 IP 地址或域名。

f. **源文件类型** - 输入源配置文件类型。只会显示有效的文件类型。（这些文件类型在**文件和文件类型**一节中做了说明）。

g. **敏感数据** - 选择应如何将敏感数据包含在备份文件中。可用的选项有：

- *排除* - 不将敏感数据包含在备份中。
- *加密* - 将敏感数据以加密的形式包含在备份中。
- *明文模式* - 将敏感数据以明文模式包含在备份中。

注 可用的敏感数据选项由当前用户的 SSD 规则决定。有关详情，请参阅**安全敏感数据管理 > SSD 规则**页面。

h. **目的文件名** - 输入目的文件名。文件名不能包含斜线 （\ 或 /）、文件名的首字母不能为句点 (.)，且文件名的字符数必须在 1 到 160 之间。（有效字符为：A-Z、 a-z、 0-9、 "."、 "-"、 "_"）。

i. 单击**应用**。将升级或备份该文件。

步骤 4 如果选择了**通过 HTTP/HTTPS**，请按本步骤中所述输入参数。

选择**保存操作**。

如果**保存操作**为 *下载* （用其他设备上的新版本替换交换机上的文件），请执行以下操作。否则，请执行本步骤中的下一个操作。

a. **源文件名** - 单击**浏览**选择文件或输入要在传输中使用的路径和源文件名。

b. **目的文件类型** - 选择配置文件类型。只会显示有效的文件类型。（这些文件类型在**文件和文件类型**一节中做了说明）。

c. 单击**应用**。将从其他设备将该文件传输到交换机上。

如果**保存操作**为 *备份* （将文件复制到其他设备中），请执行以下操作：

a. **源文件类型** - 选择配置文件类型。只会显示有效的文件类型。（这些文件类型在**文件和文件类型**一节中做了说明）。

b. **敏感数据** - 选择应如何将敏感数据包含在备份文件中。可用的选项有：

- *排除* - 不将敏感数据包含在备份中。
- *加密* - 将敏感数据以加密的形式包含在备份中。
- *明文模式* - 将敏感数据以明文模式包含在备份中。

注 可用的敏感数据选项由当前用户的 SSD 规则决定。有关详情，请参阅**安全敏感数据管理 > SSD 规则**页面。

c. 单击**应用**。将升级或备份该文件。

查看配置文件属性

通过*配置文件属性*可查看不同的系统配置文件的创建时间。通过它还可以删除启动配置和备份配置文件。您无法删除其他配置文件类型。

要对是否创建镜像配置文件进行设置，请清除配置文件并查看配置文件的创建时间：

步骤 1 单击**管理** > **文件管理** > **配置文件属性**。将打开*配置文件属性*页面。

步骤 2 如有必要，禁用**自动镜像配置**。这将禁止自动创建镜像配置文件。禁用该功能后，系统将删除镜像配置文件 （如有）。请参阅**系统文件类型**以了解镜像文件的说明以及可能需要自动创建镜像配置文件的原因。

步骤 3 如有必要，选择启动配置或备份配置或同时选中两者，然后单击**清除文件**以删除这些文件。

此页面提供了以下字段：

- **配置文件名称** - 显示文件类型。
- **创建时间** - 显示文件的修改日期和时间。

复制配置文件

在任意窗口上单击**应用**，*仅会*将交换机配置设置的更改存储在当前配置中。要保留当前配置中的参数，必须将当前配置复制到其他配置类型或保存到其他设备上。

注意 除非将当前配置复制到启动配置或其他配置文件，否则自上次复制文件后所做的所有更改将会在交换机重启后全部丢失。

允许以下内部文件类型复制组合：

- 从当前配置到启动配置或备份配置。
- 从启动配置到备份配置。
- 从备份配置到启动配置。
- 从镜像配置到启动配置或备份配置。

将一种类型的配置文件复制到另一种类型的配置文件的步骤：

步骤 1 单击**管理** > **文件管理** > **复制 / 保存配置**。将打开*复制 / 保存配置*页面。

步骤 2 选择要复制的**源文件名**。仅显示有效的文件类型 （这些文件类型在**文件和文件类型**一节中做了说明）。

步骤 3 选择将由源文件覆盖的**目的文件名**。

- 如果您正在备份某个配置文件，请为该备份文件选择以下一种格式。
  - **排除** - 敏感数据将不包含在备份文件中。
  - **加密** - 敏感数据将以加密的形式包含在备份文件中。
  - **明文模式** - 敏感数据将以纯文本形式包含在备份文件中。

  注 可用的敏感数据选项由当前用户的 SSD 规则决定。有关详情，请参阅**安全敏感数据管理 > SSD 规则**页面。

步骤 4 **保存图标闪烁**字段将表明在有未保存的数据时图标是否会闪烁。要禁用 / 启用该功能，可单击**禁用 / 启用保存图标闪烁**。

步骤 5 单击**应用**。文件将被复制。

DHCP 自动配置

交换机支持 DHCP 自动配置，这样便可以将配置信息 （包括 TFTP 服务器的 IP 地址和文件名）传递到 TCP/IP 网络上的主机。基于该协议，交换机便可通过自动配置功能从 TFTP 服务器上下载配置文件。

默认情况下，当启用自动配置功能后，便可将交换机作为 DHCP 客户端来使用。

触发 DHCP 自动配置

在以下情况下会触发自动配置过程：

- 重启后 （使用 DHCP）动态分配或续订 IP 地址时。
- 收到明确的 DHCP 续订请求且如果已为此配置了交换机和服务器。
- 自动续租 DHCP 后。

服务器名称 / 地址

可以指定 TFTP 服务器的 IP 地址或名称。如果在 DHCP 消息中未指定 IP 地址，则使用本服务器。该 DHCP 消息是指来自 DHCP 服务器的 DHCP Offer 消息。可能的选项为 BOOTP 选项 sname 和 siaddr 以及 DHCP 选项 150 或 66。这是个可选参数。

备份配置文件名

您可以指定备份配置文件名。如果 DHCP 消息中未指定文件名，则使用本文件。这是个可选参数。

自动配置过程

当触发自动配置过程后，会按顺序发生以下事件：

- 将访问 DHCP 服务器以获取 TFTP 服务器 IP 地址和配置文件名。这些参数会传递到 DHCP 选项参数中。
- 如果 DHCP 服务器未提供 IP 地址，则会使用备份服务器地址 （在用户已配置它的情况下）。
- 如果 DHCP 服务器未提供 IP 地址且备份 TFTP 服务器地址为空，则自动配置过程将停止。

  注 上述两点中的 IP 地址指的是 TFTP 服务器的 IP 地址或主机名。
- 如果 DHCP 服务器已提供配置文件名，则会按 **DHCP 自动配置**中所述选择复制协议 （TFTP）。
- 如果 DHCP 服务器未提供配置文件名，则将使用备份配置文件名。
- 如果 DHCP 服务器未提供配置文件名且备份配置文件名为空，则自动配置过程将停止。
- 系统将通过访问 TFTP 服务器下载文件。

  下载过程只有在新的配置文件名与当前的配置文件名不同时 （即使当前的配置文件为空）才能完成。
- 系统将生成系统日志消息，确认自动配置过程已完成。

配置 DHCP 自动配置

*DHCP 自动配置*页面用于在 DHCP 消息中未提供信息的情况下执行以下操作：

- 启用 DHCP 自动配置功能。
- 指定下载协议。
- 配置交换机以从特定服务器上的特定文件接收配置信息。

在 DHCP 自动配置过程中，请注意以下几点：

- 存放在 TFTP 服务器上的配置文件必须符合所支持配置文件的形式和格式要求。在将文件加载到启动配置之前，会检查文件的形式和格式，但不会检查配置参数的有效性。
- 为确保设备配置能实现预期的功能，以及鉴于要按照每一 DHCP 续订周期分配不同 IP 地址，我们建议将 IP 地址绑定到 DHCP 服务器表中的 MAC 地址。这样可确保每台设备都有自身保留的 IP 地址和其他相关信息。

配置 DHCP 服务器自动配置的步骤：

步骤 1 单击**管理** > **文件管理** > **DHCP 自动配置**。将打开 *DHCP 自动配置*页面。

步骤 2 输入值。

- **通过 DHCP 自动配置** - 选择该字段可启用 DHCP 自动配置。
- **备份服务器定义 - 按 IP 地址**或**按名称**选择可配置 TFTP 服务器。

步骤 3 如果 DHCP 自动配置未启用，或虽已启用但未从 DHCP 服务器上接收到任何配置文件，则可输入以下要使用的可选信息。

- **备份服务器 IP 地址 / 名称** - 输入当 DHCP 消息中未指定服务器 IP 地址时使用的服务器 IP 地址或名称。
- **备份配置文件名** - 输入当 DHCP 消息中未指定配置文件名时使用的文件路径和文件名。

该窗口会显示以下字段：

- **最近自动配置服务器 IP 地址** - 显示上次执行自动配置时所使用的 TFTP 服务器的 IP 地址。
- **最近自动配置文件名称** - 显示最近交换机在自动配置中所使用的文件名。

注 当交换机接收到 IP 地址后，会将**最近自动配置文件名**与从 DHCP 服务器接收到的信息进行对比。如果这些值不匹配，交换机会将 DHCP 服务器已标识的服务器上的配置文件传输到启动配置文件，然后进行重启。如果这些值匹配，则不执行任何操作。

步骤 4 单击**应用**。 DHCP 自动配置功能将在当前配置中得到更新。

5

一般管理信息

本节介绍如何在交换机上查看系统信息和配置各种选项。

具体包括以下主题：

- **交换机型号**
- **系统信息**
- **重启交换机**
- **监控风扇状态和温度**
- **定义空闲会话超时**
- **Ping 主机**

交换机型号

所有型号均可通过基于 Web 的交换机配置实用程序进行全面管理。

在第 2 层系统模式下，交换机会作为一个可识别 VLAN 的桥接器来转发数据包。在第 3 层系统模式下，交换机会执行 IPv4 路由和可识别 VLAN 的桥接。

注 将使用以下端口约定：

- GE 用于表示千兆以太网 (10/100/1000) 端口。
- FE 用于表示快速以太网 (10/100) 端口。

下表介绍了不同型号、其中所包含的端口数量和类型及其以太网供电 (PoE) 信息。

智能型交换机型号

型号名称	产品 ID (PID)	设备上的端口说明	PoE 功率	支持 PoE 的端口数
SG200-18	SLM2016T	16 个 GE 端口 + 2 个 GE 特殊用途组合端口		
SG200-26	SLM2024T	24 个 GE 端口 + 2 个 GE 特殊用途组合端口		
SG200-26P	SLM2024PT	24 个 GE 端口 + 2 个 GE 特殊用途组合端口	100W	12 个端口 FE1-FE6， FE13 - FE18
SG200-50	SLM2048T	48 个 GE 端口 + 2 个 GE 特殊用途组合端口		
SG200-50P	SLM2048PT	48 个 GE 端口 + 2 个 GE 特殊用途组合端口	180W	24 个端口 FE1-FE12， FE25 - FE36
SF200-24	SLM224GT	24 个 FE 端口 + 2 个 GE 特殊用途组合端口		
SF200-24P	SLM224PT	24 个 FE 端口 + 2 个 GE 特殊用途组合端口	100W	12 个端口 FE1-FE6， FE13 - FE18
SF200-48	SLM248GT	48 个 FE 端口 + 2 个 GE 特殊用途组合端口		
SF200-48P	SLM248PT	FE1-FE48， GE1-GE4。 48 个 FE 端口 + 2 个 GE 特殊用途组合端口	180W	24 个端口 FE1-FE12， FE25 - FE36

系统信息

*系统摘要*页面提供了交换机的图形视图，并显示交换机状态、硬件信息、固件版本信息、一般 PoE 状态以及其他项目。

显示系统摘要

若要查看系统信息，请单击**状态和统计信息** > **系统摘要**。此时将打开*系统摘要*页面。

*系统摘要*页面显示系统和硬件信息。

系统信息：

- **系统说明** - 系统的说明。
- **系统位置** - 交换机的实际位置。单击**编辑**可前往*系统设置*页面输入此信息。
- **系统联系人** - 联系人的姓名。单击**编辑**可前往*系统设置*页面输入此信息。
- **主机名** - 交换机的名称。单击**编辑**可前往*系统设置*页面输入此信息。默认情况下，交换机主机名由单词 *switch* 与交换机 MAC 地址的三个最低有效位（最右侧的六个十六进制数字）组合而成。
- **系统运行时间** - 自上次重启以来所运行的时间。
- **当前时间** - 当前系统时间。
- **基本 MAC 地址** - 交换机 MAC 地址。
- **巨型帧** - 巨型帧支持状态。可以使用“端口管理”菜单的*端口设置*页面启用或禁用此支持。

  注 巨型帧支持仅在已将其启用且重启交换机之后才会生效。

TCP/UDP 服务状态：

- **HTTP 服务** - 显示 HTTP 服务是处于启用状态还是禁用状态。
- **HTTPS 服务** - 显示 HTTPS 服务是处于启用状态还是禁用状态。
- **型号说明** - 交换机型号说明。
- **序列号** - 序列号。
- **PID VID** - 部件编号和版本 ID。

主单元的 PoE 电源信息：

- **最大可用 PoE 功率 (W)** - PoE 可提供的最大可用功率。
- **总 PoE 功率 (W)** - 为连接的 PoE 设备提供的总 PoE 功率。
- **PoE 供电模式** - 端口限制或类别限制。

配置系统设置

输入系统设置的步骤：

步骤 1 单击**管理** > **系统设置**。此时将打开*系统设置*页面。

步骤 2 查看或修改系统设置。

- **系统说明** - 显示交换机说明。
- **系统位置** - 输入交换机实际所在的位置。
- **系统联系人** - 输入联系人姓名。
- **主机名** - 选择此交换机的主机名。在 CLI 命令的提示符中会使用此主机名：
  - *使用默认设置* - 这些交换机的默认主机名 （系统名称）为：*switch123456*，其中 123456 代表交换机 MAC 地址的最后三个字节 （以十六进制格式表示）。
  - *用户定义* - 输入主机名。只能使用字母、数字和连字符。主机名不能以连字符开头或结尾。其他符号、标点符号字符或空格均不允许使用 （如 RFC1033、 1034、 1035 中规定）。
- **自定义登录屏幕设置** - 要在*登录*页面上显示文本，请在**登录横幅**文本框中输入该文本。单击**预览**查看结果。

  注 当您通过基于 Web 的配置实用程序定义登录横幅时，也会为 CLI 接口（Console、 Telnet 和 SSH）激活该横幅。

步骤 3 单击**应用**，在当前配置文件中设置这些值。

重启交换机

某些配置更改 （例如启用巨帧支持）需要重启系统才能生效。但是，重启交换机会删除当前配置，因此在重启交换机之前先将当前配置保存到启动配置至关重要。单击**应用**不会将配置保存到启动配置。有关文件和文件类型的详情，请参阅**管理系统文件**一节中的**文件和文件类型**部分。

可以使用*管理 > 文件管理 > 保存 / 复制配置*或单击窗口顶部的**保存**来备份配置。也可以从远程设备上传配置。请参阅**管理系统文件**一节中的**下载或备份配置或日志**部分。

重启交换机的步骤：

步骤 1 单击**管理** > **重启**。将打开*重启*页面。

步骤 2 单击任何一个**重启**按钮来重启交换机。

- **清除启动配置文件** - 选中此项可在下次启动交换机时清除其中的配置。
- **重启** - 您可在该窗口中重启交换机。由于当前配置中任何未保存的信息在交换机重启后都会被丢弃，因此必须单击任何窗口右上角的**保存**，以便重启后仍保留当前配置。如果未显示 “保存” 选项，则表示当前配置与启动配置相同，不需要执行任何操作。
- **使用出厂默认设置重启** - 使用出厂默认配置重启交换机。此过程会擦除启动配置文件和备份配置文件。选择此操作后，任何未保存到其他文件的设置都会被清除。恢复出厂默认设置时，不会删除镜像配置文件。

  注 清除启动配置文件并重启，不同于使用出厂默认设置重启。使用出厂默认设置重启更具侵入性。

监控风扇状态和温度

*状况*页面会显示配备风扇的所有设备上的交换机风扇状态和温度。

要查看交换机状况参数，请单击**状态和统计信息** > **状况**。将打开*状况*页面。

*状况*页面将显示以下字段：

- **风扇状态** - 风扇状态。可能的值如下所示：
  - 正常 - 风扇运转正常。
  - 失败 - 风扇无法正常运转。
  - 无 - 风扇 ID 不适用于特定型号。
- **温度 （以摄氏度和华氏度为单位）** - 交换机的内部温度 （适用于配备温度传感器的设备）。
- **告警温度 （以摄氏度和华氏度为单位）** - 会触发告警的单元内部温度 （适用于相关设备）。

定义空闲会话超时

*空闲会话超时*可配置 HTTP 会话经过多长时间的空闲后会超时，超时后您必须重新登录才能重建会话。

- **HTTP 会话超时**
- **HTTPS 会话超时**

设置 HTTP 或 HTTPS 会话闲置会话超时的步骤：

步骤 1 单击**管理** > **空闲会话超时**。将打开*空闲会话超时*页面。

步骤 2 从相应列表中为每个会话选择超时时间。超时时间的默认值为 10 分钟。

步骤 3 单击**应用**，在交换机上设置这些配置设置。

Ping 主机

Ping 是一种实用程序，用来测试是否可以访问远程主机，并测量从交换机到目的设备发送数据包所用的往返时间。

Ping 通过向目的主机发送互联网控制消息协议 (ICMP) 回显请求数据包并等待 ICMP 响应来运行，有时称为 pong。它可以测量往返时间并记录任何数据包丢失。

Ping 主机的步骤：

步骤 1 单击**管理 > Ping**。将打开 *Ping* 页面。

步骤 2 通过输入以下字段配置 Ping：

- **主机定义** - 选择是按主机 IP 地址还是主机名称来指定主机。
- **IP 版本** - 如果主机是根据其 IP 地址来进行标识，则选择 IPv4 或 IPv6 来指示将以选定格式对其进行输入。
- **IPv6 地址类型** - 选择 “链路本地”或 “全局”作为要输入的 IPv6 地址类型。
  - *链路本地* - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
  - *全局* - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。

- **链路本地接口** - 如果 IPv6 地址类型为 “链路本地”，请选择接收的来源。
- **主机 IP 地址 / 名称** - 要对其执行 Ping 操作的设备的地址或主机名。是 IP 地址还是主机名则取决于主机定义。
- **Ping 间隔** - 在 Ping 数据包之间系统等待的时间长度。Ping 操作会按照“Ping 数量”字段中配置的值重复执行相应次数，而不论成功还是失败。选择使用默认间隔，或者指定您自定的值。
- **Ping 数量** - Ping 操作的执行次数。选择使用默认设置，或者指定您自定的值。
- **状态** - 显示 Ping 是成功还是失败。

步骤 3 单击**激活 Ping** 来 Ping 主机。将会显示 Ping 状态，并且消息列表中会添加另一条消息，来显示 Ping 操作的结果。

步骤 4 在本页面的 **Ping 计数器和状态**部分中查看 Ping 结果。

6

系统时间

系统时钟同步提供了网络上所有设备之间的参考帧。网络管理、保护、规划和调试的各个方面都涉及确定事件的发生时间，因此网络时间同步至关重要。如果没有时钟同步，当跟踪安全漏洞或网络使用率时，就无法在设备之间准确关联日志文件。

不论文件系统位于哪台计算机上，保持修改时间的一致性都十分重要，因此时间同步还能使共享文件系统更加有序。

鉴于以上原因，在网络上的所有设备上准确配置时间就显得尤为重要。

注 交换机支持简单网络时间协议 (SNTP)，如果启用了该协议，交换机会动态同步交换机时间与 SNTP 服务器时间。交换机仅作为 SNTP 客户端工作，且无法为其他设备提供时间服务。

本节介绍用于配置系统时间、时区和夏时制 (DST) 的选项。具体包括以下主题：

- **系统时间选项**
- **SNTP 模式**
- **配置系统时间**

系统时间选项

系统时间可由用户手动设置，或从 SNTP 服务器动态设置，也可以与运行 GUI 的 PC 保持同步。如果选择使用 SNTP 服务器，则与该服务器建立通信后将会覆盖手动时间设置。

作为启动过程的一部分，交换机始终会配置时间、时区和 DST。这些参数可以通过以下方式获取：通过运行 GUI 的 PC、通过 SNTP、通过手动设置值，或者在所有其他方式均失败的情况下通过出厂默认值获取。

时间

以下方法可用于设置交换机上的系统时间：

- **手动** - 您必须手动设置时间。
- **通过 PC** - 可以使用浏览器信息通过 PC 接收时间。

  来自计算机的时间配置将保存到当前配置文件。要让设备能够在重启之后使用来自计算机的时间，必须将当前配置复制到启动配置。第一个 WEB 登录到设备期间，将设置重启后的时间。

  首次配置此功能时，如果尚未设置时间，设备将通过 PC 设置时间。

  这种时间设置方法需要配合 HTTP 和 HTTPS 连接使用。
- **SNTP** - 可以通过 SNTP 时间服务器接收时间。SNTP 使用 SNTP 服务器作为时钟源，可确保将交换机的网络时间同步精确到毫秒。指定 SNTP 服务器时，如果选择通过主机名进行识别，则 GUI 中会给出三个建议：
  - time-a.timefreq.bldrdoc.gov
  - time-b.timefreq.bldrdoc.gov
  - time-c.timefreq.bldrdoc.gov

通过以上任意一个时间源设置时间之后，浏览器将不会再次设置时间。

注 SNTP 是建议使用的时间设置方法。

时区和夏时制 (DST)

可以通过以下方式在交换机上设置时区和 DST：

- 通过 DHCP 服务器动态配置交换机，其中：
  - 动态 DST （如果已启用且可以使用）将始终优先于 DST 的手动配置。
  - 如果提供源参数的服务器发生故障或者用户禁用了动态配置，则将使用手动设置。
  - IP 地址的租用期限到期后，时区和 DST 的动态配置将继续有效。
- 仅当禁用了动态配置或者该功能发生故障时，手动配置的时区和 DST 才会成为运行时区和 DST。

  注 DHCP 服务器必须提供 DHCP 选项 100，才能进行动态时区配置。

SNTP 模式

交换机可以通过以下其中一种方式从 SNTP 服务器接收系统时间：

- 客户端广播接收 （被动模式）

  SNTP 服务器广播时间，而交换机则监听这些广播。如果交换机处于该模式，将无需定义单播 SNTP 服务器。

- **客户端广播传输 （主动模式）** - 作为 SNTP 客户端的交换机会定期请求 SNTP 时间更新。此模式以下列任何一种方式工作：
  - **SNTP 任播客户端模式** - 交换机向子网中的所有 SNTP 服务器广播时间请求数据包，然后等待服务器响应。
  - **单播 SNTP 服务器模式** - 交换机将单播查询发送到一组手动配置的 SNTP 服务器，然后等待服务器响应。

交换机支持同时启用以上两种模式，并根据基于最近层级 （距参考时钟的距离）的算法，选择从 SNTP 服务器接收的最佳系统时间。

配置系统时间

选择系统时间源

使用*系统时间*页面选择系统时间源。如果要以手动方式确定源，请在此处输入时间。

注意 如果系统时间为手动设置并且重启交换机，则必须重新输入手动时间设置。

定义系统时间的步骤：

步骤 1 单击**管理** > **时间设置** > **系统时间**。此时将打开*系统时间*页面。

此时将显示如下字段：

- **实际时间 (静态)** - 设备上的系统时间。
- **最近同步的服务器** - 上次从其获取时间的 SNTP 服务器的地址、层级和类型。

步骤 2 输入以下参数：

时钟源设置 - 选择用于设置系统时钟的时钟源。

- **主时钟源 (SNTP 服务器)** - 如果启用此功能，将从 SNTP 服务器获得系统时间。要使用此功能，还必须在 *SNTP 接口设置*页面中配置到 SNTP 服务器的连接。或者，使用 *SNTP 验证*页面强制执行 SNTP 会话验证。
- **备选时钟源 (使用活动 HTTP/HTTPS 会话的 PC)** - 选择该选项会通过 HTTP 协议使用配置计算机提供的时间设置日期和时间。

  注 需要将 “时钟源设置” 设置为以上任何一种模式， RIP MD5 验证才能工作。这也有助于实现与时间相关联的功能，例如：基于时间的 ACL、端口以及某些设备上支持的 802.1 端口验证。

手动设置 - 手动设置日期和时间。在没有替代时间源 （如 SNTP 服务器）的情况下使用本地时间：

- **日期** - 输入系统日期。
- **本地时间** - 输入系统时间。

时区设置 - 通过 DHCP 或时区偏移使用本地时间。

- **通过 DHCP 获取时区** - 选择该选项将实现通过 DHCP 服务器动态配置时区和 DST。能够配置其中一个参数还是两个参数，取决于在 DHCP 数据包中找到的信息。如果启用该选项，*还必须在交换机上启用 DHCP 客户端*。要执行此操作，请在 *IPv4 接口*页面中将 **IP 地址类型**设置为**动态**。

  注 DHCP 客户端支持提供动态时区设置的选项 100。交换机不支持 DHCPv6 客户端。
- **时区偏移** - 选择 *格林威治标准时间* (GMT) 与本地时间之间的时差 （以小时为单位）。例如，巴黎的 “时区偏移” 为 GMT +1，而纽约的 “时区偏移” 为 GMT – 5。

夏令时设置 - 选择定义 DST 的方式：

- **夏令时** - 选择该选项可启用夏令时时间。
- **时间设置偏移** - 输入相对于 GMT 偏移的分钟数 （范围为 1 到 1440）。默认为 60。
- **夏令时类型** - 单击以下选项之一：
  - *美国* - 依据在美国使用的日期设置 DST。
  - *欧洲* - 依据在欧盟及其他使用此标准的国家 / 地区使用的日期设置 DST。

- *按日期* - 手动设置 DST，通常针对除美国或欧盟国家 / 地区以外的国家 / 地区。输入以下参数：
- *循环* - 每年在同一天开始实行 DST。

选择*按日期*可以自定义 DST 的开始时间和结束时间：

- **起始时间** - DST 开始的日期和时间。
- **结束时间** - DST 结束的日期和时间。

选择*循环*可以使用其他方法自定义 DST 的开始时间和结束时间：

- **起始时间** - 每年开始实行 DST 的日期。
  - *日期* - 每年开始实行 DST 的日期 （星期几）。
  - *周* - 每年开始实行 DST 的星期 （在某月的第几个星期）。
  - *月* - 每年开始实行 DST 的月份。
  - *时间* - 每年开始实行 DST 的时间。
- **结束时间** - 每年结束 DST 的日期。例如，DST 每年在本地时间十月的第四个星期五的早上 5:00 点结束，参数如下：
  - *日期* - 每年结束 DST 的日期 （星期几）。
  - *周* - 每年结束 DST 的星期 （在某月的第几个星期）。
  - *月* - 每年结束 DST 的月份。
  - *时间* - 每年结束 DST 的时间。

步骤 3 单击**应用**。系统时间值将写入当前配置文件。

添加单播 SNTP 服务器

最多可配置八台单播 SNTP 服务器。

注 要按名称指定单播 SNTP 服务器，必须先在交换机上配置 DNS 服务器 （请参阅**定义 DNS 服务器**一节）。为添加单播 SNTP 服务器，请选中此框以启用 **SNTP 客户端单播**。

添加单播 SNTP 服务器的步骤：

步骤 1 单击**管理** > **时间设置** > **SNTP 设置**。将打开 *SNTP 设置*页面。

本页面会显示每台单播 SNTP 服务器的以下信息：

- **SNTP 服务器** - SNTP 服务器 IP 地址。最多可以定义八台 SNTP 服务器。根据服务器层级选择首选服务器或主机名。
- **轮询间隔** - 显示是否启用了轮询。
- **验证密钥 ID** - 在 SNTP 服务器和交换机之间通信所使用的密钥 ID。
- **层级** - 距参考时钟的距离 （用数值表示）。除非已启用轮询间隔，否则 SNTP 服务器无法成为主服务器 （层级 1）。
- **状态** - SNTP 服务器状态。可能的值包括：
  - *启用* - SNTP 服务器目前正常运行。
  - *禁用* - SNTP 服务器目前不可用。
  - *未知* - 目前交换机正在搜索 SNTP 服务器。
  - *正在进行* - SNTP 服务器尚未完全信任其自有时间服务器时（例如首次启动 SNTP 服务器时），会发生这种情况。
- **最近响应** - 上次从该 SNTP 服务器收到响应的日期和时间。
- **偏移** - 服务器时钟相对于本地时钟的预计偏差 （以毫秒为单位）。主机使用 RFC 2030 中介绍的算法确定此偏差的值。
- **延迟** - 沿服务器时钟与本地时钟之间的网络路径，服务器时钟相对于本地时钟的预计往返延迟。主机使用 RFC 2030 中介绍的算法确定此延迟的值。

步骤 2 要添加单播 SNTP 服务器，请启用 **SNTP 客户端单播**。

步骤 3 单击**添加**以显示*添加 SNTP 服务器*页面。

步骤 4 输入以下参数：

- **服务器定义** - 选择按照 SNTP 服务器的 IP 地址识别 SNTP 服务器，还是按照名称从列表中选择已知的 SNTP 服务器。

  注 要指定已知的 SNTP 服务器，必须将交换机连接到 Internet 并配置一个 DNS 服务器，或者进行配置以便使用 DHCP 识别 DNS 服务器。（请参阅**定义 DNS 服务器**一节。）

- **IP 版本** - 选择 IP 地址版本：**版本 6** 或**版本 4**。
- **IPv6 地址类型** - 选择 IPv6 地址类型 （如果使用 IPv6）。选项如下：
  - *链路本地* - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
  - *全局* - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。
- **链路本地接口** - 从列表中选择链路本地接口 （如果选择的 IPv6 地址类型为“链路本地”）。
- **SNTP 服务器 IP 地址** - 输入 SNTP 服务器的 IP 地址。格式取决于所选的地址类型。
- **SNTP 服务器** - 从已知 NTP 服务器列表中选择 SNTP 服务器的名称。如果选择**其他**，请在旁边的字段中输入 SNTP 服务器名称。
- **轮询间隔** - 选择该选项将启用针对系统时间信息对 SNTP 服务器的轮询。将会对注册供轮询的所有 NTP 服务器进行轮询，并将从所能访问的层级 （距参考时钟的距离）最低的服务器选择时钟。具有最低层级的服务器将被视为主服务器。具有次低层级的服务器为次服务器，以此类推。如果主服务器出现故障，交换机将轮询所有启用了轮询设置的服务器，并选择具有最低层级的服务器作为新的主服务器。
- **验证** - 选择该复选框将启用验证。
- **验证密钥 ID** - 如果启用了验证，请选择密钥 ID 值。（使用 *SNTP 验证*页面创建验证密钥。）

步骤 5 单击**应用**。将添加 STNP 服务器，并返回主页。

配置 SNTP 模式

交换机可以处于主动和 / 或被动模式 （请参阅 **SNTP 模式**了解详情）。

启用从子网上的所有服务器接收 SNTP 数据包和 / 或启用将时间请求传输到 SNTP 服务器的步骤：

步骤 1 单击**管理** > **时间设置** > **SNTP 组播 / 任播**。将打开 *SNTP 组播 / 任播*页面。

步骤 2 请从以下选项中进行选择：

- **SNTP 组播客户端模式 (客户端广播接收)** - 选择该选项可从子网上的任何 SNTP 服务器接收系统时间。
- **SNTP 任播客户端模式 (客户端广播传输)** - 选择该项可传输请求系统时间信息的 SNTP 广播同步数据包。如果已定义 SNTP 服务器，数据包将传输到这些服务器；否则，数据包将传输到子网上的所有 SNTP 服务器。

步骤 3 如果系统处于第 3 层系统模式下，请单击**添加**，以输入用于 SNTP 接收 / 传输的接口。将打开*添加 SNTP 接口设置*页面。

选择一个接口，然后选择接收 / 传输选项。

步骤 4 单击**应用**，以将设置保存到当前配置文件中。

定义 SNTP 验证

SNTP 客户端可以使用 HMAC-MD5 验证响应。 SNTP 服务器与密钥相关联，当与响应本身一起输入 MD5 函数时会使用该密钥； MD5 的结果也包括在响应数据包中。

使用 *SNTP 验证*页面可配置与需要验证的 SNTP 服务器通信时使用的验证密钥。

验证密钥在 SNTP 服务器上通过独立过程创建，该过程取决于用户使用的 SNTP 服务器类型。请咨询 SNTP 服务器系统管理员，了解详情。

工作流

步骤 1 在 *SNTP 验证*页面中启用验证功能。

步骤 2 在 *SNTP 验证*页面中创建一个密钥。

步骤 3 在 *SNTP 设置*页面中将此密钥与 SNTP 服务器相关联。

启用 SNTP 验证和定义密钥的步骤：

步骤 1 单击**管理** > **时间设置** > **SNTP 验证**。将打开 *SNTP 验证*页面。

步骤 2 选择 **SNTP 验证**，以支持对交换机和 SNTP 服务器之间的 SNTP 会话进行验证。

步骤 3 单击**应用**更新交换机。

步骤 4 单击**添加**。将打开*添加 SNTP 验证*页面。

步骤 5 输入以下参数：

- **验证密钥 ID** - 输入用于内部识别此 SNTP 验证密钥的数字。
- **验证密钥** - 输入用于验证的密钥 （最多八个字符）。 SNTP 服务器必须发送此密钥，交换机才会与之同步。
- **可信任密钥** - 选择该选项，可使交换机使用此验证密钥仅从 SNTP 服务器接收同步信息。

步骤 6 单击**应用**。 SNTP 验证参数将写入当前配置文件。

7

管理设备诊断

本节包含有关配置端口镜像、运行电缆测试和查看设备工作信息的信息。

具体包括以下主题：

- **测试铜缆端口**
- **显示光纤模块状态**
- **配置端口和 VLAN 镜像**
- **查看 CPU 利用率和安全的核心技术**

测试铜缆端口

*铜缆测试*页面将显示虚拟电缆测试器 (VCT) 对铜质电缆执行的集成电缆测试的结果。

VCT 执行两种测试：

- Time Domain Reflectometry (TDR) 技术测试连接到端口的铜质电缆的质量和特性。最长可以测试 140 米的电缆。这些结果将在*铜缆测试*页面 “测试结果” 框中显示。
- 可对活动的 GE 链路执行基于 DSP 的测试，以测量电缆长度。这些结果将在*铜缆测试*页面 “高级信息” 框中显示。

运行铜缆端口测试的前提条件

运行该测试之前，请执行以下操作：

- （强制操作）禁用短距模式 （请参阅*端口管理 > 绿色以太网 > 属性*页面）
- （可选操作）禁用 EEE （请参阅 “端口管理” > 绿色以太网 > *属性*页面）

使用 VCT 测试电缆时，会使用一条 CAT5 数据电缆。

测试结果的准确率可以有一个错误范围，高级测试的错误范围为 +/- 10，基本测试的错误范围为 +/- 2。

注意 测试端口时，会将端口设置为中断状态，通信会被中断。测试后，端口会恢复连接状态。不建议在用于运行 基于 Web 的交换机配置实用程序 的端口上运行铜缆端口测试，因为这会中断与该设备之间的通信。

测试连接到端口的铜质电缆的步骤：

步骤 1 单击**管理** > **诊断** > **铜缆测试**。将打开*铜缆测试*页面。

步骤 2 选择要进行铜缆测试的端口。

步骤 3 单击**铜缆测试**。

步骤 4 当显示该消息时，单击**确定**确认链路可以中断，或单击**取消**中止测试。

在 “测试结果”框中将显示以下字段：

- **最近更新** - 上次在端口上执行测试的时间。
- **测试结果** - 电缆测试结果。可能的值包括：
  - *良好* - 电缆通过测试。
  - *无电缆* - 电缆没有连接到端口。
  - *开放电缆* - 电缆只有一端连接。
  - *短电缆* - 电缆发生短路。
  - *未知测试结果* - 发生错误。
- **与故障的距离** - 端口与电缆上的故障点之间的距离。
- **运行端口状态** - 显示端口处于连接还是中断状态。

如果正在测试的端口是一个千兆端口，**高级信息**框将显示以下信息 （每次进入该页面，都将刷新该信息框）：

- **电缆长度：**提供长度的估计值。
- **对** - 所测试的电缆对。
- **状态** - 线对状态。红色表示发生故障，绿色表示状态良好。
- **通道** - 电缆通道表示该线缆是直通电缆还是交叉电缆。
- **极性** - 指示是否为线对激活了自动极性检测和更正。
- **对间偏移** - 线对间延迟的差异。

注 当端口速度为每秒 10 Mbit 时，不能执行 TDR 测试。

显示光纤模块状态

*光纤模块状态*页面会显示由 SFP （小型封装可热插拔）收发器报告的工作状况。对于不支持数字诊断监控标准 SFF-8472 的 SFP，可能不会提供某些信息。

MSA 兼容 SFP

支持以下 FE SFP (100 Mbps) 收发器：

- MFEBX1：适用于单模光纤 （1310 nm 波长）的 100BASE-BX-20U SFP 收发器，有效距离可达 20 km。
- MFEFX1：适用于多模光纤 （1310 nm 波长）的 100BASE-FX SFP 收发器，有效距离可达 2 km。
- MFELX1：适用于单模光纤 （1310 nm 波长）的 100BASE-LX SFP 收发器，有效距离可达 10 km。

支持以下 GE SFP (1000 Mbps) 收发器：

- MGBBX1：适用于单模光纤 （1310 nm 波长）的 1000BASE-BX-20U SFP 收发器，有效距离可达 40 km。
- MGBLH1：适用于单模光纤 （1310 nm 波长）的 1000BASE-LH SFP 收发器，有效距离可达 40 km。
- MGBLX1：适用于单模光纤 （1310 nm 波长）的 1000BASE-LX SFP 收发器，有效距离可达 10 km。
- MGBSX1：适用于多模光纤 （850 nm 波长）的 1000BASE-SX SFP 收发器，有效距离可达 550 m。
- MGBT1：适用于 5 类铜缆的 1000BASE-T SFP 收发器，有效距离可达 100 m。

要查看光纤测试的结果，请单击**管理** > **诊断** > **光纤模块状态**。将打开*光纤模块状态*页面。

此页面显示了以下字段：

- **端口** - 连接 SFP 的端口的端口号。
- **温度** - SFP 的工作温度 （以摄氏度为单位）。
- **电压** - SFP 的工作电压。
- **电流** - SFP 的当前功耗。
- **输出功率** - 传输的光功率。

- **输入功率** - 接收的光功率。
- **发射器故障** - 远程 SFP 报告信号丢失。值为 "True"、 "False" 和 “无信号 (N/S)”。
- **信号丢失** - 本地 SFP 报告信号丢失。值为 "True" 和 "False"。
- **数据就绪** - SFP 在工作。值为 "True" 和 "False"。

配置端口和 VLAN 镜像

在网络交换机上，可使用端口镜像将一个交换机端口、多个交换机端口或整个 VLAN 上看到的网络数据包的副本发送到交换机上另一端口上的网络监控连接。这对于需要进行网络流量监控的网络应用 （例如入侵检测系统）很常用。连接到监控端口的网络分析器会处理用于进行诊断、调试和性能监控的数据包。最多可以镜像八个源。这可以是八个独立端口和 / 或 VLAN 的任意组合。

在分配给要进行镜像的 VLAN 的网络端口上收到的数据包将被镜像到分析器端口，即使该数据包最终会被拦截或丢弃亦如此。如果激活了 “传输 (Tx) 镜像”，将会镜像由交换机发送的数据包。

镜像并不保证在分析器 （目的）端口上收到来自源端口的所有流量。如果向分析器端口发送的数据超出了其能够接收的量，则某些数据可能会丢失。

只有一个镜像实例是全系统支持的。分析器端口 （或 VLAN 镜像或端口镜像的目的端口）对于所有已镜像的 VLAN 或端口是相同的。

启用镜像的步骤：

步骤 1 单击**管理** > **诊断** > **端口和 VLAN 镜像**。将打开*端口和 VLAN 镜像*页面。

此页面显示了以下字段：

- **目的端口** - 要向其复制流量的端口，即分析器端口。
- **源接口** - 要自其向分析器端口发送流量的接口、端口或 VLAN。
- **类型** - 监控类型：传入端口 （接收）、从端口传出 （传输）或两者。
- **状态** - 显示以下内容之一：
  - *活动* - 源和目的接口都处于连接状态，并在转发流量。
  - *未就绪* - 出于某种原因，源或目的接口 （或者两者都）处于中断状态，没有转发流量。

步骤 2 单击**添加**添加要镜像的端口或 VLAN。将打开*添加端口和 VLAN 镜像*页面。

步骤 3 输入参数：

- **目的端口** - 选择要向其复制数据包的分析器端口。系统会将网络分析器 （例如运行 Wireshark 的 PC）连接到此端口。如果将一个端口确定为分析器目的端口，它会保留分析器目的端口，直到删除所有条目。
- **源接口** - 选择从其中镜像流量的源端口或源 VLAN。
- **类型** - 选择要将传入流量、传出流量还是这两种类型的流量镜像到分析器端口。如果选择**端口**，选项如下：
  - *仅接收* - 对传入数据包进行端口镜像。
  - *仅发送* - 对传出数据包进行端口镜像。
  - *发送和接收* - 对传入和传出数据包均进行端口镜像。

步骤 4 单击**应用**。端口镜像将添加到当前配置。

查看 CPU 利用率和安全的核心技术

本节介绍了安全的核心技术 (SCT) 以及如何查看 CPU 使用情况。

除终端用户流量之外，交换机还处理以下类型的流量：

- 管理流量
- 协议流量
- Snooping 流量

过多的流量会使 CPU 不堪重负，并可能影响正常的交换机运行。交换机使用安全的核心技术 (SCT) 功能，可以确保交换机无论接收的总流量是多少，都能够接收并处理管理和协议流量。默认情况下， SCT 在设备上已启用，且不能被禁用。

该功能与其他功能间没有交互。

显示 CPU 利用率的步骤：

步骤 1 单击**管理** > **诊断** > **CPU 利用率**。

将打开 *CPU 利用率*页面。

CPU 输入速率字段将显示每秒向 CPU 输入帧的速率。

该窗口显示 CPU 利用率图表。 Y 轴表示占用百分比， X 轴为样本号。

步骤 2 选择**刷新速率**，即刷新统计信息的时间间隔 （以秒为单位的时间段）。为每个时间段创建一个新样本。

8

配置发现

本节提供了有关配置发现的信息。

其中包含以下主题：

- **配置 Bonjour 发现**
- **LLDP 和 CDP**
- **配置 LLDP**
- **配置 CDP**

配置 Bonjour 发现

作为 Bonjour 客户端，交换机会定期将 Bonjour 发现协议数据包广播给直接连接的 IP 子网，以通告它的存在以及它所提供的服务，例如 HTTP 或 HTTPS。（可使用*安全 > TCP/UDP* 服务页面启用或禁用交换机服务。）网络管理系统或其他第三方应用程序可*发现*交换机。默认情况下，Bonjour 已启用并在管理 VLAN 上运行。Bonjour Console 会自动检测并显示该设备。

第 2 层系统模式下的 Bonjour

Bonjour 发现只能全局启用，而无法针对每个端口或每个 VLAN 启用它。交换机会通告由管理员启用的服务。

同时启用 Bonjour 发现和 IGMP 时，Bonjour 的 IP 组播地址会显示在*添加 IP 组播组地址*页面上。

若禁用 Bonjour 发现，交换机会停止服务类型通告，且不会对来自网络管理应用程序的服务请求作出响应。

默认情况下，会在作为管理 VLAN 成员的所有接口上启用 Bonjour。

全局启用 Bonjour 的步骤：

步骤 1 单击**管理** > **发现 - Bonjour**。系统将打开*发现 - Bonjour* 页面。

步骤 2 选择**启用**以在交换机上全局启用 Bonjour 发现。

步骤 3 单击**应用**。将根据您的选择，在交换机上启用或禁用 Bonjour。

LLDP 和 CDP

LLDP （链路层发现协议）和 CDP （思科发现协议）都是链路层协议，支持 LLDP 和 CDP 的直接连接邻居可使用这两种协议相互通告自身及其功能。默认情况下，交换机会定期向所有接口发送 LLDP/CDP 通告，并按照协议的要求终止和处理入站 LLDP 及 CDP 数据包。 LLDP 和 CDP 协议下，通告将在数据包中编码为 TLV （类型、长度、值）。

应用以下 CDP/LLDP 配置说明：

- CDP/LLDP 可全局启用或禁用，也可按端口启用 / 禁用。仅当全局启用 CDP/LLDP 时，端口的 CDP/LLDP 功能才有意义。
- 如果全局启用 CDP/LLDP，交换机将滤除来自已禁用 CDP/LLDP 端口的入站 CDP/LLDP 数据包。
- 如果全局禁用 CDP/LLDP，交换机可配置为丢弃、可识别 VLAN 泛洪或无法识别 VLAN 泛洪所有入站 CDP/LLDP 数据包。可识别 VLAN 泛洪会将入站 CDP/LLDP 数据包泛洪到接收数据包的 VLAN，其中不包括入站端口。无法识别 VLAN 泛洪会将入站 CDP/LLDP 数据包泛洪到除入站端口外的所有端口。全局禁用 CDP/LLDP 时，系统默认丢弃 CDP/LLDP 数据包。您可以分别在 “CDP 属性”页面和 “LLDP 属性”页面配置入站 CDP/LLDP 数据包的丢弃 / 泛洪操作。
- 自动智能端口需要启用 CDP 和 / 或 LLDP。自动智能端口会根据接口接收的 CDP/LLDP 通告，自动对接口进行配置。
- CDP 和 LLDP 终端设备 （如 IP 电话）会从 CDP 和 LLDP 通告中学习语音 VLAN 配置。默认情况下，交换机会根据所配置的语音 VLAN 发送 CDP 和 LLDP 通告。有关详情，请参阅 “语音 VLAN”和 “自动语音 VLAN”部分。

注 如果端口位于 LAG 中， CDP/LLDP 将不作区分。如果多个端口位于 LAG 中， CDP/LLDP 将在各端口上传输数据包，而不会考虑它们在 LAG 中这一事实。

CDP/LLDP 的操作不受接口 STP 状态的影响。

如果接口已启用 802.1x 端口访问控制，仅当该接口经过验证和授权的情况下，交换机才可在其上收发 CDP/LLDP 数据包。

如果端口是镜像目标，则根据 CDP/LLDP，它将被视为处于关闭状态。

注 CDP 和 LLDP 都是链路层协议，支持 CDP/LLDP 的直接连接设备可使用这两种协议通告自身及其功能。如果部署中支持 CDP/LLDP 的设备不是直接连接且与不支持 CDP/LLDP 的设备相分离，则仅当不支持 CDP/LLDP 的设备泛洪发送所接收 CDP/LLDP 数据包的情况下，它们才能接收来自其他设备的通告。如果不支持 CDP/LLDP 的设备执行可识别 VLAN 泛洪，则支持 CDP/LLDP 的设备只有在位于同一 VLAN 中时才能互相接收通告。如果不支持 CDP/LLDP 的设备泛洪发送 CDP/LLDP 数据包，支持 CDP/LLDP 的设备可以接收来自多个设备的通告。

配置 LLDP

本节介绍如何配置 LLDP。其中包含以下主题：

- LLDP 概述
- 设置 LLDP 属性
- 编辑 LLDP 端口设置
- LLDP MED
- 配置 LLDP MED 端口设置
- 显示 LLDP 端口状态
- 显示 LLDP 本地信息
- 显示 LLDP 邻居信息
- 获取 LLDP 统计信息
- LLDP 过载

LLDP 概述

LLDP 可使网络管理员在多供应商环境中排除故障并强化网络管理。 LLDP 提供了标准化的方法，便于网络设备向其他系统通告自身并存储已发现的信息。

LLDP 可让设备向相邻设备通告其身份、配置和功能，然后这些相邻设备会将这些数据存储在管理信息库 (MIB) 中。网络管理系统会通过查询这些 MIB 数据库来为网络拓扑建模。

LLDP 是一种链路层协议。默认情况下，交换机会按照协议的要求终止并处理所有入站 LLDP 数据包。

LLDP 协议有一个名为 LLDP 媒体终端发现 (LLDP-MED) 的扩展协议，该扩展协议可提供和接受来自 VoIP 电话和视频电话等媒体终端设备的信息。有关 LLDP-MED 的更多信息，请参阅 **LLDP MED**。

LLDP 配置工作流程

以下是可使用 LLDP 功能执行的操作示例，请按建议的顺序执行。如需有关 LLDP 配置的其他说明，请参阅 "LLDP/CDP" 一节。LLDP 配置页面可在**管理 > 发现 LLDP** 菜单下打开。

1. 使用 *LLDP 属性*页面输入 LLDP 全局参数，如发送 LLDP 更新的时间间隔。
2. 使用*端口设置*页面按端口配置 LLDP。在此页面上，接口可配置为接收 / 传输 LLDP PDU、、指定要通告的 TLV，以及通告交换机的管理地址。
3. 使用 *LLDP MED 网络策略*页面创建 LLDP MED 网络策略。
4. 使用 *LLDP MED 端口设置*页面将 LLDP MED 网络策略和可选 LLDP-MED TLV 与所需的接口关联。
5. 若要使自动智能端口检测 LLDP 设备的功能，请在 “智能端口属性” 页面中启用 LLDP。
6. 使用 *LLDP 过载*页面显示过载信息。

设置 LLDP 属性

使用 *LLDP 属性*页面可输入 LLDP 一般参数，例如全局启用 / 禁用功能和设置定时器。

输入 LLDP 属性的步骤：

步骤 1 单击**管理** > **发现 - LLDP** > **属性**。将打开*属性*页面。

步骤 2 输入参数。

- **LLDP 状态** - 选择该项可启用交换机上的 LLDP （默认启用）。
- **LLDP 帧处理** - 如果未启用 LLDP，选择在收到符合所选条件的数据包时要执行的操作：
  - *过滤* - 删除数据包。
  - *泛洪* - 将数据包转发给所有 VLAN 成员。
- **TLV 通告间隔** - 输入发送 LLDP 通告更新的速率（以秒为单位）或使用默认值。

- **拓扑更改系统日志通知间隔** - 输入系统日志通知之间的最小时间间隔。
- **保留时间 (以倍数表示)** - 输入在丢弃 LLDP 数据包之前保留这些数据包的时间（以 TLV 通告间隔的倍数计量）。例如，如果 “TLV 通告间隔” 为 30 秒，而 “保留时间 (以倍数表示)” 为 4，则系统会在 120 秒后丢弃 CDP 数据包。
- **重新初始化延迟** - 输入在一个 LLDP 启用 / 禁用周期之后，禁用 LLDP 与重新初始化 LLDP 之间的时间间隔 （以秒为单位）。
- **传输延迟** - 输入由 LLDP 本地系统 MIB 中的更改而引发的连续 LLDP 帧传输之间的时间 （以秒为单位）。

步骤 3 在**快速启动重复计数**字段中，输入初始化 LLDP-MED 快速启动机制时发送 LLDP 数据包的次数。有新的端点设备连接至交换机时会发生这种情况。有关 LLDP MED 的说明，请参阅 *LLDP MED 网络策略*一节。

步骤 4 单击**应用**。 LLDP 属性会添加至当前配置文件。

编辑 LLDP 端口设置

使用*端口设置*页面可以针对每个端口激活 LLDP 和远程日志服务器通知，并选择 LLDP PDU 中包含的 TLV。

要通告的 LLDP-MED TLV 可在 *LLDP MED 端口设置*页面进行选择，并且可以配置交换机的管理地址 TLV。

定义 LLDP 端口设置的步骤：

步骤 1 单击**管理** > **发现 - LLDP** > **端口设置**。将打开*端口设置*页面。

此页面显示端口 LLDP 信息。

步骤 2 选择一个端口，然后单击**编辑**。系统将打开*编辑 LLDP 端口设置*页面。

此页面提供了以下字段：

- **接口** - 选择要编辑的端口。
- **管理状态** - 为端口选择 LLDP 发布选项。这些值包括：
  - *仅发送* - 只发布不发现。
  - *仅接收* - 只发现不发布。
  - *发送和接收* - 发布并发现。

- *禁用* - 表示在该端口上禁用 LLDP。

- **系统日志通知** - 选择 “**Enable**”会在发生拓扑更改时通知通知接收者。

  可在 *LLDP 属性*页面的 “拓扑更改系统日志通知间隔”字段中输入通知之间的时间间隔。

- **可用的可选 TLV** - 通过将 TLV 移至**选定的可选 TLV** 列表中，可选择要由交换机发布的信息。可用 TLV 包含以下信息：

  - *端口说明* - 有关端口的信息，包括制造商、产品名称和硬件 / 软件版本。

  - *系统名称* - 系统的指定名称 （使用字母数字格式）。该值与 sysName 对象相等。

  - *系统说明* - 对网络实体的描述 （使用字母数字格式）。它包括系统名称、硬件版本、操作系统和交换机支持的网络软件。该值与 sysDescr 对象相等。

  - *系统功能* - 交换机的主要功能，以及是否已在交换机中启用这些功能。这些功能由两个八进制数表示。0 到 7 位分别表示其他、中继器、网桥、WLAN AP、路由器、电话、 DOCSIS 电缆设备以及工作站。 8 到 15 位为保留位。

  - *802.3 MAC-PHY* - 双工和比特率功能以及发送设备的当前双工和比特率设置。它还表明当前设置是通过自动协商还是手动配置而产生的。

  - *802.3 链路聚合* - 是否可以聚合链路 （与用于传输 LLDP PDU 的端口相关联）。它还表明链路当前是否已聚合；如果是，则提供聚合的端口标识符。

  - *802.3 最大帧* - MAC/PHY 实施的最大帧大小功能。

以下字段与管理地址相关：

- **通告模式** - 选择以下其中一种通告交换机 IP 管理地址的方法：

  - *自动通告* - 指定软件将从所有产品 IP 地址中自动选择一个管理地址进行通告。如果有多个 IP 地址，软件将选择动态 IP 地址中的最小 IP 地址。如果无动态地址，软件将选择静态 IP 地址中的最小 IP 地址。

  - *无* - 不通告管理 IP 地址。

  - *手动通告* - 选择该选项以及要通告的管理 IP 地址。

- **IP 地址** - 如果选择手动通告，则请从提供的地址中选择管理 IP 地址。

步骤 3 输入相关信息，然后单击**应用**。端口设置将写入当前配置文件中。

LLDP MED

LLDP 媒体终端发现(LLDP-MED) 是 LLDP 的扩展协议，可提供以下附加功能来支持媒体终端设备。 LLDP MED 网络策略的某些特性如下：

- 实现实时应用 （如语音和 / 或视频）的网络策略通告和发现。
- 发现设备位置以让您创建位置数据库；对于 IP 电话 (VoIP)、紧急电话服务 (E-911)，则使用 IP 电话位置信息。
- 故障排除信息。 LLDP MED 会向网络管理员发送以下警报：
  - 端口速度与双工模式相冲突
  - QoS 策略配置不正确

设置 LLDP MED 网络策略

LLDP-MED 网络策略是某特定实时应用 （如语音或视频）的一组相关配置设置。配置之后，网络策略将包含在出站 LLDP 数据包中发送到相连接的 LLDP 媒体终端设备。媒体终端设备必须根据所接收网络策略中的规定发送流量。例如，可以为 VoIP 流量创建一个策略，以便指引 VoIP 电话：

- 在 VLAN 10 上将语音流量作为已标记数据包进行发送，并设定 802.1p 优先级为 5。
- 使用 DSCP 46 发送语音流量。

使用 *LLDP MED 端口设置*页面可将网络策略与端口相关联。管理员可手动配置一个或多个网络策略以及要发送策略的接口。管理员负责根据网络策略及其关联的接口，手动创建 VLAN 及其端口成员关系。

此外，管理员还可指引交换机根据其保留的语音 VLAN，自动生成并通告语音应用的网络策略。有关交换机如何保留其语音 VLAN 的详情，请参阅 “自动语音 VLAN” 一节。

定义 LLDP MED 网络策略的步骤：

步骤 1 单击**管理** > **发现 - LLDP** > **LLDP MED 网络策略**。系统将打开 *LLDP MED 网络策略*页面。

此页面显示了之前创建的网络策略。

步骤 2 若要使交换机自动根据其保留的语音 VLAN，自动生成并通告语音应用的网络策略，请为语音应用的 LLDP-MED 网络策略选择**自动**。

注 选中此框后，用户将无法手动配置语音网络策略。

步骤 3 单击**应用**将此设置添加到当前配置文件。

步骤 4 要定义新策略，单击**添加**，系统将打开*添加 LLDP MED 网络策略*页面。

步骤 5 输入以下值：

- **网络策略编号** - 选择要创建的策略编号。
- **应用** - 选择正为何种类型的应用 （流量类型）定义网络策略。
- **VLAN ID** - 输入必须向其发送流量的 VLAN ID。
- **VLAN 标记** - 选择是否为流量添加标记。
- **用户优先级** - 选择要应用于此网络策略所定义流量的流量优先级。这是 CoS 值。
- **DSCP 值** - 选择要与邻居所发送应用数据相关联的 DSCP 值。该值可告诉邻居要如何标记他们发送给交换机的应用流量。

步骤 6 单击**应用**。系统将定义网络策略。

注 对于出站 LLDP 数据包，您必须使用 “LLDP MED 端口设置” 页面手动配置接口，以便将所需的手动定义网络策略包括在内。

配置 LLDP MED 端口设置

使用 “LLDP MED 端口设置” 页面可选择 LLDP-MED TLV 和 / 或网络策略，使之包含在所需接口的出站 LLDP 通告中。网络策略使用 “LLDP MED 网络策略” 页面进行配置。

注 如果语音应用的 LLDP-MED 网络策略 （“LLDP-MED 网络策略” 页面）为 “自动” 且自动语音 VLAN 正在运行，则对于所有已启用 LLDP-MED 且属于语音 VLAN 成员的端口，交换机将自动为其生成语音应用的 LLDP-MED 网络策略。

在每个端口上配置 LLDP MED 的步骤：

步骤 1 单击**管理** > **发现 - LLDP** > **LLDP MED 端口设置**。系统将打开 *LLDP MED 端口设置* 页面。

此页面显示了所有端口的 LLDP MED 设置，包括启用的 TLV。

步骤 2 该页面顶部的消息表明是否自动生成语音应用的 LLDP MED 网络策略 （参阅 **LLDP 概述**）。单击该链接以更改模式。

步骤 3 要将其他 LLDP MED TLV 和 / 或一个或多个用户定义的 LLDP MED 网络策略与某端口相关联，选择该端口，然后单击**编辑**。系统将打开*编辑 LLDP MED 端口设置*页面。

步骤 4 输入参数：

- **接口** - 选择要配置的接口。
- **LLDP MED 状态** - 在此端口上启用 / 禁用 LLDP MED。
- **系统日志通知** - 选择在发现支持 MED 的终端站时，是否针对每个端口发送日志通知。
- **可用的可选 TLV** - 通过将 TLV 移至*选定的可选 TLV* 列表中，来选择可由交换机发布的 TLV。
- **可用的网络策略** - 通过将 LLDP MED 策略移至 “选定的网络策略” 列表中，来选择将由 LLDP 发布的 LLDP MED 策略。这些策略在 *LLDP MED 网络策略*页面中进行创建。要在通告中包括一个或多个用户定义的网络策略，您还须从 “可用的可选 TLV” 中选择*网络策略*。

  注 必须按照 LLDP-MED 标准 (ANSI-TIA-1057_final_for_publication.pdf) 中定义的精确数据格式，使用十六进制字符在以下字段中输入内容：

  - **位置坐标** - 输入要由 LLDP 发布的坐标位置。
  - **位置城市地址** - 输入要由 LLDP 发布的城市地址。
  - **位置 (ECS) ELIN** - 输入要由 LLDP 发布的紧急电话服务 (ECS) ELIN 位置。

步骤 5 单击**应用**。 LLDP MED 端口设置将写入当前配置文件中。

显示 LLDP 端口状态

*LLDP 端口状态表*页面显示每个端口的 LLDP 全局信息。

步骤 1 要查看 LLDP 端口状态，请单击**管理** > **发现 - LLDP** > **LLDP 端口状态**。系统将打开 *LLDP 端口状态*页面。

步骤 2 单击 **LLDP 本地信息详情**，查看发送给邻居的 LLDP 和 LLDP-MED TLV 的详情。

步骤 3 单击 **LLDP 邻居信息详情**，查看邻居发送来的 LLDP 和 LLDP-MED TLV 的详情。

LLDP 端口状态全局信息

- **机箱 ID 子类型** - 机箱 ID 的类型 （例如， MAC 地址）。
- **机箱 ID** - 机箱的标识符。在机箱 ID 子类型为 MAC 地址处，会显示交换机的 MAC 地址。
- **系统名称** - 交换机的名称。

- **系统说明** - 对交换机的描述 （使用字母数字格式）。
- **支持的系统功能** - 设备的主要功能，例如，网桥、 WLAN AP 或路由器。
- **已启用的系统功能** - 设备已启用的主要功能。
- **端口 ID 子类型** - 显示的端口标识符的类型。

LLDP 端口状态表

- **接口** - 端口标识符。
- **LLDP 状态** - LLDP 发布选项。
- **LLDP MED 状态** - 已启用或已禁用。
- **本地 PoE** - 通告的本地 PoE 信息。
- **远程 PoE** - 邻居通告的 PoE 信息。
- **邻居数量** - 发现的邻居数目。
- **第一台设备的邻居功能** - 显示邻居的主要功能，例如：网桥或路由器。

显示 LLDP 本地信息

查看在端口上通告的 LLDP 本地端口状态的步骤：

步骤 1 单击**管理** > **发现 - LLDP** > **LLDP 本地信息**。系统将打开 *LLDP 本地信息*页面。

步骤 2 在页面底部，单击 **LLDP 端口状态表**。

单击 **LLDP 本地信息详情**，查看发送给邻居的 LLDP 和 LLDP MED TLV 的详情。

单击 **LLDP 邻居信息详情**，查看邻居发送来的 LLDP 和 LLDP-MED TLV 的详情。

步骤 3 从**端口**列表中选择所需的端口。

此页面提供了以下字段：

全局

- **机箱 ID 子类型** - 机箱 ID 的类型。（例如， MAC 地址。）
- **机箱 ID** - 机箱的标识符。在机箱 ID 子类型为 MAC 地址处，会显示交换机的 MAC 地址。
- **系统名称** - 交换机的名称。
- **系统说明** - 对交换机的描述 （使用字母数字格式）。

- **支持的系统功能** - 设备的主要功能，例如，网桥、 WLAN AP 或路由器。
- **已启用的系统功能** - 设备已启用的主要功能。
- **端口 ID 子类型** - 显示的端口标识符的类型。
- **端口 ID** - 端口的标识符。
- **端口说明** - 有关端口的信息，包括制造商、产品名称和硬件 / 软件版本。

管理地址

显示本地 LLDP 代理的地址表。其他远程管理员可以使用该地址获取与本地设备相关的信息。该地址由以下元素组成：

- **地址子类型** - 在 “管理地址” 字段中列出的管理 IP 地址的类型，例如 IPv4。
- **地址** - 返回的最适合管理用途的地址，。
- **接口子类型** - 用于定义接口编号的编号方法。
- **接口编号** - 与此管理地址相关联的具体接口。

MAC/PHY 详情

- **支持自动协商** - 端口速度自动协商支持状态。
- **已启用自动协商** - 端口速度自动协商活动状态。
- **自动协商通告功能** - 端口速度自动协商功能，例如， 1000BASE-T 半双工模式、 100BASE-TX 全双工模式。
- **运行 MAU 类型** - 介质连接单元 (MAU) 类型。 MAU 可执行物理层功能，包括通过对以太网接口进行冲突检测来转换数字数据和在网络中插入位，例如 100BASE-TX 全双工模式。

802.3 详情

- **802.3 最大帧大小** - 支持的最大 IEEE 802.3 帧大小。

802.3 链路聚合

- **聚合功能** - 表明是否可以聚合接口。
- **聚合状态** - 表明是否已聚合接口。
- **聚合端口 ID** - 通告的聚合接口 ID。

802.3 节能以太网 (EEE) （如果设备支持 EEE）

- **本地发送** - 表明传输链路伙伴在离开低功耗空闲 （LPI 模式）后，开始传输数据之前所等待的时间 （微秒）。
- **本地接收** - 表明接收链路伙伴要求传输链路伙伴在低功耗空闲 （LPI 模式）后，开始传输数据之前所等待的时间 （微秒）。
- **远程发送回波** - 表明本地链路伙伴反射远程链路伙伴的发送值。
- **远程接收回波** - 表明本地链路伙伴反射远程链路伙伴的接收值。

MED 详情

- **支持的功能** - 端口上支持的 MED 功能。
- **当前功能** - 端口上启用的 MED 功能。
- **设备类** - LLDP-MED 端点设备类。设备类可能为：
  - *第 1 类端点* - 表明一般端点类，提供基本 LLDP 服务。
  - *第 2 类端点* - 表明介质端点类，提供介质流功能以及所有第 1 类功能。
  - *第 3 类端点* - 表明通信设备类，提供所有第 1 类和第 2 类功能以及位置、911、第 2 层交换机支持和设备信息管理功能。
- **PoE 设备类型** - 端口 PoE 类型，例如，已打开电源。
- **PoE 电源** - 端口电源。
- **PoE 电源优先级** - 端口电源优先级。
- **PoE 功率值** - 端口电源值。
- **硬件版本** - 硬件版本。
- **固件版本** - 固件版本。
- **软件版本** - 软件版本。
- **序列号** - 设备序列号。
- **制造商名称** - 设备制造商名称。
- **型号名称** - 设备型号。
- **资产 ID** - 资产 ID。

位置信息

- **城市** - 街道地址。
- **坐标** - 地图坐标：纬度、经度和海拔高度。
- **ECS ELIN** - 紧急电话服务 (ECS) 紧急位置标识号 (ELIN)。

网络策略表

- **应用类型** - 网络策略应用类型，例如语音。
- **VLAN ID** - 为其定义网络策略的 VLAN ID。
- **VLAN 类型** - 为其定义网络策略的 VLAN 类型。该字段可能的值包括：
  - *Tagged* - 指示网络策略是为 Tagged VLAN 定义的。
  - *Untagged* - 指示网络策略是为 Untagged VLAN 定义的。
- **用户优先级** - 网络策略用户优先级。
- **DSCP** - 网络策略 DSCP。

显示 LLDP 邻居信息

*LLDP 邻居信息*页面显示从邻居设备接收到的信息。

超时 （根据在其间未收到邻居发送的 LLDP PDU 的邻居活动时间 TLV 发送的值）后，将会删除该信息。

查看 LLDP 邻居信息的步骤：

步骤 1 单击**管理** > **发现 - LLDP** > **LLDP 邻居信息**。系统将打开 *LLDP 邻居信息*页面。

此页面显示了以下字段：

- **本地端口** - 要将邻居与其连接的本地端口号。
- **机箱 ID 子类型** - 机箱 ID 的类型 （例如， MAC 地址）。
- **机箱 ID** - 802 LAN 相邻设备机箱的标识符。
- **端口 ID 子类型** - 显示的端口标识符的类型。
- **端口 ID** - 端口的标识符。
- **系统名称** - 已发布的交换机名称。
- **存活时间** - 在其后删除该邻居的信息的时间间隔 （以秒为单位）。

步骤 2 选择一个本地端口，然后单击**详情**。系统将打开 *邻居信息*页面。

此页面显示了以下字段：

端口详情

- **本地端口** - 端口号。
- **MSAP 条目** - 设备介质服务接入点 (MSAP) 条目编号。

基本详情

- **机箱 ID 子类型** - 机箱 ID 的类型 （例如， MAC 地址）。
- **机箱 ID** - 802 LAN 相邻设备机箱的标识符。
- **端口 ID 子类型** - 显示的端口标识符的类型。
- **端口 ID** - 端口的标识符。
- **端口说明** - 有关端口的信息，包括制造商、产品名称和硬件 / 软件版本。
- **系统名称** - 已发布的系统名称。
- **系统说明** - 对网络实体的描述 （使用字母数字格式）。它包括系统名称、硬件版本、操作系统和设备支持的网络软件。该值与 sysDescr 对象相等。
- **支持的系统功能** - 设备的主要功能。这些功能由两个八进制数表示。0 到 7 位分别表示其他、中继器、网桥、 WLAN AP、路由器、电话、 DOCSIS 电缆设备以及工作站。 8 到 15 位为保留位。
- **已启用的系统功能** - 设备已启用的主要功能。

管理地址表

- **地址子类型** - 管理的地址子类型，例如 MAC 或 IPv4。
- **地址** - 管理的地址。
- **接口子类型** - 端口子类型。
- **接口编号** - 端口编号。

MAC/PHY 详情

- **支持自动协商** - 端口速度自动协商支持状态。值可能为 True 和 False。
- **已启用自动协商** - 端口速度自动协商活动状态。值可能为 True 和 False。
- **自动协商通告功能** - 端口速度自动协商功能，例如， 1000BASE-T 半双工模式、 100BASE-TX 全双工模式。

- **运行 MAU 类型** - 介质连接单元 (MAU) 类型。 MAU 可执行物理层功能，包括通过对以太网接口进行冲突检测来转换数字数据和在网络中插入位，例如 100BASE-TX 全双工模式。

通过 MDI 提供的 802.3 电源

- **MDI 电源支持端口类** - 通告的电源支持端口类。
- **PSE MDI 电源支持** - 表明端口上是否支持 MDI 电源。
- **PSE MDI 电源状态** - 表明是否已在端口上启用 MDI 电源。
- **PSE 电源对控制功能** - 表明端口上是否支持电源对控制。
- **PSE 电源对** - 端口上支持的电源对控制类型。
- **PSE 电源类** - 通告的电源端口类。

802.3 详情

- **802.3 最大帧大小** - 端口上支持的最大通告帧大小。

802.3 链路聚合

- **聚合功能** - 表明是否可以聚合端口。
- **聚合状态** - 表明当前是否已聚合端口。
- **聚合端口 ID** - 通告的聚合端口 ID。

802.3 节能以太网 (EEE)

- **远程传输** - 表明传输链路伙伴在离开低功耗空闲 （LPI 模式）后，开始传输数据之前所等待的时间 （微秒）。
- **远程接收** - 表明接收链路伙伴要求传输链路伙伴在低功耗空闲 （LPI 模式）后，开始传输数据之前所等待的时间 （微秒）。
- **本地传输回波** - 表明本地链路伙伴反射远程链路伙伴的传输值。
- **本地接收回波** - 表明本地链路伙伴反射远程链路伙伴的接收值。

MED 详情

- **支持的功能** - 已在端口上启用的 MED 功能。
- **当前功能** - 由端口通告的 MED TLV。

- **设备类** - LLDP-MED 端点设备类。设备类可能为：
  - *第 1 类端点* - 表明一般端点类，提供基本 LLDP 服务。
  - *第 2 类端点* - 表明介质端点类，提供介质流功能以及所有第 1 类功能。
  - *第 3 类端点* - 表明通信设备类，提供所有第 1 类和第 2 类功能以及位置、911、第 2 层交换机支持和设备信息管理功能。
- **PoE 设备类型** - 端口 PoE 类型，例如，已打开电源。
- **PoE 电源** - 端口的电源。
- **PoE 电源优先级** - 端口电源优先级。
- **PoE 功率值** - 端口电源值。
- **硬件版本** - 硬件版本。
- **固件版本** - 固件版本。
- **软件版本** - 软件版本。
- **序列号** - 设备序列号。
- **制造商名称** - 设备制造商名称。
- **型号名称** - 设备型号。
- **资产 ID** - 资产 ID。

802.1 VLAN 和协议

- **PVID** - 通告的端口 VLAN ID。

PPVID 表

- **VID** - 协议 VLAN ID。
- **支持** - 支持的端口和协议 VLAN ID。
- **已启用** - 启用的端口和协议 VLAN ID。

VLAN ID

- **VID** - 端口和协议 VLAN ID。
- **VLAN 名称** - 通告的 VLAN 名称。

协议 ID

- **协议 ID 表** - 通告的协议 ID。

位置信息

按 ANSI-TIA-1057 标准中的 10.2.4 款所述，以十六进制字符输入以下数据结构：

- **城市** - 城市地址或街道地址。
- **坐标** - 位置地图坐标 - 纬度、经度和海拔高度。
- **ECS ELIN** - 设备紧急电话服务 (ECS) 紧急位置标识号 (ELIN)。
- **未知** - 未知的位置信息。

网络策略

- **应用类型** - 网络策略应用类型，例如语音。
- **VLAN ID** - 为其定义网络策略的 VLAN ID。
- **VLAN 类型** - 为其定义网络策略的 VLAN 类型 （Tagged 或 Untagged）。
- **用户优先级** - 网络策略用户优先级。
- **DSCP** - 网络策略 DSCP。

获取 LLDP 统计信息

*LLDP 统计信息*页面显示每个端口的 LLDP 统计信息。

查看 LLDP 统计信息的步骤：

步骤 1 单击**管理** > **发现 - LLDP** > **LLDP 统计信息**。系统将打开 *LLDP 统计信息*页面。

会为每个端口显示以下字段：

- **接口** - 接口的标识符。
- **发送帧总数** - 已传输的帧数。
- **接收的帧数**
  - *总数* - 已接收的帧数。
  - *丢弃* - 丢弃的已接收帧的总数。
  - *错误* - 已接收的错误帧总数。

- **接收的 TLV**
  - *丢弃* - 丢弃的已接收 TLV 的总数。
  - *未识别* - 未识别的已接收 TLV 的总数。
- **邻居的信息删除计数** - 接口上删除的邻居数。

步骤 2 单击**刷新**查看最新统计信息。

LLDP 过载

LLDP 会将信息作为 LLDP 和 LLDP-MED TLV 添加到 LLDP 数据包中。当 LLDP 数据包中包含的信息总量过大，超过接口支持的最大 PDU 大小时，就会发生 LLDP 过载。

*LLDP 过载*页面会显示 LLDP/LLDP-MED 信息的字节数、其他 LLDP 信息的可用字节数，以及所有接口的过载状态。

查看 LLDP 过载信息的步骤：

步骤 1 单击**管理** > **发现 - LLDP** > **LLDP 过载**。系统将打开 *LLDP 过载*页面。

此页面会为每个端口显示以下字段：

- **接口** - 端口标识符。
- **总数 (字节)** - 每个数据包中 LLDP 信息的总字节数。
- **等待发送 (字节)** - 要添加到各数据包中其他 LLDP 信息的剩余可用字节总数。
- **状态** - 正在传输 TLV 还是已过载。

步骤 2 要查看端口的过载详细信息，请选择该端口，然后单击**详情**。系统将打开 *LLDP 过载详情*页面。

此页面会为在该端口上发送的每个 TLV 显示以下信息：

- **LLDP 强制 TLV**
  - *大小 (字节)* - 强制 TLV 的字节总数。
  - *状态* - 正在传输强制 TLV 组，还是 TLV 组已过载。
- **LLDP MED 功能**
  - *大小 (字节)* - LLDP MED 功能数据包的字节总数。
  - *状态* - LLDP MED 功能数据包已发送还是已过载。

- **LLDP MED 位置**
  - *大小 (字节)* - LLDP MED 位置数据包的字节总数。
  - *状态* - LLDP MED 位置数据包已发送还是已过载。
- **LLDP MED 网络策略**
  - *大小 (字节)* - LLDP MED 网络策略数据包的字节总数。
  - *状态* - LLDP MED 网络策略数据包已发送还是已过载。
- **通过 MDI 提供的 LLDP MED 扩展电源**
  - *大小 (字节)* - 通过 MDI 提供的 LLDP MED 扩展电源数据包的总字节数。
  - *状态* - 通过 MDI 提供的 LLDP MED 扩展电源数据包已发送还是已过载。
- **802.3 TLV**
  - *大小 (字节)* - LLDP MED 802.3 TLV 数据包的总字节数。
  - *状态* - LLDP MED 802.3 TLV 数据包已传输还是已过载。
- **LLDP 可选 TLV**
  - *大小 (字节)* - LLDP MED 可选 TLV 数据包的总字节数。
  - *状态* - LLDP MED 可选 TLV 数据包已传输还是已过载。
- **LLDP MED 清单**
  - *大小 (字节)* - LLDP MED 清单 TLV 数据包的总字节数。
  - *状态* - LLDP MED 清单数据包已传输还是已过载。
- **总数 (字节)** - 每个数据包中 LLDP 信息的总字节数。
- **等待发送 (字节)** - 要添加到各数据包中其他 LLDP 信息的剩余可用字节总数。

配置 CDP

本节介绍如何配置 CDP。

其中包含以下主题：

- **设置 CDP 属性**
- **编辑 CDP 接口设置**
- **显示 CDP 本地信息**
- **显示 CDP 邻居信息**
- **查看 CDP 统计信息**

设置 CDP 属性

与 LLDP 相似， CDP （思科发现协议）也是一种便于直接连接邻居相互通告自身及其功能的链路层协议。与 LLDP 不同的是， CDP 是一种思科专有的协议。

CDP 配置工作流程

以下是在交换机上配置 CDP 的工作流程示例。您也可以参阅 "LLDP/CDP" 部分，了解其他 CDP 配置指南。

步骤 1 使用 *CDP 属性*页面输入 CDP 全局参数

步骤 2 使用*接口设置*页面按接口配置 CDP

步骤 3 若要使自动智能端口检测 CDP 设备的功能，请在*智能端口属性*页面中启用 CDP。

有关如何使用 CDP 标识智能端口设备功能的说明，请参阅**标识智能端口类型**一节。

输入 CDP 一般参数的步骤：

步骤 1 单击**管理** > **发现 - CDP** > **属性**。将打开*属性*页面。

步骤 2 输入参数。

- **CDP 状态** - 选择启用交换机上的 CDP。

- **CDP 帧处理** - 如果未启用 CDP，选择在收到符合所选条件的数据包时要执行的操作：
  - *桥接* - 根据 VLAN 转发数据包。
  - *过滤* - 删除数据包。
  - *泛洪* - 无法识别 VLAN 的泛洪，会将传入 CDP 数据包转发到除入站端口外的所有端口。
- **CDP 语音 VLAN 通告** - 选择该项后，交换机会在支持 CDP 且属于语音 VLAN 成员的所有端口上，通告 CDP 中的语音 VLAN。语音 VLAN 在 “语音 VLAN 属性” 页面中进行配置。
- **CDP 强制 TLV 验证** - 如果选择，系统将丢弃不包含强制 TLV 的传入 CDP 数据包，并且无效错误计数器将递增。
- **CDP 版本** - 选择要使用的 CDP 版本。
- **CDP 保持时间** - 丢弃 CDP 数据包之前保留这些数据包的时间 （以 “LV 通告间隔” 的倍数计量）。例如，如果 “TLV 通告间隔” 为 30 秒，而 “保留时间 (以倍数表示)” 为 4，则系统会在 120 秒后丢弃 CDP 数据包。可能的选项有：
  - *使用默认设置* - 使用默认时间 （180 秒）
  - *用户定义* - 输入时间 （秒）。
- **CDP 传输速率** - 发送 CDP 通告更新的速率 （以秒为单位）。可能的选项有：
  - *使用默认设置* - 使用默认速率 （60 秒）
  - *用户定义* - 输入速率 （秒）。
- **设备 ID 格式** - 选择设备 ID 的格式 （MAC 地址或序列号）。
- **源接口** - 要在帧 TLV 中使用的 IP 地址。可能的选项有：
  - *使用默认设置* - 使用传出接口的 IP 地址。
  - *用户定义* - 使用地址 TLV 中接口 （在**接口**字段中）的 IP 地址。
- **接口** - 如果为**源接口**选择*用户定义*，请选择接口。
- **系统日志语音 VLAN 不匹配** - 选中后，当检测到语音 VLAN 不匹配后，系统将发送系统日志消息。这意味着传入帧中的语音 VLAN 信息与本地设备通告的信息不匹配。
- **系统日志本征 VLAN 不匹配** - 选中后，当检测到本征 VLAN 不匹配后，系统将发送系统日志消息。这意味着传入帧中的本征 VLAN 信息与本地设备通告的信息不匹配。

- **系统日志双工模式不匹配** - 选中后，当双工模式信息不匹配时，系统将发送系统日志消息。这意味着传入帧中的双工模式信息与本地设备通告的信息不匹配。

步骤 3 单击**应用**。将定义 LLDP 属性。

编辑 CDP 接口设置

使用*接口设置*页面可以针对每个端口激活 LLDP 和远程日志服务器通知，并选择 LLDP PDU 中包含的 TLV。

设置这些属性后，便能够选择为支持 LLDP 协议的设备所提供的各种类型的信息。

要通告的 LLDP-MED TLV 可在 *LLDP MED 接口设置*页面中进行选择。

定义 LLDP 接口设置的步骤：

步骤 1 单击**管理** > **发现 - CDP** > **接口设置**。将打开*接口设置*页面。

此页面会为每个接口显示以下 CDP 信息。

- **CDP 状态** - 端口的 CDP 发布选项。
- **报告与 CDP 邻居冲突** - 显示**编辑**页面中启用 / 禁用的报告选项的状态 （语音 VLAN/ 本征 VLAN/ 双工）。
- **邻居数量** - 检测到的邻居数。

该页面底部有四个按钮：

- **复制设置** - 选中后，会将配置从一个端口复制到其他端口。
- **编辑** - 下文步骤 2 中解释的字段。
- **CDP 本地信息详情** - 引导至*管理 > 发现 - CDP > CDP 本地信息*页面。
- **CDP 邻居信息详情** - 引导至*管理 > 发现 - CDP > CDP 邻居信息*页面。

步骤 2 选择一个端口，然后单击**编辑**。系统将打开*编辑 CDP 接口设置*页面。

此页面提供了以下字段：

- **接口** - 选择要定义的接口。
- **CDP 状态** - 选择启用 / 禁用端口的 CDP 发布选项。

  注 当交换机设置为向管理站发送 Trap 时，以下三个字段属于可选字段。

- **系统日志语音 VLAN 不匹配** - 选择后，将启用在检测到语音 VLAN 不匹配时发送系统日志消息的选项，这意味着传入帧中的语音 VLAN 信息与本地设备所通告的信息不匹配。
- **系统日志本征 VLAN 不匹配** - 选择后，将启用在检测到本征 VLAN 不匹配时发送系统日志消息的选项。这意味着传入帧中的本征 VLAN 信息与本地设备通告的信息不匹配。
- **系统日志双工模式不匹配** - 选择后，将启用在检测到双工模式信息不匹配时发送系统日志消息的选项。这意味着传入帧中的双工模式信息与本地设备通告的信息不匹配。

步骤 3 输入相关信息，然后单击**应用**。端口设置将写入当前配置。

显示 CDP 本地信息

查看由 CDP 协议通告的、与本地设备有关的信息的步骤：

步骤 1 单击**管理** > **发现 - CDP** > **CDP 本地信息**。系统将打开 *CDP 本地信息*页面。

步骤 2 选择一个本地端口，然后将显示以下字段：

- **接口** - 本地端口的编号。
- **CDP 状态** - 显示是否已启用 CDP。
- **设备 ID TLV**
  - **设备 ID 类型** - 设备 ID TLV 中通告的设备 ID 类型。
  - **设备 ID** - 设备 ID TLV 中通告的设备 ID。
- **系统名称 TLV**
  - **系统名称** - 设备的系统名称。
- **地址 TLV**
  - **地址 1-3** - IP 地址 （设备地址 TLV 中通告的）。
- **端口 TLV**
  - **端口 ID** - 端口 TLV 中通告的端口标识符。
- **功能 TLV**
  - **功能** - 端口 TLV 中通告的功能。

- **版本 TLV**
  - **版本** - 设备正在运行的软件版本信息。
- **平台 TLV**
  - **平台** - 在平台 TLV 中通告的平台标识符。
- **本征 VLAN TLV**
  - **本征 VLAN** - 在本征 VLAN TLV 中通告的本征 VLAN 标识符。
- **全 / 半双工 TLV**
  - **双工** - 端口在全双工 / 半双工 TLV 中通告的是处于全双工还是半双工模式。
- **设备 TLV**
  - **设备 ID** - 在设备 TLV 中通告的、连接到端口的设备类型。
  - **设备 VLAN ID** - 设备所使用设备上的 VLAN，例如，如果设备是 IP 电话，该 ID 为语音 VLAN。
- **扩展信任 TLV**
  - **扩展信任** - 启用后，表明端口可以信任，就是说所接收数据包的来源主机 / 服务器可以信任，可以自我标记数据包。这种情况下，此类端口上接收的数据包不会重新标记。禁用此项表明端口不可信任，此时以下字段将有意义。
- **用于不信任端口 TLV 的 CoS**
  - **用于不可信端口的 CoS** - 如果在端口上禁用扩展信任，此字段将显示第 2 层 CoS 值，表示 802.1D/802.1p 优先级值。这是 COS 值，设备将使用该值对不信任端口上所接收的所有数据包进行重新标记。
- **功率 TLV**
  - **请求 ID** - 最后接收的电源请求 ID 会回显在电源请求 TLV 中最后接收的请求 ID 字段。如果自接口上次转换为 “开启” 状态以来未收到电源请求 TLV，该值为 0。
  - **电源管理 ID** - 每发生以下一个事件，该值将增加 1 （或 2，避免 0）。

    可用功率或管理电源等级字段值发生更改

    收到电源请求 TLV，其中请求 ID 字段与最后接收的集 （或收到首个值时）不同

    接口转换为 “关闭”

- **可用功率** - 端口消耗的电源量。
- **管理电源等级** - 显示供电器对受电设备功耗 TLV 的请求。设备总是在此字段中显示 “无偏好”。

显示 CDP 邻居信息

*CDP 邻居信息*页面显示从邻居设备接收到的 CDP 信息。

超时 （根据在其间未收到邻居发送的 CDP PDU 的邻居活动时间 TLV 发送的值）后，将会删除该信息。

查看 CDP 邻居信息的步骤：

步骤 1 单击**管理** > **发现 - CDP** > **CDP 邻居信息**。系统将打开 *CDP 邻居信息*页面。

该页面将为每个链路伙伴 （邻居）显示以下字段：

- **设备 ID** - 邻居的设备 ID。
- **系统名称** - 邻居的系统名称。
- **本地接口** - 要将邻居与其连接的本地端口号。
- **通告版本** - CDP 协议版本。
- **存活时间 (秒)** - 在其后删除该邻居的信息的时间间隔 （以秒为单位）。
- **功能** - 邻居通告的功能。
- **平台** - 来自邻居平台 TLV 的信息。
- **邻居接口** - 邻居的传出接口。

步骤 2 选择一个设备，然后单击**详情**。系统将打开 *CDP 邻居详情*页面。

此页面显示了有关邻居的以下字段：

- **设备 ID** - 邻居设备的标识符。
- **本地接口** - 帧到达所经由的端口的接口编号。
- **通告版本** - CDP 的版本。
- **存活时间** - 在其后删除该邻居的信息的时间间隔 （以秒为单位）。
- **功能** - 设备的主要功能。这些功能由两个八进制数表示。 0 到 7 位分别表示其他、中继器、网桥、 WLAN AP、路由器、电话、 DOCSIS 电缆设备以及工作站。 8 到 15 位为保留位。

- **平台** - 邻居的平台的标识符。
- **邻居接口** - 帧到达所经由的邻居的接口编号。
- **本征 VLAN** - 邻居的本征 VLAN。
- **双工** - 邻居接口处于半双工还是全双工模式。
- **地址** - 邻居的地址。
- **机动** - 接口上由邻居消耗的电源量。
- **版本** - 邻居的软件版本。

注 如果使用 CDP，单击**清除表**按钮将断开所有已连接的设备，如果启用自动智能端口，所有端口类型都将更改为默认值。

查看 CDP 统计信息

*CDP 统计信息*页面显示与从某端口收发的思科发现协议 (CDP) 帧有关的信息。 CDP 数据包从与交换机接口连接的设备接收，并供智能端口功能使用。有关详情，请参阅**配置 CDP**。

仅当在全局和某端口上启用了 CDP 时，才会显示该端口的 CDP 统计信息。此操作在 *CDP 属性*页面和 *CDP 接口设置*页面进行。

查看 CDP 统计信息的步骤：

步骤 1 单击**管理 > 发现 - CDP > CDP 统计信息。**系统将打开 *CDP 统计信息*页面。

将为每个接口显示以下字段：

接收 / 传输的数据包数：

- **版本 1** - 接收 / 发送的 CDP 版本 1 数据包数。
- **版本 2** - 接收 / 发送的 CDP 版本 2 数据包数。
- **总数** - 接收 / 发送的 CDP 数据包总数。

“CDP 错误统计信息”部分显示 CDP 错误计数器。

- **非法校验和** - 所接收的具有非法校验和值的数据包数。
- **其他错误** - 除非法校验和外，所接收的其他错误数据包数。
- **邻居数超过最大值** - 由于缺少空间，导致无法在缓存中存储数据包信息的次数。

要清除所有接口的所有计数器，请单击**清除所有接口的计数器**。要清除某接口的所有计数器，请单击**清除接口计数器**。

9

端口管理

本节介绍端口配置、链路聚合和绿色以太网功能。

具体包括以下主题：

- **配置端口**
- **设置基本的端口配置**
- **配置链路聚合**
- **配置绿色以太网**

配置端口

要配置端口，请执行以下操作：

1. 使用*端口设置*页面配置端口。
2. 使用 *LAG 管理*页面启用 / 禁用链路聚合控制 (LAG) 协议，并将潜在成员端口配置为所需的 LAG。默认情况下，所有 LAG 均为空。
3. 使用 *LAG 设置*页面配置以太网参数，例如 LAG 的速度和自动协商。
4. 使用 *LACP* 页面*为作为动态 LAG 成员或候选成员的端口配置 LACP 参数*
5. 使用*属性*页面配置绿色以太网和 802.3 节能以太网。
6. 使用*端口设置*页面配置每端口的绿色以太网能源模式和 802.3 节能以太网。
7. 如果交换机支持并启用 PoE，则按**管理以太网供电设备**中所述配置该交换机。

设置基本的端口配置

*端口设置*页面显示所有端口的全局设置和每端口设置。此页面可使您通过*编辑端口设置*页面选择并配置所需端口。

配置端口设置的步骤：

步骤 1 单击**端口管理** > **端口设置**，将打开*端口设置*页面。

步骤 2 选择**巨型帧**以支持最大为 10Kb 的数据包。如果未启用 （默认）**巨型帧**，则系统可支持最大为 2,000 字节的数据包。要使巨型帧生效，必须在启用该功能之后重启交换机。

步骤 3 单击**应用**以更新全局设置。

巨型帧配置更改*仅*在使用*复制 / 保存配置*页面将当前配置文件明确保存到启动配置文件，然后重启交换机之后才会生效。

步骤 4 要更新端口设置，请选择所需端口，然后单击**编辑**。将打开*编辑端口设置*页面。

步骤 5 修改以下参数：

- **接口** - 选择端口编号。
- **端口类型** - 显示端口类型和速度。可能的选项有：
  - *铜缆端口* - 常规端口而非组合端口，支持以下值：10M、 100M 和 1000M （类型：铜缆）。
  - *组合铜缆端口* - 与铜质 CAT5 电缆连接的组合端口，支持以下值：10M、100M 和 1000M （类型：组合铜缆）。
  - *组合光纤 - SFP 光纤千兆位接口转换器端口*，支持以下值：100M 和 1000M （类型：组合光纤）。
  - 10G 光纤 - 速度为 1G 或 10G 的端口。

  注 同时使用两个端口时，在组合端口中 SFP 光纤优先级较高。
- **端口说明** - 输入用户定义的端口名称或备注。
- **管理状态** - 选择重启交换机时端口必须处于 “启用” 状态还是 “禁用” 状态。
- **运行状态** - 显示端口当前是否处于 “启用” 状态。
- **重新激活挂起的端口** - 选择该选项可重新激活已挂起的端口。可用来挂起端口的方法有很多，例如通过锁定端口安全选项、 dot1x 单主机违例应对、环回检测、 STP 环回防护。无论出于何种原因挂起端口，重新激活操作均可将端口恢复为启用状态。

- **自动协商** - 选择该选项可在端口上启用自动协商。自动协商可使端口向端口链路伙伴通告其传输速度、双工模式和流量控制能力。
- **运行自动协商** - 显示端口上的当前自动协商状态。
- **管理端口速度** - 配置端口的速度。端口类型可确定可用的速度。仅当禁用端口自动协商时，您才可以指定*管理速度*。
- **运行端口速度** - 显示作为协商结果的当前端口速度。
- **管理双工模式** - 选择端口双工模式。仅当禁用自动协商时才会配置此字段，并且端口速度会设置为 10M 或 100M。端口速度为 1G 时，始终处于全双工模式。可能的选项有：
  - *全双工* - 接口支持交换机和客户端之间的同时双向传输。
  - *半双工* - 接口仅支持交换机和客户端之间在某一时刻的单向传输。
- **运行双工模式** - 显示端口当前的双工模式。
- **自动通告** - 选择启用自动协商后，要由其通告的功能。选项如下：
  - *最大容量* - 可以接受所有端口速度和双工模式设置。
  - *10 半双工* - 10 Mbps 速度和半双工模式。
  - *10 全双工* - 10 Mbps 速度和全双工模式。
  - *100 半双工* - 100 Mbps 速度和半双工模式。
  - *100 全双工* - 100 Mbps 速度和全双工模式。
  - *1000 全双工* - 1000 Mbps 速度和全双工模式。
- **运行通告** - 显示当前发布到端口邻居的功能。*管理通告*字段中指定了以下可能的选项。
- **邻居通告** - 显示通过邻居设备 （链路伙伴）通告的功能。
- **背压** - 在端口上选择 “背压” 模式 （配合使用半双工模式），以降低交换机拥挤时的数据包接收速度。它会禁用远程端口，从而避免其通过拥堵信令来发送数据包。
- **流量控制** - 启用或禁用 802.3x 流量控制，或在端口上启用流量控制的自动协商（仅适用于全双工模式）。
- **MDI/MDIX** - 端口上的*介质相关接口* (MDI)/ *具有正反接线自适应功能的介质相关接口* (MDIX) 状态。

选项如下：

- *MDIX* - 选择该项可交换端口的传输和接收对。
- *MDIX* - 选择该选项可使用直通电缆将此交换机连接到工作站。
- *自动* - 选择该选项可将此交换机配置为为其他设备的连接自动检测正确的引出线。

- **运行 MDI/MDIX** - 显示当前的 MDI/MDIX 设置。

步骤 6 单击**应用**。*端口设置*将写入当前配置文件。

配置链路聚合

本节介绍如何配置 LAG。具体包括以下主题：

- **链路聚合概述**
- **静态和动态 LAG 工作流程**
- **定义 LAG 管理**
- **配置 LAG 设置**
- **配置 LACP**

链路聚合概述

链路聚合控制协议 (LACP) 是 IEEE 规格 (802.3az) 的一部分，可使您将多个物理端口捆绑在一起以形成单个逻辑通道 (LAG)。 LAG 可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。

支持两种类型的 LAG：

- *静态* - 如果在 LAG 上禁用了 LACP，则 LAG 为静态。分配给静态 LAG 的端口组始终为活动成员。手动创建 LAG 之后，无法添加或删除 LACP 选项，直到编辑 LAG 并删除一个成员 （应用之前可以添加）之后， LACP 按钮才会变为可编辑。
- *动态* - 如果在 LAG 上启用了 LACP，则 LAG 为动态。分配给动态 LAG 的端口组为候选端口。 LACP 可确定哪个候选端口为活动成员端口。非活动候选端口是准备替换任何失败的活动成员端口的*备用*端口。

负载均衡

转发到 LAG 的流量在活动成员端口上呈负载均衡状态，从而可获得接近于 LAG 的所有活动成员端口的聚合带宽的有效带宽。

LAG 的活动成员端口上的流量负载均衡由散列式分布函数管理，该函数可根据第 2 层或第 3 层数据包报头信息分布单播和组播流量。

交换机支持两种模式的负载均衡：

- **按 MAC 地址** - 根据所有数据包的目的和源 MAC 地址
- **按 IP 和 MAC 地址** - 根据 IP 数据包的目的和源 IP 地址以及非 IP 数据包的目的和源 MAC 地址。

LAG 管理

通常，系统会将 LAG 处理为单个逻辑端口。特别是， LAG 具有类似于普通端口的端口属性，例如状态和速度。

交换机支持 4 个 LAG。

每个 LAG 均具有以下特性：

- LAG 中的所有端口必须属于相同的介质类型。
- 要将端口添加到 LAG，该端口不能属于任何 VLAN （默认 VLAN 除外）。
- 不得将某 LAG 中的端口分配给其他 LAG。
- 为静态 LAG 最多分配八个端口，并且最多有 16 个端口可以作为动态 LAG 的候选端口。
- LAG 中的所有*端口*必须禁用自动协商，但是 *LAG* 可以启用自动协商。
- 将端口添加到 LAG 后， LAG 的配置将应用至该端口。从 LAG 中删除端口后，将重新应用其原始配置。
- 生成树等协议将 LAG 中的所有端口视作一个端口。

静态和动态 LAG 工作流程

手动创建 LAG 之后，无法添加或删除 LACP，直到编辑 LAG 并删除一个成员之后，LACP 按钮才会变为可编辑。

要配置**静态** LAG，请执行以下操作：

1. 在 LAG 上禁用 LACP 以将其变为静态。从**端口列表**中选择端口并将其移动到 **LAG 成员**列表，从而为静态 LAG 最多分配八个成员端口。选择 LAG 的负载均衡算法。在 *LAG 管理*页面中执行这些操作。
2. 使用 *LAG 设置*页面配置 LAG 的各个方面，例如速度和流量控制。

要配置**动态** LAG，请执行以下操作：

1. 在 LAG 上启用 LACP。使用 *LAG 管理*页面从**端口列表**中选择端口并将其移动到 **LAG 成员**列表，从而为动态 LAG 最多分配 16 个候选端口。
2. 使用 *LAG 设置*页面配置 LAG 的各个方面，例如速度和流量控制。
3. 使用 *LACP* 页面设置 LAG 中的 LACP 优先级和端口超时。

定义 LAG 管理

*LAG 管理*页面显示全局设置和每个 LAG 的设置。该页面还可使您在*编辑 LAG 成员关系*页面上配置全局设置并选择和编辑所需 LAG。

选择 LAG 的负载均衡算法的步骤：

步骤 1 单击**端口管理** > **链路聚合** > **LACP**。将打开 *LAG 管理*页面。

步骤 2 选择以下**负载均衡算法**之一：

- *MAC 地址* - 按所有数据包上的源和目的 MAC 地址执行负载均衡。
- *IP/MAC 地址* - 按 IP 数据包上的源和目的 IP 地址以及非 IP 数据包上的目的和源 MAC 地址执行负载均衡。

步骤 3 单击**应用**。负载均衡算法将写入当前配置文件。

在 LAG 中定义成员或候选端口的步骤：

步骤 1 选择要配置的 LAG，然后单击**编辑**。将打开*编辑 LAG 成员关系*页面。

步骤 2 为以下字段输入值：

- **LAG** - 选择 LAG 号。
- **LAG 名称** - 输入 LAG 名称或备注。
- **LACP** - 选择该选项可在选择的 LAG 上启用 LACP。此操作可使其成为动态 LAG。仅在将端口移动到下一字段中的 LAG 之后，才可启用此字段。
- **端口列表** - 将那些要分配给 LAG 的端口从**端口列表**移动到 **LAG 成员**列表中。可以为每个静态 LAG 最多分配八个端口，为动态 LAG 最多分配 16 个端口。

步骤 3 单击**应用**。 LAG 成员关系将写入当前配置文件。

配置 LAG 设置

*LAG 设置*页面显示所有 LAG 的当前设置表。您可以通过启动*编辑 LAG 设置*页面来配置所选 LAG 的设置并重新激活挂起的 LAG。

配置 LAG 设置或重新激活挂起的 LAG 的步骤：

步骤 1 单击**端口管理** > **链路聚合** > **LAG 设置**。将打开 *LAG 设置*页面。

步骤 2 选择一个 LAG，然后单击**编辑**。将打开*编辑 LAG 设置*页面。

步骤 3 为以下字段输入值：

- **LAG** - 选择 LAG ID 号。
- **说明** - 输入 LAG 名称或备注。
- **LAG 类型** - 显示组成 LAG 的端口类型。
- **管理状态** - 将选定的 LAG 设置为 “启用”或 “禁用”。
- **运行状态** - 显示 LAG 当前是否处于运行状态。
- **重新激活挂起的 LAG**- 选择该选项可重新激活端口 （如果已通过锁定端口安全性选项禁用 LAG）。

- **管理自动协商** - 在 LAG 上启用或禁用自动协商。自动协商是两个链路伙伴之间的协议，可使 LAG 向其伙伴通告自己的传输速率和流量控制 （流量控制默认为 *已禁用*）。建议在聚合链路的两端同时启用或同时禁用自动协商，从而确保链路速度保持一致。
- **运行自动协商** - 显示自动协商设置。
- **管理速度** - 选择 LAG 速度。
- **运行 LAG 速度** - 显示 LAG 运行时的当前速度。
- **自动通告** - 选择要由 LAG 通告的功能。选项如下：
  - *最大容量* - 所有 LAG 速度和两种双工模式均可用。
  - *10 全双工* - LAG 可通告 10 Mbps 速度，模式为全双工。
  - *100 全双工* - LAG 可通告 100 Mbps 速度，模式为全双工。
  - *1000 全双工* - LAG 可通告 1000 Mbps 速度，模式为全双工。
- **运行通告** - 显示“管理通告”状态。LAG 可将其功能通告给相邻的 LAG，以开始协商流程。*管理通告*字段中指定了以下可能值。
- **管理流量控制** - 在 LAG 上将 “流量控制”设置为**启用**或**禁用**，或者启用流量控制的**自动协商**。
- **运行流量控制** - 显示当前的流量控制设置。

步骤 4 单击**应用**。将更新当前配置文件。

配置 LACP

动态 LAG 启用了 LACP ； 在 LAG 中定义的每个候选端口上均运行 LACP。

LACP 优先级和规则

LACP 系统优先级和 LACP 端口优先级均用来确定哪些候选端口会成为配有八个以上候选端口的动态 LAG 中的活动成员端口。

LAG 中选择的候选端口全都连接到同一远程设备。本地交换机和远程交换机均具有 LACP 系统优先级。

以下算法用来确定 LACP 端口优先级来自本地设备还是来自远程设备：将本地 LACP 系统优先级与远程 LACP 系统优先级作比较。优先级最低的设备将控制 LAG 的候选端口选择。如果二者优先级相同，则会比较本地 MAC 地址和远程 MAC 地址。 MAC 地址优先级最低的设备将控制 LAG 的候选端口选择。

动态 LAG 最多可具有 16 个相同类型的以太网端口。最多可有八个端口处于活动状态，而处于备用模式的端口也不能超过八个。如果动态 LAG 中的端口数超过 8 个，链路控制端上的交换机将使用端口优先级来确定将哪些端口捆绑到 LAG 中，以及使哪些端口处于热备份模式。系统将忽略另一个交换机 （链路的非控制端）上的端口优先级。

以下是在动态 LACP 中选择活动端口或备用端口所使用的其他规则：

- 以不同于最高速活动成员的速度运行或以半双工模式运行的任何链路均处于备用状态。动态 LAG 中的所有活动端口均以相同波特率运行。
- 如果链路的端口 LACP 优先级低于当前活动的链路成员，并且活动成员的数量已达到最大数，则该链路将处于非活动状态和备用模式。

设置端口 LACP 参数设置

LACP 页面显示 LACP 系统优先级、 LACP 超时和 LACP 端口优先级的配置，还可使用该页面对这些项目进行配置。 LACP 超时是一种每端口参数，是发送和接收连续 LACP PDU 之间的时间间隔。在所有因素相同的情况下，当 LAG 配有的候选端口数大于活动端口允许的最大数时，交换机会从具有最高优先级的动态 LAG 中选择作为活动端口的端口。

注 LACP 设置与不是动态 LAG 成员的端口不相关。

定义 LACP 设置的步骤：

步骤 1 单击**端口管理** > **链路聚合** > **LACP**。将打开 *LACP* 页面。

步骤 2 输入 LACP 系统优先级。请参阅**配置 LACP**。

步骤 3 选择一个端口，然后单击**编辑**。将打开*编辑 LACP* 页面。

步骤 4 为以下字段输入值：

- **接口** - 选择要为其指定超时值或优先级值的端口号。
- **LACP 端口优先级** - 输入端口的 LACP 优先级值。请参阅**设置端口 LACP 参数设置**。
- **LACP 超时** - 选择以较快还是较慢的传输速度来定期传输 LACP PDU，具体取决于明确的 LACP 超时首选。

步骤 5 单击**应用**。将更新当前配置文件。

配置绿色以太网

本节介绍旨在节省交换机电源的绿色以太网功能。

其中包括以下各节内容：

- 绿色以太网概述
- 设置全局绿色以太网属性
- 设置绿色以太网端口属性

绿色以太网概述

绿色以太网是一组功能的通称，这些功能专为保护环境而设计，可降低设备的功耗。绿色以太网与 EEE 的不同之处在于，所有设备上都可启用绿色以太网电量检测，而 EEE 只能在千兆端口上启用。

绿色以太网功能通过以下方法降低总电能使用量：

- **电量检测模式** - 在非活动链路上，端口会转变为非活动模式，从而节省电能，同时使端口的管理状态保持 “启用” 状态。从此模式恢复为完全运行模式的过程既快速又明显，而且不会丢失任何帧。 GE 和 FE 端口均支持此模式。
- **短距模式** - 该功能可在长度较短的电缆上提供节能功能。分析电缆长度之后，将针对各种电缆长度调整电能使用量。如果电缆短于 50 米，则交换机将使用较少电能来通过电缆发送帧，从而节省能源。仅在 RJ45 GE 端口上支持此模式；此模式不会应用到组合端口。

  默认情况下，此模式为全局禁用状态。如果启用了 EEE 模式，则无法启用短距模式 （见下文）。

除了上述绿色以太网功能之外，还可在支持 GE 端口的设备上启用 **802.3az 节能以太网 (EEE)**。 EEE 可在端口上没有流量时降低功耗。请参阅 **802.3az 节能以太网功能**了解详情 （仅在 GE 模式下可用）。

默认情况下， EEE 为全局启用状态。在指定端口上，如果启用了 EEE，则将禁用短距模式。如果启用了短距模式， EEE 将变成灰色。

这些模式在每个端口进行配置，无需考虑端口的 LAG 成员关系。

设备 LED 是消耗电能的产品。设备在大多数时间都是处于闲置状态，因此让这些 LED 亮着是对能源的一种浪费。通过绿色以太网功能，您可以在不需要端口 LED （用于监控链路、速度和 PoE）时将其禁用，也可以在需要时 （调试、连接其他设备等）启用这些 LED。

在*系统摘要*页面上，设备板图片上显示的 LED 不受 LED 禁用的影响。

可以监控节能量、当前功耗和累计节省的电量。节能总量可看作物理接口若不在绿色以太网模式下运行而本应消耗的电能百分比。

显示的节能量仅为绿色以太网的节能量。不会显示 EEE 的节能量。

802.3az 节能以太网功能

本节介绍 802.3az 节能以太网 (EEE) 功能。

具体包括以下主题：

- **802.3az EEE 概述**
- **通告功能协商**
- **802.3az EEE 链路级发现**
- **802.3az EEE 的可用性**
- **默认配置**
- **功能之间的交互**
- **802.3az EEE 配置工作流程**

802.3az EEE 概述

802.3az EEE 旨在在链路上没有流量时节省能源。绿色以太网功能是在端口关闭时节省电量。使用 802.3az EEE，可在端口处于启用状态 （端口上没有流量）时节省能源。

仅在具有 GE 端口的设备上支持 802.3az EEE。

使用 802.3az EEE 时，链路两端的系统均可禁用部分自身功能，在没有流量时节省能源。

802.3az EEE 支持 IEEE 802.3 MAC 操作，速度为 100 Mbps 和 1000 Mbps：

LLDP 用于为两台设备选择最佳参数集。如果链路伙伴不支持 LLDP 或已禁用 LLDP，802.3az EEE 仍可运行，但可能不会处于最佳运行模式。

802.3az EEE 功能是通过使用名为低功耗闲置 (LPI) 模式的端口模式实施的。如果端口上没有流量并启用了该功能，则端口将被置于可大幅降低功耗的 LPI 模式。

连接的两端 （交换机端口和连接的设备）均必须支持 802.3az EEE，以便其顺利运行。没有流量时，两端均会发送信令，表示将要减低功耗。端口接收到来自两端的信令之后，“保持活动”信令表示端口处于 LPI 状态下 （未处于 “禁用”状态）并且已降低功耗。

要使端口一直处于 LPI 模式，必须从两端不断接收 “保持活动”信令。

通告功能协商

自动协商阶段，将通告 802.3az EEE 支持。使用自动协商，连接的设备可以检测链路另一端设备所支持的能力 （运行模式）、确定共用能力，并配置自身设置以便进行联合运行。自动协商可在连接时执行，可按照管理系统命令执行，也可以在检测到链接错误时执行。链路建立过程中，链路伙伴的双方将交换各自的 802.3az EEE 功能。在设备上启用自动协商之后，该功能可自动运行，无需用户交互。

> **注** 如果端口上未启用自动协商，那么将禁用 EEE。唯一的例外情况是，如果链路速度为 1GB，那么即使禁用了自动协商， EEE 仍将保持启用状态。

802.3az EEE 链路级发现

除了上述功能之外，还将根据 IEEE 标准 802.1AB 协议 (LLDP) 的附录 G 中定义的组织特定的 TLV，使用帧来通告 802.3az EEE 的功能和设置。 LLDP 用于完成自动协商后，进一步优化 802.3az EEE 运行。 802.3az EEE TLV 用来调整系统苏醒和刷新周期。

802.3az EEE 的可用性

请查看版本备注，获得支持 EEE 产品的完整列表。

默认配置

默认情况下， 802.3az EEE 和 EEE LLDP 处于全局启用和每端口启用状态。

功能之间的交互

以下内容将介绍 802.3az EEE 与其他功能的交互：

- 如果端口上未启用自动协商，那么将禁用 802.3az EEE 运行状态。唯一的例外情况是，如果链路速度为 1GB，那么即使禁用了自动协商， EEE 仍将保持启用状态。
- 如果已启用 802.3az EEE 且将启用端口，那么将根据端口苏醒时间的最大值立即开始工作。
- 在 GUI 上，如果选中端口上的 “短距模式” 选项，则该端口的 EEE 字段不可用。
- 如果将 GE 端口上的端口速度更改为 10Mbit，则将禁用 802.3az EEE。仅在 GE 模式下支持。

802.3az EEE 配置工作流程

本节介绍如何配置 802.3az EEE 功能，以及查看其计数器的方法。

步骤 1 打开**端口管理 > 端口设置**页面，确保已在端口上启用自动协商。

a. 选择一个端口，打开*编辑端口设置*页面。

b. 选择**自动协商**字段，确保已启用该字段。

步骤 2 确保 “端口管理” > “绿色以太网” > *属性*页面中的 **802.3 节能以太网 (EEE)** 已全局启用 （默认情况下，此功能处于启用状态）。该页面还会显示已节省的能源量。

步骤 3 打开 “绿色以太网” > *端口设置*页面，确保已在端口上启用 802.3az EEE。

a. 选择一个端口，打开*编辑端口设置*页面。

b. 在端口上选中 **802.3 节能以太网 (EEE)** 模式 （默认情况下，此功能处于启用状态）。

c. 在 **802.3 节能以太网 (EEE) LLDP** 中选择是否禁用通过 LLDP 通告 802.3az EEE 功能 （默认情况下，此功能处于启用状态）。

步骤 4 要在本地设备上查看与 802.3 EEE 相关的信息，请打开 *管理 > 发现 LLDP > LLDP 本地信息*页面，查看 802.3 节能以太网 (EEE) 部分中的信息。

步骤 5 要在远程设备上显示 802.3az EEE 的信息，请打开 *管理 > 发现 LLDP > LLDP 邻居信息*页面，查看 802.3 节能以太网 (EEE) 部分中的信息。

设置全局绿色以太网属性

*属性*页面显示交换机的绿色以太网模式配置，还可用来对该模式进行配置。它还会显示当前的节电量。

启用绿色以太网和 EEE 并查看节电量的步骤：

步骤 1 单击**端口管理** > **绿色以太网** > **属性**。将打开*属性*页面。

步骤 2 为以下字段输入值：

- **电量检测模式** - 默认情况下，此模式处于禁用状态。单击该复选框可启用此模式。
- **短距** - 如果交换机上有 GE 端口，则全局启用或禁用短距模式。

  注 如果启用了短距，则必须禁用 EEE。

- **节能** - 显示运行环保以太网和短距所节约的电能百分比。显示的节能量仅指短距模式和电量检测模式节约的电能。 EEE 节能量是以端口利用率为基础的，所以具有动态性，因而不会将其考虑在内。
- **累计节省的电量** - 显示自上一次重启交换机所节省的电量。每当出现影响节电量的事件时都会更新此值。
- **802.3 节能以太网 (EEE)** - 全局启用或禁用 EEE 模式。
- **端口 LED** - 选择该选项可启用端口 LED。如果将这些端口 LED 禁用，它们将无法显示链路状态、活动等。

步骤 3 单击**应用**。绿色以太网属性将写入当前配置文件。

设置绿色以太网端口属性

*端口设置*页面显示每个端口当前的绿色以太网和 EEE 模式，使用*编辑端口设置*页面可配置端口上的绿色以太网。要在端口上运行绿色以太网模式，必须在*属性*页面*中全局激活相应模式*。

请注意，屏幕仅显示具有 GE 端口的设备的 EEE 设置。仅在端口设置为自动协商时，EEE 才会运行。例外情况是，如果端口的速度为 1GB 或更高，那么即使已禁用自动协商， EEE 仍会运行。

定义每端口绿色以太网设置的步骤：

步骤 1 单击**端口管理** > **绿色以太网** > **端口设置**。将打开*端口设置*页面。

*端口设置*页面显示以下字段：

- **全局参数状态** - 描述启用的功能。

对于每个端口，系统将会列出以下字段：

- **端口** - 端口号。
- **电量检测** - 有关电量检测模式的端口状态：
  - *管理* - 显示是否启用了电量检测模式。
  - *运行* - 显示电量检测模式当前是否处于运行状态。
  - *原因* - 如果电量检测模式未处于运行状态，则显示原因。

- **短距** - 有关短距模式的端口状态：
  - *管理* - 显示是否启用了短距模式。
  - *运行* - 显示短距模式当前是否处于运行状态。
  - *原因* - 如果短距模式为处于运行状态，则显示原因。
  - *电缆长度* - 显示 VCT 返回的电缆长度 （以米为单位）。

  注 仅在 RJ45 GE 端口上支持短距模式；此模式不会应用到组合端口。
- **802.3 节能以太网 (EEE)** - 有关 EEE 功能的端口状态：
  - *管理* - 显示是否启用了 EEE 模式。
  - *运行* - 显示 EEE 目前是否在本地端口上运行。显示是否启用过此功能 （管理状态）、是否在本地端口上已启用此功能，以及此功能是否在本地端口上运行。
  - *LLDP 管理* - 显示是否启用了通过 LLDP 通告 EEE 计数器。
  - *LLDP 运行* - 显示当前是否正在运行通过 LLDP 通告 EEE 计数器。
  - *EEE 远程支持* - 显示链路伙伴上是否支持 EEE。本地和远程链路伙伴必须均支持 EEE。

  注 该窗口将显示各个端口的短距、电量检测和 EEE 设置；但是，除非已使用*属性*页面全局启用上述模式，否则这些模式在所有端口上均为禁用状态。要全局启用短距和 EEE，请参阅**设置全局绿色以太网属性**。

步骤 2 选择一个**端口**，然后单击**编辑**。*将打开编辑端口设置*页面。

步骤 3 选择在该端口上启用还是禁用电量检测模式。

步骤 4 如果设备上带有 GE 端口，选择在该端口上启用还是禁用短距模式。

步骤 5 如果设备上带有 GE 端口，选择在该端口上启用还是禁用 802.3 节能以太网 (EEE) 模式。

步骤 6 如果设备上带有 GE 端口，选择在该端口上启用还是禁用 802.3 节能以太网 (EEE) LLDP 模式 （通过 LLDP 通告 EEE 功能）。

步骤 7 单击**应用**。绿色以太网端口设置将写入当前配置文件。

10

智能端口

本文档介绍智能端口功能。

其中包含以下主题：

- 概述
- 什么是智能端口
- 智能端口类型
- 智能端口宏
- 宏失败和重置操作
- 智能端口功能如何运作
- 自动智能端口
- 错误处理
- 默认配置
- 与其他功能的关系和向后兼容性
- 常见智能端口任务
- 使用基于 Web 的界面配置智能端口
- 内置智能端口宏

概述

智能端口功能提供了一种简便的方法来保存和共享通用配置。通过将同一智能端口宏应用到多个接口，这些接口可以共享一组通用配置。

智能端口宏可按与宏关联的智能端口类型应用到接口。

可通过两种方法按智能端口类型将智能端口宏应用到接口：

- **静态智能端口** - 您可手动将智能端口类型分配到接口。最终将相应的智能端口宏应用到接口。
- **自动智能端口** - 自动智能端口会等待设备连接到接口，然后再应用配置。当从接口检测到设备时，会自动应用与连接设备的智能端口类型相对应的智能端口宏 （如果已分配）。

智能端口功能包含多种组件，并与交换机上的其他功能相互配合。这些组件和功能将在下文予以说明：

- 本节介绍了智能端口、智能端口类型和智能端口宏。
- **语音 VLAN** 一节中介绍了语音 VLAN 和智能端口。
- 分别在**配置 LLDP** 和**配置 CDP** 部分介绍了智能端口 LLDP 和智能端口 CDP。

此外，**常见智能端口任务**一节还将介绍典型工作流程。

什么是智能端口

智能端口是可应用内置宏的接口。这些宏旨在提供一种快速配置交换机的方法，从而支持通信要求并利用各种网络设备的功能。如果接口与 IP 电话、打印机或路由器和 / 或接入点 (AP) 连接，网络接入和 QoS 要求可能不同。

智能端口类型

智能端口类型是指已与智能端口连接或将与之连接的设备的类型。交换机支持以下智能端口类型：

- 打印机
- 台式机
- 访客
- 服务器
- 主机
- IP 摄像机
- IP 电话

- IP 电话 + 台式机
- 交换机
- 路由器
- 无线接入点

智能端口类型都进行命名，以便其描述与接口连接的设备类型。每种智能端口类型都与两个智能端口宏关联。其中一个宏称为 “宏”，用于应用所需的配置。另一个宏称为 “反宏”，用于在接口成为其他智能端口类型时，撤销 “宏” 执行的所有配置。

下表列出了智能端口类型和自动智能端口的关系

智能端口和自动智能端口类型

智能端口类型	得到自动智能端口支持	默认得到自动智能端口的支持
未知	否	否
默认	否	否
打印机	否	否
台式机	否	否
访客	否	否
服务器	否	否
主机	是	否
IP 摄像机	否	否
IP 电话	是	是
IP 电话台式机	是	是
交换机	是	是
路由器	是	否
无线接入点	是	是

特殊智能端口类型

有两种特殊的智能端口类型；*默认*和*未知*。这两种类型不与宏关联，但是它们存在的目的是显示与智能端口有关的接口状态。

以下是对这些特殊智能端口类型的介绍：

- **默认**

  本身未分配 （尚未分配）智能端口类型的接口具有 “默认”智能端口状态。

  如果自动智能端口已向接口分配智能端口类型，而该接口未配置为 “自动智能端口永久”状态，则其智能端口类型将在以下情况下重新初始化为 “默认”状态：

  - 在该接口上执行断开 / 连接操作。
  - 重启交换机。
  - 与该接口连接的所有设备都已过期，过期的定义是在规定的时间内，没有来自设备的 CDP 和 / 或 LLDP 通告。

- **未知**

  如果将智能端口宏应用到接口后发生错误，该接口将被分配 “未知”状态。这种情况下，智能端口和自动智能端口功能不会在该接口上运行，直到您修正错误，并应用 “重置”动作 （在*接口设置*页面执行）重新设置智能端口状态。

  有关故障排除的提示，请参阅**常见智能端口任务**一节中的工作流程部分。

注 在本节中，“过期”一词用来描述通过其 TTL 的 LLDP 和 CDP 消息。如果已启用自动智能端口同时禁用永久状态，且在最新 CDP 和 LLDP 数据包的 TTL 降为 0 之前不再接收 CDP 或 LLDP 消息，则反宏将运行，同时智能端口类型将返回默认值。

智能端口宏

智能端口宏是 脚本，用来为特定网络设备配置适宜的接口。

智能端口宏不能与全局宏混为一谈。全局宏对交换机进行全局配置，而智能端口宏的范围限于所应用的接口。

要查找宏源，可在*智能端口类型设置*页面上单击**查看宏源**按钮。

宏与对应的反宏相互配对，并与各智能端口类型相关联。宏应用配置，而反宏移除配置。

两个智能端口宏按照其名称配对，如下所示：

- macro_name （如：printer）
- no_macro_name （如：no_printer，智能端口宏打印机的反智能端口宏）

请参阅**内置智能端口宏**。

将智能端口类型应用到接口

将智能端口类型应用到接口后，智能端口类型和关联智能端口宏中的配置将保存在当前配置文件中。如果管理员将当前配置文件保存到启动配置文件中，交换机重启后会将智能端口类型和智能端口宏应用到接口，具体包括以下几种情况：

- 如果启动配置文件未为接口指定智能端口类型，它的智能端口类型将设为“默认”。
- 如果启动配置文件指定了静态智能端口类型，接口的智能端口类型将设为此静态类型。
- 如果启动配置文件指定了由自动智能端口动态分配的智能端口类型：
  - 如果已全部**启用**自动智能端口全局运行状态、接口自动智能端口状态和永久状态，智能端口类型将设为此动态类型。
  - 否则将应用对应的反宏，并且接口状态将设为 “默认”。

宏失败和重置操作

如果接口的现有配置与智能端口宏之间存在冲突，智能端口宏可能失败。

智能端口宏失败时，系统将发送包含以下参数的系统日志消息：

- 端口编号
- 智能端口类型
- 宏中失败 CLI 命令的行号

当接口上的智能端口宏失败时，该接口的状态将设为*未知*。失败原因可显示在*接口设置*页面、**显示诊断**弹出窗口上。

在确定问题来源并修正现有配置或智能端口宏之后，必须先对接口执行重置操作，然后才可重新应用智能端口类型 （在*接口设置*页面中）。有关故障排除的提示，请参阅**常见智能端口任务**一节中的工作流程部分。

智能端口功能如何运作

智能端口宏可按或与宏关联的智能端口类型应用到接口。

某些设备不允许使用 CDP 和 / 或 LLDP 进行搜索，系统会为与这些设备对应的智能端口类型提供支持，因此这些智能端口类型必须静态分配到所需的接口。要执行此操作，可导航至*智能端口接口设置*页面，选择所需接口的单选按钮，然后单击**编辑**。接着，选择想要分配的智能端口类型，根据需要调整参数，然后单击**应用**。

可通过两种方法按智能端口类型将智能端口宏应用到接口：

- **静态智能端口**

  您可手动将智能端口类型分配到接口。相应的智能端口宏会应用到接口。您可在*智能端口接口设置*页面手动将智能端口类型分配到接口。

- **自动智能端口**

  当从接口检测到设备时，会自动应用与连接设备的智能端口类型相对应的智能端口宏 （如果有）。自动智能端口默认在全局和接口层启用。

两种情况下，当从接口移除智能端口类型时系统都会运行关联的反宏，并且反宏会以完全相同的方式运行，从而移除所有的接口配置。

自动智能端口

为使自动智能端口自动向接口分配智能端口类型，必须在全局启用自动智能端口功能的同时还要在允许配置自动智能端口的相关接口上启用该功能。默认情况下，将启用自动智能端口并且允许配置所有接口。各接口分配的智能端口类型由各接口上分别接收的 CDP 和 LLDP 数据包决定。

- 如果多个设备与接口连接，适合所有设备的配置文件将应用到接口 （如果可能）。
- 如果设备已过期 （不再接收来自其他设备的通告），接口配置会根据其永久状态进行更改。如果已启用永久状态，接口配置将得以保留。如果未启用，智能端口类型将恢复为 “默认”。

启用自动智能端口

在*属性*页面上，可通过以下方法全局启用自动智能端口：

- **已启用** - 这将手动启用自动智能端口，并立即使其生效。
- **通过自动语音 VLAN 启用** - 如果已启用自动语音 VLAN 且其处于运行状态，通过该选项便可运行自动智能端口。“通过自动语音 VLAN 启用”是默认设置。

注 除全局启用自动智能端口外，您还必须在所需接口启用自动智能端口。默认情况下，所有接口都启用自动智能端口。

有关启用自动语音 VLAN 的详情，请参阅**语音 VLAN**

标识智能端口类型

如果全局启用自动智能端口 （在*属性*页面）并在某接口启用 （在*接口设置*页面）该功能，交换机会根据连接设备的智能端口类型，将智能端口宏应用到接口。自动智能端口会根据设备通告的 CDP 和 / 或 LLDP，获取连接设备的智能端口类型。

例如，如果 IP 电话与端口连接，它将传输 CDP 或 LLDP 数据包来通告其功能。在接收到这些 CDP 和 / 或 LLDP 数据包之后，交换机将获取适用于电话的智能端口类型，然后将对应的智能端口宏应用到连接 IP 电话的接口。

除非接口上已启用永久自动智能端口，否则，当连接设备过期、断开、重启或接收到冲突功能时，自动智能端口应用的智能端口类型和结果配置将被移除。过期次数由特定时间内，未收到设备的 CDP 和 / 或 LLDP 通告来决定。

使用 CDP/LLDP 信息标识智能端口类型

交换机根据 CDP/LLDP 功能检测与端口连接的设备类型。

该映射显示于以下各表中：

CDP 功能到智能端口类型的映射

功能名	CDP 位	智能端口类型
路由器	0x01	路由器
TB 网桥	0x02	无线接入点
SR 网桥	0x04	忽略
交换机	0x08	交换机
主机	0x10	主机

CDP 功能到智能端口类型的映射 （续）

功能名	CDP 位	智能端口类型
IGMP 有条件过滤	0x20	忽略
中继器	0x40	忽略
VoIP 电话	0x80	ip_phone
远程管理设备	0x100	忽略
CAST 电话端口	0x200	忽略
二端口 MAC 中继	0x400	忽略

LLDP 功能到智能端口类型的映射

功能名	LLDP 位	智能端口类型
其他	1	忽略
中继器 IETF RFC 2108	2	忽略
MAC 网桥 IEEE 标准 802.1D	3	交换机
WLAN 接入点 IEEE 标准 802.11 MIB	4	无线接入点
路由器 IETF RFC 1812	5	路由器
电话 IETF RFC 4293	6	ip_phone
DOCSIS 电缆设备 IETF RFC 4639 和 IETF RFC 4546	7	忽略
仅站 IETF RFC 4293	8	主机
VLAN 网桥 IEEE 标准的 C-VLAN 组件 802.1Q	9	交换机
VLAN 网桥 IEEE 标准的 S-VLAN 组件 802.1Q	10	交换机
二端口 MAC 中继 (TPMR) IEEE 标准 802.1Q	11	忽略
保留	12-16	忽略

注 仅当设定 IP 电话和主机位之后，智能端口类型才可为 ip_phone_desktop。

多设备与端口连接

交换机通过连接设备在其 CDP 和 / 或 LLDP 数据包中通告的功能，来获取设备的智能端口类型。

如果多个设备通过某个接口与交换机连接，自动智能端口将考虑通过该接口接收的每个功能通告，以便分配正确的智能端口类型。类型分配根据以下算法进行：

- 如果接口上的所有设备都通告相同的功能 （无冲突），交换机会将匹配的智能端口类型应用到接口。
- 如果其中某个设备是交换机，将使用*交换机*智能端口类型。
- 如果其中某个设备是接入点，将使用*无线接入点*智能端口类型。
- 如果其中某个设备是 IP 电话，而另一个设备是主机，将使用 *ip_phone_desktop* 智能端口类型。
- 如果其中某个设备是 IP 电话台式机，而另一个设备是 IP 电话或主机，将使用 *ip_phone_desktop* 智能端口类型。
- 其他所有情况下都将使用默认智能端口类型。

有关 LLDP/CDP 的详情，请分别参阅**配置 LLDP** 和**配置 CDP** 部分。

永久自动智能端口接口

如果已在接口上启用永久状态，即使在连接设备过期、接口关闭以及交换机重启 （假设配置已保存）后，自动智能端口已动态应用的接口智能端口类型和配置仍将得到保留。除非自动智能端口检测到具有其他智能端口类型的连接设备，否则接口的智能端口类型和配置不会发生更改。如果接口禁用永久状态，当与其连接的设备过期、接口关闭或交换机重启后，该接口将恢复为默认智能端口类型。接口启用永久状态后将消除设备检测延迟，否则该延迟将不可避免。

注 只有当应用于接口的、具有智能端口类型的当前配置保存到启动配置文件中时，应用到接口的智能端口类型的永久状态在重启后才会有效。

错误处理

当智能端口宏应用到接口失败后，可在*接口设置*页面检查故障点，并可在通过*接口设置*和*接口设置编辑*修正错误之后，重置端口并重新应用该宏。

默认配置

智能端口始终可用。默认情况下，自动智能端口由自动语音 VLAN 启用，并依靠 CDP 和 LLDP 检测连接设备的智能端口类型，同时检测智能端口类型 IP 电话、IP 电话 + 台式机、交换机和无线接入点。

有关语音出厂默认设置的说明，请参阅**语音 VLAN**。

与其他功能的关系和向后兼容性

交换机默认启用自动智能端口，也可禁用该功能。电话 OUI 无法与自动智能端口及自动语音 VLAN 同时运行。要启用电话 OUI，必须先禁用自动智能端口。

常见智能端口任务

本节介绍一些设置智能端口和自动智能端口的常见任务。

工作流程 1：*要在交换机上全局启用自动智能端口，以及在端口上配置自动智能端口，请执行以下步骤：*

步骤 1 要在交换机上启用自动智能端口功能，请打开*智能端口 > 属性*页面。将**管理自动智能端口**设为**启用**或**通过语音 VLAN 启用**。

步骤 2 选择是否要使交换机处理来自连接设备的 CDP 和 / 或 LLDP 通告。

步骤 3 在**自动智能端口设备检测**字段中选择将要检测的设备类型。

步骤 4 单击**应用**

步骤 5 要在一个或多个接口上启用启用自动智能端口功能，请打开*智能端口 > 接口设置*页面。

步骤 6 选择接口，然后单击**编辑**。

步骤 7 在**智能端口应用**字段中选择自动智能端口。

步骤 8 必要时选中或取消选中**永久状态**。

步骤 9 单击**应用**。

工作流程 2：要将接口配置为静态智能端口，请执行以下步骤：

步骤 1 要在接口上启用自动智能端口功能，请打开*智能端口 > 接口设置*页面。

步骤 2 选择接口，然后单击**编辑**。

步骤 3 在**智能端口应用**字段中选择要分配给接口的智能端口类型。

步骤 4 根据需要设置宏参数。

步骤 5 单击**应用**。

工作流程 3：要调整智能端口宏参数默认值，请执行以下步骤：

通过该步骤，您可完成以下操作：

- 查看宏源。
- 更改参数默认值。
- 将参数默认值恢复为出厂设置。

1. 打开*智能端口 > 智能端口类型设置*页面。
2. 选择智能端口类型。
3. 单击**查看宏源**，查看与所选智能端口类型关联的当前智能端口宏。
4. 单击**编辑**以打开一个新窗口，在该窗口中您可修改与该智能端口类型绑定的宏中的默认参数值。当自动智能端口将所选智能端口类型 （如适用）应用到某接口时，将使用这些参数默认值。
5. 在*编辑*页面中，修改字段。
6. 如果参数已更改，单击**应用**重新运行宏；或在必要时单击**恢复默认设置**，恢复内置宏的默认参数值。

工作流程 4：要在智能端口宏失败后重新运行，请执行以下步骤：

步骤 1 在*接口设置*页面，选择一个智能端口类型为 “未知”的接口。

步骤 2 单击**显示诊断**查看问题。

步骤 3 排除故障，然后修正问题。请参阅下文中的故障排除提示。

步骤 4 单击**编辑**。系统将打开一个新窗口，您可在其中单击**重置**以重新设置接口。

步骤 5 返回主页面并使用**重新应用**（适用于非交换机、路由器或 AP 的设备）或**重新应用智能端口宏**（适用于交换机、路由器或 AP）重新应用该宏，从而实现该智能端口宏在接口上的运行。

第二种重置单一或多个未知接口的方法是：

步骤 1 在*接口设置*页面中，选择与复选框*相同的端口类型*。

步骤 2 选择*未知*，然后单击**转至**。

步骤 3 单击**重置所有未知智能端口**。然后，按上述重新应用该宏。

提示 该宏运行失败的原因可能是与在应用该宏之前所进行的配置间存在冲突（最经常遇到的是与安全性和风暴控制设置间的冲突）、端口类型错误、用户定义的宏中有错字或错误命令，以及无效的参数设置。在尝试应用宏之前未选中类型及边界参数，因此在应用宏时，输入错误或无效的参数值几乎必然会导致失败。

使用基于 Web 的界面配置智能端口

智能端口功能在*智能端口 > 属性*、*智能端口类型设置*和*接口设置*页面中进行配置。

有关语音 VLAN 配置的信息，请参阅**语音 VLAN**。

有关 LLDP/CDP 配置的信息，请分别参阅**配置 LLDP** 和**配置 CDP** 部分。

智能端口属性

全局配置智能端口功能的步骤：

步骤 1 单击**智能端口 > 属性**。系统将打开*属性页面*。

步骤 2 输入参数。

- **管理自动智能端口** - 选中后将全局启用或禁用自动智能端口。可能的选项有：
  - *禁用* - 选中后，将在设备上禁用自动智能端口。
  - *启用* - 选中后，将在设备上启用自动智能端口。

- *通过自动语音 VLAN 启用* - 选中该选项后将启用自动智能端口，但是只有在启用自动语音 VLAN 并使之运行后，自动智能端口才能正常运行。“通过自动语音 VLAN 启用”是默认设置。

- **自动智能端口设备检测方法** - 选择是否使用传入 CDP、 LLDP 类型的数据包（或同时使用两种）检测连接设备的智能端口类型。要使自动智能端口可对设备进行标识，必须至少选中一个类型。
- **运行 CDP 状态** - 显示 CDP 的运行状态。要使自动智能端口根据 CDP 通告检测智能端口类型，请启用 CDP。
- **运行 LLDP 状态** - 显示 LLDP 的运行状态。要使自动智能端口根据 LLDP/LLDP-MED 通告检测智能端口类型，请启用 LLDP。
- **自动智能端口设备检测** - 选择各种设备类型，自动智能端口会将智能端口类型分配到这些设备的接口。如果未选中，则自动智能端口不会将该智能端口类型分配到任何接口。

步骤 3 单击**应用**。这将在交换机上设置全局智能端口参数。

智能端口类型设置

使用*智能端口类型设置*页面，编辑智能端口类型设置并查看宏源。

默认情况下，每种智能端口类型都与一对内置智能端口宏相关联。要进一步了解有关宏与反宏的信息，请参阅**智能端口类型**。内置宏或用户定义的宏可以有参数。内置宏最多可有三个参数。

在*智能端口类型设置*页面中，编辑智能端口类型的这些参数 （由自动智能端口应用），会对这些参数的默认值进行配置。自动智能端口将使用这些默认值。

注 如果自动智能端口已将自动智能端口类型分配给接口，则更改该类型将会使新设置应用到这些接口中。在这种情况下，绑定无效的宏或设置无效的默认参数值会导致所有此智能端口类型的端口都变为未知。

步骤 1 单击**智能端口 > 智能端口类型设置**。系统将打开*智能端口类型设置*页面。

步骤 2 要查看与某智能端口类型关联的智能端口宏，请选择该智能端口类型，然后单击**查看宏源**。

步骤 3 要修改宏的参数，请选择智能端口类型，然后单击**编辑**。系统将打开*编辑智能端口类型设置*页面。

步骤 4 输入以下字段。

- **端口类型** - 选择一种智能端口类型。
- **宏名称** - 显示当前与该智能端口类型关联的智能端口宏的名称。
- **宏参数** - 在宏中显示以下三种参数的字段：
  - *参数名称* - 宏中的参数名称。
  - *参数值* - 宏中的当前参数值。可在此更改该值。
  - *参数说明* - 参数说明。

  可通过单击**恢复默认设置**来恢复默认参数值。

步骤 5 单击**应用**，将更改保存到当前配置。如果修改与智能端口类型关联的智能端口宏和 / 或它的参数值，自动智能端口会自动将该宏重新应用到当前已获得由自动智能端口分配的智能端口类型的接口。自动智能端口不会将更改应用到通过静态分配方式获得智能端口类型的接口。

注 因为宏参数不存在类型关联，因此无法验证宏参数。此时，输入任何值都是有效的。但是，当将智能端口类型分配到接口并应用关联的宏时，无效的参数值可能导致出错。

智能接口设置

使用*接口设置*页面可执行以下任务：

- 将特定智能端口类型静态应用到接口 （具有接口特定的宏参数值）。
- 在接口上启用自动智能端口。
- 对应用失败并导致智能端口类型变为未知的智能端口宏进行诊断。
- 智能端口宏运行失败后，将其重新应用到以下其中一种接口类型：交换机、路由器和 AP。单击**重新应用**之前，应进行必要的修正。有关故障排除的提示，请参阅**常见智能端口任务**一节中的工作流程部分。
- 将智能端口宏重新应用到接口。在某些情况下，您可能需要重新应用智能端口宏，以便接口上的配置保持最新。例如，在交换机接口上重新应用交换机智能端口宏，将使该接口成为自上次应用宏之后创建的 VLAN 的一个成员。您必须熟悉交换机上的当前配置以及宏的定义，以便确定重新应用宏是否会对接口产生任何影响。
- 重置未知接口。这将使未知接口模式设置为默认模式。

应用智能端口宏的步骤：

步骤 1 单击**智能端口 > 接口设置**。系统将打开*接口设置*页面。

可通过以下方式重新应用关联智能端口宏：

- 选择一组智能端口类型 （交换机、路由器或 AP），然后单击**重新应用智能端口宏**。宏随即会应用到所有选中的接口类型。
- 选择一个处于连接状态的接口，然后单击**重新应用**以重新应用最近应用到该接口的宏。

  该**重新应用**操作还会将该接口添加到所有新创建的 VLAN。

步骤 2 智能端口诊断。

如果智能端口宏失败，接口的智能端口类型将为 “未知”。选择未知类型的接口，然后单击**显示诊断**。这会显示导致宏应用失败的命令。有关故障排除的提示，请参阅**常见智能端口任务**一节中的工作流程部分。纠正该问题后，继续重新应用宏。

步骤 3 将所有未知接口重置为默认类型。

- 选择与复选框*相同的端口类型*。
- 选择*未知*，然后单击**转至**。
- 单击**重置所有未知智能端口**。然后，按上述重新应用该宏。这样便会在所有类型为 “未知”的接口上执行重置，这也就意味着所有接口将返回到默认类型。修正宏错误或当前接口配置错误 （或二者皆有）后，可应用新宏。

注 重置未知类型的接口不会重置失败宏所执行的配置。此操作必须通过手动进行。

将智能端口类型分配到接口或在接口上激活自动智能端口的步骤：

步骤 1 选择一个接口，然后单击**编辑**。系统将打开*编辑接口设置*页面。

步骤 2 输入以下字段。

- **接口** - 选择端口或 LAG。
- **智能端口类型** - 显示当前分配到端口 /LAG 的智能端口类型。
- **智能端口应用** - 从智能端口应用下拉菜单中选择智能端口类型。
- **智能端口应用方法** - 如果选中自动智能端口，自动智能端口将根据从连接设备接收的 CDP 和 / 或 LLDP 通告，自动分配智能端口类型，同时应用相应的智能端口宏。要将智能端口类型静态分配给接口并应用相应的智能端口宏，请选择所需的智能端口类型。

- **永久状态** - 选中后将启用永久状态。如果启用，即使接口关闭或交换机重启，智能端口类型仍会与接口关联。仅当接口的智能端口应用为 “自动智能端口” 时，永久状态才适用。接口启用永久状态后将消除设备检测延迟，否则该延迟将不可避免。
- **宏参数** - 在宏中至多显示以下三种参数的字段：
  - *参数名称* - 宏中的参数名称。
  - *参数值* - 宏中的当前参数值。可在此更改该值。
  - *参数说明* - 参数说明。

步骤 3 单击**重置**可将处于 “未知” 状态 （由未成功应用宏所致）的接口设置为默认接口。该宏可在主页面上重新应用。

步骤 4 单击**应用**更新更改，并将智能端口类型分配到接口。

内置智能端口宏

下文介绍各智能端口类型的内置宏对。每种智能端口类型都有一个用于配置接口的宏，以及一个用于移除配置的反宏。

在此提供以下智能端口类型的宏代码：

- **台式机**
- **打印机**
- **访客**
- **服务器**
- **主机**
- **ip_camera**
- **ip_phone**
- **ip_phone_desktop**
- **交换机**
- **路由器**
- **接入点**

台式机

```
[台式机]
#interface configuration, for increased network security and reliability when
connecting a desktop device, such as a PC, to a switch port.
#macro description Desktop
#macro keywords $native_vlan $max_hosts
#
#macro key description:$native_vlan:将在端口上配置的 Untagged VLAN
#                          $max_hosts:端口上允许设备的最大数量
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_desktop

```
[no_desktop]
#macro description No Desktop
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

打印机

```
[ 打印机 ]
#macro description printer
#macro keywords $native_vlan
#
#macro key description:$native_vlan: 将在端口上配置的 Untagged VLAN
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_printer

```
[no_printer]
#macro description No printer
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

guest

```
[ 访客 ]
#macro description guest
#macro keywords $native_vlan
#
#macro key description:$native_vlan: 将在端口上配置的 Untagged VLAN
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_guest]]

```
[no_guest]
#macro description No guest
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

服务器

```
[ 服务器 ]
#macro description server
#macro keywords $native_vlan $max_hosts
#
#macro key description:$native_vlan: 将在端口上配置的 Untagged VLAN
#                          $max_hosts: 端口上允许设备的最大数量
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_server

```
[no_server]
#macro description No server
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
spanning-tree portfast auto
#
@
```

主机

```
[ 主机 ]
#macro description host
#macro keywords $native_vlan $max_hosts
#
#macro key description:$native_vlan: 将在端口上配置的 Untagged VLAN
#                          $max_hosts: 端口上允许设备的最大数量
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_host

```
[no_host]
#macro description No host
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_camera

```
[ip_camera]
#macro description ip_camera
#macro keywords $native_vlan
#
#macro key description:$native_vlan: 将在端口上配置的 Untagged VLAN
#Default Values are
#$native_vlan = Default VLAN
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_camera

```
[no_ip_camera]
#macro description ip_camera
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone

```
[ip_phone]
#macro description ip_phone
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:$native_vlan: 将在端口上配置的 Untagged VLAN
#                          $voice_vlan: 语音 VLAN ID
#                          $max_hosts: 端口上允许设备的最大数量
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone

```
[no_ip_phone]
#macro description no ip_phone
#macro keywords $voice_vlan
#
#macro key description:$voice_vlan: 语音 VLAN ID
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
```

```
spanning-tree portfast auto
#
@
```

ip_phone_desktop

```
[ip_phone_desktop]
#macro description ip_phone_desktop
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:$native_vlan:将在端口上配置的 Untagged VLAN
#                          $voice_vlan:语音 VLAN ID
#                          $max_hosts:端口上允许设备的最大数量
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone_desktop

```
[no_ip_phone_desktop]
#macro description no ip_phone_desktop
#macro keywords $voice_vlan
#
#macro key description:$voice_vlan:语音 VLAN ID
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
```

```
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

交换机

```
[ 交换机 ]
#macro description switch
#macro keywords $native_vlan $voice_vlan
#
#macro key description:$native_vlan: 将在端口上配置的 Untagged VLAN
#                          $voice_vlan: 语音 VLAN ID
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
#
@
```

no_switch

```
[no_switch]
#macro description No switch
#macro keywords $voice_vlan
#
#macro key description:$voice_vlan: 语音 VLAN ID
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

路由器

```
[ 路由器 ]
#macro description router
#macro keywords $native_vlan $voice_vlan
#
#macro key description:$native_vlan: 将在端口上配置的 Untagged VLAN
#                          $voice_vlan: 语音 VLAN ID
#
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree link-type point-to-point
#
@
```

no_router

[no_router]

#macro description No router

#macro keywords $voice_vlan

#

#macro key description:$voice_vlan: 语音 VLAN ID

#

no smartport switchport trunk native vlan

smartport switchport trunk allowed vlan remove all

#

no smartport storm-control broadcast enable

no smartport storm-control broadcast level

#

no spanning-tree link-type

#

@

接入点

```
[ 接入点 ]
#macro description ap
#macro keywords $native_vlan $voice_vlan
#
#macro key description:$native_vlan: 将在端口上配置的 Untagged VLAN
#                          $voice_vlan: 语音 VLAN ID
#
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
#
@
```

no_ap

```
[no_ap]
#macro description No ap
#macro keywords $voice_vlan
#
#macro key description:$voice_vlan: 语音 VLAN ID
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

11

管理以太网供电设备

以太网供电 (PoE) 功能仅在基于 PoE 的设备上提供。如需基于 PoE 的设备列表，请参阅 “**交换机型号**”一节。

本节介绍如何使用 PoE 功能。

具体包括以下主题：

- **交换机上的 PoE**
- **配置 PoE 属性**
- **配置 PoE 功率、优先级和类别**

交换机上的 PoE

PoE 交换机为 PSE （供电设备），可通过现有的铜质电缆为连接的 PD （受电设备）供电，而不会影响网络流量，也无需更新物理网络或修改网络基础架构。

有关各种型号上 PoE 支持的信息，请参阅**交换机型号**。

PoE 功能

PoE 有如下功能：

- 可消除为有线 LAN 上的所有设备输送 110/220 V AC 电能的需求。
- 可消除将所有网络设备靠近电源放置的必要性。
- 可消除在企业中部署双线系统的需求，大大降低安装成本。

只要企业网络部署连接到以太网 LAN 的功率相对较低的设备，就可以使用以太网供电，这类低功率设备包括：

- IP 电话
- 无线接入点
- IP 网关
- 音频和视频远程监控设备

PoE 工作

PoE 分以下几个阶段实施：

- 检测 - 在铜质电缆上发送特殊脉冲。如果另一端连接了 PoE 设备，该设备会对这些脉冲做出响应。
- 分类 - 检测阶段结束后，开始供电设备 (PSE) 与受电设备 (PD) 之间的协商。在协商过程中， PD 指定其类别，这是 PD 所耗的最大功率。
- 功率消耗 - 分类阶段结束后，PSE 将为 PD 供电。如果 PD 支持 PoE，但未进行分类，则会将其假设为类别 0 （最大）。如果 PD 尝试消耗的功率超过了标准所允许的最大功率，则 PSE 会停止为该端口供电。

PoE 支持两种模式：

- 端口限制 - 交换机同意提供的最大功率取决于系统管理员配置的值，与分类结果无关。
- 类别功率限制 - 交换机同意提供的最大功率取决于分类阶段的结果。这表示将根据客户端的请求设置最大功率。

PoE 配置注意事项

使用 PoE 功能需要考虑两个因素：

- PSE 可以提供的功率
- PD 实际尝试消耗的功率

您可以决定：

- 允许 PSE 向 PD 提供的最大功率
- 在设备工作期间，将模式从类别功率限制更改为端口限制及从端口限制更改为类别功率限制。会保留为端口限制模式配置的针对端口的功率值。

- 所允许的针对端口的最大端口限制 （以 mW 为单位的数值限制），限于端口限制模式。
- 当 PD 尝试消耗过多功率时生成 Trap，以及生成 Trap 时 PD 所耗功率占最大功率的百分比。

PoE 特定硬件会自动检测 PD 类别，并根据连接到每个特定端口的设备的类别检测其功率限制 （限于类别限制模式）

如果在连接的任意时刻，所连接的 PD 从交换机请求超过所配置的功率分配所允许的功率 （不论交换机是类别限制模式还是端口限制模式），交换机将：

- 维持 PoE 端口链路的连接 / 中断状态
- 停止向 PoE 端口供电
- 记录停止供电的原因
- 生成到远程日志服务器的 Trap

注意 连接能够提供 PoE 的交换机时，请考虑以下事项：

PoE 型号的 Sx200、 Sx300 和 Sx500 系列交换机均为 PSE （供电设备），能够为连接 PD （受电设备）提供直流电源。这些设备包括 VoIP 电话、 IP 摄像机和无线接入点。 PoE 交换机可以为准标准传统 PoE 受电设备检测并提供电源。由于支持传统 PoE，因此用作 PSE 的 PoE 交换机可能会为连接 PSE（包括作为传统 PD 的其他 PoE 交换机）检测和提供电源时出错。

即使 Sx200/300/500 PoE 交换机为 PSE 并因此而应采用交流供电，但是因为会发生错误检测，所以这些交换机可作为传统 PD 由其他 PSE 为其供电。如果发生这种情况， PoE 交换机可能无法正常运作，并且可能无法为其连接 PD 正常供电。

为防止发生错误检测，您应该在用于连接 PSE 的 PoE 交换机的端口上禁用 PoE。还应该首先为 PSE 设备接通电源，然后再将其连接到 PoE 交换机。如果某设备被错误检测为 PD，您应该断开该设备与 PoE 端口的连接，并使用交流电源为该设备循环供电，然后再重新连接其 PoE 端口。

配置 PoE 属性

*PoE 属性*页面可选择采用端口限制还是类别限制 PoE 模式，及指定生成 PoE Trap。

这些设置需提前输入。当 PD 实际连接并消耗功率时，所消耗的功率可能比所允许的最大功率少得多。

在加电重启、初始化和系统配置过程中禁用功率输出，以确保不会损坏 PD。

在交换机上配置 PoE 和监控当前功率使用的步骤：

步骤 1 单击**端口管理 > PoE > 属性**。将打开 *PoE 属性*页面。

步骤 2 为以下字段输入值：

- **供电模式** - 请选择以下选项之一：
  - *端口限制* - 由用户配置针对每个端口的最大功率限制。
  - *类限制* - 由设备类别 （从分类阶段获取）决定每个端口的最大功率限制。
- **陷阱** - 启用或禁用系统日志 Trap。
- **功率 Trap 阈值** - 输入使用率阈值，该值为功率限制的百分比。如果功率超过了该值，便会发出告警。

将为每台设备显示以下计数器：

- **标称功率** - 交换机可以为连接的所有 PD 提供的总功率。
- **已消耗功率** - 当前由 PoE 端口消耗的功率。
- **可用功率** - 标称功率减去已消耗的功率所得的值。

步骤 3 单击**应用**，保存 PoE 属性。

配置 PoE 功率、优先级和类别

*PoE 设置*页面会显示关于在接口上启用 PoE 和监控每个端口的当前功率使用和最大功率限制的系统 PoE 信息。

单击**端口管理 > PoE > 设置**。将打开 *设置*页面。

本页面会根据供电模式，通过两种方式限制每个端口的功率：

- **端口限制**：将功率限制为指定的瓦特数。要使这些设置生效，系统必须为 PoE 端口限制模式。该模式在 *PoE 属性*页面中进行配置。

  当端口消耗的功率超过端口限制时，将会停止为端口供电。

- **类别限制**：根据连接的 PD 的类别限制功率。要使这些设置生效，系统必须为 PoE 类别限制模式。该模式在 *PoE 属性*页面中进行配置。

  当端口消耗的功率超过类别限制时，将会停止为端口供电。

PoE 优先级示例：

假设：一个 48 端口交换机提供 375 瓦的总功率。

管理员将所有端口配置为最大可分配 30 瓦。这样一来， 48 个端口乘以 30 瓦就等于 1440 瓦，这个数字显然是太大了。交换机无法为每个端口提供足够的功率，因此会根据优先级提供功率。

管理员针对每个端口设置优先级，为其分配可获得的功率量。

这些优先级在 *PoE 设置*页面中输入。

有关支持 PoE 的交换机型号以及可向 PoE 端口分配的最大功率说明，请参阅**交换机型号**。

配置 PoE 端口设置的步骤：

步骤 1 单击**端口管理 > PoE > 设置**。将打开 *设置*页面。下面的列表中是关于 “端口限制” 供电模式的字段。如果供电模式为 “级别限制”，这些字段会略有不同。

步骤 2 选择一个端口，然后单击**编辑**。将打开 *编辑 PoE 设置*页面。下面的列表中是关于 “端口限制” 供电模式的字段。如果供电模式为 “级别限制”，这些字段会略有不同。

步骤 3 为以下字段输入值：

- **接口** - 选择要配置的端口。
- **PoE 管理状态** - 在端口上启用或禁用 PoE。
- **电源优先级** - 选择供电不足时使用的端口优先级：低、高或重要。例如，如果供电使用率在 99%，端口 1 的优先级为高，而端口 3 的优先级为低，则将为端口 1 供电，而拒绝为端口 3 供电。
- **管理功率分配** - 仅当在 *PoE 属性*页面中将供电模式设置为 “端口限制” 才会显示该字段。如果供电模式为 “功率限制”，则请输入为该端口分配的功率 （以毫瓦为单位）。

- **最大功率分配** - 显示在此端口上所允许的最大功率。
- **类** - 仅当在 *PoE 属性*页面中将供电模式设置为 “类限制”才会显示该字段。类别将决定功率等级：

类别	交换机端口提供的最大功率
0	15.4 瓦特
1	4.0 瓦特
2	7.0 瓦特
3	15.4 瓦特
4	30.0 瓦特

- **功耗** - 显示分配给连接到所选接口的受电设备的功率 （以毫瓦为单位）。
- **过载计数器** - 显示功率过载情况发生的总次数。
- **短路计数器** - 显示功率不足情况发生的总次数。
- **拒绝供电计数器** - 显示拒绝为受电设备供电情况发生的次数。
- **缺席计数器** - 显示由于检测不到受电设备，而停止为其供电的情况发生的次数。
- **无效签名计数器** - 显示收到无效签名的次数。PSE 需通过签名来识别受电设备。签名在受电设备的检测、分类或维护过程中生成。

步骤 4 单击**应用**。端口的 PoE 设置将写入当前配置文件。

12

VLAN 管理

本节包括以下主题：

- VLAN
- 配置默认 VLAN 设置
- 创建 VLAN
- 配置 VLAN 接口设置
- 定义 VLAN 成员关系
- 语音 VLAN

VLAN

VLAN 是一个端口逻辑组，与其相关联的设备不论连接到桥接网络的哪个物理 LAN 段，都可以通过以太网 MAC 层互相通信。

VLAN 说明

系统使用会 1 到 4094 之间的值为每个 VLAN 配置一个唯一的 VID (VLAN ID)。如果桥接网络中的设备上的端口能够向 VLAN 发送数据并从 VLAN 接收数据，则该端口便为该 VLAN 的成员。如果进入 VLAN 的指定给某端口的所有数据包都不包含 VLAN 标记，则该端口为 VLAN 的 Untagged 成员。如果进入 VLAN 的指定给某端口的所有数据包都包含 VLAN 标记，则该端口为 VLAN 的 Tagged 成员。一个端口可以是一个 Untagged VLAN 或多个 Tagged VLAN 的成员。

处于 “VLAN 访问”模式的端口只能是一个 VLAN 的成员。处于 “一般”模式或 “中继”模式的端口可以是一个或多个 VLAN 的成员。

VLAN 解决了安全性和可扩展性问题。从 VLAN 发送的流量会始终处于 VLAN 之内，并且终止于 VLAN 中的设备。 VLAN 通过逻辑方式连接设备，无需实际改变这些设备的位置，因此还可以简化网络配置。

如果帧为 VLAN-tagged 帧，则会将一个 4 字节的 VLAN 标签添加到每个以太网帧。该标签中包含一个 1 到 4094 之间的 VLAN ID 和一个 0 到 7 之间的 VLAN 优先级标签 (VPT)。有关 VPT 的详情，请参阅**配置服务质量**。

当帧进入可识别 VLAN 的设备时，设备会根据帧中的 4 字节 VLAN 标记将该帧分类为属于某个 VLAN。

如果帧中不包含 VLAN 标记，或者仅为帧添加了优先级标记，则会根据于接收帧的入站端口处配置的 PVID （端口 VLAN 标识符）将该帧分类为属于某个 VLAN。

如果启用了入站过滤功能，并且入站端口不是数据包所属 VLAN 的成员，则此帧将于入站端口处被丢弃。仅当帧的 VLAN 标记中的 VID 为 0 时，才会将该帧视为添加了优先级标记。

属于某 VLAN 的帧会始终处于该 VLAN 之内。这可以通过仅向作为目的 VLAN 成员的出站端口发送或转发帧来实现。出站端口可以是 VLAN 的 Tagged 成员或 Untagged 成员。

出站端口：

- 如果出站端口是目的 VLAN 的 Tagged 成员，并且原始帧不包含 VLAN 标记，则会为此帧添加 VLAN 标记。
- 如果出站端口是目的 VLAN 的 Untagged 成员，并且原始帧包含 VLAN 标记，则会删除此帧的 VLAN 标记。

VLAN 角色

所有 VLAN 流量 （单播 / 广播 / 组播）均将处于其 VLAN 之内。连接到不同 VLAN 的设备无法通过以太网 MAC 层彼此直接连接。

设备 VLAN 仅能以静态方式创建。

某些 VLAN 可能具有其他角色，包括：

- 语音 VLAN：有关详情，请参阅*语音 VLAN* 一节。
- 访客 VLAN：在*编辑 VLAN 验证*页面*中设置*。
- 默认 VLAN：有关详情，请参阅*配置默认 VLAN 设置*一节。
- 管理 VLAN：有关详情，请参阅 “*配置 IP 信息*” 一节。

QinQ

QinQ 提供服务提供商网络与客户网络间的隔离。该交换机是一个提供商网桥，支持基于端口、已添加 c 标记的服务接口。

交换机使用 QinQ 为流量添加称为服务标记 (S-tag) 的 ID 标记，然后将其通过网络进行转发。 S-tag 用于在保留客户 VLAN 标记的同时，分离不同客户间的流量。

无论客户流量最初已包含 c 标记还是未标记，都通过一个 TPID 0x8100 的 S-tag 进行封装。 S-tag 可将此流量看作提供商网桥网络中的一个聚合，在该网络中，只能根据 S-tag VID (S-VID) 进行桥接。

当通过网络服务提供商的基础架构转发流量时， S-Tag 将被保留，并在稍后由出站设备将其删除。

QinQ 的另一个优势是，无需配置客户的边缘设备。

QinQ 在 “VLAN 管理” > *接口设置*页面中启用。

VLAN 配置工作流

配置 VLAN 的步骤：

1. 根据需要按照**配置默认 VLAN 设置**一节的说明更改默认 VLAN。
2. 按照**创建 VLAN** 一节的说明创建所需的 VLAN。
3. 按照**配置 VLAN 接口设置**一节的说明，根据需要设置 VLAN 相关端口的配置，并在接口上启用 QinQ。
4. 按照**配置 VLAN 端口**一节或**配置 VLAN 成员关系**一节的说明，将接口分配给 VLAN。
5. 在**配置 VLAN 成员关系**一节中，您可以查看所有接口的目前 VLAN 端口成员关系。

配置默认 VLAN 设置

在出厂默认设置下，交换机会自动创建 VLAN 1 作为默认 VLAN，所有端口的默认接口状态为 “中继”，并且会将所有端口配置为默认 VLAN 的 Untagged 成员。

默认 VLAN 具有以下特性：

- 该 VLAN 是独特的非静态 / 非动态 VLAN，并且在默认情况下，所有端口都是它的 Untagged 成员。
- 该 VLAN 无法删除。
- 无法为该 VLAN 指定标签。
- 不能为该 VLAN 指定任何特殊的角色 （例如未经验证的 VLAN 或语音 VLAN）。这仅适用于已启用 OUI 的语音 VLAN。
- 如果某端口不再是任何 VLAN 的成员，则交换机会自动将该端口配置为默认 VLAN 的 Untagged 成员。在以下情况下，端口将不再是 VLAN 的成员：VLAN 已被删除或者已将该端口从 VLAN 删除。

如果默认 VLAN 的 VID 发生更改，则在保存配置和重启交换机后，交换机会在 VLAN 中的所有端口上执行以下操作：

- 从原始默认 VLAN 中删除端口的 VLAN 成员关系 （可能仅在重启后会执行）。
- 将端口的 PVID （端口 VLAN 标识符）更改为新的默认 VLAN 的 VID。
- 从交换机上删除原始默认 VLAN ID。该 ID 必须经过重新创建，然后才能使用。
- 将端口添加为新的默认 VLAN 的未添加 VLAN 标记成员。

更改默认 VLAN 的步骤：

步骤 1 单击 **VLAN 管理** > **默认 VLAN 设置**。此时将显示*默认 VLAN 设置*页面。

步骤 2 为以下字段输入值：

- **当前默认 VLAN ID** - 显示目前的默认 VLAN ID。
- **重启后的默认 VLAN ID** - 输入要在重启后用于取代默认 VLAN ID 的新 VLAN ID。

步骤 3 单击**应用**。

步骤 4 单击**保存** （位于窗口的右上角），将当前配置保存到启动配置。

重启交换机后，**重启后的默认 VLAN ID** 的值将成为**当前默认 VLAN ID**。

创建 VLAN

您可以创建 VLAN，但需通过手动或自动的方式将该 VLAN 连接到一个以上的端口，该 VLAN 才会生效。端口必须始终属于一个或多个 VLAN。

200 系列交换机最多可支持 256 个 VLAN （包括默认 VLAN）。

必须使用 1 到 4094 之间的值为每个 VLAN 配置一个唯一的 VID (VLAN ID)。交换机会将 VID 4095 保留为丢弃 VLAN。所有分类为属于丢弃 VLAN 的数据包都会在入站处被丢弃，而不会被转发到端口。

创建 VLAN 的步骤：

步骤 1 单击 **VLAN 管理** > **创建 VLAN**。此时将显示*创建 VLAN* 页面。

“创建 VLAN”页面会针对所有 VLAN 显示以下字段：

- **VLAN ID** - 用户定义的 VLAN ID。
- **VLAN 名称** - 用户定义的 VLAN 名称。
- **类型** - VLAN 类型：
  - *静态* - VLAN 为用户定义。
  - *默认* - VLAN 为默认 VLAN。

步骤 2 单击**添加**添加新 VLAN，或选择现有 VLAN 并单击**编辑**，修改该 VLAN 的参数。此时将显示*添加 / 编辑 VLAN* 页面。

使用该页面可创建单个 VLAN 或一系列 VLAN。

步骤 3 要创建单个 VLAN，请选择 **VLAN** 单选按钮，输入 VLAN ID (VID) 及 VLAN 名称（可选）。

要创建一个 VLAN 范围，请选择**范围**单选按钮，然后通过输入起始 VID 和结束 VID（包含在内）来指定要创建的 VLAN 的范围。使用**范围**功能时，一次可以创建的最多 VLAN 数量是 100。

步骤 4 单击**应用**，创建 VLAN。

配置 VLAN 接口设置

使用*接口设置*页面可显示和配置所有接口的 VLAN 相关参数。

配置 VLAN 设置的步骤：

步骤 1 单击 **VLAN 管理** > **接口设置**。此时将显示*接口设置*页面。

步骤 2 选择接口类型 （端口或 LAG），然后单击**转至**。此时将显示端口或 LAG 及其 VLAN 参数。

步骤 3 选择要配置的端口或 LAG，然后单击**编辑**。此时将显示*编辑接口设置*页面。

步骤 4 为以下字段输入值：

- **接口** - 选择端口 /LAG。
- **接口 VLAN 模式** - 选择 VLAN 的接口模式。选项如下：
  - *一般* - 接口可以支持 IEEE 802.1q 规格中定义的所有功能。接口可以为一个或多个 VLAN 的 Tagged 成员或 Untagged 成员。
  - *访问* - 接口为单个 VLAN 的 Untagged 成员。在此模式下配置的端口称为访问端口。
  - *中继* - 接口最多可作为一个 VLAN 的 Untagged 成员，或者作为零个或更多 VLAN 的 Tagged 成员。在此模式下配置的端口称为中继端口。
  - *客户* - 选中此选项可使接口处于 QinQ 模式。这可让您在提供商网络间使用自有的 VLAN 部署 (PVID)。如果交换机拥有一个或更多客户端口，它将处于 Q-in-Q 模式。请参阅 **QinQ**。
- **管理 PVID** - 输入传入的 Untagged 和添加了优先级标记的帧的所属 VLAN 的端口 VLAN ID (PVID)。可能的值为 1 到 4094。
- **帧类型** - 选择接口可以接收的帧类型。不属于所配置的帧类型的帧将在入站处被丢弃。这些帧类型仅在 “一般” 模式下可用。可能的值包括：
  - *全部接受* - 接口接受所有类型的帧：Untagged 帧、 Tagged 帧和添加优先级标记的帧。
  - *只接受 Tagged* - 接口仅接受添加标记的帧。
  - *只接受 Untagged* - 接口仅接受 Untagged 帧和优先级帧。

- **入口过滤** - （仅在 “一般” 模式下可用）选择该选项可启用入站过滤功能。如果对接口启用了入站过滤功能，当传入帧所属的 VLAN 不包括该接口时，接口会丢弃这些传入帧。入口过滤功能可以在一般端口上禁用或启用，而该功能在访问端口和中继端口上始终启用。

步骤 5 单击**应用**。参数将写入当前配置文件中。

定义 VLAN 成员关系

端口到 VLAN 和 *端口 VLAN 成员关系* 页面会以多种形式显示端口的 VLAN 成员关系。可以使用其向 VLAN 添加成员关系或从 VLAN 删除成员关系。

如果对端口禁止默认 VLAN 成员关系，该端口将不能成为任何其他 VLAN 的成员。将为该端口分配 4095 作为其内部 VID。

若要正确转发数据包，必须手动配置沿终端节点间的路径传输 VLAN 流量的可识别 VLAN 的中间设备。

两个可识别 VLAN 的设备 （没有可识别 VLAN 的设备介于两者之间）之间的 Untagged 端口成员关系必须属于同一 VLAN。换言之，如果这两个设备之间的端口向 VLAN 发送 Untagged 数据包或从 VLAN 接收 Untagged 数据包，则端口上的 PVID 必须相同。否则，流量可能会从一个 VLAN 泄露到另一个 VLAN。

VLAN-tagged 帧可以通过可识别 VLAN 或无法识别 VLAN 的网络设备传输。如果目的终端节点可识别 VLAN，但将从 VLAN 接收流量，则上一个可识别 VLAN 的设备（如果存在）必须将目的 VLAN 的帧发送到 Untagged 终端节点。

配置 VLAN 端口

使用 *端口到 VLAN* 页面可显示和配置特定 VLAN 中的端口。

将端口或 LAG 映射到 VLAN 的步骤：

步骤 1 单击 **VLAN 管理** > **端口到 VLAN**。此时将显示 *端口到 VLAN* 页面。

步骤 2 选择 VLAN 和接口类型 （端口或 LAG）并单击**转至**，以针对 VLAN 显示或更改端口特性。

每个端口或 LAG 的端口模式会显示为从 *接口设置* 页面配置的目前端口模式 （“访问”、“中继” 或 “一般”）。

每个端口或 LAG 均将与其对 VLAN 的目前注册一起显示。

步骤 3 通过从以下列表中选择所需的选项来更改接口对 VLAN 的注册：

- **已禁止** - 不允许接口加入 VLAN。如果端口不是任何其他 VLAN 的成员，在端口上启用该选项会使该端口成为内部 VLAN 4095 （保留 VID）的成员。
- **已排除** - 接口目前不是 VLAN 的成员。这是在新创建 VLAN 时所有端口和 LAG 的默认选项。
- **Tagged** - 接口是 VLAN 的 Tagged 成员。
- **Untagged** - 接口为 VLAN 的 Untagged 成员。会将 Untagged VLAN 帧发送到接口 VLAN。
- **PVID** - 选择该选项会将接口的 PVID 设置为 VLAN 的 VID。PVID 是一个针对端口的设置。

步骤 4 单击**应用**。会将接口分配给 VLAN，并写入当前配置文件中。

选择另一个 VLAN ID，可以继续显示和 / 或配置另一个 VLAN 的端口成员关系。

配置 VLAN 成员关系

*端口 VLAN 成员关系*页面将显示设备上的所有端口以及一个各端口所属 VLAN 的列表。

如果某接口基于端口的验证方法为 802.1x，并且 “管理端口控制” 为 “自动”，那么：

- 在对端口进行验证之前，会将其排除在所有 VLAN 之外 （访客和未经验证的端口除外）。在 “VLAN 到端口” 页面中，端口标记有 "P"。
- 当对端口进行验证时，该端口将接收在其中进行配置的 VLAN 中的成员关系。

将端口分配给一个或多个 VLAN 的步骤：

步骤 1 单击 **VLAN 管理** > **端口 VLAN 成员关系**。此时将显示*端口 VLAN 成员关系*页面。

步骤 2 选择接口类型 （端口或 LAG），然后单击**转至**。会针对所选类型的所有接口显示以下字段：

- **接口** - 端口 /LAG ID。
- **模式** - 在*接口设置*页面中选择的接口 VLAN 模式。
- **管理 VLAN** - 显示接口可能所属的所有 VLAN 的下拉列表。
- **运行 VLAN** - 显示接口目前所属的所有 VLAN 的下拉列表。
- **LAG** - 如果选择的接口为端口，则会显示该端口所属的 LAG。

步骤 3 选择端口，然后单击**加入 VLAN** 按钮。此时将显示*加入 VLAN* 页面。

步骤 4 为以下字段输入值：

- **接口** - 选择端口或 LAG。
- **模式** - 显示在*接口设置*页面中选择的端口 VLAN 模式。
- **选择 VLAN** - 要将端口与 VLAN 关联，请使用箭头键将左侧列表中的 VLAN ID 移到右侧列表。如果默认 VLAN 添加了标记，则可能会显示在右侧列表中，但无法选择。
- **标记** - 选择以下添加标记 /PVID 选项之一：
  - **已禁止** - 不允许接口加入 VLAN。如果端口不是任何其他 VLAN 的成员，在端口上启用该选项会使该端口成为内部 VLAN 4095 （保留 VID）的成员。
  - **已排除** - 接口目前不是 VLAN 的成员。这是在新创建 VLAN 时所有端口和 LAG 的默认选项。
  - **Tagged** - 选择端口是否 Tagged。该选项不适用于访问端口。
  - **Untagged** - 选择端口是否 Untagged。该选项不适用于访问端口。
  - **PVID** - 将端口 PVID 设置为此 VLAN。如果接口为 “访问” 模式或 “中继” 模式，交换机会自动使接口成为 VLAN 的 Untagged 成员。如果接口为 “一般” 模式，则必须手动配置 VLAN 成员关系。

步骤 5 单击**应用**。将修改设置，并将其写入当前配置文件中。

步骤 6 要查看接口上的管理和运行 VLAN，请单击**详情**。

语音 VLAN

在 LAN 中，如果 IP 电话、 VoIP 端点等语音设备和语音系统位于同一个 VLAN 中，则这种 VLAN 被称为语音 VLAN。如果语音设备位于不同的语音 VLAN 中，就需要使用 IP （第 3 层）路由器来进行通信。

本节包含以下主题：

- 语音 VLAN 概述
- 配置语音 VLAN

语音 VLAN 概述

本节包含以下主题：

- 动态语音 VLAN 模式
- 自动语音 VLAN、自动智能端口、 CDP 和 LLDP
- 语音 VLAN QoS
- 语音 VLAN 限制
- 语音 VLAN 工作流

下面是使用适当配置的典型语音部署方案：

- **UC3xx/UC5xx 托管：**所有思科电话和 VoIP 端点都支持此部署模型。对于此模型， UC3xx/UC5xx、思科电话和 VoIP 端点都位于同一个语音 VLAN 中。UC3xx/UC5xx 语音 VLAN 的默认值为 VLAN 100。
- **第三方 IP PBX 托管：**思科 SBTG CP-79xx、 SPA5xx 电话和 SPA8800 端点支持此部署模型。在此模型中，电话使用的 VLAN 由网络配置确定。语音和数据 VLAN 可以分开，也可以不分开。电话和 VoIP 端点通过内建 IP PBX 注册。
- **IP Centrex/ITSP 托管：**思科 CP-79xx、SPA5xx 电话和 SPA8800 端点支持此部署模型。对于此模型，电话使用的 VLAN 由网络配置确定。语音和数据 VLAN 可以分开，也可以不分开。电话和 VoIP 端点通过 “云” 中的一个远端 SIP 代理注册。

从 VLAN 的角度来看，上述模型可以在可识别 VLAN 和不可识别 VLAN 中运行。在可识别 VLAN 环境中，语音 VLAN 是安装中配置的很多 VLAN 中的一个。不可识别 VLAN 方案与可识别 VLAN 相同，只是语音 VLAN 是唯一一个 VLAN。

交换机始终作为可识别 VLAN 交换机运行。

该交换机支持单一语音 VLAN。默认情况下，语音 VLAN 为 VLAN 1。语音 VLAN 的默认值为 VLAN 1。您可以手动配置不同的语音 VLAN。当自动语音 VLAN 启用时，还可以动态学习语音 VLAN。

要将端口手动添加至语音 VLAN，可根据*配置 VLAN 接口设置*一节中所述使用基本 VLAN 配置实现，或者手动将语音相关的智能端口宏应用到端口。或者，如果该交换机处于 “电话 OUI”模式，或已启用 “自动智能端口”，您也可以动态添加端口。

动态语音 VLAN 模式

交换机支持两种动态语音 VLAN 模式：电话 OUI （组织唯一标识符）模式和自动语音 VLAN 模式。这两种模式将影响到语音 VLAN 和 / 或语音 VLAN 端口成员关系的配置。这两种模式是相互排斥的。

- **电话 OUI**

  在 “电话 OUI”模式中，语音 VLAN 必须是一个手动配置的 VLAN，而不能是默认的 VLAN。

  当交换机处于 “电话 OUI”模式中，且端口已手动配置成为加入语音 VLAN 的候选端口时，如果交换机收到包含与其中一个已配置电话 OUI 相匹配的源 MAC 地址的数据包时，交换机会将该端口动态添加至语音 VLAN 中。OUI 是以太网 MAC 地址的前三个字节。有关电话 OUI 的详情，请参阅**配置电话 OUI**。

- **自动语音 VLAN**

  在 “自动语音 VLAN”模式中，语音 VLAN 可以是默认的语音 VLAN，可以手动进行配置，也可以从 UC3xx/5xx 等外部设备以及在 CDP 或 VSDP 中通告语音 VLAN 的交换机学习。 VSDP 是一个思科定义的语音服务发现协议。

  与电话 OUI 模式根据电话 OUI 检测语音设备不同，自动语音 VLAN 模式根据自动智能端口将端口动态添加至语音 VLAN。如果已启用自动智能端口，且检测到某端口附加设备通过 CDP 和 / 或 LLDP-MED 将其自身通告为电话或媒体端点，则会将端口添加至语音 VLAN。

语音端点

要使语音 VLAN 正常工作，则必须将思科电话和 VoIP 端点等语音设备分配给发送和接收语音流量的语音 VLAN。以下列举了一些可能的方案：

- 电话 / 端点可以静态配置语音 VLAN。
- 电话 / 端点可以在从 TFTP 服务器下载的启动文件中获得语音 VLAN。当为电话分配一个 IP 地址时， DHCP 服务器可以指定启动文件和 TFTP 服务器。
- 电话 / 端点从邻居语音系统和交换机的 CDP 和 LLDP-MED 通告中，获得语音 VLAN 信息。

交换机希望附加语音设备向语音 VLAN 发送 Tagged 数据包。在语音 VLAN 同时也是本征 VLAN 的端口上，也可发送语音 VLAN Untagged 数据包。

自动语音 VLAN、自动智能端口、 CDP 和 LLDP

默认设置

出厂默认情况下，交换机上的 CDP、 LLDP 和 LLDP-MED 已启用，自动智能端口模式已启用，基本 QoS 连同信任 DSCP 已启用，并且所有端口都是默认 VLAN 1 的成员，其中 VLAN 1 也是默认的语音 VLAN。

此外，动态语音 VLAN 模式默认为根据触发启用，自动智能端口默认为根据自动语音 VLAN 启用。

语音 VLAN 触发

如果动态语音 VLAN 模式为 “启用自动语音 VLAN”，则只有出现一个或多个触发时，语音 VLAN 模式才可运行。触发可以是静态语音 VLAN 配置、在邻居 CDP 通告中接收的语音 VLAN 信息，以及在语音 VLAN 发现协议 (VSDP) 中接收的语音 VLAN 信息。您可以在必要时立即激活自动语音 VLAN，而无需等待触发。

如果根据自动语音 VLAN 模式启用自动智能端口，则当自动语音 VLAN 运行时，将启用自动智能端口。您还可以在必要时不考虑自动语音 VLAN，独自启用自动智能端口。

注 此处的默认配置列表适用于固件版本支持开箱即用自动语音 VLAN 的交换机。该列表还适用于已升级至支持自动语音 VLAN 的固件版本的未配置交换机。

注 默认设置和语音 VLAN 触发不会对没有语音 VLAN 的任何安装和已进行配置的交换机产生任何影响。您可以按需手动禁用和启用自动语音 VLAN 和 / 或自动智能端口，使之适应您的部署。

自动语音 VLAN

自动语音 VLAN 负责维护语音 VLAN，但是需要根据自动智能端口维护语音 VLAN 端口成员关系。当运行自动语音 VLAN 模式时，将执行以下功能：

- 从直连邻居设备的 CDP 通告中发现语音 VLAN 信息。
- 如果多台邻居交换机和 / 或路由器 （例如，思科统一通信 [UC] 设备）通告其语音 VLAN，将使用 MAC 地址最低的设备的语音 VLAN。

  注 如果将交换机连接至一台思科 UC 设备，您可能需要使用 `switchport voice vlan` 命令配置 UC 设备上的端口，以确保 UC 设备在端口 CDP 中通告其语音 VLAN。

- 通过使用语音服务发现协议 (VSDP)，可以同步语音 VLAN 相关参数和其他已启用自动语音 VLAN 的交换机。交换机始终使用来自其已识别的优先级最高的源的语音 VLAN 对自身进行配置。该优先级基于提供语音 VLAN 信息的源的源类型和 MAC 地址。源类型优先级从高到低分别为：VLAN 配置、 CDP 通告、基于已更改的默认 VLAN 的默认配置和默认语音 VLAN。数值低的 MAC 地址比数值高的 MAC 地址优先级更高。
- 在发现来自优先级更高的源的新语音 VLAN 之前，或者在用户重启自动语音 VLAN 之前，系统将始终保留该语音 VLAN。重启时，交换机将语音 VLAN 重置为默认语音 VLAN，并重启自动语音 VLAN 发现。
- 当配置 / 发现新的语音 VLAN 时，交换机将自动创建该语音 VLAN，并将现有语音 VLAN 的所有端口成员关系全部替换为新的语音 VLAN。这可能会中断或终止现有的语音会话，当更改网络拓扑时预期也会导致此结果。

  注 如果交换机处于第 2 层系统模式，则可以只同步位于同一个管理 VLAN 中的支持 VSDP 的交换机。如果交换机处于第 3 层系统模式，则可以同步位于该交换机所配置的直连 IP 子网中支持 VSDP 的交换机。

自动智能端口与 CDP/LLDP 配合使用，可以在从端口检测到语音端点时维护语音 VLAN 的端口成员关系：

- 当 CDP 和 LLDP 启用时，交换机会定期发送 CDP 和 LLDP 数据包，向使用的语音端点通告语音 VLAN。
- 当连接至某端口的设备通过 CDP 和/或 LLDP 将自身作为一个语音端点通告时，自动智能端口会为该端口应用相应的智能端口宏，从而自动将该端口添加至语音 VLAN （如果不存在来自该端口的任何其他设备通告一个冲突或更高级的功能）。如果某设备将自身作为一台电话通告，则默认的智能端口宏是电话。如果某设备将自身作为电话与主机或者电话与网桥通告，则默认的智能端口宏是电话 + 桌面。

语音 VLAN QoS

语音 VLAN 可通过使用 LLDP-MED 网络策略传递 CoS/802.1p 和 DSCP 设置。如果某设备发送 LLDP-MED 数据包，则 LLDP-MED 将默认设置为响应语音 QoS 设置。支持 MED 的设备必须使用与 LLDP-MED 响应所接收的相同的 CoS/802.1p 和 DSCP 值发送其语音流量。

您可以禁止在语音 VLAN 和 LLDP-MED 间进行自动更新，并使用其自有网络策略。

若在 OUI 模式下，交换机可以根据 OUI 另外配置语音流量的映射和重新标记 (CoS/802.1p)。

默认情况下，所有接口都是 CoS/802.1p 信任接口。交换机将根据语音流中找到的 CoS/802.1p 值应用服务质量。对于电话 OUI 语音流，您可以通过指定所需的 CoS/802.1p 值，并使用 “电话 OUI”下面的重新标记选项，覆盖服务质量，并可以选择重新标记语音流的 802.1p。

语音 VLAN 限制

存在以下限制：

- 只支持一个语音 VLAN。
- 定义为语音 VLAN 的 VLAN 无法删除。

此外，以下限制也适用于电话 OUI：

- 语音 VLAN 不能是 VLAN 1 （默认 VLAN）。
- 语音 VLAN 不能启用智能端口。
- 语音 VLAN QoS 决策的优先级高于任何其他 QoS 决策 （策略决策除外）。
- 仅在当前的语音 VLAN 没有候选端口时，才能为语音 VLAN 配置新的 VLAN ID。
- 候选端口的接口 VLAN 必须处于 “一般” 模式或 “中继” 模式下。
- 语音 VLAN QoS 将应用于已加入语音 VLAN 的候选端口以及静态端口。
- 如果转发数据库 (FDB) 可学习 MAC 地址，将接受语音流。（如果 FDB 中没有可用空间，则不会发生任何操作。）

语音 VLAN 工作流

交换机的自动语音 VLAN、自动智能端口、 CDP 和 LLDP 默认设置涵盖大多数常见的语音部署方案。本节介绍了当未应用默认配置时，如何部署语音 VLAN。

工作流程 1：配置自动语音 VLAN 的步骤

步骤 1 打开 *VLAN 管理 > 语音 VLAN > 属性*页面。

步骤 2 选择语音 VLAN ID。不能将其设置为 VLAN ID 1 （动态语音 VLAN 无需此步骤）。

步骤 3 设置**动态语音 VLAN** 为 “启用自动语音 VLAN”。

步骤 4 选择**自动语音 VLAN 激活**方法。

注 如果设备目前正处于 “电话 OUI” 模式中，则您必须先将其禁用，方可配置自动语音 Vlan。

步骤 5 单击**应用**。

步骤 6 按**常见智能端口任务**一节中所述配置智能端口。

步骤 7 按**配置 LLDP** 和**配置 CDP** 节中所述，分别配置 LLDP/CDP。

步骤 8 使用 *智能端口 > 接口设置*页面启用相关端口上的智能端口特性。

注 步骤 7 和步骤 8 是可选的，因为这两项在默认情况下处于启用状态。

工作流程 2：配置电话 OUI 方法的步骤

步骤 1 打开 *VLAN 管理 > 语音 VLAN > 属性*页面。设置**动态语音 VLAN** 为 “启用电话 OUI”。

注 如果设备目前正处于 “自动语音 VLAN”模式中，则在您可以配置电话 OUI 之前，必须将其禁用。

步骤 2 在 *电话 OUI* 页面中配置电话 OUI。

步骤 3 在 *电话 OUI 接口*页面中为端口配置电话 OUI VLAN 成员关系。

配置语音 VLAN

本节介绍了如何配置语音 VLAN。具体包括以下主题：

- **配置语音 VLAN 属性**
- **显示自动语音 VLAN 设置**
- **配置电话 OUI**

配置语音 VLAN 属性

使用 *语音 VLAN 属性*页面完成以下操作：

- 查看当前语音 VLAN 的配置情况。
- 配置语音 VLAN 的 VLAN ID。
- 配置语音 VLAN QoS 设置。
- 配置语音 VLAN 模式 （电话 OUI 或自动语音 VLAN）。
- 配置自动语音 VLAN 的触发方式。

查看和配置语音 VLAN 属性的步骤：

步骤 1 单击 **VLAN 管理** > **语音 VLAN** > **属性**，此时将显示*属性*页面。

- **语音 VLAN 设置** （**管理状态**）框中将显示交换机上配置的语音 VLAN 设置。
- **语音 VLAN 设置** （**运行状态**）框中将显示实际应用于语音 VLAN 部署的语音 VLAN 设置。

步骤 2 为以下字段输入值：

- **语音 VLAN ID** - 输入要作为语音 VLAN 的 VLAN。

  注 语音 VLAN ID、 CoS/802.1p 和 / 或 DSCP 中的更改会导致交换机将管理语音 VLAN 作为静态语音 VLAN 通告。如果选择由外部语音 VLAN 触发*自动语音 VLAN 激活*，则需要保持默认值。

- **CoS/802.1p** - 选择一个 LLDP-MED 要用作语音网络策略的 CoS/802.1p 值。详情请参阅*管理 > 发现 > LLDP > LLDP MED 网络策略*。
- **DSCP** - 选择 LLDP-MED 要用作语音网络策略的 DSCP 值。详情请参阅*管理 > 发现 > LLDP > LLDP MED 网络策略*。
- **动态语音 VLAN -** 选择此字段，通过以下一种方式禁用或启用语音 VLAN 特性：
  - *启用自动语音 VLAN* - 在 “自动语音 VLAN”模式中启用动态语音 VLAN。
  - *启用电话 OUI* - 在 “电话 OUI”模式中启用动态语音 VLAN。
  - *禁用* - 禁用自动语音 Vlan 或电话 OUI。
- **自动语音 VLAN 激活** - 如果已启用自动语音 VLAN，可以选择以下选项中的一种激活自动语音 VLAN：
  - *立即* - 如果启用，将立即激活交换机上的自动语音 VLAN，并使之生效。
  - *通过外部语音 VLAN 触发* - 只有当交换机检测到某设备通告语音 VLAN 时，才能激活交换机上的自动语音 VLAN，并使之生效。

  注 手动重新配置语音 VLAN ID、 CoS/802.1p 和 / 或 DSCP，更改其默认值会产生一个静态语音 VLAN，该静态语音 VLAN 的优先级高于从外部源学习的自动语音 VLAN。

步骤 3 单击**应用**。 VLAN 属性将写入当前配置文件中。

显示自动语音 VLAN 设置

如果已启用自动语音 VLAN 模式，可以使用自动语音 VLAN 页面查看相关全局和接口参数。

您还可以单击**重启自动语音 VLAN**，使用此页面手动重启自动语音 VLAN。短暂延时之后，此操作将重置语音 VLAN 为默认语音 VLAN，并在已启用自动语音 VLAN 的 LAN 中所有交换机上重启自动语音 VLAN 发现和同步流程。

注 如果源类型处于*非活动*状态，此操作只会将语音 VLAN 重置为默认语音 VLAN。

查看自动语音 VLAN 参数的步骤：

步骤 1 单击 **VLAN 管理** > **语音 VLAN** > **自动语音 VLAN**。此时将显示*自动语音 VLAN* 页面。

此页面上的运行状态框将显示有关当前语音 VLAN 及其源的信息：

- **自动语音 VLAN 状态** - 显示是否已启用自动语音 VLAN。
- **语音 VLAN ID** - 当前语音 VLAN 标识符
- **源类型** - 显示根交换机发现的语音 VLAN 的源类型。
- **CoS/802.1p** - 显示 LLDP-MED 会用作语音网络策略的 CoS/802.1p 值。
- **DSCP** - 显示 LLDP-MED 会用作语音网络策略的 DSCP 值。
- **根交换机 MAC 地址** - 发现或配置语音 VLAN 的根设备的 MAC 地址 （语音 VLAN 就是从该设备中学习到的）。
- **交换机 MAC 地址** - 交换机的基本 MAC 地址。如果该设备的交换机 MAC 地址是根交换机 MAC 地址，则该设备即为自动语音 VLAN 根设备。
- **语音 VLAN ID 更改时间** - 上次更新语音 VLAN 的时间。

步骤 2 单击**重启自动语音 VLAN**，重置语音 VLAN 为默认语音 VLAN，并在 LAN 中的所有已启用自动语音 VLAN 的交换机上重启自动语音 VLAN 发现流程。

语音 VLAN 本地表会显示交换机上配置的语音 VLAN，以及由直连邻居设备通告的任意语音 VLAN 配置。其中显示以下字段：

- **接口** - 显示在其上接收或配置语音 VLAN 配置的接口。如果显示*无*，则表示交换机自身已完成配置。如果显示接口，则表示已从邻居接收语音配置。
- **源 MAC 地址** - 从其接收语音配置的 UC 的 MAC 地址。

- **源类型** - 从其接收语音配置的 UC 的类型。可能的选项有：
  - *默认* - 交换机上的默认语音 VLAN 配置
  - *静态* - 交换机上用户定义的语音 VLAN 配置。
  - *CDP* - 通告的语音 VLAN 配置正在运行 CDP 的 UC。
  - *LLDP* - 通告的语音 VLAN 配置正在运行 LLDP 的 UC。
  - *语音 VLAN ID* - 所通告或配置的语音 VLAN 的标识符
- **语音 VLAN ID** - 当前语音 VLAN 的标识符。
- **CoS/802.1p** - LLDP-MED 要用作语音网络策略的通告或配置的 CoS/802.1p 值。
- **DSCP** - LLDP-MED 要用作语音网络策略的通告或配置的 DSCP 值。
- **最佳本地源** - 显示交换机是否已使用此语音 VLAN。可能的选项有：
  - *是* - 交换机使用此语音 VLAN 同步已启用自动语音 VLAN 的其他交换机。除非发现来自更高优先级源的语音 VLAN，否则，此语音 VLAN 便为该网络的语音 VLAN。只能有一个本地源成为最佳本地源。
  - *否* - 此本地源并非最佳本地源。

步骤 3 单击**刷新**，刷新页面上的信息

配置电话 OUI

OUI 是由 Institute of Electrical and Electronics Engineers, Incorporated （电气电子工程师学会， IEEE）注册机构分配的。由于 IP 电话制造商数量有限且被熟知，因此已知的 OUI 值会导致将相关帧以及在其上发现这些帧的端口自动分配给语音 VLAN。

OUI 全局表最多可包含 128 个 OUI。

本节包含以下主题：

- **将 OUI 添加至电话 OUI 表**
- **将接口添加至基本 OUI 上的语音 VLAN**

将 OUI 添加至电话 OUI 表

使用 *电话 OUI* 页面可配置电话 OUI QoS 属性。此外，您还可以配置自动成员关系过期时间。如果指定的时间段内没有电话活动，则该端口将从语音 VLAN 中删除。

使用 *电话 OUI* 页面可查看现有 OUI，并添加新的 OUI。

配置电话 OUI 和 / 或添加新的语音 VLAN OUI 的步骤：

步骤 1 单击 **VLAN 管理** > **语音 VLAN** > **电话 OUI**。此时将显示 *电话 OUI* 页面。

电话 OUI 页面显示以下字段：

- **电话 OUI 运行状态** - 显示 OUI 是否用于标识语音流量。
- **CoS/802.1p** - 选择将要分配给语音流量的 CoS 队列。
- **重新标记 CoS/802.1p** - 选择是否重新标记出站流量。
- **自动成员关系过期时间** - 输入在端口上所有检测到的电话 MAC 地址过期之后，从语音 VLAN 删除端口的时间延时。

步骤 2 单击**应用**，使用这些值更新交换机的当前配置。

此时将显示电话 OUI 表：

- **电话 OUI** - 为 OUI 保留的 MAC 地址的前六位。
- **说明** - 用户指定的 OUI 说明。

步骤 3 单击**恢复 OUI 默认设置**可删除所有用户创建的 OUI，而仅在表中保留默认的 OUI。

要删除所有 OUI，请选择顶部的复选框。将选择所有 OUI，并可通过单击**删除**将它们删除。然后，如果您单击**恢复**，系统将恢复已知的 OUI。

步骤 4 要添加新的 OUI，请单击**添加**。此时将显示 *添加电话 OUI* 页面。

步骤 5 为以下字段输入值：

- **电话 OUI** - 输入新的 OUI。
- **说明** - 输入 OUI 名称。

步骤 6 单击**应用**。将 OUI 添加至电话 OUI 表。

将接口添加至基本 OUI 上的语音 VLAN

在以下一种模式下， QoS 属性可按端口分配给语音数据包：

- **全部** - 为语音 VLAN 配置的服务质量 (QoS) 值将应用于在接口上收到的被分类为属于语音 VLAN 的所有传入帧。
- **电话源 MAC 地址 (SRC)** - 为语音 VLAN 配置的 QoS 值会应用到分类为属于语音 VLAN，且在源 MAC 地址中包含一个 OUI，与已配置电话 OUI 相匹配的所有传入帧。

使用*电话 OUI 接口*页面，可根据 OUI 标识符将接口添加至语音 VLAN，并配置语音 VLAN 的 OUI QoS 模式。

在接口上配置电话 OUI 的步骤：

步骤 1 单击 **VLAN 管理** > **语音 VLAN** > **电话 OUI 接口**。此时将显示*电话 OUI 接口*页面。

*电话 OUI 接口*页面会显示所有接口的语音 VLAN OUI 参数。

步骤 2 若要将接口配置为基于电话 OUI 的语音 VLAN 的候选端口，请单击**编辑**。此时将显示*编辑接口设置*页面。

步骤 3 为以下字段输入值：

- **接口** - 选择接口。
- **电话 OUI VLAN 成员关系** - 如果已启用，则该接口即为基于电话 OUI 的语音 VLAN 的候选端口。当接收到的数据包与一个已配置电话 OUI 匹配时，即可将该端口添加至语音 VLAN。
- **语音 VLAN QoS 模式** - 选择以下选项中的一个：
  - *全部* - QoS 属性应用于分类为属于语音 VLAN 的所有数据包上。
  - *电话源 MAC 地址* - QoS 属性仅应用于来自 IP 电话的数据包上。

步骤 4 单击**应用**。将添加 OUI。

13

配置生成树协议

本节介绍了生成树协议 (STP) （IEEE802.1D 和 IEEE802.1Q），具体包括以下主题：

- **STP 模式**
- **配置 STP 状态和全局设置**
- **定义生成树接口设置**
- **配置快速生成树设置**

STP 模式

STP 通过选择性地将链路设置为备用模式，以避免形成环路，从而防止第 2 层广播域发生广播风暴。在备用模式下，这些链路会暂时性地停止传输用户数据。当拓扑发生变化以便能够传输数据时，系统会自动重新激活这些链路。

当主机之间存在备用路由时，产生环路。扩展网络中的环路可导致交换机无限制转发流量，从而造成流量负载增加、网络效率降低。

STP 提供了一种树状拓扑，该拓扑可在网络上的终端工作站之间创建唯一的路径，从而消除环路，其适用于任意部署的交换机和互联链路。

交换机支持以下生成树协议版本：

- 传统 STP - 在任意两个终端工作站之间提供单条路径，从而避免和消除环路。
- 快速 STP (RSTP) - 检测网络拓扑，以提供更快的生成树聚合。本协议在网络拓扑本身为树状结构，从而可以实现快速聚合的情况下最有效。默认情况下，系统会启用 RSTP。

  注 200 系列交换机不支持 MSTP。

配置 STP 状态和全局设置

*STP 状态和全局设置*页面包含用于启用 STP 或 RSTP 的参数。

使用 *STP 接口设置页面和 RSTP 接口设置页面将端口分别配置为相应模式。*

设置 STP 状态和全局设置的步骤：

步骤 1 单击**生成树** > **STP 状态和全局设置**。此时将显示 *STP 状态和全局设置*页面。

步骤 2 输入参数。

全局设置：

- **生成树状态** - 在交换机上启用或禁用 STP。
- **STP 运行模式** - 选择一种 STP 模式。
- **BPDU 处理** - 选择在端口或交换机上禁用 STP 时如何管理 BPDU 数据包。BPDU 用于传输生成树信息。
  - *过滤* - 在接口上禁用生成树时，过滤 BPDU 数据包。
  - *泛洪* - 在接口上禁用生成树时，泛洪 BPDU 数据包。
- **路径成本默认值** - 选择用于为 STP 端口分配默认路径成本的方式。分配给接口的默认路径成本随选择的方式而变化。
  - *短* - 为端口路径成本指定 1 到 65,535 的范围。
  - *长* - 为端口路径成本指定 1 到 200,000,000 的范围。

网桥设置：

- **优先级** - 设置网桥优先级值。交换 BPDU 后，优先级最低的设备将成为根网桥。如果所有网桥具有相同的优先级，将使用它们的 MAC 地址来确定根网桥。网桥优先级值的增量为 4096。例如 4096、 8192、 12288 等等。
- **Hello Time** - 设置根网桥在配置消息之间等待的时间间隔 （以秒为单位）。范围为 1 到 10 秒。
- **最长时间** - 设置交换机在尝试重新定义其自身配置之前，可用来等待接收配置消息的时间间隔 （以秒为单位）。
- **转发延迟** - 设置网桥在转发数据包之前保持为学习状态的时间间隔 （以秒为单位）。有关详情，请参阅**定义生成树接口设置**。

指定的根：

- **网桥 ID** - 网桥优先级与交换机的 MAC 地址串联在一起。
- **根网桥 ID** - 根网桥优先级与根网桥的 MAC 地址串联在一起。
- **根端口** - 可提供从该网桥到根网桥的最低成本路径的端口。（这在网桥不为根网桥的情况下效果很显著。）
- **根路径成本** - 从该网桥到根网桥的路径成本。
- **拓扑更改总数** - 已发生的 STP 拓扑更改总数。
- **最近拓扑更改** - 自上次拓扑更改发生以来所用的时间间隔。该时间以“天 / 小时 / 分钟 / 秒”的格式显示。

步骤 3 单击**应用**。 STP 全局设置将写入当前配置文件。

定义生成树接口设置

使用 *STP 接口设置*页面，可针对每个端口配置 STP，及查看该协议学习的信息，例如指定的网桥。

输入的定义的配置对于任何模式的 STP 协议均有效。

在接口上配置 STP 的步骤：

步骤 1 单击**生成树** > **STP 接口设置**。屏幕将显示 *STP 接口设置*页面。

步骤 2 选择一个接口，然后单击**编辑**。此时将显示*编辑接口设置*页面。

步骤 3 输入参数

- **接口** - 选择要在其上配置生成树的端口或 LAG。
- **STP** - 在端口上启用或禁用 STP。
- **边缘端口** - 在端口上启用或禁用快速链路。如果针对端口启用了快速链路模式，则当端口链路连接时，系统会自动将端口状态设置为转发状态。快速链路会优化 STP 协议聚合。选项如下：
  - *启用* - 立即启用快速链路。
  - *自动* - 在接口开始活动后的几秒内启用快速链路。这样可让 STP 在启用快速链路之前，解决环路问题。

- *禁用* - 禁用快速链路。

  注 建议将值设置为 “自动”，以便在主机连接到交换机后，该交换机将端口设置为快速链路模式，或者在连接到其他交换机后，将端口设置为常规 STP 端口。这有助于避免形成环路。

- **BPDU 处理** - 选择在端口或交换机上禁用 STP 时如何管理 BPDU 数据包。BPDU 用于传输生成树信息。
  - *使用全局设置* - 选择后将使用 *STP 状态和全局设置*页面中定义的设置。
  - *过滤* - 在接口上禁用生成树时，过滤 BPDU 数据包。
  - *泛洪* - 在接口上禁用生成树时，泛洪 BPDU 数据包。
- **路径成本** - 设置端口产生的根路径成本，或使用系统生成的默认成本。
- **优先级** - 设置端口的优先级值。如果网桥在一个环路中连接了两个端口，则优先级值会影响端口选择。优先级是从 0 到 240 的值，设置增量为 16。
- **端口状态** - 显示端口的目前 STP 状态。
  - *已禁用* - 目前在端口上禁用 STP。端口在学习 MAC 地址的同时转发流量。
  - *阻塞* - 端口目前被阻塞，无法转发流量 （BPDU 数据除外）或学习 MAC 地址。
  - *监听* - 端口处于监听模式。端口无法转发流量，也无法学习 MAC 地址。
  - *学习* - 端口处于学习模式。端口无法转发流量，但能够学习新的 MAC 地址。
  - *转发* - 端口处于转发模式。端口可以转发流量且学习新的 MAC 地址。
- **指定的网桥 ID** - 显示指定网桥的网桥优先级和 MAC 地址。
- **指定的端口 ID** - 显示所选端口的优先级和接口。
- **指定成本** - 显示加入 STP 拓扑的端口的成本。如果 STP 检测到环路，则成本越低的端口越不容易被阻塞。
- **转发转换** - 显示端口从**阻塞**状态变成**转发**状态的次数。
- **速度** - 显示端口速度。
- **LAG** - 显示端口所属的 LAG。如果端口是某 LAG 的成员，则 LAG 设置会覆盖端口设置。

步骤 4 单击**应用**。接口设置将写入当前配置文件。

配置快速生成树设置

使用快速生成树协议 (RSTP)，可实现更快的 STP 聚合，而不会创建转发环路。

使用 *RSTP 接口设置*页面可针对每个端口配置 RSTP。如果将全局 STP 模式设置为 RSTP，则在此页面上完成的任何配置均有效。

输入 RSTP 设置的步骤：

步骤 1 单击**生成树** > **STP 状态和全局设置**。此时将显示 *STP 状态和全局设置*页面。启用 **RSTP**。

步骤 2 单击**生成树** > **RSTP 接口设置**。将打开 *RSTP 接口设置*页面：

步骤 3 选择一个端口。

注 仅在选择连接至所测试的网桥伙伴的端口之后，“激活协议迁移”才可用。

步骤 4 如果使用 STP 发现了链路伙伴，请单击**激活协议迁移**运行协议迁移测试。这可确定使用 STP 的链路伙伴是否仍然存在，如果存在，可确定该链路伙伴是否已迁移到 RSTP。如果其仍作为 STP 链路存在，则设备将继续使用 STP 与其进行通信。或者，如果它已经迁移到 RSTP，设备将相应地使用 RSTP。

步骤 5 选择一个接口，并单击**编辑**。此时将显示*编辑 RSTP 接口设置*页面。

步骤 6 输入参数

- **接口** - 设置接口，并指定要配置 RSTP 的端口或 LAG。
- **点到点管理状态** - 定义点到点的链路状态。定义为全双工的端口会被视为点到点端口链路。
  - *启用* - 如果启用了此功能，该端口便是一个 RSTP 边缘端口，它可以迅速地进入转发模式 （通常在 2 秒以内）。
  - *禁用* - 不会出于 RSTP 目的将该端口视为点到点端口，这表示 STP 在该端口上将以正常速度而非高速工作。
  - *自动* - 使用 RSTP BPDU 自动确定交换机状态。
- **点到点运行状态** - 如果将**点到点运行状态**设置为 “自动”，则显示点到点运行状态。
- **角色** - 显示由 STP 指定的端口角色，以提供 STP 路径。可能的角色有：
  - *根* - 将数据包转发给根网桥的最低成本路径。
  - *指定* - 网桥通过其连接至 LAN 的接口，可提供从 LAN 到根网桥的最低成本路径。

- *备选* - 提供从根接口到根网桥的备用路径。
- *备份* - 提供指向生成树叶节点的指定端口路径的备份路径。这会提供一种配置，其中一个环路中的两个端口会通过一条点到点链路进行连接。如果 LAN 具有两条或更多条已建立的、至一个共享网段的连接，则也会使用备份端口。
- *已禁用* - 端口不会加入生成树。

- **模式** - 显示目前的生成树模式：传统 STP 或 RSTP。
- **快速链路运行状态** - 显示接口上的快速链路 （边缘端口）模式状态：已启用、已禁用或自动。这些值包括：
  - *已启用* - 启用快速链路。
  - *已禁用* - 禁用快速链路。
  - *自动* - 在接口开始活动后的几秒内启用快速链路模式。
- **端口状态** - 显示特定端口上的 RSTP 状态。
  - *已禁用* - 目前在端口上禁用 STP。
  - *阻塞* - 端口目前被阻塞，其无法转发流量或学习 MAC 地址。
  - *监听* - 端口处于监听模式。端口无法转发流量，也无法学习 MAC 地址。
  - *学习* - 端口处于学习模式。端口无法转发流量，但能够学习新的 MAC 地址。
  - *转发* - 端口处于转发模式。端口可以转发流量且学习新的 MAC 地址。

步骤 7 单击**应用**。将更新当前配置文件。

14

管理 MAC 地址表

本节介绍了如何将 MAC 地址添加到系统。具体包括以下主题：

- 配置静态 MAC 地址
- 管理动态 MAC 地址

MAC 地址的类型

有两种类型的 MAC 地址：静态地址和动态地址。根据 MAC 地址的类型，可将其与 VLAN 和端口信息一起存储在*静态地址*表或*动态地址*表中。

静态地址由用户进行配置，因此不会过期。

在到达交换机的帧中显示的新源 MAC 地址会添加到动态地址表中。此 MAC 地址会根据配置保留一段时间。如果在这段时间结束之前没有使用相同源 MAC 地址的其他帧到达交换机，则 MAC 条目将过期并从动态地址表中删除。

当帧到达交换机时，交换机会搜索静态或动态地址表中响应 / 匹配的目的 MAC 地址。如果找到匹配项，则将此帧标记为通过地址表中指定的端口输出。如果帧的目的 MAC 地址不在这两个地址表中，则会将这些帧传输 / 广播到相应 VLAN 上的所有端口。此类帧也称为未知的单播帧。

交换机最多支持 8,000 个静态和动态 MAC 地址。

配置静态 MAC 地址

可以将静态 MAC 地址分配给交换机上的特定物理接口和 VLAN。如果在其他接口上检测到静态地址，那么，系统会忽略该地址，也不会将其写入地址表。

定义静态地址的步骤：

步骤 1 单击 **MAC 地址表 > 静态地址**。将打开*静态地址*页面。

*静态地址*页面会显示已定义的静态地址。

步骤 2 单击**添加**。将打开*添加静态地址*页面。

步骤 3 输入参数。

- **VLAN ID** - 为端口选择 VLAN ID。
- **MAC 地址** - 输入接口 MAC 地址。
- **接口** - 为条目选择一个接口 （端口或 LAG）。
- **状态** - 选择条目的处理方式。选项如下：
  - *永久* - 系统永远不会删除此 MAC 地址。如果静态 MAC 地址保存在启动配置中，则重启后会保留该地址。
  - *重置即删除* - 重置设备时，会删除静态 MAC 地址。
  - *超时即删除* - 当该 MAC 地址过期时将其删除。
  - *安全* - 当接口为传统锁定模式 （请参阅**配置端口安全**）时， MAC 地址是安全的。

步骤 4 单击**应用**。将在地址表中显示一个新条目。

管理动态 MAC 地址

动态地址表 （桥接表）中包含通过监控进入交换机的帧源地址而获取的 MAC 地址。

为了防止此表溢出并为新 MAC 地址腾出空间，如果在特定的时间段内没有接收到相应的流量，系统会删除该地址。该时间段为过期间隔。

配置动态 MAC 地址过期时间

配置动态地址过期间隔的步骤：

步骤 1 单击 **MAC 地址表 > 动态地址设置**。将打开*动态地址设置*页面。

步骤 2 在**过期时间**字段中输入值。过期时间值介于用户配置的值与该值的两倍减 1 之间。例如，如果输入 300 秒，则过期时间将介于 300 到 599 秒之间。

步骤 3 单击**应用**。将更新过期时间。

查询动态地址

查询动态地址的步骤：

步骤 1 单击 **MAC 地址表 > 动态地址**。将打开*动态地址*页面。

步骤 2 在*过滤*框中，您可以输入以下查询条件：

- **VLAN ID** - 输入要在地址表中查询的 VLAN ID。
- **MAC 地址** - 输入要在地址表中查询的 MAC 地址。
- **接口** - 选择要在地址表中查询的接口。查询功能可以搜索特定单元 / 插槽、端口或 LAG。

步骤 3 在**动态地址表排序关键字**字段中输入值以作为地址表的排序依据。地址表可以按 VLAN ID、 MAC 地址或接口进行排序。

步骤 4 单击**转至**。将对动态 MAC 地址表进行查询并显示结果。

要删除所有动态 MAC 地址，请单击**清除表**。

15

配置组播转发

本节介绍了组播转发功能，具体包括以下主题：

- **组播转发**
- **定义组播属性**
- **添加 MAC 组地址**
- **添加 IP 组播组地址**
- **配置 IGMP Snooping**
- **MLD Snooping**
- **查询 IGMP/MLD IP 组播组**
- **定义组播路由器端口**
- **定义 “全部转发”组播**
- **定义未注册的组播设置**

组播转发

组播转发实现了一对多的信息传递。组播应用对于将信息传递给多个客户端非常有用，在这种情况下客户端不需要接收全部内容。类似于有线电视的服务是一种典型应用，在这种情况下客户端可以加入传输中心的频道，并在结束之前离开。

仅将数据发送给相关端口。仅对相关端口转发数据可节省链接上的带宽和主机资源。

要使组播转发能够在 IP 子网间正常工作，节点和路由器必须能进行组播。能进行组播的节点必须能够：

- 发送和接收组播数据包。
- 通过本地路由器注册节点正在监听的组播地址，以便本地路由器和远程路由器可以将组播数据包路由到节点。

典型的组播设置

当组播路由器在 IP 子网间路由组播数据包时，能进行组播的第 2 层交换机会将组播数据包转发到 LAN 或 VLAN 中已注册的节点。

典型设置包括在专用和 / 或公共 IP 网络间转发组播流的路由器、采用 Internet 组成员协议 (IGMP) 监听功能或组播侦听器发现 (MLD) 监听的交换机以及要接收组播流的组播客户端。在此设置中，路由器会定期发送 IGMP 查询。

注 针对 IPv6 的 MLD 衍生自针对 IPv4 的 IGMP v2。虽然本节中主要介绍的是 IGMP，但也涵盖了对 MLD 的隐含介绍。

这些查询会访问交换机，该交换机转而会将查询泛洪到 VLAN，并且也会学习其中包含组播路由器 (Mrouter) 的端口。当主机接收到 IGMP 查询消息时，它会通过 IGMP 加入消息作出响应，表示该主机要接收特定组播流，并且可有选择地从特定源进行接收。使用 IGMP Snooping 的交换机会分析加入消息，并了解到必须将主机所请求的组播流转发到此特定端口。然后，交换机会只将 IGMP 加入转发到 Mrouter。同样地，当 Mrouter 接收到 IGMP 加入消息后，会了解到它接收加入消息的接口要接收特定组播流。 Mrouter 会将请求的组播流转发到该接口。

组播操作

在第 2 层组播服务中，第 2 层交换机会接收发送给特定组播地址的单帧。它会为在每个相关端口上传输的帧创建副本。

当交换机启用 IGMP/MLD Snooping 并接收组播流的帧时，它会将组播帧转发到经过注册可使用 IGMP 加入消息接收组播流的所有端口。

交换机可根据以下选项之一转发组播流：

- 组播 MAC 组地址
- IP 组播组地址 (G)
- 组播数据包的源 IP 地址 (S) 和目的 IP 组播组地址 (G) 的组合。

可以为每个 VLAN 配置上述选项之一。

系统会维护每个 VLAN 的组播组列表，并且这会管理每个端口应接收的组播信息。使用 IGMP 或组播侦听器发现 (MLD) 协议监听可以静态地配置或动态地学习组播组及其进行接收的端口。

组播注册

组播注册是监听组播注册协议并对其作出响应的程序。提供的协议有针对 IPv4 的 IGMP 和针对 IPv6 的 MLD 协议。

当在 VLAN 上启用交换机中的 IGMP/MLD Snooping 时，该交换机会分析其接收的所有 IGMP/MLD 数据包 （来自连接到交换机的 VLAN 和网络中的组播路由器）。

当交换机了解到主机正在使用 IGMP/MLD 消息进行注册以接收组播流时 （或者从特定源进行接收），该交换机会在其组播转发数据库中添加注册。

IGMP/MLD Snooping 可有效减少来自带宽密集型串流 IP 应用程序的组播流量。使用 IGMP/MLD Snooping 的交换机只会将组播流量转发给对需要该流量的主机。这种组播流程的减少还会减少交换机上处理的数据包，也会减少终端主机上的工作负荷，这是因为它们不必接收和过滤网络中生成的所有组播流量。

系统可支持以下版本：

- IGMP v1/v2/v3
- MLD v1/v2

组播地址属性

组播地址具有以下属性：

- 每个 IPv4 组播地址均处于 224.0.0.0 到 239.255.255.255 的地址范围之内。
- IPv6 组播地址为 FF00:/8。
- 将 IP 组播组地址映射至第 2 层组播地址的步骤：
  - 通过从 IPv4 地址中取得 23 个低序位并将它们添加到 01:00:5e 前缀之后，可以映射 IPv4。标准情况下，前九位 IP 地址会被忽略，并且会将任何仅不同于这前几位值的 IP 地址映射至同一第 2 层地址，这是因为所使用的后 23 位相同。例如，会将 234.129.2.3 映射至 MAC 组播组地址 01:00:5e:01:02:03。会将最多 32 个 IP 组播组地址映射至同一第 2 层地址。
  - 通过取得 32 个低序位组播地址并添加前缀 33:33，可映射 IPv6。例如，会将 IPv6 组播地址 FF00:1122:3344 映射至第 2 层组播 33:33:11:22:33:44。

定义组播属性

使用*属性*页面可配置网桥组播过滤状态。

默认情况下，会将所有组播帧泛洪到 VLAN 的所有端口。要选择性地仅转发到相关端口并过滤 （丢弃）其余端口上的组播，请在*属性*页面*中启用网桥组播过滤状态。*

如果启用过滤，则会将组播帧转发到相关 VLAN 中端口的子网，如组播转发数据库中所定义。将对所有流量实施组播过滤。默认情况下，会将此类流量泛洪到所有相关端口，但是您可以限制转发到较小的子网。

表示组播成员关系的常见方法是 (S,G) 标记法，其中 "S" 是指发送数据组播流的 （单个）源，"G" 是指 IPv4 或 IPv6 组地址。如果组播客户端可以从特定组播组的任何源接收组播流量，则写作 (*,G)。

以下是转发组播帧的方法：

- **MAC 组地址** - 根据以太网帧中的目的 MAC。

  注 如上所述，可将一个或多个 IP 组播组地址映射至一个 MAC 组地址。根据 MAC 组地址进行转发，可导致 IP 组播流被转发至没有流接收器的端口。

- **IP 组地址** - 根据 IP 数据包的目的 IP 地址 (*,G)。
- **源特定 IP 组地址** - 根据 IP 数据包的目的 IP 地址和源 IP 地址 (S,G)。

通过选择转发模式，您可以定义硬件用来确定按以下选项之一的组播流量的方法：“MAC 组地址”、“IP 组地址”或 “源特定 IP 组地址”。

IGMPv3 和 MLDv2 支持 (S,G)，而 IGMPv1/2 和 MLDv1 仅支持恰好为组 ID 的 (*.G)。

交换机最多支持 256 个静态和动态组播组地址。

启用组播过滤并选择转发方法的步骤：

步骤 1 单击**组播 > 属性**。将打开*属性*页面。

步骤 2 输入参数。

- **网桥组播过滤状态** - 选择该选项可启用过滤功能。
- **VLAN ID** - 选择 VLAN ID 可设置其转发方法。
- **IPv6 的转发方法** - 将以下方法之一设置为 IPv6 地址的转发方法：“MAC 组地址”、“IP 组地址”或 “源特定 IP 组地址”。
- **IPv4 的转发方法** - 将以下方法之一设置为 IPv4 地址的转发方法：“MAC 组地址”、“IP 组地址”或 “源特定 IP 组地址”。

步骤 3 单击**应用**。将更新当前配置文件。

添加 MAC 组地址

交换机支持根据组播组信息转发传入的组播流量。此信息衍生自接收到的或作为手动配置结果的 IGMP/MLD 数据包，并存储在组播转发数据库 (MFDB) 中。

当从 VLAN （配置为根据 MAC 组地址转发组播流）接收帧并且其目的地址为第 2 层组播地址时，会将该帧转发到作为 MAC 组地址成员的所有端口。

*MAC 组地址*页面具有以下功能：

- 查询并查看来自 MFDB 的与特定 VLAN ID 或特定 MAC 地址组相关的信息。可通过 IGMP/MLD Snooping 动态获取或通过手动输入静态获取此数据。
- 添加或删除 MFDB 的静态条目，该 MFDB 可根据 MAC 目的地址来静态转发信息。
- 显示作为每个 VLAN ID 和 MAC 地址组成员的所有端口 /LAG 的列表，并输入是否对其转发流量。

要在模式为 *IP 地址组*或 *IP 和源组*时查看转发信息，请使用 *IP 组播组地址*页面。

定义和查看 MAC 组播组的步骤：

步骤 1 单击**组播 > MAC 组地址**。将打开 *MAC 组地址*页面。

步骤 2 输入参数。

- **VLAN ID 为** - 设置要显示的组的 VLAN ID。
- **MAC 组地址为** - 设置要显示的组播组的 MAC 地址。如果未指定 MAC 组地址，页面将显示来自所选 VLAN 的所有 MAC 组地址。

步骤 3 单击 **转至**，将在下侧块中显示 MAC 组播组地址。

此时将显示在此页面和 *IP 组播组地址*页面创建的条目。对于那些在 *IP 组播组地址页面*中创建的条目， IP 地址将转换为 MAC 地址。

步骤 4 单击**添加**以添加静态 MAC 组地址。将打开*添加 MAC 组地址*页面。

步骤 5 输入参数。

- **VLAN ID** - 定义新组播组的 VLAN ID。
- **MAC 组地址** - 定义新组播组的 MAC 地址。

步骤 6 单击**应用**， MAC 组播组将写入当前配置文件。

要配置和显示组中接口的注册，请选择一个地址，然后单击**详情**。将打开 *MAC 组地址设置*页面。

该页面显示：

- **VLAN ID** - 定于组播组的 VLAN ID。
- **MAC 组地址** - 组的 MAC 地址。

步骤 7 从**过滤器：接口类型**菜单中选择要显示的端口或 LAG。

步骤 8 单击**转至** 以显示端口或 LAG 成员关系。

步骤 9 选择每个接口与组播组进行关联的方法：

- **静态** - 将接口作为静态成员连接到组播组。
- **动态** - 表示由于 IGMP/MLD Snooping 已将接口添加到组播组。
- **已禁止** - 指定禁止此端口加入此 VLAN 上的这个组。
- **无** - 指定端口目前不是此 VLAN 上该组播组的成员。

步骤 10 单击 **应用**，将更新当前配置文件。

注 无法在此页面中删除在 *IP 组播组地址*页面中创建的条目 （即使已选定这些条目）。

添加 IP 组播组地址

除组播组由 IP 地址确定之外， *IP 组播组地址*页面与 *MAC 组地址*页面*在其他方面均相似。*

使用 *IP 组播组地址*页面可查询和添加 IP 组播组。

定义和查看 IP 组播组的步骤：

步骤 1 单击**组播 > IP 组播组地址**。将打开 *IP 组播组地址*页面。

该页面显示通过 Snooping 学习的所有 IP 组播组地址。

步骤 2 输入进行过滤所需的参数。

- **VLAN ID 为** - 定义要显示的组的 VLAN ID。
- **IP 版本为** - 选择 IPv6 或 IPv4。

- **IP 组播组地址为** - 定义要显示的组播组的 IP 地址。这仅在转发模式为 (S,G) 时才相关。
- **源 IP 地址为** - 定义发送设备的源 IP 地址。如果模式为 (S,G)，则输入发送者 S。这与 IP 组地址一起作为要显示的组播组 ID (S,G)。如果模式为 (*,G)，则输入 * 以表示组播组仅由目的定义。

步骤 3 单击**转至**。结果将显示在选择下侧块中。在处于第 2 层系统模式下的交换机上启用 Bonjour 和 IGMP 后，将显示 Bonjour 的 IP 组播地址。

步骤 4 单击**添加**以添加静态 IP 组播组地址。将打开*添加 IP 组播组地址*页面。

步骤 5 输入参数。

- **VLAN ID** - 定义要添加的组的 VLAN ID。
- **IP 版本** - 选择 IP 地址类型。
- **IP 组播组地址** - 定义新组播组的 IP 地址。
- **源特定** - 表示该条目包含特定源，并在 “IP 源地址” 字段中添加地址。否则，该条目将添加为 (*,G) 条目，即来自任何 IP 源的 IP 组地址。
- **IP 源地址** - 定义要包括的源地址。

步骤 6 单击**应用**。将添加 IP 组播组，并更新设备。

步骤 7 要配置和显示 IP 组地址的注册，请选择一个地址，然后单击**详情**。将打开 *IP 组播接口设置*页面。

选定的 VLAN ID、IP 版本、IP 组播组地址和源 IP 地址将以只读的方式显示在窗口的顶端。您可以选择过滤器类型：

- **接口类型为** - 选择显示端口还是 LAG。

步骤 8 为每个接口选择其关联类型。选项如下：

- **静态** - 将接口作为静态成员连接到组播组。
- **已禁止** - 指定禁止将此端口添加到此 VLAN 上的这个组。
- **无** - 表示端口目前不是此 VLAN 上该组播组的成员。默认情况下选定此项，直到选择 “静态” 或 “已禁止”。

步骤 9 单击**应用**。将更新当前配置文件。

配置 IGMP Snooping

要支持选择的组播转发 (IPv4)，必须启用网桥组播过滤 （在*属性*页面中），并且必须针对每个相关 VLAN 全局启用 IGMP Snooping。（在 *IGMP Snooping* 页面中）。

默认情况下，第 2 层交换机会将组播帧转发到相关 VLAN 的所有端口，实质上似乎是将帧作为广播进行处理。使用 IGMP Snooping，交换机会将组播帧转发到已注册组播客户端的端口。

注 交换机仅在静态 VLAN 上支持 IGMP Snooping。它不支持动态 VLAN 上的 IGMP Snooping。

全局启用 IGMP Snooping 后，所有 IGMP 数据包都将被转发至 CPU。 CPU 则会分析传入的数据包，然后确定以下信息：

- 哪些端口要求加入哪个 VLAN 上的哪些组播组。
- 将哪些端口连接到了生成 IGMP 查询的组播路由器 (Mrouter)。
- 哪些端口正在接收 PIM、 DVMRP 或 IGMP 查询协议。

这些信息均显示在 *IGMP Snooping* 页面上。

要求加入特定组播组的端口将发送 IGMP 报告来指定主机要加入的组。这将在组播转发数据库中创建转发条目。

在 VLAN 上启用 IGMP Snooping 并识别作为 IGMP Snooping 查询器的交换机的步骤：

步骤 1 单击**组播** > **IGMP Snooping**。将打开 *IGMP Snooping* 页面。

步骤 2 启用或禁用 “IGMP Snooping 状态”。

全局启用 IGMP Snooping 时，监控网络流量的设备可确定哪些主机已请求接收组播流量。

仅当同时启用 IGMP Snooping 和网桥组播过滤时，交换机才会执行 IGMP Snooping。

步骤 3 选择一个 VLAN，然后单击**编辑**。将打开*编辑 IGMP Snooping* 页面。

步骤 4 输入参数。

- **VLAN ID** - 选择其中定义 IGMP Snooping 的 VLAN ID。
- **IGMP Snooping 状态** - 启用或禁用选定 VLAN 的网络流量监控。
- **运行 IGMP 的 Snooping 状态** - 为选定 VLAN 显示 IGMP Snooping 的当前状态。
- **组播路由器端口自动学习** - 启用或禁用自动学习 Mrouter 所连接的端口。

- **查询健壮性** - 输入当此交换机是选择的查询器时要使用的健壮性变量值。
- **运行查询健壮性** - 显示选择的查询器所发送的健壮性变量。
- **查询间隔** - 输入当此交换机是选择的查询器时要使用的普通查询的时间间隔。
- **运行查询间隔** - 由所选查询器发送的普通查询的时间间隔 （以秒为单位）。
- **查询最大响应间隔** - 输入用来计算插入定期普通查询的最大响应代码的延迟时间。
- **运行查询最大响应间隔** - 显示由所选查询器发送的普通查询中包括的 “查询最大响应间隔”。
- **最近成员查询计数器** - 输入交换机中假定不再存在组成员之前所发送的特定于 IGMP 组的查询数 （如果该交换机是选择的查询器）。
- **最近成员运行查询计数器** - 显示 “最近成员查询计数器”的运行值。
- **最近成员查询间隔** - 输入要使用的最大响应延迟时间 （如果交换机无法从所选查询器发送的特定于组的查询读取最大响应时间值）。
- **最近成员运行查询间隔** - 显示由所选查询器发送的 “最近成员查询间隔”。
- **立即离开** - 启用 “立即离开”可减少当在成员端口上接收 IGMP 组离开消息时阻止将组播流发送到该端口所花费的时间。

步骤 5 单击**应用**。将更新当前配置文件。

MLD Snooping

主机使用 MLD 协议来报告它们在组播会话中的参与情况，而交换机则使用 MLD Snooping 来构建组播成员关系列表。它使用这些列表来将组播数据包仅转发到其中存在作为组播组成员的主机节点的交换机端口。交换机不支持 MLD 查询器。

主机使用 MLD 协议来报告组播会话中这些主机的参与情况。

交换机支持两个版本的 MLD Snooping：

- MLDv1 Snooping 检测 MLDv1 控制数据包，并根据 IPv6 目的组播地址设置流量桥接。
- MLDv2 Snooping 使用 MLDv2 控制数据包，根据源 IPv6 地址和目的 IPv6 组播地址转发流量。

实际的 MLD 版本由网络中的组播路由器选择。

通过一种类似于 IGMP Snooping 的方法，可在交换机将 MLD 帧从多个工作站转发到一个上行组播路由器时侦听这些帧，反之亦然。此设备可使交换机能够推断以下信息：

- 想要加入特定组播组的工作站位于哪些端口上
- 发送组播帧的组播路由器位于哪些端口上

这些信息用于从传入组播帧的转发集中排除不相关的端口 （这些端口上没有经过注册可接收特定组播组的工作站）。

除手动配置的组播组之外，如果您还启用了 MLD Snooping，则结果是衍生自手动设置和通过 MLD Snooping 的动态发现的组播组和端口成员关系的联合。重启系统时，只会保留静态定义。

启用 MLD Snooping 的步骤：

步骤 1 单击**组播** > **MLD Snooping**。将打开 *MLD Snooping* 页面。

步骤 2 启用或禁用 **MLD Snooping 状态**。全局启用 MLD Snooping 时，监控网络流量的设备可确定哪些主机已请求接收组播流量。如果同时启用了 MLD Snooping 和网桥组播过滤，则交换机将执行 MLD Snooping。

步骤 3 选择一个 VLAN，然后单击**编辑**。将打开*编辑 MLD Snooping* 页面。

步骤 4 输入参数。

- **VLAN ID** - 选择 VLAN ID。
- **MLD Snooping 状态** - 在 VLAN 上启用或禁用 MLD Snooping。交换机会监控网络流量，以确定哪些主机已要求接收组播流量。仅当同时启用 MLD Snooping 和网桥组播过滤时，交换机才会执行 MLD Snooping。
- **运行 MLD Snooping 状态** - 为选择的 VLAN 显示 MLD Snooping 的当前状态。
- **组播路由器端口自动学习** - 启用或禁用自动学习组播路由器。
- **查询健壮性** - 输入要使用的健壮性变量值 （如果交换机无法从所选查询器发送的消息读取此值）。
- **运行查询健壮性** - 显示选择的查询器所发送的健壮性变量。
- **查询间隔** - 输入交换机要使用的 “查询间隔” 间隔值 （如果该交换机无法从所选查询器发送的消息获取此值）。
- **运行查询间隔** - 从所选查询器接收的普通查询的时间间隔 （以秒为单位）。
- **查询最大响应间隔** - 输入要使用的查询最大响应延迟时间 （如果交换机无法从所选查询器发送的普通查询读取最大响应时间值）。

- **运行查询最大响应间隔** - 显示用来计算插入普通查询的最大响应代码的延迟时间。
- **最近成员查询计数器** - 输入要使用的最后成员查询次数 （如果交换机无法从所选查询器发送的消息获取此值）。
- **最近成员运行查询计数器** - 显示 “最近成员查询计数器”的运行值。
- **最近成员查询间隔** - 输入要使用的最大响应延迟时间 （如果交换机无法从所选查询器发送的特定于组的查询读取最大响应时间值）。
- **最近成员运行查询间隔** - 由所选查询器发送的 “最近成员查询间隔”。
- **立即离开** - 启用该选项时，将减少用来阻止发送到交换机端口的多余 MLD 流量的时间。

步骤 5 单击**应用**。将更新当前配置文件。

查询 IGMP/MLD IP 组播组

*IGMP/MLD IP 组播组*页面显示从 IGMP/MLD 消息学习的 IPv4 和 IPv6 组地址。

此页面上的信息与 *MAC 组地址*等页面*上所显示的信息可能有所不同*。假定系统位于基于 MAC 的组和请求加入以下组播组 224.1.1.1 和 225.1.1.1 的端口中，两者均被映射到同一 MAC 组播地址 01:00:5e:01:01:01 中。在这种情况下， *MAC 组播*页面中有一个条目，而此页面上则有两个条目。

查询 IP 组播组的步骤：

步骤 1 单击**组播** > **IGMP/MLD IP 组播组**。将打开 *IGMP/MLD IP 组播组*页面。

步骤 2 设置要搜索的侦听组类型：IGMP 或 MLD。

步骤 3 输入以下查询过滤条件的一部分或全部：

- **组地址为** - 定义要查询的组播组 MAC 地址或 IP 地址。
- **源地址为** - 定义要查询的发送者地址。
- **VLAN ID 为** - 定义要查询的 VLAN ID。

步骤 4 单击**转至**。将为每个组播组显示以下字段：

- **VLAN** - VLAN ID。
- **组地址** - 组播组 MAC 地址或 IP 地址。
- **源地址** - 所有指定组端口的发送者地址。

- **包括的端口** - 组播流目的端口的列表。
- **排除的端口** - 不包括在组中的端口的列表。
- **兼容模式** - 通过交换机在 IP 组地址上接收的主机注册的最旧版本的 IGMP/MLD。

定义组播路由器端口

组播路由器 (Mrouter) 端口是连接至组播路由器的端口。当交换机转发组播流和 IGMP/MLD 注册消息时，会包括组播路由器端口编号。为使所有组播路由器都可以反过来将组播流转发到其他子网并将注册消息传递到其他子网，这是必需的。

静态配置或动态监测端口连接至组播路由器的步骤：

步骤 1 单击**组播** > **组播路由器端口**。将打开*组播路由器端口*页面。

步骤 2 输入以下查询过滤条件的一部分或全部：

- **VLAN ID 为** - 为介绍的路由器端口选择 VLAN ID。
- **IP 版本为** - 选择组播路由器支持的 IP 版本。
- **接口类型为** - 选择显示端口还是 LAG。

步骤 3 单击**转至**。此时将显示与查询条件相匹配的接口。

步骤 4 为每个端口选择其关联类型。选项如下：

- **静态** - 将端口静态配置为组播路由器端口。
- **动态** - （仅显示）通过 MLD/IGMP 查询将端口动态配置为组播路由器端口。要启用动态学习组播路由器端口，请转至**组播** > **IGMP Snooping** 和**组播** > **MLD Snooping** 页面。
- **已禁止** - 不将此端口配置为组播路由器端口，即使此端口上接收 IGMP 或 MLD 查询。如果端口上已启用 “已禁止”，此端口上将无法学习组播路由器 （即此端口上未启用 “组播路由器端口自动学习”）。
- **无** - 端口当前不是组播路由器端口。

步骤 5 单击**应用**更新交换机。

定义 “全部转发”组播

使用*全部转发*页面可启用并显示要从特定 VLAN 接收组播流的端口和 / 或 LAG 的配置。此功能需要在*属性*页面中启用网桥组播过滤。如果禁用网桥组播过滤，则所有组播流量均会被泛洪到交换机中的所有端口。

如果连接到端口的设备不支持 IGMP 和 / 或 MLD，您可以将该端口静态配置为 “全部转发”。

IGMP 或 MLD 消息不会被转发到定义为*全部转发*的端口。

注 该配置仅会影响作为所选 VLAN 的成员的端口。

定义 “全部转发”组播的步骤：

步骤 1 单击**组播** > **全部转发**。将打开*全部转发*页面。

步骤 2 定义以下选项：

- **VLAN ID 为** - 将显示的端口 /LAG 的 VLAN ID。
- **接口类型为** - 定义显示端口还是 LAG。

步骤 3 单击**转至**。此时将显示所有端口 /LAG 的状态。

步骤 4 选择要通过使用以下方法来定义为 “全部转发”的端口 /LAG：

- **静态** - 端口接收所有组播流。
- **已禁止** - 端口无法接收任何组播流，即使 IGMP/MLD Snooping 已指定端口加入组播组。
- **无** - 端口当前不是 “全部转发”端口。

步骤 5 单击**应用**。将更新当前配置文件。

定义未注册的组播设置

一般会将组播帧转发到 VLAN 中的所有端口。如果启用 IGMP/MLD Snooping，交换机将学习组播组的存在，并监控哪些端口已加入哪些组播组。还可以静态配置组播组。动态学习或静态配置的组播组均被视为已注册。

交换机会将组播帧 （从已注册的组播组）仅转发到注册至组播组的端口。

使用*未注册的组播*页面可处理属于不为交换机所知的组 （未注册的组播组）的组播帧。通常会将未注册的组播帧转发到 VLAN 中的所有端口。

您可以选择一个端口来接收或过滤未注册的组播流。该配置适用于作为成员 （将成为成员）的任何 VLAN。

此功能可确保客户仅接收请求的组播组，而不接收可能在网络中传输的其他组播组。

定义未注册的组播设置的步骤：

步骤 1 单击**组播** > **未注册的组播**。将打开*未注册的组播*页面。

步骤 2 定义以下选项：

- **接口类型为** - 作为所有端口或所有 LAG 的视图。
- **端口 /LAG** - 显示端口 ID 或 LAG ID。
- **未注册的组播** - 显示所选接口的转发状态。可能的值包括：
  - *转发* - 可将未注册的组播帧转发到选择的接口。
  - *过滤* - 可过滤 （拒绝）到所选接口的未注册的组播帧。

步骤 3 单击**应用**。将保存设置，并更新当前配置文件。

16

配置 IP 信息

IP 接口地址由用户手动配置或由 DHCP 服务器自动配置。本节介绍关于手动定义交换机 IP 地址，或通过将交换机设置为 DHCP 客户端来定义其 IP 地址的信息。

本节包含以下主题：

- 管理与 IP 接口
- 配置 ARP
- 域名系统

管理与 IP 接口

第 2 层 IP 寻址

交换机的管理 VLAN 中有一个单独的 IP 地址。此 IP 地址和默认网关可手动配置，也可由 DHCP 进行配置。静态 IP 地址和默认网关在 *IPv4 接口*页面上进行配置。交换机使用默认网关（如果已配置）来和与该交换机机位于不同 IP 子网的设备进行通信。默认情况下， VLAN 1 为管理 VLAN，但可修改此设置。仅可通过交换机的管理 VLAN 在配置的 IP 地址上访问交换机。

IP 地址配置的出厂默认设置为 *DHCP*。这表示交换机被用作 DHCP 客户端，并在启动期间发出 DHCP 请求。

如果交换机收到 DHCP 服务器使用 IP 地址进行的 DHCP 响应，它会发送地址解析协议 (ARP) 数据包，来确认该 IP 地址是唯一的。如果 ARP 响应显示该 IP 地址正在使用中，则交换机会向提供 IP 地址的 DHCP 服务器发送一条 DHCPDECLINE 消息，并发送另一个重新启动该过程的 DHCPDISCOVER 数据包。

如果交换机在 60 秒内未收到 DHCP 响应，它会继续发送 DHCPDISCOVER 查询并采用默认 IP 地址：192.168.1.254/24.

如果同一 IP 子网内的多个设备使用同一 IP 地址，则会发生 IP 地址冲突。地址冲突需要对与交换机发生冲突的 DHCP 服务器和 / 或设备执行管理操作。

将 VLAN 配置为使用动态 IP 地址时，交换机会发出 DHCP 请求，直到 DHCP 服务器为其分配 IP 地址。管理 VLAN 可以使用静态或动态 IP 地址进行配置。

交换机的 IP 地址分配规则如下：

- 除非使用静态 IP 地址配置交换机，否则交换机会发出 DHCP 请求，直到收到 DHCP 服务器的响应。
- 如果交换机上的 IP 地址发生更改，交换机会向相应的 VLAN 发出免费 ARP 数据包，来检查 IP 地址冲突问题。将交换机恢复到默认 IP 地址时，此规则也适用。
- 收到来自 DHCP 服务器的新的唯一 IP 地址时，系统状态 LED 会产生变化。如果已设置静态 IP 地址，则系统状态 LED 也会变为以绿色持续亮起。如果交换机正获取 IP 地址并且当前正在使用出厂默认 IP 地址 192.168.1.254，则 LED 会闪烁。
- 如果客户端必须在其到期日期之前通过 DHCPREQUEST 消息续租，则相同的规则也适用。
- 在出厂默认设置下，如果没有静态定义的 IP 地址或 DHCP 获取的 IP 地址可用，则会使用默认 IP 地址。有其他 IP 地址可用时，会自动使用这些地址。默认 IP 地址始终在管理 VLAN 上。

定义 IPv4 接口

要使用基于 Web 的交换机配置实用程序管理交换机，必须定义并知道 IPv4 交换机管理 IP 地址。交换机 IP 地址可以手动配置或从 DHCP 服务器自动获得。

配置 IPv4 交换机 IP 地址的步骤：

步骤 1 单击 **管理 > 管理接口 > IPv4 接口**。将打开 *IPv4 接口*页面。

步骤 2 为以下字段输入值：

- **管理 VLAN** - 选择用于通过 Telnet 或 Web GUI 来访问交换机的管理 VLAN。VLAN1 为默认的管理 VLAN。
- **IP 地址类型** - 选择以下其中一个选项：
  - *动态* - 使用 DHCP 从管理 VLAN 发现 IP 地址。
  - *静态* - 手动定义静态的 IP 地址。

  注 如果设备为 DHCP 客户端，则支持 DHCP 选项 12 （主机名选项）。如果 DHCP 选项 12 是从 DHCP 服务器获取的，则会保存为该服务器的主机名。交换机不会发出 DHCP 选项 12 请求。无论哪种请求， DHCP 服务器均必须配置为发送选项 12，才能使用此功能。

如果使用静态 IP 地址，请配置以下字段。

- **IP 地址** - 输入 IP 地址，并配置以下其中一个字段：
  - **网络掩码** - 选择并输入 IP 地址掩码。
  - **前缀长度** - 选择并输入 IPv4 地址前缀的长度。
- **管理默认网关** - 选择**用户定义**并输入默认网关 IP 地址，或选择**无**以从接口中删除选择的默认网关 IP 地址。
- **运行默认网关** - 显示当前的默认网关状态。

  注 如果未使用默认网关配置交换机，则它无法与同一 IP 子网内的其他设备进行通信。

如果从 DHCP 服务器检索动态 IP 地址，请选择以下启用的字段：

- **立即更新 IP 地址** - 可在 DHCP 服务器分配 IP 地址后的任何时间更新交换机动态 IP 地址。请注意，根据您的 DHCP 服务器配置，交换机可能会在续订后收到新的 IP 地址，从而需要将基于 Web 的交换机配置实用程序设置为新的 IP 地址。
- **通过 DHCP 进行自动配置** - 显示自动配置功能的状态。您可以通过 *管理* > *文件管理* > *DHCP 自动配置*配置此功能。

步骤 3 单击**应用**。 IPv4 接口设置将写入当前配置文件。

管理 IPv6

Internet 协议版本 6 (TCP/IPv6) 是一种网络层协议，用于数据包交换的互联网。设计 IPv6 是为了替换占据主导的 Internet 协议 IPv4。

由于地址大小从 32 位地址增加到 128 位地址，因此 IPv6 在分配 IP 地址方面有更大弹性。 IPv6 地址写为八组十六进制数 （四位一组），例如，FE80:0000:0000:0000:0000:9C00:876A:130B。缩写形式也可接受，其中可将由零组成的组省略并用 “::” 替换，例如， ::-FE80::9C00:876A:130B。

IPv6 节点需要使用中间映射机制来与仅使用 IPv4 网络的其他 IPv6 节点进行通信。此机制称为隧道，可让仅使用 IPv6 的主机获得 IPv4 服务，并让独立的 IPv6 主机和网络访问 IPv4 基础架构上的 IPv6 节点。

隧道使用 ISATAP 机制。此协议将 IPv4 网络视为虚拟的 IPv6 本地链路，该链路将每个 IPv4 地址映射到一个链路本地 IPv6 地址。

交换机会根据 IPv6 Ethertype 检测 IPv6 帧。

定义 IPv6 全局配置

*IPv6 全局配置*页面可定义交换机生成的 IPv6 ICMP 错误消息的频率。

定义 IPv6 全局参数的步骤：

步骤 1 单击**管理 > 管理接口 > IPv6 全局配置**。

将打开 *IPv6 全局配置*页面。

步骤 2 为以下字段输入值：

- **ICMPv6 限速 单位时间间隔** - 输入生成 ICMP 错误消息的频率。
- **ICMPv6 限速 单位时间间隔最大消息数** - 输入在每个间隔时间内交换机可发送的 ICMP 错误消息的最大数目。

步骤 3 单击**应用**。 IPv6 全局参数将写入当前配置文件。

定义 IPv6 接口

可以在端口、LAG、VLAN 或 ISATAP 隧道接口上配置 IPv6 接口。交换机支持将一个 IPv6 接口用作一个 IPv6 终端设备。

隧道接口根据 *IPv6 隧道*页面中定义的设置，使用 IPv6 地址进行配置。

定义 IPv6 接口的步骤：

步骤 1 单击**管理 > 管理接口 > IPv6 接口**。

将打开 *IPv6 接口*页面。

此页面显示了已配置的 IPv6 接口。

步骤 2 单击**添加**，在启用了 IPv6 的接口上添加新的接口。

步骤 3 将打开*添加 IPv6 接口*页面。

步骤 4 输入值。

- **IPv6 接口** - 选择具体的端口、 LAG、 VLAN 或 ISATAP 隧道。
- **DAD 尝试次数** - 输入对接口的单播 IPv6 地址执行重复地址检测 (DAD) 时发送的连续邻居请求消息的数目。 DAD 分配地址之前会验证新的单播 IPv6 地址的唯一性。在 DAD 验证期间，新的地址会保持暂定状态。在此字段中输入 **0** 可禁用对指定接口执行的重复地址检测处理。在此字段中输入 **1** 表示没有后续传输的单次传输。
- **IPv6 地址自动配置** - 启用自动地址配置。如果启用，则交换机支持对来自接口上接收的 IPv6 路由器通告的网站本地 IP 地址和全域 IP 地址，执行 IPv6 无状态地址自动配置。交换机不支持有状态地址自动配置。如果未启用自动配置，则从 *IPv6 地址*页面定义 IPv6 地址。
- **发送 ICMPv6 消息** - 可生成提示无法访问的目的消息。

步骤 5 单击**应用**可对选择的接口进行 IPv6 处理。常规 IPv6 接口已自动配置以下地址：

- 根据设备的 MAC 地址使用 EUI-64 格式的接口 ID 的链路本地地址
- 所有节点链路本地组播地址 (FF02::1)
- 请求的节点组播地址 （格式为 FF02::1:FFXX:XXXX）

步骤 6 单击 **IPv6 地址表**可为接口手动分配 IPv6 地址 （如果需要）。有关该页面的描述，请参阅 “**定义 IPv6 地址**”一节。

定义 IPv6 地址

为 IPv6 接口分配 IPv6 地址的步骤：

步骤 1 单击**管理** > **管理接口** > **IPv6 地址**

将打开 *IPv6 地址*页面。

步骤 2 要过滤表格，请选择一个接口名称，然后单击**转至**。会在 “IPv6 地址表”中显示该接口。

步骤 3 单击**添加**。将打开*添加 IPv6 地址*页面。

步骤 4 为以下字段输入值。

- **IPv6 接口** - 显示在其上定义 IPv6 地址的接口。
- **IPv6 地址类型** - 选择 “链路本地”或 “全局”作为要添加的 IPv6 地址类型。
  - *链路本地* - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
  - *全局* - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。
- **IPv6 地址** - 该交换机支持一个 IPv6 接口。除了默认链路本地地址和组播地址外，设备将根据它接收的路由器通告自动向接口添加全局地址。该设备在接口上支持最多 128 个地址。每个地址必须是使用以冒号分隔的 16 位值以十六进制格式指定的有效 IPv6 地址。

  注 您无法直接在 ISATAP 隧道接口上配置任何 IPv6 地址。
- **前缀长度** - 全局 IPv6 前缀的长度，是 0-128 间的值，表示构成前缀 （地址的网络部分）的地址高位的连续位数。
- **EUI-64** - 选择该选项可使用 EUI-64 参数来根据设备的 MAC 地址，使用 EUI-64 格式标识全局 IPv6 地址的接口 ID 部分。

步骤 5 单击**应用**。将更新当前配置文件。

定义 IPv6 默认路由器列表

使用 *IPv6 默认路由器列表*页面可配置和查看默认 IPv6 路由器地址。该列表中包含一些候选路由器，这些路由器可能成为用于非本地流量 （可能为空）的交换机默认路由器。交换机会从列表中随机选择一个路由器。交换机支持一个静态 IPv6 默认路由器。动态默认路由器是将路由器通告发送给交换机 IPv6 接口的路由器。

添加或删除 IP 地址时，会发生以下事件：

- 删除 IP 接口时，所有默认路由器 IP 地址都会被删除。
- 无法删除动态 IP 地址。
- 尝试插入多个用户定义的地址后，会显示一个警报消息。
- 尝试插入非链路本地类型的地址 （即 “fe80:”）时，会显示一个警报消息。

定义默认路由器的步骤：

步骤 1 单击**管理 > 管理接口 > IPv6 默认路由器列表**。

将打开 *IPv6 默认路由器列表*页面。

该页面将为每个默认路由器显示以下字段：

- **默认路由器 IPv6 地址** - 默认路由器的链路本地 IP 地址。
- **接口** - 默认路由器所在的传出 IPv6 接口。
- **类型** - 默认路由器配置，包括以下选项：
  - *静态* - 通过**添加**按钮将默认路由器添加到此表格。
  - *动态* - 动态配置默认路由器。

  状态 - 默认路由器状态选项如下：
  - *不完整* - 正在解析地址。默认路由器尚未作出响应。
  - *可以访问* - 在 *可访问时间*内收到了肯定的确认。
  - *过时* - 无法访问之前已知的相邻网络，并且在需要发送流量之前不会执行任何操作来验证其可访问性。
  - *延迟* - 无法访问之前已知的相邻网络。设备处于 “延迟” 状态 （根据预定义的*延迟时间*）。如果收不到任何确认，状态将更改为 “探测”。
  - *探测* - 无法访问相邻网络，并且正发送单播邻居请求探测器，以确认该状态。

步骤 2 单击**添加**以添加静态默认路由器。将打开*添加默认路由器*页面。

该窗口会显示链路本地接口。接口可以为端口、 LAG、 VLAN 或隧道。

步骤 3 在**默认路由器 IPv6 地址**字段中，输入静态默认路由器 IP 地址。

步骤 4 单击**应用**。默认路由器将写入当前配置文件。

配置 IPv6 隧道

使用 ISATAP （站内自动隧道寻址协议）可以在 IPv4 数据包内封装 IPv6 数据包，以在 IPv4 网络上进行传输。要配置隧道，请执行以下操作：

- 手动启用和配置 ISATAP 隧道。
- 手动为 ISATAP 隧道定义 IPv6 接口。

进行以上操作后，交换机会自动配置 IPv6 接口的链路本地 IPv6 地址。

定义 ISATAP 隧道时，请注意以下方面：

- 会将 IPv6 链路本地地址分配给 ISATAP 接口。会将初始 IP 地址分配给该接口，然后再启用该接口。
- 如果一个 ISATAP 接口处于活动状态，则会使用 ISATAP 至 IPv4 映射，通过 DNS 来解析 ISATAP 路由器 IPv4 地址。如果未解析 ISATAP DNS 记录，则会在主机映射表中搜索 ISATAP 主机名至地址映射。
- 如果未通过 DNS 过程解析 ISATAP 路由器 IPv4 地址，则 ISATAP IP 接口仍处于活动状态。但是，系统没有用于 ISATAP 流量的默认路由器，直到解析 DNS 过程。

配置 IPv6 隧道的步骤：

步骤 1 单击**管理 > 管理接口 > IPv6 隧道**。

将打开 *IPv6 隧道*页面。

步骤 2 为以下字段输入值：

- **隧道编号** - 显示自动隧道路由器域号。
- **隧道类型** - 始终显示为 ISATAP。
- **源 IPv4 地址** - 禁用 ISATAP 隧道，或通过 IPv4 接口启用 ISATAP 隧道。选择的 IPv4 接口的 IPv4 地址用于构成 ISATAP 隧道接口上 IPv6 地址的一部分。IPv6 地址具有 64 位网络前缀 fe80::，剩余 64 位由 0000:5EFE 与 IPv4 地址连接而成。
  - *自动* - 自动从其配置的所有 IPv4 接口中选择最低的 IPv4 地址。
  - *无* - 禁用 ISATAP 隧道。
  - *手动* - 手动配置 IPv4 地址。配置的 IPv4 地址必须为交换机 IPv4 接口上的 IPv4 地址之一。
- **隧道路由器的域名** - 表示特定自动隧道路由器域名的整体字符串。该名称可以为默认名称 (ISATAP) 或用户定义的名称。
- **查询间隔** - 该隧道 DNS 查询之间 10-3600 的秒数 （获知 ISATAP 隧道的 IP 地址之前）。该间隔可以为默认值 （10 秒）或用户定义的间隔。
- **ISATAP 请求间隔** - 没有 ISATAP 路由器处于活动状态时， ISATAP 路由器请求消息之间 10-3600 的秒数。该间隔可以为默认值 （10 秒）或用户定义的间隔。

- **ISATAP 健壮性** - 用于计算 DNS 或路由器请求查询的间隔。数字越大，查询越频繁。默认值为 3，范围为 1-20。

  注 如果 IPv4 接口不在使用中，则 ISATAP 隧道不可用。

步骤 3 单击**应用**。隧道将写入当前配置文件。

定义 IPv6 邻居信息

使用 *IPv6 邻居*页面可以配置和查看 IPv6 接口上的 IPv6 邻居列表。 IPv6 邻居表 （也称为 IPv6 邻居发现缓存）会显示与交换机位于同一 IPv6 子网内的 IPv6 邻居的 MAC 地址。该表格用于验证该邻居的可访问性。该表格是与 IPv4 ARP 表格对等的 IPv6 表格。当交换机需要与其邻居进行通信时，交换机会使用 IPv6 邻居表来根据邻居的 IPv6 地址确定 MAC 地址。

该页面会显示自动检测条目或手动配置条目的邻居。每个条目都会显示与该邻居相连接的接口、该邻居的 IPv6 地址和 MAC 地址、条目类型 （静态或动态）以及该邻居的状态。

定义 IPv6 邻居的步骤：

步骤 1 单击**管理 > 管理接口 > IPv6 邻居**

将打开 *IPv6 邻居*页面。

步骤 2 您可以选择**清除表**中的一个选项，以清除 IPv6 邻居表中的部分或全部 IPv6 地址。

- **仅静态** - 删除静态 IPv6 地址条目。
- **仅动态** - 删除动态 IPv6 地址条目。
- **全部动态和静态** - 删除静态和动态 IPv6 地址条目。

会为相邻接口显示以下字段：

- **接口** - 相邻 IPv6 接口类型。
- **IPv6 地址** - 邻居的 IPv6 地址。
- **MAC 地址** - 映射到指定 IPv6 地址的 MAC 地址。
- **类型** - 邻居发现高速缓存信息条目类型 （静态或动态）。
- **状态** - 指定 IPv6 邻居状态。这些值包括：
  - *不完整* - 正在解析地址。邻居尚未作出响应。
  - *可以访问* - 已知可以访问邻居。

- *过时* - 无法访问之前已知的邻居。在必须发送流量之前不会执行任何操作来验证其可访问性。
- *延迟* - 无法访问之前已知的邻居。接口处于 “延迟” 状态 （根据预定义的延迟时间）。如果收不到任何可访问性确认，状态将更改为 “探测”。
- *探测* - 无法再访问邻居，并且正发送单播邻居请求探测器，以确认可访问性。

步骤 3 要将邻居添加到表格中，请单击**添加**。将打开*添加 IPv6 邻居*页面。

步骤 4 为以下字段输入值：

- **接口** - 要添加的相邻 IPv6 接口。
- **IPv6 地址** - 输入为该接口分配的 IPv6 网络地址。该地址必须为有效的 IPv6 地址。
- **MAC 地址** - 输入映射到指定 IPv6 地址的 MAC 地址。

步骤 5 单击**应用**。将更新当前配置文件。

步骤 6 要将 IP 地址类型从 “动态” 更改为 “静态”，请使用*编辑 IPv6 邻居*页面。

查看 IPv6 路由表

*IPv6 路由*页面将显示 *IPv6 路由表*。该表格包含一个默认路由 （IPv6 地址 :0），该路由使用从 “IPv6 默认路由器列表” 中选择的默认路由器，将数据包传送给与交换机不在同一 IPv6 子网内的设备。除了包含默认路由之外，该表格还包含动态路由，这些动态路由是使用 ICMP 重定向消息从 IPv6 路由器接收的 ICMP 重定向路由。如果交换机使用的默认路由器不是将流量传输到交换机要与其进行通信的 IPv6 子网的路由器，则会发生这种情况。

查看 IPv6 路由条目的步骤：

步骤 1 单击**管理 > 管理接口 > IPv6 路由**。

将打开 *IPv6 路由*页面。

此页面显示了以下字段：

- **IPv6 地址** - IPv6 子网地址。
- **前缀长度** - 目的 IPv6 子网地址的 IP 路由前缀长度。它前面有一个正斜杠。
- **接口** - 用于转发数据包的接口。
- **下一跳** - 将数据包转发到的地址。通常，该地址为相邻路由器的地址。该地址必须为链路本地地址。

- **度量** - 用于将该路由与 IPv6 路由器列表中目的相同的其他路由进行比较的值。所有默认路由具有相同值。
- **有效期限** - 在删除数据包之前可将其发送和再次发送的时间段。
- **路由类型** - 连接目的的方法以及用于获取条目的方法。值如下：
  - *本地* - 一种直接连接的网络，其前缀衍生自手动配置的交换机 IPv6 地址。
  - *动态* - 目的地址是间接连接的 （远程） IPv6 子网地址。条目是通过 ND 或 ICMP 协议动态获取的。
  - *静态* - 条目是由用户手动配置的。

配置 ARP

交换机会为位于其直接连接的 IP 子网内的所有已知设备维护一个 ARP （地址解析协议）表。直接连接的 IP 子网是指交换机的 IPv4 接口所连接的子网。当交换机需要将数据包发送 / 路由至本地设备时，它会搜索 ARP 表以取得该设备的 MAC 地址。 ARP 表包含静态地址和动态地址。静态地址是手动配置的，不会过期。交换机会根据其收到的 ARP 数据包创建动态地址。动态地址会在超过配置的时间之后过期。

注 交换机会使用 ARP 表中的 IP/MAC 地址映射信息，来转发由交换机生成的流量。

定义 ARP 表的步骤：

步骤 1 单击 **IP 配置 > ARP**。将打开 *ARP 表*页面。

步骤 2 输入参数。

- **ARP 条目过期时间** - 输入动态地址可在 ARP 表中保留的时间 （秒数）。当动态地址在该表中的时间超过 “ARP 条目过期时间” 时间后，动态地址便会过期。动态地址过期后，将从表中删除该地址，需要重新学习该地址才能回到表中。
- **清除 ARP 表条目** - 选择要从系统中清除的 ARP 条目类型。
  - *全部* - 立即删除所有静态地址和动态地址。
  - *动态* - 立即删除所有动态地址。
  - *静态* - 立即删除所有静态地址。
  - *正常过期时间* - 根据配置的 “正常过期时间” 时间删除动态地址。

步骤 3 单击**应用**。 ARP 全局设置将写入当前配置文件。

ARP 表将显示以下字段：

- **接口** - IP 设备所在的直接连接的 IP 子网的 IPv4 接口。
- **IP 地址** - IP 设备的 IP 地址。
- **MAC 地址** - IP 设备的 MAC 地址。
- **状态** - 是手动输入条目还是动态学习条目。

步骤 4 单击**添加**。将打开*添加 ARP 条目*页面。

步骤 5 输入参数：

- **IP 版本** - 主机支持的 IP 地址格式。仅支持 IPv4 格式。
- **接口** - 交换机上的 IPv4 接口。

只有一个直接连接的 IP 子网，该 IP 子网始终位于管理 VLAN 中。ARP 表中的所有静态地址和动态地址都位于管理 VLAN 中。

- **IP 地址** - 输入本地设备的 IP 地址。
- **MAC 地址** - 输入本地设备的 MAC 地址。

步骤 6 单击**应用**。 ARP 条目将写入当前配置文件。

域名系统

域名系统 (DNS) 会将用户定义的域名转换为 IP 地址，以找到这些对象并对其进行寻址。

作为一个 DNS 客户端，交换机可通过一个或对多个配置的 DNS 服务器将域名解析为 IP 地址。

定义 DNS 服务器

使用 *DNS 服务器*页面可启用 DNS 功能、配置 DNS 服务器，以及设置交换机使用的默认域名。

步骤 1 单击 **IP 配置** > **域名系统** > **DNS 服务器**。将打开 *DNS 服务器*页面。

步骤 2 输入参数。

- **DNS** - 选择该选项可将交换机指定为一个 DNS 客户端，来通过一个或对多个配置的 DNS 服务器将 DNS 名称解析为 IP 地址。
- **默认域名** - 输入默认 DNS 域名 （1 – 158 个字符）。交换机会对非完全限定的域名 (FQDN) 进行追加，以将其转换为 FQDN。
- **类型** - 显示默认域类型选项：
  - *DHCP* - 默认域名由 DHCP 服务器动态分配。
  - *静态* - 默认域名由用户定义。
  - 无 - 无默认域名。

DNS 服务器表：

- **DNS 服务器** - DNS 服务器的 IP 地址。您最多可定义八个 DNS 服务器。
- **服务器状态** - DNS 服务器可以处于活动状态或非活动状态。只能有一个服务器处于活动状态。每个静态服务器都有一个优先级，值越小优先级越高。首次发送请求时，会选择优先级最低的静态服务器。如果在两次重试后此服务器仍没有响应，则会选择下一优先级最低的服务器。如果所有静态服务器均没有响应，则会根据 IP 地址 （从低到高排序），选择该表中的第一个动态服务器。

步骤 3 单击**应用**。将更新当前配置文件。

步骤 4 要添加 DNS 服务器，请单击**添加**。将打开*添加 DNS 服务器*页面。

步骤 5 输入参数。

- **IP 版本** - 为 IPv6 选择 “版本 6”，或为 IPv4 选择 “版本 4”。
- **IPv6 地址类型** - 选择 IPv6 地址类型 （如果使用 IPv6）。选项如下：
  - *链路本地* - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
  - *全局* - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。
- **链路本地接口** - 如果 IPv6 地址类型为 “链路本地”，请选择通过 VLAN2 还是 ISATAP 接收。
- **DNS 服务器 IP 地址** - 输入 DNS 服务器的 IP 地址。
- **设置 DNS 服务器激活** - 选择该选项可激活新的 DNS 服务器。

步骤 6 单击**应用**。 DNS 服务器将写入当前配置文件。

映射 DNS 主机

交换机会将从 DNS 服务器获取的频繁查询的域名保存到本地 DNS 缓存中。该缓存最对可容纳 64 个静态条目、64 个动态条目，以及用于 DHCP 在交换机上配置的每个 IP 地址的一个条目。名称解析始终从检查这些静态条目开始、然后继续检查动态 DNS 条目，最后向外部 DNS 服务器发送请求。

可以针对每个主机名的每个 DNS 支持多个 IP 地址。

添加域名及其 IP 地址的步骤：

步骤 1 单击 **IP 配置** > **域名系统** > **主机映射**。将打开*主机映射*页面。

此页面显示了以下字段：

- **主机名** - 用户定义的域名 （最多 158 个字符）。
- **IP Address** - 主机名 IP 地址。

步骤 2 要添加主机映射，请单击**添加**。将打开*添加主机映射*页面。

步骤 3 输入参数。

- **IP 版本** - 为 IPv6 选择 “版本 6”，或为 IPv4 选择 “版本 4”。
- **IPv6 地址类型** - 选择 IPv6 地址类型 （如果使用 IPv6）。选项如下：
  - *链路本地* - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
  - *全局* - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。
- **链路本地接口** - 如果 IPv6 地址类型为 “链路本地”，请选择通过 VLAN2 还是 ISATAP 接收。
- **主机名** - 输入域名 （最多 158 个字符）。
- **IP 地址** - 输入一个 IPv4 地址，或输入最多四个 IPv6 主机地址。第 2 到 4 个地址为备用地址。

步骤 4 单击**应用**。 DNS 主机将写入当前配置文件。

17

配置安全

本节介绍交换机安全和访问控制。系统可处理多种类型的安全。

以下主题列表描述了本节中所介绍的多种类型的安全功能：某些功能用于多种类型的安全或控制，因此它们会在下面的主题列表中出现两次。

以下各节介绍了管理交换机的权限：

- **定义用户**
- **配置 RADIUS**
- **配置管理访问验证**
- **定义管理访问方法**
- **配置 TCP/UDP 服务**

以下各节介绍了针对交换机 CPU 的防攻击保护：

- **配置 TCP/UDP 服务**
- **定义风暴控制**

以下各节介绍了如何通过交换机控制终端用户对网络的访问：

- **配置管理访问验证**
- **定义管理访问方法**
- **配置 RADIUS**
- **配置端口安全**
- **配置 802.1X**

以下各节介绍了对其他网络用户的防御。这些攻击通过交换机进行，而非针对交换机。

- **配置 TCP/UDP 服务**
- **定义风暴控制**
- **配置端口安全**

定义用户

默认的用户名 / 密码为 **cisco/cisco**。第一次使用默认用户名和密码登录时，您需要输入新密码。默认情况下，将启用密码复杂性设置。如果您选择的密码不够复杂 （已在*密码强度*页面中启用**密码复杂性设置**），系统将提示您创建其他密码。

设置用户帐户

*用户帐户*页面可添加有权访问交换机 （只读或读写）的用户，或更改现有用户的密码。

添加用户后 （如下所述），将从系统中移除默认用户。

注 系统不允许删除所有用户。如果选择所有用户，**删除**按钮会被禁用。

添加新用户的步骤：

步骤 1 单击**管理** > **用户帐户**，此时将显示*用户帐户*页面。

此页面显示系统中定义的用户及其用户权限等级。

步骤 2 选择**密码恢复服务**，启用此功能。当此功能启用时，具有设备 Console 端口物理访问权限的最终用户可以进入引导菜单，并触发密码恢复流程。当引导系统流程结束时，您无需密码验证即可登录该设备。只有通过 Console，且只有当该 Console 连接至具有物理访问权限的设备时，才可以进入该设备。

禁用密码恢复机制时，依然可用访问启动菜单，您可以触发密码恢复流程。区别在于，在此情况下，在系统引导进程期间将移除所有配置和用户文件，并为终端生成适用的日志消息。

步骤 3 单击**添加**以添加新用户，或单击**编辑**以修改用户。此时将显示*添加 （或编辑）用户帐户*页面。

步骤 4 输入参数。

- **用户名** - 输入新用户名，长度应介于 0 到 20 个字符之间。不允许使用 UTF-8 字符。
- **密码** - 输入一个密码 （不允许使用 UTF-8 字符）。如果已定义密码强度和复杂性，则用户密码必须与在**设置密码复杂度规则**一节中配置的策略相符。
- **确认密码** - 再次输入密码。
- **密码强度计** - 显示密码的强度。密码强度和复杂性的策略在*密码强度*页面中配置。

步骤 5 单击**应用**。用户将添加到交换机的当前配置文件中。

设置密码强度规则

密码用于验证访问交换机的用户。简单的密码可能会危害安全。因此，默认情况下，将实施密码复杂性要求，并可在必要时进行配置。密码复杂性要求在**密码强度**页面上进行配置，该页面可通过安全下拉菜单打开。此外，还可以在此页面上配置密码过期时间。

定义密码复杂性规则的步骤：

步骤 1 单击**安全** > **密码强度**，此时将显示*密码强度*页面。

步骤 2 输入以下密码过期参数：

- **密码过期** - 如果选择此选项，则当**密码过期时间**到期时，系统将提示用户更改密码。
- **密码过期时间** - 输入在提示用户更改密码之前可经过的天数。

  注 密码过期时间也适用于零长度密码 （无密码）。

步骤 3 选择**密码复杂性设置**启用密码复杂性规则。

如果已启用密码复杂性，新密码必须符合下列默认设置：

- 密码最小长度为 8 个字符。
- 包含至少三个字符类别的字符 （大写字母、小写字母、数字和标准键盘上提供的特殊字符）。
- 不同于当前密码。
- 不得包含连续重复 3 次以上的字符。
- 不能与用户名重复，不能是以反向顺序排列的用户名，或者是通过更改字符大小写产生的任意变体。
- 不能与制造商名称重复，或者是通过更改字符大小写产生的任意变体。

步骤 4 如果**密码复杂性设置**已启用，可以配置以下参数：

- **最短密码长度** - 输入密码所需的最少字符数。

  注 可以设置零长度密码 （无密码），而且依然可以为其指定密码过期时间。
- **允许的字符重复** - 字符可以重复输入的次数。
- **最少字符类别数** - 输入密码中必须提供的字符类别数。字符类别包括小写字母 (1)、大写字母 (2)、数字 (3) 和符号或特殊字符 (4)。

- **新密码必须与当前密码不同** - 如果选择此选项，则更改密码时新密码不能与当前密码相同。

步骤 5 单击**应用**。密码设置将写入当前配置文件中。

配置 RADIUS

远程授权拨入用户服务 (RADIUS) 服务器提供了集中的 802.1X 或基于 MAC 的网络访问控制。交换机是一种 RADIUS 客户端，可以使用 RADIUS 服务器来提供集中的安全保护。

设置 RADIUS 服务器参数的步骤：

步骤 1 单击**安全** > **RADIUS**，此时将显示 *RADIUS* 页面。

步骤 2 若需要，输入默认的 RADIUS 参数。在*默认参数*中输入的值适用于所有服务器。如果没有 （在*添加 RADIUS 服务器*页面中）为特定服务器输入值，则交换机将使用这些字段中的值。

- **IP 版本** - 显示支持的 IP 版本：IPv6 和 / 或 IPv4 子网。
- **重试次数** - 输入在认为已发生故障之前发送到 RADIUS 服务器之请求的传输次数。
- **应答超时** - 输入交换机在重试查询或转换到下一个服务器之前等待从 RADIUS 服务器中返回响应的秒数。
- **无响应时间** - 输入服务请求绕过无响应 RADIUS 服务器之前经过的分钟数。如果值为 0，则表示未绕过服务器。
- **密钥字符串** - 输入用于在交换机与 RADIUS 服务器之间进行验证和加密的默认密钥字符串。此密钥必须与在 RADIUS 服务器上配置的密钥相匹配。密钥字符串用于加密使用 MD5 进行的通信。密钥可以以**加密**或**明文**的形式进行输入。如果您没有加密的密钥字符串 （从其他设备获得），可以以明文模式输入密钥字符串，并单击**应用**。系统将生成并显示加密的密钥字符串。

如果已定义密钥字符串，这将会覆盖默认的密钥字符串。

- **源 IPv4 地址** — 输入要使用的源 IPv4 地址。
- **源 IPv6 地址** — 输入要使用的源 IPv6 地址。

步骤 3 单击**应用**。将会在当前配置文件中更新交换机 RADIUS 默认设置。

若要添加 RADIUS 服务器，请单击**添加**。此时将显示*添加 RADIUS 服务器*页面。

步骤 4 在字段中输入每个 RADIUS 服务器的值。要使用在 *RADIUS* 页面中输入的默认值，请选择**使用默认设置**。

- **IP 版本** - 如果 RADIUS 服务器根据 IP 地址进行标识，则选择 IPv4 或 IPv6 来指示将以选定格式对其进行输入。
- **IPv6 地址类型** - 将显示 IPv6 地址类型是全局的。
- **服务器 IP 地址 / 名称** - 选择是按照 IP 地址还是名称来指定 RADIUS 服务器。
- **优先级** - 输入服务器的优先级。优先级可确定交换机尝试联系服务器以验证用户的顺序。交换机将首先从优先级最高的 RADIUS 服务器开始。 0 代表最高优先级。

  密钥字符串 - 输入用于验证和加密在交换机与 RADIUS 服务器之间通信的密钥字符串。此密钥必须与在 RADIUS 服务器上配置的密钥相匹配。如果选择**使用默认设置**，交换机将尝试使用默认的密钥字符串验证 RADIUS 服务器。
- **应答超时** - 输入交换机在重试查询或切换到下一个服务器 （如果已达最大重试次数）之前等待 RADIUS 服务器返回响应的秒数。如果选择**使用默认设置**，交换机将使用默认的超时值。
- **验证端口** - 输入用于验证请求的 RADIUS 服务器端口 UDP 端口号。
- **重试次数** - 输入在认为已发生故障之前发送到 RADIUS 服务器的请求次数。如果选择**使用默认设置**，交换机将使用重试次数的默认值。
- **无响应时间** - 输入服务请求绕过无响应 RADIUS 服务器之前必须经过的分钟数。如果选择**使用默认设置**，交换机将使用无响应时间的默认值。如果输入 0 分钟，则表示没有无响应时间。
- **用途类型** - 输入 RADIUS 服务器的验证类型。选项如下：
  - *登录* - RADIUS 服务器用于验证想要管理交换机的用户。
  - *802.1X* - RADIUS 服务器用于 802.1x 验证。
  - *全部* - RADIUS 服务器用于验证想要管理交换机的用户和 802.1X 验证。

步骤 5 若要以明文形式显示配置文件中的敏感数据，单击**将敏感数据显示为明文模式**。

步骤 6 单击**应用**。 RADIUS 服务器定义将添加到交换机的当前配置文件中。

配置管理访问验证

可将验证方法分配给 HTTP/HTTPS 会话。可以在本地或在 RADIUS 服务器上执行此验证。

为了使 RADIUS 服务器能够授予对基于 Web 的交换机配置实用程序的访问权限，RADIUS 服务器必须返回 cisco-avpair = shell:priv-lvl=15。

用户验证按照选择验证方法的顺序进行。如果第一种验证方法不可用，则使用选择的下一个方法。例如，如果选择的验证方法为 “RADIUS”和 “本地”，并且以优先级顺序对所有已配置 RADIUS 服务器进行查询但未获得响应，则会在本地对用户进行验证。

如果验证方法失败或用户的权限级别不足，则系统会拒绝用户访问交换机。换句话说，如果验证因验证方法而失败，则交换机会停止验证尝试；交换机不会继续工作，且不会尝试使用下一个验证方法。

为访问方法定义验证方法的步骤：

步骤 1 单击**安全** > **管理访问验证**，此时将显示*管理访问验证*页面。

步骤 2 从**应用**列表中选择一种访问方法。

步骤 3 使用箭头在 “可选方法”列与 “选定的方法”列之间移动验证方法。选择的第一种方法即为使用的第一种方法。

- *RADIUS* - 在 RADIUS 服务器上验证用户。您必须已配置了一个或多个 RADIUS 服务器。
- *无* - 允许用户在不经过验证的情况下访问交换机。
- *本地* - 根据存储在本地交换机上的数据检查用户名和密码。这些用户名和密码对是在*用户帐户*页面中定义的。

  注 必须始终最后选择**本地**或**无**验证方法。在**本地**或**无**之后选择的所有验证方法均会被忽略。

步骤 4 单击**应用**。选择的验证方法将与访问方法相关联。

定义管理访问方法

访问配置文件用于确定如何验证和授权通过各种访问方法访问交换机的用户。访问配置文件可以限制来自特定源的管理访问。

只有通过活动的访问配置文件和管理访问验证方法的用户才会获得对交换机的管理访问权限。

在任何时间交换机上只能有一个访问配置文件处于活动状态。

访问配置文件由一个或多个规则组成。按照访问配置文件中规则的优先级顺序 （从上到下）执行这些规则。

规则由包括以下元素的过滤器组成：

- **访问方法** - 访问和管理交换机的方法：
  - 超文本传输协议 (HTTP)
  - 安全 HTTP (HTTPS)
  - 以上全部
- **操作** - 允许或拒绝访问接口或源地址。
- **接口** - 被允许或拒绝访问基于 Web 的交换机配置实用程序的端口、 LAG 或 VLAN。
- **源 IP 地址** - 可允许访问的 IP 地址或子网。

活动的访问配置文件

*访问配置文件*页面可显示已定义的访问配置文件，并可用来选择一个将要处于活动状态的访问配置文件。

当用户尝试通过一种访问方法访问交换机时，交换机需要查看活动的访问配置文件是否明确允许通过此方法对交换机进行管理访问。如果找不到匹配项，则拒绝进行访问。

当访问交换机的尝试违反了活动的访问配置文件时，交换机会生成一条系统日志消息来向系统管理员发送有关该尝试的警报。

有关详情，请参阅**定义配置文件规则**。

使用*访问配置文件*页面可以创建访问配置文件，并添加第一个规则。如果访问配置文件只包含一个规则，则添加工作即已完成。若要向配置文件添加其他规则，请使用“配置文件规则”页面。

步骤 1 单击**安全** > **管理访问方法** > **访问配置文件**，此时将显示*访问配置文件*页面。

此页面显示所有处于和未处于活动状态的访问配置文件。

步骤 2 要更改活动的访问配置文件，请从**活动的访问配置文件**下拉菜单中选择一个配置文件，然后单击**应用**。此操作可使选择的配置文件成为活动的访问配置文件。

当您选择任何其他访问配置文件时，系统会根据选择的访问配置文件显示警告消息，提醒您系统可能会断开您与基于 Web 的交换机配置实用程序的连接。

步骤 3 单击**确定**以选择活动的访问配置文件，或单击**取消**以停止此操作。

步骤 4 单击**添加**以打开*添加访问配置文件*页面。您可以使用该页面配置新配置文件和一个规则。

步骤 5 输入**访问配置文件名称**。此名称可包含最多 32 个字符。

步骤 6 输入参数。

- **规则优先级** - 输入规则优先级。当数据包与规则相匹配时，系统会允许或拒绝用户组访问交换机。由于根据首次匹配原则对数据包进行匹配，因此在将数据包与规则进行匹配时，规则优先级至关重要。 1 代表最高优先级。
- **管理方法** - 选择为其定义了规则的管理方法。选项如下：
  - *全部* - 将所有管理方法分配给规则。
  - *HTTP* - 符合 HTTP 访问配置文件标准的用户，在请求访问交换机时，会获得允许或遭到拒绝。
  - *安全 HTTP (HTTPS)* - 符合 HTTPS 访问配置文件标准的用户，在请求访问交换机时，会获得允许或遭到拒绝。
- **操作** - 选择规则所关联的操作。选项如下：
  - *允许* - 如果用户与配置文件中的设置不匹配，则允许该用户访问交换机。
  - *拒绝* - 如果用户与配置文件中的设置相匹配，则拒绝该用户访问交换机。
- **应用到接口** - 选择规则所关联的接口。选项如下：
  - *全部* - 适用于所有端口、 VLAN 和 LAG。
  - *用户定义* - 适用于选中的接口。
- **接口** - 输入接口编号 （如果已选中用户定义）。
- **应用到源 IP 地址** - 选择访问配置文件适用的源 IP 地址类型。*源 IP 地址*字段适用于子网。请选择以下其中一个值：

- *全部* - 适用于所有类型的 IP 地址。
- *用户定义* - 仅适用于在该字段中定义的 IP 地址类型。

- **IP 版本** - 选择支持的源地址 IP 版本：IPv6 或 IPv4。
- **IP 地址** - 输入源 IP 地址。
- **掩码** - 为源 IP 地址选择子网掩码的格式，并在以下其中一个字段中输入值：
  - *网络掩码* - 选择源 IP 地址所归属的子网，并按照点分十进制格式输入子网掩码。
  - *前缀长度* - 选择 “前缀长度”，并输入组成源 IP 地址前缀的位数。

步骤 7 单击**应用**。访问配置文件将写入当前配置文件中。现在，您可以选择此访问配置文件作为活动的访问配置文件。

定义配置文件规则

访问配置文件最多可包含 128 个规则，以确定有权管理和访问交换机的人以及可能使用的访问方法。

访问配置文件中的每个规则均包含要匹配的操作和条件 （一个或多个参数）。每个规则均具有优先级；会首先检查优先级最低的规则。如果传入数据包与规则相匹配，则会执行与规则相关联的操作。如果在活动的访问配置文件中找不到匹配的规则，则会丢弃数据包。

例如，您可以限制所有 IP 地址对交换机的访问，仅允许分配到 IT 管理中心的 IP 地址访问交换机。这样一来，仍可以管理交换机，并使其获得另一层的安全。

将配置文件规则添加到访问配置文件的步骤：

步骤 1 单击**安全** > **管理访问控制** > **配置文件规则**，此时将显示*配置文件规则*页面。

步骤 2 选择 “过滤器”字段，然后选择一个访问配置文件。单击**转至**。

选择的访问配置文件将显示在配置文件规则表中。

步骤 3 单击**添加**以向其中添加一个规则。此时将显示*添加配置文件规则*页面。

步骤 4 输入参数。

- **访问配置文件名称** - 选择一个访问配置文件。
- **规则优先级** - 输入规则优先级。当数据包与规则相匹配时，系统会允许或拒绝用户组访问交换机。由于根据首次匹配原则对数据包进行匹配，因此在将数据包与规则进行匹配时，规则优先级至关重要。
- **管理方法** - 选择为其定义了规则的管理方法。选项如下：
  - *全部* - 将所有管理方法分配给规则。
  - *HTTP* - 将 HTTP 访问分配给规则。符合 HTTP 访问配置文件标准的用户，在请求访问交换机时，会获得允许或遭到拒绝。
  - *安全 HTTP (HTTPS)* - 符合 HTTPS 访问配置文件标准的用户，在请求访问交换机时，会获得允许或遭到拒绝。
- **操作** - 选择**允许**以允许尝试使用配置的访问方法通过按照此规则定义的接口或 IP 源来访问交换机的用户进行访问。或选择**拒绝**以拒绝访问。
- **应用到接口** - 选择规则所关联的接口。选项如下：
  - *全部* - 适用于所有端口、 VLAN 和 LAG。
  - *用户定义* - 仅适用于选择的端口、 VLAN 或 LAG。
- **接口** - 输入接口编号。
- **应用到源 IP 地址** - 选择访问配置文件适用的源 IP 地址类型。*源 IP 地址*字段适用于子网。请选择以下其中一个值：
  - *全部* - 适用于所有类型的 IP 地址。
  - *用户定义* - 仅适用于在该字段中定义的 IP 地址类型。
- **IP 版本** - 选择支持的源地址 IP 版本：IPv6 或 IPv4。
- **IP 地址** - 输入源 IP 地址。
- **掩码** - 为源 IP 地址选择子网掩码的格式，并在以下其中一个字段中输入值：
  - *网络掩码* - 选择源 IP 地址所归属的子网，并按照点分十进制格式输入子网掩码。
  - *前缀长度* - 选择 “前缀长度”，并输入组成源 IP 地址前缀的位数。

步骤 5 单击**应用**，将规则添加到访问配置文件。

配置 TCP/UDP 服务

出于安全考虑，通常会通过 *TCP/UDP 服务*页面在交换机上启用基于 TCP 或基于 UDP 的服务。

交换机可提供以下 TCP/UDP 服务：

- **HTTP** - 出厂默认设置为启用
- **HTTPS** - 出厂默认设置为启用

此窗口中还会显示活动的 TCP 连接。

配置 TCP/UDP 服务的步骤：

步骤 1 单击**安全** > **TCP/UDP 服务**，此时将显示 *TCP/UDP 服务*页面。

步骤 2 根据显示的服务启用或禁用以下 TCP/UDP 服务。

- **HTTP 服务** - 表示 HTTP 服务是处于启用状态还是禁用状态。
- **HTTPS 服务** - 表示 HTTPS 服务是处于启用状态还是禁用状态。

TCP 服务表显示了每个服务的以下字段：

- **服务名称** - 交换机正通过其提供 TCP 服务的访问方法。
- **类型** - 服务所使用的 IP 协议。
- **本地 IP 地址** - 交换机正通过其提供服务的本地 IP 地址。
- **本地端口** - 交换机正通过其提供服务的本地 TCP 端口。
- **远程 IP 地址** - 正请求服务的远程设备的 IP 地址。
- **远程端口** - 正请求服务的远程设备的 TCP 端口。
- **状态** - 服务的状态。

UDP 服务表显示以下信息：

- **服务名称** - 交换机正通过其提供 UDP 服务的访问方法。
- **类型** - 服务所使用的 IP 协议。
- **本地 IP 地址** - 交换机正通过其提供服务的本地 IP 地址。
- **本地端口** - 交换机正通过其提供服务的本地 UDP 端口。

- **应用实例** - UDP 服务的服务实例。（例如，两个发送者向同一目的地发送数据的情况。）

步骤 3 单击**应用**。服务将写入当前配置文件中。

定义风暴控制

接收到广播帧、组播帧或未知的单播帧后，系统会对它们进行复制，并将副本发送到所有可能的出口端口。这意味着，实际上已将它们发送到属于相关 VLAN 的所有端口。这样一来，一个入口帧会转变为多个入口帧，因此会产生流量风暴隐患。

您可以通过风暴保护来限制进入交换机的帧数，并定义计入此限制的帧类型。

在系统中输入阈值后，端口会丢弃达到阈值之后的流量。端口将保持阻塞状态，直到流量速率降至此阈值之下。然后，端口将继续进行正常转发。

定义风暴控制的步骤：

步骤 1 单击**安全** > **风暴控制**，此时将显示*风暴控制*页面。

在*编辑风暴控制*页面中，对此页面上除**风暴控制速率阈值 (%)** 之外的所有字段进行了介绍。它显示了在端口上应用风暴控制之前未知的单播、组播和广播数据包的总可用带宽的百分比。默认值为端口最大速率的 10%，它是在*编辑风暴控制*页面中设置的。

步骤 2 选择一个端口，然后单击**编辑**。此时将显示*编辑风暴控制*页面。

步骤 3 输入参数。

- **接口** - 选择已启用风暴控制的端口。
- **风暴控制** - 选择该选项可启用风暴控制。
- **风暴控制速率阈值** - 输入可用来转发未知数据包的最大速率。此阈值的默认值为 10,000 （针对 FE 设备）和 100,000 （针对 GE 设备）。
- **风暴控制模式** - 选择其中一种模式：
  - *未知单播、组播和广播* - 将未知的单播、广播和组播流量计入带宽阈值。
  - *组播和广播* - 将广播和组播流量一起计入带宽阈值。
  - *仅广播* - 仅将广播流量计入带宽阈值。

步骤 4 单击**应用**。将修改风暴控制，并更新当前配置文件。

配置端口安全

限制用户通过特定的 MAC 地址访问端口可增强网络安全。可以动态地学习或静态地配置 MAC 地址。

端口安全功能可监控接收的和学习的数据包。限制用户通过特定的 MAC 地址访问锁定的端口。

端口安全具有四种模式：

- **传统锁定** - 端口上学习的所有 MAC 地址均被锁定，并且端口未学习任何新 MAC 地址。学习的地址不会过期或无需重新学习。
- **有限动态锁定** - 交换机学习的 MAC 地址数不超过配置的允许地址极限。达到极限之后，交换机不会学习其他地址。在这种模式下，地址不会过期且无需重新学习。
- **永久安全** - 保持当前的动态 MAC 地址与端口相关联，并最多学习端点上允许的最大地址数量 （由允许的最大地址数量设定）。启用重新学习和老化。
- **重置即安全删除** - 重置后删除当前与端口相关联的动态 MAC 地址。新的 MAC 地址可作为重置即删除地址学习，数量最多为端口上允许的最大地址数量。禁用重新学习和老化。

当在新 MAC 地址未经授权的端口 （该端口已按照传统模式进行锁定且具有新 MAC 地址，或者该端口已被动态锁定且已超过了允许地址的最大数量）上检测到来自该地址的帧时，会调用保护机制，并且可能会执行以下操作之一：

- 丢弃帧
- 转发帧
- 关闭端口

当在另一个端口上发现安全 MAC 地址时，将转发帧，但不会学习该端口上的 MAC 地址。

除了以上这些操作，您还可以生成 Trap，并限制其频率和数量以避免设备过载。

注 Trap 为与系统日志有关的 Trap，不是通过 SNMP 生成的。

注 若要在端口上使用 802.1X，则端口必须处于多主机或多会话模式。如果端口处于单个模式，则不能在端口上设置安全 （请参阅 *802.1x、主机和会话验证*页面）。

配置端口安全的步骤：

步骤 1 单击**安全** > **端口安全**，此时将显示*端口安全*页面。

步骤 2 选择要修改的接口，然后单击**编辑**，此时将显示*编辑端口安全接口设置*页面。

步骤 3 输入参数。

- **接口** - 选择接口名称。
- **接口状态** - 选择该选项可锁定端口。
- **学习模式** - 选择端口锁定的类型。要配置此字段，必须取消锁定 “接口状态”。仅当锁定*接口状态*字段时，才会启用 “学习模式”字段。要更改学习模式，必须清除 “锁定接口”。更改模式之后，可以恢复 “锁定接口”的设置。选项如下：
  - *传统锁定* - 立即锁定端口，而不考虑已学习的地址数量。
  - *有限动态锁定* - 通过删除与端口相关联的当前动态 MAC 地址来锁定端口。端口最多可学习端口上允许的最大地址数量。同时启用 MAC 地址的重新学习和过期机制。
  - *永久安全* — 保持当前的动态 MAC 地址与端口相关联，并最多学习端点上允许的最大地址数量 （由**允许的最大地址数量设定**）。启用重新学习和老化。
  - *重置即安全删除* — 重置后删除当前与端口相关联的动态 MAC 地址。新的 MAC 地址可作为重置即删除地址学习，数量最多为端口上允许的最大地址数量。禁用重新学习和老化。
- **允许的最大地址数量** - 输入当选择*有限动态锁定*学习模式时可在端口上学习的 MAC 地址的最大数。数值 0 表示接口上仅支持静态地址。
- **违反规则响应措施** - 选择对到达锁定端口的数据包所应用的操作。选项如下：
  - *丢弃* - 丢弃来自任何未学习源的数据包。
  - *转发* - 转发来自任何未知源的数据包，而无需学习 MAC 地址。
  - *关闭* - 丢弃来自任何未学习源的数据包，并关闭端口。在重新激活端口或重启交换机之前，该端口将保持关闭状态。
- **Trap** - 选择该选项可在锁定端口接收到数据包时启用 Trap。这与违反锁定的行为有关。对于传统锁定，这是指任何接收到的新地址。对于有限动态锁定，这是指超过允许地址数量的任何新地址。

  注 Trap 与系统日志有关，不是通过 SNMP 生成的。
- **Trap 频率** - 输入 Trap 之间的最短时间间隔 （以秒为单位）。

步骤 4 单击**应用**。将修改端口安全，并更新当前配置文件。

配置 802.1X

基于端口的访问控制可在交换机端口上创建两种类型的访问。其中一个访问点启用非受控通信，而不考虑授权状态 （*非受控端口*）。另一个访问点对主机与交换机之间的通信进行授权。

802.1x 是一种 IEEE 标准，适用于基于端口的网络访问控制。 802.1x 框架可使设备（请求方）请求从其连接到的远程设备 （验证方）进行端口访问。仅当请求进行端口访问的请求方已经过验证和授权时，才允许请求方将数据发送到端口。否则，验证方会丢弃请求方数据。

验证方通过外部的 RADIUS 服务器对请求方执行验证，并监控验证的结果。

按照 802.1x 标准，设备可以同时作为端口处的请求方和验证方，既可请求进行端口访问也可授予端口访问权限。但是，此设备只能是验证方，并且不会充当请求方的角色。

802.1X 具有以下类型：

- **单会话 802.1X**：
  - **单个会话/单个主机** — 在这种模式下，交换机作为验证方会支持一个 802.1x 会话，并将端口的使用权限授予经授权的请求方。而其他设备从该相同端口接收到的所有访问请求均会遭到拒绝，除非经授权的请求方不再使用该端口或访问对象为未经验证的 VLAN。
  - **单会话 / 多主机** - 这种模式遵循 802.1x 标准。在这种模式下，交换机作为验证方允许任何设备使用端口，只要设备已具有权限。
- **多会话 802.1X** - 交换机 （验证方）必须在不同的 802.1x 会话中对连接到端口的每台设备 （请求方）分别进行验证和授权。

如标准中所述，交换机支持 802.1x 验证机制，以便对 802.1x 请求方进行验证和授权。

802.1X 参数工作流程

按照以下操作定义 802.1X 参数：

- （可选）按**定义 802.1X 属性**一节中所述，将一个或多个静态 VLAN 定义为未经验证的 VLAN。经过 802.1x 授权和未经其授权的设备或端口可以始终将数据包发送到未经验证的 VLAN 或从其接收数据包。
- 使用*编辑端口验证*页面为每个端口定义 802.1X 设置。

请注意以下方面：

- 您可以选择 “访客 VLAN”字段，以便将 Untagged 传入帧转至访客 VLAN。
- 使用*端口验证*页面为每个端口定义主机验证参数。
- 使用*已验证的主机*页面查看 802.1X 验证历史记录。

定义 802.1X 属性

*802.1X 属性*页面用于在全局启用 802.1X，并定义端口如何进行验证。要发挥 802.1X 的作用，必须在每个端口上全局且单独地激活 802.1X。

定义基于端口的验证的步骤：

步骤 1 单击**安全** > **802.1X** > **属性**，此时将显示*属性*页面。

步骤 2 输入参数。

- **基于端口的验证** - 启用或禁用基于端口的 802.1X 验证。
- **验证方法** - 选择用户验证方法。选项如下：
  - *RADIUS，无* - 首先使用 RADIUS 服务器执行端口验证。如果未从 RADIUS 接收到任何响应 （例如，如果服务器已停机），则不会执行验证，且允许进行会话。
  - *RADIUS* - 在 RADIUS 服务器上验证用户。如果未执行验证，则不允许进行会话。
  - *无* - 不验证用户。允许进行会话。

步骤 3 单击**应用**。 802.1X 属性将写入当前配置文件中。

定义 802.1X 端口验证

*端口验证*页面可配置每个端口的 802.1X 参数。因为仅当端口处于*强制授权*状态时，某些配置更改才有可能实现，例如主机验证，因此我们建议您在进行更改之前，将端口控制更改为*强制授权*。完成配置之后，将端口控制恢复为以前状态。

注 其上定义了 802.1x 的端口不能成为 LAG 的成员。

定义 802.1X 验证的步骤：

步骤 1 单击**安全** > **802.1X** > **端口验证**，此时将显示*端口验证*页面。

此页面显示所有端口的验证设置。

步骤 2 选择一个端口，然后单击**编辑**，此时将显示*编辑端口验证*页面。

步骤 3 输入参数。

- **接口** - 选择端口。
- **用户名** - 显示端口的用户名。
- **当前端口控制** - 显示当前端口授权的状态。如果状态为*已授权*，则端口可能已经过验证，或者*管理端口控制*为*强制授权*。反之，如果状态为*未授权*，则端口可能未经验证，或者*管理端口控制*为*强制未授权*。
- **管理端口控制** - 选择管理端口授权状态。选项如下：
  - *强制未授权* - 通过将接口转变为未授权状态来拒绝接口访问。交换机不为通过接口的客户端提供验证服务。
  - *自动* - 在交换机上启用基于端口的验证和授权。接口根据交换机与客户端之间的验证交换在授权状态和未经授权状态之间转换。
  - *强制授权* - 对接口进行授权，但不进行验证。
- **验证方法** - 选择端口的验证方法。选项如下：
  - *仅 802.1X* - 802.1X 验证是在端口上执行的唯一一种验证方法。
- **定期重新验证** - 选择该选项可在指定的重新验证时段之后尝试重新验证端口。
- **重新验证间隔** - 输入经过多少秒后对选定端口进行重新验证。
- **立即重新验证** - 选择该选项可立即对端口进行重新验证。
- **验证方状态** - 显示定义的端口授权状态。选项如下：
  - *强制授权* - 受控的端口状态设置为 “强制授权”（转发流量）。

    注 如果端口未处于 “强制未授权”状态，则处于自动模式下，且验证方会显示进行中的验证状态。对端口进行验证之后，状态会显示为 “已验证”。
- **静默期** - 输入在验证交换失败之后交换机保持静默状态的秒数。
- **重新发送 EAP** - 输入在重新发送请求之前交换机等待来自请求方 （客户端）的对可扩展验证协议 (EAP) 请求 / 身份帧的响应的秒数。

- **最大 EAP 请求** - 输入可发送的 EAP 请求的最大数。如果在定义时段 （请求方超时）之后未接收到响应，则重新启动验证程序。
- **请求方超时** - 输入将 EAP 请求重新发送到请求方之前经过的秒数。
- **服务器超时** - 输入交换机将请求重新发送到验证服务器之前经过的秒数。
- **终止原因** - 显示终止端口验证的原因 （如果适用）。

步骤 4 单击**应用**。端口设置将写入当前配置文件中。

定义主机和会话验证

使用*主机和会话验证*页面可定义 802.1X 在端口上的运作模式以及当检测到违例行为时要执行的操作。

802.1X 模式有：

- **单个** - 只有单台经授权的主机才可访问端口。（在单台主机模式下无法在端口上启用端口安全。）
- **多主机 (802.1X)** - 可将多台主机连接到单个启用 802.1X 的端口。只有第一个主机必须经过授权，然后，该端口将面向希望访问网络的所有客户端开放。如果主机验证失败，或收到了 EAPOL-logoff 消息，则会拒绝所有连接的客户端访问网络。
- **多会话** - 可使多台经授权的特定主机访问端口。每台主机均被视作第一个也是唯一一个用户，且必须经过验证。根据源 MAC 地址进行过滤。

为端口定义 802.1X 高级设置的步骤：

步骤 1 单击**安全** > **802.1X** > **主机和会话验证**，此时将显示*主机和会话验证*页面。

会说明所有端口的 802.1X 验证参数。在*编辑主机和会话验证*页面中介绍了除以下字段以外的所有字段。

- **状态** - 显示主机状态。星号表示没有链接端口或链接已断开。选项如下：
  - *未授权* - 端口控制为*强制未授权*且端口链接已断开，或者端口控制为*自动*但尚未通过端口验证客户端。
  - *强制授权* - 客户端具有完全的端口访问权限。
  - *单个主机锁定* - 端口控制为*自动*，且仅使用端口对一个客户端进行了验证。
  - *无单个主机* - 端口控制为*自动*，且已启用多主机模式。至少已对一个客户端进行了验证。

  - *未处于自动模式* - 未启用自动端口控制。
- **反入侵次数** - 显示在单台主机模式下从其 MAC 地址不是请求方 MAC 地址的主机到达接口的数据包数量。

步骤 2 选择一个端口，然后单击**编辑**，此时将显示*编辑主机和会话验证*页面。

步骤 3 输入参数。

- **接口** - 输入为其启用了主机验证的端口号。
- **主机验证** - 选择其中一种模式。这些模式在上面的*定义主机和会话验证*部分进行了介绍。

  注 以下字段仅当您在 “主机验证” 字段中选择了 “单个” 时才适用。

单个主机违反规则设置：

- **违反规则响应措施** - 选择对在单会话 / 单台主机模式下从其 MAC 地址不是请求方 MAC 地址的主机到达的数据包所应用的操作。选项如下：
  - *保护 (丢弃)* - 丢弃数据包。
  - *限制 (转发)* - 转发数据包。
  - *关闭* - 丢弃数据包并关闭端口。在重新激活端口或重启交换机之前，端口保持关闭状态。
- **Trap (单个主机违反规则)** - 选择该选项可启用 Trap。

  注 Trap 与系统日志有关，与 SNMP 无关。
- **Trap 频率（单个主机违反规则）** - 定义向主机发送 Trap 的频率。仅当禁用多台主机时才可定义此字段。

步骤 4 单击**应用**。设置将写入当前配置文件中。

查看经验证的主机

查看有关经验证的用户详情的步骤：

步骤 1 单击**安全** > **802.1X** > **已验证的主机**，此时将显示*已验证的主机*页面。

此页面显示了以下字段：

- **用户名** - 在每个端口上进行了验证的请求方名称。
- **端口** - 端口号。
- **会话时间 (DD:HH:MM:SS)** - 请求方在端口上保持登录状态的时间量。

- **验证方法** - 验证上一个会话所使用的方法。选项如下：
  - *无* - 未应用任何验证；自动进行授权。
  - *RADIUS* - 由 RADIUS 服务器对请求方进行了验证。
- **MAC 地址** - 显示请求方的 MAC 地址。

DoS 防护

DoS (DoS) 防护可阻止包含某些 IP 地址参数的数据包进入网络，从而提高网络安全。

SCT

思科交换机是一种高级交换机，除终端用户流量之外，还处理以下类型的流量：

- 管理流量
- 协议流量
- Snooping 流量

不需要的流量会使 CPU 不堪重负，并可能影响正常的交换机运行。

交换机使用安全的核心技术 (SCT) 功能，可以确保交换机无论接收的总流量是多少，都能够接收并处理管理和协议流量。

在默认情况下， SCT 在设备上已启用，且不能被禁用。

该功能与其他功能间没有交互。

SCT 可在 *DoS > DoS 防护 > 安全套件设置*页面中进行监控 （“详情”按钮）。

DoS 安全套件设置

注 激活 DoS 防护之前，您必须解除绑定所有绑定到端口的访问控制列表 (ACL) 策略或高级 QoS 策略。当端口启用 DoS 保护时，ACL 策略和高级 QoS 策略均不处于活动状态。

配置 DoS 防护全局设置并监控 SCT 的步骤：

步骤 1 单击**安全** > **DoS 防护** > **安全套件设置**，此时将显示*安全套件设置*。

CPU 保护机制：**已启用**表示 SCT 已启用。

步骤 2 单击 **CPU 利用率**旁边的**详情**以启用查看 CPU 资源利用率信息的功能。

18

使用 SSL 功能

本节介绍安全套接字层 (SSL) 功能。

其中包含以下主题：

- SSL 概述
- 默认设置和配置
- SSL 服务器验证设置

SSL 概述

安全套接字层 (SSL) 功能用于为设备打开 HTTPS 会话。

HTTPS 会话可以使用设备上存在的默认证书打开。

某些浏览器在使用默认证书时会生成警告，因为此证书未由证书颁发机构 (CA) 签名。最好使用由可信任 CA 签名的证书。

要使用用户创建的证书打开 HTTPS 会话，请执行以下操作：

1. 生成证书。
2. 请求 CA 认证证书。
3. 将已签名证书导入设备。

默认设置和配置

默认情况下，交换机包含可以进行修改的证书。

默认情况下，系统会启用 HTTPS。

SSL 服务器验证设置

可能需要生成新的证书才能替换设备上的默认证书。

创建新证书、修改现有证书或导入证书的步骤：

步骤 1 单击**安全** > **SSL 服务器** > **SSL 服务器验证设置**。此时将显示 *SSL 服务器验证设置* 页面。

SSL 服务器密钥表中会显示证书 1 和 2 的信息。除以下字段之外，相关字段会在**编辑**页面中定义：

- **有效期开始时间** - 指定证书有效期的开始日期。
- **有效期结束时间** - 指定证书有效期的结束日期。
- **证书来源** - 指定证书是由系统生成 （**自动生成**）还是由用户生成 （**用户定义**）。

步骤 2 选择活动证书。

步骤 3 您可以通过单击相关按钮执行以下任何操作：

- **编辑** - 选择其中一个证书，并为其输入以下字段：
  - **重新生成 RSA 密钥** - 选择此项可重新生成 RSA 密钥。
  - **密钥长度** - 输入要生成的 RSA 密钥的长度。
  - **通用名称** - 指定完全合格的设备 URL 或 IP 地址。如果未指定，会默认为设备的最小 IP 地址 （证书生成时）。
  - **组织单元** - 指定组织单元或部门名称。
  - **组织名称** - 指定组织名称。
  - **位置** - 指定位置或城市名称。
  - **省 / 自治区 / 直辖市** - 指定省 / 自治区 / 直辖市名称。
  - **国家 / 地区** - 指定国家 / 地区名称。
  - **持续时间** - 指定证书的有效天数。
- **生成证书请求** - 生成证书请求以便 CA 签名。
  - 输入证书字段 （与**编辑**页面中的字段相同）。

步骤 4 单击**生成证书请求**。此操作将会生成密钥，必须在 CA 中输入该密钥。

- **导入证书** - 收到 CA 批准后，请输入以下字段：
  - **证书 ID** - 选择活动证书。
  - **证书** - 复制到已收到证书中。
  - **导入 RSA 密钥对** - 选择此项可复制到新 RSA 密钥对中。
  - **公共密钥** - 复制到 RSA 公共密钥中。
  - **专用密钥 (加密模式)** - 选择并复制到加密形式的 RSA 专用密钥中。
  - **专用密钥 (明文模式)** - 选择并复制到明文形式的 RSA 专用密钥中。
  - **将敏感数据显示为加密模式** - 单击此按钮可以加密模式显示此密钥。单击此按钮后，专用密钥会以加密形式写入配置文件 （单击**应用**后）。
- **详情** - 显示证书和 RSA 密钥对。这用于将证书和 RSA 密钥对复制到其他设备（使用复制 / 粘贴）。单击**将敏感数据显示为加密模式**后，密钥会以加密形式显示。

步骤 5 单击**应用**将更改应用到当前配置。

19

安全敏感数据

安全敏感数据 (SSD) 是一种能够加强设备上敏感数据 （例如：密码和密钥）保护的结构。该工具利用密码、加密、访问控制和用户验证来提供一种管理敏感数据的安全解决方案。

该工具还可用于保护配置文件的完整性，确保配置过程的顺利进行以及支持 SSD 零接触自动配置。

简介

SSD 可保护设备上的敏感数据，例如：密码和密钥，允许和拒绝对基于用户凭证和 SSD 规则加密的明文模式敏感数据的访问 , 并可保护包含敏感数据的配置文件，使其免遭破坏。

此外，通过 SSD 还可确保含有敏感数据的配置文件在备份和共享过程中的安全。

用户可通过 SSD 灵活配置所需的敏感数据保护级别；可对明文模式的敏感数据不设保护，可通过基于默认密码加密进行最低程度的保护，也可通过基于用户定义的密码加密实现更有效的保护。

SSD 将根据 SSD 规则，仅向经过验证和授权的用户授予敏感数据的读取权限。设备将通过用户验证程序验证管理权限并将其授予用户。

无论是否使用 SSD，我们都建议管理员使用本地验证数据库来确保验证程序的顺利进行，并 / 或确保能够通过用户验证程序中使用的外部验证服务器进行安全通信。

总之， SSD 可通过 SSD 规则、 SSD 属性和用户验证来保护设备上的敏感数据。设备的 SSD 规则、 SSD 属性和用户验证配置本身作为敏感数据也将受到 SSD 的保护。

SSD 管理

SSD 管理包括对敏感数据的处理方法和安全性进行定义的诸多配置参数的管理。SSD 配置参数本身作为敏感数据也将受到 SSD 的保护。

SSD 的所有配置将通过 SSD 页面执行，只有具有正确权限的用户才能访问这些页面（请参阅 **SSD 规则**）。

SSD 规则

SSD 规则对授予管理通道上用户会话的读取权限和默认读取模式作出定义。

SSD 规则将由其用户通过 SSD 管理通道进行唯一识别。不同的 SSD 规则可能适用于同一用户但同时适用于不同的通道，反之，不同的规则也可能适用于同一通道但同时适用于不同的用户。

读取权限将决定敏感数据的查看方式：仅以加密模式、仅以明文模式、两种模式兼而有之或不允许查看敏感数据。 SSD 规则本身作为敏感数据也将受到保护。

一台设备总共可支持 32 条 SSD 规则。

当 SSD 规则与用户身份 / 用户凭证以及作为用户目前 / 将要访问敏感数据的管理通道的类型实现最佳匹配时，设备将向用户授予该规则的 SSD 读取权限。

设备会自带一套默认的 SSD 规则。管理员可按需要添加、删除和更改 SSD 规则。

注 设备可能并非 支持 SSD 定义的所有通道。

SSD 规则的内容

SSD 规则包含以下内容：

- **用户类型 -** 以下是按最高优先级到最低优先级顺序支持的用户类型：（如果用户与多条 SSD 规则匹配，则应用具有最高优先级用户类型的规则）。
  - **特定** - 该规则应用于特定用户。
  - **默认用户 (cisco)** - 该规则应用于默认用户 (cisco)。

  - **第 15 级** - 该规则应用于具有 15 级权限的用户。
  - **全部** - 该规则应用于所有用户。
- **用户名** - 如果用户类型为 “特定”，则需要提供用户名。
- **通道。**规则适用的 SSD 管理通道类型。受支持的通道类型有：
  - **安全** - 指定该规则仅应用于安全通道。根据不同的设备，可能会支持以下部分或所有的安全通道：
    Console 端口界面、 SCP、 SSH 和 HTTPS。
  - **不安全** - 指定该规则仅应用于不安全通道。根据不同的设备，可能会支持以下部分或所有的不安全通道：
    Telnet、 TFTP 和 HTTP。
  - **安全 XML SNMP** - 指定该规则仅应用于带保密功能的 XML over HTTPS [Sx300-500]。设备可能支持或不支持所有的 XML 和 SNMP 安全通道。
  - **不安全 XML SNMP** - 指定该规则仅应用于不带保密功能的 XML over HTTP [Sx300-500]/。设备可能支持或不支持所有的 XML 和 SNMP 安全通道。
- **读取权限** - 读取权限与各规则相关联。这些权限可分为以下类别：
  - （最低）**无** - 不允许用户访问任何形式的敏感数据。
  - （一般）**仅加密模式** - 仅允许用户访问加密的敏感数据。
  - （较高）**仅明文模式** - 仅允许用户访问明文模式的敏感数据。用户还将拥有 SSD 参数的读取和写入权限。
  - （最高）**所有模式** - 用户拥有加密和明文模式两种权限，并可访问加密模式和明文模式的敏感数据。用户还将拥有 SSD 参数的读取和写入权限。

每一管理通道都允许特定的读取权限。以下是对上述内容的总结。

表 1 每一管理通道允许的读取权限

管理通道	允许的读取权限选项
安全	所有模式、仅加密模式
不安全	所有模式、仅加密模式
安全 XML SNMP	无、仅明文模式
不安全 XML SNMP	无、仅明文模式

- **默认读取模式** - 所有的默认读取模式均受规则读取权限的限制。存在以下选项，但有些选项可能会被拒绝，这取决于读取权限。例如，如果用户的用户定义的读取权限为 “无”且默认读取模式为 “加密模式”，则以用户定义的读取权限为准。
  - **无** - 不允许读取敏感数据。
  - **加密模式** - 以加密形式显示敏感数据。
  - **明文模式** - 以明文形式显示敏感数据。

每一管理通道都允许特定的读取权限。以下是对上述内容的总结。

表 2 读取权限的默认读取模式

读取权限	允许的默认读取模式
无	无
仅加密模式	* 加密模式
仅明文模式	* 明文模式
所有模式	* 明文模式、加密模式

* 如果新的读取模式不违反读取权限，可在 SSD *属性*页面临时更改会话的读取模式。

注 请注意以下方面：

- 安全 XML SNMP 和不安全 XML SNMP 管理通道的默认读取模式必须与各自的读取权限保持一致。
- 只有安全 XML SNMP 和不安全 XML SNMP 管理通道才允许使用读取权限 “无”；常规安全和不安全通道不允许使用读取权限 “无”。
- 在安全和不安全 XML-SNMP 管理通道中不包含敏感数据表示敏感数据将显示为 0 （即：空字符串或数字 0）。如果用户想查看敏感数据，则必须将规则更改为明文模式。
- 默认情况下，带保密功能和安全通道上 XML 读取权限的 SNMPv3 用户将被视为第 15 级用户。
- 在不安全 XML 和 SNMP （不带保密功能的 SNMPv1、 v2 和 v3）通道上的 SNMP 用户将被视为 “所有用户”。
- 必须始终至少有一条具有读取权限的规则：仅明文模式或所有模式，因为只有具有这些权限的用户才能访问 SSD 页面。

- 在规则的默认读取模式和读取权限中所做的更改将生效，并将立即应用于受到影响的用户和所有处于活动状态的管理会话的通道，但不包括正在进行更改的会话，即使该规则适用于该会话。当规则更改 （添加、删除或编辑）后，系统将更新所有受到影响的 CLI/GUI 会话。

  注 当在会话登录时应用的 SSD 规则在该会话内部更改后，用户必须先退出，然后重新登录以查看更改的内容。

SSD 规则和用户验证

SSD 将根据 SSD 规则，仅向经过验证和授权的用户授予 SSD 权限。设备依靠其用户验证程序来验证和授予管理权限。要保护设备和其数据 （包括敏感数据和 SSD 配置），使其免遭未授权访问，我们建议在设备上执行用户验证程序。要确保用户验证程序的顺利进行，您可以使用本地验证数据库，同时确保能够通过外部验证服务器（例如：RADIUS 和 TACACS 服务器）进行安全通信。外部验证服务器的安全通信配置作为敏感数据将受到 SSD 的保护。

注 本地验证的数据库中的用户凭证已受到与 SSD 无关的机制的保护

如果来自某通道的用户发布了一个使用备选通道的操作，则设备将应用 SSD 规则中与该用户凭证和备选通道相匹配的读取权限和默认读取模式。例如，如果用户通过某安全通道登录并开始 TFTP 上传会话，则系统将应用不安全通道 (TFTP) 上用户的 SSD 读取权限

默认 SSD 规则

设备具有以下出厂默认规则：

表 3 默认 SSD 规则

规则密钥		规则操作	
用户	通道	读取权限	默认读取模式
第 15 级	安全 XML SNMP	仅明文模式	明文模式
第 15 级	安全	所有模式	加密模式
第 15 级	不安全	所有模式	加密模式
全部	不安全 XML SNMP	无	无
全部	安全	仅加密模式	加密模式
全部	不安全	仅加密模式	加密模式

可以修改默认规则，但无法删除它们。如果已更改 SSD 默认规则，则还可以将它们恢复。

SSD 默认读取模式会话覆盖

系统将根据用户的读取权限和默认读取模式，在会话中显示加密模式或明文模式的敏感数据。

只要默认读取模式不与会话的 SSD 读取权限相冲突，便可以临时覆盖它。该更改将立即在当前会话中生效，直至出现下列情况：

- 用户再次进行更改。
- 会话终止。
- 应用于会话用户的 SSD 规则的读取权限将发生更改且将不再与该会话的当前读取模式兼容。在这种情况下，该会话读取模式将返回该 SSD 规则的默认读取模式。

SSD 属性

SSD 属性是一组参数，这些参数将与 SSD 规则一起定义和控制设备的 SSD 环境。SSD 环境由以下属性组成：

- 控制敏感数据的加密方式。
- 控制配置文件的安全强度。
- 控制当前会话内敏感数据的查看方式。

密码

密码是 SSD 功能中安全机制的基础，用于为敏感数据的加密和解密生成密钥。拥有相同密码的 Sx200、Sx300、Sx500 和 SG500x 系列交换机能够解密彼此的敏感数据，这些数据通常通过从密码中生成的密钥进行了加密。

密码必须符合以下规则：

- **长度** - 在 8 到 16 个字符之间。
- **字符类别数** - 密码必须至少包含一个大写字符、一个小写字符、一个数字字符和一个特殊字符 （例如：#、 $）。

默认密码和用户定义的密码

所有设备均提供开箱即用的默认密码，用户可以查看。默认密码不会显示在配置文件或 CLI/GUI 中。

如果希望进一步加强保护和提高安全性，管理员应在设备上配置 SSD 以使用用户定义的密码而不是默认密码。用户定义的密码应严格对外保密，以便有效保障设备上敏感数据的安全性。

用户定义的密码可以明文模式进行手动配置。也可以衍生自配置文件。（请参阅“SSD 零接触自动配置”）。设备始终会显示用户定义的加密密码。

本地密码

设备将维护本地密码，该密码是设备当前配置的密码。 SSD 通常会通过从本地密码生成的密钥执行敏感数据的加密和解密。

本地密码可配置为默认密码或用户定义的密码。默认情况下，本地密码和默认密码是一致的。可通过命令行界面 （如可用）或基于 Web 的界面上的管理操作更改本地密码。当启动配置成为设备的当前配置后，本地密码将自动更改为启动配置文件中的密码。当设备重置回出厂默认配置后，本地密码将重置为默认密码。

配置文件密码控制

文件密码控制为用户定义的密码以及在基于文本的配置文件中通过从用户定义的密码生成的密钥来加密的敏感数据提供了进一步的保护。

以下是现有的密码控制模式：

- **无限制** （默认情况下）- 设备在创建配置文件时会将其密码包含在内。这就使任何接受配置文件的设备都能从文件中学习密码。
- **已限制** - 设备将限制向配置文件导入其密码。已限制模式可防止没有密码的设备访问配置文件中加密的敏感数据。如果用户不希望在配置文件中显示密码，则应使用该模式。

当设备重置回出厂默认配置后，其本地密码将重置为默认密码。设备将因此无法解密任何加密的敏感数据，无论是基于从管理会话 (GUI/CLI) 输入的用户定义的密码加密的敏感数据，还是在任何带有限制模式的配置文件 （包括设备重置回出厂默认配置前由其创建的文件）中加密的敏感数据。这种情况将一直持续到通过用户定义的密码手动重新配置该设备或该设备从配置文件中学习用户定义的密码为止。

配置文件完整性控制

用户可通过 “配置文件完整性控制”创建配置文件，藉此使配置文件免遭破坏或修改。我们建议当设备通过 “无限制配置文件密码控制”使用用户定义的密码时应启用 “配置文件完整性控制”。

注意 对受完整性保护的配置文件所做的任何修改都将被视为对该文件的破坏。

设备可通过检查配置文件的 “SSD 控制”块中的 “文件完整性控制”命令来确定配置文件的完整性是否受到了保护。如果文件的完整性受到保护但设备却发现文件的完整性并不完整，则设备将拒绝该文件。否则，将接受该文件以作进一步处理。

当基于文本的配置文件下载或复制到启动配置文件中时，设备将检查该文件的完整性。

读取模式

每一会话都有一种读取模式。这将决定敏感数据的显示方式。读取模式可以为明文模式，敏感数据在其中将显示为常规文本；也可以为加密模式，敏感数据在其中将以加密的形式显示。

配置文件

配置文件中包含设备的配置。设备中将包含一个当前配置文件、一个启动配置文件、一个镜像配置文件 （可选）和一个备份配置文件。用户可以将配置文件手动上传和下载到远程文件服务器上，反之亦可。设备在使用 DHCP 进行自动配置时，可自动从远程文件服务器上下载其启动配置。存储在远程文件服务器上的配置文件称为远程配置文件。

当前配置文件中含有设备正在使用的配置。重启后，启动配置中的配置将变成当前配置。当前配置文件和启动配置文件的格式均为内部格式。镜像配置文件、备份配置文件和远程配置文件均为基于文本的文件，保留它们的目的通常是为了存档、记录或恢复。在复制、上传和下载源配置文件的过程中，如果配置文件和目标文件的格式不同，设备会自动将源内容的格式转换成目标文件的格式。

文件 SSD 指示器

在将当前配置文件或启动配置文件复制到基于文本的配置文件中时，设备会生成文件 SSD 指示器并将其置入基于文本的配置文件中，以显示文件中是含有加密的敏感数据、明文模式的敏感数据，还是不包含敏感数据。

- 如果存在 SSD 指示器，则其必须置于配置标题文件中。
- 不包含 SSD 指示器的基于文本的配置将视为其中不包含敏感数据。
- SSD 指示器可用于强制执行基于文本的配置文件的 SSD 读取权限，但在将配置文件复制到当前配置文件或启动配置文件中时，可将其忽略。

在复制文件过程中，可根据用户的说明将文件中的 SSD 指示器设置为文件中包含机密模式或明文模式的敏感数据或不包含敏感数据。

SSD 控制块

如果用户要求在文件中包含敏感数据，则设备在从其启动配置文件或当前配置文件创建基于文本的配置文件时，会在该文件中插入一个 SSD 控制块。 SSD 控制块可免遭破坏且其中含有正在创建该文件的设备的 SSD 规则和 SSD 属性。 SSD 控制块以“ssd-control-start”开始，以 “sd-control-end”结束。

启动配置文件

设备目前支持将当前配置文件、备份配置文件和远程配置文件复制到启动配置文件中。重启后，启动配置中的配置将生效并变成当前配置。用户可根据 SSD 读取权限和管理会话的当前 SSD 读取模式，在启动配置文件中检索加密模式或明文模式的敏感数据。

如果启动配置文件中的密码与本地密码不同，则将不包括启动配置中任何形式的敏感数据的读取权限。

SSD 在将备份配置文件、镜像配置文件和远程配置文件复制到启动配置中时会添加以下规则：

- 当设备重置回出厂默认配置后，其所有配置 （包括 SSD 规则和属性）都将重置回默认配置。
- 如果源配置文件中包含加密的敏感数据但缺少 SSD 控制块，则设备将拒绝该源文件且会造成复制失败。
- 如果源配置文件中没有 SSD 控制块，启动配置文件中的 SSD 配置将重置回默认配置。

- 如果源配置文件的 SSD 控制块中含有密码，且文件中加密的敏感数据并未通过 SSD 控制块中的密码生成的密钥进行加密，则设备将拒绝该源文件并会造成复制失败。
- 如果源配置文件中含有 SSD 控制块且该文件的 SSD 完整性检查和/或文件完整性检查失败，则设备将拒绝该源文件并会造成复制失败。
- 如果源配置文件的 SSD 控制块中部含有密码，则该文件中所有加密的敏感数据必须通过从本地密码生成的密钥进行加密，或通过从默认密码生成的密钥进行加密，但不能通过前述两种方式同时加密。否则，设备将拒绝该源文件并会造成复制失败。
- 无论是源配置文件中的 SSD 控制块还是启动配置文件，设备都会对密码、密码控制和文件完整性 （如有）进行配置。设备配置启动配置文件所用的密码将用于生成解密源配置文件中的敏感数据所需的密钥。未发现的任何 SSD 配置都将重置回默认配置。
- 如果源配置文件中含有 SSD 控制块，且该文件中含有明文模式的敏感数据但不含有 SSD 控制块中的 SSD 配置，则设备将接受该文件。

当前配置文件

当前配置文件中含有设备正在使用的配置。用户可根据 SSD 读取权限和管理会话的当前 SSD 读取模式，在当前配置文件中检索加密模式或明文模式的敏感数据。用户可通过由 CLI、 XML 和 [Sx300-500] 等产生的其他管理操作来复制备份配置文件或镜像配置文件，从而更改当前配置。

当用户直接更改当前配置中的 SSD 配置时，设备将应用以下规则：

- 如果已打开管理会话的用户没有 SSD 权限 （即所有模式或仅明文模式的读取权限），则设备将拒绝所有的 SSD 命令。
- 当从源文件进行复制时，既不会验证文件 SSD 指示器、 SSD 控制块完整性和 SSD 文件完整性，也不会增强它们。
- 当从源文件进行复制时，如果源文件中的密码为明文模式，则复制将失败。如果密码为加密模式，则忽略不计。
- 当在当前配置中直接配置密码 （非文件复制）时，必须以明文形式输入命令中的密码。否则，命令将被拒绝。
- 配置命令中所含的加密敏感数据将通过由本地密码生成的密钥进行加密，且配置命令将配置为当前配置。否则，配置命令将显示错误并将不会纳入当前配置文件中。

备份配置文件和镜像配置文件

如果已启用自动镜像配置服务，设备将定期通过启动配置文件生成其镜像配置文件。设备始终都会生成带有机密敏感数据的镜像配置文件。因此，镜像配置文件中的文件 SSD 指示器会始终显示文件中是否含有加密的敏感数据。

默认情况下，自动镜像配置服务为启用状态。要将自动镜像配置配置为启用或禁用，请单击**管理 > 文件管理 > 配置文件属性**。

用户可根据 SSD 读取权限、会话中的当前读取模式和源文件中的文件 SSD 指示器用户可以按如下所述显示、复制和上传完整的镜像和备份配置文件以及会话中的当前读取模式以及源文件中的文件 SSD 指示器 （根据 SSD 读取权限）：

- 如果镜像配置文件或备份配置文件中不含有文件 SSD 指示器，则所有用户均可访问该文件。
- 具有 “所有权限”读取权限的用户可访问所有的镜像配置文件和备份配置文件。但是，如果会话的当前读取模式与文件 SSD 指示器不同，则用户会看到一个提示窗口，该窗口显示不允许进行该操作。
- 如果具有 “仅明文模式”权限的用户的文件 SSD 指示器显示 “无”或 “仅明文模式”敏感数据，则这些用户可以访问镜像和备份配置文件。
- 如果具有 “仅加密模式”权限的用户的文件 SSD 指示器显示 “无”或 “加密模式”敏感数据，则这些用户可以访问镜像和备份配置文件。
- 如果具有 “无”权限的用户的文件 SSD 指示器显示包含加密模式或明文模式的敏感数据，则这些用户不能访问镜像和备份配置文件。

用户不应手动更改与敏感数据有冲突的文件 SSD 指示器 （若文件中存在）。否则，可能会意外地明文显示敏感数据。

敏感数据零接触自动配置

SSD 零接触自动配置是使用加密的敏感数据对目标设备进行自动配置，而无需使用密码 （其密钥用于加密模式的敏感数据）对目标设备进行预先手动配置。

该设备目前支持自动配置，默认情况下即已启用。如果设备已启用自动配置，将收到 DHCP 选项，指定文件服务器和引导文件，该设备会将引导文件 （远程配置文件）从文件服务器下载至启动配置文件中，然后重启。

> **注** 文件服务器可由 bootp siaddr 和 sname 字段以及 DHCP 选项 150 指定，也可以在设备上进行静态配置。

用户通过先从包含自动配置的设备中创建要在该配置中使用的配置文件，可以使用加密的敏感数据安全地对目标设备进行自动配置。必须对设备进行配置和指引，以：

- 加密文件中的敏感数据
- 提高文件内容的完整性
- 包括安全的验证配置命令和 SSD 规则，正确控制和保护对设备和敏感数据的访问

如果配置文件使用用户密码生成，且 SSD 文件密码控制已受限，则可使用产生的配置文件对期望的目标设备进行自动配置。但是，要想使用用户定义的密码成功进行自动配置，必须对目标设备进行预先手动配置，使其与生成该文件的设备使用相同的密码，此过程不是零接触。

如果创建该配置文件的设备处于未限制密码控制模式，则该设备在文件中已包括密码。因此，用户可使用该配置文件对目标设备进行自动配置，包括并非开箱即用或者处于出厂默认设置的设备，而无需使用密码对目标设备预先进行手动配置。这是零接触过程，因为目标设备可直接从配置文件学习密码。

SSD 管理通道

可通过 telnet、 SSH 和 Web 等管理通道对设备进行管理。 SSD 根据通道的安全性和 / 或协议将其分成以下几类：安全、不安全、安全 -XML-SNMP 和不安全 -XML-SNMP。

下面我们将介绍 SSD 认为每种管理通道安全与否。如果认为该通道不安全，表中将会指出类似的安全通道。

管理通道的安全性

管理通道

管理通道	SSD 管理通道类型	类似的安全管理通道
GUI/HTTP	不安全	GUI/HTTPS
GUI/HTTPS	安全	
XML/HTTP	不安全 -XML-SNMP	XML/HTTPS
XML/HTTPS	安全 -XML-SNMP	
TFTP	不安全	[Sx300-500]

基于 HTTP 的文件传输	不安全	基于 HTTPS 的文件传输
基于 HTTPS 的文件传输	安全	

菜单 CLI 和密码恢复

只有阅读权限为 “所有模式”或 “仅明文模式”的用户允许使用菜单 CLI 接口。拒绝其他用户使用。菜单 CLI 中的敏感数据始终以明文模式显示。

目前，密码恢复可从引导菜单激活，用户无需身份验证即可登录到终端。如果支持 SSD，只有当本地密码与默认密码相同时，才允许使用此选项。如果设备已配置用户定义的密码，则该用户将不能激活密码恢复。

配置 SSD

在以下页面中配置 SSD 功能：

- 在*属性*页面中设置 SSD 属性。
- 在 *SSD 规则*页面中定义 SSD 规则。

SSD 属性

只有具有 “仅明文模式”或 “所有模式”SSD 读取权限的用户允许设置 SSD 属性。

配置全局 SSD 属性的步骤：

步骤 1 单击**安全** > **安全敏感数据管理** > **属性**。此时将显示*属性*页面。此时将显示以下字段：

- **当前本地密码类型** — 显示当前正在使用的是默认密码还是用户定义的密码。

步骤 2 输入以下**永久设置**字段：

- **配置文件密码控制** — 按照**配置文件密码控制**中的说明选择选项。
- **配置文件完整性控制** — 选择后，将启用此功能。请参阅**配置文件完整性控制**。

步骤 3 为当前会话选择读取模式 （请参阅 **SSD 规则的内容**）。

更改本地密码的步骤：

步骤 4 单击**更改本地密码**，然后输入新的**本地密码**：

- **默认** — 使用设备的默认密码。
- **用户定义 (明文模式)** — 输入并确认新密码。

SSD 规则

只有具有 “仅明文模式”或 “所有模式”SSD 读取权限的用户允许设置 SSD 规则。

配置 SSD 规则的步骤：

步骤 1 单击**安全** > **安全敏感数据管理** > **SSD 规则**。此时将显示 *SSD 规则*页面。

此时将显示当前定义的规则。

步骤 2 要添加新规则，请单击**添加**。输入以下字段：

- **用户** — 此字段定义规则所应用的用户。请选择以下其中一个选项：
  - *特定用户* — 选择并输入此规则所应用的特定用户名 （不一定非要定义此用户）。
  - *默认用户 (cisco)* — 表示此规则所应用的默认用户。
  - *第 15 级* — 表示此规则应用于具有 15 级权限的所有用户。
  - *全部* — 表示此规则应用于所有用户。
- **通道** — 此字段定义规则所应用的输入通道的安全级别：请选择以下其中一个选项：
  - *安全* — 表示此规则仅应用于安全通道 （Console、 [Sx300-500]SSH 和 HTTPS），不包括 [Sx300-500] XML 通道。
  - *不安全* — 表示此规则仅应用于不安全通道 （Telnet、 TFTP 和 HTTP），不包括 [Sx300-500]XML 通道。
  - *安全 XML SNMP* — 表示此规则仅应用于带保密功能的 XML over HTTPS [Sx300-500]。
  - *不安全 XML SNMP* — 表示此规则仅应用于不带保密功能的 XML over HTTP 或 [Sx300-500]。

- **读取权限** — 读取权限与规则相关联。这些权限可分为以下类别：
  - *无* — 级别最低的读取权限。用户不允许以任何形式获取敏感数据。
  - *仅明文模式* — 高于上述级别的读取权限。用户只允许以明文模式获取敏感数据。
  - *仅加密模式* — 中等级别的读取权限。用户只允许以加密模式获取敏感数据。
  - *所有模式（明文模式和加密模式）* — 级别最高的读取权限。如果用户同时具有加密模式和明文模式权限，可允许以加密模式和明文模式获取敏感数据。
- **默认读取模式** — 所有默认读取模式需遵循规则的读取权限。存在以下选项，但根据规则的读取权限，有些选项可能会被拒绝。
  - *无* — 不允许读取敏感数据。
  - *加密模式* — 敏感数据以加密模式提供。
  - *明文模式* — 敏感数据以明文模式提供。

步骤 3 可以执行以下操作：

- **恢复为默认设置** — 将用户修改的默认规则恢复为默认规则。
- **将所有规则恢复为默认设置** — 将所有用户修改的默认规则恢复为默认规则，并移除所有用户定义的规则。

20

配置服务质量

在整个网络中应用服务质量功能，可确保根据所需条件设置网络流量的优先级，从而优先处理所需的流量。

本节包含以下主题：

- **QoS 功能和组件**
- **配置 QoS - 一般**
- **管理 QoS 统计信息**

QoS 功能和组件

QoS 功能可用于优化网络性能。

QoS 可实现：

- 根据以下属性将传入流量分为不同的流量类：
  - 设备配置
  - 入口接口
  - 数据包内容
  - 以上属性的组合

QoS 包括：

- **流量分类** - 根据数据包内容和 / 或端口，将每个传入数据包分类为属于特定数据流。分类操作由 ACL （访问控制列表）完成，并且仅对符合 ACL 标准的流量进行 CoS 或 QoS 分类。
- **分配至硬件队列** - 将传入数据包分配给转发队列。数据包所属流量类所具有的功能会将数据包发送到特定的队列进行处理。
- **其他流量类处理属性** - 将 QoS 机制应用到各种类，包括带宽管理。

QoS 操作

使用 QoS 功能时将对类相同的所有流量进行相同的处理，其中包括根据传入帧中指明的 QoS 值确定出口端口上的出口队列的唯一 QoS 操作。这是第 2 层中的 VLAN 优先级标记 (VPT) 802.1p 值和第 3 层中的 IPv4 差分服务代码点 (DSCP) 值或 IPv6 流量类 (TC) 值。在基本模式下工作时，交换机信任此外部分配的 QoS 值。数据包的外部分配 QoS 值将决定其流量类和 QoS。

在*全局设置*页面中输入受信任的头字段类型。对于该字段的每个值，在 *CoS/802.1p 到队列*页面或 *DSCP 到队列*页面 （具体取决于信任模式为 CoS/802.1p 还是 DSCP）中指定出口队列，指示会通过该队列发送帧。

QoS 工作流程

要配置一般 QoS 参数，请执行以下操作：

步骤 1 通过使用 *QoS 属性*页面选择信任模式来启用 QoS。然后使用*接口设置*页面在端口上启用 QoS。

步骤 2 使用 *QoS 属性*页面为每个接口指定一个默认的 CoS 或 DSCP 优先级。

步骤 3 使用*队列*页面为出口队列指定调度方法 （“严格优先级”或 “WRR”）及 WRR 的带宽分配。

步骤 4 使用 *DSCP 到队列*页面，为每个 IP DSCP/TC 值指定一个出口队列。如果交换机处于 DSCP 信任模式，则会根据传入数据包的 DSCP/TC 值将传入数据包放入出口队列。

步骤 5 为每个 CoS/802.1p 优先级指定一个出口队列。如果交换机处于 CoS/802.1 信任模式，则会根据传入数据包中的 CoS/802.1p 优先级将所有传入数据包放入指定的出口队列。此项操作可使用 *CoS/802.1p 到队列*页面完成。

步骤 6 在以下页面中输入带宽和速率限制：

a. 使用*每队列出口整形*页面设置每队列的出口整形。

b. 使用*带宽*页面设置每端口的入口速率限制和出口整形速率。

配置 QoS - 一般

*QoS 属性*页面包含用于启用 QoS 并选择要使用的信任模式的字段。此外，还可以使用该页面来定义每个接口的默认 CoS 优先级或 DSCP 值。

设置 QoS 属性

启用 QoS 的步骤：

步骤 1 单击**服务质量** > **一般** > **QoS 属性**。此时将显示 *QoS 属性*页面。

步骤 2 在交换机上启用 QoS。

步骤 3 选择一种信任模式 （CoS/802.1p 或 DSCP）并单击**应用**。

步骤 4 如果您选择了 DSCP，转至**步骤 6**；如果选择了 CoS，则继续进行下一步操作。

步骤 5 选择**端口 /LAG** 并单击**转至**以显示 / 修改设备上的所有端口 /LAG 及其 CoS 信息。

以下字段会对所有端口 /LAG 显示：

- **接口** - 接口类型。
- **默认 CoS** - 不包含 VLAN 标记的传入数据包的默认 VPT 值。默认 CoS 为 0。该默认值仅在选择了*信任 CoS* 时对 Untagged 的帧有效。

选择**恢复默认设置**会为此接口还原出厂 CoS 默认设置。

步骤 6 单击 **DSCP 覆盖表**输入 DSCP 值。此时将显示 *DSCP 覆盖表*。

步骤 7 “传入 DSCP”会显示需要重新标记为替代值的传入数据包 DSCP 值。选择可取代传入值的新 DSCP 值。

选择 “恢复默认设置”可恢复出厂 DSCP 值。

步骤 8 单击**应用**。将更新当前配置文件。

要在接口上设置 QoS，先选择该接口，然后单击**编辑**。此时将显示*编辑接口 CoS 配置*页面。

步骤 1 输入参数。

- **接口** - 选择端口或 LAG。
- **默认 CoS** - 选择要为不包含 VLAN 标记的传入数据包指定的默认 CoS（服务等级）值。该值的范围是 0-7。

步骤 2 单击**应用**。接口默认 CoS 值将写入当前配置文件。

接口 QoS 设置

使用*接口设置*页面可在交换机的每个端口上配置 QoS，如下所示：

已在接口上禁用 QoS 状态 - 端口上的所有入口流量均被映射到尽力服务队列，并且不进行任何分类 / 优先级划分。

已启用端口的 QoS 状态 - 端口将根据在整个系统中配置的信任模式 （CoS/802.1p 信任模式或 DSCP 信任模式），为入口流量设置优先级。

输入每个接口的 QoS 设置的步骤：

步骤 1 单击**服务质量** > **一般** > **接口设置**。此时将显示*接口设置*页面。

步骤 2 选择**端口**或 **LAG** 以显示端口或 LAG 列表。

会显示端口 /LAG 的列表。 **QoS 状态**会显示是否在接口上启用了 QoS。

步骤 3 选择一个接口，并单击**编辑**。此时将显示*编辑 QoS 接口设置*页面。

步骤 4 选择**端口**或 **LAG** 接口。

步骤 5 单击以针对该接口启用或禁用 **QoS 状态**。

步骤 6 单击**应用**。将更新当前配置文件。

配置 QoS 队列

交换机在每个接口支持四个队列。编号为 4 的队列为最高优先级队列，而编号为 1 的队列为最低优先级队列。

有两种方式可确定队列中流量的处理方式：“严格优先级”和 “加权轮循 (WRR)”。

严格优先级 - 最先传输最高优先级队列中的出口流量。最高优先级队列传输完毕后，才会处理更低优先级队列中的流量，从而为编号最高的队列提供最高的流量处理优先级。

加权轮循 (WRR) - 在 WRR 模式下，从队列发送的数据包数量与队列加权成正比 （加权越高，发送的帧越多）。例如，如果四个队列都为 WRR 模式且使用默认加权，则队列 1 将接收 1/15 的带宽（假设所有队列均饱和且存在拥塞）、队列 2 接收 2/15 的带宽、队列 3 接收 4/15 的带宽、队列 4 接收 8/15 的带宽。设备中使用的 WRR 算法类型并非标准的 Deficit WRR (DWRR)，而是 Shaped Deficit WRR (SDWRR)。

排队模式可以在*队列*页面*中选择*。如果排队模式为 “严格优先级”，则优先级将决定处理队列的顺序，从队列 4 （最高优先级队列）开始处理，每当完成一个队列后就继续处理下一优先级的队列。

如果排队模式为 “加权轮循”，则会按照配额处理队列，在一个队列的配额用尽后开始处理另一个队列。

也可以将部分较低优先级的队列指定为 WRR 模式，同时保持部分较高优先级的队列为 “严格优先级”模式。在这种情况下，“严格优先级”队列中的流量会始终先于 WRR 队列中的流量发送。仅当 “严格优先级”队列中的流量发送完毕后才会转发 WRR 队列中的流量。（每个 WRR 队列的相对配额取决于其加权）。

选择优先级方法及输入 WRR 资料的步骤：

步骤 1 单击**服务质量** > **一般** > **队列**。此时将显示*队列*页面。

步骤 2 输入参数。

- **队列** - 显示队列编号。
- **调度方法**：请选择以下其中一个选项：
  - *严格优先级* - 针对所选队列及所有更高优先级队列的流量调度将严格遵循队列优先级。
  - *WRR* - 针对所选队列的流量调度将遵循 WRR。在不为空的 WRR 队列 （表示队列具有要输出的描述符）之间划分时段。仅当 “严格优先级” 队列为空时，才会采用此方法。
  - *WRR 加权* - 如果选择了 WRR，请输入为队列分配的 WRR 加权。
  - *WRR 带宽百分比* - 显示已为队列分配的带宽。这些值表示 WRR 加权的百分比。

步骤 3 单击**应用**。将配置队列，并更新当前配置文件。

将 CoS/802.1p 到队列

使用 *CoS/802.1p 到队列*页面，可以将 802.1p 优先级映射到出口队列。“CoS/802.1p 到队列表” 可根据传入数据包 VLAN 标记中的 802.1p 优先级确定数据包的出口队列。对于传入的 Untagged 数据包， 802.1p 优先级是指定给入口端口的默认 CoS/802.1p 优先级。

默认映射队列

802.1p 值 （0-7， 7 为最高优先级）	队列 （4 个队列 1-4，4 为最高优先级）	队列 （2 个队列：正常和高）	注
0	1	正常	后台
1	1	正常	尽力服务
2	2	正常	最大努力
3	3	正常	关键应用 LVS 电话 SIP

802.1p 值（0-7，7 为最高优先级）	队列 （4 个队列 1-4，4 为最高优先级）	队列 （2 个队列：正常和高）	注
4	3	正常	视频
5	4	高	视频默认思科 IP 电话
6	4	高	交互操作控制 LVS 电话 RTP
7	4	高	交互操作控制

通过更改 “CoS/802.1p 到队列” 映射和队列调度方法及带宽分配，可以在网络中达到所需的服务质量。

“CoS/802.1p 到队列” 映射仅在 CoS/802.1p 为信任模式并且数据包属于 CoS 信任数据流时才适用。

队列 1 的优先级最低，队列 4 的优先级最高。

将 CoS 值映射到出口队列的步骤：

步骤 1 单击**服务质量** > **一般** > **CoS/802.1p 到队列**。此时将显示 *CoS/802.1p 到队列*页面。

步骤 2 输入参数。

- **802.1p** - 显示要指定给出口队列的 802.1p 优先级标记值，其中 0 为最低优先级，7 为最高优先级。
- **输出队列** - 选择 802.1p 优先级所映射的出口队列。支持四个出口队列，其中队列 4 优先级最高，队列 1 优先级最低。

步骤 3 针对每个 802.1p 优先级，选择它所映射的出口队列。

步骤 4 单击**应用**。将 801.1p 优先级值映射到队列 , 并更新当前配置文件。

将 DSCP 到队列

使用 “DSCP （IP *差分服务代码点*）映射到队列” 页面，可以将 DSCP 映射到出口队列。“DSCP 到队列表” 可根据传入 IP 数据包的 DSCP 值确定数据包的出口队列。数据包的原始 VPT （VLAN 优先级标记）不会发生更改。

只需更改 “DSCP 到队列” 映射和队列调度方法及带宽分配，即可在网络中达到所需的服务质量。

“DSCP 到队列”映射仅当 DSCP 为信任模式时适用于 IP 数据包。

非 IP 数据包始终分类为尽力服务队列。

将 DSCP 到队列的步骤：

步骤 1 单击**服务质量** > **一般** > **DSCP 到队列**。此时将显示 *DSCP 到队列*页面。

*DSCP 到队列*页面包含**入口 DSCP**。它将显示传入数据包中的 DSCP 值及其关联类。

步骤 2 选择 DSCP 值所映射的**出口队列** （流量转发队列）。

步骤 3 单击**应用**。将更新当前配置文件。

配置带宽

使用*带宽*页面，用户可以定义两组值 （入口速率限制和出口整形速率）来确定系统可以接收和发送的流量。

入口速率限制是入口接口每秒能够接收的位数。超过此限制的带宽将被丢弃。

为出口整形输入以下值：

- 承诺信息速率 (CIR)，设置允许在出口接口上发送的平均最大数据量，以 “位 / 秒”为单位。
- 承诺突发数据量 (CBS)，即允许发送的突发数据量 （即使数据量超出 CIR 也会照常发送）。该值以数据字节数定义。

输入带宽限制的步骤：

步骤 1 单击**服务质量** > **一般** > **带宽**。此时将显示*带宽*页面。

*带宽*页面会显示每个接口的带宽信息。

% 列为端口带宽除以总端口带宽所得的入口速率限制。

步骤 2 选择一个接口，并单击**编辑**。此时将显示*编辑带宽*页面。

步骤 3 选择**端口或 LAG** 接口。

步骤 4 针对选择的接口，为以下字段输入值：

- **入口速率限制** - 选择该选项将启用入口速率限制，该限制在下面的字段中定义。
- **入口速率限制** - 输入接口所允许的最大带宽。

注 当接口类型为 LAG 时，不会显示这两个**入口速率限制**字段。

- **出口整形速率** - 选择该选项将在接口上启用出口整形。
- **承诺的信息传输速率 (CIR)** - 输入出口接口的最大带宽。
- **承诺突发数据大小 (CBS)** - 以数据字节数的形式输入出口接口的最大突发数据量。即使此数据量会暂时增大带宽，使其超出允许的限制，仍可发送这些数据。

步骤 5 单击**应用**。带宽设置将写入当前配置文件。

配置每队列的出口整形

除限制每端口的传输速率 （在*带宽*页面中完成）*之外*，，交换机还可以在每队列每端口基础上，限制所选出口帧的传输速率。出口速率限制由输出负载整形功能执行。

交换机将限制除管理帧以外的所有帧。在速率计算中将忽略所有未限制的帧，表示其大小不包括在总限制之内。

可以禁用每队列出口速率整形功能。

定义每队列出口整形功能的步骤：

步骤 1 单击**服务质量** > **一般** > **每队列出口整形**。此时将显示*每队列出口整形*页面。

*每队列出口整形*页面会显示每队列的速率限制和突发数据量。

步骤 2 选择接口类型 （端口或 LAG），然后单击**转至**。会显示端口 /LAG 的列表。

步骤 3 选择一个端口 /LAG，然后单击**编辑**。此时将显示*编辑每队列出口整形*页面。

使用该页面可对每个接口上最多四个队列的出口进行整形。

步骤 4 选择**接口**。

步骤 5 针对每个所需队列，为以下字段输入值：

- **启用整形** - 选择该选项可针对队列启用出口整形功能。
- **承诺的信息传输速率 (CIR)** - 以千位每秒 (Kbps) 为单位输入最大速率 (CIR)。CIR 是能够发送的平均最大数据量。
- **承诺突发数据大小 (CBS)** - 以字节为单位输入最大突发数据量 (CBS)。 CBS 是在突发数据量超过 CIR 的情况下允许发送的最大突发数据量。

步骤 6 单击**应用**。带宽设置将写入当前配置文件。

管理 QoS 统计信息

您可以从此页面管理队列统计信息。

查看队列统计信息

*队列统计信息*页面会根据接口、队列和丢弃优先级显示队列统计信息，包括已转发和已丢弃的数据包的统计信息。

注 仅当交换在 QoS 高级模式下，才会显示 QoS 统计信息。可在**一般** > **QoS 属性**中进行此更改。

查看队列统计信息的步骤：

步骤 1 单击**服务质量** > **QoS 统计信息** > **队列统计信息**。此时将显示*队列统计信息*页面。

此页面显示了以下字段：

- **刷新速率** - 选择刷新接口以太网统计信息的间隔时间。可用选项有：
  - *无刷新* - 不刷新统计信息。
  - *15 秒* - 每隔 15 秒刷新统计信息。
  - *30 秒* - 每隔 30 秒刷新统计信息。
  - *60 秒* - 每隔 60 秒刷新统计信息。
- **计数器设置** - 选项如下：
  - *设置 1* - 显示“设置 1”（包含所有具有高 DP [丢弃优先级] 的接口和队列）的统计信息。
  - *设置 2* - 显示 “设置 2”（包含所有具有低 DP 的接口和队列）的统计信息。
- **接口** - 显示此接口的队列统计信息。
- **队列** - 从此队列转发的数据包或丢弃的尾部数据包。
- **丢弃优先级** - 最低的丢弃优先级表示被丢弃的优先级最低。
- **数据包总数** - 被转发的数据包或被丢弃的尾部数据包的数量。
- **丢弃的尾部数据包** - 被丢弃的尾部数据包所占的百分比。

步骤 2 单击**添加**。此时将显示*添加队列统计信息*页面。

步骤 3 输入参数。

- **计数器设置** - 选择计数器集：
  - *设置 1* - 显示“设置 1”（包含所有具有高 DP [丢弃优先级] 的接口和队列）的统计信息。
  - *设置 2* - 显示 “设置 2”（包含所有具有低 DP 的接口和队列）的统计信息。
- **接口** - 选择要显示其统计信息的端口。选项如下：
  - *端口* - 选择所选单元号上要显示其统计信息的端口。
  - *全部端口* - 指定将显示所有端口的统计信息。
- **队列** - 选择要显示其统计信息的队列。
- **丢弃优先级** - 输入丢弃优先级，以表示被丢弃的优先级。

步骤 4 单击**应用**。将添加队列统计信息计数器，并更新当前配置文件。

OL-22849-02