



345139

管理指南

思科 500 系列可堆叠管理型交换机管理指南（版本 1.3.5）

目录

第 1 章：使用入门	1
启动基于 Web 的配置实用程序	1
设备配置快速入门	4
接口命名约定	5
500 设备之间的差异	5
窗口导航	6
第 2 章：状态和统计信息	9
系统摘要	9
查看以太网接口	9
查看 Etherlike 统计信息	11
查看 GVRP 统计信息	11
查看 802.1X EAP 统计信息	13
查看 TCAM 利用率	14
状况	14
管理 RMON	15
查看日志	21
第 3 章：管理：系统日志	22
设置系统日志设置	22
设置远程记录设置	24
查看内存日志	25
第 4 章：管理：文件管理	27
系统文件	27
升级 / 备份固件 / 语言	29

活动映像	33
下载 / 备份配置 / 日志	34
配置文件属性	38
复制 / 保存配置	39
通过 DHCP 进行自动配置	40

第 5 章：管理：堆栈管理 46

概述	46
堆叠中的单元类型	47
堆叠拓扑	49
单元 ID 分配	50
主装置选择流程	51
堆叠更改	52
堆叠中的单元故障	54
堆叠中的软件自动同步	55
堆叠单元模式	55
堆叠端口	59
默认配置	63
与其他功能进行交互	64
系统模式	64

第 6 章：管理 67

设备型号	68
系统设置	69
Console 设置（自动波特率支持）	72
管理接口	73
系统模式和堆栈管理	73
用户帐户	73
定义空闲会话超时	73
时间设置	74

系统日志	74
文件管理	74
重启设备	74
路由资源	76
健康状况	78
诊断	79
发现 - Bonjour	80
发现 - LLDP	80
发现 - CDP	80
Ping	80
Traceroute	81

第 7 章：管理：时间设置 **83**

系统时间选项	83
SNTP 模式	85
配置系统时间	85

第 8 章：管理：诊断 **94**

测试铜缆端口	94
显示光纤模块状态	96
配置端口和 VLAN 镜像	97
查看 CPU 使用率和安全的核心技术	99

第 9 章：管理：发现协议 **100**

Bonjour	100
LLDP 和 CDP	102
配置 LLDP	103
配置 CDP	120

第 10 章：端口管理	128
配置端口	128
设置端口配置	129
链路聚合	132
UDLD	139
PoE	139
配置绿色以太网	139
第 11 章：端口管理：单向链路检测	146
UDLD 概述	146
UDLD 操作	147
使用指南	149
与其他功能的依赖性	150
默认设置和配置	150
使用说明	150
常见 UDLD 任务	151
配置 UDLD	152
第 12 章：智能端口	155
概述	155
什么是智能端口	156
智能端口类型	156
智能端口宏	158
宏失败和重置操作	159
智能端口功能如何运作	160
自动智能端口	161
错误处理	164
默认配置	164
与其他功能的关系和向后兼容性	164
常见智能端口任务	164

使用基于 Web 的界面配置智能端口	166
内置智能端口宏	171
第 13 章：端口管理：PoE	182
设备上的 PoE	182
配置 PoE 属性	185
配置 PoE 设置	186
第 14 章：VLAN 管理	188
VLAN	188
配置默认 VLAN 设置	191
创建 VLAN	192
配置 VLAN 接口设置	193
定义 VLAN 成员关系	194
GVRP 设置	197
VLAN 组	198
语音 VLAN	202
访问端口组播 TV VLAN	213
客户端口组播 TV VLAN	216
第 15 章：生成树	218
STP 模式	218
配置 STP 状态和全局设置	219
定义生成树接口设置	221
配置快速生成树设置	223
多生成树	224
定义 MSTP 属性	225
将 VLAN 映射到 MSTP 实例	226
定义 MSTP 实例设置	227
定义 MSTP 实例设置	228

第 16 章：管理 MAC 地址表	230
配置静态 MAC 地址	231
管理动态 MAC 地址	232
定义保留 MAC 地址	233
第 17 章：组播	234
组播转发	234
定义组播属性	237
添加 MAC 组地址	238
添加 IP 组播组地址	239
配置 IGMP Snooping	241
MLD Snooping	243
查询 IGMP/MLD IP 组播组	245
定义组播路由器端口	246
定义“全部转发”组播	246
定义未注册的组播设置	247
第 18 章：IP 配置	249
概述	249
IPv4 管理和接口	252
DHCP 服务器	270
IPv6 管理和接口	277
域名	294
第 19 章：IP 配置：RIPv2	298
概述	298
Rip 在设备上的运行方式	299
配置 RIP	303

第 20 章：IP 配置：VRRP	310
概述	310
VRRP 的可配置元素	313
配置 VRRP	316
 第 21 章：安全	 319
定义用户	320
配置 TACACS+	323
配置 RADIUS	326
密钥管理	330
管理访问方法	333
管理访问验证	337
安全敏感数据管理	338
SSL 服务器	338
SSH 服务器	341
SSH 客户端	341
配置 TCP/UDP 服务	341
定义风暴控制	342
配置端口安全	343
802.1X	345
DoS 防护	345
DHCP Snooping	353
IP 源防护	354
ARP 检测	357
第一步跳安全性	362
 第 22 章：安全：802.1x 验证	 363
802.1X 概述	363
验证方概述	365
常见任务	373

通过 GUI 进行 802.1X 配置	375
定义时间范围	384
验证方法和端口模式支持	385
第 23 章：安全：IPv6 第一步跳安全性	387
第一步跳安全性概述	387
路由器通告防护	391
邻居发现检测	391
DHCPv6 防护	392
邻近绑定完整性	392
攻击保护	394
策略、全局参数和系统默认值	396
常见任务	397
默认设置和配置	398
使用说明	399
通过 Web GUI 配置第一步跳安全性	399
第 24 章：安全：SSH 客户端	409
安全复制 (SCP) 和 SSH	409
保护方法	410
SSH 服务器验证	411
SSH 客户端验证	412
使用说明	413
常见任务	413
GUI 中的 SSH 客户端配置	414
第 25 章：安全：SSH 服务器	418
概述	418
常见任务	418
SSH 服务器配置页面	419

第 26 章：安全：安全敏感数据管理	422
简介	422
SSD 规则	423
SSD 属性	427
配置文件	429
SSD 管理通道	433
菜单 CLI 和密码恢复	434
配置 SSD	434
 第 27 章：访问控制	 437
访问控制列表	437
定义基于 MAC 的 ACL	439
基于 IPv4 的 ACL	441
基于 IPv6 的 ACL	445
定义 ACL 绑定	448
 第 28 章：服务质量	 450
QoS 功能和组件	450
配置 QoS - 一般	453
QoS 基本模式	463
QoS 高级模式	465
管理 QoS 统计信息	474
 第 29 章：SNMP	 478
SNMP 版本和工作流程	478
型号 OID	480
SNMP 引擎 ID	481
配置 SNMP 视图	483
创建 SNMP 组	484
管理 SNMP 用户	486

定义 SNMP 社区	487
定义 Trap 设置	489
通知接收设备	489
SNMP 通知过滤器	493

使用入门

本节介绍了基于 Web 的配置实用程序，具体包括以下主题：

- 启动基于 Web 的配置实用程序
- 设备配置快速入门
- 接口命名约定
- 500 设备之间的差异
- 窗口导航

启动基于 Web 的配置实用程序

本节介绍了如何导航基于 Web 的交换机配置实用程序。

如果您使用了弹出窗口拦截器，请确保已将其禁用。

浏览器限制

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

启动配置实用程序

打开基于 Web 的配置实用程序的步骤：

步骤 1 打开任一 Web 浏览器。

步骤 2 在浏览器地址栏中输入要配置的设备的 IP 地址，然后按 **Enter**。

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

登录

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

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

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

登录到设备配置实用程序的步骤：

- 步骤 1** 输入用户名/密码。该密码最多可以包含 64 个 ASCII 字符。在“**配置安全性**”一章中的“**设置密码复杂性规则**”一节中介绍了密码复杂性规则。
- 步骤 2** 如果不使用英文，可以从 *语言* 下拉菜单中选择所需的语言。要为设备添加新语言或更新当前语言，请参阅“**升级/备份固件/语言**”一节。
- 步骤 3** 如果这是首次使用默认用户 ID (**cisco**) 和默认密码 (**cisco**) 登录，或者密码已过期，将会打开“**更改密码**”页面。有关其他信息，请参阅“**密码过期**”。
- 步骤 4** 选择是否选择**禁用密码复杂性规则**。有关密码复杂性的详情，请参阅“**设置密码复杂性规则**”一节。
- 步骤 5** 输入新密码并单击**应用**。

如果登录尝试成功，将会显示“使用入门”页面。

如果输入了错误的用户名或密码，将显示错误消息，而窗口上会继续显示“登录”页面。如果登录时遇到问题，请参阅“**管理指导**”中的“**启动配置实用程序**”一节了解详情。

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

HTTP/HTTPS

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

注 在单击**安全浏览 (HTTPS)** 按钮之前，无需输入用户名/密码。

有关如何配置 HTTPS 的信息，请参阅 [SSL 服务器](#)。

密码过期

此时将显示“新密码”页面：

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

注销

默认情况下，如果应用程序在十分钟内无活动，将会注销。您可以按[定义闲置会话超时](#)一节中所述更改此默认值。



注意

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

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

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

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

要注销，只需单击任意页面右上角的**退出**。系统便会注销设备。

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

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

设备配置快速入门

为通过快速导航简化设备配置，“使用入门”页面提供了最常用页面的链接。

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

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

接口命名约定

在 GUI 内，可结合以下元素表示接口：

- **接口类型**：以下类型的接口在各种类型的设备上均有提供：
 - **快速以太网（10/100 位）** - 这种类型的接口显示为 **FE**。
 - **千兆以太网端口（10/100/1000 位）** - 这种类型的接口显示为 **GE**。
 - **万兆以太网端口（10000 位）** - 这种类型的接口显示为 **XG**。
 - **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**。
- **单元编号** - 堆叠中单元的编号。在独立式型号中，单元编号始终为 1。
- **插槽编号** - 插槽编号为 1 或 2。
- **接口编号**：端口、LAG、隧道或 VLAN ID

500 设备之间的差异

本指南适用于 Sx500、SG500X、SG500XG 和 ESW2-550X 设备。如果某项功能只与其中一台设备相关，文中会予以注明。

下面总结了这两款设备之间的差异：

- 只有在独立式模式下运行的 SG500X、SG500XG 和 ESW2-550X 设备（以及在高级混合堆叠下运行的 SG500X 和 Sx500 设备 - 有关详情，请参阅[管理：堆栈管理](#)）支持 RIP 和 VRRP 功能。
- TCAM 大小，请参阅[查看 TCAM 利用率](#)
- 这两款设备上的堆叠端口不同。请参阅[堆叠端口](#)。
- 这两款设备上每种电缆类型的端口速度可用性不同。请参阅[电缆类型](#)。
- 在这些设备中，启用 IPv4 路由的方式不同，如下所示：
 - SG500XSG500XG/ESW2-550X - 必须在“IPv4 接口”页面中启用 IPv4 路由。

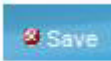
- Sx500 - 将设备的系统模式从第 2 层切换为第 3 层后，系统会自动启用 IPv4 路由。

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

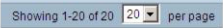
应用报头显示在每个页面上。可以提供以下应用程序链接：

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，将不再显示红色 X 图标和“保存”应用程序链接。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。
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 。）
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。 ▪ 删除语言：删除设备上的第二种语言。第一种语言（英文）无法删除。 ▪ 调试：用来进行转换。如果选择此选项，所有基于 Web 的配置实用程序标签将消失，其原来的位置上将显示与语言文件中的 ID 对应的字符串 ID。 注 要升级语言文件，请使用“升级/备份固件/语言”页面。
退出	单击该按钮可注销基于 Web 的交换机配置实用程序。
关于	单击该链接会显示设备名称和设备版本号。

应用程序链接名称	说明
帮助	单击该按钮会显示在线帮助。
	如果记录了严重性级别高于严重的系统日志消息，则会显示“系统日志警报状态”图标。单击该图标将打开 RAM 页面。访问该页面后，将不会再显示“系统日志警报状态”图标。要在没有活动的系统日志消息的情况下显示该页面，请单击 状态和统计信息 > 查看日志 > RAM 。

管理按钮

下表介绍了系统中各页面上显示的常用按钮。

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。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。

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](#)
- [查看以太网接口](#)
- [查看 Etherlike 统计信息](#)
- [查看 GVRP 统计信息](#)
- [查看 802.1X EAP 统计信息](#)
- [查看 TCAM 利用率](#)
- [状况](#)
- [管理 RMON](#)
- [查看日志](#)

系统摘要

请参阅[系统设置](#)。

查看以太网接口

“接口”页面会显示每个端口的流量统计信息。该信息的刷新速率是可以选择的。

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

显示以太网统计信息和/或设置刷新率的步骤：

步骤 1 单击**状态和统计信息 > 接口**。

步骤 2 输入参数。

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

接收统计信息区域显示关于传入数据包的信息。

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

传输数据统计区域显示关于传出数据包的信息。

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

清除或查看统计信息计数器的步骤：

- 单击**清除接口计数器**清除显示的接口的计数器。
- 单击**查看所有接口统计信息**，在单个页面中查看所有端口。

查看 Etherlike 统计信息

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

查看 Etherlike 统计信息和/或设置刷新速率的步骤：

步骤 1 单击 **状态和统计信息 > Etherlike**。

步骤 2 输入参数。

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

将针对选定接口显示以下字段。

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

清除统计信息计数器的步骤：

- 单击 **清除接口计数器** 清除选定的接口计数器。
- 单击 **查看所有接口统计信息**，在单个页面中查看所有端口。

查看 GVRP 统计信息

GVRP 页面显示关于从一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 页面。

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 统计信息的间隔时间。

属性计数器块显示每个接口的各种类型数据包的计数器。

- **Join Empty** - 接收/传输的 GVRP Join Empty 数据包数。
- **空** - 接收/传输的 GVRP 空数据包数。
- **Leave Empty** - 接收/传输的 GVRP Leave Empty 数据包数。
- **Join In** - 接收/传输的 GVRP Join In 数据包数。
- **Leave In** - 接收/传输的 GVRP Leave In 数据包数。
- **Leave All** - 接收/传输的 GVRP Leave All 数据包数。

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。

清除统计信息计数器的步骤：

- 单击**清除接口计数器**清除选定的计数器。
- 单击**查看所有接口统计信息**，在单个页面中查看所有端口。

查看 802.1X EAP 统计信息

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

查看 EAP 统计信息和/或设置刷新速率的步骤：

步骤 1 单击**状态和统计信息 > 802.1x EAP**。

步骤 2 选择需要轮询统计信息的**接口**。

步骤 3 选择刷新 EAP 统计信息的间隔时间（**刷新速率**）。

将针对选定接口显示以下值。

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

清除统计信息计数器的步骤：

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

查看 TCAM 利用率

设备架构使用三重内容可寻址存储器 (TCAM) 来支持线速数据包操作。

TCAM 存放由应用生成的规则，如 ACL（访问控制列表）、服务质量 (QoS) 和 IP 路由，以及用户创建的规则。

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 TCAM 利用率，请单击**状态和统计信息 > TCAM 利用率**。

对于第 3 层系统模式下以及作为堆栈（每单元）一部分的 SG500X/SG500XG 设备和 Sx500 设备，将显示以下字段：

- **单元编号** - 显示 TCAM 利用率的堆栈中的单元。如果设备处于独立式模式，将不显示此字段。
- **IPv4 和 IPv6 路由的最大 TCAM 条目数** - 最大可用 TCAM 条目数。
- **IPv4 路由**
 - **使用中** - 用于 IPv4 路由的 TCAM 条目数。
 - **最大值** - 可用于 IPv4 路由的可用 TCAM 条目数。
- **IPv6 路由** - 用于 IPv6 路由的 TCAM 条目数。
 - **使用中** - 用于 IPv6 路由的 TCAM 条目数。
 - **最大值** - 可用于 IPv6 路由的可用 TCAM 条目数。
- **非 IP 规则的最大 TCAM 条目数** - 可用于非 IP 规则的最大 TCAM 条目数。
- **非 IP 规则**
 - **使用中** - 用于非 IP 规则的 TCAM 条目数。
 - **最大值** - 可用于非 IP 规则的可用 TCAM 条目数。

若要查看如何更改各种流程间的分配（对于 500 系列），请参阅[路由器资源](#)一节。

状况

请参阅[健康状况](#)。

管理 RMON

RMON（远程网络监控）是一项 SNMP 规范，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 Trap。本地 SNMP 代理比较实际的实时计数器与预定义阈值并生成告警，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（因为计数器值已清除）。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”（定义告警），然后指定发生该事件后执行什么操作（记录、发送 Trap 或记录并发送 Trap）。

查看 RMON 统计信息

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

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

查看 RMON 统计信息和/或设置刷新速率的步骤：

步骤 1 单击**状态和统计信息 > RMON > 统计信息**。

步骤 2 选择要显示以太网统计信息的**接口**。

步骤 3 选择刷新速率，即刷新接口统计信息的间隔时间。

将针对选定接口显示以下统计信息。

- **已接收的字节数** - 接收的八位字节数，包括坏数据包和 FCS 八位字节数，但不包括帧位。
- **丢弃事件** - 丢弃的数据包数。
- **已接收的数据包** - 接收的好数据包数，包括组播数据包和广播数据包。
- **已接收的广播数据包数** - 接收到的正常广播数据包数。该数量不包括组播数据包。
- **已接收的组播数据包数** - 接收到的正常组播数据包数。
- **CRC 和 Align 错误数** - 发生的 CRC 和 Align 错误数。
- **过小数据包数** - 接收的大小不足（小于 64 八位字节）的数据包数。
- **过大数据包数** - 接收的大小过大（大于 2000 八位字节）的数据包数。
- **分片数** - 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 八位字节的数据包总数。该数量不包括帧位，但包括具有整数数量八位字节（FCS 错误）的坏 FCS（帧校验序列）或具有非整数八位字节（校正误差）的坏 FCS 的 FCS 八位字节数。超时发送帧数据包定义为满足以下条件的以太网帧：
 - 数据包数据长度大于 MRU。
 - 数据包具有无效的 CRC。
 - 尚未检测 Rx 错误事件。
- **冲突数** - 接收的冲突数。如果启用了巨型帧，超时发送帧的阈值将提升为巨型帧的最大大小。
- **64 字节的帧数** - 接收的包含 64 字节的帧数。
- **65 至 127 字节的帧数** - 接收的包含 65-127 字节的帧数。
- **128 至 255 字节的帧数** - 接收的包含 128-255 字节的帧数。
- **256 至 511 字节的帧数** - 接收的包含 256-511 字节的帧数。
- **512 至 1023 字节的帧数** - 接收的包含 512-1023 字节的帧数。
- **Frames of 1024 Bytes or More（超过 1024 字节的帧数）** - 接收的包含 1024 - 2000 字节的帧和巨型帧的数量。

清除统计信息计数器的步骤：

- 单击**清除接口计数器**清除选定的接口计数器。
- 单击**查看所有接口统计信息**，在单个页面中查看所有端口。

配置 RMON 历史记录

RMON 功能可以监控每个接口的统计信息。

“历史控制表”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**查看实际统计信息。

查看 RMON 历史表

“历史表”页面显示特定于接口的统计性网络样本。该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**列表中，选择要显示的样本条目数。

将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。
- **取样编号** - 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删除的数据包数。它可能不表示删除的数据包的精确数量，而是表示检测到的数据包丢弃次数。
- **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。
- **利用率** - 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。

定义 RMON 事件控制

您可以控制触发警告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** - 配置触发告警时发生的事件。可以是记录和 Trap 的任意组合。
- **告警页面** - 配置触发告警的情况。

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。

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 Trap 时要包括的 SNMP 社区字符串（可选）。请注意，必须使用**定义 SNMPv1, 2 通知接收设备**或**定义 SNMPv3 通知接收设备**页面定义社区，以便 Trap 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 告警”页面中为事件附加告警。
- **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** - 告警消失时不执行操作。
 - **日志 (事件日志表)** - 触发告警时向事件日志表添加一条日志条目。
 - **Trap (SNMP 管理器和系统日志服务器)** - 告警消失时向远程日志服务器发送 Trap。
 - **日志和 Trap** - 告警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 Trap。
- **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）。
- **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告警日志（请参阅下面的说明）。

查看 RMON 事件日志

“事件日志表”页面会显示发生的事件（操作）的日志。可记录两种事件：*日志*或*日志和 Trap*。当将事件与告警（请参阅“告警”页面）绑定，并达到了告警的条件时，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**。

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** - 触发告警的事件说明。

定义 RMON 告警

RMON 告警提供了一种机制，可用于设置阈值和取样间隔，以在任何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。告警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。发出下降告警后，将在超过上限阈值时发出下一个告警。

一个或多个告警绑定至事件，表明告警发生时采取的措施。

在“告警”页面中，您可以配置告警并将其与事件绑定。可以通过绝对值或计数器值中的变化（差值）来监控告警计数器。

输入 RMON 告警的步骤：

步骤 1 单击**状态和统计信息 > RMON > 告警**。此时将显示以前定义的所有告警。字段将在下面的“添加 RMON 告警”页面中进行说明。除这些字段之外，还将显示以下字段：

- **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。

- **告警条目** - 显示告警条目编号。
- **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** - 选择用于生成告警的取样方法。选项如下：
 - *绝对值* - 如果超过了阈值，则生成告警。
 - *差值* - 从当前值中减去上次取样的值，将差值与阈值进行比较。如果超过了阈值，则生成告警。
- **上限阈值** - 输入触发上限阈值告警的值。
- **上升事件** - 选择触发上升事件时要执行的事件。事件将在“事件”页面中创建。
- **下限阈值** - 输入触发下限阈值告警的值。
- **下降事件** - 选择触发下降事件时要执行的事件。
- **启动告警** - 选择启动告警生成的第一个事件。上升被定义为从阈值向较高阈值变化的行为。
 - *上升告警* - 上升值触发上限阈值告警。
 - *下降告警* - 下降值触发下限阈值告警。
 - *上升和下降* - 上升值和下降值都触发该告警。
- **间隔** - 输入以秒表示的告警间隔。
- **所有者** - 输入接收该告警的用户或网络管理系统的名称。

步骤 4 单击**应用**。RMON 告警将保存至当前配置文件中。

查看日志

请参阅[查看内存日志](#)。

管理：系统日志

本节介绍系统日志功能，使用此功能，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 Console 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 Trap 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。

本节包含以下小节：

- [设置系统日志设置](#)
- [设置远程记录设置](#)
- [查看内存日志](#)

设置系统日志设置

在“日志设置”页面上，您可以启用或禁用记录，及选择是否汇总日志消息。

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

下面按照从高到低的顺序列出了事件的严重性级别：

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

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

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

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

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

设置全局日志参数的步骤：

步骤 1 单击**管理 > 系统日志 > 日志设置**。

步骤 2 输入参数。

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

步骤 3 单击**应用**。将更新当前配置文件。

设置远程记录设置

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

定义系统日志服务器的步骤：

步骤 1 单击**管理 > 系统日志 > 远程日志服务器**。

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。

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 地址还是名称来识别远程日志服务器。
- **IP 版本** - 选择支持的 IP 格式。
- **IPv6 地址类型** - 选择 IPv6 地址类型（如果使用 IPv6）。选项如下：
 - **链路本地** - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
 - **全局** - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。
- **链路本地接口** - 从列表中选择链路本地接口（如果选择的 IPv6 地址类型为“链路本地”）。
- **日志服务器 IP 地址/名称** - 输入日志服务器的 IP 地址或域名。
- **UDP 端口** - 输入要向其发送日志消息的 UDP 端口。

- **设备** - 选择从其将系统日志发送给远程服务器的设备值。只能为服务器指定一个设备值。如果指定第二个设备代码，其将覆盖第一个设备值。
- **说明** - 输入服务器说明。
- **最低严重程度** - 选择要发送到服务器的系统日志消息的最低严重性级别。

步骤 5 单击**应用**，将会关闭“添加远程日志服务器”页面，添加系统日志服务器，并更新当前配置文件。

查看内存日志

设备可以写入以下日志：

- RAM 中的日志（在重启过程中被清除）。
- Flash 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

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

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

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

该页面包含以下字段：

- **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。

Flash

Flash 页面会按时间先后顺序显示存储在 Flash 中的消息。所记录事件的最低严重程度在“日志设置”页面中配置。设备重启时，Flash 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 > Flash**。

该页面包含以下字段：

- **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。

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
- 升级/备份固件/语言
- 活动映像
- 下载/备份配置/日志
- 配置文件属性
- 复制/保存配置
- 通过 DHCP 进行自动配置

系统文件

系统文件是指包含配置信息、固件映像或引导代码的文件。

通过这些文件可进行各种操作，例如：选择用于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。

可用的文件传输方法有以下几种：

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

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。

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

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

设备上的其他文件包括固件、引导代码和日志文件，这些文件称为*工作文件*。

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

文件和文件类型

在设备上可以找到以下类型的配置和工作文件：

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

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

要保留对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（通常为当前配置）复制到启动配置而保存的参数值。

启动配置保留在闪存中，并且在设备重启后会保留。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，可以将镜像配置复制到其他文件类型或其他设备。

可在“配置文件属性”页面禁用自动将当前配置复制到镜像配置的选项。

- **备份配置** - 用于系统关机保护或特定工作状态维护的配置文件手动副本。可以将镜像配置、启动配置或当前配置复制到备份配置文件。备份配置存放在闪存中，并且当设备重启时会保留。
- **固件** - 可控制设备的操作和功能的程序。更多时候被称为映像。
- **Boot 代码** - 控制基本系统启动及启动固件映像。
- **语言文件** - 能够使基于 Web 的配置实用程序窗口以选定语言显示的字典。

- **Flash** - 存储在闪存中的系统日志消息。

文件操作

可以执行以下操作来管理固件和配置文件：

- 按 **升级/备份固件/语言** 一节中所述升级固件或引导代码，或者更换第二语言。
- 按 **活动映像** 一节中所述查看当前使用的固件映像或选择下次重启时要使用的映像。
- 按 **下载/备份配置/日志** 一节中所述将设备上的配置文件保存到其他设备上的位置。
- 按 **配置文件属性** 一节中所述清除启动配置或备份配置文件类型。
- 按 **复制/保存配置** 一节中所述将一种配置文件类型复制到另一种配置文件类型。
- 按 **通过 DHCP 进行自动配置** 一节中所述启用将配置文件从 DHCP 服务器自动上传到设备的功能。

本节包含以下主题：

- **升级/备份固件/语言**
- **活动映像**
- **下载/备份配置/日志**
- **配置文件属性**
- **复制/保存配置**
- **通过 DHCP 进行自动配置**

升级/备份固件/语言

升级/备份固件/语言 流程可用于：

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

支持以下文件传输方法：

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

如果将新语言文件加载到了设备上，便可以从下拉菜单中选择这种新语言。（无需重启设备）。此语言文件会自动复制到堆栈中的所有设备。

堆栈上的所有软件映像必须保持一致以确保堆栈的正确运行。如果堆叠上添加了新设备且其软件映像与主装置的软件映像不一致，则主装置将自动将正确的映像载入到该新设备中。

可通过两种方法更新堆叠上的所有映像：

- 可在将单元与堆叠相连接之前更新映像。这是我们建议使用的方法。
- 升级设备或堆栈。如果堆栈已更新，从单元会自动更新。此执行过程如下所示：
 - 使用“升级/备份固件/语言”页面将映像从 TFTP/SCP 服务器复制到主装置。
 - 使用“活动映像”页面更改活动映像。
 - 使用“重启”页面重启。

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*。

升级固件时，新映像总是会替换已标识为非活动映像的映像。

即使在将新固件上传到设备后，设备也会继续使用活动映像（旧版本）引导，直至您使用 **活动映像** 一节中介绍的步骤将新映像的状态更改为活动映像。然后引导设备。

注 如果设备正在以堆叠模式运行，则新固件将会被推送到所有的堆叠单元。如果带有不同固件版本的新设备加入该堆栈，则主单元将自动同步该新加入单元的固件版本。该同步过程将以透明的方式进行且无需进行手动干预。

升级/备份固件或语言文件

升级或备份软件映像或语言文件的步骤：

步骤 1 单击**管理 > 文件管理 > 升级/备份固件/语言**。

步骤 2 单击“传输方法”。按以下步骤进行：

- 如果选择了TFTP，则转至**步骤 3**。
- 如果选择了通过 HTTP/HTTPS，则转至**步骤 4**。
- 如果选择了通过 SCP，则转至**步骤 5**。

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

请选择以下**保存操作**之一：

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

输入以下字段：

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

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

- **文件类型** - 选择以下文件类型之一：
 - *固件映像* - 选择它可升级固件映像。
 - *语言* - 选择它可升级语言文件。
- **文件名** - 单击**浏览**选择文件或输入要在传输中使用的路径和源文件名。

步骤 5 如果选择了通过 **SCP (藉由 SSH)**，请参阅 **SSH 客户端验证**以了解说明。然后输入以下字段：（仅对独有的字段进行说明，对于非独有字段，请参阅上述说明）

- **远程 SSH 服务器验证** - 要启用 SSH 服务器验证（默认情况下为禁用），请单击**编辑**。系统将转到 **SSH 服务器验证**页面以配置 SSH 服务器，然后再返回本页。使用 **SSH 服务器验证**页面可选择 SSH 用户验证方法（密码或公共/专用密钥），在设备上设置用户名和密码（如果已选中密码方法），以及根据需要生成 RSA 或 DSA 密钥。

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。

注 一次性凭证的用户名和密码将不会保存在配置文件中。

请选择以下**保存操作**之一：

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

输入以下字段：

- **文件类型** - 选择目的文件类型。只会显示有效的文件类型。（这些文件类型在**文件和文件类型**一节中做了说明）。
- **SCP 服务器定义** - 选择是按照 IP 地址还是域名来指定 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，可从其他网络查看和访问。
- **链路本地接口** - 从列表中选择链路本地接口。
- **SCP 服务器 IP 地址/名称** - 输入 SCP 服务器的 IP 地址或域名。
- **（用于升级）源文件名** - 输入源文件的名称。
- **（用于备份）目的文件名** - 输入备份文件的名称。

步骤 6 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。

活动映像

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**。设备将从设置为**活动映像**的映像引导。您可以将已标识为**非活动映像**的映像更改为**活动映像**。（可以使用**管理接口**一节中介绍的流程重启设备）。

选择活动映像的步骤：

步骤 1 单击**管理 > 文件管理 > 活动映像**。

该页面显示以下字段：

- **活动映像** - 显示当前在设备上处于活动状态的映像文件。
- **活动映像版本号** - 显示活动映像的固件版本。
- **重启后的活动映像** - 显示重启后处于活动状态的映像。
- **重启后的活动映像版本号** - 原样显示重启后的活动映像的固件版本。

步骤 2 从**重启后的活动映像**菜单中选择映像，以标识设备重启后作为活动映像的固件映像。
重启后的活动映像版本号会显示设备重启后所使用的活动映像的固件版本。

步骤 3 单击**应用**。将更新活动映像选择。

下载/备份配置/日志

通过“下载/备份配置/日志”页面，可实现以下操作：

- 将配置文件或日志从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。

注 如果设备正在堆叠模式下运行，则将从主单元提取配置文件。

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或备份配置文件时，新文件会替换旧文件。

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

配置文件向后兼容性

将配置文件从外部设备还原到设备时，可能会出现以下兼容性问题：

- **将队列模式从 4 改为 8** - 必须检查队列相关配置并对其进行调整，以满足新队列模式的 QoS 目标。请参阅 *CLI 参考指南*，获取包含这些 QoS 命令的列表。
- **将队列模式从 8 改为 4** - 与新的队列模式冲突的队列相关配置命令将被拒绝，这就意味着配置文件下载失败。使用“系统模式和堆栈管理”页面更改队列模式。
- **更改系统模式** - 如果下载到设备的配置文件包含系统模式，且此文件中的系统模式与当前系统模式相匹配，则可忽略此信息。否则，如果系统模式已更改，可能会出现以下情况：
 - 如果配置文件已下载到设备中（使用“下载/备份配置/日志”页面），操作将中止，并且将显示一条消息，表示必须在“系统模式和堆栈管理”页面更改系统模式。

- 如果配置文件已在自动配置过程中下载，将删除启动配置文件，且设备会在新的系统模式下自动重启。将使用空的配置文件配置设备。请参阅[通过 DHCP 进行自动配置](#)。
- 请参阅[重启后的配置](#)，了解有关堆叠模式更改时所出现情况的说明。

下载或备份配置或日志文件

备份或还原系统配置文件的步骤：

步骤 1 单击 **管理 > 文件管理 > 下载/备份配置/日志**。

步骤 2 选择传输方法。

步骤 3 如果选择了[通过 TFTP](#)，请输入参数。否则，请跳至**步骤 4**。

选择下载或备份**保存操作**。

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

- a. **服务器定义** - 选择是按照 IP 地址还是域名来指定 TFTP 服务器。
- b. **IP 版本** - 选择使用 IPv4 还是 IPv6 地址。

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

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

- **链路本地** - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
- **全局** - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。

d. **链路本地接口** - 从列表中选择链路本地接口。

e. **TFTP 服务器** - 输入 TFTP 服务器的 IP 地址。

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

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

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

- a. **服务器定义** - 选择是按照 IP 地址还是域名来指定 TFTP 服务器。
 - b. **IP 版本** - 选择使用 IPv4 还是 IPv6 地址。
 - c. **IPv6 地址类型** - 选择 IPv6 地址类型（如果使用 IPv6）。选项如下：
 - **链路本地** - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
 - **全局** - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。
 - d. **链路本地接口** - 从列表中选择链路本地接口。
 - e. **TFTP 服务器 IP 地址/名称** - 输入 TFTP 服务器的 IP 地址或域名。
 - f. **源文件类型** - 输入源配置文件类型。只会显示有效的文件类型。（这些文件类型在 [文件和文件类型](#) 一节中做了说明）。
 - g. **敏感数据** - 选择应如何将敏感数据包含在备份文件中。可能的选项有：
 - **排除** - 不将敏感数据包含在备份中。
 - **加密** - 将敏感数据以加密的形式包含在备份中。
 - **明文模式** - 将敏感数据以明文模式包含在备份中。
- 注** 可用的敏感数据选项由当前用户的 SSD 规则决定。有关详情，请参阅“安全敏感数据管理 > SSD 规则”页面。
- h. **目的文件名** - 输入目的文件名。文件名不能包含斜线（\ 或 /）、文件名的首字母不能为句点（.），且文件名的字符数必须在 1 到 160 之间。（有效字符为：A-Z、a-z、0-9、“.”、“-”、“_”）。
 - i. 单击**应用**。将升级或备份该文件。

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

选择**保存操作**。

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

- a. **源文件名** - 单击**浏览**选择文件或输入要在传输中使用的路径和源文件名。
- b. **目的文件类型** - 选择配置文件类型。只会显示有效的文件类型。（这些文件类型在 [文件和文件类型](#) 一节中做了说明）。

c. 单击**应用**。将从其他设备将该文件传输到本设备上。

如果**保存操作为备份**（将文件复制到其他设备中），请执行以下操作：

- a. **源文件类型** - 选择配置文件类型。只会显示有效的文件类型。（这些文件类型在[文件和文件类型](#)一节中做了说明）。
- b. **敏感数据** - 选择应如何将敏感数据包含在备份文件中。可能的选项有：
 - **排除** - 不将敏感数据包含在备份中。
 - **加密** - 将敏感数据以加密的形式包含在备份中。
 - **明文模式** - 将敏感数据以明文模式包含在备份中。

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

c. 单击**应用**。将升级或备份该文件。

步骤 5 如果选择了**通过 SCP (藉由 SSH)**，请参阅[GUI 中的 SSH 客户端配置](#)以了解说明。然后输入以下字段：

- **远程 SSH 服务器验证** - 要启用 SSH 服务器验证（默认情况下为禁用），请单击**编辑**，它会将您带到[SSH 服务器验证](#)页面以配置服务器，然后再返回该页面。使用[SSH 服务器验证](#)页面可选择 SSH 用户验证方法（密码或公共/专用密钥），在设备上设置用户名和密码（如果已选中密码方法），以及根据需要生成 RSA 或 DSA 密钥。

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** - 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。
- **SCP 服务器定义** - 选择是按照 IP 地址还是域名来指定 TFTP 服务器。
- **IP 版本** - 选择使用 IPv4 还是 IPv6 地址。
- **IPv6 地址类型** - 选择 IPv6 地址类型（如果使用 IPv6）。选项如下：
 - **链路本地** - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
 - **全局** - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。

- **链路本地接口** - 从列表中选择链路本地接口。
- **SCP 服务器 IP 地址/名称** - 输入 TFTP 服务器的 IP 地址或域名。

如果**保存操作**为**下载**（用其他设备上的新版本替换本设备上的文件），请输入以下字段。

- **源文件名** - 输入源文件的名称。
- **目的文件类型** - 选择配置文件类型。只会显示有效的文件类型。（这些文件类型在[文件和文件类型](#)一节中做了说明）。

如果**保存操作**为**备份**（将文件复制到其他设备中），请输入以下字段（除应输入以上列出的那些字段外）：

- **源文件类型** - 选择配置文件类型。只会显示有效的文件类型。（这些文件类型在[文件和文件类型](#)一节中做了说明）。
- **敏感数据** - 选择应如何将敏感数据包含在备份文件中。可能的选项有：
 - *排除* - 不将敏感数据包含在备份中。
 - *加密* - 将敏感数据以加密的形式包含在备份中。
 - *明文模式* - 将敏感数据以明文模式包含在备份中。

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

- **目的文件名** - 复制操作的目标文件的名称。

步骤 6 单击**应用**。将升级或备份该文件。

配置文件属性

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

注 如果设备正在堆叠模式下运行，则将从主单元提取配置文件。

要对是否创建镜像配置文件进行设置，请清除配置文件并查看配置文件的创建时间：

步骤 1 单击 **管理 > 文件管理 > 配置文件属性**。

此页面显示了以下字段：

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

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

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

复制/保存配置

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。要保留当前配置中的参数，必须将当前配置复制到其他配置类型或保存到其他设备上。



注意

除非将当前配置复制到启动配置或其他配置文件，否则自上次复制文件后所做的所有更改将会在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备份配置。
- 从启动配置到当前配置、启动配置或备份配置。
- 从备份配置到当前配置、启动配置或备份配置。
- 从镜像配置到当前配置、启动配置或备份配置。

将一种类型的配置文件复制到另一种类型的配置文件的步骤：

步骤 1 单击 **管理 > 文件管理 > 复制/保存配置**。

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

步骤 3 选择将由源文件覆盖的**目的文件名**。

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

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

步骤 4 保存图标闪烁字段将表明在有未保存的数据时图标是否会闪烁。要禁用/启用该功能，可单击**禁用/启用保存图标闪烁**。**步骤 5** 单击**应用**。文件将被复制。

通过 DHCP 进行自动配置

DHCP 自动配置可将配置信息传递到 TCP/IP 网络中的主机。基于该协议，设备便可通过自动配置功能从 TFTP/SCP 服务器上下载配置文件。

要使用此功能，设备必须配置为 DHCPv4 客户端（此时，支持从 DHCPv4 服务器自动配置）和/或 DHCPv6 客户端（此时，支持从 DHCPv6 服务器自动配置）。

默认情况下，当启用通过 DHCP 进行自动配置功能后，便可将设备作为 DHCP 客户端来使用。

在自动配置过程中还可使用安全复制协议 (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[安全：安全敏感数据管理](#)）。

在以下情况下会触发通过 DHCPv4 进行自动配置的功能：

- 重启后（使用 DHCPv4）动态分配或续订 IP 地址时。
- 收到明确的 DHCPv4 续订请求且如果已为此配置了设备和服务器。
- 自动续租 DHCPv4 后。

满足以下条件时会触发通过 DHCPv6 进行自动配置的功能：

- 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。

DHCP 服务器选项

DHCP 消息可能会包含配置服务器名称/地址和配置文件名/路径（这些是可选选项）。这些选项可在来自 DHCPv4 服务器的 **Offer** 消息和来自 DHCPv6 服务器的**信息应答**消息中找到。

可在“自动配置”页面配置备份信息（配置服务器名称/地址和配置文件名/路径）。此信息用于 DHCPv4 消息不包含此信息的情况（但不适用于 DHCPv6）。

自动配置下载协议（TFTP 或 SCP）

自动配置下载协议可进行如下配置：

- **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。
- **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 客户端验证参数

默认情况下，禁用远程 SSH 服务器验证，因此，设备将接受任何开箱使用的远程 SSH 服务器。您可以启用远程 SSH 服务器验证以只允许通过信任服务器列表中的服务器进行的连接。

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 当下载文件以进行手动下载（指不是通过 DHCP 自动配置功能进行的下载）时，也可使用 SSH 客户端验证参数。

自动配置过程

当触发自动配置过程后，会按顺序发生以下事件：

- 将访问 DHCP 服务器以获取 TFTP/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 DHCP 服务器未提供服务器和配置文件选项，那么：
 - **对于 DHCPv4：**将使用用户定义的备份配置文件名。
 - **对于 DHCPv6：**此过程将停止。
- 如果 DHCP 服务器未发送这些选项，且备份 TFTP/SCP 服务器地址参数为空，那么：
 - **对于 DHCPv4：**
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过程。
 - **对于 DHCPv6：**自动配置过程将停止。
- 如果 DHCP 服务器提供配置文件名（DHCPv4：选项 67；DHCPv6：选项 60），那么将选择复制协议（SCP/TFTP），如[自动配置下载协议（TFTP 或 SCP）](#)中所述。
- 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。注意：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 TFTP/SCP 服务器，以从中下载文件。

下载过程只有在新的配置文件名与当前的配置文件名不同时（即使当前的配置文件为空）才能完成。

- 系统将生成系统日志消息，确认自动配置过程已完成。

配置 DHCP 自动配置

工作流程

配置 DHCP 自动配置的步骤。

1. 配置 DHCPv4 和/或 DHCPv6 服务器以发送所需的选项。此过程在本指南中尚无描述。
2. 配置自动配置参数。
3. 在在**第 2 层系统模式下定义 IPv4 接口**或在**第 3 层系统模式下定义 IPv4 接口**页面中将设备定义为 DHCPv4 客户端，以及/或者在**IPv6 接口**页面中将设备定义为 DHCPv6 客户端。

Web 配置

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

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

在 DHCP 自动配置过程中，请注意以下几点：

- 存放在 TFTP/SCP 服务器上的配置文件必须符合所支持配置文件的形式和格式要求。在将文件加载到启动配置之前，会检查文件的形式和格式，但不会检查配置参数的有效性。
- 在 IPv4 中，为确保设备配置能实现预期的功能，以及鉴于要按照每一 DHCP 续订周期分配不同 IP 地址，我们建议将 IP 地址绑定到 DHCP 服务器表中的 MAC 地址。这样可确保每台设备都有自身保留的 IP 地址和其他相关信息。

配置自动配置的步骤：

步骤 1 单击**管理 > 文件管理 > DHCP 自动配置**。

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启用状态，但是可在此处禁用。
- **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。
- **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。

步骤 3 输入在未收到来自 DHCP 服务器的任何配置文件名的情况下将使用的以下可选信息。

- **备份服务器定义** - 选择**按 IP 地址**或**按名称**可配置服务器。
- **IP 版本** - 选择使用 IPv4 还是 IPv6 地址。
- **IPv6 地址类型** - 选择 IPv6 地址类型（如果使用 IPv6）。选项如下：
 - **链路本地** - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 FE80，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
 - **全局** - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。
- **链路本地接口** - 从列表中选择链路本地接口（如果使用 IPv6）。
- **备份服务器 IP 地址/名称** - 输入当 DHCP 消息中未指定服务器 IP 地址时使用的服务器 IP 地址或名称。

- **备份配置文件名** - 输入当 DHCP 消息中未指定配置文件名时使用的文件路径和文件名。

步骤 4 单击**应用**。参数将复制到当前配置文件中。

管理：堆栈管理

本节介绍了如何管理堆叠。其中包含以下主题：

- 概述
- 堆叠中的单元类型
- 堆叠拓扑
- 单元 ID 分配
- 主装置选择流程
- 堆叠更改
- 堆叠中的单元故障
- 堆叠中的软件自动同步
- 堆叠单元模式
- 堆叠端口
- 默认配置
- 与其他功能进行交互
- 系统模式

概述

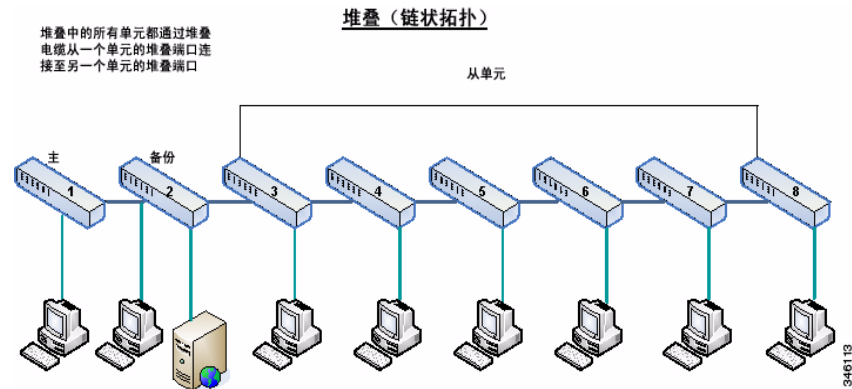
设备可以自己运行（独立式模式），也可以连接至由最多八台处于不同堆叠模式的设备组成的堆叠（请参阅[堆叠单元模式](#)）。

堆叠中的设备（单元）通过堆叠端口连接。随后，可将这些设备共同作为单个逻辑设备进行管理。

堆叠基于单个主/备用和多个从装置模型。

下面举例说明了八台设备连接至一个堆叠的情况：

堆叠架构（链状拓扑）



使用堆叠有以下优势：

- 可大幅扩展或压缩网络容量。通过添加单元，管理员可以在显著增加堆叠中端口数量的同时，维护逻辑受管的单一设备。同样，也可以移除单元，以减少网络容量。
- 已堆叠系统可通过以下方式支持冗余：
 - 如果初始主装置出现故障，则备用单元将成为主装置。
 - 堆叠系统支持两种拓扑：链状（请参阅“[堆叠架构（链状拓扑）](#)”）和环状（请参阅“[环状拓扑堆叠](#)”）。在环状拓扑中，如果其中一个堆叠端口出现故障，则该堆叠将继续以链状拓扑正常运行。（请参阅[堆叠拓扑](#)）。
 - 在环状堆叠的端口上支持一种叫做快速堆叠链路故障切换的流程，可在其中一个堆叠端口链路出现故障时缩短数据包丢失的持续时间。在堆叠恢复至新的链状拓扑之前，当前处于中断状态的堆叠端口将本应通过该端口发送的数据包回送，从而能够使用其余堆叠链路将数据包送至目的地。在快速堆叠链路故障切换期间，主/备用单元始终保持活动状态，且正常运行。

堆叠中的单元类型

一个堆叠最多包括八个单元。堆叠中的单元属于以下类型中的一种：

- **主** - 主单元的 ID 必须为 1 或 2。堆叠通过主单元进行管理，而主单元可管理其自身、备用单元和从单元。
- **备用** - 如果主单元出现故障，则备用单元承担主装置角色（故障切换）。备用单元 ID 必须为 1 或 2。

- 从 - 这些单元由主单元进行管理。

要想将单元组作为堆叠运行，则必须存在一个已启用主装置的单元。当已启用主装置的单元出现故障时，只要存在备用单元，则该堆叠即可继续正常运行（活动单元将承担主装置角色）。

如果除了主装置外，备用单元也出现故障，只有从单元正常运行，那么这些从单元也将在一分钟后停止运行。举例来说，这表示，如果 1 分钟后，将电缆插入一个在没有主装置的情况下运行的从单元，将不会形成链路。

堆叠中单元数量的向后兼容性

先前版本的设备支持最多四个单元，而非和当前版本一样可支持八个单元。可在不更改配置文件的情况下从早期版本的软件升级。

将不支持混合堆叠模式的固件版本载入堆叠，然后重启堆叠时，堆叠将恢复至原生堆叠模式。当处于混合堆叠模式的设备载入不支持混合堆叠模式的固件版本时，其系统模式将恢复至默认系统模式（SG500X：第 3 层和第 2 层；Sx500：第 2 层）。

如果堆叠的单元 ID 已手动配置，则 ID 大于 4 的单元将切换至自动编号。

单元 LED

设备拥有 4 个 LED，分别标记为 1、2、3、4，用于显示每个单元的单元 ID（例如，在单元 ID 1 上，LED 1 亮起而其他 LED 熄灭）。为了支持单元 ID 大于 4 的单元，LED 显示将根据以下定义进行更改：

- 单元 1 到 4：分别亮起 LED 1 到 4。
- 单元 5：LED 1 和 4 亮起。
- 单元 6：LED 2 和 4 亮起。
- 单元 7：LED 3 和 4 亮起。
- 单元 8：LED 1、3 和 4 亮起。

堆叠拓扑

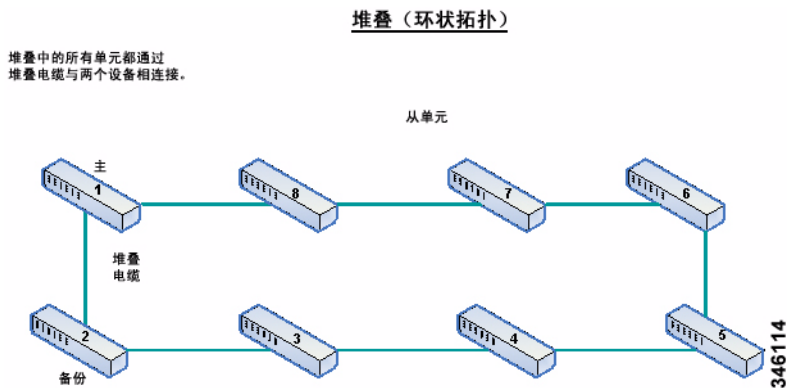
堆叠拓扑类型

堆叠中的单元可以通过以下其中一种拓扑类型进行连接：

链状拓扑 - 第一个单元的一个堆叠端口（可以在左侧，也可以在右侧）连接至第二个单元中的堆叠端口。除第一个和最后一个单元之外，堆叠中的所有单元都连接至下一个单元的堆叠端口。“堆叠架构（链状拓扑）”展示了链状拓扑。

环状拓扑 - 堆叠中的所有单元以链状连接。最后一个单元与第一个单元首尾相连。下图展示了包含八单元堆叠的环状拓扑。

环状拓扑堆叠



环状拓扑比链状拓扑更加可靠。在环状连接中，一条链路出现故障不会影响堆叠的正常运行，但是，在链状连接中，一条链路出现故障可能会导致堆叠断开。

拓扑发现

堆叠通过一个叫做拓扑发现的流程构建。此流程可通过更改堆叠端口的连接/中断状态触发。

以下是触发此过程的事件示例：

- 将堆叠拓扑从环状更改为链状
- 将两个堆叠合并为单个堆叠
- 断开堆叠
- 将其他从单元插入堆叠，例如，由于单元出现故障，因此之前从该堆叠中断开。在链状拓扑中，如果堆叠中间的单元出现故障，则可能会发生这种情况。

在拓扑发现期间，堆叠中的每个单元都交换数据包，其中包含拓扑信息。
完成拓扑发现流程后，每个单元均包含堆叠中所有单元的堆叠映射信息。

单元 ID 分配

拓扑发现过程完成后，堆叠中的每个单元都分配了一个唯一的单元 ID。
您可以通过以下方式在“系统模式和堆栈管理”页面中设置单元 ID：

- **自动** - 由拓扑发现流程分配单元 ID。此选项为系统默认的设置。
- **手动** - 单元 ID 可手动设置为从 1 到 8 的整数。此外，手动编号还包含以下选项：
 - **1 - 强制主装置** - 强制单元 1 为主装置。
 - **2 - 强制主装置** - 强制单元 2 为主装置。

重复的单元 ID

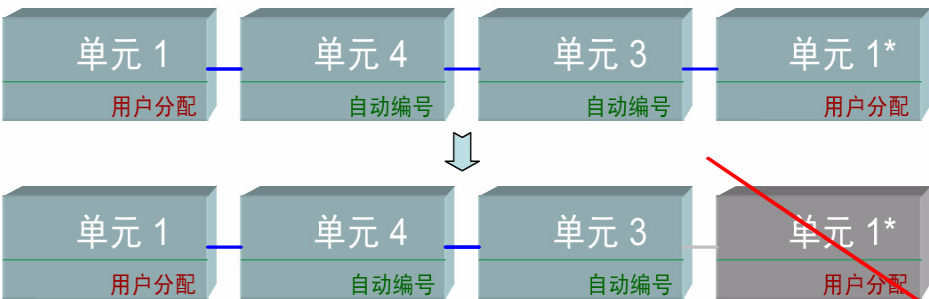
如果您将同一个单元 ID 分配给两个单独的单元，则只有其中一个单元能够使用该单元 ID 加入堆叠。

如果已选择自动编号，则重复的单元将分配一个新的单元编号。如果未选择自动编号，则将关闭重复的单元。

下面的示例显示的是可能出现重复单元 ID 的情况。

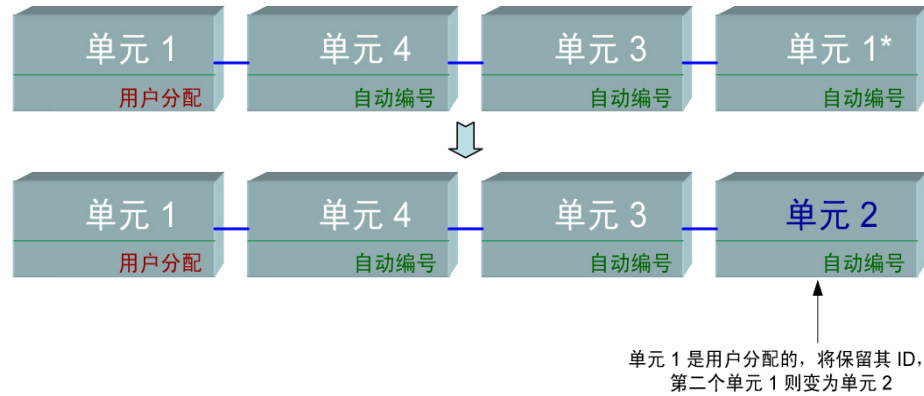
以下显示了两个单元手动分配了同一单元 ID 的情况。单元 1 未加入堆叠且会被关闭。在已启用主装置的单元（1 或 2）间进行的主装置选择流程中，并未选择该单元。

关闭重复的单元



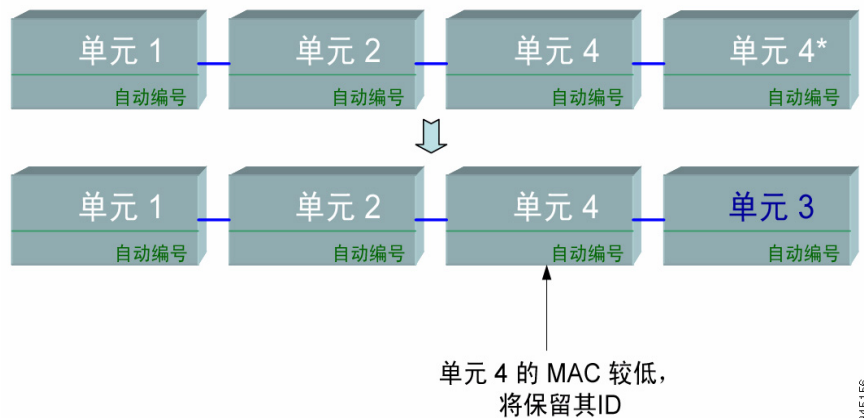
在下面显示的示例中，将其中一个重复的单元（自动编号）重新编号。

将重复的单元重新编号



在下面显示的示例中，将其中一个重复的单元重新编号。MAC 较低的单元将保留其单元 ID（有关此流程说明，请参阅[主装置选择流程](#)）。

两个采用自动编号单元 ID 的单元间出现重复



注 如果新堆叠的单元数量超过最大值 (8)，将关闭所有额外的单元。

主装置选择流程

主单元将在已启用主装置的单元（1 或 2）中进行选择。选择主单元时考虑的因素主要有以下这些：

- **强制主装置** - 如果某单元上已激活强制主装置，则将选择该单元。

- **系统运行时间** - 已启用主装置的单元交换运行时间，以 10 分钟的分段数来衡量该时间。选择分段数较高的单元。如果两个单元的时间分段数值相同，且其中一个单元的单元 ID 为手动设置而另一个单元的单元 ID 为自动设置，则选择具有手动定义单元 ID 的单元，否则将选择具有最低单元 ID 的单元。如果两个单元 ID 相同，则选择具有最低 MAC 地址的单元。**注：**在故障切换进程中，当将备用单元选为主装置时，将保留其运行时间。
- **单元 ID** - 如果两个单元的时间分段数值相同，则将选择具有最低单元 ID 的单元。
- **MAC 地址** - 如果两个单元 ID 相同，则选择具有最低 MAC 地址的单元。

注 堆叠若要运行，则必须具有主单元。主单元定义为承担主装置角色的活动单元。在完成主装置选择流程后，该堆叠必须包含单元 1 和/或单元 2。否则，堆叠及其所有单元会部分关闭，而非全部关闭，但将停止流量传输功能。

堆叠更改

本节介绍可导致堆叠更改的各种事件。当出现以下这些情况时，将更改堆叠拓扑：

- 一个或多个单元连接至堆叠和/或从堆叠断开。
- 任何堆叠端口出现链路连接或中断情况。
- 堆叠在环状和链状形式之间切换。

当向堆叠添加或从堆叠移除单元时，将触发拓扑更改、主装置选择流程和/或单元 ID 分配。

连接新单元

当将单元插入堆叠时，将触发堆叠拓扑更改。系统会分配单元 ID（若是自动编号），且由主装置配置单元。

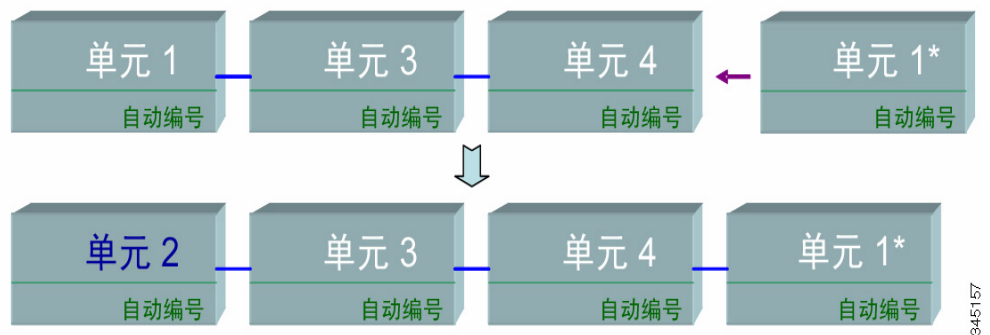
当连接新单元与现有堆叠时，可能出现以下这些情况：

- 不存在重复的单元 ID。
 - 使用用户定义 ID 的单元将保留其单元 ID。
 - 使用自动分配 ID 的单元将保留其单元 ID。
 - 出厂默认单元将自动获得单元 ID，编号从可用的最低 ID 开始。

- 存在一个或多个重复的单元 ID。通过自动编号解决冲突，并分配单元 ID。如果进行手动编号，则只有一个单元能够保留其单元 ID，其余单元将关闭。
- 堆叠中的单元数量超过允许的单元最大数量。将关闭加入堆叠的新单元，并且会生成系统日志消息并显示在主单元中。

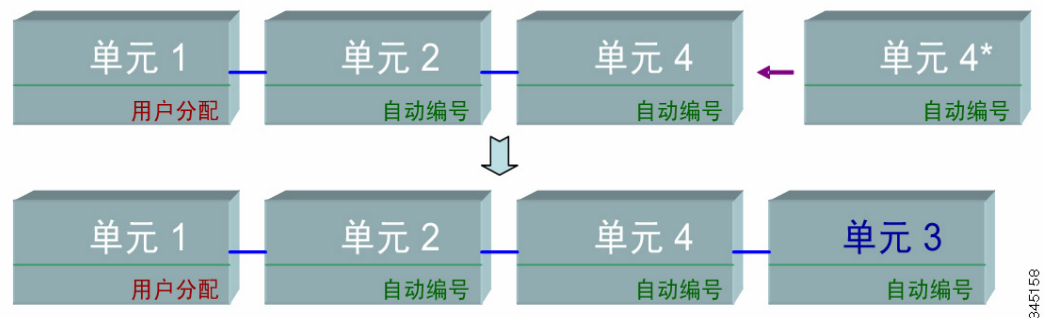
在下面介绍的示例中，当已启用主装置的单元加入堆叠时，会进行自动编号。单元 ID = 1 的单元共有两个。主装置选择流程将选择最佳单元成为主单元。最佳单元即为拥有较长正常运行时间（以 10 分钟的分段数来计算）的单元。另一个单元将作为备用单元。

已启用主装置的自动编号单元



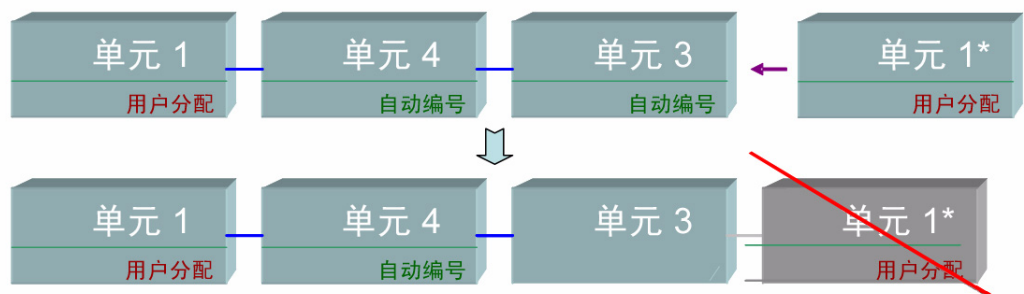
在下面介绍的示例中，当新单元加入堆叠时，会进行自动编号。现有单元将保留其 ID。新单元将获得最低的可用 ID。

自动编号单元



下面介绍了单元 ID 为 1、已启用主装置的用户分配单元加入已存在用户分配单元 ID 为 1 的主单元的堆叠后会发生的状况。新的单元 1 不会加入堆叠，且将关闭。

已启用主装置的用户分配单元



堆疊中的單元故障

主单元故障

如果主装置出现故障，则备用单元将取代主装置，使堆叠继续正常运行。

为了使备用单元能够承担主装置角色，两个单元应始终保持热备用状态。在热备用模式下，主装置及其备用单元与静态配置保持同步（静态配置包含于启动和当前配置文件中）。备用配置文件未同步。备用配置文件依然保留在之前的主装置上。

动态流程状态信息（例如 STP 状态表、动态学习的 MAC 地址、动态学习的智能端口类型、MAC 组播表、LACP 和 GVRP）未同步。

配置主装置时，会立即同步备用单元。命令一执行，即开始进行同步。这是一个透明的过程。

如果将单元插入一个正在运行的堆叠，且将该单元选为备用单元，则主装置将对其进行同步，使之具有最新的配置，然后生成“同步完成系统日志”消息。这是一个独特的系统日志消息，仅当备用装置与主单元合并时才会显示，消息如下所示：

```
%DSYNCH-I-SYNCH SUCCEEDED: 与单元 2 的同步已成功完成。
```

主/备用故障切换

当主装置出现故障或者在设备单元上配置强制主装置时，即会进行故障切换。

备用单元变成主装置，并且系统将初始化其所有流程和协议堆叠，使之负责整个堆叠。因此，此单元暂时不转发流量，但是从单元依然处于活动状态。

注 当使用 STP 且端口处于连接状态时，STP 端口的状态将临时变成“阻塞”，将不能转发流量或学习 MAC 地址。这样可以防止生成树在活动单元间进行循环。

从单元处理

当备用装置成为主装置时，活动从单元将保持活动状态，并根据来自原有主装置的配置继续转发数据包。这样可以最大限度地减少单元中的数据流量中断。

备用单元完成到主装置状态的过渡之后，它会通过执行以下操作逐个初始化从单元：

- 清除从单元的配置，并将其重置为默认配置（以防止获得来自新主单元的错误配置）。因此，从单元上将不转发流量。
- 对从单元应用相关的用户配置。
- 在主装置和从单元间交换动态信息，例如端口 STP 状态、动态 MAC 地址和链路连接/中断状态。在主装置根据 STP 将从单元端口状态设为转发之后，即恢复从单元上的数据包转发。

注 在学习或重新学习数据包的 MAC 地址之前，数据包将泛洪至未知单播 MAC 地址。

故障切换后重新连接原有的主单元

故障切换后，如果原有主装置重新连接，将执行主装置选择流程。如果重新将原有主装置（单元 1）选为主装置，则当前的主装置（单元 2，即原有备用单元）将重启，再次成为备用装置。

注 在主/备用故障切换期间，备用单元会保持运行状态。

堆叠中的软件自动同步

堆叠中的所有单元必须运行相同的软件版本（固件和引导代码）。如果单元和主装置运行的固件和/或引导代码不同，则堆叠中的每个单元将从主单元自动下载固件和引导代码。单元将对自身自动进行重启，以运行新版本。

堆叠单元模式

设备的堆叠单元模式指示它可以是堆叠的一部分还是可以自行运行。

设备可在以下堆叠单元模式下运行：

- **独立式** - 独立式堆叠单元模式下的设备未与任何其他设备连接，且没有堆叠端口。

- **原生堆叠** - 原生堆叠模式下的设备可以与*同类型*的其他设备通过其堆叠端口连接，以组成堆叠。原生堆叠下的所有单元都必须是同种类型（全部是 Sx500、全部是 SG500X/ESW2-550X 或全部是 SG500XG）。
- **基本混合** - 基本混合模式下的设备可连接至 Sx500 和 SG500X/ESW2-550X 设备以形成堆叠。唯一的限制（这也是此模式被称为基本混合而非高级混合的原因）是不支持 VRRP 或 RIP。在此模式下，即使堆叠主装置为 SG500X/ESW2-550X，由于功能集与 Sx500 相同，GUI 将显示 Sx500 的页面。

在此模式中，任何类型的设备均可承担主装置/备用装置角色。只有 5G 堆叠端口才能用作堆叠端口。

- **高级混合** - 高级混合模式下的设备可连接至 Sx500 和 SG500X/ESW2-550X 设备以形成堆叠。在此模式下，由于仅 SG500X 或 ESW2-550X 设备可用作主装置/备用装置，因此，VRRP 和/或 RIP 可受支持，但单元的自动编号不受支持。

Sx500 设备只能作为从装置，因此最多可将 6 个 Sx500 单元和 2 个 SG500X/ESW2-550X 设备堆叠在一起。

- **高级混合 XG** - 高级混合 XG 模式下的设备可连接至 SG500X/ESW2-550X 和 SG500XG 设备以形成堆叠。

所有单元都可用作主单元或从单元。

堆叠配置选项

以下描述的是一些典型的堆叠配置：

可能的堆叠配置	可能的 RIP/ VRRP 支持	堆叠端口速度
堆叠全部由处于原生堆叠模式的 SG500X 组成。	已启用 / 已禁用	1G/10G 或 1G/5G
堆叠全部由处于原生堆叠模式的 ESW2-550X 组成。	已启用 / 已禁用	1G/10G 或 1G/5G
堆叠全部由处于原生堆叠模式的 Sx500 组成。	不支持。	1G/5G（默认端口） 或 1G 铜质 /SFP（组合端口）

可能的堆叠配置	可能的 RIP/ VRRP 支持	堆叠端口速度
堆叠由处于基本混合模式的混合设备类型组成。 ▪ 主单元： SG500X、 ESW2-550X 或 Sx500 ▪ 备用单元： 两种类型的设备皆可 ▪ 从单元： 两种类型的设备皆可	不支持。	1G/5G
堆叠由处于高级混合模式的混合设备类型组成。 ▪ 主单元： SG500X ▪ 备用单元： SG500X ▪ 从单元： 两种类型的设备皆可	已启用 / 已禁用	1G/5G
堆叠由处于高级混合 XG 模式的混合设备类型组成。 ▪ 主单元： SG500X/ESW2-550X 或 SG500XG ▪ 备用单元： SG500X/ESW2-550X 或 SG500XG ▪ 从单元： 两种类型的设备皆可	已启用 / 已禁用	1G 或 10G

堆叠中堆叠单元模式的一致性

堆叠中的所有单元必须处于相同的堆叠单元模式。

堆叠初始化时，会运行可收集堆叠单元上的信息的拓扑发现算法。

选择一个单元作为主装置后，如果某邻居所处的堆叠单元模式不同，该单元可以拒接该邻居加入堆叠的请求。由于堆叠单元模式不同而拒绝单元时，该单元将逻辑关闭（端口不能发送/接收流量），且其所有的 LED（系统、风扇、单元 ID、网络端口和堆叠端口 LED）将会亮起。有关堆叠单元模式的信息将在主单元中显示为系统日志错误。

注意，将单元从此模式中恢复的唯一方法是拔掉其电源并重新接通电源。

更改堆叠单元模式

更改设备的堆叠单元模式后，可将其从堆叠中移除（通过将堆叠单元模式更改为独立式），或将其配置为某堆叠的一部分（通过将堆叠单元模式更改为原生堆叠、基本混合堆叠或高级混合堆叠）。

以下各节介绍了堆叠单元模式更改时，设备重启后的系统模式和配置。

重启后的系统模式（500 设备）

更改设备的堆叠模式后，重启后设备的系统模式可能已更改：

- **Sx500 设备** - 备用和从 Sx500 单元的系统模式（第 2 层或第 3 层）取自自己启用主装置的单元。如果重启前未特别设置系统模式，重启后为第 2 层模式（这是默认设置）。如果希望重启后设备处于第 3 层模式，必须在重启前特别设置。
- **SG500X/ESW2-550X 设备** - 如果设备处于独立式或原生堆叠模式，则其系统模式始终为第 2 层和第 3 层。当设备处于基本或高级混合模式时，其运行方式如上文的 Sx500 设备部分所述。当设备处于高级混合 XG 模式时，其系统模式始终为第 2 层和第 3 层。
- **SG500XG 设备** - 始终为第 2 层和第 3 层。

重启后的配置

更改设备的堆叠模式并重启设备时，启动配置文件通常会被**移除**，这是因为它可能包含不适用于新模式的配置信息。

在以下情况下启动后会保留启动配置文件：

- **SG500X/ESW2-550X 设备：**
 - **独立式到原生堆叠** - 仅当强制单元作为主单元（单元 ID = 1）时才会保留
 - **基本混合到高级混合** - 仅当强制单元作为主单元（单元 ID = 1）时才会保留
 - **基本混合到高级混合 XG** - 仅当强制单元作为主单元（单元 ID = 1）时才会保留
- **SG500XG：**
 - **独立式到原生堆叠** - 仅当强制单元作为主单元（单元 ID = 1）时才会保留
 - **原生到高级混合 XG** - 仅当强制单元作为主单元（单元 ID = 1）时才会保留
- **Sx500 设备：**
 - **独立式到原生堆叠** - 仅当强制单元作为主单元（单元 ID = 1）时才会保留

- **独立式到基本混合** - 仅当强制单元作为主单元（单元 ID = 1）时才会保留
- **原生堆叠到基本混合** - 仅当强制单元作为主单元（单元 ID = 1）时才会保留

堆叠端口

堆叠中的端口必须为以下端口类型之一：

- **网络端口** - 也称为上行端口。这些端口与网络连接。
- **堆栈端口** - 用于连接堆叠中两个单元的端口。堆叠端口用于在单元之间传输数据和协议数据包。

您必须向系统指明（保留）计划将哪些端口用作堆叠端口（在“系统模式和堆栈管理页面”）。将所有未保留为堆叠端口的端口都视为网络端口。

默认堆叠和网络端口

以下是默认堆叠和网络端口：

- **Sx500 设备** - 当 Sx500 设备在原生堆叠模式下运行时，默认情况下 S1-S2-1G 将作为常规网络端口运行，而 S3-S4-5G 则作为堆叠端口运行。
- **SG500X/ESW2-550X 设备** - 在默认情况下，S1-S2-10G 是堆叠端口。您可以手动将 S1-S2-10G 和 S1-S2-5G 重新配置为网络端口或堆叠端口。
- **SG500XG 设备** - 任意端口都可以为堆叠或网络端口。默认情况下，设备为独立式。

将设备从一种堆叠模式转换为独立式模式时，其所有的堆叠端口都将自动变为常规网络端口。

端口对

下表介绍了处于各种堆叠单元模式的设备上可用的端口对。

设备类型 / 端口对	堆叠	独立式
Sx500 S3-S4 5G 堆叠	- 原生堆叠模式：可用作网络 and 堆叠端口 - 混合模式：可用作堆叠端口	可用作网络端口
Sx500 组合插槽 1G 光纤 / 铜缆 S1-S2 1G 堆叠	- 原生堆叠模式：可用作网络 and 堆叠端口 - 混合模式：可用作网络端口	可用作网络端口
SG500X/ESW2-550X S1-S2 5G 堆叠 S1-S2 10G 堆叠	- 原生堆叠模式：5G 插槽或 10G 插槽可用。 - 混合模式：仅 5G 插槽可用。	只能用作 10G 插槽
SG500XG XG1- XG16 端口。 为 10G 插槽。	- 原生堆叠模式：1G 或 10G 端口可用。 - 混合模式：1G 或 10G 端口可用。	可用作网络端口

端口速度

堆叠端口的速度可手动设置，也可设置为自动选择。下表介绍了可能的堆叠端口类型及其在各种设备上的速度：

设备类型	端口对	在堆栈中的可能速度	是否提供自动速度选择功能
Sx500	S1-S2	1G	否
Sx500	S3-S4	5G/1G	是
SG500X/ ESW2-550X	S1-S2-XG	10G/1G	是
SG500X/ ESW2-550X	S1-S2-5G	5G/1G	是
SG500XG	XG1 - XG16 的任意端口对	1G 或 10G	是

端口速度的自动选择

您可以将堆叠电缆类型设置为在连接到端口时自动被发现（自动发现为默认设置）。系统会自动识别堆叠电缆类型并选择电缆和端口支持的最高速度。

未识别出电缆类型时，将显示要求用户手动配置端口速度的系统日志消息（报告级别）。

连接单元

只有当链路两端的端口速度相同时，堆叠中的两个单元才可以连接。可以通过将堆叠端口速度配置为以下模式来实现：

- 自动速度模式
- 每个连接端的速度相同

电缆类型

每种类型的堆叠端口都可与特定类型的电缆一起使用。

堆叠模式设置为原生堆叠时，可以使用光纤或铜质电缆作为堆叠电缆。如果同时连接了这两种电缆（光纤和铜缆），光纤为首选介质。双连接可用于冗余。介质更改（例如，断开光纤堆叠电缆的连接，且铜缆堆叠电缆处于活动状态）后，系统将启动拓扑更改事件。

下表介绍了可能的电缆类型和端口组合。

连接器类型	堆叠端口			网络端口		
	SG500X/ ESW2-550X 的 S1-S2-5G 以及 Sx500 的 S3-S4	Sx500 中的 S1、S2	SG500X/ ESW2-550X 中的 S1、S2 - XG	S1、S2 - 5G（对于 SG500X） 和 S3、S4 （对于 Sx500）	Sx500 中 的 S1、S2	SG500X 中的 S1、 S2 - XG
思科 SFP-H10GB-CU1M - 无源铜缆	5G	1G	10G	1G	1G	10G
思科 SFP-H10GB-CU3M - 无源铜缆	5G	1G	10G	1G	1G	10G
思科 SFP-H10GB-CU5M - 无源铜缆	5G	1G	10G	1G	1G	10G
思科 SFP-10G-SR	不支持	不支持	10G	不支持	不支持	10G
思科 SFP-10G-LRM	不支持	不支持	10G	不支持	不支持	10G

堆叠端口				网络端口		
连接器类型	SG500X/ ESW2-550X 的 S1-S2-5G 以及 Sx500 的 S3-S4	Sx500 中的 S1、S2	SG500X/ ESW2-550X 中的 S1、S2 - XG	S1、S2 - 5G (对于 SG500X) 和 S3、S4 (对于 Sx500)	Sx500 中 的 S1、S2	SG500X 中的 S1、 S2 - XG
思科 SFP-10G-LR	不支持	不支持	10G	不支持	不支持	10G
1G SFP 模块 MGBSX1	1G	1G	1G	1G	1G	1G
1G SFP 模块 MGBT1	1G	1G	1G	1G	1G	1G
1G SFP 模块 MGBLX1	1G	1G	1G	1G	1G	1G
1G SFP 模块 MGBBX1	1G	1G	1G	1G	1G	1G
100Mbps SFP 模块 MFELX1	不支持	不支持	不支持	不支持	100Mbps	不支持
100Mbps SFP 模块 MFEFX1	不支持	不支持	不支持	不支持	100Mbps	不支持
100Mbps SFP 模块 MFEBX1	不支持	不支持	不支持	不支持	100Mbps	不支持
其他 SFP	1G	根据： 强制用户速度 EEPROM 速度 1G 速度	根据： 强制用户速度 EEPROM 速度 1G 速度	1G	根据： 强制用户 速度 EEPROM 速度 1G 速度	根据： 强制用户 速度 EEPROM 速度 10G 速度

堆叠端口或网络端口	
连接器类型	全部端口
思科 SFP-H10GB-CU1M - 无源铜缆	1G - 10G
思科 SFP-H10GB-CU3M - 无源铜缆	1G - 10G
思科 SFP-H10GB-CU5M - 无源铜缆	1G - 10G
思科 SFP-10G-SR	不支持
思科 SFP-10G-LRM	不支持
思科 SFP-10G-LR	不支持
1G SFP 模块 MGBSX1	1G

堆叠端口或网络端口	
连接器类型	全部端口
1G SFP 模块 MGBT1	1G
1G SFP 模块 MGBLX1	1G
1G SFP 模块 MGBBX1	1G
100Mbps SFP 模块 MFELX1	不支持
100Mbps SFP 模块 MFEFX1	不支持
100Mbps SFP 模块 MFEBX1	不支持
其他 SFP	1G

默认配置

以下是各种堆叠模式下的设备默认设置：

设备类型	堆叠模式	默认堆叠端口	默认系统模式
Sx500	原生堆叠	S3-S4 5G 堆叠	第 2 层
	基本混合	S3-S4 5G 堆叠	第 2 层
	高级混合	S3-S4 5G 堆叠	第 2 层
SG500X/ ESW2- 550X	原生堆叠	S1-S2 10G 堆叠	第 2 层 + 第 3 层
	基本混合	S1-S2 5G 堆叠	第 2 层
	高级混合	S1-S2 5G 堆叠	第 2 层
	高级混合 XG	S1-S2 5G 堆叠	第 2 层
SG500XG	原生堆叠	用户可选择任意对	第 2 层 + 第 3 层
	高级混合 XG	用户可选择任意对	第 2 层 + 第 3 层

与其他功能进行交互

基本混合堆叠模式不支持 RIP 和 VRRP。

系统模式

使用“系统模式和堆栈管理”页面执行以下操作：

- 将设备的堆叠模式更改为独立式。
- 将设备的堆叠模式更改为某种堆叠模式，更改堆叠中所有设备的单元 ID、堆叠端口和堆叠端口的速度。
- 更改独立式设备或堆叠的系统模式（第 2 层/第 3 层）。
- 将队列模式从支持 4 个队列更改为支持 8 个队列，或反过来。

有关这些模式的信息存储在配置文件中，如下所示：

- **配置文件标题** - 包含系统模式和队列模式（即使这些为默认值）。
- **配置文件正文** - 包含配置命令。

系统模式向后兼容性

以下模式已在设备的当前软件版本中得到扩展。在先前软件版本中使用这些功能时必须注意：

- **队列模式** - 此模式可从 4 个 QoS 队列更改为 8 个 QoS 队列。从先前不支持 8 个队列的软件版本进行升级时不会出现问题，因为在当前软件版本中，4 个队列模式为默认队列模式。但是，将队列模式更改为 8 个队列时，必须检查配置并对其进行调整，以满足新队列模式所需的 QoS 要求。重启系统后，对队列模式的更改便会生效。将拒绝与新的队列模式冲突的队列相关配置。
- **堆叠模式** - 堆叠模式进行了扩展，以包含混合堆叠模式。从先前的软件版本进行升级不会出现问题，因为设备将使用现有堆叠模式（原生堆叠模式）进行引导。如果要从在混合堆叠模式中配置的设备将软件降级为不支持混合堆叠的软件版本，请先将设备配置为原生堆叠模式。

系统模式和堆叠管理

配置堆叠的步骤：

步骤 1 单击**管理 > 系统模式和堆叠管理**。

独立式设备或堆叠的运行状态将在**运行状态**区域中显示：

- **堆叠单元模式** - 显示设备的以下值之一：
 - **独立式** - 设备未加入堆叠。
 - **原生堆叠** - 设备所在的堆叠中的所有单元均为同一类型。
 - **基本混合堆叠** - 设备所在的堆叠可同时包含拥有 Sx500 功能集的 SG500X 和 Sx500 设备。
 - **高级混合堆叠** - 设备所在的堆叠可同时包含拥有 SG500X 功能集的 SG500X 和 Sx500 设备。
 - **高级混合堆叠 XG** - 设备所在的堆叠可同时包含拥有 SG500X 功能集的 SG500X/ESW2-550X 和 SG500XG 设备。
- **堆叠拓扑** - 显示堆叠拓扑是链状还是环状。
- **系统模式** - 显示堆叠/独立式设备是在第 2 层、第 3 层还是第 2 层和第 3 层系统模式下运行。
- **堆叠主装置** - 显示堆叠主单元的单元 ID。
- **主装置选择状态** - 显示堆叠主单元的选择方式。请参阅[主装置选择流程](#)。

步骤 2 要在重启后配置系统模式，请选择第 2 层或第 3 层模式。

步骤 3 若要在重启后配置队列模式，请选择是在设备上配置 4 个还是 8 个 QoS 队列。请参阅[配置 QoS 队列](#)。

步骤 4 在**堆栈管理设置表**中配置堆叠中的单元。这些更改将在重启后生效。

注 如果设备是 Sx500，且其堆叠单元模式已从原生堆叠模式更改为独立式，则除非您此时将**系统模式**字段更改为第 3 层，否则，重启后，该设备将处于第 2 层系统模式。

表中将显示堆叠中每个单元的以下运行状态。

- **堆叠单元编号** - 显示已知活动单元的单元 ID。
- **型号名称** - 已知活动单元的型号名称。

- **堆栈连接 1** - 有关第一个堆叠连接的信息：
 - *端口* - 连接的堆叠端口类型。
 - *速度* - 连接的堆叠端口速度。
 - *邻居* - 连接的堆叠单元的单元 ID。

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：

- 设备型号
- 系统设置
- Console 设置（自动波特率支持）
- 管理接口
- 系统模式和堆栈管理
- 用户帐户
- 定义空闲会话超时
- 时间设置
- 系统日志
- 文件管理
- 路由资源
- 健康状况
- 诊断
- 发现 - Bonjour
- 发现 - LLDP
- 发现 - CDP
- Ping
- Traceroute

设备型号

所有型号均可通过基于 Web 的交换机配置实用程序进行全面管理。

注 使用“系统模式和堆栈管理”页面，可以将每种型号都设置为在第 3 层系统模式下工作。

当设备在第 3 层系统模式下运行时，VLAN 速率限制和 QoS 策略器将无法运行。其他 QoS 高级模式功能可正常工作。

只有 SG500X/SG500XG/ESW2-550X 型号支持虚拟路由器冗余协议 (VRRP) 和路由信息协议 (RIP)。

注 将使用以下端口约定：

- GE 用于表示千兆以太网 (10/100/1000) 端口。
- FE 用于表示快速以太网 (10/100) 端口。
- XG 用于表示万兆以太网端口。

下表介绍了不同型号、设备上的端口数量和类型及其 PoE 信息。

型号名称	产品 ID (PID)	设备上的端口说明	PoE 专用功率	支持 PoE 的端口数
SF500-24	SF500-24-K9	24 端口 10/100M 可堆叠管理型交换机	不适用	不适用
SF500-24P	SF500-24P-K9	24 端口 10/100M PoE 可堆叠管理型交换机	180W	24
SF500-48	SF500-48-K9	48 端口 10/100M 可堆叠管理型交换机	不适用	不适用
SF500-48P	SF500-48P-K9	48 端口 10/100M PoE 可堆叠管理型交换机	375W	48
SG500-28	SG5000-28-K9	28 端口千兆可堆叠管理型交换机	不适用	不适用
SG500-28MPP	SG500-28MPP-K9	28 端口千兆 PoE 管理型交换机	740W	24
SG500-28P	SG500-28P-K9	28 端口千兆 PoE 可堆叠管理型交换机	180W	24
SG500-52	SG500-52-K9	52 端口千兆可堆叠管理型交换机	不适用	不适用
SG500-52MP	SG500-52MP-K9	52 端口千兆最大 PoE 管理型交换机	740W	48
SG500-52P	SG500-52P-K9	52 端口千兆 PoE 可堆叠管理型交换机	375W	48
SG500X-24	SG500X-24-K9	24 端口千兆与 4 端口 10 千兆可堆叠管理型交换机	不适用	不适用

型号名称	产品 ID (PID)	设备上的端口说明	PoE 专用功率	支持 PoE 的端口数
SG500X-24P	SG500X-24P-K9	24 端口千兆与 4 端口 10 千兆 PoE 可堆叠管理型交换机	375W	24
SG500X-48	SG500X-48-K9	48 端口千兆与 4 端口 10 千兆可堆叠管理型交换机	不适用	不适用
SG500X-48P	SG500X-48P-K9	48 端口千兆与 4 端口 10 千兆 PoE 可堆叠管理型交换机	375W	48
ESW2-550X-48	ESW2-550X-48-K9	48 端口千兆与 4 端口 10 千兆可堆叠管理型交换机	不适用	不适用
ESW2-550X-48DC	ESW2-550X-48DC-K9	48 端口千兆与 4 端口 10 千兆可堆叠管理型交换机	不适用	不适用
SG500XG-8F8T	SG500XG-8F8T-K9	16 端口 10 千兆可堆叠管理型交换机	不适用	不适用

系统设置

“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 状态以及其他项目。

显示系统摘要

若要查看系统信息，请单击**状态和统计信息 > 系统摘要**。

“系统摘要”页面包含系统和硬件信息。

系统信息：

- **基本 MAC 地址** - 设备 MAC 地址。如果系统处于堆叠模式，将显示主单元的基本 MAC 地址。

注 如果系统处于“原生堆叠”模式，显示的固件版本号将以主装置的版本为依据。

- **固件版本 (非活动)** - 非活动映像的固件版本号。如果系统处于“原生堆叠”模式，则会显示主单元的版本。
- **系统堆叠模式** - 显示设备是否是堆叠（**原生堆叠或独立式**）的一部分。可能的选项有：

- **系统运行模式** - 指定系统是在第 2 层还是第 3 层系统模式下运行（适用于 500 设备）。
- **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。如果系统处于堆叠模式，将显示主单元的基本 MAC 地址。
- **巨型帧** - 巨型帧支持状态。可以使用“端口管理”菜单的“端口设置”页面启用或禁用此支持。

注 巨型帧支持仅在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）** - 活动映像的固件版本号。
注 如果系统处于堆叠模式（“原生堆叠”模式），显示的固件版本号将以主装置的版本为依据。有关堆叠模式的详情，请参阅[堆叠单元模式](#)一节。
- **固件 MD5 校验和（活动映像）** - 活动映像的 MD5 校验和。
- **固件版本（非活动映像）** - 非活动映像的固件版本号。如果系统处于堆叠模式，则会显示主单元的版本。
- **固件 MD5 校验和（非活动映像）** - 非活动映像的 MD5 校验和。
- **启动版本** - 启动版本号。
- **启动 MD5 校验和** - 启动版本的 MD5 校验和。
- **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:

- **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 PoE 电源信息:

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

主单元的 PoE 电源信息旁边有一个 [详情](#) 链接，单击该链接，您可以直接转至“端口管理 > PoE > 属性”页面。此页面按单元显示 PoE 电源信息。

堆叠中的单元会以图表形式显示，并且会针对每个单元显示以下信息：

- **主单元的单元 ID**
- **型号说明** - 设备型号说明。
- **序列号** - 序列号。
- **PID VID** - 部件编号和版本 ID。

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** - 输入设备实际所在的位置。
- **系统联系人** - 输入联系人姓名。

- **主机名** - 选择此设备的主机名。在 CLI 命令的提示符中会使用此主机名：
 - **使用默认设置** - 这些交换机的默认主机名（系统名称）为：*switch123456*，其中 123456 代表设备 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（Console、Telnet 和 SSH）激活该横幅。

步骤 3 单击**应用**，在当前配置文件中保存这些值。

Console 设置（自动波特率支持）

可以将 Console 端口速度设置为以下速度之一：4800、9600、19200、38400、57600 和 115200，或者设置为“自动检测”。

自动检测可使设备自动检测您的 Console 速度，如此一来，您便无需明确设置此值。

如果未启用自动检测，系统会将 Console 端口速度自动设置为上次手动设置的速度（默认为 115,200）。

如果已启用自动检测但尚未发现 Console 波特率，系统会使用速度 115,200 来显示文本（例如，启动信息）。

在“Console 设置”页面中启用自动检测后，可以通过将 Console 连接到设备来进行激活，然后按两次 Enter 键。设备将自动检测波特率。

启用自动检测或手动设置 Console 波特率的步骤：

步骤 1 单击**管理 > Console 设置**。

步骤 2 请选择以下选项之一：

- **自动检测** - 自动检测 Console 波特率。
- **静态** - 请从提供的速度中选择其中之一。

管理接口

请参阅 [IPv4 管理和接口](#)。

系统模式和堆栈管理

请参阅 [管理：堆栈管理](#)。

用户帐户

请参阅 [定义用户](#)。

定义空闲会话超时

*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**
- **Console 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

请参阅[管理：系统日志](#)。

文件管理

请参阅[管理：文件管理](#)。

重启设备

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。

可以使用 [管理 > 文件管理 > 保存/复制配置](#) 或单击窗口顶部的**保存**来备份配置。也可以从远程设备上传配置。请参阅[下载/备份配置/日志](#)一节。

在某些情况下，您可能想要为将来某段时间设置重启时间。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恢复与远程设备的连接。如果这些操作成功，则可以取消延迟重启。
- 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 单击任何一个**重启**按钮来重启设备。

- **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。

可能的选项有：

- **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。如果您指定月和日，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。

- **在** - 在指定的小时和分钟数之内重启。最长时间为 24 天。

- **使用出厂默认设置重启** - 使用出厂默认配置重启设备。此过程会擦除启动配置文件和备份配置文件。

堆叠单元 ID 将设置为自动，且在 Sx500 中，系统模式将设置为第 2 层。

恢复出厂默认设置时，不会删除镜像配置文件。

- **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。

注 如果设备处于“原生堆叠”模式，使用此按钮可恢复整个堆叠上的出厂默认设置。

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

路由资源

在 Sx500 和 SG500X/ESW2-550X 设备中，对 TCAM 分配的处理方式是不同的。Sx500 拥有单个 TCAM，可用于所有路由和 ACL 规则。SG500X/SG500XG/ESW2-550X 设备拥有两个 TCAM；一个 TCAM 专用于路由，另一个专用于 ACL 规则。

当 SG500X/ESW2-550X 设备处于混合堆叠模式时，仅拥有单个 TCAM（正如 Sx500 设备一样）。请参阅[堆叠单元模式](#)。

TCAM 条目可分为以下几组：

- **IP 条目** - 保留用于 IP 静态路由、IP 接口和 IP 主机的 TCAM 条目。
- **非 IP 条目** - 保留用于 ACL 规则、CoS 策略器和 VLAN 速率限制等其他应用的 TCAM 条目。

如果设备启用了 IPv4 路由，请参见下表了解各种功能所用的 TCAM 条目数：

逻辑实体	IPv4
IP 邻居	1 个条目
接口上的 IP 地址	2 个条目
IP 远程路由	1 个条目

如果设备启用了 IPv6 路由，请参见下表了解各种功能所用的 TCAM 条目数：

逻辑实体	IPv4	IPv6 (PCL TCAM)	IPv6（路由器 TCAM）
IP 邻居	1 个条目	1 个条目	4 个条目
接口上的 IP 地址	2 个条目	2 个条目	8 个条目
IP 远程路由	1 个条目	1 个条目	4 个条目
On-Link-Prefix		1 个条目	4 个条目

使用“路由器资源”页面可调整 TCAM 分配。

如果您错误地更改 TCAM 分配，将显示一条错误消息。如果您的 TCAM 分配可行，将显示一条消息，说明将执行自动重启，使用新设置。可能会错误修改路由器资源，有以下几种可能情况：

- 您分配的 TCAM 条目数量少于当前使用的条目数量。
- 您分配的 TCAM 条目数量超过该类别可用的最大值（最大值会显示在页面上）。

查看和修改路由器资源的步骤：

步骤 1 单击**管理 > 路由器资源**。

对于 IPv4 路由，将显示以下字段：

- **邻居 - 计数**是设备中记录的邻居的数量，**TCAM 条目数**是用于这些邻居的 TCAM 条目的数量。
- **接口 - 计数**是设备接口中的 IP 地址的数量，**TCAM 条目数**是用于 IP 地址的 TCAM 条目数量。
- **路由 - 计数**是设备中记录的路由的数量，**TCAM 条目数**是用于路由的 TCAM 条目的数量。
- **总数** - 显示当前正在使用的 TCAM 条目的数量。
- **最大条目数** - 请选择以下选项之一：
 - *使用默认设置* - 在 Sx500 中，TCAM 条目数量是 TCAM 大小的 25%。在 SG500X/SG500XG 中，路由器 TCAM 条目数量是路由器 TCAM 大小的 50%。
 - *用户定义* - 输入一个值。

对于 IPv6 路由，将显示以下字段：

- **邻居 - 计数**是设备中记录的邻居的数量，**TCAM 条目数**是用于这些邻居的 TCAM 条目的数量。
- **接口 - 计数**是设备接口中的 IP 地址的数量，**TCAM 条目数**是用于 IP 地址的 TCAM 条目数量。
- **链路前缀上 - 计数**是设备中定义的前缀数量，**TCAM 条目数**是用于前缀的 TCAM 条目的数量。
- **路由 - 计数**是设备中记录的路由的数量，**TCAM 条目数**是用于路由的 TCAM 条目的数量。
- **总数** - 显示当前正在使用的 TCAM 条目的数量。
- **最大条目数** - 请选择以下选项之一：
 - *使用默认设置* - 在 Sx500 中，TCAM 条目数量是 TCAM 大小的 25%。在 SG500X/SG500XG 中，路由器 TCAM 条目数量是路由器 TCAM 大小的 50%。
 - *用户定义* - 输入一个值。

步骤 2 单击**应用**以保存新设置。这可检查路由器资源设置的可行性。如果不正确，将显示一条错误消息。如果正确，设置将复制到当前配置文件中。

注 此页面底部将显示实际正在使用和可用的 TCAM 条目的摘要。有关这些字段的说明，请参阅[查看 TCAM 利用率](#)。

步骤 3 单击**应用**以保存新设置。这可检查 TCAM 分配的可行性。如果不正确，将显示一条错误消息。如果正确，该分配将保存到当前配置文件中，并将执行重启。

健康状况

“状况”页面监控配备风扇的所有设备上的风扇状态。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。

在安装有温度传感器的设备中，为在设备硬件过热时提供保护，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 Warning 阈值	会生成以下信息： ▪ 系统日志消息 ▪ SNMP Trap
至少有一个温度传感器超出 Critical 阈值	会生成以下信息： ▪ 系统日志消息 ▪ SNMP Trap 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 Critical 温度两分钟时，将关闭所有端口。 ▪ （在支持 PoE 的设备中）禁用 PoE 电路，以减少功耗和释放的热量。

事件	操作
超出 Critical 阈值后的冷却期 (所有传感器都比 Warning 阈值至少低 2 °C)。	所有传感器均冷却到比 Warning 阈值至少低 2 °C 后， 将重新启用 PHY，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 的设备中) PoE 电路将启用。

要查看设备状况参数，请单击**状态和统计信息 > 状况**。

如果设备处于独立式模式，将显示以下字段：

- **风扇状态** - 风扇状态。可能的值如下所示：
 - 正常 - 风扇运转正常。
 - 失败 - 风扇无法正常运转。
 - 无 - 风扇不适用于特定型号。
- **风扇方向** - 风扇转动的方向。

如果设备处于原生堆叠模式，“状况”页面将显示每个设备的以下字段：

- **单元** - 单元编号。
- **风扇状态** - 风扇状态。有 4 列可供显示风扇状态，但是只能显示特定设备型号上的风扇的信息。可能的值如下所示：
 - 正常 - 风扇运转正常。
 - 失败 - 风扇无法正常运转。
 - 无 - 风扇 ID 不适用于特定型号。
- **风扇方向** - 风扇转动的方向。

诊断

请参阅**管理：诊断**。

发现 - Bonjour

请参阅 [Bonjour](#)。

发现 - LLDP

请参阅 [配置 LLDP](#)。

发现 - CDP

请参阅 [配置 CDP](#)。

Ping

Ping 是一种实用程序，用来测试是否可以访问远程主机，并测量从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) 回显请求数据包并等待 ICMP 响应来运行，有时称为 pong。它可以测量往返时间并记录任何数据包丢失。

Ping 主机的步骤：

步骤 1 单击 **管理 > Ping**。

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 接口** - 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** - 选择“链路本地”或“全局”作为要输入的目的 IP 地址的类型。
 - **链路本地** - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
 - **全局** - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。
- **链路本地接口** - 如果 IPv6 地址类型为“链路本地”，请选择接收的来源。
- **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。将会显示 Ping 状态，并且消息列表中会添加另一条消息，来显示 Ping 操作的结果。

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

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 路径。Traceroute 页面将显示设备和目标主机间的每一步跳以及到每一步跳处的往返时间。

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 接口** - 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。

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** - 选择“链路本地”或“全局”作为要输入的 IPv6 地址类型。
 - **链路本地** - IPv6 地址唯一识别单条网络链路上的主机。链路本地地址具有前缀 **FE80**，无法路由，并且只能用于本地网络上的通信。仅支持一个链路本地地址。如果接口上存在链路本地地址，此条目会替换配置中的地址。
 - **全局** - IPv6 地址为全局单播 IPV6 类型，可从其他网络看到和访问。
- **链路本地接口** - 如果 IPv6 地址类型为“链路本地”，请选择接收的来源。
- **主机 IP 地址/名称** - 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。当达到目的地或达到此值时，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旅程的往返时间 (RTT) 和状态：

- **索引** - 显示步跳的次数。
- **主机** - 显示路由至目的地的一个停止。
- **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。

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：

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

系统时间选项

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

作为启动过程的一部分，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** - 您必须手动设置时间。

- **通过 PC** - 可以使用浏览器信息通过 PC 接收时间。

来自计算机的时间配置将保存到目前配置文件。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。

配置系统时间

选择系统时间源

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



注意

如果系统时间为手动设置并且重启设备，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**。

此时将显示以下字段：

- **实际时间 (静态)** - 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** - 上次从其获取时间的 SNTP 服务器的地址、层级和类型。

步骤 2 输入以下参数：

时钟源设置 - 选择用于设置系统时钟的时钟源。

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

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

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

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

时区设置 - 通过 DHCP 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，**还必须在设备上启用 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** - 输入表示已配置时区的用户定义名称。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。输入以下参数：
- *循环* - 每年在同一天开始实行 DST。

选择 *按日期* 可以自定义 DST 的开始时间和结束时间：

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

选择 *循环* 可以使用其他方法自定义 DST 的开始时间和结束时间：

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

步骤 3 单击 **应用**。系统时间值将写入当前配置文件。

添加单播 SNTP 服务器

最多可配置 16 台单播 SNTP 服务器。

注 要按名称指定单播 SNTP 服务器，必须先要在设备上配置 DNS 服务器（请参阅 **DNS 设置**）。为添加单播 SNTP 服务器，请选中此框以启用 **SNTP 客户端单播**。

添加单播 SNTP 服务器的步骤：

步骤 1 单击**管理 > 时间设置 > SNTP 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：
 - *启用* - SNTP 服务器目前正常运行。
 - *禁用* - SNTP 服务器目前不可用。
 - *未知* - 目前设备正在搜索 SNTP 服务器。
 - *正在进行* - SNTP 服务器尚未完全信任其自有时间服务器时（例如首次启动 SNTP 服务器时），会发生这种情况。
- **最近响应** - 上次从该 SNTP 服务器收到响应的日期和时间。
- **偏移** - 服务器时钟相对于本地时钟的预计偏差（以毫秒为单位）。主机使用 RFC 2030 中介绍的算法确定此偏差的值。
- **延迟** - 沿服务器时钟与本地时钟之间的网络路径，服务器时钟相对于本地时钟的预计往返延迟。主机使用 RFC 2030 中介绍的算法确定此延迟的值。

- **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**。

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 Internet 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** - 输入 SNTP 服务器的 IP 地址。格式取决于所选的地址类型。
- **SNTP 服务器** - 从已知 NTP 服务器列表中选择 SNTP 服务器的名称。如果选择**其他**，请在旁边的字段中输入 SNTP 服务器名称。
- **轮询间隔** - 选择该选项将启用针对系统时间信息对 SNTP 服务器的轮询。将会对注册供轮询的所有 NTP 服务器进行轮询，并将从所能访问的层级（距参考时钟的距离）最低的服务器选择时钟。具有最低层级的服务器将被视为主服务器。具有次低层级的服务器为次服务器，以此类推。如果主服务器出现故障，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**。将添加 STNP 服务器，并返回主页。

配置 SNTP 模式

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**。

步骤 2 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 3 如果系统处于第 3 层模式下，请单击**添加**，以选择用于 SNTP 接收/传输的接口。

选择一个接口，然后选择接收/传输选项。

步骤 4 单击**应用**，以将设置保存到当前配置文件中。

定义 SNTP 验证

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

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

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

工作流程

步骤 1 在“SNTP 验证”页面中启用验证功能。

步骤 2 在“SNTP 验证”页面中创建一个密钥。

步骤 3 在“SNTP 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** - 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
- 802.1X 端口验证
- 端口状态
- 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与该时间范围相关联的程序。达到任何一个时间范围后都会禁用该程序。

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（请参阅第 10 章，“配置端口”和第 10 章，“配置 LAG 设置”）
- 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 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。

管理： 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：

- [测试铜缆端口](#)
- [显示光纤模块状态](#)
- [配置端口和 VLAN 镜像](#)
- [查看 CPU 使用率和安全的核心技术](#)

测试铜缆端口

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

VCT 执行两种测试：

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

运行铜缆端口测试的前提条件

运行该测试之前，请执行以下操作：

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

使用 VCT 测试电缆时，会使用一条 CAT5 数据电缆。

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

**注意**

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

测试连接到端口的铜质电缆的步骤：

- 步骤 1** 单击 **管理 > 诊断 > 铜缆测试**。
- 步骤 2** 选择要进行铜缆测试的端口。
- 步骤 3** 单击 **铜缆测试**。
- 步骤 4** 当显示该消息时，单击**确定**确认链路可以中断，或单击**取消**中止测试。

在“测试结果”框中将显示以下字段：

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

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

- **电缆长度**：提供长度的估计值。
- **对** - 所测试的电缆对。
- **状态** - 线对状态。红色表示发生故障，绿色表示状态良好。
- **通道** - 电缆通道表示该线缆是直通电缆还是交叉电缆。

- **极性** - 指示是否为线对激活了自动极性检测和更正。
- **对间偏移** - 线对间延迟的差异。

注 当端口速度为每秒 10 Mbit，不能执行 TDR 测试。

显示光纤模块状态

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

MSA 兼容 SFP

支持以下 FE SFP (100 Mbps) 收发器：

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

支持以下 GE SFP (1000 Mbps) 收发器：

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

要查看光纤测试的结果，请单击 **管理 > 诊断 > 光纤模块状态**。

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 在工作。值为 “True” 和 “False”。

配置端口和 VLAN 镜像

在网络设备上，可使用端口镜像将一个设备端口、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网络应用（例如入侵检测系统）。连接到监控端口的网络分析器会处理用于进行诊断、调试和性能监控的数据包。最多可以镜像八个源。这可以是八个独立端口和/或 VLAN 的任意组合。

最多可以镜像八个源。

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

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。

VLAN 镜像在非手动创建的 VLAN 上无效。例如，如果 VLAN 23 由 GVRP 创建，而您手动创建 VLAN 34，则可以创建包括 VLAN 23、VLAN 34 或这两者的端口镜像，随后删除 VLAN 34，则端口镜像中的状态将被设置为**未就绪**，因为 VLAN34 已不在数据库中，而 VLAN 23 不是手动创建的。

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

启用镜像的步骤：

步骤 1 单击**管理 > 诊断 > 端口和 VLAN 镜像**。

此时将显示以下字段：

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

步骤 2 单击**添加**添加要镜像的端口或 VLAN。

步骤 3 输入参数：

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

步骤 4 单击**应用**。端口镜像将添加到当前配置。

查看 CPU 使用率和安全的核心技术

本节介绍了安全的核心技术 (SCT) 以及如何查看 CPU 使用情况。

除终端用户流量之外，设备还处理以下类型的流量：

- 管理流量
- 协议流量
- Snooping 流量

过多的流量会使 CPU 不堪重负，并可能影响正常的设备运行。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 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 **管理 > 诊断 > CPU 使用率**。

将显示 “CPU 使用率” 页面。

“CPU 输入速率” 字段将显示每秒向 CPU 输入帧的速率。

该窗口包含 CPU 使用率图表。Y 轴表示占用百分比，X 轴为样本号。

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

管理：发现协议

本节提供了有关配置发现的信息。

其中包含以下主题：

- [Bonjour](#)
- [LLDP 和 CDP](#)
- [配置 LLDP](#)
- [配置 CDP](#)

Bonjour

作为 Bonjour 客户端，设备会定期将 Bonjour 发现协议数据包广播给直接连接的 IP 子网，以通告它的存在以及它所提供的服务，例如 HTTP、HTTPS 和 Telnet。（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，管理 VLAN 上已启用 Bonjour。Bonjour Console 会自动检测并显示该设备。

第 2 层系统模式下的 Bonjour

当设备处于第 2 层系统模式时，会在全局启用 Bonjour 发现，但无法针对每个端口或每个 VLAN 启用它。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 组播组地址”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。

当系统处于第 2 层系统模式时全局启用 Bonjour 的步骤：

-
- 步骤 1** 单击**管理 > 发现 - Bonjour**。
 - 步骤 2** 选择**启用**以在设备上全局启用 Bonjour 发现。
 - 步骤 3** 单击**应用**。将根据您的选择，在设备上启用或禁用 Bonjour。
-

第 3 层系统模式下的 Bonjour

在第 3 层系统模式下，每个接口（VLAN、端口或 LAG）都可分配一个 IP 地址。启用 Bonjour 后，设备便可以在具有 IP 地址的所有接口上发送 Bonjour 发现数据包。可以针对端口和/或 VLAN 单独启用 Bonjour。启用 Bonjour 后，设备便可以将 Bonjour 发现数据包发送到 IP 地址已在 Bonjour 发现协议接口控制表中与 Bonjour 关联的接口。（设备在第 3 层系统模式下运行时，可依次进入 **IP 配置 > 管理与 IP 接口 > IPv4 接口**，以便为各接口配置 IP 地址。）

如果删除了一个接口（例如 VLAN），则系统会发送 Goodbye 数据包，以注销设备正从本地网络中的相邻缓存表通告的服务。Bonjour 发现协议接口控制表显示 IP 地址已与 Bonjour 功能关联的接口。任何 Bonjour 通告只能广播至此表中列出的接口。（请参阅“管理 > 发现协议 - Bonjour”页面上的 Bonjour 发现协议接口控制表。）如果可用服务发生更改，则会通告这些更改，注销关闭的服务并注册打开的服务。如果 IP 地址发生更改，则会通告该更改。

如果禁用 Bonjour，则设备不会发送 Bonjour 发现通告，也不会监听由其他设备发送的 Bonjour 发现通告。

当设备处于第 3 层系统模式时配置 Bonjour 的步骤：

-
- 步骤 1** 单击**管理 > 发现 - Bonjour**。
 - 步骤 2** 选择**启用**以全局启用 Bonjour 发现。
 - 步骤 3** 单击**应用**更新当前配置文件。
 - 步骤 4** 要在某接口上启用 Bonjour，请单击**添加**。
 - 步骤 5** 选择一个接口，然后单击**应用**。

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相互通告自身及其功能。默认情况下，设备会定期向所有接口发送 LLDP/CDP 通告，并按照协议的要求终止和处理入站 LLDP 及 CDP 数据包。LLDP 和 CDP 协议下，通告将在数据包中编码为 TLV（类型、长度、值）。

应用以下 CDP/LLDP 配置说明：

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

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

CDP/LLDP 的操作不受接口 STP 状态的影响。

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

如果端口是镜像目标，则根据 CDP/LLDP，它将被视为处于关闭状态。

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

接收通告。如果不支持 CDP/LLDP 的设备泛洪发送 CDP/LLDP 数据包，支持 CDP/LLDP 的设备可以接收来自多个设备的通告。

配置 LLDP

本节介绍如何配置 LLDP。其中包含以下主题：

- [LLDP 概述](#)
- [设置 LLDP 属性](#)
- [编辑 LLDP 端口设置](#)
- [LLDP MED 网络策略](#)
- [配置 LLDP MED 端口设置](#)
- [显示 LLDP 端口状态](#)
- [显示 LLDP 本地信息](#)
- [显示 LLDP 邻居信息](#)
- [获取 LLDP 统计信息](#)
- [LLDP 过载](#)

LLDP 概述

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

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

LLDP 是一种链路层协议。默认情况下，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。LLDP 配置页面可在**管理 > 发现 LLDP**菜单下打开。

1. 使用“LLDP 属性”页面输入 LLDP 全局参数，如发送 LLDP 更新的时间间隔。
2. 使用“端口设置”页面按端口配置 LLDP。在该页面上，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“智能端口属性”页面中启用 LLDP。
6. 使用“LLDP 过载”页面显示过载信息。

设置 LLDP 属性

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

输入 LLDP 属性的步骤：

步骤 1 单击**管理 > 发现协议 - 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**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 数据包的数量。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。

编辑 LLDP 端口设置

使用“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**，则会在发生拓扑更改时向 SNMP 通知接收者（例如 SNMP 管理系统）发送通知。

在“LLDP 属性”页面的“拓扑更改 SNMP 通知间隔”字段中，可输入发送通知的时间间隔。可使用“SNMP > 通知接收设备 SNMPv1, 2”和/或“SNMP > 通知接收设备 SNMPv3”页面，来定义 SNMP 通知接收者。

- **可用的可选 TLV** - 通过将 TLV 移至**选定的可选 TLV** 列表中，可选择要由设备发布的信息。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。
 - **802.3 链路聚合** - 是否可以聚合链路（与用于传输 LLDP PDU 的端口相关联）。它还表明链路当前是否已聚合；如果是，则提供聚合的端口标识符。
 - **802.3 最大帧** - MAC/PHY 实施的最大帧大小功能。

以下字段与管理地址相关：

- **通告模式** - 选择以下其中一种通告设备 IP 管理地址的方法：
 - **自动通告** - 指定软件将从所有产品 IP 地址中自动选择一个管理地址进行通告。如果有多个 IP 地址，软件将选择动态 IP 地址中的最小 IP 地址。如果无动态地址，软件将选择静态 IP 地址中的最小 IP 地址。
 - **无** - 不通告管理 IP 地址。
 - **手动通告** - 选择该选项以及要通告的管理 IP 地址。在设备处于第 3 层系统模式下并使用多个 IP 地址进行配置时，建议选择此选项（始终适用于 SG500X/ESW2-550X 设备）。
- **IP 地址** - 如果选择手动通告，则请从提供的地址中选择管理 IP 地址。

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

LLDP MED 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。LLDP MED 网络策略的某些特性如下：

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

设置 LLDP MED 网络策略

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

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

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

此外，管理员还可指引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“LLDP-MED 网络策略”选择**自动**。

注 选中此框后，用户将无法手动配置语音网络策略。

步骤 3 单击**应用**将此设置添加到当前配置文件。

步骤 4 要定义新策略，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 标记** - 选择是否为流量添加标记。
- **用户优先级** - 选择要应用于此网络策略所定义流量的流量优先级。这是 CoS 值。
- **DSCP 值** - 选择要与邻居所发送应用数据相关联的 DSCP 值。该值可告诉邻居要如何标记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。

配置 LLDP MED 端口设置

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

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

此页面包含所有端口的 LLDP MED 设置，包括启用的 TLV。

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

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

步骤 4 输入参数：

- **接口** - 选择要配置的接口。
- **LLDP MED 状态** - 在此端口上启用/禁用 LLDP MED。

- **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。
- **可用的可选 TLV** - 通过将 TLV 移至 *选定的可选 TLV* 列表中，来选择可由设备发布的 TLV。
- **可用的网络策略** - 通过将 LLDP MED 策略移至“选定的网络策略”列表中，来选择将由 LLDP 发布的 LLDP MED 策略。这些策略在“LLDP MED 网络策略”页面中进行创建。要在通告中包括一个或多个用户定义的网络策略，您还须从“可用的可选 TLV”中选择 *网络策略*。

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

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

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

显示 LLDP 端口状态

“LLDP 端口状态表”页面包含每个端口的 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**。

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

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

LLDP 端口状态全局信息

- **机箱 ID 子类型** - 机箱 ID 的类型（例如，MAC 地址）。
- **机箱 ID** - 机箱的标识符。如果机箱 ID 子类型为 MAC 地址，则会显示设备的 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** - 通告的本地 PoE 信息。
- **远程 PoE** - 邻居通告的 PoE 信息。
- **邻居数量** - 发现的邻居数目。
- **第一台设备的邻居功能** - 显示邻居的主要功能，例如：网桥或路由器。

显示 LLDP 本地信息

查看在端口上通告的 LLDP 本地端口状态的步骤：

步骤 1 单击 **管理 > 发现协议 - LLDP > LLDP 本地信息**。

步骤 2 在页面底部，单击 **LLDP 端口状态表**。

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

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

步骤 3 从端口列表中选择所需的端口。

此页面显示了以下字段：

全局

- **机箱 ID 子类型** - 机箱 ID 的类型。（例如，MAC 地址。）
- **机箱 ID** - 机箱的标识符。如果机箱 ID 子类型为 MAC 地址，则会显示设备的 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：

- **地址子类型** - 在“管理地址”字段中列出的管理 IP 地址的类型，例如 IPv4。
- **地址** - 返回的最适合管理用途的地址，通常为第 3 层地址。
- **接口子类型** - 用于定义接口编号的编号方法。
- **接口编号** - 与此管理地址相关联的具体接口。

MAC/PHY 详情

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

802.3 详情

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

802.3 链路聚合

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

802.3 节能以太网 (EEE) (如果设备支持 EEE)

- **本地发送** - 表明传输链路伙伴在离开低功耗空闲 (LPI 模式) 后，开始传输数据之前所等待的时间 (微秒)。
- **本地接收** - 表明接收链路伙伴要求传输链路伙伴在低功耗空闲 (LPI 模式) 后，开始传输数据之前所等待的时间 (微秒)。

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

MED 详情

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

位置信息

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

网络策略表

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

显示 LLDP 邻居信息

“LLDP 邻居信息”页面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，将会删除该信息。

查看 LLDP 邻居信息的步骤：

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

该页面包含以下字段：

- **本地端口** - 要将邻居与其连接的本地端口号。
- **机箱 ID 子类型** - 机箱 ID 的类型（例如，MAC 地址）。
- **机箱 ID** - 802 LAN 相邻设备机箱的标识符。
- **端口 ID 子类型** - 显示的端口标识符的类型。
- **端口 ID** - 端口的标识符。
- **系统名称** - 已发布的设备名称。
- **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 2 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。

802.3 详情

- **802.3 最大帧大小** - 端口上支持的最大通告帧大小。

802.3 链路聚合

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

802.3 节能以太网 (EEE)

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

MED 详情

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

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

802.1 VLAN 和协议

- **PVID** - 通告的端口 VLAN ID。

PPVID 表

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

VLAN ID

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

协议 ID

- **协议 ID 表** - 通告的协议 ID。

位置信息

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

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

网络策略

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

获取 LLDP 统计信息

“LLDP 统计信息”页面会显示每个端口的 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** - 接口的标识符。
- **发送帧总数** - 已传输的帧数。
- **接收的帧数**
 - **总数** - 已接收的帧数。
 - **丢弃** - 丢弃的已接收帧的总数。

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

步骤 2 单击**刷新**查看最新统计信息。

LLDP 过载

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

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

查看 LLDP 过载信息的步骤：

步骤 1 单击**管理 > 发现协议 - 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。
- **总数 (字节)** - 每个数据包中 LLDP 信息的总字节数。
- **等待发送 (字节)** - 要添加到各数据包中其他 LLDP 信息的剩余可用字节总数。
- **状态** - 正在传输 TLV 还是已过载。

步骤 2 要查看端口的过载详细信息，请选择该端口，然后单击**详情**。

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 数据包已传输还是已过载。
- **LLDP 可选 TLV**
 - 大小 (字节) - LLDP MED 可选 TLV 数据包的总字节数。
 - 状态 - LLDP MED 可选 TLV 数据包已传输还是已过载。
- **LLDP MED 清单**
 - 大小 (字节) - LLDP MED 清单 TLV 数据包的总字节数。
 - 状态 - LLDP MED 清单数据包已传输还是已过载。
- **总数 (字节)** - 每个数据包中 LLDP 信息的总字节数。
- **等待发送 (字节)** - 要添加到各数据包中其他 LLDP 信息的剩余可用字节总数。

配置 CDP

本节介绍如何配置 CDP。

其中包含以下主题：

- [设置 CDP 属性](#)
- [编辑 CDP 接口设置](#)
- [显示 CDP 本地信息](#)
- [显示 CDP 邻居信息](#)
- [查看 CDP 统计信息](#)

设置 CDP 属性

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

CDP 配置工作流程

以下是在设备上配置 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“接口设置”页面按接口配置 CDP
- 步骤 3** 若要使自动智能端口检测 CDP 设备的功能，请在“智能端口属性”页面中启用 CDP。

有关如何使用 CDP 标识智能端口设备功能的说明，请参阅[标识智能端口类型](#)。

输入 CDP 一般参数的步骤：

-
- 步骤 1** 单击**管理 > 发现 - 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，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。可能的选项有：
 - **使用默认设置** - 使用默认时间（180 秒）
 - **用户定义** - 输入时间（秒）。
- **CDP 传输速率** - 发送 CDP 通告更新的速率（以秒为单位）。可能的选项有：
 - **使用默认设置** - 使用默认速率（60 秒）
 - **用户定义** - 输入速率（秒）。
- **设备 ID 格式** - 选择设备 ID 的格式（MAC 地址或序列号）。可能的选项有：
 - **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。可能的选项有：
 - **使用默认设置** - 使用传出接口的 IP 地址。
 - **用户定义** - 使用地址 TLV 中接口（在**接口**字段中）的 IP 地址。
- **接口** - 如果为**源接口**选择**用户定义**，请选择接口。
- **系统日志语音 VLAN 不匹配** - 选中后，当检测到语音 VLAN 不匹配后，系统将发送系统日志消息。这意味着传入帧中的语音 VLAN 信息与本地设备通告的信息不匹配。
- **系统日志本征 VLAN 不匹配** - 选中后，当检测到本征 VLAN 不匹配后，系统将发送系统日志消息。这意味着传入帧中的本征 VLAN 信息与本地设备通告的信息不匹配。

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

步骤 3 单击**应用**。将定义 LLDP 属性。

编辑 CDP 接口设置

管理员可使用“接口设置”页面按端口启用/禁用 CDP。当与 CDP 邻居存在冲突时也会触发通知。冲突可能是语音 VLAN 数据、本征 VLAN 或双工模式。

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

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

定义 CDP 接口设置的步骤：

步骤 1 单击**管理 > 发现 - CDP > 接口设置**。

此页面包含每个接口的以下 CDP 信息。

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

该页面底部有四个按钮：

- **复制设置** - 选中后，会将配置从一个端口复制到其他端口。
- **编辑** - 下文步骤 2 中解释的字段。
- **CDP 本地信息详情** - 引导至“管理 > 发现协议 - CDP > CDP 本地信息”页面。
- **CDP 邻居信息详情** - 引导至“管理 > 发现协议 - CDP > 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站发送 Trap 时，以下三个字段属于可选字段。

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

步骤 3 输入相关信息，然后单击**应用**。端口设置将写入当前配置。

显示 CDP 本地信息

查看由 CDP 协议通告的、与本地设备有关的信息的步骤：

步骤 1 单击**管理 > 发现 - CDP > CDP 本地信息**。

步骤 2 选择一个本地端口，然后将显示以下字段：

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

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

- **管理电源等级** - 显示供电对受电设备功耗 TLV 的请求。设备总是在此字段中显示“无偏好”。

显示 CDP 邻居信息

“CDP 邻居信息”页面显示从邻居设备接收到的 CDP 信息。

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

查看 CDP 邻居信息的步骤：

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

该页面包含每个链路伙伴（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 2 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** - 邻居的平台标识符。
- **邻居接口** - 帧到达所经由的邻居的接口编号。
- **本征 VLAN** - 邻居的本征 VLAN。
- **双工** - 邻居接口处于半双工还是全双工模式。
- **地址** - 邻居的地址。
- **机动** - 接口上由邻居消耗的电源量。
- **版本** - 邻居的软件版本。

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

查看 CDP 统计信息

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

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

查看 CDP 统计信息的步骤：

步骤 1 单击**管理 > 发现 - CDP > CDP 统计信息**。

将为每个接口显示以下字段：

接收/传输的数据包数：

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

“CDP 错误统计信息”部分显示 CDP 错误计数器。

- **非法校验和** - 所接收的具有非法校验和值的数据包数。

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

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

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：

- [配置端口](#)
- [设置端口配置](#)
- [链路聚合](#)
- [UDLD](#)
- [配置绿色以太网](#)

配置端口

要配置端口，请执行以下操作：

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

设置端口配置

可在以下页面配置端口。

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。此页面可使您通过“编辑端口设置”页面选择并配置所需端口。

配置端口设置的步骤：

步骤 1 单击**端口管理 > 端口设置**。

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

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“复制/保存配置”页面将当前配置文件明确保存到启动配置文件，然后重启设备之后才会生效。

步骤 4 要更新端口设置，请选择所需端口，然后单击**编辑**。

步骤 5 修改以下参数：

- **Port** - 选择端口号。
 - **端口说明** - 输入用户定义的端口名称或备注。
 - **端口类型** - 显示端口类型和速度。可能的选项有：
 - *铜缆端口* - 常规端口而非组合端口，支持以下值：10M、100M 和 1000M（类型：铜缆）。
 - *组合铜缆端口* - 与铜质 CAT5 电缆连接的组合端口，支持以下值：10M、100M 和 1000M（类型：组合铜缆）。
 - *组合光纤 - SFP 光纤千兆位接口转换器端口*，支持以下值：100M 和 1000M（类型：组合光纤）。
 - 10G 光纤 - 速度为 1G 或 10G 的端口。
- 注** 同时使用两个端口时，在组合端口中 SFP 光纤优先级较高。
- **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 Trap，可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。如果尚未定义时间范围，请单击**编辑**转至“时间范围”页面。
- **时间范围名称** - 选择指定时间范围的模板。
- **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。
- **重新激活挂起的端口** - 选择该选项可重新激活已挂起的端口。可用来挂起端口的方法有很多，例如通过锁定端口安全选项、dot1x 单主机违例应对、环回检测、STP 环回防护或访问控制列表 (ACL) 配置。无论出于何种原因挂起端口，重新激活操作均可将端口恢复为启用状态。
- **自动协商** - 选择该选项可在端口上启用自动协商。自动协商可使端口向端口链路伙伴通告其传输速度、双工模式和流量控制能力。
- **运行自动协商** - 显示端口上的当前自动协商状态。
- **管理端口速度** - 配置端口的速度。端口类型可确定可用的速度。仅当禁用端口自动协商时，您才可以指定 *管理速度*。
- **运行端口速度** - 显示作为协商结果的当前端口速度。
- **管理双工模式** - 选择端口双工模式。仅当禁用自动协商时才会配置此字段，并且端口速度会设置为 10M 或 100M。端口速度为 1G 时，始终处于全双工模式。可能的选项有：
 - *全双工* - 接口支持设备和客户端之间的同时双向传输。
 - *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。
- **运行双工模式** - 显示端口当前的双工模式。
- **自动通告** - 选择启用自动协商后，要由其通告的功能。选项如下：
 - *最大容量* - 可以接受所有端口速度和双工模式设置。
 - *10 半双工* - 10 Mbps 速度和半双工模式。
 - *10 全双工* - 10 Mbps 速度和全双工模式。
 - *100 半双工* - 100 Mbps 速度和半双工模式。

- **100 全双工** - 100 Mbps 速度和全双工模式。
- **1000 全双工** - 1000 Mbps 速度和全双工模式。
- **运行通告** - 显示当前发布到端口邻居的功能。*管理通告*字段中指定了以下可能的选项。
- **邻居通告** - 显示通过邻居设备（链路伙伴）通告的功能。
- **背压** - 在端口上选择“背压”模式（配合使用半双工模式），以降低设备拥挤时的数据包接收速度。它会禁用远程端口，从而避免其通过拥堵信令来发送数据包。
- **流量控制** - 启用或禁用 802.3x 流量控制，或在端口上启用流量控制的自动协商（仅适用于全双工模式）。
- **MDI/MDIX** - 端口上的 *介质相关接口 (MDI)*/ *具有正反接线自适应功能的介质相关接口 (MDIX)* 状态。

选项如下：

- **MDIX** - 选择该项可交换端口的传输和接收对。
- **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。
- **受保护的端口** - 选择该选项可使端口成为受保护的端口。（受保护的端口也称为专用 VLAN 边缘 [PVE]。）受保护的端口功能如下：
 - 受保护的端口可在接口（共享同一 VLAN 的以太网端口和 LAG）之间提供第 2 层隔离保护。
 - 从受保护的端口接收到的数据包仅可以转发到不受保护的出口端口。受保护的端口过滤规则也适用于通过软件（例如侦测应用程序）转发的数据包。
 - 端口保护不受 VLAN 成员关系的影响。连接到受保护端口的设备不得与其他端口通信，即使这些端口是同一 VLAN 的成员。
 - 端口和 LAG 均可定义为“受保护的”或“不受保护的”。受保护的 LAG 在 [配置 LAG 设置](#) 一节中做了说明。
- **LAG 中的成员** - 如果端口为 LAG 的成员，则显示 LAG 号；否则将此字段留空。

步骤 6 单击 **应用**。“端口设置”将写入当前配置文件。

错误恢复设置

此页面可启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** - 选择该选项可为端口安全错误禁用状态启用错误恢复机制。
- **端口安全** - 选择该选项可为端口安全错误禁用状态启用错误恢复机制。
- **802.1x 单主机违反规则** - 选择该选项可为 802.1x 错误禁用状态启用错误恢复机制。
- **ACL 拒绝** - 选择该选项可为 ACL 拒绝错误禁用状态启用错误恢复机制。
- **STP BPDU 防护** - 选择该选项可为 STP BPDU 防护错误禁用状态启用错误恢复机制。
- **UDLD** - 选择该选项可为 UDLD 关闭状态启用错误恢复机制。

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**。

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**
- **静态和动态 LAG 工作流程**

- 定义 LAG 管理
- 配置 LAG 设置
- 配置 LACP

链路聚合概述

链路聚合控制协议 (LACP) 是 IEEE 规格 (802.3az) 的一部分，可使您将多个物理端口捆绑在一起以形成单个逻辑通道 (LAG)。LAG 可使设备之间的带宽成倍增加、增强端口灵活性并提供链路冗余。

支持两种类型的 LAG：

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

负载均衡

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

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

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

设备支持 32 个 LAG，每个 LAG 组中最多有 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。

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

默认设置和配置

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

要配置静态 LAG，请执行以下操作：

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

要配置动态 LAG，请执行以下操作：

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

定义 LAG 管理

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

选择 LAG 的负载均衡算法的步骤：

步骤 1 单击**端口管理 > 链路聚合 > 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**。

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。
- **单元/插槽** - 显示已定义 LAG 信息的堆叠成员。
- **端口列表** - 将那些要分配给 LAG 的端口从**端口列表**移动到 **LAG 成员列表**中。可以为每个静态 LAG 最多分配八个端口，为动态 LAG 最多分配 16 个端口。

步骤 3 单击**应用**。LAG 成员关系将保存至当前配置文件中。

配置 LAG 设置

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

配置 LAG 设置或重新激活挂起的 LAG 的步骤：

步骤 1 单击**端口管理 > 链路聚合 > LAG 设置**。

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。
- **说明** - 输入 LAG 名称或备注。
- **LAG 类型** - 显示组成 LAG 的端口类型。
- **管理状态** - 将选定的 LAG 设置为“启用”或“禁用”。
- **运行状态** - 显示 LAG 当前是否处于运行状态。
- **链路状态 SNMP 陷阱** - 选择该选项可生成 SNMP Trap，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。如果尚未定义时间范围，请单击**编辑**转至“时间范围”页面。
- **时间范围名称** - 选择指定时间范围的模板。
- **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。
- **重新激活挂起的 LAG** - 选择该选项可重新激活端口（如果已通过锁定端口安全性选项或 ACL 配置禁用 LAG）。
- **管理自动协商** - 在 LAG 上启用或禁用自动协商。自动协商是两个链路伙伴之间的协议，可使 LAG 向其伙伴通告自己的传输速率和流量控制（流量控制默认为已禁用）。建议在聚合链路的两端同时启用或同时禁用自动协商，从而确保链路速度保持一致。
- **运行自动协商** - 显示自动协商设置。
- **管理速度** - 选择 LAG 速度。
- **运行 LAG 速度** - 显示 LAG 运行时的当前速度。

- **自动通告** - 选择要由 LAG 通告的功能。选项如下：
 - **最大容量** - 所有 LAG 速度和两种双工模式均可用。
 - **10 全双工** - LAG 可通告 10 Mbps 速度，模式为全双工。
 - **100 全双工** - LAG 可通告 100 Mbps 速度，模式为全双工。
 - **1000 全双工** - LAG 可通告 1000 Mbps 速度，模式为全双工。
- **运行通告** - 显示“管理通告”状态。LAG 可将其功能通告给相邻的 LAG，以开始协商流程。*管理通告*字段中指定了以下可能值。
- **管理流量控制** - 在 LAG 上将“流量控制”设置为**启用**或**禁用**，或者启用流量控制的**自动协商**。
- **运行流量控制** - 显示当前的流量控制设置。
- **受保护的 LAG** - 选择该选项可使 LAG 成为受保护的端口，以接受第 2 层隔离保护。有关受保护的端口和 LAG 的详情，请参阅[设置基本端口配置](#)中的端口配置说明。

步骤 4 单击**应用**。将更新当前配置文件。

配置 LACP

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

LACP 优先级和规则

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

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

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

动态 LAG 最多可具有 16 个相同类型的以太网端口。最多可有八个端口处于活动状态，而处于备用模式的端口也不能超过八个。如果动态 LAG 中的端口数超过 8 个，链路控制端上的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。

设置 LACP 参数设置

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。请参阅 **LACP 优先级和规则**。

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。请参阅 **设置 LACP 参数设置**。
- **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。

UDLD

请参阅**端口管理：单向链路检测**。

PoE

请参阅**端口管理：PoE**。

配置绿色以太网

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**
- **设置全局绿色以太网属性**
- **设置绿色以太网端口属性**

绿色以太网概述

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

绿色以太网功能通过以下方法降低总电能使用量：

- **电量检测模式** - （不适用于 SG500XG）在非活动链路上，端口会转变为非活动模式，从而节省电能，同时使端口的管理状态保持“启用”状态。从此模式恢复为完全运行模式的过程既快速又明显，而且不会丢失任何帧。GE 和 FE 端口均支持此模式。

- **短距模式** - 该功能可在长度较短的电缆上提供节能功能。分析电缆长度之后，将针对各种电缆长度调整电能使用量。如果电缆短于 50 米，则设备将使用较少电能来通过电缆发送帧，从而节省能源。仅在 RJ45 GE 端口上支持此模式；此模式不会应用到组合端口。

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

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

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

这些模式在每个端口进行配置，无需考虑端口的 LAG 成员关系。

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

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

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

显示的节能量仅为绿色以太网的节能量。不会显示 EEE 的节能量。

通过禁用端口 LED 节能

通过禁用端口 LED 功能，用户可以节约设备 LED 消耗的额外功率。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。

在“绿色以太网 -> 属性”页面，用户可以禁用设备上的端口 LED 以节省能源。

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。

仅在具有 GE 端口的设备上支持 802.3az EEE。

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

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

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

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

连接的两端（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，那么即使禁用了自动协商，EEE 仍将保持启用状态。

802.3az EEE 链路级发现

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

802.3az EEE 的可用性

请查看版本备注，获得支持 EEE 产品的完整列表。

默认配置

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

功能之间的交互

以下内容将介绍 802.3az EEE 与其他功能的交互：

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

802.3az EEE 配置工作流程

本节介绍如何配置 802.3az EEE 功能，以及查看其计数器的方法。

- 步骤 1** 打开**端口管理 > 端口设置**页面，确保已在端口上启用自动协商。
 - a. 选择一个端口，打开“编辑端口设置”页面。
 - b. 选择**自动协商**字段，确保已启用该字段。
- 步骤 2** 确保“端口管理 > 绿色以太网 > 属性”页面中的**802.3 节能以太网 (EEE)**已全局启用（默认情况下，此功能处于启用状态）。该页面还会显示已节省的能量量。
- 步骤 3** 打开“绿色以太网 > 端口设置”页面，确保已在端口上启用 802.3az EEE。
 - a. 选择一个端口，打开“编辑端口设置”页面。
 - b. 在端口上选中**802.3 节能以太网 (EEE)**模式（默认情况下，此功能处于启用状态）。
 - c. 在**802.3 节能以太网 (EEE) LLDP**中选择是否禁用通过 LLDP 通告 802.3az EEE 功能（默认情况下，此功能处于启用状态）。
- 步骤 4** 要在本地设备上查看与 802.3 EEE 相关的信息，请打开“管理 > 发现协议 - LLDP > LLDP 本地信息”页面，查看“802.3 节能以太网 (EEE)”部分中的信息。
- 步骤 5** 要在远程设备上显示 802.3az EEE 的信息，请打开“管理 > 发现协议 - LLDP > LLDP 邻居信息”页面，查看“802.3 节能以太网 (EEE)”部分中的信息。

设置全局绿色以太网属性

“属性”页面显示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** - （不适用于 SG500XG）默认情况下，此模式处于禁用状态。单击该复选框可启用此模式。
 - **短距** - 如果设备上有 GE 端口，则全局启用或禁用短距模式。

注 如果启用了短距，则必须禁用 EEE。
 - **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。

- **节能** - 显示运行环保以太网和短距所节约的电能百分比。显示的节能量仅指短距模式和电量检测模式节约的电能。EEE 节能量是以端口利用率为基础的，所以具有动态性，因而不会将其考虑在内。通过比较未启动节能时的最大功耗和当前消耗来计算节约的电能。
- **累计节省的电量** - 显示自上一次重启设备所节省的电量。每当出现影响节电量的事件时都会更新此值。
- **802.3 节能以太网 (EEE)** - 全局启用或禁用 EEE 模式（仅当设备上具有 GE 端口时适用）。

步骤 3 单击**应用**。绿色以太网属性将写入当前配置文件。

设置绿色以太网端口属性

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

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

定义每端口绿色以太网设置的步骤：

步骤 1 单击**端口管理 > 绿色以太网 > 端口设置**。

“端口设置”页面显示以下字段：

- **全局参数状态** - 描述启用的功能。

对于每个端口，系统将会列出以下字段：

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

- **运行** - 显示短距模式当前是否处于运行状态。
- **原因** - 如果短距模式为处于运行状态，则显示原因。
- **电缆长度** - 显示 VCT 返回的电缆长度（以米为单位）。

注 仅在 RJ45 GE 端口上支持短距模式；此模式不会应用到组合端口。

▪ **802.3 节能以太网 (EEE) - 有关 EEE 功能的端口状态：**

- **管理** - 显示是否启用了 EEE 模式。
- **运行** - 显示 EEE 目前是否在本地端口上运行。显示是否启用过此功能（管理状态）、是否在本地端口上已启用此功能，以及此功能是否在本地端口上运行。
- **LLDP 管理** - 显示是否启用了通过 LLDP 通告 EEE 计数器。
- **LLDP 运行** - 显示当前是否正在运行通过 LLDP 通告 EEE 计数器。
- **EEE 远程支持** - 显示链路伙伴上是否支持 EEE。本地和远程链路伙伴必须均支持 EEE。

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

步骤 2 选择一个端口，然后单击**编辑**。

步骤 3 选择在该端口上启用还是禁用**电量检测**模式。

步骤 4 如果设备上带有 GE 端口，选择在该端口上启用还是禁用**短距**模式。

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

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

步骤 7 单击**应用**。绿色以太网端口设置将写入当前配置文件。

端口管理：单向链路检测

本部分介绍单向链路检测 (UDLD) 功能如何发挥作用。

其中包含以下主题：

- [UDLD 概述](#)
- [UDLD 操作](#)
- [使用指南](#)
- [与其他功能的依赖性](#)
- [默认设置和配置](#)
- [使用说明](#)
- [常见 UDLD 任务](#)
- [配置 UDLD](#)

UDLD 概述

UDLD 是一个第 2 层协议，可使通过光纤或双绞线以太网电缆连接的设备检测单向链路。每当本地设备收到来自相邻设备的流量，但邻居未收到来自本地设备的流量时，就发生了单向链路。

UDLD 的目的是检测邻居未收到本地设备流量的端口（单向链路），并关闭这些端口。

所有连接的设备都必须支持 UDLD，才能让协议成功检测到单向链路。如果仅本地设备支持 UDLD，则设备无法检测链路状态。在这种情况下，链路的状态将设置为待定。用户可以进行配置，是关闭处于待定状态的端口还是仅触发通知。

UDLD 操作

UDLD 状态和模式

根据 UDLD 协议，端口将分配以下状态：

- **检测** - 系统正在尝试确定链路是双向还是单向。这是一种临时状态。
- **双向** - 本地设备发送的流量会由其邻居接收，且来自邻居的流量会由本地设备接收。
- **关闭** - 链路为单向。本地设备发送的流量会由其邻居接收，但来自邻居的流量未被本地设备接收。
- **待定** - 由于发生了以下情况之一，系统无法确定端口的状态：
 - 邻居不支持 UDLD。
 - 或
 - 邻居未收到来自本地设备的流量。

此时，UDLD 的行为取决于设备的 UDLD 模式，如下所述。

UDLD 支持以下操作模式：

- **正常**
 - 如果链路为单向，则端口将关闭。
 - 如果链路为待定，则端口不会关闭。其状态将更改为待定，并会发送通知。
- **Aggressive**

如果链路为单向或待定，则端口将关闭。

发生以下一种情况时，端口上将启用 UDLD：

- 端口为光纤端口且 UDLD 已全局启用。
- 端口为铜缆端口，且您专门在端口上启用了 UDLD。

UDLD 的工作方式

UDLD 在端口上启用后，将执行以下操作：

- UDLD 启动端口检测状态。

在此状态下，UDLD 在每个活动接口上定期向所有邻居发送消息。这些消息包含所有已知邻居的设备 ID。它会根据用户定义的消息时间发送这些消息。
- UDLD 接收来自相邻设备的 UDLD 消息。它会缓存这些信息，直到过期时间（消息时间的 3 倍）个结束。如果在过期之前收到新消息，则新消息中的信息将替换旧消息。
- 过期时间结束后，设备会对收到的信息执行以下操作：
 - **如果邻居消息包含本地设备 ID** - 端口的链路状态将设置为双向。
 - **如果邻居消息不包含本地设备 ID** - 端口的链路状态将设置为单向，且端口将关闭。
- 如果在过期时间范围内未从相邻设备收到 UDLD 消息，端口的链路状态将设置为待定，且会发生以下情况：
 - **如果设备在正常 UDLD 模式下**：将发出通知。
 - **如果设备在积极 UDLD 模式下**：端口将关闭。

如果接口处于双向或待定状态，则设备将每隔消息时间（秒）就定期发送一条消息。上述步骤将一再重复执行。

已关闭的端口可在“端口管理 > 错误恢复设置”页面手动重新激活。有关详情，请参阅[重新激活关闭的端口](#)。

如果一个接口已关闭且 UDLD 已启用，设备将删除所有邻居信息，并向邻居发送至少一条 UDLD 消息，告知它们端口已关闭。端口开启后，UDLD 状态将更改为检测。

UDLD 在邻居上不受支持或已禁用

如果 UDLD 在邻居上不受支持或已禁用，那么设备不会从邻居收到任何 UDLD 消息。在这种情况下，设备无法确定链路是单向还是双向。然后，接口的状态将设置为待定。设备将采取的行动取决于 UDLD 模式是正常还是积极。

本地和相邻设备中的 UDLD 模式不一致

本地设备及其邻居可以设置为处于不同 UDLD 模式（正常和积极）。UDLD 消息中不包含 UDLD 模式，因此，本地设备与邻居并不知道对方的 UDLD 模式。

如果本地和邻居设备的 UDLD 模式不同，设备将按如下方式运行：

- 当链路的 UDLD 状态为双向或单向时，两个设备都会关闭其端口。
- 当端口的 UDLD 状态为待定时，处于正常 UDLD 模式的一端仅发出一个通知，而处于积极 UDLD 模式的一端会关闭端口。

如果两个设备都处于正常模式，则端口在状态为待定时不会关闭。

重新激活关闭的端口

您可以使用以下方式之一重新激活被 UDLD 关闭的端口：

- **自动** - 您可以在“端口管理 > 错误恢复设置”页面将系统配置为自动激活由 UDLD 关闭的端口。在这种情况下，如果端口被 UDLD 关闭，则在自动恢复间隔到期后，端口会自动重新激活。UDLD 会再次开始在端口上运行。例如，如果链路仍然为单向，则在 UDLD 过期时间结束后，UDLD 会再次将其关闭。
- **手动** - 您可以在“端口 > 错误恢复设置”页面重新激活端口。

使用指南

思科不建议您在与不支持或禁用 UDLD 的设备连接的端口上启用 UDLD。如果在与不支持 UDLD 的设备连接的端口上发送数据包，则会导致端口上出现更多流量，不会提供任何益处。

此外，配置 UDLD 时请考虑以下事项：

- 根据关闭单向链接端口的紧急程度设置消息时间。消息时间越短，发送和分析的 UDLD 数据包就越多，但如果链路为单向，则端口关闭的速度就越快。
- 如果希望在铜缆端口上启用 UDLD，则必须在每个端口上启用。如果全局启用 UDLD，则 UDLD 仅会在光纤端口上启用。
- 如果只希望在确信链路为单向时关闭端口，请将 UDLD 模式设置为正常。
- 如果希望在链路有可能为待定时就关闭所有端口，则将 UDLD 模式设置为积极。

与其他功能的依赖性

- **UDLD 和第 1 层**

如果 UDLD 已在端口上启用，则 UDLD 会在端口启用时在端口上活跃运行。如果端口关闭，UDLD 会进入 UDLD 关闭状态。在此状态下，UDLD 会删除所有已学习的邻居。如果端口已从关闭更改为开启，UDLD 会恢复积极运行状态。

- **UDLD 和第 2 层协议**

UDLD 的运行独立于同一端口上运行的其他第 2 层协议，如 STP 或 LACP。例如，无论端口的 STP 状态如何，也无论端口是否属于 LAG，UDLD 都会向端口分配一个状态。

默认设置和配置

此功能存在以下默认设置：

- 默认状态下，UDLD 在设备的所有端口上都为禁用状态。
- 默认消息时间为 15 秒。
- 默认过期时间为 45 秒（消息时间的 3 倍）。
- 默认端口 UDLD 状态：
 - 光纤接口处于全局 UDLD 状态。
 - 非光纤接口处于禁用状态。

使用说明

无需执行任何预备任务。

常见 UDLD 任务

本部分介绍设置 UDLD 的一些常见任务。

工作流程 1：要在光纤端口上全局启用 UDLD，请执行以下步骤：

-
- 步骤 1** 打开“端口管理 > UDLD 全局设置”页面。
- a. 在消息时间字段中输入值。
 - b. 选择**已禁用**、**正常**或 **Aggressive** 作为全局 UDLD 状态。

- 步骤 2** 单击应用

工作流程 2：要更改光纤端口的 UDLD 配置或要在铜缆端口上启用 UDLD，请执行以下步骤：

-
- 步骤 1** 打开端口管理 > UDLD 全局设置页面。
- a. 选择一个端口。
 - b. 选择**默认**、**已禁用**、**正常**或 **Aggressive** 作为端口的 UDLD 状态。如果选择了“默认”，则端口会接收全局设置。

- 步骤 2** 单击应用。

工作流程 3：要在端口被 UDLD 关闭且未配置自动重新激活的情况下开启端口，请执行以下步骤：

-
- 步骤 1** 打开端口管理 > 错误恢复设置页面。
- a. 选择一个端口。
 - b. 单击**重新激活**。

配置 UDLD

可同时针对所有光纤端口配置 UDLD 功能（位于“UDLD 全局设置”页面），也可以对每个端口单独配置（位于“UDLD 接口设置”页面）。

UDLD 全局设置

“光纤端口 UDLD 默认状态”仅适用于光纤端口。

“消息时间”字段适用于铜缆端口和光纤端口。

全局配置 UDLD 的步骤：

步骤 1 单击**端口管理 > UDLD > UDLD 全局设置**。

步骤 2 输入以下字段：

- **消息时间** - 输入两个发送的 UDLD 消息之间的时间间隔。此字段适用于光纤端口和铜缆端口。
- **光纤端口 UDLD 默认状态** - 此字段仅适用于**光纤**端口。铜缆端口的 UDLD 状态必须在“UDLD 接口设置”页面单独设置。可能的状态包括：
 - *已禁用* - UDLD 在设备的所有端口上都为禁用状态。
 - *正常* - 如果链路为单向，设备将关闭接口。如果链路为待定，则将发送通知。
 - *Aggressive* - 如果链路为单向或待定，设备将关闭接口。

步骤 3 单击**应用**，以将设置保存到当前配置文件中。

UDLD 接口设置

使用“UDLD 接口设置”页面更改特定端口的 UDLD 状态。此处的状态可针对铜缆或光纤端口设置。

要将一组特定的值复制到不止一个端口，请设置一个端口的值，并使用**复制**按钮将其复制到其他端口。

为接口配置 UDLD 的步骤：

步骤 1 单击**端口管理 > UDLD > UDLD 接口设置**。

系统将针对所有启用了 UDLD 的端口显示信息，或者，如果您仅筛选了某一组端口，则将针对这组端口显示信息。

- **端口** - 端口标识符。
- **UDLD 状态** - 可能的状态有：
 - *已禁用* - UDLD 在设备的所有光纤端口上都为禁用状态。
 - *正常* - 如果设备检测到链路为单向，则将关闭接口。如果链路为待定，则将发出通知。
 - *Aggressive* - 如果链路为单向或待定，设备将关闭端口。
- **双向状态** - 为选定端口选择此字段的值。可能的状态包括：
 - *检测* - 端口的最新 UDLD 状态正在确定过程中。从上次确定（如有）或 UDLD 开始在端口上运行开始，过期时间尚未结束，因此，状态还不确定。
 - *双向* - 本地设备发送的流量会由其邻居接收，且来自邻居的流量会由本地设备接收。
 - *待定* - 端口及其连接端口之间的链路状态无法确定，原因可能为未收到 UDLD 消息，或者 UDLD 消息中未包含本地设备 ID。
 - *已禁用* - UDLD 已在此端口上禁用。
 - *关闭* - 由于端口与连接设备之间的链路在积极模式下为单向或待定，因此端口已关闭。
- **邻近数量** - 检测到的已连接设备数量。

步骤 2 要为特定端口修改 UDLD 状态，请选择端口并单击**编辑**。

步骤 3 修改 UDLD 状态的值。如果选择**默认**，端口会接收“全局 UDLD 设置”页面中**光纤端口 UDLD 默认状态**的值。

步骤 4 单击**应用**，以将设置保存到当前配置文件中。

UDLD 邻近

查看所有与本地设备连接的设备的步骤：

步骤 1 单击**端口管理 > UDLD > UDLD 邻近**。

以下字段会对所有启用了 UDLD 的端口显示：

- **接口名称** - 启用了 UDLD 的本地端口的名称。
- **邻近信息：**
 - *设备 ID* - 远程设备的 ID。
 - *设备 MAC* - 远程设备的 MAC 地址。
 - *设备名称* - 远程设备的名称。
 - *端口 ID* - 远程端口的名称。
- **状态 - 本地端口上本地设备与相邻设备之间的链路状态。可能的值如下所示：**
 - *检测* - 端口的最新 UDLD 状态正在确定过程中。从上次确定（如有）或 UDLD 开始在端口上运行开始，过期时间尚未结束，因此，状态还不确定。
 - *双向* - 本地设备发送的流量会由其邻居接收，且来自邻居的流量会由本地设备接收。
 - *待定* - 端口及其连接端口之间的链路状态无法确定，原因可能为未收到 UDLD 消息，或者 UDLD 消息中未包含本地设备 ID。
 - *已禁用* - UDLD 已在此端口上禁用。
 - *关闭* - 由于端口与连接设备之间的链路在积极模式下为单向或待定，因此端口已关闭。
- **邻近到期时间 (秒)** - 显示在确定端口 UDLD 状态之前必须经历的时间。此时间为消息时间的三倍。
- **邻近消息时间 (秒)** - 显示 UDLD 消息之间的时间。

智能端口

本文档介绍智能端口功能。

其中包含以下主题：

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

概述

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

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。只有通过 CLI 才能按照宏名称应用智能端口宏。有关详情，请参阅 CLI 指南。

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**配置 LLDP** 和**配置 CDP** 部分介绍了智能端口 LLDP 和智能端口 CDP。

此外，**常见智能端口任务**一节还将介绍典型工作流程。

什么是智能端口

智能端口是可应用内置（或用户定义）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。

您可通过以下方法应用智能端口宏：

- 通过关联的智能端口类型。
- 按名称从智能端口宏静态应用（仅可使用 CLI）。

智能端口宏可使用 CLI 和 GUI，按其智能端口类型静态进行应用，也可按自动智能端口动态应用。自动智能端口根据 CDP 功能、LLDP 系统功能和/或 LLDP-MED 功能，获取连接设备的智能端口类型。

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 CLI 命令脚本，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，可在 CLI 特权执行模式下执行显示解析器宏名称 [macro_name] 命令，或在“智能端口类型设置”页面上单击[查看宏源](#)按钮。

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

有两种智能端口宏类型：

- **内置** - 这些宏由系统提供。一个宏应用配置模板，另一个移除配置模板。内置智能端口宏的宏名称以及他们与之关联的智能端口类型如下：
 - macro-name (例如: printer)
 - no_macro-name (例如: no_printer)
- **用户定义** - 这些宏由用户编写。有关详情，请参阅 CLI 参考指南。要将用户定义的宏与智能端口类型关联，必须同时定义它的反宏。
 - smartport-type-name (例如: my_printer)
 - no_smartport-type-name (例如: no_my_printer)

在“编辑智能端口类型设置”页面中，智能端口宏与智能端口类型绑定。

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

智能端口宏可按宏名称或与宏关联的智能端口类型应用到接口。只有通过 CLI 才能按宏名称应用智能端口宏，有关详情，请参阅 CLI 指南。

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结果配置将被移除。过期次数由特定时间内，未收到设备的 CDP 和/或 LLDP 通告来决定。

使用 CDP/LLDP 信息标识智能端口类型

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
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

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
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 [配置 LLDP](#) 和 [配置 CDP](#) 部分。

永久自动智能端口接口

如果已在接口上启用永久状态，即使在连接设备过期、接口关闭以及设备重启（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

如果智能端口宏无法应用到接口，您可在“接口设置”页面检查故障点，并在“接口设置”页面和“编辑接口设置”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](#)。

与其他功能的关系和向后兼容性

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

常见智能端口任务

本节介绍一些设置智能端口和自动智能端口的常见任务。

工作流程 1: 要在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“智能端口 > 属性”页面。将**管理自动智能端口**设为**启用**或**通过语音 VLAN 启用**。
- 步骤 2** 选择是否要使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自动智能端口功能，请打开“智能端口 > 接口设置”页面。
- 步骤 6** 选择接口，然后单击**编辑**。
- 步骤 7** 在**智能端口应用**字段中选择自动智能端口。
- 步骤 8** 必要时选中或取消选中**永久状态**。
- 步骤 9** 单击**应用**。

工作流程 2：要将接口配置为静态智能端口，请执行以下步骤：

- 步骤 1** 要在接口上启用自动智能端口功能，请打开“智能端口 > 接口设置”页面。
- 步骤 2** 选择接口，然后单击**编辑**。
- 步骤 3** 在**智能端口应用**字段中选择要分配给接口的智能端口类型。
- 步骤 4** 根据需要设置宏参数。
- 步骤 5** 单击**应用**。

工作流程 3：要调整智能端口宏参数默认值和/或将用户定义的宏对与某种智能端口类型绑定，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。
 - 将用户定义的宏对（宏及其对应的反宏）与智能端口类型绑定。
1. 打开“智能端口 > 智能端口类型设置”页面。
 2. 选择智能端口类型。
 3. 单击**查看宏源**，查看与所选智能端口类型关联的当前智能端口宏。
 4. 单击**编辑**以打开一个新窗口，在该窗口中您可将用户定义的宏与所选的智能端口类型绑定并/或修改与该智能端口类型绑定的宏中的默认参数值。当自动智能端口将所选智能端口类型（如适用）应用到某接口时，将使用这些参数默认值。
 5. 在“编辑”页面中，修改字段。

6. 如果参数已更改，单击**应用**重新运行宏；或在必要时单击**恢复默认设置**，恢复内置宏的默认参数值。

工作流程 4：要在智能端口宏失败后重新运行，请执行以下步骤：

- 步骤 1** 在“接口设置”页面，选择一个智能端口类型为“未知”的接口。
- 步骤 2** 单击**显示诊断**查看问题。
- 步骤 3** 排除故障，然后修正问题。请参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**配置 LLDP**和**配置 CDP**部分。

智能端口属性

全局配置智能端口功能的步骤：

步骤 1 单击**智能端口 > 属性**。

步骤 2 输入参数。

- **管理自动智能端口** - 选中后将全局启用或禁用自动智能端口。可能的选项有：
 - **禁用** - 选中后，将在设备上禁用自动智能端口。
 - **启用** - 选中后，将在设备上启用自动智能端口。
 - **通过自动语音 VLAN 启用** - 选中该选项后将启用自动智能端口，但是只有在启用自动语音 VLAN 并使之运行后，自动智能端口才能正常运行。“通过自动语音 VLAN 启用”是默认设置。
- **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。

智能端口类型设置

使用“智能端口类型设置”页面，编辑智能端口类型设置并查看宏源。

默认情况下，每种智能端口类型都与一对内置智能端口宏相关联。要进一步了解有关宏与反宏的信息，请参阅[智能端口类型](#)。此外，您也可将已进行定制配置的用户定义的宏对与一种智能端口类型相关联。用户定义的宏仅可通过 CLI 编写。有关详情，请参阅 CLI 参考指南。

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 要修改宏的参数或分配用户定义的宏，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。
- **宏类型** - 选择与该智能端口宏类型关联的一对宏和反宏是内置宏还是用户定义的宏。
- **用户定义的宏** - 如果必要，选择要与所选智能端口类型关联的用户定义的宏。该宏必须已与一个反宏配对。

两个宏按名称进行配对，并在“智能端口宏”一节进行说明。

- **宏参数** - 在宏中显示以下三种参数的字段：
 - **参数名称** - 宏中的参数名称。
 - **参数值** - 宏中的当前参数值。可在此更改该值。
 - **参数说明** - 参数说明。

可通过单击**恢复默认设置**来恢复默认参数值。

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

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

接口设置

使用“接口设置”页面可执行以下任务：

- 将特定智能端口类型静态应用到接口（具有接口特定的宏参数值）。
- 在接口上启用自动智能端口。
- 对应用失败并导致智能端口类型变为未知的智能端口宏进行诊断。
- 智能端口宏运行失败后，将其重新应用到以下其中一种接口类型：交换机、路由器和 AP。单击**重新应用**之前，应进行必要的修正。有关故障排除的提示，请参阅[常见智能端口任务](#)一节中的工作流程部分。
- 将智能端口宏重新应用到接口。在某些情况下，您可能需要重新应用智能端口宏，以便接口上的配置保持最新。例如，在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。

可通过以下方式重新应用关联智能端口宏：

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

该**重新应用**操作还会将该接口添加到所有新创建的 VLAN。

步骤 2 智能端口诊断。

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

步骤 3 将所有未知接口重置为默认类型。

- 选择与复选框 *相同的端口类型*。
- 选择 *未知*，然后单击**转至**。

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

注 重置未知类型的接口不会重置失败宏所执行的配置。此操作必须通过手动进行。

将智能端口类型分配到接口或在接口上激活自动智能端口的步骤：

步骤 1 选择一个接口，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

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

```

smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@

```

no_desktop

```

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

```

打印机

```

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

```

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

no_printer

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

guest

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


no_guest]]

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

服务器

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

no_server

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

主机

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

no_host

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

ip_camera

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

no_ip_camera

```
[no_ip_camera]
#macro description ip_camera
#
```

```

no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@

```

ip_phone

```

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

```

no_ip_phone

```

[no_ip_phone]
#macro description no ip_phone
#macro keywords $voice_vlan
#
#macro key description:$voice_vlan: 语音 VLAN ID

```

```
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone_desktop

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

no_ip_phone_desktop

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

交换机

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

no_switch

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

路由器

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

no_router

```
[no_router]

#macro description No router

#macro keywords $voice_vlan

#

#macro key description:$voice_vlan: 语音 VLAN ID

#
```

```
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
no spanning-tree link-type
#
@
```

接入点

```
[接入点]
#macro description ap
#macro keywords $native_vlan $voice_vlan
#
#macro key description:$native_vlan: 将在端口上配置的 Untagged VLAN
```


端口管理：PoE

以太网供电 (PoE) 功能仅在基于 PoE 的设备上提供。如需基于 PoE 的设备列表，请参阅“[设备型号](#)”一节。

本节介绍如何使用 PoE 功能。

注 PoE 功能未在 SG500XG/ESW2-550X 设备上启用。

其中包含以下主题：

- [设备上的 PoE](#)
- [配置 PoE 属性](#)
- [配置 PoE 设置](#)

设备上的 PoE

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

有关各种型号上 PoE 支持的信息，请参阅[设备型号](#)。

PoE 功能

PoE 有如下功能：

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

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

- IP 电话
- 无线接入点
- IP 网关
- 音频和视频远程监控设备

PoE 工作

PoE 分以下几个阶段实施：

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

PoE 支持两种模式：

- **端口限制** - 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 配置注意事项

使用 PoE 功能需要考虑两个因素：

- PSE 可以提供的功率
- PD 实际尝试消耗的功率

您可以决定：

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

注 在设备运行时将模式从“级别限制”更改为“端口限制”会强制受电设备重启，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 Trap，以及生成 Trap 时 PD 所耗功率占最大功率的百分比。

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

如果在连接的任意时刻，所连接的 PD 从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 Trap

注 如果将低电压 PoE 设备连接到采用 PoE 的 SG500 系列设备，并通过连接两端的启用 PoE 的端口进行连接，低电压设备将丧失为任何受电设备供电的能力。为避免出现这种情况，需在 SG500 上禁用 PoE 支持或使用非 PoE 端口。



注意

连接能够提供 PoE 的交换机时，请考虑以下事项：

PoE 型号的 Sx200、Sx300 和 SF500 系列交换机均为 PSE（供电设备），能够为连接 PD（受电设备）提供直流电源。这些设备包括 VoIP 电话、IP 摄像头和无线接入点。PoE 交换机可以检测出非标准的旧式 PoE 受电设备并为其供电。由于支持传统 PoE，因此用作 PSE 的 PoE 设备可能会为连接 PSE（包括作为传统 PD 的其他 PoE 交换机）检测和提供电源时出错。

即使 Sx200/300/500 PoE 交换机为 PSE 并因此而应采用交流供电，但是因为会发生错误检测，所以这些交换机可作为传统 PD 由其他 PSE 为其供电。发生这种情况时，PoE 设备可能无法正常工作，并且可能无法正确地为其连接的 PD 供电。

为防止检测错误，您应禁用 PoE 交换机上用于连接 PSE 的端口的 PoE 功能。您还应先接通 PSE 设备的电源，然后再将其连接至 PoE 设备。如果某设备被错误地检测为 PD，您应断开该设备与 PoE 端口的连接，并用交流电源为其供电，然后再将其重新连接至 PoE 端口。

配置 PoE 属性

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

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

在加电重启、初始化和系统配置过程中禁用功率输出，以确保不会损坏 PD。

在设备上配置 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** - 请选择以下选项之一：
 - **端口限制** - 由用户配置针对每个端口的最大功率限制。
 - **类限制** - 由设备类别（从分类阶段获取）决定每个端口的最大功率限制。
- **Trap** - 启用或禁用 Trap。如果已启用 Trap，您还必须启用 SNMP，并配置至少一个 SNMP 通知接收设备。
- **功率 Trap 阈值** - 输入使用率阈值，该值为功率限制的百分比。如果功率超过了该值，便会发出告警。

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。

对于每台设备或堆叠的所有单元，将显示以下计数器：

- **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。

步骤 3 单击**应用**，保存 PoE 属性。

配置 PoE 设置

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

注 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。

单击**端口管理 > PoE > 设置**。

本页面会根据供电模式，通过两种方式限制每个端口的功率：

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

当端口消耗的功率超过端口限制时，将会停止为端口供电。

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

当端口消耗的功率超过类别限制时，将会停止为端口供电。

PoE 优先级示例：

假设：一个 48 端口设备提供 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[设备型号](#)。

配置 PoE 端口设置的步骤：

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

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

步骤 3 为以下字段输入值：

- **接口** - 选择要配置的端口。

- **PoE 管理状态** - 在端口上启用或禁用 PoE。
- **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。时间范围已在[时间范围](#)页面进行过定义。
- **电源优先级** - 选择供电不足时使用的端口优先级：低、高或重要。例如，如果供电使用率在 99%，端口 1 的优先级为高，而端口 3 的优先级为低，则将为端口 1 供电，而拒绝为端口 3 供电。
- **管理功率分配** - 仅当在 PoE “属性”页面中将供电模式设置为“端口限制”才会显示该字段。如果供电模式为“功率限制”，则请输入为该端口分配的功率（以毫瓦为单位）。
- **最大功率分配** - 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。
- **类** - 仅当在 PoE “属性”页面中将供电模式设置为“级别限制”才会显示该字段。类别将决定功率等级：

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

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

步骤 4 单击**应用**。端口的 PoE 设置将写入当前配置文件。

VLAN 管理

本节包括以下主题：

- VLAN
- 配置默认 VLAN 设置
- 创建 VLAN
- 配置 VLAN 接口设置
- 定义 VLAN 成员关系
- GVRP 设置
- VLAN 组
- 语音 VLAN
- 访问端口组播 TV VLAN
- 客户端口组播 TV VLAN

VLAN

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

VLAN 说明

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

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

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

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

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

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

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

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

出站端口：

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

VLAN 角色

VLAN 作用于第 2 层。所有 VLAN 流量（单播/广播/组播）均将始终处于其 VLAN 之内。连接到不同 VLAN 的设备无法通过以太网 MAC 层彼此直接连接。属于不同 VLAN 的设备只能通过第 3 层路由器相互通信。例如，如果每个 VLAN 代表一个 IP 子网，则需要 IP 路由器在 VLAN 之间路由 IP 流量。

IP 路由器可以是传统路由器，其上的每个接口仅连接到一个 VLAN。在传统 IP 路由器上收发的流量必须为 VLAN Untagged。该 IP 路由器可以为可识别 VLAN 的路由器，其上的每个接口可以连接到一个或多个 VLAN。在可识别 VLAN 的 IP 路由器上收发的流量可以为 VLAN Tagged，也可以为 VLAN Untagged。

毗邻的可识别 VLAN 的设备使用通用 VLAN 注册协议 (GVRP) 互相交换 VLAN 信息。因此，VLAN 信息将通过桥接网络进行传递。

可以根据设备之间交换的 GVRP 信息，以静态或动态方式创建设备上的 VLAN。VLAN 可以是静态的，也可以是动态的（通过 GVRP 创建），但不能既为静态又为动态。有关 GVRP 的详情，请参阅“GVRP 设置”一节。

某些 VLAN 可能具有其他角色，包括：

- 语音 VLAN：有关详情，请参阅“语音 VLAN”一节。
- 访客 VLAN：在“编辑 VLAN 验证”页面中设置。
- 默认 VLAN：有关详情，请参阅“配置默认 VLAN 设置”一节。
- 管理 VLAN（在第 2 层系统模式系统中）：有关详情，请参阅“第 2 层 IP 寻址”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，然后将其通过网络进行转发。S-tag 用于在保留客户 VLAN 标记的同时，分离不同客户间的流量。

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

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

QinQ 的另一个优势是，无需配置客户的边缘设备。

QinQ 在“VLAN 管理 > 接口设置”页面中启用。

VLAN 配置工作流程

配置 VLAN 的步骤：

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

6. 根据需要，按照**基于 MAC 的组**和**基于协议的 VLAN**两节中所述配置 VLAN 组。
7. 根据需要，按照**访问端口组播 TV VLAN**和**客户端端口组播 TV VLAN**两节中所述配置 TV VLAN。

配置默认 VLAN 设置

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

默认 VLAN 具有以下特性：

- 该 VLAN 是独特的非静态/非动态 VLAN，并且在默认情况下，所有端口都是它的 Untagged 成员。
- 该 VLAN 无法删除。
- 无法为该 VLAN 指定标签。
- 不能为该 VLAN 指定任何特殊的角色（例如未经验证的 VLAN 或语音 VLAN）。这仅适用于已启用 OUI 的语音 VLAN。
- 如果某端口不再是任何 VLAN 的成员，则设备会自动将该端口配置为默认 VLAN 的 Untagged 成员。在以下情况下，端口将不再是 VLAN 的成员：VLAN 已被删除或者已将该端口从 VLAN 删除。
- RADIUS 服务器无法使用动态 VLAN 分配将默认 VLAN 分配给 802.1x 请求方。

如果默认 VLAN 的 VID 发生更改，则在保存配置和重启设备后，设备会在 VLAN 中的所有端口上执行以下操作：

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

更改默认 VLAN 的步骤：

步骤 1 单击 **VLAN 管理 > 默认 VLAN 设置**。

步骤 2 为以下字段输入值：

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

步骤 3 单击**应用**。

步骤 4 单击**保存**（位于窗口的右上角），将当前配置保存到启动配置。

重启设备后，**重启后的默认 VLAN ID** 的值将成为**当前默认 VLAN ID**。

创建 VLAN

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

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

创建 VLAN 的步骤：

步骤 1 单击 **VLAN 管理 > VLAN 设置**。

此页面会为所有 VLAN 显示以下字段：

- **VLAN ID** - 用户定义的 VLAN ID。
- **VLAN 名称** - 用户定义的 VLAN 名称。
- **始发站** - VLAN 类型：
 - *GVRP* - VLAN 为通过通用 VLAN 注册协议 (GVRP) 动态创建。
 - *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 (VID)** 及 **VLAN 名称**（可选）。

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

步骤 4 单击**应用**，创建 VLAN。

配置 VLAN 接口设置

使用“接口设置”页面可显示和配置所有接口的 VLAN 相关参数

配置 VLAN 设置的步骤：

步骤 1 单击 **VLAN 管理 > 接口设置**。

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

步骤 3 选择要配置的端口或 LAG，然后单击**编辑**。

步骤 4 为以下字段输入值：

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

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

步骤 5 单击**应用**。参数将写入当前配置文件中。

定义 VLAN 成员关系

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

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

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，或者这些设备必须通过通用 VLAN 注册协议 (GVRP) 动态学习 VLAN 及其端口成员关系。

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

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

配置 VLAN 端口

使用 “端口到 VLAN” 页面显示和配置特定 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”或“客户”）。

每个端口或 LAG 均将与其对 VLAN 的目前注册一起显示。

步骤 3 通过从以下列表中选择所需的选项来更改接口对 VLAN 的注册：

- **已禁止** - 不允许接口加入 VLAN（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。这是所有端口和 LAG 的默认选项。端口可以通过 GVRP 注册加入 VLAN。
- **Tagged** - 接口是 VLAN 的 Tagged 成员。
- **Untagged** - 接口为 VLAN 的 Untagged 成员。会将 Untagged VLAN 帧发送到接口 VLAN。
- **组播 TV VLAN** - 用于使用组播 IP 的数字 TV 的接口。端口加入 VLAN 标记为组播 TV VLAN 的 VLAN。有关详情，请参阅[访问端口组播 TV VLAN](#)。
- **PVID** - 选择该选项会将接口的 PVID 设置为 VLAN 的 VID。PVID 是一个针对端口的设置。

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

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

配置 VLAN 成员关系

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

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

- 在对端口进行验证之前，会将其排除在所有 VLAN 之外（访客和未经验证的端口除外）。在“VLAN 到端口”页面中，端口标记有大写的 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。

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。在 500 系列设备上选择“单元/插槽”。
- **模式** - 显示在“接口设置”页面中选择的端口 VLAN 模式。
- **选择 VLAN** - 要将端口与 VLAN 关联，请使用箭头键将左侧列表中的 VLAN ID 移到右侧列表。如果默认 VLAN 添加了标记，则可能会显示在右侧列表中，但无法选择。
- **标记** - 选择以下添加标记/PVID 选项之一：
 - **Tagged** - 选择端口是否 Tagged。该选项不适用于访问端口。
 - **Untagged** - 选择端口是否 Untagged。该选项不适用于访问端口。
 - **PVID** - 将端口 PVID 设置为此 VLAN。如果接口为“访问”模式或“中继”模式，设备会自动使接口成为 VLAN 的 Untagged 成员。如果接口为“一般”模式，则必须手动配置 VLAN 成员关系。

步骤 5 单击**应用**。将修改设置，并将其写入当前配置文件中。

要查看接口上的管理和运行 VLAN，请单击**详情**。

GVRP 设置

可识别 VLAN 的相邻设备可使用通用 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。

由于 GVRP 需要支持添加标记，因此必须在“中继”模式或“一般”模式下配置端口。

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，将在全局和端口上禁用 GVRP。

定义 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**。将修改 GVRP 设置，并将其写入当前配置文件中。

VLAN 组

VLAN 组用于第 2 层网络上的流量负载均衡。

根据已配置的各种分类（例如 VLAN 组）将数据包分配给一个 VLAN。

如果已定义多个分类机制，则会按照以下顺序将数据包分配给一个 VLAN：

- **TAG：**如果数据包为 Tagged 数据包，则可以根据该标签获取 VLAN。
- **基于 MAC 的 VLAN：**如果已定义基于 MAC 的 VLAN，则会通过入口接口的源 MAC 到 VLAN 映射获取该 VLAN。
- **基于协议的 VLAN：**如果已定义基于协议的 VLAN，则会通过入口接口的（以太网类型）协议到 VLAN 映射获取 VLAN。
- **PVID：**根据端口默认 VLAN ID 获取 VLAN。

基于 MAC 的组

基于 MAC 的 VLAN 分类可根据数据包的源 MAC 地址分类数据包。随后，您可以定义每个接口的 MAC 到 VLAN 映射。

您可以定义多个基于 MAC 的 VLAN 组，每个组包含不同的 MAC 地址。

可以将这些基于 MAC 的组分配给特定端口/LAG。基于 MAC 的 VLAN 组不能包含相同端口上范围重叠的 MAC 地址。

下表介绍各种 SKU 中基于 MAC 的 VLAN 组的可用性：

表 1 基于 MAC 的 VLAN 组可用性

SKU	系统模式	支持的基于 MAC 的 VLAN 组
Sx300	第 2 层	是
	第 3 层	否
Sx500、Sx500ESW2-550X	第 2 层	是
	第 3 层	否
SG500X	原生	是
	基本混合 - 第 2 层	是
	基本混合 - 第 3 层	否
SG500XG	与 Sx500 相同	是

工作流程

定义基于 MAC 的 VLAN 组的步骤：

1. 将 MAC 地址分配给一个 VLAN 组 ID（使用“基于 MAC 的组”页面）。
2. 针对每个必需接口：
 - a. 将 VLAN 组分配给一个 VLAN（使用“基于 MAC 的组到 VLAN”页面）。接口必须处于“一般”模式下。
 - b. 如果接口不属于 VLAN，请使用“端口到 VLAN 页面”手动将其分配给 VLAN。

分配基于 MAC 的 VLAN 组

请参阅表 1，了解有关此功能可用性的说明。

将 MAC 地址分配给 VLAN 组的步骤：

步骤 1 单击 **VLAN 管理 > VLAN 组 > 基于 MAC 的组**。

步骤 2 单击**添加**。

步骤 3 为以下字段输入值：

- **MAC 地址** - 输入要分配给 VLAN 组的 MAC 地址。
注 不得将该 MAC 地址分配给任何其他 VLAN 组。
- **掩码** - 输入以下内容之一：
 - **主机** - MAC 地址的源主机
 - **长度** - MAC 地址的**前缀**
- **组 ID** - 输入用户创建的 VLAN 组 ID 号。

步骤 4 单击**应用**。会将该 MAC 地址分配给一个 VLAN 组。

针对每个接口将 VLAN 组映射到 VLAN

请参阅表 1，了解有关此功能可用性的说明。

端口/LAG 必须处于“一般”模式下。

将基于 MAC 的组分配给接口上的一个 VLAN 的步骤：

步骤 1 单击 **VLAN 管理 > VLAN 组 > 基于 MAC 的组到 VLAN**。

步骤 2 单击**添加**。

步骤 3 为以下字段输入值：

- **组类型** - 显示该组是基于 MAC 的。
- **接口** - 输入通过其接收流量的一般接口（端口/LAG）。
- **组 ID** - 选择一个在“基于 MAC 的组”页面中定义的 VLAN 组。
- **VLAN ID** - 选择将向其转发来自 VLAN 组的流量的 VLAN。

步骤 4 单击**应用**，设置 VLAN 组至 VLAN 的映射。此映射不会将接口动态绑定到 VLAN；必须将接口手动添加到 VLAN。

基于协议的 VLAN

可以定义多组协议，然后将它们绑定到一个端口。将协议组绑定到端口后，源自该组中协议的每个数据包都会分配给在“基于协议的组”页面中配置的 VLAN。

工作流程

定义基于协议的 VLAN 组的步骤：

1. 定义协议组（使用“基于协议的组”页面）。
2. 针对每个必需接口，将协议组分配给一个 VLAN（使用“基于协议的组至 VLAN”页面）。接口必须处于“一般”模式下，且不能有其分配的动态 VLAN (DVA)。

基于协议的组

定义协议集的步骤。

步骤 1 单击 **VLAN 管理 > VLAN 组 > 基于协议的组**。

“基于协议的组”页面包含以下字段：

- **封装** - 显示 VLAN 组所依据的协议。
- **协议值 (十六进制)** - 以十六进制格式显示协议值。
- **组 ID** - 显示要添加接口的协议组 ID。

步骤 2 单击**添加**按钮。此时将显示“添加基于协议的组”页面

步骤 3 输入以下字段：

- **封装** - 协议数据包类型。可能的选项有：
 - **以太网 V2** - 如果已选择该选项，请选择**以太网类型**。
 - **LLC-SNAP (rfc1042)** - 如果已选择该选项，请输入**协议值**。
 - **LLC** - 如果已选择该选项，请选择**DSAP-SSAP 值**。
- **以太网类型** - 为以太网 V2 封装选择以太网类型。这是以太网帧中的两位字节字段，用于指示以太网数据包的有效负荷中所封装的协议。
- **协议值** - 输入 LLC-SNAP (rfc 1042) 封装的协议。
- **DSAP-SSAP** - 为 LLC 封装输入这些值。
- **组 ID** - 输入协议组 ID。

步骤 4 单击**应用**。系统将添加协议组，并将其写入当前配置文件。

基于协议的组至 VLAN 映射

要将协议组映射到端口，该端口必须处于“一般”模式下且该端口上未配置 DVA（请参阅[配置 VLAN 接口设置](#)）。

可以将多个组绑定到单个端口，每个端口都与其自身的 VLAN 相关联。

也可以将多个组映射到单个 VLAN。

将协议端口映射到 VLAN 的步骤：

步骤 1 单击 **VLAN 管理 > VLAN 组 > 基于协议的组至 VLAN**。

会显示当前定义的映射。

步骤 2 要将接口与基于协议的组和 VLAN 关联，请单击**添加**。

步骤 3 输入以下字段：

- **接口** - 根据基于协议的组分配给 VLAN 的端口号或 LAG 号。
- **组 ID** - 协议组 ID。
- **VLAN ID** - 将接口连接到用户定义的 VLAN ID。

步骤 4 单击应用。系统会将协议端口映射到 VLAN，并将其写入当前配置文件。

语音 VLAN

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

本节包含以下主题：

- [语音 VLAN 概述](#)
- [配置语音 VLAN](#)

语音 VLAN 概述

本节包含以下主题：

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

下面是使用适当配置的典型语音部署方案：

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

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

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[配置电话 OUI](#)。

- **自动语音 VLAN**

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

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

语音端点

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

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

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

自动语音 VLAN、自动智能端口、CDP 和 LLDP

默认设置

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

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

语音 VLAN 触发

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

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

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

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

自动语音 VLAN

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

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

注 如果将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。

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

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

- 当 CDP 和 LLDP 启用时，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 + 桌面。

语音 VLAN QoS

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

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

若在 OUI 模式下，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。在自动语音 VLAN 模式下，您可以使用高级 QoS 覆盖语音流的值。对于电话 OUI 语音流，您可以通过指定所需的 CoS/802.1p 值，并使用“电话 OUI”下面的重新标记选项，覆盖服务质量，并可以选择重新标记语音流的 802.1p。

语音 VLAN 限制

存在以下限制：

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

此外，以下限制也适用于电话 OUI：

- 语音 VLAN 不能是 VLAN 1（默认 VLAN）。
- 语音 VLAN 不能启用智能端口。
- 语音 VLAN 不能支持 DVA（动态 VLAN 分配）。
- 如果语音 VLAN 模式为“OUI”，则语音 VLAN 不能是访客 VLAN。如果语音 VLAN 模式为“自动”，则语音 VLAN 可以是访客 VLAN。
- 语音 VLAN QoS 决策的优先级高于任何其他 QoS 决策（策略/ACL QoS 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。本节介绍了当未应用默认配置时，如何部署语音 VLAN。

工作流程 1: 配置自动语音 VLAN 的步骤:

步骤 1 打开“VLAN 管理 > 语音 VLAN > 属性”页面。

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

步骤 3 设置**动态语音 VLAN**为“启用自动语音 VLAN”。

步骤 4 选择**自动语音 VLAN 激活方法**。

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

步骤 5 单击**应用**。

步骤 6 按**常见智能端口任务**一节中所述配置智能端口。

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

步骤 8 使用“智能端口 > 接口设置”页面启用相关端口上的智能端口特性。

注 步骤 7 和步骤 8 是可选的，因为这两项在默认情况下处于启用状态。

工作流程 2: 配置电话 OUI 方法的步骤

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

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

步骤 2 在“电话 OUI”页面中配置电话 OUI。

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

配置语音 VLAN

本节介绍了如何配置语音 VLAN。其中包含以下主题：

- [配置语音 VLAN 属性](#)
- [显示自动语音 VLAN 设置](#)
- [配置电话 OUI](#)

配置语音 VLAN 属性

使用“语音 VLAN 属性”页面完成以下操作：

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

查看和配置语音 VLAN 属性的步骤：

步骤 1 单击 **VLAN 管理 > 语音 VLAN > 属性**。

- **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 为以下字段输入值：

- **语音 VLAN ID** - 输入要作为语音 VLAN 的 VLAN。
注 语音 VLAN ID、CoS/802.1p 和/或 DSCP 中的更改会导致设备将管理语音 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](#)。
- **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。

显示自动语音 VLAN 设置

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

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

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

查看自动语音 VLAN 参数的步骤：

步骤 1 单击 **VLAN 管理 > 语音 VLAN > 自动语音 VLAN**。

此页面上的运行状态框将显示有关当前语音 VLAN 及其源的信息：

- **自动语音 VLAN 状态** - 显示是否已启用自动语音 VLAN。
- **语音 VLAN ID** - 当前语音 VLAN 标识符
- **源类型** - 显示根设备发现的语音 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。可能的选项有：
 - **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。可能的选项有：
 - **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

配置电话 OUI

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

OUI 全局表最多可包含 128 个 OUI。

本节包含以下主题:

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

将 OUI 添加至电话 OUI 表

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

使用“电话 OUI”页面可查看现有 OUI, 并添加新的 OUI。

配置电话 OUI 和/或添加新的语音 VLAN OUI 的步骤:

步骤 1 单击 **VLAN 管理 > 语音 VLAN > 电话 OUI**。

“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。

此时将显示电话 OUI 表:

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

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

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

步骤 4 要添加新的 OUI, 请单击**添加**。

步骤 5 为以下字段输入值：

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

步骤 6 单击**应用**。将 OUI 添加至电话 OUI 表。

将接口添加至基本 OUI 上的语音 VLAN

在以下一种模式下，QoS 属性可按端口分配给语音数据包：

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

使用“电话 OUI 接口”页面，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。
- **电话 VLAN QoS 模式** - 选择以下选项中的一个：
 - **全部** - QoS 属性应用于分类为属于语音 VLAN 的所有数据包上。
 - **电话源 MAC 地址** - QoS 属性仅应用于来自 IP 电话的数据包上。

步骤 4 单击**应用**。将添加 OUI。

访问端口组播 TV VLAN

使用组播 TV VLAN，可对位于不同数据 VLAN（第 2 层隔离）中的用户进行组播传输，而不会复制每个用户 VLAN 的组播传输帧。

用户若位于不同数据 VLAN（第 2 层隔离）且连接到具有不同 VLAN ID 成员关系的设备，则可以通过将端口加入到相同组播 VLAN ID 来共享相同组播流。

连接到组播服务器的网络端口会静态配置为组播 VLAN ID 中的成员。

用户与组播服务器进行通信（通过发送 IGMP 消息）所经由的网络端口，会接收来自组播服务器的组播流，而且包括组播数据包报头中的组播 TV VLAN。为此，必须将网络端口静态配置为以下类型：

- 中继或一般端口类型（请参阅[配置 VLAN 接口设置](#)）
- 组播 TV VLAN 上的成员

可以将用户接收器端口与组播 TV VLAN 关联，但前提是必须使用以下其中一种类型定义组播 TV VLAN：

- 访问端口
- 客户端口（请参阅[客户端口组播 TV VLAN](#)）。

可以将一个或多个 IP 组播地址组与相同组播 TV VLAN 关联。

任何 VLAN 都可以配置为组播 TV VLAN。分配给组播 TV VLAN 的端口：

- 加入组播 TV VLAN。
- 通过组播 TV VLAN 中出口端口的数据包为 Untagged 数据包。
- 端口的帧类型参数设置为**全部接受**，从而允许接收 Untagged 数据包（请参阅[配置 VLAN 接口设置](#)）。

组播 TV VLAN 配置是按照每个端口进行定义的。可使用“组播 TV VLAN”页面将客户端口配置为组播 TV VLAN 的成员。

IGMP Snooping

组播 TV VLAN 依赖于 IGMP Snooping，这表示：

- 用户使用 IGMP 消息可加入或离开组播组。
- 设备根据其在组播 TV VLAN 上的组播成员关系，执行 IGMP Snooping 并配置访问端口。

设备针对每个在访问端口上接收的 IGMP 数据包，根据以下规则决定要将数据包与访问 VLAN 关联还是与组播 TV VLAN 关联：

- 如果在使用与端口的组播 TV VLAN 关联的目的组播 IP 地址的访问端口上接收 IGMP 消息，则软件会将 IGMP 数据包与组播 TV VLAN 关联。
- 另外，IGMP 消息还会关联至访问 VLAN，并且只会在该 VLAN 内转发此 IGMP 消息。
- 若出现以下情况，则会丢弃 IGMP 消息：
 - 访问端口上的 STP/RSTP 状态为**丢弃**。
 - 访问 VLAN 的 MSTP 状态为**丢弃**。
 - 组播 TV VLAN 的 MSTP 状态为**丢弃**，且 IGMP 消息与此组播 TV VLAN 关联。

常规 VLAN 与组播 TV VLAN 之间的差异

常规 VLAN 与组播 TV VLAN 的特性

	常规 VLAN	组播 TV VLAN
VLAN 成员关系	源和所有接收器端口必须为同一数据 VLAN 中的静态成员。	源和接收器端口不能为同一数据 VLAN 中的成员。
组注册	所有组播组注册均是动态的。	必须将组静态关联至组播 VLAN，但工作站的实际注册是动态的。
接收器端口	VLAN 可用来发送和接收流量（组播和单播）。	组播 VLAN 只能用来通过端口上的工作站接收流量（仅组播）。
安全与隔离	同一组播流的接收器位于同一数据 VLAN 中，可相互通信	同一组播流的接收器位于不同访问 VLAN 中，彼此隔离

配置

工作流程

通过以下步骤配置 TV VLAN：

1. 通过将组播组关联至 VLAN（使用“组播组至 VLAN”页面）来定义 TV VLAN。
2. 指定每个组播 VLAN 中的访问端口（使用“端口组播 VLAN 成员关系”页面）。

组播 TV 组至 VLAN

定义组播 TV VLAN 配置的步骤：

步骤 1 单击 **VLAN 管理 > 访问端口组播 TV VLAN > 组播组至 VLAN**。

此时将显示以下字段：

- **组播组** - 组播组的 IP 地址。
- **组播 TV VLAN** - 组播数据包所分配给的 VLAN。

步骤 2 单击**添加**以将组播组关联至 VLAN。可以选择任何 VLAN。选择 VLAN 后，该 VLAN 将成为组播 TV VLAN。

步骤 3 单击**应用**。将修改组播 TV VLAN 设置，并将其写入当前配置文件。

端口组播 VLAN 成员关系

定义组播 TV VLAN 配置的步骤：

步骤 1 单击 **VLAN 管理 > 访问端口组播 TV VLAN > 端口组播 VLAN 成员关系**。

步骤 2 从**组播 TV VLAN** 字段中选择一个 VLAN。

步骤 3 **候选访问端口**列表中包含设备上配置的所有访问端口。将所需端口从**候选访问端口**字段移至**成员访问端口**字段。

步骤 4 单击**应用**。将修改组播 TV VLAN 设置，并将其写入当前配置文件。

客户端口组播 TV VLAN

三网融合服务通过单个宽带连接提供三种宽带服务：

- 高速互联网接入
- 视频
- 语音

三网融合服务专为服务提供商用户提供，同时可保持这些用户之间的第 2 层隔离。

每个用户都有一个 CPE MUX 盒。MUX 有多个连接至用户设备（PC、电话等）的访问端口，以及一个连接至访问设备的网络端口。

该 CPE MUX 盒会根据数据包的 VLAN 标签，将数据包从网络端口转发到用户的设备中。每个 VLAN 均映射到其中一个 MUX 访问端口。

从用户到服务提供商网络的数据包会作为 VLAN tagged 帧转发，以便区分服务类型，这表示对于每个服务类型，CPE 盒中只有唯一的 VLAN ID。

访问设备会使用配置为客户 VLAN（外层标签，即 S-VID）的用户 VLAN，对从用户到服务提供商网络的所有数据包进行封装，来自 TV 接收器且与组播 TV VLAN 关联的 IGMP Snooping 消息除外。对于也是从 TV 接收器发送的 VOD 信息，其发送方式与任何其他类型的流量一样。

在网络端口上接收的、从服务提供商网络到用户的数据包会在服务提供商网络上作为双层标签数据包发送，而外层标签（服务标签，即 S-Tag）则代表以下两种 VLAN 类型的其中之一：

- 用户的 VLAN（包括互联网和 IP 电话）
- 组播 TV VLAN

内层 VLAN (C-Tag) 是确定用户网络中的目的地址（通过 CPE MUX）的标签。

工作流程

1. 将访问端口配置为客户端口（使用“VLAN 管理 > 接口设置”页面）。有关详情，请参阅 [QinQ](#)。
2. 使用作为 Tagged VLAN 的用户和组播 TV VLAN 将网络端口配置为中继端口或一般端口。（使用“VLAN 管理 > 接口设置”页面。）
3. 创建最多具有 4094 个不同 VLAN 的组播 TV VLAN。（通过常规 VLAN 管理设置完成 VLAN 的创建）
4. 使用“端口组播 VLAN 成员关系”页面将客户端口关联至组播 TV VLAN。

5. 使用“CPE VLAN 至 VLAN”页面将 CPE VLAN (C-TAG) 映射至组播 TV VLAN (S-Tag)。

将 CPE VLAN 映射至组播 TV VLAN

要支持使用用户 VLAN 的 CPE MUX，用户可能需要多个视频提供商，并且要为每个提供商分配一个不同的外部 VLAN。

CPE（内部）组播 VLAN 必须映射至组播提供商（外部）VLAN。

CPE VLAN 映射至组播 VLAN 之后，便可以加入 IGMP Snooping。

映射 CPE VLAN 的步骤：

步骤 1 单击 **VLAN 管理 > 客户端口组播 TV VLAN > CPE VLAN 至 VLAN**。

步骤 2 单击**添加**。

步骤 3 输入以下字段：

- **CPE VLAN** - 输入在 CPE 盒上定义的 VLAN。
- **组播 TV VLAN** - 选择映射至 CPE VLAN 的组播 TV VLAN。

步骤 4 单击**应用**。将修改 CPE VLAN 映射，并将其写入当前配置文件。

CPE 端口组播 VLAN 成员关系

与组播 VLAN 关联的端口必须配置为客户端口（请参阅[配置 VLAN 接口设置](#)）。

根据[端口组播 VLAN 成员关系](#)中所述，使用“端口组播 VLAN 成员关系”页面将这些端口映射至组播 TV VLAN

生成树

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

- **STP 模式**
- **配置 STP 状态和全局设置**
- **定义生成树接口设置**
- **配置快速生成树设置**
- **多生成树**
- **定义 MSTP 属性**
- **将 VLAN 映射到 MSTP 实例**
- **定义 MSTP 实例设置**
- **定义 MSTP 实例设置**

STP 模式

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

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

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

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。本协议在网络拓扑本身为树状结构，从而可以实现快速聚合的情况下最有效。默认情况下，系统会启用 RSTP。
- 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 VLAN A 中存在环路，而 VLAN B 中没有环路的情况。如果两个 VLAN 都在端口 X 上，而 STP 为缓解环路造成的影响，将会停止整个端口上的流量传输，包括 VLAN B 流量。

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。通过将实例与 VLAN 相关联，每个实例都将与要在其上执行环路检测和缓解的第 2 层域关联。这样可实现在一个实例中停止一个端口，例如停止造成环路的 VLAN A 中的流量，而其他不存在环路的域（例如 VLAN B）中的流量可以保持传输。

配置 STP 状态和全局设置

“STP 状态和全局设置”页面包含用于启用 STP、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** - 在设备上启用或禁用 STP。
- **STP 运行模式** - 选择一种 STP 模式。
- **BPDU 处理** - 选择在端口或设备上禁用 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，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。
- **Hello Time** - 设置根网桥在配置消息之间等待的时间间隔（以秒为单位）。
- **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[定义生成树接口设置](#)。

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。

定义生成树接口设置

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

输入的定义的配置对于任何模式的 STP 协议均有效。

在接口上配置 STP 的步骤：

步骤 1 单击**生成树 > STP 接口设置**。

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。

- **根防护** - 在设备上启用或禁用“根防护”。“根防护”选项提供了一种在网络中强制执行根网桥放置的方法。

根防护可确保启用此功能的端口为指定端口。通常，除非根网桥的两个或更多端口连接在一起，否则所有根网桥端口均为指定端口。如果网桥在启用根网桥的端口上收到高级 BPDU，则根防护会将此端口转换为根不一致 STP 状态。这种根不一致状态实际上等同于监听状态。此时不会通过此端口转发任何流量。这样一来，根防护便可强制确定根网桥的位置。

- **BPDU 防护** - 在端口上启用或禁用网桥协议数据单元 (BPDU) 防护功能。

使用 BPDU 防护，可以强制实施 STP 域边界，并使活动拓扑保持可预测状态。启用 BPDU 防护的端口后的设备无法影响 STP 拓扑。接收 BPDU 时，BPDU 防护操作会禁用已配置 BPDU 的端口。在这种情况下，会接收 BPDU 消息并生成相应的 SNMP Trap。
- **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“STP 状态和全局设置”页面中定义的设置。
 - *过滤* - 在接口上禁用生成树时，过滤 BPDU 数据包。
 - *泛洪* - 在接口上禁用生成树时，泛洪 BPDU 数据包。
- **路径成本** - 设置端口产生的根路径成本，或使用系统生成的默认成本。
- **优先级** - 设置端口的优先级值。如果网桥在一个环路中连接了两个端口，则优先级值会影响端口选择。优先级是从 0 到 240 的值，设置增量为 16。
- **端口状态** - 显示端口的目前 STP 状态。
 - *已禁用* - 目前在端口上禁用 STP。端口在学习 MAC 地址的同时转发流量。
 - *阻塞* - 端口目前被阻塞，无法转发流量（BPDU 数据除外）或学习 MAC 地址。
 - *监听* - 端口处于监听模式。端口无法转发流量，也无法学习 MAC 地址。
 - *学习* - 端口处于学习模式。端口无法转发流量，但能够学习新的 MAC 地址。
 - *转发* - 端口处于转发模式。端口可以转发流量且学习新的 MAC 地址。
- **指定的网桥 ID** - 显示指定网桥的网桥优先级和 MAC 地址。
- **指定的端口 ID** - 显示所选端口的优先级和接口。
- **指定成本** - 显示加入 STP 拓扑的端口的成本。如果 STP 检测到环路，则成本越低的端口越不容易被阻塞。
- **转发转换** - 显示端口从阻塞状态变成转发状态的次数。
- **速度** - 显示端口速度。
- **LAG** - 显示端口所属的 LAG。如果端口是某 LAG 的成员，则 LAG 设置会覆盖端口设置。

步骤 4 单击**应用**。接口设置将写入当前配置文件。

配置快速生成树设置

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

使用“RSTP 接口设置”页面可针对每个端口配置 RSTP。如果将全局 STP 模式设置为 RSTP 或 MSTP，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**。启用 **RSTP**。

步骤 2 单击**生成树 > RSTP 接口设置**。此时将显示“RSTP 接口设置”页面：

步骤 3 选择一个端口。

注 仅在选择连接至所测试的网桥伙伴的端口之后，“激活协议迁移”才可用。

步骤 4 如果使用 STP 发现了链路伙伴，请单击**激活协议迁移**运行协议迁移测试。这可确定使用 STP 的链路伙伴是否仍然存在，如果存在，可确定该链路伙伴是否已迁移到 RSTP 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 5 选择一个接口，并单击**编辑**。

步骤 6 输入参数：

- **接口** - 设置接口，并指定要配置 RSTP 的端口或 LAG。
- **点到点管理状态** - 定义点到点的链路状态。定义为全双工的端口会被视为点到点端口链路。
 - **启用** - 如果启用了此功能，该端口便是一个 RSTP 边缘端口，它可以迅速地进入转发模式（通常在 2 秒以内）。
 - **禁用** - 不会出于 RSTP 目的将该端口视为点到点端口，这表示 STP 在该端口上将以正常速度而非高速工作。
 - **自动** - 使用 RSTP BPDU 自动确定设备状态。
- **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** - 提供从根接口到根网桥的备用路径。
 - **备份** - 提供指向生成树叶节点的指定端口路径的备份路径。这会提供一种配置，其中一个环路中的两个端口会通过一条点到点链路进行连接。如果 LAN 具有两条或更多条已建立的、至一个共享网段的连接，则也会使用备份端口。
 - **已禁用** - 端口不会加入生成树。
- **模式** - 显示目前的生成树模式：传统 STP 或 RSTP。
- **快速链路运行状态** - 显示接口上的快速链路（边缘端口）模式状态：已启用、已禁用或自动。这些值包括：
 - **已启用** - 启用快速链路。
 - **已禁用** - 禁用快速链路。
 - **自动** - 在接口开始活动后的几秒内启用快速链路模式。
- **端口状态** - 显示特定端口上的 RSTP 状态。
 - **已禁用** - 目前在端口上禁用 STP。
 - **阻塞** - 端口目前被阻塞，其无法转发流量或学习 MAC 地址。
 - **监听** - 端口处于监听模式。端口无法转发流量，也无法学习 MAC 地址。
 - **学习** - 端口处于学习模式。端口无法转发流量，但能够学习新的 MAC 地址。
 - **转发** - 端口处于转发模式。端口可以转发流量且学习新的 MAC 地址。

步骤 7 单击**应用**。将更新当前配置文件。

多生成树

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：

1. 按[配置 STP 状态和全局设置](#)页面中所述将“STP 运行模式”设置为 MSTP。
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[将 VLAN 映射到 MSTP 实例](#)一节。
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。
4. 通过以下操作配置 MSTP 属性：
 - [定义 MSTP 属性](#)
 - [定义 MSTP 实例设置](#)
 - [将 VLAN 映射到 MSTP 实例](#)

定义 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**。启用 MSTP。

步骤 2 单击[生成树](#) > **MSTP 属性**。

步骤 3 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 4 单击**应用**。将定义 MSTP 属性，并更新当前配置文件。

将 VLAN 映射到 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。

在 500 系列交换机上，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：

- **MST 实例 ID** - 显示所有 MST 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 输入参数。

- **MST 实例 ID** - 选择 MST 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**。将定义 MSTP VLAN 映射，并更新当前配置文件。

定义 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** - 显示保留到下个目的地的跃点数。

步骤 3 单击**应用**。将定义 MST 实例配置，并更新当前配置文件。

定义 MSTP 实例设置

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**。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。
 - *阻塞* - 该实例上的端口目前被阻塞，无法转发流量（BPDU 数据除外）或学习 MAC 地址。
 - *监听* - 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* - 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* - 该接口提供从根接口到根设备的备用路径。
 - *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** - 显示到下个目的地剩余的步跳数。
- **转发转换** - 显示端口从转发状态变成阻塞状态的次数。

步骤 6 单击**应用**。将更新当前配置文件。

管理 MAC 地址表

本节介绍了如何将 MAC 地址添加到系统。其中包含以下主题：

- 配置静态 MAC 地址
- 管理动态 MAC 地址
- 定义保留 MAC 地址

MAC 地址的类型

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

静态地址由用户进行配置，因此不会过期。

在到达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/匹配的目的 MAC 地址。如果找到匹配项，则将此帧标记为通过地址表中指定的端口输出。如果帧的目的 MAC 地址不在这两个地址表中，则会将这些帧传输/广播到相应 VLAN 上的所有端口。此类帧也称为未知的单播帧。

设备最多支持 8,000 个静态和动态 MAC 地址。

配置静态 MAC 地址

可以将静态 MAC 地址分配给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（单元/插槽、端口或 LAG）。
- **状态** - 选择条目的处理方式。选项如下：
 - **永久** - 系统永远不会删除此 MAC 地址。如果静态 MAC 地址保存在启动配置中，则重启后会保留该地址。
 - **重置即删除** - 重置设备时，会删除静态 MAC 地址。
 - **超时即删除** - 当该 MAC 地址过期时将其删除。
 - **安全** - 当接口为传统锁定模式（请参阅[配置端口安全](#)）时，MAC 地址是安全的。

步骤 4 单击**应用**。将在地址表中显示一个新条目。

管理动态 MAC 地址

动态地址表（桥接表）中包含通过监控进入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内没有接收到相应的流量，系统会删除该地址。该时间段为过期间隔。

配置动态 MAC 地址过期时间

配置动态地址过期间隔的步骤：

- 步骤 1** 单击 **MAC 地址表 > 动态地址设置**。
- 步骤 2** 在**过期时间**字段中输入值。过期时间值介于用户配置的值与该值的两倍减 1 之间。例如，如果输入 300 秒，则过期时间将介于 300 到 599 秒之间。
- 步骤 3** 单击**应用**。将更新过期时间。

查询动态地址

查询动态地址的步骤：

- 步骤 1** 单击 **MAC 地址表 > 动态地址**。
- 步骤 2** 在**过滤框**中，您可以输入以下查询条件：
 - **VLAN ID** - 输入要在地址表中查询的 VLAN ID。
 - **MAC 地址** - 输入要在地址表中查询的 MAC 地址。
 - **接口** - 选择要在地址表中查询的接口。查询功能可以搜索特定单元/插槽、端口或 LAG。
- 步骤 3** 在**动态地址表排序关键字**字段中输入值以作为地址表的排序依据。地址表可以按 VLAN ID、MAC 地址或接口进行排序。
- 步骤 4** 单击**转至**。将对动态 MAC 地址表进行查询并显示结果。
要删除所有动态 MAC 地址，请单击**清除表**。

定义保留 MAC 地址

如果设备收到目的 MAC 地址在保留地址范围（根据 IEEE 标准的规定）内的帧，可以丢弃或桥接此帧。保留的 MAC 地址表中的条目可以指定保留的 MAC 地址，或者指定保留的 MAC 地址和帧类型：

添加保留的 MAC 地址条目的步骤：

步骤 1 单击 **MAC 地址表 > 保留的 MAC 地址**。将打开“保留的 MAC 地址”页面。

步骤 2 单击**添加**。

步骤 3 为以下字段输入值：

- **MAC 地址** - 选择要保留的 MAC 地址。
- **帧类型** - 根据以下标准选择帧类型：
 - *以太网 V2*- 适用于具有该特定 MAC 地址的以太网 V2 数据包。
 - *LLC*- 适用于具有该特定 MAC 地址的逻辑链路控制 (LLC) 数据包。
 - *LLC-SNAP*- 适用于具有该特定 MAC 地址的逻辑链路控制/子网接入协议 (LLC-SNAP) 数据包。
 - *全部*- 适用于所有使用特定 MAC 地址的数据包。
- **操作** - 选择以下其中一项操作，以便在接收到符合所选标准的数据包时执行该操作：
 - *丢弃*- 删除数据包。
 - *网桥*- 将数据包转发给所有 VLAN 成员。

单击**应用**。将保留一个新的 MAC 地址。

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
- 定义组播属性
- 添加 MAC 组地址
- 添加 IP 组播组地址
- 配置 IGMP Snooping
- MLD Snooping
- 查询 IGMP/MLD IP 组播组
- 定义组播路由器端口
- 定义“全部转发”组播
- 定义未注册的组播设置

组播转发

组播转发实现了一对多的信息传递。组播应用对于将信息传递给多个客户端非常有用，在这种情况下客户端不需要接收全部内容。类似于有线电视的服务是一种典型应用，在这种情况下客户端可以加入传输中心的频道，并在结束之前离开。

仅将数据发送给相关端口。仅对相关端口转发数据可节省链接上的带宽和主机资源。

要使组播转发能够在 IP 子网间正常工作，节点和路由器必须能进行组播。能进行组播的节点必须能够：

- 发送和接收组播数据包。
- 通过本地路由器注册节点正在监听的组播地址，以便本地路由器和远程路由器可以将组播数据包路由到节点。

典型的组播设置

当组播路由器在 IP 子网间路由组播数据包时，能进行组播的第 2 层交换机会将组播数据包转发到 LAN 或 VLAN 中已注册的节点。

典型设置包括在专用和/或公共 IP 网络间转发组播流的路由器、采用 Internet 组成员协议 (IGMP) Snooping 功能或组播侦听器发现 (MLD) Snooping 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 查询。

注 针对 IPv6 的 MLD 衍生自针对 IPv4 的 IGMP v2。虽然本节中主要介绍的是 IGMP，但也涵盖了对 MLD 的隐含介绍。

这些查询会访问设备，该设备转会将查询泛洪到 VLAN，并且也会学习其中包含组播路由器（组播路由器）的端口。当主机接收到 IGMP 查询消息时，它会通过 IGMP 加入消息作出响应，表示该主机要接收特定组播流，并且可有选择地从特定源进行接收。使用 IGMP Snooping 的设备会分析加入消息，并了解到必须将主机所请求的组播流转发到此特定端口。然后，交换机会只将 IGMP 加入转发到 Mrouter。同样地，当 Mrouter 接收到 IGMP 加入消息后，会了解到它接收加入消息的接口要接收特定组播流。Mrouter 会将请求的组播流转发到该接口。

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 Snooping 并接收组播流的帧时，它会将组播帧转发到经过注册可使用 IGMP 加入消息接收组播流的所有端口。

设备可根据以下选项之一转发组播流：

- 组播 MAC 组地址
- IP 组播组地址 (G)
- 组播数据包的源 IP 地址 (S) 和目的 IP 组播组地址 (G) 的组合。

可以为每个 VLAN 配置上述选项之一。

系统会维护每个 VLAN 的组播组列表，并且这会管理每个端口应接收的组播信息。使用 IGMP 或组播侦听器发现 (MLD) 协议监听可以静态地配置或动态地学习组播组及其进行接收的端口。

组播注册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 Snooping 时，该设备会分析其接收的所有 IGMP/MLD 数据包（来自连接到设备的 VLAN 和网络中的组播路由器）。

当设备了解到主机正在使用 IGMP/MLD 消息进行注册以接收组播流时（或者从特定源进行接收），该设备会在其组播转发数据库中添加注册。

IGMP/MLD Snooping 可有效减少来自带宽密集型串流 IP 应用程序的组播流量。使用 IGMP/MLD Snooping 的设备只会将组播流量转发给对该流量感兴趣的主机。这种组播流程的减少还会减少设备上处理的数据包，也会减少终端主机上的工作负荷，这是因为它们不必接收和过滤网络中生成的所有组播流量。

系统可支持以下版本：

- IGMP v1/v2/v3
- MLD v1/v2
- 简单的 IGMP Snooping 查询器

为便于在指定子网上使用 IGMP 协议，IGMP 查询器是必需的。通常，组播路由器也可作为 IGMP 查询器。当一个子网中有多个 IGMP 查询器时，这些查询器会选择单个查询器作为主要查询器。

可以将设备配置为作为备份查询器的 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。

组播地址属性

组播地址具有以下属性：

- 每个 IPv4 组播地址均处于 224.0.0.0 到 239.255.255.255 的地址范围之内。
- IPv6 组播地址为 FF00:/8。
- 将 IP 组播组地址映射至第 2 层组播地址的步骤：
 - 通过从 IPv4 地址中取得 23 个低序位并将它们添加到 01:00:5e 前缀之后，可以映射 IPv4。标准情况下，前九位 IP 地址会被忽略，并且会将任何仅不同于这前几位值的 IP 地址映射至同一第 2 层地址，这是因为所使用的后 23 位相同。例如，会将 234.129.2.3 映射至 MAC 组播组地址 01:00:5e:01:02:03。会将最多 32 个 IP 组播组地址映射至同一第 2 层地址。
 - 通过取得 32 个低序位组播地址并添加前缀 33:33，可映射 IPv6。例如，会将 IPv6 组播地址 FF00:1122:3344 映射至第 2 层组播 33:33:11:22:33:44。

定义组播属性

使用“属性”页面可配置网桥组播过滤状态。

默认情况下，会将所有组播帧泛洪到 VLAN 的所有端口。要选择性地将帧转发到相关端口并过滤（丢弃）其余端口上的组播，请在“属性”页面中启用网桥组播过滤状态。

如果启用过滤，则会将组播帧转发到相关 VLAN 中端口的子网，如组播转发数据库中所定义。将对所有流量实施组播过滤。默认情况下，会将此类流量泛洪到所有相关端口，但是您可以限制转发到较小的子网。

表示组播成员关系的常见方法是 (S,G) 标记法，其中 S 是指发送数据组播流的（单个）源，G 是指 IPv4 或 IPv6 组地址。如果组播客户端可以从特定组播组的任何源接收组播流量，则保存为 (*,G)。

以下是转发组播帧的方法：

- **MAC 组地址** - 根据以太网帧中的目的 MAC。

注 如上所述，可将一个或多个 IP 组播组地址映射至一个 MAC 组地址。根据 MAC 组地址进行转发，可导致 IP 组播流被转发至没有流接收器的端口。

- **IP 组地址** - 根据 IP 数据包的目的 IP 地址 (*,G)。
- **源特定 IP 组地址** - 根据 IP 数据包的目的 IP 地址和源 IP 地址 (S,G)。

通过选择转发模式，您可以定义硬件用来确定按以下选项之一的组播流量的方法：“MAC 组地址”、“IP 组地址”或“源特定 IP 组地址”。

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

设备最多支持 256 个静态和动态组播组地址。

启用组播过滤并选择转发方法的步骤：

步骤 1 单击**组播 > 属性**。

步骤 2 输入参数。

- **网桥组播过滤状态** - 选择该选项可启用过滤功能。
- **VLAN ID** - 选择 VLAN ID 可设置其转发方法。
- **IPv6 的转发方法** - 将以下方法之一设置为 IPv6 地址的转发方法：“MAC 组地址”、“IP 组地址”或“源特定 IP 组地址”。
- **IPv4 的转发方法** - 将以下方法之一设置为 IPv4 地址的转发方法：“MAC 组地址”、“IP 组地址”或“源特定 IP 组地址”。

步骤 3 单击**应用**。将更新当前配置文件。

添加 MAC 组地址

设备支持根据组播组信息转发传入的组播流量。此信息衍生自接收到的或作为手动配置结果的 IGMP/MLD 数据包，并存储在组播转发数据库 (MFDB) 中。

当从 VLAN（配置为根据 MAC 组地址转发组播流）接收帧并且其目的地址为第 2 层组播地址时，会将该帧转发到作为 MAC 组地址成员的所有端口。

“MAC 组地址”页面具有以下功能：

- 查询并查看来自 MFDB 的与特定 VLAN ID 或特定 MAC 地址组相关的信息。可通过 IGMP/MLD Snooping 动态获取或通过手动输入静态获取此数据。
- 添加或删除 MFDB 的静态条目，该 MFDB 可根据 MAC 目的地址来静态转发信息。
- 显示作为每个 VLAN ID 和 MAC 地址组成员的所有端口/LAG 的列表，并输入是否对其转发流量。

要在模式为 *IP 地址组* 或 *IP 和源组* 时查看转发信息，请使用“IP 组播组地址”页面。

定义和查看 MAC 组播组的步骤：

步骤 1 单击**组播 > MAC 组地址**。

步骤 2 输入参数。

- **VLAN ID 为** - 设置要显示的组的 VLAN ID。
- **MAC 组地址为** - 设置要显示的组播组的 MAC 地址。如果未指定 MAC 组地址，页面将包含来自所选 VLAN 的所有 MAC 组地址。

步骤 3 单击**转至**，将在下侧块中显示 MAC 组播组地址。

此时将显示在此页面和“IP 组播组地址”页面创建的条目。对于那些在“IP 组播组地址”页面中创建的条目，IP 地址将转换为 MAC 地址。

步骤 4 单击**添加**以添加静态 MAC 组地址。

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**。

该页面包含以下内容：

- **VLAN ID** - 定于组播组的 VLAN ID。
- **MAC 组地址** - 组的 MAC 地址。

步骤 7 从**过滤器：接口类型**菜单中选择要显示的端口或 LAG。

步骤 8 单击**转至**以显示端口或 LAG 成员关系。

步骤 9 选择每个接口与组播组进行关联的方法：

- **静态** - 将接口作为静态成员连接到组播组。
- **动态** - 表示由于 IGMP/MLD Snooping 已将接口添加到组播组。
- **已禁止** - 指定禁止此端口加入此 VLAN 上的这个组。
- **无** - 指定端口目前不是此 VLAN 上该组播组的成员。

步骤 10 单击**应用**，将更新当前配置文件。

注 无法在此页面中删除在“IP 组播组地址”页面中创建的条目（即使已选定这些条目）。

添加 IP 组播组地址

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

使用“IP 组播组地址”页面可查询和添加 IP 组播组。

定义和查看 IP 组播组的步骤：

步骤 1 单击**组播 > IP 组播组地址**。

该页面包含通过 Snooping 学习的所有 IP 组播组地址。

步骤 2 输入进行过滤所需的参数。

- **VLAN ID 为** - 定义要显示的组的 VLAN ID。
- **IP 版本为** - 选择 IPv6 或 IPv4。
- **IP 组播组地址为** - 定义要显示的组播组的 IP 地址。这仅在转发模式为 (S,G) 时才相关。
- **源 IP 地址为** - 定义发送设备的源 IP 地址。如果模式为 (S,G)，则输入发送者 S。这与 IP 组地址一起作为要显示的组播组 ID (S,G)。如果模式为 (*,G)，则输入 * 以表示组播组仅由目的定义。

步骤 3 单击**转至**。结果将显示在选择下侧块中。在处于第 2 层系统模式下的设备上启用 Bonjour 和 IGMP 后，将显示 Bonjour 的 IP 组播地址。对于 SG500X/ESW2-550X 设备，始终显示地址。

步骤 4 单击**转至**。结果将显示在选择下侧块中。

步骤 5 单击**添加**以添加静态 IP 组播组地址。

步骤 6 输入参数。

- **VLAN ID** - 定义要添加的组的 VLAN ID。
- **IP 版本** - 选择 IP 地址类型。
- **IP 组播组地址** - 定义新组播组的 IP 地址。
- **源特定** - 表示该条目包含特定源，并在“IP 源地址”字段中添加地址。否则，该条目将添加为 (*,G) 条目，即来自任何 IP 源的 IP 组地址。
- **源 IP 地址** - 定义要包括的源地址。

步骤 7 单击**应用**。将添加 IP 组播组，并更新设备。

步骤 8 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 组播组地址和源 IP 地址将以只读的方式显示在窗口的顶端。您可以选择过滤器类型：

- **接口类型为** - 选择显示端口还是 LAG。

步骤 9 为每个接口选择其关联类型。选项如下：

- **静态** - 将接口作为静态成员连接到组播组。
- **已禁止** - 指定禁止将此端口添加到此 VLAN 上的这个组。
- **无** - 表示端口目前不是此 VLAN 上该组播组的成员。默认情况下选定此项，直到选择“静态”或“已禁止”。

步骤 10 单击**应用**。将更新当前配置文件。

配置 IGMP Snooping

要支持选择的组播转发 (IPv4)，必须启用网桥组播过滤（在“属性”页面中），并且必须针对每个相关 VLAN 全局启用 IGMP Snooping。（在 IGMP Snooping 页面中）。

默认情况下，第 2 层设备会将组播帧转发到相关 VLAN 的所有端口，实质上似乎是将帧作为广播进行处理。使用 IGMP Snooping，设备会将组播帧转发到已注册组播客户端的端口。

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

全局启用 IGMP Snooping 后，所有 IGMP 数据包都将被转发至 CPU。CPU 则会分析传入的数据包，然后确定以下信息：

- 哪些端口要求加入哪个 VLAN 上的哪些组播组。
- 将哪些端口连接到了生成 IGMP 查询的组播路由器 (Mrouter)。
- 哪些端口正在接收 PIM、DVMRP 或 IGMP 查询协议。

这些信息均显示在 IGMP Snooping 页面上。

要求加入特定组播组的端口将发送 IGMP 报告来指定主机要加入的组。这将在组播转发数据库中创建转发条目。

当没有组播路由器时，IGMP Snooping 查询器将用于支持 Snooping 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。

IGMP 查询器活动的速度必须与启用 IGMP Snooping 的交换机保持一致。必须以与 Snooping 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。这将在“编辑 IGMP Snooping”页面中执行。

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

步骤 1 单击**组播 > IGMP Snooping**。

步骤 2 启用或禁用“IGMP Snooping 状态”。

全局启用 IGMP Snooping 时，监控网络流量的设备可确定哪些主机已请求接收组播流量。

仅当同时启用 IGMP Snooping 和网桥组播过滤时，设备才会执行 IGMP Snooping。

步骤 3 选择一个 VLAN，然后单击**编辑**。

网络中只能存在一个 IGMP 查询器。设备支持基于标准的 IGMP 查询器选择。此表中的某些运行参数值由选择的查询器发送。其他值则衍生自本设备。

步骤 4 输入参数。

- **VLAN ID** - 选择其中定义 IGMP Snooping 的 VLAN ID。
- **IGMP Snooping 状态** - 启用或禁用选定 VLAN 的网络流量监控。
- **运行 IGMP 的 Snooping 状态** - 为选定 VLAN 显示 IGMP Snooping 的当前状态。
- **组播路由器端口自动学习** - 启用或禁用自动学习 Mrouter 所连接的端口。
- **查询健壮性** - 输入当此设备是选择的查询器时要使用的健壮性变量值。
- **运行查询健壮性** - 显示选择的查询器所发送的健壮性变量。
- **查询间隔** - 输入当此设备是选择的查询器时要使用的普通查询的时间间隔。
- **运行查询间隔** - 由所选查询器发送的普通查询的时间间隔（以秒为单位）。
- **查询最大响应间隔** - 输入用来计算插入定期普通查询的最大响应代码的延迟时间。
- **运行查询最大响应间隔** - 显示由所选查询器发送的普通查询中包括的“查询最大响应间隔”。
- **最近成员查询计数器** - 输入设备中假定不再存在组成员之前所发送的特定于 IGMP 组的查询数（如果该设备是选择的查询器）。
- **最近成员运行查询计数器** - 显示“最近成员查询计数器”的运行值。
- **最近成员查询间隔** - 输入要使用的最大响应延迟时间（如果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）。
- **最近成员运行查询间隔** - 显示由所选查询器发送的“最近成员查询间隔”。
- **立即离开** - 启用“立即离开”可减少当在成员端口上接收 IGMP 组离开消息时阻止将组播流发送到该端口所花费的时间。
- **IGMP 查询器状态** - 启用或禁用 IGMP 查询器。
- **管理查询器源 IP 地址** - 选择 IGMP 查询器的源 IP 地址。它可以是 VLAN 的 IP 地址，或者可以是管理 IP 地址。
- **运行查询器源 IP 地址** - 显示所选查询器的源 IP 地址。

- **IGMP 查询器版本** - 选择当设备成为选择的查询器时使用的 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。

步骤 5 单击**应用**。将更新当前配置文件。

MLD Snooping

主机使用 MLD 协议来报告它们在组播会话中的参与情况，而设备则使用 MLD Snooping 来构建组播成员关系列表。它使用这些列表来将组播数据包仅转发到其中存在作为组播组成员的主机节点的设备端口。设备不支持 MLD 查询器。

主机使用 MLD 协议来报告组播会话中这些主机的参与情况。

设备支持两个版本的 MLD Snooping：

- MLDv1 Snooping 检测 MLDv1 控制数据包，并根据 IPv6 目的组播地址设置流量桥接。
- MLDv2 Snooping 使用 MLDv2 控制数据包，根据源 IPv6 地址和目的 IPv6 组播地址转发流量。

实际的 MLD 版本由网络中的组播路由器选择。

通过一种类似于 IGMP Snooping 的方法，可在设备将 MLD 帧从多个工作站转发到一个上行组播路由器时 Snooping 这些帧，反之亦然。此设施可使设备能够推断以下信息：

- 想要加入特定组播组的工作站位于哪些端口上
- 发送组播帧的组播路由器位于哪些端口上

这些信息用于从传入组播帧的转发集中排除不相关的端口（这些端口上没有经过注册可接收特定组播组的工作站）。

除手动配置的组播组之外，如果您还启用了 MLD Snooping，则结果是衍生自手动设置和通过 MLD Snooping 的动态发现的组播组和端口成员关系的联合。重启系统时，只会保留静态定义。

在 VLAN 上启用 MLD Snooping 并进行配置的步骤：

步骤 1 单击**组播 > MLD Snooping**。

步骤 2 启用或禁用 **MLD Snooping 状态**。全局启用 MLD Snooping 时，监控网络流量的设备可确定哪些主机已请求接收组播流量。如果同时启用了 MLD Snooping 和网桥组播过滤，则设备将执行 MLD Snooping。

步骤 3 选择一个 VLAN，然后单击**编辑**。

步骤 4 输入参数。

- **VLAN ID** - 选择 VLAN ID。
- **MLD Snooping 状态** - 在 VLAN 上启用或禁用 MLD Snooping。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 Snooping 和网桥组播过滤时，设备才会执行 MLD Snooping。
- **运行 MLD Snooping 状态** - 为选择的 VLAN 显示 MLD Snooping 的当前状态。
- **组播路由器端口自动学习** - 启用或禁用自动学习组播路由器。
- **查询健壮性** - 输入要使用的健壮性变量值（如果设备无法从所选查询器发送的消息读取此值）。
- **运行查询健壮性** - 显示选择的查询器所发送的健壮性变量。
- **查询间隔** - 输入设备要使用的“查询间隔”间隔值（如果该设备无法从所选查询器发送的消息获取此值）。
- **运行查询间隔** - 从所选查询器接收的普通查询的时间间隔（以秒为单位）。
- **查询最大响应间隔** - 输入要使用的查询最大响应延迟时间（如果设备无法从所选查询器发送的普通查询读取最大响应时间值）。
- **运行查询最大响应间隔** - 显示用来计算插入普通查询的最大响应代码的延迟时间。
- **最近成员查询计数器** - 输入要使用的最后成员查询次数（如果设备无法从所选查询器发送的消息获取此值）。
- **最近成员运行查询计数器** - 显示“最近成员查询计数器”的运行值。
- **最近成员查询间隔** - 输入要使用的最大响应延迟时间（如果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）。
- **最近成员运行查询间隔** - 由所选查询器发送的“最近成员查询间隔”。
- **立即离开** - 启用该选项时，将减少用来阻止发送到设备端口的多余 MLD 流量的时间。

步骤 5 单击**应用**。将更新当前配置文件。

查询 IGMP/MLD IP 组播组

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

此页面上的信息与“MAC 组地址”等页面上所显示的信息可能有所不同。假定系统位于基于 MAC 的组和请求加入以下多播组 224.1.1.1 和 225.1.1.1 的端口中，两者均被映射到同一 MAC 多播地址 01:00:5e:01:01:01 中。在这种情况下，“MAC 组播”页面中有一个条目，而此页面上则有两个条目。

查询 IP 组播组的步骤：

步骤 1 单击**组播 > IGMP/MLD IP 组播组**。

步骤 2 设置要搜索的 Snooping 组类型：IGMP 或 MLD。

步骤 3 输入以下查询过滤条件的一部分或全部：

- **组地址为** - 定义要查询的组播组 MAC 地址或 IP 地址。
- **源地址为** - 定义要查询的发送者地址。
- **VLAN ID 为** - 定义要查询的 VLAN ID。

步骤 4 单击**转至**。将为每个组播组显示以下字段：

- **VLAN** - VLAN ID。
 - **组地址** - 组播组 MAC 地址或 IP 地址。
 - **源地址** - 所有指定组端口的发送者地址。
 - **包括的端口** - 组播流目的端口的列表。
 - **排除的端口** - 不包括在组中的端口的列表。
 - **兼容模式** - 通过设备在 IP 组地址上接收的主机注册的最旧版本的 IGMP/MLD。
-

定义组播路由器端口

组播路由器 (Mrouter) 端口是连接至组播路由器的端口。当设备转发组播流和 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**组播 > IGMP Snooping** 和**组播 > MLD Snooping** 页面。
- **已禁止** - 不将此端口配置为组播路由器端口，即使此端口上接收 IGMP 或 MLD 查询。如果端口上已启用“已禁止”，此端口上将无法学习组播路由器（即此端口上未启用“组播路由器端口自动学习”）。
- **无** - 端口当前不是组播路由器端口。

步骤 5 单击**应用**更新设备。

定义“全部转发”组播

使用“全部转发”页面可启用并显示要从特定 VLAN 接收组播流的端口和/或 LAG 的配置。此功能需要在“属性”页面中启用网桥组播过滤。如果禁用网桥组播过滤，则所有组播流量均会被泛洪到设备中的所有端口。

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”。

IGMP 或 MLD 消息不会被转发到定义为 *全部转发* 的端口。

注 该配置仅会影响作为所选 VLAN 的成员的端口。

定义“全部转发”组播的步骤：

步骤 1 单击**组播 > 全部转发**。

步骤 2 定义以下选项：

- **VLAN ID 为** - 将显示的端口/LAG 的 VLAN ID。
- **接口类型为** - 定义显示端口还是 LAG。

步骤 3 单击**转至**。此时将显示所有端口/LAG 的状态。

步骤 4 选择要通过使用以下方法来定义为“全部转发”的端口/LAG：

- **静态** - 端口接收所有组播流。
- **已禁止** - 端口无法接收任何组播流，即使 IGMP/MLD Snooping 已指定端口加入组播组。
- **无** - 端口当前不是“全部转发”端口。

步骤 5 单击**应用**。将更新当前配置文件。

定义未注册的组播设置

一般会将组播帧转发到 VLAN 中的所有端口。如果启用 IGMP/MLD Snooping，设备将学习组播组的存在，并监控哪些端口已加入哪些组播组。还可以静态配置组播组。动态学习或静态配置的组播组均被视为已注册。

设备会将组播帧（从已注册的组播组）仅转发到注册至组播组的端口。

使用“未注册的组播”页面可处理属于不为设备所知的组（未注册的组播组）的组播帧。通常会将未注册的组播帧转发到 VLAN 中的所有端口。

您可以选择一个端口来接收或过滤未注册的组播流。该配置适用于作为成员（将成为成员）的任何 VLAN。

此功能可确保客户仅接收请求的组播组，而不接收可能在网络中传输的其他组播组。

定义未注册的组播设置的步骤：

步骤 1 单击**组播 > 未注册的组播**。

步骤 2 定义以下选项：

- **接口类型为** - 作为所有端口或所有 LAG 的视图。
- **端口/LAG** - 显示端口 ID 或 LAG ID。
- **未注册的组播** - 显示所选接口的转发状态。可能的值包括：
 - **转发** - 可将未注册的组播帧转发到选择的接口。
 - **过滤** - 可过滤（拒绝）到所选接口的未注册的组播帧。

步骤 3 单击**应用**。将保存设置，并更新当前配置文件。

IP 配置

IP 接口地址由用户手动配置或由 DHCP 服务器自动配置。本节介绍关于手动定义设备 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](#)
- [IPv4 管理和接口](#)
- [DHCP 服务器](#)
- [IPv6 管理和接口](#)
- [域名](#)

概述

注 SG500X 设备始终在高级 L3 模式下工作，但在作为 Sx500 设备运行时采用混合模式（请参阅[堆叠单元模式](#)）。另一方面，Sx500 设备必须始终设置为在第 2 层或第 3 层系统模式下工作。因此，如果本节提到在第 3 层系统模式下工作的设备，即指所有处于原生堆叠模式的 SG500X 设备和已经手动设置为第 3 层系统模式的所有设备。如果本文档提到在第 2 层系统模式下工作的设备，即指所有 Sx500 设备和已经手动设置为第 2 层模式的 SG500X 设备（处于混合模式）。

有些功能仅在第 2 层或第 3 层系统模式下才可用，如下所述：

- 在第 2 层系统模式下（仅限 Sx500 设备），设备作为第 2 层可识别 VLAN 的设备运行，无路由功能。
- 在第 3 层系统模式下，设备具有 IP 路由功能以及第 2 层系统模式的功能。在此系统模式下，第 3 层端口仍会保留大量的第 2 层功能，例如生成树协议和 VLAN 成员关系。
- 在第 3 层系统模式下（仅限 Sx500 设备），设备不支持基于 MAC 的 VLAN、动态 VLAN 分配、VLAN 速率限制、SYN 速率 DoS 保护以及高级 QoS 策略器。

对于 Sx500 设备而言，要配置系统模式（第 2 层或第 3 层），请参阅“系统模式和堆栈管理”页面

注 要从一种系统模式（层）切换到另一种模式（在 Sx500 设备上），需要强制重启，随后将删除设备的启动配置。

第 2 层 IP 寻址

注 本节仅适用于 Sx500 设备。

在第 2 层系统模式下，此类设备在管理 VLAN 中最多有一个 IPv4 地址和两个 IPv6 接口（“本地”接口或隧道）。此 IP 地址和默认网关可手动配置，也可由 DHCP 进行配置。第 2 层系统模式的静态 IP 地址和默认网关在“IPv4 接口”和“IPv6 接口”页面中进行配置。在第 2 层系统模式下，设备使用默认网关（如果已配置）来和与该设备位于不同 IP 子网的设备进行通信。默认情况下，VLAN 1 为管理 VLAN，但可修改此设置。在第 2 层系统模式下运行时，仅可通过设备的管理 VLAN 在配置的 IP 地址上访问设备。

IPv4 地址配置的出厂默认设置为 *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。地址冲突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。

将 VLAN 配置为使用动态 IPv4 地址后，设备会发出 DHCPv4 请求，直到 DHCPv4 服务器为其分配 IPv4 地址。在第 2 层系统模式下，只有管理 VLAN 可以使用静态或动态 IP 地址进行配置。在第 3 层系统模式下，设备上的所有接口类型（端口、LAG 和/或 VLAN）均能够使用静态或动态 IP 地址进行配置。

设备的 IP 地址分配规则如下：

- 在第 2 层系统模式下，除非使用静态 IP 地址配置设备，否则设备会发出 DHCPv4 请求，直到收到 DHCP 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 会产生变化。如果已设置静态 IP 地址，则系统状态 LED 也会变为以绿色持续亮起。如果设备正获取 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，则会使用默认 IP 地址。有其他 IP 地址可用时，会自动使用这些地址。默认 IP 地址始终在管理 VLAN 上。

第 3 层 IP 寻址

在第 3 层系统模式下，设备可具有多个 IP 地址。可将每个 IP 地址分配给指定的端口、LAG 或 VLAN。这些 IP 地址在第 3 层系统模式下的“IPv4 接口”和“IPv6 接口”页面中进行配置。与只能配置单一 IP 地址的第 2 层系统模式相比，此模式可提供更高的网络弹性。在第 3 层模式下运行时，可从相应接口的所有 IP 地址上访问设备。

在第 3 层系统模式下，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。此操作在“IPv4 静态路由”和“IPv6 路由”页面中进行。

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。

如果第 2 层和第 3 层的页面不同，屏幕将显示两个版本。

环回接口

综述

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。

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。

当交换机处于第 2 层模式时，支持以下规则：

- 只支持一个环回接口。
- 可配置两个 IPv4 接口：一个在 VLAN 或以太网端口上，另一个在环回接口上。

- 如果在默认 VLAN 上配置 IPv4 地址，而默认 VLAN 更改，则交换机会将 IPv4 地址移动到新的默认 VLAN 上。

配置环回接口

要配置 IPv4 环回接口，请执行以下操作：

- 在第 2 层中，在“管理 > 管理接口 > IPv4 接口”页面启用“环回接口”并配置其地址。此页面在 SG500X、ESW2-550X 和 SG500XG 设备中不可用。
- 在第 3 层中，在“IP 配置 > IPv4 管理和接口 > IPv4 接口”中添加一个环回接口。

要配置 IPv6 环回接口，请执行以下操作：

- 在第 2 层中，在“管理 > 管理接口 > IPv6 接口”页面添加一个环回接口。在“管理 > 管理接口 > IPv6 地址”页面配置该接口的 IPv6 地址。此页面在 SG500X、ESW2-550X 和 SG500XG 设备中不可用。
- 在第 3 层中，在“IP 配置 > IPv6 管理和接口 > IPv6 接口”中添加一个环回接口。在“IP 配置 > IPv6 管理和接口 > IPv6 地址”页面配置该接口的 IPv6 地址。

IPv4 管理和接口

IPv4 接口

设备处于第 2 层或第 3 层系统模式时可以定义 IPv4 接口。

在第 2 层系统模式下定义 IPv4 接口

本节不适用于 SG500X、ESW2-550X 或 SG500XG 设备。

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。

配置 IPv4 设备 IP 地址的步骤：

步骤 1 单击 **管理 > 管理接口 > IPv4 接口**。

步骤 2 为以下字段输入值：

- **管理 VLAN** - 选择用于通过 Telnet 或 Web GUI 访问设备的管理 VLAN。VLAN1 为默认的管理 VLAN。

- **IP 地址类型** - 选择以下其中一个选项：
 - **动态** - 使用 DHCP 从管理 VLAN 发现 IP 地址。
 - **静态** - 手动定义静态的 IP 地址。

注 如果设备为 DHCP 客户端，则支持 DHCP 选项 12（主机名选项）。如果 DHCP 选项 12 是从 DHCP 服务器获取的，则会保存为该服务器的主机名。设备不会发出 DHCP 选项 12 请求。无论哪种请求，DHCP 服务器均必须配置为发送选项 12，才能使用此功能。

要配置静态 IP 地址，请配置以下字段。

- **IP 地址** - 输入 IP 地址，并配置以下掩码字段之一：
 - **网络掩码** - 选择并输入 IP 地址掩码。
 - **前缀长度** - 选择并输入 IPv4 地址前缀的长度。
- **环回接口** - 选择该选项可启用环回接口配置（请参阅[环回接口](#)）。
- **环回 IP 地址** - 输入环回接口的 IPv4 地址。

填写环回接口的以下字段之一：

- **环回掩码** - 输入环回接口 IPv4 地址的掩码。
- **前缀长度** - 输入环回接口 IPv4 地址的前缀长度。
- **管理默认网关** - 选择用户定义并输入默认网关 IP 地址，或选择无以从接口中删除选择的默认网关 IP 地址。
- **运行默认网关** - 显示当前的默认网关状态。

注 如果未使用默认网关配置设备，则它无法与同一 IP 子网内的其他设备进行通信。

如果从 DHCP 服务器检索动态 IP 地址，请选择以下启用的字段：

- **立即更新 IP 地址** - 可在 DHCP 服务器分配 IP 地址后的任何时间更新设备动态 IP 地址。请注意，根据您的 DHCP 服务器配置，设备可能会在续订后收到新的 IP 地址，从而需要将基于 Web 的配置实用程序设置为新的 IP 地址。
- **通过 DHCP 进行自动配置** - 显示自动配置功能的状态。您可以通过 *管理 > 文件管理 > DHCP 自动配置* 配置此功能。

步骤 3 单击**应用**。IPv4 接口设置将写入当前配置文件。

在第 3 层系统模式下定义 IPv4 接口

当设备处于第 3 层模式时，需要使用“IPv4 接口”页面。使用该模式可以配置多个 IP 地址来进行设备管理，并提供路由服务。

可以在端口、LAG、VLAN 或环回接口上配置 IP 地址。

在第 3 层模式下运行时，设备可在设备上配置的直接连接的 IP 子网之间路由流量。设备可持续在同一 VLAN 中的设备之间桥接流量。用于路由到非直接连接的子网的其他 IPv4 路由可以在“IPv4 静态路由”页面中进行配置。

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**。

仅对于 SG500X 设备而言，要启用 IPv4 路由，请选中**启用框**。在 Sx500 设备中，将系统模式从第 2 层更改为第 3 层后，系统会自动启用 IP 路由。

步骤 2 选择 **IPv4 路由** 让设备作为 IPv4 路由器运行。

步骤 3 单击**应用**。参数将保存至当前配置文件。

此页面显示了“IPv4 接口表”中的以下字段：

- **接口** - 为其定义 IP 地址的接口。
- **IP 地址类型** - 定义为静态或 DHCP 的 IP 地址。
 - *动态 IP 地址* - 接收自 DHCP 服务器。
 - *静态* - 手动输入。
- **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。DHCP 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 4 单击**添加**。

步骤 5 请选择以下字段之一：

- **接口** - 选择“端口”、“LAG”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 6 选择**动态地址**或**静态地址**。

步骤 7 如果选择了**静态地址**，请为此接口输入“IP 地址”，并输入以下内容之一。

- **网络掩码** - 此地址的 IP 掩码。
- **前缀长度** - IPv4 前缀的长度。

步骤 8 单击**应用**。IPv4 地址设置将写入当前配置文件。



注意

如果系统处于某个堆叠模式且存在备份主装置，建议将 IP 地址配置为静态地址，以防止在堆叠主装置切换时断开与网络的连接。这是因为，当备用主装置控制堆叠时，如果使用的是 DHCP，则收到的 IP 地址可能与该堆叠原始已启用主装置的单元所收到的 IP 地址不同。

IPv4 路由

当设备处于第 3 层系统模式时，使用该页面可以配置和查看设备上的 IPv4 静态路由。路由流量时，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。

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 路由**。

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** - 选择以下选项之一，并为其输入信息：
 - **网络掩码** - 目的 IP 的 IP 路由前缀。
 - **前缀长度** - 目的 IP 的 IP 路由前缀。
- **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。
 - *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。范围为 1 - 255。

步骤 4 单击**应用**。IP 静态路由将保存至当前配置文件。

RIPv2

请参阅 **IP 配置：RIPv2**。

访问列表

请参阅 **访问列表**。

VRRP

请参阅 **IP 配置：VRRP**

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。动态地址会在超过配置的时间之后过期。

注 在第 2 层模式下，设备会使用 ARP 表中的 IP 地址与 MAC 地址映射，来转发由设备生成的流量。在第 3 层模式下，会将该映射信息用于第 3 层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 输入参数：

- **IP 版本** - 主机支持的 IP 地址格式。仅支持 IPv4 格式。
- **接口** - （仅针对第 3 层）设备上的 IPv4 接口。

- **VLAN** - (仅针对第 2 层) 在第 2 层中显示管理 VLAN ID。

对于处于第 2 层模式下的设备，只有一个直接连接的 IP 子网，该 IP 子网始终位于管理 VLAN 中。ARP 表中的所有静态地址和动态地址都位于管理 VLAN 中。

接口 - 对于处于第 3 层系统模式下的设备，可以在端口、LAG 或 VLAN 上配置 IPv4 接口。从设备上已配置 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 技术来回答对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**。将启用 ARP 代理，并更新当前配置文件。

UDP 中继/IP 助手

UDP 中继/IP 助手功能仅在设备处于第 3 层系统模式下时才可用。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的 IP 地址。

要配置从特定 IPv4 接口接收的 UDP 数据包与特定目的 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，手动输入号码。
 - 步骤 5** 输入接收 UDP 数据包中继的**目的 IP 地址**。如果此字段为 0.0.0.0，则会丢弃 UDP 数据包。如果此字段为 255.255.255.255，则会将 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。
-

DHCPv4 Snooping/中继

DHCPv4 Snooping

DHCP Snooping 提供了一种安全机制，可防止接收假冒的 DHCP 响应数据包，并且可记录 DHCP 地址。它通过将设备上的端口视为信任端口或不信任端口来实现这一目的。

信任端口是指连接到 DHCP 服务器且允许分配 DHCP 地址的端口。信任端口上接收的 DHCP 消息允许通过设备。

不信任端口是指不能分配 DHCP 地址的端口。默认情况下，在您确定端口为信任端口（在“DHCP Snooping 接口设置”页面中）之前，所有端口均被视为不信任端口。

DHCPv4 中继

DHCP 中继可将 DHCP 数据包中继到 DHCP 服务器。

第 2 层和第 3 层中的 DHCPv4

在第 2 层系统模式下，设备可以中继从已启用 DHCP 中继的 VLAN 接收的 DHCP 消息。

在第 3 层系统模式下，设备还可以中继从没有 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。

透明 DHCP 中继

针对透明 DHCP 中继，如果其中使用的是外部 DHCP 中继代理，请执行以下操作：

- 启用 DHCP Snooping。
- 启用选项 82 插入。
- 禁用 DHCP 中继。

针对常规 DHCP 中继：

- 启用 DHCP 中继。
- 无需启用选项 82 插入。

选项 82

选项 82（DHCP 中继代理信息选项）会将端口和代理信息传递到中央 DHCP 服务器，以指示分配的 IP 地址会物理连接到网络的位置。

选项 82 的主要目的是帮助 DHCP 服务器选择最佳 IP 子网（网络池），通过该子网可获取一个 IP 地址。

设备上具有以下选项 82 选项：

- **DHCP 插入** - 将选项 82 信息添加到没有外部选项 82 信息的数据包。
- **DHCP 通道** - 转发包含选项 82 信息的 DHCP 数据包；若数据包来自不信任端口，则予以拒绝。在信任端口上，凡是包含选项 82 信息的 DHCP 数据包都会转发。

下表展示了通过 DHCP 中继、DHCP Snooping 和选项 82 模块的数据包流：

可能的情况有：

- DHCP 客户端和 DHCP 服务器均连接到同一 VLAN。在这种情况下，常规桥接设备会在 DHCP 客户端和 DHCP 服务器之间传递 DHCP 消息。
- DHCP 客户端和 DHCP 服务器连接到不同 VLAN。在这种情况下，仅 DHCP 中继可以且确实会在 DHCP 客户端和 DHCP 服务器之间广播 DHCP 消息。单播 DHCP 消息由常规路由器传递，因此，如果在没有 IP 地址的 VLAN 上启用 DHCP 中继，或者设备不是路由器（第 2 层设备），则需要使用外部路由器。

DHCP 中继（且只有 DHCP 中继）可以将 DHCP 消息中继到 DHCP 服务器

DHCPv4 Snooping、DHCPv4 中继和选项 82 之间的交互

以下各表介绍了设备在 DHCP Snooping、DHCP 中继和选项 82 的不同组合下的运作方式。

下表介绍了在未启用 DHCP Snooping 而启用 DHCP 中继的情况下，对 DHCP 请求数据包的处理方式。

	DHCP 中继 具有 IP 地址的 VLAN		DHCP 中继 没有 IP 地址的 VLAN	
	数据包到达时没有选项 82	数据包到达时含有选项 82	数据包到达时没有选项 82	数据包到达时含有选项 82
禁用选项 82 插入	发送不含选项 82 的数据包	发送含有原始选项 82 的数据包	中继 - 插入选项 82 桥接 - 不插入选项 82	中继 - 丢弃数据包 桥接 - 发送含有原始选项 82 的数据包
已启用选项 82 插入	中继 - 发送含有选项 82 的数据包 桥接 - 不发送选项 82	发送含有原始选项 82 的数据包	中继 - 发送含有选项 82 的数据包 桥接 - 不发送选项 82	中继 - 丢弃数据包 桥接 - 发送含有原始选项 82 的数据包

下表介绍了在 DHCP Snooping 和 DHCP 中继均启用的情况下，对 DHCP 请求数据包的处理方式：

	DHCP 中继 具有 IP 地址的 VLAN		DHCP 中继 没有 IP 地址的 VLAN	
	数据包到达时没有选项 82	数据包到达时含有选项 82	数据包到达时没有选项 82	数据包到达时含有选项 82
禁用选项 82 插入	发送不含选项 82 的数据包	发送含有原始选项 82 的数据包	中继 - 插入选项 82 桥接 - 不插入选项 82	中继 - 丢弃数据包 桥接 - 发送含有原始选项 82 的数据包

	DHCP 中继 具有 IP 地址的 VLAN		DHCP 中继 没有 IP 地址的 VLAN	
已启用选项 82 插入	中继 - 发送含有选项 82 的数据包 桥接 - 添加选项 82 (如果端口为信任端口, 则会按照 DHCP Snooping 未启用的情况进行运作)	发送含有原始选项 82 的数据包	中继 - 发送含有选项 82 的数据包 桥接 - 插入选项 82 (如果端口为信任端口, 则会按照 DHCP Snooping 未启用的情况进行运作)	中继 - 丢弃数据包 桥接 - 发送含有原始选项 82 的数据包

下表介绍了在禁用 DHCP Snooping 的情况下, 对 DHCP 中继数据包的处理方式:

	DHCP 中继 具有 IP 地址的 VLAN		DHCP 中继 没有 IP 地址的 VLAN	
	数据包到达时没有选项 82	数据包到达时含有选项 82	数据包到达时没有选项 82	数据包到达时含有选项 82
禁用选项 82 插入	发送不含选项 82 的数据包	发送含有原始选项 82 的数据包	中继 - 丢弃选项 82 桥接 - 发送不含选项 82 的数据包	中继 - 1. 如果设备中生成回复, 则会发送不含选项 82 的数据包 2. 如果设备中未生成回复, 则会丢弃数据包 桥接 - 发送含有原始选项 82 的数据包

	DHCP 中继 具有 IP 地址的 VLAN		DHCP 中继 没有 IP 地址的 VLAN	
已启用选项 82 插入	发送不含选项 82 的数据包	中继 - 发送不含选项 82 的数据包 桥接 - 发送含有选项 82 的数据包	中继 - 丢弃选项 82 桥接 - 发送不含选项 82 的数据包	中继 - 发送不含选项 82 的数据包 桥接 - 发送含有选项 82 的数据包

下表介绍了在启用 DHCP Snooping 和 DHCP 中继的情况下，对 DHCP 回复数据包的处理方式

	DHCP 中继 具有 IP 地址的 VLAN		DHCP 中继 没有 IP 地址的 VLAN	
	数据包到达时没有选项 82	数据包到达时含有选项 82	数据包到达时没有选项 82	数据包到达时含有选项 82
禁用选项 82 插入	发送不含选项 82 的数据包	发送含有原始选项 82 的数据包	中继 - 丢弃选项 82 桥接 - 发送不含选项 82 的数据包	中继 1. 如果设备中生成回复，则会发送不含选项 82 的数据包 2. 如果设备中未生成回复，则会丢弃数据包 桥接 - 发送含有原始选项 82 的数据包
已启用选项 82 插入	发送不含选项 82 的数据包	发送不含选项 82 的数据包	中继 - 丢弃选项 82 桥接 - 发送不含选项 82 的数据包	发送不含选项 82 的数据包

DHCP Snooping 绑定数据库

DHCP Snooping 可构建一个数据库（称为 DHCP Snooping 绑定数据库），其衍生自从通过信任端口进入设备的 DHCP 数据包获取的信息。

该 DHCP Snooping 绑定数据库包含以下数据：输入端口、输入 VLAN、客户端的 MAC 地址和客户端的 IP（如果存在）。

IP 源防护和动态 ARP 检查功能还会使用 DHCP Snooping 绑定数据库来确定合法的数据包源。

DHCP 信任端口

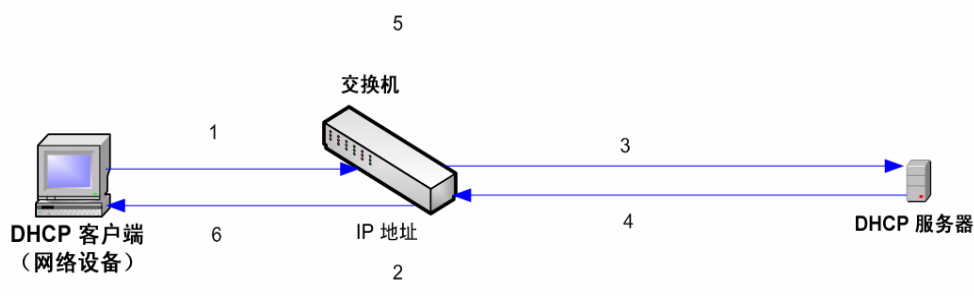
端口可以是 DHCP 信任端口，也可以是 DHCP 不信任端口。默认情况下，所有端口均为不信任端口。要将端口创建为信任端口，请使用“DHCP Snooping 接口设置”页面。系统会自动转发来自这些端口的数据包。来自信任端口的数据包用于创建绑定数据库，将按照下文所述进行处理。

如果未启用 DHCP Snooping，所有端口会默认为信任端口。

DHCP Snooping 绑定数据库的构建方式

以下介绍了在 DHCP 客户端和 DHCP 服务器均受信任的情况下，设备对 DHCP 数据包的处理方式。可通过此过程构建 DHCP Snooping 绑定数据库。

DHCP 信任数据包处理方式



这些操作包括：

- 步骤 1** 设备发送 DHCPDISCOVER 以请求一个 IP 地址，或发送 DHCPREQUEST 以接受 IP 地址和租用。
- 步骤 2** 设备侦听数据包并将 IP-MAC 信息添加到 DHCP Snooping 绑定数据库。
- 步骤 3** 设备转发 DHCPDISCOVER 或 DHCPREQUEST 数据包。

- 步骤 4** DHCP 服务器发送 DHCPOFFER 数据包以提供一个 IP 地址，发送 DHCPACK 以分配一个 IP 地址，或者发送 DHCPNAK 以拒绝地址请求。
- 步骤 5** 设备侦听数据包。如果 DHCP Snooping 绑定表中存在的某条目与该数据包匹配，则设备会在收到 DHCPACK 时，将该条目替换为 IP-MAC 绑定。
- 步骤 6** 设备转发 DHCPOFFER、DHCPACK 或 DHCPNAK。

下表总结了对来自信任端口和不信任端口的 DHCP 数据包的处理方式。DHCP Snooping 绑定数据库存储在永久性存储器中。

DHCP Snooping 数据包处理方式

数据包类型	来自不信任的入口接口	来自信任的入口接口
DHCPDISCOVER	仅转发到信任接口。	仅转发到信任接口。
DHCPOFFER	过滤。	根据 DHCP 信息转发数据包。如果目的地址未知，则会过滤数据包。
DHCPREQUEST	仅转发到信任接口。	仅转发到信任接口。
DHCPACK	过滤。	与 DHCPOFFER 相同，也会将一个条目添加到 DHCP Snooping 绑定数据库。
DHCPNAK	过滤。	与 DHCPOFFER 相同。删除条目（如果存在）。
DHCPDECLINE	检查数据库中是否存在信息。如果信息存在且与接收消息的接口不匹配，则会过滤数据包。否则，会将数据包仅转发到信任接口，并且会从数据库中删除条目。	仅转发到信任接口
DHCPRELEASE	与 DHCPDECLINE 相同。	与 DHCPDECLINE 相同。
DHCPINFORM	仅转发到信任接口。	仅转发到信任接口。
DHCPLEASEQUERY	过滤。	转发。

DHCP Snooping 和 DHCP 中继

如果全局启用 DHCP Snooping 和 DHCP 中继，当在客户端 VLAN 上启用 DHCP Snooping 时，将应用 DHCP Snooping 绑定数据库中包含的 DHCP Snooping 规则，并且会针对中继的数据包，在客户端的 VLAN 以及 DHCP 服务器的 VLAN 中更新 DHCP Snooping 绑定数据库。

DHCP 默认配置

下表介绍了 DHCP Snooping 和 DHCP 中继的默认选项。

DHCP 默认选项

选项	默认状态
DHCP Snooping	已启用
选项 82 插入	未启用
选项 82 通道	未启用
确认 MAC 地址	已启用
备份 DHCP Snooping 绑定数据库	未启用
DHCP 中继	已禁用

配置 DHCP 工作流程

配置 DHCP 中继和 DHCP Snooping 的步骤：

- 步骤 1 在 IP 配置 > DHCP > 属性页面或安全 > DHCP Snooping > 属性页面中，启用 DHCP Snooping 和/或 DHCP 中继。
- 步骤 2 在 IP 配置 > DHCP > 接口设置页面中，定义启用 DHCP Snooping 的接口。
- 步骤 3 在 IP 配置 > DHCP > DHCP Snooping 接口设置页面中，将接口配置为信任接口或不信任接口。
- 步骤 4 可选。在 IP 配置 > DHCP > DHCP Snooping 绑定数据库页面中，将条目添加到 DHCP Snooping 绑定数据库。

DHCP Snooping/中继

本节介绍了如何通过基于 Web 的接口实施 DHCP 中继和 DHCP Snooping 功能。

属性

配置 DHCP 中继、DHCP Snooping 和选项 82 的步骤：

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > DHCP 监听/中继 > 属性或安全 > DHCP Snooping**。

输入以下字段：

- **选项 82** - 选择**选项 82** 可将选项 82 信息插入数据包中。
- **DHCP 中继** - 选择该选项可启用 DHCP 中继。
- **DHCP Snooping 状态** - 选择该选项可启用 DHCP Snooping。如果启用了 DHCP Snooping，则可以启用以下选项：
 - **选项 82 通道** - 选择该选项可在转发数据包时保留外部选项 82 信息。
 - **确认 MAC 地址** - 选择该选项可确认第 2 层报头的源 MAC 地址是否与 DHCP 不信任端口上 DHCP 报头（有效负荷的一部分）中显示的客户端硬件地址相匹配。
 - **备份数据库** - 选择该选项可在设备闪存中备份 DHCP Snooping 绑定数据库。
 - **备份数据库更新间隔** - 输入备份 DHCP Snooping 绑定数据库的频率（**如果已选择“备份数据库”**）。

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

在第 2 层中，只能在具有 IP 地址的 VLAN 上启用 DHCP 中继和 DHCP Snooping。

在第 3 层中，可以在具有 IP 地址的任何接口以及具有或没有 IP 地址的 VLAN 上启用 DHCP 中继和 DHCP Snooping。

在特定接口上启用 DHCP Snooping/中继的步骤：

- 步骤 1** 单击 **IP 配置 > IPv4 管理和接口 > DHCP 监听/中继 > 接口设置**。
- 步骤 2** 要在接口上启用 DHCP 中继或 DHCP Snooping，请单击**添加**。
- 步骤 3** 选择要启用的接口和功能：**DHCP 中继**或 **DHCP Snooping**。
- 步骤 4** 单击**应用**。设置将写入当前配置文件中。

DHCP Snooping 信任接口

对照 DHCP Snooping 绑定数据库检查来自不信任端口/LAG 的数据包（请参阅“DHCP Snooping 绑定数据库”页面）。

默认情况下，接口为信任接口。

将接口指定为不信任接口的步骤：

- 步骤 1** 单击 **IP 配置 > IPv4 管理和接口 > DHCP 监听/中继 > DHCP Snooping 信任接口**。
- 步骤 2** 选择接口，然后单击**编辑**。
- 步骤 3** 选择**信任接口（是或否）**。
- 步骤 4** 单击**应用**，以将设置保存到当前配置文件中。

DHCP Snooping 绑定数据库

有关如何将动态条目添加到 DHCP Snooping 绑定数据库的说明，请参阅 **DHCP Snooping 绑定数据库的构建方式**。

请注意以下有关维护 DHCP Snooping 绑定数据库的要点：

- 当工作站移至其他接口时，设备不会更新 DHCP Snooping 绑定数据库。
- 如果端口已断开，则不会删除该端口的条目。
- 针对 VLAN 禁用 DHCP Snooping 后，将删除为该 VLAN 收集的绑定条目。
- 如果数据库已满，DHCP Snooping 会继续转发数据包，但不会创建新条目。请注意，如果 IP 源防护和/或 ARP 检测功能处于活动状态，则未在 DHCP Snooping 绑定数据库中写入的客户端将无法连接到网络。

将条目添加到 DHCP Snooping 绑定数据库的步骤：

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > DHCP 监听/中继 > DHCP Snooping 绑定数据库**。

要在 DHCP Snooping 绑定数据库中查看条目的子集，请输入相关搜索条件，然后单击**转至**。

将显示 DHCP Snooping 绑定数据库中的字段。这些字段如“添加”页面中所述，**IP 源防护**字段除外：

- **状态 -**
 - 活动 - 设备上的“IP 源防护”处于活动状态。
 - 非活动 - 设备上的“IP 源防护”不处于活动状态。
- **原因 -**
 - 没问题
 - 无资源
 - 无侦听 VLAN
 - 信任端口

步骤 2 要添加条目，请单击**添加**。

步骤 3 输入以下字段：

- **VLAN ID** - 预期数据包所在的 VLAN。
- **MAC 地址** - 数据包的 MAC 地址。
- **IP 地址** - 数据包的 IP 地址。
- **接口** - 预期数据包所在的单元/插槽/接口。
- **类型** - 该字段可能的值包括：
 - *动态* - 条目具有有限的租用时间。
 - *静态* - 已静态配置条目。
- **租用时间** - 如果条目是静态的，则输入该条目在 DHCP 数据库中处于活动状态的时间量。（如果没有租用时间，则选中“无限期”。）

步骤 4 单击**应用**。将定义设置，并更新设备。

DHCP 服务器

您可以借助 DHCPv4 服务器功能将设备配置为 DHCPv4 服务器。DHCPv4 服务器用于将 IPv4 地址和其他信息分配到其他设备（DHCP 客户端）

DHCPv4 从用户定义的 IPv4 地址池分配 IPv4 地址。

可分为以下模式：

- **静态分配** - 主机硬件地址或客户端标识符手动映射到一个 IP 地址。此项操作将在“静态主机”页面中完成。
- **动态分配** - 客户端获取特定时间内（可以是无限期的）可用的租用 IP 地址。如果 DHCP 客户端未更新分配的 IP 地址，IP 地址将在规定时间结束后取消，而客户端必须请求其他 IP 地址。此项操作可在“网络池”页面中完成。

功能之间的依赖性

- DHCP 服务器和 DHCP 客户端无法同时在系统上配置。也就是说，如果一个接口启用了 DHCP 客户端，则无法全局启用 DHCP 服务器。
- 如果启用了 DHCPv4 中继，设备将无法配置为 DHCP 服务器。

默认设置和配置

- 默认情况下，设备未配置为 DHCPv4 服务器。
- 如果设备启用为 DHCPv4 服务器，默认情况下将不会定义网络地址池。

启用 DHCP 服务器功能的工作流程

将设备配置为 DHCPv4 服务器的步骤：

-
- 步骤 1** 在“DHCP 服务器 > 属性”页面将设备启用为 DHCP 服务器。
 - 步骤 2** 如果存在任何您不想分配的 IP 地址，可在“排除地址”页面进行配置。
 - 步骤 3** 在“网络池”页面定义最多 8 个网络 IP 地址池。
 - 步骤 4** 在“静态主机”页面配置即将分配永久 IP 地址的客户端。
 - 步骤 5** 在“DHCP 选项”页面配置所需的 DHCP 选项。这将配置要为每个相关 DHCP 选项返回的值。

步骤 6 添加一个 IP 接口，取值范围为“网络池”页面配置的 DHCP 池之一。设备会答复来自此 IP 接口的 DHCP 请求。例如：当池的范围为 1.1.1.1 - 1.1.1.254 时，如果希望直接连接的客户端接收来自此已配置池的 IP 地址，则添加一个此范围内的 IP 地址。在“IP 配置 > IPv4 接口”页面执行此操作。

步骤 7 在“地址绑定”页面查看分配的 IP 地址。IP 地址可在此页面删除。

DHCPv4 服务器

将设备配置为 DHCPv4 服务器的步骤：

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > DHCP 服务器 > 属性** 以显示“属性”页面。

步骤 2 选择**启用**将设备配置为 DHCP 服务器。

步骤 3 单击**应用**。设备将立即作为 DHCP 服务器运行。但是，在创建地址池之前，设备不会为客户端分配 IP 地址。

网络池

当某个设备作为 DHCP 服务器运行时，必须定义一个或多个 IP 地址池，设备将从中为客户端分配 IP 地址。每个网络池均包括属于特定子网的一系列地址。这些地址将分配到相应子网内的不同客户端。

当客户端请求 IP 地址时，作为 DHCP 服务器运行的设备会根据以下客户端连接类型分配 IP 地址：

- **直接连接的客户端** - 设备分配来自某个网络池的地址，该网络池的子网能匹配收到 DHCP 请求的设备 IP 接口上配置的子网。
- **远程客户端** - 设备获取来自某个网络池的 IP 地址，该网络池的第一个中继子网（直接连接到客户端）能匹配某个交换机 IP 接口上配置的子网。

您最多可定义八个网络池。

创建 IP 地址池并定义其租用期限的步骤：

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > DHCP 服务器 > 网络池** 以显示“网络池”页面。

将显示以前定义的网络池。

步骤 2 单击**添加**定义新网络池。注意，您可以输入“子网 IP 地址”和“掩码”，或者输入“掩码”、“地址池开始”和“地址池结束”。

步骤 3 输入以下字段：

- **池名** - 输入池名。

- **子网 IP 地址** - 输入网络池所在的子网。
- **掩码** - 输入以下内容之一：
 - **网络掩码** - 选中并输入该池的网络掩码。
 - **前缀长度** - 选中并输入构成地址前缀的位数。
- **地址池开始** - 输入网络池 IP 地址系列中的第一个地址。
- **地址池结束** - 输入网络池 IP 地址系列中的最后一个地址。
- **租用期限** - 输入 DHCP 客户端可以使用来自该池的 IP 地址的时限。可配置最长 49,710 天的租用期限或无限期。
 - **无限期** - 租用期限不受限制。
 - **天** - 租用期限的天数。范围为 0 到 49710 天。
 - **小时** - 租用小时数。指定天数后才能添加小时数值。
 - **分钟** - 租用分钟数。指定天数和小时数值后才能添加分钟数值。
- **默认路由器 IP 地址 (选项 3)** - 输入 DHCP 客户端的默认路由器。
- **域名服务器 IP 地址 (选项 6)** - 选择一个设备 DNS 服务器（如已配置）或选择其他并输入 DHCP 客户端可用的 DNS 服务器的 IP 地址。
- **域名 (选项 15)** - 输入 DHCP 客户端域名。
- **NetBIOS WINS 服务器 (选项 44)** - 输入 DHCP 客户端可用的 NetBIOS WINS 名称服务器。
- **NetBIOS 节点类型 (选项 46)** - 选择解析 NetBIOS 名称的方式。有效节点类型包括：
 - **混合** - 混合使用 b 节点和 p 节点。如果配置为使用 h 节点，计算机将始终首先尝试 p 节点，并仅在 p 节点失败后使用 b 节点。此为默认设置。
 - **混合** - 结合使用 b 节点和 p 节点通信来注册和解析 NetBIOS 名称。M 节点首先使用 b 节点，然后再使用 p 节点（如有必要）。M 节点通常不是大型网络的最佳选择，因为它会优先选择 b 节点进行广播，这会增加网络流量。
 - **点对点** - 使用与 NetBIOS 名称服务器的点对点通信向 IP 地址注册和解析计算机名。
 - **广播** - 使用 IP 广播消息向 IP 地址注册和解析 NetBIOS 名称。
- **SNTP 服务器 IP 地址 (选项 4)** - 选择一个设备 SNTP 服务器（如已配置）或选择其他并输入 DHCP 客户端可用的时间服务器的 IP 地址。

- **文件服务器 IP 地址 (siaddr)** - 输入配置文件下载源位置所在的 TFTP/SCP 服务器 IP 地址。
- **文件服务器主机名 (sname)** - 输入 TFTP/SCP 服务器名。
- **配置文件名称 (file)** - 输入作为配置文件使用的文件名称。

排除地址

默认情况下，DHCP 服务器假设池中的所有池地址都可以分配到客户端。可以排除单个 IP 地址或 IP 地址系列。排除地址会排除在所有 DHCP 池之外。

定义排除地址系列的步骤：

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > DHCP 服务器 > 排除地址** 以显示“排除地址”页面。

将显示以前定义的排除 IP 地址。

步骤 2 要添加待排除的 IP 地址系列，请单击**添加**，然后输入以下字段：

- **起始 IP 地址** - 排除 IP 地址系列中的第一个 IP 地址。
- **结束 IP 地址** - 排除 IP 地址系列中的最后一个 IP 地址。

静态主机

您可能想为某些 DHCP 客户端配置永不更改的永久 IP 地址。客户端则作为静态主机。

为特定客户端手动分配永久 IP 地址的步骤：

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > DHCP 服务器 > 静态主机** 以显示“静态主机”页面。

将显示静态主机。

步骤 2 要添加静态主机，请单击**添加**，然后输入以下字段：

- **IP 地址** - 输入静态分配到主机的 IP 地址。
- **主机名** - 输入主机名，可以为一串符号和一个整数。
- **掩码** - 输入静态主机的网络掩码。
 - *网络掩码* - 选中并输入静态主机的网络掩码。
 - *前缀长度* - 选中并输入构成地址前缀的位数。

- **标识符类型** - 设定识别特定静态主机的方式。
 - **客户端标识符** - 输入以十六进制表示的客户端唯一标识，例如：
01b60819681172。
- 或：
 - **MAC 地址** - 输入客户端的 MAC 地址。
- **客户端名称** - 使用标准 ASCII 字符集输入静态主机名称。客户端名称不得包含域名。
- **默认路由器 IP 地址 (选项 3)** - 输入静态主机的默认路由器。
- **域名服务器 IP 地址 (选项 6)** - 选择一个设备 DNS 服务器（如已配置）或选择其他并输入 DHCP 客户端可用的 DNS 服务器的 IP 地址。
- **域名 (选项 15)** - 输入静态主机域名。
- **NetBIOS WINS 服务器 (选项 44)** - 输入静态主机可用的 NetBIOS WINS 名称服务器。
- **NetBIOS 节点类型 (选项 46)** - 选择解析 NetBIOS 名称的方式。有效节点类型包括：
 - **混合** - 混合使用 b 节点和 p 节点。如果配置为使用 h 节点，计算机将始终首先尝试 p 节点，并仅在 p 节点失败后使用 b 节点。此为默认设置。
 - **混合** - 结合使用 b 节点和 p 节点通信来注册和解析 NetBIOS 名称。M 节点首先使用 b 节点，然后再使用 p 节点（如有必要）。M 节点通常不是大型网络的最佳选择，因为它会优先选择 b 节点进行广播，这会增加网络流量。
 - **点对点** - 使用与 NetBIOS 名称服务器的点对点通信向 IP 地址注册和解析计算机名。
 - **广播** - 使用 IP 广播消息向 IP 地址注册和解析 NetBIOS 名称。
- **SNTP 服务器 IP 地址 (选项 4)** - 选择一个设备 SNTP 服务器（如已配置）或选择其他并输入 DHCP 客户端可用的时间服务器的 IP 地址。
- **文件服务器 IP 地址 (siaddr)** - 输入配置文件下载源位置所在的 TFTP/SCP 服务器 IP 地址。
- **文件服务器主机名 (sname)** - 输入 TFTP/SCP 服务器名。
- **配置文件名称 (file)** - 输入作为配置文件使用的文件名称。

DHCP 选项

当设备用作 DHCP 服务器时，可使用“十六进制”选项配置 DHCP 选项。这些选项的说明位于 RFC2131 中。

这些选项的配置可确定发送给 DHCP 客户端的回复，其数据包包含对已配置 DHCP 选项的请求（使用选项 55）。

在“DHCP 服务器 > 网络池”和“DHCP 服务器 > 静态主机”页面（选项 3 - 6、15、44、46、66 和 67）上专门配置的选项无法使用“DHCP 选项”页面配置。

示例：DHCP 选项 66 配置为“DHCP 选项”页面中 TFTP 服务器的名称。收到包含选项 66 的客户端 DHCP 数据包时，TFTP 服务器将作为选项 66 的值返回。

配置一个或多个 DHCP 选项的步骤：

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > DHCP 服务器 > DHCP 选项**。

将显示之前配置的 DHCP 选项。

步骤 2 配置尚未配置的选项并填写此字段的步骤：

- **DHCP 服务器池名称** - 选择“网络池”页面定义的网络地址池之一。

步骤 3 单击**添加**并填写以下字段：

- **代码** - 输入 DHCP 选项代码。
- **类型** - 此字段的单选按钮，可根据 DHCP 选项的参数类型更改。选择以下代码之一，并输入 DHCP 选项参数的值：
 - **十六进制** - 如果希望输入 DHCP 选项参数的十六进制值，则选择此选项。可提供十六进制值来代替其他所有类型的值。例如，可以提供 IP 地址的十六进制值，而非 IP 地址本身。

十六进制值无需验证，因此，如果您输入一个表示非法值的十六进制值，将不会返回任何错误，且客户端可能无法处理来自服务器的 DHCP 数据包。
 - **IP** - 如果希望输入适用于选定 DHCP 选项的 IP 地址，则选择此选项。
 - **IP 列表** - 输入一系列由逗号分隔的 IP 地址。
 - **Integer** - 如果希望为选定 DHCP 选项参数输入整数值，则选择此选项
 - **Boolean** - 如果选定 DHCP 选项的参数为 Boolean，则选择此选项。
- **Boolean 值** - 如果类型为“Boolean”，则选择要返回的值：**True** 或 **False**。
- **值** - 如果类型不是“Boolean”，则输入要为此代码发送的值。

- **说明** - 输入描述文档目的的文本说明。

地址绑定

使用“地址绑定”页面可查看和删除由设备分配的 IP 地址及其相应的 MAC 地址。

查看和/或删除地址绑定的步骤：

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > DHCP 服务器 > 地址绑定** 以显示“地址绑定”页面。

将显示以下有关地址绑定的字段：

- **IP 地址** - DHCP 客户端的 IP 地址。
- **地址类型** - DHCP 客户端地址是显示为 MAC 地址还是使用客户端标识符。
- **MAC 地址/客户端标识符** - 以 MAC 地址或十六进制表示的客户端唯一标识，如 01b60819681172。
- **租用到期** - 租用期限定义的主机 IP 地址租用到期日期和时间，或无期限。
- **类型** - IP 地址分配到客户端的方式。可能的选项有：
 - **静态** - 主机硬件地址映射到一个 IP 地址。
 - **动态** - 从设备动态获取的 IP 地址在某个特定时间段内属于客户端。IP 地址将在期限结束后取消，届时客户端必须请求其他 IP 地址。
- **状态** - 可能的选项有：
 - **已分配** - IP 地址已分配。配置静态主机后，其状态即已分配。
 - **已被拒** - 提供了 IP 地址，但未获得接受，因此未分配。
 - **已过期** - 已超过 IP 地址租期。
 - **已预分配** - 在要约的时间到客户端发送 DHCP ACK 的时间之间，一个条目将处于已预分配状态。然后将变为已分配状态。

IPv6 管理和接口

Internet 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 是为了替换占据主导的 Internet 协议 IPv4。

由于地址大小从 32 位地址增加到 128 位地址，因此 IPv6 在分配 IP 地址方面有更大弹性。IPv6 地址写为八组十六进制数（四位一组），例如，FE80:0000:0000:0000:9C00:876A: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。

IPv6 静态路由

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，在用户明确将这些路由条目移除之前，这些条目由系统保存和使用，并且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 在第 2 层系统模式下，单击 **管理 > 管理接口 > IPv6 全局配置**。

在第 3 层系统模式下，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** -（仅针对第 3 层）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。
- **ICMPv6 限速 单位时间间隔** - 输入生成 ICMP 错误消息的频率。
- **ICMPv6 限速 单位时间间隔最大消息数** - 输入在每个间隔时间内设备可发送的 ICMP 错误消息的最大数目。
- **IPv6 跳数限制** -（仅针对第 3 层）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，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句点或冒号隔开。
- **DHCPv6 唯一标识符 (DUID)** - 显示所选标识符。

IPv6 接口

可以在端口、LAG、VLAN、环回接口或隧道上配置 IPv6 接口。

隧道接口根据“IPv6 隧道”页面中定义的设置，使用 IPv6 地址进行配置。

定义 IPv6 接口的步骤：

-
- 步骤 1** 在第 2 层系统模式下，单击**管理 > 管理接口 > IPv6 接口**。
在第 3 层系统模式下，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** - (仅针对第 3 层) 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** - (仅针对第 3 层) 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**添加**，在启用了 IPv6 的接口上添加新的接口。
- 步骤 4** 填写以下字段：
- **IPv6 接口** - 选择 IPv6 地址的具体端口、LAG、VLAN 或隧道。对于 Sx500 设备，只能配置 **ISATAP** 隧道。对于其他 500 设备，可以配置手动和 ISATAP 隧道。
 - **隧道类型** - (Sx500 没有该选项) 如果 IPv6 接口是隧道，请选择其类型：**手动** 或 **ISATAP** (请参阅 [IPv6 隧道](#))。
- 步骤 5** 要将接口配置为 DHCPv6 客户端，即使接口能够接收来自 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：
- **无状态** - 选择该字段可将接口启用为无状态 DHCPv6 客户端。这样可支持从 DHCP 服务器接收配置信息。
 - **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 6** 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。

注 设备不支持来自 DHCPv6 服务器的有状态地址自动配置。

- **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。
- **MLD 版本** - (仅针对第 3 层) IPv6 MLD 版本。
- **IPv6 重定向** - (仅针对第 3 层) 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 7 单击 **应用** 可对选择的接口进行 IPv6 处理。常规 IPv6 接口已自动配置以下地址：

- 根据设备的 MAC 地址使用 EUI-64 格式的接口 ID 的链路本地地址
- 所有节点链路本地组播地址 (FF02::1)
- 请求的节点组播地址 (格式为 FF02::1:FFXX:XXXX)

步骤 8 单击 **IPv6 地址表** 可为接口手动分配 IPv6 地址 (如果需要)。有关该页面的描述，请参阅 **“定义 IPv6 地址”** 一节。

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。

DHCPv6 客户端详细信息

DHCPv6 客户端详细信息 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。

按下按钮后，将显示以下字段 (针对接收自 DHCP 服务器的信息)：

- **DHCPv6 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 无状态客户端。
- **无状态服务** - 客户端是否定义为无状态 (从 DHCP 服务器接收配置信息)。
- **DHCPv6 服务器地址** - DHCPv6 服务器地址。
- **DHCPv6 服务器 DUID** - DHCPv6 服务器唯一标识符。
- **DHCPv6 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 地址和一个目的 IPv4 地址。IPv6 数据包封装在这些地址之间。

注 只能在未启用 IPv6 路由时在设备上启用 ISATAP 隧道，且只有 IPv6 管理接口可以通过隧道传输。要创建 IPv6 隧道，请在“IPv6 接口”接口页面将 IPv6 接口定义为隧道，然后继续在“IPv6 隧道”页面配置该隧道。

隧道类型

可在设备上配置两种类型的隧道，如下所示：

- **ISATAP 隧道**

站内自动隧道寻址协议 (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：

- 会将 IPv6 链路本地地址分配给 ISATAP 接口。会将初始 IP 地址分配给该接口，然后再启用该接口。
- 如果一个 ISATAP 接口处于活动状态，则会使用 ISATAP 至 IPv4 映射，通过 DNS 来解析 ISATAP 路由器 IPv4 地址。如果未解析 ISATAP DNS 记录，则会在主机映射表中搜索 ISATAP 主机名至地址映射。

- 如果未通过 DNS 过程解析 ISATAP 路由器 IPv4 地址，则 ISATAP IP 接口仍处于活动状态。但是，系统没有用于 ISATAP 流量的默认路由器，直到解析 DNS 过程。

- **手动隧道**

这是一种点对点定义。创建手动隧道时，需要输入源 IP 地址（设备 IP 地址之一）和目的 IPv4 地址。

最多可定义 16 条隧道（其中一条可以是 ISATAP）。

配置隧道

注 要配置隧道，首先要在“IPv6 接口”页面将一个 IPv6 接口配置为隧道。

配置 IPv6 隧道的步骤：

步骤 1 在第 2 层系统模式下，单击 **管理 > 管理接口 > IPv6 隧道**。

只有处于混合堆叠模式的 Sx500 设备和 SG500X 设备才能启用第 2 层模式。

步骤 2 在第 3 层系统模式下，单击 **IP 配置 > IPv6 管理和接口 > IPv6 隧道**。

步骤 3 输入 **ISATAP 参数**。

- **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。
- **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。

注 如果 IPv4 接口不在使用中，则 ISATAP 隧道不可用。

步骤 4 单击 **应用**，以将 ISATAP 参数保存到当前配置文件中。

步骤 5 要编辑隧道，请选择 IPv6 隧道表中的一个接口（在“IPv6 接口”页面定义为隧道），然后单击 **编辑**。

步骤 6 输入以下字段：

- **类型** - 显示隧道类型：**手动**或 **ISATAP**。
- **隧道状态** - 选择该选项以启用隧道。
- **链路状态 SNMP 陷阱** - 选择该选项可在端口链路状态更改时生成 Trap。如果不希望在特定端口上接收此类 Trap（例如，ISP 仅在连接到其基础设置的端口上需要 Trap，而连接到用户设备的端口无需 Trap），可以禁用此功能。

- **源** - 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。
 - 如果 IPv4 地址更改，隧道接口的本地地址也会更改。
 - *IPv4 地址* - 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 IPv4 地址更改，隧道接口的本地地址不会更改。

- *接口* - 选择其 IPv4 地址将用作隧道源地址的接口。

如果接口上有多个 IPv4 地址，将使用最小的 IPv4 地址作为源地址。如果最小的 IPv4 地址已从接口上删除（完全删除，移到其他接口），则将选择下一个最小的 IPv4 地址作为本地 IPv4 地址。

- **目标** - （仅针对手动隧道）选择以下一个选项，以指定隧道目的地址：
 - *主机名* - 远程主机的 DNS 名称。
 - *IPv4 地址* - 远程主机的 IPv4 地址。
- **ISATAP 路由器名** - （仅针对 ISATAP 隧道）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 7 单击**应用**。隧道将保存至当前配置文件。

定义 IPv6 地址

为 IPv6 接口分配 IPv6 地址的步骤：

- 步骤 1** 在第 2 层系统模式下，单击**管理 > 管理接口 > IPv6 地址**。
在第 3 层系统模式下，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**。会在“IPv6 地址表”中显示该接口。
- 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** - (仅针对第 3 层) 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。无法在 ISATAP 隧道接口上直接配置 IPv6 地址。
- **前缀长度** - 全局 IPv6 前缀的长度，是 0-128 间的值，表示构成前缀 (地址的网络部分) 的地址高位的连续位数。
- **EUI-64** - 选择该选项可使用 EUI-64 参数来根据设备的 MAC 地址，使用 EUI-64 格式标识全局 IPv6 地址的接口 ID 部分。

步骤 5 单击**应用**。将更新当前配置文件。

IPv6 路由器配置

以下各节介绍了配置 IPv6 路由器的方法。

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：

- **IPv6 前缀** - 选择**默认**更改在接口上定义地址时创建的默认前缀配置。使用**用户定义**输入以下内容：
 - **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 在第 2 层系统模式下，单击**管理 > 管理接口 > IPv6 默认路由器列表**。
在第 3 层系统模式下，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：

- **默认路由器 IPv6 地址** - 默认路由器的链路本地 IP 地址。
- **接口** - 默认路由器所在的传出 IPv6 接口。
- **类型** - 默认路由器配置，包括以下选项：
 - **静态** - 通过**添加**按钮将默认路由器添加到此表格。
 - **动态** - 动态配置默认路由器。
- **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** - 数据包发送到的下一个目的 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。
 - **点到点** - 点到点隧道。
- **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。

定义 IPv6 邻居信息

使用“IPv6 邻居”页面可以配置和查看 IPv6 接口上的 IPv6 邻居列表。IPv6 邻居表（也称为 IPv6 邻居发现缓存）会显示与设备位于同一 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 在第 2 层系统模式下，单击**管理 > 管理接口 > IPv6 邻居**。
在第 3 层系统模式下，单击**IP 配置 > IPv6 管理和接口 > IPv6 邻居**。

您可以选择一个**清除表**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 为以下字段输入值：

- **接口** - 要添加的相邻 IPv6 接口。
- **IPv6 地址** - 输入为该接口分配的 IPv6 网络地址。该地址必须为有效的 IPv6 地址。
- **MAC 地址** - 输入映射到指定 IPv6 地址的 MAC 地址。

步骤 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**动态**更改为**静态**，请选择地址，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 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**大于**和**小于**参数都输入了，则范围在用**大于**和**小于**的值之间。

创建前缀列表的步骤：

步骤 1 （在第 3 层中）单击 **IP 配置 > IPv6 管理接口 > IPv6 前缀列表**。

-或-

（在第 2 层中）单击**管理 > 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。序列号等于最后一个序列号加 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。

查看 IPv6 路由表

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 路由器或手动添加路由的步骤：

在第 2 层系统模式下查看 IPv6 路由条目的步骤：

步骤 1 单击**管理 > 管理接口 > IPv6 路由**。

-或

在第 3 层系统模式下查看 IPv6 路由条目的步骤：

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** - 目的 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。
- **接口** - 用于转发数据包的接口。
- **下一跳** - 将数据包转发到的地址。通常，该地址为相邻路由器的地址。可采用以下类型之一。
 - **链路本地** - IPv6 接口和 IPv6 地址用于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。
 - **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：
 - **本地** - 一种直接连接的网络，其前缀衍生自手动配置的设备 IPv6 地址。
 - **动态** - 目的地址是间接连接的（远程）IPv6 子网地址。条目是通过 ND 或 ICMP 协议动态获取的。
 - **静态** - 条目是由用户手动配置的。

DHCPv6 中继

DHCPv6 中继用于向 DHCPv6 服务器中继 DHCPv6 消息。在 RFC 3315 中进行定义。

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。
- **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 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。
- **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

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 > 域名 > DNS 设置**。

步骤 2 输入参数。

- **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。
$$\text{此值} = 2 * (\text{轮询重试次数} + 1) * \text{轮询超时}$$
 - **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。设备会对非完全限定的域名 (NFQDN) 进行追加，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 3 单击**应用**。将更新当前配置文件。

DNS 服务器表：将为每个配置的 DNS 服务器显示以下字段：

- **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 4 您最多可定义八个 DNS 服务器。要添加 DNS 服务器，请单击**添加**。

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 5 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。

查看设备上已配置的域名的步骤：

步骤 1 单击 **IP 配置 > 域名 > 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 > 域名系统 > 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合格的名称。
- **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** - 如果是动态条目，将在缓存中保存的时间。
- **剩余 TTL** - 如果是动态条目，还能在缓存中保存的时间。

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）。

您可以选择**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。

IP 配置：RIPv2

本节将介绍路由信息协议 (RIP) 版本 2 功能。

其中包含以下主题：

- [概述](#)
- [Rip 在设备上的运行方式](#)
- [配置 RIP](#)

注 RIP 在以下设备中受到支持：

- 独立式堆叠模式下的 SG500X/SG500XG。
- 第 3 层高级混合堆叠模式下的 SG500X/SG500XG。

概述

路由信息协议 (RIP) 是针对局域网和广域网实施距离矢量的协议。它将路由器分为 *主动路由器* 或 *被动路由器*（静默）两类。主动路由器向其他路由器通告其路由；被动路由器根据通告监听并更新其路由，但并不发布通告。一般来讲，路由器在主动模式下运行 RIP，而主机则使用被动模式。

默认网关是一个静态路由，如果在配置中启用，则其接收 RIP 发布的通告的方式将与其他所有静态路由器一样。

当启动 IP 路由后，RIP 将全面运行。当禁用 IP 路由后，RIP 将在被动模式下运行，这就意味着它只从所接收到的 RIP 消息中学习路由且不将其发出。

注 IP 路由控制仅适用于 SG500X/ESW2-550X 型号。若要启用“IP 路由”，请转至 **配置 > 管理与 IP 接口 > IPv4 接口** 页面。

设备支持基于以下标准的 RIP 版本 2：

- RFC2453 RIP 版本 2，1998 年 11 月
- RFC2082 RIP-2 MD5 验证，1997 年 1 月

- RFC1724 RIP 版本 2 MIB 扩展

将丢弃接收到的 RIPv1 数据包。

Rip 在设备上的运行方式

以下部分介绍 RIP 的启用、偏移量配置、被动模式、验证、统计计数器和对等数据库。

启用 RIP

启用 RIP

- RIP 必须以全局的方式在每个接口上启用。
- 只有在启用的情况下才能配置 RIP。
- 全局禁用 RIP 将删除系统中的 RIP 配置。
- 禁用接口上的 RIP 将会删除指定接口上的 RIP 配置。
- 如果禁用了“IP 路由”，则将不发送 RIP 消息，但当收到 RIP 消息后，它们将用于更新路由表信息。

注 RIP 只能在手动配置的 IP 接口上定义，这就意味着如果接口的 IP 地址已从 DHCP 服务器上接收到或接口的 IP 地址为默认的 IP 地址，则无法在该接口上定义 RIP。

偏移量配置

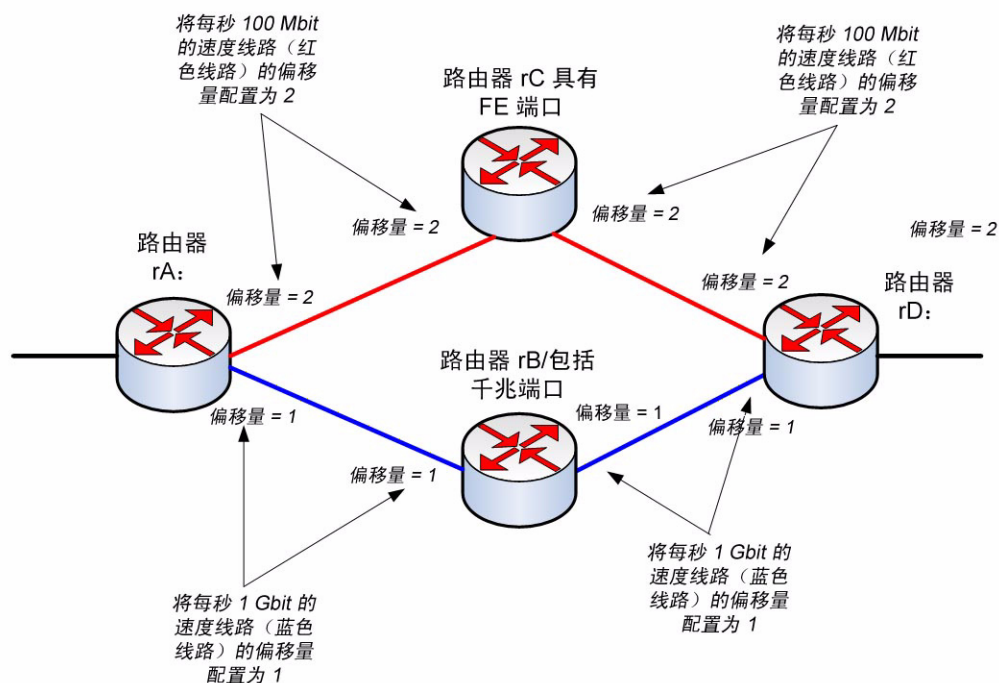
RIP 消息中包含每一路由的度量标准（跃点数）。

偏移量是添加到度量标准以影响路径成本的额外数量。偏移量按每一接口进行设置并可反映该特定接口的速度、延迟或其他一些特征。通过这种方式，可按照需要调整接口的相关成本。

您应当承担起为每一接口设置偏移量（默认情况下为 1）的责任。

下图表明了如何基于端口速度对不同的接口进行度量标准偏移量的配置。

偏移量的配置（基于端口速度）



3945141

路由器 rD 可通过 rB 或 rC 将数据发送到 rA。由于 rC 只支持高速以太网 (FE) 端口，rB 支持千兆以太网 (GE) 端口，且通过路由器 rC 从路由器 rD 到路由器 rA 的路径成本（成本路径增加 4 步）要高于通过路由器 rB 的路径成本（成本路径增加 2 步），因此，建议通过路由 rB 转发流量。要实现该目的，应在每一接口上根据其线路速度配置不同的偏移量（度量标准值）。

有关详情，请参阅[偏移量配置](#)。

被动模式

可禁用通过特定的 IP 接口传输路由更新消息。在本例中，路由器为被动路由器，只接收该端口上更新的 RIP 信息。默认情况下，在 IP 接口上传输路由更新为启用状态。

有关详情，请参阅[IP 接口上的 RIPv2 设置](#)。

过滤路由更新

可使用两种标准访问列表（一种为输入列表，另一种为输出列表）为指定的 IP 接口过滤传入和传出的路由。

标准访问列表是一种带有成对 IP 前缀（IP 地址和 IP 掩码长度）和操作的已命名和排序列表。操作可以为拒绝，也可以为允许。

如果已定义了访问列表，将从第一对开始按照列表检查来自 RIP 消息的每一路由：如果路由与第一对相匹配且操作为允许，则将传递该路由；如果操作为拒绝，则将不传递该路由。如果该路由与之不匹配，则将考虑与第二对是否匹配。

如果没有与该路由匹配的对，则将执行拒绝操作。

在 IP 接口上通告默认路由条目

用于描述默认路由的特定地址为 0.0.0.0。当系统中一个或多个紧密相连的路由器准备好将流量传输到未明确列明的网络上时，默认路由就会用于避免在路由更新中列明每一可能的网络。这些路由器将为地址 0.0.0.0 创建 RIP 条目，就像它是与这些条目相连接的网络一样。

您可以启用默认路由通告并通过指定的度量标准对其进行配置。

重新分布功能

存在以下路由类型，且 RIP 可以对它们进行分发：

- **连接** - 与所定义的禁用 RIP 的 IP 接口（本地定义）相对应的 RIP 路由。默认情况下，RIP 路由表只包含与启用了 RIP 的 IP 接口相对应的路由。
- **静态** - 手动定义的（远程）路由。

您可以通过 RIP 配置**重新分布静态路由**或**重新分布连接的路由**功能来确定是否重新分布静态或连接的路由。

这些功能在默认状态下为禁用状态并可全局启用。

如果启用这些功能，则将由度量标准值为 16 的路由通告被拒绝的路由。

可使用以下选项之一传递路由配置：

- **默认度量标准**
可使 RIP 将预定义的默认度量标准值用于要传递的路由配置。
- **透明（默认情况下）**
可使 RIP 将路由表度量标准用作 RIP 度量标准并将其用于要传递的路由配置。

这将导致出现以下行为:

- 如果路由的度量标准值等于或小于 15, 则在通告该路由时将在 RIP 协议中使用该值。
- 如果静态路由的度量标准值大于 15, 则在使用 RIP 时将不向其他路由器通告该路由。

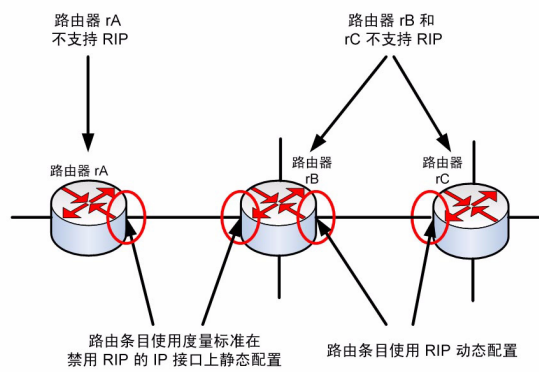
▪ 用户定义的度量标准

导致 RIP 使用用户输入的度量标准值。

在包含不支持 RIP 设备的网络中使用 RIP

在使用 RIP 时必须考虑静态路由配置和连接的接口。这将反映在下图中, 在该图给出的网络中, 有些路由器支持 RIP, 而有些则不支持。

网络中包含支持 RIP 的路由器和不支持 RIP 的路由器



路由器 rA 不支持 RIP。因此, 将在该路由器上静态配置带有相应度量标准的路由条目。在路由器 rB 上, 将视指向路由器 rA 的路由为连接的路由。相比之下, 路由器 rB 和 rC 则使用 RIP 获取和分发其路由条目。

使用默认度量标准或透明系统均可将路由器 rB 的连接路由配置传递到路由器 rC。可通过路由的度量标准 (透明度量标准) 或由默认度量标准命令定义的度量标准重新分布静态/连接的路由。

有关详情, 请参阅[重新分布功能](#)。

RIP 验证

您可以在每个 IP 接口上禁用 RIP 消息验证或启用以下验证类型之一：

- **纯文本或密码** - 使用随路由一起发送到路由器的密钥密码（字符串）。接收路由器会将该密钥与自身配置的密钥相对比。如果两者相同，则它将接受该路由。
- **MD5** - 使用 MD5 摘要验证。每一路由器都配置有一组机密密钥。这组密钥称为**密钥链**。每个密钥链均由一个或多个密钥组成。每个密钥均含有一个识别码（**密钥标识符**）、**密钥字符串**以及可选的**发送有效期限**和**接受有效期限**值。发送有效期限是指发送密钥链上的验证密钥的有效时间段；接受有效期限是指接收密钥链上的验证密钥的有效时间段。

每则传输的 RIP 消息都含有已计算好的该消息的 MD5 摘要（包含密钥链）以及所使用的密钥字符串的密钥标识符。接收器上也配置有密钥链。接收器将使用密钥标识符来选择验证 MD5 摘要所需的密钥。

RIP 统计计数器

您可通过查看每一接口的统计计数器来监控 RIP 的运行。有关这些计数器的描述，请参阅[显示 RIPv2 统计计数器](#)。

RIP 对等数据库

您可以监控每一个 IP 接口的 RIP 对等数据库。有关这些计数器的描述，请参阅[显示 RIPv2 对等数据库](#)。

配置 RIP

可执行以下操作。

- 强制操作：
 - 使用“RIPv2 属性”页面全局启用/禁用 RIP 协议。
 - 使用“RIPv2 设置”页面在 IP 接口上启用/禁用 RIP 协议。
- 可选操作（如果以下操作未执行，则系统将使用默认值）
 - 使用“RIPv2 属性”页面启用/禁用 RIP，以在 IP 接口上通告静态或连接的路由和其度量标准。

- 针对 IP 接口上的传入路由的度量标准，使用“RIPv2 设置”页面配置添加于其上的偏移量。
- 使用“RIPv2 设置”页面在 IP 接口上启用/禁用被动模式。
- 通过在 IP 接口上指定 IP 地址列表（请参阅[访问列表](#)）对将在传入/传出的路由更新中处理哪些路由进行控制。
- 使用“RIPv2 设置”页面在 IP 接口上通告默认路由条目。
- 使用“RIPv2 设置”页面在 IP 接口上启用/禁用 RIP 验证。

RIPv2 属性

在设备上启用/禁用 RIP 的步骤：

步骤 1 单击 **IP 配置 > RIPv2 > RIPv2 属性**。

步骤 2 按要求选择以下选项：

- **RIP** - 可用的选项有：
 - *启用* - 启用 RIP。
 - *禁用* - 禁用 RIP。禁用 RIP 将删除系统中的 RIP 配置。
 - *关闭* - 将 RIP 全局状态设置为关闭状态。
- **RIP 通告** - 选择该选项以在所有 RIP IP 接口上启用发送路由更新。
- **默认路由通告** - 选择该选项以启用发送默认路由到 RIP 域。此路由将用作默认路由器。
- **默认度量标准** - 输入默认度量标准值（请参阅[重新分布功能](#)）。

步骤 3 **重新分发静态路由** - 选择该选项可启用该功能（如[重新分布功能](#)中所述）。

步骤 4 如果已启用**重新分布静态路由**，应为**重新分布静态度量标准**字段选择一个选项。可能的选项有：

- **默认度量标准** - 可使 RIP 使用所传递的静态路由配置的默认度量标准值（请参阅[重新分布功能](#)）。
- **透明** - 可使 RIP 将路由表度量标准用作 RIP 度量标准并将其用于要传递的静态路由配置。这将导致出现以下行为：
 - 如果静态路由的度量标准值等于或小于 15，则在通告该静态路由时将在 RIP 协议中使用该值。

- 如果静态路由的度量标准值大于 15，则在使用 RIP 时将不向其他路由器通告该静态值。

- **用户定义的度量标准** - 输入度量标准值。

步骤 5 重新分布连接的路由 - 选择该选项可启用该功能（如“重新分布静态路由配置”中所述）。

步骤 6 如果已启用**重新分布连接的路由**，应为**重新分布静态度量标准**字段选择一个选项。可能的选项有：

- **默认度量标准** - 可使 RIP 使用所传递的静态路由配置的默认度量标准值（请参阅**重新分布功能**）。
- **透明** - 可使 RIP 将路由表度量标准用作 RIP 度量标准并将其用于要传递的静态路由配置。这将导致出现以下行为：
 - 如果静态路由的度量标准值等于或小于 15，则在通告该静态路由时将在 RIP 协议中使用该值。
 - 如果静态路由的度量标准值大于 15，则在使用 RIP 时将不向其他路由器通告该静态值。
- **用户定义的度量标准** - 输入度量标准值。

步骤 7 单击**应用**。设置将写入当前配置文件中。

IP 接口上的 RIPv2 设置

在接口上配置 RIP 的步骤：

步骤 1 单击 **IP 配置 > RIPv2 > RIPv2 设置**。

步骤 2 RIP 参数将显示于每一 IP 接口上。

要添加新的 IP 接口，单击**添加**以打开“添加 RIPv2 设置”页面，然后输入以下字段：

- **IP 地址** - 选择一个在第 2 层接口上定义的 IP 接口。
- **关闭** - 选择该选项可启用接口上的 RIP（即使处于关闭状态）。
- **被动** - 指定是否允许在指定的 IP 接口上发送 RIP 路由更新消息。如果未启用该字段，将不发送 RIP 更新（被动）。
- **偏移量** - 为指定 IP 接口指定度量标准值这将能够反映出基于接口速度使用该接口的额外成本。

- **默认路由通告** - 此选项在 **RIPv2 属性** 页面全局定义。您可以使用全局定义或者为特定接口定义此字段。可能的选项有：
 - **全局** - 使用 **RIPv2 属性** 屏幕中定义的全局设置。
 - **禁用** - 在此 RIP 接口中不通告默认路由。
 - **启用** - 在此 RIP 接口中通告默认路由。
- **默认路由通告度量标准** - 为此接口输入指定默认路由的度量标准。
- **验证模式** - 在指定 IP 接口上的 RIP 验证状态（启用/禁用）。可能的选项有：
 - **无** - 没有已执行的验证。
 - **文本** - 以下输入的密钥密码将用于验证。
 - **MD5** - 以下所选择的密钥链的 MD5 摘要将用于验证。
- **密钥密码** - 如果已选中 **文本** 作为验证类型，请输入要使用的密码。
- **密钥链** - 如果已选中 **MD5** 作为验证模式，请输入用于编写摘要的密钥链。该密钥链将按照 **密钥管理** 这一节中所述创建。
- **分布列表进** - 选择该选项以为“访问列表名称”中指定 IP 地址的 RIP 传入路由配置过滤功能。如果已启用该字段，请选择以下访问列表名称：
- **访问列表名称** - 为指定的 IP 接口选择 RIP 传入路由过滤的访问列表名称（包括 IP 地名列表）。有关访问列表的描述，请参阅 **创建访问列表**。
- **分布列表出** - 选择该选项以为“访问列表名称”中指定 IP 地址的 RIP 传出路由配置过滤功能。如果已启用该字段，请选择以下访问列表名称：
- **访问列表名称** - 为指定的 IP 接口选择 RIP 传出路由过滤的访问列表名称（包括 IP 地名列表）。有关访问列表的描述，请参阅 **创建访问列表**。

步骤 3 单击 **应用**。设置将写入当前配置文件中。

显示 RIPv2 统计计数器

查看每一 IP 地址的 RIP 统计计数器的步骤：

步骤 1 单击 **IP 配置 > RIPv2 > RIPv2 统计信息**。

此时将显示以下字段：

- **IP 接口** - 在第 2 层接口上定义的 IP 接口。

- **已接收的错误数据包数** - 指定由 IP 接口上的 RIP 识别的错误数据包数。
- **已接收的错误路由数** - 指定由 IP 接口上的 RIP 识别的错误路由数。错误路由指的是错误的路由参数。例如，IP 目标地址是广播地址，或度量标准为 0 或大于 16
- **已发送更新** - 指定由 IP 接口上的 RIP 发送的数据包数。

步骤 2 要清除所有的接口计数器，请单击**清除所有的接口计数器**。

显示 RIPv2 对等数据库

查看 RIP 对等（邻居）数据库的步骤：

步骤 1 单击 **IP 配置 > RIPv2 > RIPv2 对等路由器数据库**。

将为对等路由器数据库显示以下字段：

- **路由器 IP 地址** - 在第 2 层接口上定义的 IP 接口。
- **已接收的错误数据包数** - 指定由 IP 接口上的 RIP 识别的错误数据包数。
- **已接收的错误路由数** - 指定由 IP 接口上的 RIP 识别的错误路由数。错误路由指的是错误的路由参数。例如，IP 目标地址是广播地址，或度量标准为 0 或大于 16
- **上次更新** - 显示 RIP 上次从远程 IP 地址接收 RIP 路由的时间。

步骤 2 要清除所有的计数器，请单击**清除所有的接口计数器**。

访问列表

有关访问列表的描述，请参阅[过滤路由更新](#)。

要创建访问列表，请执行以下操作：

1. 使用“访问列表设置”页面创建带有单个 IP 地址的访问列表。
2. 必要时，可使用“源 IPv4 地址列表”页面添加其他 IP 地址。

创建访问列表

设置访问列表全局配置的步骤:

步骤 1 单击 **IP 配置 > 访问列表 > 访问列表设置**。

步骤 2 要添加新的访问列表，单击**添加**以打开“添加访问列表”页面，然后输入以下字段：

- **名称** - 为访问列表定义名称。
- **源 IPv4 地址** - 输入源 IPv4 地址。可能的选项有：
 - *任意* - 包括所有 IP 地址。
 - *用户定义* - 输入 IP 地址。
- **源 IPv4 地址** - 输入源 IPv4 地址掩码类型和值。可能的选项有：
 - *网络掩码* - 输入网络掩码。
 - *前缀长度* - 输入前缀的长度。
- **操作** - 为访问列表选择一种操作。可能的选项有：
 - *允许* - 允许在访问列表中加入来自 IP 地址的数据包条目。
 - *拒绝* - 拒绝在访问列表中加入来自 IP 地址的数据包条目。

填充访问列表

通过 IP 地址填充访问列表的步骤:

步骤 1 单击 **IP 配置 > 访问列表 > 源 IPv4 地址列表**。

步骤 2 要更改访问列表的参数，单击**添加**以打开“编辑访问列表”页面，然后修改以下任一字段：

- **访问列表名称** - 访问列表的名称。
- **源 IPv4 地址** - 源 IPv4 地址。可能的选项有：
 - *任意* - 包括所有 IP 地址。
 - *用户定义* - 输入 IP 地址。
- **源 IPv4 掩码** - 输入源 IPv4 地址掩码类型和值。可能的选项有：
 - *网络掩码* - 输入网络掩码（例如 255.255.0.0）。

- *前缀长度* - 输入前缀的长度。
 - **操作** - 针对访问列表的操作。可能的选项有：
 - *允许* - 允许在访问列表中加入来自 IP 地址的数据包条目。
 - *拒绝* - 拒绝在访问列表中加入来自 IP 地址的数据包条目。
-

IP 配置：VRRP

本章介绍了虚拟路由器冗余协议 (VRRP) 的工作原理以及如何通过 WEB GUI 配置运行 VRRP 的虚拟路由器。

注 SF500 型号不支持 VRRP 功能。

其中包含以下主题：

- [概述](#)
- [VRRP 的可配置元素](#)
- [配置 VRRP](#)

概述

VRRP 是一个选择和冗余协议，用于向 LAN 上的物理路由器动态分配虚拟路由器责任。这样可以提高网络中路由路径的畅通性和可靠性。

在 VRRP 中，虚拟路由器中的一台物理路由器会选作主装置，而同一个虚拟路由器中的另一物理路由器则作为备用装置，以备主装置出现故障时使用。物理路由器也称为 VRRP 路由器。

参与主机的默认网关会分配给虚拟路由器，而非物理路由器。如果正在代表虚拟路由器路由数据包的物理路由器出现故障，将选择另一台物理路由器自动替换。在任意指定时间转发数据包的物理路由器称为主路由器。

VRRP 还能够对流量进行负载共享。通过将 VRRP 配置为由多台路由器共享进出 LAN 客户端的流量，流量可以在可用路由器间公平分享。

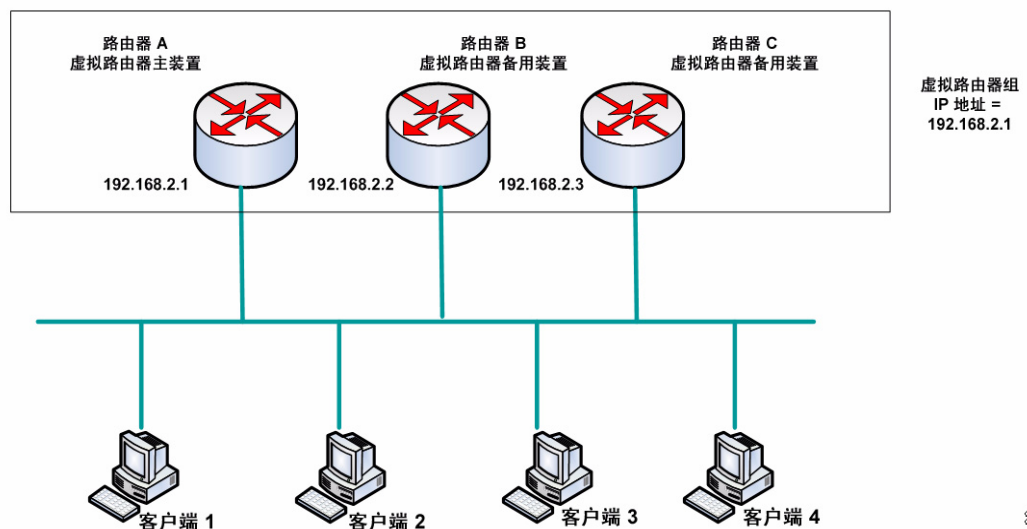
限制

只有 SG500X/ESW2-550X 交换机支持 VRRP。

VRRP 拓扑

下图显示了一个已配置 VRRP 的 LAN 拓扑。在此示例中，路由器 A、B 和 C 均为 VRRP，包含一个虚拟路由器。该虚拟路由器的 IP 地址与路由器 A 的以太网接口配置的 IP 地址相同 (198.168.2.1)。

基本 VRRP 拓扑



由于该虚拟路由器使用的是路由器 A 的物理以太网接口的 IP 地址，路由器 A 承担*虚拟路由器主装置*的角色，也称为 *IP 地址所有者*。作为虚拟路由器主装置，路由器 A 控制虚拟路由器的 IP 地址，并负责代表虚拟路由器路由数据包。客户端 1 至 3 配置为默认网关 IP 地址 198.168.2.1。客户端 4 配置为默认网关 IP 地址 198.168.2.2。

注 作为 IP 地址所有者的 VRRP 路由器响应/处理目的地址为该 IP 地址的数据包。作为虚拟路由器主装置、但不是 IP 地址所有者的 VRRP 路由器不会响应/处理这些数据包。

路由器 B 和 C 用作*备用虚拟路由器*。如果虚拟路由器主装置出现故障，则配置较高优先级的路由器成为虚拟路由器主装置，为 LAN 主机提供服务，最大限度地减少业务中断。

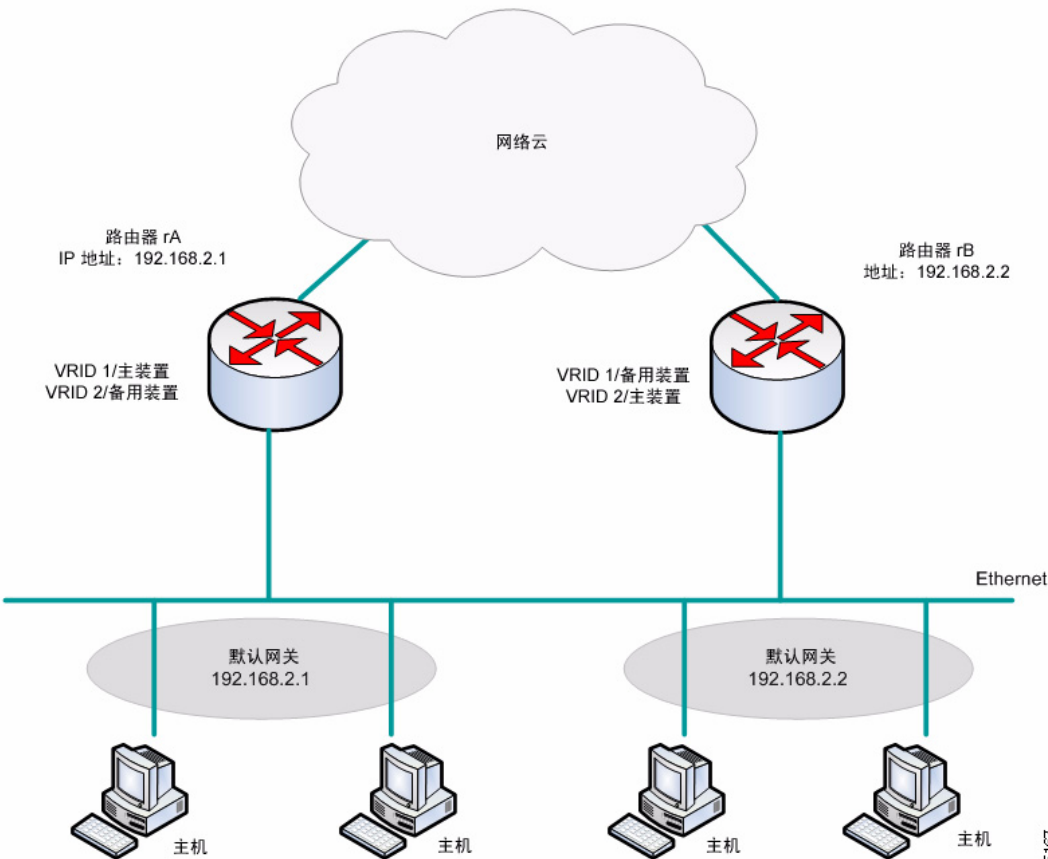
注 VRRP 路由器优先级取决于以下因素：如果 VRRP 路由器是所有者，其优先级为 255（最高），如果不是所有者，则须手动配置其优先级（始终小于 255）。

当路由器 A 恢复时，将再次成为虚拟路由器主装置。在主装置恢复期间，两个主装置都转发数据包，因此会出现重复情况（定期行为），但不会产生业务中断。

有关 VRRP 路由器所承担角色以及虚拟路由器主装置出现故障时所出现情况的更多详情，请参阅 [VRRP 路由器优先级和抢占](#)。

下图显示了一个已配置 VRRP 的 LAN 拓扑。路由器 A 和 B 共享进出客户端 1 至 4 的流量，如果任意一台路由器出现故障，路由器 A 和 B 可相互作为对方的备用虚拟路由器。

负载共享 VRRP 拓扑



在此拓扑中，配置了两个虚拟路由器。对于虚拟路由器 1，rA 是 IP 地址 192.168.2.1 的所有者，也是虚拟路由器主装置，而 rB 则是 rA 的备用虚拟路由器。客户端 1 和 2 配置为默认网关 IP 地址 198.168.2.1。

对于虚拟路由器 2，rB 是 IP 地址 192.168.2.2 的所有者，也是虚拟路由器主装置，而 rA 则是 rB 的备用虚拟路由器。客户端 3 和 4 配置为默认网关 IP 地址 198.168.2.2。

VRRP 的可配置元素

必须为同一个 LAN 上的所有虚拟路由器分配唯一的虚拟路由器标识符 (VRID)。必须使用与虚拟路由器有关的所有信息（包括其 VRID）对支持同一个虚拟路由器的所有 VRRP 路由器进行配置。只有当设备上也已启动 IP 路由时，才应启动该设备上的虚拟路由器。

如**配置 VRRP**节所述，您可以使用 CLI 命令或通过 Web GUI 将 VRRP 路由器配置为参与一个或多个虚拟路由器。

若要配置虚拟路由器，您需在支持该虚拟路由器的每个 VRRP 路由器上配置其信息，例如虚拟路由器 ID 及其 IP 地址。可以配置和自定义以下元素。

虚拟路由器标识

必须分配一个标识符 (VRID)，还可以分配一个说明。下节将介绍虚拟路由器的各种属性。

VRRP 支持最多 255 个虚拟路由器（VRRP 组）。

VRRP 版本

设备支持以下 VRRP 版本类型：

- 基于 RFC5798 的 IPv4 VRRPv3。将发送 VRRPv3 消息。
- 基于 RFC5798 的 IPv4 VRRPv3 和 VRRPv2。将发送 VRRPv3 和 VRRP v2 消息。
- 基于 RFC3768 的 IPv4 VRRPv2。将发送 VRRPv2 消息。

会为每个虚拟路由器配置 VRRP 版本。默认配置为 VRRPv2。

配置虚拟路由器时，可能会出现以下情况：

- 虚拟路由器的所有现有 VRRP 路由器都在 VRRPv3 下运行。在此情况下，请将您的新 VRRP 路由器配置为在 VRRPv3 下运行。
- 虚拟路由器的所有现有 VRRP 路由器都在 VRRPv2 下运行。在此情况下，将您的新 VRRP 路由器配置为在 VRRPv2 下运行。
- 如果虚拟路由器中至少有一个 VRRP 路由器同时在 VRRPv2 和 VRRPv3 下运行，在此情况下，尽管在 VRRPv2 下也能进行互操作，也要将您的 VRRP 路由器配置为在 VRRPv3 下运行。

注 如果虚拟路由器中有只能在 VRRPv2 下运行的路由器和只能在 VRRPv3 下运行的路由器，则您必须配置至少一台 VRRPv2 和 VRRPv3 路由器。

注 当 VRRP 路由器上同时启用了 VRRPv2 和 VRRPv3 时，VRRP 路由器可传输 VRRPv2 和 VRRPv3 两种数据包。根据 VRRPv3 标准，当从 v2 升级至 v3 时，应该同时启用 VRRPv2 和 VRRPv3。混合使用两种版本不是长久解决方案。有关 VRRPv2 和 VRRPv3 互操作的详情，请参阅 VRRPv3 标准。

虚拟路由器 IP 地址

每个虚拟路由器都会分配一个或多个由当前主装置负责的 IP 地址。

支持虚拟路由器的 VRRP 路由器必须使用与虚拟路由器上配置的 IP 地址处于同一个 IP 子网的 IP 接口。

根据以下规则，为虚拟路由器分配 IP 地址：

- 支持虚拟路由器的所有 VRRP 路由器在其虚拟路由器配置中必须配置相同的虚拟路由器 IP 地址。
- IP 地址不能在其他虚拟路由器中使用，也不能在不支持该虚拟路由器的 VRRP 中使用。
- 支持虚拟路由器的 VRRP 路由器中必须有一个是虚拟路由器所有 IP 地址的所有者。如果 IP 地址是在 VRRP 路由器的 IP 接口上配置的实际地址，则该路由器即为 IP 地址的所有者。
- 如果 VRRP 路由器（物理路由器）是虚拟路由器的 IP 地址所有者，则必须在 VRRP 路由器上手动配置该虚拟路由器的 IP 地址，而不能进行 DHCP 分配。
- 如果 VRRP 路由器不是虚拟路由器的 IP 地址所有者：
 - 非所有者 VRRP 路由器配置的 IP 接口必须与该虚拟路由器 IP 地址处于相同 IP 子网。
 - 必须在 VRRP 路由器中手动配置相应的 IP 子网，而不能进行 DHCP 分配。

支持同一个虚拟路由器的所有 VRRP 路由器必须使用相同的配置。如果配置不相同，将使用主装置的配置。当配置与主装置的配置不同时，备用 VRRP 路由器会记录一条系统消息。

VRRP 路由器中的源 IP 地址

在虚拟路由器流出 VRRP 消息中，每个支持虚拟路由器的 VRRP 路由器均使用其自己的 IP 地址作为源 IP 地址。同一个虚拟路由器的 VRRP 路由器在 VRRP 消息中进行相互通信。如果 VRRP 路由器是虚拟路由器的 IP 地址所有者，则 IP 地址即其中一个虚拟路由器 IP 地址。如果 VRRP 路由器不是虚拟路由器 IP 地址的所有者，则该 IP 地址即连接同一个虚拟路由器 IP 子网的 VRRP 路由器接口的 IP 地址。

如果源 IP 地址为手动配置，则将删除该配置，并使用默认的源 IP 地址（在该接口上定义的最低的 VRRP 路由器 IP 地址）。如果源 IP 地址是默认地址，将使用新的默认源 IP 地址。

VRRP 路由器优先级和抢占

VRRP 冗余方案的主要功能是能够为每个 VRRP 路由器分配一个 VRRP 优先级。VRRP 优先级必须明确表示 VRRP 路由器作为在 VRRP 路由器中定义的虚拟路由器的备用装置的执行效率。如果虚拟路由器存在多个备用 VRRP 路由器，则如果当前主装置出现故障，将根据优先级确定将哪个备用 VRRP 路由器指定为主装置。

如果虚拟路由器是 IP 地址的所有者，则系统将自动为其分配 255 的 VRRP 优先级，且启动运行时，分配此虚拟路由器的 VRRP 路由器将自动用作虚拟路由器主装置。

在图中，如果作为虚拟路由器主装置的路由器 A 出现故障，将通过选择流程确定是虚拟路由器备用装置 B 还是 C 接管成为主装置。如果路由器 B 和 C 配置的优先级分别为 101 和 100，则将选择路由器 B 成为虚拟路由器主装置，因为该路由器的优先级较高。如果两台路由器的优先级相同，则将选择 IP 地址数值较高的路由器作为虚拟路由器主装置。

在默认情况下，将启用抢占功能，其说明如下：

- 已启用 - 如果某 VRRP 路由器比当前运行的主装置配置了更高的优先级，则该路由器将替换当前的主装置。
- 已禁用 - 即使某 VRRP 路由器比当前运行的主装置配置了更高的优先级，该路由器也不会替换当前的主装置。只有原始主装置（当其变成可用时）可替换备用装置。

VRRP 通告

虚拟路由器主装置向同一个组中的路由器（配置了相同的虚拟路由器标识）发送 VRRP 通告。

VRRP 通告封装在 IP 数据包中，并发送至该 VRRP 组分配的 IP v4 组播地址。默认情况下，通告每秒发送一次，通告间隔可配置。

通告间隔以毫秒为单位（范围：50 - 40950，默认为：1000）。非数值无效。

- 在 VRRP 第 3 版中，运行通告间隔会四舍五入为最接近的 10 毫秒数。
- 在 VRRP 第 2 版中，运行通告间隔会四舍五入为最接近的秒数。最小运行值为 1 秒。

配置 VRRP

可在以下页面配置端口。

虚拟路由器

可以在 VRRP 虚拟路由器页面中对 VRRP 属性进行配置和自定义。

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > 虚拟路由器**。

步骤 2 若要添加虚拟路由器，单击**添加**。

步骤 3 输入以下字段：

- **接口** - 定义了虚拟路由器的接口。
- **虚拟路由器标识符** - 用户定义的用于识别虚拟路由器的编号。
- **说明** - 用户定义的用于识别虚拟路由器的字符串。
- **状态** - 选中后，将在设备上启用 VRRP。
- **版本** - 选择要在此路由器上使用的 VRRP 版本。
- **IP 地址所有者** - 如果选中**是**，则表示设备的 IP 地址是虚拟路由器的 IP 地址。从**可用 IP 地址**列表中选择所有者 IP 地址，并将其移至**所有者 IP 地址**列表。
- 如果选中**否**，则您必须在**虚拟路由器 IP 地址**字段中输入虚拟路由器的地址。如果此处添加了多个 IP 地址，请按如下格式将其隔开：1.1.1.1, 2.2.2.2.
- **源 IP 地址** - 选择要在 VRRP 消息中使用的 IP 地址。默认的源 IP 地址是接口上定义的最低的 IP 地址。
- **优先级** - 如果此设备为所有者，则此字段将赋值为 255，且此值不能更改。如果此设备不是所有者，将根据其能力决定是否能成为主装置。非所有者设备的默认值是 100。

- **抢占模式** - 按照 **VRRP 路由器优先级和抢占** 中的说明, 选择 true/false 以启用/禁用抢占模式。
- **通告间隔** - 按照 **VRRP 通告** 中的说明, 输入时间间隔。

注 如果这些参数已更改 (**编辑**), 则虚拟路由器即已修改, 系统将发送带有新参数的新消息。

步骤 4 若要参阅有关虚拟路由器的更多信息, 请单击**详情**。

步骤 5 会为选定的虚拟路由器显示以下字段:

- **接口** - 定义了虚拟路由器的第 2 层接口 (端口、LAG 或 VLAN)
- **虚拟路由器标识符** - 虚拟路由器识别编号。
- **虚拟路由器 MAC 地址** - 虚拟路由器的虚拟 MAC 地址。
- **虚拟路由器 IP 地址表** - 与此虚拟路由器相关联的 IP 地址。
- **说明** - 虚拟路由器名称。
- **版本** - 虚拟路由器版本。
- **状态** - 是否已启用 VRRP。
- **IP 地址所有者** - 虚拟路由器 IP 地址的所有者。
- **主/备用装置状态** - 虚拟路由器是主装置还是备用装置。
- **偏移时间** - 计算主装置停机间隔所用的时间。
- **主装置停机时间** - 备用装置声明主装置停机的时间间隔。
- **优先模式** - 优先模式是否已启用。
- 选定虚拟路由器的**我的参数**:
 - **优先级** - 此虚拟路由器设备的优先级, 取决于其作为主装置运行的能力。
 - **通告间隔** - 如 **VRRP 通告** 中所述的时间间隔。
 - **源 IP 地址** - 要在 VRRP 消息中使用的 IP 地址。
- 主设备的**主装置参数**:
 - **优先级** - 255
 - **通告间隔** - 如 **VRRP 通告** 中所述的时间间隔。
 - **源 IP 地址** - 要在 VRRP 消息中使用的 IP 地址。

VRRP 统计信息

查看 VRRP 统计信息并清除接口计数器的步骤：

步骤 1 单击 **IP 配置 > IPv4 管理和接口 > VRRP 统计信息**。

对于每个启用了 VRRP 的端口，将显示以下字段：

- **接口** - 显示启用了 VRRP 的接口。
- **无效校验和** - 显示具有无效校验和的数据包数。
- **无效数据包长度** - 显示具有无效数据包长度的数据包数。
- **无效 TTL** - 显示具有无效存活时间值的数据包数。
- **无效 VRRP 数据包类型** - 显示具有无效 VRRP 数据包类型的数据包数。
- **无效 VRRP ID** - 显示具有无效 VRRP ID 的数据包数。
- **无效协议编号** - 显示具有无效协议编号的数据包数。
- **无效 IP 列表** - 显示具有无效 IP 列表的数据包数。
- **无效间隔** - 显示具有无效间隔的数据包数。
- **无效验证** - 显示具有无效验证的数据包数。

步骤 2 选择一个接口。

步骤 3 单击**清除接口计数器**清除该接口的计数器。

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：

- **定义用户**
- **配置 TACACS+**
- **配置 RADIUS**
- **管理访问方法**
- **密钥管理**
- **安全敏感数据管理**
- **SSL 服务器**

以下各节介绍了针对设备 CPU 的防攻击保护：

- **配置 TCP/UDP 服务**
- **定义风暴控制**
- **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**
- **配置 TACACS+**
- **配置 RADIUS**
- **配置端口安全**
- **802.1X**
- **定义时间范围**

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。

- **DoS 防护**
- **DHCP Snooping**
- **SSL 服务器**
- **定义风暴控制**
- **配置端口安全**
- **IP 源防护**
- **ARP 检测**
- **访问控制**
- **第一步跳安全性**

定义用户

默认的用户名/密码为 **cisco/cisco**。第一次使用默认用户名和密码登录时，您需要输入新密码。默认情况下，将启用密码复杂性设置。如果您选择的密码不够复杂（已在“密码强度”页面中启用**密码复杂性设置**），系统将提示您创建其他密码。

设置用户帐户

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），将从系统中移除默认用户。

注 系统不允许删除所有用户。如果选择所有用户，**删除**按钮会被禁用。

添加新用户的步骤：

步骤 1 单击**管理 > 用户帐户**，

此页面显示系统中定义的用户及其用户权限等级。

步骤 2 选择**密码恢复服务**，启用此功能。当此功能启用时，具有设备 Console 端口物理访问权限的最终用户可以进入引导菜单，并触发密码恢复流程。当引导系统流程结束时，您无需密码验证即可登录该设备。只有通过 Console，且只有当该 Console 连接至具有物理访问权限的设备时，才可以进入该设备。

禁用密码恢复机制时，依然可用访问启动菜单，您可以触发密码恢复流程。区别在于，在此情况下，在系统引导进程期间将移除所有配置和用户文件，并为终端生成适用的日志消息。

步骤 3 单击**添加**以添加新用户，或单击**编辑**以修改用户。

步骤 4 输入参数。

- **用户名** - 输入新用户名，长度应介于 0 到 20 个字符之间。不允许使用 UTF-8 字符。
- **密码** - 输入一个密码（不允许使用 UTF-8 字符）。如果已定义密码强度和复杂性，则用户密码必须与在**设置密码复杂度规则**一节中配置的策略相符。
- **确认密码** - 再次输入密码。
- **密码强度计** - 显示密码的强度。密码强度和复杂性的策略在“密码强度”页面中配置。
- **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 5 单击**应用**。用户将添加到设备的当前配置文件中。

设置密码强度规则

密码用于验证访问设备的用户。简单的密码可能会危害安全。因此，默认情况下，将实施密码复杂性要求，并可在必要时进行配置。密码复杂性要求在**密码强度**页面上进行配置，该页面可通过安全下拉菜单打开。此外，还可以在此页面上配置密码过期时间。

定义密码复杂性规则的步骤：

步骤 1 单击**安全 > 密码强度**，

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*。

配置 TACACS+

组织可建立终端接入控制器接入控制系统(TACACS+)服务器，为所有设备提供集中的安全保护。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。

设备可作为 TACACS+ 客户端工作，使用 TACACS+ 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，TACACS+ 服务器将检查用户权限。
- **帐务** - 使用 TACACS+ 服务器启用登录会话帐务功能。让系统管理员可以从 TACACS+ 服务器生成帐务报告。

除提供验证和授权服务之外，TACACS+ 协议还可通过加密 TACACS 正文消息帮助确保 TACACS 消息受到保护。

TACACS+ 仅支持 IPv4。

某些 TACACS+ 服务器支持单个连接，其可使设备接收单个连接中的所有信息。如果 TACACS+ 服务器不支持单个连接，则设备将恢复到多个连接。

使用 TACACS+ 服务器的帐务

用户可使用 RADIUS 或 TACACS+ 服务器启用登录会话帐务功能。

用于 TACACS+ 服务器帐务且可由用户配置的 TCP 端口是用于 TACACS+ 服务器验证与授权的同一 TCP 端口。

用户登录或注销时，设备将向 TACACS+ 服务器发送以下信息：

表 2:

参数	说明	包含在开始消息中	包含在停止消息中
task_id	唯一的帐务会话标识符。	是	是
user	用于登录验证而输入的用户名。	是	是
rem-addr	用户 IP 地址。	是	是
elapsed-time	用户已登录时间。	否	是
reason	会话终止的原因。	否	是

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 TACACS+ 服务器。
- 配置 TACACS+ 服务器时，默认情况下帐务功能会禁用。

与其他功能进行交互

无法同时在 RADIUS 和 TACACS+ 服务器上启用帐务。

工作流程

要使用 TACACS+ 服务器，请执行以下操作：

-
- 步骤 1** 在 TACACS+ 服务器上开立一个用户帐户。
- 步骤 2** 在 TACACS+ 页面和“添加 TACACS+ 服务器”页面配置服务器和其他参数。
- 步骤 3** 在“管理访问验证”页面中选择 **TACACS+**，这样，当用户登录设备时，将在 TACACS+ 服务器而非本地数据库中执行验证。
- 注** 如果配置了多个 TACACS+ 服务器，设备将使用已配置的可用 TACACS+ 服务器优先级选择设备要使用的 TACACS+ 服务器。

配置 TACACS+ 服务器

TACACS+ 页面可配置 TACACS+ 服务器。

只有在 TACACS+ 服务器上具有 15 级权限的用户才能管理设备。根据下面的用户或组定义中的字符串，为 TACACS+ 服务器上的用户或用户组赋予 15 级权限：

```
service = exec {  
  priv-lvl = 15  
}
```

配置 TACACS+ 服务器参数的步骤：

-
- 步骤 1** 单击 **安全 > TACACS+**，
- 步骤 2** 根据需要启用 TACACS+ 帐务。请参阅[使用 TACACS+ 服务器的帐务](#)一节中的说明。

步骤 3 输入以下默认参数：

- **密钥字符串** - 输入默认**密钥字符串**，用于与在**加密或明文**模式下的所有 TACACS+ 服务器进行通信。可将设备配置为使用此密钥或使用一个为特定服务器输入的密钥（在“添加 TACACS+ 服务器”页面中输入）。

如果您未在此字段中输入密钥字符串，则在“添加 TACACS+ 服务器”页面中输入的服务器密钥必须与 TACACS+ 服务器所使用的加密密钥相匹配。

如果您在此处同时输入了密钥字符串，并且为单个 TACACS+ 服务器输入了密钥字符串，则为单个 TACACS+ 服务器配置的密钥字符串优先级较高。
- **应答超时** - 输入设备与 TACACS+ 服务器之间的连接超时之前经过的时间量。如果未在“添加 TACACS+ 服务器”页面中为特定服务器输入值，则会从此字段中获取该值。
- **源 IPv4 接口** - （仅在第 3 层系统模式下）选择要在与 TACACS+ 服务器通信的消息中使用的设备 IPv4 源接口。
- **源 IPv6 接口** - （仅在第 3 层系统模式下）选择要在与 TACACS+ 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 4 单击**应用**。将 TACACS+ 默认设置添加至当前配置文件。如果“添加”页面中未定义对等参数，则使用这些设置。

步骤 5 若要添加一台 TACACS+ 服务器，请单击**添加**。

步骤 6 输入参数。

- **服务器定义** - 选择以下其中一种方法来识别 TACACS+ 服务器：
 - **按 IP 地址** - 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 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** - 选择支持的源地址 IP 版本：IPv6 或 IPv4。
- **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 TACACS+ 服务器的 IP 地址或名称。
- **优先级** - 输入使用此 TACACS+ 服务器的顺序。0 代表优先级最高的 TACACS+ 服务器，也是使用的第一个服务器。如果它无法建立与优先级最高的服务器的会话，设备将尝试使用下一个优先级最高的服务器。
- **源 IP 地址** - （适用于处于第 3 层系统模式下的 SG500X 设备和其他设备）。选择该选项使用默认设备源地址或可用设备 IP 地址之一与 TACACS+ 服务器通信。
- **密钥字符串** - 输入用于在设备与 TACACS+ 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 TACACS+ 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。您可以选择设备上的默认密钥，或者以**加密**或**明文**形式输入密钥。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。

如果输入密钥，该密钥将覆盖在主页上为设备定义的默认密钥字符串（如果有）。

- **应答超时** - 输入设备与 TACACS+ 服务器之间的连接超时之前经过的时间量。选择**使用默认设置**可使用此页面上所显示的默认值。
- **验证 IP 端口** - 输入通过其进行 TACACS+ 会话的端口号。
- **单个连接** - 选择后，可以通过单个连接接收所有信息。如果 TACACS+ 服务器不支持单个连接，则设备将恢复到多个连接。

步骤 7 若要以明文形式显示配置文件中的敏感数据，单击**将敏感数据显示为明文模式**。

步骤 8 单击**应用**。TACACS+ 服务器将添加到设备的当前配置文件中。

配置 RADIUS

远程授权拨入用户服务 (RADIUS) 服务器提供了集中的 802.1X 或基于 MAC 的网络访问控制。设备是一种 RADIUS 客户端，可以使用 RADIUS 服务器来提供集中的安全保护。

组织可建立远程身份验证拨入用户服务 (RADIUS) 服务器，为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。

设备可作为 RADIUS 客户端工作，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。
- **帐务** - 使用 RADIUS 服务器启用登录会话帐务功能。让系统管理员可以从 RADIUS 服务器生成帐务报告。

使用 RADIUS 服务器的帐务

用户可使用 RADIUS 服务器启用登录会话帐务功能。

用于 RADIUS 服务器帐务且可由用户配置的 TCP 端口是用于 RADIUS 服务器验证与授权的同一 TCP 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，默认情况下帐务功能会禁用。

与其他功能进行交互

无法同时在 RADIUS 和 TACACS+ 服务器上启用帐务。

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**，

步骤 2 输入 RADIUS 帐务选项。可能的选项有：

- **基于端口的访问控制 (802.1X、基于 MAC、Web 验证)** - 指定 RADIUS 服务器用于 802.1x 端口帐务。
- **管理访问** - 指定 RADIUS 服务器用于用户登录帐务。
- **基于端口的访问控制和管理访问** - 指定 RADIUS 服务器用于用户登录帐务和 802.1x 端口帐务。
- **无** - 指定 RADIUS 服务器不用于帐务。

步骤 3 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** - （仅在第 3 层系统模式下）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** - （仅在第 3 层系统模式下）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 4 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 5 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** - 将显示 IPv6 地址类型是全局的。
- **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** - 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。
- **帐务端口** - 输入用于帐务请求的 RADIUS 服务器端口 UDP 端口号。
- **重试次数** - 输入在认为已发生故障之前发送到 RADIUS 服务器的请求次数。如果选择**使用默认设置**，设备将使用重试次数的默认值。
- **无响应时间** - 输入服务请求绕过无响应 RADIUS 服务器之前必须经过的分钟数。如果选择**使用默认设置**，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 6 若要以明文形式显示配置文件中的敏感数据，单击**将敏感数据显示为明文模式**。

步骤 7 单击**应用**。RADIUS 服务器定义将添加到设备的当前配置文件中。

密钥管理

密钥管理

注 该功能仅适用于 SG500X/ESW2-550X 设备。

本节介绍如何为应用和协议（例如 RIP）配置密钥链。有关 RIP 如何使用密码链进行验证的描述，请参阅 [RIP 验证](#)。

要配置密钥链，请执行以下操作：

步骤 1 使用“密钥链设置”页面创建一个含有单个密钥的密钥链。

步骤 2 使用“密钥设置”页面添加其他密钥。

创建密钥链

使用“密钥链设置”页面创建新的密钥链。

步骤 1 单击**安全 > 密钥管理 > 密钥链设置**。

步骤 2 要添加新的密钥链，单击**添加**以打开“添加密钥链”页面，然后输入以下字段：

- **密钥链** - 密钥链的名称。
- **密钥标识符** - 密钥链的整数标识符。
- **密钥字符串** - 密钥链字符串的值。输入以下其中一个选项：
 - **用户定义 (加密模式)** - 输入加密版本。

- *用户定义 (明文模式)* - 输入明文版本。

注 既可输入**接受有效期限**值，也可输入**发送有效期限**值。接受有效期限表明用于接受数据包的密钥标识符在何时有效。发送有效期限表明用于发送数据包的密钥标识符在何时有效。

- **接受有效期限/发送有效期限** - 指定何时接受带有该密钥的数据包。请选择以下其中一个选项。
 - *始终有效* - 对密钥标识符的有效期不设限制。
 - *用户定义* - 限定密钥链的有效期。如果选择该选项，请在以下字段中输入值：

注 如果您选择“用户定义”，则必须手动或从 SNTP 设置系统时间。否则，接受有效期限和发送有效期限始终会失败。

以下字段适用于“接受有效期限”和“发送有效期限”字段：

- **开始日期** - 输入密钥标识符生效的最早日期。
- **开始时间** - 输入密钥标识符于开始日期生效的最早时间。
- **结束日期** - 输入密钥标识符有效期的最后日期。请选择以下其中一个选项。
 - *无限期* - 对密钥标识符的有效期不设限制。
 - *持续时间* - 限定密钥链的有效期。如果选择该选项，请在以下字段中输入值：
- **持续时间** - 密钥标识符的有效时间长度。输入以下字段：
 - *天数* - 密钥标识符的有效天数。
 - *小时数* - 密钥标识符的有效小时数。
 - *分钟数* - 密钥标识符的有效分钟数。
 - *秒数* - 密钥标识符的有效秒数。

步骤 3 单击**应用**。设置将写入当前配置文件中。

创建密钥设置

使用“密钥链设置”页面将密钥添加到已存在的密钥链中。

步骤 1 单击**安全 > 密钥管理 > 密钥设置**。

步骤 2 要添加新的密钥字符串，请单击**添加**。

步骤 3 输入以下字段：

- **密钥链** - 密钥链的名称。
- **密钥标识符** - 密钥链的整数标识符。
- **密钥字符串** - 密钥链字符串的值。输入以下其中一个选项：
 - *用户定义 (加密模式)* - 输入加密版本。
 - *用户定义 (明文模式)* - 输入明文版本。

注 既可输入**接受有效期限**值，也可输入**发送有效期限**值。**接受有效期限**表明用于接受数据包的密钥标识符在何时有效。**发送有效期限**表明用于发送数据包的密钥链在何时有效。仅描述**接受有效期限**的字段。**发送有效期限**的字段与接受有效期限的字段相同。

- **接受有效期限** - 指定何时接受带有该密钥的数据包。请选择以下其中一个选项。
 - *始终有效* - 对密钥标识符的有效期不设限制。
 - *用户定义* - 限定密钥链的有效期。如果选择该选项，请在以下字段中输入值：
- **开始日期** - 输入密钥标识符生效的最早日期。
- **开始时间** - 输入密钥标识符于开始日期生效的最早时间。
- **结束日期** - 输入密钥标识符有效期的最后日期。请选择以下其中一个选项。
 - *无限期* - 对密钥标识符的有效期不设限制。
 - *持续时间* - 限定密钥链的有效期。如果选择该选项，请在以下字段中输入值：
- **持续时间** - 密钥标识符的有效时间长度。输入以下字段：
 - *天数* - 密钥标识符的有效天数。
 - *小时数* - 密钥标识符的有效小时数。
 - *分钟数* - 密钥标识符的有效分钟数。
 - *秒数* - 密钥标识符的有效秒数。

步骤 4 要始终将敏感数据以明文模式（而非以加密模式）显示，单击**以明文模式显示敏感数据**。

步骤 5 单击**应用**。设置将写入当前配置文件中。

管理访问方法

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。

活动的访问模板

“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。

如果已激活仅 Console 访问模板，则将其禁用的唯一方式是从管理站直接连接到设备上的物理 Console 端口。

有关详情，请参阅[定义模板规则](#)。

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。

注 如果您选择了“仅 Console”，则系统会显示一条警告消息。如果您继续操作，则系统会立即断开您与基于 Web 的配置实用程序的连接，并且您只能通过 Console 端口访问设备。这只适用于提供 Console 端口的设备类型。

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。1 代表最高优先级。
- **管理方法** - 选择为其定义了规则的管理方法。选项如下：
 - **全部** - 将所有管理方法分配给规则。
 - **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 SSH 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** - 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 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。

定义模板规则

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 > 管理访问控制 > 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** - 选择为其定义了规则的管理方法。选项如下：
 - **全部** - 将所有管理方法分配给规则。
 - **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**允许**以允许尝试使用配置的访问方法通过按照此规则定义的接口或 IP 源来访问设备的用户进行访问。或选择**拒绝**以拒绝访问。
- **应用到接口** - 选择规则所关联的接口。选项如下：
 - **全部** - 适用于所有端口、VLAN 和 LAG。
 - **用户定义** - 仅适用于选择的端口、VLAN 或 LAG。
- **接口** - 输入接口编号。
- **应用到源 IP 地址** - 选择访问模板适用的源 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、Console、Telnet、HTTP 和 HTTPS。可以在本地或在 TACACS+ 或 RADIUS 服务器上执行验证。

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`。

用户验证按照选择验证方法的顺序进行。如果第一种验证方法不可用，则使用选择的下一个方法。例如，如果选择的验证方法为“RADIUS”和“本地”，并且以优先级顺序对所有已配置 RADIUS 服务器进行查询但未获得响应，则会在本地对用户进行验证。

如果验证方法失败或用户的权限级别不足，则系统会拒绝用户访问设备。换句话说，如果验证因验证方法而失败，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。

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 从**应用**列表中选择一种访问方法。

步骤 3 使用箭头在“可选方法”列与“选定的方法”列之间移动验证方法。选择的第一种方法即为使用的第一种方法。

- *RADIUS* - 在 RADIUS 服务器上验证用户。您必须已配置了一个或多个 RADIUS 服务器。
- *TACACS+* - 在 TACACS+ 服务器上验证用户。您必须已配置了一个或多个 TACACS+ 服务器。
- 无 - 允许用户在不经过程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 4 单击**应用**。选择的验证方法将与访问方法相关联。

安全敏感数据管理

请参阅 **安全：安全敏感数据管理**。

SSL 服务器

本节介绍安全套接字层 (SSL) 功能。

SSL 概述

安全套接字层 (SSL) 功能用于为设备打开 HTTPS 会话。

HTTPS 会话可以使用设备上存在的默认证书打开。

某些浏览器在使用默认证书时会生成警告，因为此证书未由证书颁发机构 (CA) 签名。最好使用由可信任 CA 签名的证书。

要使用用户创建的证书打开 HTTPS 会话，请执行以下操作：

1. 生成证书。
2. 请求 CA 认证证书。
3. 将已签名证书导入设备。

默认设置和配置

默认情况下，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证书 1 和 2 的信息。除以下字段之外，相关字段会在**编辑**页面中定义：

- **有效起始日期** - 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：

- **重新生成 RSA 密钥** - 选择此项可重新生成 RSA 密钥。
- **密钥长度** - 输入要生成的 RSA 密钥的长度。
- **通用名称** - 指定完全合格的设备 URL 或 IP 地址。如果未指定，会默认为设备的最小 IP 地址（证书生成时）。
- **组织单元** - 指定组织单元或部门名称。
- **组织名称** - 指定组织名称。
- **位置** - 指定位置或城市名称。
- **省/自治区/直辖市** - 指定省/自治区/直辖市名称。
- **国家/地区** - 指定国家/地区名称。
- **持续时间** - 指定证书的有效天数。

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。
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** - 复制到已收到证书中。
- **导入 RSA 密钥对** - 选择此项可复制到新 RSA 密钥对中。
- **公共密钥** - 复制到 RSA 公共密钥中。
- **专用密钥 (加密模式)** - 选择并复制到加密形式的 RSA 专用密钥中。
- **专用密钥 (明文模式)** - 选择并复制到明文形式的 RSA 专用密钥中。

步骤 4 单击**将敏感数据显示为加密模式**可以加密模式显示此密钥。单击此按钮后，专用密钥会以加密形式写入配置文件（单击“应用”后）。

步骤 5 单击**应用**将更改应用到当前配置。

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，密钥会以加密形式显示。

SSH 服务器

请参阅[安全：SSH 服务器](#)。

SSH 客户端

请参阅[安全：SSH 客户端](#)。

配置 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。

TCP 服务表显示了每个服务的以下字段：

- **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。）

步骤 3 单击**应用**。服务将写入当前配置文件中。

定义风暴控制

接收到广播帧、组播帧或未知的单播帧后，系统会对它们进行复制，并将副本发送到所有可能的出口端口。这意味着，实际上已将它们发送到属于相关 VLAN 的所有端口。这样一来，一个入口帧会转变为多个入口帧，因此会产生流量风暴隐患。

您可以通过风暴保护来限制进入设备的帧数，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。

定义风暴控制的步骤：

步骤 1 单击 **安全 > 风暴控制**，

在“编辑风暴控制”页面中，对此页面上除**风暴控制速率阈值 (%)**之外的所有字段进行了介绍。它显示了在端口上应用风暴控制之前未知的单播、组播和广播数据包的总可用带宽的百分比。默认值为端口最大速率的 10%，它是在“编辑风暴控制”页面中设置的。

步骤 2 选择一个端口，然后单击**编辑**。

步骤 3 输入参数。

- **接口** - 选择已启用风暴控制的端口。
- **风暴控制** - 选择该选项可启用风暴控制。
- **风暴控制速率阈值** - 输入可用来转发未知数据包的最大速率。此阈值的默认值为 10,000（针对 FE 设备）和 100,000（针对 GE 设备）。
- **风暴控制模式** - 选择其中一种模式：
 - *未知单播、组播和广播* - 将未知的单播、广播和组播流量计入带宽阈值。
 - *组播和广播* - 将广播和组播流量一起计入带宽阈值。
 - *仅广播* - 仅将广播流量计入带宽阈值。

步骤 4 单击**应用**。将修改风暴控制，并更新当前配置文件。

配置端口安全

限制用户通过特定的 MAC 地址访问端口可增强网络安全。可以动态地学习或静态地配置 MAC 地址。

端口安全功能可监控接收的和学习的数据包。限制用户通过特定的 MAC 地址访问锁定的端口。

端口安全具有四种模式：

- **传统锁定** - 端口上学习的所有 MAC 地址均被锁定，并且端口未学习任何新 MAC 地址。学习的地址不会过期或无需重新学习。
- **有限动态锁定** - 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，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。

当在新 MAC 地址未经授权的端口（该端口已按照传统模式进行锁定且具有新 MAC 地址，或者该端口已被动态锁定且已超过了允许地址的最大数量）上检测到来自该地址的帧时，会调用保护机制，并且可能会执行以下操作之一：

- 丢弃帧
- 转发帧
- 关闭端口

当在另一个端口上发现安全 MAC 地址时，将转发帧，但不会学习该端口上的 MAC 地址。

除了以上这些操作，您还可以生成 Trap，并限制其频率和数量以避免设备过载。

注 若要在端口上使用 802.1X，则端口必须处于多主机或多会话模式。如果端口处于单个模式，则不能在端口上设置安全（请参阅 802.1x “主机和会话验证” 页面）。

配置端口安全的步骤：

步骤 1 单击**安全 > 端口安全**，

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**）。启用重新学习和老化。
- **重置即安全删除** - 重置后删除当前与端口相关联的动态 MAC 地址。新的 MAC 地址可作为重置即删除地址学习，数量最多为端口上允许的最大地址数量。禁用重新学习和老化。
- **允许的最大地址数量** - 输入当选择**有限动态锁定**学习模式时可在端口上学习的 MAC 地址的最大数。数值 0 表示接口上仅支持静态地址。
- **违反规则响应措施** - 选择对到达锁定端口的数据包所应用的操作。选项如下：
 - **丢弃** - 丢弃来自任何未学习源的数据包。
 - **转发** - 转发来自任何未知源的数据包，而无需学习 MAC 地址。
 - **关闭** - 丢弃来自任何未学习源的数据包，并关闭端口。在重新激活端口或重启设备之前，该端口将保持关闭状态。
- **Trap** - 选择该选项可在锁定端口接收到数据包时启用 Trap。这与违反锁定的行为有关。对于传统锁定，这是指任何接收到的新地址。对于有限动态锁定，这是指超过允许地址数量的任何新地址。
- **Trap 频率** - 输入 Trap 之间的最短时间间隔（以秒为单位）。

步骤 4 单击**应用**。将修改端口安全，并更新当前配置文件。

802.1X

请参阅[安全：802.1x 验证](#)一章，了解有关 802.1X 验证的信息。其中包括基于 MAC 和基于 web 的验证。

DoS 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。

安全的核心技术 (SCT)

设备用于抵御 DoS 攻击的方法之一是使用 SCT。在默认情况下，SCT 在设备上已启用，且不能被禁用。

思科设备是一种高级设备，除最终用户 (TCP) 流量之外还可以处理管理流量、协议流量和 Snooping 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。

SCT 可在“DoS > DoS 防护 > 安全套件设置”页面中进行监控（[详情按钮](#)）。

DoS 攻击类型

拒绝服务攻击可能涉及以下几种数据包或其他策略：

- **TCP SYN 数据包** - 这种数据包通常带有错误的发送者地址。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），使设备将其作为连接请求处理，导致服务器生成半开放式连接。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。
- **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，应将其阻塞。
- **Martian 地址** - 从 IP 协议的角度，Martian 地址是非法的。有关详情，请参阅 [Martian 地址](#)。
- **ICMP 攻击** - 向被攻击设备发送恶意 ICMP 数据包或过量的 ICMP 数据包，可能导致系统崩溃。
- **IP 分片** - 向设备发送带有重叠和过大净荷的严重受损 IP 分片。由于多种操作系统的 TCP/IP 分片重组代码中存在漏洞，这种攻击可能导致操作系统崩溃。Windows 3.1x、Windows 95 和 Windows NT 操作系统，以及版本 2.0.32 和 2.1.63 之前的 Linux 版本都容易受到此类攻击。
- **Stacheldraht Distribution** - 攻击程序使用一种客户端程序连接到处理程序（向僵尸代理发送命令的受损系统），转而又促进了 DoS 攻击。代理通过处理程序受到攻击程序的损害。

使用自动例行程序发现程序中存在的漏洞 - 接受目标远程主机上运行的远程连接。每个处理程序最多可控制一千个代理。

- **Invasor Trojan** - 攻击程序可通过 trojan 下载僵尸代理（或 trojan 本身包含僵尸代理）。攻击程序还可以使用能够发现程序缺陷（监听来自远程主机的连接）的自动化工具侵入设备。这种情况大多发生在设备用作网络服务器时。
- **Back Orifice Trojan** - 这是 trojan 的一种变体，使用 Back Orifice 软件植入 trojan。

针对 DoS 攻击的防御措施

拒绝服务 (DoS) 防护功能通过以下方式帮助系统管理员抵御此类攻击：

- 启用 TCP SYN 保护。如果启用此功能，将在发现 SYN 数据包攻击时发出报告，并暂时关闭受攻击的端口。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。
- 阻塞 SYN-FIN 数据包。
- 阻塞包含保留 Martian 地址的数据包（“Martian 地址”页面）
- 阻止 TCP 连接特定接口（“SYN 过滤”页面）以及对数据包进行速率限制（“SYN 速率保护”页面）
- 配置某些 ICMP 数据包的阻塞状态（“ICMP 过滤”页面）
- 从特定接口丢弃分片的 IP 数据包（“IP 分片过滤”页面）
- 拒绝 Stacheldraht Distribution、Invasor Trojan 和 Back Orifice Trojan 的攻击（“安全套件设置”页面）。

功能之间的依赖性

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。如果您试图在已定义 ACL 的接口上启用 DoS 防护，或试图在启用 DoS 防护的接口上定义 ACL，则会显示错误消息。

如果接口上有处于活动状态的 ACL，将无法阻止 SYN 攻击。

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，默认防护模式为**阻塞并报告**。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。

配置 DoS 防护

可使用以下页面配置此功能。

安全套件设置

注 激活 DoS 防护之前，您必须解除绑定所有绑定到端口的访问控制列表 (ACL) 策略或高级 QoS 策略。当端口启用 DoS 保护时，ACL 策略和高级 QoS 策略均不处于活动状态。

配置 DoS 防护全局设置并监控 SCT 的步骤：

步骤 1 单击 **安全 > DoS 防护 > 安全套件设置**，此时将显示 **安全套件设置**。

CPU 保护机制：已启用表示 SCT 已启用。

步骤 2 单击 **CPU 使用率**旁边的**详情**，以转到“CPU 使用率”页面并查看 CPU 资源利用率信息。

步骤 3 单击 **TCP SYN 保护**旁边的**编辑**，以转到“SYN 保护”页面并启用此功能。

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 单击**应用**。DoS 防护安全套件设置将写入当前配置文件中。

- 如果选择“接口级预防”，则单击相应的**编辑**按钮以配置所需的防护。

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。

如果该数量超过用户定义的特定阈值，将对端口应用符合 MAC-to-me 规则的拒绝 SYN。此规则以用户定义的间隔（SYN 保护期限）从端口上解除绑定。

配置 SYN 保护的步骤：

步骤 1 单击 **安全 > DoS 防护 > SYN 保护**。

步骤 2 输入参数。

- **阻塞 SYN-FIN 数据包** - 选择以启用此功能。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**。
 - **阻塞并报告** - 发现 TCP SYN 攻击后，指定给系统的 TCP SYN 数据包会被丢弃，端口状态将更改为**已阻塞**。
- **SYN 保护阈值** - SYN 数据包阻塞前每秒可通过的 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 数据包阻塞前的秒数（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。

- *已阻塞* - 流量未在此端口上转发。
- *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（**已报告或已阻塞并报告**）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 > DoS 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 > DoS 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。
- **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**。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。

仅当设备处于第 2 层系统模式下时，该功能才可用。

定义 SYN 速率保护的步骤：

步骤 1 单击 **安全 > DoS 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**。将定义 SYN 速率保护，并更新当前配置。

ICMP 过滤

使用“ICMP 过滤”页面可阻塞来自某些源的 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 > DoS 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* 以阻塞来自所有源地址的 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**。将定义 ICMP 过滤，并更新当前配置。

IP 分片过滤

使用“IP 分片”页面可阻塞分片的 IP 数据包。

配置分片的 IP 阻塞的步骤：

步骤 1 单击**安全 > DoS 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*以阻塞来自所有地址的 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**。将定义 IP 分片，并更新当前配置文件。

DHCP Snooping

请参阅 [DHCPv4 Snooping/中继](#)。

IP 源防护

IP 源防护作为一种安全功能，可用于预防当主机试图使用其邻近的 IP 地址时引起的攻击。

启用 IP 源防护时，设备将只向 DHCP Snooping 绑定数据库中包含的 IP 地址传输客户端 IP 流量。其中包括通过 DHCP Snooping 添加的地址和手动添加的条目。

如果数据包与数据库中的一个条目匹配，则设备将转发该数据包。如果不匹配，则丢弃该数据包。

与其他功能进行交互

下面这些内容都与 IP 源防护有关：

- 必须全局启用 DHCP Snooping，以便在接口上启用 IP 源防护。
- 只有符合以下条件时，IP 源防护才能在接口上处于活动状态：
 - DHCP Snooping 已在端口的至少一个 VLAN 上启用
 - 接口是 DHCP 不受信任的。信任端口上的所有数据包都已转发。
- 如果端口是 DHCP 受信任的，即使 IP 源防护在该条件下未处于活动状态，通过在端口上启用 IP 源防护，依然可以配置静态 IP 地址的过滤。
- 当端口状态从 DHCP 不信任更改为 DHCP 信任时，静态 IP 地址过滤条目依然位于绑定数据库中，但是它们将变成不活动状态。
- 如果端口上配置了源 IP 和 MAC 地址过滤，将不能启用端口安全。
- IP 源防护使用 TCAM 资源，需要针对每个 IP 源防护地址条目使用单个 TCAM 规则。如果 IP 源防护条目数量超过 TCAM 规则的可用数量，则超出的地址将处于不活动状态。

过滤

如果端口上已启用 IP 源防护，则：

- 将允许 DHCP Snooping 允许的 DHCP 数据包。
- 如果已启用源 IP 地址过滤：
 - IPv4 流量：只允许使用与端口相关联的源 IP 地址的流量。
 - 非 IPv4 流量：允许（包括 ARP 数据包）。

配置 IP 源防护工作流程

配置 IP 源防护的步骤：

- 步骤 1** 在“IP 配置 > DHCP > 属性”页面或“安全 > DHCP Snooping > 属性”页面启用 DHCP Snooping。
- 步骤 2** 定义在“IP 配置 > DHCP > 接口设置”页面中启用 DHCP Snooping 的 VLAN。
- 步骤 3** 在“IP 配置 > DHCP > DHCP Snooping 接口设置”页面中，将接口配置为信任接口或不信任接口。
- 步骤 4** 在“安全 > IP 源防护 > 属性”页面上启用 IP 源防护。
- 步骤 5** 根据需要在“安全 > IP 源防护 > 接口设置”页面中在不信任的接口上启用 IP 源防护。
- 步骤 6** 在“安全 > IP 源防护 > 绑定数据库”页面中查看绑定数据库中的条目。

启用 IP 源防护

全局启用 IP 源防护的步骤：

- 步骤 1** 单击 **安全 > IP 源防护 > 属性**。
- 步骤 2** 选择 **启用**，全局启用 IP 源防护。

在接口上配置 IP 源防护

如果在不信任端口/LAG 上启用 IP 源防护，将传输 DHCP Snooping 允许的 DHCP 数据包。如果已启用源 IP 地址过滤，则将按如下说明允许数据包传输：

- **IPv4 流量** - 只允许使用与特定端口相关联的源 IP 地址的 IPv4 流量。
- **非 IPv4 流量** - 允许所有非 IPv4 流量。

有关在接口上启用 IP 源防护的详情，请参阅[与其他功能进行交互](#)。

在接口上配置 IP 源防护的步骤：

- 步骤 1** 单击 **安全 > IP 源防护 > 接口设置**。
- 步骤 2** 从**过滤**字段中选择端口/LAG，并单击**转至**。此时将显示此单元上的端口/LAG 连同以下信息：
 - **IP 源防护** - 表示端口上是否已启用 IP 源防护。

- **DHCP Snooping 信任接口** - 表示是否是 DHCP 受信任的接口。

步骤 3 选择端口/LAG，然后单击**编辑**。在 **IP 源防护** 字段中选择**启用**，启用该接口上的 IP 源防护。

步骤 4 单击**应用**，将设置复制到当前配置文件。

绑定数据库

IP 源防护使用 DHCP Snooping 绑定数据库检查来自不信任端口的数据包。如果设备尝试向 DHCP Snooping 绑定数据库写入过多的条目，则超出的条目将始终处于不活动状态。超过其租用时间的条目将被删除，这样，处于不活动状态的条目可变成活动状态。

请参阅 **DHCPv4 Snooping/中继**。

注 “绑定数据库”页面将**只**显示已启用 IP 源防护端口上定义的 DHCP Snooping 绑定数据库中的条目。

若要查看 DHCP Snooping 绑定数据库和 TCAM 利用率，可以设定**插入非活动**：

步骤 1 单击**安全 > IP 源防护 > 绑定数据库**。

步骤 2 DHCP Snooping 绑定数据库使用 TCAM 资源管理数据库。填写**插入非活动**字段，选择设备尝试激活非活动条目的频率。可提供以下选项：

- **重试频率** - 检查 TCAM 资源的频率。
- **从不** - 从不试图重新激活处于不活动状态的地址。

步骤 3 单击**应用**，以保存对当前配置文件进行的上述更改并/或**立即重试**，以检查 TCAM 资源。

此时将显示绑定数据库中的条目：

- **VLAN ID** - 预期数据包所在的 VLAN。
- **MAC 地址** - 要匹配的 MAC 地址。
- **IP 地址** - 要匹配的 IP 地址。
- **接口** - 预计将传输数据包的接口。
- **状态** - 显示接口是否处于活动状态。
- **类型** - 显示条目是动态还是静态。

- **原因** - 如果接口未处于活动状态，显示其原因。可能的原因有：
 - **没问题** - 接口处于活动状态。
 - **无 Snooping VLAN** - VLAN 上未启用 DHCP Snooping。
 - **信任端口** - 端口已成为信任端口。
 - **资源问题** - TCAM 资源已用尽。

若要查看这些条目的子网，请输入相关搜索标准，并单击**转至**。

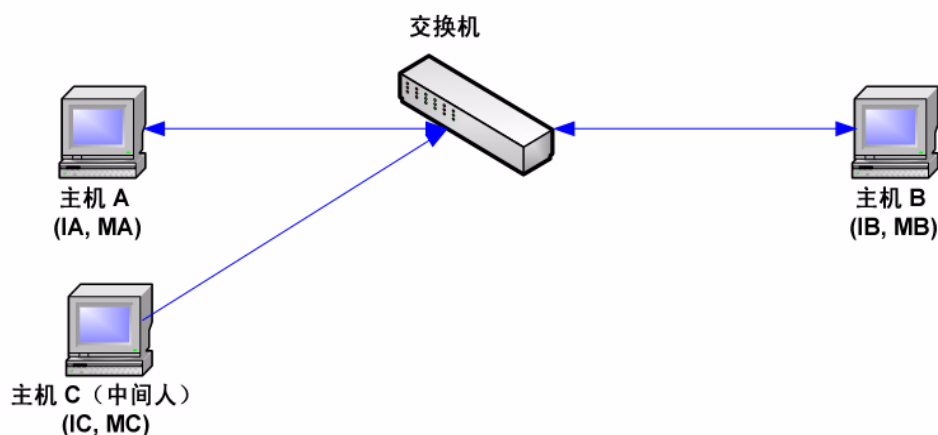
ARP 检测

ARP 通过将 IP 地址映射到 MAC 地址，能够在第 2 层广播域中进行 IP 通信。

恶意用户可以通过向连接至子网的系统 ARP 缓存投毒及拦截流向子网上其他主机的流量，攻击连接至第 2 层网络的主机、交换机和路由器。之所以能发生这种攻击是因为即使未收到 ARP 请求，ARP 也允许来自主机的无理由回复。攻击发生后，来自受攻击设备的所有流量将流经攻击者的计算机，然后流向路由器、交换机或主机。

下面显示了一个 ARP 缓存中毒示例。

ARP 缓存中毒



345140

主机 A、B 和 C 连接至交换机接口 A、B 和 C，它们全部位于同一个子网上。其 IP、MAC 地址在括号中显示；例如，主机 A 使用 IP 地址 IA 和 MAC 地址 MA。当主机 A 需要在 IP 层与主机 B 进行通信时，将广播一条有关与 IP 地址 IB 相关联的 MAC 地址的 ARP 请求。主机 B 使用一个 ARP 回复进行回应。交换机和主机 A 使用主机 B 的 MAC 和 IP 更新其 ARP 缓存。

主机 C 可通过广播伪造的 ARP 响应，将主机与 IA（或 IB）IP 地址和 MC MAC 地址绑定，向交换机、主机 A 和主机 B 的 ARP 缓存投毒。使用已中毒 ARP 缓存的主机将 MAC 地址 MC 用作流向 IA 或 IB 流量的目的 MAC 地址，从而使主机 C 能够拦截该流量。因为主机 C 知道与 IA 和 IB 相关联的真正的 MAC 地址，通过将正确的 MAC 地址用作目的地址，可将拦截的流量转发至这些主机。主机 C 将自身插入从主机 A 到主机 B 的流量流中，这就是经典的中间人攻击。

ARP 如何预防缓存中毒

ARP 检查功能对于信任和不信任接口都适用（请参阅“安全 > ARP 检测 > 接口设置”页面）。

接口根据用户分类，如下所示：

- **信任** - 不检测数据包。
- **不信任** - 对数据包进行如上所述的检测。

ARP 检测仅在不信任接口上执行。在信任接口上收到的 ARP 数据包可完全转发。

当数据包到达不信任接口时，将实施以下逻辑：

- 搜索有关该数据包 IP/MAC 地址的 ARP 访问控制规则。如果找到 IP 地址，且列表中的 MAC 地址与数据包的 MAC 地址相匹配，则该数据包有效；否则，该数据包无效。
- 如果未找到数据包的 IP 地址，且该数据包的 VLAN 已启用 DHCP Snooping，则针对该数据包的 <VLAN - IP 地址> 对搜索 DHCP Snooping 绑定数据库。如果找到 <VLAN - IP 地址> 对，且数据库中的 MAC 地址和接口与该数据包的 MAC 地址和入站接口相匹配，则数据包有效。
- 如果在 ARP 访问控制规则或 DHCP Snooping 绑定数据库中未找到该数据包的 IP 地址，则该数据包无效，会被丢弃。系统将生成一条系统日志消息。
- 如果数据包有效，则将其转发，并更新 ARP 缓存。

如果已选中 ARP 数据包验证选项（“属性”页面），将执行下面的附加验证检查：

- **源 MAC** - 将以太网报头中该数据包的源 MAC 地址与 ARP 请求中发送方的 MAC 地址相比较。此检查针对 ARP 请求和响应执行。

- **目的 MAC** - 将以太网报头中该数据包的目的 MAC 地址与目的接口 MAC 地址相比较。此检查针对 ARP 响应执行。
- **IP 地址** - 比较 ARP 正文，以找出无效和意外 IP 地址。地址包括 0.0.0.0、255.255.255.255 和所有 IP 组播地址。

将记录使用无效 ARP 检测绑定的数据包，并将其丢弃。

ARP 访问控制表中最多可以定义 1024 个条目。

ARP 检测与 DHCP Snooping 间的交互

如果已启用 DHCP Snooping，则 ARP 检测除了使用 ARP 访问控制规则之外，还使用 DHCP Snooping 绑定数据库。如果未启用 DHCP Snooping，则只使用 ARP 访问控制规则。

ARP 默认设置

下表介绍 ARP 默认设置：

选项	默认状态
动态 ARP 检测	未启用
ARP 数据包验证	未启用
在 VLAN 上启用 ARP 检测	未启用
日志缓冲间隔	已启用针对已丢弃的数据包生成系统日志消息，时间间隔为 5 秒

ARP 检测工作流程

配置 ARP 检测的步骤：

- 步骤 1** 在“安全 > ARP 检测 > 属性”页面中启用 ARP 检测，并配置各种选项。
- 步骤 2** 在“安全 > ARP 检测 > 接口设置”页面中将接口配置为 ARP 信任或不信任。
- 步骤 3** 在“安全 > ARP 检测 > ARP 访问控制”及“ARP 访问控制规则”页面中添加规则。
- 步骤 4** 在“安全 > ARP 检测 > VLAN 设置”页面中定义已启用 ARP 检测的 VLAN 以及每个 VLAN 的访问控制规则。

定义 ARP 检测属性

配置 ARP 检测的步骤：

步骤 1 单击**安全 > ARP 检测 > 属性**。

输入以下字段：

- **ARP 检测状态** - 选择后，将启用 ARP 检测。
- **ARP 数据包验证** - 选择后，将启用以下验证检查：
 - **源 MAC** - 将以太网报头中该数据包的源 MAC 地址与 ARP 请求中发送方的 MAC 地址相比较。此检查针对 ARP 请求和响应执行。
 - **目的 MAC** - 将以太网报头中该数据包的目的 MAC 地址与目的接口 MAC 地址相比较。此检查针对 ARP 响应执行。
 - **IP 地址** - 比较 ARP 正文，以找出无效和意外 IP 地址。地址包括 0.0.0.0、255.255.255.255 和所有 IP 组播地址。
- **日志缓冲间隔** - 选择以下其中一个选项：
 - **重试频率** - 启用针对已丢弃数据包发送系统日志消息。输入发送该消息的频率。
 - **从不** - 禁用针对已丢弃数据包发送系统日志消息。

步骤 2 单击**应用**。将定义设置，并更新当前配置文件。

定义动态 ARP 检测接口设置

针对 ARP 访问规则表和 DHCP Snooping 绑定数据库（如果已启用 DHCP Snooping）检查来自不信任端口/LAG 的数据包（请参阅“DHCP Snooping 绑定数据库”页面）。

默认情况下，端口/LAG 是 ARP 检测不信任的。

更改端口/LAG ARP 信任状态的步骤：

步骤 1 单击**安全 > ARP 检测 > 接口设置**。

此时将显示端口/LAG 及其 ARP 信任/不信任状态。

步骤 2 若要将端口/LAG 设置为不信任，选择该端口/LAG，并单击**编辑**。

步骤 3 选择**信任或不信任**，并单击**应用**，将该设置保存到当前配置文件中。

定义 ARP 检测访问控制

将条目添加至 ARP 检测表的步骤：

步骤 1 单击**安全 > ARP 检测 > ARP 访问控制**。

步骤 2 要添加条目，请单击**添加**。

步骤 3 输入以下字段：

- **ARP 访问控制名称** - 输入用户创建的名称。
- **MAC 地址** - 数据包的 MAC 地址。
- **IP 地址** - 数据包的 IP 地址。

步骤 4 单击**应用**。将定义设置，并更新当前配置文件。

定义 ARP 检测访问控制规则

将多条规则添加到以前创建的 ARP 访问控制组的步骤：

步骤 1 单击**安全 > ARP 检测 > ARP 访问控制规则**。

此时将显示当前定义的访问规则。

步骤 2 若要将多条规则添加至组，请单击**添加**。

步骤 3 选择一个访问控制组，并输入以下字段：

- **MAC 地址** - 数据包的 MAC 地址。
- **IP 地址** - 数据包的 IP 地址。

步骤 4 单击**应用**。将定义设置，并更新当前配置文件。

定义 ARP 检测 VLAN 设置

在 VLAN 和使用 VLAN 的相关访问控制组上启用 ARP 检测的步骤：

- 步骤 1** 单击**安全 > ARP 检测 > VLAN 设置**。
- 步骤 2** 若要在 VLAN 上启用 ARP 检测，将该 VLAN 从**可用 VLAN** 列表移至**已启用 VLAN** 列表。
- 步骤 3** 若要将一个 ARP 访问控制组与 VLAN 相关联，请单击**添加**。选择该 VLAN 编号，并选择以前定义的**ARP 访问控制组**。
- 步骤 4** 单击**应用**。将定义设置，并更新当前配置文件。

第一步跳安全性

安全：IPv6 第一步跳安全性

安全：802.1x 验证

本部分介绍 802.1X 验证。

其中包含以下主题：

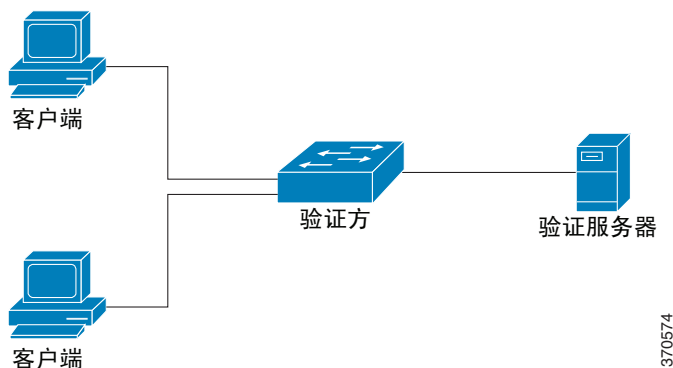
- [802.1X 概述](#)
- [验证方概述](#)
- [常见任务](#)
- [通过 GUI 进行 802.1X 配置](#)
- [定义时间范围](#)
- [验证方法和端口模式支持](#)

802.1X 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到局域网。802.1x 验证是一种客户端-服务器模型。在此模型中，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

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。客户端连接到验证方。

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。

客户端使用基于 MAC 或基于 Web 的验证时无需特殊软件。

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。

以下端口验证模式可受支持（这些模式在“安全 > 802.1X/MAC/Web 验证 > 主机和会话验证”中设置）：

- **单个主机** - 以每个端口单个客户端的方式支持基于端口的验证。
- **多个主机** - 以每个端口多个客户端的方式支持基于端口的验证。
- **多会话** - 以每个端口多个客户端的方式支持基于客户端的验证。

有关详情，请参阅[端口主机模式](#)。

以下验证方法可受支持：

- **基于 802.1x** - 在所有验证模式下都可受支持。
- **基于 Mac** - 在所有验证模式下都可受支持。

- **基于 Web** - 仅在多会话模式下可受支持。

在基于 802.1x 的验证中，验证方从 802.1x 消息（EAPOL 帧）中提取 EAP 消息，并将其传递到验证服务器，在此过程中会使用 RADIUS 协议。

在基于 MAC 或基于 Web 的验证中，验证方本身执行软件的 EAP 客户端部分。

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。

验证方概述

端口管理验证状态

端口管理状态可确定客户端是否已被授予访问网络的权限。

端口管理状态可在“安全 > 802.1X/MAC/Web 验证 > 端口验证”页面配置。

可用值如下：

- **强制授权**

端口验证禁用，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-start 消息时，会发送带有 EAP success 消息的 802.1x EAP 数据包。

此为默认状态。

- **强制未授权**

端口验证禁用，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[定义主机和会话验证](#)。交换机在收到 802.1x EAPOL-Start 消息时，会发送带有 EAP failure 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 802.1 x 验证。

端口主机模式

端口可置于以下端口主机模式（在“安全 > 802.1X/MAC/Web 验证 > 主机和会话验证”页面配置）：

- 单个主机模式

如果有一个经过授权的客户端，则对一个端口进行授权。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 Untagged 流量将重新映射到访客 VLAN。除非 Tagged 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，则只有属于未经验证的 VLAN 的 Tagged 流量才会被桥接。

如果端口经过授权，来自授权主机的 Untagged 流量和 Tagged 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 Untagged 流量重新映射到 RADIUS 服务器在验证过程中分配的 VLAN。除非 Tagged 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“安全 > 802.1X/MAC/Web 验证 > 端口验证”页面设置。

- 多个主机模式

如果至少有一个授权客户端，则对端口进行授权。

如果端口未经授权且访客 VLAN 为启用状态，则 Untagged 流量将重新映射到访客 VLAN。除非 Tagged 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，则只有属于未经验证的 VLAN 的 Tagged 流量才会被桥接。

如果端口经过授权，来自所有与端口连接的主机的 Untagged 流量和 Tagged 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 Untagged 流量重新映射到 RADIUS 服务器在验证过程中分配的 VLAN。除非 Tagged 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”页面配置。

- 多会话模式

与单个主机和多个主机模式不同，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。此模式需要 TCAM 查询。由于第 3 层模式交换机（请参阅[多会话模式支持](#)）没有为多会话模式分配的 TCAM 查询，因此，它们支持有限形式的多会话模式，该模式不支持访客 VLAN 和 RADIUS VLAN 属性。端口上允许的最大授权主机数量在“端口配置”页面配置。

无论主机是否经过授权，属于未经验证 VLAN 的 Tagged 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 Tagged 流量和 Untagged 流量将重新映射到访客 VLAN；如果端口上未启用访客 VLAN，则此类流量会被丢弃。

如果 RADIUS 服务器为授权主机分配了一个 VLAN，则其所有不属于未经验证 VLAN 的 Tagged 和 Untagged 流量都将通过 VLAN 进行桥接；如果未分配 VLAN，其所有流量都将根据静态 VLAN 成员关系端口配置进行桥接。

以下设备支持无访客 VLAN 和 RADIUS-VLAN 分配的多会话模式：

- 第 3 层路由器模式下的 Sx500/ESW2-550X
- 基本和高级混合堆叠模式下的 SG500X
- SG500XG

多种验证方法

如果交换机启用了不止一种验证方法，则适用如下验证方法层级：

- 802.1x 验证：最高
- 基于 WEB 的验证
- 基于 MAC 的验证：最低

多种方法可同时运行。当一种方法成功完成时，客户端会变为已授权状态，优先级更低的方法将停止，而优先级更高的方法则会继续运行。

当同时运行的多种验证方法有一种失败时，其他方法会继续运行。

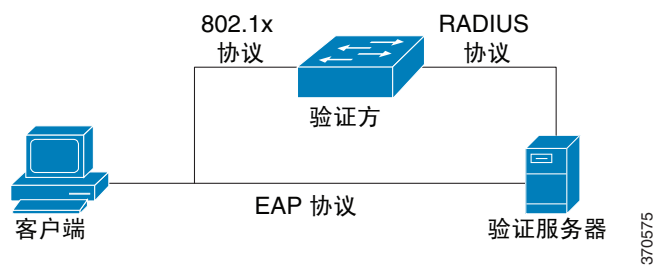
当验证方法针对一个已由较低优先级验证方法验证的客户端成功完成时，将适用新验证方法的属性。如果新方法失败，则客户端将保留经旧方法授权的状态。

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

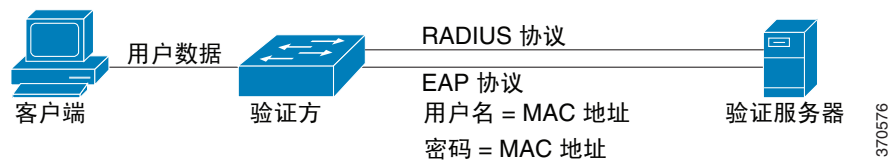


基于 MAC 的验证

基于 MAC 的验证是 802.1X 验证的替代方法，可使不具有 802.1X 请求方功能的设备（如打印机和 IP 电话）访问网络。基于 MAC 的验证使用连接设备的 MAC 地址来授予或拒绝网络访问权限。

在这种情况下，交换机支持 EAP MD5 功能，用户名和密码都为客户端 MAC 地址，如下所示。

图 2 基于 MAC 的验证



此方法没有任何特定配置。

基于 WEB 的验证

基于 WEB 的验证用于对请求通过交换机访问网络的最终用户进行验证。它能够让直接与交换机连接的客户端在获得网络访问权限之前通过强制网络门户机制进行验证。基于 Web 的验证是基于客户端的验证，在第 2 层和第 3 层的多会话模式下均受支持。

此验证方法按端口启用，当端口启用时，每个主机必须对自身进行验证，然后才能访问网络。因此，在已启用的端口上，您可以拥有经验证和未经验证的主机。

如果端口上启用了基于 web 的验证，交换机将丢弃所有从未经授权客户端进入端口的流量，但 ARP、DHCP、DNS 和 NETBIOS 数据包除外。这些数据包可以由交换机转发，这样一来，即使是未经授权的客户端，也可以获取 IP 地址并解析主机名或域名。

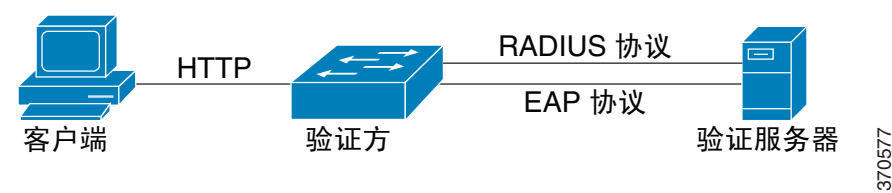
所有来自未经授权客户端且通过 IPv4 的 HTTP/HTTPS 数据包都将捕获到交换机的 CPU。当最终用户请求访问网络时，如果端口上启用了基于 Web 的验证，则在请求的页面显示之前，将首先显示一个登录页面。用户必须输入其用户名/密码，这将由 RADIUS 服务器使用 EAP 协议进行验证。如果验证成功，用户会获得通知。

现在，用户拥有经验证的会话。在使用过程中，会话会保持打开状态。如果在特定时间间隔内未使用会话，会话会关闭。此时间间隔由系统管理员配置，称为静默时间。如果会话超时，用户名/密码会被丢弃，并且访客必须重新输入用户名/密码以打开新会话。

请参阅表 1. 端口模式和身份验证方法。

验证完成后，交换机将转发端口上所有来自客户端的流量，如下图所示。

图 3 基于 WEB 的验证



基于 Web 的验证无法在启用了访客 VLAN 或 RADIUS 分配的 VLAN 功能的端口上配置。

基于 Web 的验证支持以下页面：

- 登录页面
- 登录成功页面

这些页面有预定义的嵌入集。

这些页面可以在“安全 > 802.1X/MAC/Web 验证 > Web 验证自定义”页面修改。

您可以预览各个自定义页面。配置将保存至当前配置文件。

下表介绍哪些 SKU 支持基于 web 的验证以及相应的系统模式：

SKU	系统模式	是否支持 WBA
Sx300	第 2 层	是
	第 3 层	否
Sx500、Sx500ESW2-550X	第 2 层	是
	第 3 层	否

SKU	系统模式	是否支持 WBA
SG500X	原生	是
	基本混合 - 第 2 层	是
	基本混合 - 第 3 层	否
SG500XG	与 Sx500 相同	是

注

- 如果基于 web 的验证不受支持，则访客 VLAN 和 DVA 无法在多会话模式下配置。
- 如果基于 web 的验证受到支持，则访客 VLAN 和 DVA 可以在多会话模式下配置

未经验证的 VLAN 和访客 VLAN

未经验证的 VLAN 和访客 VLAN 可提供对一类服务的访问权限，该类服务不需要对订用设备或端口进行基于 802.1X 或 MAC 的验证和授权。

访客 VLAN 是分配给未经授权客户端的 VLAN。您可以在“安全 > 802.1X/MAC/Web 验证 > 属性”页面配置访客 VLAN 以及一个或多个未经验证的 VLAN。

未经验证的 VLAN 是一种允许已授权的和未授权的设备或端口进行访问的 VLAN。

未经验证的 VLAN 具有以下特性：

- 它必须为静态 VLAN，并且不能是访客 VLAN 或默认的 VLAN。
- 必须将成员端口手动配置为 Tagged 成员。
- 成员端口必须为中继和/或一般的端口。访问端口不能是未经验证的 VLAN 的成员。

经过配置的访客 VLAN 是具有以下特性的静态 VLAN：

- 它必须根据现有的静态 VLAN 手动进行了定义。
- 访客 VLAN 不能用作语音 VLAN 或未经验证的 VLAN。

请参阅表 3. 访客 VLAN 支持和 RADIUS-VLAN 分配支持，查看支持访客 VLAN 的模式总结。

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：

- **单个主机和多个主机模式**

属于访客 VLAN 且到达未经授权端口的 Untagged 流量和 Tagged 流量将通过访客 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。

- **第 2 层中的多会话模式**

不属于未经验证的 VLAN 且来自未经授权客户端的 Untagged 流量和 Tagged 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 Tagged 流量将通过 VLAN 进行桥接。

此模式无法在与基于策略的 VLAN 相同的界面上配置。

- **第 3 层中的多会话模式**

此模式不支持访客 VLAN。

RADIUS VLAN 分配或动态 VLAN 分配

RADIUS 服务器可以向授权客户端分配 VLAN，前提是此选项已在“端口验证”页面启用。这称为动态 VLAN 分配 (DVA)，也称为 RADIUS 分配的 VLAN。本指南使用“RADIUS 分配的 VLAN”这一术语。

当端口处于多会话模式下且已启用 RADIUS 分配的 VLAN 时，设备会自动添加端口作为 RADIUS 服务器在验证过程中所分配的 VLAN 的 Untagged 成员。如果 Untagged 数据包源自经过验证和授权的设备或端口，则设备会将这些数据包划分为分配的 VLAN。

有关设备上启用 RADIUS 分配的 VLAN 时不同模式如何运作的更多信息，请参阅表 3. 访客 VLAN 支持和 RADIUS-VLAN 分配支持以及下表介绍在不同情况下处理验证流量和未经验证流量的方式。

注 RADIUS VLAN 分配仅在 Sx500 设备处于第 2 层系统模式时受到支持。SG500X 和 SG500XG 设备在基本和高级混合堆叠模式下的作用类似 Sx500 设备。

对于要在已启用 DVA 的端口处进行验证和授权的设备：

- RADIUS 服务器必须验证该设备，并为其动态分配一个 VLAN。您可以在“端口验证”页面将“RADIUS VLAN 分配”字段设置为静态。这可以让主机根据静态配置进行桥接。

- RADIUS 服务器必须支持 RADIUS 属性为 tunnel-type (64) = VLAN (13)、tunnel-media-type (65) = 802 (6) 以及 tunnel-private-group-id = VLAN ID 的 DVA。

启用 RADIUS 分配的 VLAN 功能时，主机模式的运作方式如下：

- 单个主机和多个主机模式
属于 RADIUS 分配的 VLAN 的 Untagged 流量和 Tagged 流量将通过此 VLAN 进行桥接。其他所有不属于未经验证 VLAN 的流量都会被丢弃。
- 完整的多会话模式
不属于未经验证的 VLAN 且来自客户端的 Untagged 流量和 Tagged 流量将使用 TCAM 规则分配给 RADIUS 分配的 VLAN，并通过该 VLAN 进行桥接。
- 第 3 层系统模式下的多会话模式
此模式不支持 RADIUS 分配的 VLAN，除原生堆叠模式下的 SG500X 和 SG500XG 设备以外

下表介绍访客 VLAN 和 RADIUS-VLAN 分配支持，具体取决于验证方法和端口模式。

验证方法	单个主机	多个主机	多会话	
			L3 中的设备	L2 中的设备
802.1x	†	†	N/S	†
MAC	†	†	N/S	†
WEB	N/S	N/S	N/S	N/S

图例：

† - 端口模式支持访客 VLAN 和 RADIUS-VLAN 分配

N/S - 端口模式不支持验证方法。

违例模式

在单个主机模式下，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。此配置可以在“主机和会话验证”页面完成。

可能的选项有：

- **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 Trap。Trap 之间的最短时间间隔为 1 秒。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 Trap，且连续 Trap 之间具有可配置的最短时间间隔。如果间隔秒数 = 0，将禁用 Trap。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（单个主机或多个主机模式）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。在单个主机或多个主机模式下，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。

静默期仅适用于基于 802.1x 和基于 Web 的验证。

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/MAC/Web 验证 > 属性。
- 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/MAC/Web 验证 > 主机和会话验证。
- 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/MAC/Web 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 Trap

- 步骤 1** 单击**安全 > 802.1X/MAC/Web 验证 > 属性**。
- 步骤 2** 选择所需 Trap。
- 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 的验证或基于 Web 的验证

- 步骤 1** 单击**安全 > 802.1X/MAC/Web 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**定义 802.1X 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/MAC/Web 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：

- 步骤 1 单击 **安全 > 802.1X/MAC/Web 验证 > 属性**。
- 步骤 2 在“访客 VLAN”字段中选择启用。
- 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。

工作流程 6：配置未经验证的 VLAN

- 步骤 1 单击 **安全 > 802.1X/MAC/Web 验证 > 属性**。
- 步骤 2 选择一个 VLAN，然后单击 **编辑**，
- 步骤 3 选择一个 VLAN。
- 步骤 4 或者，取消选中 **验证** 以将 VLAN 变为未经验证的 VLAN。
- 步骤 5 单击 **应用**，将更新当前配置文件。

通过 GUI 进行 802.1X 配置

定义 802.1X 属性

802.1X “属性”页面用于在全局启用 802.1X，并定义端口如何进行验证。要发挥 802.1X 的作用，必须在每个端口上全局且单独地激活 802.1X。

定义基于端口的验证的步骤：

- 步骤 1 单击 **安全 > 802.1X/MAC/Web 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，802.1X、基于 MAC 和基于 web 的验证将禁用。

- **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），则不会执行验证，且允许进行会话。如果服务器可用，但是用户凭证不正确，则将拒绝访问，并终止会话。
 - *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 用于未经授权的端口。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，则将从访客 VLAN 中删除该端口。
- **访客 VLAN ID** - 从 VLAN 列表选择访客 VLAN。
- **访客 VLAN 超时** — 定义时间段：
 - 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。
- **Trap** - 要启用 Trap，请选择以下一个或多个选项：
 - *802.1x 验证失败陷阱* - 选择该选项可在 802.1x 验证失败时生成 Trap。
 - *802.1x 验证成功陷阱* - 选择该选项可在 802.1x 验证成功时生成 Trap。
 - *MAC 验证失败陷阱* - 选择该选项可在 MAC 验证失败时生成 Trap。
 - *MAC 验证成功陷阱* - 选择该选项可在 MAC 验证成功时生成 Trap。
- 当交换机处于第 2 层交换机模式下：
 - *Web 验证失败陷阱* - 选择该选项可在 Web 验证失败时生成 Trap。
 - *Web 验证成功陷阱* - 选择该选项可在 Web 验证成功时生成 Trap。
 - *Web 验证静默陷阱* - 选择该选项可在静默期开始时生成 Trap。

当设备处于第 3 层路由器模式时，“VLAN 验证表”将显示所有 VLAN，并指示 VLAN 上是否已启用验证。

步骤 3 单击应用。 802.1X 属性将写入当前配置文件中。

定义 802.1X 端口验证

“端口验证”页面可配置每个端口的 802.1X 参数。因为仅当端口处于强制授权状态时，某些配置更改才有可能实现，例如主机验证，因此我们建议您在进行更改之前，将端口控制更改为“强制授权”。完成配置之后，将端口控制恢复为以前状态。

注 其上定义了 802.1x 的端口不能成为 LAG 的成员。

定义 802.1X 验证的步骤：

步骤 1 单击 **安全 > 802.1X/MAC/Web 验证 > 端口验证**。

此页面显示所有端口的验证设置。

步骤 2 选择一个端口，然后单击 **编辑**。

步骤 3 输入参数。

- **接口** - 选择端口。
- **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*。
- **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。
- **RADIUS VLAN 分配** - 选择该选项可在选择的端口上启用动态 VLAN 分配。
 - *禁用* - 功能未启用。
 - *拒绝* - 如果 RADIUS 服务器对请求方进行了授权，但未提供请求方 VLAN，请求方将遭到拒绝。
 - *静态* - 如果 RADIUS 服务器对请求方进行了授权，但未提供请求方 VLAN，请求方将获得接受。

- **访客 VLAN** - 选择该选项可指示已为设备启用以前定义的访客 VLAN。选项如下：
 - *已选定* - 为未授权的端口启用访客 VLAN。如果已启用访客 VLAN，则未经授权的端口会自动加入在 802.1X “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 Untagged VLAN 自动分配给未经授权的端口。
 - *已清除* - 在端口上禁用访客 VLAN。
- **基于 802.1x 的验证** - 802.1X 验证是在端口上执行的唯一一种验证方法。
- **基于 MAC 的验证** - 根据请求方的 MAC 地址验证端口。仅可在端口上使用 8 种基于 MAC 的验证。

注 要成功进行 MAC 验证，RADIUS 服务器请求方的用户名和密码必须为请求方的 MAC 地址。MAC 地址必须为小写字母，并且在输入时不包含 . 或 - 分隔符；例如：0020aa00bbcc。
- **基于 Web 的验证** - 仅适用于第 2 层交换机模式。选择该选项可在交换机上启用基于 web 的验证。
- **定期重新验证** - 选择该选项可在指定的重新验证时段之后尝试重新验证端口。
- **重新验证间隔** - 输入经过多少秒后对选定端口进行重新验证。
- **立即重新验证** - 选择该选项可立即对端口进行重新验证。
- **验证方状态** - 显示定义的端口授权状态。选项如下：
 - *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** - 在已启用 802.1x（选中 “基于端口” 验证）时对授权可供使用的特定端口进行时间限制。
- **时间范围名称** - 选择指定时间范围的模板。
- **WBA 登录尝试最大次数** - 仅适用于第 2 层交换机模式。输入接口上允许的最大登录尝试次数。选择 **无限期** 不进行限制，或选择 **用户定义** 设置限制。

- **WBA 最长静默时段** - 仅适用于第 2 层交换机模式。输入接口上允许的静默期最长时段。选择**无限期**不进行限制，或选择**用户定义**设置限制。
- **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。
注 将此值设置为 1，可在多会话模式下模拟基于 web 验证的单个主机模式。
- **静默期** - 输入在验证交换失败之后设备保持静默状态的秒数。
- **重新发送 EAP** - 输入在重新发送请求之前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** - 输入可发送的 EAP 请求的最大数。如果在定义时段（请求方超时）之后未接收到响应，则重新启动验证程序。
- **请求方超时** - 输入将 EAP 请求重新发送到请求方之前经过的秒数。
- **服务器超时** - 输入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。

定义主机和会话验证

使用“主机和会话验证”页面可定义 802.1X 在端口上的运作模式以及当检测到违例行为时要执行的操作。

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/MAC/Web 验证 > 主机和会话验证**。

会说明所有端口的 802.1X 验证参数。在“编辑主机和会话验证”页面中介绍了除以下字段以外的所有字段。

- **单个主机违反规则次数** - 显示在单个主机模式下从其 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。

以下字段仅当您在“主机验证”字段中选择了“单个”时才适用。

单个主机违反规则设置：

- **违反规则响应措施** - 选择对在单会话/单台主机模式下从其 MAC 地址不是请求方 MAC 地址的主机到达的数据包所应用的操作。选项如下：
 - *保护 (丢弃)* - 丢弃数据包。
 - *限制 (转发)* - 转发数据包。
 - *关闭* - 丢弃数据包并关闭端口。在重新激活端口或重启设备之前，端口将保持关闭状态。
- **Trap (单个主机违反规则)** - 选择该选项可启用 Trap。
- **Trap 频率 (单个主机违反规则)** - 定义向主机发送 Trap 的频率。仅当禁用多台主机时才可定义此字段。
- **违反规则次数** - 显示违例的数量（在单会话/单个主机模式下来自 MAC 地址不是请求方 MAC 地址的主机的数据包数量）。

步骤 4 单击**应用**。设置将写入当前配置文件中。

查看经验证的主机

查看有关经验证的用户详情的步骤：

步骤 1 单击**安全 > 802.1X/MAC/Web 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)** - 请求方在端口上保持登录状态的时间量。
- **验证方法** - 验证上一个会话所使用的方法。
- **验证服务器** - RADIUS 服务器。
- **MAC 地址** - 显示请求方的 MAC 地址。
- **VLAN ID** - 端口的 VLAN。

锁定的客户端

查看因失败登录尝试而锁定的客户端以及对锁定的客户端进行解锁：

步骤 1 单击 **安全 > 802.1X/MAC/Web 验证 > 锁定的客户端**。

此时将显示以下字段：

- **接口** - 端口已锁定。
- **MAC 地址** - 显示当前端口授权状态。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*。
- **剩余时间 (秒)** - 端口仍要保持锁定的时间。

步骤 2 选择一个端口。

步骤 3 单击 **解锁**。

Web 验证自定义

此页面支持以多种语言设计基于 web 的验证页面。

最多可添加 4 种语言。

注 多达 5 个 HTTP 用户和 1 个 HTTPS 用户可以同时请求基于 web 的验证。当这些用户进行验证时，可以有更多用户请求验证。

为基于 web 的验证添加语言：

步骤 1 单击 **安全 > 802.1X/MAC/Web 验证 > Web 验证自定义**。

步骤 2 单击 **添加**。

步骤 3 从 **语言** 下拉列表中选择一种语言。

步骤 4 如果此语言为默认语言，则选择 **设置为默认显示语言**。如果最终用户未选择语言，将显示默认语言页面。

步骤 5 单击 **应用**，设置将保存到当前配置文件。

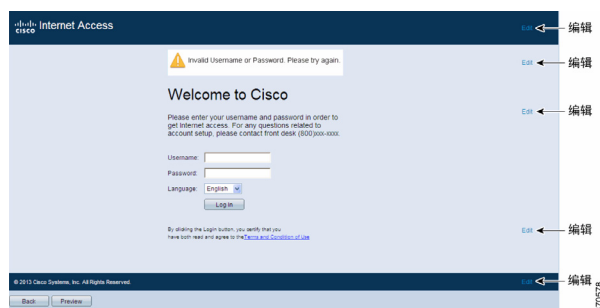
自定义 web 验证页面：

步骤 1 单击**安全 > 802.1X/MAC/Web 验证 > Web 验证自定义**。

此页面显示可以自定义的语言。

步骤 2 单击**编辑登录页面**。

图 4 将显示以下页面



步骤 3 单击**编辑 1**。此时将显示以下字段：

- **语言** - 显示页面的语言。
- **颜色方案** - 选择对比度选项之一：

选择**自定义**选项后，可用的选项有：

- **页面背景颜色** - 输入背景颜色的 ASCII 码。选定的颜色将显示在“文本”字段中。
- **页眉和页脚背景颜色** - 输入页眉和页脚背景颜色的 ASCII 码。选定的颜色将显示在“文本”字段中。
- **页眉和页脚文字颜色** - 输入页眉和页脚文字颜色的 ASCII 码。选定的颜色将显示在“文本”字段中。
- **超链接颜色** - 输入超链接颜色的 ASCII 码。选定的颜色将显示在“文本”字段中。
- **当前徽标图像** - 选择以下其中一个选项：
 - **无** - 无徽标。
 - **默认** - 使用默认徽标。
 - **其他** - 选择该选项以输入自定义徽标。

选择**其他**徽标选项后，可用的选项有：

- **徽标图像文件名称** - 输入徽标文件名称或**浏览**到图像。
- **应用文字** - 输入伴随徽标出现的文字。
- **窗口标题文字** - 输入“登录”页面的标题。

步骤 4 单击**应用**，设置将保存到当前配置文件。

步骤 5 单击**编辑 2**。此时将显示以下字段：

- **无效用户凭证** - 输入要在最终用户输入无效用户名和密码时显示的消息文本。
- **服务不可用** - 输入要在验证服务不可用时显示的消息文本。

步骤 6 单击**应用**，设置将保存到当前配置文件。

步骤 7 单击**编辑 3**。此时将显示以下字段：

- **欢迎消息** - 输入要在最终用户登录时显示的消息文本。
- **说明消息** - 输入要对最终用户显示的说明。
- **RADIUS 验证** - 显示是否已启用 RADIUS 验证。如果已启用，则必须在登录页面加入用户名和密码。
- **用户名文本框** - 为要显示的用户名文本框选择此选项。
- **用户名文本框标签** - 选择要在用户名文本框之前显示的标签。
- **密码文本框** - 为显示的密码文本框选择此选项。
- **密码文本框标签** - 选择要在密码文本框之前显示的标签。
- **语言选择** - 选择该选项可让最终用户选择一个语言。
- **语言下拉标签** - 输入语言选择下拉的标签。
- **登录按钮标签** - 输入登录按钮的标签。
- **登录进度标签** - 输入要在登录过程中显示的文本。

步骤 8 单击**应用**，设置将保存到当前配置文件。

步骤 9 单击**编辑 4**。此时将显示以下字段：

- **条款和条件** - 选择该选项可启用条款和条件文本框。
- **条款和条件警告** - 输入要作为进入条款和条件的说明显示的消息文本。
- **条款和条件内容** - 输入要作为条款和条件显示的消息文本。

步骤 10 单击**应用**，设置将保存到当前配置文件。

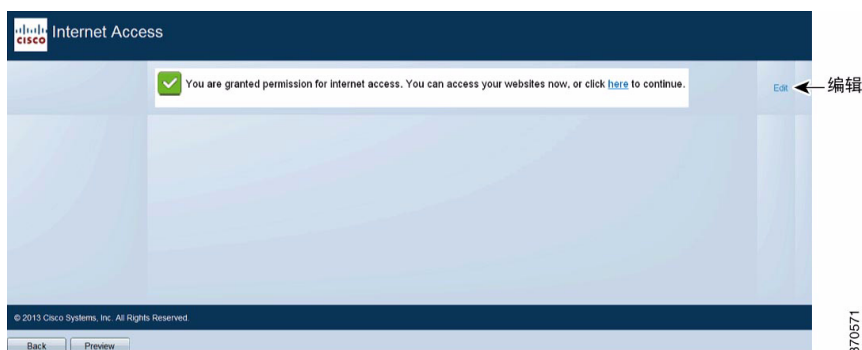
步骤 11 **编辑 5**。此时将显示以下字段：

- **版权** - 选择该选项可启用版权文本显示。
- **版权文本** - 输入版权文本。

步骤 12 单击**应用**，设置将保存到当前配置文件。

步骤 13 单击**编辑成功页面**。

图 5 将显示以下页面



步骤 14 单击页面右侧的**编辑**按钮。

步骤 15 输入**成功消息**，这是最终用户成功登录后将显示的文本。

步骤 16 单击**应用**，设置将保存到当前配置文件。

若要预览登录或成功消息，单击**预览**。

若要将一种语言设置为默认语言，单击**设置默认显示语言**。

定义时间范围

有关此功能的说明，请参阅**时间范围**。

验证方法和端口模式支持

下表显示了支持的授权方法和端口模式组合。

验证方法	单个主机	多个主机	多会话	
			L3 中的设备	L2 中的设备
802.1x	†	†	†	†
MAC	†	†	†	†
WEB	N/S	N/S	N/S	†

图例：

† - 端口模式还支持访客 VLAN 和 RADIUS-VLAN 分配。

N/S - 端口模式不支持此验证方法。

注 基于 Web 的验证需要针对输入流量分类的 TCAM 支持，仅在完整的多会话模式下受支持。您可以在“端口验证”页面将“最大主机数”参数设置为 1，以模拟单个主机模式。

模式行为

下表介绍在不同情况下处理验证流量和未经验证流量的方式。

	未经验证的流量				经验证的流量			
	带访客 VLAN		不带访客 VLAN		带 Radius VLAN		不带 Radius VLAN	
	Untagged	Tagged	Untagged	Tagged	Untagged	Tagged	Untagged	Tagged
单个主机	帧将重映射到访客 VLAN	除非帧属于访客 VLAN 或未经授权的 VLAN，否则会被丢弃	帧会被丢弃	除非帧属于未经授权的 VLAN，否则会被丢弃	帧将重映射到 RADIUS 分配的 VLAN	除非帧属于 RADIUS VLAN 或未经授权的 VLAN，否则帧会被丢弃	帧将根据静态 VLAN 配置进行桥接	帧将根据静态 VLAN 配置进行桥接

	未经验证的流量				经验证的流量			
	带访客 VLAN		不带访客 VLAN		带 Radius VLAN		不带 Radius VLAN	
	Untagged	Tagged	Untagged	Tagged	Untagged	Tagged	Untagged	Tagged
多个主机	帧将重映射到访客 VLAN	除非帧属于访客 VLAN 或未经授权的 VLAN，否则帧会被丢弃	帧会被丢弃	除非帧属于未经验证的 VLAN，否则会被丢弃	帧将重映射到 Radius 分配的 VLAN	除非帧属于 Radius VLAN 或未经授权的 VLAN，否则帧会被丢弃	帧将根据静态 VLAN 配置进行桥接	帧将根据静态 VLAN 配置进行桥接
精简的多会话	N/S	N/S	帧会被丢弃	除非帧属于未经验证的 VLAN，否则会被丢弃	N/S	N/S	帧将根据静态 VLAN 配置进行桥接	帧将根据静态 VLAN 配置进行桥接
完整的多会话	帧将重映射到访客 VLAN	除非帧属于未经授权的 VLAN，否则帧将重映射到访客 VLAN	帧会被丢弃	除非帧属于未经验证的 VLAN，否则会被丢弃	帧将重映射到 RADIUS 分配的 VLAN	除非帧属于未经授权的 VLAN，否则帧将重映射到 Radius VLAN	帧将根据静态 VLAN 配置进行桥接	帧将根据静态 VLAN 配置进行桥接

安全：IPv6 第一步跳安全性

本节介绍第一步跳安全性 (FHS) 的工作原理以及如何在 GUI 中对其进行配置。

其中包含以下主题：

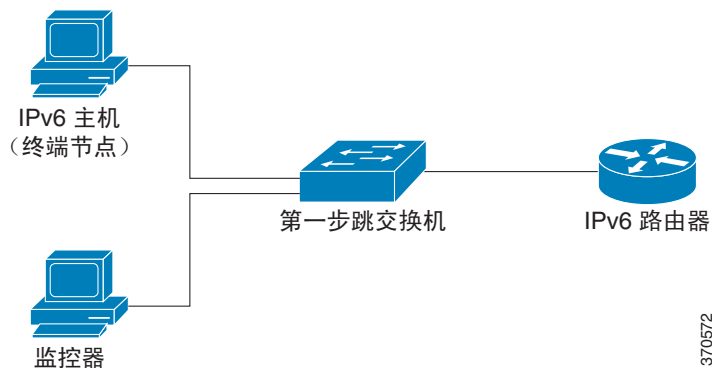
- [第一步跳安全性概述](#)
- [路由器通告防护](#)
- [邻居发现检测](#)
- [DHCPv6 防护](#)
- [邻近绑定完整性](#)
- [攻击保护](#)
- [策略、全局参数和系统默认值](#)
- [常见任务](#)
- [默认设置和配置](#)
- [使用说明](#)
- [通过 Web GUI 配置第一步跳安全性](#)

第一步跳安全性概述

IPv6 FHS 是一套用于在启用 IPv6 的网络中保护链路操作的功能。它基于邻居发现协议和 DHCPv6 消息。

在此功能中，第 2 层交换机（如 [图 6](#)）根据多个不同的规则过滤邻居发现协议消息、DHCPv6 消息和用户数据消息。

图 6 第一步跳安全性配置



IPv6 第一步跳安全性的单个独立实例在启用了该功能的各 VLAN 上运行。

缩写

名称	说明
CPA 消息	证书路径通告消息
CPS 消息	证书路径请求消息
DAD-NS 消息	重复地址检测邻居请求消息
FCFS-SAVI	先来先服务 - 源地址验证改进
NA 消息	邻居通告消息
NDP	邻居发现协议
NS 消息	邻居请求消息
RA 消息	路由器通告消息
RS 消息	路由器请求消息
SAVI	源地址验证改进

IPv6 第一步跳安全性组件

IPv6 第一步跳安全性提供以下功能：

- IPv6 第一步跳安全性通用功能
- RA 防护

- ND 检测
- 邻近绑定完整性
- DHCPv6 防护

这些组件可在 VLAN 上启用或禁用。

每个功能有两个预定义的空策略，名称为：vlan_default 和 port_default。第一个连接到未与用户定义策略连接的各 VLAN，第二个连接到未与用户定义策略连接的各接口和 VLAN。这些策略无法由用户显式连接。请参阅[策略、全局参数和系统默认值](#)。

IPv6 第一步跳安全性管道功能

如果 IPv6 第一步跳安全性已在 VLAN 上启用，则交换机会 Trap 以下消息：

- 路由器通告 (RA) 消息
- 路由器请求 (RS) 消息
- 邻居通告 (NA) 消息
- 邻居请求 (NS) 消息
- ICMPv6 重定向消息
- 证书路径通告 (CPA) 消息
- 证书路径请求 (CPS) 消息
- DHCPv6 消息

拦截的 RA、CPA 和 ICMPv6 重定向消息将传递到 RA 防护功能。RA 防护将验证这些信息并丢弃非法消息，而合法消息将传递到 ND 检测功能。

ND 检测将验证这些信息并丢弃非法消息，而合法消息将传递到 IPv6 源防护功能。

拦截的 DHCPv6 消息将传递到 DHCPv6 防护功能。DHCPv6 防护将验证这些信息并丢弃非法消息，而合法消息将传递到 IPv6 源防护功能。

拦截的数据消息将传递到 IPv6 源防护功能。IPv6 源防护将使用邻近绑定表验证接收的消息（拦截的数据消息、来自 ND 检测的 NDP 消息以及来自 DHCPv6 防护的 DHCPv6 消息），丢弃非法消息，并将合法消息传递到转发。

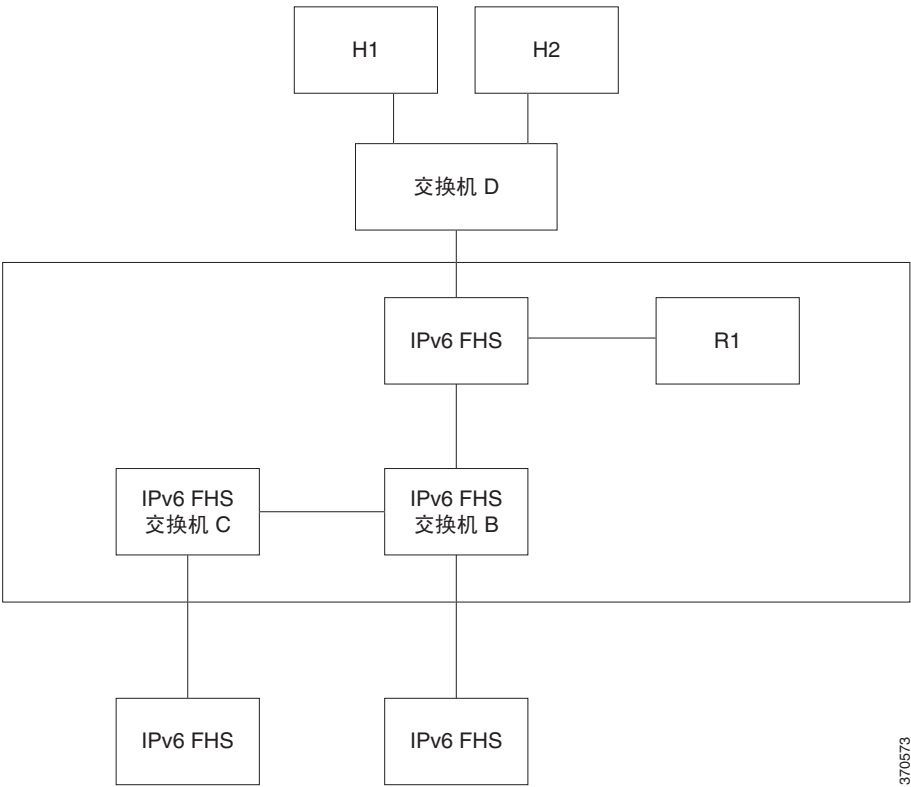
邻近绑定完整性从接收的消息（NDP 和 DHCPv6 消息）中学习邻居，并将其存储在邻近绑定表中。此外，可以手动添加静态条目。学习地址后，NBI 功能可传递框架以供转发。

拦截的 RS、CPS NS 和 NA 消息也会传递到 ND 检测功能。ND 检测将验证这些信息并丢弃非法消息，然后将合法消息传递到 IPv6 源防护功能。

IPv6 第一步跳安全性周界

IPv6 第一步跳安全性交换机可形成一个周界，将不受信任的区域与受信任的区域隔离开。周界内的所有交换机都支持 IPv6 第一步跳安全性，周界内的主机和路由器为受信任的设备。例如，图 7 上的链路 SwitchC-H3、SwitchB-H4 和 SwitchA-SwitchD 形成了周界，而链路 SwitchA-SwitchB、SwitchB-SwitchC 和 SwitchA-R1 是受保护区域内的内部链路。

图 7 IPv6 第一步跳安全性周界



邻近绑定策略配置屏幕中的 **device-role** 命令指定周界。

每个 IPv6 第一步跳安全性交换机为由边缘划分的邻居建立绑定。通过这种方式，绑定条目将在形成周界的 IPv6 第一步跳安全性设备上分发。然后，IPv6 第一步跳安全性设备可以向周界内部提供绑定完整性，无需为各设备上的所有地址设置绑定。

路由器通告防护

路由器通告 (RA) 防护为处理拦截的 RA 消息的第一个 FHS 功能。RA 防护支持以下功能：

- 过滤接收的 RA、CPA 和 ICMPv6 重定向消息。
- 验证接收的 RA 消息。

过滤接收的 RA、CPA 和 ICMPv6 重定向消息

RA 防护会丢弃未作为路由器角色的接口上的 RA 和 CPA 消息。接口角色在“安全”>“IPv6 第一步跳安全性”>“RA 防护设置”页面配置。

RA 消息验证

RA 防护将根据与接口连接的 RA 防护策略使用过滤验证 RA 消息。这些策略可在“RA 防护设置”页面配置。

如果消息未通过验证，则会被丢弃。如果 FHS 常见组件上的记录数据包丢弃配置已启用，则将发送限速系统日志消息。

邻居发现检测

邻居发现 (ND) 检测支持以下功能：

- 验证接收的邻居发现协议消息。
- 出口过滤

消息验证

ND 检测可根据与接口连接的 ND 检测策略验证邻居发现协议消息。此策略可在“ND 检测设置”页面定义。

如果消息未通过策略中定义的验证，则会被丢弃，且将发送限速系统日志消息。

出口过滤

ND 检测将阻止配置为主机接口的接口上的 RS 和 CPS 消息转发。

DHCPv6 防护

DHCPv6 防护会处理拦截的 DHCPv6 消息。DHCPv6 防护支持以下功能：

- 过滤接收的 DHCPv6 消息。

DHCP 防护将丢弃在作为客户端角色的接口上接收的 DHCPv6 回复消息。接口角色可在“DHCP 防护设置”页面配置。

- 验证接收的 DHCPv6 消息。

DHCPv6 防护将根据与接口连接的 DHCPv6 防护策略验证匹配过滤的 DHCPv6 消息。

如果消息未通过验证，则会被丢弃。如果 FHS 常见组件上的记录数据包丢弃配置已启用，则将发送限速系统日志消息。

邻近绑定完整性

邻近绑定 (NB) 完整性可建立邻近绑定。

NB 完整性的单个独立实例在启用了该功能的各 VLAN 上运行。

学习通告的 IPv6 前缀

NB 完整性学习 RA 消息中通告的 IPv6 前缀，并将其保存在邻居前缀表中。这些前缀用于验证已分配的全局 IPv6 地址。

默认情况下，此验证为禁用状态。如果启用，地址将根据“邻近绑定设置”页面中的前缀进行验证。

用于地址验证的静态前缀可在“邻近绑定表”页面中添加。

邻近绑定表溢出

如果没有用于新建条目的可用空间，新条目将覆盖创建时间最久的条目。

建立邻近绑定

IPv6 第一步跳安全性交换机可使用以下方法发现并记录绑定信息：

- **NBI-NDP 方法：**从侦听的邻居发现协议消息中学习 IPv6 地址
- **NBI 手动方法：**通过手动配置

IPv6 地址将绑定到主机网络附件的链路层属性。此属性称为“绑定锚点”，包含接口标识符 (ifIndex)，主机将通过它连接到主机 MAC 地址。

IPv6 第一步跳安全性交换机仅在周界接口上建立绑定（请参阅 [IPv6 第一步跳安全性周界](#)）。

绑定信息将保存在邻近绑定表中。

NBI-NDP 方法

使用的 NBI-NDP 方法基于 RFC6620 中规定的 FCFS- SAVI 方法，不同之处如下：

- 与仅支持链路本地 IPv6 地址绑定的 FCFS-SAVI 不同，NBI-NDP 还支持绑定全局 IPv6 地址。
- NBI-NDP 仅针对从 NDP 消息中学习的 IPv6 地址支持 IPv6 地址绑定。数据消息的源地址验证由 IPv6 源地址防护提供。
- 在 NBI-NDP 中，地址所有权证明基于先来先服务的原则。第一个声明给定源地址的主机是该地址的所有者，直到再次获得通知。如果没有可接受的主机更改，则必须找到一个方法来确定地址所有权，无需使用新协议。为此，无论何时从 NDP 消息中首次学习 IPv6 地址时，交换机都会将地址绑定到接口。后续包含此 IPV6 的 NDP 消息可根据同一绑定锚点来进行检查，以确定发起人拥有该源 IP 地址。

如果 IPv6 主机在第 2 层域中漫游或更改其 MAC 地址，此规则将发生异常。此时，主机仍然是 IP 地址的所有者，但关联的绑定锚点可能会更改。为配合此情况，定义的 NBI-NDP 行为将隐含主机是否可通过向上一绑定接口发送 DAD-NS 消息访问的验证。如果主机无法在之前记录的绑定锚点处访问，则 NBI-NDP 将假定新的锚点有效并更改绑定锚点。如果主机仍然可以使用之前记录的绑定锚点访问，则绑定接口将不会更改。

为减少邻近绑定表的大小，NBI-NDP 仅在周界接口上建立绑定（请参阅 [IPv6 第一步跳安全性周界](#)），并使用 NS 和 NA 消息通过内部接口分发绑定信息。在创建 NBI-NDP 本地绑定之前，设备会发送一个 DAD-NS 消息，用于查询涉及的地址。如果主机通过 NA 消息回复该消息，则发送 DAD-NS 消息的设备将推断该地址的绑定存在于另一设备中，且不会为其创建本地绑定。如果没有收到作为 DAD-NS 消息回复的 NA 消息，本地设备会推断其他设备中不存在该地址的绑定，并将为该地址创建本地绑定。

NBI-NDP 支持有效期限定时器。定时器的值可在“邻近绑定设置”页面设置。计时器在每次绑定的 IPv6 地址得到确认后都将重新启动。如果计时器过期，设备将发送多达 2 条 DAD-NS 消息，其中带有较短间隔，用于验证邻居。

NB 完整性策略

与其他 IPv6 第一步跳安全性功能的运作方式相同，NB 完整性在与接口连接的 NB 完整性策略指定的接口上运行。这些策略可在“邻近绑定设置”页面设置。

攻击保护

本节介绍 IPv6 第一步跳安全性提供的攻击保护

防止 IPv6 路由器欺骗

IPv6 主机可将接收的 RA 消息用于以下方面：

- IPv6 路由器发现
- 无状态地址配置

恶意主机可能会发送 RA 消息，将自身通告为 IPv6 路由器，并为无状态地址配置提供假冒前缀。

RA 防护可为 IPv6 路由器无法连接到的所有接口将接口角色配置为主机接口，从而防止此类攻击。

防止 IPv6 地址解析欺骗

恶意主机可能会发送 NA 消息，将自身通告为具有给定 IPv6 地址的 IPv6 主机。

NB 完整性可通过以下方式防止此类攻击：

- 如果给定 IPv6 地址未知，则邻居请求 (NS) 消息仅在内部接口上转发。
- 如果给定 IPv6 地址已知，则 NS 消息仅在 IPv6 地址绑定到的接口上转发。
- 如果目标 IPv6 地址与另一个接口绑定，邻居通告 (NA) 消息会被丢弃。

防止 IPv6 重复地址检测欺骗

IPv6 主机必须通过发送特殊 NS 消息（重复地址检测邻居请求消息 (DAD_NS) 消息），为每个已分配的 IPv6 地址执行重复地址检测。

恶意主机可能会发送对 DAD_RS 消息的回复，将自身通告为具有给定 IPv6 地址的 IPv6 主机。

NB 完整性可通过以下方式防止此类攻击：

- 如果给定 IPv6 地址未知，则 DAD_NS 消息仅在内部接口上转发。
- 如果给定 IPv6 地址已知，则 DAD_NS 消息仅在 IPv6 地址绑定到的接口上转发。
- 如果目标 IPv6 地址与另一个接口绑定，NA 消息会被丢弃。

防止 DHCPv6 服务器欺骗

IPv6 主机可将 DHCPv6 协议用于以下方面：

- 无状态信息配置
- 无状态地址配置

恶意主机可能会发送 DHCPv6 回复消息，将自身通告为 DHCPv6 服务器，并提供假冒无状态信息和 IPv6 地址。DHCPv6 防护可为 DHCPv6 服务器无法连接到的所有端口将接口角色配置为客户端口，从而防止此类攻击。

防止 NBD 缓存欺骗

IPv6 路由器支持将 IPv6 地址映射到上一步跳路由 MAC 地址的邻居发现协议 (NDP)。

恶意主机可能会发送带有不同上一步跳转发目的地 IPv6 地址的 IPv6 消息，导致 NBD 缓存溢出。

NDP 实现中的一个嵌入式机制可限制邻居发现缓存不完整状态中允许的条目数量，从而提供保护。

策略、全局参数和系统默认值

FHS 的每个功能都可以单独启用/禁用。默认情况下，功能都为禁用状态。

功能最初必须在特定 VLAN 上启用。启用功能时，您也可以定义该功能验证规则的全局配置值。如果未定义包含不同验证规则值的策略，则将功能应用到数据包时将使用全局值。

策略

策略包含在输入数据包上执行的验证规则。它们可以连接到 VLAN，还可以连接到端口和 LAG。如果 VLAN 上未启用该功能，策略将无效。

策略可以是用户定义的策略，也可以是默认策略（见下文）。

默认策略

每个 FHS 功能都存在空的默认策略，这些策略在默认状态下都与所有 VLAN 和接口连接。默认策略名为：“vlan_default”和“port_default”（对于各功能）：

- 规则可以添加到这些默认策略。您无法将默认策略手动连接到接口。默认情况下，它们处于连接状态。
- 默认策略无法删除。您只能删除用户定义的配置。

用户定义的策略

您可以定义除默认策略以外的策略。

当用户定义的策略连接到接口时，该接口的默认策略将解除连接。如果用户定义的策略与接口解除连接，则默认策略将重新连接。

在以下情况发生之前，策略不会生效：

- 策略中的功能在包含接口上的 VLAN 上启用
- 策略连接到接口（VLAN、端口或 LAG）。

连接一个策略时，该接口的默认策略将解除连接。从接口移除策略时，默认策略将重新连接。

您只能将 1 个策略（针对一个功能）连接到 VLAN。

如果指定了不同 VLAN，则可将多个策略（针对特定功能）连接到一个接口。

验证规则的级别

应用于接口上输入数据包的最终规则集通过以下方式构建：

- 在与数据包到达的接口（端口或 LAG）连接的策略中配置的规则将添加到此集。
- 如果在与 VLAN 连接的策略中配置的规则尚未在端口级别添加，则将添加到此集。
- 如果全局规则尚未在 VLAN 或端口级别添加，则将添加到此集。

在端口级别定义的规则将覆盖在 VLAN 级别设置的规则。在 VLAN 级别定义的规则将覆盖全局配置的规则。全局配置的规则将覆盖系统默认值。

常见任务

第一步跳安全性常见工作流程

- 步骤 1** 在“FHS 设置”页面，输入启用了此功能的 VLAN 列表。
- 步骤 2** 在同一页面，设置全局数据包丢弃记录功能。
- 步骤 3** 如果需要，可以配置用户定义的策略，也可以将规则添加到此功能的默认策略。
- 步骤 4** 使用“策略连接 (VLAN)”或“策略连接 (端口)”页面将策略连接到 VLAN、端口或 LAG。

路由器通告防护工作流程

- 步骤 1** 在“RA 防护设置”页面，输入启用了此功能的 VLAN 列表。
- 步骤 2** 在同一页面，设置在策略中未设置值时使用的全局配置值。
- 步骤 3** 如果需要，可以配置用户定义的策略，也可以将规则添加到此功能的默认策略。
- 步骤 4** 使用“策略连接 (VLAN)”或“策略连接 (端口)”页面将策略连接到 VLAN、端口或 LAG。

DHCPv6 防护工作流程

- 步骤 1** 在“DHCPv6 防护设置”页面，输入启用了此功能的 VLAN 列表。
- 步骤 2** 在同一页面，设置在策略中未设置值时使用的全局配置值。
- 步骤 3** 如果需要，可以配置用户定义的策略，也可以将规则添加到此功能的默认策略。
- 步骤 4** 使用“策略连接 (VLAN)”或“策略连接 (端口)”页面将策略连接到 VLAN、端口或 LAG。

邻居发现检测工作流程

- 步骤 1** 在“ND 检测设置”页面，输入启用了此功能的 VLAN 列表。
- 步骤 2** 在同一页面，设置在策略中未设置值时使用的全局配置值。
- 步骤 3** 如果需要，可以配置用户定义的策略，也可以将规则添加到此功能的默认策略。
- 步骤 4** 使用“策略连接 (VLAN)”或“策略连接 (端口)”页面将策略连接到 VLAN、端口或 LAG。

邻近绑定工作流程

- 步骤 1** 在“邻近绑定设置”页面，输入启用了此功能的 VLAN 列表。
- 步骤 2** 在同一页面，设置在策略中未设置值时使用的全局配置值。
- 步骤 3** 如果需要，可以配置用户定义的策略，也可以将规则添加到此功能的默认策略。
- 步骤 4** 在“邻近绑定表”页面添加任何需要的手动条目
- 步骤 5** 使用“策略连接 (VLAN)”或“策略连接 (端口)”页面将策略连接到 VLAN、端口或 LAG。

默认设置和配置

如果 IPv6 第一步跳安全性已在 VLAN 上启用，则默认情况下，交换机会 Trap 以下消息：

- 路由器通告 (RA) 消息
- 路由器请求 (RS) 消息

- 邻居通告 (NA) 消息
- 邻居请求 (NS) 消息
- ICMPv6 重定向消息
- 证书路径通告 (CPA) 消息
- 证书路径请求 (CPS) 消息
- DHCPv6 消息

默认情况下，FHS 功能处于禁用状态。

使用说明

无需执行任何预备任务。

通过 Web GUI 配置第一步跳安全性

FHS 常见设置

使用“FHS 设置”页面，可在一组指定的 VLAN 上启用 FHS 常见功能，并为数据包丢弃记录设置全局配置值。如果需要，可以添加策略，也可以将数据包丢弃记录添加到系统定义的默认策略。

在端口或 LAG 上配置第一步跳安全性常见的步骤：

步骤 1 单击 **安全 > 第一步跳安全性 > FHS 设置**。

步骤 2 填写以下全局配置字段：

- **FHS VLAN 列表** - 输入启用了第一步跳安全性的一个或多个 VLAN。
- **数据包丢弃记录** - 选择该选项以在数据包通过第一步跳安全性功能丢弃时创建系统日志。这是未定义策略时的全局默认值。

步骤 3 如果需要，通过单击**添加**创建一个 FHS 策略。

输入以下字段：

- **策略名称** - 输入用户定义的策略名称。

- **数据包丢弃记录** - 选择该选项以在数据包因此策略中的第一步跳安全性功能而丢弃时创建系统日志。
 - *继承* - 使用 VLAN 或全局配置中的值。
 - *启用* - 在数据包因第一步跳安全性而丢弃时创建系统日志。
 - *禁用* - 在数据包因第一步跳安全性而丢弃时，不创建系统日志。

RA 防护设置

使用“RA 防护设置”页面，可在一组指定的 VLAN 上启用 RA 防护功能，并为此功能设置全局配置值。如果需要，可以在此页面添加一个策略或者配置系统定义的默认 RA 防护策略。

在端口或 LAG 上配置 RA 防护的步骤：

步骤 1 单击 **安全 > 第一步跳安全性 > RA 防护设置**。

步骤 2 输入以下全局配置字段：

- **RA 防护 VLAN 列表** - 输入启用了 RA 防护的一个或多个 VLAN。
- **最小步跳限制** - 此字段指示 RA 防护策略是否将检查已收数据包的最小步跳限制。
 - *最小步跳限制* - 验证步跳数限制是否大于或等于此值。
 - *无校验* - 禁用对步跳数限制下边界的验证。
- **最大步跳限制** - 此字段指示 RA 防护策略是否将检查已收数据包的最大步跳限制。
 - *最大步跳限制* - 验证步跳数限制是否小于或等于此值。上边界的值必须等于或大于下边界的值。
 - *无校验* - 禁用对步跳数限制上边界的验证。
- **受管配置标签** - 此字段指定 IPv6 RA 防护策略内已通告受管地址配置标志的验证。
 - *无校验* - 禁用对已通告受管地址配置标志的验证。
 - *接通* - 启用已通告受管地址配置标志的验证。
 - *断开* - 标志的值必须为 0。

- **其他配置标签** - 此字段指定 IPv6 RA 防护策略内已通告其他配置标志的验证。
 - *无校验* - 禁用对已通告其他配置标志的验证。
 - *接通* - 启用已通告受管其他标志的验证。
 - *断开* - 标志的值必须为 0。
- **最低路由器优先级** - 此字段指示 RA 防护策略是否将验证 RA 防护策略内 RA 消息中的最小已通告默认路由器优先级值。
 - *无校验* - 禁用对已通告默认路由器优先级下边界的验证。
 - *低* - 指定允许的最小已通告默认路由器优先级值。可接受的值如下：低、中和高（见 RFC4191）。
 - *中* - 指定允许的最小已通告默认路由器优先级值。可接受的值如下：低、中和高（见 RFC4191）。
 - *高* - 指定允许的最小已通告默认路由器优先级值。可接受的值如下：低、中和高（见 RFC4191）。
- **最高路由器优先级** - 此字段指示 RA 防护策略是否将验证 RA 防护策略内 RA 消息中的最大已通告默认路由器优先级值。
 - *无校验* - 禁用对已通告默认路由器优先级上边界的验证。
 - *低* - 指定允许的最大已通告默认路由器优先级值。可接受的值如下：低、中和高（见 RFC4191）。
 - *中* - 指定允许的最大已通告默认路由器优先级值。可接受的值如下：低、中和高（见 RFC4191）。
 - *高* - 指定允许的最大已通告默认路由器优先级值。可接受的值如下：低、中和高（见 RFC4191）。

要创建 RA 防护策略或配置系统定义的默认策略，请单击**添加**并输入上述参数。

如果需要，单击**将策略连接到 VLAN** 或**将策略连接到接口**。

DHCPv6 防护设置

使用“DHCPv6 防护设置”页面，可在一组指定的 VLAN 上启用 DHCPv6 防护功能，并为此功能设置全局配置值。如果需要，可以在此页面添加一个策略或者配置系统定义的默认 DHCPv6 防护策略。

在端口或 LAG 上配置 DHCPv6 防护的步骤：

步骤 1 单击 **安全 > 第一步跳安全性 > DHCPv6 防护设置**。

步骤 2 输入以下全局配置字段：

- **DHCPv6 防护 VLAN 列表** - 输入启用了 DHCPv6 防护的一个或多个 VLAN。
- **最低优先级** - 此字段指示 DHCPv6 防护策略是否将检查已收数据包的最小已通告优先级值。
 - *无校验* - 禁用对已收数据包最小已通告优先级值的验证。
 - *用户定义的* - 验证已通告优先级值是否大于或等于此值。此值必须小于“最高优先级”值。
- **最高优先级** - 此字段指示 DHCPv6 防护策略是否将检查已收数据包的最大已通告优先级值。此值必须大于“最低优先级”值。
 - *无校验* - 禁用对步跳数限制下边界的验证。
 - *用户定义的* - 验证已通告优先级值是否小于或等于此值。

步骤 3 如果需要，单击**添加**以创建 DHCPv6 策略。

步骤 4 输入以下字段：

- **策略名称** - 输入用户定义的策略名称。
- **设备角色** - 选择**服务器**或**客户端**，以指定与 DHCPv6 防护端口连接的设备的角色。
 - *继承* - 设备角色继承自 VLAN 或系统默认（客户端）。
 - *客户端* - 设备角色为客户端。
 - *主机* - 设备角色为主机。
- **匹配回复前缀** - 选择该选项可启用对 DHCPv6 防护策略内已收 DHCP 回复消息中的已通告前缀的验证。
 - *继承* - 值继承自 VLAN 或系统默认（无校验）。
 - *无校验* - 不验证已通告前缀。
 - *匹配列表* - 要匹配的 IPv6 前缀列表。
- **匹配服务器地址** - 选择该选项可启用对 DHCPv6 防护策略内已收 DHCP 回复消息中的 DHCP 服务器 IPv6 地址和中继 IPv6 地址的验证。
 - *继承* - 值继承自 VLAN 或系统默认（无校验）。

- *无校验* - 禁用对 DHCP 服务器 IPv6 地址和中继 IPv6 地址的验证。
- *匹配列表* - 要匹配的 IPv6 前缀列表。
- **最低优先级** - 见上文。
- **最高优先级** - 见上文。

步骤 5 如果需要，单击**将策略连接到 VLAN 或将策略连接到接口**。

邻居发现检测设置

使用“ND 检测设置”页面，可在一组指定的 VLAN 上启用 ND 检测功能，并为此功能设置全局配置值。如果需要，可以在此页面添加一个策略或者配置系统定义的默认 ND 检测策略。

在端口或 LAG 上配置 ND 检测的步骤：

步骤 1 单击**安全 > 第一步跳安全性 > ND 检测设置**。

步骤 2 输入以下全局配置字段：

- **ND 检测 VLAN 列表** - 输入启用了 ND 检测的一个或多个 VLAN。
- **丢弃不安全的** - 选择该选项可丢弃 IPv6 ND 检测策略内无 CGA 或 RSA 签名选项的消息。
- **最低安全等级** - 如果不丢弃不安全的消息，请选择可转发消息的最低安全等级。
 - *无校验* - 禁用对安全等级的验证。
 - *用户定义的* - 指定要转发的消息的安全等级。

步骤 3 如果需要，单击**添加**以创建 ND 检测策略。

步骤 4 输入以下字段：

- **策略名称** - 输入用户定义的策略名称。
- **设备角色** - 选择**服务器**或**客户端**，以指定与 ND 检测端口连接的设备的角色。
 - *继承* - 设备角色继承自 VLAN 或系统默认（客户端）。
 - *客户端* - 设备角色为客户端。
 - *主机* - 设备角色为主机。
- **丢弃不安全的** - 见上文。
- **最低安全等级** - 见上文。

- **验证源 MAC** - 指定是否全局启用对照链路层地址的源 MAC 地址检查：
 - *继承* - 从 VLAN 或系统默认（已禁用）继承值。
 - *启用* - 启用对照链路层地址的源 MAC 地址检查。
 - *禁用* - 禁用对照链路层地址的源 MAC 地址检查。

步骤 5 如果需要，单击**将策略连接到 VLAN 或将策略连接到接口**。

邻近绑定设置

邻近绑定表是一个包含与设备连接的 IPv6 邻居的数据库表，从邻居发现协议 (NDP) 侦听等信息源中创建。此数据库（或称绑定）表由各种 IPv6 防护功能用于阻止侦听并重定向攻击。

使用“邻近绑定设置”页面，可在一组指定的 VLAN 上启用邻近绑定功能，并为此功能设置全局配置值。如果需要，可以在此页面添加一个策略或者配置系统定义的默认邻近绑定策略。

在端口或 LAG 上配置邻近绑定的步骤：

步骤 1 单击**安全 > 第一步跳安全性 > 邻近绑定设置**。

步骤 2 输入以下全局配置字段：

- **邻近绑定 VLAN 列表** - 输入启用了邻近绑定的一个或多个 VLAN。
- **Manual Neighbor Binding（手动邻近绑定）** - 选择该选项以指示条目是否可以手动添加到邻近绑定表。
- **邻近绑定有效期限** - 输入地址在邻近绑定表中保留的时间长度。
- **邻近绑定记录** - 此字段指示是否对照邻居前缀表验证绑定 IPv6 地址，以及是否记录绑定表主要事件。
- **邻近绑定条目限制** - 指定每个接口类型或地址类型的最大邻近绑定条目数量：
 - *每个 VLAN 的条目*:- 指定每个 VLAN 的邻近绑定限制。
 - *每个接口的条目*:- 指定每个接口的邻近绑定限制。
 - *每个 MAC 地址的条目*:- 指定每个 MAC 地址的邻近绑定限制。

步骤 3 如果需要，单击**添加**以创建邻近绑定策略。

步骤 4 输入以下字段：

- **策略名称** - 输入用户定义的策略名称。

- **设备角色** - 选择**服务器**或**客户端**，以指定与邻近绑定策略端口连接的设备的角色。
 - **继承** - 设备角色继承自 VLAN 或系统默认（客户端）。
 - **客户端** - 设备角色为客户端。
 - **主机** - 设备角色为主机。
- **邻近绑定记录** - 见上文。
- **邻近绑定条目限制** - 见上文。

步骤 5 如果需要，单击**将策略连接到 VLAN** 或**将策略连接到接口**。

策略连接 (VLAN)

将策略连接到一个或多个 VLAN 的步骤：

步骤 1 单击**安全 > 第一步跳安全性 > 策略连接 (VLAN)**。

已连接的策略列表将与其**策略类型**、**策略名称**和 **VLAN 列表**一起显示。

步骤 2 要将策略连接到 VLAN，请单击**添加**并填写以下字段：

- **策略类型** - 选择要连接到接口的策略类型。
- **策略名称** - 选择要连接到接口的策略的名称。
- **VLAN 列表** - 选择策略要连接的 VLAN。选择**所有 VLAN** 或输入一系列 VLAN。

步骤 3 单击**应用**将设置添加到当前配置文件。

策略连接 (端口)

将策略连接到一个或多个端口或 LAG 的步骤：

步骤 1 单击**安全 > 第一步跳安全性 > 策略连接 (端口)**。

已连接的策略列表将与其**接口号**、**策略类型**、**策略名称**和 **VLAN 列表**一起显示。

步骤 2 要将策略连接到端口或 LAG，请单击**添加**并填写以下字段：

- **接口** - 选择在其上连接策略的接口。
- **策略类型** - 选择要连接到接口的策略类型。

- **策略名称** - 选择要连接到接口的策略的名称。
- **VLAN 列表** - 选择策略要连接的 VLAN。选择**所有 VLAN** 或输入一系列 VLAN。

步骤 3 单击**应用**将设置添加到当前配置文件。

邻近绑定表

在邻近绑定表中添加或修改条目的步骤：

步骤 1 单击**安全 > 第一步跳安全性 > 邻近绑定表**。

步骤 2 请选择以下其中一个清除表选项：

- **仅静态** - 清除表中的所有静态条目。
- **仅动态** - 清除表中的所有动态条目。
- **全部动态和静态** - 清除表中的所有动态和静态条目。

步骤 3 单击**添加**，向表中添加新的条目。

步骤 4 输入以下字段：

- **VLAN ID** - 条目的 VLAN ID。
- **IPv6 地址** - 条目的源 IPv6 地址。
- **接口名称** - 接收数据包的端口。
- **MAC 地址** - 数据包的邻近 MAC 地址。

FHS 状态

显示 FHS 功能全局配置的步骤：

步骤 1 单击**安全 > 第一步跳安全性 > FHS 状态**。

步骤 2 选择报告了 FHS 状态的端口、LAG 或 VLAN。

步骤 3 将针对选定接口显示以下字段：

- **FHS 状态**
 - **当前 VLAN 上的 FHS 状态** - FHS 是否已在当前 VLAN 上启用。
 - **数据包丢弃记录** - 此功能是否已针对当前接口启用（在全局配置级别或与接口连接的策略中）。

- **RA 防护状态**

- **当前 VLAN 上的 RA 防护状态:**- RA 防护是否已在当前 VLAN 上启用。
- **设备角色:**- RA 设备角色。
- **管理型配置标志:**- 是否已启用对管理型配置标志的验证。
- **其他配置标志:**- 是否已启用对其他配置标志的验证。
- **RA 地址列表:**- 要匹配的 RA 地址列表。
- **RA 前缀列表:**- 要匹配的 RA 前缀列表。
- **最小步跳限制:**- 是否已启用最小 RA 步跳限制验证。
- **最大步跳限制:**- 是否已启用最大 RA 步跳限制验证。
- **最低路由器优先级:**- 是否已启用最低路由器优先级验证。
- **最高路由器优先级:**- 是否已启用最高路由器优先级验证。

- **ND 检测状态**

- **当前 VLAN 上的 ND 检测状态:**- ND 检测是否已在当前 VLAN 上启用。
- **设备角色:**- ND 检测设备角色。
- **丢弃不安全的:**- 不安全的消息是否已丢弃。
- **最低安全等级:**- 如果不安全的消息未丢弃，可转发数据包的最低安全等级是哪一级。
- **验证源 MAC:**- 是否已启用源 MAC 地址验证。

- **DHCP 防护状态**

- **当前 VLAN 上的 DHCPv6 防护状态:**- DHCPv6 防护是否已在当前 VLAN 上启用。
- **设备角色:**- DHCP 设备角色。
- **匹配回复前缀:**- 是否已启用 DHCP 回复前缀验证。
- **匹配服务器地址:**- 是否已启用 DHCP 服务器地址验证。
- **最低优先级:**- 是否已启用最低优先级验证。
- **最高优先级:**- 是否已启用最高优先级验证。

- **邻近绑定状态**

- **当前 VLAN 上的邻近绑定状态**:- 邻近绑定是否已在当前 VLAN 上启用。
- **设备角色**:- 邻近绑定设备角色。
- **记录绑定**:- 是否已启用邻近绑定表事件记录。
- **每个 VLAN 的最多条目数**:- 每个 VLAN 允许的最大动态邻近绑定表条目数量。
- **每个接口的最多条目数**:- 每个接口允许的最大邻近绑定表条目数量。
- **每个 MAC 地址的最多条目数**:- 每个 MAC 地址允许的最大邻近绑定表条目数量。

FHS 统计信息

显示 FHS 统计信息的步骤：

步骤 1 单击 **安全 > 第一步跳安全性 > FHS 统计信息**。

步骤 2 此时将显示以下字段：

- **NDP（邻居发现协议）消息** - 将显示以下消息类型的已收及已桥接消息数量：
 - *RA* - 路由器通告消息。
 - *CPA* - 证书路径通告消息。
 - *ICMPv6* - 互联网控制信息 IPv6 协议信息。
 - *NS* - 邻居请求消息。
 - *RS* - 路由器请求消息。
 - *CPS* - 证书路径请求消息。
- **DHCPv6 消息** - 将显示各种 DHCPv6 消息类型的已收和已桥接消息数量

将显示“FHS 丢弃消息表”中的以下字段

- **协议** - 丢弃的消息协议。
- **消息类型** - 丢弃的消息类型。
- **计数** - 丢弃的消息的数量。
- **原因** - 消息丢弃的原因。

安全：SSH 客户端

本节介绍了作为 SSH 客户端的设备。

其中包含以下主题：

- [安全复制 \(SCP\) 和 SSH](#)
- [保护方法](#)
- [SSH 服务器验证](#)
- [SSH 客户端验证](#)
- [使用说明](#)
- [常见任务](#)
- [GUI 中的 SSH 客户端配置](#)

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。

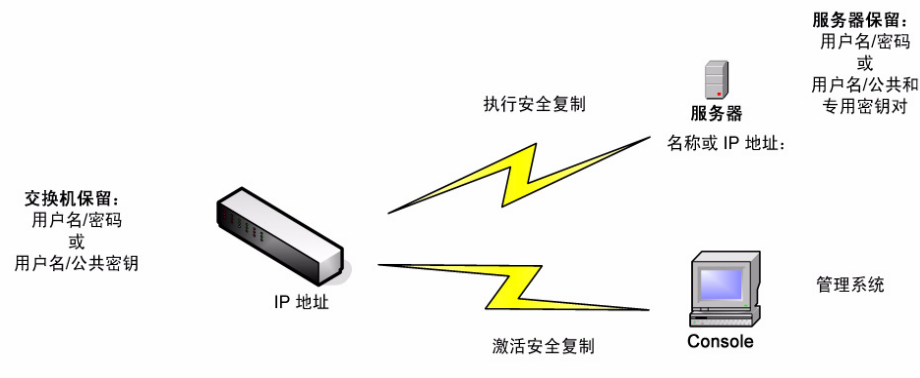
通过 TFTP 或 HTTP 下载文件时，无法确保数据传输的安全性。

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



345165

保护方法

将数据从 SSH 服务器传输到设备（客户端）时，SSH 服务器会使用多种方法验证客户端。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。将数据从服务器传输到设备时，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

要使用公共/专用密钥方法，需在 SSH 服务器上创建用户名和公共密钥。在设备上生成公共密钥（如下所述），然后将其复制到服务器。本指南未介绍在服务器上创建用户名以及将公共密钥复制到服务器这两项操作。

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。

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，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，将完成搜索，但无法进行验证。
- 如果在信任服务器列表中找到 SSH 服务器的条目，该过程将无法进行。

SSH 客户端验证

默认情况下，启用藉由密码进行 SSH 客户端验证，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。

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。

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-cbc
 - 3des-cbc
 - arcfour

- aes192-cbc
- aes256-cbc
- 消息验证码算法
 - hmac-sha1
 - hmac-md5

注 不支持压缩算法。

使用说明

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

本节介绍了一些使用 SSH 客户端执行的常见任务。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 SSH 服务器的数据，请执行以下步骤：

步骤 1 确定要使用的验证方法：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. 能够实现真正的安全数据传输后，在“SSH 用户验证”页面中创建全局密码，或者在“升级/备份固件/语言”或“下载/备份配置/日志”页面中创建临时密码。
- b. 在“升级/备份固件/语言”页面中选择**通过 SCP (藉由 SSH)**选项，以使用 SCP 来升级固件、引导映像或语言文件。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“下载/备份配置/日志”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 SSH 服务器上设置用户名/密码，或者在 SSH 服务器上修改密码。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“升级/备份固件/语言”页面中选择**通过 SCP (藉由 SSH)**选项，以使用 SCP 来升级/备份固件或语言文件。
- d. 在“下载/备份配置/日志”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。

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“安全敏感数据管理 > 属性”页面中设置 SSD 属性，并创建一个新的本地密码。

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**。

GUI 中的 SSH 客户端配置

本节介绍了用于配置 SSH 客户端功能的页面。

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：

- **藉由密码** - 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。
- **藉由 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。
- **藉由 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**藉由密码**方法，请输入一个密码（**加密模式**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**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。
- **IP 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 4 单击**应用**。信任服务器定义将存储在当前配置文件中。

在 SSH 服务器上更改用户密码

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。
- **IP 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**。将修改 SSH 服务器中的密码。

安全：SSH 服务器

本节介绍了如何在设备上建立 SSH 会话。

其中包含以下主题：

- [概述](#)
- [常见任务](#)
- [SSH 服务器配置页面](#)

概述

使用 SSH 服务器功能，用户可以创建至设备的 SSH 会话。类似于建立 telnet 会话，只是会话会受到保护。

设备上会自动生成公共和专用密钥。用户可以修改这些密钥。

SSH 会话通过特殊的 SSH 客户端应用（如 PuTTY）打开。

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：要使用设备自动创建的（默认）密钥通过 SSH 登录设备，请执行以下步骤：

-
- 步骤 1** 在“TCP/UDP 服务”页面中启用 SSH 服务器，并确保“SSH 用户验证”页面中已禁用通过公共密钥的 SSH 用户验证。
 - 步骤 2** 使用设备的 IP 地址登录外部 SSH 客户端应用（如 PuTTY）（不必使用设备已知的用户名或密钥）。

工作流程 2：要创建 SSH 用户并使用该用户通过 SSH 登录设备，请执行以下步骤：

-
- 步骤 1** 在外部 SSH 客户端应用（如 PuTTY）上生成 RSA 或 DSA 密钥。
 - 步骤 2** 在“SSH 用户验证”页面中启用通过公共密钥或密码的 SSH 用户验证。
 - 步骤 3** 根据需要启用自动登录（请参阅下文的[自动登录](#)）。
 - 步骤 4** 在“SSH 用户验证”页面中添加用户并复制到外部生成的公共密钥中。
 - 步骤 5** 使用设备的 IP 地址和用户的用户名登录外部 SSH 客户端应用（如 PuTTY）。

工作流程 3：要将设备 A 的 RSA 或 DSA 密钥导入设备 B，请执行以下步骤：

-
- 步骤 1** 在设备 A 上的“SSH 服务器验证”页面选择 RSA 或 DSA 密钥。
 - 步骤 2** 单击[详情](#)并将选定密钥类型的公共密钥复制到记事本或其他文本编辑器应用。
 - 步骤 3** 登录到设备 B 并打开“SSH 服务器验证”页面。选择 RSA 或 DSA 密钥，单击[编辑](#)并粘贴设备 A 的密钥。
-

SSH 服务器配置页面

本节介绍用于配置 **SSH 服务器** 功能的页面。

SSH 用户验证

在“SSH 用户验证”页面中，可以启用通过公共密钥和/或密码进行 SSH 用户验证，并在通过公共密钥进行验证时，添加用于在外部 SSH 应用（如 PuTTY）中创建 SSH 会话的 SSH 客户端用户。

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（Console、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[定义用户](#)）。
- **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。请参阅[自动登录](#)。

对于配置的用户，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 3 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。

SSH 服务器验证

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。

要重新生成 RSA 或 DSA 密钥或者要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**。

将为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。
- **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。

步骤 4 如果复制了来自其他设备的新密钥，请单击**应用**。密钥存储在当前配置文件中。

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 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的外部验证服务器进行安全通信。

总之，SSD 可通过 SSD 规则、SSD 属性和用户验证来保护设备上的敏感数据。设备的 SSD 规则、SSD 属性和用户验证配置本身作为敏感数据也将受到 SSD 的保护。

SSD 管理

SSD 管理包括对敏感数据的处理方法和安全性进行定义的诸多配置参数的管理。SSD 配置参数本身作为敏感数据也将受到 SSD 的保护。

SSD 的所有配置将通过 SSD 页面执行，只有具有正确权限的用户才能访问这些页面（请参阅 [SSD 规则](#)）。

SSD 规则

SSD 规则对授予管理通道上用户会话的读取权限和默认读取模式作出定义。

SSD 规则将由其用户通过 SSD 管理通道进行唯一识别。不同的 SSD 规则可能适用于同一用户但同时适用于不同的通道，反之，不同的规则也可能适用于同一通道但同时适用于不同的用户。

读取权限将决定敏感数据的查看方式：仅以加密模式、仅以明文模式、两种模式兼而有之或不允许查看敏感数据。SSD 规则本身作为敏感数据也将受到保护。

一台设备总共可支持 32 条 SSD 规则。

当 SSD 规则与用户身份/用户凭证以及作为用户目前/将要访问敏感数据的管理通道的类型实现最佳匹配时，设备将向用户授予该规则的 SSD 读取权限。

设备会自带一套默认的 SSD 规则。管理员可按需要添加、删除和更改 SSD 规则。

注 设备可能并非支持 SSD 定义的所有通道。

SSD 规则的内容

SSD 规则包含以下内容：

- **用户类型** - 以下是按最高优先级到最低优先级顺序支持的用户类型：（如果用户与多条 SSD 规则匹配，则应用具有最高优先级用户类型的规则）。
 - **特定** - 该规则应用于特定用户。
 - **默认用户 (cisco)** - 该规则应用于默认用户 (cisco)。

- **第 15 级** - 该规则应用于具有 15 级权限的用户。
- **全部** - 该规则应用于所有用户。
- **用户名** - 如果用户类型为“特定”，则需要提供用户名。
- **通道**。规则适用的 SSD 管理通道类型。受支持的通道类型有：
 - **安全** - 指定该规则仅应用于安全通道。根据不同的设备，可能会支持以下部分或所有的安全通道：Console 端口界面、SCP、SSH 和 HTTPS。
 - **不安全** - 指定该规则仅应用于不安全通道。根据不同的设备，可能会支持以下部分或所有的不安全通道：Telnet、TFTP 和 HTTP。
 - **安全 XML SNMP** - 指定该规则仅应用于带保密功能的 XML over HTTPS 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** - 所有的默认读取模式均受规则读取权限的限制。存在以下选项，但有些选项可能会被拒绝，这取决于读取权限。例如，如果用户的用户定义的读取权限为“无”且默认读取模式为“加密模式”，则以用户定义的读取权限为准。

- 无 - 不允许读取敏感数据。
- **加密模式** - 以加密形式显示敏感数据。
- **明文模式** - 以明文形式显示敏感数据。

每一管理通道都允许特定的读取权限。以下是对上述内容的总结。

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 社团名称将不用作与 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：

表 3

规则密钥		规则操作	
用户	通道	读取权限	默认阅读模式
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 Sx200、Sx300、Sx500 和 SG500X/SG500XG/ESW2-550X 系列交换机能够解密彼此的敏感数据，这些数据通常通过从密码中生成的密钥进行了加密。

密码必须符合以下规则：

- **长度** - 在 8 到 16 个字符之间。
- **字符类别数** - 密码必须至少包含一个大写字符、一个小写字符、一个数字字符和一个特殊字符（例如：#、\$）。

默认密码和用户定义的密码

所有设备均提供开箱即用的默认密码，用户可以查看。默认密码不会显示在配置文件或 CLI/GUI 中。

如果希望进一步加强保护和提高安全性，管理员应在设备上配置 SSD 以使用用户定义的密码而不是默认密码。用户定义的密码应严格对外保密，以便有效保障设备上敏感数据的安全性。

用户定义的密码可以明文模式进行手动配置。也可以衍生自配置文件。（请参阅[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，该密码是设备当前配置的密码。SSD 通常会通过从本地密码生成的密钥执行敏感数据的加密和解密。

本地密码可配置为默认密码或用户定义的密码。默认情况下，本地密码和默认密码是一致的。可通过命令行界面（如可用）或基于 Web 的界面上的管理操作更改本地密码。当启动配置成为设备的当前配置后，本地密码将自动更改为启动配置文件中的密码。当设备重置回出厂默认配置后，本地密码将重置为默认密码。

配置文件密码控制

文件密码控制为用户定义的密码以及在基于文本的配置文件中通过从用户定义的密码生成的密钥来加密的敏感数据提供了进一步的保护。

以下是现有的密码控制模式：

- **无限制**（默认情况下） - 设备在创建配置文件时会将其密码包含在内。这就使任何接受配置文件的设备都能从文件中学习密码。
- **已限制** - 设备将限制向配置文件导入其密码。已限制模式可防止没有密码的设备访问配置文件中加密的敏感数据。如果用户不希望在配置文件中显示密码，则应使用该模式。

当设备重置回出厂默认配置后，其本地密码将重置为默认密码。设备将因此无法解密任何加密的敏感数据，无论是基于从管理会话 (GUI/CLI) 输入的用户定义的密码加密的敏感数据，还是在任何带有限制模式的配置文件（包括设备重置回出厂默认配置前由其创建的文件）中加密的敏感数据。这种情况将一直持续到通过用户定义的密码手动重新配置该设备或该设备从配置文件中学习用户定义的密码为止。

配置文件完整性控制

用户可通过“配置文件完整性控制”创建配置文件，藉此使配置文件免遭破坏或修改。我们建议当设备通过“无限制配置文件密码控制”使用用户定义的密码时应启用“配置文件完整性控制”。



注意

对受完整性保护的配置文件所做的任何修改都将被视为对该文件的破坏。

设备可通过检查配置文件的“SSD 控制”块中的“文件完整性控制”命令来确定配置文件的完整性是否受到了保护。如果文件的完整性受到保护但设备却发现文件的完整性并不完整，则设备将拒绝该文件。否则，将接受该文件以作进一步处理。

当基于文本的配置文件下载或复制到启动配置文件中时，设备将检查该文件的完整性。

阅读模式

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中时，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 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 > 配置文件属性**。

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
Console	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

管理通道	SSD 管理通道类型	类似的安全管理通道
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

只有阅读权限为“所有模式”或“仅明文模式”的用户允许使用菜单 CLI 接口。拒绝其他用户使用。菜单 CLI 中的敏感数据始终以明文模式显示。

目前，密码恢复可从引导菜单激活，用户无需身份验证即可登录到终端。如果支持 SSD，只有当本地密码与默认密码相同时，才允许使用此选项。如果设备已配置用户定义的密码，则该用户将不能激活密码恢复。

配置 SSD

在以下页面中配置 SSD 功能：

- 在“属性”页面中设置 SSD 属性。
- 在“SSD 规则”页面中定义 SSD 规则。

SSD 属性

只有具有“仅明文模式”或“所有模式” SSD 读取权限的用户允许设置 SSD 属性。

配置全局 SSD 属性的步骤：

步骤 1 单击 **安全 > 安全敏感数据管理 > 属性**。将显示以下字段：

- 当前本地密码类型** - 显示当前正在使用的是默认密码还是用户定义的密码。

步骤 2 输入以下永久设置字段：

- **配置文件密码控制** - 按照**配置文件密码控制**中的说明选择选项。
- **配置文件完整性控制** - 选择后，将启用此功能。请参阅**配置文件完整性控制**。

步骤 3 为当前会话选择读取模式（请参阅 **SSD 规则的内容**）。

更改本地密码的步骤：

步骤 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。

SSD 规则

只有具有“仅明文模式”或“所有模式” SSD 读取权限的用户允许设置 SSD 规则。

配置 SSD 规则的步骤：

步骤 1 单击**安全 > 安全敏感数据管理 > SSD 规则**。

此时将显示当前定义的规则。

步骤 2 要添加新规则，请单击**添加**。输入以下字段：

- **用户** - 此字段定义规则所应用的用户。请选择以下其中一个选项：
 - **特定用户** - 选择并输入此规则所应用的特定用户名（不一定非要定义此用户）。
 - **默认用户 (cisco)** - 表示此规则所应用的默认用户。
 - **第 15 级** - 表示此规则应用于具有 15 级权限的所有用户。
 - **全部** - 表示此规则应用于所有用户。

- **通道** - 此字段定义规则所应用的输入通道的安全级别：请选择以下其中一个选项：
 - **安全** - 表示此规则仅应用于安全通道（Console、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。
- **默认阅读模式** - 所有默认阅读模式需遵循规则的读取权限。存在以下选项，但根据规则的读取权限，有些选项可能会被拒绝。
 - **无** - 不允许读取敏感数据。
 - **加密模式** - 敏感数据以加密模式提供。
 - **明文模式** - 敏感数据以明文模式提供。

步骤 3 可以执行以下操作：

- **恢复为默认设置** - 将用户修改的默认规则恢复为默认规则。
- **将所有规则恢复为默认设置** - 将所有用户修改的默认规则恢复为默认规则，并移除所有用户定义的规则。

访问控制

访问控制列表 (ACL) 功能是安全机制的一部分。ACL 定义可用作多种机制之一，这些机制用于定义为特定服务质量 (QoS) 提供的流量。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：

- [访问控制列表](#)
- [定义基于 MAC 的 ACL](#)
- [基于 IPv4 的 ACL](#)
- [基于 IPv6 的 ACL](#)
- [定义 ACL 绑定](#)

访问控制列表

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。

设备最多支持 512 个 ACL 以及 512 个 ACE。

如果数据包与 ACE 过滤器匹配，则会执行 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，则会丢弃该数据包（为默认操作）。由于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，例如指向该设备本身的 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 Snooping，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 Snooping 将在该端口处失败。

ACL 中 ACE 的顺序很重要，因为 ACE 是以首次匹配方式应用的。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优先化。

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 IPv6 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（请参阅 [QoS 高级模式](#)）。

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”页面和“基于 MAC 的 ACE”页面创建基于 MAC 的 ACL
 - b. 使用“基于 IPv4 的 ACL”页面和“基于 IPv4 的 ACE”页面创建基于 IP 的 ACL
 - c. 使用“基于 IPv6 的 ACL”页面和“基于 IPv6 的 ACE”页面创建基于 IPv6 的 ACL

2. 使用“ACL 绑定”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。下文介绍了解除绑定 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”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，则您必须按如下所示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。

定义基于 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。

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。

为基于 MAC 的 ACL 添加规则

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，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。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。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“端口设置”页面重新激活这类端口。
- **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。时间范围已在时间范围节中进行过定义。
- **目的 MAC 地址** - 如果所有目的地址均可接受，则选择任意；或选择用户定义，以输入一个目的地址或输入目的地址的范围。
- **目的 MAC 地址值** - 输入要将目的 MAC 地址与其相匹配的 MAC 地址及其掩码（如果相关）。
- **目的 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（例如，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 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。

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/目的端口
- TCP 帧的标签值
- ICMP 和 IGMP 类型和代码
- 源 IP 地址/目的 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（请参阅“**QoS 高级模式**”）。

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。

定义基于 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。

为基于 IPv4 的 ACL 添加规则 (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，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**。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。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“端口管理”页面重新激活端口。
- **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**时间范围**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，从下拉列表中选择以下协议之一：
 - *ICMP* - Internet 控制消息协议
 - *IGMP* - Internet 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 碎片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* - Internet 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
 - *PIP* - 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（例如，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 0。在此示例中，因为 1111 1111 = 255，因此该掩码将写成：0.0.0.255。

- **目的 IP 地址** - 如果所有目的地址均可接受，则选择*任意*；或选择*用户定义*，以输入一个目的地址或输入目的地址的范围。
- **目的 IP 地址值** - 输入要将目的 MAC 地址与其相匹配的 IP 地址。
- **目的 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。
 - *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，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（源端口与目的端口共享）。TCP 和 UDP 协议各有八个端口范围。
- **目的端口** - 从与上述“源端口”字段相同的一组值中选择一个可用值。

注 您必须为 ACE 指定 IP 协议，才能输入源端口和/或目的端口。

- **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。
- **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。

基于 IPv6 的 ACL

“基于 IPv6 的 ACL” 页面可显示并创建 IPv6 ACL，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（请参阅 [QoS 高级模式](#)）。

定义基于 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。

为基于 IPv6 的 ACL 添加规则 (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**。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。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“端口管理”页面重新激活端口。
- **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**时间范围**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 Internet 控制消息协议 (ICMP) 相匹配。
- **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。
 - **目的 IP 地址** - 如果所有目的地址均可接受，则选择 *任意*；或选择 *用户定义*，以输入一个目的地址或输入目的地址的范围。
 - **目的 IP 地址值** - 输入要将目的 MAC 地址与其相匹配的 IP 地址及其掩码（如果相关）。
 - **目的 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。
 - *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 IP 协议下拉菜单中选择 800/6-TCP 或 800/17-UDP 后，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。
 - **目的端口** - 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 ACL 指定 IPv6 协议，才能配置源端口和/或目的端口。
- **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。
 - *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。
 - *Dont care* - 忽略 TCP 标签。
 - **服务类型** - IP 数据包的服务类型。
 - **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**。

定义 ACL 绑定

将一个 ACL 与一个接口（端口、LAG 或 VLAN）绑定后，会将该 ACL 的 ACE 规则应用于到达该接口的数据包。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。

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**。针对选择的每种接口类型，会显示该类型的所有接口及其当前 ACL 的列表：

- **接口** - 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）。

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 请选择以下选项之一：

- **选择基于 MAC 的 ACL** - 选择要与该接口绑定的基于 MAC 的 ACL。
- **选择基于 IPv4 的 ACL** - 选择要与该接口绑定的基于 IPv4 的 ACL。
- **选择基于 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**。将修改 ACL 绑定，并更新当前配置文件。

注 如果不选择任何 ACL，则会将之前与该接口绑定的 ACL 解除绑定。

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，请新增一个。

步骤 3 请选择以下选项之一：

- **选择基于 MAC 的 ACL** - 选择要与该接口绑定的基于 MAC 的 ACL。
- **选择基于 IPv4 的 ACL** - 选择要与该接口绑定的基于 IPv4 的 ACL。
- **选择基于 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**。将修改 ACL 绑定，并更新当前配置文件。

注 如果不选择任何 ACL，则会将之前与该 VLAN 绑定的 ACL 解除绑定。

服务质量

在整个网络中应用服务质量功能，可确保根据所需条件设置网络流量的优先级，从而优先处理所需的流量。

本节包含以下主题：

- **QoS 功能和组件**
- **配置 QoS - 一般**
- **QoS 基本模式**
- **QoS 高级模式**
- **管理 QoS 统计信息**

QoS 功能和组件

QoS 功能可用于优化网络性能。

QoS 可实现：

- 根据以下属性将传入流量分为不同的流量类：
 - 设备配置
 - 入口接口
 - 数据包内容
 - 以上属性的组合

QoS 包括：

- **流量分类** - 根据数据包内容和/或端口，将每个传入数据包分类为属于特定数据流。分类操作由 ACL（访问控制列表）完成，并且仅对符合 ACL 标准的流量进行 CoS 或 QoS 分类。

- **分配至硬件队列** - 将传入数据包分配给转发队列。数据包所属流量类所具有的功能会将数据包发送到特定的队列进行处理。请参阅[配置 QoS 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头字段类型。对于该字段的每个值，在“CoS/802.1p 到队列”页面或“DSCP 到队列”页面（具体取决于信任模式为 CoS/802.1p 还是 DSCP）中指定出口队列，指示会通过该队列发送帧。

QoS 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)。

将对类相同的所有流量进行相同的处理，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）中指定从中发送帧的出口队列。

- **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，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，将不会保留基本模式下的 QoS 信任模式配置。
- 如果禁用 QoS，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/802.1p 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** 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。

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。

配置 QoS - 一般

“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。此外，还可以使用该页面来定义每个接口的默认 CoS 优先级。

设置 QoS 属性

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。可能的选项有：

- **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。该默认值仅对 Untagged 帧有效，而且系统必须处于基本模式，并在“全局设置”页面中选择“信任 CoS”的情况下有效。

选择**恢复默认设置**会为此接口还原出厂 CoS 默认设置。

步骤 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。

配置 QoS 队列

设备支持每个接口 4 或 8 个队列（在“系统模式和堆栈管理”页面中选择）。编号为 4 或 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，从队列 4 或队列 8（最高优先级队列）开始处理，每当完成一个队列后就继续处理下一优先级的队列。

如果排队模式为“加权轮循”，则会按照配额处理队列，在一个队列的配额用尽后开始处理另一个队列。

也可以将部分较低优先级的队列指定为 WRR 模式，同时保持部分较高优先级的队列为“严格优先级”模式。在这种情况下，“严格优先级”队列中的流量会始终先于 WRR 队列中的流量发送。仅当“严格优先级”队列中的流量发送完毕后会转发 WRR 队列中的流量。（每个 WRR 队列的相对配额取决于其加权）。

选择优先级方法及输入 WRR 资料的步骤：

- 步骤 1 单击服务质量 > 一般 > 队列。
- 步骤 2 输入参数。
 - 队列 - 显示队列编号。
 - 调度方法：请选择以下其中一个选项：
 - 严格优先级 - 针对所选队列及所有更高优先级队列的流量调度将严格遵循队列优先级。
 - WRR - 针对所选队列的流量调度将遵循 WRR。在不为空的 WRR 队列（表示队列具有要输出的描述符）之间划分时段。仅当“严格优先级”队列为空时，才会采用此方法。
 - WRR 加权 - 如果选择了 WRR，请输入为队列分配的 WRR 加权。
 - WRR 带宽百分比 - 显示已为队列分配的带宽。这些值表示 WRR 加权的百分比。
- 步骤 3 单击应用。将配置队列，并更新当前配置文件。

将 CoS/802.1p 映射到队列

使用“CoS/802.1p 到队列”页面，可以将 802.1p 优先级映射到出口队列。“CoS/802.1p 到队列表”可根据传入数据包 VLAN 标记中的 802.1p 优先级确定数据包的出口队列。对于传入的 Untagged 数据包，802.1p 优先级是指定给入口端口的默认 CoS/802.1p 优先级。

下表介绍 4 个队列时的默认映射：

802.1p 值 (0-7, 7 为最高优先级)	队列 (4 个队列 1-4, 4 为最高优先级)	注
0	1	后台
1	1	尽力服务
2	2	最大努力
3	3	关键应用 - LVS 电话 SIP
4	3	视频

802.1p 值 (0-7, 7 为最高优先级)	队列 (4 个队列 1-4, 4 为最高优先级)	注
5	4	视频 - 默认思科 IP 电话
6	4	交互操作控制 - LVS 电话 RTP
7	4	交互操作控制

下表介绍 8 个队列时的默认映射：

802.1p 值 (0-7, 7 为最高优先级)	队列 (8 个队列 1-8, 8 为最高优先级) 独立式	7 个队列 (8 为最高优先级, 用于堆栈控制流量) 堆栈	注
0	1	1	后台
1	2	1	尽力服务
2	3	2	最大努力
3	6	5	关键应用 - LVS 电话 SIP
4	5	4	视频
5	8	7	视频 - 默认思科 IP 电话
6	8	7	交互操作控制 LVS 电话 RTP
7	7	6	交互操作控制

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，队列 4 或 8 的优先级最高。

将 CoS 值映射到出口队列的步骤：

步骤 1 单击 **服务质量 > 一般 > CoS/802.1p 到队列**。

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**。将 801.1p 优先级值映射到队列,并更新当前配置文件。

将 DSCP 映射到队列

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 4 队列系统的默认 DSCP 到队列映射：

DSCP	63	55	47	39	31	23	15	7
队列	3	3	4	3	3	2	1	1
DSCP	62	54	46	38	30	22	14	6
队列	3	3	4	3	3	2	1	1
DSCP	61	53	45	37	29	21	13	5
队列	3	3	4	3	3	2	1	1

DSCP	60	52	44	36	28	20	12	4
队列	3	3	4	3	3	2	1	1
DSCP	59	51	43	35	27	19	11	3
队列	3	3	4	3	3	2	1	1
DSCP	58	50	42	34	26	18	10	2
队列	3	3	4	3	3	2	1	1
DSCP	57	49	41	33	25	17	9	1
队列	3	3	4	3	3	2	1	1
DSCP	56	48	40	32	24	16	8	0
队列	3	3	4	3	3	2	1	1

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。

配置带宽

使用“带宽”页面，用户可以定义两组值（入口速率限制和出口整形速率）来确定系统可以接收和发送的流量。

入口速率限制是入口接口每秒能够接收的位数。超过此限制的带宽将被丢弃。

为出口整形输入以下值：

- **承诺的信息传输速率 (CIR)** 设置允许在出口接口上发送的平均最大数据量，以“位/秒”为单位
- **承诺突发数据大小 (CBS)**，即允许发送的突发数据量（即使数据量超出 CIR 也会照常发送）。该值以数据字节数定义。

输入带宽限制的步骤：

步骤 1 单击**服务质量 > 一般 > 带宽**。

“带宽”页面会显示每个接口的带宽信息。

% 列为端口带宽除以总端口带宽所得的入口速率限制。

步骤 2 选择一个接口，并单击**编辑**。

步骤 3 选择**端口或LAG**接口。500 系列交换机也有一个可选择单元/端口的选项。

步骤 4 针对选择的接口，为以下字段输入值：

- **入口速率限制** - 选择该选项将启用入口速率限制，该限制在下面的字段中定义。
- **入口速率限制** - 输入接口所允许的最大带宽。

注 当接口类型为 LAG 时，不会显示这两个**入口速率限制**字段。

- **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。
- **出口整形速率** - 选择该选项将在接口上启用出口整形。
注 在以下交换机上，可在“出口整形速率”字段中配置的最小 CIR 为 2Mbps 而非 64Kbps：SF500 端口 GE1—GE4 和 SG500 端口 GE—49-GE52。
- **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。

配置每队列的出口整形

除限制每端口的传输速率（在“带宽”页面中完成）之外，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

注 如果设备在第 3 层模式下，VLAN 速率限制功能将不可用。

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**。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

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。

配置全局设置

“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**，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** 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。
- 传入 DSCP** 会显示需要重新标记为替代值的传入数据包 DSCP 值。
- 步骤 5** 选择**传出 DSCP** 值以指示已映射传出值。
- 步骤 6** 单击**应用**。将使用新 DSCP 值更新当前配置文件。
-

接口 QoS 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

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“超出策略 DSCP 重标记”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 的工作流程”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。

配置全局设置

“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 值将被忽略，所有流量将转到队列 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 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。有关详情，请参阅“DSCP 覆盖表”页面。

配置超出策略 DSCP 重标记

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*。

如果超出限制时执行的操作为“超出模板 DSCP”，设备会根据“超出策略 DSCP 重标记表”，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的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 DSCP 映射表”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 基本模式，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等级：银牌 (Silver)、金牌 (Gold) 和优质 (Premier)，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等级，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 DSCP 映射**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 DSCP 映射**。使用该页面可设置进入或离开设备的流量的更改 DSCP 值。

“传入 DSCP”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**。将使用新 DSCP 映射表更新当前配置文件。

定义类映射

类映射使用 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，称为一个策略（请参阅[配置策略](#)）。

“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**。

此页面会显示已定义的类映射。

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。

QoS 策略器

注 如果 Sx500 设备在第 3 层系统模式，将不支持 QoS 策略器。SG500X 设备始终支持。

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。

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。

定义汇总监察器

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，并且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。

注 只有支持独立第 2 层系统模式的设备在第 2 层模式中操作时，设备才支持集合策略器和单个策略器。

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。可能的值有：
 - **转发** - 转发超出已定义的 CIR 值的数据包。
 - **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 DSCP 映射表”，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。

配置策略

“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**以显示“策略类映射”页面。
-或者
单击**添加**以打开“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**。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。

注 如果设备在第 3 层模式下工作，您将无法为类映射配置策略器。设备仅在第 2 层模式下支持策略器。

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** - 忽略入口 CoS/802.1p 和/或 DSCP 值。将按尽力服务模式发送匹配数据包。
 - **始终信任** - 如果选择了此选项，设备将信任匹配数据包的 CoS/802.1p 和 DSCP。如果为 IP 数据包，设备会根据数据包的 DSCP 值及“DSCP 到队列表”将数据包放入出口队列。否则，将根据数据包的 CoS/802.1p 值及“CoS/802.1p 到队列表”指定数据包的出口队列。

- **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。

- **监察类型** - 仅在第 2 层系统模式下可用。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。
- **集合策略器** - 仅在第 2 层系统模式下可用。如果**监察类型**为**集合**，请选择先前在“集合策略器”页面中定义的集合策略器。

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：
 - **无** - 不执行任何操作。
 - **丢弃** - 丢弃超出已定义的 CIR 值的数据包。
 - **超出模板 DSCP** - 使用从“超出模板 DSCP 映射”中取得的新 DSCP，转发超出已定义的 CIR 的 IP 数据包。

步骤 5 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。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模板，但一个策略可以绑定至多个端口。

将策略绑定至端口后，该策略会过滤入口流量，并将 QoS 应用到属于策略中定义的数据流的入口流量。该策略不会应用到输出到同一端口的流量。

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，选择**策略名称**和**接口类型**。

步骤 3 单击**转至**。将选择策略。

步骤 4 为策略/接口选择以下选项：

- **绑定** - 选择该选项可将策略绑定到接口。
- **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 5 单击**应用**。将定义 QoS 策略绑定，并更新当前配置文件。

管理 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** - 选择类映射名称。

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。
- **模板内的字节数** - 接收到的模板内的数据包数量。
- **模板外的字节数** - 接收到的超出模板的数据包数量。

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。

查看队列统计信息

“队列统计信息”页面会根据接口、队列和丢弃优先级显示队列统计信息，包括已转发和已丢弃的数据包的统计信息。

查看队列统计信息的步骤：

步骤 1 单击**服务质量 > QoS 统计信息 > 队列统计信息**。

此页面显示了以下字段：

- **刷新速率** - 选择刷新接口以太网统计信息的间隔时间。可用选项有：
 - *无刷新* - 不刷新统计信息。
 - *15 秒* - 每隔 15 秒刷新统计信息。
 - *30 秒* - 每隔 30 秒刷新统计信息。
 - *60 秒* - 每隔 60 秒刷新统计信息。
- **计数器设置** - 选项如下：
 - *设置 1* - 显示“设置 1”（包含所有具有高 DP [丢弃优先级] 的接口和队列）的统计信息。
 - *设置 2* - 显示“设置 2”（包含所有具有低 DP 的接口和队列）的统计信息。
- **接口** - 显示此接口的队列统计信息。
- **队列** - 从此队列转发的数据包或丢弃的尾部数据包。
- **丢弃优先级** - 最低的丢弃优先级表示被丢弃的优先级最低。
- **数据包总数** - 被转发的数据包或被丢弃的尾部数据包的数量。
- **丢弃的尾部数据包** - 被丢弃的尾部数据包所占的百分比。

步骤 2 单击**添加**。

步骤 3 输入参数。

- **计数器设置** - 选择计数器集：
 - *设置 1* - 显示“设置 1”（包含所有具有高 DP [丢弃优先级] 的接口和队列）的统计信息。
 - *设置 2* - 显示“设置 2”（包含所有具有低 DP 的接口和队列）的统计信息。

- **接口** - 选择要显示其统计信息的端口。选项如下：
 - *单元编号* - 选择单元编号。
 - *端口* - 选择所选单元号上要显示其统计信息的端口。
 - *全部端口* - 指定将显示所有端口的统计信息。
- **队列** - 选择要显示其统计信息的队列。
- **丢弃优先级** - 输入丢弃优先级，以表示被丢弃的优先级。

步骤 4 单击**应用**。将添加队列统计信息计数器，并更新当前配置文件。

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：

- **SNMP 版本和 workflows**
- **型号 OID**
- **SNMP 引擎 ID**
- **配置 SNMP 视图**
- **创建 SNMP 组**
- **管理 SNMP 用户**
- **定义 SNMP 社区**
- **定义 Trap 设置**
- **通知接收设备**
- **SNMP 通知过滤器**

SNMP 版本和 workflows

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 Trap，将系统事件报告给 Trap 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团的 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 Trap 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。
- **密钥管理** - 定义密钥生成、密钥更新和密钥使用。设备支持基于 *对象 ID* (OID) 的 SNMP 通知过滤器。OID 由系统用来管理设备功能。

SNMP 工作流程

注 出于安全方面的考虑，默认情况下应禁用 SNMP。必须先在“安全 > TCP/UDP 服务”页面打开 SNMP，才能通过 SNMP 管理设备。

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“SNMP -> 社区”页面并单击**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 管理站点限制在一个地址，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“Trap 设置”页面启用 Trap（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“通知接收设备 SNMPv1, 2”页面配置通知接收设备。

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。可创建唯一引擎 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）。这会限制社团或组可用的 OID 范围。
- 步骤 3 使用“组”页面定义组。
- 步骤 4 使用“SNMP 用户”页面定义用户，在该页面中可以将用户与组相关联。如果未设置 SNMP 引擎 ID，那么将无法创建用户。
- 步骤 5 使用“Trap 设置”页面启用或禁用 Trap（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“通知接收设备 SNMPv3”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

以下为设备型号对象 ID(OID)：

型号名称	说明	对象 ID
SF500-24	24 端口 10/100M 可堆叠管理型交换机	9.6.180.24.1
SF500-24P	24 端口 10/100M PoE 可堆叠管理型交换机	9.6.180.24.2
SF500-48	48 端口 10/100M 可堆叠管理型交换机	9.6.180.48.1

型号名称	说明	对象 ID
SF500-48P	48 端口 10/100M PoE 可堆叠管理型交换机	9.6.1.80.48.2
SG500-28	28 端口千兆可堆叠管理型交换机	9.6.1.81.28.1
SG500-28P	28 端口千兆 PoE 可堆叠管理型交换机	9.6.1.81.28.2
SG500-52	52 端口千兆可堆叠管理型交换机	9.6.1.81.52.1
SG500-52P	52 端口千兆 PoE 可堆叠管理型交换机	9.6.1.81.52.2
SG500X-24	24 端口千兆与 4 端口 10 千兆可堆叠管理型交换机	9.6.1.85.24.1
SG500X 24P	24 端口千兆与 4 端口 10 千兆 PoE 可堆叠管理型交换机	9.6.1.85.24.2
SG500X-48	48 端口千兆与 4 端口 10 千兆可堆叠管理型交换机	9.6.1.85.48.1
SG500X-48P	48 端口千兆与 4 端口 10 千兆 PoE 可堆叠管理型交换机	9.6.1.85.48.2
ESW2-550X-48	48 端口千兆与 4 端口 10 千兆可堆叠管理型交换机	9.6.1.86.48.1
ESW2-550X-48DC	48 端口千兆与 4 端口 10 千兆可堆叠管理型交换机	9.6.1.86.48.6
SG500-52MP	52 端口千兆最大 PoE 管理型交换机	9.6.1.81.5.3.0
ESW2-550X-48DC	48 端口千兆与 4 端口 10 千兆可堆叠管理型交换机	9.6.1.86.48.6

专用对象 ID 被置于 enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1).switch001(101) 下面。

SNMP 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（“Ge”、“GetNext”、“GetBulk”、“Set”），并将 Trap 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四个只读 MIB 变量中：snmpEngineId、snmpEngineBoots、snmpEngineTime 和 snmpEngineMaxMessageSize。

**注意**

如果引擎 ID 发生更改，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。

配置 SNMP 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“社团”页面将视图绑定到使用基本访问模式的社团。

定义 SNMP 视图的步骤：

步骤 1 单击 **SNMP > 视图**。

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*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。

可以添加其他视图。

- **对象 ID 子树** - 显示要包括在 SNMP 视图中或要排除在该视图之外的子树。
- **对象 ID 子树视图类型** - 显示是否将已定义的子树包括在所选的 SNMP 视图中或排除在该视图之外。

创建 SNMP 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，但不对其消息加密。
 - **验证和隐私** - 验证 SNMP 消息并对它们加密。
- **视图** - 将视图与组的访问权限（读取、写入和通知）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。
 - **视图** - 针对“读取”、“写入”和“通知”权限选择以前定义的视图。
 - **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 Trap 可用的内容限制在选定视图包含的范围内。否则，将不对 Trap 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。

管理 SNMP 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。此项操作可在“引擎 ID”页面中完成。
- 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**。

此页面包含现有用户。

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 密码 - 通过 MD5 验证方法生成密钥所使用的密码。
 - SHA 密码 - 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**加密模式**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**保存您的设置。

定义 SNMP 社区

SNMPv1 和 SNMPv2 中的访问权限通过在“社团”页面中定义社团进行管理。社区名称是在 SNMP 管理站点和设备之间共享的一种密码。该名称用于验证 SNMP 管理站点。

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“社团”页面可以将社团与访问权限相关联，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，还可以将社团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“SNMP 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。

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 管理站点** - 单击**用户定义**，输入可以访问 SNMP 社区的管理站点 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 管理站点 IP 地址。
- **社区字符串** - 输入用于验证设备管理站点的社区名称。
- **基本** - 为所选社区选择此模式。在此模式下，不存在到任何组的连接。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）。
- **高级** - 为选定的社区选择此模式。
 - **组名称** - 选择确定访问权限的 SNMP 组。

步骤 4 单击**应用**。将定义 SNMP 社区，并更新当前配置文件。

定义 Trap 设置

使用“Trap 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“通知接收设备 SNMPv1, 2”页面或“通知接收设备 SNMPv3”页面中配置 SNMP 通知的接收设备。

定义 Trap 设置的步骤：

步骤 1 单击 **SNMP > Trap 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 Trap 设置将写入当前配置文件。

通知接收设备

系统会生成 Trap 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 Trap。

Trap 接收器（亦称通知接收设备）是接收设备发送的 Trap 消息的网络节点。系统会定义一系列通知接收设备作为 Trap 消息的接收设备。

Trap 接收器条目中包含的节点 IP 地址和 SNMP 凭证与 Trap 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 Trap 消息的事件时，系统会将 Trap 消息发送到通知接收设备表上所列的每个节点。

使用“通知接收设备 SNMPv1, 2”页面和“通知接收设备 SNMPv3”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（Trap 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 管理站点发送的消息，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”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，过滤发送到管理站点的 SNMP 通知的类型。

定义 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。
- **Trap IPv4 源接口** - 选择其 IPv6 地址将用作与 IPv6 SNMP 服务器通信中 Trap 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。
- **Trap IPv6 源接口** - 选择其 IPv6 地址将用作与 IPv6 SNMP 服务器通信中 Trap 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 Trap 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 Trap 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 Trap 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 Trap SNMP 版本。SNMPv1 和 SNMPv2 均可作为 Trap 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站点的 SNMP 通知类型。过滤器在“通知过滤”页面中创建。
- **过滤条目名称** - 选择定义 Trap 中包含的信息的 SNMP 过滤器（在“通知过滤”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。

定义 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。
- **Trap IPv4 源接口** - 选择其 IPv6 地址将用作与 IPv6 SNMP 服务器通信中 Trap 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。
- **Trap IPv6 源接口** - 选择其 IPv6 地址将用作与 IPv6 SNMP 服务器通信中 Trap 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 Trap 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 Trap 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/Trap 之前，设备等待的时间（以秒为单位）。超时范围：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: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“SNMP 用户”页面定义该用户，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** - 表示既要验证数据包，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站点的 SNMP 通知类型。过滤器在“通知过滤”页面中创建。

- **过滤条目名称** - 选择定义 Trap 中包含的信息的 SNMP 过滤器（在“通知过滤”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。

SNMP 通知过滤器

使用“通知过滤”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，可以在“通知接收设备 SNMPv1, 2”页面和“通知接收设备 SNMPv3”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，过滤发送到管理站点的 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**。

“通知过滤”页面包含每个过滤的通知信息。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。
 - 如果使用**对象 ID**，则是否将**输入的对象标识符**包括在视图将取决于是否选择**包含在过滤中**选项。

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**。将定义 SNMP 视图，并更新当前配置文件。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的注册商标。若要查看思科的商标列表，请访问此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有人的财产。使用“合作伙伴”一词并不暗示思科和任何其他公司之间存在合作关系。(1110R)

颜色：500、300 和 500

Sx500 和 SG500X 印刷版本管理指南的载体文件

条件标签

文件中定义了以下条件标签：

条件标签名称			说明
备注	断开		用于内部编辑问题 / 备注
内部	断开		为开发者目的不显示给客户的内部信息
OnLineHelp	断开		适用于所有模式 + 在线帮助版本
印刷文档	接通	■	适用于所有模式 + 印刷版本
Sx200	断开		适用于 Sx200 印刷和帮助版本
Sx200_Help	断开		适用于 Sx200 帮助版本
Sx200_Print	断开		适用于 Sx200 印刷版本
Sx300	断开		适用于 Sx300 印刷和帮助版本
Sx300_Help	断开		适用于 Sx300 帮助版本
Sx300_Print	断开		适用于 Sx300 印刷版本
Sx500	接通	■	适用于 Sx500 印刷和帮助版本
Sx500_Help	断开		适用于 Sx500 帮助版本
Sx500_Print	接通	■	适用于 Sx500 印刷版本

颜色：500、300 和 500

文件中定义变量的列表

变量名称	
	说明
书名	思科 500 系列可堆叠管理型交换机管理指南
版权	版权所有 © 2012-2013
defaultusername	cisco
defaultpassword	cisco
接口	基于 Web 的交换机配置实用程序
产品系列	思科 Small Business
版本	78-21349-01