管理指南

思科 Sx250 系列管理型交换机，固件版本 2.4.x，版本 0.3

目录

第 1 章：快速入门 9

使用准备 9
机架安装式交换机 10
以太网供电注意事项 11
配置交换机 13
使用控制台端口配置交换机 15
USB 端口 16
交换机功能 16

第 2 章：一般信息 21

基本或高级显示模式 21
设备配置快速入门 22
接口命名约定 23
窗口导航 23
搜索设备 26

第 3 章：控制面板 27

网格管理 27
系统状况 29
资源使用率 29
身份标识 30
端口使用率 31
PoE 使用率 32
最新日志 33
挂起的接口 33
流量错误 34

第 4 章：配置向导 36

使用入门向导 36
VLAN 配置向导 38
ACL 向导 39

第 5 章：状态和统计信息 42

系统摘要 42
CPU 使用率 44
接口 45
Etherlike 46
端口使用率 47
GVRP 48
802.1X EAP 49
ACL 50
硬件资源使用率 50
运行状况和电源 51
交换端口分析器（SPAN） 54
诊断 56
RMON 59
查看日志 66

第 6 章：管理 69

系统设置 70
用户帐户 70
空闲会话超时 71
时间设置 72
系统日志 72
文件管理 75
即插即用 (PNP) 75
重启 78

目录

发现协议 - Bonjour 79
发现协议 - LLDP 79
发现协议 - CDP 80
定位设备 80
Ping 80
Traceroute 82

第 7 章：管理：文件管理 83
系统文件 83
固件操作 84
文件操作 88
文件目录 95
DHCP 自动配置/映像更新 96

第 8 章：管理：时间设置 104
系统时间配置 104
SNTP 模式 106
系统时间 106
SNTP 单播 108
SNTP 组播/任播 111
SNTP 验证 111
时间范围 112
循环时间范围 114

第 9 章：管理：发现协议 115
Bonjour 115
LLDP 和 CDP 116
发现协议 - LLDP 117
发现协议 - CDP 137

第 10 章：端口管理 146
工作流程 146
端口设置 147
错误恢复设置 150
环回检测设置 151
链路聚合 153
PoE 159
绿色以太网 167
第 11 章：智能端口 174
概述 174
智能端口功能如何运作 178
自动智能端口 179
错误处理 182
默认配置 182
与其他功能的关系 182
常见智能端口任务 183
使用基于 Web 的界面配置智能端口 185
内置智能端口宏 189
第 12 章：VLAN 管理 200
常规 VLAN 202
GVRP 设置 208
语音 VLAN 209
第 13 章：生成树 221
STP 模式 221
STP 状态和全局设置 222
STP 接口设置 223
RSTP 接口设置 225

目录

多生成树概述 227
MSTP 属性 228
VLAN 到 MSTP 实例 229
MSTP 实例设置 230
MSTP 接口设置 230

第 14 章：管理 MAC 地址表 233
静态地址 233
动态地址 234

第 15 章：组播 236
组播转发概述 236
属性 240
MAC 组地址 241
IP 组播群地址 243
IPv4 组播配置 244
IPv6 组播配置 247
IGMP/MLD 侦听 IP 组播组 249
组播路由器端口 250
全部转发 251
未注册的组播 252

第 16 章：IP 配置 253
概述 253
环回接口 254
IPv4 管理和接口 255
IPv6 管理和接口 263
域名系统 280

第 17 章：安全 285
RADIUS 286
密码强度 289
管理访问方法 290
管理访问验证 295
SSL 服务器 296
SSH 客户端 298
TCP/UDP 服务 299
风暴控制 300
端口安全 302
802.1X 验证 304
拒绝服务防护 305
第 18 章：安全：802.1X 验证 314
概述 314
属性 322
端口验证 323
主机和会话验证 325
已验证的主机 326
第 19 章：安全：安全敏感数据管理 327
简介 327
SSD 管理 328
SSD 规则 328
SSD 属性 333
配置文件 335
SSD 管理通道 339
菜单 CLI 和密码恢复 339
配置 SSD 340

目录

第 20 章：安全：SSH 服务器 343

概述 343

常见任务 344

SSH 用户验证 345

SSH 服务器验证 346

第 21 章：安全：SSH 客户端 348

概述 348

SSH 用户验证 353

SSH 服务器验证 354

更改 SSH 服务器的用户密码 356

第 22 章：访问控制 357

概述 357

创建基于 MAC 的 ACL 361

创建基于 IPv4 的 ACL 363

创建基于 IPv6 的 ACL 367

ACL 绑定 371

第 23 章：服务质量 374

QoS 功能和组件 374

常规 377

QoS 基本模式 386

QoS 高级模式 388

QoS 统计信息 398

第 24 章：SNMP 401

概述 401

引擎 ID 404

视图 406

组 407
用户 409
社区 410
陷阱设置 412
通知接收设备 412
通知过滤器 416

1

快速入门

本节包含以下主题：

使用准备

机架安装式交换机

以太网供电注意事项

配置交换机

使用控制台端口配置交换机

USB 端口

USB 端口

堆叠交换机

交换机功能

使用准备

开始安装设备之前，请确保准备好以下物品：

- 用于连接网络设备的 RJ-45 以太网电缆。对于 10G 端口，必须使用 6A 类或更高级别的电缆；对于所有其他端口，必须使用 5E 类或更高级别的电缆。
- 用于通过控制台端口管理交换机的控制台电缆。
- 用于安装硬件的工具。交换机附带的机架固定套件包含 4 个用于桌面安放的橡胶支脚、2 个支架和 12 个用于机架式安装的螺钉。如果附带的螺钉遗失，请使用以下尺寸的螺钉作为替代：
  - 螺钉头直径：6.9 毫米
  - 螺钉全长（钉头至钉尖）：5.9 毫米
  - 钉身直径：3.94 毫米

- 装有 Internet Explorer（版本 9.0、10.0 或 11.0）、Firefox（版本 36.0、37.0 或更高版本）或 Chrome（版本 40、41、42 或更高版本）的计算机，用于通过基于 Web 的界面或控制台端口来管理交换机。

机架安装式交换机

本交换机可以安装在标准的 19 英寸（约 48 厘米）机架中。交换机需要占用 1 个机架单元 (RU) 高的空间（即 1.75 英寸，约 44.45 毫米）。

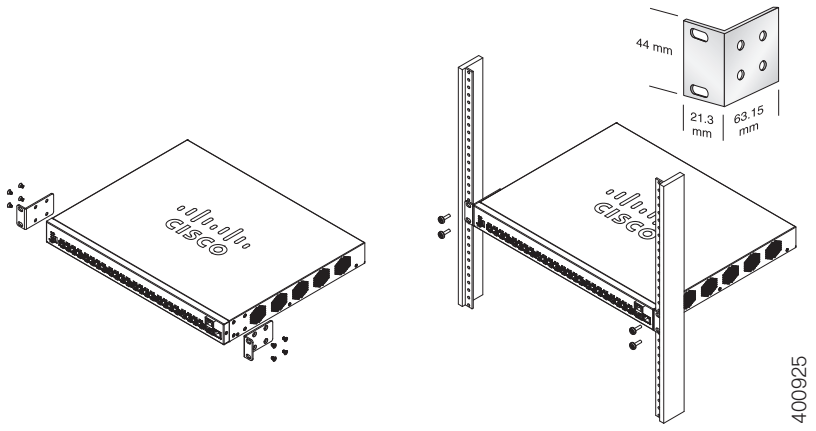
注意 为确保稳固，请按从下到上的顺序装载机架，将最重的设备安放在机架底部。如果机架顶部过重，则有可能安放不稳固，甚至发生倾倒。

要将交换机安装到标准的 19 英寸机架中，请执行以下操作：

步骤 1 将其中一个附带的支架放于交换机的一侧，使支架上的四个孔与交换机上的螺钉孔对齐，然后使用附带的四个螺钉将其固定。

步骤 2 重复上一步骤，将另一个支架安装到交换机的另一侧。

步骤 3 支架安装牢固后，即可将交换机装入标准的 19 英寸机架中。



以太网供电注意事项

警告 本交换机可以仅连接到 PoE 网络，而不必连接外部电源。

有的设备支持 PoE，有的设备不支持 PoE。如果一个型号支持 PoE，则型号末尾会带有一个字母 P，例如：SF250-48HP。

系统会在所有相关页面上介绍 PoE 字段，尽管只有支持 PoE 的设备才支持这些字段。

如果您的交换机是其中一种以太网供电 (PoE) 型号，请注意以下电源要求

表 1 具有以太网供电功能的交换机

SKU 名称	说明	PoE PD 芯片集类型	PoE PSE 芯片集类型	PoE PD AF/AT/60W	PoE PSE AF/AT/60W
SF250-24P	SF250-24P 24 端口 10/100 PoE 智能交换机	不适用	3*69208**M** (0x4B42)	不适用	AF/AT
SF250-48HP	SF250-48HP 48 端口 10/100 PoE 智能交换机	不适用	6* PD69208 (0x4AC2) / 6*69208**M** (0x4B42)（截至 2.2.7）	不适用	AF/AT
SG250-08HP	SG250-08HP 8 端口千兆 PoE 智能交换机	不适用	1*69208**M** (0x4B42)	不适用	AF/AT
SG250-10P	SG250-10P 10 端口千兆 PoE 智能交换机	2x PD70210 + 2x PD70222 + 1?x LX7309	1* PD69208 (0x4AC2) / 1*69208**M** (0x4B42)	AF/AT/60W	AF/AT
SG250-26HP	SG250-26HP 26 端口千兆 PoE 智能交换机	不适用	3* PD69208 (0x4AC2) / 3*69208**M** (0x4B42)	不适用	AF/AT
SG250-26P	SG250-26P 26 端口千兆 PoE 智能交换机	不适用	3* PD69208 (0x4AC2) / 3*69208**M** (0x4B42)	不适用	AF/AT

表 1　具有以太网供电功能的交换机（续）

SKU 名称	说明	PoE PD 芯片集类型	PoE PSE 芯片集类型	PoE PD AF/AT/60W	PoE PSE AF/AT/60W
SG250-50HP	SG250-50HP 50 端口千兆 PoE 智能交换机	不适用	6*69208**M** (0x4B42)	不适用	AF/AT
SG250-50P	SG250-50P 50 端口千兆 PoE 智能交换机	不适用	6*69208**M** (0x4B42)	不适用	AF/AT
SG250X-24P	SG250X-24P 24 端口千兆 PoE + 4 端口万兆智能交换机	NA	3*69208**M** (0x4B42)	NA	AF/AT
SG250X-48P	SG250X-48P 48 端口千兆 PoE + 4 端口万兆智能交换机	NA	6*69208**M** (0x4B42)	NA	AF/AT

注　60 瓦 PoE 对 IEEE 增强型以太网供电标准进行了延伸，使每端口功率增加一倍，达到 60 瓦。

注意　连接具有 PoE 功能的交换机时，请注意以下事项：
本交换机的 PoE 型号为供电设备 (PSE)，能够向连接的用电设备 (PD) 供应直流电，这类设备包括 IP 电话 (VoIP)、IP 摄像头和无线接入点。PoE 交换机可以检测出准标准型旧式 PoE 用电设备，并为其供电。由于要支持旧式 PoE 设备，作为供电设备使用的 PoE 交换机可能会发生检测错误，将连接的供电设备（包括其他 PoE 交换机）也当作旧式用电设备，并为其供电。
尽管 PoE 交换机是供电设备，并因此应采用交流电供电，但它们也可能由于检测错误而被其他供电设备当作旧式用电设备而供电。如果发生这种情况，PoE 交换机可能无法正常工作，而且可能无法正确地为所连接的用电设备供电。
为防止检测错误，应针对 PoE 交换机上用于连接供电设备的端口禁用 PoE 功能。此外，在将通供电设备连接到 PoE 交换机之前，应先接通该供电设备的电源。如果某设备被错误地检测为用电设备，您应断开该设备与 PoE 端口的连接，并使用交流电源为其供电，然后再将其重新连接到 PoE 端口。

配置交换机

使用准备

此系列交换机可通过两种方法访问和管理：使用基于 Web 的界面通过 IP 网络进行访问和管理；通过控制台端口使用命令行接口 (CLI) 进行访问和管理。使用控制台端口要求用户具有高级技能。

下表显示了首次配置交换机时使用的默认设置：

参数	默认值
用户名	**cisco**
密码	**cisco**
LAN IP	**192.168.1.254**

使用基于 Web 的界面配置交换机

要使用基于 Web 的界面访问交换机，您必须知道交换机所使用的 IP 地址。本交换机的出厂默认 IP 地址为 192.168.1.254，子网掩码为 /24。

当交换机使用出厂默认 IP 地址时，其系统 LED 将持续闪烁。如果交换机使用 DHCP 服务器分配的 IP 地址，或者管理员为其配置了静态 IP 地址，系统 LED 将会呈绿色稳定亮起（默认情况下 DHCP 处于启用状态）。

如果您通过网络连接来管理交换机，而交换机的 IP 地址已通过 DHCP 服务器或以手动方式进行了更改，您将无法再度访问交换机。要使用基于 Web 的界面，您必须在浏览器中输入交换机的新 IP 地址。如果您通过控制台端口连接管理交换机，此链路将被保留。

要使用基于 Web 的界面配置交换机，请执行以下操作：

步骤 1 接通计算机和交换机的电源。

步骤 2 对于思科 350-550 XG 交换机，请将计算机连接到交换机前面板上的 OOB 端口；对于所有其他交换机，可将计算机连接到交换机的任何网络端口。

步骤 3 设置计算机上的 IP 配置。

a. 如果交换机使用默认静态 IP 地址 192.168.1.254/24，您必须在 IP 地址范围 192.168.1.2 至 192.168.1.253 内为计算机选择一个尚未使用的 IP 地址。

b. 如果 IP 地址由 DHCP 进行分配，则请确保您的 DHCP 服务器正在运行，并且可以从交换机和计算机进行访问。您可能需要先断开设备连接，然后再重新连接，才能使设备发现来自 DHCP 服务器的新 IP 地址。

注 更改计算机上的 IP 地址的具体操作，视您所使用的架构类型和操作系统而定。请使用计算机的“帮助和支持”功能搜索“IP 寻址”。

步骤 4 系统将打开一个 Web 浏览器窗口。如果在连接到设备时系统提示您安装 ActiveX 插件，请按照提示接受该插件。

步骤 5 在地址栏中输入交换机的 IP 地址，然后按 **Enter** 键。例如，输入 **http://192.168.1.254**。

步骤 6 出现登录页面时，请选择您希望在基于 Web 的界面中使用的语言，然后输入用户名和密码。

默认用户名为 **cisco**。默认密码为 **cisco**。用户名和密码均区分大小写。

步骤 7 单击**登录**。

如果这是您第一次使用默认用户名和密码登录，系统会打开“更改密码”页面。页面上将显示创建新密码的规则。

步骤 8 输入新密码和确认密码。

注 默认情况下，将启用密码复杂性设置。密码必须符合默认复杂性规则。您也可以选中“密码强度规则”旁边的**禁用**复选框来暂时禁用该规则。

步骤 9 单击**应用**。

注意 对配置进行任何更改后，请单击**保存**图标以保存更改，然后再退出基于 Web 的界面。如果在保存配置之前退出，则会导致所有更改丢失。

系统将打开“配置向导”页面。您现在即可配置交换机。有关更多信息，请参阅《管理指南》或访问帮助页面。

浏览器限制

如果正在管理工作站上使用 IPv6 接口，则可以使用 IPv6 全局地址（而非 IPv6 链路本地地址）从浏览器访问设备。

使用控制台端口配置交换机

要使用控制台端口配置交换机，请执行以下操作：

步骤 1 使用附带的控制台端口电缆将计算机连接到交换机控制台端口。

步骤 2 启动计算机上的控制台端口实用程序（例如 HyperTerminal）。

步骤 3 使用以下参数配置实用程序：

- 每秒 115200 位
- 8 个数据位
- 无奇偶校验位
- 1 个停止位
- 无流量控制

步骤 4 输入用户名和密码。默认用户名为 **cisco**，默认密码为 **cisco**。用户名和密码均区分大小写。

第一次使用默认用户名和密码登录时，系统会显示以下消息：

```
"Please change your password from the default settings. Please change the
password for better protection of your network. Do you want to change the
password (Y/N) [Y]?"
```

步骤 5 输入 **Y**，然后设置一个新的管理员密码。

注 默认情况下，将启用密码复杂性设置。密码必须符合默认复杂性规则。

注意 退出之前，请务必先保存您所做的任何配置更改。

您现在即可配置交换机。请参阅适用于您的交换机的 CLI 指南。

注 如果您未在网络中使用 DHCP，请在交换机上将 IP 地址类型设置为**静态**，然后更改静态 IP 地址和子网掩码，以便与您的网络拓扑相匹配。否则可能导致多台交换机使用相同的出厂默认 IP 地址 192.168.1.254。

USB 端口

USB 端口可用于连接外部存储（闪存盘）设备。它可以保存配置、系统日志和映像文件。USB 端口对 FAT32 文件系统提供完全支持，对 NTFS 文件系统提供部分支持（只读）。

两个相对路径或完全限定路径可同时使用。

系统支持通过 GUI 在 USB 端口上执行的以下用户操作：

- 显示 USB 内容
- 将文件复制到 USB 或者从 USB 复制文件（与使用 TFTP 相同）
- 删除、重命名和显示 USB 文件内容

交换机功能

本节介绍交换机的外观，以帮助您熟悉您的交换机。

产品型号

下面是提供的产品型号：

表 2 产品型号

SKU 名称	说明
SF250-24	SF250-24 24 端口 10/100 智能交换机
SF250-24P	SF250-24P 24 端口 10/100 PoE 智能交换机
SF250-48	SF250-48 48 端口 10/100 智能交换机
SF250-48HP	SF250-48HP 48 端口 10/100 PoE 智能交换机

表 2　产品型号（续）

SKU 名称	说明
SG250-08	SG250-08 8 端口千兆智能交换机
SG250-08HP	SG250-08HP 8 端口千兆 PoE 智能交换机
SG250-10P	SG250-10P 10 端口千兆 PoE 智能交换机
SG250-18	SG250-18 18 端口千兆智能交换机
SG250-26	SG250-26 26 端口千兆智能交换机
SG250-26HP	SG250-26HP 26 端口千兆 PoE 智能交换机
SG250-26P	SG250-26P 26 端口千兆 PoE 智能交换机
SG250-50	SG250-50 50 端口千兆智能交换机
SG250-50HP	SG250-50HP 50 端口千兆 PoE 智能交换机
SG250-50P	SG250-50P 50 端口千兆 PoE 智能交换机
SG250X-24	SG250X-24 24 端口千兆 + 4 端口万兆智能交换机
SG250X-24P	SG250X-24P 24 端口千兆 PoE + 4 端口万兆智能交换机
SG250X-48	SG250X-48 48 端口千兆 + 4 端口万兆智能交换机
SG250X-48P	SG250X-48P 48 端口千兆 PoE + 4 端口万兆智能交换机

前面板

端口、LED 和重置按钮均位于交换机的前面板上，如下图所示。下面显示的并不是所有 SKU，而是一组具有代表性的 SKU。

TBD

SF240_24P

SG250-10P

下列组件可在设备的前面板上找到：

- USB 端口 — USB 端口用于连接交换机与 USB 设备，以便您可以通过所连接的 USB 设备保存并存储配置文件、固件映像和 SYSLOG 文件。
- RJ-45 以太网端口 — 这些端口用于将网络设备（例如计算机、打印机和无线接入点）连接到交换机。
- 多千兆以太网端口 — 以蓝色突出标明，支持基于 5E 类电缆的 100 Mbps、1 Gbps 和 2.5 Gbps 传输速度。目前在全球范围内，许多已部署的布线都存在速度限制 (1 Gbps) 和距离限制（100 米）。思科多千兆以太网无需更换电缆，即可在相同的基础设施上支持最高 2.5 Gbps 传输速度。
- 60 瓦 PoE 端口 — 以黄色突出标明。60 瓦 PoE 端口可以使 PoE 功率增加一倍，达到 60 瓦。250 设备或 SF350-48P 设备不具备此功能。
- SFP+ 端口（如果有）— 增强型小型封装热插拔 (SFP+) 端口是模块的连接点，可用于在交换机之间建立链路。这些端口也常称为小型万兆接口转换器端口。本指南中使用 SFP+ 这一术语。
- SFP+ 端口只能与下列思科 SFP 1G 光纤模块 MGBSX1、MGBLH1、MGBT1 以及其他品牌的模块兼容。
- 思科交换机支持的思科 SFP+ 10G 光纤模块包括：SFP-10G-SR、SFP-10G-LR、SFP-10G-SR-S 和 SFP-10G-LR-S。
- 思科交换机支持的思科 SFP+ 铜缆堆叠模块包括：SFP-H10GB-CU1M、SFP-H10GB-CU3M 和 SFP-H10GB-CU5M。
- SFP+ 端口是一个组合端口，与交换机的某个 RJ-45 端口共用一个端口。SFP+ 处于活动状态时，毗邻的 RJ-45 端口会被禁用。
- 某些 SFP 接口与交换机的某个 RJ-45 接口共用一个端口，称为组合端口。SFP 处于活动状态时，毗邻的 RJ-45 端口会被禁用。
- 当设备对 SFP 接口流量作出响应时，相应 RJ-45 端口的 LED 会呈绿色闪烁。
- OOB 端口（如果有）— 带外 (OOB) 端口是 CPU 的以太网端口，只能作为管理接口使用。交换机不支持 OOB 端口与带内第二层接口之间的桥接。这一点在 250 设备上不会出现。

前面板 LED

下面列出了可在设备上找到的全局 LED：

- 主单元 —（绿色）当交换机为堆叠的主单元时，此 LED 会持续亮起。
- 系统 —（绿色）当交换机接通电源时，此 LED 会持续亮起；当交换机启动、执行自检或获取 IP 地址时，此 LED 会闪烁。如果此 LED 呈绿色闪烁，则表示交换机检测到硬件故障、固件故障和/或配置文件错误。
- 堆叠 ID —（绿色）此 LED 会在交换机处于堆叠模式时持续亮起，相应数字表示交换机的堆叠 ID。

下面是每端口 LED：

- 链路/活动 LED —（绿色）位于每个端口左侧。当检测到相应端口与其他设备之间的链路时，此 LED 会持续亮起；当端口正在传输流量时，此 LED 会闪烁。
- XG —（绿色）位于 10G 端口右侧。此 LED 在接通电源的其他设备连接到端口且设备之间建立了 10 Gbps 链路时持续亮起。如果此 LED 熄灭，则表示连接速度低于 10 Gbps，或者没有设备通过电缆连接到端口。
- 千兆 —（绿色）位于 OOB 端口右侧。此 LED 在接通电源的其他设备连接到端口且设备之间建立了 1000 Mbps 链路时持续亮起。如果此 LED 熄灭，则表示连接速度低于 1000 Mbps，或者没有设备通过电缆连接到端口。
- SFP+（如果有）—（绿色）位于 10G 端口右侧。当通过共用端口建立了链路时，此 LED 会持续亮起；当端口正在传输流量时，此 LED 会闪烁。
- PoE（如果有）—（琥珀色）位于端口右侧。当交换机正在为连接到相应端口的设备供电时，此 LED 会持续亮起。

重置按钮

将大头针或曲别针插入交换机前面板上的**重置**按钮孔中，可以重置交换机。要使用**重置**按钮重启或重置交换机，请执行以下操作：

- 要重启交换机，请按住**重置**按钮不超过 10 秒。
- 要将交换机还原为出厂默认设置，请执行以下操作：
  - 断开交换机与网络的连接，或禁用网络上的所有 DHCP 服务器。
  - 接通电源，并按住**重置**按钮 10 秒以上。

后面板

下列按钮可在后面板上找到：

- 电源 — 用于连接交换机与交流电源。
- 控制台 — 用于通过串行电缆连接到计算机串行端口，以便使用终端仿真程序配置交换机。

2

一般信息

本节包含以下主题：

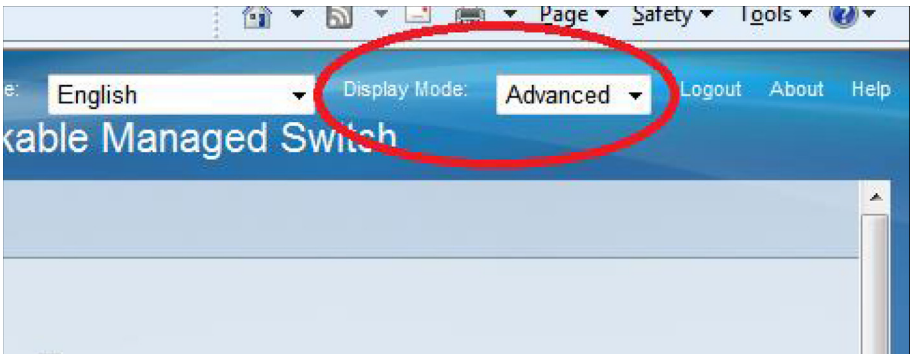
- 基本或高级显示模式
- 设备配置快速入门
- 接口命名约定
- 窗口导航
- 搜索设备

基本或高级显示模式

产品支持许多功能，因此，WEB GUI 包括数百个配置和显示页面。这些页面可分为以下显示模式：

- **基本** — 配置选项的基本子集可用。如果缺失一些配置选项，请在设备标头中选择“高级”模式。
- **高级** — 全套配置选项可用。

从一个模式导航到另一个模式，如下所示：



当用户从基本模式切换到高级模式时，浏览器重新加载页面。不过，在重新加载之后，用户会留在原来的页面。

当用户从高级模式切换到基本模式时，浏览器重新加载页面。如果页面也在基本模式下，用户将留在原来的页面。如果页面不在基本模式下，浏览器将加载用户使用的文件夹的首页。如果文件夹不存在，系统会显示“使用入门”页面。

如果有高级配置，而且页面在基本模式下加载，系统会向用户显示一条页面级消息（例如，配置了 2 个 radius 服务器，但在基本模式下只能显示一个服务器，或者虽然存在配置了时间范围的 802.1X 端口验证，但时间范围在基本模式下不可见）。

从一个模式切换到另一个模式时，系统会删除在此页面上所做的任何配置（无“应用”）。

设备配置快速入门

对于快速初始设置，您可以使用 VLAN 配置向导中介绍的配置向导，或者使用“使用入门”页面上的链接，如下所示：

类别	链接名称（在页面上）	链接的页面
初始设置	更改管理应用和服务	TCP/UDP 服务
	更改设备 IP 地址	IPv4 接口
	创建 VLAN	VLAN 设置
	配置端口设置	端口设置
设备状态	系统摘要	系统摘要
	端口统计信息	接口
	RMON 统计信息	统计信息
	查看日志	RAM 内存
快速访问	更改设备密码	用户帐户
	升级设备软件	固件操作
	备份设备配置	文件操作
	创建基于 MAC 的 ACL	创建基于 MAC 的 ACL
	创建基于 IP 的 ACL	创建基于 IPv4 的 ACL
	配置 QoS	QoS 属性
	配置 SPAN	交换端口分析器（SPAN）

在“使用入门”页面上有两个热链接，可引导您前往思科 Web 页面了解详情。单击**支持**链接，可跳转到设备产品支持页面，而单击**论坛**链接可跳转到“支持社区”页面。

接口命名约定

GUI 内通过结合以下元素来表示接口：

- **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**。
  - **带外端口** — 这种类型的接口显示为 **OOB**。
  - **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

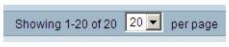
应用报头显示在每个页面上。可以提供以下应用程序链接：

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。在设备上，通过将当前配置文件复制到启动配置文件类型来保存该文件。保存后，系统将不再显示红色 X 图标和“保存”应用链接。设备重启时，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设备参数。

应用程序链接名称	说明
用户名	显示登录到设备的用户名。默认的用户名为 **cisco**。（默认密码是 **cisco**）。
主机名	显示在“系统设置”页面中分配的主机名。如果主机名超过 20 个字符，仅显示前 20 个字符并追加省略号 (...)。将鼠标悬停于删节的主机名将显示工具提示，显示完整的主机名。
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设备。 注 要升级语言文件，请使用“升级/备份固件/语言”页面。
注销	单击该链接可注销基于 Web 的交换机配置实用程序。
关于	单击该链接会显示设备名称和设备版本号。
帮助	单击该链接会显示在线帮助。
	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，系统将不会再显示“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 内存**。

管理按钮

下表介绍了系统中各页面上显示的常用按钮。

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，并在设备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设备上的当前配置。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，否则当设备重启时，当前配置会丢失。单击**保存**会显示“复制/保存配置”页面，并在设备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	清除页面上的信息。
清除过滤	单击该按钮会清除用于选择显示信息的过滤器。
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。

按钮名称	说明
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。
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**。系统此时将显示“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。
刷新	单击**刷新**可刷新计数器值。
测试	单击**测试**可执行相关测试。
恢复默认设置	单击**恢复默认设置**可以恢复出厂默认设置。
取消默认设置	单击**取消默认设置**可以恢复出厂默认设置。

搜索设备

搜索功能可帮助用户找到相关的 GUI 页面。

关键字搜索结果会包含到相关页面的链接，以及到相关帮助页面的链接。

要访问搜索功能，请输入关键字，单击放大镜图标。

3

控制面板

控制面板由 8 个方格组成，这些方格最初为空，之后可填充各类信息。

您可以从可用模块中选择一些模块，并将它们放在此网格中。也可以自定义当前显示的模块的设置。

加载控制面板时，您为控制面板选择的模块将在网格中的对应位置加载。模块中的数据定期更新，时间间隔取决于模块类型。对于某些模块，可以配置这些时间间隔。

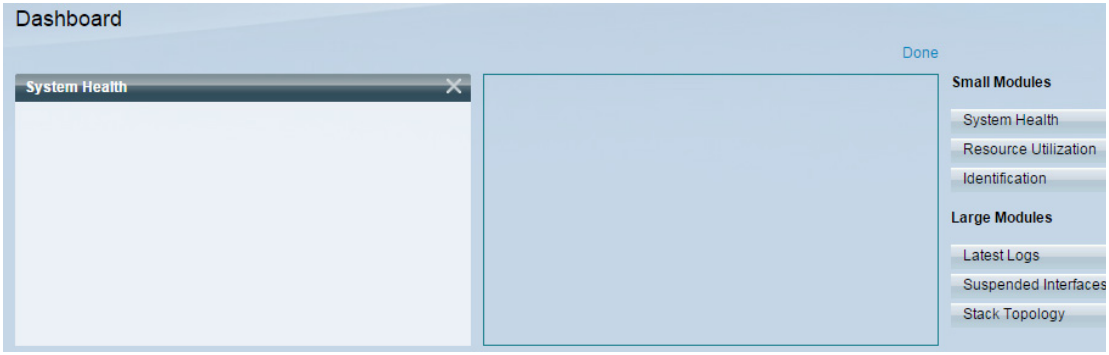
本章包含以下主题：

- 网格管理
- 系统状况
- 资源使用率
- 身份标识
- 端口使用率
- PoE 使用率
- 最新日志
- 挂起的接口
- 流量错误

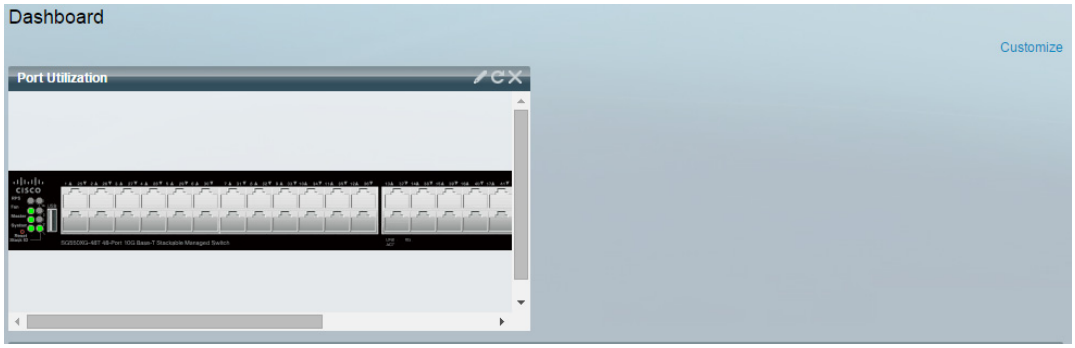
网格管理

控制面板由多个模块构成，但只有一部分模块可以同时查看。

打开控制面板时，系统显示网格的线框图，如下所示（下面的屏幕截图中仅显示了 2 个方格）：



要显示当前未显示的模块，请单击控制面板右上角的**自定义**，如下所示：



从右侧模块列表中选择一个模块并拖放到网格中的任意位置，将模块添加到网格中。

模块分为以下几组：

- **小模块**指的是占用一个方格的模块。
- **大模块**占用两个方格。

如果将模块拖动到当前已被占用的空间，新模块将替代以前的模块。

将模块从一个已占用网格位置拖动到另一个位置，可以调整模块在网格中的位置。可以将模块放在未被占用的位置，或者放在已被相同大小的模块占用的位置。如果所选位置已被占用，模块将交换位置。

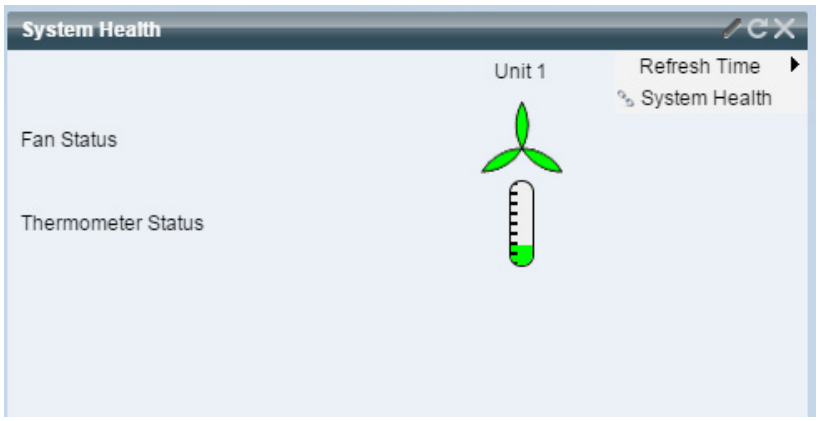
仅在单击**完成**（位于右上角）时，系统才会在模块中填充相关信息控制面板中每个模块的标题栏中显示模块标题和三个按钮：

这些按钮可以执行以下操作：

- 铅笔 — 打开配置选项（取决于模块）。
- 刷新 — 刷新信息。
- X — 从控制面板中删除模块。

系统状况

此模块显示设备，如下所示：



系统显示以下图标：

- **风扇状态** — 如果一个风扇发生故障并且由冗余风扇提供支持，显示黄色；如果风扇运行正常，显示绿色；如果风扇发生故障，显示红色。
- **温度计状态**
  - *温度正常* — 温度计为绿色，呈近乎为空的状态。
  - *温度生成警告* — 黄色，温度计半满。
  - *温度达到临界值* — 红色，温度计全满。

下列配置选项（右上角的铅笔图标）可用：

- **刷新时间** — 选择显示的选项之一。

资源使用率

此模块用条形图显示以各种系统资源百分比表示的使用率状态，监控的资源包括：

- **组播组** — 以所允许定义的最大组播组数量的百分比表示的现有组播组百分比。
- **MAC 地址表** — 正在使用的 MAC 地址百分比表。
- **TCAM** — QoS 和 ACL 条目使用的 TCAM 百分比。
- **CPU** — 正在使用的 CPU 百分比。

如果资源使用率超过 80%，每个条形将变为红色。

将光标悬停在条形上可显示工具提示，显示以数字表示的使用率信息（已用资源/最大可用资源的比值）。

以下配置选项（右上角）可用：

- **刷新时间** — 选择显示的选项之一。
- **组播组** — 单击打开 MAC 组地址
- **MAC 地址表** — 单击打开动态地址。
- **TCAM 使用率信息** — 单击打开硬件资源使用率。
- **CPU 使用率信息** — 单击打开 CPU 使用率。

身份标识

此模块显示关于设备的基本信息，如下所示：

此模块显示以下字段：

- **系统说明** — 显示设备说明。
- **主机名** — 在系统设置页面中输入主机名或使用默认主机名。也可以在使用入门向导中添加。
- **固件版本** — 设备上当前运行的固件版本。
- **MAC 地址** — 设备的 MAC 地址。
- **序列号** — 设备的序列号。

- **系统位置** — 输入设备的物理位置。
- **系统联系人** — 输入联系人姓名。
- **可用功率总计** — 设备可用的功率。
- **当前功耗** — 设备消耗的功率。

以下配置选项（右上角）可用：

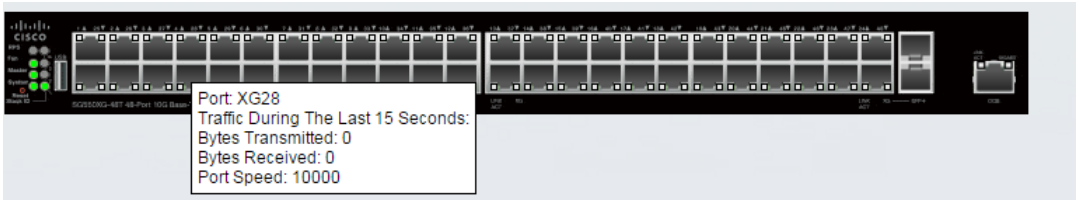
- **刷新时间** — 选择显示的选项之一。
- **系统设置** — 单击可打开系统设置。
- **系统摘要** — 单击可打开系统摘要。

端口使用率

此模块在设备视图或图表视图中显示设备上的端口。此视图可在配置选项中选择（右上角的铅笔图标）。

- **显示模式 — 设备视图**

  显示设备。将光标悬停在某个端口上会显示该端口的相关信息。



- **显示模式 — 图表视图**

  显示端口列表。端口使用率以条形格式显示：

对于每个端口，系统显示以下端口使用率信息：

Tx—%（红色）

Rx—%（蓝色）

- **刷新时间** — 选择显示的选项之一。
- **接口统计信息** — 链接至**状态和统计信息 -> 接口**页面。

PoE 使用率

此模块显示 PoE 使用率状态的图示，如下所示：

此模块显示一个仪表，表盘数值范围为 0-100。在表盘中，从陷阱阈值到 100 的部分为红色。在仪表中间，实际 PoE 使用率值以瓦特为单位显示。

每个条形表示设备 PoE 使用率的百分比值，取值范围为 0 到 100。如果 PoE 使用率高于陷阱阈值，则条形为红色。否则，条形为绿色。

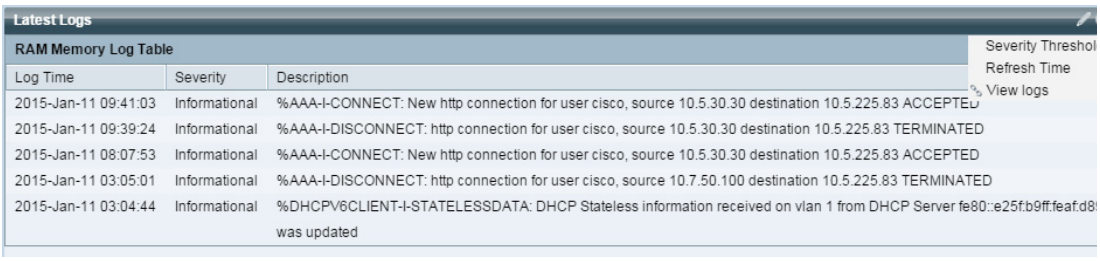
将光标悬停在条形上时，出现工具提示，显示设备的实际 PoE 使用率，以瓦特为单位。

更多视图可在配置选项中选择（右上角的铅笔图标）。

- **刷新时间** — 选择显示的选项之一。
- **PoE 全局属性** — 链接至**端口管理 -> PoE -> 属性**页面。
- **PoE 端口设置** — 链接至**端口管理 -> PoE -> 设置**页面。

最新日志

此模块包含系统记录为系统日志的 5 个最新事件的相关信息，如下所示：



以下配置选项（右上角）可用：

- **严重程度阈值** — 日志设置中进行了介绍。
- **刷新时间** — 选择显示的选项之一。
- **查看日志** — 单击可打开 RAM 内存。

注 有关详情，请参阅查看日志。

挂起的接口

此模块在设备视图或表视图中显示已挂起的接口。此视图可在配置选项中选择（右上角的铅笔图标）。

- **设备视图**

  在此视图中，显示设备。如下所示：

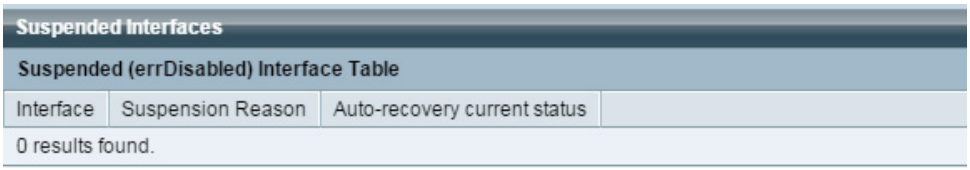
  设备中的所有已挂起端口将显示为红色。

将光标悬停在已挂起端口上，会显示工具提示以及下列信息：

- 端口名称。
- 如果端口是 LAG 的成员，则显示端口的 LAG 身份。
- 如果端口已挂起，则显示挂起原因。

- **表格视图**

  信息将以表格形式显示，如下所示：



  系统将显示以下字段：

  - **接口** — 已被挂起的端口或 LAG。
  - **挂起原因** — 接口被挂起的原因。
  - **自动恢复当前状态** — 针对引起挂起的功能启用自动恢复。

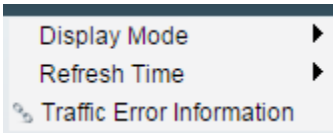
以下配置选项（右上角）可用：

- **显示模式** — 选择**设备视图**或**表视图**。
- **刷新时间** — 选择显示的选项之一。
- **错误恢复设置** — 单击可打开错误恢复设置。

流量错误

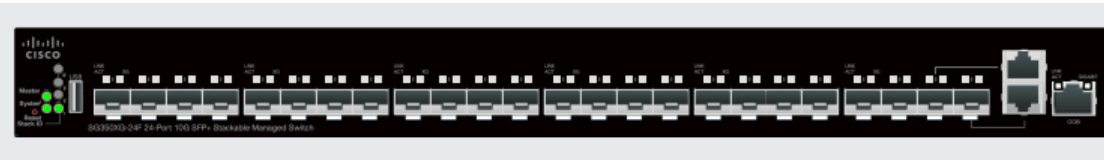
此模块显示在 RMON 统计信息中统计的各个类型的错误数据包数量。此视图可在配置选项中选择（右上角的铅笔图标）。

可通过铅笔图标选择以下字段：



- **显示模式 — 设备视图**

  设备模块模式显示设备示意图，如下所示：



  设备中的所有已挂起端口将显示为红色。

  将光标悬停在已挂起端口上，会显示工具提示以及下列信息：

  - 端口名称。
  - 如果端口是 LAG 的成员，则显示端口的 LAG 身份。
  - 在端口上记录的最后一个错误的详细信息。

- **显示模式 — 表视图**
  - *接口* — 端口名称
  - *最后一次流量错误* — 发生在端口上的流量错误以及错误发生的最后时间。
- **刷新时间** — 选择其中一种刷新速率。
- **流量错误信息** — 单击可链接到统计信息页面。

4

配置向导

本节将介绍以下配置向导：

其中包含以下主题：

- 使用入门向导
- VLAN 配置向导
- ACL 向导

使用入门向导

该向导帮助完成设备的初始配置。

步骤 1 单击**配置向导** > **使用入门向导**。

步骤 2 单击**启动向导**和**下一步**。

步骤 3 输入以下字段：

- **系统位置** — 输入设备的物理位置。
- **系统联系人** — 输入联系人姓名。
- **主机名** — 选择此设备的主机名。系统会在 CLI 命令的提示符中使用此主机名：
  - *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 代表设备 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）。

步骤 4 单击**下一步**。

步骤 5 输入以下字段：

- **接口** — 选择系统的 IP 接口。
- **IP 接口源** — 选择以下其中一个选项：
  - *DHCP* — 选择后，设备能从 DHCP 服务器接收 IP 地址。
  - *静态* — 选择后，手动输入设备的 IP 地址。

如果选择“静态”作为 IP 接口源，请在以下字段输入值：

- **IP 地址** — 接口的 IP 地址。
- **网络掩码** — 此地址的 IP 掩码。
- **管理默认网关** — 输入默认网关 IP 地址。
- **DNS 服务器** — 输入 DNS 服务器的 IP 地址。

步骤 6 单击**下一步**

步骤 7 输入以下字段：

- **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，则用户密码必须与密码强度中配置的策略相符。
- **确认密码** — 再次输入密码。
- **密码强度** — 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。
- **保留当前用户名和密码** — 选择该选项可保留当前用户名和密码。

步骤 8 单击**下一步**

步骤 9 输入以下字段：

- **时钟源** — 选择以下其中一项：
  - *手动设置* — 选择后输入设备系统时间。如果选中此选项，请输入**日期**和**时间**。
  - *默认 SNTP 服务器* — 选择使用默认 SNTP 服务器。

  注 默认 SNTP 服务器由名称定义，因此 DNS 必须经过配置并且可运行（DNS 服务器已配置并且可访问）。这是在 DNS 设置中进行的。
  - *手动 SNTP 服务器* — 选择并输入 SNTP 服务器的 IP 地址。

步骤 10 单击**下一步**，查看您输入的配置的摘要。

步骤 11 单击**应用**，保存配置数据。

VLAN 配置向导

此向导帮助配置 VLAN。每次运行此向导时，您可以在单个 VLAN 中配置端口成员关系。前几个步骤用于配置中继端口模式（在这里，配置添加标签的中继端口和未添加标签的端口），然后配置访问端口模式。

步骤 1 单击**配置向导** > **VLAN 配置向导**。

步骤 2 单击**启动向导**和**下一步**。

步骤 3 选择要配置为中继端口的端口（用鼠标在图形显示中单击所需端口）。已配置为中继端口的端口是预先选择的。

步骤 4 单击**下一步**。

步骤 5 输入以下字段：

- **VLAN ID** — 选择您想配置的 VLAN。您可以选择现有 VLAN 或**新建 VLAN**。
- **新建 VLAN ID** — 输入新建 VLAN 的 ID。
- **VLAN 名称** — 可以选择输入 VLAN 名称。

步骤 6 选择要配置为 VLAN 的未添加标签的成员的中继端口（用鼠标在图形显示中单击所需端口）。在此步骤中未选择的中继端口变成 VLAN 的已添加标签的成员。

步骤 7 单击**下一步**。

步骤 8 选择要成为 VLAN 的访问端口的端口。VLAN 的访问端口是 VLAN 的非标记成员。（用鼠标在图形显示中单击所需的端口）。

步骤 9 单击**下一步**，查看您输入的信息的摘要。

步骤 10 单击**应用**。

ACL 向导

创建新 ACL 的步骤。

步骤 1 单击**配置向导** > **ACL 向导**。

步骤 2 单击**下一步**。

步骤 3 输入以下字段：

- **ACL 名称** — 输入新 ACL 的名称。
- **ACL 类型** — 选择 ACL 的类型：**IPv4** 或 **MAC**。

步骤 4 单击**下一步**。

步骤 5 输入以下字段：

- **匹配时的操作** — 选择以下选项之一：
  - *允许流量* — 转发符合 ACL 标准的数据包。
  - *拒绝流量* — 丢弃符合 ACL 标准的数据包。
  - *关闭接口* — 丢弃符合 ACL 标准的数据包，并禁用从其接收数据包的端口。可以从错误恢复设置页面重新激活这类端口。

步骤 6 对于基于 MAC 的 ACL，填写以下字段：

- **源 MAC 地址** — 如果所有源地址均可接受，则选择*任意*；或选择*用户定义*，以输入一个源地址或输入源地址的范围。
- **源 MAC 值** — 输入要将源 MAC 地址与其相匹配的 MAC 地址及其掩码（如果相关）。
- **源 MAC 通配符掩码** — 输入掩码以定义 MAC 地址的范围。
- **目标 MAC 地址** — 如果所有目标地址均可接受，则选择*任意*；或选择*用户定义*，以输入一个目标地址或输入目标地址的范围。
- **目标 MAC 地址值** — 输入要将目标 MAC 地址与其相匹配的 MAC 地址及其掩码（如果相关）。
- **目标 MAC 通配符掩码** — 输入掩码以定义 MAC 地址的范围。请注意，此掩码与其他用途的掩码（如子网掩码）不同。在此处，将位设置为 **1** 表示不掩盖，设置为 **0** 表示掩盖该值。

注 指定一个掩码 0000 0000 0000 0000 0000 0000 1111 1111（意思是如果匹配，则该位为 0，如不匹配，则该位为 1）。您需要将有 1 的数字转换为十进制整数，而每四个 0 要写成一个 0。在此示例中，因为 1111 1111 = 255，因此该掩码将写成：0.0.0.255。

- **时间范围名称** — 如果已选中**时间范围**，请选择要使用的时间范围。时间范围已在系统时间配置一节中进行过定义。此字段仅在预先创建时间范围的情况下显示。

步骤 7 对于基于 IPv4 的 ACL，填写以下字段：

- **协议** — 选择以下其中一个选项，根据一个特定协议来创建 ACL：
  - *任意 (IP)* — 接受所有 IP 协议数据包
  - *TCP* — 接受传输控制协议数据包
  - *UDP* — 接受用户数据协议数据包
  - *ICMP* — 接受 ICMP 协议数据包
  - *IGMP* — 接受 IGMP 协议数据包
- **TCP/UDP 的源端口** — 从下拉列表选择一个端口。
- **TCP/UDP 的目标端口** — 从下拉列表选择一个端口。
- **源 IP 地址** — 如果所有源地址均可接受，则选择*任意*；或选择*用户定义*，以输入一个源地址或输入源地址的范围。
- **源 IP 值** — 输入要将源 IP 地址与其相匹配的 IP 地址。
- **源 IP 通配符掩码** — 输入掩码以定义 IP 地址的范围。请注意，此掩码与其他用途的掩码（如子网掩码）不同。在此处，将位设置为 1 表示不掩盖，设置为 0 表示掩盖该值。
- **目标 IP 地址** — 如果所有源地址均可接受，则选择*任意*；或选择*用户定义*，以输入一个源地址或输入源地址的范围。
- **目标 IP 值** — 输入要将源 IP 地址与其相匹配的 IP 地址。
- **目标 IP 通配符掩码** — 输入掩码以定义 IP 地址的范围。请注意，此掩码与其他用途的掩码（如子网掩码）不同。在此处，将位设置为 1 表示不掩盖，设置为 0 表示掩盖该值。
- **时间范围名称** — 如果已选中**时间范围**，请选择要使用的时间范围。时间范围已在系统时间配置一节中进行过定义。此字段仅在预先创建时间范围的情况下显示。

步骤 8 单击**下一步**。

步骤 9 确认您要创建 ACL 和 ACE。

显示 ACL 规则的详细信息。您可以单击**向此 ACL 添加一个规则**，添加一个规则。

步骤 10 单击**下一步**，输入 ACL 绑定信息：

- **绑定类型** — 选择以下其中一个选项来绑定 ACL：
  - *仅物理接口* — 将 ACL 绑定到端口。在此情况下，单击与 ACL 绑定的一个或多个端口。
  - *仅 VLAN* — 将 ACL 绑定到 VLAN。在**输入要与 ACL 绑定的 VLAN 的列表**字段中输入 VLAN 列表。
  - *无绑定* — 不绑定 ACL。

单击**应用**。

5

状态和统计信息

本节介绍如何查看设备统计信息。

其中包含以下主题：

- 系统摘要
- CPU 使用率
- 接口
- Etherlike
- 端口使用率
- GVRP
- 802.1X EAP
- ACL
- 硬件资源使用率
- 运行状况和电源
- 交换端口分析器（SPAN）
- 诊断
- RMON
- 查看日志

系统摘要

“系统摘要”页面提供了设备的图形视图，并显示设备状态、硬件信息、固件版本信息、一般 PoE（以太网供电）状态以及其他项目。

若要查看系统信息，请单击**状态和统计信息** > **系统摘要**。

系统信息：

- **系统说明** — 系统的说明。
- **系统位置** — 设备的实际位置。单击**编辑**可前往系统设置页面输入该值。
- **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该值。
- **主机名** — 设备的名称。单击**编辑**可前往系统设置页面输入该值。默认情况下，设备主机名由单词 *switch* 与设备 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。
- **系统对象 ID** — 实体（在 SNMP 中使用）中包含的网络管理子系统的唯一供应商标识。
- **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** — 设备 MAC 地址。
- **巨型帧** — 巨型帧支持状态。可以使用端口设置启用或禁用该支持。

  注 巨型帧支持仅在启用且重启设备之后才会生效。

软件信息：

- **固件版本**— 活动映像的固件版本号。
- **固件 MD5 校验和**— 活动映像的 MD5 校验和。

  注 以下三个字段可显示两次，每次针对设备上的一种语言。
- **区域设置** — 第一语言的区域设置。（第一语言始终是英文。）
- **语言版本** — 第一语言或英语的语言包版本。
- **语言 MD5 校验和** — 语言文件的 MD5 校验和。

TCP/UDP 服务状态：

要重置以下字段，请单击**编辑**，打开 TCP/UDP 服务页面。

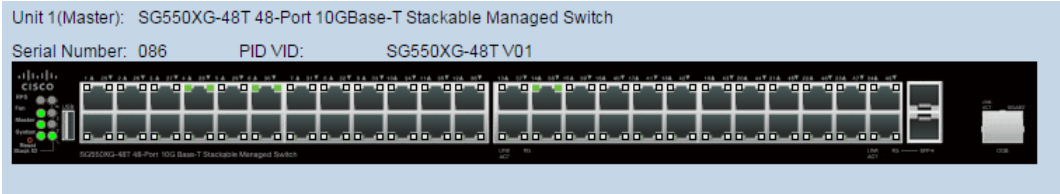
- **HTTP 服务** — 显示 HTTP 服务是处于启用状态还是禁用状态。
- **HTTPS 服务** — 显示 HTTPS 服务是处于启用状态还是禁用状态。
- **SNMP 服务** — 显示 SNMP 服务是处于启用状态还是禁用状态。

- **Telnet 服务** — 显示 Telnet 服务是处于启用状态还是禁用状态。
- **SSH 服务** — 显示 SSH 服务是处于启用状态还是禁用状态。

主单元的：（在支持 PoE 的设备上）

- **PoE 电源信息**— 单击**详情**，您可直接转至 PoE 属性页面。此页面按单元显示。
- **最大可用 PoE 功率 (W)** — 交换机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。

单元会以图表形式显示，如下所示：



将光标悬停在端口上可显示其名称。

系统将显示设备的以下信息：

- **序列号** — 序列号。
- **PID VID** — 部件编号和版本 ID。

CPU 使用率

除处理管理接口的终端用户流量之外，设备 CPU 还处理以下类型的流量：

- 管理流量
- 协议流量
- 侦听流量

过多的流量会使 CPU 不堪重负，并可能影响正常的设备运行。设备使用安全的核心技术 (SCT) 功能，可以确保设备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（安全核心技术）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 使用率的步骤：

步骤 1 单击**状态和统计信息 > CPU 使用率**。

CPU 输入速率字段将显示每秒向 CPU 输入帧的速率。

该窗口包含一个图表，显示设备上的 CPU 使用率。Y 轴表示占用百分比，X 轴为样本号。

步骤 2 确保 **CPU 使用率**复选框处于启用状态。

步骤 3 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。

系统会显示一个包含设备 CPU 使用率图表的窗口。

接口

“接口”页面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**。

步骤 2 输入参数。

- **接口** — 选择要显示以太网统计信息的接口。
- **刷新速率** — 选择刷新接口以太网统计信息的间隔时间。

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。

步骤 3 在表视图或图形视图中查看统计信息计数器的步骤：

- 单击**查看所有接口统计信息**，在表视图中查看所有端口。
- 单击**查看接口历史记录图表**，以图形形式显示这些结果。在该视图中，您可以选择显示结果的**时限**以及要显示的统计信息类型。例如，如果选择**过去 5 分钟**和**单播数据包数**，系统将显示过去 5 分钟内接收的单播数据包数量。

Etherlike

Etherlike 页面根据 Etherlike MIB（管理信息库）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。该页面提供有关物理层（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**。

步骤 2 输入参数。

- **接口** — 选择要显示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。

系统会针对选定接口显示以下字段。

注 如果以下其中一个字段显示一些错误（不是 0），则显示**上次更新**时间。

- **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。
- **单个冲突帧数** — 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。
- **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。此字段仅支持 XG 端口。当端口速度为 1G 时，接收的暂停帧计数器不运行。
- **已发送的暂停帧数** — 从选定接口传输的流控制暂停帧数。

步骤 3 如要在表视图中查看统计信息计数器，请单击**查看所有接口统计信息**，在表视图中查看所有端口。

端口使用率

“端口使用率”页面显示每端口的带宽（传入和传出）使用情况。

显示端口使用率的步骤：

步骤 1 单击**状态和统计信息** > **端口使用率**。

步骤 2 输入**刷新速率**，即刷新接口以太网统计信息的间隔时间。

将为每个端口显示以下字段：

- **接口** — 端口名称。
- **Tx 使用率** — 传出数据包使用的带宽数量。
- **Rx 使用率** — 传入数据包使用的带宽数量。

选择一个端口并单击**查看接口历史记录图表**，可查看端口上一段时间内的历史使用率图表。除上述字段以外，还显示以下字段：

- **时限** — 选择时间单位。图表用此时间单位显示端口使用率。

GVRP

GVRP 页面会显示关于从某个端口发送或接收的 GARP VLAN 注册协议 (GVRP) 帧的信息。GVRP 是一种基于标准的第 2 层网络协议，用于在交换机上自动配置 VLAN 信息。它是在对 802.1Q-2005 的 802.1ak 修订中定义的。

仅当在全局和某端口上启用了 GVRP 时，才会显示该端口的 GVRP 统计信息。请参阅 GVRP 设置页。

查看 GVRP 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** > **GVRP**。

步骤 2 输入参数。

- **接口** — 选择要显示 GVRP 统计信息的具体接口。
- **刷新速率** — 选择刷新 GVRP 页面的间隔时间。

属性计数器块显示每个接口的各种类型数据包的计数器。为**已接收**和**已传输**数据包显示这些信息。

- **Join Empty** — 接收/传输的 GVRP Join Empty 数据包。
- **Empty** — 接收/传输的 GVRP Empty 数据包。
- **Leave Empty** — 接收/传输的 GVRP Leave Empty 数据包。
- **Join In** — 接收/传输的 GVRP Join In 数据包。
- **Leave In** — 接收/传输的 GVRP Leave In 数据包。
- **Leave All** — 接收/传输的 GVRP Leave All 数据包。

GVRP 错误统计信息部分显示 GVRP 错误计数器。

- **无效协议 ID** — 无效协议 ID 错误数。
- **无效属性类型** — 无效属性 ID 错误数。
- **无效属性值** — 无效属性值错误数。
- **无效属性长度** — 无效属性长度错误数。
- **无效事件** — 无效事件数。

步骤 3 要清除统计信息计数器，请单击**查看所有接口统计信息**，在单个页面中查看所有端口。

802.1X EAP

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（“安全”>“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**。

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**刷新速率**（间隔时间）。

系统会针对选定接口显示以下值。

- **已接收的 EAPOL EAP 帧数** — 在端口上接收的有效 EAPOL帧数。
- **已接收的 EAPOL 开始帧数** — 在端口上接收的 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 EAPOL 通告帧数** — 在端口上接收的 EAPOL 通告帧数。
- **已接收的 EAPOL 通告请求帧数** — 在端口上接收的 EAPOL 通告请求帧数。
- **已接收的 EAPOL 无效帧数** — 在端口上接收的 EAPOL 无效帧数。
- **已接收的 EAPOL 长度错误帧数** — 在此端口上接收的具有无效数据包正文长度的 EAPOL 帧数。
- **已接收的具有未识别 CKN 的 MKPDU 帧数** — 此端口上接收的具有未识别 CKN 的 EAP 帧数。
- **已接收的 MKPDU 无效帧数** — 在该端口上接收的 MKPDU 无效帧数。
- **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。
- **已发送的 EAPOL EAP 请求方帧数** — 在该端口上传输的 EAPOL EAP 请求方帧数。
- **已发送的 EAPOL 开始帧数** — 在该端口上传输的 EAPOL 开始帧数。
- **已发送的 EAPOL 注销帧数** — 在该端口上传输的 EAPOL 注销帧数。
- **已发送的 EAPOL 通告帧数** — 在该端口上传输的 EAPOL 通告帧数。
- **已发送的 EAPOL 通告请求帧数** — 在该端口上传输的 EAPOL 通告请求帧数。

- **已发送的 EAPOL EAP 验证方帧数** — 在该端口上传输的 EAP 验证方帧数。
- **已发送的没有 CKN 的 MKA 帧数** — 此端口上接收的没有 CKN 的 EAP 帧数。

步骤 4 清除统计信息计数器的步骤：

- 单击**查看所有接口统计信息**，查看所接口的计数器。
- 单击**清除接口计数器**，清除所有接口的计数器。

ACL

启用 ACL 记录功能时，系统会为与 ACL 规则匹配的数据包生成系统日志通知消息。

查看基于 ACL 转发或拒绝数据包的接口的步骤：

步骤 1 单击**状态和统计信息** > **ACL**。

步骤 2 选择**刷新速率**，即刷新页面的时间间隔（以秒为单位的时间段）。为每个时间段创建一组新接口。

系统将显示以下信息：

- **已生成全局陷阱的数据包计数器** — 由于缺少资源已生成全局陷阱的数据包数量。
- **拦截的数据包 — 基于端口/LAG** — 基于 ACL 规则转发或拒绝数据包的接口。
- **拦截的数据包 — 基于 VLAN** — 基于 ACL 规则转发或拒绝数据包的 VLAN。

步骤 3 要管理统计信息计数器，请单击**清除计数器**，以清除所有接口的计数器。

硬件资源使用率

此页显示系统使用的资源，例如 ACL（访问控制列表）和服务质量 (QoS)。

有的应用一开始就分配规则。此外，在系统启动期间初始化的流程会在启动过程中使用它们的一些规则。

要查看硬件资源使用率，请单击**状态和统计信息** > **硬件资源使用率**。

系统将显示以下字段：

- **ACL 和 QoS 规则**
  - *使用中* — 用于 ACL 和 QoS 规则的 TCAM 条目数。
  - *最大数* — 可用于 ACL 和 QoS 规则的可用 TCAM 条目数。

要查看如何更改各种流程间的分配，请参阅硬件资源一节。

运行状况和电源

运行状况和电源页面监控所有相关设备上的温度状态、电源状态和风扇状态。根据型号，设备上可能有一个或多个风扇。某些型号根本没有风扇。

风扇

在某些设备中，设备运行期间必须使用风扇，因为如果没有风扇，设备会变得过热并自动关闭。风扇是一种运转部件，因此有可能会发生故障。系统上安装了冗余风扇。此风扇仅在一个或多个系统风扇发生故障时才会运转。在这种情况下，冗余风扇将成为设备环境监控的一部分。

建议每天让冗余风扇运转至少 1 分钟。

某些设备具有温度传感器，可在过热时保护其硬件。在此情况下，设备在过热时以及过热后的冷却期间会执行以下操作：

事件	操作
至少有一个温度传感器超出“警告”阈值	会生成以下信息： • 系统日志消息 • SNMP 陷阱

事件	操作
至少有一个温度传感器超出“临界”阈值	会生成以下信息： • 系统日志消息 • SNMP 陷阱 将执行以下操作： • 系统 LED 设置为琥珀色常亮（如果硬件支持）。 • 禁用端口 — 超出“临界”温度两分钟时，系统将关闭所有端口。 • （在支持 PoE 的设备上）禁用 PoE 电路，以降低功耗和释放的热量。
超出“临界”阈值后的冷却期（所有传感器都比“警告”阈值至少低 2°C）。	所有传感器均冷却到比“警告”阈值至少低 2°C 后，将重新启用 PHY（端口物理层），且所有端口也将重新开启。 如果风扇状态为“正常”，端口将启用。 （在支持 PoE 的设备上）PoE 电路将启用。

“运行状况和电源”字段

要查看设备运行状况参数，请单击**状态和统计信息** > **运行状况和电源**。

注 仅显示适用于设备的字段。

本部分显示设备通过绿色以太网和 LED 禁用功能以及关闭端口（关闭开关或通过时间范围设置）节省的电量。

“PoE 节能”显示使用 PoE 时间范围功能节省的总电量，该功能可在特定时间（通常在 PoE 网络元素未使用时）关闭为端口供电的 PoE。

系统将显示以下信息（字段的顺序可能因设备而异）：

环保效益

- **风扇状态** — 可能的值如下所示：
  - *正常* — 风扇运转正常。
  - *故障* — 风扇无法正常运转。
  - *无* — 风扇 ID 不适用于特定型号。

- **传感器状态** — 可能的值如下所示：
  - *正常* — 传感器运转正常。
  - *故障* — 传感器无法正常运转。
  - *无* — 传感器 ID 不适用于特定型号。
- **温度** — 选项包括：
  - *正常* — 温度低于警告阈值。
  - *警告* — 温度介于警告阈值与临界阈值之间。
  - *临界* — 温度高于临界阈值。
  - *无* — 不相关。
- **主电源状态** — 为主电源显示以下字段之一：
  - *活动* — 电源正在使用。
  - *故障* — 主电源发生故障。

节能

- **绿色以太网和端口当前节省的电量** — 自设备通电以来，所有端口上截至目前节省的电量。
- **绿色以太网和端口累计节省的电量** — 当前在所有端口上累计节省的电量。
- **预计绿色以太网和端口每年节省的电量** — 根据设备在一周内节省的电量预计一年将节省的电量。此值根据设备在过去一周内节省的电量计算。
- **当前节省的 PoE 电量** — 在连接了 PD（受电设备）的端口上和在因时间范围功能而未运行 PoE 的端口上，当前节省的 PoE 电量。
- **累计节省的 PoE 电量** — 自设备通电以来，在连接了 PD 的端口上和在因时间范围功能而未运行 PoE 的端口上，累计节省的 PoE 电量。
- **预计每年节省的 PoE 电量** — 自设备通电以来，在连接了 PD 的端口上和在因时间范围功能而未运行 PoE 的端口上，预计每年节省的 PoE 电量。此预估值根据设备在过去一周内节省的电量计算。

以太网供电表（仅在设备支持 PD 端口时显示）。系统将显示以下字段：

- **端口名称** — 端口号。
- **PD 状态** — 显示以下值之一：
  - *已连接* — PD 端口已连接供电的 PSE 设备。
  - *未连接* — PD 端口未连接 PSE 设备。
- **协商模式** — 以下值之一。
  - *自动* — 使用 CDP（思科发现协议）和 LLDP（链路层发现协议）协商确定电源等级。
  - *强制 802.3AF* — 两端均使用 AF 电源标准。
  - *强制 802.3AT* — 两端均使用 AT 电源标准。
  - *强制 60W* — 两端均使用 60W 电源。
- **功率预算** — 实际分配给端口的电量。

交换端口分析器（SPAN）

SPAN 功能有时称作“端口镜像或端口监控”，选择网络流量供网络分析器分析。网络分析器可以是思科 SwitchProbe 设备，也可以是其他远程监视 (RMON) 探测。

在网络设备上，可使用端口镜像将单个设备端口、多个设备端口或整个 VLAN 上看到的网络数据包的副本发送到设备上另一端口上的网络监控连接。它经常用于需要进行网络流量监控的设备（例如入侵检测系统）。连接到监控端口的网络分析器负责处理数据包。

对于每个会话，设备最多可以镜像四个接口。

在网络端口上收到的分配给要进行镜像的 VLAN 的数据包将镜像到分析器端口，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”，将会镜像由设备发送的数据包。

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。

SPAN 会话目的

监控会话由一个或多个源端口以及单个目标端口组成。

添加目标端口的步骤：

步骤 1 单击**状态和统计信息** > **SPAN** > **会话目的**。

此时将显示以前定义的目标。

步骤 2 单击**添加**。

步骤 3 输入以下字段：

- **会话 ID** — 选择会话 ID。它必须与源端口的会话 ID 相匹配。
- **端口** — 选择要将流量复制到的端口号。

  此处是分析器端口。系统会将网络分析器（例如运行 Wireshark 的 PC）连接到此端口。
- **网络流量** — 选择该选项将允许受监控流量以外的流量在该端口上通过。

步骤 4 单击**应用**。

SPAN 会话源

必须在设备上配置一个或多个 SPAN 源。

配置要镜像的源端口的步骤：

步骤 1 单击**状态和统计信息** > **SPAN** > **会话源**。

步骤 2 单击**添加**。

步骤 3 从**会话 ID** 中选择会话编号。该编号对于所有源端口和目标端口必须相同。

步骤 4 选择从中将流量发送到分析器端口的端口或 VLAN（**源接口**）。

步骤 5 在**监控类型**字段中，选择是镜像传入流量还是传出流量，还是同时镜像这两种流量。

- *接收和发送* — 对传入和传出数据包均进行端口镜像。
- *Rx* — 对传入数据包进行端口镜像。
- *Tx* — 对传出数据包进行端口镜像。

步骤 6 单击**应用**。配置用于镜像的源接口。

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。

其中包含以下主题：

- 铜缆端口测试
- 光纤模块状态
- 技术支持信息

铜缆端口测试

“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（虚拟电缆测试器）执行两种测试：

- 时域反射计 (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”页面中的“测试结果”框中显示。
- 可对活动的 XG 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”页面中的“高级信息”框中显示。此测试仅在链路速度为 10G 时运行。

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：

- （必需）禁用短距模式（请参见属性页面）
- （可选）禁用 EEE（请参阅属性页面）

使用 VCT 测试电缆时，会使用一条 CAT6a 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**状态和统计信息** > **诊断** > **铜缆测试**。

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。

高级信息版块包括以下信息，这些信息会在您每次进入页面时刷新：

- **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。

光纤模块状态

“光纤模块状态”页面会显示由 SFP（小型封装热插拔）收发器报告的工作状况。

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。

支持以下 XG SFP+ (10,000 Mbps) 收发器：

- 思科 SFP-10GSR
- 思科 SFP-10GLRM
- 思科 SFP-10GLR

支持以下 XG 无源电缆 (Twinax/DAC)：

- 思科 SFP-H10GCU1m
- 思科 SFP-H10GCU3m
- 思科 SFP-H10GCU5m

要查看光纤测试的结果，请单击**状态和统计信息** > **诊断** > **光纤模块状态**。

此页面显示了以下字段：

- **端口** — 连接 SFP 的端口的端口号。
- **说明** — 光纤收发器的说明。

- **序列号** — 光纤收发器的序列号。
- **PID** — VLAN ID。
- **VID** — 光纤收发器的 ID。
- **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 正在工作。值为 True 和 False。

技术支持信息

该页提供详细的设备状态日志。这在技术支持人员尝试帮助用户解决问题时非常有用，因为它可以在一个命令中提供许多显示命令（包括调试命令）的输出。

查看用于调试的重要技术支持信息的步骤：

步骤 1 单击**状态和统计信息** > **诊断** > **技术支持信息**。

步骤 2 单击**生成**。

显示来自工作**显示** CLI 命令的信息。

注 从此命令生成输出可能需要一些时间。生成信息后，您可以单击**选择技术支持数据**从屏幕上的文本框复制信息。

RMON

RMON（远程网络监控）使设备中的 SNMP 代理能够在指定时间段内前瞻性地监控流量统计信息并向 SNMP 管理器发送陷阱。本地 SNMP 代理比较实际的实时计数器与预定义阈值并生成警报，而不需要中央 SNMP 管理平台进行轮询。如果用户设置了相对于网络基线的正确阈值，那么这会是一种有效的前瞻性管理机制。

RMON 会降低管理器与设备之间的流量，因为 SNMP 管理器不必频繁地轮询设备来获得信息；而且能使管理器及时地获得状态报告，因为设备会在事件发生时进行报告。

有了这一功能，您可以执行以下操作：

- 查看当前的统计信息（从计数器值被清除的时间起）。您还可以收集这些计数器在一段时间内的值，然后查看列出所收集数据的表格，其中每个收集的数据集都是*历史*选项卡里的一行。
- 对计数器值定义有意义的更改，例如“滞后冲突达到一定数量”（定义警报），然后指定发生该事件后执行什么操作（记录日志、发送陷阱或记录日志并发送陷阱）。

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。
- 尚未检测接收 (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**。

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。

系统会针对选定接口显示以下统计信息。

注 如果以下其中一个字段显示一些错误（不是 0），则显示**上次更新**时间。

- **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。
- **已接收的数据包** — 接收的正常数据包，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。
- **分片数** — 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）或具有非整数数量八位字节（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。
  - 尚未检测接收 (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** — 发送或接收的包含 64 字节的帧数。
- **65 至 127 字节的帧数** — 发送或接收的包含 65-127 字节的帧数。
- **128 至 255 字节的帧数** — 发送或接收的包含 128-255 字节的帧数。
- **256 至 511 字节的帧数** — 发送或接收的包含 256-511 字节的帧数。
- **512 至 1023 字节的帧数** — 发送或接收的包含 512-1023 字节的帧数。
- **超过 1024 字节的帧数** — 发送或接收的包含 1024 - 2000 字节的帧和巨型帧的数量。

步骤 4 在表视图或图形视图中查看计数器的步骤：

- 单击**查看所有接口统计信息**，在表视图中查看所有端口。
- 单击**图形视图**，以图形形式显示这些结果。在该视图中，您可以选择显示结果的**时限**以及要显示的统计信息类型。

RMON 历史

RMON 功能可以监控每个接口的统计信息。

“历史记录”页面可定义取样频率、要存储的样本数量以及要从中收集数据的端口。

数据经过取样和存储后，将显示在“历史表”页面中，可通过单击**历史表**进行查看。

输入 RMON 控制信息的步骤：

步骤 1 单击**状态和统计信息** > **RMON** > **历史**。此页面上显示的字段在下面的“添加 RMON 历史”页面中定义。在此页面中定义而不在“添加”页面中定义的唯一一个字段就是：

- **当前的样本数** — 标准允许 RMON 不授予所有请求的样本，而是限制每个请求的样本数。因此，该字段表示实际授予请求的样本数，等于或小于请求的值。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **新历史条目** — 显示新的历史表条目的数量。
- **源接口** — 选择从中捕获历史记录样本的接口类型。
- **保存的最大样本数** — 输入要存储的样本数。
- **取样间隔** — 输入以秒表示的从端口收集样本的时间间隔。该字段的取值范围是 1-3600。
- **所有者** — 输入请求 RMON 信息的 RMON 站或用户。

步骤 4 单击**应用**。条目将添加到“历史控制表”页面中，然后当前配置文件会更新。

步骤 5 单击**历史表**（如下所述）查看实际统计信息。

RMON 历史表

“历史”页面显示特定于接口的统计性网络样本。这些样本在上述历史控制表中配置。

查看 RMON 历史统计信息的步骤：

步骤 1 单击**状态和统计信息** > **RMON** > **历史**。

步骤 2 单击**历史表**。

步骤 3 从**历史条目编号**下拉菜单中，选择要显示的样本条目数（可选）。

系统会针对选定样本显示以下字段。

- **所有者** — 历史记录表条目所有者。
- **样本编号** — 从该样本中抽取的统计信息。
- **丢弃事件** — 在取样间隔中由于缺少网络资源而丢弃的数据包数。它可能不表示丢弃数据包的精确数量，而表示检测到丢弃数据包的次数。
- **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。
- **已接收的数据包数** — 接收的数据包数，包括坏数据包、组播数据包和广播数据包。
- **广播数据包数** — 正常广播数据包数（不包括组播数据包）。
- **组播数据包数** — 接收到的正常组播数据包数。
- **CRC 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。
- **分片数** — 接收的片段（小于 64 八位字节的数据包）数，不包括帧位，但包括 FCS 八位字节。
- **超时发送帧数** — 接收的大于 2000 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）或具有非整数数量八位字节（校正误差）的坏 FCS 的 FCS 八位字节数。
- **冲突数** — 接收的冲突数。
- **使用率** — 当前接口流量相对于该接口可以处理的最大流量的百分比。

RMON 事件控制

您可以控制触发警报情况的发生和出现的通知类型。此执行过程如下所示：

- **事件页面** — 配置触发警报时发生的事件。可以是日志和陷阱的任意组合。
- **警报页面** — 配置触发警报的情况。

定义 RMON 事件的步骤：

步骤 1 单击**状态和统计信息 > RMON > 事件**。

该页面显示以前定义的事件。

此页面上的字段通过“添加 RMON 事件”对话框定义，但“时间”字段除外。

- **时间** — 显示事件发生的时间。（这是位于父窗口的只读表，不能对其进行定义）。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **事件条目** — 显示新条目的事件条目索引号。
- **社区** — 输入在发送陷阱时要包括的 SNMP 社区字符串（可选）。请注意，必须使用通知接收设备页面定义社区，以便陷阱到达网络管理站。
- **说明** — 为该事件输入名称。该名称将用于在**添加 RMON 警报**页面中为事件附加警报。
- **通知类型** — 选择此事件将引发的操作的类型。可选择以下值：
  - *无* — 警报消失时不执行操作。
  - *日志（事件日志表）* — 触发警报时向事件日志表添加一条日志条目。
  - *陷阱（SNMP 管理器和系统日志服务器）* — 警报消失时向远程日志服务器发送陷阱。
  - *日志和陷阱* — 警报消失时向事件日志表添加一条日志条目并向远程日志服务器发送陷阱。
- **所有者** — 输入定义该事件的设备或用户。

步骤 4 单击**应用**。RMON 事件将保存至当前配置文件中。

步骤 5 单击**事件日志表**，显示已经出现和已经记录的警报日志（请参阅下面的说明）。

RMON 事件日志

“事件”页面显示发生的事件（操作）的日志。可记录两种事件：*日志*或*日志和陷阱*。当将事件与警报（请参阅 RMON 警报页面）绑定，并达到了警报的条件时，将会执行事件中的操作。

步骤 1 单击**状态和统计信息 > RMON > 事件**。

步骤 2 单击**事件日志表**。

您可以在过滤器中选择接口，以查看特定接口上发生的事件。

此页面显示了以下字段：

- **事件条目编号** — 事件的日志条目编号。
- **日志编号** —（事件中的）日志编号。
- **日志时间** — 输入该日志条目的时间。
- **说明** — 触发警报的事件说明。

RMON 警报

RMON 警报提供了一种机制，可用于设置阈值和取样间隔，以在计数器或代理维护的任何其他 SNMP 对象计数器上生成异常事件。警报中必须配置上限阈值与下限阈值。超过上限阈值后，不会再生成上升事件，直到超过了伴随的下限阈值。发出下降警报后，系统会在超过上限阈值时发出下一个警报。

一个或多个警报绑定至事件，表明警报发生时会采取的措施。

可以通过绝对值或计数器值中的变化（差值）来监控警报计数器。

输入 RMON 警报的步骤：

步骤 1 单击**状态和统计信息 > RMON > 警报**。

此时系统会显示以前定义的所有警报。字段将在下面的“添加 RMON 警报”页面中进行说明。除这些字段之外，系统还会显示以下字段：

- **计数器值** — 显示最近一次取样周期中的统计信息值。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **警报条目** — 显示警报条目编号。
- **接口** — 选择要显示其 RMON 统计信息的接口的类型。
- **计数器名称** — 选择指示衡量事件类型的 MIB 变量。

- **样本类型** — 选择用于生成警报的取样方法。选项如下：
  - *绝对值* — 如果超过了阈值，则生成警报。
  - *差值* — 从当前值中减去上次取样的值，系统会将差值与阈值进行比较。如果超过了阈值，则生成警报。
- **上限阈值** — 输入触发上限阈值警报的值。
- **上升事件** — 选择触发上升事件时要执行的事件。事件将在 RMON 事件控制页面中配置。
- **下限阈值** — 输入触发下限阈值警报的值。
- **下降事件** — 选择触发下降事件时要执行的事件。
- **启动警报** — 选择启动警报生成的第一个事件。上升被定义为从低阈值向较高阈值变化的行为。
  - *上升警报* — 上升值触发上限阈值警报。
  - *下降警报* — 下降值触发下限阈值警报。
  - *上升和下降* — 上升值和下降值都触发该警报。
- **间隔** — 输入以秒表示的警报间隔。
- **所有者** — 输入接收该警报的用户或网络管理系统的名称。

步骤 4 单击**应用**。RMON 警报将保存至当前配置文件中。

查看日志

设备可以写入以下日志：

- 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

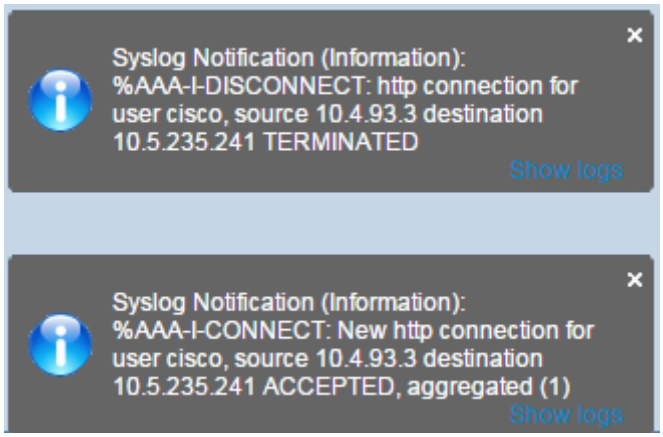
“RAM 内存”页面会按时间先后顺序显示保存到 RAM（缓存）中的所有消息。系统会根据日志设置页面中的配置将这些条目存储到 RAM 日志中。

弹出系统日志通知

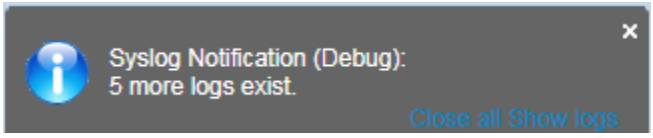
向 RAM 日志文件写入新的系统日志消息时，Web GUI 中会出现一个显示其内容的通知。

Web GUI 将每隔 10 秒轮询一次 RAM 日志。在过去 10 秒中创建的所有系统日志的弹出通知将出现在屏幕右下方。

系统会显示弹出通知如下所示：



如果显示七个以上的弹出通知，将显示一个弹出摘要。此弹出摘要将说明有多少系统日志通知没有显示。它还包含一个按钮，可用来关闭所有显示的弹出通知，如下所示：



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

以下信息显示在页面顶部：

- **警告图标闪烁** — 在禁用和启用之间切换。
- **弹出系统日志通知** — 如上文所述，启用即可接收弹出系统日志。
- **当前日志记录阈值** — 指定生成的日志记录等级。您可以通过单击字段名称旁边的**编辑**进行更改。

此页面包含每个日志文件的以下字段：

- **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。设备重启时，闪存日志会保留。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**。

当前记录阈值用于指定所生成的记录等级。您可以通过单击字段名称旁边的**编辑**进行更改。

此页面包含每个日志文件的以下字段：

- **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。

6

管理

本节介绍如何在设备上查看系统信息和配置各种选项。

其中包含以下主题：

- 系统设置
- 用户帐户
- 空闲会话超时
- 时间设置
- 系统日志
- 文件管理
- 即插即用 (PNP)
- 重启
- 发现协议 - Bonjour
- 发现协议 - LLDP
- 发现协议 - CDP
- 定位设备
- Ping
- Traceroute

系统设置

输入系统设置的步骤：

步骤 1 单击**管理** > **系统设置**。

步骤 2 查看或修改系统设置。

- **系统说明** — 显示设备说明。
- **系统位置** — 输入设备的物理位置。
- **系统联系人** — 输入联系人姓名。
- **主机名** — 选择此设备的主机名。系统会在 CLI 命令的提示符中使用此主机名：
  - *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 代表设备 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）。
- **自定义横幅设置** — 可设置以下横幅：
  - *登录横幅* — 输入登录前显示在“登录”页面上的文本。单击**预览**查看结果。
  - *欢迎横幅* — 输入登录后显示在“登录”页面上的文本。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（控制台、Telnet 和 SSH）激活该横幅。

  该横幅最多可以包含 1000 个字符。在 510 个字符后，按 <Enter> 以继续。

步骤 3 单击**应用**，在当前配置文件中保存这些值。

用户帐户

使用“用户帐户”页面可添加有权访问设备（只读或读写）的用户，或更改现有用户的密码。

添加 15 级用户后（如下所述），默认用户将从系统中移除。

注 有关密码恢复的信息，请参阅菜单 CLI 和密码恢复。

添加新用户的步骤：

步骤 1 单击**管理** > **用户帐户**。

此页面显示系统中定义的用户及其用户权限等级。

步骤 2 单击**添加**以添加新用户，或单击**编辑**以修改用户。

步骤 3 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，则用户密码必须与密码强度中配置的策略相符。
- **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。
- **用户等级** — 选择添加/编辑的用户权限级别。
  - *只读 CLI 访问 (1)* — 用户不能访问 GUI，只能访问不会更改设备配置的 CLI 命令。
  - *读/受限写入 CLI 访问 (7)* — 用户不能访问 GUI，只能访问某些可以更改设备配置的 CLI 命令。有关详情，请参阅 *CLI 参考指南*。
  - *读/写管理访问 (15)* — 用户能够访问 GUI，并配置设备。

步骤 4 单击**应用**。用户将添加到设备的当前配置文件中。

空闲会话超时

空闲会话超时可配置管理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以下会话之一：

- HTTP 会话超时
- HTTPS 会话超时
- Telnet 会话超时
- SSH 会话超时

设置各种会话的空闲会话超时的步骤：

步骤 1 单击**管理** > **空闲会话超时**。

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

步骤 3 单击**应用**，在设备上设置这些配置设置。

时间设置

请参阅管理：时间设置。

系统日志

本节介绍系统记录功能。通过此功能，设备可以生成多个独立的日志。每个日志是一组描述系统事件的消息。

设备可生成以下本地日志：

- 将日志发送至控制台接口。
- 写入到 RAM 中的记录事件循环列表中的日志，重启设备会将其擦除。
- 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 SNMP 陷阱和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。

本部分包含以下小节：

- 日志设置
- 远程记录设置

日志设置

可以按严重性级别选择要记录的事件。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*仅供参考*。

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。
- 参考 — 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。这些日志会分别显示在 RAM 内存页面和闪存页面中。

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“注意”、“参考”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**。

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陷阱汇总。如果启用了此选项，系统会汇总最大聚合时间内的相同和相邻的系统日志消息及陷阱，并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。
- **发起人标识符** — 可将发起人标识符添加到系统日志消息。选项如下：
  - *无* — 系统日志消息中不包含发起人标识符。
  - *主机名* — 系统日志消息中包含系统主机名。
  - *IPv4 地址* — 系统日志消息中包含发送接口的 IPv4 地址。

- *IPv6 地址* — 系统日志消息中包含发送接口的 IPv6 地址。
- *用户定义* — 输入一个说明，并将其包含在系统日志消息中。

- **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。
- 单击**应用**。将更新当前配置文件。

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**。

步骤 2 输入以下字段：

- **IPv4 源接口** — 选择其 IPv4 地址将在发送给系统日志服务器的系统日志消息中用作 IPv4 地址的源接口。
- **IPv6 源接口** — 选择其 IPv6 地址将在发送给系统日志服务器的系统日志消息中用作 IPv6 地址的源接口。

  注 如果已选择“自动”选项，系统将使用传出接口上定义的 IP 地址的源 IP 地址。

系统将显示之前配置的每个日志服务器的信息。字段将在下面的**添加**页面中进行说明。

步骤 3 单击**添加**。

步骤 4 输入参数。

- **服务器定义** — 选择是按照 IP 地址还是按照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::/10，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 5 单击**应用**。系统将会关闭“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。

文件管理

请参阅管理：文件管理。

即插即用 (PNP)

如果以手动方式安装新网络设备或更换网络设备，那么可能会成本高昂贵、耗时，且容易出错。通常，新设备会先被送往中央试运行设施，设备在那里会被拆箱，连接试运行网络，更新合适的许可证、配置和映像；然后再装箱并运往实际安装位置。完成这些过程后，专家必须前往安装位置执行安装。由于设备数量众多，即便设备的实际安装位置就在 NOC/数据中心，提供安装支持的专家仍然可能人手不足。所有这些问题都会造成部署延迟，并增加运营成本。

思科即插即用 (PNP) 解决方案可降低与网络设备部署/安装相关的成本、提高安装速度并降低部署复杂性，同时不会影响安全性。利用思科即插即用解决方案，您可以在各种部署场景和部署位置执行交换机零接触安装。

PNP 设置

配置 PNP 设置的步骤：

注 默认情况下，此功能为禁用状态。

步骤 1 单击**管理 > PNP > PNP 设置**。

步骤 2 通过在以下字段中输入信息来配置 PNP：

- **PNP 状态** — 默认情况下处于启用状态。

PNP 传输 — 定义 PNP 代理会话信息和参数。

- **设置定义** — 选择以下选择之一来指定配置信息，也就是指定要使用的传输协议、PNP 服务器地址，以及要使用的 TCP 端口：
  - *默认设置* — 如果选择该选项，系统会从 DHCP 选项 43 提取 PNP 设置。如果系统未能从 DHCP 选项 43 接受到完整或部分设置，将会使用以下默认值：默认传输协议“HTTP”，PNP 服务器的 DNS 名称“pnpserver”，以及与 HTTP 相关的端口。

    选择**默认设置**选项后，**PNP 传输**部分的所有字段会变成灰色。
  - *手动设置* — 手动设置用于 PNP 传输的 TCP 端口和服务器设置。
- **TCP 端口** — TCP 端口号。该编号由系统自动输入：HTTP 对应的编号为 80。
- **服务器定义** — 选择是**按 IP 地址**还是**按名称**来指定 PNP 服务器。
- **IP 版本** — 选择支持的 IP 格式。
- **服务器 IPv6 地址类型** — 如果 IP 版本类型为 IPv6，则选择以下选项之一：
  - *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 源地址类型为“链路本地”，请选择接收的来源。
- **服务器 IP 地址/名称** — 输入 PNP 服务器的 IP 地址或域名。

PNP 用户

- **用户定义** — 要发送给 PNP 数据包，然后发送至 PNP 服务器的用户信息。请选择以下其中一个选项：
  - *默认值* — 如果选择该选项，系统会从 DHCP 选项 43 提取用户名和密码。如果选择该选项，用户名和密码字段会变成灰色。
  - *手动设置* — 选择该选项以手动配置 PNP 用户名和密码。
- **用户名** — 在 PNP 数据包中输入的用户名。
- **密码** — **加密模式**或**明文模式**的密码。

PNP 行为设置 — 输入以下参数：

- **重新连接间隔** — 断开连接后，系统等待多少秒后尝试重新连接会话。
- **发现超时** — 指定在发现 PNP 服务器失败后，等待多少秒后重新尝试发现。
- **超时指数因子** — 该值会以指数形式触发发现尝试，具体原理为在上次超时值的基础上乘以指数值，并将所得结果用于新的超时值（前提是所得的值小于最大超时值）。
- **最大发现超时时间** — 超时时间最大值。必须大于**发现超时**值。
- **监视器超时** — 在活动 PNP 会话中（例如文件下载过程），在等待 PnP 或文件服务器回复时，等待多长时间后超时。

步骤 3 单击**应用**。参数将复制到当前配置文件中。

单击**将敏感数据显示为明文模式**能够显示加密的密码。

PNP 会话

此页面显示目前有效的 PNP 参数值。参数来源显示在括号中（如有相关来源）。

显示 PNP 参数相关信息的步骤：

步骤 1 单击**管理 > PNP > PNP 会话**。

系统将显示以下字段：

- **管理状态** — 是否已启用 PNP。
- **运行状态** — PNP 是否处于运行状态。

- **PNP 代理状态** — 指示是否存在活动的 PNP 会话。可能的值包括**发现等待**；**发现**；**未就绪**；**已禁用**；**会话**；**会话等待**。
- **传输协议** – 显示 PNP 代理会话信息。
- **TCP 端口** — PNP 会话的 TCP 端口
- **服务器 IP 地址** — PNP 服务器的 IP 地址
- **用户名** — 在 PNP 数据包中发送的用户名
- **密码 MD5** — 在 PNP 数据包中发送的密码
- **发现超时** — 配置的发现超时时间
- **会话间隔超时** — 配置的会话间隔超时时间（只有 **PNP 代理状态**为**正在等待**时，系统才会显示该字段）
- **剩余超时时间** — 剩余超时时间的值。

注 单击**恢复**按钮能够通过以下方式让 PnP 代理立即解除等待状态：

- 如果代理处于“发现等待”状态，则将其状态设置为“发现”。
- 如果代理处于“PnP 会话等待”状态，则将其状态设置为“PnP 会话”。

重启

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，重启设备会删除当前配置，因此在重启设备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，请参阅系统文件部分。

您可以通过文件操作页面或单击窗口顶部的**保存**备份设备配置，也可以在同一页面从远程设备上传配置。

您可能希望将重启时间设置在将来的某个时间。例如，在以下某种情况下，可能会出现这种需求：

- 您正在远程设备上执行操作，且这些操作中的错误可能会导致与远程设备的连接中断。预安排的重启可以恢复工作配置并在指定时间过后恢复与远程设备的连接。如果这些操作成功，则可以手动取消延迟重启。
- 重载设备会导致网络连接中断，因而通过使用延迟重启，您可以在用户更加方便的时间（例如深夜）安排重启。

重启设备的步骤：

步骤 1 单击**管理** > **重启**。

步骤 2 单击**重启**按钮可重启设备。

- **重启** — 可重启设备。由于当前配置中任何未保存的信息在设备重启后都会被丢弃，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。

  可用的选项如下：

  - *立即* — 立即重启。
  - *日期* — 输入计划重启的日期（月/日）和时间（小时和分钟）。此操作计划在特定时间（使用 24 小时制）执行软件的重载。如果您指定月份和日期，重载将在指定的时间和日期按计划执行。如果您未指定月份和日期，重载将在当天的指定时间执行（如果指定时间晚于当前时间），或者在次日的指定时间执行（如果指定时间早于当前时间）。指定 00:00 可在午夜进行重载。重载必须在 24 天内进行。

  注 仅当系统时间通过手动设置或由 SNTP 设置时，才能使用此选项。

  注 在安排了重启时间后，单击**取消重启**可取消安排的重启。

  - *在* — 在指定的小时和分钟数之内重启。最长时间为 24 天。
- **恢复出厂默认设置** — 使用出厂默认配置重启设备。该过程会擦除活动映像、镜像配置和本地化文件以外的一切内容。
- **清除启动配置文件** — 选中此项可在下次启动设备时清除启动配置。

发现协议 - Bonjour

请参阅 Bonjour。

发现协议 - LLDP

请参阅发现协议 - LLDP。

发现协议 - CDP

请参阅发现协议 - CDP。

定位设备

此功能可以让网络中特定设备上的所有网络端口 LED 闪烁，从而找到设备的物理位置。当房间中有许多互联的设备时，此功能对于在该房间中寻找设备非常有用。此功能激活后，设备上的所有网络端口 LED 都会在配置的持续时间（默认为一分钟）内闪烁。

步骤 1 单击**管理** > **定位设备**。

步骤 2 为以下字段输入值：

- **持续时间** — 输入端口 LED 闪烁的时间长度（以秒为单位）。
- **剩余时间** — 此字段仅在此功能处于激活状态时才显示。它用于显示 LED 闪烁的剩余时间。

步骤 3 单击**开始**可以激活此功能。

此功能激活后，“开始”按钮会替换为**停止**按钮。利用这个按钮，您可以让 LED 在定义的计时器到期之前停止闪烁。

Ping

Ping 实用程序用于测试是否可以访问远程主机，并测量从设备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) 回应请求数据包并等待 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**。

步骤 2 通过输入以下字段配置 Ping：

- **主机定义** — 选择是按 IP 地址还是名称来指定源接口。此字段会影响源 IP 字段中显示的接口，如下所述。
- **IP 版本** — 如果源接口根据其 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。
- **源 IP** — 选择其 IPv4 地址将在与目标的通信中用作源 IPv4 地址的源接口。如果“主机定义”为“按名称”，则此下拉字段中会显示所有 IPv4 和 IPv6 地址。如果“主机定义”为“按 IP 地址”，则仅显示“IP 版本”字段中指定类型的现有 IP 地址。

  注 如果选择“自动”选项，系统将根据目的地址计算源地址。
- **目标 IPv6 地址类型** — 请选择以下其中一个选项：
  - *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。
- **目标 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。系统会显示 Ping 状态，并且消息列表中会添加一条消息，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：

- **已发送的数据包数** — 由 ping 发送的数据包数
- **已接收的数据包数** — 由 ping 接收的数据包数
- **数据包丢失** — 在 ping 过程中丢失的数据包百分比
- **最短往返时间** — 数据包返回的最短时间

- **最长往返时间** — 数据包返回的最长时间
- **平均往返时间** — 数据包返回的平均时间
- **状态** — 失败或成功

Traceroute

Traceroute 通过向目标主机发送 IP 数据包并返回给设备，发现数据包的转发 IP 路由。“Traceroute”页面将显示设备和目标主机间的每一步跳以及每个此类步跳的往返时间。

步骤 1 单击**管理 > Traceroute**。

步骤 2 通过在以下字段中输入信息来配置 Traceroute：

- **主机定义** — 选择是按主机 IP 地址还是主机名来标识主机。
- **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。
- **源 IP** — 选择其 IPv4 地址将在通信消息中用作源 IPv4 地址的源接口。如果“主机定义”为“按名称”，则此下拉字段中会显示所有 IPv4 和 IPv6 地址。如果“主机定义”为“按 IP 地址”，则仅显示“IP 版本”字段中指定类型的现有 IP 地址。
- **主机 IP 地址/名称** — 输入主机地址或主机名。
- **TTL** — 输入 Traceroute 允许的最大步跳次数。此字段用于防止发送帧进入无限循环。当达到目标地址或达到此值时，Traceroute 命令将终止。要使用默认值 (30)，请选择**使用默认设置**。
- **超时** — 输入在宣布帧丢失之前系统等待帧返回的时间长度，或者选择**使用默认设置**。

步骤 3 单击**激活 Traceroute**。将执行该操作。

此时将显示一个页面，在以下字段中显示每个行程的往返时间 (RTT) 和状态：

- **索引** — 显示步跳的次数。
- **主机** — 显示路由至目标地址的一个停止。

往返时间 *(1-3)* — 显示第一个到第三个帧的往返时间（以毫秒为单位）以及第一个到第三个操作的状态。

7

管理：文件管理

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
- 固件操作
- 文件操作
- 文件目录
- DHCP 自动配置/映像更新

系统文件

系统文件是包含信息的文件，例如：配置信息或固件映像。

一般情况下，**flash://system/** 文件夹下的每个文件都是系统文件。

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

设备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。

设备上的其他文件包括固件和日志文件，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

以下是可以在设备上找到的一些类型的文件：

- **当前配置** — 包含当前设备工作所使用的参数。当您更改设备上的参数值时，此文件会相应修改。

  如果重启设备，当前配置将会丢失。

  要保留对设备所做的任何更改，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（通常为运行配置）复制到启动配置而保存的参数值。

  启动配置保留在闪存中，并且在设备重启后会保留。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，由设备创建的启动配置副本：

  - 设备已连续工作 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，系统可以将镜像配置复制到其他文件类型或其他设备。

  可在文件目录页面禁用自动将当前配置复制到镜像配置的选项。

- **备份文件** — 用于提供系统关机保护或维护特定工作状态的手动文件副本。例如，可以将镜像配置、启动配置或当前配置复制到备份文件。备份保存在闪存或 PC 或 USB 驱动器中，在设备重启时会得到保留。
- **固件** — 可控制设备的操作和功能的程序。更多时候被称为*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。
- **日志记录文件** — 存储在闪存中的系统日志消息。

固件操作

“固件操作”页面可用于：

- 更新或备份固件映像
- 交换活动映像

设备支持以下文件传输方法：

- 使用浏览器提供的工具的 HTTP/HTTPS
- USB
- 需要 TFTP 服务器的 TFTP
- 需要 SCP 服务器的安全复制协议 (SCP)

设备上存储有两个固件映像。其中一个映像确定为*活动映像*，另一个被确定为*非活动映像*。

更新设备的固件时，新固件始终覆盖非活动映像。在将新固件上传到设备后，设备下次启动时将使用新版本。重新启动后，旧版本将变为非活动版本。

使用 HTTP/HTTPS 或 USB 更新或备份固件的步骤：

步骤 1 单击**管理** > **文件管理** > **固件操作**。

系统将显示以下字段：

- **活动固件文件** — 显示当前活动固件文件。
- **活动固件版本** — 显示当前活动固件文件的版本。

步骤 2 输入以下字段：

- **操作类型** — 选择**更新固件**或**备份固件**。
- **复制方法** — 选择 **HTTP/HTTPS** 或 **USB**。
- **文件名** — 输入要更新的文件的名称（不适用于 HTTP/HTTPS 备份）。

步骤 3 单击**应用**。

步骤 4 单击**重启**。

使用 TFTP 更新或备份固件的步骤：

步骤 1 单击**管理** > **文件管理** > **固件操作**。

系统将显示以下字段：

- **活动固件文件** — 显示当前活动固件文件。
- **活动固件版本** — 显示当前活动固件文件的版本。

步骤 2 输入以下字段：

- **操作类型** — 选择**更新固件**或**备份固件**。
- **复制方法** — 选择 **TFTP**。
- **服务器定义** — 选择是**按照 IP 地址**还是**按照名称**指定 TFTP 服务器。

如果服务器定义是“按照地址”：

- **IP 版本** —（如果“服务器定义”是“按地址”）选择对于服务器使用 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）。
- **服务器 IP 地址/名称** — 据实际情况，输入 TFTP 服务器的 IP 地址或名称。
- **（更新）源** — 输入源文件的名称。
- **（备份）目标** — 输入备份文件的名称。

步骤 3 单击**应用**开始操作。

使用 SCP 更新/备份固件的步骤：

步骤 1 单击**管理** > **文件管理** > **固件操作**。

系统将显示以下字段：

- **活动固件文件** — 显示当前活动固件文件。
- **活动固件版本** — 显示当前活动固件文件的版本。

步骤 2 输入以下字段：

- **操作类型** — 选择**更新固件**或**备份固件**。
- **复制方法** — 选择 **SCP**。

步骤 3 要启用 SSH 服务器验证（默认情况下为禁用），请单击**远程 SSH 服务器验证**所对应的**编辑**。您将跳转到 SSH 服务器验证页面，您需要在此页面中配置 SSH 服务器

步骤 4 返回此页面。

步骤 5 选择以下其中一个方法，执行 **SSH 客户端验证**：

- **使用 SSH 客户端系统凭证** — 设置永久性 SSH 用户凭证。单击**系统凭证**可转至“SSH 用户验证”页面，在该页面设置一次用户/密码即可供日后永久性使用。
- **使用 SSH 客户端一次性凭证** — 输入以下内容：
  - *用户名* — 为该复制操作输入用户名。
  - *密码* — 为该副本输入密码。

  注 一次性凭证的用户名和密码将不会保存在配置文件中。

步骤 6 输入以下字段：

- **服务器定义** — 选择是按照 IP 地址还是按照域名来指定 SCP 服务器。

如果“服务器定义”是**按照地址**：

- **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。

- **服务器 IP 地址/名称** — 输入 SCP 服务器的 IP 地址或域名，以相关者为准。
- **（更新）源** — 输入源文件的名称。
- **（备份）目标** — 输入备份文件的名称。

步骤 7 单击**应用**。如果文件、密码和服务器地址正确，会出现以下其中一种结果：

- 如果已启用 SSH 服务器验证（在“SSH 服务器验证”页面）且 SCP 服务器处于受信状态，则该操作便会成功。如果 SCP 服务器处于非受信状态，则该操作将失败并显示错误。
- 如果未启用 SSH 服务器验证，则该操作针对任何 SCP 服务器都会成功。

交换映像文件的步骤：

步骤 1 单击**管理** > **文件管理** > **固件操作**。

系统将显示以下字段：

- **活动固件文件** — 显示当前活动固件文件。
- **活动固件版本** — 显示当前活动固件文件的版本。

步骤 2 填写屏幕上显示的以下字段：

- **操作类型** — 选择**交换映像**。
- **重新启动后的活动映像** — 选择重新启动后保持活动的固件文件。
- **重新启动后的活动映像版本号** — 显示重新启动后的固件文件的版本。

步骤 3 单击**应用**，显示成功消息后，如果想立即重新加载新固件，请单击**重新启动**。

文件操作

使用“文件操作”页面可以：

- 将配置文件或日志从设备备份到外部设备中。
- 将配置文件从外部设备还原到设备中。
- 复制配置文件。

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时，新文件会*替换*旧文件。

还原至启动配置时，必须重启设备，才能将还原的启动配置作为当前配置使用。可以使用重启一节中介绍的流程重启设备。

在任意窗口上单击**应用**，*仅会*将设备配置设置的更改存储在当前配置中。

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设备重启后全部丢失。

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其他备份文件。
- 从启动配置到当前配置或其他备份文件。
- 从备份文件到当前配置或启动配置。
- 从镜像配置到当前配置、启动配置或备份文件。

以下几节将介绍这些操作。

使用 HTTP/HTTPS、USB 或内部闪存更新系统配置文件的步骤：

步骤 1 单击**管理** > **文件管理** > **文件操作**。

步骤 2 输入以下字段：

- **操作类型** — 选择**更新文件**。
- **目的文件类型** — 选择一种要更新的配置文件类型。
- **复制方法** — 选择 **HTTP/HTTPS**、**USB** 或**内部闪存**。
- **文件名** — 输入要从（源文件）更新的文件的名称。

步骤 3 单击**应用**开始操作。

使用 TFTP 更新系统配置文件的步骤：

步骤 1 单击**管理** > **文件管理** > **文件操作**。

步骤 2 输入以下字段：

- **操作类型** — 选择**更新文件**。
- **目的文件类型** — 选择一种要更新的配置文件类型。
- **复制方法** — 选择 **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。

如果“服务器定义”是**按照地址**：

- **IP 版本** — 选择使用 IPv4 还是 IPv6 地址。

  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。

- **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。

- **服务器 IP 地址/名称** — 输入 TFTP 服务器的 IP 地址或名称。
- **源** — 输入更新文件名称。

步骤 3 单击**应用**开始操作。

使用 SCP 更新系统配置文件的步骤：

步骤 1 单击**管理** > **文件管理** > **文件操作**。

步骤 2 输入以下字段：

- **操作类型** — 选择**更新文件**。
- **目的文件类型** — 选择一种要更新的配置文件类型。
- **复制方法** — 选择 **SCP**。

步骤 3 要启用 SSH 服务器验证（默认情况下为禁用），请单击**远程 SSH 服务器验证**所对应的**编辑**。您将跳转到 SSH 服务器验证页面，您需要在此页面中配置 SSH 服务器

步骤 4 返回此页面。

步骤 5 选择以下其中一个方法，执行 **SSH 客户端验证**：

- **使用 SSH 客户端系统凭证** — 设置永久性 SSH 用户凭证。单击**系统凭证**可转至“SSH 用户验证”页面，在该页面设置一次用户/密码即可供日后永久性使用。
- **使用 SSH 客户端一次性凭证** — 输入以下内容：
  - *用户名* — 为该复制操作输入用户名。
  - *密码* — 为该副本输入密码。

  注 一次性凭证的用户名和密码将不会保存在配置文件中。
- **服务器定义** — 选择是按照 IP 地址还是按照域名来指定 SCP 服务器。

  如果“服务器定义”是**按照地址**：
  - **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。
- **服务器 IP 地址/名称** — 输入 SCP 服务器的 IP 地址或名称。
- **源** — 输入源文件的名称。

步骤 6 单击**应用**开始操作。

使用 HTTP/HTTPS 备份系统配置文件的步骤：

步骤 1 单击**管理** > **文件管理** > **文件操作**。

步骤 2 输入以下字段：

- **操作类型** — 选择**备份文件**。
- **源文件类型** — 选择一种要备份的配置文件类型。
- **复制方法** — 选择 **HTTP/HTTPS**。
- **敏感数据处理** — 选择应如何将敏感数据包含在备份文件中。可用的选项如下：

- *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 SSD 规则页面。

步骤 3 单击**应用**开始操作。

使用 USB 或内部闪存备份系统配置文件的步骤：

步骤 1 单击**管理** > **文件管理** > **文件操作**。

步骤 2 输入以下字段：

- **操作类型** — 选择**备份文件**。
- **源文件类型** — 选择一种要备份的配置文件类型。
- **复制方法** — 选择 **USB** 或**内部闪存**。
- **文件名** — 输入目标备份文件的名称。
- **敏感数据处理** — 选择应如何将敏感数据包含在备份文件中。可用的选项如下：
  - *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 SSD 规则页面。

步骤 3 单击**应用**开始操作。

使用 TFTP 备份系统配置文件的步骤：

步骤 1 单击**管理** > **文件管理** > **文件操作**。

步骤 2 输入以下字段：

- **操作类型** — 选择**备份文件**。
- **源文件类型** — 选择要备份的文件的类型。
- **复制方法** — 选择 **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。

  如果“服务器定义”是**按照地址**：

  - **IP 版本** — 选择使用 IPv4 还是 IPv6 地址。

    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。

  - **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。
- **服务器 IP 地址/名称** — 输入 TFTP 服务器的 IP 地址或名称。
- **目标** — 输入备份文件名称。
- **敏感数据处理** — 选择应如何将敏感数据包含在备份文件中。可用的选项如下：

  - *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。

步骤 3 单击**应用**开始操作。

使用 SCP 备份系统配置文件的步骤：

步骤 1 单击**管理** > **文件管理** > **文件操作**。

步骤 2 输入以下字段：

- **操作类型** — 选择**备份文件**。
- **源文件类型** — 选择要备份的文件的类型。
- **复制方法** — 选择 **SCP**。
- **远程 SSH 服务器验证** — 远程 SSH 服务器验证的当前状态。单击**编辑**，转至 **SSH 服务器验证**，更改设置。

SSH 客户端验证 — 可通过以下方式进行客户端验证：

- **使用 SSH 客户端系统凭证** — 设置永久性 SSH 用户凭证。单击**系统凭证**可转至“SSH 用户验证”页面，在该页面设置一次用户/密码即可供日后永久性使用。
- **使用 SSH 客户端一次性凭证** — 输入以下内容：
  - *用户名* — 为该复制操作输入用户名。
  - *密码* — 为该副本输入密码。
- **服务器定义** — 选择是按照 IP 地址还是按照域名来指定 SCP 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。
- **服务器 IP 地址/名称** — 输入 SCP 服务器的 IP 地址或名称。
- **目标** — 输入备份文件的名称。
- **敏感数据处理** — 选择应如何将敏感数据包含在备份文件中。可用的选项如下：
  - *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。

步骤 3 单击**应用**开始操作。

将系统配置文件复制到另一类型的配置文件的步骤：

步骤 1 单击**管理** > **文件管理** > **文件操作**。

步骤 2 输入以下字段：

- **操作类型** — 选择**复制**。
- **源文件名** — 选择要复制的配置文件类型之一。
- **目标文件名** — 输入目标配置文件的名称。

步骤 3 单击**应用**开始操作。

文件目录

“文件目录”页面显示系统中的系统文件。

步骤 1 单击**管理** > **文件管理** > **文件目录**。

步骤 2 如有必要，启用**自动镜像配置**。这将启用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 选择您想显示文件和目录的驱动器。可用的选项如下：

- **闪存** — 显示管理工作站根目录中的所有文件。
- **USB** — 显示 USB 驱动器上的文件。

步骤 4 单击**转至**将显示以下字段：

- **文件名** — 系统文件类型或实际文件名，取决于文件类型。
- **权限** — 户对文件的读/写权限。
- **大小** — 文件的大小。

- **上次修改** — 文件的修改日期和时间。
- **完整路径** — 文件的路径。

DHCP 自动配置/映像更新

自动配置/映像更新功能提供了一种在网络中自动配置交换机以及升级其固件的便捷方法。通过该过程，管理员可以在网络中远程确保这些设备的配置和固件为最新。

此功能包含以下部分：

- **自动映像更新** — 自动从远程 TFTP/SCP 服务器下载固件映像。自动配置/映像更新过程结束时，设备将使用该固件映像自动重启。
- **自动配置** — 自动从远程 TFTP/SCP 服务器下载配置文件。自动配置/映像过程结束时，设备将使用该配置文件自动重启。

注 如果同时请求自动映像更新和自动配置，系统将先执行自动映像更新，然后在重启后执行自动配置，再执行最终重启。

要使用此功能，请使用设备的配置文件和固件映像的位置和名称，在网络中配置 DHCP 服务器。设备在网络中默认配置为 DHCP 客户端。当 DHCP 服务器为设备分配 IP 地址时，设备还会收到有关配置文件和固件映像的信息。如果配置文件和/或固件映像与设备上当前使用的文件和/或映像不同，设备会在下载文件和/或映像后自动重启。本节将介绍这些过程。

除了可以在网络中让设备的配置文件和固件映像保持最新以外，自动更新/配置功能还可以在网络中快速安装新设备，因为开箱即用设备配置为从网络检索其配置文件和软件映像，而无需系统管理员进行任何手动干预。设备首次向 DHCP 服务器申请 IP 地址时，会下载 DHCP 服务器指定的配置文件和/或映像，并使用这些文件和/或映像自动重启。

在自动配置过程中可以使用安全复制协议 (SCP) 和安全敏感数据 (SSD) 功能下载含有敏感信息（例如 RADIUS 服务器密钥和 SSH/SSL 密钥）的配置文件（请参阅 SSH 客户端验证和安全：安全敏感数据管理）。

下载协议（TFTP 或 SCP）

配置文件和固件映像可以从 TFTP 或 SCP 服务器下载。

用户可对要使用的协议进行如下配置：

- **按文件扩展名自动执行** —（默认）如果选择了该选项，用户定义的文件扩展名表示带有此扩展名的文件将使用 SCP（藉由 SSH）下载，而带有其他扩展名的文件将使用 TFTP 下载。例如，如果指定的文件扩展名为 *.xyz*，则可使用 SCP 下载带有 *.xyz* 扩展名的文件，而带有其他扩展名的文件可使用 TFTP 下载。默认扩展名为 .scp。
- **仅 TFTP** — 无论配置文件名的文件扩展名是什么，都通过 TFTP 进行下载。
- **仅 SCP** — 无论配置文件名的文件扩展名是什么，都通过 SCP（藉由 SSH）进行下载。

SSH 客户端验证

SCP 基于 SSH。默认情况下，远程 SSH 服务器验证处于禁用状态。因此，设备将接受任何开箱即用的远程 SSH 服务器。您可以启用远程 SSH 服务器验证，以便仅允许使用信任服务器列表中的服务器。

客户端（即设备）需要 SSH 客户端验证参数才能访问 SSH 服务器。默认的 SSH 客户端验证参数为：

- SSH 验证方法：按用户名/密码
- SSH 用户名：anonymous
- SSH 密码：anonymous

注 当手动下载文件（即未通过 DHCP 自动配置/映像更新功能进行的下载）时，也可使用 SSH 客户端验证参数。

自动配置/映像更新过程

DHCP 自动配置功能使用所接收 DHCP 消息中的配置服务器名称/地址和配置文件名/路径（如果有）。此外，DHCP 映像更新使用消息中的固件间接文件名（如果有）。在来自 DHCPv4 服务器的 **Offer** 消息和来自 DHCPv6 服务器的 **Information Reply** 消息中，这些信息会被指定为 DHCP 选项。

如果在 DHCP 服务器消息中找不到这些信息，系统将使用在 DHCP 自动配置/映像更新页面中配置的备份信息。

当触发自动配置/映像更新过程后（请参阅自动配置/映像更新的触发），会按顺序发生下述事件。

自动映像更新开始：

- 交换机使用来自所接收 DHCP 消息中的选项 125 (DHCPv4) 和选项 60 (DHCPv6)（如果有）的间接文件名。
- 如果 DHCP 服务器未发送固件映像文件的间接文件名，系统将使用“备份间接映像文件名”（来自 DHCP 自动配置/映像更新页面）。
- 交换机将下载间接映像文件，并从中提取 TFTP/SCP 服务器的映像文件名。
- 交换机会将 TFTP 服务器映像文件的版本与交换机活动映像的版本相比较。
- 如果这两个版本不同，则将新版本载入非活动映像，然后执行重启，非活动映像将成为活动映像。
- 使用 SCP 协议时，系统将生成系统日志消息，通知您重启即将开始。
- 使用 SCP 协议时，系统将生成系统日志消息，确认自动更新过程已完成。
- 使用 TFTP 协议时，系统日志消息通过复制过程生成。

自动配置开始

- 设备使用来自所接收 DHCP 消息的 TFTP/SCP 服务器名称/地址和配置文件名/路径（DHCPv4 选项：66、150 和 67；DHCPv6 选项：59 和 60）（如果有）。
- 如果 DHCP 服务器未发送这些信息，系统将使用“备份服务器 IP 地址/名称”和“备份配置文件名”（来自 DHCP 自动配置/映像更新）。
- 如果新配置文件的名称与设备上之前使用的配置文件的名称不同，或设备从未进行过配置，系统将使用新配置文件。
- 自动配置/映像更新过程结束时，设备将使用新配置文件重启。
- 系统日志消息通过复制过程生成。

缺失选项

- 如果 DHCP 服务器未在 DHCP 选项中发送 TFTP/SCP 服务器地址，且备份 TFTP/SCP 服务器地址参数未配置，那么：
  - **SCP** — 自动配置过程将停止。
  - **TFTP** — 设备将向其 IP 接口上的有限广播地址（针对 IPv4）或 ALL NODES 地址（针对 IPv6）发送 TFTP 请求消息，并使用第一个应答的服务器继续自动配置/映像更新过程。

下载协议选项

- 选择复制协议 (SCP/TFTP)，如下载协议（TFTP 或 SCP）中所述。

SCP

- 当使用 SCP 下载时，在以下任一情况下，设备将接受任何指定的 SCP/SSH 服务器（且不对其进行验证）：
  - SSH 服务器验证过程为禁用状态。SSH 服务器验证在默认情况下为禁用状态，这样便可以为带有出厂默认配置的设备（例如开箱设备）下载配置文件。
  - SSH 服务器将在 SSH 信任服务器列表中配置。

  如果已启用 SSH 服务器验证过程但在 SSH 信任服务器列表中未找到 SSH 服务器，则自动配置过程将停止。
- 如果信息可用，系统将访问 SCP 服务器，以从中下载配置文件或映像。

自动配置/映像更新的触发

满足以下条件时，会触发通过 DHCPv4 进行自动配置/映像更新的功能：

- 设备的 IP 地址在重启时动态分配或续订、通过管理操作显式续订或者由于租用到期而自动续订。可以在“IPv4 接口”页面激活显性续订。
- 如果启用自动映像更新，当从 DHCP 服务器接收到间接映像文件名或已配置备份间接映像文件名时，将触发自动映像更新过程。间接意味着这不是映像本身，而是包含映像路径名称的文件。
- 如果启用自动配置，当从 DHCP 服务器接收到配置文件名或已配置备份配置文件名时，将触发自动配置过程。

满足以下条件时，会触发通过 DHCPv6 进行自动配置/映像更新的功能：

- DHCPv6 服务器向设备发送信息时。这发生在以下情况下：
  - 当一个启用了 IPv6 的接口被定义为 DHCPv6 无状态配置客户端时。
  - 收到来自服务器的 DHCPv6 消息时（例如，当您按“IPv6 接口”页面上的**重新启动**按钮时）。
  - 设备刷新 DHCPv6 信息时。
  - 在启用无状态 DHCPv6 客户端时重启设备后。

- DHCPv6 服务器数据包中包含配置文件名选项时。
- 当 DHCP 服务器提供间接映像文件名或已配置备份间接映像文件名时，将触发自动映像更新过程。间接意味着这不是映像本身，而是包含映像路径名称的文件。

DHCP 自动配置/映像更新

使用 DHCP 自动配置/映像更新页面可将设备配置为 DHCP 客户端。

系统中存在以下默认设置：

- 自动配置处于禁用状态。
- 自动映像更新处于禁用状态。
- 设备作为 DHCP 客户端启用。
- 远程 SSH 服务器验证为禁用状态。

使用说明

要使用此功能，设备必须配置为 DHCPv4 或 DHCPv6 客户端。在设备上定义的 DHCP 客户端类型与在设备上定义的接口类型相关联。

自动配置准备

要准备 DHCP 和 TFTP/SCP 服务器，请进行以下操作：

TFTP/SCP 服务器

- 将配置文件放置到工作目录下。此文件可以通过从设备复制配置文件进行创建。设备启动时，此文件将成为当前配置文件。

DHCP 服务器

使用以下选项配置 DHCP 服务器：

- DHCPv4：
  - 66（单个服务器地址）或 150（服务器地址列表）
  - 67（配置文件名称）
- DHCPv6
  - 选项 59（服务器地址）
  - 选项 60（配置文件名加间接映像文件名，以英文逗号分隔）

自动映像更新准备工作

要准备 DHCP 和 TFTP/SCP 服务器，请进行以下操作：

TFTP/SCP 服务器

1. 在主目录下创建一个子目录。在其中放置软件映像文件。
2. 创建包含固件版本的路径和名称的间接文件（例如，包含 cisco\cisco-version.ros 的 indirect-cisco.txt）。
3. 将此间接文件复制到 TFTP/SCP 服务器的主目录。

DHCP 服务器

使用以下选项配置 DHCP 服务器

- DHCPv4 — 选项 125（间接文件名）
- DHCPv6 — 选项 60（配置文件名加间接映像文件名，以英文逗号分隔）

DHCP 客户端工作流程

步骤 1 在 DHCP 自动配置/映像更新页面中配置自动配置和/或自动映像更新参数。

步骤 2 在“IP 配置”>“IPv4 接口”页面中将“IP 地址类型”设置为“动态”。在 IPv4 接口页面中将“IP 地址类型”设置为“动态”，并且/或者在 IPv6 接口页面中将设备定义为无状态 DHCPv6 客户端。

Web 配置

配置自动配置和/或自动更新的步骤：

步骤 1 单击**管理** > **文件管理** > **DHCP 自动配置/映像更新**。

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。该功能在默认状态下为禁用状态，但是可在此处启用。
- **下载协议** — 选择以下其中一种选项：
  - *按文件扩展名自动执行* — 选择该选项可指示自动配置根据配置文件的扩展名使用 TFTP 或 SCP 协议。如果选中该选项，则无需给出配置文件的扩展名。如果未给出扩展名，则使用默认的扩展名（如下所示）。

- *SCP 的文件扩展名* — 如果选中**按文件扩展名自动执行**，便可以在此注明文件扩展名。使用 SCP 便可下载任何带有该扩展名的文件。如果未输入扩展名，则将使用默认的文件扩展名 **.scp**。
- *仅 TFTP* — 选择该选项可指示仅使用 TFTP 协议进行自动配置。
- *仅 SCP* — 选择该选项可指示仅使用 SCP 协议进行自动配置。

- **通过 DHCP 自动更新映像** — 选择该字段可启用来自 DHCP 服务器的固件映像更新。该功能在默认状态下为禁用状态，但是可在此处启用。
- **下载协议** — 选择以下其中一种选项：
  - *按文件扩展名自动执行* — 选择该选项可指示自动更新根据映像文件的扩展名使用 TFTP 或 SCP 协议。如果选中该选项，则无需给出映像文件的扩展名。如果未给出扩展名，则使用默认的扩展名（如下所示）。
  - *SCP 的文件扩展名* — 如果选中**按文件扩展名自动执行**，便可以在此注明文件扩展名。使用 SCP 便可下载任何带有该扩展名的文件。如果未输入扩展名，则将使用默认的文件扩展名 **.scp**。
  - *仅 TFTP* — 选择该选项可指示仅使用 TFTP 协议进行自动更新。
  - *仅 SCP* — 选择该选项可指示仅使用 SCP 协议进行自动更新。
- **SCP 的 SSH 设置** — 当使用 SCP 下载配置文件时，请选择以下选项之一：
- **远程 SSH 服务器验证** — 单击**启用/禁用**链接以导航至“SSH 服务器验证”页面。您可在该页面启用下载需使用的 SSH 服务器验证并在必要时输入信任 SSH 服务器。
- **SSH 客户端验证** — 单击“系统凭证”链接以在“SSH 用户验证”页面输入用户凭证。
- **备份服务器定义** — 选择是**按照 IP 地址**还是**按照名称**来配置备份服务器。

步骤 3 如果“服务器定义”是**按照地址**：

- **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）。

步骤 4 输入以下可选信息，以便在 DHCP 服务器未提供所需信息时使用。

- **备份服务器 IP 地址/名称** — 输入备份服务器 IP 地址或名称。
- **备份配置文件名** — 输入备份配置文件名。
- **备份间接映像文件名** — 输入要使用的间接映像文件名。这是包含映像路径的文件。间接映像文件名的一个示例是：indirect-cisco.scp。此文件包含固件映像的路径和名称。

系统将显示以下字段：

- **最近自动配置/映像服务器 IP 地址** — 最近备份服务器的地址。
- **最近自动配置文件名称** — 最近配置文件名称。

步骤 5 单击**应用**。参数将复制到当前配置文件中。

8

管理：时间设置

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 设备支持简单网络时间协议 (SNTP)，如果启用了该协议，设备会动态同步设备时间与 SNTP 服务器时间。设备仅作为 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、时区和夏令时 (DST) 的选项。其中包含以下主题：

- 系统时间配置
- SNTP 模式
- 系统时间
- SNTP 单播
- SNTP 组播/任播
- SNTP 验证
- 时间范围
- 循环时间范围

系统时间配置

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，设备始终会配置时间、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设备上的系统时间：

- **手动** — 用户必须手动设置时间。
- **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，可确保将设备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。

时区和夏令时 (DST)

可以通过以下方式在设备上设置时区和 DST：

- 通过 DHCP 服务器动态配置设备，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

设备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，而设备则监听这些广播。如果设备处于该模式，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 客户端的设备会定期请求 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** — 设备向子网中的所有 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** — 设备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。

设备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。

系统时间

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设备，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**。

系统将显示以下字段：

- **实际时间（*系统时间源*）**— 设备上的系统时间。此字段显示 DHCP 时区或用户定义时区的缩写词（如果用户进行了定义）。
- **最近同步的服务器** — 上次从其获取系统时间的 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 组播/任播页面中配置到 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。
- **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 服务器或时区偏移使用本地时间。
  - *从 DHCP 获取时区* — 选择该选项可实现通过 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，*必须在设备上启用 DHCP 客户端*。

  注 DHCP 客户端支持提供动态时区设置的选项 100。
  - *来自 DHCP 的时区* — 显示从 DHCP 服务器配置的时区的缩写词。缩写词显示在**实际时间**字段中
  - *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。
  - *时区缩写* — 输入表示此时区的名称。缩写词显示在**实际时间**字段中。
- **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。按照以下说明输入参数。

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。

步骤 3 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 4 单击**应用**。系统时间值将写入当前配置文件。

SNTP 单播

最多可配置 16 台单播 SNTP 服务器。

注 要按名称指定单播 SNTP 服务器，必须先在设备上配置 DNS 服务器（请参阅 DNS 设置）。

添加单播 SNTP 服务器的步骤：

步骤 1 单击**管理** > **时间设置** > **SNTP 单播**。

步骤 2 输入以下字段：

- **SNTP 客户端单播** — 选择该选项可让设备将预定义了 SNTP 的单播客户端与组播 SNTP 服务器配合使用。
- **IPv4 源接口** — 选择其 IPv4 地址将用作与 SNTP 服务器通信中消息的源 IPv4 地址的 IPv4 接口。
- **IPv6 源接口** — 选择其 IPv6 地址将用作与 SNTP 服务器通信中消息的源 IPv6 地址的 IPv6 接口。

  注 如果已选择“自动”选项，系统将使用传出接口上定义的 IP 地址的源 IP 地址。

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。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 服务器和设备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：
  - *运行* — SNTP 服务器目前正常运行。
  - *关闭* — SNTP 服务器目前不可用。
  - *未知* — SNTP 服务器的状态未知。
  - *正在进行* — 正在连接到 SNTP 服务器。
- **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。

- **源** — 如何定义 SNTP 服务器，例如：手动定义或从 DHCPv6 服务器定义。
- **接口** — 接收数据包的接口。

步骤 3 要添加单播 SNTP 服务器，请启用 **SNTP 客户端单播**。

步骤 4 单击**添加**。

注 要移除所有用户定义的 SNTP 服务器，请单击**恢复默认服务器**。

步骤 5 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，必须将设备连接到互联网并配置一个 DNS 服务器，或者配置为使用 DHCP 可以识别 DNS 服务器。（请参阅 DNS 设置）

- **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/名称** — 输入 SNTP 服务器的 IP 地址或名称。格式取决于所选的地址类型。
- **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。系统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，设备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 6 单击**应用**。系统将添加 STNP 服务器，并返回主页。

SNTP 组播/任播

设备可以处于主动和/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**。

请从以下选项中进行选择：

- **SNTP IPv4 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 IPv4 组播传输。
- **SNTP IPv6 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 IPv6 组播传输。
- **SNTP IPv4 任播客户端模式（客户端广播传输）**— 选择该选项可传输请求系统时间信息的 SNTP IPv4 同步数据包。数据包传输至子网中的所有 SNTP 服务器。
- **SNTP IPv6 任播客户端模式 (客户端广播传输)** - 选择该选项可传输请求系统时间信息的 SNTP IPv6 同步数据包。数据包传输至子网中的所有 SNTP 服务器。

步骤 2 单击**应用**，以将设置保存到当前配置文件中。

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。

工作流程

步骤 1 在下面的“SNTP 验证”页面中启用验证功能。

步骤 2 在下面的“SNTP 验证”页面中创建一个密钥。

步骤 3 在 SNTP 单播页面中将此密钥与 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**。

步骤 2 选择 **SNTP 验证**，以支持对设备和 SNTP 服务器之间的 SNTP 会话进行验证。

步骤 3 单击**应用**更新设备。

步骤 4 单击**添加**。

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（已加密）**— 以加密格式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，设备才会与之同步。
- **验证密钥（纯文本）**— 以纯文本格式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，设备才会与之同步。
- **信任密钥** — 选择该选项，可使设备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。

时间范围

可以定义时间范围，并将其与以下类型的命令相关联，以便仅在该时间范围内应用这些命令：

- ACL
- 8021X 端口验证
- 端口设置
- 基于时间的 PoE

有两种类型的时间范围：

- **绝对值** — 此类型的时间范围始于特定日期或立即开始，结束于特定日期或没有结束日期。可在时间范围页面中进行创建，还可以在其中添加循环元素。
- **循环** — 此类型的时间范围包含添加到绝对范围的时间范围元素，以及循环开始和结束的时间。可在“循环范围”页面中进行定义。

如果时间范围既包括绝对范围，也包括循环范围，则仅会在同时达到绝对开始时间和循环时间范围时才会激活关联命令的运行。达到任何一个时间范围后都会禁用关联命令的运行。

设备最多可支持 10 个绝对时间范围。

所有时间规格均可解释为本地时间（夏令时对此没有影响）。要确保时间范围条目在所需时间内有效，必须设置系统时间。

时间范围功能可用于以下目的：

- 例如，限制计算机在办公时间访问网络，执行此功能后将锁定网络端口，并阻塞对其余网络的访问（请参阅端口设置和链路聚合）
- 将 PoE 操作限制在特定的时间段。

绝对时间范围

定义绝对时间范围的步骤：

步骤 1 单击**管理** > **时间设置** > **时间范围**。

此时将显示现有时间范围。

步骤 2 要添加新的时间范围，请单击**添加**。

步骤 3 输入以下字段：

- **时间范围名称** — 输入新的时间范围名称。
- **绝对开始时间** — 要定义开始时间，请输入以下字段：
  - *立即* — 选择该选项，时间范围将立即开始。
  - *日期，时间* — 输入时间范围的开始日期和时间。
- **绝对结束时间** — 要定义结束时间，请输入以下字段：
  - *无限期* — 选择该选项，时间范围将没有结束日期。
  - *日期，时间* — 输入时间范围的结束日期和时间。

步骤 4 单击**应用**。

步骤 5 要添加循环时间范围，请单击**循环范围**。

循环时间范围

可以为绝对时间范围添加循环时间元素。这会限制在绝对范围内的某些时间段内执行操作。

向绝对时间范围添加循环时间范围元素的步骤：

步骤 1 单击**管理** > **时间设置** > **循环范围**。

此时将显示现有的循环时间范围（根据特定的绝对时间范围进行过滤）。

步骤 2 选择要添加循环范围的绝对时间范围。

步骤 3 要添加新的循环时间范围，请单击**添加**。

步骤 4 输入以下字段：

- **循环开始时间** — 输入时间范围循环开始的日期和时间。
- **循环结束时间** — 输入时间范围循环结束的日期和时间。

步骤 5 单击**应用**。

步骤 6 单击**时间范围**访问**绝对时间范围**页面。

9

管理：发现协议

本节提供有关配置发现的信息。

其中包含以下主题：

- Bonjour
- LLDP 和 CDP
- 发现协议 - LLDP
- 发现协议 - CDP

Bonjour

作为 Bonjour 客户端，设备会定期向直接连接的 IP 子网广播 Bonjour 发现协议数据包，通告其存在以及所提供的服务，例如 HTTP 或 HTTPS。（可使用“安全 > TCP/UDP 服务”页面启用或禁用设备服务。）网络管理系统或其他第三方应用可*发现*设备。默认情况下，Bonjour 已启用并在管理 VLAN 上运行。

当设备处于第 2 层系统模式时，系统会全局启用 Bonjour 发现，向管理 VLAN 发送 Bonjour 通告。设备会按照“服务”页面上的配置，通告管理员开启的所有服务。

同时启用 Bonjour 发现和 IGMP 时，Bonjour 的 IP 组播地址会显示在“添加 IP 组播群地址”页面上。

若禁用 Bonjour 发现，设备会停止所有服务类型通告，且不会响应来自网络管理应用的服务请求。

Bonjour 发现只能全局启用，而无法针对每个端口或每个 VLAN 单独启用。设备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 组播群地址”页面上。

若禁用 Bonjour 发现，设备会停止服务类型通告，且不会对来自网络管理应用的服务请求作出响应。

默认情况下，系统会在作为管理 VLAN 成员的所有接口上启用 Bonjour。

配置 Bonjour 的步骤：

步骤 1 单击**管理** > **发现协议 - Bonjour**。

步骤 2 选择**启用**以全局启用 Bonjour 发现。

步骤 3 要在特定接口上启用 Bonjour，请单击**添加**。

步骤 4 **选择**接口。如果已向接口分配了 IP 地址，系统会显示该地址。

步骤 5 单击**应用**更新当前配置文件。

注 单击**删除**可在接口上禁用 Bonjour（仅执行删除操作，而不会执行诸如**应用**等任何其他操作）。

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通告自身及其功能。默认情况下，设备会定期向所有接口发送 LLDP/CDP 通告，并按照协议的要求处理入站 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 可全局或按端口启用或禁用。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，设备将滤除来自已禁用 CDP/LLDP 端口的入站 CDP/LLDP 数据包。
- 如果全局禁用 CDP/LLDP，设备可配置为对所有入站 CDP/LLDP 数据包执行丢弃、VLAN 感知泛洪或 VLAN 非感知泛洪。VLAN 感知泛洪会将入站 CDP/LLDP 数据包泛洪到接收数据包的 VLAN，其中不包括入站端口。VLAN 非感知泛洪会将入站 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 和 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，设备会根据所配置的语音 VLAN 发送 CDP 和 LLDP 通告。有关详细信息，请参阅语音 VLAN。

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，设备才可在其上收发 CDP/LLDP 数据包。

如果端口是镜像目标，则 CDP/LLDP 会将其视为处于关闭状态。

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。

发现协议 - LLDP

本节介绍如何配置 LLDP。其中包含以下主题：

- LLDP 概述
- LLDP 配置工作流程
- LLDP 属性
- 端口设置
- LLDP MED 网络策略
- LLDP MED 端口设置
- LLDP 端口状态
- LLDP 本地信息
- LLDP 邻居信息

- 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 可让设备向邻居设备通告其身份、配置和功能，然后这些邻居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，设备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 网络策略。

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。有关如何访问 LLDP 配置页面，请参阅 LLDP 和 CDP 一节。

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. 使用端口设置页面配置每个端口的 LLDP。在该页面上，接口可配置为接收/传输 LLDP PDU、发送 SNMP 通知、指定要通告的 TLV，以及通告设备的管理地址。
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，请在属性页面中启用 LLDP。
6. 使用 LLDP 过载页面显示过载信息。

LLDP 属性

使用“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** > **发现协议 - LLDP** > **属性**。

步骤 2 输入参数。

- **LLDP 状态** — 选择该选项可启用设备上的 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 SNMP 通知间隔** — 输入 SNMP 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 LLDP 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）。
- **机箱 ID 通告** — 为 LLDP 消息中的通告选择以下一个选项：
  - *MAC 地址* — 通告设备的 MAC 地址。
  - *主机名* — 通告设备的主机名。

步骤 3 在 **LED-MED 属性快速启动重复计数**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设备时会发生这种情况。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。

端口设置

使用“LLDP 端口设置”页面可针对每个端口激活 LLDP 和 SNMP 通知，并输入在 LLDP PDU 中发送的 TLV。

要通告的 LLDP-MED TLV 可在 LLDP MED 端口设置页面进行选择，并且可以配置设备的管理地址 TLV。

定义 LLDP 端口设置的步骤：

步骤 1 单击**管理** > **发现协议 - LLDP** > **端口设置**。

此页面包含端口 LLDP 信息。

步骤 2 选择一个端口，然后单击**编辑**。

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。
- **SNMP 通知** — 如果选择**启用**，则系统会在发生拓扑更改时向 SNMP 通知接收设备（例如 SNMP 管理系统）发送通知。

  可在 LLDP 属性页面的“拓扑更改 SNMP 通知时间间隔”字段中输入通知之间的时间间隔。使用 SNMPv1.2 通知接收设备定义 SNMP 通知接收设备。
- **选定的可选 TLV** — 通过将 TLV 从**可用的可选 TLV** 列表移至此列表，来选择要由设备发布的信息。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、操作系统和设备支持的网络软件。该值与 sysDescr 对象相等。
  - *系统功能* — 设备的主要功能，以及是否已在设备中启用这些功能。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。
- *通过 MDI 提供的 802.3 电源* — 通过 MDI 传输的最大电源。
- *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 最大帧大小* — MAC/PHY 实施的最大帧大小功能。
- *通过 MDI 提供的 4 芯电源* —（与支持 60 瓦 PoE 的 PoE 端口相关）定义的思科专有 TLV，支持功率为 60 瓦的以太网供电功能（标准支持最高为 30 瓦）。

管理地址可选 TLV

- **通告模式** — 选择以下其中一种通告设备 IP 管理地址的方法：
  - *自动通告* — 指定软件从所有设备的 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。

802.1 VLAN 和协议

- **PVID** — 选择该选项可在 TLV 中通告 PVID。
- **端口和协议 VLAN ID** — 输入端口上启用的基于协议的 VLAN。
- **VLAN ID** — 选择将通告的 VLAN。
- **协议 ID** — 选择将通告的协议。
- **选定的协议 ID** — 在**协议 ID** 框中选择要使用的协议，将这些协议移到**选定的协议 ID** 框。

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 网络策略

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：

- 实现实时应用（如语音和/或视频）的网络策略通告和发现。
- 通过设备位置发现可创建位置数据库；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。

可使用 LLDP MED 端口设置页面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，管理员还可指引设备根据其保留的语音 VLAN，自动生成并通告语音应用的网络策略。有关设备如何保留其语音 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** > **发现协议 - LLDP** > **LLDP MED 网络策略**。

此页面包含之前创建的网络策略。

步骤 2 若要使设备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“LDP-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，请单击**添加**。

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 类型** — 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它们发送给设备的应用流量。

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。

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“LDP-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，设备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** > **发现协议 - LLDP** > **LLDP MED 端口设置**。

此页面将为所有端口显示以下 LLDP MED 设置（仅列出**编辑**页面中未介绍的字段）：

- **用户定义的网络策略** — 为各种类型的流量（即应用）定义策略。策略在 LLDP MED 网络策略中定义。在这种情况下，系统会显示端口策略的以下信息：
  - *活动* — 端口上活动的流量类型。
  - *应用* — 为其定义策略的流量类型。
- **位置** — 显示是否传输位置 TLV。

- **PoE** — 是否传输 PoE-PSE TLV。
- **清单** — 显示是否传输清单 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（请参阅 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**。

步骤 4 输入以下参数：

- **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。
- **SNMP 通知** — 选择在发生拓扑更改时，是否在发现支持 MED 的终端工作站（例如，SNMP 管理系统）时，针对每个端口发送 SNMP 通知。
- **选定的可选 TLV** — 通过将 TLV 从**可用的可选 TLV** 列表移至“选定的可选 TLV”列表中，来选择可由设备发布的 TLV。
- **选定的网络策略** — 通过将 LLDP MED 策略从**可用的网络策略**列表移至**选定的网络策略**列表中，选择将由 LLDP 发布的 LLDP MED 策略。这些策略是在 LLDP MED 网络策略页面中创建的。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。

LLDP 端口状态

“LLDP 端口状态”页面包含每个端口的 LLDP 全局信息。

步骤 1 要查看 LLDP 端口状态，请单击**管理** > **发现协议 - LLDP** > **LLDP 端口状态**。

系统将显示所有端口的信息。

步骤 2 选择具体端口，单击 **LLDP 本地信息详情**，查看发送给此端口的 LLDP 和 LLDP-MED TLV 的详情。

步骤 3 选择具体端口，单击 **LLDP 邻居信息详情**，查看从此端口接收的 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。如果机箱 ID 子类型为 MAC 地址，则系统会显示设备的 MAC 地址。
- **系统名称** — 设备的名称。
- **系统说明** — 对设备的描述（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（电源类型、电源、电源优先级、功率值）** — 通告的本地 PoE 信息。
- **远程 PoE（电源类型、电源、电源优先级、功率值）** — 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。

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** > **发现协议 - LLDP** > **LLDP 本地信息**。

步骤 2 选择要显示 LLDP 本地信息的接口。

此页面将为选定接口显示以下字段：

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。如果机箱 ID 子类型为 MAC 地址，则系统会显示设备的 MAC 地址。
- **系统名称** — 设备的名称。
- **系统说明** — 对设备的描述（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：

- **IPv4 地址** — 返回的最适合管理用途的 IPv4 地址。
- **IPv6 全局地址** — 返回的最适合管理用途的 IPv6 全局地址。
- **IPv6 链路本地地址**— 返回的最适合管理用途的 IPv6 链路本地地址。

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。

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。
- **电源类型** — 连接到端口的 Pod 设备类型。
- **电源** — 端口电源。
- **电源优先级** — 端口电源优先级。
- **PD 请求的功率值** — PSE 分配给 PD 的功率量。
- **PSE 分配功率值** — 分配给供电设备 (PSE) 的功率量。

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）。
- **远程发送回应** — 表明本地链路伙伴反射远程链路伙伴的发送值。
- **远程接收回应** — 表明本地链路伙伴反射远程链路伙伴的接收值。

通过 MDI 提供的 4 线电源

- **支持的 4 对 PoE** — 表示系统和端口支持启用 4 对电线（仅适用于拥有此硬件功能的具体端口）。
- **需要备用对检测/分类** — 表示需要 4 对电线。
- **PD 备用线对理想状态** — 表示 Pod 设备请求启用四对线功能。
- **PD 备用线对工作状态** — 表示是启用还是禁用四对线功能。

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* — 一般端点类，提供基本 LLDP 服务。
  - *第 2 类端点* — 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* — 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 层设备支持和设备信息管理功能。
- **PoE 设备类型** — 端口 PoE 类型；例如 PD。
- **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：
  - *已标记* — 指示网络策略是为已标记 VLAN 定义的。
  - *无标记* — 指示网络策略是为无标记 VLAN 定义的。
- **用户优先级** — 网络策略用户优先级。
- **DSCP** — 网络策略 DSCP。

步骤 3 在页面底部，单击 **LLDP 端口状态表**可在 **LLDP 端口状态表**中查看详情（请参阅端口设置）。

LLDP 邻居信息

“LLDP 邻居信息”页面包含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，系统会删除该信息。

查看 LLDP 邻居信息的步骤：

步骤 1 单击**管理** > **发现协议 - LLDP** > **LLDP 邻居信息**。

步骤 2 选择要显示 LLDP 邻居信息的接口。

此页面将为选定接口显示以下字段：

- **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 邻居设备机箱的标识符。
- **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** — 已发布的设备名称。
- **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 3 选择一个本地端口，然后单击**详情**。

“LLDP 邻居信息”页面包含以下字段：

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。
- **电源类型** — 连接到端口的 Pod 设备类型。
- **电源** — 端口电源。
- **电源优先级** — 端口电源优先级。
- **PD 请求的功率值** — Pod 设备请求的功率。
- **PSE 分配的功率值** — PSE 分配给 PD 的功率量。

通过 MDI 提供的 4 线电源

- **支持的 4 对 PoE** — 表示系统和端口支持启用 4 对电线（仅适用于拥有此硬件功能的具体端口）。
- **需要备用对检测/分类** — 表示需要 4 对电线。
- **PD 备用线对理想状态** — 表示 Pod 设备请求启用四对线功能。
- **PD 备用对工作状态** — 表示是启用还是禁用 4 对功能。

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）。
- **本地传输回应** — 表明本地链路伙伴反射远程链路伙伴的传输值。
- **本地接收回应** — 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 PD/PSE。
- **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

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

VLAN ID 表

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

协议 ID 表

- **协议 ID** — 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（已标记或无标记）。
- **用户优先级** — 网络策略用户优先级。
- **DSCP** — 网络策略 DSCP。

步骤 4 选择端口并单击 **LLDP 端口状态表**可在“LDP 端口状态表”中查看详情。

LLDP 统计信息

“LLDP 统计信息”页面会显示每个端口的 LLDP 统计信息。

查看 LLDP 统计信息的步骤：

步骤 1 单击**管理** > **发现协议 - LLDP** > **LLDP 统计信息**。

会为每个端口显示以下字段：

- **接口** — 接口标识符。
- **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**可查看最新统计信息。

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。

“LDP 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** > **发现协议 - LLDP** > **LLDP 过载**。

此页面包含每个端口的以下字段：

- **接口** — 端口标识符。
- **正在使用的字节总数** — 每个数据包中 LLDP 信息的总字节数。
- **剩余可用字节** — 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**。

此页面包含在该端口上发送的每个 TLV 的以下信息：

- **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 数据包已发送还是已过载。
- **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 数据包已发送还是已过载。
- **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 清单数据包已发送还是已过载。
- **总计**
  - *总数（字节）*— 每个数据包中 LLDP 信息的总字节数。
  - *剩余可用字节*— 每个数据包中，可用于发送其他 LLDP 信息的剩余可用字节总数。

发现协议 - CDP

本节介绍如何配置 CDP。

其中包含以下主题：

- CDP 属性
- CDP 接口设置
- CDP 本地信息
- CDP 邻居信息
- CDP 统计信息

CDP 属性

与 LLDP 相似，思科发现协议 (CDP) 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

以下是在设备上配置 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 CDP 接口设置页面按接口配置 CDP

步骤 3 如果使用自动智能端口检测 CDP 设备的功能，请在属性页面中启用 CDP。

有关如何使用 CDP 标识智能端口设备功能的说明，请参阅智能端口类型。

输入 CDP 一般参数的步骤：

步骤 1 单击**管理** > **发现协议 - CDP** > **属性**。

步骤 2 输入参数。

- **CDP 状态** — 选择启用设备上的 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** — 选择该选项后，设备会在支持 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** — 如果选择该选项，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 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 LLDP 数据包。可用的选项如下：
  - *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）。可用的选项如下：
  - *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）。可用的选项如下：
  - *MAC 地址* — 使用设备的 MAC 地址作为设备 ID。
  - *序列号* — 使用设备的序列号作为设备 ID。
  - *主机名* — 使用设备的主机名作为设备 ID。
- **源接口** — 要在帧 TLV 中使用的 IP 地址。可用的选项如下：
  - *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**。系统将定义 LLDP 属性。

CDP 接口设置

使用“接口设置”页面可以针对每个端口激活 CDP 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。

可以在 LLDP MED 端口设置页面中选择要通告的 LLDP-MED TLV。

定义 CDP 接口设置的步骤：

步骤 1 单击**管理** > **发现协议 - CDP** > **接口设置**。

此页面将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** — 在**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** — 对下文步骤 2 中说明的字段进行编辑。
- **CDP 本地信息详情** — 可跳转到 CDP 本地信息页面。
- **CDP 邻居信息详情** — 可跳转到 CDP 邻居信息页面。

步骤 2 选择一个端口，然后单击**编辑**。

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 当设备设置为向管理工作站发送陷阱时，以下三个字段属于可选字段。

- **系统日志语音 VLAN 不匹配** — 选择该选项可以在检测到语音 VLAN 不匹配时，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** — 选择该选项可以在检测到本征 VLAN 不匹配时，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** — 选择该选项可以在检测到双工模式信息不匹配时，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 输入相关信息，然后单击**应用**。端口设置将写入当前配置。

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”>“发现协议 - CDP”>“CDP 本地信息”。**

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（在设备地址 TLV 中通告）。

- **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。
- **可用电源 TLV**
  - *请求 ID* — 最后接收的电源请求 ID 会回应在电源请求 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 — 电源或管理电源等级更改

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* — 端口消耗的功率。
- *管理电源等级* — 显示供电器对 Pod 设备功耗 TLV 的请求。设备总是在此字段中显示“无偏好”。

- **通过 MDI 提供的 4 线电源 (UPOE) TLV**

  显示是否支持此 TLV。

  - *支持的 4 对 PoE* — 显示是否支持 PoE。
  - *需要备用对检测/分类* — 显示是否需要此分类。
  - *PD 备用对理想状态* — 显示 PD 备用对理想状态。
  - *PD 备用线对工作状态* — 显示 PSE 备用线对状态。

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，系统会删除该信息。

查看 CDP 邻居信息的步骤：

步骤 1 单击**管理** > **发现协议 - CDP** > **CDP 邻居信息**。

步骤 2 要选择过滤器，请单击**过滤器**复选框，选择本地接口，然后单击**执行**。

此时将触发过滤器，而且**清除过滤器**按钮会被激活。

步骤 3 单击**清除过滤器**可停止过滤。

“CDP 邻居信息”页面包含链路伙伴（邻居）的以下字段：

- **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 4 选择一个设备，然后单击**详情**。

此页面包含有关邻居的以下字段：

- **设备 ID** — 邻居设备的标识符。
- **系统名称** — 邻居设备 ID 的名称。
- **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。
- **应用** — 邻居上所运行应用的名称。
- **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。
- **电源请求** — 与端口连接的受电设备 (PD) 的电源请求。
- **电源请求列表** — 每个受电设备 (PD) 可以发送一系列（最多 3 个）受支持电源等级。
- **可用电源**

- *请求 ID* — 最后接收的电源请求 ID 会回应在电源请求 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* — 端口消耗的功率。
- *管理电源等级* — 显示供电器对 Pod 设备功耗 TLV 的请求。设备总是在此字段中显示“无偏好”。

• **通过 MDI 提供的 4 线电源**

- *支持的 4 对 PoE* — 表示系统和端口支持启用 4 对电线（仅适用于拥有此硬件功能的具体端口）。
- *需要备用对检测/分类* — 表示需要 4 对电线。
- *PD 备用线对理想状态* — 表示 Pod 设备请求启用四对线功能。
- *PD 备用线对工作状态* — 表示是启用还是禁用四对线功能。

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。

CDP 统计信息

“CDP 统计信息”页面会显示与从某端口收发的 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，请参阅发现协议 - 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 接口设置页面中进行。

查看 CDP 统计信息的步骤：

步骤 1 单击**管理 > 发现协议 - CDP > CDP 统计信息**。

系统会针对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。

步骤 2 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，请选择该接口并单击**清除接口计数器**。

10

端口管理

本节介绍端口配置、链路聚合和绿色以太网功能。

其中包含以下主题：

- 工作流程
- 端口设置
- 错误恢复设置
- 环回检测设置
- 链路聚合
- PoE
- 绿色以太网

工作流程

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. 如果设备支持并启用 PoE，则按“端口管理：PoE”中所述配置该设备。

端口设置

“端口设置”页面显示所有端口的全局设置和每端口设置。在这个页面上，您可以通过“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**。

显示所有端口的端口设置。

步骤 2 输入以下字段：

- **链路摆动预防** — 选择此选项可以最大限度减少网络中断。启用后，此命令会自动禁用出现链路摆动事件的端口。
- **巨型帧** — 选中此选项，可支持最大为 9 KB 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。注意，接收大于 9 KB 的数据包可能会导致接收端口关闭。此外，发送大于 10 KB 字节的数据包可能会导致接收端口关闭。

  要使巨型帧生效，必须在启用该功能之后重启设备。

步骤 3 单击**应用**以更新全局设置。

巨型帧配置更改*仅*在使用文件操作页面将运行时配置明确保存到启动配置文件之后才会生效，然后设备将重新启动。

步骤 4 要更新端口设置，请选择所需端口，然后单击**编辑**。

步骤 5 修改以下参数：

- **接口** — 选择端口编号。
- **端口说明** — 输入用户定义的端口名称或备注。

	注： **接口**和**端口说明**显示在主页中的**端口**列。

- **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、1000M（类型：铜缆）和 10G。
  - *组合端口* — 与铜质 CAT6a 电缆或 *SFP 光纤千兆接口相连的组合端口*。
  - /SX550X/SX350X

注 同时使用两个端口时，在组合端口中 SFP 光纤优先级较高。

- **管理状态** — 选择重启设备时端口必须处于“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。如果端口由于错误而关闭，将会显示错误描述。
- **链路状态 SNMP 陷阱** — 选择该选项可生成 SNMP 陷阱，用于通知端口链路状态的更改。
- **时间范围** — 选择该选项可在端口处于“启用”状态时启用时间范围。如果时间范围未处于活动状态，端口将处于关闭状态。如果已配置时间范围，则它仅会在人为启用端口时有效。
- **时间范围名称** — 选择指定时间范围的模板。不适用于 OOB 端口。如果尚未定义时间范围，请单击**编辑**转至时间范围页面。不适用于 OOB 端口。
- **运行时间范围状态** — 显示时间范围当前处于活动状态还是非活动状态。
- **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** — 选择端口的速度。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** —（仅在非 XG 端口上显示）选择端口双工模式。仅当禁用自动协商，并且端口速度会设置为 10M 或 100M 时，才能配置此字段。端口速度为 1G 时，始终处于全双工模式。可能的选项有：
  - *半双工* — 接口仅支持设备和客户端之间在某一时刻的单向传输。
  - *全双工* — 接口支持设备和客户端之间的同时双向传输。
- **运行双工模式** —（仅在非 XG 端口上显示）显示端口的当前双工模式。
- **自动通告** — 选择启用自动协商后，要由其通告的功能。

  注 并非所有选项都适用于所有设备。

  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（在 XG 设备上不显示）
  - *10 全双工* — 10 Mbps 速度和全双工模式（在 XG 设备上不显示）。

- *100 半双工* — 100 Mbps 速度和半双工模式（在 XG 设备上不显示）
- *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。
- **偏好模式** — 仅在启用自动协商时，系统才提供此选项。为自动协商操作选择接口的主从模式。请选择以下其中一个选项：
  - *从* — 以设备端口在自动协商过程中为从的偏好设置开始协商。
  - *主* — 以设备端口在自动协商过程中为主的偏好设置开始协商。
- **邻居通告** — 显示通过邻居设备（链路伙伴）通告的功能。
- **背压** —（仅支持非 XG 端口）在端口上选择“背压”模式（配合使用半双工模式），以降低设备拥塞时的数据包接收速度。选择此选项会禁用远程端口，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）。无法在组合端口上启用流量控制自动协商。
- **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。
  - *MDI* — 选择该选项可使用直通电缆将此设备连接到工作站。
  - *自动* — 选择该选项可将此设备配置为自动检测连接到其他设备的正确引出线。
- **运行 MDI/MDIX** — 显示当前的 MDI/MDIX 设置。
- **LAG 中的成员** — 如果端口为 LAG 的成员，则显示 LAG 编号；否则系统会将此字段留空。

步骤 6 单击**应用**。端口设置将写入当前配置文件中。

错误恢复设置

利用此页面，可以在自动恢复间隔过后，自动重新激活因错误情况而关闭的端口。

配置错误恢复设置的步骤：

步骤 1 单击**端口管理** > **错误恢复设置**。

步骤 2 输入以下字段：

- **自动恢复间隔** — 指定在端口关闭后进行自动错误恢复的时间延时（如果启用）。
- **端口假死自动恢复**
  - **端口安全** — 选择该选项可在端口因违反安全规则而关闭时，启用自动错误恢复。
  - **802.1x 单主机违反规则** — 选择该选项可在 802.1x 关闭端口时，启用自动错误恢复。
  - **ACL 拒绝** — 选择该选项可通过 ACL 操作启用自动错误恢复机制。
  - **STP 环回防护** — 在 STP 环回防护关闭端口时，启用自动恢复。
  - **环回检测** — 选择该选项可为环回检测关闭的端口启用错误恢复机制。
  - **风暴控制** — 选择该选项可为风暴控制关闭的端口启用错误恢复机制。
  - **链路摆动预防** — 选择此选项可以最大限度减少网络中断。启用后，此命令会自动禁用出现链路摆动事件的端口。

步骤 3 单击**应用**以更新全局设置。

手动重新激活端口的步骤：

步骤 1 单击**端口管理** > **错误恢复设置**。

将显示未激活端口及其**挂起原因**的列表。

步骤 2 选择要重新激活的接口。

步骤 3 单击**重新激活**。

环回检测设置

环回检测 (LBD) 通过将环路协议数据包传输到已启用环路保护的端口之外，来提供环路保护。当交换机发出环路协议数据包，然后又收到相同的数据包时，会关闭接收到该数据包的端口。

环回检测独立于 STP 运行。发现环路后，系统会将接收到环路的端口置于关闭状态。系统还将发送陷阱，并记录该事件。网络管理员可以定义检测间隔来设置 LBD 数据包之间的时间间隔。

环回检测协议可以检测以下环路情况：

- **短路** — 环回所有接收流量的端口。
- **直接多端口环路** — 交换机通过多个端口连接到其他交换机，同时 STP 会被禁用。
- **LAN 区段环路** — 交换机通过一个或多个端口连接到存在环路的 LAN 区段。

LBD 的工作方式

LBD 协议定期广播环回检测数据包。交换机在接收自己的 LBD 数据包时会检测环路。

要使 LBD 对端口有效，以下条件必须成立：

- 全局启用 LBD。
- 在端口上启用 LBD。
- 端口工作状态为运行。
- 端口处于 STP 转发/禁用状态（MSTP 实例转发状态，实例 0）。

LBD 帧通过最高优先级队列在启用 LBD 的端口上传输（如果是 LAG，则 LBD 会在 LAG 中的每个活动端口成员上传输）。

如果检测到环路，交换机将执行以下操作：

- 将接收端口或 LAG 设置为错误禁用状态。
- 发出相应的 SNMP 陷阱。
- 生成相应的系统日志消息。

默认设置和配置

默认情况下，环回检测为禁用状态。

与其他功能进行交互

如果在已启用环回检测的端口上启用 STP，该端口必须为 STP 转发状态。

配置 LBD

启用和配置 LBD 的步骤：

步骤 1 在“环回检测设置”页面中为整个系统启用环回检测（见下文）。

步骤 2 在“环回检测设置”页面中为访问端口启用环回检测（见下文）。

步骤 3 在错误恢复设置页面中为环回检测启用自动恢复。

配置环回检测的步骤：

步骤 1 单击**端口管理** > **环回检测设置**。

步骤 2 在**环回检测**全局字段中选择**启用**以启用此功能。

步骤 3 输入**检测间隔**。这是传输 LBD 数据包的间隔。

步骤 4 单击**应用**，以将配置保存到当前配置文件中。

系统还将对每个接口显示以下有关**环回检测状态**的字段：

- **管理** — 环回检测已启用。
- **运行** — 环回检测已启用，但在接口上无效。

步骤 5 在过滤器的**接口类型为**字段中选择是在端口上还是在 LAG 上启用 LBD。

步骤 6 选择要启用 LBD 的端口或 LAG，然后单击**编辑**。

步骤 7 在**环回检测状态**字段中为选定的端口或 LAG 选择**启用**。

步骤 8 单击**应用**，以将配置保存到当前配置文件中。

链路聚合

本节介绍如何配置 LAG。其中包含以下主题：

- 链路聚合概述
- 默认设置和配置
- 静态和动态 LAG 工作流程
- LAG 管理
- LAG 设置
- 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 可使两个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** — LAG 中的端口可以手动配置。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，将无法添加或删除 LACP 选项，直到编辑 LAG 并删除一个成员（应用之前可以添加回去）；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。

设备支持两种模式的负载平衡：

- **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 作为单个逻辑端口对待。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。

系列

设备支持 8 个 LAG，每个 LAG 中最多有 8 个端口。

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。
- 不得将某 LAG 中的端口分配给其他 LAG。
- 为静态 LAG 最多分配 8 个端口，并且最多有 16 个端口可以作为动态 LAG 的候选端口。
- 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，系统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。

默认设置和配置

默认情况下，端口不是 LAG 的成员，并且不能作为候选端口加入 LAG。

静态和动态 LAG 工作流程

手动创建 LAG 之后，将无法添加或删除 LACP，直到编辑 LAG 并删除一个成员，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。为 LAG 选择负载均衡算法。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**中选择端口并将其从该列表中移动到 **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。

LAG 管理

“LAG 管理”页面显示全局设置和每个 LAG 的设置。利用该页面，您还可以在“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 负载均衡算法的步骤：

步骤 1 单击**端口管理** > **链路聚合** > **LAG 管理**。

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**。负载均衡算法将保存至当前配置文件中。

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**。

系统将对每个 LAG 显示以下字段（仅介绍“编辑”页面中没有的字段）：

- **链路状态** — 显示端口处于连接还是中断状态。
- **活动成员** — LAG 中的活动端口。
- **备用成员** — 此 LAG 的候选端口。

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 8 个端口，为动态 LAG 最多分配 16 个端口。这些端口为候选端口。

步骤 3 单击**应用**。LAG 成员关系将保存至当前配置文件中。

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**。

屏幕上会显示系统中的 LAG。

步骤 2 选择一个 LAG，然后单击**编辑**。

步骤 3 为以下字段输入值：

- **LAG** — 选择 LAG ID 号。
- **LAG 类型** — 显示组成 LAG 的端口类型。
- **说明** — 输入 LAG 名称或备注。
- **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。
- **链路状态 SNMP 陷阱** — 选择该选项可生成 SNMP 陷阱，可通知 LAG 中端口链路状态的更改。
- **时间范围** — 选择该选项可在端口处于“启用”状态时启用时间范围。如果时间范围未处于活动状态，端口将处于关闭状态。如果已配置时间范围，则它仅会在人为启用端口时有效。
- **时间范围名称** — 选择指定时间范围的模板。如果尚未定义时间范围，请单击**编辑**转至时间范围页面。
- **运行时间范围状态** — 显示时间范围当前处于活动状态还是非活动状态。
- **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 中端口的速度。
- **运行 LAG 速度** — 显示 LAG 运行时的当前速度。

- **管理通告** — 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 可将其功能通告给邻居 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。

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 8 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，则系统会比较本地 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 8 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，链路控制端上的设备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。系统将忽略另一个设备（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。

无链路伙伴的 LACP

为了让 LACP 创建 LAG，应该针对 LACP 配置链路两端上的端口（即端口发送 LACP PDU 并处理已接收的 PDU）。

但是，存在暂时未针对 LACP 配置其中一个链路伙伴的情况。例如，链路伙伴处于正在使用自动配置协议接收配置的设备上。此设备的端口尚未配置为 LACP。如果 LAG 链路无法启用，则无法配置设备。双 NIC 网络引导计算机（例如 PXE）也会出现类似情况，它们只有在启动后才能接收 LAG 配置。

配置多个已配置 LACP 的端口后，如果在一个或多个端口中启用链路，但是链路伙伴没有对这些端口提供任何 LACP 响应，那么第一个连接的端口将添加到 LACP LAG 并处于激活状态（其他端口将成为非候选端口）。例如，通过这种方式，邻居设备便可以使用 DHCP 获取 IP 地址，并使用自动配置获取配置。

LACP 设置

使用 LACP 页面为 LAG 配置候选端口并针对每个端口配置 LACP 参数。

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（8 个）时，设备会从具有最高优先级的设备上的动态 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**。

步骤 2 输入 **LACP 系统优先级**。

步骤 3 选择一个端口，然后单击**编辑**。

步骤 4 为以下字段输入值：

- **端口** — 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。
- **LACP 超时** — 连续 LACP PDU 的发送与接收之间的时间间隔。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。

PoE

本节介绍如何使用 PoE 功能。

其中包含以下主题：

- 概述
- PoE 属性
- 设置
- 统计信息
- 绿色以太网概述

概述

PoE 设备为供电设备 (PSE)，可通过现有的铜质电缆为连接的 Pod 设备 (PD) 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。

特性

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 Pod 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

操作

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 Pod 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** — 设备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** — 设备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 设备

上行链路端口可充当具有 1 个或 2 个 PD 端口的受电设备 (PD)。在 8 端口设备上，最高端口为 PD（PD 端口不具备供电 [PSE] 功能）。如果有 2 个 PD 端口，建议将它们连接到一个 PSE 上。如果 PD 端口由相同的标准电源（都是 AF、都是 AT 或都是 60W PoE）供电，它们都将正常工作。

有关各种 SKU 及其 PoE 信息的更多信息，请参阅具有以太网供电功能的交换机

PoE 配置注意事项

配置 PoE 时应注意以下事项：

- PSE 可以提供的功率
- PD 实际尝试消耗的功率

可以进行以下配置：

- 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。系统会保留为端口限制模式配置的针对端口的功率值。

  注 在设备运行时将模式从“级别限制”更改为“端口限制”会强制 PD 重启，反之亦然。
- 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陷阱，以及生成陷阱时 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 从设备请求超过所配置的功率分配所允许的功率（不论设备是类别限制模式还是端口限制模式），设备将：

- 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 SNMP 陷阱

PoE 属性

注 本节仅适用于支持 PoE 的设备。

“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 陷阱。

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。

在设备上配置 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**。

步骤 2 为以下字段输入值：

- **供电模式** — 选择以下选项中的一个：
  - *类别限制* — 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。
  - *端口限制* — 由用户配置针对每个端口的最大功率限制。

  注 从“端口限制”更改为“级别限制”时（反之亦然），必须禁用 PoE 端口，并更改功率配置后再次启用。
- **陷阱** — 启用或禁用陷阱。如果已启用陷阱，您还必须启用 SNMP，并配置至少一个 SNMP 通知接收设备。
- **功率陷阱阈值** — 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，便会发出警报。
- **软件版本** — 显示 PoE 芯片的软件版本。

对于设备或堆叠的所有单元，系统显示以下计数器：

- **标称功率** — 设备可以为连接的所有 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。
- **PSE 芯片集和硬件版本** — PoE 芯片集和硬件版本号。

步骤 3 单击**应用**，保存 PoE 属性。

设置

“设置”页面会显示关于在接口上启用 PoE 以及当 PoE 模式为“端口限制”时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。

注 PoE 可以在设备上针对某一特定时间段配置 PoE。使用此功能，可以为每个端口定义一周中哪几天以及每天哪几个小时启用 PoE。如果未指定时间范围，PoE 将处于禁用状态。若要使用此功能，必须首先在时间范围页面定义一个时间范围。

此页面将每端口的功率限制为指定瓦数。要使这些设置生效，系统必须处于 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。

PoE 优先级示例：

假设：一个 48 端口设备提供 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。设备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 的设备型号以及可向 PoE 端口分配的最大功率说明，请参阅系统设置。

配置 PoE 端口限制设置的步骤：

步骤 1 单击**端口管理 > PoE > 设置**。

系统此时将显示端口以及相关 PoE 信息。“编辑”页面中会介绍除以下字段外的相关字段：

- **管理功率分配 (mW)** — 输入可分配的功率。
- **工作状态** — 显示端口上的 PoE 当前是否处于活动状态。
- **PoE 标准** — 显示受支持的 PoE 类型，例如 60W PoE 和 802.3 AT PoE。

步骤 2 选择一个端口，然后单击**编辑**。

步骤 3 输入以下字段：

- **接口** — 选择要配置的端口。
- **管理状态** — 在端口上启用或禁用 PoE。
- **时间范围** — 选择该选项可启用端口上的 PoE。
- **时间范围名称** — 如果“时间范围”已启用，请选择要使用的时间范围。时间范围的定义见时间范围页面。要定义新的时间范围，请单击**编辑**。
- **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）。
- **强制连接四对线** — 选择该选项将强制使用备用线对供电。该选项允许对不支持 CDP/LLDP PoE 协商的 PD 使用 60 瓦 PoE。

- **最大功率分配** — 仅当在“PoE 属性”页面中将供电模式设置为“功率限制”才会显示该字段。显示在此端口上所允许的最大功率。
- **协商功率** — 分配给设备的功率。
- **功率协商协议** — 用于确定协商功率的协议。
- **功耗** — 显示在“设置”（类别限制）中分配的功率（以毫瓦为单位）。
- **类别** — 显示产生的功率类别。

（类别限制）“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。

注 PoE 可以在设备上针对某一特定时间段配置 PoE。使用此功能，可以为每个端口定义一周中哪几天以及每天哪几个小时启用 PoE。如果未指定时间范围，PoE 将处于禁用状态。若要使用此功能，必须首先在*时间范围*页面定义一个时间范围。

本页面根据所连接 PD 的类别限制每个端口的功率。要使这些设置生效，系统必须处于 PoE 类别限制模式。该模式在“PoE 属性”页面配置。

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

有关支持 PoE 的设备型号以及可向 PoE 端口分配的最大功率说明，请参阅系统设置。

配置 PoE 类别限制设置的步骤：

步骤 1 单击**端口管理 > PoE > 设置（类别限制）**。

系统此时将显示端口以及相关 PoE 信息。“编辑”页面中会介绍除以下字段外的相关字段：

- **PoE 标准** — 显示受支持的 PoE 类型，例如 60W PoE 和 802.3 AT PoE。
- **工作状态** — 显示端口上的 PoE 当前是否处于活动状态。

步骤 2 选择一个端口，然后单击**编辑**。

步骤 3 为以下字段输入值：

- **接口** — 选择要配置的端口。
- **管理状态** — 在端口上启用或禁用 PoE。

- **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。
- **强制连接四对线** — 启用此功能后将提供增强的电源。
- **功耗** — 以毫瓦为单位显示分配的功率量设置（类别限制）
- **类别** — 显示设备类别，用于指示设备的最大功率等级：

类别	设备端口提供的最大功率
0	30.0 瓦特
1	4.0 瓦特
2	7.0 瓦特
3	15.4 瓦特
4	30.0 瓦特

- **最大功率分配** — 仅当在“PoE 属性”页面中将供电模式设置为“功率限制”才会显示该字段。显示在此端口上所允许的最大功率。
- **协商功率** — 分配给设备的功率。
- **功率协商协议** — 用于确定协商功率的协议。

步骤 4 单击**应用**。端口的 PoE 设置将写入当前配置文件。

统计信息

此页面显示功耗趋势，即一段时间内的平均功耗。此功能对监控和调试 PoE 行为非常有用。

设备会存储 PoE 端口在一段时间内的功耗值（以瓦特为单位）。这让计算和显示指定天/周/月的 PoE 平均功耗，以及检测功耗趋势成为可能。提供的信息既包括针对每个接口的信息，也包括针对设备整体的信息。

系统每 1 分钟获取一次 PoE 功耗读数。每日、每周和每月统计信息保存在闪存中，因此在重启后仍然可用。

每端口/设备的平均 PoE 功耗示例如下：

一段时间内的所有 PoE 功耗数据的总和/取样期间的分钟数。

查看设备 PoE 功耗趋势以及定义视图设置的步骤：

步骤 1 单击**端口管理 > PoE > 统计信息**。

步骤 2 在以下字段中选择端口：**接口**字段。

步骤 3 选择**刷新速率**。

步骤 4 将针对选定接口显示以下字段：

功耗历史记录

- **过去一小时的平均功耗** — 所有 PoE 功耗数据在过去一小时内的平均值。
- **过去一天的平均功耗** — 所有 PoE 功耗数据在过去一天内的平均值。
- **过去一周的平均功耗** — 所有 PoE 功耗数据在过去一周内的平均值。

PoE 事件计数器

- **过载计数器** — 检测到发生过载情形的次数。
- **短路计数器** — 检测到发生短路情形的次数
- **拒绝供电计数器** — 检测到发生拒绝供电情形的次数
- **无电源计数器** — 检测到发生无电源情形的次数
- **无效签名计数器** — 检测到发生无效签名情形的次数

在主页上可以执行以下操作：

- **清除事件计数器** — 清除显示的事件计数器。
- **查看所有接口统计信息** — 针对所有接口显示以上统计信息。
- **查看接口历史记录图形** — 以图形格式显示计数器。
- **刷新** — 刷新显示的计数器。

单击**查看所有接口统计信息**可以执行以下操作：

- **清除事件计数器** — 清除显示的事件计数器。
- **查看接口统计信息** — 针对选定的接口显示以上统计信息
- **查看接口历史记录图形** — 针对选定的接口，以图形格式显示计数器
- **刷新** — 刷新显示的计数器。

单击**查看接口历史记录图形**可以执行以下操作：

- **查看接口统计信息** — 针对选定的接口，以表格形式显示图形统计信息。以小时、天、周或年为单位，输入**时限**。
- **查看所有接口统计信息** — 针对所有接口，以表格格式显示以上统计信息。以小时、天、周或年为单位，输入**时限**。
- **清除事件计数器** — 清除计数器。

绿色以太网

本节介绍旨在节省设备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
- 属性
- 端口设置

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。默认情况下，此模式为禁用状态。
- **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。如果万兆端口的电缆短于 30 米，其他类型端口的电缆短于 50 米，设备将使用较少电能来通过电缆发送帧，从而节省电量。仅在 RJ45 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，此模式为禁用状态。

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 GE 或 FE 端口上，如果启用了 EEE，则必须禁用短距模式。同样，用户必须先禁用 EEE，才能启用短距模式。在 XG 接口上，短距始终处于启用状态，并且不对 EEE 设置进行限制。

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 会消耗电能。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。系统不会显示 EEE 的节能量。

通过禁用端口 LED 实现节能

通过禁用端口 LED 功能，可以节约设备 LED 消耗的电量。由于设备经常处于闲置状态，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。

端口 LED 可在属性页面上禁用。

802.3az 节能以太网功能

本节介绍 802.3az 节能以太网 (EEE) 功能。

其中包含以下主题：

- 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。

802.3az EEE 不支持带外端口。

注 远程链路伙伴状态仅在链路速度为 1G 或 10G 时显示。

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（设备端口和连接的设备）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 或 10G，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 1 GB，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。
- 如果将 GE 端口上的端口速度更改为 10 MB，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 **802.3 节能以太网 (EEE)** 已在属性页面中全局启用（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 要查看本地设备的 802.3az EEE 相关信息，请打开 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 信息，请打开 LLDP 邻居信息页面，查看“802.3 节能以太网 (EEE)”部分中的信息。

属性

“属性”页面显示设备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**。

步骤 2 为以下字段输入值：

- **电量检测模式** — 单击相应复选框可启用此模式。某些 XG 设备不支持此设置。
- **短距** —（针对非 XG 设备）单击相应复选框可启用此功能。
- **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。
- **802.3 节能以太网 (EEE)** — 全局启用或禁用 EEE 模式。

步骤 3 单击**重置节能计数器** — 重置“累计节省的电量”信息。

步骤 4 单击**应用**。绿色以太网属性将写入当前配置文件。

端口设置

“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。对于要在端口上执行的环保以太网模式，必须在属性页面中全局激活相应模式。

系统仅显示具有 GE 端口的设备的 EEE 设置。系统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。

在 XG 设备上，短距和电量检测功能始终处于启用状态，且无法禁用。在具有 FE 或 GE 端口的设备上，这些功能既可启用也可禁用。

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**。

“端口设置”页面显示以下字段：

- **全局参数状态** — 显示以下字段：
  - *电量检测模式* — 是否启用此模式。
  - *短距模式* — 是否启用此模式。
  - *802.3 节能以太网 (EEE) 模式* — 是否启用此模式。

对于每个端口，系统将会列出以下字段：

注 某些字段在某些 SKU 上可能不会显示。

- **端口** — 端口号。
- **电量检测** — 有关电量检测功能的端口状态：
  - 管理 — 显示是否启用电量检测功能。
  - 工作 — 显示电量检测功能当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。
  - 原因 — 显示电量检测功能在启用后仍无法运行的原因。
- **短距** — 有关短距功能的端口状态：
  - *管理* — 显示是否启用了短距。
  - *运行* — 显示短距当前是否正在本地端口上运行。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。
  - *原因* — 显示短距即使已启用也不运行的原因。
  - *电缆长度* — 电缆的长度。
- **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。

步骤 2 选择一个**端口**，然后单击**编辑**。

步骤 3 （仅适用于非 XG 设备）选择在该端口上启用还是禁用**电量检测**模式。

步骤 4 （仅适用于非 XG 设备）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 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 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。

11

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
- 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
- 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。

智能端口宏可按宏名称或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，并与设备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。
- 分别在发现协议 - LLDP 和发现协议 - 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设备的方法，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。设备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。
  - 重启设备。
  - 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。全局宏对设备进行全局配置，而智能端口宏的范围限于所应用的接口。

要查找宏源，在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（例如：printer）
- no_macro_name（例如：no_printer，智能端口宏打印机的反智能端口宏）

有关各设备类型的内置智能端口宏的列表，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，设备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模板将应用到接口（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，设备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，设备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生成的配置将被删除。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

设备根据 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
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

LLDP 功能到智能端口类型的映射（续）

功能名	LLDP 位	智能端口类型
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

设备通过连接设备在其 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该设备连接，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，请分别参阅发现协议 - LLDP 和发现协议 - 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、接口关闭以及设备重启（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、接口关闭或设备重启后，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，您可在接口设置页面检查故障点，您可在接口设置页面修正错误之后，重置端口并重新应用宏。

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

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：要在设备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 要在设备上启用自动智能端口功能，请打开属性页面。将**管理自动智能端口**设为**启用**或**通过语音 VLAN 启用**。

步骤 2 选择是否要使设备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 要在接口上启用智能端口功能，请打开接口设置页面。

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。

步骤 1 打开类型设置页面。

步骤 2 选择智能端口类型。

步骤 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。

步骤 4 单击**编辑**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。

步骤 5 在“编辑”页面中，修改字段。

步骤 6 如果参数已更改，单击**应用**返回宏。

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。请参考下文中的故障排除提示。

步骤 4 单击**编辑**。将显示一个新窗口，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，请分别参阅发现协议 - LLDP 和发现协议 - CDP 部分。

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**。

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。可用的选项如下：
  - *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。
- **运行自动智能端口** — 显示自动智能端口状态。
- **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**。这将在设备上设置全局智能端口参数。

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**。

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**。

步骤 4 输入各个字段。

- **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。

步骤 5 单击**应用**可将更改保存到当前配置中。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。

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，将其重新应用到所有接口或以下其中一种接口类型：交换机、路由器和接入点。单击**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，在设备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。您必须熟悉设备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**。

要重新应用最后一个与一组接口管理的智能端口宏，请单击以下其中一个选项：

- **所有交换机、路由器和无线接入点** — 将宏重新应用到所有接口。
- **所有交换机** — 将宏重新应用到所有定义为交换机的接口。
- **所有路由器** — 将宏重新应用到所有定义为路由器的接口。
- **所有无线接入点** — 将宏重新应用到所有定义为接入点的接口。

  要重新应用与特定接口关联的智能端口宏，请选择此接口（必须为 UP），单击**重新应用**，将应用到接口的最后一个宏进行重新应用。

  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*相同的智能端口类型*。
- 选择*未知*。
- 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 选择一个接口并单击**编辑**。

步骤 2 输入各个字段。

- **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，即使接口关闭或设备重启，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

```
[desktop]
#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: The untag VLAN which will be
configured on the port
#                        $max_hosts: The maximum number of allowed devices on
the port
#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

```
[printer]
#macro description printer
#macro keywords $native_vlan
#
#macro key description: $native_vlan: The untag VLAN which will be configured
on the port
#Default Values are
#$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
#
@
```

访客

```
[guest]
#macro description guest
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
#Default Values are
#$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

```
[server]
#macro description server
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: The untag VLAN which will be
configured on the port
#                        $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$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

```
[host]
#macro description host
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: The untag VLAN which will be
configured on the port
#                        $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$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:  $native_vlan: The untag VLAN which will be
configured on the port
#Default Values are
#$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 No 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: The untag VLAN which will be
configured on the port
#                          $voice_vlan: The voice VLAN ID
#                        $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$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:   $voice_vlan: The voice VLAN ID
#
#Default Values are
#$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: The untag VLAN which will be
configured on the port
#                          $voice_vlan: The voice VLAN ID
#                        $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$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:   $voice_vlan: The voice VLAN ID
#
#Default Values are
#$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

```
[switch]
#macro description switch
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
#                        $voice_vlan: The voice 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: The voice VLAN ID
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

路由器

```
[router]
#macro description router
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
#                        $voice_vlan: The voice VLAN ID
#
#Default Values are
#$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: The voice 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

```
[ap]
#macro description ap
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
```

12

VLAN 管理

本节包含以下主题：

- 常规 VLAN
- GVRP 设置
- 语音 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

系统会使用 1 到 4094 之间的值为每个 VLAN 配置一个唯一的 VLAN ID (VID)。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 的非标记成员。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 的标记成员。一个端口可以仅是一个非标记 VLAN 的成员，也可以是多个标记 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 标记帧，则系统会将一个 4 字节的 VLAN 标记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 优先级标记 (VPT)。有关 VPT 的详情，请参阅服务质量。

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，则系统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，系统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 的标记成员或非标记成员。

出站端口：

- 如果出站端口是目的 VLAN 的标记成员，并且原始帧不包含 VLAN 标记，则系统会为此帧添加 VLAN 标记。
- 如果出站端口是目的 VLAN 的非标记成员，并且原始帧包含 VLAN 标记，则系统会删除此帧的 VLAN 标记。

VLAN 角色

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：有关详细信息，请参阅“语音 VLAN”一节。
- 访客 VLAN：在属性页面中设置。
- 默认 VLAN：VLAN1。
- 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。该设备是一个提供商网桥，支持基于端口、已添加 c 标记的服务接口。

设备使用 QinQ 为流量添加称为服务标记 (S-tag) 的 ID 标记，然后将数据包转发到提供商网络中。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。利用 S-tag，系统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 是在接口设置页面中启用的。

常规 VLAN

本节介绍用于配置各种 VLAN 的 GUI 页面。本节将介绍以下内容：

- 常规 VLAN 概述
- VLAN 设置
- 接口设置
- 端口到 VLAN
- 端口 VLAN 成员关系

常规 VLAN 概述

VLAN 配置工作流程

配置 VLAN 的步骤：

步骤 1 按照 VLAN 设置一节的说明，创建所需 VLAN。

步骤 2 按照*接口设置*一节中的说明，根据需要设置 VLAN 相关端口的配置，并在接口上启用 QinQ。

步骤 3 按照端口到 VLAN 一节或端口 VLAN 成员关系一节的说明，将接口分配给 VLAN。

步骤 4 按端口 VLAN 成员关系一节的说明，查看所有接口的目前 VLAN 端口成员关系。

默认 VLAN 设置

设备自动创建 VLAN 1 作为默认 VLAN，所有端口的默认接口状态为“访问”并且会将所有端口配置为默认 VLAN 的未添加标签的成员。

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，所有端口都是它的非标记成员。
- 该 VLAN 无法删除。
- 无法为该 VLAN 指定标签。

- 它会自动用作已启用 OUI 的语音 VLAN 的语音 VLAN。
- 如果某端口不再是任何 VLAN 的成员，则设备会自动将该端口配置为默认 VLAN 的非标记成员。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。

VLAN 设置

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。

250 系列设备最多可支持 256 个 VLAN（包括默认 VLAN）。

系统会使用 1 到 4094 之间的值为每个 VLAN 配置一个唯一的 VID。设备会将 VID 4095 保留为丢弃 VLAN。所有分类为属于丢弃 VLAN 的数据包都会在入口处被丢弃，而不会被转发到端口。

创建 VLAN 的步骤：

步骤 1 单击 **VLAN 管理** > **VLAN 设置**。

系统此时将显示所有已定义 VLAN 的信息。字段将在下面的**添加**页面下进行定义。以下字段不在**添加**页面上。

- **发起人** — VLAN 的创建方式
  - *静态* — VLAN 为用户定义。
  - *默认* — VLAN 为默认 VLAN。

步骤 2 单击**添加**来添加一个或多个新 VLAN。

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** 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。

注 部分 VLAN 必须供系统内部使用，因此用户无法创建或配置这些 VLAN。供系统内部使用的 VLAN 如下：

- 供每个 IP 接口使用的一个 VLAN，该 VLAN 直接在以太网端口或端口通道 (LAG) 上定义。
- 供每个 IPv6 隧道使用的一个 VLAN
- 供 802.1x 使用的一个 VLAN

用于 IPv6 和 802.1x 隧道的 VLAN 是预先分配的，而用于以太网端口/端口通道 IP 配置的 VLAN 是在应用 IP 配置时分配的。内部 VLAN 从最高的可用 VLAN（默认为 VLAN 4094）开始分配。

步骤 4 为新 VLAN 添加以下字段。

- **VLAN 接口状态** — 选择该选项可关闭 VLAN。在此状态下，VLAN 不会接收来自更高级别的消息，或者向更高级别传输消息。例如，如果您关闭已配置 IP 接口的 VLAN，至 VLAN 的桥接会继续，但是交换机无法在 VLAN 上传输和接收 IP 流量。
- **链路状态 SNMP 陷阱** — 选择该选项可生成链路状态 SNMP 陷阱。

步骤 5 单击**应用**，创建 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**。

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

步骤 4 为以下字段输入值：

- **接口** — 选择端口/LAG。
- **交换机端口模式** — 选择第 2 层或第 3 层。

- **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 的标记成员或非标记成员。
  - *访问* — 接口为单个 VLAN 的未添加标签的成员。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 的未添加标签的成员，或者作为零个或更多 VLAN 的添加标签的成员。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)。如果设备拥有一个或更多客户端口，它将处于 Q-in-Q 模式。请参阅 QinQ。
- **帧类型** —（仅在“一般”模式下提供）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。可能的值包括：
  - *全部接受* — 接口接受所有类型的帧：非标记帧、标记帧和添加优先级标记的帧。
  - *只接受已标记项* — 接口仅接受添加标记的帧。
  - *只接受非标记项* — 接口仅接受非标记帧和优先级帧。
- **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。

端口到 VLAN

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。系统将为该端口分配 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）之间的非标记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 发送非标记数据包或从 VLAN 接收非标记数据包，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。

标记 VLAN 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 的帧发送到非标记终端节点。

使用“端口到 VLAN”页面显示和配置特定 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**。

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 的端口模式都会显示为从接口设置页面配置的目前端口模式（“访问”、“中继”、“一般”“专用主机”、“专用混杂”或“客户”）。

每个端口或 LAG 均将与其对 VLAN 的目前注册一起显示。

系统将显示以下字段：

- **VLAN 模式** — 显示 VLAN 中的端口的端口类型。
- **成员关系类型**：请选择以下其中一个选项：
  - *已禁止* — 不允许接口加入 VLAN（即使通过 GVRP 注册也不行）。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。
  - *已标记* — 接口是 VLAN 的已标记成员。
  - *非标记* — 接口为 VLAN 的非标记成员。系统会将非标记 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 3 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。

端口 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，端口标记有大写的 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。

注 支持 VLAN IS 模式。这意味着可提前为各种 VLAN 模式配置端口 VLAN 成员关系。当端口进入特定 VLAN 模式时，配置进入活动状态。更改为不同的模式时，保存更改前的模式设置，如果在接口上重新激活模式，将再次应用这些设置。

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**。

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。

步骤 4 为以下字段输入值：

- **接口** — 选择端口或 LAG。
- **当前 VLAN 模式** — 显示在接口设置页面中选的端口 VLAN 模式。
- **访问模式成员关系（活动）**
  - *访问 VLAN ID* — 当端口处于“访问”模式时，它是此 VLAN 的成员。

- **中继模式成员关系**
  - *本征 VLAN ID* — 当端口处于“中继”模式时，它将是此 VLAN 的成员。
  - *添加标签的 VLAN* — 当端口处于“中继”模式时，它将是这些 VLAN 的成员。可用的选项如下：

    所有 VLAN — 当端口处于“中继”模式时，它将是所有 VLAN 的成员。

    用户定义 — 当端口处于“中继”模式时，它将是在此处输入的 VLAN 的成员。
- **常规模式成员关系**
  - *未添加标签的 VLAN* — 当端口处于“一般”模式时，它将是此 VLAN 的未添加标签的成员。
  - *添加标签的 VLAN* — 当端口处于“一般”模式时，它将是这些 VLAN 的添加标签的成员。
  - *已禁止 VLAN* — 当端口处于“一般”模式时，不允许接口加入 VLAN（即使通过 GVRP 注册也不行）。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
  - *一般 PVID* — 当端口处于“一般”模式时，它将是这些 VLAN 的成员。
- **客户模式成员关系**
  - *客户 VLAN ID* — 当端口处于“客户”模式时，它将是此 VLAN 的成员。

步骤 5 选择某个端口，然后单击**详情**查看以下字段：

- **管理 VLAN** — 已为这些 VLAN 配置端口。
- **运行 VLAN** — 目前端口是这些 VLAN 的成员。

步骤 6 单击**应用**（适用于加入 VLAN）。将修改设置，并将其写入当前配置文件中。

GVRP 设置

可识别 VLAN 的邻居设备可使用通用 VLAN 注册协议 (GVRP) 来互相交换 VLAN 信息。GVRP 以通用属性注册协议 (GARP) 为基础，并通过桥接网络传递 VLAN 信息。

要在接口上启用 GVRP，则必须在“一般”模式下进行配置。

当端口使用 GVRP 加入 VLAN 时，除非在端口 VLAN 成员关系页面中明确禁止，否则会将该端口作为已标记的动态成员添加到 VLAN 中。如果 VLAN 不存在，则会在为该端口启用动态 VLAN 创建时动态创建 VLAN（在 GVRP 设置页面中）。

必须在全局并在每个端口上激活 GVRP。激活 GVRP 后，GARP 会传输和接收 GARP 数据包数据单位 (GPDU)。不会传递已定义但未激活的 VLAN。要传递 VLAN，它必须至少在一个端口上为活动状态。

默认情况下，系统将在全局和端口上禁用 GVRP。

GVRP 设置

为接口定义 GVRP 设置的步骤：

步骤 1 单击 **VLAN 管理** > **GVRP 设置**。

步骤 2 选择 **GVRP 全局状态**以全局启用 GVRP。

步骤 3 单击**应用**设置全局 GVRP 状态。

步骤 4 选择接口类型（端口或 LAG），然后单击**转至**，显示该类型的所有接口。

步骤 5 要为某端口定义 GVRP 设置，请选择该端口，然后单击**编辑**。

步骤 6 为以下字段输入值：

- **接口** — 选择要编辑的接口（端口或 LAG）。
- **GVRP 状态** — 选择该选项将在该接口上启用 GVRP。
- **动态 VLAN 创建** — 选择该选项将在该接口上启用动态 VLAN 创建。
- **GVRP 注册** — 选择该选项将在该接口上启用使用 GVRP 进行的 VLAN 注册。

步骤 7 单击**应用**。系统将修改 GVRP 设置，并将其写入当前配置文件中。

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
- 语音 VLAN 配置
- 电话 OUI

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。

设备始终作为可识别 VLAN 交换机运行。

该设备支持单一语音 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，如果该设备处于“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

设备支持两种动态语音 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。

  当设备处于“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，如果设备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，设备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。

设备希望附加语音设备向语音 VLAN 发送标记数据包。在语音 VLAN 同时也是本征 VLAN 的端口上，也可发送语音 VLAN 非标记数据包。

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，CDP、LLDP、LLDP-MED、自动智能端口模式以及基本 QoS 连同信任 DSCP 处于启用状态。所有端口都是默认 VLAN 1（默认的语音 VLAN）的成员。

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 的安装或者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 如果将设备连接至一台思科 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。设备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，设备将语音 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，设备将自动创建该语音 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。

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，设备会定期发送 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 + 台式机。

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，并使用您自己的网络策略。

若在 OUI 模式下，设备可以根据 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。设备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

设备的自动语音 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 按发现协议 - LLDP 和发现协议 - CDP 节中所述，分别配置 LLDP/CDP。

步骤 8 使用接口设置页面启用相关端口上的智能端口特性。

注 第 7 步和第 8 步是可选的，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 表页面中配置电话 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。

语音 VLAN 配置

本节介绍如何配置语音 VLAN。其中包含以下主题：

- 语音 VLAN 属性
- 自动语音 VLAN 设置
- 电话 OUI

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**。

- **语音 VLAN 设置（管理状态）**框中将显示设备上配置的语音 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 输入以下**管理状态**字段的值：

- **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 中的更改会导致设备将管理语音 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*。

显示以下**运行状态**字段：

- **语音 VLAN ID** — 语音 VLAN。

- **CoS/802.1p** — 被 LLDP-MED 用作语音网络策略的值。详情请参阅*管理 > 发现 > LLDP > LLDP MED 网络策略*。

- **DSCP** — 被 LLDP-MED 用作语音网络策略的值。

显示以下**动态语音 VLAN 设置**字段：

- **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，将立即激活设备上的自动语音 VLAN，并使之生效。
  - *通过外部语音 VLAN 触发器* — 只有当设备检测到某设备通告语音 VLAN 时，才能激活设备上的自动语音 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。

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 的标识符。
- **源类型** — 显示根设备发现的语音 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** — 设备的基本 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 本地源表会显示设备上配置的语音 VLAN，以及由直连邻居设备通告的任意语音 VLAN 配置。其中包含以下字段：

- **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”，则表示设备自身已完成配置。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。可用的选项如下：
  - *默认* — 设备上的默认语音 VLAN 配置
  - *静态* — 设备上用户定义的语音 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** — 显示设备是否已使用此语音 VLAN。可用的选项如下：
  - *是* — 设备使用此语音 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

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：

- 电话 OUI 表
- 电话 OUI 接口

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**。

“电话 OUI”页面包含以下字段：

- **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**，使用这些值更新设备的当前配置。

系统此时将显示电话 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**恢复默认 OUI** 可删除所有用户创建的 OUI，而仅在表中保留默认的 OUI。恢复完成之前，OUI 信息可能不准确。这可能需要几秒钟时间。几秒钟过后，通过退出并重新进入页面来刷新页面。

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**恢复默认 OUI**，系统将恢复已知 OUI。

步骤 4 要添加新的 OUI，请单击**添加**。

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**。系统会将 OUI 添加至电话 OUI 表。

电话 OUI 接口

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，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**。

“电话 OUI 接口”页面包含所有接口的语音 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**。

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（主页面中的电话 OUI QoS 模式）** — 选择以下选项之一：
  - *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

生成树

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

- STP 模式
- STP 状态和全局设置
- STP 接口设置
- RSTP 接口设置
- 多生成树概述
- MSTP 属性
- VLAN 到 MSTP 实例
- MSTP 实例设置
- MSTP 接口设置

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径时，产生环路。环路会导致交换机无限制地中继相同数据包，从而使数据包无法到达目标地址并造成广播/组播风暴以及网络效率降低。

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。

设备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。当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，本协议最有效。默认情况下，系统会启用 RSTP。
- 多 STP (MSTP) – MSTP 以 RSTP 为基础。MSTP 会检测第 2 层环路，并尝试通过阻止所涉及的端口传输流量来缓解环路造成的影响。由于在每个第 2 层域上都存在环路，会发生端口被阻塞以消除 STP 环路的情况。向未被阻塞的端口转发流量，不向被阻塞的端口转发流量。这不是高效的带宽使用，因为被阻塞端口始终得不到利用。
- MSTP 将通过启用多个 STP 实例来解决此问题，以便可以分别在每个实例中检测环路及缓解环路造成的影响。这使得端口对一个或多个 STP 实例被阻塞，但对于其他 STP 实例不会被阻塞。如果不同的 VLAN 与不同的 STP 实例相关联，则根据关联的 MST 实例的 STP 端口状态中继流量。更高的带宽使用率结果。

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、RSTP 或 MSTP 的参数。

分别使用“STP 接口设置”页面、“RSTP 接口设置”页面和“MSTP 属性”页面配置每种模式。

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**。

步骤 2 输入参数。

全局设置：

- **生成树状态** — 选择该选项可在设备上启用。
- **STP 环回防护** — 选择该选项可在设备上启用环回防护。
- **STP 运行模式** — 选择一种 STP 模式。
- **BPDU 处理** — 选择在端口或设备上禁用 STP 时如何管理网桥协议数据单元 (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，系统将使用它们的 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。
- **间隔时间** — 设置根网桥在配置消息之间等待的时间间隔（以秒为单位）。
- **最长不过期时间** — 设置设备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 STP 接口设置。

指定的根：

- **网桥 ID** — 网桥优先级与设备的 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。

STP 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**。

步骤 2 选择一个接口并单击**编辑**。

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”，以便在主机连接到设备后，该设备将端口设置为快速链路模式，或者在连接到其他设备后，将端口设置为常规 STP 端口。这有助于避免形成环路。

  - 边缘端口在 MSTP 模式中不工作。
- **BPDU 处理** — 选择在端口或设备上禁用 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* — 选择该选项以使用在 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，并且必须是 16 的倍数。
- **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。

RSTP 接口设置

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**。

步骤 2 启用 **RSTP**。

步骤 3 单击**生成树** > **RSTP 接口设置**。系统此时将显示“RSTP 接口设置”页面：

步骤 4 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 5 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，并且如果存在，可确定该链路伙伴是否已迁移到 RSTP 或 MSTP。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 或 MSTP，设备将相应地使用 RSTP 或 MSTP 与其进行通信。

步骤 6 选择一个接口，并单击**编辑**。

步骤 7 输入以下参数：

- **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。
  - *已启用* — 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）。
  - *已禁用* — 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 自动确定设备状态。
- **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* — 提供从根端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。
  - 丢弃 — 端口目前丢弃/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 8 单击**应用**。将更新当前配置文件。

多生成树概述

多生成树协议 (MSTP) 用于区分各种域（位于不同 VLAN 上）之间的 STP 端口状态。例如，如果端口 A 由于 VLAN A 上存在环路而在一个 STP 实例中被阻塞，则可以在另一个 STP 实例中将该端口置于转发状态。使用“MSTP 属性”页面，您可以定义全局 MSTP 设置。

配置 MSTP 的步骤：

步骤 1 按 STP 状态和全局设置页面所述将“STP 运行模式”设置为 MSTP。

步骤 2 定义 MSTP 实例。每个 MSTP 实例均会进行计算并构建一个无环路拓扑，从映射到该实例的 VLAN 桥接数据包。请参阅 VLAN 到 MSTP 实例一节。

步骤 3 决定哪个 MSTP 实例在哪个 VLAN 中处于活动状态，并将这些 MSTP 实例与相应的 VLAN 相关联。

步骤 4 通过以下操作配置 MSTP 属性：

- *MSTP 属性*
- MSTP 实例设置
- *VLAN 到 MSTP 实例*

MSTP 属性

全局 MSTP 会为每个 VLAN 组配置一个单独的生成树，并在每个生成树实例内保留一条备用路径，所有其他可能的路径全部阻塞。使用 MSTP，可以构建可运行多 MST 实例 (MSTI) 的 MST 区域。多个区域和其他 STP 网桥使用一个公共生成树 (CST) 进行互联。

MSTP 与 RSTP 网桥完全兼容，原因是 RSTP 网桥可以将 MSTP BPDU 解译为 RSTP BPDU。这不仅可实现在不更改配置的情况下与 RSTP 网桥兼容，还会导致 MSTP 区域之外的所有 RSTP 网桥将该区域视为一个 RSTP 网桥，而不管在该区域内存在多少个 MSTP 网桥。

对于将在同一个 MST 区域内的两台或更多台交换机，它们必须具有相同的 VLAN 到 MST 实例映射、相同的配置修订编号以及相同的区域名称。

将在同一个 MST 区域内的交换机永远不会被另一个 MST 区域内的交换机分开。如果它们被分开，该区域将成为两个独立的区域。

此映射可以在 VLAN 到 MSTP 实例页面中完成。

如果系统在 MSTP 模式下运行，请使用此页面。

定义 MSTP 的步骤：

步骤 1 单击**生成树** > **STP 状态和全局设置**。

步骤 2 启用 MSTP。

步骤 3 单击**生成树** > **MSTP 属性**。

步骤 4 输入参数。

- **区域名称** — 定义 MSTP 区域名称。
- **版本** — 定义标识目前 MST 配置的修订的未签名 16 位数。该字段值的范围为 0 到 65535。

- **最大跳数** — 设置丢弃 BPDU 之前特定区域内可发生的跃点总数。丢弃 BPDU 后，端口信息即过期。该字段值的范围为 1 到 40。
- **主 IST** — 显示区域的主端口。

步骤 5 单击**应用**。将定义 MSTP 属性，并更新当前配置文件。

VLAN 到 MSTP 实例

使用“VLAN 到 MSTP 实例”页面可将每个 VLAN 映射到一个多生成树实例 (MSTI)。对于要在同一区域中的设备，它们必须具有相同的 VLAN 到 MSTI 映射。

注 同一个 MSTI 可以映射到多个 VLAN，但每个 VLAN 只能有一个 MST 实例与之连接。

如果系统 STP 模式为 MSTP，该页面（及所有 MSTP 页面）上的配置便会生效。

除实例 0 之外，最多可定义 16 个 MST 实例。

对于那些未明确映射到某个 MST 实例的 VLAN，设备会自动将其映射到 CIST（核心内部生成树）实例。CIST 实例为 MST 实例 0。

将 VLAN 映射到 MST 实例的步骤：

步骤 1 单击**生成树** > **VLAN 到 MSTP 实例**。

“VLAN 到 MSTP 实例”页面包含以下字段：

- **MSTP 实例 ID** — 显示所有 MSTP 实例。
- **VLAN** — 显示所有属于 MST 实例的 VLAN。

步骤 2 要将 VLAN 添加到 MSTP 实例，请选择 MSTP 实例并单击**编辑**。

步骤 3 输入以下参数：

- **MSTP 实例 ID** — 选择 MSTP 实例。
- **VLAN** — 定义将映射到该 MST 实例的 VLAN。
- **操作** — 定义将 VLAN **添加**（映射）到该 MST 实例，还是从该实例**删除** VLAN。

步骤 4 单击**应用**。系统将定义 MSTP VLAN 映射，并更新当前配置文件。

MSTP 实例设置

使用“MSTP 实例设置”页面可配置和查看每个 MST 实例的参数。此为针对每个实例的操作，等同于*配置 STP 状态和全局设置*。

输入 MSTP 实例设置的步骤：

步骤 1 单击**生成树** > **MSTP 实例设置**。

步骤 2 输入参数。

- **实例 ID** — 选择要显示和定义的 MST 实例。
- **包含的 VLAN** — 显示映射到所选实例的 VLAN。默认映射为将所有 VLAN 映射到公共内部生成树 (CIST) 实例 (0)。
- **网桥优先级** — 为所选 MST 实例设置此网桥的优先级。
- **指定的根网桥 ID** — 显示 MST 实例的根网桥的优先级和 MAC 地址。
- **根端口** — 显示所选实例的根端口。
- **根路径成本** — 显示所选实例的根路径成本。
- **网桥 ID** — 显示所选实例的此设备的网桥优先级和 MAC 地址。
- **剩余的跳数** — 显示保留到下个目标地址的跃点数。

步骤 3 单击**应用**。系统将定义 MST 实例配置，并更新当前配置文件。

MSTP 接口设置

使用“MSTP 接口设置”页面可为每个 MST 实例配置端口 MSTP 设置，以及查看协议目前已学习到的信息，例如每个 MST 实例的指定网桥。

配置 MST 实例中的端口的步骤：

步骤 1 单击**生成树** > **MSTP 接口设置**。

步骤 2 输入参数。

- **实例为** — 选择要配置的 MSTP 实例。
- **接口类型为** — 选择显示端口列表还是 LAG 列表。

步骤 3 单击**转至**。系统此时将显示实例上的接口的 MSTP 参数。

步骤 4 选择一个接口，并单击**编辑**。

步骤 5 输入参数。

- **实例 ID** — 选择要配置的 MST 实例。
- **接口** — 选择要为其定义 MSTI 设置的接口。
- **接口优先级** — 设置指定接口和 MST 实例的端口优先级。
- **路径成本** — 在**用户定义**文本框中输入端口产生的根路径成本，或选择**使用默认设置**以使用默认值。
- **端口状态** — 显示特定 MST 实例上的特定端口的 MSTP 状态。参数定义如下：
  - *已禁用* — STP 目前被禁用。
  - *丢弃* — 该实例上的端口目前丢弃/被阻塞，无法转发流量（BPDU 数据除外）或学习 MAC 地址。
  - *监听* — 该实例上的端口处于监听模式。端口无法转发流量，也无法学习 MAC 地址。
  - *学习* — 该实例上的端口处于学习模式。端口无法转发流量，但能够学习新的 MAC 地址。
  - *转发* — 该实例上的端口处于转发模式。端口可以转发流量且学习新的 MAC 地址。
  - *边界* — 该实例上的端口为边界端口。其状态继承自实例 0，可在 STP 接口设置页面中进行查看。
- **端口角色** — 显示每个实例的每个端口或 LAG 的端口或 LAG 角色（由 MSTP 算法指定以提供 STP 路径）：
  - *根* — 通过此接口转发数据包可提供将数据包转发给根设备的最低成本路径。
  - *指定的端口* — 网桥通过其连接至 LAN 的接口，可提供从 LAN 到 MST 实例的根网桥的最低根路径成本。
  - *备选* — 接口提供从根端口到根网桥的备用路径。
  - *备用* — 该接口提供指向生成树叶节点的指定端口路径的备用路径。如果一个环路中的两个端口通过一条点到点链路进行连接，则会出现备用端口。如果 LAN 已建立了两条或更多条至一个共享网段的连接，也会出现备用端口。

- *已禁用* — 接口不会加入生成树。
- *边界* — 该实例上的端口为边界端口。其状态继承自实例 0，可在 STP 接口设置页面中进行查看。

- **模式** — 显示目前的接口生成树模式。
  - 如果链路伙伴使用 MSTP 或 RSTP，则显示的端口模式为 RSTP。
  - 如果链路伙伴使用 STP，则显示的端口模式为 STP。
- **类型** — 显示端口的 MST 类型。
  - *边界* — 边界端口可将 MST 网桥连接至边远地区中的 LAN。如果端口为边界端口，它还可表示链路另一端的设备是在 RSTP 还是 STP 模式下工作。
  - *内部* — 端口为内部端口。
- **指定的网桥 ID** — 显示将链路或共享 LAN 连接到根的网桥 ID 号。
- **指定的端口 ID** — 显示指定网桥上将链路或共享 LAN 连接到根的端口 ID 号。
- **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。
- **剩余的步跳数** — 显示到下个目标地址剩余的步跳数。
- **转发转换** - 显示端口从转发状态变成丢弃状态的次数。

步骤 6 单击**应用**。将更新当前配置文件。

14

管理 MAC 地址表

本节介绍如何将 MAC 地址添加到系统。其中包含以下主题：

- 静态地址
- 动态地址

MAC 地址有两种类型：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。

在到达设备的帧中显示的新源 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 地址的其他帧到达设备，则 MAC 条目将过期并从动态地址表中删除。

当帧到达设备时，设备会搜索静态或动态地址表中响应/匹配的目标 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。如果帧要发送到的目标 MAC 地址不在这两个表中，则系统会将这些帧传输/广播到相应 VLAN 上的所有端口。此类帧也称为未知的单播帧。

设备最多支持 8,000 个静态和动态 MAC 地址。

静态地址

可以将静态 MAC 地址分配给设备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**。

“静态地址”页面包含当前已定义的静态地址。

步骤 2 单击**添加**。

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，则重启后系统会保留该地址。
  - *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。

动态地址

动态地址表（桥接表）中包含通过监控进入设备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（称为“过期时间”）内没有接收到相应的流量，系统会删除该地址。

动态地址设置

配置动态地址过期时间的步骤：

步骤 1 单击 **MAC 地址表 > 动态地址设置**。

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。

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**。

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端口或 LAG。

步骤 3 单击**转至**。系统将对动态 MAC 地址表进行查询并显示结果。

步骤 4 要删除所有动态 MAC 地址，请单击**清除表**。

15

组播

本节介绍了组播转发功能，具体包括以下主题：

- 组播转发概述
- 属性
- MAC 组地址
- IP 组播群地址
- IPv4 组播配置
- IPv6 组播配置
- IGMP/MLD 侦听 IP 组播组
- 组播路由器端口
- 全部转发
- 未注册的组播

组播转发概述

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。

默认情况下，系统会将所有组播帧泛洪到 VLAN 的所有端口。通过在属性页面中启用网桥组播过滤状态，可以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。

如果启用过滤，则系统会将组播帧转发到相关 VLAN 中端口的子集，如组播转发数据库 (MFDB) 中所定义。将对所有流量实施组播过滤。

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 群地址。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，则保存为 (*,G)。

可以配置以下组播帧转发方法之一：

- **MAC 组地址** — 根据以太网帧中的目的 MAC。

  注 可将一个或多个 IP 组播群地址映射至一个 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)。

IGMPv3 和 MLDv2 支持 (S,G)，而 IGMPv1/2 和 MLDv1 仅支持恰好为组 ID 的 (*.G)。

设备最多支持 256 个静态和动态组播群地址。

只能为每个 VLAN 配置上述选项之一。

典型的组播设置

当组播路由器在 IP 子网间路由多播数据包时，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 IGMP/MLD 侦听功能的设备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/MLD 查询。

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。

当设备启用 IGMP/MLD 侦听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/MLD 加入消息接收组播流的所有端口。

系统会维护每个 VLAN 的组播组列表，而这些列表会管理每个端口应接收的组播信息。使用 IGMP 或 MLD 协议侦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（IGMP/MLD 侦听）

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 上启用设备中的 IGMP/MLD 侦听时，该设备会分析其接收的 IGMP/MLD 数据包（来自连接到设备的 VLAN 和网络中的组播路由器）。

当设备学习到主机正在使用 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），该设备会在其 MFDB 中添加注册。

系统可支持以下版本：

- IGMP v1/v2/v3
- MLD v1/v2

注 设备仅在静态 VLAN 上支持 IGMP/MLD 侦听。它不支持动态 VLAN 上的 IGMP/MLD 侦听。

全局启用 IGMP/MLD 侦听后，所有 IGMP/MLD 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/MLD 查询的组播路由器 (Mrouter)。
- 哪些端口正在接收 PIM、DVMRP 或 IGMP/MLD 查询协议。

这些 VLAN 显示在 IGMP/MLD 侦听 IP 组播组页面上。

要求加入特定组播组的端口将发送 IGMP/MLD 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。

IGMP 侦听查询器

当没有组播路由器时，IGMP/MLD 侦听查询器将用于支持侦听交换机的第 2 层组播域。例如，本地服务器提供了组播内容，但该网络上的路由器（如果存在一个）不支持组播。

可以将设备配置为作为备用查询器的 IGMP 查询器，或当不存在普通 IGMP 查询器时对其进行配置。设备不是全功能 IGMP 查询器。

如果设备作为 IGMP 查询器启用，则它会在从组播路由器中未检测到任何 IGMP 流量（查询）起的 60 秒后启动。如果存在其他 IGMP 查询器，则设备可能会（也可能不会）停止发送查询，具体取决于标准查询器选择流程的结果。

IGMP/MLD 查询器活动的速度必须与启用 IGMP/MLD 侦听的交换机保持一致。必须以与侦听表过期时间相一致的速率发送查询。如果发送查询的速度低于过期时间，则用户将无法接收组播数据包。这是在 IGMP/MLD 侦听 IP 组播组页面中执行的。

如果禁用 IGMP/MLD 查询器选择机制，则 IGMP/MLD 侦听查询器会在启用后 60 秒延迟发送常规查询消息。如果没有其他查询器，便会开始发送常规查询消息。如果检测到其他查询器，便会停止发送常规查询消息。

如果 IGMP/MLD 侦听查询器在以下时间间隔内未侦听到其他查询器，则会恢复发送常规查询消息：

查询被动间隔 = 健壮性 * 查询间隔 + 0.5 * 查询响应间隔。

注 如果 VLAN 上有 IPM 组播路由器，建议禁用 IGMP/MLD 查询器选择机制。

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 组播群地址映射至第 2 层多播地址的步骤：
  - 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，并且系统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，234.129.2.3 会映射至 MAC 组播群地址 01:00:5e:01:02:03。最多 32 个 IP 组播群地址可映射至同一第 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，IPv6 组播地址 FF00:1122:3344 会映射至第 2 层组播 33:33:11:22:33:44。

IGMP/MLD 代理

IGMP/MLD 代理是一种简单的 IP 组播协议。

使用 IGMP/MLD 代理复制设备上的组播流量（例如，边缘盒），可以大大简化这些设备的设计和实施。不支持更加复杂的组播路由协议，如协议独立组播 (PIM) 或距离矢量组播路由协议 (DVMRP)，这样不仅减少了设备的成本，而且也减少了运行开销。另一项优点在于可以让代理设备不受核心网络路由器使用的组播路由协议影响。因而可以将代理设备轻松部署到任何组播网络中。

IGMP/MLD 代理树

IGMP/MLD 代理在一个简单的树拓扑中工作，无需运行复杂的组播路由协议（例如，PIM）。这足以基于学习组成员关系信息和代理组成员关系信息使用简单的 IPM 协议，并基于这些信息转发组播路由数据包，

此树必须通过在每台代理设备上指定上游和下游接口来手动配置。此外，还应配置适用于代理树拓扑的 IP 寻址方案，确保代理设备可以赢得 IGMP/MLD 查询器选择，以便能够转发组播流量。在树中除了代理设备不应有其他组播路由器，而且树的根应连接到更广泛的组播基础设施。

执行基于 IGMP/MLD 的转发的代理设备具有一个上游接口，以及一个或多个下游接口。这些设置均为显式配置；没有协议用于确定每个接口的类型。代理设备通过其下游接口执行 IGMP/MLD 的路由器部分，通过其上游接口执行 IGMP/MLD 的主机部分。

只支持一个树。

转发规则和查询器

应用以下规则：

- 转发上游接口接收的组播数据包：
  - 转发到上游接口
  - 仅当代理设备为接口上的查询器时，转发到所有请求数据包的下游接口
- 如果代理设备不是接口上的查询器，则会丢弃下游接口接收的组播数据包。
- 仅当代理设备为接口上的查询器时，代理设备为查询器的下游接口接收的组播数据包才会转发到上游接口和所有请求数据包的下游接口。

下游接口保护

默认情况下，系统会转发到达 IGMP/MLD 树的接口的 IP 组播流量。您可以禁用到达下游接口的 IP 组播流量转发。此设置可以在全局范围内实现，也可以在指定的下游接口上实现。

属性

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**。

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* — 根据 MAC 组播群地址转发数据包
  - *IP 组地址* — 根据 IPv6 组播群地址转发数据包
  - *源特定 IP 组地址* — 根据源 IPv6 地址和 IPv6 组播群地址转发数据包。如果在 VLAN 上配置了 IPv6 地址，IPv6 组播的可行转发方法将为 IP 组地址。

  注 在 IPv6 IP 组地址和源特定 IP 组地址模式下，设备仅检查与目标组播地址或源地址的 4 个字节匹配的项。对于目标组播地址，系统将匹配组 ID 的最后 4 个字节。对于源地址，系统将匹配最后 3 个字节以及倒数第 5 个字节。
- **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* — 根据 MAC 组播群地址转发数据包
  - *IP 组地址* — 根据 IPv4 组播群地址转发数据包
  - *源特定 IP 组地址* — 根据源 IPv4 地址和 IPv4 组播群地址转发数据包。如果在 VLAN 上配置了 IPv4 地址，IPv4 组播的可行转发方法将为 IP 组地址。

步骤 3 单击**应用**。将更新当前配置文件。

MAC 组地址

“MAC 组地址”页面具有以下功能：

- 查询并查看来自组播转发数据库 (MFDB) 的与特定 VLAN ID 或特定 MAC 地址组相关的信息。可通过 IGMP/MLD 侦听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。

定义和查看 MAC 组播组的步骤：

步骤 1 单击**组播 > MAC 组地址**。

步骤 2 输入“过滤器”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，页面将包含来自所选 VLAN 的所有 MAC 组地址。

步骤 3 单击**转至**，将在下侧块中显示 MAC 组播群地址。

此时将显示在此页面和 IP 组播群地址页面创建的条目。对于那些在 IP 组播群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。

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 组播组将保存至当前配置文件中。

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**。

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**菜单选择端口或 LAG。

步骤 8 单击**转至**以显示 VLAN 的端口或 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 侦听已将接口添加到组播组。
- **已禁止** — 指定禁止此端口加入此 VLAN 上的这个组播组。
- **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 组播群地址页面创建的条目（即使已选定这些条目）。

IP 组播群地址

除组播组由 IP 地址确定之外，“IP 组播群地址”页面与“MAC 组地址”页面在其他方面均相似。

使用“IP 组播群地址”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 组播群地址**。

该页面包含通过侦听学习的所有 IP 组播群地址。

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 组播群地址为** — 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地址定义。

步骤 3 单击**转至**。结果将显示在选择下侧块中。

步骤 4 单击**添加**以添加静态 IP 组播群地址。

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 组播群地址** — 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。
- **源 IP 地址** — 定义要包括的源地址。

步骤 6 单击**应用**。系统将添加 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**。

选定的 VLAN ID、IP 版本、IP 组播群地址和源 IP 地址将以只读的方式显示在窗口的顶部。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。
- **动态** — 将接口作为动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。

IPv4 组播配置

以下页面用于配置 IPv4 组播配置：

- IGMP 侦听
- IGMP VLAN 设置

IGMP 侦听

要支持选择性 IPv4 组播转发，必须启用网桥组播过滤（在属性页面中，并且必须在“IGMP 侦听”页面中针对每个相关 VLAN 全局启用 IGMP 侦听。

在 VLAN 上启用 IGMP 侦听并识别作为 IGMP 侦听查询器的设备的步骤：

步骤 1 单击**组播** > **IPv4 组播配置** > **IGMP 侦听**。

全局启用 IGMP 侦听时，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 侦听和网桥组播过滤时，设备才会执行 IGMP 侦听。

系统会显示 IGMP 侦听表。显示的字段将在下面的**编辑**页面中进行说明。此外，将显示以下字段：

- **IGMP 侦听状态** — 显示 IGMP 侦听是否已启用（**管理**）以及它实际是否正在 VLAN（**运行**）上运行。
- **IGMP 查询器状态** — 显示 IGMP 查询器是否已启用（**管理**）及其是否正在 VLAN 上实际运行（**运行**）。

启用或禁用以下功能：

- **IGMP 侦听状态** — 选择该选项可在所有接口上全局启用 IGMP 侦听。
- **IGMP 查询器状态** — 选择该选项可在所有接口上全局启用 IGMP 查询器。

步骤 2 要在接口上配置 IGMP，请选择一个静态 VLAN 并单击**编辑**。输入以下字段：

- **IGMP 侦听状态** — 选择该选项可在 VLAN 上启用 IGMP 侦听。设备会监控网络流量，以确定哪些主机已要求接收组播流量。仅当同时启用 IGMP 侦听和网桥组播过滤时，设备才会执行 IGMP 侦听。
- **组播路由器端口自动学习** — 选择该选项可启用组播路由器的自动学习。
- **立即离开** — 选择该选项可使交换机删除从转发表发送离开消息的接口，而不必首先向接口发出基于 MAC 的一般查询。从主机接收到 IGMP 组离开消息时，系统会从表条目中删除主机端口。在中继来自组播路由器的 IGMP 查询后，如果未从组播客户端接收到任何 IGMP 成员关系报告，系统会定期检测条目。启用时，此功能会减少用来阻止发送到设备端口的多余 IGMP 流量的时间。
- **最近成员查询计数器** — 设备中假定不再存在组成员之前所发送的特定于 MLD 组的查询数（如果该设备是选择的查询器）。
  - *使用查询健壮性 (x)* — 此值在 MLD VLAN 设置页面中设置。括号中的数字是当前查询健壮性值。
  - *用户定义* — 输入一个用户定义的值。
- **IGMP 查询器状态** — 选择该选项可启用此功能。如果没有组播路由器，则需要使用此功能。

- **IGMP 查询器选择** — 是启用还是禁用 IGMP 查询器选择。如果启用 IGMP 查询器选择机制，则 IGMP 侦听查询器会支持 RFC3810 中指定的标准 IGMP 查询器选择机制。

  如果禁用 IGMP 查询器选择机制，则 IGMP 侦听查询器会在启用后 60 秒延迟发送常规查询消息，如果没有其他查询器，便会开始发送常规查询消息。当检测到其他查询器时，便会停止发送常规查询消息。如果 IGMP 侦听查询器在通过以下方式计算的查询被动间隔内未侦听到其他查询器，则会恢复发送常规查询消息：健壮性 * (查询间隔) + 0.5 * 查询响应间隔。

- **IGMP 查询器版本** — 选择当设备成为选择的查询器时要使用的 IGMP 版本。如果执行特定于源的 IP 组播转发的 VLAN 中存在交换机和/或组播路由器，则选择 IGMPv3。否则，请选择 IGMPv2。
- **查询源 IP 地址** — 选择要在发送的消息中使用的设备源接口。在 MLD 中，系统会自动选择此地址。

  注 如果已选择“自动”选项，系统将使用传出接口上定义的 IP 地址的源 IP 地址。

步骤 3 单击**应用**。将更新当前配置文件。

注 IGMP 侦听定时器配置中的更改，例如：“查询健壮性”、“查询间隔”等，在已创建的定时器上不起作用。

IGMP VLAN 设置

在特定 VLAN 上配置 IGMP 的步骤：

步骤 1 单击**组播** > **IPv4 组播配置** > **IGMP VLAN 设置**。

对于每个启用了 IGMP 的 VLAN，系统将显示以下字段：

- **查询健壮性** — 输入链路上的预期数据包丢失数。
- **查询间隔（秒）** — 当此设备是选择的查询器时要使用的普通查询的时间间隔。
- **查询最大响应间隔（秒）** — 用来计算插入定期普通查询的最大响应代码的延迟时间。
- **最近成员查询间隔（毫秒）** — 输入要使用的最大响应延迟时间（如果设备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）。

  TTL 值小于该阈值的组播数据包将不会在接口上转发。

默认值 0 表示在接口上转发所有组播数据包。

值 256 表示在接口上不转发任何组播数据包。

仅在边界路由器上配置 TTL 阈值。反之，在其中配置 TTL 阈值的路由器会自动成为边界路由器。

步骤 2 选择一个接口，并单击**编辑**。输入上述字段的值。

步骤 3 单击**应用**。将更新当前配置文件。

IPv6 组播配置

以下页面用于配置 IPv6 组播配置：

- MLD 侦听
- MLD VLAN 设置

MLD 侦听

要支持选择性 IPv6 组播转发，必须启用网桥组播过滤（在属性页面中），并且必须在 MLD 侦听页面中针对每个相关 VLAN 全局启用 MLD 侦听。

在 VLAN 上启用 MLD 侦听并进行配置的步骤：

步骤 1 单击**组播** > **IPv6 组播配置** > **MLD 侦听**。

全局启用 MLD 侦听时，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 侦听和网桥组播过滤，则设备将执行 MLD 侦听。

系统会显示 MLD 侦听表。显示的字段将在下面的“编辑”页面中进行说明。此外，将显示以下字段：

- **MLD 侦听状态** — 显示 MLD 侦听是否已启用（**管理**）以及它实际是否正在 VLAN 上运行（**运行**）。
- **MLD 查询器状态** — 显示 MLD 查询器是否已启用（**管理**）及其是否正在 VLAN 上实际运行（**运行**）。

步骤 2 启用或禁用以下功能：

- **MLD 侦听状态** — 选择该选项可在所有接口上全局启用 MLD 侦听。
- **MLD 查询器状态** — 选择该选项可在所有接口上全局启用 MLD 查询器。

步骤 3 要在接口上配置 MLD 代理，请选择一个静态 VLAN 并单击**编辑**。输入以下字段：

- **MLD 侦听状态** — 选择该选项可在 VLAN 上启用 MLD 侦听。设备会监控网络流量，以确定哪些主机已要求接收组播流量。仅当同时启用 MLD 侦听和网桥组播过滤时，设备才会执行 MLD 侦听。
- **组播路由器端口自动学习** — 选择该选项可启用组播路由器的自动学习。
- **立即离开** — 选择该选项可使交换机删除从转发表发送离开消息的接口，而不必首先向接口发出基于 MAC 的一般查询。从主机接收到 MLD 组离开消息时，系统会从表条目中删除主机端口。在中继来自组播路由器的 MLD 查询后，如果未从组播客户端接收到任何 MLD 成员关系报告，系统会定期检测条目。启用时，此功能会减少用来阻止发送到设备端口的多余 MLD 流量的时间。
- **最近成员查询计数器** — 设备中假定不再存在组成员之前所发送的特定于 MLD 组的查询数（如果该设备是选择的查询器）。
  - *使用查询健壮性 (x)* — 此值在 MLD VLAN 设置页面中设置。括号中的数字是当前查询健壮性值。
  - *用户定义* — 输入一个用户定义的值。
- **MLD 查询器状态** — 选择该选项可启用此功能。如果没有组播路由器，则需要使用此功能。
- **MLD 查询器选择** — 是启用还是禁用 MLD 查询器选择。如果启用 MLD 查询器选择机制，则 MLD 侦听查询器会支持 RFC3810 中指定的标准 MLD 查询器选择机制。

  如果禁用 MLD 查询器选择机制，则 MLD 侦听查询器会在启用后 60 秒延迟发送常规查询消息，如果没有其他查询器，便会开始发送常规查询消息。当检测到其他查询器时，便会停止发送常规查询消息。如果 MLD 侦听查询器在通过以下方式计算的查询被动间隔内未侦听到其他查询器，则会恢复发送常规查询消息：健壮性 * (查询间隔) + 0.5 * 查询响应间隔。
- **MLD 查询器版本** — 选择当设备成为选择的查询器时要使用的 MLD 版本。如果执行特定于源的 IP 组播转发的 VLAN 中存在交换机和/或组播路由器，则选择 MLDv2。否则，请选择 MLDv1。

步骤 4 单击**应用**。将更新当前配置文件。

注 MLD 侦听定时器配置中的更改，例如：“查询健壮性”、“查询间隔”等，在已创建的定时器上不起作用。

MLD VLAN 设置

在特定 VLAN 上配置 MLD 的步骤：

步骤 1 单击**组播** > **IPv6 组播配置** > **MLD VLAN 设置**。

对于每个启用了 MLD 的 VLAN，系统将显示以下字段：

- **接口名称** — 显示其 MLD 信息的 VLAN。
- **查询健壮性** — 输入链路上的预期数据包丢失数。
- **查询间隔（秒）** — 当此设备是选择的查询器时要使用的普通查询的时间间隔。
- **查询最大响应间隔（秒）** — 用来计算插入定期普通查询的最大响应代码的延迟时间。
- **最近成员查询间隔（毫秒）** — 输入要使用的最大响应延迟时间（如果设备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）。

步骤 2 要配置某个 VLAN，请选中该 VLAN，然后单击**编辑**。输入上述字段。

步骤 3 单击**应用**。将更新当前配置文件。

IGMP/MLD 侦听 IP 组播组

“IGMP/MLD 侦听 IP 组播组”页面显示从 IGMP/MLD 消息学习的 IPv4 和 IPv6 群地址。

此页面上的信息与“MAC 组地址”页面上的信息可能有所不同。示例如下：假定系统根据基于 MAC 的组和请求加入以下组播组 224.1.1.1 和 225.1.1.1 的端口进行过滤，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 侦听 IP 组播组**。

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：

- **群地址为** — 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。
- **群地址** — 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** — 通过设备在 IP 组地址上接收的主机注册的最旧版本的 IGMP/MLD。

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。当设备转发组播流和 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**。

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 IGMP 侦听页面或 MLD 侦听页面
- **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**更新设备。

全部转发

启用网桥组播过滤时，系统将根据 IGMP 侦听和 MLD 侦听向端口转发以已注册组播组作为目标的组播数据包。如果禁用网桥组播过滤，系统将向对应的 VLAN 转发所有组播数据包。

使用“全部转发”页面，可以配置要从特定 VLAN 接收组播流的端口和/或 LAG。此功能需要在组播地址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设备中的所有端口。

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”。

始终向已定义为“全部转发”的端口转发组播数据包，但不包括 IGMP 和 MLD 消息。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**。

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**。系统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 侦听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。

未注册的组播

此功能可用于确保客户仅接收请求的组播组（已注册），而不接收可能在网络中传输的其他组播组（未注册）。

系统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拒绝（过滤）未注册的组播流。该配置适用于其端口为成员（或将成为成员）的任何 VLAN。

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**。

步骤 2 选择**接口类型为** — 查看端口或 LAG。

步骤 3 单击**转至**。

步骤 4 定义以下选项：

- **端口/LAG** — 显示端口 ID 或 LAG ID。
- 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 5 单击**应用**。将保存设置，并更新当前配置文件。

16

IP 配置

IP 接口地址可以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设备 IP 地址，或通过将设备设置为 DHCP 客户端来定义其 IP 地址的信息。

本节包含以下主题：

- 概述
- 环回接口
- IPv4 管理和接口
- IPv6 管理和接口
- 域名系统

概述

如果禁用了巨型帧，流量的第 3 层流量 MTU 限制为 1518 字节。

如果启用了巨型帧，流量的第 3 层流量 MTU 限制为 9000 字节。

默认 VLAN 的 IPv4 接口出厂默认设置为 *DHCPv4*。这表示设备被用作 DHCPv4 客户端，并在启动期间发出 DHCPv4 请求。

如果设备收到 DHCPv4 服务器使用 IPv4 地址进行的 DHCPv4 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 IPv4 地址正在使用中，则设备会向提供 IPv4 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。

如果设备在 60 秒内未收到 DHCPv4 响应，它会继续发送 DHCPDISCOVER 查询并采用默认 IPv4 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。如果地址冲突，则需要对与设备发生冲突的 DHCP 服务器和/或设备执行管理操作。

默认 VLAN 的 IP 地址分配规则如下：

- 除非使用静态 IPv4 地址配置设备，否则设备会发出 DHCPv4 查询，直到收到 DHCPv4 服务器的响应。
- 如果设备上的 IP 地址发生更改，设备会向相应的 VLAN 发出免费 ARP 数据包，来检查 IP 地址冲突问题。将设备恢复到默认 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 会变为以绿色持续亮起。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。如果设备正获取 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，则系统会使用默认 IP 地址。有其他 IP 地址可用时，系统会自动使用这些地址。默认 IP 地址始终位于管理 VLAN 上。

设备可以具有多个 IP 地址可将每个 IP 地址分配给指定的端口、LAG 或 VLAN。这些 IP 地址是在 IPv4 接口和 IPv6 接口页面中配置的。可以从相应的接口在设备的所有 IP 地址访问设备。

不提供预定义的默认路由。要远程管理设备，必须定义默认路由。所有 DHCP 分配的默认网关都被存储成默认路由。此外，您可以手动定义默认路由。请在 IPv4 静态路由和 IPv6 路由页面中进行此定义。

在此指南中，所有为设备配置或分配的 IP 地址均被称为管理 IP 地址。

环回接口

概述

环回接口是操作状态始终启用的虚拟接口。如果此虚拟接口上配置的 IP 地址用作与远程 IP 应用通信时的本地地址，那么，即使到远程应用的实际路由更改，此通信也不会中止。

环回接口的操作状态始终启用。您可以在上面定义 IP地址（IPv4 或 IPv6），并将此 IP 地址用作与远程 IP 应用进行 IP 通信的本地 IP 地址。只要能够从交换机的任一活动（非环回）IP 接口访问远程应用，通信就会保持完整。另一方面，如果使用 IP 接口的 IP 地址与远程应用通信，当 IP 接口关闭时，通信将终止。

环回接口不支持桥接；它无法成为任何 VLAN 的成员，也不支持任何第 2 层协议。

IPv6 链路本地接口标识符为 1。

配置环回接口

要配置 IPv4 环回接口，请在 IPv4 接口中添加环回接口。

要配置 IPv6 环回接口，请在 IPv6 地址中添加环回接口。

IPv4 管理和接口

本节包含以下主题：

- IPv4 接口
- IPv4 静态路由
- IPv4 转发表
- RIPv2
- ARP
- ARP 代理
- UDP 中继/IP 助手
- DHCP 中继

IPv4 接口

要使用基于 Web 的配置实用程序管理设备，必须定义并知道 IPv4 设备管理 IP 地址。设备 IP 地址可以手动配置或从 DHCP 服务器自动获得。

“IPv4 接口”页面用于为设备管理配置 IP 地址。此 IP 地址可以在端口、LAG、VLAN、环回接口或带外接口上配置。

您可以在设备上配置多个 IP 地址（接口）。这样，它既支持这些不同接口之间的流量路由，又支持到远程网络的流量路由。在默认和通常情况下，路由功能由硬件执行。如果硬件资源耗尽或者硬件中有路由表溢出，IP 路由将由软件执行。

硬件路由提供线速第 3 层流量转发，而软件路由会受 CPU 功能以及软件正在执行的其他任务的限制。

注 设备软件会为在端口或 LAG 上配置的每个 IP 地址使用一个 VLAN ID (VID)。设备会使用从 4094 开始第一个未使用的 VID。

配置 IPv4 地址的步骤：

步骤 1 单击 **IP 配置** > **IPv4 管理和接口** > **IPv4 接口**。

输入以下字段：

- **IPv4 路由** — 勾选**启用**复选框以启用 IPv4 路由（默认情况下处于启用状态）。
- **基于硬件的路由** — 显示基于硬件的路由当前是否处于活动状态，或者基于软件的路由是否已激活。

如果基于硬件的路由未激活，单击**重新激活基于硬件的路由**按钮将其启用。基于硬件的路由的激活取决于可用于支持当前路由配置的硬件资源。

步骤 2 单击**应用**。参数将保存至当前配置文件。

IPv4 接口表中显示以下字段：

- **接口** — 为其定义 IP 地址的接口。这也可以是带外端口。
- **IP 地址类型** — 可用选项有：
  - *DHCP* — 从 DHCP 服务器接收。
  - *静态* — 手动输入。静态接口是由用户创建的非 DHCP 接口。
  - *默认设置* — 进行任何配置之前，默认情况下设备上存在的默认地址。
- **IP 地址** — 为接口配置的 IP 地址。
- **掩码** — 配置的 IP 地址掩码。
- **状态** — IP 地址重复检查的结果。
  - *不确定* — IP 地址重复检查没有最终结果。
  - *有效* — 已完成 IP 地址冲突检查，未检测到 IP 地址冲突。
  - *有效重复* — 已完成 IP 地址重复检查，检测到一个重复的 IP 地址。
  - *重复* — 检测到一个与默认 IP 地址重复的 IP 地址。
  - *延迟* — 如果启动时启用了 DHCP 客户端，那么 IP 地址分配会延迟 60 秒，以便留出时间发现 DHCP 地址。
  - *未收到* — 与 DHCP 地址有关。DCHP 客户端开始发现流程时，会在获取真实地址之前分配一个虚拟 IP 地址 0.0.0.0。该虚拟地址的状态为“未收到”。

步骤 3 单击**添加**。

步骤 4 请选择以下字段之一：

- **接口** — 选择端口、LAG、环回或 VLAN 作为与此 IP 配置关联的接口，并从列表中选择一个接口。
- **IP 地址类型** — 选择以下其中一个选项：
  - *动态 IP 地址* — 从 DHCP 服务器接收 IP 地址。
  - *静态 IP 地址* — 输入 IP 地址。

步骤 5 如果选择了**静态 IP 地址**，请输入以下字段：

- **IP 地址** — 输入接口的 IP 地址。
- **掩码**
  - *网络掩码* — 此地址的 IP 掩码。
  - *前缀长度* — IPv4 前缀的长度。

步骤 6 单击**应用**。IPv4 地址设置将写入当前配置文件。

IPv4 静态路由

使用此页面可以在设备上配置和查看 IPv4 静态路由。路由流量时，系统会根据最长前缀匹配（LPM 算法）决定下一步跳。目的 IPv4 地址可能与 IPv4 静态路由表中的多个路由匹配。设备将使用子网掩码最高（即匹配的前缀最长）的匹配路由。如果使用相同的度量标准值定义了多个默认网关，系统会从所有配置的默认网关中选用最低的 IPv4 地址。

定义 IP 静态路由的步骤：

步骤 1 单击 **IP 配置** > **IPv4 管理和接口** > **IPv4 静态路由**。

系统会显示 IPv4 静态路由表。将为每个条目显示以下字段：

- **目的 IP 前缀** — 目的 IP 地址的前缀。
- **前缀长度** — 目的 IP 的 IP 路由前缀。
- **路由类型** — 指示该路由是拒绝还是远程路由。
- **下一跳路由器 IP 地址** — 路由上的下一跳 IP 地址或 IP 别名。

- **度量标准** — 本步跳的成本（首选较低的值）。
- **传出接口** — 此路由的传出接口。

注 为一个路由条目定义一个 IP SLA 对象跟踪 ID，用于通过指定的检查下一步跳检查与远程网络的连接。如果无连接，对象跟踪状态会被设置为“禁用”，并且路由器会被从转发表中移除（详情见 IP 配置：SLA 部分）。

步骤 2 单击**添加**。

步骤 3 为以下字段输入值：

- **目的 IP 前缀** — 输入目的 IP 地址的前缀。
- **掩码** — 选择并输入：
  - **网络掩码** — 目的 IP 地址的 IP 路由前缀，采用掩码格式（路由网络地址中的位数）。
  - **前缀长度** — 目的 IP 地址的 IP 路由前缀长度，采用 IP 地址格式。
- **路由类型** — 选择路由类型。
  - *拒绝* — 拒绝路由并停止通过所有网关至目的网络的路由。这样可以确保在某个帧使用此路由的目的 IP 时，会丢弃该帧。选择这个值会禁用以控制：下一步跳 IP 地址、度量标准和 IP SLA 跟踪。
  - *远程* — 表示该路由为远程路径。
- **下一跳路由器 IP 地址** — 输入路由上的下一跳 IP 地址或 IP 别名。

  注 您无法通过直接连接的 IP 子网（在其中设备从 DHCP 服务器取得其 IP 地址）来配置静态路由。
- **度量** — 输入至下一跳的管理距离。取值范围是 1-255。

步骤 4 单击**应用**。IP 静态路由将保存至当前配置文件。

IPv4 转发表

查看 IPv4 转发表的步骤：

步骤 1 单击 **IP 配置** > **IPv4 管理和接口** > **IPv4 转发表**。

系统会显示 IPv4 转发表。将为每个条目显示以下字段：

- **目的 IP 前缀** — 目的 IP 地址的前缀。
- **前缀长度** — 目的 IP 地址的 IP 路由前缀的长度。
- **路由类型** — 指示该路由是本地、拒绝还是远程路由。
- **下一步跳路由器 IP 地址** — 下一步跳 IP 地址。
- **路由所有者** — 这可以是以下选项之一：
  - *默认* — 按照默认系统配置来配置路由。
  - *静态* — 手动创建路由。
  - *动态* — 路由是由 IP 路由协议创建的。
  - *DHCP* — 从 DHCP 服务器接收路由。
  - *直接连接* — 路由是连接设备的子网。
- **度量标准** — 本步跳的成本（首选较低的值）。
- **管理距离** — 到下一跳的管理距离（首选较低的值）。该选项不适用于静态路由。
- **传出接口** — 此路由的传出接口。

ARP

设备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 子网是指设备的 IPv4 接口所连接的子网。当设备需要将数据包发送/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。设备会根据其收到的 ARP 数据包创建动态地址。动态地址会在经过配置的时间之后过期。

注 映射信息用于进行路由以及转发生成的流量。

定义 ARP 表的步骤：

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > ARP**。

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**。

步骤 5 输入以下参数：

- **IP 版本** — 主机支持的 IP 地址格式。仅支持 IPv4。
- **接口** — 可以在端口、LAG 或 VLAN 上配置 IPv4 接口。从设备上的已配置 IPv4 接口列表中选择所需接口。
- **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 条目将保存至当前配置文件。

ARP 代理

给定 IP 子网上的设备可使用代理 ARP 技术来回答不在该网络上的网络地址的 ARP 查询。

注 ARP 代理功能仅在设备处于第 3 层模式下时才可用。

ARP 代理可识别流量目的地，并提供其他 MAC 地址作为回复。用作其他主机的 ARP 代理，可将 LAN 流量目的地有效地定向至该主机。然后，该代理通常会使用其他接口或使用隧道，将捕获的流量路由至预期的目的地。

ARP 查询为代理目的而要求其他 IP 地址，从而导致节点使用其自己的 MAC 地址进行响应的过程有时也称为发布。

在所有 IP 接口上启用 ARP 代理的步骤：

步骤 1 单击 **IP 配置 > IPv4 管理和接口** > **ARP 代理**。

步骤 2 选择 **ARP 代理**，以让设备使用设备 MAC 地址来响应对远程节点的 ARP 请求。

步骤 3 单击**应用**。系统将启用 ARP 代理，并更新当前配置文件。

UDP 中继/IP 助手

交换机通常不会在 IP 子网之间路由 IP 广播数据包。但是，如果启用此功能，设备可以将从其 IPv4 接口接收的特定 UDP 广播数据包中继到特定目标 IP 地址。

要配置从特定 IPv4 接口接收的 UDP 数据包与特定目标 UDP 端口之间的中继，请添加一个 UDP 中继：

步骤 1 单击 **IP 配置 > IPv4 管理和接口** > **UDP 中继/IP 助手**。

步骤 2 单击**添加**。

步骤 3 选择**源 IP 接口**，设备会根据配置的 UDP 目的端口将 UDP 广播数据包中继到该接口。该接口必须为在设备上配置的 IPv4 接口之一。

步骤 4 输入设备要中继的数据包的 **UDP 目的端口**号。从下拉列表中选择众所周知的端口或单击端口单选按钮，手动输入端口号。

步骤 5 输入接收 UDP 数据包中继的**目标 IP 地址**。如果此字段为 0.0.0.0，则系统会丢弃 UDP 数据包。如果此字段为 255.255.255.255，则系统会将 UDP 数据包传输到所有 IP 接口。

步骤 6 单击**应用**。UDP 中继设置将写入当前配置文件。

DHCP 中继

本节包含以下主题：

- 概述
- 属性

DHCPv4 中继概述

DHCP 中继可将 DHCP 数据包中继到 DHCP 服务器。

设备可以中继从没有 IP 地址的 VLAN 接收的 DHCP 消息。只要在没有 IP 地址的 VLAN 上启用 DHCP 中继，系统便会自动插入选项 82。此插入操作是在特定 VLAN 中进行的，不会影响选项 82 插入的全局管理状态。

针对常规 DHCP 中继：

- 启用 DHCP 中继。

属性

配置 DHCP 中继的步骤:

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > DHCP 侦听/中继 > 属性**。

输入以下字段：

- **DHCP 中继** — 选择该选项可启用 DHCP 中继。

步骤 2 单击**应用**。设置将写入当前配置文件中。

步骤 3 要定义 DHCP 服务器，请单击**添加**。

步骤 4 输入 DHCP 服务器的 IP 地址，并单击**应用**。设置将写入当前配置文件中。

接口设置

可在任意接口或 VLAN 上启用 DHCP 中继。要使 DHCP 中继正常工作，必须在该 VLAN 或接口上配置 IP 地址。

在特定接口上启用 DHCP 中继的步骤：

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > DHCP 中继 > 接口设置。**

步骤 2 要在接口上启用 DHCP 中继，请单击**添加**。

步骤 3 选择要启用的接口和功能：**DHCP 中继**。

步骤 4 单击**应用**。设置将写入当前配置文件中。

IPv6 管理和接口

本节包含以下主题：

- 概述
- IPv6 全局配置
- IPv6 接口
- IPv6 隧道
- IPv6 地址
- IPv6 路由器配置
- IPv6 默认路由器列表
- IPv6 邻居
- IPv6 前缀列表
- IPv6 路由
- DHCPv6 中继

概述

互联网协议版本 6 (IPv6) 是一种网络层协议，用于数据包交换的互联网。设计 IPv6 是为了替换占主导地位的互联网协议 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 或手动机制（请参阅 IPv6 隧道）。隧道将 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。

设备会根据 IPv6 以太网类型检测 IPv6 帧。

与 IPv4 路由中发生的情况一样，帧寻址到设备的 MAC 地址，但是会到达设备未知的 IPv6 地址，然后转发到下一跳设备。设备可能为目标终端站，也可能是目标附近的路由器。转发机制需要在接收到的（基本上）未更改的第 3 层数据包周围重新构建第 2 层帧，以下一跳设备的 MAC 地址作为目的 MAC 地址。

系统使用静态路由和邻居发现消息（类似于 IPv4 ARP 消息）构建相应的转发表和下一跳地址。

路由定义两个网络设备之间的路径。用户添加的路由条目是静态的，并且由系统使用，直到用户显式删除这些条目为止。它们不会被路由协议更改。如果必须更新静态路由，则必须由用户执行明确操作。用户应负责阻止网络中路由环路的出现。

静态 IPv6 路由可以为以下两种形式：

- 直接连接，即目标直接连接到设备端口，因此数据包目标（接口）用作下一跳地址。
- 循环，此时仅指定下一跳，且传出接口源自下一跳。

同样，下一跳设备（包括直接连接的终端设备）的 MAC 地址使用网络发现自动衍生。但是，用户可以通过向邻居表手动添加条目的方式进行覆盖和补充。

IPv6 全局配置

定义 IPv6 全局参数和 DHCPv6 客户端设置的步骤：

步骤 1 单击 **IP 配置** > **IPv6 管理和接口** > **IPv6 全局配置**。

步骤 2 为以下字段输入值：

- **IPv6 路由** — 选择该选项可启用 IPv6 路由。如果未启用该选项，设备将作为主机（而非路由器）运行并且可以接收管理数据包，但无法转发数据包。如果启用了路由，设备可以转发 IPv6 数据包。

  启用 IPv6 路由将通过自动配置操作，从路由器在网络中发送的 RA 删除之前分配给设备接口的任何地址。

- **ICMPv6 限速时间间隔** — 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设备可发送的 ICMP 错误消息的最大数目。

- **IPv6 跳数限制** — 输入连接到数据包可通过的最终目的地的中间路由器最大数目。每当数据包转发到其他路由器时，跳数限制就会减少。跳数限制变成零后，将丢弃数据包。这样可以防止数据包无限传输。
- **DHCPv6 客户端设置**
  - *唯一标识符 (DUID) 格式* — DHCP 客户端的唯一标识符，DHCP 服务器使用其定位客户端。可采用以下格式之一：

    链接层 —（默认）。如果选择该选项，系统将使用设备 MAC 地址。

    企业编号 — 如果选择该选项，请输入以下字段。
  - *企业编号* — 供应商注册的专用企业编号，由 IANA 维护。
  - *标识符* — 供应商定义的十六进制字符串（最多 64 个十六进制字符）。如果字符数量不为偶数，则在右端添加数字零。每 2 个十六进制字符可由英文句点或冒号隔开。
- **DHCPv6 唯一标识符 (DUID)** — 显示所选标识符。

步骤 3 单击**应用**。更新 IPv6 全局参数和 DHCPv6 客户端设置。

IPv6 接口

可以在端口、LAG、VLAN、环回接口或隧道上配置 IPv6 接口。

与其他类型的接口不同，隧道接口应先在 IPv6 隧道页面进行创建，然后在此页面中的隧道上配置 IPv6 接口。

定义 IPv6 接口的步骤：

步骤 1 单击 **IP 配置** > **IPv6 管理和接口** > **IPv6 接口**。

步骤 2 输入参数。

- **IPv6 链接本地默认区域** — 选择该参数可定义默认区域。此接口用于出口没有特定接口或默认区域为 0 的链路本地数据包。
- **IPv6 链接本地默认区域接口** — 选择作为默认区域使用的接口。可以是以前定义的隧道或其他接口。

步骤 3 单击**应用**配置默认区域。

系统会显示 IPv6 接口表与以下字段：

- **隧道类型** —“手动”、“6to4”和“ISATAP”。

步骤 4 单击**添加**，在启用了 IPv6 的接口上添加新的接口。

步骤 5 输入以下字段：

- **IPv6 接口** — 选择 IPv6 地址的具体、端口、LAG、环回接口或 VLAN。

步骤 6 要将接口配置为 DHCPv6 客户端，即让接口能够接收来自 DHCPv6 服务器的信息（例如：SNTP 配置和 DNS 信息），请输入 **DHCPv6 客户端**字段：

- **DHCPv6 客户端** — 选择此项可以在接口上启用 DHCPv6 客户端（无状态和有状态）。
- **快速备注** — 选择此项可以启用成对消息交换，以用于地址分配和其他配置。如果启用此选项，客户端会在请求消息中包含快速备注选项。
- **最小信息刷新时间** — 此值用于设定刷新时间值的下限。如果服务器发送的刷新时间选项小于此值，则将使用此值。选择**无限期**（除非服务器发送此选项，否则不进行刷新）或者**用户定义**来设定值。
- **信息刷新时间** — 此值表示设备对接收自 DHCPv6 服务器的信息进行刷新的频率。如果未从服务器收到该选项，将使用此处输入的值。选择**无限期**（除非服务器发送此选项，否则不进行刷新）或者**用户定义**来设定值。

步骤 7 要配置其他 IPv6 参数，请输入以下字段：

- **IPv6 地址自动配置** — 选择该字段可启用来自邻居发送的路由器通告的自动地址配置。
- **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。
- **发送 ICMPv6 消息** — 可生成提示无法访问的目的消息。
- **IPv6 重定向** — 选择该字段可发送 ICMP IPv6 重定向消息。这些消息会通知其他设备不要向该设备发送流量，而是发送到其他设备。

步骤 8 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:X）

步骤 9 按**重新启动**按钮开始刷新接收自 DHCPv6 服务器的无状态信息。

步骤 10 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“IPv6 地址”一节。

步骤 11 要添加隧道，请选择 IPv6 隧道表中的一个接口（其已在 IPv6 接口页面定义为隧道），然后单击 **IPv6 隧道**。请参阅 IPv6 隧道。

DHCPv6 客户端详细信息

详细信息按钮显示接口上接收自 DHCPv6 服务器的信息。

当所选接口定义为 DHCPv6 无状态客户端时，该按钮可用。

按下该按钮后，系统将显示以下字段（针对接收自 DHCP 服务器的信息）：

- **DHCP 运行模式** — 满足以下条件时显示“已启用”：
  - 接口已启用。
  - 已启用 IPv6。
  - 已启用 DHCPv6 客户端。
- **有状态服务的状态** — 客户端是否从 DHCP 服务器接收有状态配置信息。
- **无状态服务的状态** — 客户端是否从 DHCP 服务器接收无状态配置信息。
- **IPv6 地址 IA NA** — IA ID 使用 C/IANAID、T1-C/T1、T2、- C/T2 标签值。当接口接收到至少一个地址时，可以使用 T1 和 T2。
- **DHCP 服务器地址** — DHCPv6 服务器地址。
- **DHCP 服务器 DUID** — DHCPv6 服务器唯一标识符。
- **DHCP 服务器偏好** — DHCPv6 服务器优先级。
- **信息最短刷新时间** — 见上文。
- **信息刷新时间** — 见上文。
- **已接收的信息刷新时间** — 从 DHCPv6 服务器接收的刷新时间。
- **剩余信息刷新时间** — 下次刷新之前的剩余时间。
- **DNS 服务器** — 接收自 DHCPv6 服务器的 DNS 服务器列表。
- **DNS 域搜索列表** — 接收自 DHCPv6 服务器的域列表。
- **SNTP 服务器** — 接收自 DHCPv6 服务器的 SNTP 服务器列表。
- **POSIX 时区字符串** — 接收自 DHCPv6 服务器的时区。

- **配置服务器** — 包含了接收自 DHCPv6 服务器的配置文件的服务器。
- **配置路径名称** — 从接收自 DHCPv6 服务器的位于配置服务器上的配置文件路径。

IPv6 隧道

隧道实现了 IPv6 数据包在 IPv4 网络上的传输。每个隧道都有一个源 IPv4 地址，如果是手动隧道，还有一个目的 IPv4 地址。IPv6 数据包封装在这些地址之间。

ISATAP 隧道

设备支持单个站内自动隧道寻址协议 (ISATAP) 隧道。

ISATAP 隧道是一种点对多点隧道。源地址是设备的 IPv4 地址（或 IPv4 地址之一）。

配置 ISATAP 隧道时，目的 IPv4 地址由路由器提供。请注意：

- 系统会将 IPv6 链路本地地址分配给 ISATAP 接口。系统会将初始 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，则系统会使用 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，则系统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，在 DNS 过程得到解析之前，系统没有用于 ISATAP 流量的默认路由器。

配置隧道

配置 IPv6 隧道的步骤：

步骤 1 单击 **IP 配置 > IPv6 管理和接口 > IPv6 隧道**。

步骤 2 单击**创建 ISATAP 隧道**。

步骤 3 系统会显示**隧道编号**和**隧道类型：1** 和 **ISATAP**。

步骤 4 输入以下字段：

- **源 IPv4 地址** — 设置隧道接口的本地（源）IPv4 地址。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* — 自动从配置的所有 IPv4 接口中选择最低的 IPv4 地址作为隧道接口上发送的数据包的源地址。
- *手动* — 指定作用隧道接口上发送数据包的源地址使用的 IPv4 地址。IPv4 地址移动到另一个接口时，隧道接口的本地地址不会改变。

  注 如果设备 IPv4 地址更改，隧道接口的本地地址也会更改。
- *接口* — 选择源接口。

• **ISATAP 路由器名** — 选择以下一个选项，以配置代表特定自动隧道路由器域名的全局字符串。

- *使用默认设置* — 始终为 ISATAP。
- *用户定义* — 输入路由器的域名。

步骤 5 输入参数。

• **ISATAP 请求间隔** — 未发现任何 ISATAP 路由器处于活动状态时，ISATAP 路由器请求消息之间的秒数。该间隔可以为**默认值**或**用户定义的**间隔。

• **ISATAP 健壮性** — 用于计算路由器请求查询的间隔。数字越大，查询越频繁。该间隔可以为**默认值**或**用户定义的**间隔

注 如果 IPv4 接口不在使用中，则 ISATAP 隧道不可用。

步骤 6 单击**应用**，以将 ISATAP 参数保存到当前配置文件中。

步骤 7 要删除 ISATAP 隧道，请单击**删除 ISATAP 隧道**按钮

IPv6 地址

为 IPv6 接口分配 IPv6 地址的步骤：

步骤 1 单击 **IP 配置** > **IPv6 管理和接口** > **IPv6 地址**。

步骤 2 要过滤表格，请选择一个接口名称，然后单击**转至**。系统会在 IPv6 地址表中显示该接口。除以下字段外，系统会在“添加”页面介绍这些字段：

• **地址源** — 显示以下地址源类型之一：“DHCP”、“系统”或“静态”。

• **DAD 状态** — 显示“重复访问检测”是否处于活动状态并且显示 DAD 状态。

• **首选有效期限** — 显示条目首选有效期限。

- **有效期限** — 显示条目有效期限。
- **到期时间** — 显示到期时间。

步骤 3 单击**添加**。

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。如果显示 *，则代表 IPv6 未启用但已配置。
- **IPv6 地址类型** — 选择要添加的 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。
  - *任播* — IPv6 地址为任播地址。该地址会分配到通常属于不同节点的一组接口。发送到任播地址的数据包将传输到任播地址确定的最近接口（由使用的路由协议定义）。

  注 如果 IPv6 地址位于 ISATAP 接口，则无法使用任播。
- **IPv6 地址** — 在第 2 层中，设备只支持一个 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。

  以下类型的地址可以添加到各种类型的隧道：
  - *添加到手动隧道* — 全局或任播地址
  - *添加到 ISATAP 隧道* — 含 EUI-6 的全局地址
  - *6to4 隧道* — 无
- **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。

IPv6 路由器配置

以下各节介绍了配置 IPv6 路由器的方法。其中包含以下主题：

- 路由器通告
- IPv6 前缀

路由器通告

IPv6 路由器可以将其前缀通告到邻居设备。此功能可以按接口启用或取消，如下所示：

步骤 1 单击 **IP 配置** > **IPv6 管理和接口** > **IPv6 路由器配置** > **路由器通告**。

步骤 2 要配置路由器通告表中列出的接口，请选择相应接口并单击**编辑**。

步骤 3 输入以下字段：

- **取消路由器通告** — 选择**是**可取消接口上的 IPv6 路由器通告传输。如果该功能未取消，请为以下字段输入值。
- **路由器偏好** — 选择路由器偏好：**低**、**中**或**高**。路由器通告消息将以此字段内配置的偏好发送。如果未配置偏好，将以中等偏好发送。

将偏好关联到路由器有时非常有用，例如，链路上的两个路由器提供等同（但不等价）的路由，且策略可能指示主机选择某个路由器。

- **包括通告间隔选项** — 选择该选项表示系统将使用通告选项。该选项告知访问移动节点该节点收到路由器通告的预计间隔。该节点可在其移动检测算法中使用此信息。
- **跳数限制** — 路由器通告的值。如果此值非零，主机会将其用作跳数限制。
- **受管地址配置标志** — 选择此标志可告知连接的主机应使用有状态的自动配置获取地址。主机可以同时使用有状态和无状态的地址自动配置。
- **其他具有状态的配置标志** — 选择此标志可告知连接的主机应使用有状态的自动配置获取其他（非地址）信息。

  注 如果设置了“受管地址配置标志”，无论此标志设置如何，连接的主机都可以使用有状态的自动配置获取其他（非地址）信息。

- **邻居请求重发间隔** — 设置间隔，确定解析地址或探测某个邻居的可达性时邻居请求消息重发之间的时间。
- **最长路由器通告间隔** — 输入路由器通告之间可经历的最长间隔时间。

如果使用此命令将路由器配置为默认路由器，则传输之间的间隔应小于或等于 IPv6 路由器通告有效期限。为阻止与其他 IPv6 节点同步，实际使用的间隔将在最大值和最小值之间随机选取。

- **最短路由器通告间隔** — 输入路由器通告之间可经历的最短间隔时间（**用户定义**），或选择**使用默认设置**以使用系统默认设置。

  注 最短路由器通告间隔不得超过最长路由器通告间隔的 75% 且不得短于 3 秒。

- **路由器通告有效期限** — 输入此路由器可继续用作默认路由器的剩余时间长度（秒）。如果为零，则表示路由器不再用作默认路由器。
- **可访问时间** — 输入远程 IPv6 节点为可访问状态的时间（**用户定义**），或选择**使用默认设置**选项使用系统默认设置。

步骤 4 单击**应用**，以将配置保存到当前配置文件中。

IPv6 前缀

定义设备接口上通告的前缀的步骤：

步骤 1 单击 **IP 配置** > **IPv6 管理和接口** > **IPv6 路由器配置** > **IPv6 前缀**。

步骤 2 如有需要，启用**过滤器**字段并单击**转至**。将显示与过滤器匹配的接口组。

步骤 3 要添加接口，请单击**添加**。

步骤 4 选择要添加前缀的所需 IPv6 接口。

步骤 5 输入以下字段：

- **前缀地址** — IPv6 网络。此参数必须以 RFC 4293 的形式记录，其中地址会使用以英文冒号分隔的 16 位值以十六进制格式指定。
- **前缀长度** — IPv6 前缀的长度。是一个十进制值，表示构成前缀（地址的网络部分）的地址高位的连续位数。十进制值之前必须加斜线。
- **前缀通告** — 选择该选项可通告前缀。
- **有效期限** — 此前缀继续有效的剩余时间长度（秒），即失效之前的时间。从已失效前缀生成的地址不应显示为数据包的目的地址或源地址。
  - *无限期* — 选择此值可将字段设置为 4,294,967,295，即无限期。
  - *用户定义* — 输入一个值。

- **首选有效期限** — 此前缀继续作为首选前缀的剩余时间长度（秒）。这段时间过后，前缀在新通信中将不再用作源地址，但接收自此类接口的数据包仍按计划处理。首选有效期限不得长于有效期限。
  - *无限期* — 选择此值可将字段设置为 4,294,967,295，即无限期。
  - *用户定义* — 输入一个值。
- **自动配置** — 使用接口上的无状态自动配置启用 IPv6 地址自动配置并启用接口上的 IPv6 处理。将根据路由器通告消息中接收的前缀配置地址
- **前缀状态** — 请选择以下选项之一：
  - *链接打开* — 将指定前缀配置为链接打开。将流量发送到包含指定前缀的地址的节点认为目标可在链路上本地访问。链接打开前缀作为已连接前缀（L 位集）插入到路由表中。
  - *没有打开链接* — 将指定前缀配置为没有打开链接。没有打开链接前缀作为已连接前缀插入到路由表中，但作为不带 L 位的前缀进行通告。
  - *链接断开* — 将特定前缀配置为链接断开。该前缀作为不带 L 位的前缀进行通告。该前缀不会作为已连接前缀插入到路由表中。如果该前缀已经作为已连接前缀在路由表中显示（例如，因为该前缀还通过添加 IPv6 地址的方式进行了配置），则将被删除。

步骤 6 单击**应用**，以将配置保存到当前配置文件中。

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）的设备默认路由器。设备会从列表中随机选择一个路由器。设备支持一个静态 IPv6 默认路由器。动态默认路由器是将路由器通告发送给设备 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 **IP 配置** > **IPv6 管理和接口** > **IPv6 默认路由器列表**。

该页面将为每个默认路由器显示以下字段：

- **传出接口** — 默认路由器所在的传出 IPv6 接口。
- **默认路由器 IPv6 地址** — 默认路由器的链路本地 IP 地址。
- **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。
- **度量标准** — 本步跳的成本。

步骤 2 单击**添加**以添加静态默认路由器。

步骤 3 输入以下字段：

- **下一步跳类型** — 数据包发送到的下一个目标 IP 地址。包括以下选项：
  - *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* — IPv6 接口和 IPv6 地址用于唯一标识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。
- **传出接口** — 显示传出链路本地接口。
- **默认路由器 IPv6 地址** — 静态默认路由器的 IP 地址。
- **度量标准** — 输入本步跳的成本。

步骤 4 单击**应用**。默认路由器将保存至当前配置文件。

IPv6 邻居

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）会显示与设备位于同一 IPv6 子网内的 IPv6 邻居的 MAC 地址。该表格是与 IPv4 ARP 表格对等的 IPv6 表格。当设备需要与其邻居进行通信时，设备会使用 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 **IP 配置** > **IPv6 管理和接口** > **IPv6 邻居**。

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。
- **路由器** — 指定邻居是否为路由器（**是**或**否**）。

步骤 2 要将邻居添加到表格中，请单击**添加**。

步骤 3 系统将显示以下字段：

- **接口** — 显示要添加的相邻 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 4 单击**应用**。将更新当前配置文件。

步骤 5 要将 IP 地址类型从**静态更改为动态**，请选择该地址，然后单击**编辑**，并使用“编辑 IPv6 邻居”页面。

IPv6 前缀列表

配置第一步跳安全后，可以根据 IPv6 前缀定义过滤规则。这些列表可在“IPv6 前缀列表”页面定义。

前缀列表将配置为包含**允许**或**拒绝**关键字，以根据匹配条件允许或拒绝前缀。隐式拒绝可应用于不匹配任何前缀列表条目的流量。

前缀列表条目包含一个 IP 地址和一个位掩码。IP 地址可用于有类网络、子网或单个主机路由。位掩码为介于 1 至 32 之间的数字。

前缀列表经过配置，使用 ge 和 le 关键字时，可根据精确前缀长度的匹配或范围内的匹配过滤流量。

大于和**小于**参数用于指定前缀长度的范围，并提供比仅使用网络/长度参数更灵活的配置。未指定**大于**或**小于**参数时，将使用精确匹配处理前缀列表。如果仅指定了**大于**参数，则范围在为**大于**输入的值到完整的 32 位长度之间。如果仅指定了**小于**，则范围在为网络/长度参数和**小于**输入的值之间。如果同时输入了**大于**和**小于**参数，则范围在**大于**值和**小于**值之间。

创建前缀列表的步骤：

步骤 1 单击 **IP 配置 > IPv6 管理接口 > IPv6 前缀列表**。

步骤 2 单击**添加**。

步骤 3 输入以下字段：

- **列表名称** — 请选择以下其中一个选项：
  - *使用目前列表* — 选择向之前定义的列表中添加一个前缀。
  - *创建新列表* — 输入名称，新建一个列表。
- **序列号** — 指定前缀在前缀列表中的位置。请选择以下其中一个选项：
  - *自动编号* — 将新的 IPV6 前缀置于前缀列表的最后一个条目之后。这个序号等于最后一个序号加 5。如果列表为空，则前缀列表的第一个条目将分配编号 5，后面的前缀列表条目编号将以 5 为增量递增。
  - *用户定义* — 将新的 IPV6 前缀置于参数定义的位置。如果已存在带有该编号的条目，则将其替换为新的条目。
- **规则类型** — 输入前缀列表的规则：
  - *允许* — 允许与条件匹配的网络。
  - *拒绝* — 拒绝与条件匹配的网络。
  - *说明* — 文本。
- **IPv6 前缀** — IP 路由前缀。
- **前缀长度** — IP 路由前缀的长度。
- **大于** — 要用于匹配的最小前缀长度。请选择以下其中一个选项：
  - *无限制* — 没有要用于匹配的最小前缀长度。
  - *用户定义* — 要匹配的最小匹配长度。
- **小于** — 要用于匹配的最大前缀长度。请选择以下其中一个选项：
  - *无限制* — 没有要用于匹配的最大前缀长度。
  - *用户定义* — 要匹配的最大匹配长度。
- **说明** — 输入前缀列表的说明。

步骤 4 单击**应用**，以将配置保存到当前配置文件中。

IPv6 路由

IPv6 转发表包括多个已配置的路由。其中一个路由是默认路由 (IPv6 address:0)，该路由使用从“IPv6 默认路由器列表”中选择的默认路由器，将数据包传送给与设备不在同一 IPv6 子网内的目的设备。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。如果设备使用的默认路由器不是将流量传输到设备要与其进行通信的 IPv6 子网的路由器，则会发生这种情况。

查看 IPv6 路由的步骤：

单击 **IP 配置** > **IPv6 管理和接口** > **IPv6 路由**。

此页面显示了以下字段：

- **IPv6 前缀** — 目标 IPv6 子网地址的 IP 路由前缀。
- **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。
- **传出接口** — 用于转发数据包的接口。
- **下一跳** — 数据包转发到的目标地址的类型。通常，该地址为相邻路由器的地址。可采用以下类型之一。
  - *链路本地* — IPv6 接口和 IPv6 地址用于唯一标识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。
  - *点到点* — 点到点隧道。
- **度量标准** — 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：
  - *S（静态）* — 条目是由用户手动配置的。
  - *I（ICMP 重定向）* — 条目是使用 ICMP 重定向消息从 IPv6 路由器接收的 ICMP 重定向动态路由。
  - *ND（路由器通告）* — 条目是从路由器通告消息获取的。

步骤 1 要添加新路由，请单击**添加**，然后填写上述字段。此外，还要填写以下字段：

- **IPv6 地址** — 添加新路由的 IPv6 地址。

步骤 2 单击**应用**保存更改。

DHCPv6 中继

本节包含以下主题：

- 全局目标
- 接口设置

DHCPv6 中继用于向 DHCPv6 服务器中继 DHCPv6 消息。定义见于 RFC 3315。

如果 DHCPv6 客户端未直接连接到 DHCPv6 服务器，此 DHCPv6 客户端直接连接的 DHCPv6 中继代理（设备）会封装接收自直接连接的 DHCPv6 客户端的消息，并将其转发到 DHCPv6 服务器。

在相反方向，中继代理会解开接收自 DHCPv6 服务器的数据包封装，并将其转发到 DHCPv6 客户端。

用户必须配置数据包转发的目的 DHCP 服务器。可配置两组 DHCPv6 服务器：

- **全局目标** — 数据包始终中继到这些 DHCPv6 服务器。
- **接口列表** — 这是按接口列出的 DHCPv6 服务器。接口上接收到 DHCPv6 数据包后，数据包会中继到接口列表（如果存在）上的服务器和全局目标列表上的服务器。

与其他功能的依赖性

DHCPv6 客户端与 DHCPv6 中继功能在同一接口上相互排斥。

全局目标

配置作为所有 DHCPv6 数据包中继目标的 DHCPv6 服务器列表的步骤：

步骤 1 单击 **IP 配置 > IPv6 管理和接口 > DHCPv6 中继 > 全局目标**。

步骤 2 要添加默认 DHCPv6 服务器，请单击**添加**。

步骤 3 输入以下字段：

- **IPv6 地址类型** — 输入客户端消息转发到的目的地址类型。地址类型可以是**链路本地**、**全局**或**组播** (All_DHCP_Relay_Agents_and_Servers)。
- **DHCPv6 服务器 IP 地址** — 输入作为数据包转发目标的 DHCPv6 服务器地址。
- **IPv6 接口** — 输入当 DHCPv6 服务器地址类型为**链路本地**或**组播**时穿上数据包的目标接口。接口可以为 VLAN、LAG 或隧道。

步骤 4 单击**应用**。将更新当前配置文件。

接口设置

在接口上启用 DHCPv6 中继功能以及配置作为 DHCPv6 数据包中继目标（在接口上收到这些数据包时）的 DHCPv6 服务器的步骤：

步骤 1 单击 **IP 配置 > IPv6 管理和接口 > DHCPv6 中继 > 接口设置**。

步骤 2 要在接口上启用 DHCPv6 并选择性地为某个接口添加 DHCPv6 服务器，请单击**添加**。

输入以下字段：

- **源接口** — 选择启用 DHCPv6 中继的接口（端口、LAG、VLAN 或隧道）。
- **只使用全局目标** — 选择该选项仅将数据包转发到 DHCPv6 全局目标服务器。
- **IPv6 地址类型** — 输入客户端消息转发到的目的地址类型。地址类型可以是**链路本地**、**全局**或**组播** (All_DHCP_Relay_Agents_and_Servers)。
- **DHCPv6 服务器 IP 地址** — 输入作为数据包转发目标的 DHCPv6 服务器地址。
- **目标 IPv6 接口** — 输入当 DHCPv6 服务器地址类型为**链路本地**或**组播**时传输数据包的接口。

步骤 3 单击**应用**。将更新当前配置文件。

域名系统

域名系统 (DNS) 会将域名转换为 IP 地址，以找到这些主机并对其进行寻址。

作为一个 DNS 客户端，设备可通过使用一个或多个配置的 DNS 服务器将域名解析为 IP 地址。

DNS 设置

使用“DNS 设置”页面可启用 DNS 功能、配置 DNS 服务器，以及设置设备使用的默认域名。

步骤 1 单击 **IP 配置** > **DNS** > **DNS 设置**。

步骤 2 在基本模式下，输入以下参数：

- **服务器定义** — 选择以下其中一个选项来定义 DNS 服务器：
  - *按 IP 地址* — 将为 DNS 服务器输入 IP 地址。
  - *已禁用* — 不定义任何 DNS 服务器。
- **服务器 IP 地址** — 如果您选择了上述“按 IP 地址”，请输入 DNS 服务器的 IP 地址。
- **默认域名** — 输入用于完成不合格主机名的 DNS 域名。设备会对将此部分追加到非完全限定域名 (NFQDN) 后面，以将其转换为 FQDN。

  注 不要加入使不合格名称与域名（例如 cisco.com）分离开的起始句点。

步骤 3 在高级模式下，输入以下参数。

- **DNS** — 选择该选项可将设备指定为一个 DNS 客户端，它可通过一个或多个配置的 DNS 服务器将 DNS 名称解析为 IP 地址。
- **轮询重试次数** — 输入在设备决定 DNS 服务器不存在之前向 DNS 服务器发送 DNS 查询的次数。
- **轮询超时** — 输入设备等待 DNS 查询响应的时间（以秒为单位）。
- **轮询间隔** — 输入超出重试次数后设备发送 DNS 查询数据包的间隔时间（以秒为单位）。
  - *使用默认设置* — 选择使用默认值。

    此值 = 2 *(轮询重试次数 + 1)* 轮询超时
  - *用户定义* — 选择该选项可输入用户定义的值。
- **默认参数** — 输入以下默认参数：
  - *默认域名* — 输入用于完成不合格主机名的 DNS 域名。设备会对将此部分追加到非完全限定域名 (NFQDN) 后面，以将其转换为 FQDN。

    注 不要加入使不合格名称与域名（例如 cisco.com）分离开的起始句点。
  - *DHCP 域搜索列表* — 单击**详情**查看设备上配置的 DNS 服务器列表。

步骤 4 单击**应用**。将更新当前配置文件。

DNS 服务器表为配置的每个 DNS 服务器显示以下信息：

- **DNS 服务器** — DNS 服务器的 IP 地址。
- **偏好** — 每个服务器都有偏好值，值越低代表使用几率越高。
- **源** — 服务器 IP 地址源（静态、DHCPv4 或 DHCPv6）。
- **接口** — 服务器 IP 地址接口。

步骤 5 您最多可定义八个 DNS 服务器。要添加 DNS 服务器，请单击**添加**。

步骤 6 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”，请选择接收的接口。
- **DNS 服务器 IP 地址** — 输入 DNS 服务器的 IP 地址。
- **偏好** — 选择可确定域使用顺序（从低到高）的值。该选项可有效确定在 DNS 查询过程中不合格名称的完成顺序。

步骤 7 单击**应用**。DNS 服务器将保存至当前配置文件。

搜索列表

搜索列表包含一个由用户使用 DNS 设置页面定义的静态条目和接收自 DHCPv4 与 DHCPv6 服务器的动态条目。

要查看设备上已配置的域名，请单击 **IP 配置** > **DNS** > **搜索列表**。

将为设备上配置的每个 DNS 服务器显示以下字段。

- **域名** — 设备上可使用的域的名称。
- **源** — 该域的服务器 IP 地址源（静态、DHCPv4 或 DHCPv6）。

- **接口** — 该域的服务器 IP 地址接口。
- **偏好** — 使用域的顺序（从低到高）。该选项可有效确定在 DNS 查询过程中不合格名称的完成顺序。

主机映射

主机名/IP 地址映射存储在主机映射表（DNS 缓存）中。

该缓存可包含以下类型的条目：

- **静态条目** — 手动添加到缓存的映射对。最多 64 条静态条目。
- **动态条目** — 这些映射对可以在用户使用后由系统添加，也可以是 DHCP 针对设备上配置的每个 IP 地址添加的条目。可以有 256 条动态条目。

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 服务器支持 8 个 IP 地址。

添加主机名及其 IP 地址的步骤：

步骤 1 单击 **IP 配置** > **DNS** > **主机映射**。

步骤 2 如果需要，选择**清除表**选项，以清除主机映射表中的部分或全部条目。

- **仅静态** — 删除静态主机。
- **仅动态** — 删除动态主机。
- **全部动态和静态** — 删除静态和动态主机。

主机映射表将显示以下字段：

- **主机名** — 用户定义的主机名或完全限定的名称。
- **IP 地址** — 主机 IP 地址。
- **IP 版本** — 主机 IP 地址的 IP 版本。
- **类型** — 对缓存而言是**动态**还是**静态**条目。
- **状态** — 显示尝试访问主机的结果
  - *确定* — 尝试已成功。
  - *负高速缓存* — 尝试失败，请勿再次尝试。
  - *未响应* — 没有响应，但系统可稍后继续尝试。

- **TTL（秒）**— 如果是动态条目，则表示将在缓存中保存的时间。
- **剩余 TTL（秒）**— 如果是动态条目，则表示可在缓存中保存的剩余时间。

步骤 3 要添加主机映射，请单击**添加**。

步骤 4 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”，请选择接收的接口。
- **主机名** — 输入用户定义的主机名或完全合格的名称。主机名只能包含从 A 到 Z 的 ASCII 字母、数字 0 到 9、下划线和连字符。句点 (.) 用于分隔标签。
- **IP 地址** — 输入单个 IP 地址或最多八个相关的 IP 地址（IPv4 或 IPv6）。

步骤 5 单击**应用**。设置将保存到当前配置文件中。

17

安全

本节介绍设备安全和访问控制。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设备的权限：

- 密码强度
- 管理访问方法
- 管理访问验证
- SSL 服务器

以下各节介绍针对设备 CPU 的防攻击保护：

- TCP/UDP 服务
- 风暴控制
- 访问控制

以下各节介绍了如何通过设备控制终端用户对网络的访问：

- 管理访问方法
- RADIUS
- 端口安全

以下各节介绍了对其他网络用户的防御。这些攻击通过设备进行，而非针对设备。

- 拒绝服务防护
- SSL 服务器
- 风暴控制
- 端口安全
- 访问控制

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。

可以将设备配置为可使用 RADIUS 服务器提供集中安全保护的 RADIUS 客户端，也可以配置为 RADIUS 服务器。

RADIUS 客户端

组织可以将设备用作远程授权拨入用户服务 (RADIUS) 服务器，为其所有设备提供集中的 802.1X 或基于 MAC 的网络访问控制。通过这种方式，对组织内所有设备的验证和授权可在一台服务器上执行。

将设备配置为 RADIUS 客户端后，它可以使用 RADIUS 服务器执行以下服务：

- **验证** — 对使用用户名和用户定义的密码登录到设备的常规用户和 802.1X 用户进行验证。
- **授权** — 在登录时执行此服务。验证会话完成之后，将使用经验证的用户名开始授权会话。然后，RADIUS 服务器将检查用户权限。

记帐 — 使用 RADIUS 服务器启用登录会话记帐功能。让系统管理员可以从 RADIUS 服务器生成记帐报告。用于 RADIUS 服务器记帐且可由用户配置的 TCP 端口与用于 RADIUS 服务器验证与授权的 TCP 端口是同一端口。

默认设置

以下默认设置与此功能相关：

- 默认情况下未定义默认 RADIUS 服务器。
- 配置 RADIUS 服务器时，默认情况下记帐功能会禁用。

Radius 工作流程

要使用 RADIUS 服务器，请执行以下操作：

步骤 1 在 RADIUS 服务器上开立一个设备帐户。

步骤 2 在 RADIUS 页面和“添加 RADIUS 服务器”页面配置服务器和其他参数。

注 如果配置了多个 RADIUS 服务器，设备将使用已配置的可用 RADIUS 服务器优先级选择设备要使用的 RADIUS 服务器。

设置 RADIUS 服务器参数的步骤：

步骤 1 单击**安全** > **RADIUS 客户端**。

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，则设备将使用这些字段中的值。

- **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** — 输入设备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** — 输入用于在设备与 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 接口** — 选择要在与 RADIUS 服务器通信的消息中使用的设备 IPv4 源接口。
- **源 IPv6 接口** — 选择要在与 RADIUS 服务器通信的消息中使用的设备 IPv6 源接口。

  注 如果已选择“自动”选项，系统将使用传出接口上定义的 IP 地址的源 IP 地址。

步骤 3 单击**应用**。设备 RADIUS 默认设置将在当前配置文件中更新。

若要添加 RADIUS 服务器，请单击**添加**。

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**。

- **服务器定义** — 选择是按照 IP 地址还是名称来指定 RADIUS 服务器。
- **IP 版本** — 选择 RADIUS 服务器 IP 地址的版本。

- **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”）。
- **服务器 IP 地址/名称** — 按照 IP 地址或名称输入 RADIUS 服务器。
- **优先级** — 输入服务器的优先级。优先级可确定设备尝试联系服务器以验证用户的顺序。设备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设备与 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。密钥可以**加密**或**明文**形式输入。如果选择**使用默认设置**，设备将尝试使用默认的密钥字符串验证 RADIUS 服务器。
- **应答超时** — 选择**用户定义**并输入设备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**，设备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** — 选择**用户定义**并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**，设备将使用重试次数的默认值。
- **无响应时间** — 选择**用户定义**并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**，设备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设备的用户。
  - *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设备的用户和 802.1X 验证。

步骤 5 单击**应用**。RADIUS 服务器定义将添加到设备的当前配置文件中。

步骤 6 要以明文形式显示页面中的敏感数据，请单击**将敏感数据显示为明文模式**。

密码强度

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。

有关如何创建用户账户的信息，请参阅用户帐户。

由于密码用于验证访问设备的用户，所以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。

定义密码复杂性规则的步骤：

步骤 1 单击**安全** > **密码强度**。

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、数字和标准键盘上可用的特殊字符）。
- 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。
- 不能与制造商名重复，不能是以反向顺序排列的制造商名，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** — 输入密码所需的最小字符数。

  注 可以设置零长度密码（无密码），而且依然可以为其分配密码过期时间。

- **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。

注 您可以通过 CLI 配置用户名 — 密码等效值和制造商 — 密码等效值。有关详情，请参阅 *CLI 参考指南*。

管理访问方法

本节介绍各种管理方法的访问规则。

其中包含以下主题：

- 访问模板
- 模板规则

访问模板用于确定如何验证和授权通过各种访问方法访问设备的用户。访问模板可以限制来自特定源的管理访问。

只有通过活动的访问模板和管理访问验证方法的用户才会获得对设备的管理访问权限。

在任何时间设备上只能有一个访问模板处于活动状态。

访问模板由一个或多个规则组成。按照访问模板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** — 访问和管理设备的方法：
  - Telnet
  - 安全 Telnet (SSH)

- 超文本传输协议 (HTTP)
- 安全 HTTP (HTTPS)
- 简单网络管理协议 (SNMP)
- 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 的配置实用程序的端口、LAG 或 VLAN。
- **源 IP 地址** — IP 地址或子网。各用户组对管理方法的访问权限可能有所不同。例如，一个用户组可能只能使用 HTTPS 会话来访问设备模块，而另一个用户组可能能够使用 HTTPS 会话和 Telnet 会话来访问设备模块。

访问模板

“访问模板”页面可显示已定义的访问模板，并可用来选择一个将要处于活动状态的访问模板。

当用户尝试通过一种访问方法访问设备时，设备需要查看活动的访问模板是否明确允许通过此方法对设备进行管理访问。如果找不到匹配项，则拒绝进行访问。

当访问设备的尝试违反了活动的访问模板时，设备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，请参阅模板规则。

使用“访问模板”页面可以创建访问模板，并添加第一个规则。如果访问模板只包含一个规则，则添加工作即已完成。若要向模板添加其他规则，请使用“模板规则配置”页面。

步骤 1 单击**安全** > **管理访问方法** > **访问模板**。

此页面显示所有处于和未处于活动状态的访问模板。

步骤 2 要更改当前选中的访问模板，请从**当前选中的访问模板**下拉菜单中选择一个模板，然后单击**应用**。此操作可使选择的模板成为当前选中的访问模板。

当您选择任何其他访问模板时，系统会根据选择的访问模板显示警告消息，提醒您系统可能会断开您与基于 Web 的配置实用程序的连接。

步骤 3 单击**确定**以选择当前选中的访问模板，或单击**取消**以停止此操作。

步骤 4 单击**添加**以打开“添加访问模板”页面。您可以使用该页面配置新模板和一个规则。

步骤 5 输入**访问模板名称**。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设备。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。最高优先级为“1”。
- **管理方法** — 选择定义规则所针对的管理方法。选项如下：
  - *全部* — 将所有管理方法分配给规则。
  - *Telnet* — 符合 Telnet 访问模板标准的用户，在请求访问设备时，会获得允许或遭到拒绝。
  - *安全 Telnet (SSH)* — 请求访问符合 SSH 访问模板标准设备的用户，会获得允许或遭到拒绝。
  - *HTTP* — 请求访问符合 HTTP 访问模板标准的设备的用户，会获得允许或遭到拒绝。
  - *安全 HTTP (HTTPS)* — 符合 HTTPS 访问模板标准的用户，在请求访问设备时，会获得允许或遭到拒绝。
  - *SNMP* — 符合 SNMP 访问模板标准的用户，在请求访问设备时，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* — 如果用户与模板中的设置相匹配，则允许该用户访问设备。
  - *拒绝* — 如果用户与模板中的设置不匹配，则拒绝该用户访问设备。
- **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（如果已选择“用户定义”）。
- **应用到源 IP 地址** — 选择访问模板适用的源 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** — 输入源 IP 地址版本：版本 6 或版本 4。
- **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**。访问模板将写入当前配置文件中。现在，您可以选择此访问模板作为当前选中的访问模板。

模板规则

访问模板最多可包含 128 个规则，以确定有权管理和访问设备的人以及可能使用的访问方法。

访问模板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。如果在活动的访问模板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 地址对设备的访问，仅允许分配到 IT 管理中心的 IP 地址访问设备。这样一来，仍可以管理设备，并使其获得另一层的安全。

将模板规则添加到访问模板的步骤：

步骤 1 单击**安全** > **管理访问方法** > **模板规则**。

步骤 2 选择“过滤器”字段，然后选择一个访问模板。单击**转至**。

选择的访问模板将显示在模板规则表中。

步骤 3 单击**添加**添加一条规则。

步骤 4 输入参数。

- **访问模板名称** — 选择一个访问模板。
- **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设备。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** — 选择定义规则所针对的管理方法。选项如下：
  - *全部* — 将所有管理方法分配给规则。
  - *Telnet* — 符合 Telnet 访问模板标准的用户，在请求访问设备时，会获得允许或遭到拒绝。

- *安全 Telnet (SSH)* — 符合 Telnet 访问模板标准的用户，在请求访问设备时，会获得允许或遭到拒绝。
- *HTTP* — 将 HTTP 访问分配给规则。符合 HTTP 访问模板标准的用户，在请求访问设备时，会获得允许或遭到拒绝。
- *安全 HTTP (HTTPS)* — 符合 HTTPS 访问模板标准的用户，在请求访问设备时，会获得允许或遭到拒绝。
- *SNMP* — 符合 SNMP 访问模板标准的用户，在请求访问设备时，会获得允许或遭到拒绝。

- **操作** — 选择以下选项之一：
  - *允许* — 允许来自此规则定义的接口和 IP 源的用户访问设备。
  - *拒绝* — 拒绝来自此规则定义的接口和 IP 源的用户访问设备。
- **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** — 选择访问模板适用的源 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**，将规则添加到访问模板。

管理访问验证

您可以为各种管理访问方法分配验证方法，例如 SSH、Telnet、HTTP 和 HTTPS。可以在本地或在 RADIUS 服务器上执行此验证。

如果启用授权，系统会验证用户的身份和读/写权限。如果未启用授权，系统仅验证用户的身份。

使用的授权/验证方法取决于选择验证方法的顺序。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授权/验证。

如果启用授权，并且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设备。换句话说，如果某种验证方法验证失败，则设备会停止验证尝试；设备不会继续工作，且不会尝试使用下一个验证方法。

同样，如果未启用授权并且某种方法验证失败，则设备会停止验证尝试。

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**。

步骤 2 输入管理访问方法的**应用**（类型）。

步骤 3 选择**验证**按照下述方法列表启用用户验证和授权。如果未选择该字段，则仅执行验证。如果启用授权，系统会检查用户的读/写权限。此权限级别在“用户帐户”页面中设置。

步骤 4 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 服务器上对用户进行授权/验证。您必须已配置了一个或多个 RADIUS 服务器。为了使 RADIUS 服务器能够授予对基于 Web 的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。
- *无* — 允许用户在未经授权/验证的情况下访问设备。
- *本地* — 根据存储在本地设备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 5 单击**应用**。选择的验证方法将与访问方法相关联。

SSL 服务器

本节介绍安全套接字层 (SSL) 功能。

其中包含以下主题：

- SSL 概述
- 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。

默认情况下，设备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。

新建证书的步骤：

步骤 1 单击**安全 > SSL 服务器 > SSL 服务器验证设置**。

SSL 服务器密钥表中会显示 **SSL 活动证书编号** 1 和 2 的信息。请选择以下字段之一。

除以下字段之外，相关字段会在**编辑**页面中定义：

- **有效起始日期** — 指定证书有效期的开始日期。
- **有效终止日期** — 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 单击**生成证书请求**。

步骤 4 输入以下字段：

- **证书 ID** — 选择活动证书。
- **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。
- **证书请求** - 显示按**生成证书请求**按钮时创建的密钥。

步骤 5 单击**生成证书请求**。此操作将会生成密钥，必须在证书颁发机构 (CA) 中输入该密钥。从**证书请求**字段复制该密钥。

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**。

步骤 2 单击**导入证书**。

步骤 3 输入以下字段：

- **证书 ID** — 选择活动证书。
- **证书来源** — 显示证书为用户定义。
- **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。
- **公钥** — 复制到 RSA 公钥中。
- **私钥（加密模式）** — 选择并复制到加密形式的 RSA 私钥中。
- **私钥（明文模式）** — 选择并复制到明文形式的 RSA 私钥中。

步骤 4 单击**应用**将更改应用到当前配置。

步骤 5 单击**将敏感数据显示为加密模式**能够以加密模式显示此密钥。单击此按钮后，私钥会以加密形式写入配置文件（单击“应用”后）。当文本以加密形式显示时，此按钮会变为**将敏感数据显示为明文模式**，让您可以再次以明文形式查看文本。

详情按钮显示证书和 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，私钥会以加密形式显示。

在设备上创建新的自生成证书的步骤：

步骤 1 单击**安全 > SSL 服务器 > SSL 服务器验证设置**。

步骤 2 选择一个证书，然后单击**编辑**。

步骤 3 根据需要输入以下字段：

- **重新生成 RSA 密钥** - 选择此项可重新生成 RSA 密钥。
- **密钥长度** — 从选项中选择所需的密钥长度。
- **通用名称** — 输入一个通用名称。
- **组织单元** — 为证书输入组织单元名称。
- **位置** — 为证书输入组织单元所在的位置。
- **省/自治区/直辖市** — 为证书输入组织单元所在的省/自治区/直辖市。
- **国家/地区** — 为证书输入组织单元所在的国家/地区。
- **持续时间** — 输入让证书在多长时间内保持有效。

步骤 4 单击**应用**将更改应用到当前配置。

SSH 客户端

请参阅安全：SSH 客户端。

TCP/UDP 服务

出于安全考虑，通常会通过“TCP/UDP 服务”页面在设备上启用基于 TCP 或基于 UDP 的服务。

设备可提供以下 TCP/UDP 服务：

- **HTTP** — 出厂默认设置为启用
- **HTTPS** — 出厂默认设置为启用
- **SNMP** — 出厂默认设置为禁用
- **Telnet** — 出厂默认设置为禁用
- **SSH** — 出厂默认设置为禁用

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**。

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。
- **SNMP 服务** — 表示 SNMP 服务是处于启用状态还是禁用状态。
- **Telnet 服务** — 表示 Telnet 服务是处于启用状态还是禁用状态。
- **SSH 服务** — 表示 SSH 服务器服务是处于启用状态还是禁用状态。

步骤 3 单击**应用**。服务将写入当前配置文件中。

TCP 服务表针对每个服务显示以下字段：

- **服务名称** — 设备正通过其提供 TCP 服务的访问方法。
- **类型** — 服务所使用的 IP 协议。
- **本地 IP 地址** — 设备正通过其提供服务的本地 IP 地址。
- **本地端口** — 设备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** — 设备正通过其提供 UDP 服务的访问方法。
- **类型** — 服务所使用的 IP 协议。
- **本地 IP 地址** — 设备正通过其提供服务的本地 IP 地址。
- **本地端口** — 设备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。）

风暴控制

本节介绍风暴控制。其中包含以下主题：

- 风暴控制
- 风暴控制统计信息

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设备的帧数，并定义计入此限制的帧类型。

如果广播、组播或未知单播帧速率高于用户定义的阈值，超过阈值的帧将被丢弃。

风暴控制

定义风暴控制的步骤：

步骤 1 单击**安全** > **风暴控制** > **风暴控制设置**。

步骤 2 选择一个端口，然后单击**编辑**。

步骤 3 输入参数。

- **接口** — 选择已启用风暴控制的端口。

未知单播风暴控制

- **风暴控制状态** — 选择该选项可启用单播数据包风暴控制。
- **速率阈值** — 输入可用来转发未知数据包的最大速率。该值可以按**千位/秒**或**按总可用带宽的百分比**输入。
- **风暴中生成陷阱** — 选择此选项可在端口上发生风暴时发送陷阱。如果不选择此选项，则不发送陷阱。
- **风暴中关闭** — 选择此选项可在端口上发生风暴时关闭端口。如果不选择此选项，则丢弃额外流量。

组播风暴控制

- **风暴控制状态** — 选择该选项可启用组播数据包的风暴控制。
- **组播类型** — 选择以下其中一个实施风暴控制的组播数据包的类型：
  - *全部* — 在端口上的所有组播数据包上启用风暴控制。
  - *已注册组播* — 仅在端口上的已注册组播地址上启用风暴控制。
  - *未注册的组播* — 在端口上仅启用未注册的组播风暴控制。
- **速率阈值** — 输入可用来转发未知数据包的最大速率。该值可以按**千位/秒**或**按总可用带宽的百分比**输入。
- **风暴中生成陷阱** — 选择此选项可在端口上发生风暴时发送陷阱。如果不选择此选项，则不发送陷阱。
- **风暴中关闭** — 选择此选项可在端口上发生风暴时关闭端口。如果不选择此选项，则丢弃额外流量。

广播风暴控制

- **风暴控制状态** — 选择该选项可启用广播数据包风暴控制。
- **速率阈值** — 输入可用来转发未知数据包的最大速率。该值可以按**千位/秒**或**按总可用带宽的百分比**输入。
- **风暴中生成陷阱** — 选择此选项可在端口上发生风暴时发送陷阱。如果不选择此选项，则不发送陷阱。
- **风暴中关闭** — 选择此选项可在端口上发生风暴时关闭端口。如果不选择此选项，则丢弃额外流量。

步骤 4 单击**应用**。将修改风暴控制，并更新当前配置文件。

风暴控制统计信息

查看风暴控制统计信息的步骤：

步骤 1 单击**安全** > **风暴控制** > **风暴控制统计信息**。

步骤 2 选择一个接口。

步骤 3 输入**刷新速率** — 选择统计信息的刷新频率。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。

系统为未知单播、组播和广播风暴控制显示以下统计信息：

- **组播流量类型** —（仅用于组播流量）已注册或未注册。
- **传递的字节数** — 接收的字节数。
- **丢弃的字节数** — 由于风暴控制而被丢弃的字节数。
- **上次丢弃时间** — 丢弃最后一个字节的时间。

步骤 4 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，请选择该接口并单击**清除接口计数器**。

端口安全

注 无法在启用了 802.1X 的端口或定义为 SPAN 目标的端口上启用端口安全。

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** — 设备学习的 MAC 地址数不超过配置的允许地址极限。达到极限之后，设备不会学习其他地址。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（前提是已将配置保存到启动配置文件）。新的 MAC 地址可作为永久安全地址学习，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。
- **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，系统将转发帧，但不会学习该端口上的 MAC 地址。

除了以上这些操作，您还可以生成陷阱，并限制其频率和数量以避免设备过载。

配置端口安全的步骤：

步骤 1 单击**安全** > **端口安全**。

步骤 2 选择要修改的接口，然后单击**编辑**。

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**）。禁用重新学习和老化。
  - *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设备之前，该端口将保持关闭状态。
- **陷阱** — 选择该选项可在锁定端口接收到数据包时启用陷阱。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。
- **陷阱频率** — 输入陷阱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。

802.1X 验证

请参阅安全：802.1X 验证一章，了解有关 802.1X 验证的信息。

拒绝服务防护

拒绝服务 (DoS) 攻击是指黑客企图使用户无法使用设备。

DoS 攻击使用外部通信请求让设备饱和，导致其无法响应合法的流量。此类攻击通常会导致设备 CPU 过载。

- Martian 地址
- SYN 过滤
- SYN 速率保护
- ICMP 过滤
- IP 分片过滤

安全核心技术 (SCT)

设备用于抵御 DoS 攻击的方法之一是使用 SCT。默认情况下，SCT（安全核心技术）在设备上已启用，且不能被禁用。

思科设备是一种高级设备，除终端用户 (TCP) 流量之外还可以处理管理流量、协议流量和侦听流量。

SCT 确保设备可以接收和处理管理和协议流量，无论收到的总流量为多少。这可通过限制流向 CPU 的 TCP 流量速率来实现。

该功能与其他功能间没有交互。

可以在安全套件设置页面（**详情**按钮）中监控 SCT。

DoS 攻击类型

DoS 攻击可通过以下方式发起（仅列举部分）：

- TCP SYN 数据包 — TCP SYN 数据包洪流（通常带有错误的发送者地址）可引发攻击。每个数据包通过发回 TCP/SYN-ACK 数据包（确认）并等待来自发送者地址的数据包（响应 ACK 数据包）导致设备生成半开放式连接。但是，由于发送者地址是错误的，所以永远不会收到响应。这种半开放式连接导致设备原先可提供的可用连接数减少，因此无法响应合法请求。此外，CPU 可接收的潜在数据包数量有限，而攻击流量可能会占用此数据包数量。

  可在“SYN 保护”页面阻止这些数据包。

- TCP SYN-FIN 数据包 — 发送 SYN 数据包可创建新的 TCP 连接。发送 TCP FIN 数据包可关闭连接。不能存在同时带有 SYN 和 FIN 标签的数据包。因此，这些数据包可能会攻击设备，应阻止这些数据包。

  可在“SYN 保护”页面设置构成 SYN 攻击的定义。当设备在接口上发现此类攻击时，将在此页面进行报告。

针对 DoS 攻击的防御措施

*拒绝服务 (Do*S) 防护功能通过以下方式帮助系统管理员抵御 DoS 攻击：

- 启用 TCP SYN 保护。如果启用了此功能，系统将在发现 SYN 数据包攻击时发送报告。如果每秒 SYN 数据包数超出用户配置的阈值，将判断为 SYN 攻击。
- SYN-FIN 数据包可被阻止。

功能之间的依赖性

此功能与其他功能不相互依赖。

默认配置

DoS 防护功能有以下默认设置：

- 默认情况下，DoS 防护功能为禁用状态。
- 默认启用 SYN-FIN 防护（即使已禁用 DoS 防护）。
- 如果启用了 SYN 保护，默认设置为“报告”。默认阈值为每秒 30 个 SYN 数据包。
- 默认情况下，其他所有 DoS 防护功能均为禁用状态。

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** > **拒绝服务防护** > **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 使用率**旁边的**详情**，以转到 CPU 使用率页面并查看 CPU 资源使用率信息。

步骤 3 单击 **TCP SYN 保护**旁边的**编辑**以设置该功能。

步骤 4 选择 **DoS 防护**以启用该功能。

- **禁用** — 禁用该功能。
- **系统级预防** — 启用该部分功能可阻止 Stacheldraht Distribution、Invasor Trojan 和 Back Orifice Trojan 的攻击。
- **系统级和接口级预防** — 启用部分功能可阻止 Stacheldraht Distribution、Invasor Trojan 和 Back Orifice Trojan 的攻击。

步骤 5 如果选择**系统级预防**或**系统级预防和接口级预防**，则会启用以下一个或多个“DoS 防护”选项：

- **Stacheldraht Distribution** — 丢弃源 TCP 端口等于 16660 的 TCP 数据包。
- **Invasor Trojan** — 丢弃目的 TCP 端口等于 2140、源 TCP 端口等于 1024 的 TCP 数据包。
- **Back Orifice Trojan** — 丢弃目的 UDP 端口等于 31337、源 UDP 端口等于 1024 的 UDP 数据包。

步骤 6 根据需要单击以下选项：

- **Martian 地址** — 单击**编辑**，转至 Martian 地址页面。
- **SYN 过滤** — 单击**编辑**，转至 SYN 过滤页面。
- **SYN 速率保护** -（仅在第 2 层）单击**编辑**，转至 SYN 速率保护页面。
- **ICMP 过滤** — 单击**编辑**，转至 ICMP 过滤页面。
- **IP 分片** — 单击**编辑**，转至 IP 分片过滤页面。

步骤 7 单击**应用**。拒绝服务防护安全套件设置将写入当前配置文件中。

SYN 保护

在 SYN 攻击中，黑客可能利用网络端口对设备进行攻击，这将消耗 TCP 资源（缓存）和 CPU 功率。

由于 CPU 使用 SCT 进行保护，流向 CPU 的 TCP 流量会受到限制。但是，如果一个或多个端口受到高速 SYN 数据包的攻击，CPU 仅接收攻击程序的数据包，从而导致拒绝服务。

使用 SYN 保护功能时，CPU 计算每秒从每个网络端口进入 CPU 的 SYN 数据包数。

如果该数量高于阈值，将生成系统日志消息，但不会阻止数据包。

配置 SYN 保护的步骤：

步骤 1 单击**安全** > **拒绝服务防护** > **SYN 保护**。

步骤 2 输入参数。

- **阻止 SYN-FIN 数据包** — 选择此项以启用此功能。所有端口均丢弃了同时带 SYN 和 FIN 标签的所有 TCP 数据包。
- **SYN 保护模式** — 在以下三种模式间选择：
  - *禁用* — 在特定接口上禁用此功能。
  - *报告* — 生成系统日志消息。超过阈值时端口状态会更改为**被攻击**。
  - *阻止并报告* — 发现 TCP SYN 攻击后，指定给系统的 TCP SYN 数据包将被丢弃，端口状态将更改为**已阻止**。
- **SYN 保护阈值** — SYN 数据包阻止前每秒可通过的 SYN 数据包数（将对端口应用符合 MAC-to-me 规则的拒绝 SYN）。
- **SYN 保护期限** — 解除 SYN 数据包阻止前的秒数（符合 MAC-to-me 规则的拒绝 SYN 从端口上解除绑定）。

步骤 3 单击**应用**。将定义 SYN 保护，并更新当前配置文件。

SYN 保护接口表显示以下针对各端口或 LAG（根据用户请求）的字段。

- **当前状态** — 接口状态。可能的值包括：
  - *正常* — 此端口上未发现攻击。
  - *被攻击* — 此端口上发现攻击。
- **上一个攻击** — 系统发现上一个 SYN-FIN 攻击并采取系统操作（**已报告**）的日期。

Martian 地址

使用“Martian 地址”页面可输入表示攻击的 IP 地址（如果在网络上看到这些地址）。将丢弃来自这些地址的数据包。

设备支持一组保留的 Martian 地址，这些地址从 IP 协议的角度来看是非法的。支持的保留 Martian 地址有：

- 在“Martian 地址”页面中定义为非法的地址。
- 从协议角度来看是非法的地址（例如环回地址），包括以下范围中的地址：
  - **0.0.0.0/8（作为源地址的 0.0.0.0/32 除外）** — 此地址块中的地址指的是此网络上的源主机。
  - **127.0.0.0/8** — 用作 Internet 主机环回地址。
  - **192.0.2.0/24** — 用作文档和示例代码中的 TEST-NET。
  - **224.0.0.0/4（作为源 IP 地址）** — 用于 IPv4 组播地址分配，以前称为 D 类地址空间。
  - **240.0.0.0/4（作为目的地址的 255.255.255.255/32 除外）** — 保留的地址范围，以前称为 E 类地址空间。

您还可以为 DoS 防护添加新的 Martian 地址。具有 Martian 地址的数据包会被丢弃。

定义 Martian 地址的步骤：

步骤 1 单击**安全** > **拒绝服务防护** > **Martian 地址**。

步骤 2 选择**保留的 Martian 地址**，并单击**应用**以包括系统级防护列表中的保留 Martian 地址。

步骤 3 要添加 Martian 地址，请单击**添加**。

步骤 4 输入参数。

- **IP 版本** — 表示支持的 IP 版本。当前仅提供对 IPv4 的支持。
- **IP 地址** — 输入将要拒绝的 IP 地址。可能的值包括：
  - *来自保留的列表* — 从保留的列表中选择众所周知的 IP 地址。
  - *新 IP 地址* - 输入 IP 地址。
- **掩码** — 输入 IP 地址掩码，以定义拒绝的 IP 地址范围。这些值包括：
  - *网络掩码* — 网络掩码采用点分十进制格式。
  - *前缀长度* — 输入 IP 地址的前缀，以定义为其启用了 DoS 防护的 IP 地址的前缀。

步骤 5 单击**应用**。Martian 地址将写入当前配置文件中。

SYN 过滤

使用“SYN 过滤”页面可对包含 SYN 标签且指定给一个或多个端口的 TCP 数据包进行过滤。

定义 SYN 过滤器的步骤：

步骤 1 单击**安全** > **拒绝服务防护** > **SYN 过滤**。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **接口** — 选择在其上定义过滤器的接口。
- **IPv4 地址** — 输入为其定义了过滤器的 IP 地址，或选择*全部地址*。
- **网络掩码** — 以 IP 地址格式输入为其启用了过滤器的网络掩码。请输入以下字段之一：
  - *掩码* — 网络掩码采用点分十进制格式。
  - *前缀长度* — 输入 IP 地址的前缀，以定义为其启用了 DoS 防护的 IP 地址的前缀。

- **TCP 端口** — 选择要进行过滤的目的 TCP 端口：
  - *已知端口* - 从列表中选择端口。
  - *用户定义* - 输入端口号。
  - *全部端口* — 选择该选项可指示对所有端口进行过滤。

步骤 4 单击**应用**。系统将定义 SYN 过滤器，并更新当前配置文件。

SYN 速率保护

使用“SYN 速率保护”页面可对入站端口上接收的 SYN 数据包数量进行速率限制。这可以通过对开放以用于处理数据包的新连接数量进行速率限制，减弱 SYN 洪流对服务器的影响。

定义 SYN 速率保护的步骤：

步骤 1 单击**安全** > **拒绝服务防护** > **SYN 速率保护**。

此页面显示当前每个接口所定义的 SYN 速率保护。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **接口** — 选择要在其上定义速率保护的接口。
- **IP 地址** — 输入为其定义了 SYN 速率保护的 IP 地址，或选择*全部地址*。如果您输入 IP 地址，请输入掩码或前缀长度。
- **网络掩码** — 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：
  - *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。
- **SYN 速率限制** — 输入允许的 SYN 数据包数量。

步骤 4 单击**应用**。系统将定义 SYN 速率保护，并更新当前配置。

ICMP 过滤

使用“ICMP 过滤”页面可阻止来自某些源的 ICMP 数据包。这可以减少网络负载，以防备 ICMP 攻击。

定义 ICMP 过滤的步骤：

步骤 1 单击**安全** > **拒绝服务防护** > **ICMP 过滤**。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **接口** — 选择要在其上定义 ICMP 过滤的接口。
- **IP 地址** — 输入为其激活了 ICMP 数据包过滤的 IPv4 地址，或选择*所有地址*以阻止来自所有源地址的 ICMP 数据包。如果您输入 IP 地址，请输入掩码或前缀长度。
- **网络掩码** — 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：
  - *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 4 单击**应用**。系统将定义 ICMP 过滤，并更新当前配置。

IP 分片过滤

使用“IP 分片”页面可阻止分片的 IP 数据包。

配置分片的 IP 阻止的步骤：

步骤 1 单击**安全** > **拒绝服务防护** > **IP 分片过滤**。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **接口** — 选择要在其上定义 IP 分片的接口。
- **IP 地址** — 输入已对其分片 IP 数据包进行过滤的 IP 网络，或选择*所有地址*以阻止来自所有地址的 IP 分片数据包。如果您输入 IP 地址，请输入掩码或前缀长度。

- **网络掩码** — 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：
  - *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 4 单击**应用**。系统将定义 IP 分片，并更新当前配置文件。

18

安全：802.1X 验证

本部分介绍 802.1X 验证。

其中包含以下主题：

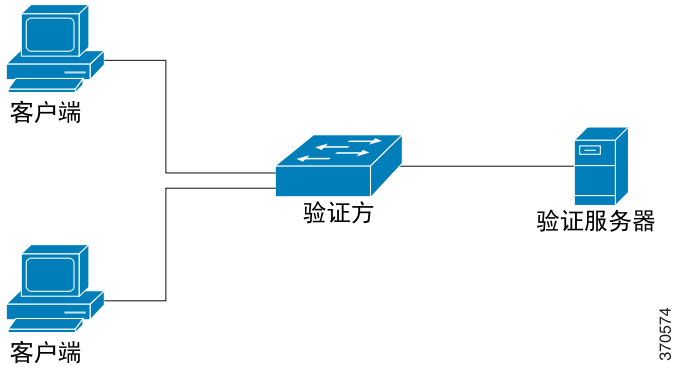
- 概述
- 属性
- 端口验证
- 主机和会话验证
- 已验证的主机

概述

802.1x 验证可限制未经授权的客户端通过可公开访问的端口连接局域网。802.1x 验证是一种客户端-服务器模式。在此模式中，网络设备具有以下特定角色。

- 客户端或请求方
- 验证方
- 验证服务器

具体如下图所示：



网络设备可以作为每个端口的客户端/请求方或验证方，或者兼此二职。

客户端或请求方

客户端或请求方是请求访问局域网的网络设备。客户端连接验证方。

如果客户端使用 802.1x 协议进行验证，则它会运行 802.1x 协议的请求方部分以及 EAP 协议的客户端部分。

验证方

验证方是提供网络服务的网络设备，是请求方端口连接的对象。

在基于 802.1x 的验证中，验证方使用 RADIUS 协议从 802.1x 消息（EAPOL 数据包）中提取 EAP 消息并将其传递到验证服务器。

端口应设置为验证模式。有关详情，请参阅端口主机模式。

验证服务器

验证服务器执行实际的客户端验证。设备的验证服务器是带有 EAP 扩展的 RADIUS 验证服务器。

开放式访问

开放式（监控）访问功能有助于在 802.1x 环境中将真正的验证失败与由于误配置和/或缺少资源引起的验证失败区分开。

开放式访问可帮助系统管理员了解连接到网络的主机的问题、监控不良状况并使这些问题得以修复。

在接口上启用开放式访问时，交换机会将从 RADIUS 服务器接收的所有失败验证视为成功验证，无论验证结果如何，都允许访问与接口连接的工作站网络。

在启用身份验证的端口上，正常情况下会在验证和授权成功之前阻止流量，而开放式访问功能可更改这一正常行为。验证的默认行为仍然是阻止所有流量，但局域网的可扩展验证协议 (EAPoL) 除外。但是，开放式访问让管理员可以为所有流量提供不受限制的访问，即便是在启用了验证（基于 802.1X、MAC 和/或 WEB 的验证）的情况下，也是如此。

当启用 RADIUS 记帐时，您可以记录验证尝试以及通过审计跟踪了解有哪些人员和设备连接到您的网络。

完成所有这一切操作都不会影响终端用户或与网络连接的主机。开放式访问可以在端口验证页面中激活。

端口验证状态

端口验证状态可确定客户端是否已获得网络访问权限。

端口管理状态可在端口验证页面中配置。

可用值如下：

- **强制授权**

  系统禁用端口验证，并且端口会根据其静态配置传输所有流量，无需请求任何验证。交换机在收到 802.1x EAPOL 开始消息时，会发送带有 EAP 成功消息的 802.1x EAP 数据包。

  此为默认状态。

- **强制未授权**

  系统禁用端口验证，并且端口会通过访客 VLAN 以及未经验证的 VLAN 传输所有流量。有关详情，请参阅主机和会话验证。交换机在收到 802.1x EAPOL-Start 消息时，会发送带有 EAP 故障消息的 802.1x EAP 数据包。

- **自动**

  根据配置的端口主机模式和端口上配置的验证方法启用端口验证。

端口主机模式

端口可置于以下端口主机模式（在主机和会话验证页面中配置）：

- **单主机模式**

  如果有经过授权的客户端，则对端口进行授权。一个端口上只能对一台主机进行授权。

  如果端口未经授权且访客 VLAN 为启用状态，则无标记流量将重新映射到访客 VLAN。除非标记流量属于访客 VLAN 或未经验证的 VLAN，否则会被丢弃。如果端口上未启用访客 VLAN，则只桥接属于未经验证的 VLAN 的标记流量。

  如果端口经过授权，来自授权主机的无标记流量和标记流量将根据静态 VLAN 成员关系端口配置进行桥接。来自其他主机的流量会被丢弃。

  用户可以指定将来自授权主机的无标记流量重新映射到 RADIUS 服务器在验证过程中分配的 VLAN。除非标记流量属于 RADIUS 分配的 VLAN 或未经验证的 VLAN，否则会被丢弃。端口上的 RADIUS VLAN 分配可在端口验证页面中设置。

- **多主机模式**

  如果至少有一个授权客户端，即可对端口进行授权。

  如果端口未经授权且访客 VLAN 为启用状态，则无标记流量将重新映射到访客 VLAN。除非标记流量属于访客 VLAN 或未经验证的 VLAN，否则会被丢弃。如果端口上未启用访客 VLAN，则只桥接属于未经验证的 VLAN 的标记流量。

  如果端口经过授权，来自所有与端口连接的主机的无标记流量和标记流量都将根据静态 VLAN 成员关系端口配置进行桥接。

  您可以指定将来自授权端口的无标记流量重新映射到 RADIUS 服务器在验证过程中分配的 VLAN。除非标记流量属于 RADIUS 分配的 VLAN 或未经验证的 VLAN，否则会被丢弃。端口上的 RADIUS VLAN 分配可在端口验证页面中设置。

- **多会话模式**

  与单主机模式和多主机模式不同，多会话模式下的端口不具有验证状态。此状态会分配给每个与端口连接的客户端。

  无论主机是否经过授权，属于未经验证 VLAN 的标记流量始终会被桥接。

  如果 VLAN 上已定义和启用访客 VLAN，那么来自未经授权主机且不属于未经验证 VLAN 的标记流量和无标记流量都将重新映射到访客 VLAN；如果端口上未启用访客 VLAN，则此类流量会被丢弃。

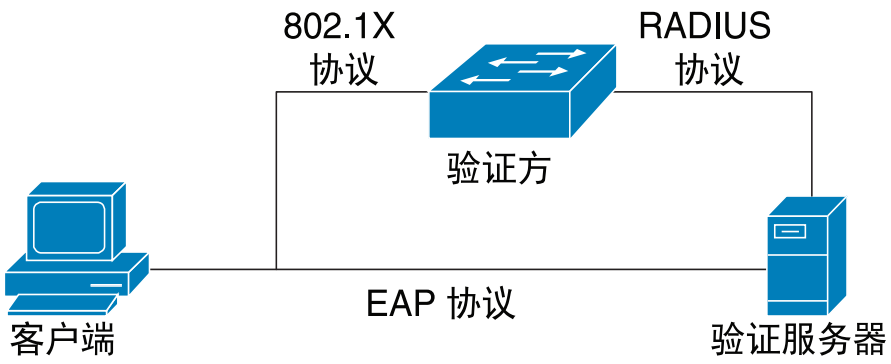
您可以指定将来自授权端口的无标记流量重新映射到 RADIUS 服务器在验证过程中分配的 VLAN。除非标记流量属于 RADIUS 分配的 VLAN 或未经验证的 VLAN，否则会被丢弃。端口上的 RADIUS VLAN 分配可在端口验证页面中设置。

基于 802.1x 的验证

基于 802.1x 的验证方依赖于 802.1x 请求方和验证服务器之间透明的 EAP 消息。请求方和验证方之间的 EAP 消息将封装到 802.1x 消息中，而验证方和验证服务器之间的 EAP 消息将封装到 RADIUS 消息中。

如下所示：

图 1　基于 802.1x 的验证



访客 VLAN

访客 VLAN 可提供对一类服务的访问权限，该类服务不需要对请求方设备或端口进行验证和授权。

访客 VLAN 是分配给未经授权客户端的 VLAN。您可以在属性页面中配置访客 VLAN 和一个或多个未经验证的 VLAN。

经过配置的访客 VLAN 是具有以下特性的静态 VLAN：

- 它必须从现有静态 VLAN 手动进行定义。
- 访客 VLAN 不能用作语音 VLAN 或未经验证的 VLAN。

主机模式与访客 VLAN

主机模式可通过以下方式与访客 VLAN 一起使用：

- **单主机和多主机模式**

  到达未经授权端口的属于访客 VLAN 的无标记流量和标记流量都将通过访客 VLAN 进行桥接。其他所有流量都会被丢弃。属于未经验证 VLAN 的流量将通过 VLAN 进行桥接。

- **多会话模式**

  不属于未经验证的 VLAN 且来自未经授权客户端的无标记流量和标记流量将使用 TCAM 规则分配给访客 VLAN，并通过访客 VLAN 进行桥接。属于未经验证 VLAN 的标记流量将通过 VLAN 进行桥接。

  此模式无法在与基于策略的 VLAN 相同的接口上配置。

如果 tunnel-private-group ID 属性以 VLAN 名称的形式提供，那么，在大多数情况下，具有此名称的 VLAN 将在设备上进行静态配置。如果在此属性中使用 VLAN ID (2-4094)，那么在验证请求方身份后，系统将动态创建 VLAN。

如标准中所述，设备支持 802.1x 验证机制，以便对 802.1x 请求方进行验证和授权。

违例模式

在单主机模式下，您可以配置未经授权端口上未经授权的主机尝试访问接口时要采取的操作。这是在主机和会话验证页面中进行的。

可用的选项如下：

- **限制** — 当 MAC 地址不是请求方 MAC 地址的站尝试访问接口时，生成一个陷阱。陷阱之间的最短时间间隔为 1 秒。系统将转发这些帧，但不会学习其源地址。
- **保护** — 丢弃源地址不是请求方地址的帧。
- **关闭** — 丢弃源地址不是请求方地址的帧，并关闭端口。

您还可以将设备配置为发送 SNMP 陷阱，且连续陷阱之间具有可配置的最短时间间隔。如果间隔秒数等于 0，系统将禁用陷阱。如果未指定最短时间间隔，则限制模式默认为 1 秒，其他模式默认为 0。

静默期

静默期是端口（单主机或多主机模式）或客户端（多会话模式）在验证交换失败之后无法尝试验证的时段。在单主机或多主机模式下，该时段按端口进行定义；在多会话模式下，该时段按客户端进行定义。在该静默期内，交换机不接受也不发出验证请求。

您还可以指定触发静默期的最大登录尝试次数。数值 0 表示不限制登录尝试次数。

静默期的持续时间和最大登录尝试次数可在端口验证页面设置。

常见任务

工作流程 1：在端口上启用 802.1x 验证：

步骤 1 单击**安全 > 802.1X 验证 > 属性**，全局启用 802.1x 验证。

步骤 2 启用基于端口的验证。

步骤 3 选择**验证方法**。

步骤 4 单击**应用**，将更新当前配置文件。

步骤 5 **单击“安全”>“802.1X 验证”>“主机和会话”。**

步骤 6 选择所需端口，然后单击**编辑**。

步骤 7 选择主机验证模式。

步骤 8 单击**应用**，将更新当前配置文件。

步骤 9 单击**安全 > 802.1X 验证 > 端口验证**。

步骤 10 选择一个端口，然后单击**编辑**。

步骤 11 将“管理端口控制”字段设置为**自动**。

步骤 12 定义验证方法。

步骤 13 单击**应用**，将更新当前配置文件。

工作流程 2：配置陷阱

步骤 1 单击**安全 > 802.1X 验证** > **属性**。

步骤 2 选择所需陷阱。

步骤 3 单击**应用**，将更新当前配置文件。

工作流程 3：配置基于 802.1x 的验证

步骤 1 单击**安全 > 802.1X 验证 > 端口验证**。

步骤 2 选择所需端口，然后单击**编辑**。

步骤 3 输入对端口必填的字段。

此页面中的字段如端口验证中所述。

步骤 4 单击**应用**，将更新当前配置文件。

使用**复制设置**按钮将设置从一个端口复制到另一个端口。

工作流程 4：配置静默期

步骤 1 单击**安全 > 802.1X 验证 > 端口验证**。

步骤 2 选择一个端口，然后单击**编辑**。

步骤 3 在“静默期”字段中输入静默期。

步骤 4 单击**应用**，将更新当前配置文件。

工作流程 5：配置访客 VLAN 的步骤：

步骤 1 单击**安全 > 802.1X 验证 > 属性**。

步骤 2 在“访客 VLAN”字段选择**启用**。

步骤 3 在“访客 VLAN ID”字段中选择访客 VLAN。

步骤 4 将“访客 VLAN 超时”配置为“立即”，或者在“用户定义”字段中输入一个值。

步骤 5 单击**应用**，将更新当前配置文件。

属性

“属性”页面用于全局启用端口/设备验证。要发挥验证的作用，必须在每个端口上全局且单独地激活验证。

定义基于端口的验证的步骤：

步骤 1 单击**安全 > 802.1X 验证 > 属性**。

步骤 2 输入参数。

- **基于端口的验证** — 启用或禁用基于端口的验证。

  如果禁用此选项，则 802.1X 将被禁用。

- **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），则系统不会执行验证，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。

- **访客 VLAN** — 选择该选项可将访客 VLAN 用于未授权的端口。如果已启用访客 VLAN，则所有未经授权的端口会自动加入在*访客 VLAN ID* 字段中选择的 VLAN。如果稍后对端口进行授权，系统会从访客 VLAN 中删除该端口。

  像其他任何 VLAN 一样，VLAN 可以定义为第 3 层接口（为其指定 IP 地址）。然而，设备管理不能通过访客 VLAN IP 地址实现。

- **访客 VLAN ID** — 从 VLAN 列表选择访客 VLAN。

- **访客 VLAN 超时** — 将时间段定义为**立即**，或在**用户定义**中输入值。该值的用途如下所示：

  连接之后，如果软件未检测到 802.1X 请求方或验证失败，则只会在*访客 VLAN 超时*期限过期之后，才将端口添加到访客 VLAN。

如果端口状态从*已授权*更改为*未授权*，则只会在*访客 VLAN* 超时过期之后才将端口添加到访客 VLAN。

- **陷阱设置** — 要启用陷阱，请选择以下一个或多个选项：
  - *802.1x 验证失败陷阱* — 选择此选项可在 802.1x 验证失败时生成陷阱。
  - *802.1x 验证成功陷阱* — 选择此选项可在 802.1x 验证成功时生成陷阱。

步骤 3 单击**应用**。802.1X 属性将写入当前配置文件中。

端口验证

“端口验证”页面可配置每个端口的参数。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 定义了 802.1x 的端口不能成为 LAG 的成员。
802.1x 和“端口安全”不能同时在同一端口上启用。如果在一个接口上启用端口安全，则无法将“管理端口控制”更改为“自动”模式。

定义 802.1X 验证的步骤：

步骤 1 单击**安全 > 802.1X 验证 > 端口验证**。

步骤 2 此页面显示所有端口的验证设置。选择一个端口，然后单击**编辑**。

步骤 3 输入参数。

- **接口** — 选择一个端口。
- **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*。如果请求方在一个接口上处于启用状态，则“当前端口控制”将为“请求方”。
- **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。设备不为通过接口的客户端提供验证服务。
  - *自动* — 在设备上启用基于端口的验证和授权。接口根据设备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。

- **访客 VLAN** — 选择此选项可将访客 VLAN 用于未授权的端口。如果已启用访客 VLAN，则未经授权的端口会自动加入在端口验证页面的“访客 VLAN ID”字段中选择的 VLAN。验证失败之后，如果在给定端口上全局激活访客 VLAN，则会将访客 VLAN 作为无标记 VLAN 自动分配给未经授权的端口。
- **定期重新验证** — 选择此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** — 选择此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：
  - *初始化* — 处于启动阶段。
  - *强制授权* — 受控的端口状态设置为“强制授权”（转发流量）。
  - *强制未授权* — 受控的端口状态设置为“强制未授权”（丢弃流量）。

  注 如果端口未处于“强制授权”或“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”。
- **时间范围** — 选择该选项可将验证限定到具体的时间范围。
- **时间范围名称** — 如果已选中**时间范围**，请选择要使用的时间范围。时间范围已在系统时间配置一节中进行过定义。
- **最大主机数** — 输入主机上允许的最大授权主机数量。选择无限期不进行限制，或选择用户定义设置限制。
- **静默期** — 输入静默期的长度。
- **重新发送 EAP** — 输入在重新发送请求之前设备等待来自请求方（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 请求数** — 输入可发送的 EAP 请求的最大数量。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** — 输入设备将请求重新发送到验证服务器之前经过的秒数。

步骤 4 单击**应用**。端口设置将写入当前配置文件中。

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。

有关这些模式的说明，请参阅端口主机模式。

为端口定义 802.1X 高级设置的步骤：

步骤 1 单击**安全 > 802.1X 验证** > **主机和会话验证**。

页面上会说明所有端口的验证参数。在**编辑**页面中介绍了除以下字段以外的所有字段。

- **反入侵次数** — 显示在单主机模式下从其 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**。

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。这些模式在上面的端口主机模式部分进行了介绍。

单主机违反规则设置（仅在主机验证为“单主机”时显示）：

- **违反规则响应措施** — 选择对在单会话/单主机模式下从其 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设备之前，端口将保持关闭状态。
- **陷阱** — 选择此选项可启用陷阱。
- **陷阱频率** — 定义向主机发送陷阱的频率。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。

已验证的主机

要查看关于已验证用户的详细信息，请单击**安全 > 802.1X 验证** > **已验证的主机**。

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)** — 请求方在端口上经过验证和授权访问的时间量。
- **验证服务器** — RADIUS 服务器。
- **MAC 地址** — 显示请求方的 MAC 地址。

19

安全：安全敏感数据管理

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 管理
- SSD 规则
- SSD 属性
- 配置文件
- SSD 管理通道
- 菜单 CLI 和密码恢复
- 配置 SSD

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/或确保能够与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。
- **渠道** — 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：控制台端口界面、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 或 SNMPv3。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 或 SNMPv1/v2 和 SNMPv3。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。

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** — 所有默认读取模式需遵循规则的读取权限。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。

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”。
- SNMP 社区名称将不用作与 SSD 规则匹配的用户名。
- 可通过配置用户名与 SNMPv3 用户名相匹配的 SSD 规则来控制特定 SNMPv3 用户的访问权限。
- 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。

注 在执行由 XML 或 SNMP 命令发起的文件传输时，优先使用的协议是 TFTP。因此，将应用不安全通道的 SSD 规则。

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 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：

规则密钥		规则操作	
用户	信道	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，在会话中包含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。拥有相同密码的设备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（含 8 和 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，用户可以查看该密码。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。（请参阅敏感数据零接触自动配置）。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，该密码是设备运行配置的密码。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“ssd-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 SNMP 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** > **固件操作**。

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。

注 开箱即用或者处于出厂默认状态的设备使用默认的匿名用户访问 SCP 服务器。

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	SSD 管理通道类型	类似的安全管理通道
控制台	安全	
Telnet	不安全	SSH
SSH	安全	
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	
不带保密功能的 SNMPv1/v2/v3	不安全-XML-SNMP	安全-XML-SNMP
带保密功能的 SNMPv3	安全-XML-SNMP（第 15 级用户）	
TFTP	不安全	SCP
SCP（安全复制）	安全	
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

只有读取权限为“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 SSD 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**。

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）。

步骤 4 单击**应用**。设置将保存到当前配置文件中。

更改本地密码的步骤：

步骤 1 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）** — 输入新密码。
- **确认密码** — 确认新密码。

步骤 2 单击**应用**。设置将保存到当前配置文件中。

SSD 规则配置

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**。

此时将显示当前定义的规则。**规则类型**字段指示规则是用户定义的规则还是默认规则。

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（控制台、SCP、SSH 和 HTTPS），不包括 SNMP 和 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 SNMP 和 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 和 SNMPv3。
  - *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/和 SNMPv1/v2 与 SNMPv3。
- **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 单击**应用**。设置将保存到当前配置文件中。

步骤 4 可以对选定的规则执行以下操作：

- **添加**、**编辑**或**删除**规则或者**恢复默认设置**。
- **将所有规则恢复默认设置** — 将用户修改的默认规则恢复为默认规则。

20

安全：SSH 服务器

本节介绍如何在设备上建立 SSH 会话。

其中包含以下主题：

- 概述
- 常见任务
- SSH 用户验证
- SSH 服务器验证

概述

通过 SSH 服务器功能，远程用户可以与设备建立 SSH 会话。这类似于建立 telnet 会话，不过会话会受到保护。

作为 SSH 服务器，设备支持“SSH 用户验证”，通过密码或通过公共密钥验证远程用户。同时，作为 SSH 客户端的远程用户可以执行 SSH 服务器验证，使用设备公共密钥（指纹）验证设备。

SSH 服务器可以在以下模式下运行：

- **按内部生成的 RSA/DSA 密钥（默认设置）**— 会生成 RSA 和 DSA 密钥。用户登录 SSH 服务器应用，并在其提供设备 IP 地址时自动进行验证以打开设备会话。
- **公共密钥模式** — 在设备上定义用户。其 RSA/DSA 密钥在外部 SSH 服务器应用（如 PuTTY）中生成。这些密钥会输入设备。随后用户就可以通过外部 SSH 服务器应用在设备上打开 SSH 会话。

常见任务

本节介绍一些使用 SSH 服务功能执行的常见任务。

工作流程 1：要创建无 SSH 用户验证的 SSH 会话，请执行以下步骤：

步骤 1 在 TCP/UDP 服务页面中启用 SSH 服务器。

步骤 2 在 SSH 用户验证页面中禁用通过密码和公共密钥进行 SSH 用户验证。

步骤 3 建立从 SSH 客户端应用程序（例如 PUTTY）到设备的 SSH 会话。

工作流程 2：要创建通过密码进行 SSH 用户验证的 SSH 会话，请执行以下步骤：

步骤 1 在 TCP/UDP 服务页面中启用 SSH 服务器。

步骤 2 在 SSH 用户验证页面中启用通过密码进行 SSH 用户验证。

步骤 3 建立从 SSH 客户端应用程序（例如 PUTTY）到设备的 SSH 会话。

工作流程 3：要创建通过公共密钥进行 SSH 用户验证（忽略/不忽略管理验证）的 SSH 会话，请执行以下步骤：

步骤 1 在 TCP/UDP 服务页面中启用 SSH 服务器。

步骤 2 在 SSH 用户验证页面中启用按公共密钥进行 SSH 用户验证。公共密钥必须已在 SSH 客户端创建，并且由 SSH 客户端用于在设备上建立到 SSH 服务器的 SSH 会话。

步骤 3 如果需要，请在 SSH 用户验证页面中启用通过管理验证的自动登录。

步骤 4 在 SSH 用户验证页面中将用户及其公钥添加到“SSH 用户验证表”中。

步骤 5 建立从 SSH 客户端应用程序（例如 PUTTY）到设备的 SSH 会话。

SSH 用户验证

使用“SSH 用户验证”页面启用通过公共密钥和/或密码进行 SSH 用户验证。对于使用公共密钥建立 SSH 服务器的用户，其用户名和公共密钥必须输入“SSH 用户验证表”中。对于使用密码建立 SSH 会话的用户，其用户名和密码必须是拥有管理访问权限的用户的用户名和密码。

在添加用户之前，必须在外部 SSH 密钥生成/客户端应用（例如 PuTTY）中为用户生成 RSA 或 DSA 密钥。

自动登录

如果在“SSH 用户验证”页面中为已在本地用户数据库中配置的用户创建 SSH 用户名，则可以通过配置**自动登录**功能阻止其他验证，操作步骤如下：

- **已启用** — 如果已在本地数据库中定义了用户，且此用户使用公共密钥通过了 SSH 验证，则将跳过通过本地数据库用户名和密码的验证。

  注 为此特定管理方法（控制台、Telnet 和 SSH 等）配置的验证方法必须为*本地*（即，不是 *RADIUS* 或 *TACACS+*）。有关详情，请参阅管理访问方法。

- **未启用** — 通过 SSH 公共密钥成功进行验证后，即使本地用户数据库中已配置了用户名，也将根据管理访问验证页面配置的验证方法再次验证用户。

本页面是可选页面。您不必在 SSH 中使用用户验证。

启用验证并添加用户的步骤：

步骤 1 单击**安全 > SSH 服务器 > SSH 用户验证**。

步骤 2 选择以下字段：

- **SSH 用户通过密码验证** — 选择该选项以使用本地数据库中配置的用户名/密码执行 SSH 客户端用户验证（请参阅用户帐户）。
- **藉由公共密钥的 SSH 用户验证** — 选择该选项以使用公共密钥执行 SSH 客户端用户验证。
- **自动登录** — 如果选择了**藉由公共密钥的 SSH 用户验证**功能，此字段便可启用。

步骤 3 单击**应用**。设置将保存到当前配置文件中。

对于配置的用户，系统将显示以下字段：

- **SSH 用户名** — 用户的用户名。
- **密钥类型** — 指示该密钥是 RSA 还是 DSA 密钥。
- **指纹** — 从公共密钥生成的指纹。

步骤 4 单击**添加**以添加新用户并输入以下字段：

- **SSH 用户名** — 输入用户名。
- **密钥类型** — 选择 **RSA** 或 **DSA**。
- **公共密钥** — 将外部 SSH 客户端应用（如 PuTTY）生成的公共密钥复制到此文本框。

步骤 5 单击**应用**保存新用户。

系统会为所有活动用户显示以下字段：

- **IP 地址** — 活动用户的 IP 地址。
- **SSH 用户名** — 活动用户的用户名。
- **SSH 版本** — 活动用户使用的 SSH 版本。
- **密码** — 活动用户的密码。
- **验证代码** — 活动用户的验证代码。

SSH 服务器验证

远程 SSH 客户端可以执行 SSH 服务器验证，确保它正在建立到预期 SSH 驱动程序的 SSH 会话。要执行 SSH 服务器验证，远程 SSH 客户端必须拥有目标 SSH 服务器的 SSH 服务器公共密钥（或指纹）的副本

“SSH 服务器验证”页面生成/导入供作为 SSH 服务器的设备使用的公共/专用密钥。若要在 SSH 会话上执行 SSH 服务器验证，用户应当将此设备的 SSH 服务器公共密钥（或指纹）复制到应用程序中。设备从出厂默认设置引导后，会自动生成公共和专用 RSA 和 DSA 密钥。用户删除每个相应的用户配置密钥后也会自动生成密钥。

重新生成 RSA 或 DSA 密钥或者复制到其他设备上生成的 RSA/DSA 密钥中的步骤：

步骤 1 单击**安全 > SSH 服务器 > SSH 服务器验证**。

系统将针对每个密钥显示以下字段：

- **密钥类型** — RSA 或 DSA。
- **密钥来源** — 自动生成或用户定义。
- **指纹** — 从密钥生成的指纹。

步骤 2 选择 RSA 或 DSA 密钥。

步骤 3 您可以进行以下任何操作：

- **生成** — 生成指定类型的密钥。
- **编辑** — 使您可以复制到来自其他设备的密钥中。输入以下字段：
  - *密钥类型* — 如上所述。
  - *公钥* — 输入公钥。
  - *私钥* — 选择**加密**或**纯文本**，然后输入私钥。

  单击**将敏感数据显示为加密**或**将敏感数据显示为纯文本**，设置敏感数据的显示方式。
- **删除** — 使您可以删除密钥。
- **详情** — 使您可以查看生成的密钥。您还可以在“详情”窗口中单击**将敏感数据显示为明文模式**。如果单击此项，这些密钥将显示为明文模式而不是加密形式。如果密钥已显示为明文模式，则可以单击**将敏感数据显示为加密模式**以加密形式显示文本。

21

安全：SSH 客户端

本节介绍作为 SSH 客户端的设备。

其中包含以下主题：

- 概述
- SSH 用户验证
- SSH 服务器验证
- 更改 SSH 服务器的用户密码

概述

安全复制 (SCP) 和 SSH

Secure Shell (SSH) 是一种网络协议，可在 SSH 客户端（在此情况下，指设备）与 SSH 服务器之间的安全通道上实现数据交换。

SSH 客户端可帮助用户管理由一个或多个交换机组成的网络，其中的各种系统文件均存储在中央 SSH 服务器中。通过网络传输配置文件时，安全复制（Secure Copy，简称 SCP，一种利用 SSH 协议的应用程序）可确保用户名/密码等敏感数据不会遭到拦截。

安全复制 (SCP) 用于将固件、引导映像、配置文件和日志文件从中央 SCP 服务器安全传输到设备。

就 SSH 而言，设备上运行的 SCP 是一种 SSH 客户端应用程序，而 SCP 服务器则是一种 SSH 服务器应用程序。

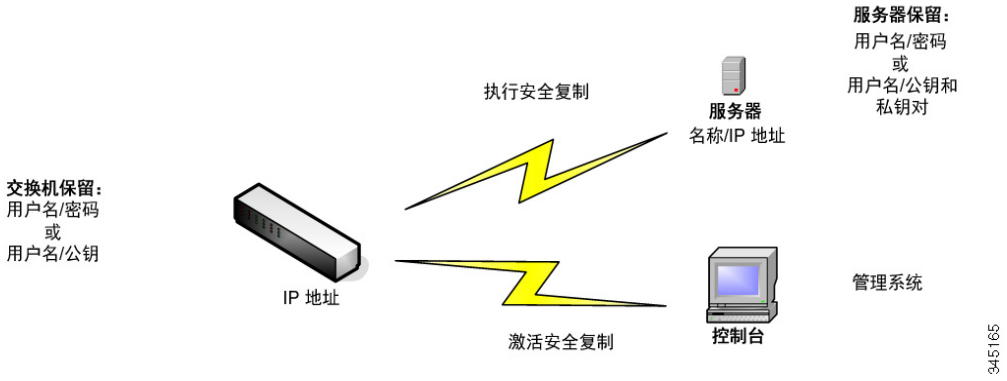
通过 TFTP 或 HTTP 下载文件时，无法确保数据传输的安全性。

如果通过 SCP 下载文件，则会通过安全通道将信息从 SCP 服务器下载到设备上。此安全通道可在验证之前创建，以确保允许用户执行此操作。

虽然本指南未介绍服务器操作，但是设备和 SSH 服务器上的验证信息必须由用户输入。

下图说明了可能会在其中使用 SCP 功能的典型网络配置。

典型网络配置



SSH 服务器验证

作为 SSH 客户端的设备仅与信任的 SSH 服务器进行通讯。如果禁用 SSH 服务器验证（默认设置），则所有 SSH 服务器均被视为信任服务器。如果启用 SSH 服务器验证，用户必须将信任服务器的条目添加到信任的 SSH 服务器表中。此表可为每台信任的 SSH 服务器（最多 16 台服务器）存储以下信息，具体包括：

- 服务器 IP 地址/主机名
- 服务器公共密钥指纹

启用 SSH 服务器验证后，在设备上运行的 SSH 客户端会使用以下验证过程来验证 SSH 服务器：

- 设备计算接收的 SSH 服务器公共密钥的指纹。
- 设备在信任的 SSH 服务器表中搜索 SSH 服务器的 IP 地址/主机名。可能会出现以下其中一种情况：
  - 如果未找到服务器 IP 地址/主机名及其指纹的匹配项，将对服务器进行验证。
  - 如果已找到匹配的 IP 地址/主机名，但没有匹配的指纹，搜索将继续进行。如果找不到匹配的指纹，系统将完成搜索，但无法进行验证。
  - 如果找不到匹配的 IP 地址/主机名，系统将完成搜索，但无法进行验证。
- 如果在信任服务器列表中找不到 SSH 服务器的条目，该过程将无法进行。

为了支持自动配置开箱即用型设备（采用出厂默认配置的设备），SSH 服务器验证默认为禁用状态。

SSH 用户验证

当设备（SSH 客户端）尝试建立到 SSH 服务器的 SSH 会话时，SSH 服务器使用各种方法进行客户端验证。具体方法如下所述。

密码

要使用密码方法，首先要确保 SSH 服务器上已建立用户名/密码。尽管此操作无法通过设备的管理系统完成，但是，在服务器上建立用户名后，可以通过设备的管理系统更改服务器密码。

然后，必须在设备上创建用户名/密码。当设备尝试建立到 SSH 服务器的 SSH 会话时，设备提供的用户名/密码必须与服务器上的用户名/密码相匹配。

可以使用在会话期间协商的一次性对称密钥来加密数据。

虽然多台交换机可使用相同的用户名/密码，但是经管理的每台设备都必须具有自身的用户名/密码。

密码方法是设备上的默认方法。

公共/专用密钥

要将公共/专用密钥方法用于 SSH 服务器进行的客户端验证，请在作为 SSH 客户端的设备上创建一个用户并生成/导入公共/专用密钥对。然后，在 SSH 服务器上创建相同的用户，将在 SSH 客户端生成/输入的公钥（或指纹）复制到 SSH 服务器上。创建用户和将公钥（或指纹）复制到 SSH 服务器上的操作不在本指南的讨论范围之内。

启动设备时，系统会为其生成 RSA 和 DSA 默认密钥对。其中一个密钥用于加密从 SSH 服务器下载的数据。默认情况下，使用 RSA 密钥。

如果用户删除了其中一个密钥或将其全部删除，系统会重新生成。

公共/专用密钥存储于设备内存中，并在其中进行加密。密钥是设备配置文件的一部分，专用密钥可以以加密形式或明文形式对用户显示。

因为无法将专用密钥直接复制为其他设备的专用密钥，所以出现了一种可将专用密钥从一台设备复制到另一台设备的导入方法（如*导入密钥*中所述）。

导入密钥

使用该密钥方法，必须为每个单独的设备创建单独的公共/专用密钥，并且出于安全性的考虑，不能将这些专用密钥从一台设备直接复制到另一台设备。

如果网络中存在多台交换机，因为公共/专用密钥必须逐个创建然后还要加载到 SSH 服务器，所以为所有交换机创建公共/专用密钥的过程便可能会很耗时。

要加速此过程，可使用其他功能，将加密的专用密钥安全传输到系统中的所有交换机。

在设备上创建专用密钥后，还可以创建相关联的*密码*。此密码用于加密专用密钥以及将其导入其余交换机中。通过这种方法，所有交换机都可以使用相同的公共/专用密钥。

默认密码

默认情况下，启用通过密码进行 SSH 用户验证，此时用户名/密码是“匿名”的。

用户必须配置以下信息才能进行验证：

- 要使用的验证方法。
- 用户名/密码或公共/专用密钥对。

支持的算法

在设备（作为 SSH 客户端）与 SSH 服务器之间建立连接后，该客户端和 SSH 服务器会交换数据，以确定要在 SSH 传输层中使用的算法。

客户端上支持以下算法：

- 密钥交换算法 — diffie-hellman
- 加密算法
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - Chacha
  - Poly1305
- 消息验证码算法
  - hmac-sha1

注 不支持压缩算法。

使用准备

必须先执行以下操作，然后再使用 SCP 功能：

- 使用密码验证方法时，必须在 SSH 服务器上设置用户名/密码。
- 使用公共/专用密钥验证方法时，必须将公共密钥存储在 SSH 服务器上。

常见任务

本节介绍一些作为 SSH 客户端的设备执行的常见任务。参考的所有页面均可在菜单树的“SSH 客户端”分支下找到。

工作流程 1：要配置 SSH 客户端以及将数据传输到 SSH 服务器/传输来自远程 SSH 服务器的数据，请执行以下步骤：

步骤 1 确定要使用的方法：密码或公共/专用密钥。使用 SSH 用户验证页面。

步骤 2 如果已选择密码方法，请执行以下步骤：

a. 当您实际激活安全数据传输时，在 SSH 用户验证页面中创建全局密码，或者在固件操作或文件操作页面中创建临时密码。

b. 在固件操作页面中选择 **SCP** 选项，使用 SCP 升级固件、启动映像或语言文件。可以在此页面中直接输入密码，或者可以使用在 SSH 用户验证页面中输入的密码。

c. 在文件操作页面中选择**通过 SCP（藉由 SSH）**选项，以使用 SCP 来下载/备份配置文件。可以在此页面中直接输入密码，或者可以使用在 SSH 用户验证页面中输入的密码。

步骤 3 在远程 SSH 服务器上设置用户名/密码或者修改密码。此操作取决于服务器，在此不做说明。

步骤 4 如果使用的是公共/专用密钥方法，请执行以下步骤：

a. 选择使用 RSA 密钥还是 DSA 密钥，创建用户名，然后生成公共/专用密钥。

b. 单击**详情**按钮查看生成的密钥，然后将用户名和公共密钥传输到 SSH 服务器。此操作取决于服务器，本指南中不做说明。

c. 在固件操作页面中选择 **SCP** 选项，使用 SCP 升级/备份固件。

d. 在文件操作页面中选择 **SCP** 选项，以使用 SCP 下载/备份配置文件。

工作流程 2：将公共/专用密钥从一台设备导入另一台设备的步骤：

步骤 1 在 SSH 用户验证页面中生成公共/专用密钥。

步骤 2 在 SSD 属性页面中设置 SSD 属性并新建本地密码。

步骤 3 单击**详情**查看生成的已加密密钥，然后将它们（包括开始页脚和结束页脚）从“详情”页面复制到外部设备。分别复制公共密钥和专用密钥。

步骤 4 登录到其他设备，然后打开 SSH 用户验证页面。选择所需密钥的类型，然后单击**编辑**。粘贴公共/专用密钥。

步骤 5 单击**应用**，将公共/专用密钥复制到第二台设备上。

工作流程 3：在 SSH 服务器上更改密码的步骤：

步骤 1 在更改 SSH 服务器的用户密码页面中识别服务器。

步骤 2 输入新密码。

步骤 3 单击**应用**。

SSH 用户验证

使用此页面可选择一种 SSH 用户验证方法。如果选择密码方法，可设置设备的用户名和密码；如果选择公共/专用密钥方法，可生成 RSA 或 DSA 密钥。

选择一种验证方法并设置用户名/密码/密钥的步骤：

步骤 1 单击**安全 > SSH 客户端 > SSH 用户验证**。

步骤 2 选择一种 **SSH 用户验证方法**。这是针对安全复制 (SCP) 定义的全局方法。请选择以下选项之一：

- **通过密码** — 此选项为默认设置。如果选择此选项，请输入一个密码或保留默认密码。
- **通过 RSA 公共密钥** — 如果选择此选项，请在 **SSH 用户密钥表**框中创建一个 RSA 公共/专用密钥。
- **通过 DSA 公共密钥** — 如果选择此选项，请在 **SSH 用户密钥表**框中创建一个 DSA 公共/专用密钥。

步骤 3 输入**用户名**（无论选择什么方法），或者使用默认用户名。此用户名必须与在 SSH 服务器上定义的用户名相匹配。

步骤 4 如果已选择*通过密码*方法，请输入一个密码（**加密**或**明文**模式），或者保留默认的已加密密码。

步骤 5 请执行以下操作之一：

- **应用** — 选择的验证方法与访问方法相关。
- **恢复默认凭证** — 将恢复默认的用户名和密码（匿名）。
- **将敏感数据显示为明文模式** — 当前页面的敏感数据将显示为明文模式。

SSH 用户密钥表针对每个密钥包含以下字段：

- **密钥类型** — RSA 或 DSA。
- **密钥来源** — 自动生成或用户定义。
- **指纹** — 从密钥生成的指纹。

步骤 6 要处理 RSA 或 DSA 密钥，请选择 RSA 或 DSA，然后执行以下操作之一：

- **生成** — 生成一个新密钥。
- **编辑** — 显示要复制/粘贴到其他设备的密钥。
- **删除** — 删除密钥。
- **详情** — 显示密钥。

SSH 服务器验证

启用 SSH 服务器验证以及定义信任服务器的步骤：

步骤 1 单击**安全 > SSH 客户端 > SSH 服务器验证**。

步骤 2 选择**启用**以启用 SSH 服务器验证。

- **IPv4 源接口** — 选择其 IPv4 地址将用作与 IPv4 SSH 服务器通信中所用消息的源 IPv4 地址的源接口。
- **IPv6 源接口** — 选择其 IPv6 地址将用作与 IPv6 SSH 服务器通信中所用消息的源 IPv6 地址的源接口。

注 如果已选择“自动”选项，系统将使用传出接口上定义的 IP 地址的源 IP 地址。

步骤 3 单击**应用**。

步骤 4 单击**添加**，然后针对信任的 SSH 服务器输入以下字段：

- **服务器定义** — 选择以下其中一种方法来识别 SSH 服务器：
  - *按 IP 地址* — 如果选择此选项，请在下面的字段中输入服务器的 IP 地址。
  - *按名称* — 如果选择此选项，请在**服务器 IP 地址/名称**字段中输入服务器的名称。
- **IP 版本** — 如果选择按 IP 地址指定 SSH 服务器，请选择 IP 地址是 IPv4 还是 IPv6 地址。
- **IPv6 地址类型** — 如果 SSH 服务器 IP 地址是 IPv6 地址，请选择 IPv6 地址类型。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** — 从接口列表中选择链路本地接口。
- **服务器 IP 地址/名称** — 输入 SSH 服务器的 IP 地址或服务器名称（取决于**服务器定义**中的选择）。
- **指纹** — 输入 SSH 服务器的指纹（从该服务器进行复制）。

步骤 5 单击**应用**。信任服务器定义将存储在当前配置文件中。

更改 SSH 服务器的用户密码

在 SSH 服务器上更改密码的步骤：

步骤 1 单击**安全 > SSH 客户端 > 更改 SSH 服务器的用户密码**。

步骤 2 输入以下字段：

- **服务器定义** — 选择**按 IP 地址**或**按名称**定义 SSH 服务器。在**服务器 IP 地址/名称**字段中输入服务器的名称或 IP 地址。
- **IP 版本** — 如果选择按 IP 地址指定 SSH 服务器，请选择 IP 地址是 IPv4 还是 IPv6 地址。
- **IPv6 地址类型** — 如果 SSH 服务器 IP 地址是 IPv6 地址，请选择 IPv6 地址类型。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** — 从接口列表中选择链路本地接口。
- **服务器 IP 地址/名称** — 输入 SSH 服务器的 IP 地址或服务器名称（取决于**服务器定义**中的选择）。
- **用户名** — 此用户名必须与服务器上的用户名相匹配。
- **旧密码** — 此密码必须与服务器上的密码相匹配。
- **新密码** — 输入新密码，然后在**确认密码**字段中进行确认。

步骤 3 单击**应用**。系统将修改 SSH 服务器中的密码。

22

访问控制

访问控制列表 (ACL) 功能是安全机制的一部分。ACL 定义可用作定义获得特定服务质量 (QoS) 的流量的多种机制之一。有关详情，请参阅服务质量。

ACL 可让网络管理员定义用于入口流量的模式（过滤器和操作）。在具有活动 ACL 的端口或 LAG 上进入设备的数据包会被接受或拒绝进入。

本节包含以下主题：

- 概述
- 创建基于 MAC 的 ACL
- 创建基于 IPv4 的 ACL
- 创建基于 IPv6 的 ACL
- ACL 绑定

概述

访问控制列表 (ACL) 是分类过滤器和操作的已排序列表。每个单独的分类规则与其操作一起被称为一个访问控制元素 (ACE)。

每个 ACE 由多个过滤器组成，这些过滤器可区分流量组以及关联的操作。一个单独的 ACL 可能包含一个或多个 ACE，这些 ACE 会与传入帧的内容进行匹配。会将拒绝操作或允许操作应用于内容与过滤器匹配的帧。

各种设备支持以下数量的 ACL 和 ACE：

设备	最大 ACL 数	最大 ACE 数
SG550XG/SX550X	2K	2K
Sx550X	3K	3K

设备	最大 ACL 数	最大 ACE 数
SG350XG/SX350X	2K	2K
SG350 和 Sx350	1K	1K
Sx250	512	512

在单个端口或单个 ACL 中最多可配置 256 个 ACE。

如果数据包与 ACE 过滤器匹配，则系统会执行 ACE 操作并停止 ACL 处理。如果数据包与 ACE 过滤器不匹配，则系统会处理下一个 ACE。如果在处理完一个 ACL 的所有 ACE 后都找不到匹配项，并且存在另一个 ACL，则系统会以相似方式处理该 ACL。

注 如果在所有相关 ACL 的所有 ACE 中都找不到匹配项，则系统会丢弃该数据包（默认操作）。由于系统会执行此默认丢弃操作，因此您必须将 ACE 明确添加到 ACL 中，以允许所需的流量（包括管理流量，例如指向设备本身的 Telnet、HTTP 或 SNMP）。例如，如果您不希望丢弃 ACL 中不满足条件的所有数据包，则您必须将最低优先级的 ACE 明确添加到允许所有流量的 ACL 中。

如果在与一个 ACL 绑定的端口上启用了 IGMP/MLD 侦听，请在该 ACL 中添加 ACE 过滤器，以将 IGMP/MLD 数据包转发给设备。否则，IGMP/MLD 侦听将在该端口处失败。

ACL 中 ACE 的顺序很重要，因为系统会按照顺序应用第一个匹配的 ACE。系统会从第一个 ACE 开始，按顺序处理 ACE。

ACL 可用于确保安全性（例如允许或拒绝一定的流量），也可用于在 QoS 高级模式下进行流量分类和确定优先级。

注 可使用 ACL 保护端口，或使用高级 QoS 策略配置端口，但不可同时使用这两种方法。

每个端口只能有一个 ACL，但例外的是，可以同时将一个基于 IP 的 ACL 和一个基于 IPv6 的 ACL 与一个单独的端口相关联。

要将多个 ACL 与一个端口相关联，必须使用具有一个或多个类映射的策略。

可以定义以下类型的 ACL（具体取决于检查的帧报头部分）：

- MAC ACL — 只检查第 2 层字段，如*定义基于 MAC 的 ACL* 中所述
- IP ACL — 检查 IP 帧的第 3 层，如*基于 IPv4 的 ACL* 中所述
- IPv6 ACL — 检查 IPv4 帧的第 3 层，如*定义基于 IPv6 的 ACL* 中所述

如果一个帧与一个 ACL 中的过滤器相匹配，则系统会将该帧定义为具有该 ACL 名称的流量。在高级 QoS 中，可以使用此流量名称指代这些帧，并将 QoS 应用于这些帧。

ACL 记录

此功能可以向 ACE 添加记录选项。当启用此功能时，ACE 允许或拒绝任何数据包时都会生成与之相关的系统日志通知消息。

如果启用 ACL 记录，可以通过将 ACL 绑定到接口按接口指定此功能。在此情况下，系统会为与接口相关联的允许或拒绝 ACE 相匹配的数据包生成系统日志。

数据流会定义为具有相同特性的数据包流，如下所示：

- **第 2 层数据包** — 相同的源和目标 MAC 地址
- **第 3 层数据包** — 相同的源和目标 IP 地址
- **第 4 层数据包** — 相同的源和目标 IP 地址及 L4 端口

对于新数据流，从特定接口拦截的首个数据包会导致生成系统日志通知消息。来自同一个数据流的其他数据包会通过陷阱产生并送往 CPU，但是此数据流的系统日志消息会限制为每 5 分钟发送一条消息。此系统日志将通知您在过去 5 分钟内至少通过陷阱产生了一个数据包。

系统在处理拦截的数据包后，会转发允许的数据包，并丢弃拒绝的数据包。

支持数据流的数量为每单元 150 个。

系统日志

系统日志消息具有参考性严重性级别，并表明数据包是与拒绝规则还是允许规则相匹配。

- 对于第 2 层数据包，系统日志中包含以下信息（如果适用）：源 MAC 地址、目标 MAC 地址、以太网类型、VLAN-ID 和 CoS 队列。
- 对于第 3 层数据包，系统日志中包含以下信息（如果适用）：源 IP 地址、目标 IP 地址、协议、DSCP 值、ICMP 类型、ICMP 代码和 IGMP 类型。
- 对于第 4 层数据包，系统日志中包含以下信息（如果适用）：源端口、目标端口和 TCP 标签。

以下是可能的系统日志的示例：

- 对于非 IP 数据包：
  - 06-Jun-2013 09:49:56 %3SWCOS-I-LOGDENYMAC: gi0/1: deny ACE 00:00:00:00:00:01 -> ff:ff:ff:ff:ff:ff, Ethertype-2054, VLAN-20, CoS-4, trapped
- 对于 IP 数据包（IPv4 和 IPv6）：
  - 06-Jun-2013 12:38:53 %3SWCOS-I-LOGDENYINET: gi0/1: deny ACE IPv4(255) 1.1.1.1 -> 1.1.1.10, protocol-1, DSCP-54, ICMP Type-Echo Reply, ICMP code-5 , trapped
- 对于第 4 层数据包：
  - 06-Jun-2013 09:53:46 %3SWCOS-I-LOGDENYINETPORTS: gi0/1: deny ACE IPv4(TCP) 1.1.1.1(55) -> 1.1.1.10(66), trapped

配置 ACL

本节介绍如何创建 ACL 以及如何为其添加规则 (ACE)。

创建 ACL 工作流程

要创建 ACL 并将其与一个接口相关联，请执行以下操作：

1. 创建以下类型的一个或多个 ACL：
   a. 使用基于 MAC 的 ACL 和基于 MAC 的 ACE 页面创建基于 MAC 的 ACL
   b. 使用基于 IPv4 的 ACL 和基于 IPv4 的 ACE 页面创建基于 IP 的 ACL
   c. 使用基于 IPv6 的 ACL 和基于 IPv6 的 ACE 页面创建基于 IPv6 的 ACL
2. 使用 ACL 绑定 (VLAN) 或 ACL 绑定（端口）页面将 ACL 与接口相关联。

修改 ACL 工作流程

只有在未使用 ACL 时，才可以对其进行修改。下文介绍解除绑定 ACL 以对其进行修改的过程：

1. 如果 ACL 不属于 QoS 高级模式类映射，但已将其与一个接口相关联，请使用 ACL 绑定 (VLAN) *或* ACL 绑定（端口）页面解除其与该接口的绑定。
2. 如果 ACL 是类映射的一部分并且未与接口绑定，则可以对其进行修改。

3. 如果 ACL 是一个类映射的一部分，且该类映射属于与一个接口绑定的策略，则您必须按如下步骤执行解除绑定的一系列操作：
   - 使用*策略绑定*解除包含类映射的策略与该接口的绑定。
   - 使用*配置策略*（**编辑**）从策略中删除包含 ACL 的类映射。
   - 使用*定义类映射*删除包含 ACL 的类映射。

只有在执行这些操作后，才可以按本节所述修改 ACL。

创建基于 MAC 的 ACL

基于 MAC 的 ACL 用于根据第 2 层字段过滤流量。基于 MAC 的 ACL 会检查所有帧，看是否有匹配项。

基于 MAC 的 ACL 是在基于 MAC 的 ACL 页面中定义的。规则是在基于 MAC 的 ACE 页面中定义的。

基于 MAC 的 ACL

定义基于 MAC 的 ACL 的步骤：

步骤 1 单击**访问控制** > **基于 MAC 的 ACL**。

此页面包含所有当前定义的基于 MAC 的 ACL 列表。

步骤 2 单击**添加**。

步骤 3 在 **ACL 名称**字段中输入新的 ACL 的名称。ACL 名称区分大小写。

步骤 4 单击**应用**。基于 MAC 的 ACL 将保存至当前配置文件中。

基于 MAC 的 ACE

注 每条基于 MAC 的规则都会消耗一条 TCAM 规则。请注意，TCAM 分配将成对执行，这样，对于第一个 ACE，系统将分配 2 条 TCAM 规则，第二条 TCAM 规则将分配给下一个 ACE，以此类推。

为 ACL 添加规则 (ACE) 的步骤：

步骤 1 单击**访问控制** > **基于 MAC 的 ACE**。

步骤 2 选择一个 ACL，然后单击**转至**。系统会列出该 ACL 中的 ACE。

步骤 3 单击**添加**。

步骤 4 输入参数。

- **ACL 名称** — 显示要为其添加 ACE 的 ACL 名称。
- **优先级** — 输入 ACE 的优先级。系统会先处理优先级较高的 ACE。1 代表最高优先级。
- **操作** — 选择找到匹配项时应执行的操作。选项如下：
  - *允许* — 转发符合 ACE 标准的数据包。
  - *拒绝* — 丢弃符合 ACE 标准的数据包。
  - *关闭* — 丢弃符合 ACE 标准的数据包，并禁用从其接收数据包的端口。可以从错误恢复设置页面重新激活这类端口。
- **记录** — 选择该选项可启用与 ACL 规则匹配的 ACL 流的记录功能。
- **时间范围** — 选择后，能够对于具体时间范围限制 ACL 的使用。
- **时间范围名称** — 如果已选中**时间范围**，请选择要使用的时间范围。时间范围已在系统时间配置一节中进行过定义。
- **目标 MAC 地址** — 如果所有目标地址均可接受，则选择*任意*；或选择*用户定义*，以输入一个目标地址或输入目标地址的范围。
- **目标 MAC 地址值** — 输入要将目标 MAC 地址与其相匹配的 MAC 地址及其掩码（如果相关）。
- **目标 MAC 通配符掩码** — 输入掩码以定义 MAC 地址的范围。请注意，此掩码与其他用途的掩码（如子网掩码）不同。在此处，将位设置为 **1** 表示不掩盖，设置为 **0** 表示掩盖该值。

  注 指定一个掩码 0000 0000 0000 0000 0000 0000 1111 1111（意思是如果匹配，则该位为 0，如不匹配，则该位为 1）。您需要将有 1 的数字转换为十进制整数，而每四个 0 要写成一个 0。在此示例中，因为 1111 1111 = 255，因此该掩码将写成：0.0.0.255。
- **源 MAC 地址** — 如果所有源地址均可接受，则选择*任意*；或选择*用户定义*，以输入一个源地址或输入源地址的范围。

- **源 MAC 地址值** — 输入要将源 MAC 地址与其相匹配的 MAC 地址及其掩码（如果相关）。
- **源 MAC 通配符掩码** — 输入掩码以定义 MAC 地址的范围。
- **VLAN ID** — 输入 VLAN 标记中要匹配的 VLAN ID 部分。
- **802.1p** — 选择**包含**以使用 802.1p。
- **802.1p 值** — 输入要添加到 VPT 标记的 802.1p 值。
- **802.1p 掩码** — 输入要应用于 VPT 标记的通配符掩码。
- **以太网类型** — 输入要匹配的帧以太网类型。

步骤 5 单击**应用**。基于 MAC 的 ACE 将保存至当前配置文件中。

创建基于 IPv4 的 ACL

基于 IPv4 的 ACL 用于检查 IPv4 数据包，而不检查其他类型的帧（例如 ARP）。

可以匹配以下字段：

- IP 协议（按照已知协议的名称或直接按照值）
- TCP/UDP 流量的源端口/目标端口
- TCP 帧的标签值
- ICMP 和 IGMP 类型和代码
- 源 IP 地址/目标 IP 地址（包括通配符）
- DSCP/IP 优先级值

注 ACL 也用作流量定义的构建元素，流量定义用于进行每个流量的 QoS 处理。

使用基于 IPv4 的 ACL 页面可以为系统添加 ACL。规则是在基于 IPv4 的 ACE 页面中定义的。

IPv6 ACL 是在“基于 IPv6 的 ACL”页面中定义的。

基于 IPv4 的 ACL

定义基于 IPv4 的 ACL 的步骤：

步骤 1 单击**访问控制** > **基于 IPv4 的 ACL**。

此页面包含所有当前定义的基于 IPv4 的 ACL。

步骤 2 单击**添加**。

步骤 3 在 **ACL 名称**字段中输入新的 ACL 的名称。名称区分大小写。

步骤 4 单击**应用**。基于 IPv4 的 ACL 将保存至当前配置文件中。

基于 IPv4 的 ACE

注 每条基于 IPv4 的规则都会消耗一条 TCAM 规则。请注意，TCAM 分配将成对执行，这样，对于第一个 ACE，系统将分配 2 条 TCAM 规则，第二条 TCAM 规则将分配给下一个 ACE，以此类推。

为基于 IPv4 的 ACL 添加规则 (ACE) 的步骤：

步骤 1 单击**访问控制** > **基于 IPv4 的 ACE**。

步骤 2 选择一个 ACL，然后单击**转至**。系统会显示当前为选择的 ACL 定义的所有 IP ACE。

步骤 3 单击**添加**。

步骤 4 输入参数。

- **ACL 名称** — 显示 ACL 的名称。
- **优先级** — 输入优先级。系统会先处理优先级较高的 ACE。
- **操作** — 选择为与 ACE 匹配的数据包分配的操作。选项如下：
  - *允许* — 转发符合 ACE 标准的数据包。
  - *拒绝* — 丢弃符合 ACE 标准的数据包。
  - *关闭* —丢弃符合 ACE 标准的数据包，并禁用将数据包发送到的端口。可以从错误恢复设置页面重新激活端口。
- **记录** — 选择该选项可启用与 ACL 规则匹配的 ACL 流的记录功能。
- **时间范围** — 选择后，能够对于具体时间范围限制 ACL 的使用。

- **时间范围名称** — 如果已选中**时间范围**，请选择要使用的时间范围。时间范围已在系统时间配置一节中进行过定义。
- **协议** — 选择该选项可根据一个特定协议或协议 ID 来创建 ACE。选择*任意 (IPv4)* 可接受所有 IP 协议。或者，从下拉列表**从列表中选择**选择以下协议之一：
  - *ICMP* — 互联网控制消息协议
  - *IGMP* — 互联网组管理协议
  - *IP-in-IP* — IP-in-IP 封装
  - *TCP* — 传输控制协议
  - *EGP* — 外部网关协议
  - *IGP* — 内部网关协议
  - *UDP* — 用户数据报协议
  - *HMP* — 主机映射协议
  - *RDP* — 可靠数据报协议
  - *IDPR* — 域间策略路由协议
  - *IPV6* — IPv6-over-IPv4 隧道
  - *IPV6:ROUT* — 对属于通过一个网关的 IPv6-over-IPv4 路由的数据包进行匹配
  - *IPV6:FRAG* — 对属于 IPv6-over-IPv4 片段报头的数据包进行匹配
  - *IDRP* — 域间路由协议
  - *RSVP* — 保留协议
  - *AH* — 身份验证报头
  - *IPV6:ICMP* — 互联网控制消息协议
  - *EIGRP* — 增强型内部网关路由协议
  - *OSPF* — 首先打开最短路径
  - *IPIP* — IP-in-IP
  - *PIM* — 协议独立组播
  - *L2TP* — 第 2 层隧道协议
  - *ISIS* — 特定于 IGP 的协议
  - *要匹配的协议 ID* — 不选择名称，而输入协议 ID。

- **源 IP 地址** — 如果所有源地址均可接受，则选择*任意*；或选择*用户定义*，以输入一个源地址或输入源地址的范围。
- **源 IP 地址值** — 输入要将源 IP 地址与其相匹配的 IP 地址。
- **源 IP 通配符掩码** — 输入掩码以定义 IP 地址的范围。请注意，此掩码与其他用途的掩码（如子网掩码）不同。在此处，将位设置为 1 表示不掩盖，设置为 0 表示掩盖该值。

  注 指定一个掩码 0000 0000 0000 0000 0000 0000 1111 1111（意思是如果匹配，则该位为 0，如不匹配，则该位为 1）。您需要将有 1 的数字转换为十进制整数，而每四个 0 要写成一个 0。在此示例中，因为 1111 1111 = 255，因此该掩码将写成：0.0.0.255。
- **目标 IP 地址** — 如果所有目标地址均可接受，则选择*任意*；或选择*用户定义*，以输入一个目标地址或输入目标地址的范围。
- **目标 IP 地址值** — 输入要将目标 MAC 地址与其相匹配的 IP 地址。
- **目标 IP 通配符掩码** — 输入掩码以定义 IP 地址的范围。
- **源端口** — 请选择以下选项之一：
  - *任意* — 与所有源端口匹配。
  - *从列表选择单个* — 选择要将数据包与其相匹配的一个单独 TCP/UDP 源端口。仅当您在“从列表中选择”下拉菜单中选择 800/6-TCP 或 800/17-UDP 后，系统才会激活这个字段。
  - *按编号选择单个* — 输入要将数据包与其相匹配的一个单独 TCP/UDP 源端口。仅当您在从列表中选择下拉菜单中选择 800/6-TCP 或 800/17-UDP 后，系统才会激活这个字段。
  - *范围* — 选择要将数据包与其相匹配的 TCP/UDP 源端口的范围。可配置八个不同的端口范围（源端口与目标端口共享）。TCP 和 UDP 协议各有八个端口范围。
- **目标端口** — 请选择可用值之一。这些可用值与上述源端口字段中的可用值相同。

  注 您必须为 ACE 指定 IP 协议，才能输入源端口和/或目标端口。
- **TCP 标签** — 选择要用来过滤数据包的一个或多个 TCP 标签。会转发或丢弃过滤的数据包。通过 TCP 标签过滤数据包可以加强数据包控制，从而提高网络安全性。

- **服务类型** — IP 数据包的服务类型。
  - *任意* — 任意服务类型
  - *要匹配的 DSCP* — 与差分服务代码点 (DSCP) 相匹配
  - *要匹配的 IP 优先级* — IP 优先级是一个 TOS（服务类型）模式，网络使用该模式可有助于兑现相应的 QoS 承诺。此模式使用 IP 报头中服务类型字节的 3 个最高位，如 RFC 791 和 RFC 1349 中所述。
- **ICMP** — 如果 ACL 的 IP 协议为 ICMP，请选择用于过滤用途的 ICMP 消息类型。按照名称选择消息类型或输入消息类型编号：
  - *任意* — 可接受所有消息类型。
  - *从列表中选择* — 按照名称选择消息类型。
  - *要匹配的 ICMP 类型* — 要用于过滤用途的消息类型编号。
- **ICMP 代码** — ICMP 消息可能有一个代码字段，指示如何处理消息。请选择以下选项之一，以配置是否对此代码进行过滤：
  - *任意* — 接受所有代码。
  - *用户定义* — 输入用于过滤用途的 ICMP 代码。
- **IGMP** — 如果 ACL 基于 IGMP，请选择用于过滤用途的 IGMP 消息类型。按照名称选择消息类型或输入消息类型编号：
  - *任意* — 可接受所有消息类型。
  - *从列表中选择* — 按照名称选择消息类型。
  - *要匹配的 IGMP 类型* — 将用于过滤用途的消息类型编号。

步骤 5 单击**应用**。基于 IPv4 的 ACE 将保存至当前配置文件中。

创建基于 IPv6 的 ACL

基于 IPv6 的 ACL 页面会显示并启用 IPv6 ACL 的创建操作，该操作会检查单纯基于 IPv6 的流量。IPv6 ACL 不会检查 IPv6-over-IPv4 或 ARP 数据包。

注 ACL 也用作流量定义的构建元素，流量定义用于进行每个流量的 QoS 处理。

基于 IPv6 的 ACL

定义基于 IPv6 的 ACL 的步骤：

步骤 1 单击**访问控制** > **基于 IPv6 的 ACL**。

该窗口包含所定义 ACL 及其内容的列表

步骤 2 单击**添加**。

步骤 3 在 **ACL 名称**字段中输入新的 ACL 的名称。名称区分大小写。

步骤 4 单击**应用**。基于 IPv6 的 ACL 将保存至当前配置文件中。

基于 IPv6 的 ACE

注 每条基于 IPv6 的规则都会消耗两条 TCAM 规则。

步骤 1 单击**访问控制** > **基于 IPv6 的 ACE**。

该窗口包含一个指定 ACL（规则组）的 ACE（规则）。

步骤 2 选择一个 ACL，然后单击**转至**。系统会显示当前为选择的 ACL 定义的所有 IP ACE。

步骤 3 单击**添加**。

步骤 4 输入参数。

- **ACL 名称** — 显示要为其添加 ACE 的 ACL 名称。
- **优先级** — 输入优先级。系统会先处理优先级较高的 ACE。
- **操作** — 选择为与 ACE 匹配的数据包分配的操作。选项如下：
  - *允许* — 转发符合 ACE 标准的数据包。
  - *拒绝* — 丢弃符合 ACE 标准的数据包。
  - *关闭* — 丢弃符合 ACE 标准的数据包，并禁用将数据包发送到的端口。可以从错误恢复设置页面重新激活端口。
- **记录** — 选择该选项可启用与 ACL 规则匹配的 ACL 流的记录功能。
- **时间范围** — 选择后，能够对于具体时间范围限制 ACL 的使用。
- **时间范围名称** — 如果已选中**时间范围**，请选择要使用的时间范围。时间范围已在系统时间一节中进行过介绍。

- **协议** — 选择该选项可根据一个特定协议来创建 ACE。选择*任意 (IPv6)* 可接受所有 IP 协议。

  或者，选择以下协议之一：

  - *TCP* — 传输控制协议。可让两个主机进行通信并交换数据流。TCP 可保证将数据包送达，并保证按照发送数据包的顺序来传输和接收数据包。
  - *UDP* — 用户数据报协议。传输数据包，但不保证将数据包送达。
  - *ICMP* — 将数据包与互联网控制消息协议 (ICMP) 相匹配。

  或

  - *要匹配的协议 ID* — 输入要匹配的协议的 ID。
- **源 IP 地址** — 如果所有源地址均可接受，则选择*任意*；或选择*用户定义*，以输入一个源地址或输入源地址的范围。
- **源 IP 地址值** — 输入要将源 IP 地址与其相匹配的 IP 地址及其掩码（如果相关）。
- **源 IP 前缀长度** — 输入源 IP 地址的前缀长度。
- **目标 IP 地址** — 如果所有目标地址均可接受，则选择*任意*；或选择*用户定义*，以输入一个目标地址或输入目标地址的范围。
- **目标 IP 地址值** — 输入要将目标 MAC 地址与其相匹配的 IP 地址及其掩码（如果相关）。
- **目标 IP 前缀长度** — 输入 IP 地址的前缀长度。
- **源端口** — 请选择以下选项之一：
  - *任意* — 与所有源端口匹配。
  - *从列表选择* — 选择要将数据包与其相匹配的一个单独 TCP/UDP 源端口。仅当您在 IP 协议下拉菜单中选择 800/6-TCP 或 800/17-UDP 后，此字段才会激活。
  - *按编号* — 输入要将数据包与其相匹配的一个单独 TCP/UDP 源端口。仅当您在 IP 协议下拉菜单中选择 800/6-TCP 或 800/17-UDP 后，此字段才会激活。
- **目标端口** — 请选择可用值之一。这些可用值与上述源端口**源端口**字段中的可用值相同。

  注 您必须为 ACL 指定 IPv6 协议，然后才能配置源端口和/或目标端口。

- **流标签** — 根据 IPv6“流标签”字段对 IPv6 流量分类。该字段长度 20 位，是 IPv6 数据包报头的组成部分。源工作站可使用 IPv6 流标签为属于相同数据流的一系列数据包加标签。如果可接受所有流标签，则选择*任意*；或选择*用户定义*，以输入要接受的特定流标签。
- **TCP 标签** — 选择要用来过滤数据包的一个或多个 TCP 标签。会转发或丢弃过滤的数据包。通过 TCP 标签过滤数据包可以加强数据包控制，从而提高网络安全性。为每一种标签类型选择以下选项之一：
  - *设置* — 如果标签为“设置”，则匹配。
  - *未设置* — 如果标签为“未设置”，则匹配。
  - *忽略* — 忽略 TCP 标签。
- **服务类型** — IP 数据包的服务类型。
  - *任意* — 任意服务类型
  - *要匹配的 DSCP* — 与差分服务代码点 (DSCP) 相匹配
  - *要匹配的 IP 优先级* — IP 优先级是一个 TOS（服务类型）模式，网络使用该模式可有助于兑现相应的 QoS 承诺。此模式使用 IP 报头中服务类型字节的 3 个最高位，如 RFC 791 和 RFC 1349 中所述。
- **ICMP** — 如果 ACL 基于 ICMP，请选择用于过滤用途的 ICMP 消息类型。按照名称选择消息类型或输入消息类型编号。如果可接受所有消息类型，请选择*任意*。
  - *任意* — 可接受所有消息类型。
  - *从列表中选择* — 从下拉列表中，按名称选择消息类型。
  - *要匹配的 ICMP 类型* — 将用于过滤用途的消息类型编号。
- **ICMP 代码** — ICMP 消息可能有一个代码字段，指示如何处理消息。请选择以下选项之一，以配置是否对此代码进行过滤：
  - *任意* — 接受所有代码。
  - *用户定义* — 输入用于过滤用途的 ICMP 代码。

步骤 5 单击**应用**。

ACL 绑定

将一个 ACL 与一个接口（端口、LAG 或 VLAN）绑定后，系统会将该 ACL 的 ACE 规则应用于到达该接口的数据包。系统会将与该 ACL 中任何 ACE 均不匹配的数据包与默认规则相匹配，该默认规则的操作为丢弃不匹配的数据包。

虽然只能将每个接口与一个 ACL 绑定，但也可以将多个接口与同一 ACL 绑定，方法是：将多个接口分组到一个策略映射，然后将该策略映射与该接口绑定。

将一个 ACL 与一个接口绑定后，便无法编辑、修改或删除该 ACL，直到您将其从与其绑定或正在使用它的所有端口中删除。

注 可以将接口（端口、LAG 或 VLAN）绑定到策略或 ACL，但它们无法同时绑定到策略和 ACL。

注 在相同的类映射中，MAC ACL 不能与拥有目标 IPv6 地址作为过滤条件的 IPv6 ACE 一起使用。

ACL 绑定 (VLAN)

将 ACL 绑定到 VLAN 的步骤：

步骤 1 单击**访问控制** > **ACL 绑定 (VLAN)**。

步骤 2 选择一个 VLAN，然后单击**编辑**。

如果您需要的 VLAN 未显示，请添加一个 VLAN。

步骤 3 选择以下选项之一：

- **基于 MAC 的 ACL** — 选择要与该接口绑定的基于 MAC 的 ACL。
- **基于 IPv4 的 ACL** — 选择要与该接口绑定的基于 IPv4 的 ACL。
- **基于 IPv6 的 ACL** — 选择要与该接口绑定的基于 IPv6 的 ACL。
- **默认操作** — 请选择以下其中一个选项：
  - *拒绝任意* — 如果数据包与 ACL 不匹配，将被拒绝（丢弃）。
  - *允许任意* — 如果数据包与 ACL 不匹配，将被允许（转发）。

  注 仅当接口上未激活“IP 源防护”时，才能定义“默认操作”。

步骤 4 单击**应用**。系统将修改 ACL 绑定，并更新当前配置文件。

注 如果不选择任何 ACL，则系统会将之前与该 VLAN 绑定的 ACL 解除绑定。

ACL 绑定（端口）

将 ACL 绑定到端口或 LAG 的步骤：

步骤 1 单击**访问控制** > **ACL 绑定（端口）**。

步骤 2 选择接口类型**端口/LAG**（端口或 LAG）。

步骤 3 单击**转至**。对于选中的每个类型的接口，该类型的所有接口都与其当前 ACL 一同显示（对于**输入 ACL** 和**输出 ACL**）：

- **接口** — 在其上定义 ACL 的接口的标识符。
- **MAC ACL** — 与接口绑定的 MAC 类型的 ACL（如果有）。
- **IPv4 ACL** — 与接口绑定的 IPv4 类型的 ACL（如果有）。
- **IPv6 ACL** — 与接口绑定的 IPv6 类型的 ACL（如果有）。
- **默认操作** — ACL 规则的操作（丢弃任意还是允许任意）。

注 要解除绑定某接口绑定的所有 ACL，请选择该接口，然后单击**清除**。

步骤 4 选择一个接口，并单击**编辑**。

步骤 5 对于输入和输出 ACL，输入以下信息：

输入 ACL

- **基于 MAC 的 ACL** — 选择要与该接口绑定的基于 MAC 的 ACL。
- **基于 IPv4 的 ACL** — 选择要与该接口绑定的基于 IPv4 的 ACL。
- **基于 IPv6 的 ACL** — 选择要与该接口绑定的基于 IPv6 的 ACL。
- **默认操作** — 请选择以下其中一个选项：
  - *拒绝任意* — 如果数据包与 ACL 不匹配，将被拒绝（丢弃）。
  - *允许任意* — 如果数据包与 ACL 不匹配，将被允许（转发）。

注 仅当接口上未激活“IP 源防护”时，才能定义“默认操作”。

输出 ACL

- **基于 MAC 的 ACL** — 选择要与该接口绑定的基于 MAC 的 ACL。
- **基于 IPv4 的 ACL** — 选择要与该接口绑定的基于 IPv4 的 ACL。

- **基于 IPv6 的 ACL** — 选择要与该接口绑定的基于 IPv6 的 ACL。
- **默认操作** — 请选择以下其中一个选项：
  - *拒绝任意* — 如果数据包与 ACL 不匹配，将被拒绝（丢弃）。
  - *允许任意* — 如果数据包与 ACL 不匹配，将被允许（转发）。

  注 仅当接口上未激活“IP 源防护”时，才能定义“默认操作”。

步骤 6 单击**应用**。系统将修改 ACL 绑定，并更新当前配置文件。

注 如果不选择任何 ACL，则系统会将之前与该接口绑定的 ACL 解除绑定。

23

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
- 常规
- QoS 基本模式
- QoS 高级模式
- 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。
- **分配至软件队列** — 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。请参阅队列。
- **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

在全局设置页面中输入受信任的报头字段。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 模式

选择的 QoS 模式将应用到系统中的所有接口。

- **基本模式** — 服务等级 (CoS)。

  相同等级的所有流量接受的处理相同，这是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。这可以是第 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，设备信任此外部分配的 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报头字段。对于该字段的每个值，在 CoS/802.1p 到队列或 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，系统会通过该队列发送帧。

- **高级模式** — 每数据流服务质量 (QoS)。

  在高级模式中，每数据流 QoS 由一个类映射和/或一个策略器组成：

  - 类映射定义数据流中的流量类型，其中包含一个或多个 ACL。符合这些 ACL 的数据包将属于该数据流。
  - 策略器会将配置的 QoS 应用到数据流。数据流的 QoS 配置可由出口队列、DSCP 或 CoS/802.1p 值，以及对超出模板的（超限）流量执行的操作组成。

- **禁用模式** — 在此模式中，会将所有流量映射到单个尽力服务队列，以便为所有类型的流量设置相同的优先级。

一次只能有一个模式处于活动状态。如果将系统配置为在 QoS 高级模式下工作，则 QoS 基本模式的设置将处于非活动状态，反之亦然。

如果更改模式，将发生以下情况：

- 如果从 QoS 高级模式更改为任何其他模式，系统将会删除策略模板定义和类映射。直接绑定到接口的 ACL 会保持绑定状态。
- 如果从 QoS 基本模式更改为高级模式，系统将不会保留基本模式下的 QoS 信任模式配置。
- 如果禁用 QoS，系统会将整形程序和队列设置（WRR/SP 带宽设置）重置为默认值。

所有其他用户配置将保持不变。

QoS 工作流程

要配置一般 QoS 参数，请执行以下操作：

步骤 1 使用 QoS 属性页面为系统选择 QoS 模式（基本模式、高级模式或禁用模式，如“QoS 模式”一节中所述）。下面的工作流程步骤假设您选择启用 QoS。

步骤 2 使用 QoS 属性页面为每个接口指定一个默认的 CoS 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。如果设备处于 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。如果设备处于 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。可以使用 CoS/802.1p 到队列页面完成此操作。

步骤 6 如果只需要第 3 层流量，请使用 DSCP 到队列页面为每个 DSCP/TC 值指定一个队列。

步骤 7 在以下页面中输入带宽和速率限制：

a. 使用每队列的出口整形页面为每个队列设置出口整形。

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。

步骤 8 通过执行下面的一项操作来配置选择的模式：

a. 按“*配置基本 QoS 模式的工作流程*”中所述配置基本模式。

b. 按“*配置高级 QoS 模式的工作流程*”中所述配置高级模式。

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。如果设备处于 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。如果设备处于 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。

常规

本节包含以下主题：

- QoS 属性
- 队列
- CoS/802.1p 到队列
- DSCP 到队列
- 带宽
- 每队列的出口整形
- VLAN 入口速率限制
- TCP 拥塞避免

QoS 属性

“QoS 属性”页面包含用于设置系统 QoS 模式（基本模式、高级模式或禁用模式，如“QoS 模式”一节中所述）的字段。

启用 QoS 并选择 QoS 模式的步骤：

步骤 1 单击**服务质量** > **一般** > **QoS 属性**。

步骤 2 设置 QoS 模式。可用的选项如下：

- **禁用** — 在设备上禁用 QoS。
- **基本** — 在设备上启用基本模式的 QoS。
- **高级** — 在设备上启用高级模式的 QoS。

步骤 3 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。该默认值仅当系统处于基本模式，并在全局设置页面中选择“信任 CoS”的情况下，对无标记帧有效。

步骤 4 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**。

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。

步骤 2 单击**应用**。接口默认 CoS 值将保存至当前配置文件。

要恢复默认 CoS 值，请单击**恢复 CoS 默认设置**。

队列

设备的每个接口支持 8 个队列。编号为 8 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，如果最多只可能有四个队列且四个队列都为 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”，则系统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 数据的步骤：

步骤 1 单击**服务质量** > **一般** > **队列**。

步骤 2 输入参数。

- **队列** — 显示队列编号。
- **调度方法** — 选择以下选项之一：
  - *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，才会采用此划分方法。

- *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。

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。对于传入的无标记数据包，802.1p 优先级是指定给入口端口的默认 CoS/802.1p 优先级。

下表介绍 8 个队列时的默认映射：

通过更改“CoS/802.1p 到队列”映射（CoS/802.1p 到队列）和队列调度方法及带宽分配（“队列”页面），可以在网络中达到所需的服务质量。

仅当存在以下条件之一时，“CoS/802.1p 到队列”映射才适用：

- 设备处于 QoS 基本模式和 CoS/802.1p 信任模式
- 设备处于 QoS 高级模式，且数据包属于 CoS/802.1p 信任数据流

队列 1 的优先级最低，350 和 550 系列中队列 8 的优先级最高。

将 CoS 值映射到出站队列的步骤：

步骤 1 单击**服务质量** > **一般** > **CoS/802.1p 到队列**。

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 4 或 8 个出口队列，其中队列 4 或队列 8 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**、**取消**或**恢复默认设置**。系统执行 801.1p 优先级值到队列的映射，并更新当前配置文件，输入的更改将取消或恢复之前定义的值。

DSCP 到队列

使用“DSCP（IP 差分服务代码点）到队列”页面，可以将 DSCP 值映射到出口队列。“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”映射仅在以下条件下适用于 IP 数据包：

- 设备处于 QoS 基本模式，DSCP 处于信任模式，或者
- 设备处于 QoS 高级模式，且数据包属于 DSCP 信任数据流

非 IP 数据包始终分类为尽力服务队列。

以下各表介绍 7 最高且 8 用于堆栈控制目的时 8 队列系统的默认 DSCP 到队列映射。

DSCP	63	55	47	39	31	23	15	7
队列	6	6	7	5	4	3	2	1
DSCP	62	54	46	38	30	22	14	6
队列	6	6	7	5	4	3	2	1
DSCP	61	53	45	37	29	21	13	5
队列	6	6	7	5	4	3	2	1
DSCP	60	52	44	36	28	20	12	4
队列	6	6	7	5	4	3	2	1
DSCP	59	51	43	35	27	19	11	3
队列	6	6	7	5	4	3	2	1
DSCP	58	50	42	34	26	18	10	2
队列	6	6	7	5	4	3	2	1
DSCP	57	49	41	33	25	17	9	1
队列	6	6	7	5	4	3	2	1

DSCP	56	48	40	32	24	16	8	0
队列	6	6	6	7	6	6	1	1

以下各表介绍 8 最高时 8 队列系统的默认 DSCP 到队列映射：

DSCP	63	55	47	39	31	23	15	7
队列	7	7	8	6	5	4	3	1
DSCP	62	54	46	38	30	22	14	6
队列	7	7	8	6	5	4	3	1
DSCP	61	53	45	37	29	21	13	5
队列	7	7	8	6	5	4	3	1
DSCP	60	52	44	36	28	20	12	4
队列	7	7	8	6	5	4	3	1
DSCP	59	51	43	35	27	19	11	3
队列	7	7	8	6	5	4	3	1
DSCP	58	50	42	34	26	18	10	2
队列	7	7	8	6	5	4	3	1
DSCP	57	49	41	33	25	17	9	1
队列	7	7	8	6	5	4	3	1
DSCP	56	48	40	32	24	16	8	0
队列	7	7	7	8	7	7	1	2

将 DSCP 映射到队列的步骤：

步骤 1 单击**服务质量** > **一般** > **DSCP 到队列**。

“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。

带宽

“带宽”页面会显示每个接口的带宽信息。

查看带宽信息的步骤：

步骤 1 单击**服务质量** > **一般** > **带宽**。

除以下字段外，此页面中的相关字段会在下面的“编辑”页面介绍：

- **入口速率限制：**
  - *状态* — 显示“入口速率限制”是否已启用。
  - *速率限制（千位/秒）* — 显示端口的入口速率限制。
  - *%* — 显示端口带宽除以总端口带宽所得的入口速率限制。
  - *CBS（字节）* — 以数据字节数表示的入口接口的最大突发数据大小。
- **出口整形速率：**
  - *状态* — 显示“出口整形速率”是否已启用。
  - *CIR（千位/秒）* — 显示出口接口的最大带宽。
  - *CBS（字节）* — 以数据字节数表示的出口接口的最大突发数据大小。

步骤 2 选择一个接口，并单击**编辑**。

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。（不适用于 LAG）
- **入口速率限制（千位/秒）** — 输入接口所允许的最大带宽。（不适用于 LAG）

- **入口承诺突发数据大小 (CBS)** — 以数据字节数的形式输入入口接口的最大突发数据大小。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。该字段仅在接口为端口时可用。（不适用于 LAG）
- **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。
- **出口承诺突发数据大小 (CBS)** — 以数据字节数的形式输入出口接口的最大突发数据大小 。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。

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，设备还可以在每队列每端口基础上，限制所选出站帧的传输速率。出口速率限制由输出负载整形功能执行。

设备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**，

“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大小。

步骤 2 选择接口类型（端口或 LAG），然后单击**转至**。

步骤 3 选择一个端口/LAG，然后单击**编辑**。

使用该页面可对每个接口上最多八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。

VLAN 入口速率限制

通过每 VLAN 速率限制（在“VLAN 入口速率限制”页面中执行），可实现 VLAN 上的流量限制。如果配置了 VLAN 入站速率限制，它将限制从设备上的所有端口汇总的流量。

以下限制适用于每 VLAN 速率限制：

- 它所具有的优先级低于系统中定义的任何其他流量管制。例如，如果数据包既受 QoS 速率限制，也受 VLAN 速率限制，而这两种速率限制冲突，在这种情况下 QoS 速率限制优先。
- 它在设备层面上以及数据包处理器层面的设备中应用。如果设备上具有多个数据包，配置的 VLAN 速率限制值将分别应用到每个数据包处理器。具有最多 24 个端口的设备有一个数据包处理器，而具有 48 个或更多端口的设备则有两个数据包处理器。

速率限制是分别针对一个单元中的每个数据包处理器以及一个堆叠中的每个单元进行计算的。

定义 VLAN 入口速率限制的步骤：

步骤 1 单击**服务质量** > **一般** > **VLAN 入口速率限制**。

此页面会显示 VLAN 入口速率限制表。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **VLAN ID** — 选择 VLAN。
- **承诺的信息传输速率 (CIR)** — 以千字节每秒为单位输入 VLAN 可以接受的平均最大数据量。
- **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。无法针对 LAG 输入该字段的值。

步骤 4 单击**应用**。系统将定义 VLAN 速率限制，并更新当前配置文件。

TCP 拥塞避免

使用“TCP 拥塞避免”页面可激活 TCP 拥塞避免算法。该算法可破除或避免拥塞节点（拥塞由众多发送具有相同字节数的数据包的源引起）中的 TCP 全局同步。

配置 TCP 拥塞避免的步骤：

步骤 1 单击**服务质量** > **一般** > **TCP 拥塞避免**。

步骤 2 单击**启用**以启用 TCP 拥塞避免，然后单击**应用**。

QoS 基本模式

本节包含以下主题：

- 概述
- 全局设置
- 接口设置

概述

在 QoS 基本模式中，可以将网络中的特定域定义为信任域。在该域中，将使用 802.1p 优先级和/或 DSCP 标记数据包，以标志数据包需要的服务类型。该域中的节点可使用这些字段将数据包分配给特定的出口队列。最初的数据包分类和对这些字段的标记是在信任域的入口流量中完成的。

配置基本 QoS 模式的工作流程

要配置基本 QoS 模式，请执行以下操作：

1. 使用“QoS 属性”页面为系统选择基本模式。
2. 使用“全局设置”页面选择信任行为。设备支持 CoS/802.1p 信任模式和 DSCP 信任模式。CoS/802.1p 信任模式在 VLAN 标记中使用 802.1p 优先级。DSCP 信任模式在 IP 报头中使用 DSCP 值。

如果存在任何不该信任传入 CoS 标记的例外端口，请使用“接口设置”页面禁用该端口上的 QoS 状态。

使用“接口设置”页面可以在端口启用或禁用选择的全局信任模式。如果端口被禁用，无信任模式，则其所有入口数据包均将按照尽力服务规则转发。建议在传入数据包中的 CoS/802.1p 和/或 DSCP 值不值得信任的情况下，在端口禁用信任模式。否则可能会对网络性能产生负面影响。

全局设置

“全局设置”页面包含用于在设备上启用信任模式的信息（请参阅下面的“信任模式”字段）。如果 QoS 模式为基本模式，该配置便有效。进入 QoS 域的数据包将在 QoS 域的边缘进行分类。

定义信任配置的步骤：

步骤 1 单击**服务质量** > **QoS 基本模式** > **全局设置**。

步骤 2 设备为基本模式时，选择**信任模式**。如果将数据包 CoS 等级和 DSCP 标记映射至独立队列，信任模式将确定数据包所分配的队列：

- **CoS/802.1p** — 根据 VLAN 标记中的 VPT 字段或每端口的默认 CoS/802.1p 值（如果传入数据包中没有 VLAN 标记）将流量映射到队列，实际的 VPT 到队列映射可以在映射“CoS/802.1p 到队列”页面配置。
- **DSCP** — 将根据 IP 报头中的 DSCP 字段将所有 IP 流量映射到队列。实际的 DSCP 到队列映射可以在“DSCP 到队列”页面中配置。如果流量不是 IP 流量，系统会将其映射到尽力服务队列。
- **CoS/802.1p-DSCP** — 已进行过设置的 CoS/802.1p 或 DSCP。

步骤 3 选择**覆盖入口 DSCP**，使用在 DSCP 覆盖表中输入的新值取代传入数据包中的原始 DSCP 值。启用“覆盖入口 DSCP”后，设备会对出口排队使用新的 DSCP 值。还会使用新的 DSCP 值取代数据包中的原始 DSCP 值。

注 系统将使用新的（改写后的）DSCP 值而非原始 DSCP 值将帧映射到出口队列。

步骤 4 如果启用了**覆盖入口 DSCP**，请单击 **DSCP 覆盖表**重新配置 DSCP。（请参阅 **DSCP 覆盖表**。）

步骤 5 **DSCP 传入**会显示需要重新标记为替代值的传入数据包 DSCP 值。选择**传出 DSCP** 值以指示已映射传出值。

步骤 6 单击**应用**。系统将使用新 DSCP 值更新当前配置文件。

接口设置

使用“接口设置”页面可在设备的每个端口上配置 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** > **QoS 基本模式** > **接口设置**。

步骤 2 选择**端口**或 **LAG** 以显示端口或 LAG 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**。

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。

QoS 高级模式

本节包含以下主题：

- 概述
- 配置高级 QoS 模式的工作流程
- 全局设置
- 超出模板的 DSCP 重新标记
- 类映射
- 集合策略器
- 策略表
- 策略类映射
- 策略绑定

概述

符合 ACL 并被允许进入的帧将使用允许其进入的 ACL 的名称进行隐式标记。然后，即可将 QoS 高级模式操作应用到这些数据流。

在 QoS 高级模式中，设备会使用策略支持每个数据流的 QoS。策略及其组件具有以下特性及关系：

- 一个策略包含一个或多个类映射。
- 类映射使用一个或多个关联 ACL 定义数据流。仅符合带许可（转发）操作的类映射中的 ACL 规则 (ACE) 的数据包将被视为属于同一个数据流，将遵循相同的服务质量。因此，策略包含一个或多个数据流，每个数据流均有一个用户定义的 QoS。
- 类映射（数据流）的 QoS 由关联的策略器强制执行。存在两种策略器：单策略器和集合策略器。每种策略器通过一个 QoS 规格进行配置。单策略器可根据相应的策略器 QoS 规格将 QoS 应用到单个类映射，从而应用到单个数据流。集合策略器可将 QoS 应用到一个或多个类映射，从而应用到一个或多个数据流。集合策略器可以支持来自不同策略的类映射。
- 通过将策略绑定至所需的端口，可将每数据流 QoS 应用到数据流。可以将一个策略及其类映射绑定至一个或多个端口，但每个端口最多只能与一个策略绑定。

注：

- 设备为第 2 层模式时，单策略器和集合策略器均可用。
- 不论策略为何，均可以将一个 ACL 配置到一个或多个类映射。
- 一个类映射只能属于一个策略。
- 将使用单策略器的类映射绑定至多个端口时，每个端口都具有其自己的单策略器实例；每个实例在相互独立的端口处对该类映射（数据流）应用 QoS。
- 不论策略和端口为何，集合策略器均会将 QoS 应用到其在集合中的所有数据流。

高级 QoS 设置由三部分组成：

- 要符合的规则的定义。符合单独的一组规则的所有帧将被视为一个*数据流*。
- 要对每个数据流中符合规则的帧应用的操作的定义。
- 将规则和操作的组合绑定至一个或多个接口。

配置高级 QoS 模式的工作流程

要配置高级 QoS 模式，请执行以下操作：

1. 使用“QoS 属性”页面为系统选择高级模式。使用“全局设置”页面选择信任模式。如果将数据包 CoS 等级和 DSCP 标记映射至独立队列，信任模式将确定数据包所分配的队列：
   - 如果内部 DSCP 值与传入数据包中使用的 DSCP 值不同，请使用“超出模板的 DSCP 重新标记”页面将外部值映射到内部值。该操作将打开“DSCP 重新标记”页面。
2. 按“创建 ACL 工作流程”中所述创建 ACL。
3. 如果定义了 ACL，请通过“类映射”页面创建类映射并将 ACL 与创建的类映射相关联。
4. 使用“策略表”页面创建一个策略，并使用“策略类映射”页面将该策略与一个或多个类映射相关联。您还可以根据需要，在将类映射关联至策略时，通过将策略器指定给类映射来指定 QoS。
   - **单策略器** — 使用“策略表”页面和“类映射”页面创建将类映射与单策略器关联的策略。在该策略内，定义单策略器。
   - **集合策略器** — 使用“集合策略器”页面针对每个数据流创建如下 QoS 操作：将所有符合的帧发送到同一个策略器（集合策略器）。使用“策略表”页面创建将类映射与集合策略器关联的策略。
5. 使用“策略绑定”页面将策略绑定至接口。

全局设置

“全局设置”页面包含用于在设备上启用信任模式的信息。进入 QoS 域的数据包将在 QoS 域的边缘进行分类。

定义信任配置的步骤：

步骤 1 单击**服务质量** > **QoS 高级模式** > **全局设置**。

步骤 2 设备为高级模式时，选择**信任模式**。如果将数据包 CoS 等级和 DSCP 标记映射至独立队列，信任模式将确定数据包所分配的队列：

- **CoS/802.1p** — 根据 VLAN 标记中的 VPT 字段或每端口的默认 CoS/802.1p 值（如果传入数据包中没有 VLAN 标记）将流量映射到队列，实际的 VPT 到队列映射可以在映射“CoS/802.1p 到队列”页面配置。

- **DSCP** — 将根据 IP 报头中的 DSCP 字段将所有 IP 流量映射到队列。实际的 DSCP 到队列映射可以在“DSCP 到队列”页面中配置。如果流量不是 IP 流量，系统会将其映射到尽力服务队列。
- **CoS/802.1p-DSCP** — 选择此项对非 IP 流量使用“信任 CoS”模式，对 IP 流量使用“信任 DSCP”模式。

步骤 3 在**默认模式状态**字段中为接口选择默认高级模式 QoS 信任模式（可信任或不可信任）。这可以在高级 QoS 上提供基本 QoS 功能，因此默认情况下（无需创建策略），您可以在高级 QoS 上信任 CoS/DSCP。

在 **QoS 高级模式**中，“默认模式状态”设置为“不信任”时，接口上配置的默认 CoS 值会被忽略并且所有流量都会加入队列 1。有关详情，请参阅“服务质量”>“QoS 高级模式”>“全局设置”页面。

如果接口上已存在策略，则默认模式无效，系统将按照策略配置采取操作，并将丢弃不匹配的流量。

步骤 4 选择**覆盖入口 DSCP**，以根据“DSCP 覆盖表”，使用新值取代传入数据包中的原始 DSCP 值。启用“覆盖入口 DSCP”后，设备会对出口排队使用新的 DSCP 值。还会使用新的 DSCP 值取代数据包中的原始 DSCP 值。

注 系统将使用新的（改写后的）DSCP 值而非原始 DSCP 值将帧映射到出口队列。

步骤 5 如果启用了**覆盖入口 DSCP**，请单击 **DSCP 覆盖表**重新配置 DSCP。

DSCP 覆盖表

步骤 1 输入以下字段：

- **DSCP 传入** — 显示需要重新标记为替代值的传入数据包 DSCP 值。
- **DSCP 传出** — 选择“DSCP 传出”值以指示已映射传出值。

步骤 2 单击**应用**。

超出模板的 DSCP 重新标记

如果为类映射（数据流）指定了策略器，则可以指定当数据流中的流量超出 QoS 规定的限制时执行的操作。导致数据流超出其 QoS 限制的流量部分称为*超出模板的数据包*。

如果超限/违反时执行的操作为“超出模板的 DSCP”，设备会根据“超出模板的 DSCP 重新标记表”，使用新值重新映射超出模板的 IP 数据包的原始 DSCP 值。设备会使用新值为这些数据包指定资源和出口队列。设备还会使用新的 DSCP 值实际取代超出模板数据包中的原始 DSCP 值。

要使用“超出模板 DSCP”超出限制操作，请重新映射“超出模板的 DSCP 重新标记”中的 DSCP 值。否则操作将为空，因为在出厂默认设置下，该表格中的 DSCP 值会将数据包重新映射到其本身。

本功能将更改 DSCP 标记，以便在信任的 QoS 域之间交换传入流量。更改在一个域中使用的 DSCP 值，会将该类型的流量的优先级设置为在另一个域中使用的 DSCP 值，以标识同一类型的流量。

如果系统为 QoS 高级模式，这些设置便有效，并且一经激活，将作用于整个系统。

例如：假设存在以下三个服务级别：银级、金级和白金级，用于标记这三个等级的 DSCP 传入值分别为 10、20 和 30。如果将此流量转发给具有相同的三个服务级别，但使用的 DSCP 值为 16、24 和 48 的另一个服务提供商，则在将这些值映射到传出值时，**超出模板都 DSCP 重新标记**会更改这些值。

映射 DSCP 值的步骤：

步骤 1 单击**服务质量 > QoS 高级模式 > 超出模板的 DSCP 重新标记**。使用该页面可设置流入或留出设备的流量的 DSCP 值。

“DSCP 传入”会显示需要重新标记为替代值的传入数据包 DSCP 值。

步骤 2 选择要将传入值映射至的**传出 DSCP** 值。

步骤 3 单击**应用**。系统将使用新 DSCP 重新标记表更新当前配置文件。

步骤 4 单击**恢复默认设置**会恢复此接口的出厂 CoS 默认设置。

类映射

类映射使用在其上定义的 ACL（访问控制表）定义数据流。在类映射中可以包含 MAC ACL、IP ACL 和 IPv6 ACL 的组合。按照全部符合或皆符合的原则配置类映射，以符合数据包标准。按照首个匹配原则（这表示系统将执行与第一个匹配的类映射关联的操作）将类映射与数据包进行匹配。与同一个类映射匹配的数据包将被视为属于同一个数据流。

注 定义类映射不会对 QoS 产生任何影响；这是一个过渡性步骤，作用是启用将在后续使用的类映射。

如果需要更复杂的规则集合，可以将多个类映射分组为一个超级组，该组称为策略（请参阅策略表一节）。

注 在相同的类映射中，MAC ACL 不能与拥有目标 IPv6 地址作为过滤条件的 IPv6 ACE 一起使用。

“类映射”页面会显示已定义类映射及组成每个类映射的 ACL 的列表。使用该页面可添加/删除类映射。

定义类映射的步骤：

步骤 1 单击**服务质量** > **QoS 高级模式** > **类映射**。

对于每个类映射，系统会显示其上定义的 ACL 以及它们之间的关系。最多有 3 个 ACL 可以与其**匹配**关系一同显示，可能是**和**或**或**的关系。这表示 ACL 之间的关系。这样，“类映射”就是这 3 个 ACL 用“和”或“或”组合的结果。

步骤 2 单击**添加**。

通过选择一个或两个 ACL 并指定类映射的名称来添加类映射。如果一个类映射包含两个 ACL，您可以指定帧必须与这两个 ACL 都匹配，或者必须与选择的一个或两个 ACL 匹配。

步骤 3 输入参数。

- **类映射名称** — 输入新类映射的名称。
- **匹配 ACL 类型** — 要被视为属于该类映射中定义的数据流，数据包必须符合的标准。选项如下：
  - *IP* — 数据包必须与类映射中任一基于 IP 的 ACL 匹配。
  - *MAC* — 数据包必须与类映射中任一基于 MAC 的 ACL 匹配。
  - *IP 和 MAC* — 数据包必须与类映射中基于 IP 的 ACL 和基于 MAC 的 ACL 匹配。
  - *IP 或 MAC* — 数据包必须与类映射中基于 IP 的 ACL 或基于 MAC 的 ACL 匹配。
- **IP** — 为类映射选择基于 IPv4 的 ACL 或基于 IPv6 的 ACL。
- **MAC** — 为类映射选择基于 MAC 的 ACL。
- **偏好的 ACL** — 选择先将数据包与基于 IP 的 ACL 还是与基于 MAC 的 ACL 进行比对。

步骤 4 单击**应用**。将更新当前配置文件。

集合策略器

您可以测量符合一组预定义规则的流量的速率，及强制执行限制，例如限制端口上允许的文件传输流量的速率。

这可以通过在类映射中使用 ACL 以匹配所需的流量，以及使用策略器对匹配的流量应用 QoS 来实现。

策略器通过 QoS 规格进行配置。存在两种类型的策略器：

- **单（常规）策略器** — 单策略器会将 QoS 应用到单个类映射，以及基于策略器的 QoS 规格的单个数据流。将使用单策略器的类映射绑定至多个端口时，每个端口都具有其自己的单策略器实例；每个实例在相互独立的端口处对该类映射（数据流）应用 QoS。单策略器在“策略表”页面中创建。
- **集合策略器** — 集合策略器可将 QoS 应用到一个或多个类映射，从而应用到一个或多个数据流。集合策略器可以支持来自不同策略的类映射。不论策略和端口为何，集合策略器均会将 QoS 应用到其在集合中的所有数据流。集合策略器在“集合策略器”页面中创建。

  如果要与多个类共享策略器，请定义集合策略器。无法与另一设备中的其他策略器共享端口上的策略器。

每个策略器均使用其自己的 QoS 规则，通过以下参数的组合进行定义：

- 所允许的最大速率，称为承诺信息速率 (CIR)，以 Kbps 计。
- 以字节表示的流量，称为承诺的最大突发流量 (CBS)。这是允许作为临时突发数据传输的流量，即便其超出了所定义的最大速率也会照常传输。
- 将对超出限制的帧（称为超出模板的流量）应用的操作，可以如常传输或放弃这些帧，或者传输帧，但将它们重新映射到新的 DSCP 值，该值将使这些帧成为对于设备内的所有后续处理而言优先级更低的帧。
- 根据指定速率和可选操作配置流量管制。输入 CIR 和这些可选的值与操作。

将类映射添加到策略的同时会为该类映射指定策略器。如果策略器为集合策略器，则必须使用“集合策略器”页面进行创建。

定义集合策略器的步骤：

步骤 1 单击**服务质量** > **QoS 高级模式** > **集合策略器**。

此页面显示现有的集合策略器。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **集合策略器名称** — 输入集合策略器的名称。
- **入口承诺的信息传输速率 (CIR)** — 以位/秒为单位输入所允许的最大带宽。请参阅带宽页面中的相关说明。
- **入口承诺突发数据大小 (CBS)** — 以字节为单位输入最大突发数据量（即使其超出 CIR）。请参阅带宽页面中的相关说明。
- **超出操作** — 选择要对超出 CIR 的传入数据包执行的操作。可能的值包括：
  - *丢弃* — 丢弃超出已定义的 CIR 值的数据包。
  - *超出模板 DSCP* — 根据“超出模板的 DSCP 重新标记表”，将超出已定义的 CIR 值的数据包的 DSCP 值重新映射到新的值。

步骤 4 单击**应用**。将更新当前配置文件。

策略表

“策略表映射”页面会显示系统中已定义的高级 QoS 策略列表。通过该页面，还可以创建和删除策略。只有绑定到接口的策略才有效（请参阅“策略绑定”页面）。

每个策略由以下项目组成：

- 一个或多个 ACL（在策略中定义数据流）类映射。
- 一个或多个集合，其将 QoS 应用到策略中的数据流。

添加策略后，可以使用“策略表”页面添加类映射。

添加 QoS 策略的步骤：

步骤 1 单击**服务质量** > **QoS 高级模式** > **策略表**。

此页面会显示已定义的策略列表。

步骤 2 单击**策略类映射表**显示“策略类映射”页面。
-或者
单击**添加**打开“添加策略表”页面。

步骤 3 在**新策略名称**字段中输入新策略的名称。

步骤 4 单击**应用**。系统将添加 QoS 策略模板，并更新当前配置文件。

策略类映射

可以在一个策略中添加一个或多个类映射。类映射定义被视为属于同一个数据流的数据包的类型。

在策略中添加类映射的步骤：

步骤 1 单击**服务质量** > **QoS 高级模式** > **策略类映射**。

步骤 2 在过滤中选择一个策略，然后单击**转至**。此时将显示该策略中的所有类映射。

步骤 3 要添加新的类映射，请单击**添加**。

步骤 4 输入参数。

- **策略名称** — 显示要在其中添加类映射的策略。
- **类映射名称** — 选择要与该策略关联的现有类映射。类映射在“类映射”页面中创建。
- **操作类型** — 根据所有匹配数据包的入口 CoS/802.1p 和/或 DSCP 值选择操作。
  - *使用默认信任模式* — 如果选择此选项，系统将在全局信任模式中使用默认模式状态。如果默认模式状态为“不信任”，则入口 CoS/802.1p 和/或 DSCP 值会被忽略，匹配数据包将按尽力服务模式发送。
  - *始终信任* — 如果选择此选项，设备会根据全局信任模式（在**全局设置**页面选择）信任匹配的数据包。设备会忽略默认模式状态（在**全局设置**页面中选择）。
  - *设置* — 如果选择了该选项，将使用在**新值**框中输入的值来确定匹配数据包的出口队列，具体如下：

    如果新值 (0..7) 为 CoS/802.1p 优先级，请使用该优先级值和“CoS/802.1p 到队列表”来确定所有匹配数据包的出口队列。

    如果新值 (0..63) 为 DSCP，请使用该新的 DSCP 和“DSCP 到队列表”来确定匹配的 IP 数据包的出口队列。

    否则，请使用新值 (1..8) 作为所有匹配数据包的出口队列号。
- **策略类型** — 为策略选择策略器类型。选项如下：
  - *无* — 不使用任何策略。
  - *单个* — 策略策略器为单策略器。
  - *集合* — 策略策略器为集合策略器。

步骤 5 如果**策略类型**为*集合*，请选择**集合策略器**。

步骤 6 如果**监察类型**为*单个*，请输入以下 QoS 参数：

- **入口承诺的信息传输速率 (CIR)** — 以 Kbps 为单位输入 CIR。请参阅“带宽”页面中的相关说明。
- **入口承诺突发数据大小 (CBS)** — 以字节为单位输入 CBS。请参阅“带宽”页面中的相关说明。
- **超出操作** — 选择要对超出 CIR 的传入数据包执行的操作。选项如下：
  - *丢弃* — 丢弃超出已定义的 CIR 值的数据包。
  - *超出模板的 DSCP* — 使用从“超出模板的 DSCP 重新标记表”中取得的新 DSCP，转发超出已定义的 CIR 的 IP 数据包。

步骤 7 单击**应用**。

策略绑定

“策略绑定”页面显示绑定的策略模板及绑定到的端口。可将策略绑定到接口作为入口（输入）策略或出口（输出）策略。如果将策略模板绑定到特定端口，则该策略仅在该端口有效。一个端口只能配置一个策略简档，但一个策略可以绑定至多个端口。

将策略绑定至端口后，该策略会过滤属于策略中定义的数据流的流量，并向其应用 QoS。

要编辑策略，必须先将其从所绑定的端口删除（解除绑定）。

注 可以将端口与策略绑定，也可以与 ACL 绑定，但不能同时都绑定。

定义策略绑定的步骤：

步骤 1 单击**服务质量** > **QoS 高级模式** > **策略绑定**。

步骤 2 如果需要，请选择**接口类型**。

步骤 3 单击**转至**。显示该接口的策略。

步骤 4 单击**编辑**。

步骤 5 为输入策略/接口选择以下选项：

- **输入策略绑定** — 选择该选项可以将输入策略绑定到接口。
- **策略名称** — 选择绑定的输入策略。

- **默认操作** — 选择数据包与策略匹配时的操作：
  - *拒绝任意* — 选择该选项可在接口上的数据包与任何策略匹配时转发这些数据包。
  - *允许任意* — 选择该选项可在接口上的数据包与任何策略不匹配时转发这些数据包。

  注 仅当接口上未激活“IP 源防护”时，才能定义“允许任意”。

步骤 6 为输出策略/接口选择以下选项：

- **输出策略绑定** — 选择该选项可以将输出策略绑定到接口。
- **策略名称** — 选择已绑定的输出策略。
- **默认操作** — 选择数据包与策略匹配时的操作：
  - *拒绝任意* — 选择该选项可在接口上的数据包与任何策略匹配时转发这些数据包。
  - *允许任意* — 选择该选项可在接口上的数据包与任何策略不匹配时转发这些数据包。

  注 仅当接口上未激活“IP 源防护”时，才能定义“允许任意”。

步骤 7 单击**应用**。系统将定义 QoS 策略绑定，并更新当前配置文件。

QoS 统计信息

您可以从这些页面管理单策略器和集合策略器，并可查看队列统计信息。

策略器统计信息

单策略器通过单个策略绑定到单个类映射。集合策略器通过一个或多个策略绑定到一个或多个类映射。

查看单策略器统计信息

“单个策略器统计信息”页面表示符合策略类映射中定义的条件的接口接收到的预约带宽内和超出模板的数据包的数量。

注 如果设备在第 3 层模式下，将不会显示该页面。

查看策略器统计信息的步骤：

步骤 1 单击**服务质量** > **QoS 统计信息** > **单策略器 统计信息**。

此页面显示了以下字段：

- **接口** — 显示此接口的统计信息。
- **策略** — 显示此策略的统计信息。
- **类映射** — 显示此类映射的统计信息。
- **模板内的字节数** — 接收到的模板内的字节数。
- **模板外的字节数** — 接收到的超出模板的字节数。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **接口** — 选择为其累积统计信息的接口。
- **策略名称** — 选择策略名称。
- **类映射名称** — 选择类名称。

步骤 4 单击**应用**。将创建一个新的统计信息请求，并更新当前配置文件。

查看汇总监察器统计信息

查看集合策略器统计信息的步骤：

步骤 1 单击**服务质量** > **QoS 统计信息** > **集合策略器统计信息**。

此页面显示了以下字段：

- **集合策略器名称** — 要查看其统计信息的策略器。
- **简档内的字节数** — 接收到的简档内的数据包数量。
- **简档外的字节数** — 接收到的简档外的数据包数量。

步骤 2 单击**添加**。

步骤 3 选择一个**集合策略器名称**（先前创建的集合策略器之一，系统会为其显示统计信息）。

步骤 4 单击**应用**。将创建一个新的统计信息请求，并更新当前配置文件。

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。

查看队列统计信息并定义要显示的统计信息（计数器集）的步骤：

步骤 1 单击**服务质量** > **QoS 统计信息** > **队列统计信息**。

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。

要查看特定单位和接口，请在过滤器中选择单位/接口，然后单击**转至**。

要查看特定接口，请在过滤器中接口，然后单击**转至**。

“队列统计信息表”针对每个队列显示以下字段：

- **队列** — 从此队列转发的数据包或丢弃的尾部数据包。
- **已传输数据包** — 已传输的数据包数。
- **丢弃的尾部数据包** — 被丢弃的尾部数据包所占的百分比。
- **已传输字节** — 已传输的字节数。
- **丢弃的尾部字节** — 被丢弃的尾部字节所占的百分比。

24

SNMP

本节介绍简单网络管理协议 (SNMP) 功能，该功能提供了一种管理网络设备的方法。

其中包含以下主题：

- 概述
- 引擎 ID
- 视图
- 组
- 用户
- 社区
- 陷阱设置
- 通知接收设备
- 通知过滤器

概述

SNMP 版本和工作流程

设备可作为 SNMP 代理，并且支持 SNMPv1、v2 和 v3。交换机还会使用支持的 MIB（管理信息库）中定义的陷阱，将系统事件报告给陷阱接收器。

SNMPv1 和 v2

为控制对系统的访问，系统中会定义一个社区条目列表。每个社区条目由一个*社区字符串*及其访问权限组成。系统仅会对指定具有恰当权限和正确操作的社区的 SNMP 消息作出响应。

SNMP 代理会维护用于管理设备的变量列表。这些变量在*管理信息库* (MIB) 中定义。

注 由于其他版本具有安全漏洞，因此建议使用 SNMPv3。

SNMPv3

除具备 SNMPv1 和 v2 提供的功能外，SNMPv3 还可将访问控制和新的陷阱机制应用到 SNMPv1 和 SNMPv2 PDU。SNMPv3 还可定义用户安全模式 (USM)，该模式包括：

- **验证** — 提供数据完整性和数据源验证。
- **隐私** — 防止消息内容泄露。使用*密码块链接* (CBC-DES) 技术进行加密。可以只对 SNMP 消息启用验证功能，也可以一并启用验证和保密功能。但无法在不启用验证功能的情况下单独启用保密功能。
- **时效性** — 防止消息延迟或反演攻击。SNMP 代理会将传入消息的时间戳与消息的到达时间进行比较。

SNMP 工作流程

注 出于安全方面的考虑，默认情况下应禁用 SNMP。在可以通过 SNMP 管理设备之前，必须在 TCP/UDP 服务页面上启用 SNMP。

建议使用下面的一系列操作来配置 SNMP：

如果决定使用 SNMPv1 或 v2，请执行以下操作：

步骤 1 导航至社区页面，单击**添加**。可以将该社区与访问权限和视图相关联（在基本模式下），也可以将其与组相关联（在高级模式下）。有两种方式可以定义社区的访问权限：

- **基本模式** — 可以将社区的访问权限配置为“只读”、“读写”或“SNMP 管理”。此外，还可以将社区的访问权限限制为只能通过视图访问特定的 MIB 对象。视图在视图页面中定义。
- **高级模式** — 社区的访问权限由组定义（在组页面中定义）。可以使用特定的安全模式来配置组。组的访问权限为“读取”、“写入”和“通知”。

步骤 2 选择是将 SNMP 管理工作站限制在一个地址，还是允许来自所有地址的 SNMP 管理。如果选择将 SNMP 管理限制在一个地址，则在“IP 地址”字段中输入 SNMP 管理 PC 的地址。

步骤 3 在“社区字符串”字段中输入唯一的社区字符串。

步骤 4 使用陷阱设置页面启用陷阱（可选）。

步骤 5 使用通知过滤器页面定义通知过滤器（可选）。

步骤 6 在 SNMPv1.2 通知接收设备页面上配置通知接收设备。

如果决定使用 SNMPv3，请执行以下操作：

步骤 1 使用引擎 ID 页面定义 SNMP 引擎。创建唯一引擎 ID 或使用默认引擎 ID。应用引擎 ID 配置会清除 SNMP 数据库。

步骤 2 使用视图页面定义 SNMP 视图（可选）。这会限制社区或组可用的 OID 范围。

步骤 3 使用组页面定义组。

步骤 4 使用用户页面定义用户，可以在该页面中将用户与组相关联。如果未设置 SNMP 引擎 ID，那么将无法创建用户。

步骤 5 使用陷阱设置页面启用或禁用陷阱（可选）。

步骤 6 使用通知过滤器页面定义通知过滤器（可选）。

步骤 7 使用 SNMPv3 通知接收设备页面定义通知接收设备。

支持的 MIB

如需支持的 MIB 列表，请访问以下 URL，并导航到名为**思科 MIBS** 的下载区域：

www.cisco.com/cisco/software/navigator.html

型号 OID

以下是适用于 250 系列的 OID。

SKU 名称	说明	系统对象 ID
F250-24	SF250-24 24 端口 10/100 智能交换机	9.6.1.98.24.1
SF250-24P	SF250-24P 24 端口 10/100 PoE 智能交换机	9.6.1.98.24.5
SF250-48	SF250-48 48 端口 10/100 智能交换机	9.6.1.98.24.1
SF250-48HP	SF250-48HP 48 端口 10/100 PoE 智能交换机	9.6.1.98.24.4

SKU 名称	说明	系统对象 ID
SG250-08	SG250-08 8 端口千兆智能交换机	9.6.1.97.8.3
SG250-08HP	SG250-08HP 8 端口千兆 PoE 智能交换机	9.6.1.97.8.4S
SG250-10P	SG250-10P 10 端口千兆 PoE 智能交换机	9.6.1.97.10.5
SG250-18	SG250-18 18 端口千兆智能交换机	9.6.1.97.18.1
SG250-26	SG250-26 26 端口千兆智能交换机	9.6.1.97.26.1
SG250-26HP	SG250-26HP 26 端口千兆 PoE 智能交换机	9.6.1.97.26.4
SG250-26P	SG250-26P 26 端口千兆 PoE 智能交换机	9.6.1.97.26.5
SG250-50	SG250-50 50 端口千兆智能交换机	9.6.1.97.50.1
SG250-50HP	SG250-50HP 50 端口千兆 PoE 智能交换机	9.6.1.97.50.4
SG250-50P	SG250-50P 50 端口千兆 PoE 智能交换机	9.6.1.97.50.5
SG250X-24	SG250X-24 24 端口千兆 + 4 端口万兆智能交换机	9.6.1.99.24.1
SG250X-24P	SG250X-24P 24 端口千兆 PoE + 4 端口万兆智能交换机	9.6.1.99.24.5
SG250X-48	SG250X-48 48 端口千兆 + 4 端口万兆智能交换机	9.6.1.99.48.1
SG250X-48P	SG250X-48P 48 端口千兆 PoE + 4 端口万兆智能交换机	9.6.1.99.48.5

专用对象 ID 被置于 enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1).switch001(101) 下面。

引擎 ID

引擎 ID 由 SNMPv3 实体用来唯一标识其自身。SNMP 代理被视为权威 SNMP 引擎。这表示该代理会响应传入消息（Get、GetNext、GetBulk、Set），并将陷阱消息发送给管理器。该代理的本地信息会封装在消息的字段中。

每个 SNMP 代理都会保留 SNMPv3 消息交换中使用的本地信息。默认的 SNMP 引擎 ID 由企业编号和默认 MAC 地址组成。引擎 ID 对于管理域必须唯一，以便在一个网络中不会出现拥有相同引擎 ID 的两个设备。

本地信息存储在以下只读 MIB 变量中（snmpEngineId、snmpEngineBoots、snmpEngineTime 和 snmpEngineMaxMessageSize）。

注意 如果引擎 ID 发生更改，系统将会删除所有已配置的用户和组。

定义 SNMP 引擎 ID 的步骤：

步骤 1 单击 **SNMP** > **引擎 ID**。

步骤 2 选择用于**本地引擎 ID** 的选项。

- **使用默认设置** — 选择该选项将使用设备生成的引擎 ID。默认的引擎 ID 以设备 MAC 地址为基础，并且根据标准进行定义，具体如下：
  - *前 4 个八位字节* — 第一位 = 1，其余为 IANA 企业编号。
  - *第五个八位字节* — 设置为 3 以表示随后的 MAC 地址。
  - *后 6 个八位字节* — 设备的 MAC 地址。
- **无** — 不使用引擎 ID。
- **用户定义** — 输入本地设备引擎 ID。该字段值是一个十六进制字符串（**范围为：10 - 64**）。该十六进制字符串中的每个字节都由两个十六进制数字表示。

所有远程引擎 ID 及其 IP 地址均显示在远程引擎 ID 表中。

步骤 3 单击**应用**。将更新当前配置文件。

远程引擎 ID 表显示引擎的 IP 地址与引擎 ID 之间的映射。

添加引擎 ID 的 IP 地址的步骤：

步骤 4 单击**添加**。输入以下字段：

- **服务器定义** — 选择是按照 IP 地址还是名称来指定引擎 ID 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”）。
- **服务器 IP 地址/名称** — 输入日志服务器的 IP 地址或域名。
- **引擎 ID** — 输入引擎 ID。

步骤 5 单击**应用**。将更新当前配置文件。

视图

视图是 MIB 子树集合的用户定义标签。每个子树 ID 均由相应子树根节点的*对象 ID* (OID) 定义。可以使用熟悉的名称来指定所需子树的根，也可以输入 OID（请参阅型号 OID）。

每个子树要么包括在所定义的视图中，要么被排除在该视图之外。

使用“视图”页面可创建和编辑 SNMP 视图。默认视图（“默认”、“DefaultSuper”）无法更改。

可以在组页面中将视图绑定到组，或通过社区页面将视图绑定到使用基本访问模式的社区。

定义 SNMP 视图的步骤：

步骤 1 单击 **SNMP** > **视图**。

将为每个视图显示以下字段：

- **对象 ID 子树** — MIB 树中包括在所选 SNMP 视图中或被排除在该视图之外的节点。
- **对象 ID 子树视图** — 节点是包含在内还是排除在外。

步骤 2 单击**添加**定义新视图。

步骤 3 输入参数。

- **视图名称** — 输入视图名称（长度为 0 到 30 个字符）。
- **对象 ID 子树** — 选择 MIB 树中包括在所选 SNMP 视图中或被排除在该视图之外的节点。用于选择对象的选项如下：

- *从列表中选择* — 使用该选项可以导航 MIB 树。按*向上*箭头可前往所选节点的父节点层或兄弟节点层；按*向下*箭头可进入所选节点的子节点层。单击视图中的节点可从一个节点到达其兄弟节点。使用滚动条可在视图中显示兄弟节点。
- *用户定义* — 输入*从列表中选择*选项中未提供的 OID（如果需要）。

步骤 4 选择或取消选择**包含在视图中。**如果选择了此项，会将选定的 MIB 包含在视图中，否则不会包含这些 MIB。

步骤 5 单击**应用**。

步骤 6 要验证您的视图配置，请从**过滤器：视图名称**列表中选择用户定义的视图。默认情况下，存在以下视图：

- **默认** — 可读和可读写视图的默认 SNMP 视图。
- **DefaultSuper** — 管理员视图的默认 SNMP 视图。

组

在 SNMPv1 和 SNMPv2 中，社区字符串会随 SNMP 帧一起发送。社区字符串将作为访问 SNMP 代理的密码。但是，帧和社区字符串均未加密。因此 SNMPv1 和 SNMPv2 不安全。

在 SNMPv3 中，可配置以下安全机制。

- **验证** — 设备会检查 SNMP 用户是否是获授权的系统管理员。该验证会针对每个帧进行。
- **隐私** — SNMP 帧可以传输加密数据。

因此，在 SNMPv3 中，存在以下三个安全等级：

- 无安全验证（不验证且无隐私）
- 验证（验证且无隐私）
- 验证和隐私

SNMPv3 提供了一种方式来控制每个用户能够读取或写入的内容，以及他们会收到的通知。组将定义读/写权限和安全等级。与 SNMP 用户或社区关联时便可运行。

注 要将非定义视图关联至组，请先在视图页面中创建一个视图。

创建 SNMP 组的步骤：

步骤 1 单击 **SNMP** > **组**。

此页面包含现有的 SNMP 组及其安全等级。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **组名称** — 输入新的组名称。
- **安全模式** — 选择要应用到该组的 SNMP 版本（SNMPv1、v2 或 v3）。

可以定义三种类型的具有多种安全等级的视图。对于每种安全等级，可通过输入以下字段针对“读取”、“写入”和“通知”权限选择视图：

- **启用** — 选择此字段可启用“安全等级”。
- **安全等级** — 定义要应用到该组的安全等级。SNMPv1 和 SNMPv2 不支持“验证”和“隐私”。如果选择了 SNMPv3，则选择以下选项之一：
  - *不验证且无隐私* —既不为组指定“验证”安全等级，也不为其指定“隐私”安全等级。
  - *验证且无隐私* — 验证 SNMP 消息，并确保 SNMP 消息源经过验证，但不对消息加密。
  - *验证和隐私* — 验证 SNMP 消息并对它们加密。
- **视图** — 选择将视图与组的访问权限（读取、写入和/或通知）相关联可将 MIB 树的范围限制在组具有访问权限（读取、写入和通知）的范围内。
  - *读取* — 所选视图的管理访问权限为只读。否则，与该组关联的用户或社区将能够读取除控制 SNMP 本身的 MIB 之外的所有 MIB。
  - *写入* — 所选视图的管理访问权限为可写。否则，与该组关联的用户或社区将能够写入除控制 SNMP 本身的 MIB 之外的所有 MIB。
  - *通知* — 将陷阱可用的内容限制在选定视图包含的范围内。否则，将不对陷阱内容进行限制。只能针对 SNMPv3 选择该选项。

步骤 4 单击**应用**。SNMP 组将保存至当前配置文件中。

用户

SNMP 用户由登录凭证（用户名、密码和验证方法），及其工作（通过与组和引擎 ID 关联实现）的环境和范围定义。

经过配置的用户具有其组的属性，并具有在关联的视图中配置的访问权限。

网络管理员可使用组将访问权限分配给整组用户而非单个用户。

一个用户只能属于一个组。

要创建 SNMPv3 用户，必须先满足以下条件：

- 事先在设备上配置一个引擎 ID。这是在引擎 ID 页面中进行的。
- 必须有一个可用的 SNMPv3 组。可在组页面中定义 SNMPv3 组。

显示 SNMP 用户和定义新用户的步骤：

步骤 1 单击 **SNMP** > **用户**。

此页面会显示现有用户。除以下字段外，此页面中的相关字段会在“添加”页面介绍：

- **IP 地址** — 显示引擎的 IP 地址。

步骤 2 单击**添加**。

此页面将提供有关将 SNMP 访问控制权限指定给 SNMP 用户的信息。

步骤 3 输入参数。

- **用户名** — 为该用户输入名称。
- **引擎 ID** — 选择该用户要连接的本地或远程 SNMP 实体。更改或删除本地 SNMP 引擎 ID 会删除 SNMPv3 用户数据库。要想一并接收通知消息和请求信息，必须定义本地和远程两种用户。
  - *本地* — 该用户将连接到本地设备。
  - *远程 IP 地址* — 用户除本地设备之外，还将连接其他 SNMP 实体。如果定义了远程引擎 ID，则远程设备可以接收通知消息，但无法请求信息。

    输入远程引擎 ID。
- **组名称** — 选择该 SNMP 用户所属的 SNMP 组。SNMP 组在“添加组”页面中定义。

  注 属于已删除的组的用户仍会保留，但会处于非活动状态。

- **验证方法** — 选择会根据分配的组名称而变化的验证方法。如果组不需要验证，则用户无法配置任何验证。选项如下：
  - *无* — 不使用用户验证。
  - *MD5* — 通过 MD5 验证方法生成密钥所使用的密码。
  - *SHA* — 通过 SHA（安全散列算法）验证方法生成密钥所使用的密码。
- **验证密码** — 如果通过 MD5 或 SHA 密码实施验证，请在**加密**或**明文**模式下输入本地用户密码。系统会将本地用户密码与本地数据库进行比较，本地用户密码最多可以包含 32 个 ASCII 字符。
- **隐私方法** — 选择以下选项之一：
  - *无* — 未加密私有密码。
  - *DES* — 根据数据加密标准 (DES) 加密私有密码。
- **私有密码** — 如果选择了 DES 隐私方法，则需要 16 个字节（DES 加密密钥）。此字段的长度必须是 32 个十六进制字符。可以选择**加密**或**明文**模式。

步骤 4 单击**应用**保存设置。

社区

SNMPv1 和 SNMPv2 中的访问权限通过在“社区”页面中定义社区进行管理。社区名称是在 SNMP 管理工作站和设备之间共享的一种密码。该名称用于验证 SNMP 管理工作站。

由于 SNMPv3 面向用户而非社区，因此社区只能在 SNMPv1 和 v2 中定义。用户属于具有访问权限的组。

通过“社区”页面可以将社区与访问权限相关联，可以直接关联（基本模式），也可以通过组进行关联（高级模式）。

- **基本模式** — 可以将社区的访问权限配置为“只读”、“读写”或“SNMP 管理”。此外，还可以将社区的访问权限限制为只能通过视图访问特定的 MIB 对象。视图在视图页面中定义。
- **高级模式** — 社区的访问权限由组定义（在组页面中定义）。可以使用特定的安全模式来配置组。组的访问权限为“读取”、“写入”和“通知”。

定义 SNMP 社区的步骤：

步骤 1 单击 **SNMP** > **社区**。

此页面包含记录已配置的 SNMP 社区及其属性的表格。除以下字段外，此页面中的相关字段会在“添加”页面介绍：

- **社区类型** — 显示社区的模式（**基本**或**安全**）。

步骤 2 单击**添加**。

使用此页面，网络管理员可以定义和配置新的 SNMP 社区。

步骤 3 **SNMP 管理工作站** — 单击**用户定义**，输入可以访问 SNMP 社区的管理工作站 IP 地址。单击**全部**，表示任何 IP 设备均可以访问该 SNMP 社区。

- **IP 版本** — 选择 IPv4 或 IPv6。
- **IPv6 地址类型** — 选择支持的 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 VLAN 还是 ISATAP 接收。
- **IP 地址** — 输入 SNMP 管理工作站 IP 地址。
- **社区字符串** — 输入用于验证设备管理工作站的社区名称。
- **（社区类型）基本** — 在此社区类型中，没有到任何组的连接。您可以只选择社区访问级别（“只读”、“读写”或“管理”），也可以进一步授予社区对特定视图的访问权限。默认情况下，该模式会应用到整个 MIB。如果选择该模式，请为以下字段输入值：
  - *访问模式* — 选择社区的访问权限。选项如下：

    只读 — 将管理访问权限限制为只读。不能更改社区。

    读写 — 管理访问权限为可读写。可以对设备配置进行更改，但不能更改社区。

    SNMP 管理 — 用户具有所有设备配置选项的访问权限，以及修改社区的权限。对于除 SNMP MIB 之外的所有 MIB，“SNMP 管理”等同于“读写”。要访问 SNMP MIB，需要具有“SNMP 管理”权限。
  - *视图名称* — 选择 SNMP 视图（要授予对其的访问权限的 MIB 子树集合）。

- **（社区类型）高级** — 为选定的社区选择 此类型。
  - *组名称* — 选择确定访问权限的 SNMP 组。

步骤 4 单击**应用**。系统将定义 SNMP 社区，并更新当前配置文件。

陷阱设置

使用“陷阱设置”页面可配置是否从设备发送 SNMP 通知，以及在哪些情况下发送通知。可以在 SNMPv1.2 通知接收设备页面或 SNMPv3 通知接收设备页面中配置 SNMP 通知的介绍设备。

定义陷阱设置的步骤：

步骤 1 单击 **SNMP** > **陷阱设置**。

步骤 2 对 **SNMP 通知**选择**启用**，将指定设备可以发送 SNMP 通知。

步骤 3 对**验证通知**选择**启用** 将启用 SNMP 验证失败通知。

步骤 4 单击**应用**。SNMP 陷阱设置将写入当前配置文件。

通知接收设备

系统会生成陷阱消息来报告系统事件（如 RFC 1215 中所定义）系统可以生成在支持的 MIB 中定义的陷阱。

陷阱接收器（通知接收设备）是设备将陷阱消息发送到的网络节点。您可以定义通知接收设备列表。

陷阱接收器条目中包含的节点 IP 地址和 SNMP 凭证与陷阱消息中包括的节点 IP 地址和 SNMP 凭证相对应。当发生要求发送陷阱消息的事件时，系统会将陷阱消息发送到通知接收设备表上所列的每个节点。

使用 SNMPv1.2 通知接收设备页面和 SNMPv3 通知接收设备页面可配置 SNMP 通知的接收设备，以及向每个接收设备发送的 SNMP 通知的类型（陷阱或通知）。使用“添加/编辑”弹出式窗口可配置通知的属性。

SNMP 通知是设备向 SNMP 管理工作站发送的消息，在其中说明发生了某个事件，例如链路连接/中断。

您还可以过滤特定通知，这可以通过在通知过滤器页面中创建过滤器并将其应用到 SNMP 通知接收设备来实现。使用通知过滤器，可以根据将要发送的通知的 OID，过滤发送到管理工作站的 SNMP 通知的类型。

SNMPv1.2 通知接收设备

定义 SNMPv1，2 中的接收设备的步骤：

步骤 1 单击 **SNMP** > **通知接收设备 SNMPv1,2**。

此页面会显示 SNMPv1，2 的接收设备。

步骤 2 输入以下字段：

- **通知 IPv4 源接口** — 选择其 IPv4 地址将用作与 IPv4 SNMP 服务器通信中通知消息的源 IPv4 地址的源接口。
- **陷阱 IPv4 源接口** — 选择其 IPv6 地址将用作与 IPv6 SNMP 服务器通信中陷阱消息的源 IPv6 地址的源接口。
- **通知 IPv6 源接口** — 选择其 IPv4 地址将用作与 IPv4 SNMP 服务器通信中通知消息的源 IPv4 地址的源接口。
- **陷阱 IPv6 源接口** — 选择其 IPv6 地址将用作与 IPv6 SNMP 服务器通信中陷阱消息的源 IPv6 地址的源接口。

  注 如果已选择“自动”选项，系统将使用传出接口上定义的 IP 地址的源 IP 地址。

步骤 3 单击**添加**。

步骤 4 输入参数。

- **服务器定义** — 选择是按照 IP 地址还是名称来指定远程日志服务器。
- **IP 版本** — 选择 IPv4 或 IPv6。
- **IPv6 地址类型** — 选择*链路本地*或*全局*。
  - *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 VLAN 还是 ISATAP 接收。
- **接收方 IP 地址/名称** — 输入接收陷阱的 IP 地址或服务器名称。
- **UDP 端口** — 输入接收设备上用于接收通知的 UDP 端口。
- **通知类型** — 选择发送陷阱还是发送通知。如果需要发送两种类型的通知，则必须创建两个接收设备。
- **超时** — 输入重新发送通知之前，设备等待的时间（以秒为单位）。
- **重试次数** — 输入设备重新发送通知请求的次数。
- **社区字符串** — 从下拉列表中选择陷阱管理器的社区字符串。社区字符串名称从社区页面中所列出的内容中产生。
- **通知版本** — 选择陷阱 SNMP 版本。
  SNMPv1 和 SNMPv2 均可作为陷阱版本使用，但一次只能启用一个版本。
- **通知过滤器** — 选择该选项，将可以过滤发送到管理工作站的 SNMP 通知类型。过滤器在通知过滤器页面中创建。
- **过滤器名称** — 选择定义陷阱中包含的信息的 SNMP 过滤器（在通知过滤器页面中定义）。

步骤 5 单击**应用**。SNMP 通知接收设备设置将写入当前配置文件。

SNMPv3 通知接收设备

定义 SNMPv3 中的接收设备的步骤：

步骤 1 单击 **SNMP** > **通知接收设备 SNMPv3**。

此页面会显示 SNMPv3 的接收设备。

- **通知 IPv4 源接口** — 选择其 IPv4 地址将用作与 IPv4 SNMP 服务器通信中通知消息的源 IPv4 地址的源接口。
- **陷阱 IPv4 源接口** — 选择其 IPv6 地址将用作与 IPv6 SNMP 服务器通信中陷阱消息的源 IPv6 地址的源接口。

- **通知 IPv6 源接口** — 选择其 IPv4 地址将用作与 IPv4 SNMP 服务器通信中通知消息的源 IPv4 地址的源接口。
- **陷阱 IPv6 源接口** — 选择其 IPv6 地址将用作与 IPv6 SNMP 服务器通信中陷阱消息的源 IPv6 地址的源接口。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **服务器定义** — 选择是按照 IP 地址还是名称来指定远程日志服务器。
- **IP 版本** — 选择 IPv4 或 IPv6。
- **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”）。
- **接收方 IP 地址/名称** — 输入接收陷阱的 IP 地址或服务器名称。
- **UDP 端口** — 输入接收设备上用于接收通知的 UDP 端口。
- **通知类型** — 选择发送陷阱还是发送通知。如果需要发送两种类型的通知，则必须创建两个接收设备。
- **超时** — 输入重新发送通知/陷阱之前，设备等待的时间（以秒为单位）。超时范围：取值范围 1 到 300，默认值 15。
- **重试次数** — 输入设备重新发送通知请求的次数。重试次数: 取值范围 1 到 255，默认值：3
- **用户名** — 从下拉列表中选择接收 SNMP 通知的用户。要接收通知，必须已在用户页面中定义该用户，且其引擎 ID 必须为远程。
- **安全等级** — 选择将对数据包应用的验证。

  注 此处的“安全等级”取决于选定的“用户名”。如果将该“用户名”配置为“不验证”，那么“安全等级”仅为“不验证”。但是，如果在用户页面上将该“用户名”分配为“验证和隐私”，那么此页面上的安全等级可以为“不验证”、“仅验证”或“验证和隐私”。

选项如下：

- *不验证* — 表示既不对数据包进行验证，也不对其加密。
- *验证* — 表示对数据包进行验证，但不对其加密。
- *隐私* — 表示既要对数据包进行验证，又要对其加密。

- **通知过滤器** — 选择该选项，将可以过滤发送到管理工作站的 SNMP 通知类型。过滤器在通知过滤器页面中创建。
- **过滤器名称** — 选择定义陷阱中包含的信息的 SNMP 过滤器（在通知过滤器页面中定义）。

步骤 4 单击**应用**。SNMP 通知接收设备设置将写入当前配置文件。

通知过滤器

使用“通知过滤器”页面可配置 SNMP 通知过滤器和要检查的对象 ID (OID)。创建通知过滤器后，可在 SNMPv1.2 通知接收设备页面和 SNMPv3 通知接收设备页面中将其绑定到通知接收设备。

使用通知过滤器，可以根据要发送的通知的 OID，过滤发送到管理工作站的 SNMP 通知的类型。

定义通知过滤器的步骤：

步骤 1 单击 **SNMP** > **通知过滤器**。

“通知过滤器”页面包含针对每个过滤器的通知信息。该表格可以通过“过滤器名称”来过滤通知条目。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **过滤器名称** — 输入名称（长度为 0 到 30 个字符）。
- **对象 ID 子树** — 选择 MIB 树中包括在所选 SNMP 过滤器中或被排除在该过滤器之外的节点。用于选择对象的选项如下：

- *从列表中选择* — 使用该选项可以导航 MIB 树。按*向上*箭头可前往所选节点的父节点层或兄弟节点层；按*向下*箭头可进入所选节点的子节点层。单击视图中的节点可从一个节点到达其兄弟节点。使用滚动条可在视图中显示兄弟节点。
- 使用*对象 ID* 时，如果选择**包含在过滤器中**选项，则会将**输入的对象标识符**包含在视图中。

步骤 4 选择或取消选择**包含在过滤器中。**如果选择了此项，会将选定的 MIB 包含在过滤器中，否则不会包含这些 MIB。

步骤 5 单击**应用**。系统将定义 SNMP 视图，并更新当前配置文件。