用户手册

思科 220 系列智能增强型交换机用户手册
1.0.0.x

OL-30455-01

目　录

Chapter 1: 入门 11

使用基于 Web 的管理界面 11

配置前准备 11

登录基于 Web 的管理界面 12

HTTP/HTTPS 13

修改管理密码 13

注销登录 14

交换机配置快速导航 15

接口命名约定 16

窗口导航 17

应用报头 17

管理按钮 18

Chapter 2: 状态和统计信息 20

查看以太网接口信息 20

查看 Etherlike 统计信息 22

查看 TCAM 利用率 23

查看风扇状态和温度 23

管理 RMON 25

查看 RMON 统计信息 25

设置和查看 RMON 历史 27

设置 RMON 历史控制样本 27

查看 RMON 历史统计信息 28

设置和查看 RMON 事件 29

设置 RMON 事件 29

查看 RMON 事件日志 30

设置 RMON 告警 30

Chapter 3: 管理 : 系统日志 32

系统日志设置 32

设置远程日志服务器 33

查看日志 34

查看 RAM 日志 34
查看闪存日志 35

Chapter 4: 管理 : 系统文件 36

文件和文件类型 36
文件操作 38
升级或备份固件 / 语言 38
升级 / 备份固件映像 39
升级语言文件 40
活动映像 41
下载或备份配置或日志 41
导入配置文件 42
备份配置文件或日志 43
配置文件属性 44
复制或保存配置 44
DHCP 自动配置 45
DHCP 服务器选项 46
自动配置过程 46
设置 DHCP 自动配置参数 46

Chapter 5: 管理 : 系统参数 48

设备型号 48
查看系统摘要 50
定义系统设置 52
设置控制台波特率 53
重新启动交换机 53
设置闲置会话超时 54
Ping 主机 55
Traceroute 55

Chapter 6: 管理 : 系统时间 57

系统时间选项 57
设置系统时间 58
设置 SNTP 服务器 60

Chapter 7: 管理 : 设备诊断 61

测试铜质端口 61
查看光模块状态 62
设置端口和 VLAN 镜像 63
查看 CPU 使用率 65

Chapter 8: 管理 : 设备发现 66

设置 Bonjour 66
关于 LLDP 和 CDP 67
设置 LLDP 68
设置 LLDP 属性 69
定义 LLDP 端口设置 70
设置 LLDP MED 网络策略 71
LLDP MED 端口设置 72
查看 LLDP 端口状态 73
查看 LLDP 本地信息 74
查看 LLDP 邻居信息 77
查看 LLDP 统计信息 77
查看 LLDP 过载信息 78
设置 CDP 80
设置 CDP 属性 80
定义 CDP 端口设置 81
查看 CDP 本地信息 82
查看 CDP 邻居信息 84
查看 CDP 统计信息 85

Chapter 9: 端口管理 87

端口管理工作流程 87
设置端口基本配置 88
设置错误恢复配置 90
设置链路聚合 91
负载均衡 91
LAG 管理 92
静态和动态 LAG 配置流程 92
设置 LAG 算法 93
定义 LAG 设置 94
设置 LACP 95
LACP 优先级和规则 95
无链路伙伴的 LACP 96
设置 LACP 参数 96
设置节能以太网 97

Chapter 10: 设置以太网供电 98

PoE 特性 98
交换机上的 PoE 100
PoE 功能 100
PoE 工作模式 100
PoE 配置注意事项 101
设置 PoE 属性 101
定义 PoE 端口设置 103

Chapter 11: 设置 VLAN 105

VLAN 105
VLAN 说明 105
VLAN 角色 106
设置 VLAN 工作流程 107
设置默认 VLAN 107
创建 VLAN 108

定义接口 VLAN 配置 109
设置端口到 VLAN 110
设置 VLAN 成员关系 111
设置 GVRP 113
设置语音 VLAN 114
动态语音 VLAN 模式 114
语音 VLAN 限制 114
语音 VLAN 选项 115
设置语音 VLAN 属性 115
设置电话 OUI 116
设置电话 OUI 接口 117

Chapter 12: 设置生成树协议 119

STP 模式 119
定义 STP 状态和全局设置 120
定义 STP 接口设置 121
定义 RSTP 接口设置 122
设置 MSTP 124
设置 MSTP 属性 125
映射 VLAN 到 MSTP 实例 125
设置 MSTP 实例 126
设置 MSTP 接口配置 127

Chapter 13: 管理 MAC 地址表 129

MAC 地址类型 129
设置静态 MAC 地址 130
设置静态 MAC 地址过滤 130
设置动态 MAC 地址过期时间 131
查询动态 MAC 地址 131
设置保留的 MAC 地址 132

Chapter 14: 设置组播转发 133

组播转发 133

典型的组播设置 134

组播注册 134

组播地址属性 135

设置组播属性 136

设置 IP 组播组地址 136

设置 IGMP 侦听 137

设置 MLD 侦听 139

查询 IGMP/MLD IP 组播组 141

设置组播路由器端口 142

设置全部转发端口 142

设置最大 IGMP/MLD 组播组 143

设置组播过滤 144

设置组播过滤模板 144

设置接口组播过滤 144

Chapter 15: 配置 IP 信息 146

IP 寻址 146

设置 IPv4 管理接口 147

设置 IPv6 管理接口 148

设置域名系统 149

定义 DNS 设置 149

搜素 DNS 列表 150

映射 DNS 主机 151

Chapter 16: 设置安全性 152

设置用户帐号 153

设置 TACACS+ 服务器 154

设置 RADIUS 服务器 155

管理访问方法 157
访问模板规则、过滤器和元素 157
活动的访问模板 158
设置访问模板 158
设置访问规则 160
设置密码强度规则 161
管理访问验证 163
设置 TCP/UDP 服务 164
设置风暴控制 165
设置端口安全性 166
设置 802.1X 168
访客 VLAN 168
802.1X 工作流程 169
设置 802.1X 属性 169
设置 802.1X 端口验证 170
查看已验证的主机 171
设置 DoS 防护 171
安全核心技术 (SCT) 172
默认设置 172
定义拒绝服务安全套件设置 172
定义 DoS 接口设置 174
设置 SYN 保护 174
设置 DHCP 侦听 176
设置 DHCP 侦听属性 176
定义 DHCP 侦听 VLAN 设置 177
设置 DHCP 侦听信任接口 177
查询 DHCP 侦听绑定数据库 178
查看 Option 82 统计信息 179
定义 Option 82 接口设置 179
定义 Option 82 接口 CID 设置 180
设置 IP 源防护 180

定义 IP 源防护接口设置 181
查询 IP 源绑定数据库 181
设置动态 ARP 检测 182
ARP 缓存污染 182
ARP 如何预防缓存污染 183
ARP 检测与 DHCP 侦听之间的交互 184
ARP 检测工作流程 185
设置 ARP 检测属性 185
设置 ARP 检测信任接口 186
查看 ARP 检测统计信息 186
应用 ARP 检测到 VLAN 187

Chapter 17: 设置访问控制 188

访问控制列表 188
创建 ACL 工作流程 190
修改 ACL 工作流程 190
设置基于 MAC 的 ACL 191
设置基于 MAC 的 ACE 191
设置基于 IPv4 的 ACL 192
设置基于 IPv4 的 ACE 193
设置基于 IPv6 的 ACL 196
设置基于 IPv6 的 ACE 197
设置 ACL 绑定 199

Chapter 18: 设置服务质量 201

QoS 功能和组件 201
设置 QoS 的工作流程 203
设置 QoS 属性 204
设置 QoS 队列 204
映射 CoS/802.1P 到队列 206
映射 IP 优先权到队列 207

映射 DSCP 到队列 207
映射队列到 CoS/802.1p 208
映射队列到 IP 优先权 208
映射队列到 DSCP 209
设置接口重新标记 209
设置带宽限制 210
设置每队列出口整形 210
设置 VLAN 入口速率限制 211
设置 VLAN 端口入口速率限制 212
设置 TCP 拥塞避免算法 212
设置 QoS 基本模式 213
设置基本 QoS 信任模式 213
设置接口 QoS 功能 214
设置 QoS 高级模式 214
设置高级 QoS 信任模式 216
设置类映射 217
QoS 策略 218
设置集合策略器 218
设置 QoS 策略 219
设置策略类映射 220
设置策略绑定 221

Chapter 19: 设置 SNMP 222

SNMP 版本和工作流程 222
SNMPv1 和 v2 222
SNMPv3 223
SNMP 工作流程 223
支持的 MIB 224
对象 ID 225
设置 SNMP 引擎 ID 226
设置 SNMP 视图 227

设置 SNMP 组 228
设置 SNMP 用户 229
设置 SNMP 社团 230
设置 SNMP 通知接收设备 231
设置 SNMPv1,2 通知接收设备 232
设置 SNMPv3 通知接收设备 233

Appendix A: 快速索引 **234**

1

入门

本章介绍思科 220 交换机的基于 Web 的管理界面的相关信息，包括以下内容：

- 使用基于 **Web** 的管理界面
- 交换机配置快速导航
- 接口命名约定
- 窗口导航

使用基于 **Web** 的管理界面

您可以通过以下两种方式访问和管理思科 220 智能增强型交换机：

- 通过您的 IP 网络使用基于 Web 的管理界面访问和管理交换机
- 通过控制台端口连接使用命令行接口访问和管理交换机

其中，使用控制台端口需要用户具备高级技能。有关如何使用控制台端口连接和管理交换机的详细信息，请参考 《思科 220 系列智能增强型交换机命令行接口参考手册》。

配置前准备

使用基于 Web 的管理界面之前请确保您的计算机安装有 Internet Explorer 8.0 （或更高版本）、 Firefox 20.0 （或更高版本）、 Chrome 23.0 （或更高版本）或 Safari 5.7 （或更高版本）。

首次登录交换机时，可使用以下出厂默认设置：

参数	默认值
用户名	**cisco**
密码	**cisco**

参数	默认值
交换机 IP	**192.168.1.254**

登录基于 Web 的管理界面

如需访问交换机的基于 Web 的管理界面，您必须知道交换机当前所用的 IP 地址。默认情况下，在交换机自动从 DHCP 服务器获取一个 IP 地址之前，交换机将使用其出厂默认的 IP 地址 **192.168.1.254**。

注释 如果您当前通过网络连接管理交换机且交换机的 IP 地址发生了变化 （如 DHCP 服务器重新分配了一个新的 IP 地址或您手动修改了交换机的 IP 地址），您对交换机的访问将断开。您必须在浏览器中输入新的交换机 IP 地址重新登录基于 Web 的管理界面。如果您当前通过控制台端口连接和管理交换机，此连接链路将被保留。

使用基于 Web 的管理界面设置交换机的步骤：

步骤 **1** 接通计算机和交换机的电源。

步骤 **2** 将计算机连接至交换机。

使用以太网电缆直接连接计算机和交换机或通过其他交换机连接至交换机所处的同一 LAN，即可连接至交换机子网相同的 IP 子网。您还可以通过一个或多个 IP 路由器将计算机连接至其他 IP 子网的交换机。

步骤 **3** 确定交换机的 IP 地址。

a. 通过思科网络工具和服务 （包括思科 FindIT Network Discovery Utility）可访问和管理思科 220 交换机。思科 FindIT Network Discovery Utility 可自动发现所有与您的 PC 相同网段内的思科设备。您可以获得每一台设备的快照视图，也可以启动产品配置工具查看和设置相关参数。更多关于思科 FindIT 的信息，请访问 www.cisco.com/go/findit。

b. 访问您的路由器或者 DHCP 服务器并查看由 DHCP 服务器分配给交换机的 IP 地址。详情请参考您的 DHCP 服务器的操作指南。请确保您的 DHCP 服务器正在运行且可访问。

步骤 **4** 设置您计算机上的 IP 配置。

- 如果交换机使用出厂默认 IP 地址 **192.168.1.254**，则您必须在尚未使用的 IP 地址范围 192.168.1.2-192.168.1.253 内选择一个 IP 地址。
- 如果 IP 地址由 DHCP 服务器自动分配，请确保您的 DHCP 服务器正在运行并且可以通过交换机和计算机进行访问。您可能需要先断开设备连接，再重新连接设备，以便设备可以搜索到来自 DHCP 服务器的新 IP 地址。

注释 有关如何变更计算上 IP 地址的详细信息，取决于您正在使用的架构和操作系统的类型。使用计算机的本机帮助和支持功能，并搜索 IP 寻址。

步骤 5 打开一个浏览器窗口。如果在连接至交换机时系统提示您安装 Active-X 插件，请按照提示接受该插件。

步骤 6 在地址栏中输入交换机的 IP 地址，然后按 **Enter** 键。例如 **http://192.168.1.254**。

步骤 7 在打开的登录界面中，选择基于 Web 的管理界面使用的语言版本，然后输入用户名和密码。

默认的用户名为 **cisco**。默认的密码为 **cisco**。用户名和密码均区分大小写。

步骤 8 点击 “**登录**”。

如果这是您第一次使用默认用户名和密码登录，系统自动显示 “更改密码”页面，提示您修改默认的管理密码。为了更好地保护您的网络，请更改默认的管理员密码。

HTTP/HTTPS

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

注释 在单击 “安全浏览 （**HTTPS**）”前，您无需输入用户名和密码。

修改管理密码

出于安全考虑，首次登录交换机或者交换机当前的管理密码过期时，您需要修改交换机的管理密码。

交换机默认启用密码强度检测机制。“更改密码”页面上显示了用于构建新密码的最低复杂性要求。新密码必须符合默认的密码复杂性要求。您也可以通过选择 “禁用密码强度规则”选项来临时禁用密码强度检测机制。有关密码强度设置的详细信息，请参考 “设置密码强度规则”一节。

修改管理密码的步骤：

步骤 1 在 “新密码设置”区域，设定以下参数：

- 旧密码 — 输入当前管理密码 （默认为 **cisco**）。
- 密码 — 输入一个新密码。
- 确认密码 — 再次输入新密码。

- 密码强度计 — 显示新密码的复杂性强度。
- 禁用密码强度规则 — 启用密码强度规则（默认为启用）要求新的管理密码必须符合以下密码复杂性要求：
  - 不可与当前用户名相同
  - 最少 8 个字符长度
  - 包含最少 3 种字符类别（可用的字符类别包括大写字母、小写字母、数字和标准键盘上的特殊字符）

注释 如果暂时不想修改管理密码，请勾选 “禁用密码强度规则”选项然后单击 “应用”。

步骤 2 单击 “应用”。

此时，系统显示 “使用入门”页面。您可以开始配置交换机。

步骤 3 勾选 “启动时不显示此页面”选项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，下次登录系统时，将打开 “系统摘要”页面而不是 “使用入门”页面。

注销登录

默认情况下，如果您在十分钟内没有任何操作，将会注销您的登录。您可以按照 “设置闲置会话超时”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，否则自上次保存文件以来所做的所有更改将会在交换机重新启动后全部丢失。建议在注销前先将当前配置保存到启动配置，以保留在该会话期间所做的一切更改。

显示在 “保存”应用程序链接左侧的红色 **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。

当交换机自动发现了一台设备时 （如 IP 电话），交换机会自动为此设备配置端口。这些配置命令都会被写入交换机的当前配置。因此，当用户登录交换机后，尽管此时用户没有执行任何配置修改，此操作也会导致 “保存”应用程序链接开始闪烁。

单击 “保存”会打开 “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。

要注销登录，只需单击任意页面右上角的 “退出”，系统便会注销登录。

如果发生超时或者您故意注销系统，系统会显示一则告警消息并且打开登录页面，其中显示一则消息，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。

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

交换机配置快速导航

为通过快速导航简化交换机配置，“使用入门”页面提供了以下常用页面的链接：

类别	链接名称	链接的页面
初始设置	更改管理应用和服务	“安全” > “TCP/UDP 服务”页面
	更改设备 IP 地址	“管理” > “管理接口” > “IPv4 接口”页面
	创建 VLAN	“VLAN 管理” > “创建 VLAN”页面
	配置端口设置	“端口管理” > “端口设置”页面
设备状态	系统摘要	“状态和统计信息” > “系统摘要”页面
	端口统计信息	“状态和统计信息” > “接口”页面
	RMON 统计信息	“状态和统计信息” > “RMON” > “统计信息”页面
	查看日志	“状态和统计信息” > “查看日志” > “RAM”页面

类别	链接名称	链接的页面
快速访问	更改设备密码	“管理” > “用户帐号”页面
	升级设备软件	“管理” > “文件管理” > “升级 / 备份固件 / 语言”页面
	备份设备配置	“管理” > “文件管理” > “下载 / 备份配置 / 日志”页面
	创建基于 MAC 的 ACL	“访问控制” > “基于 MAC 的 ACL”页面
	创建基于 IP 的 ACL	“访问控制” > “基于 IPv4 的 ACL”页面
	配置 QoS	“服务质量” > “一般” > “QoS 属性”页面
	配置端口镜像	“管理” > “诊断” > “端口和 VLAN 镜像”页面

“使用入门”页面提供了两个热链接，帮助您访问指定的思科网站获取更多信息。单击 “支持”链接，您将访问交换机的产品主页，了解最新的产品信息；单击 “论坛”链接，您将访问思科技术支持社区页面。

接口命名约定

在基于 Web 的管理界面中，系统根据以下几个要素来表示接口：

- 接口类型 — 以下类型的接口在不同型号的交换机上有提供：
  - 快速以太网 （**10/100** 位） — 这种类型的接口显示为 **FE**。
  - 千兆以太网 （**10/100/1000** 位） — 这种类型的接口显示为 **GE**。
  - **LAG** （端口通道） — 这种类型的接口显示为 **LAG**。
  - **VLAN**— 这种类型的接口显示为 **VLAN**。
  - 隧道 — 这种类型的接口显示为隧道。
- 接口编号 — 端口、 LAG、隧道或 VLAN ID。

窗口导航

本节介绍基于 Web 的管理界面的基本特性。

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
警报	如果系统记录了高于严重级别的系统日志消息，则会显示“警报”图标。单击此图标可打开 “RAM”页面。访问此页面后，将不会再显示 “警报”图标。要在没有活动的系统日志消息的情况下显示此页面，请单击 “状态和统计信息” > “查看日志” > “RAM”。
保存	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”可打开 “复制 / 保存配置”页面。在交换机上，通过将当前配置文件复制到启动配置文件来保存该文件。保存后，将不再显示红色 **X** 图标和 “保存”应用程序链接。交换机重启时，会将启动配置文件复制到当前配置，并根据当前配置文件中的数据设置交换机参数。
用户名	显示登录到交换机的用户名。默认的用户名为 **cisco** （默认的密码为 **cisco**）。
语言菜单	此菜单提供以下选项： ▪ 选择语言 — 从菜单下拉框所显示的语言中选择一种语言，基于 Web 的管理界面将切换到选中的语言版本。 ▪ 下载语言 — 上传新的语言文件到交换机。使用“升级 / 备份固件 / 语言”页面可上传或更新一个语言文件。 ▪ 删除语言 — 删除交换机上的备选语言。主选语言（英文）不能被删除。
退出	单击此按钮可注销登录。

应用程序链接名称	说明
关于	单击此按钮可显示交换机名称和软件版本。
帮助	单击此按钮可打开在线帮助文件。

管理按钮

下表介绍各页面上显示的常用按钮，包括：

按钮名称	说明
添加	单击此按钮会打开相关的添加页面并在添加一个条目。输入信息并单击 “应用”，可将所有更改保存到当前配置中 。单击 “关闭”可返回主页面。单击 “保存”会打开 “复制 / 保存配置”页面，并在交换机上将当前配置保存到启动配置文件。
应用	单击此按钮将配置更改保存到交换机上的当前配置。除非将当前配置保存到启动配置文件类型或其他文件类型 ，否则当交换机重启时，当前配置会丢失。单击 “保存”打开 “复制 / 保存配置”页面，并在交换机上将当前配置保存到启动配置文件。
取消	单击此按钮会重置对页面所做的更改。
清除所有接口的计数器	单击此按钮会清除所有接口的计数器。
清除接口计数器	单击此按钮会清除所选接口的计数器。
清除日志	单击此按钮会清除日志文件。
清除表	单击此按钮会清除表格条目。
关闭	关闭当前页面或窗口并返回到主页面。如果所有更改均未应用到当前配置，将显示一条提示消息。
铜缆测试	单击此按钮执行相关测试。

按钮名称	说明
复制配置	一个表格中通常会包含一个或多个包含配置条目。当某一配置可应用到多个条目时，为简化配置，您无需单独修改每一个条目，而是可以先修改其中一个条目，然后再将所选条目的配置复制到多个条目。方法如下： 1. 选择要复制的条目，然后单击 “复制配置”。 2. 在 “至”字段中输入目的条目编号。 3. 单击 “应用”，将所选条目的配置复制到目的条目。 4. 单击 “关闭”，返回到主页面。
删除	在表格中选择一个条目后，单击此按钮可删除此条目。
详情	单击此按钮可显示所选条目的详细信息。
编辑	选择一个条目然后单击此按钮，可打开编辑页面，并对相关参数进行修改。 1. 参数设置完毕后，单击 “应用”可将更改保存到当前配置文件。 2. 单击 “关闭”，返回到主页面。
确定	输入查询条件并单击此按钮，查询结果显示在页面上。
刷新	单击此按钮可手动刷新页面数据。
查看所有接口统计信息	单击此按钮可在单个页面上查看所有接口的计数器。
查看接口统计信息	单击此按钮可查看所选接口的计数器。

2

状态和统计信息

本章介绍如何查看交换机的状态和统计信息，包括以下内容：

- 查看以太网接口信息
- 查看 **Etherlike** 统计信息
- 查看 **TCAM** 利用率
- 查看风扇状态和温度
- 管理 **RMON**

查看以太网接口信息

“接口”页面显示每个端口的流量统计信息。您可以选择此页面的刷新频率。

通过此页面，您可以分析每个端口或所有端口发送和接收的流量数量及其传播方式（单播、组播和广播）。

查看接口统计信息和 / 或设置刷新频率的步骤：

步骤 **1** 单击 “状态和统计信息” > “接口”。

步骤 **2** 设定以下参数：

- 接口 — 选择要显示统计信息的端口或 LAG。
- 刷新速率 — 选择刷新统计信息的间隔时间。可选项如下：
  - *不刷新* — 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。

在 “接收统计信息”区域，显示接口接收的数据包的相关信息。

- 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。

在 “传输统计信息”区域，显示接口发送的数据包的相关信息。

- 字节总数 （八位字节）— 发送的八位字节数，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 — 发送的正常单播数据包数。
- 组播数据包数 — 发送的正常组播数据包数。
- 广播数据包数 — 发送的正常广播数据包数。

步骤 3 单击 “清除接口计数器”，清除所选接口的计数器。

步骤 4 单击 “刷新”，手动刷新所选接口的计数器。

步骤 5 单击 “查看所有接口统计信息”，可在单一页面查看全部接口的计数器。在此页面您还可以执行以下操作：

- 从 “刷新速率”下拉框中选择页面的刷新频率。
- 选择一个接口然后单击 “清除接口计数器”，清除所选接口的统计信息。
- 单击 “清除所有接口的计数器”，清除全部接口的统计信息。
- 选择一个接口然后单击 “查看接口统计信息”，在单个页面查看所选接口的统计信息。
- 单击 “刷新”，手动刷新全部接口的统计信息。

查看 Etherlike 统计信息

“Etherlike”页面根据 Etherlike MIB 标准定义显示每个接口的统计信息。您可以选择此页面的刷新频率。

此页面提供关于物理层 （第 1 层）中错误 （可能中断流量）的详细信息。

查看 Etherlike 统计信息和 / 或设置刷新频率的步骤：

步骤 1 单击 “状态和统计信息” > “**Etherlike**”。

步骤 2 设定以下参数：

- 接口 — 选择要显示 Etherlike 统计信息的端口或 LAG。
- 刷新速率 — 选择刷新 Etherlike 统计信息的间隔时间。

此页面显示以下信息：

- 帧检查序列 **(FCS)** 错误数 — 接收到的未能通过循环冗余校验 （Cyclic Redundancy Checks， CRC）的帧。
- 单个冲突帧数 — 出现单个冲突但成功传输的帧数。
- 滞后冲突数 — 在数据的前 512 位后检测到的冲突。
- 过量冲突数 — 由于过量冲突而引起的传输数。
- 过大数据包数 — 接收到的大于 1518 八位字节的数据包数。
- 内部 **MAC** 接收错误数 — 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。
- 已传输的暂停帧数 — 从选定接口传输的流控制暂停帧数。

步骤 3 单击 “清除接口计数器”，清除所选接口的 Etherlike 统计信息。

步骤 4 单击 “刷新”，手动刷新所选接口的 Etherlike 统计信息。

步骤 5 单击 “查看所有接口统计信息”，可在单一页面查看全部接口的 Etherlike 统计信息。在此页面您还可以执行以下操作：

- 从 “刷新速率”下拉框中选择页面的刷新频率。
- 选择一个接口然后单击 “清除接口计数器”，清除所选接口的 Etherlike 统计信息。
- 单击 “清除所有接口的计数器”，清除全部接口的 Etherlike 统计信息。

- 选择一个接口然后单击 “查看接口统计信息”，在单个页面查看所选接口的 Etherlike 统计信息。
- 单击 “刷新”，手动刷新全部接口的 Etherlike 统计信息。

查看 TCAM 利用率

思科 220 交换机架构使用三态内容寻址存储器 （Ternary Content Addressable Memory，TCAM）以支持线速数据包操作。TCAM 可存放由 ACL 和 QoS 应用生成的规则以及系统创建的规则。

只有系统应用会根据交换机启动初始化过程来分配规则。

如需查看 TCAM 利用率，单击 “状态和统计信息” > “**TCAM** 利用率”。

此页面显示以下信息：

- 最大 **TCAM** 条目数 — 可用的最大 TCAM 条目数。
- 使用中 — 正在使用的 TCAM 条目数。

查看风扇状态和温度

“风扇和温度状态”页面显示支持 PoE 功能的交换机的风扇运行状态和温度情况。

下表列出了不同型号的 PoE 交换机所支持的风扇通道和温度监控通道的数量：

型号	风扇通道数	温度监控通道数
SF220-24P	2	2
SF220-48P	4	2
SG220-26P	2	2
SG220-28MP	3	2
SG220-50P	4	2

如需查看交换机的风扇和温度状态，单击 “状态和统计信息” > “风扇和温度状态”。

此页面显示以下信息：

- 风扇 ***x*** 状态 — 显示交换机各个风扇的运行状态，其中：
  - *运行状态* — 交换机风扇运行良好显示为 “正常”，交换机风扇运行不正常显示为 “错误”。
  - *转速值* — 显示交换机风扇的转速。单位为每分钟转速 （RPM）。
- 温度监控 ***x*** 状态 — 显示交换机各个温度监控通道的运行状态，其中：
  - *运行状态* — 温度监控模块运行良好显示为 “正常”，温度监控模块运行不正常显示为 “错误”。
  - *温度值* — 显示交换机当前的温度值。
  - *温度状态* — 显示交换机当前温度状态。

    绿色 — 表示温度监控模块的温度低于黄色预警阈值。

    黄色 — 表示温度监控模块的温度介于黄色和红色预警阈值之间。

    红色 — 表示温度监控模块的温度高于红色预警阈值。
  - *黄色阈值* — 温度监控模块的温度状态显示为黄色时的临界值。
  - *红色阈值* — 温度监控模块的温度状态显示为红色时的临界值。

下表列出了不同型号的 PoE 交换机不同温度监控模块所支持的黄色阈值和红色阈值：

型号	温度监控模块 1 的黄色阈值	温度监控模块 1 的红色阈值	温度监控模块 2 的黄色阈值	温度监控模块 2 的红色阈值
SF220-24P	129°F (54°C)	138°F (59°C)	131°F (55°C)	140°F (60°C)
SF220-48P	118°F (48°C)	129°F (54°C)	120°F (49°C)	131°F (55°C)
SG220-26P	126°F (52°C)	133°F (56°C)	136°F (58°C)	144°F (62°C)
SG220-28MP	118°F (48°C)	129°F (54°C)	120°F (49°C)	131°F (55°C)
SG220-50P	124°F (51°C)	135°F (57°C)	122°F (50°C)	131°F (55°C)

管理 RMON

远程网络监控（Remote Network Monitoring， RMON）是一项 SNMP 规范，使交换机中的 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 代理会比较实际的实时计数器与预定义的阈值并生成告警，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，那么这会是一种非常有效的前瞻性管理机制。

因为 SNMP 管理器不必频繁地轮询交换机来获得信息，因此 RMON 会降低管理器与交换机之间的流量。因为交换机会在事件发生时进行报告， RMON 还能使管理器及时地获得状态报告。

通过 RMON 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定时间内的值，然后查看收集的数据的表格。每一个收集的数据集都是 “历史表”中的一个条目。
- 对计数器值定义有意义的更改。例如，当滞后冲突达到一定数量 （定义告警）时，然后指定发生该事件后应执行什么操作，如记录日志、发送 Trap、记录日志并发送 Trap 等。

注释 在使用 RMON 功能前，请确保您的交换机已经启用了 SNMP 服务。您可以在 “安全” > “TCP/UDP 服务”页面启用此服务 （详见 “设置 **TCP/UDP** 服务”）。

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一些信息。显示的信息基于 RMON 标准。过大数据包被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
- 未检测到冲突事件
- 未检测到延时冲突事件
- 未检测到接收错误事件
- 数据包具有有效的 CRC

查看 RMON 统计信息和 / 或设置刷新频率的步骤：

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

步骤 2 设定以下参数：

- 接口 — 选择要显示 RMON 统计信息的端口或 LAG。
- 刷新速率 — 选择 RMON 统计信息的刷新频率。

此页面显示以下信息：

- **RMON** 已接收的字节数 （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。
- **RMON** 丢弃事件 — 删除的数据包数。
- **RMON** 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。
- 已接收的 **RMON** 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 **RMON** 组播数据包数 — 接收到的正常组播数据包数。
- **RMON CRC** 和 **Align** 错误数 — 发生的 CRC 和 Align 错误数。
- **RMON** 过小数据包数 — 接收的小于 64 八位字节的数据包数。
- **RMON** 过大数据包数 — 接收的大于 1518 八位字节的数据包数。
- **RMON** 分片数 — 接收的分片数。分片是指小于 64 八位字节的数据包，不包括帧位，但包括 FCS 八位字节。
- **RMON** 超时发送帧数 — 接收的大于 1632 八位字节的数据包数。该数值不包括帧位，但包括具有整数数量八位字节 （FCS 错误）的坏 FCS （帧校验序列）或者具有非整数八位字节 （校正误差）的坏 FCS 的 FCS 八位字节数。超时发送帧数据包被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
  - 未检测到接收错误事件
- **RMON** 冲突数 — 接收的冲突数。如果启用了巨型帧，巨型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 至 127 字节的帧数。
- **128** 至 **255** 字节的帧数 — 接收的包含 128 至 255 字节的帧数。
- **256** 至 **511** 字节的帧数 — 接收的包含 256 至 511 字节的帧数。
- **512** 至 **1023** 字节的帧数 — 接收的包含 512 至 1023 字节的帧数。

- 大于等于 **1024** 字节的帧数 — 接收的包含 1024 至 2000 字节的帧数以及巨型帧数 。

步骤 **3** 单击 “清除接口计数器”，清除所选接口的 RMON 统计信息。

步骤 **4** 单击 “刷新”，手动刷新所选接口的 RMON 统计信息。

步骤 **5** 单击 “查看所有接口统计信息”，可在单一页面上查看交换机所有接口的 RMON 统计信息。在此页面您还可以执行以下操作：

- 从 “刷新速率”下拉框中选择页面数据的刷新频率。
- 选择单个接口然后单击 “清除接口计数器”，清除所选接口的 RMON 统计信息。
- 单击 “清除所有接口的计数器”，清除全部接口的 RMON 统计信息。
- 选择单个接口然后单击 “查看接口统计信息”，在单一页面查看所选接口的 RMON 统计信息。
- 单击 “刷新”，手动刷新所有接口的 RMON 统计信息。

设置和查看 RMON 历史

RMON 可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接口。数据经过取样和存储后，将显示在 “历史表”页面中。用户可单击 “历史表”进行查看。

设置 RMON 历史控制样本

设置 RMON 历史控制样本的步骤：

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

根据标准， RMON 不会授予给所有请求的样本，而是限制每个请求的样本数。“当前样本数”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”，添加 RMON 历史控制样本。

步骤 **3** 设定以下参数：

- 新历史条目 — 显示 RMON 历史条目编号。
- 源接口 — 选择捕获历史记录样本的端口或 LAG。
- 可保存的最大样本数 — 输入要存储的样本数。

- 间隔 — 输入从接口收集样本的时间间隔，单位为秒。
- 所有者 — 输入请求 RMON 信息的 站点或用户。

步骤 **4** 单击 “应用”。添加 RMON 历史控制样本，并更新交换机的当前配置。

步骤 **5** 单击 “历史表”，可查看实际的 RMON 历史统计信息。

查看 RMON 历史统计信息

“历史表”页面显示特定接口的网络样本统计信息。该样本在 “历史控制表”页面中配置。

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** 从下拉框中选择要查看的历史控制条目，点击 “确定”。

显示以下字段：

- 历史条目编号 — 历史条目编号。
- 所有者 — 历史条目的所有者。
- 样本编号 — 从该样本中取出的统计信息。
- 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，而是检测到的删除数据包的次数。
- 已接收的字节数 — 接收的八位字节数，包括坏数据包和 FCS 八位字节数，但不包括帧位。
- 已接收的数据包数 — 接收的数据包数，包括坏数据包、组播数据包和广播数据包。
- 广播数据包数 — 接收到的正常广播数据包数。该数量不包括组播数据包。
- 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 — 接收的小于 64 八位字节的数据包数。
- 过大数据包数 — 接收的大于 1518 八位字节的数据包数。
- 分片数 — 接收的分片总数，不包括帧位，但包括 FCS 八位字节。

- 超时发送帧数 — 接收的大于 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）或者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。

步骤 4 单击 “历史控制表”，返回到 “历史控制表”页面。

设置和查看 RMON 事件

您可以设置触发告警的事件和当事件发生时采取的通知类型。执行以下操作可实现此功能：

- 使用 “事件”页面设置当事件发生并触发告警时应采取的动作。您可以选择记录事件和 / 或发送 Trap。
- 使用 “告警”页面设置当哪些事件发生时将触发告警。

设置 RMON 事件

使用 “事件”页面可设置当生成告警 （在 “告警”页面定义）时应该采取操作的事件。事件可以是记录或发送 Trap 的任意组合。如果设定的操作中包括记录，则该事件将记录到事件表。

设置 RMON 事件的步骤：

步骤 1 单击 “状态和统计信息” > “**RMON**” > “事件”。

步骤 2 单击 “添加”，添加 RMON 事件。

步骤 3 设定以下参数。

- 事件条目 — 显示事件条目编号。
- 社团 — 输入在发送 Trap 时要包含的 SNMP 社团字符串。
- 说明 — 输入事件名称，提供此事件的简单说明。事件名称可用于将告警关联到此事件。
- 通知类型 — 选择此事件发生时应采取的动作。可选项如下：
  - *无* — 告警消失时不执行操作。
  - *日志 （事件日志表）* — 告警消失时添加一条日志到事件日志表。

- *Trap（SNMP 管理器和系统日志服务器）* — 告警消失时发送 Trap 到远程日志服务器。
- *日志和 Trap* — 告警消失时添加一条日志到事件日志表并发送 Trap 到远程日志服务器。

- 所有者 — 输入定义此事件的设备或用户。

步骤 **4** 单击 “应用”。添加 RMON 事件，并更新交换机的当前配置。

步骤 **5** 单击 “事件日志表”，可查看已发生且被记录日志的告警的日志信息。

查看 RMON 事件日志

“事件日志表”页面显示发生的事件 （操作）的日志。当事件的通知类型设置为 “日志”或 “日志和 Trap”时，会记录此事件到系统日志。当事件与某一告警绑定并达到了告警的条件时，系统将会执行事件中定义的操作。

查看 RMON 事件日志的步骤：

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”。

此页面显示以下信息：

- 事件条目编号 — 事件条目编号。
- 日志编号 — 日志编号。
- 日志时间 — 记录此日志条目的时间。
- 说明 — 触发告警的事件名称。

步骤 **3** 单击 “事件表”，返回到 “事件表”页面。

设置 RMON 告警

RMON 告警可设置告警阈值和取样间隔，以在任何 RMON 计数器或 SNMP 代理维护的任何其他 SNMP 对象计数器上生成异常事件。告警中必须定义上升阈值与下降阈值。超过上升阈值后，不会再生成其他上升事件，直到超过了伴随的下降阈值。发出下降告警后，将在超过上升阈值时发出下一个告警。

一个或多个告警可绑定到一个事件 （事件表示发生告警时将采取的操作）。

使用 “告警”页面可设置告警并将其与事件绑定。您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。

设置 RMON 告警的步骤：

步骤 **1** 单击 “状态和统计信息” > “**RMON**” > “告警”。

步骤 **2** 单击 “添加”，添加 RMON 告警。

步骤 **3** 设定以下参数：

- 告警条目 — 显示 RMON 告警条目编号。
- 接口 — 选择此告警关联的端口或 LAG。
- 计数器名称 — 选择表示衡量事件类型的 MIB 变量。
- 样本类型 — 选择用于生成告警的取样方法。可选项如下：
  - *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采样的值，将差值与阈值进行比较。如果超过了阈值，则生成告警。
- 上升阈值 — 输入触发上升阈值告警的上升计数器值。
- 上升事件 — 从您在事件表中定义的事件中选择在触发了上升事件时要执行的事件。
- 下降阈值 — 输入触发下降阈值告警的下降计数器值。
- 下降事件 — 从您在事件表中定义的事件中选择在触发了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。上升被定义为超过低阈值向高阈值变化的行为。
  - *上升告警* — 上升计数器值触发上升阈值告警。
  - *下降告警* — 下降计数器值触发下降阈值告警。
  - *上升和下降告警* — 上升计数器值和下降计数器值都触发该告警。
- 间隔 — 输入告警间隔，单位为秒。
- 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”。添加 RMON 告警，并更新交换机的当前配置。

3

管理：系统日志

本章介绍系统日志功能。使用此功能，交换机可以保留若干独立的日志。每个日志是一组记录系统事件的消息。

交换机可生成以下本地日志：

- 发送到控制台接口的日志
- 写入到 RAM 中的记录事件循环列表中的日志。重新启动交换机会将其擦除。
- 写入到保存至闪存的循环日志文件的日志。重新启动不会将其擦除。

此外，还可以 SYSLOG 消息的形式将系统日志保存到远程日志服务器上。

本章介绍如何设置系统日志功能，包含以下内容：

- 系统日志设置
- 设置远程日志服务器
- 查看日志

系统日志设置

使用 “日志设置”页面可启用或禁用交换机的日志功能以及选择需要记入日志的事件的严重级别。

下面按照从高到低的顺序列出了事件的严重级别：

- 紧急 （**Emergency**）— 系统无法使用。
- 警报 （**Alert**）— 需要执行操作。
- 严重 （**Critical**）— 系统处于高危状态。
- 错误 （**Error**）— 系统出错。
- 警告 （**Warning**）— 发出了系统警告。
- 通知 （**Notice**）— 系统能够正常工作，但发出了系统通知。

- 报告 （**Informational**）— 设备信息。
- 调试 （**Debug**）— 提供关于事件的详细信息。

您可以选择将不同严重级别的事件分别存储到 RAM 和闪存中。这些日志将分别显示在 “RAM” 和 “闪存” 页面。

选择要存储在日志中的严重级别后，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”，则会将严重级别为 “警告” 及更高 （即严重级别为 “紧急”、“警报”、“严重”、“错误” 和 “警告”）的所有事件都存储在日志中，但是严重级别低于 “警告”（即严重级别为 “通知”、“报告” 和 “调试”）的事件则不会保存。

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** 设定以下参数：

- 日志 — 选择启用或禁用系统日志功能。
- **RAM** 日志 — 选择启用或禁用 RAM 日志功能。如启用此功能，请勾选要记录到 RAM 中的消息的严重级别。
- 闪存日志 — 选择启用或禁用闪存日志功能。如启用此功能，请勾选要记录到闪存中的消息的严重级别。

步骤 **3** 单击 “应用”。全局设置系统日志参数，并更新交换机的当前配置。

设置远程日志服务器

使用 “远程日志服务器” 页面可设置向其发送日志消息 （使用 SYSLOG 协议）的远程日志服务器，并设定每个服务器接收的消息的严重级别。

设置远程日志服务器的步骤：

步骤 **1** 单击 “管理” > “系统日志” > “远程日志服务器”。

步骤 **2** 单击 “添加”，添加远程日志服务器。

步骤 **3** 设定以下参数：

- 服务器定义 — 选择按照 IP 地址或按照名称来定义远程日志服务器。

- **IP** 版本 — 选择支持的 IP 版本。
- 日志服务器 **IP** 地址 / 名称 — 输入要向其发送日志的服务器的 IP 地址或域名。
- **UDP** 端口 — 输入要向其发送日志消息的 UDP 端口。
- 系统类别 — 选择日志相关的系统类别。
- 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级别。

步骤 **4** 单击 “应用”。添加远程日志服务器，并更新交换机的当前配置。

查看日志

交换机可以写入以下日志：

- RAM 中的日志（在重新启动过程中将自动清除）。如需查看 RAM 日志的详细信息，详见 “查看 **RAM** 日志”。
- 闪存中的日志 （只能由用户手动来清除）。如需查看闪存日志的详细信息，详见 “查看闪存日志”。

您可以设置写入每个日志的消息的严重级别。一则消息可以被写入到多个日志，包括存放在远程日志服务器上的日志。

查看 RAM 日志

“RAM”页面会按逆时间顺序显示保存到 RAM 中的所有日志消息。系统会根据 “日志设置”页面中的设置将消息存储到 RAM 中。

查看 RAM 日志的步骤：

步骤 **1** 单击 “状态和统计信息” > “查看日志” > “**RAM**”。

显示以下信息：

- 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 — 事件的严重级别。
- 说明 — 描述事件的消息文本。

步骤 2 单击 “清除日志”，删除 RAM 中的日志消息。

步骤 3 默认情况下，当出现严重或更高级别的系统消息被记入日志时，警报图标将显示并不停闪烁。单击 “禁用警报图标闪烁”按钮可取消警报图标闪烁功能。系统日志警报图标将不再出现。

查看闪存日志

“闪存”页面会按时间顺序显示存储在闪存中的消息。保存到闪存日志的事件的严重级别可在 “日志配置”页面中设置。当交换机重新启动时，闪存日志会保留在闪存中。您可以手动清除这些日志。

查看闪存日志的步骤：

步骤 1 单击 “状态和统计信息” > “查看日志” > “闪存”。

显示以下信息：

- 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 — 事件的严重级别。
- 说明 — 描述事件的消息文本。

步骤 2 单击 “清除日志”，手动清除闪存日志消息。

4

管理：系统文件

本章介绍如何管理系统文件，比如升级系统固件，重启交换机，恢复设备到出厂默认设置、管理系统配置文件和日志文件等。包括以下内容：

- 文件和文件类型
- 文件操作
- 升级或备份固件 / 语言
- 活动映像
- 下载或备份配置或日志
- 配置文件属性
- 复制或保存配置
- **DHCP** 自动配置

文件和文件类型

系统文件是指包含配置信息或固件映像的文件。

您可以针对这些文件执行各种操作，比如：

- 选择交换器启动的固件映像文件
- 在交换机内部复制不同类型的配置文件
- 从其他设备 （如一台外部服务器）导入配置文件或者导出配置文件到其他设备

交换机支持的文件传输方式包括：

- 内部复制
- 使用浏览器提供的工具的 HTTP/HTTPS
- TFTP 客户端 （需要一台 TFTP 服务器）

交换机上的配置文件由其类型定义。文件中包含交换机的设置和参数值。在交换机上参考配置时，会依据其配置文件类型 （如启动配置或者当前配置），而不是由用户修改的文件名进行参考。用户可以将配置文件的内容从一种文件类型复制到另一种文件类型，但无法更改其文件类型的名称。交换机上的其他文件包括固件映像和日志文件，这些文件统称为操作文件。

配置文件是文本文件，在将其复制到外部设备如 PC 之后，可以在文本编辑器中对其进行编辑。

在交换机上可以找到以下类型的配置文件和操作文件：

- 当前配置 — 包含当前交换机工作所使用的参数。在使用某个配置界面更改参数值后，只有此文件类型会发生修改，并且必须手动保存才能保留。

  如果重新启动交换机，当前配置会丢失。重新启动交换机后，会将此文件类型从存储在闪存中的启动配置复制到存储在 RAM 中的当前配置。

  要保留对交换机所做的更改，必须将当前配置保存为启动配置或其他文件类型（如果不希望交换机在重新启动时使用该配置）。如果已将当前配置保存到启动配置，则当交换机重新启动时，它会重新创建一个当前配置，该配置会包括自上次将当前配置保存到启动配置以来所做的更改。

- 启动配置 — 用户通过将其他配置 （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，并且在每次交换机重新启动时都会保留。交换机重新启动时，会将启动配置复制到 RAM 并将其作为当前配置。

- 备份配置 — 系统关机保护或特定工作状态维护之参数定义的手动副本。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，并且当设备重新启动时会保留。

- 镜像配置 — 在下述情况下由交换机创建的启动配置副本。

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

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

  交换机重新启动时，会将镜像配置重置为出厂默认参数。在所有其他方面，镜像配置均与备份配置相同，即在交换机重新启动时提供保留的参数值副本。

- 固件 — 控制交换机运转和功能的程序，更多时候被称为映像。

- 语言文件 — 能够使交换机的基于 Web 的管理界面以选定的语言显示的字典。

- 闪存日志 — 存储在闪存中的系统日志消息。

文件操作

您可以执行以下操作来管理固件映像、配置文件、语言文件和日志文件：

- 升级系统固件映像、导入语言文件或者备份系统固件映像。详见 “升级或备份固件 / 语言”。
- 查看当前使用的固件映像或选择下次重启时要使用的固件映像。详见 “活动映像”。
- 将交换机上的文件保存到其他设备上。详见 “下载或备份配置或日志”。
- 清除启动配置或备份配置。详见 “配置文件属性”。
- 将一个配置文件类型复制到另一个配置文件类型。详见 “复制或保存配置”。
- 自动从 DHCP 服务器下载配置文件到交换机 （交换机将重启）。详见 “**DHCP** 自动配置”。

注意

除非将当前配置手动复制到启动配置、备份配置或外部文件，否则自上次保存文件以来所做的所有更改将会在交换机重新启动后全部丢失。建议在注销前先将当前配置保存到启动配置，以保留在该会话期间所做的一切更改。

显示在 “保存”应用程序链接左侧的红色 X 图标表明进行了配置更改，但尚未将更改保存到启动配置文件。

单击 “保存”会打开 “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。

升级或备份固件 / 语言

使用 “升级 / 备份固件 / 语言”页面可升级或备份固件映像以及导入语言文件。

交换机支持的文件传输方式包括：

- 使用浏览器提供的工具的 HTTP/HTTPS

- TFTP 客户端 （需要一台 TFTP 服务器）

升级 / 备份固件映像

交换机上存储了两个固件映像：Image1 和 Image2。其中一个映像被确定为活动映像，而另一个映像则被确定为非活动映像。

升级固件时，新的固件映像文件将始终替换交换机的非活动映像文件。将新的固件映像上传到交换机之后，交换机仍然会继续使用旧版本的活动映像启动，直至您在 “活动映像” 页面将新的固件映像设为活动映像，然后重新启动交换机。

您也可以将交换机的活动映像保存到其他位置，如一台 TFTP 服务器。

升级或备份系统固件映像的步骤：

步骤 1 单击 “管理” > “文件管理” > “升级 / 备份固件 / 语言”。

步骤 2 如需将保存在 TFTP 服务器上的固件映像上传到交换机，以替换交换机上的非活动映像，设定以下参数：

- 传输方法 — 选择 “通过 **TFTP**”。
- 保存操作 — 选择 “升级”。
- 文件类型 — 选择 “固件映像”。
- **TFTP** 服务器定义 — 选择按照 IP 地址或主机名称来定义 TFTP 服务器。
- **IP** 版本 — 选择支持的 IP 格式。
- **TFTP** 服务器 **IP** 地址 / 名称 — 输入 TFTP 服务器的 IP 地址或主机名。
- 源文件名 — 输入位于 TFTP 服务器上的固件映像源文件的名称。

步骤 3 单击 “应用”。

步骤 4 如需从其他设备 （如连接到交换机用来管理的本地 PC）上传一个固件映像，以替换交换机上的非活动映像，设定以下参数：

- 传输方法 — 选择 “通过 **HTTP/HTTPS**”。
- 保存操作 — 选择 “升级”。
- 文件类型 — 选择 “固件映像”。
- 文件名 — 单击 “浏览”，选择要上传的固件映像文件。

步骤 5 单击 “应用”。

步骤 6 如果希望将交换机上的活动映像复制到远程 TFTP 服务器，设定以下参数：

- 传输方法 — 选择 “通过 **TFTP**”。
- 保存操作 — 选择 “备份”。
- 文件类型 — 选择 “固件映像”。
- **TFTP** 服务器定义 — 选择按照 IP 地址或者主机名称来定义 TFTP 服务器。
- **IP** 版本 — 选择支持的 IP 格式。
- **TFTP** 服务器 **IP** 地址 / 名称 — 输入 TFTP 服务器的 IP 地址或主机名。
- 目的文件名 — 输入保存到 TFTP 服务器上的固件映像的文件名称。

步骤 7 单击 “应用”。

升级语言文件

如果一个新的语言文件被导入到交换机，可以从 “语言”下拉框中选择此语言版本（无需重新启动交换机）。

升级语言文件的步骤：

步骤 1 单击 “管理” > “文件管理” > “升级 / 备份固件 / 语言”。

步骤 2 如需从一台远程 TFTP 服务器上传语言文件到交换机，设定以下参数：

- 传输方法 — 选择 “通过 **TFTP**”。
- 保存操作 — 选择 “升级”。
- 文件类型 — 选择 “语言文件”。
- **TFTP** 服务器定义 — 选择按照 IP 地址或者主机名称定义 TFTP 服务器。
- **IP** 版本 — 选择支持的 IP 格式。
- **TFTP** 服务器 **IP** 地址 / 名称 — 输入 TFTP 服务器的 IP 地址或主机名。
- 源文件名 — 输入保存在 TFTP 服务器上的语言文件的名称。

步骤 3 单击 “应用”。

步骤 4 如需从其他设备 （如本地 PC）上传语言文件到交换机，设定以下参数：

- 传输方法 — 选择 “通过 **HTTP/HTTPS**”。

- 保存操作 — 选择 “升级”。
- 文件类型 — 选择 “语言文件”。
- 文件名 — 单击 “浏览”，选择要上传的语言文件 。

步骤 5 单击 “应用”。

活动映像

交换机上存储了两个固件映像：Image1 和 Image2。其中一个映像被确定为活动映像，而另一个映像则被确定为非活动映像。交换机会从活动固件映像进行启动。您也可以将非活动映像更改为活动映像 （需重新启动交换机）。

选择活动映像的步骤：

步骤 1 单击 “管理” > “文件管理” > “活动映像”。

此页面显示以下信息：

- 活动映像 — 显示交换机当前使用的活动映像名称。
- 活动映像版本号 — 显示交换机当前使用的活动映像的版本号。
- 重启后的活动映像版本号 — 显示交换机重启后将使用的活动映像的版本号。

步骤 2 从 “重启后的活动映像”下拉框中选择一个固件映像。此固件映像在交换机重新启动后将作为交换机的活动映像。

步骤 3 单击 “应用”。

下载或备份配置或日志

通过 “下载 / 备份配置 / 日志”页面，可执行以下操作：

- 将交换机上的配置文件类型和日志备份到其他设备上
- 将配置文件从其他设备还原到交换机上

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所有配置命令，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时，新文件会替换旧文件。

将配置文件还原至启动配置时，必须重新启动交换机才能将还原的启动配置作为当前配置使用。

导入配置文件

使用保存的配置文件替换交换机的配置文件的步骤：

步骤 1 单击 “管理” > “文件管理” > “下载 / 备份配置 / 日志”。

步骤 2 如需将远程 TFTP 服务器上的配置文件上传到交换机，并替换交换机上的某一配置文件类型，设定以下参数：

- 传输方法 — 选择 “通过 **TFTP**”。
- 保存操作 — 选择 “下载”。
- **TFTP** 服务器定义 — 选择按照 IP 地址或者主机名称定义 TFTP 服务器。
- **IP** 版本 — 选择支持的 IP 格式。
- **TFTP** 服务器 **IP** 地址 / 名称 — 输入 TFTP 服务器的 IP 地址或主机名。
- 源文件名 — 输入源配置文件的文件名。
- 目的文件类型 — 选择要替换的目标配置文件类型，如当前配置、启动配置或备份配置。

步骤 3 单击 “应用”。

步骤 4 如需将其他设备上保存的配置文件上传到交换机，并替换交换机上的某一配置文件类型，设定以下参数：

- 传输方法 — 选择 “通过 **HTTP/HTTPS**”。
- 保存操作 — 选择 “下载”。
- 源文件名 — 单击 “浏览”，选择要上传的配置文件。
- 目的文件类型 — 选择要替换的目标配置文件类型，如当前配置、启动配置或备份配置。

步骤 5 单击 “应用”。

备份配置文件或日志

将交换机的配置文件或闪存日志保存到其他设备上的步骤：

步骤 1 单击 “管理” > “文件管理” > “下载 / 备份配置 / 日志”。

步骤 2 如需将交换机的配置文件或闪存日志备份到 TFTP 服务器，设定以下参数：

- 传输方法 — 选择 “通过 **TFTP**”。
- 保存操作 — 选择 “备份”。
- **TFTP** 服务器定义 — 选择按照 IP 地址或者主机名称定义 TFTP 服务器。
- **IP** 版本 — 选择支持的 IP 格式。
- **TFTP** 服务器 **IP** 地址 / 名称 — 输入 TFTP 服务器的 IP 地址或主机名。
- 源文件类型 — 选择要备份的配置文件类型或日志。
- 目的文件名 — 输入保存到 TFTP 服务器上的目的文件名。

步骤 3 单击 “应用”。所选配置文件类型或日志将保存到 TFTP 服务器上 （文件名为设定的目的文件名）。

步骤 4 如需将交换机的配置文件或日志备份到本地 PC 或其他设备，设定以下参数：

- 传输方法 — 选择 “通过 **HTTP/HTTPS**”。
- 保存操作 — 选择 “备份”。
- 源文件类型 — 选择要备份的配置文件类型或日志。

步骤 5 单击 “应用”。

步骤 6 选择文件保存路径，单击 “确定”。

配置文件属性

使用 “配置文件属性”页面可查看系统配置文件的创建日期和时间。您也可以手动删除启动配置和备份配置。无法删除其他配置文件类型。

查看配置文件属性和 / 或删除配置文件的步骤：

步骤 1 单击 “管理” > “文件管理” > “配置文件属性”。

此页面显示以下信息：

- 配置文件名称 — 显示配置文件类型。
- 创建时间 — 显示配置文件创建的日期和时间。

步骤 2 要清除启动配置和备份配置，请选择相应的配置文件类型并单击 “清除文件”。

复制或保存配置

在任意窗口上单击 “应用”，只会将对交换机所做的更改保存到当前配置中。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为其他设备上的配置文件。

使用 “复制 / 保存配置”页面可将一个配置文件复制或保存到其他配置文件，以进行备份。页面下方有一个按钮，点击此按钮可启用或禁用 “保存”图标闪烁。

注意 除非将当前配置复制到启动配置或其他类型的配置文件，否则自上次复制文件以来所做的所有更改将会在交换机重新启动后全部丢失。

您可以执行以下文件类型的内部复制：

- 从当前配置复制到当前配置、启动配置或备份配置
- 从启动配置复制到当前配置、启动配置或备份配置
- 从备份配置复制到当前配置、启动配置或备份配置
- 从镜像配置复制到当前配置、启动配置或备份配置

将交换机配置从一个文件类型复制到另一个文件类型的步骤：

步骤 1 单击 “管理” > “文件管理” > “复制 / 保存配置”。

步骤 2 设定以下参数：

- 源文件名 — 选择要复制的源文件类型。
- 目的文件名 — 选择将由源文件覆盖的目标文件类型。

步骤 3 单击 “应用”。将选定的源配置文件复制到目标配置文件类型。

步骤 4 当交换机有未保存的数据时，在页面右上方会显示红色 X 图标和 “保存”应用程序链接。“保存图标闪烁”字段显示保存图标闪烁功能是否启用或禁用。如需启用或禁用此功能，可分别单击 “启用保存图标闪烁”或 “禁用保存图标闪烁”按钮。

DHCP 自动配置

交换机支持 DHCP 自动配置，这样便可以将配置信息传送到 TCP/IP 网络上的主机。基于此协议，交换机可使用自动配置功能从远程 TFTP 服务器上下载配置文件。

默认情况下，当自动配置功能启用时，交换机可作为一个 DHCP 客户端来使用。根据支持自动配置的 DHCP 服务器的类型 （DHCPv4 或 DHCPv6），交换机既可以作为一台 DHCPv4 客户端，也可以作为一台 DHCPv6 客户端。

在以下情况下会触发 DHCPv4 自动配置：

- 交换机重启后 （使用 DHCPv4）动态分配或自动续订 IP 地址时
- 收到明确的 DHCP 续订请求且如果已为此配置了交换机和服务器
- 自动续租 DHCP 后

在以下情况下会触发 DHCPv6 自动配置：

- 当 DHCPv6 服务器发送信息给交换机时。通常出现在以下几种情形下：
  - IPv6 无状态客户端启用时
  - 收到服务器发送的 DHCPv6 消息时
  - 交换机刷新 DHCPv6 信息时
  - 交换机重启后且 DHCPv6 无状态客户端启用时

- DHCPv6 服务器数据包包含有配置文件名选项

DHCP 服务器选项

DHCP 消息可能包含配置服务器名称 / 地址以及配置文件名 / 路径 （这些都是可选的 DHCP 选项）。这些选项可在来自 DHCPv4 服务器的 Offer 消息中找到，或者在来自 DHCPv6 服务器的 Information Reply 消息中找到。

备份信息 （包括配置服务器名称 / 地址以及配置文件名 / 路径）可以在 “DHCP 自动配置”页面设定。这些信息只有在 DHCPv4 或 DHCPv6 消息中没有包含以上选项时才会起作用。

自动配置过程

当触发自动配置过程后，将按顺序发生以下事件：

- 访问 DHCP 服务器以获取 TFTP 服务器名称 /IP 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 服务器没有提供 TFTP 服务器和配置文件选项，此时用户自定义的备份配置文件名将被使用。
- 如果 DHCP 服务器没有发送这些选项且备份的 TFTP 服务器地址参数为空，那么交换机会发送 TFTP 请求消息到有限广播的 IPv4 地址，然后与第一个响应的 TFTP 服务器继续自动配置过程。

设置 DHCP 自动配置参数

如需设定 DHCP 自动配置功能，请执行以下步骤：

- 设置 DHCPv4 和 / 或 DHCPv6 服务器发送必要的 DHCP 选项。此步骤在本手册没有描述。
- 设置交换机上 DHCP 自动配置功能的相关参数。
- 在 “IPv4 接口”页面将 IP 地址类型设为动态。详见 “设置 IPv4 管理接口”。

当 DHCP 消息没有提供 DHCP 选项时，使用 “DHCP 自动配置”页面执行以下操作：

- 启用 DHCP 自动配置功能
- 设定交换机从特定服务器的某个特定配置文件获取配置信息

DHCP 自动配置过程中，需注意以下几个方面：

- 存放在TFTP服务器上的配置文件必须符合交换机所支持的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，交换机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 模式下，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 续订周期分配不同的 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。

注释 DHCP 自动配置功能要求交换机的 IP 地址设置为动态。

设置 DHCP 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 设定以下参数：

- 通过 **DHCP** 进行自动配置 — 选择启用或禁用 DHCP 自动配置功能。
- 备份服务器定义 — 选择按 IP 地址或主机名定义 TFTP 服务器。
- **IP** 版本 — 选择支持的 IP 版本。
- 备份**TFTP**服务器**IP**地址/名称 — 输入用作备份的TFTP服务器的IP地址或主机名。当 DHCP 选项中没有提供 TFTP 服务器以及配置文件等信息时，此时交换机将访问此 TFTP 服务器并下载指定的配置文件。
- 备份配置文件 — 输入备份TFTP服务器上存放的配置文件的名称。当DHCP选项中没有提供 TFTP 服务器以及配置文件等信息时，此时交换机将访问备份 TFTP 服务器并下载此配置文件。
- 最近自动配置**TFTP**服务器**IP**地址 — 显示交换机当前使用的TFTP服务器的IP地址或主机名。
- 最近自动配置文件名 — 显示交换机当前使用的 TFTP 服务器上存放的配置文件名称。

步骤 3 单击 “应用”。保存 DHCP 自动配置，并更新交换机的当前配置。

5

管理：系统参数

本章介绍如何查看系统信息和设置各种系统参数，包括以下内容：

- 设备型号
- 查看系统摘要
- 定义系统设置
- 设置控制台波特率
- 重新启动交换机
- 设置闲置会话超时
- **Ping** 主机
- **Traceroute**

设备型号

所有交换机型号都可以通过基于 Web 的管理界面进行完全管理。下表介绍不同交换机型号上所支持的端口类型和数量，是否支持 PoE 功能以及相应的 PID 信息：

型号	端口和扩展端口	支持 **PoE** 的端口	**PID**
快速以太网			
SF220-24	24 个 FE 铜缆端口和 2 个组合端口（GE/SFP）	不支持	SF220-24-K9-NA, SF220-24-K9-EU, SF220-24-K9-UK, SF220-24-K9-AU, SF220-24-K9-CN

型号	端口和扩展端口	支持 PoE 的端口	PID
SF220-24P	24 个 FE 铜缆端口和 2 个 组合端口（GE/SFP）	1 至 24	SF220-24P-K9-NA, SF220-24P-K9-EU, SF220-24P-K9-UK, SF220-24P-K9-AU, SF220-24P-K9-CN
SF220-48	48 个 FE 铜缆端口和 2 个 组合端口（GE/SFP）	不支持	SF220-48-K9-NA, SF220-48-K9-EU, SF220-48-K9-UK, SF220-48-K9-AU, SF220-48-K9-CN
SF220-48P	48 个 FE 铜缆端口和 2 个 组合端口（GE/SFP）	1 to 48	SF220-48P-K9-NA, SF220-48P-K9-EU, SF220-48P-K9-UK, SF220-48P-K9-AU, SF220-48P-K9-CN
千兆以太网			
SG220-26	24 个 GE 铜缆端口和 2 个组合端口（GE/SFP）	不支持	SG220-26-K9-NA, SG220-26-K9-EU, SG220-26-K9-UK, SG220-26-K9-AU, SG220-26-K9-BR, SG220-26-K9-AR
SG220-26P	24 个 GE 铜缆端口和 2 个组合端口（GE/SFP）	1 至 24	SF220-26P-K9-NA, SF220-26P-K9-EU, SF220-26P-K9-UK, SF220-26P-K9-AU, SF220-26P-K9-BR, SF220-26P-K9-AR
SG220-50	48 个 GE 铜缆端口和 2 个组合端口（GE/SFP）	不支持	SG220-50-K9-NA, SG220-50-K9-EU, SG220-50-K9-UK, SG220-50-K9-AU, SG220-50-K9-BR, SG220-50-K9-AR

型号	端口和扩展端口	支持 PoE 的端口	PID
SG220-50P	48 个 GE 铜缆端口和 2 个组合端口（GE/SFP）	1 至 48	SF220-50P-K9-NA, SF220-50P-K9-EU, SF220-50P-K9-UK, SF220-50P-K9-AU, SF220-50P-K9-BR, SF220-50P-K9-AR
SG220-28	24个GE铜缆端口和 4 个 SFP 端口	不支持	SG220-28-K9-CN
SG220-28MP	24个GE铜缆端口和 4 个 SFP 端口	1 至 24	SG220-28MP-K9-CN
SG220-52	48 个 GE 铜缆端口和 4 个 SFP 端口	不支持	SG220-52-K9-CN

注释 有些交换机功能仅在销售给中国大陆地区的交换机型号上支持。从交换机的 PID 中可以判断您的交换机是否为售往中国大陆地区的交换机型号 （即交换机 PID 的目的国家为 -CN）。本手册针对这些功能都添加了特别注释，标明此功能仅适用于某些特定的交换机型号。您可以从 “系统概览”页面中找到您的交换机的 PID 信息。

查看系统摘要

“系统摘要”页面提供交换机的图形视图，并显示交换机状态、硬件信息、固件版本、以太网供电信息 （如果有）、 TCP/UDP 服务状态以及其他信息。

如需查看系统摘要信息，单击 “状态和统计信息” > “系统摘要”。

此页面显示以下信息：

系统信息

- 系统说明 — 产品名称。
- 系统位置 — 交换机的实际位置。单击 “编辑”可前往 “系统设置”页面输入该值。
- 系统联系人 — 联系人姓名。单击 “编辑”可前往 “系统设置”页面输入该值。
- 主机名 — 交换机的名称。单击 “编辑”可前往 “系统设置”页面输入该值。默认情况下，交换机主机名由单词 switch 与交换机 MAC 地址的最后三个字节（最右侧的六个十六进制数字）串联组成。
- 系统对象 **ID** — SNMP 实体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 — 自上次重新启动以来运行的时间。
- 当前时间 — 当前系统时间。
- 基本 **MAC** 地址 — 交换机的 MAC 地址。
- 巨型帧 — 巨型帧的支持状态。使用 “端口设置”页面可启用或禁用巨型帧功能。

  注　启用巨型帧功能只有在交换机重启后才会生效。

软件信息

- 固件版本 （活动映像）— 活动映像的固件版本号。
- 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）— 非活动映像的固件版本号。
- 固件 **MD5** 校验和 （非活动）— 非活动映像的 MD5 校验和。
- **Boot** 版本 — 交换机的 bootloader 版本。
- 区域设置 — 第一语言的区域 （第一语言区域始终是英文）。
- 语言版本 — 第一语言的语言文件包的版本。
- 语言 **MD5** 校验和 — 第一语言文件包的 MD5 校验和。
- 区域设置 — 第二语言的区域。
- 语言版本 — 第二语言的语言文件包的版本。
- 语言 **MD5** 校验和 — 第二语言文件包的 MD5 校验和。

TCP/UDP 服务状态

- **HTTP** 服务 — 交换机当前是否启用或禁用 HTTP 服务。
- **HTTPS** 服务 — 交换机当前是否启用或禁用 HTTPS 服务。
- **SNMP** 服务 — 交换机当前是否启用或禁用 SNMP 服务。
- **Telnet** 服务 — 交换机当前是否启用或禁用 Telnet 服务。
- **SSH** 服务 — 当前是否启用或禁用 SSH 服务。

注 单击 “编辑”按钮可转到 “安全” > “TCP/UDP 服务”页面启用或禁用相应的服务。

PoE 电源信息 （仅适用于支持 **PoE** 功能的交换机）

- 最大可用 **PoE** 功率 — 所有 PoE 端口可提供的最大功率。

- 总 **PoE** 功耗 — 受电设备已消耗的总功率。
- **PoE** 供电模式 — 当前使用的 PoE 供电模式。

其他信息

- 序列号 — 交换机的序列号。
- **PID VID** — 交换机的端口号和版本 ID。

定义系统设置

查看或编辑系统设置的步骤：

步骤 **1** 单击 “管理” > “系统设置”。

步骤 **2** 查看或修改以下系统设置：

- 系统说明 — 显示交换机的系统说明。
- 系统位置 — 输入交换机实际所在的位置。
- 系统联系人 — 输入联系人姓名。
- 主机名 — 选择如何定义主机名。可选项如下：
  - *使用默认设置* — 选择此选项使用默认的主机名 （即系统名称）。交换机默认的主机名为 Switch123456，其中 123456 代表交换机 MAC 地址的最后三个字节 （以十六进制格式表示）。
  - *用户定义* — 选择此选项可手动设定主机名。只能使用字母、数字和连字符。主机名不能以连字符开头或结尾。其他符号、标点符号字符或空格均不允许使用 （如 RFC1033、 1034、 1035 中规定）。

步骤 **3** 在 “自定义登录屏幕设置”区域，您可以设置登录横幅和欢迎横幅的内容：

- 登录横幅 — 登录横幅是指在交换机登录页面上显示的消息，类似标语或问候语。输入相应的消息内容，然后单击 “预览”查看显示效果。设置范围为 0 到 2000 个字符。
- 欢迎横幅 — 欢迎横幅是指在执行完 EXEC 进程后显示的信息。输入相应的消息内容，然后单击 “预览”查看显示效果。设置范围为 0 到 2000 个字符。

  注　在基于 Web 的管理界面上设定的登录横幅和欢迎横幅同样可应用到命令行管理接口 （通过 Console、 Telnet 和 SSH 访问交换机的命令行管理接口）。

步骤 4 单击 “应用”。修改系统设置，并更新交换机的当前配置。

设置控制台波特率

使用 “控制台设置”页面可修改交换机的控制台端口波特率。交换机默认的控制台设置为：

- 每秒位数 = 9600 比特 / 秒
- 数据位 = 8
- 奇偶校验 = 无
- 停止位 = 1
- 数据流控制 = 无

设置控制台端口波特率的步骤：

步骤 1 单击 “管理” > “控制台设置”。

步骤 2 从 “控制台端口波特率”下拉框中选择任意值。可选项为 2400、 4800、 9600、 19200、 38400、 57600 和 115200 比特 / 秒。

步骤 3 单击 “应用”。修改控制台端口波特率，并更新交换机的当前配置。

重新启动交换机

某些配置更改 （如启用巨型帧支持）需要重新启动交换机才能生效。但是，重新启动交换机会删除当前配置。因此，在重新启动交换机之前应先将当前配置保存到启动配置。单击 “应用”不会将当前配置保存到启动配置。

用户可以使用 “管理” > “复制 / 保存配置”页面或单击窗口顶部的 “保存”链接来备份当前配置。详见 “复制或保存配置”。

重新启动交换机的步骤：

步骤 1 单击 “管理” > “重启”。

步骤 2 单击 “重启”可重新启动交换机。由于当前配置中的任何未保存的信息在交换机重新启动时都会被丢弃，因此必须单击任何窗口右上角的 “保存”，以便在启动程序保留当前配置。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。

步骤 3 您也可以勾选 “恢复出厂默认设置”选项，然后单击 “重启”，以出厂默认配置重新启动交换机。该过程会清除启动配置文件。如果选择该操作，将会清除未保存到其他文件的所有设置。

镜像配置文件在恢复出厂默认设置时不会被擦除。

设置闲置会话超时

使用 “空闲会话超时”页面可设置管理会话经过多长时间的闲置后会超时。超时后用户必须重新登录才能重建以下会话之一：

- HTTP 会话
- HTTPS 会话
- Console 会话
- Telnet 会话
- SSH 会话

设置闲置会话超时时间的步骤：

步骤 1 单击 “管理” > “空闲会话超时”。

步骤 2 从相应下拉框中为每种会话选择超时时间。默认为 10 分钟。

步骤 3 单击 “应用”。设置空闲会话超时，并更新交换机的当前配置。

Ping 主机

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

Ping 通过向目的主机发送互联网控制消息协议 （ICMP）回显请求数据包并等到 ICMP 响应来运行，有时也称为 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 设定以下参数：

- 主机定义 — 选择按 IP 地址或名称来定义主机。
- **IP** 版本 — 选择支持的 IP 版本。
- 主机 **IP** 地址或名称 — 输入要 ping 的主机 IP 地址或名称。
- **Ping** 数量 — 设定 ping 操作执行的次数。选择 “使用默认配置”使用默认值，或选择 “用户定义”手动输入。

步骤 3 单击 “激活 **Ping**”。开始执行 Ping 操作。

执行完毕后，页面显示相应的 Ping 计数器和状态信息。

Traceroute

Traceroute 通过向目标主机发送 IP 数据包并返回给交换机，从而发现数据包的转发 IP 路由。

使用 “Traceroute”页面可查询交换机和目标主机间的每一跳以及到每一跳的往返时间。

使用 Traceroute 步骤：

步骤 1 单击 “管理” > “**Traceroute**”。

步骤 2 设定以下参数：

- 主机定义 — 选择按 IP 地址或名称来定义主机。

- 主机 **IP** 地址或名称 — 输入要追踪路由的主机 IP 地址或名称。
- **TTL** — 此字段用来设定 Traceroute 允许的最大跳数，以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。选择 “使用默认配置”使用默认值，或选择 “用户定义”手动输入。

步骤 **3** 单击 “应用”。执行 Traceroute 操作并显示操作结果。

6

管理：系统时间

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

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示尤为重要。

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

本章介绍如何设置系统时间、时区和夏时制，包括以下内容：

- 系统时间选项
- 设置系统时间
- 设置 **SNTP** 服务器

系统时间选项

系统时间可由用户手动设置，也可以使用 SNTP 服务器来动态设置。如果选择使用 SNTP 服务器，则与该服务器建立通信后将会覆盖手动时间设置。

作为启动过程的一部分，交换机始终设置时间、时区和夏令时。这些参数可以从 SNTP 服务器获取，也可以手动设置。如果两者都无法成功，还可以从出厂默认配置获得。

交换机提供以下方式设置系统时间：

- 由用户手动输入系统时间
- 使用 SNTP 服务器作为时钟源 （可确保将交换机的网络时间同步精确到毫秒）

注释 如果没有时间同步，将很难甚至无法在设备之间准确关联日志文件。我们建议使用 SNTP 服务器作为时钟源。

设置系统时间

使用 “系统时间”页面可以设置交换机的当前时间、时区、夏时制等。

注意 交换机没有可以更新手动时间的内部时钟。因此，如果系统时间为手动设置并且重新启动了交换机，则必须重新输入手动时间设置。

设置系统时间的步骤：

步骤 1 单击 “管理” > “时间设置” > “系统时间”。

“实际时间”字段显示交换机当前的系统时间以及使用的时钟源。

步骤 2 勾选 “主时钟源 （**SNTP** 服务器）”选项，交换机将从 SNTP 服务器获得系统时间。此功能要求您首先在 “SNTP 设置”页面添加一个 SNTP 服务器。详见 “设置 **SNTP** 服务器”。

步骤 3 在 “手动设置”区域，手动设定系统时间。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 — 输入当前系统的日期。
- 本地时间 — 输入当前系统的时间。

您也可以单击 “此处”链接，通过浏览器信息从您的本地 PC 获取时间和日期信息。

步骤 4 在 “时区设置”区域，根据设定的时区偏移量使用本地时间。

- 时区偏移量 — 选择与协调世界时（Universal Time Coordinated，UTC）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 UTC+10:00，而纽约的时区偏移为 UTC-5:00。
- 时区缩写 — 输入一个名称以表示您配置的时区。此时区缩写将显示在 “实际时间”字段。

步骤 5 在 “夏令时设置”区域，设定以下夏令时参数：

- 夏令时 — 选择启用或禁用夏时制。
- 时间设置偏移 — 输入夏令时导致时钟调整的分钟数。设置范围为 1 到 1440 分钟，默认为 60 分钟。
- 夏令时类型 — 选择定义夏时制的方式。可选项如下：
  - *美国* — 依据在美国使用的日期。
  - *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。
  - *按日期* — 手动设置夏令时（通常针对除美国或欧盟国家 / 地区以外的国家 / 地区）。
  - *循环* — 每年在同一天开始实行夏时制。

如您选择*按日期*，设定以下参数：

- 自 — 输入夏时制开始的日期和时间。
- 至 — 输入夏时制结束的日期和时间。

如您选择*循环*，设定以下参数：

- 自 — 输入每年开始实行夏时制的日期和时间。
  - *日期* — 每年夏令时开始的的日期 （星期几）。
  - *周* — 每年开始执行夏令时的星期 （在某月的第几个星期）。
  - *月* — 每年开始执行夏令时的月份。
  - *时间* — 每年开始执行夏令时的时间。
- 至 — 输入每年夏令时结束的日期和时间。
  - *日期* — 每年结束夏令时的的日期 （星期几）。
  - *周* — 每年结束夏令时的星期 （在某月的第几个星期）。
  - *月* — 每年结束夏令时的月份。
  - *时间* — 每年结束夏令时的时间。

步骤 6 单击 “应用”。保存系统时间设置，并更新交换机的当前配置。

设置 SNTP 服务器

使用 “SNTP 设置”页面可设置用于同步交换机的系统时钟的 SNTP 服务器。

如果按照主机名定义 SNTP 服务器，您首先需要在交换机上定义 DNS 服务器以及在“系统时间”页面上启用 “主时钟源 （**SNTP** 服务器）”选项。

设置 SNTP 服务器的步骤：

步骤 **1** 单击 “管理” > “时间设置” > “**SNTP** 设置”。

步骤 **2** 设定以下参数：

- 主机定义 — 选择按照 IP 地址或主机名来定义 SNTP 服务器。
- **SNTP** 服务器 **IP** 地址 / 名称 — 输入 SNTP 服务器的 IP 地址或主机名。
- **SNTP** 服务器端口 — 输入 SNTP 服务器使用的端口号，默认为 123。

步骤 **3** 单击 “应用”。添加 SNTP 服务器，并更新交换机的当前配置。

7

管理：设备诊断

本章介绍如何设置端口镜像、执行铜缆测试以及查看光纤模块状态和 CPU 使用率，包括以下内容：

- 测试铜质端口
- 查看光模块状态
- 设置端口和 **VLAN** 镜像
- 查看 **CPU** 使用率

测试铜质端口

使用 “铜缆测试”页面可对铜质电缆执行集成电缆测试以及查看测试结果。

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。不建议对正在访问基于 Web 的管理界面的端口执行铜质端口测试，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** 从下拉框中选择要执行测试的端口。

步骤 **3** 单击 “铜缆测试”。

步骤 **4** 系统弹出消息框，提示您测试期间此端口将关闭。如需继续请单击 “确定”。

测试完成后，显示以下字段：

- 测试结果 — 铜缆测试结果。
- 电缆长度 — 预测的电缆长度。端口启用了 PoE 功能时显示为未知。

注　　如果端口链接当前为连接状态或者实际连接的电缆长度低于 10 米，此字段显示的预测电缆长度可能不是十分准确，仅作参考。

- 运行端口状态 — 端口是否连接或断开。

查看光模块状态

“光纤模块状态”页面显示由小型封装可热插拔 （Small Form-factor Pluggable，SFP）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。

交换机支持以下百兆 SFP 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。

交换机支持以下千兆 SFP 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。

要查看光纤模块测试的结果，单击 “管理” > “诊断” > “光纤模块状态”。

此页面将显示以下字段：

- 端口 — 连接 SFP 的端口。

- 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。
- 信号丢弃 — 本地 SFP 报告信号丢失。值为 “True” 和 “False”。

设置端口和 **VLAN** 镜像

在网络交换机上，可使用端口镜像将一个交换机端口、多个交换机端口或整个 VLAN 上看到的网络数据包的副本发送到用于网络监控连接的另一交换机端口上。这对于需要进行网络流量监控的网络应用 （例如入侵检测系统）很常用。连接到监控端口的网络分析器会处理这些复制的数据包进行诊断、调试和性能监控。

交换机支持最多 4 个镜像会话。每一个镜像会话既可以用于本地镜像也可以用于远程镜像。镜像不会影响交换机源端口或 VLAN 上的网络流量的交换。每一个镜像会话必须有一个不同的目的端口，除非明确要求镜像目的端口只接收镜像报文，目的端口还可以正常接收和转发普通报文。

当从某个端口接收的数据包被指定的 VLAN 做镜像，即使此数据包在交换机内会被丢弃或发送到 CPU，此数据包仍然会被发送到监控端口。当端口启用了传入 （TX）镜像时，从端口传输出去的数据包会被镜像。

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。

注释 RSPAN VLAN 镜像功能仅在销售到中国大陆地区的交换机型号上支持。

设置端口和 VLAN 镜像的步骤：

步骤 **1** 单击 “管理” > “诊断” > “端口和 **VLAN** 镜像”。

步骤 **2** 如果您的交换机支持 RSPAN VLAN 镜像功能，设定以下参数：

- **RSPAN VLAN**— 选择启用或禁用 RSPAN VLAN 镜像功能。
- **RSPAN VLAN ID**— 如启用 RSPAN VLAN 镜像功能，选择要镜像的 VLAN。当您设置一个 RSPAN 镜像任务时，您必须选择此 VLAN 作为 RSPAN VLAN。

步骤 **3** 单击 “添加”，添加一个 SPAN 或 RSPAN 镜像会话。

步骤 4 设定以下参数：

- 会话 **ID**— 选择镜像会话的编号。
- 会话类型 — 选择镜像会话的类型。可选项包括：
  - *基于本地端口* — 将各个端口的 Tx、 RX 或 TX&RX 流量复制到目的端口。
  - *基于本地 VLAN* — 将本地 VLAN 的流量复制到目的端口。
  - *RSPAN 源会话* — 利用 VLAN 将源端口或源 VLAN 的流量复制到其他设备。
  - *RSPAN 目的会话* — 利用 VLAN 将目的端口的流量复制到其他设备。

步骤 5 如果选择 “基于本地端口”，设定以下参数：

- 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连接到此端口。
- 允许入口数据包 — 选择允许或禁止目的端口发送或接收镜像报文之外的普通数据包。
- 源端口 — 选择向分析器端口的发送流量的源端口，将从其镜像以下流量：
  - *仅接收* — 对传入数据包进行端口镜像。
  - *仅传输* — 对传出数据包进行端口镜像。
  - *传输和接收* — 对传入和传出数据包都进行端口镜像。
  - *不适用* — 不进行端口镜像。

步骤 6 如果选择 “基于本地 VLAN”，设定以下参数：

- 目的端口 — 选择要向其复制流量的端口，即分析器端口。
- 允许入口数据包 — 选择允许或禁止目的端口发送或接收镜像报文之外的普通数据包。
- **VLAN**— 选择被镜像的源 VLAN。

步骤 7 如果选择 “RSPAN 源会话”，设定以下参数：

- **RSPAN VLAN**— 选择一个 VLAN 以利用此 VLAN 复制流量到其他设备。此 VLAN 必须与步骤 2 中 “**RSPAN VLAN ID**”字段所定义的 VLAN 保持一致。
- 反射器端口 — 选择用来连接另一个设备的端口或 LAG。
- 源类型 — 选择要复制流量的源端口或源 VLAN。

  如果选择端口作为来源，设定向分析器端口发送流量的源端口，将从其镜像以下流量：

- *仅接收* — 对传入数据包进行端口镜像。
- *仅传输* — 对传出数据包进行端口镜像。
- *传输和接收* — 对传入和传出数据包都进行端口镜像。
- *不适用* — 不进行端口镜像。

如果选择 VLAN 作为来源，设定向分析器端口发送流量的 VLAN。

- *VLAN*— 选择向分析器端口发送流量的 VLAN，将从其镜像流量。

步骤 8 如果选择 “RSPAN 目的会话”，设定以下参数：

- **RSPAN VLAN**— 选择一个 VLAN 以利用此 VLAN 复制流量到其他设备。此 VLAN 必须与步骤 2 中 “**RSPAN VLAN ID**”字段所定义的 VLAN 保持一致。
- 目的端口 — 选择要向其复制数据包的分析器端口。
- 允许入口数据包 — 选择允许或禁止目的端口发送或接收镜像报文之外的普通数据包。

步骤 9 单击 “应用”。保存端口和 VLAN 镜像设置，并更新交换机的当前配置。

查看 CPU 使用率

查看 CPU 使用率和 / 或设置刷新频率的步骤：

步骤 1 单击 “管理” > “诊断” > “**CPU** 使用率”。

“**CPU** 使用率”字段显示交换机当前的 CPU 利用率，即每秒向 CPU 输入帧的速率。

步骤 2 在 “刷新速率”字段，选择刷新 CPU 使用率的时间间隔 （以秒为单位）。

8

管理：设备发现

本章介绍如何设置交换机的发现功能（如 Bonjour、 LLDP 和 CDP），包括以下内容：

- 设置 **Bonjour**
- 关于 **LLDP** 和 **CDP**
- 设置 **LLDP**
- 设置 **CDP**

设置 **Bonjour**

作为 Bonjour 客户端，交换机会定期将 Bonjour 发现协议数据包广播给直接连接的 IP 子网，以通告它的存在以及它所提供的服务，例如 HTTP、 HTTPS 和 Telnet。

网络管理系统或其他第三方应用可发现交换机。默认情况下，管理 VLAN 上已启用 Bonjour。 Bonjour 控制台会自动监测并显示该设备。

Bonjour 发现只可以全局启用，无法针对单个端口或单个 VLAN 启用。交换机会根据“TCP/UDP 服务”页面的配置，通告管理员启用的所有服务。

如果 Bonjour 被禁用，交换机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。

默认情况下，所有管理 VLAN 的成员端口上均启用 Bonjour。

设置 Bonjour 的步骤：

步骤 1 单击 “管理” > “发现协议 - **Bonjour**”。

步骤 2 全局启用或禁用 Bonjour。

步骤 3 单击 “应用”。全局启用或禁用 Bonjour，并更新交换机的当前配置。

关于 LLDP 和 CDP

链路层发现协议 （Link Layer Discovery Protocol， LLDP）和思科发现协议 （Cisco Discovery Protocol， CDP）都是链路层协议，针对直接连接到交换机的邻居设备通告其自身和相互之间通告功能。默认情况下，交换机定期发送一个 LLDP/CDP 通告到它的所有端口，并且终止和处理协议所要求的接入 LLDP/CDP 数据包。在 LLDP/CDP 数据包内，通告在数据包中被编码为 TLV （类型、长度和值）。

在具备 LLDP/CDP 功能的设备没有相互直接连接且与不具备 LLDP/CDP 功能的设备相分离的部署环境下，只有在不具备 LLDP/CDP 功能的设备泛洪它们接收到的 LLDP/CDP 数据包时，具备 LLDP/CDP 功能的设备才有可能从其他设备上接收到通告。如果不具备 LLDP/CDP 功能的设备执行 VLAN 有意识泛洪，且具备 LLDP/CDP 功能的设备在相同的 VLAN 内，可彼此接听到对方。

必须注意的是，当不具备 LLDP/CDP 功能的设备泛洪 LLDP/CDP 数据包时，一个具备 LLDP/CDP 功能的设备可能接收来自超过一个设备的通告。

设置 LLDP 和 CDP 时需特别注意以下事项：

- 可全局启用或禁用LLDP/CDP功能，也可以分别针对单个端口启用或禁用LLDP/CDP 功能。只有在 LLDP/CDP 功能被全局启用时，才可以针对单个端口启用或禁用 LLDP/CDP 功能。
- 当全局启用 LLDP/CDP 功能时，默认情况下，交换机会过滤掉从禁用 LLDP/CDP 功能的端口传入的 LLDP/CDP 数据包。
- 当全局禁用 LLDP/CDP 功能时，交换机被设置为丢弃、 VLAN 有意识泛洪或者 VLAN 无意识泛洪所有的 LLDP/CDP 数据包。 VLAN 有意识泛洪是指将一个接入 LLDP/CDP 数据包泛洪到除接入端口之外的接收数据包的 VLAN。 VLAN 无意识泛洪是指将一个接入 LLDP/CDP 数据包泛洪到除接入端口之外的全部端口。如全局禁用 LLDP/CDP 功能，默认将 VLAN 无意识泛洪 LLDP/CDP 数据包。您可以分别在 “LLDP 属性”和 “CDP 属性”页面选择丢弃或泛洪 LLDP/CDP 数据包。
- LLDP/CDP 终端设备（如 IP 电话）从 CDP/LLDP 通告中学习语音 VLAN 配置。默认情况下，交换机被允许根据交换机上设置的语音 VLAN 发送 CDP/LLDP 通告。详见 “设置语音 VLAN”。

  注　　LLDP/CDP 无法区分端口是否在 LAG 内。如果一个 LAG 内包含多个端口， LLDP/CDP 在每个端口上传输数据包时，将不考虑端口是否在 LAG 内。
- LLDP/CDP 操作与一个端口的 STP 状态互不相关。
- 如果某一端口上启用了 802.1X 访问控制，只有当端口被验证和授权时，交换机才传输和接收通过此端口的 LLDP/CDP 数据包。
- 如果某一端口是一个镜像目标端口， LLDP/CDP 将会认为此端口断开。

设置 LLDP

LLDP 可让网络管理员进行故障排除，并通过在多供应商环境中发现和维护网络拓扑来增强网络管理。 LLDP 通过标准化网络设备向其他系统通告自身存在以及存储所发现信息的方法，来发现网络邻居。

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 （Management Information Base， MIB）中。网络管理系统会通过查询这些 MIB 数据库来为网络拓扑建模。

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

LLDP 协议有一个名为 LLDP 介质端点发现 （LLDP Media Endpoint Discovery，LLDP MED）的扩展协议，该扩展协议可提供和接受来自语音或视频设备的信息。

本节介绍如何设置 LLDP 功能，包括以下操作 （请按建议的顺序执行）：

- 在 “属性”页面全局启用 LLDP （默认为启用）并设置 LLDP 全局参数。详见 “设置 **LLDP** 属性”。
- 在 “端口设置”页面设置每个端口的 LLDP 功能。在此页面，端口可以设置为接收或传输 LLDP PDU 以及指定要通告的 TLV。详见 “定义 **LLDP** 端口设置”。
- 在 “LLDP MED 网络策略”页面创建 LLDP MED 网络策略。详见 “设置 **LLDP MED** 网络策略”。
- 在 “LLDP MED 端口设置”页面将创建的 LLDP MED 网络策略关联到端口。详见 “**LLDP MED** 端口设置”。
- 在 “LLDP 端口状态”页面查看 LLDP 全局信息以及每个端口的 LLDP 状态。详见 “查看 **LLDP** 端口状态”。
- 在 “LLDP 本地信息”页面查看 LLDP 本地端口状态。详见 “查看 **LLDP** 本地信息”。
- 在 “LLDP 邻居”页面查看从邻居发现的 LLDP 信息。详见 “查看 **LLDP** 邻居信息”。
- 在 “LLDP 统计信息”页面查看每个端口的 LLDP 统计信息。详见 “查看 **LLDP** 统计信息”。
- 在 “LLDP 过载”页面查看 LLDP 过载信息。详见 “查看 **LLDP** 过载信息”。

设置 LLDP 属性

使用 “属性”页面可全局启用或禁用 LLDP 以及设置 LLDP 基本属性。

设置 LLDP 属性的步骤：

步骤 1 单击 “管理” > “发现协议 - **LLDP**” > “属性”。

步骤 2 设定以下参数：

- **LLDP** 状态 — 全局启用或禁用交换机上的 LLDP （默认为启用）。
- **LLDP** 帧处理 — 如果全局禁用 LLDP，选择如何处理接收到的符合条件的 LLDP 帧。可选项如下：
  - *过滤* — 删除数据包。
  - *桥接* — （VLAN 有意识泛洪）转发数据包到所有 VLAN 成员端口。
  - *泛洪* — 转发 LLDP 数据包到所有端口。
- **TLV** 通告间隔 — 设定发送 LLDP 通告更新的速率 （以秒为单位）。
  - *使用默认设置* — 选择此选项，使用默认的 TLV 通告间隔值 （30 秒）。
  - *用户定义* — 选择此选项，手动输入发送 LLDP 通告更新的速率。
- 保留时间 （以倍数表示）— 设定在丢弃 LLDP 数据包之前保留这些数据包的时间，一般为 TLV 通告间隔的倍数。例如，如果 TLV 通告间隔为 30 秒，而此选项设为 4，则会在 120 秒后丢弃 LLDP 数据包。
  - *使用默认设置* — 选择此选项，使用默认值 （默认为 4 倍）。
  - *用户定义* — 选择此选项，手动输入保留倍数值。
- 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）。
  - *使用默认设置* — 选择此选项，使用默认值 （默认为 2 秒）。
  - *用户定义* — 选择此选项，手动输入禁用 LLDP 与重新初始化 LLDP 之间的时间间隔。
- 传输延迟 — 设定由 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）。
  - *使用默认设置* — 选择此选项，使用默认值 （默认为 2 秒）。
  - *用户定义* — 选择此选项，手动输入传输延迟时间。

步骤 3 在 “快速启动重复计数”字段中，输入初始化 LLDP MED 快速启动机制时发送 LLDP 数据包的次数。有新的端点设备连接至交换机时会发生这种情况。

步骤 4 单击 “应用”。设置 LLDP 属性，并更新交换机的当前配置。

定义 LLDP 端口设置

使用 “端口设置”页面可在每个端口上激活 LLDP 并设定在 LLDP PDU 中发送的 TLV。

设定 LLDP 端口设置的步骤：

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

步骤 2 选择一个端口，然后单击 “编辑”。

步骤 3 设定以下参数：

- 接口 — 选择要设置的端口。
- 管理状态 — 为端口选择 LLDP 发布选项。可选项如下：
  - *仅传输* — 只发布不发现。
  - *仅接收* — 只发现不发布。
  - *传输和接收* — 发布并发现。
  - *禁用* — 表示在该端口上禁用 LLDP。
- 可用的可选 **TLV** — 通过将 TLV 移动到 “选定的可选 **TLV**” 列表中，来选择要由交换机发布的信息。可选的 TLV 包含：
  - *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）。
  - *系统说明* — 对网络实体的描述 （使用字母数字格式）。它包括系统名称、硬件版本、操作系统和交换机支持的网络软件。
  - *系统功能* — 交换机的主要功能，以及是否已在交换机中启用这些功能。这些功能由两个八进制数表示。 0 到 7 位分别表示其他、中继器、网桥、WLAN AP、路由器、电话、DOCSIS 电缆设备以及工作站。8 到 15 位为保留位。
  - *802.3 MAC-PHY* — 双工和比特率功能以及发送设备的当前双工和比特率设置。它还指出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）。它还指出链路当前是否已聚合；如果是，则提供聚合的端口标识符。
- *802.3 最大帧大小* — MAC/PHY 实施的最大帧大小功能。
- *管理 IP 地址* — 交换机的管理 IP 地址。

步骤 4 单击 “应用”。修改 LLDP 端口设置，并更新交换机的当前配置。

设置 LLDP MED 网络策略

LLDP 介质端点发现 （LLDP MED）是 LLDP 的增强功能，提供其他功能以支持介质设备。 LLDP MED 具备以下功能：

- 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）和紧急电话服务（E-911），则使用 IP 电话位置信息。

注释 交换机会根据你的配置自动通告策略；但是，您还必须将交换机手动配置为使用该策略。

LLDP MED 网络策略是某些特定实时应用 （如语音或视频）的一组相关配置的集合。配置之后，网络策略将包含在附加到相连接的 LLDP 媒体终端设备的传出 LLDP 数据包中。而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。

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网络策略的端口。管理员负责根据网络策略及其关联的端口，手动创建 VLAN 及其端口成员关系。

设置 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”。

步骤 2 在 “适用于语音应用的 **LLDP MED** 网络策略”字段，如勾选 “启用”，交换机将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。

步骤 3 单击 “应用”。

步骤 4 单击 “添加”，添加 LLDP MED 网络策略。

步骤 5 设定以下参数：

- 网络策略编号 — 选择要创建的 LLDP MED 网络策略编号。
- 应用 — 从列表中选择网络策略通告的应用程序类型 （流量类型）。可选项包括：

- 语音
- 语音信令
- 访客语音
- 访客语音信令
- 软件电话语音
- 视频会议
- 流媒体视频
- 视频信令

- **VLAN ID** — 输入要向其发送流量的 VLAN。
- **VLAN** 标记 — 选择是否为流量添加标签。
- 用户优先级 — 选择要应用到此网络策略所定义的流量的优先级。
- **DSCP** 值 — 选择与邻居所发送的应用程序数据相关联的 DSCP 值。该值可告诉邻居应如何标记他们发送给交换机的应用程序流量。

步骤 6 单击 “应用”。设置 LLDP MED 网络策略，并更新交换机的当前配置。

LLDP MED 端口设置

使用 “LLDP MED 端口设置”页面可选择端口上要通告的 LLDP MED 网络策略以及要在 LLDP PDU 内发送的 LLDP MED TLV。

在每个端口上设置 LLDP MED 网络策略的步骤：

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

步骤 2 如需将 LLDP MED 网络策略与端口相关联，选择一个端口然后单击 “编辑”。

步骤 3 设定以下参数：

- 接口 — 选择要配置的端口。
- **LLDP MED** 状态 — 在此端口上启用或禁用 LLDP MED 功能。
- 可用的可选 **TLV** — 通过将 TLV 移动到“选定的可选 **TLV**”列表中，来选择可由交换机通告的 TLV。

- 可用的网络策略 — 通过将 LLDP MED 网络策略移动到 “选定的网络策略”列表中，来选择将由 LLDP 通告的 LLDP MED 网络策略。这些策略是在 “LLDP MED 网络策略”页面中创建的。

  注　必须按照 LLDP MED 标准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 通告的坐标位置。
- 位置城镇地址 — 输入要由 LLDP 通告的城市地址。
- 位置 **ECS ELIN** — 输入要由 LLDP 通告的紧急电话服务 （ECS）ELIN 位置。

步骤 4 单击 “应用”。修改 LLDP MED 端口设置，并更新交换机的当前配置。

步骤 5 如需查看 LLDP 本地信息详情，选择一个端口然后单击 “**LLDP** 本地信息详情”。转到 “LLDP 本地信息”页面。

查看 LLDP 端口状态

“LLDP 端口状态”页面显示 LLDP 全局信息以及每个端口的 LLDP 状态。

查看 LLDP 端口状态的步骤：

步骤 1 单击 “管理” > “发现协议 - **LLDP**” > “**LLDP** 端口状态”。

显示以下 LLDP 全局信息：

- 机箱 **ID** 子类型 — 机箱 ID 的类型 （如 MAC 地址）。
- 机箱 **ID** — 机箱标识符。当机箱 ID 子类型为 MAC 地址时，会显示为交换机的 MAC 地址。
- 系统名称 — 交换机的名称。
- 系统说明 — 交换机的描述信息。
- 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”显示每个端口的以下 LLDP 信息：

- 接口 — 端口标识符。
- **LLDP** 状态 — LLDP 发布选项。

- **LLDP MED** 状态 — 端口是否启用或禁用 LLDP MED 网络策略。
- 本地 **PoE** —（仅适用于支持 PoE 的交换机型号）通告的本地 PoE 信息，包括电源类型、电源、电源优先级和功率值。
- 远程 **PoE** —（仅适用于支持 PoE 的交换机型号）邻居通告的 PoE 信息，包括电源类型、电源、电源优先级和功率值。
- 邻居数量 — 发现的 LLDP 邻居数量。
- 第一台设备的邻居功能 — 显示邻居的主要功能，如网桥或路由器。

步骤 2 如需查看发送给邻居的 LLDP 和 LLDP MED TLV 的详细信息，选择一个端口然后单击“**LLDP** 本地信息详情”。转到 “LLDP 本地信息”页面。

步骤 3 如需查看邻居发送来的 LLDP 和 LLDP MED TLV 的详细信息，选择一个端口然后单击“**LLDP** 邻居信息详情”。转到 “LLDP 邻居”页面。

查看 LLDP 本地信息

“LLDP 本地信息”页面显示端口上通告的 LLDP 本地端口状态。

查看在端口上通告的 LLDP 本地端口状态的步骤：

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

步骤 2 选择要查看的端口。此页面显示以下信息：

全局

- 机箱 **ID** 子类型 — 机箱 ID 的类型 （如 MAC 地址）。
- 机箱 **ID** — 机箱标识符。当机箱 ID 子类型为 MAC 地址时，会显示交换机的 MAC 地址。
- 系统名称 — 交换机的名称。
- 系统说明 — 交换机的描述信息。
- 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。
- 地址 — 返回的最适合管理用途的地址。
- 接口子类型 — 用于定义接口编号的编号方法。
- 接口编号 — 与此管理地址相关联的具体接口。

MAC/PHY 详情

- 支持自动协商 — 端口是否支持速度自动协商。
- 已启用自动协商 — 端口当前是否启用或禁用速度自动协商。
- 自动协商通告功能 — 端口速度自动协商通告的功能。
- 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。

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 — 指出是否可以聚合端口。
- 聚合状态 — 指出是否已聚合端口。
- 聚合端口 **ID** — 通告的聚合端口 ID。

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。
- **PoE** 设备类型 — （仅适用于支持 PoE 的交换机型号）端口的 PoE 类型。
- **PoE** 电源 — （仅适用于支持 PoE 的交换机型号）端口电源。
- **PoE** 电源优先级 — （仅适用于支持 PoE 的交换机型号）端口电源优先级。
- **PoE** 功率值 — （仅适用于支持 PoE 的交换机型号）端口电源功率值。

- 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

按 ANSI-TIA-1057 标准中的 10.2.4 款所述，以十六进制字符显示以下信息：

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

网络策略表

- 应用类型 — 网络策略应用程序类型。
- **VLAN ID** — 网络策略中定义的 VLAN。
- **VLAN** 类型 — 网络策略中定义的 VLAN 类型。该字段的值可能为：
  - *已标记* — 表示网络策略针对添加标签的 VLAN 定义。
  - *未标记* — 指示网络策略针对未添加标签的 VLAN 定义。
- 用户优先级 — 网络策略用户优先级。
- **DSCP** — 网络策略 DSCP 值。

步骤 **3** 单击 “端口状态表”，转到 “LLDP 端口状态”页面。

查看 LLDP 邻居信息

“LLDP 邻居信息”页面显示了使用来自相邻设备的 LLDP 协议接收的信息。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”。

步骤 2 选择一个本地端口，单击 “确定”。

“LLDP 邻居表”显示与所选端口相关的 LLDP 邻居信息：

- 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 相邻设备的机箱的标识符。
- 端口 **ID** 子类型 — 显示的端口标识符的类型。
- 端口 **ID** — 端口标识符。
- 系统名称 — 已发布的交换机名称。
- 存活时间 — 在其后删除该邻居的信息的时间间隔 （以秒为单位）。

步骤 3 单击 “详情”，查看端口的 LLDP 状态的详细信息。

步骤 4 单击 “刷新”，刷新 “LLDP 邻居表”显示的数据。

查看 LLDP 统计信息

“LLDP 统计信息”页面显示每个端口的 LLDP 统计信息。

查看 LLDP 统计信息的步骤：

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

此页面显示每个端口的 LLDP 统计信息：

- 接口 — 端口标识符。
- 传输的帧数 （总数）— 已传输的帧数。
- 接收的帧数：

- *总数* — 已接收帧的总数。
- *已丢弃* — 已丢弃的已接收帧数。
- *错误* — 已接收的帧中发生错误的总数。

- 接收的 **TLV**：
  - *已丢弃* — 已丢弃的已接收 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 — 端口上删除的邻居总数。

步骤 2 单击 “刷新”，刷新 “LLDP 统计信息表”显示的数据。

查看 LLDP 过载信息

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并超过端口所支持的最大 PDU 大小时，就会发生 LLDP 过载。

“LLDP 过载”页面显示 LLDP 或 LLDP MED 信息的字节数、其他 LLDP 信息的可用字节数以及每个端口的 LLDP 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”。

“LLDP 过载表”显示每个端口的 LLDP 过载信息：

- 接口 — 端口标识符。
- 正在使用的字节总数 — 每个数据包中 LLDP 信息的字节总数。
- 剩余可用字节 — 要添加到数据包中的其他 LLDP 信息的剩余可用字节总数。
- 状态 — TLV 正被传输还是已过载。

步骤 2 要查看端口的 LLDP 过载详细信息，选择相应的端口然后单击 “详情”。

显示以下信息：

LLDP 强制 **TLV**

- 大小 （字节）— 强制 TLV 的字节总数。
- 状态 — 强制 TLV 组正被传输还是已过载。

LLDP MED 功能

- 大小 （字节）— LLDP MED 功能 TLV 数据包的字节总数。
- 状态 — LLDP MED 功能 TLV 数据包已传输还是已过载。

LLDP MED 位置

- 大小 （字节）— LLDP MED 位置数据包的字节总数。
- 状态 — LLDP MED 位置数据包已传输还是已过载。

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 网络策略数据包已传输还是已过载。

通过 **MDI** 提供的 **LLDP MED** 扩展电源

- 大小 （字节）— LLDP MED 通过 MDI 提供的扩展电源数据包的字节总数。
- 状态 — LLDP MED 通过 MDI 提供的扩展电源数据包已传输还是已过载。

802.3 TLV

- 大小 （字节）— LLDP 802.3 TLV 数据包的字节总数。
- 状态 — LLDP 802.3 TLV 数据包已传输还是已过载。

LLDP 可选 **TLV**

- 大小 （字节）— LLDP 可选 TLV 数据包的字节总数。
- 状态 — LLDP 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 数据包的字节总数。
- 状态 — LLDP MED 清单 TLV 数据包已传输还是已过载。

802.1 TLV

- 大小 （字节）— LLDP 802.1 TLV 数据包的字节总数。
- 状态 — LLDP 802.1 TLV 数据包已传输还是已过载。

总数

- 总数 （字节）— 每个数据包中 LLDP 信息的总字节数。

- 剩余可用字节 — 要添加到各数据包中的其他 LLDP 信息的剩余可用字节总数。

设置 CDP

与 LLDP 相似， CDP 是一个链路层协议，针对直接连接到交换机的邻居设备通告其自身和相互之间通告功能。与 LLDP 不同的是， CDP 是一个思科专属的协议。

设置 CDP 属性

使用 “CDP 属性”页面可全局启用或禁用 CDP 并设置 CDP 全局参数。

设置 CDP 属性的步骤：

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

STEP 1 设定以下参数：

- **CDP** 状态 — 选择全局启用或禁用 CDP 功能。
- **CDP** 帧处理 — 如果 CDP 功能被禁用，选择当交换机接收到匹配所选标准的数据包时采取何种措施处理 CDP 帧。可选项如下：
  - *桥接* — （VLAN 有意识泛洪）基于 VLAN 转发数据包。
  - *过滤* — 删除数据包。
  - *泛洪* — （VLAN 无意识泛洪）转发传入 CDP 数据包到入站端口之外的所有端口。
- **CDP** 语音 **VLAN** 通告 — 启用此功能，交换机将在启用 CDP 的所有端口以及语音 VLAN 的成员端口上在 CDP 数据包中通告语音 VLAN。
- **CDP** 强制 **TLV** 验证 — 启用此功能，将丢弃不包含强制 TLV 的传入 CDP 数据包，并且增加无效错误计数器的计数。
- **CDP** 版本 — 选择要使用的 CDP 版本。
- **CDP** 保持时间 — 表示在丢弃数据包之前保留 CDP 数据包的时间 （以秒为单位），一般为 TLV 通告间隔的倍数。例如，如果 TLV 通告间隔为 30 秒，保持时间倍数为 4，那么 CDP 数据包在 120 秒后将被丢弃。可选项如下：
  - *使用默认设置* — 使用默认值 （默认为 180 秒）。

- *用户定义* — 手动输入 CDP 保持时间。

- **CDP** 传输速率 — 表示发送 CDP 通告更新的速率（以秒为单位）。可选项如下：
  - *使用默认设置* — 使用默认的传输速率 （默认为 60 秒）。
  - *用户定义* — 手动输入传输速率。
- 设备 **ID** 格式 — 选择设备 ID 的格式，如 MAC 地址、序列号或主机名。
- 源接口 — 选择在帧 TLV 中使用的 IP 地址。可选项如下：
  - *使用默认设置* — 使用传出接口的 IP 地址。
  - *用户定义* — 使用地址 TLV 中接口 （在 “接口”字段定义）的 IP 地址。
- 接口 — 如选择自定义源接口，在此字段选择相应的源接口。
- 系统日志语音 **VLAN** 不匹配 — 勾选“启用”，当检测到一个语音 VLAN 不匹配（在传入帧中的语音 VLAN 信息与本地设备通告的语言 VLAN 不匹配）时，发送一条系统日志。
- 系统日志本征 **VLAN** 不匹配 — 勾选“启用”，当检测到一个本征 VLAN 不匹配（在传入帧中的本征 VLAN 信息与本地设备通告的本征 VLAN 不匹配）时，发送一条系统日志。
- 系统日志双工不匹配 — 勾选 “启用”，当检测到一个双工不匹配 （在传入帧中的双工信息与本地设备通告的双工信息不匹配）时，发送一条系统日志。

步骤 **2** 单击 “应用”。保存 CDP 属性配置，并更新交换机的当前配置。

定义 CDP 端口设置

使用 “端口设置”页面可启用或禁用每端口的 CDP 功能。当与 CDP 邻居发生冲突时，系统会触发通知功能。冲突可以是与语音数据、本征 VLAN 或双工的冲突。

定义 CDP 端口设置的步骤：

步骤 **1** 单击 “管理” > “发现协议 - **CDP**” > “端口设置”。

显示以下 CDP 信息：

- 接口 — 端口标识号。
- **CDP** 状态 — 端口是否启用或禁用 CDP。

- 报告与 **CDP** 邻居冲突 — 是否启用或禁用报告与 CDP 邻居冲突选项 （如语音 VLAN/ 本征 VLAN/ 双工）。
- 邻居数量 — 检测到的邻居数。

步骤 2 如需编辑端口的 CDP 设置，选择一个端口，然后单击 “编辑”。

步骤 3 设定以下参数：

- 接口 — 选择要设置的端口。
- **CDP** 状态 — 选择启用或禁用 CDP 发布选项。

  注　以下三个选项只有在交换机被设置为发送 Trap 到管理站点时可选。
- 系统日志语音 **VLAN** 不匹配 — 勾选 “启用”，当检测到一个语音 VLAN 不匹配（在传入帧中的语音 VLAN 信息与本地设备通告的语言 VLAN 不匹配）时，发送一条系统日志。
- 系统日志本征 **VLAN** 不匹配 — 勾选 “启用”，当检测到一个本征 VLAN 不匹配（在传入帧中的本征 VLAN 信息与本地设备通告的本征 VLAN 不匹配）时，发送一条系统日志。
- 系统日志双工不匹配 — 勾选 “启用”，当检测到一个双工不匹配 （在传入帧中的双工信息与本地设备通告的双工信息不匹配）时，发送一条系统日志。

步骤 4 单击 “应用”。修改 CDP 端口设置，并更新交换机的当前配置。

查看 CDP 本地信息

“CDP 本地信息”页面显示由 CDP 协议通告的有关本地设备的信息。

查看 CDP 本地信息的步骤：

步骤 1 单击 “管理” > “发现协议 - **CDP**” > “**CDP** 本地信息”。

步骤 2 选择要查看 CDP 本地信息的端口。

显示以下信息：

- **CDP** 状态 — 显示此端口是否启用或禁用 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。

- 地址 **TLV**
  - *地址 （x）* — 设备 ID TLV 中通告的 IP 地址。
- 端口 **TLV**
  - *端口 ID* — 端口 TLV 中通告的端口 ID。
- 功能 **TLV**
  - *功能* — 端口 TLV 中通告的功能 TLV。
- 版本 **TLV**
  - *版本* — 设备正在运行的软件版本信息。
- 平台 **TLV**
  - *平台* — 平台 TLV 中通告的平台 ID。
- 本征 **VLAN TLV**
  - *本征 VLAN* — 本征 VLAN TLV 中通告的本征 VLAN ID。
- 全 / 半双工 **TLV**
  - *双工* — 全双工 / 半双工 TLV 中通告的端口是否为全双工 / 半双工。
- 设备 **TLV**
  - *设备 ID* — 连接到设备 TLV 中通告的端口的设备类型。
  - *设备 VLAN ID* — 设备使用的 VLAN。如果设备为一台 IP 电话，那么此字段显示为语音 VLAN。
- 用于不可信端口 **TLV** 的 **CoS**
  - *用于不可信端口的 CoS/802.1p* — 如果此端口的扩展信任功能被关闭，此字段显示二层 CoS 值和 802.1D/802.1p 优先级值。此 CoS 值为设备标记为不可信端口所接收的全部数据包的 CoS 值。
- 功率 **TLV** （仅适用于支持 **PoE** 功能的交换机）
  - *请求 ID* —（仅适用于支持 **PoE** 功能的交换机）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* —（仅适用于支持 **PoE** 功能的交换机）当可用功率或管理电源等级字段值发生更改时，该值将增加 1 （或 2，避免 0）。

当收到电源请求 TLV，其中请求 ID 字段与最后接收的集 （或收到首个值时）不同时，端口转换为 “关闭”。

- *可用功率* — （仅适用于支持 **PoE** 功能的交换机）此端口消耗的电源量。
- *管理电源等级* — （仅适用于支持 **PoE** 功能的交换机）显示供电器对受电设备功耗 TLV 的请求。此字段始终显示为 “No Preference （无偏好）”。

查看 CDP 邻居信息

“CDP 邻居信息”页面显示从相邻设备收到的 CDP 信息。超时 （根据在其间未收到邻居发送的 CDP PDU 的邻居存活时间 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”。

步骤 2 选择一个本地端口，单击 “确定”。

显示以下信息：

- 设备 **ID** — 相邻设备的 ID。
- 本地接口 — 相邻设备连接的本地端口号。
- 通告版本 — CDP 协议版本。
- 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 — 邻居通告的功能。
- 平台 — 来自邻居的平台 TLV 的信息。
- 邻居接口 — 邻居的外发端口。

步骤 3 如需查看 CDP 邻居的详细信息，单击 “详情”。

显示以下信息：

- 设备 **ID**— 邻居设备的标识符。
- 本地接口 — 帧到达所经由的端口号。
- 通告版本 — CDP 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、 VLAN 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 — 邻居平台的标识符。
- 邻居接口 — 帧到达所经由的邻居的接口编号。
- 本征 **VLAN**— 邻居的本征 VLAN。
- 双工 — 邻居接口处于半双工还是全双工模式。
- 地址 — 邻居的地址。
- 功率消耗 — 接口上由邻居消耗的电源量。
- 版本 — 邻居的软件版本。

步骤 **4** 单击 “清除表”，断开所有连接的 CDP 设备。

步骤 **5** 单击 “刷新”，刷新页面信息。

查看 CDP 统计信息

“CDP 统计信息”页面显示从端口发送或接收的 CDP 帧的相关信息。

CDP 统计信息只有当交换机在全局和在端口上都启用 CDP 的情况下才能显示。

查看 CDP 统计信息的步骤：

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

显示以下 CDP 统计信息：

- 接口 — 端口标识符。
- 已接收的数据包数 — 显示每个接口已接收的不同类型数据包的计数器。
  - *版本 1*— 显示已接收的 CDPv1 数据包的数量。
  - *版本 2*— 显示已接收的 CDPv2 数据包的数量。
  - *总数* — 显示已接收的 CDP 数据包的总数。
- 已传输的数据包数 — 显示每个接口已发送的不同类型数据包的计数器。
  - *版本 1*— 显示已发送的 CDPv1 数据包的数量。

- *版本 2*— 显示已发送的 CDPv2 数据包的数量。
- *总数* — 显示已发送的 CDP 数据包的总数。

▪ **CDP** 错误统计信息 — 显示 CDP 错误计数器，包括：

- *非法校验和* — 已接收带有非法的校验和值的错误数据包的数量。
- *其他错误* — 已接收的带有其他非法校验和的错误数据包的数量。
- *邻居数超过最大值* — 数据包信息因为缺少空间而不能存储到缓存的最大次数。

步骤 **2** 选择一个端口并单击 “清除接口计数器”，清除单个端口的 CDP 统计信息计数器。

步骤 **3** 单击 “清除所有接口计数器”，清除所有端口的 CDP 统计信息计数器。

步骤 **4** 单击 “刷新”，刷新所有端口的 CDP 统计信息。

9

端口管理

本章介绍端口配置、链路聚合和节能以太网等功能，包含以下内容：

- 端口管理工作流程
- 设置端口基本配置
- 设置错误恢复配置
- 设置链路聚合
- 设置节能以太网

端口管理工作流程

要配置端口，请执行以下操作：

步骤 1 在 “端口设置”页面设置端口的基本配置。详见 “设置端口基本配置”。

步骤 2 在 “错误恢复设置”页面启用或禁用端口从故障状态中自动恢复功能或手动重新激活已挂起的端口。详见 “设置端口基本配置”。

步骤 3 在 “LAG 管理”页面启用或禁用链路聚合控制协议，并将潜在成员端口设置为所需的链路聚合组 （LAG）。默认情况下，所有 LAG 均没有端口成员。详见 “设置 **LAG** 算法”。

步骤 4 在 “LAG 设置”页面设置 LAG 的速度和自动协商等功能。详见 “定义 **LAG** 设置”。

步骤 5 在 “LACP”页面设置 LAG 的成员端口或候选成员端口的 LACP 参数。详见 “设置 **LACP**”。

步骤 6 在 “节能以太网”页面启用或禁用每端口的节能以太网功能。详见 “设置节能以太网”。

步骤 7 如果交换机支持并启用 PoE 功能，则按 “设置以太网供电”章节中所述设置交换机的 PoE 端口。

设置端口基本配置

使用 “端口设置”页面可全局设置巨型帧功能以及修改每端口的设置。

注释 同时使用两个端口时， SFP 光纤优先级较高。

定义端口设置的步骤：

步骤 1 单击 “端口管理” > “端口设置”。

步骤 2 在 “巨型帧”字段，启用或禁用巨型帧功能。如启用此功能，交换机可支持最大 10000 字节的数据包。如禁用此功能 （默认为禁用），交换机最大可支持 1522 字节的数据包。

步骤 3 单击 “应用”。保存端口的全局设置，并更新交换机的当前配置。

步骤 4 如需修改单个端口的设置，选择相应的端口然后单击 “编辑”。

步骤 5 设定以下参数：

- 接口 — 选择要设置的端口。
- 端口说明 — 输入端口名称。
- 端口类型 — 显示端口类型。
- 管理状态 — 选择当重新启动交换机时端口应处于运行状态 （启用）还是非运行状态 （禁用）。
- 运行状态 — 显示端口当前是否启用或禁用。
- 自动协商 — 勾选 “启用”，在端口上启用自动协商功能。自动协商可使端口向其他设备通告其传输速率、双工模式和流量控制能力。
- 运行自动协商 — 显示端口当前是否启用或禁用自动协商功能。
- 管理端口速度 — 选择端口的速率。端口类型决定了可用的速度设置选项。仅当端口禁用自动协商时，您才可以设置其管理速度。
- 运行端口速度 — 显示端口的当前速度。

- 管理双工模式 — 选择端口的双工模式。仅当端口禁用自动协商时功能才可设置其双工模式。可选项如下：
  - *半双工* — 端口仅支持交换机和客户端之间在某一时刻的单向传输。
  - *全双工* — 端口支持交换机和客户端之间的同时双向传输。
- 运行双工模式 — 显示端口的当前双工模式。
- 自动通告速度 — 选择要由端口通告的速度。可选项如下：
  - *全速* — 可以接受所有端口速度设置。
  - *10M* — 10 Mbps 速度。
  - *100M* — 100 Mbps 速度。
  - *10/100M* — 10 或 100 Mbps 速度。
  - *1000M* — 1000 Mbps 速度。
- 自动通告双工 — 选择要由端口通告的双工模式。可选项如下：
  - *所有双工模式* — 可以接受所有双工模式。
  - *半双工* — 端口支持交换机和客户端之间在某一时刻的单向传输。
  - *全双工* — 端口支持交换机和客户端之间的同时双向传输。
- 运行通告 — 显示端口当前通告的速度和双工模式。
- 背压 — 在端口上启用背压模式（配合使用半双工模式），可以降低交换机拥挤时的数据包接收速度。启用背压模式会禁用远程端口，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）功能。
- 当前流量控制 — 显示端口当前是否启用或禁用 802.3X 流量控制功能。
- 受保护的端口 — 勾选 “启用”，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）。受保护的端口具有以下功能：
  - 受保护的端口可在共享同一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输出端口。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 均可设置为 “受保护的”或 “不受保护的”。

- **LAG** 中的成员 — 如果此端口是某一LAG的成员端口，那么在此字段显示其所属的 LAG 编号。否则此字段显示为空。

步骤 6 单击 “应用”。修改端口设置，并更新交换机的当前配置。

设置错误恢复配置

使用 “错误恢复设置”页面可全局设置自动恢复间隔，启用或禁用端口从特定原因造成的故障状态中恢复。用户也可以手动重新激活挂起的端口。

设置错误恢复配置的步骤：

步骤 1 单击 “端口管理” > “错误恢复设置”。

步骤 2 设定以下全局参数：

- 自动恢复间隔 — 输入端口从故障状态中自动恢复的时间。此间隔设置适用于所有的故障恢复原因。默认为 300 秒。

- 端口假死自动恢复 — 启用或禁用端口从各种故障状态中自动恢复。可选项如下：

  - *ACL* — 当由于访问控制列表功能而导致端口挂起时，启用此选项会进行自动恢复。

  - *ARP 检测* — 当由于 ARP 检测功能而导致端口挂起时，启用此选项会进行自动恢复。

  - *BPDU 防护* — 当由于 BPDU 防护功能导致端口挂起时，启用此选项会进行自动恢复。

  - *广播泛洪* — 当由于广播泛洪功能而导致端口挂起时，启用此选项会进行自动恢复。

  - *DHCP 速率限制* — 当由于 DHCP 速率限制功能而导致端口挂起时，启用此选项会进行自动恢复。

  - *PoE* —（此选项仅适用于支持 PoE 功能的交换机型号）当由于 PoE 功能而导致端口挂起时，启用此选项会进行自动恢复。

  - *端口安全* — 当由于端口安全功能而导致端口挂起时，启用此选项会进行自动恢复。

- *自环回* — 当由于自身回路侦测功能导致端口挂起时，启用此选项会进行自动恢复。
- *单播泛洪* — 当由于单播泛洪功能而导致端口挂起时，启用此选项会进行自动恢复。
- *未知组播泛洪* — 当由于未知组播泛洪功能而导致端口挂起时，启用此选项会进行自动恢复。

步骤 3 单击 “应用”。定义端口的错误恢复设置，并更新交换机的当前配置。

步骤 4 “挂起的接口表”显示交换机当前所有挂起的端口。如需手动重新激活挂起的端口，选择此端口然后单击 “重新激活”。

设置链路聚合

链路聚合控制协议 （Link Aggregation Control Protocol， 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。链路聚合通过将多个端口链接在一起形成一个链路聚合组 （LAG）来优化端口的使用。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。

交换机支持两种类型的 LAG：

- 静态 — 如果禁用 LACP，则 LAG 为静态 LAG。分配给静态 LAG 的端口组始终为活动成员。手动创建 LAG 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 — 如果启用 LACP，则 LAG 为动态 LAG。您可以将一组端口定义为动态 LAG 的候选端口。LACP 可确定来自 LAG 的哪些候选端口为活动的成员端口。非活动成员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 层数据包报头信息分布单播流量。组播数据包的运作方式与单播数据包相同。

交换机支持两种负载均衡算法：

- 按 **MAC** 地址 — 根据所有数据包的目标和源 MAC 地址。

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

LAG 管理

LAG 中的活动成员端口可通过明确的用户分配进行静态定义，也可通过 LACP 进行动态选择。在本地设备和远程设备之间交换 LACP 信息后，LACP 选择流程会为 LAG 选择活动成员端口。

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

交换机支持 8 个 LAG。每个 LAG 均具有以下特性：

- LAG 中的所有端口必须属于相同的介质类型。
- 不得将某 LAG 中的端口分配给其他 LAG。
- 为静态 LAG 最多分配 8 个端口，并且最多有 16 个端口可以作为动态 LAG 的候选端口。
- 将端口添加到 LAG 后，LAG 配置将应用到此端口。从 LAG 中删除端口后，此端口将重新使用其初始配置。
- 生成树等协议将 LAG 中的所有端口视作一个端口。
- LAG 中的所有端口必须具有相同的 802.1p 优先级。

默认情况下，所有端口均不是 LAG 的成员，也不是 LAG 的候选成员。

静态和动态 LAG 配置流程

对于有成员端口的静态 LAG，无法启用 LACP。在编辑此静态 LAG 并删除所有成员端口之后， LACP 按钮才能启用。

要配置静态 LAG，请执行以下操作：

步骤 1 在 LAG 上禁用 LACP 可将其设置为静态 LAG。在 “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，可为静态 LAG 最多分配 8 个活动成员端口。详见 “设置 **LAG** 算法”。

步骤 2 使用 “LAG 设置”页面设置 LAG 的速度和流量控制。详见 “定义 **LAG** 设置”。

要配置动态 LAG，请执行以下操作：

步骤 1 在 LAG 上启用 LACP 可将其设置为动态 LAG。在 “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，可为动态 LAG 最多分配 16 个候选端口。详见 “设置 **LAG** 算法”。

步骤 2 使用 “LAG 设置”页面设置 LAG 的速度和流量控制。详见 “定义 **LAG** 设置”。

步骤 3 使用 “LACP”页面设置 LAG 中端口的 LACP 优先级和超时。详见 “设置 **LACP**”。

设置 LAG 算法

使用 “LAG 管理”页面可全局设置负载均衡算法和定义 LAG 中的成员端口。

设置 LAG 参数的步骤：

步骤 1 请单击 “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 — 按所有数据包的源和目标 MAC 地址执行负载均衡。
- **IP/MAC**地址 — 按所有数据包的目的和源IP地址以及目的和源MAC地址执行负载均衡。

步骤 3 单击 “应用”。设置负载均衡算法，并更新交换机的当前配置。

步骤 4 选择要配置的 LAG，然后单击 “编辑”。

步骤 5 设定以下参数：

- **LAG** — 选择要设置的 LAG。
- **LAG** 名称 — 输入 LAG 名称。
- **LACP** — 启用此选项可在所选的 LAG 上启用 LACP。此操作可使其成为动态 LAG。
- 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。您可以为每个静态 LAG 分配最多 8 个端口和为动态 LAG 分配最多 16 个端口。

步骤 6 单击 “应用”。设置 LAG 的成员端口，并更新交换机的当前配置。

定义 LAG 设置

使用 “LAG 设置”页面可查看和修改所有 LAG 的当前设置，并重新激活挂起的 LAG。

定义 LAG 设置的步骤：

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 设定以下参数：

- **LAG** — 选择要设置的 LAG。
- **LAG** 类型 — 显示组成 LAG 的端口类型。
- 说明 — 输入 LAG 名称。
- 管理状态 — 选择启用或禁用 LAG。
- 运行状态 — 显示 LAG 当前是否启用或禁用。
- 自动协商 — 在 LAG 上启用或禁用自动协商功能。自动协商是两个链路合作伙伴之间的协议，可使 LAG 向其合作伙伴通告自己的传输速率和流量控制 （流量控制默认为禁用）。建议在聚合链路的两端同时启用或禁用此功能，从而确保链路速度保持一致。
- 运行自动协商 — 显示当前的自动协商设置。
- 管理端口速度 — 如禁用自动协商功能，选择 LAG 的速度。
- 运行 **LAG** 速度 — 显示 LAG 当前的速度。
- 自动通告速度 — 选择要由 LAG 通告的速度。可选项如下：
  - *全速* — 所有速度均可接受。
  - *10M* — 仅通告 10 Mbps 速度。
  - *100M* — 仅通告 100 Mbps 速度。
  - *10/100M* — 仅通告 10 和 100 Mbps 速度。
  - *1000M*— 仅通告 1000 Mbps 速度。
- 运行通告 — 显示LAG 当前通告的功能。LAG 可将其功能通告给相邻的LAG，以开始协商流程。

- 背压 — 在 LAG 上选择“背压”模式（配合使用半双工模式），可降低交换机拥挤时的数据包接收速度。背压模式会禁用远程端口，从而避免其通过拥堵信令来发送数据包。
- 流量控制 — 在 LAG 上启用或禁用流量控制，或启用流量控制的自动协商功能。
- 当前流量控制 — 显示当前的流量控制设置。
- 受保护的端口 — 启用此功能，可使 LAG 成为受保护的端口，以接受第 2 层隔离保护。

步骤 4 单击 “应用”。修改 LAG 设置，并更新交换机的当前配置。

设置 LACP

动态 LAG 启用 LACP 功能，且 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 端口优先级都可以确定哪些候选端口成为动态 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。

通过将本地 LACP 系统优先级与远程 LACP 系统优先级作比较，可确定 LACP 端口优先级来自本地设备还是来自远程设备。优先级最低的设备将决定 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决定 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。其中，最多可有 8 个端口处于活动状态，而处于备用模式的端口也不能超过 8 个。如果动态 LAG 中的端口数超过 8 个，链路控制端上的交换机将使用端口优先级来确定将哪些端口捆绑到通道中，以及使哪些端口处于热备份模式。系统将忽略另一个交换机 （链路的非控制端）上的端口优先级。

在动态 LACP 中选择活动端口或备用端口所依据的其他规则如下：

- 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的优先级，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

为通过 LACP 创建一个动态 LAG，必须确保链路两端的端口都启用了 LACP 功能。也就是说，这些端口都应相互发送 LACP PDU 和处理接收到的 PDU。

但是，某些情况下一个链路伙伴可能暂时没有启用 LACP 功能。比如，当链路伙伴在一台正处于使用自动配置协议接收配置信息的过程中的设备上时，此设备的端口还没有设定 LACP 功能。如果 LAG 链路没有建立连接 （链路中断），那么此设备设置无法被设置。相似的情况在双 NIC 网络启动计算机上也会发生，两台 NIC 网络启动计算机只有在它们重启后才会接收到它们的 LAG 配置信息。

当多个启用了 LACP 功能的端口被设定时，将会从其中一个或多个端口建立链路连接。但是，当这些端口没有收到来自其链路伙伴的 LACP 响应时，建立链路连接的第一个端口将被加入到 LACP LAG 且成为其活动端口 （其他端口将成为 LAG 的非候选成员端口）。通过这种方式，相邻设备可以通过 DHCP 获取 IP 地址，并使用自动配置功能获取配置信息。

设置 LACP 参数

使用 “LACP”页面可 LACP 系统优先级、 LACP 超时和 LACP 端口优先级。

LACP 超时是发送和接收连续 LACP PDU 之间的时间间隔。在所有因素相同的情况下，当 LAG 的候选端口数大于活动端口允许的最大数时，交换机会从具有最高优先级的动态 LAG 中选择作为活动端口的端口。

注释 LACP 设置与非动态 LAG 的成员端口不相关。

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 在 “**LACP** 系统优先级”字段，输入全局 LACP 系统优先级值，以确定哪些候选端口将成为 LAG 的成员。

步骤 3 单击 “应用”。全局定义 LACP 系统优先级，并更新交换机的当前配置。

步骤 4 如需编辑端口的 LACP 设置，选择一个端口然后单击 “编辑”。

步骤 5 设定以下参数：

- 接口 — 选择要设置的端口。
- **LACP** 端口优先级 — 输入端口的 LACP 优先级值。
- **LACP** 超时 — 选择以较长还是较短的超时时间存储的邻居 LACP PDU 信息，邻居会对应以较长或较短的传输速率定期传输 LACP PDU。
- 模式 — 选择 LACP 模式：主动或被动。

步骤 6 单击 “应用”。修改端口的 LACP 设置，并更新交换机的当前配置。

设置节能以太网

节能以太网 （Energy Efficient Ethernet， EEE）可在链路没有流量传输时节省电源。使用此功能，当端口有连接但无流量时可有效地降低电能消耗。

在电量检测模式下，节能以太网功能可以降低总电能使用量。无需考虑其 LAG 成员关系，可按照每个端口来定义其节能以太网功能。

设置端口节能以太网功能的步骤：

步骤 1 单击 “端口管理” > “节能以太网” > “ 端口设置”。

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节能以太网功能。

步骤 4 单击 “应用”。保存端口的节能以太网设置，并更新交换机的当前配置。

10

设置以太网供电

以太网供电 （Power over Ethernet， PoE）功能仅在部分交换机型号上提供。详情可参考 “设备型号”一节获取哪些交换机型号支持 PoE 功能。

本章介绍如何使用 PoE 功能，包括以下内容：

- **PoE** 特性
- 交换机上的 **PoE**
- 设置 **PoE** 属性
- 定义 **PoE** 端口设置

PoE 特性

如果您的交换机支持 PoE 功能，请注意以下事项：

作为一种供电设备 （Power Sourcing Equipment， PSE），以下型号的交换机的 PoE 端口 （1-4）可向受电设备 （Powered Device， PD）提供最高 30 W 的功率，其他 PoE 端口可向受电设备提供最高 15.4 W 的功率。

型号	**PoE** 标称功率	**PoE** 端口	支持的 **PoE** 标准
SF220-24P	180W	1-24 均为 PoE 端口	端口 1-4 支持 802.3at 端口 5-24 支持 802.3af
SG220-26P	180W	1-24 均为 PoE 端口	端口 1-4 支持 802.3at 端口 5-24 支持 802.3af
SF220-48P	375W	1-48 均为 PoE 端口	端口 1-4 支持 802.3at 端口 5-48 支持 802.3af
SG220-50P	375W	1-48 均为 PoE 端口	端口 1-4 支持 802.3at 端口 5-48 支持 802.3af

作为一种供电设备，销售往中国大陆地区的以下型号的交换机的每 PoE 端口可向受电设备提供最高 30 W 的功率。

型号	PoE 标称功率	PoE 端口	支持的 PoE 标准
SF220-24P	180W	1-24 均为 PoE 端口	802.3at
SF220-48P	375W	1-48 均为 PoE 端口	802.3at
SG220-28MP	375W	1-24 均为 PoE 端口	802.3at

注意 在没有路由到外部设备的情况下， PoE 交换机只能连接到 PoE 网络。

注意 连接具有 PoE 功能的交换机时，请注意以下事项：

PoE 型号的交换机为供电设备，它们可向连接的受电设备供应直流电。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。由于要支持旧式 PoE，作为供电设备的 PoE 交换机可能会发生检测错误，将连接的供电设备 （包括其他 PoE 交换机）也当成旧式受电设备并为其供电。

尽管 PoE 交换机是供电设备，且因此应采用交流电供电，但它们也可能由于检测错误而被另一供电设备当作旧式受电设备供电。发生这种情况时， PoE 交换机可能无法正常工作，并且可能无法正确地为所连接的受电设备供电。

为防止检测错误，您应禁用用于连接供电设备的 PoE 交换机上端口的 PoE 功能。您还应先接通供电设备的电源，然后再将其连接到 PoE 交换机。如果某设备被错误地检测为受电设备，您应断开该设备与 PoE 端口的连接，并使用交流电源为其供电，然后再将其重新连接到 PoE 端口。

交换机上的 PoE

PoE 交换机作为供电设备，可通过现有的铜质电缆为连接的受电设备供电，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。

PoE 功能

PoE 具有如下功能：

- 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并大大降低安装成本

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 工作模式

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，开始供电设备与受电设备之间的协商。在协商过程中，受电设备指定其类别，这是受电设备所耗的最大功率。
- 功率消耗 — 分类阶段结束后，供电设备将为受电设备供电。如果受电设备支持 PoE 但未进行分类，则会将其假设为类别 0 （最大）。如果受电设备尝试消耗的功率超过了标准所允许的最大功率，则供电设备会停止为该端口供电。

PoE 支持两种模式：

- 端口限制 — 交换机同意提供的最大功率取决于系统管理员配置的值，与分类结果无关。

- 级别限制 — 交换机同意提供的最大功率取决于分类阶段的结果。这表示将根据客户端的请求设置最大功率。

PoE 配置注意事项

使用 PoE 功能需要考虑两个因素：

- 供电设备可以提供的最大功率
- 受电设备实际尝试消耗的功率

您可以决定：

- 在设备工作期间，将模式从级别限制更改为端口限制及从端口限制更改为级别限制时，系统将保留在端口限制模式下所设定的端口功率配置。

  注　只有当交换机要求受电设备重新连接时需要将供电模式。

- 端口限制模式下，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）。
- 当受电设备尝试消耗过多功率时生成 Trap，以及生成 Trap 时受电设备所耗功率占最大功率的百分比。

在级别限制模式下， PoE 特定硬件会根据连接到每个特定端口的设备的类别自动检测受电设备类别及其功率限制。

如果在连接的任意时刻，当所连接的受电设备从交换机请求的功率超过所分配的最大功率时 （不论交换机处于级别限制模式还是端口限制模式下），交换机都将：

- 保持 PoE 端口链路的连接状态
- 停止向此 PoE 端口供电
- 继续向其他 PoE 端口供电
- 记录停止供电的原因
- 生成 SNMP Trap

设置 PoE 属性

使用 “PoE 属性”页面可选择 PoE 供电模式 （端口限制模式或级别限制模式），指定是否生成 Trap。

这些设置需提前设定。当受电设备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。

在加电重新启动、初始化和系统配置过程中不输出功率，以确保不会损坏受电设备。

在交换机上配置 PoE 和监控当前功率使用的步骤：

步骤 **1** 单击 “端口管理” > “**PoE**” > “**PoE** 属性”。

步骤 **2** 设定以下参数：

- 供电模式 — 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。
  - *级别限制* — 由设备类别 （从分类阶段获取）决定每个端口的最大功率限制。

  注　　更改供电模式后，端口将重新连接。
- 传统 — 启用或禁用是否支持传统受电设备功能。此功能只有在建立连接协商时启作用。对于已经连接的传统受电设备，如果禁用此功能，只有在重新插拔线缆后才会被禁用。
- **Trap** — 启用或禁用 Trap 功能。如果启用 Trap，则还必须启用 SNMP 并至少设置一个 SNMP 通知接收设备。有关 SNMP 设置的详细信息，请参考 “设置 **SNMP**”一章的说明。
- 供电 **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，便会发出警报。

此页面还显示以下计数器：

- 运行状态 — PoE 交换机的运行状态。
- 标称功率 — 交换机可为连接的所有供电设备提供的总功率。
- 消耗的功率 — 当前由 PoE 端口消耗的总功率。
- 分配的功率 — 当前 PoE 端口预留的功率。
- 可用功率 — 当前可用的功率 （标称功率减去分配的功率）。

步骤 **3** 单击 “应用”。设置 PoE 属性，并更新交换机的运行时配置。

定义 PoE 端口设置

使用 “端口设置”页面可在端口上启用或禁用 PoE 功能并监控每个端口当前使用的功率以及允许的最大功率。

根据供电模式，交换机可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，交换机必须运行在 PoE 端口限制模式。当端口消耗的功率超过端口限制时，将会停止为端口供电。
- 级别限制 — 根据连接的受电设备的类别限制功率。要使这些设置生效，交换机必须运行在 PoE 级别限制模式。当端口消耗的功率超过类别限制时，将会停止为端口供电。

在某些情况下，交换机没有足够的功率，无法一次性为所有端口提供所允许的功率。要解决此问题，请为端口指定限制和优先级。例如，在所有 24 个端口上均允许 30 W 的功率，但由于功率限制 （所有端口最大可提供 370 W 的功率），由优先级决定为哪些端口供电，不为哪些端口供电。

定义 PoE 端口设置的步骤：

步骤 1 单击 “端口管理” > “**PoE**” > “**PoE** 端口设置”。

步骤 2 选择一个端口，然后单击 “编辑”。

步骤 3 设定以下参数：

- 端口 — 选择要设置的端口。
- **PoE** 管理状态 — 在端口上启用或禁用 PoE 功能。
- 电源优先级 — 选择供电不足时使用的端口优先级。例如，当系统供电不足时，并且受电设备插入到端口 1 （其供电优先级为高），此时系统将不会对哪些供电优先级低的端口进行供电。
- 管理功率分配 — 如供电模式被设置为端口限制，在此字段输入分配给端口的最大功率，单位为毫瓦。如端口支持的 PoE 标准为 802.3at，默认为 30000 mW ；如端口支持的 PoE 标准为 802.3af，默认为 15400 mW。

以下字段在所有设备上均显示：

- 最大功率分配 — 显示分配给连接到此端口的受电设备的最大功率 （以毫瓦为单位）。在级别限制模式下，最大功率分配一般由连接的受电设备上检测到的级别来确定，如 15.4W （802.3af, class 0 或 3）或 30W （802.3at, class 4）。在端口限制模式下，最大功率分配则根据端口支持的 PoE 标准来确定，如 15.4W （802.3af）或 30W （802.3at）。

- 功耗 — 显示连接到此端口的受电设备消耗的功率 （以毫瓦为单位）。
- 等级 — 当供电模式被设置为级别限制时，此字段显示连接的受电设备的级别信息。级别将决定功率等级。下表给出了不同级别预设的可分配功率值：

等级	交换机端口所提供的最大功率
Class 0	15.4 W
Class 1	4.0 W
Class 2	7.0 W
Class 3	15.4 W
Class 4	30.0 W

- 过载计数器 — 显示功率过载情况发生的总次数。
- 短路计数器 — 显示硬件短路情况发生的总次数。
- 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。供电设备需通过特征码来识别受电设备。特征码在受电设备的检测、分类或维护过程中生成。

步骤 **4** 单击 “应用”。修改端口的 PoE 设置，并更新交换机的运行时配置。

11

设置 VLAN

本章介绍如何设置 VLAN 功能，包含以下内容：

- VLAN
- 设置默认 VLAN
- 创建 VLAN
- 定义接口 VLAN 配置
- 设置端口到 VLAN
- 设置 VLAN 成员关系
- 设置 GVRP
- 设置语音 VLAN

VLAN

VLAN 是一个逻辑端口组。连接到 VLAN 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

每个 VLAN 会都分配一个唯一的范围在 1 到 4094 之间的 VLAN ID （VID）。如果桥接网络中某一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 标签，则该端口为 VLAN 的未添加标签成员。如果进入 VLAN 的指定给某端口的所有数据包都包含 VLAN 标签，则该端口为 VLAN 的已添加标签成员。一个端口可以是一个或多个 VLAN 的成员。

处于 VLAN 接入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 可用于解决安全和稳定性问题。来自于 VLAN 的流量会始终停留在 VLAN 内，并最终发送到 VLAN 内的设备。通过逻辑地连接网络设备， VLAN 可以有效地简化网络配置，而不需要重新调整这些设备的位置。

如果一个帧添加了 VLAN 标签，那么一个 4 位字节的 VLAN 标签将被加入到每一个以太网帧。此标签包含 VLAN 标识符 （范围为 1 到 4094）和一个 VLAN 优先级标签（范围为 0 到 7）。

当一个帧进入到一个 VLAN 有意识的设备，根据帧中所包含的 4 位 VLAN 标签，它会被认定为属于某个 VLAN。

如果帧中不包含 VLAN 标签或者仅为帧添加了优先级标签，则会根据于接收帧的传入端口所设置的 PVID （端口 VLAN 标识符）将该帧分类为属于某个 VLAN。

如果启用了入口过滤功能，并且传入端口不是数据包所属 VLAN 的成员，则此帧将在传入端口处被丢弃。仅当帧的 VLAN 标签中的 VID 为 0 时，才会将该帧视为添加了优先级标签。

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标 VLAN 成员的输出端口发送或转发帧来实现。输出端口可以是 VLAN 的已添加标签成员或未添加标签成员。

输出端口的特性包括：

- 如果输出端口是目标 VLAN 的已添加标签成员，并且原始帧不包含 VLAN 标签，则会为此帧添加 VLAN 标签。
- 如果输出端口是目标 VLAN 的未添加标签成员，并且原始帧包含 VLAN 标签，则会删除此帧的 VLAN 标签。

VLAN 角色

所有 VLAN 流量 （单播 / 广播 / 组播）将始终处于该 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。

毗邻的可识别 VLAN 的设备使用通用 VLAN 注册协议 （Generic VLAN Registration Protocol，GVRP）相互交换 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，静态或动态地创建设备上的 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 的详细信息，详见 “设置 GVRP”。

某些 VLAN 可能具有其他角色，如语音 VLAN、访客 VLAN、默认 VLAN 和管理 VLAN。

设置 VLAN 工作流程

设置 VLAN 的步骤：

- 如有必要，修改默认 VLAN 设置。详见 “设置默认 VLAN”。
- 根据需要创建 VLAN。详见 “创建 VLAN”。
- 根据需要定义每个端口的 VLAN 设置。详见 “定义接口 VLAN 配置”。
- 将端口分配给 VLAN。详见 “设置端口到 VLAN”。
- 查看所有端口当前的 VLAN 成员关系。详见 “设置 VLAN 成员关系”。
- 全局和在每个端口上分别启用 GVRP。详见 “设置 GVRP”。
- 设置语音 VLAN 及其相关参数。详见 “设置语音 VLAN”。

设置默认 VLAN

当交换机使用出厂默认配置时，交换机自动创建 VLAN 1 作为默认 VLAN，所有端口的端口状态默认为中继，并且所有端口被设定为默认 VLAN 的未添加标签成员。

默认 VLAN 具有以下特性：

- 该 VLAN 是独特的、非静态或非动态 VLAN。并且所有端口都是它的未添加标签成员。
- 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，如未认证的 VLAN 或语音 VLAN （仅限于启用了 OUI 的语音 VLAN）。
- 如果某端口不再是任何 VLAN 的成员，则交换机会自动将该端口设为默认 VLAN 的未添加标签成员。如果 VLAN 被删除或者此端口从 VLAN 中移除，那么此端口将不再是 VLAN 的成员。

如果默认 VLAN 发生更改，交换机会在此 VLAN 中的所有端口上将执行以下操作：

- 从初始默认 VLAN 中删除端口的 VLAN 成员关系
- 将端口的 PVID 更改为新的默认 VLAN 的 VID
- 将端口添加为新默认 VLAN 的未添加标签成员

更改默认 VLAN 设置的步骤：

步骤 1 单击 “**VLAN** 管理” > “默认 **VLAN** 设置”。

步骤 2 设定以下参数：

- 当前默认 **VLAN ID** — 显示当前默认 VLAN 的 VLAN ID。
- 默认 **VLAN ID** — 输入新的默认 VLAN 的 VLAN ID。

步骤 3 单击 “应用”。更改默认 VLAN 配置，并更新交换的当前配置。

创建 VLAN

您可以创建新 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，新 VLAN 才会生效。端口必须始终属于一个或多个 VLAN。交换机支持 4094 个 VLAN （包括默认 VLAN 在内）。

必须使用 1 到 4094 之间的值为每个 VLAN 配置一个唯一的 VLAN ID。交换机始终将 VLAN ID 4095 保留给丢弃 VLAN。所有分类为属于丢弃 VLAN 的数据包都会在传入端口处被丢弃，而永远不会被转发到端口。

创建 VLAN 的步骤：

步骤 1 单击 “**VLAN** 管理” > “创建 **VLAN** ”。

此页面显示以下字段：

- **VLAN ID** — VLAN 标识符。
- **VLAN** 名称 — VLAN 的名称。
- 类型 — VLAN 的类型。可选项如下：
  - *GVRP* — 表示此 VLAN 通过 GVRP 自动创建。
  - *静态* — 表示此 VLAN 由用户手动创建。
  - *默认* — 表示此 VLAN 为默认 VLAN。

步骤 2 单击 “添加”，添加一个新 VLAN ；或选择一个 VLAN 然后单击 “编辑”，修改 VLAN 的参数。

步骤 3 要创建单个 VLAN，选择 “**VLAN**”选项并在 “**VLAN ID**”和 “**VLAN** 名称”字段分别输入相应的 VLAN ID 和 VLAN 名称。

步骤 4 要创建一个 VLAN 范围，选择 “范围”选项并在 “**VLAN** 范围”字段输入起始 VLAN ID 和结束 VLAN ID。

步骤 5 单击 “应用”。保存 VLAN 设置，并更新交换机的当前配置。

定义接口 VLAN 配置

使用 “接口设置”页面可设置所有接口的 VLAN 相关参数。交换机支持 4094 个 VLAN （包括默认 VLAN 在内）。

定义接口的 VLAN 配置的步骤：

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 “确定”。

步骤 3 选择一个端口或 LAG，然后单击 “编辑”。

步骤 4 设定以下参数：

- 接口 — 选择要设定的端口或 LAG。
- 接口 **VLAN** 模式 — 选择 VLAN 模式。可选项如下：
  - *一般* — 接口可以支持 IEEE 802.1q 规格中定义的所有功能。接口可以是一个或多个 VLAN 的已添加标签成员或未添加标签成员。
  - *接入* — 接口必须是单个 VLAN 的未添加标签成员。在此模式下配置的端口称为接入端口。
  - *中继* — 接口最多可作为一个 VLAN 的未添加标签成员或者作为零个或更多 VLAN 的已添加标签成员。在此模式下配置的端口称为中继端口。
  - *Dot1q 隧道* — 选择此选项可使接口处于 QinQ 模式。这可让您在提供商网络间使用自有的 VLAN 部署 （PVID）。如果交换机拥有一个或多个 dot1 q 隧道端口，它将处于 QinQ 模式。
- 管理 **PVID** — （一般模式和中继模式下可用）输入传入的未添加标签和添加了优先级标签的帧的所属 VLAN 的 PVID。

- 帧类型 — （一般模式下可用）选择接口可以接收的帧类型。不属于所配置的帧类型的帧将在入站处被丢弃。可选项包括：
  - *全部接受* — 接受所有类型的帧：未添加标签的帧、已添加标签的帧和添加优先级标签的帧。
  - *只接受已标记* — 仅接受添加标签的帧。
  - *只接受未标记* — 仅接受未添加标签的帧和优先级帧。
- 入口过滤 — （一般模式下可用）选择启用或禁用入站过滤功能。如果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。入口过滤功能仅可以在一般端口上禁用或启用。此功能始终在接入端口和中继端口上启用。
- 上行链路 — （中继模式下可用）选择启用或禁用上行链路功能。
- **TPID** — （中继模式下可用）如启用了上行链路功能，为此接口选择一个 TPID。

步骤 5 单击 “应用”。定义接口的 VLAN 设置，并更新交换机的当前配置。

设置端口到 VLAN

使用 “端口到 VLAN”页面可查看和设定端口对 VLAN 的注册。

设定端口到 VLAN 的注册的步骤：

步骤 1 单击 “**VLAN** 管理” > “端口到 **VLAN**”。

步骤 2 选择一个 VLAN 和接口类型 （端口或 LAG），单击 “确定”。

每个端口或 LAG 的端口模式均显示为在 “接口设置”页面所设定的端口模式：一般、接入、中继或 Dot1p 隧道。

步骤 3 选择以下选项，可更改接口对此 VLAN 的注册：

- 已禁止 — 不允许接口加入此 VLAN（即使通过 GVRP 注册也不行）。如果接口不是任何其他 VLAN 的成员，启用此选项会使接口成为保留的丢弃 VLAN（VLAN ID 4095）的成员。
- 已排除 — 接口目前不是此 VLAN 的成员（默认选项）。接口可以通过 GVRP 注册加入此 VLAN。

- 已标记 — 接口是此 VLAN 的已添加标签成员。
- 未标记 — 接口是此 VLAN 的未添加标签成员。交换机会将未添加标签的此 VLAN 帧发送到接口 VLAN。
- **PVID** — 勾选此选项会将接口的 PVID 设置为此 VLAN 的 VID。

步骤 4 单击 “应用”。将接口分配给此 VLAN，并更新交换机的当前配置。

设置 VLAN 成员关系

“端口 VLAN 成员关系”页面显示每个端口是哪些 VLAN 的成员。

如果对端口禁止默认 VLAN 成员关系，那么此端口将不能成为任何其他 VLAN 的成员。此端口将被分配给保留的丢弃 VLAN （VLAN ID 4095）。

要正确转发数据包，必须手动设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 GVRP 动态获取 VLAN 及其端口成员关系。

在两台可识别 VLAN 的设备 （没有可识别 VLAN 的设备介于两者之间）之间的未添加标签的端口成员关系应该属于同一 VLAN。换言之，如果这两个设备之间的端口向 VLAN 发送未添加标签的数据包或从 VLAN 接收未添加标签的数据包，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。

添加了 VLAN 标签的帧可以通过可识别 VLAN 或无法识别 VLAN 的网络设备进行传输。如果目标终端节点可识别 VLAN，但将从 VLAN 接收流量，则上一个可识别 VLAN 的设备 （如果存在）必须将目标 VLAN 的帧发送到未添加标签的终端节点。即连接终端节点的出站端口必须为 VLAN 的未添加标签成员。

查看 VLAN 成员关系的步骤：

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 “确定”。

显示以下字段：

- 接口 — 显示端口号。
- 模式 — 显示端口模式。
- 管理 **VLANs** — 显示此端口可能为其成员的 VLAN 列表。

- 运行 **VLAN** — 显示此端口当前为其成员的 VLAN 列表。
- **LAG** — 如果接口类型为 “端口”，此字段显示此端口所属的 LAG。

步骤 **3** 如需将一个端口注册到 VLAN，选择一个端口然后单击 “加入 **VLAN**”。

步骤 **4** 设定以下参数：

- 接口 — 选择要设置的端口或 LAG。
- 模式 — 显示端口模式。
- 选择**VLAN** — 如需将端口关联到VLAN，将左侧列表中的VLAN添加到右侧的列表。如果此端口为已添加标签，那么默认 VLAN 有可能出现在其右侧列表，不过您无法选中它，表示您无法取消此端口关联到默认 VLAN。
- 标记 — 选择是否标记此端口或端口的 PVID。可选项如下：
  - *已禁止* — 表示此端口不能加入 VLAN，即便通过 GVRP 注册也不行。当一个端口不是其他 VLAN 的成员时，启用此选项可使端口成为保留的丢弃 VLAN（VLAN ID 为 4095）的成员。
  - *已排除* — 表示此端口当前不是 VLAN 的成员 （默认选项）。此端口可通过 GVRP 注册加入到 VLAN。
  - *已标记* — 表示此端口已添加标签。此选项不适用于接入端口 （端口模式为接入）。
  - *未标记* — 表示此端口未添加标签。此选项不适用于接入端口 （端口模式为接入）。
  - *PVID* — 此字段表示 VLAN 的 PVID。如果端口处于接入模式或者中继模式，交换机会自动将此端口设为 VLAN 的一个未添加标签的成员。如果端口处于一般模式，您必须手动将其设为 VLAN 的成员。

步骤 **5** 单击 “应用”。修改端口到 VLAN 的注册，并更新交换的当前配置。

步骤 **6** 如需查看端口的管理 VLAN 和运行 VLAN 的详细信息，选择一个端口然后单击 “详情”。

设置 GVRP

可识别 VLAN 的相邻设备可使用通用 VLAN 注册协议 （Generic VLAN Registration Protocol， GVRP）来互相交换 VLAN 信息。 GVRP 以通用属性注册协议 （Generic Attribute Registration Protocol，GARP）为基础，并通过桥接网络传递 VLAN 信息。

由于 GVRP 需要支持标记功能且必须中继允许的 VLAN，端口必须设为中继模式。

当端口使用 GVRP 加入 VLAN 时，会将该端口作为动态成员添加到 VLAN 中 （除非在 “端口 VLAN 成员关系”页面明确禁止其成为 VLAN 成员）。如果 VLAN 不存在，当在 “GVRP 设置”页面启用了端口的动态 VLAN 创建功能时，系统会自动为该端口创建一个 VLAN。

定义 GVRP 设置的步骤：

步骤 1 单击 “**VLAN** 管理” > “**GVRP** 设置”。

步骤 2 在 “**GVRP** 全局状态”字段，选择全局启用或禁用 GVRP 功能。

步骤 3 单击 “应用”。

步骤 4 选择接口类型 （端口或 LAG），然后单击 “确定”。

步骤 5 要编辑某一端口的 GVRP 设置，选择该端口然后单击 “编辑”。

步骤 6 设定以下参数：

- 接口 — 选择要设置的端口或 LAG。
- **GVRP** 状态 — 选择启用或禁用 GVRP 功能。
- 动态 **VLAN** 创建 — 选择启用或禁用动态 VLAN 创建功能。启用此功能可使得系统在 VLAN 不存在时自动为端口创建一个 VLAN。
- **GVRP** 注册 — 选择在该端口上使用 GVRP 注册到 VLAN 的模式。

步骤 7 单击 “应用”。修改端口的 GVRP 设置，并更新交换机的当前配置。

设置语音 VLAN

在局域网内，像 IP 电话、 VoIP 终端以及语音系统都放置在同一个 VLAN 内。此 VLAN 也就是我们常说的语音 VLAN。语音 VLAN 用于将来自 VoIP 设备或电话的流量分配给特定 VLAN。交换机可自动检测端口成员并将其添加到语音 VLAN，并将配置的 QoS 分配给来自语音 VLAN 的数据包。

动态语音 VLAN 模式

交换机支持两种动态语音模式，分别是电话 OUI （Organization Unique Identifier）模式和自动语音 VLAN 模式。这两种模式将影响如何设置语音 VLAN 以及语音 VLAN 的端口成员关系。这两种模式相互之间完全互斥。

- 电话 **OUI** — 电话 OUI 模式下，语音 VLAN 必须是手动创建的 VLAN，不能设为默认 VLAN。

  当交换机处于电话 OUI 模式下且一个端口被手动添加为语音 VLAN 的候选端口时，如果端口接收到源 MAC 地址与电话 OUI 设置的相匹配的数据包，那么交换机会动态地将此端口添加到语音 VLAN。一个 OUI 是一个以太网 MAC 地址的前三个字节。有关电话 OUI 的更多信息，详见 “设置电话 OUI”。

- 自动语音 **VLAN** — 自动语音 VLAN 模式下，语音 VLAN 可以是默认 VLAN 或手动创建的 VLAN。

  与电话 OUI 模式基于电话 OUI 检测语音设备不同的是，自动语音 VLAN 模式会根据 CDP 和 LLDP MED （如果启用）动态地将端口添加到语音 VLAN。如果交换机检测连接到端口的设备通过 CDP/LLDP MED 将其广播为一个电话或者媒体终端设备，那么此端口将被添加到语音 VLAN。

语音 VLAN 限制

语音 VLAN 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，电话 OUI 还存在以下限制：

- 语音 VLAN 不能是 VLAN1 （默认 VLAN）
- 只有在当前的语音 VLAN 没有候选端口时才能将一个新的 VLAN ID 指定为语音 VLAN

- 如果语音 VLAN 模式为电话 OUI，则语音 VLAN 不能为访客 VLAN。
- 作为语音 VLAN 候选端口的端口必须处于一般模式或中继模式
- 语音 VLAN QoS 决策的优先级高于任何其他 QoS 决策（QoS 策略和 ACL QoS 决策除外）
- 语音 VLAN QoS 属性将应用于作为语音 VLAN 候选端口而成为静态端口的传送的语音数据包

语音 VLAN 选项

使用语音 VLAN 功能，可执行以下配置操作：

- 全局设定语音 VLAN 配置以及动态语音 VLAN 的模式。详见 “设置语音 **VLAN** 属性”。
- 设置或者更新电话 OUI 表。最多支持 16 个 OUI 条目（每个条目是一个由三个八进制数组成的数字）。对于使用语音 VLAN 自动模式的端口，交换机将使用此电话 OUI 表确定是否将端口加入语音 VLAN 中。详见 “设置电话 **OUI**”。
- 根据电话 OUI 标识符将端口添加到语音 VLAN 并设定语音 VLAN 的 OUI QoS 模式。详见 “设置电话 **OUI** 接口”。

设置语音 VLAN 属性

使用 “属性”页面可全局配置语音 VLAN 相关参数。

设置语音 VLAN 参数的步骤：

步骤 1 单击 “**VLAN** 管理” > “语音 **VLAN**” > “属性”。

步骤 2 设定以下参数：

- 语音 **VLAN ID** — 输入要作为语音 VLAN 的 VLAN。
- **CoS/802.1p** — LLDP MED 将选择此设定值作为语音网络策略的值。可能的值为 0 到 7，其中 7 表示最高优先级。 0 被用作尽力服务。在未设置任何其他值（默认设置）的情况下，会自动调用该值。
- **DSCP** — 选择由 LLDP MED 使用的 DSCP 值，作为一个语音网络策略。默认为 46。
- 动态语音 **VLAN** — 选择动态语音 VLAN 的工作模式。可选项如下：
  - *启用自动语音 VLAN* — 选择此选项，启用自动语音 VLAN 功能。

- *启用电话 OUI* — 选择此选项，启用电话 OUI 功能。
- *禁用* — 选择此选项，禁用语音 VLAN 功能。

步骤 3 单击 “应用”。设置语音 VLAN 属性，并更新交换机的当前配置。

设置电话 OUI

组织唯一标识符 （Organizationally Unique Identifier，OUI）是由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。

电话 OUI 表最多可包含 16 个 OUI 条目。

使用 “电话 OUI”页面可查看和设置 OUI。如果没有电话活动的时间超过了指定的自动成员关系过期时间，那么端口将会从语音 VLAN 中移除。

设置电话 OUI 的步骤：

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

步骤 2 设定电话 OUI 的全局参数：

- 电话 **OUI** 运行状态 — 显示电话 OUI 功能是否启用，以识别语音流量。
- **CoS/802.1p** — 选择分配给语音流量的 CoS 优先级。
- 重新标记 **CoS/802.1p** — 勾选此选项可将分配给语音流量的 CoS 值在发送出去时加入标记。
- 自动成员关系过期时间 — 当所有端口检测到的所有电话的MAC地址都过期时，输入将端口从语音 VLAN 上移除的延迟时间。

步骤 3 单击 “应用”。

步骤 4 “电话 OUI 表”最多可包含 16 个 OUI。单击 “添加”，添加电话 OUI。

步骤 5 设定以下参数：

- 电话 **OUI** — 输入新的 OUI。通常为 OUI 保留的 MAC 地址的前六位。
- 说明 — 输入 OUI 名称。

步骤 6 单击 “应用”。添加电话 OUI，并更新交换机的当前配置。

步骤 7 单击 “恢复默认 **OUI**”可删除所有用户创建的 OUI，而仅保留默认的 OUI。

设置电话 OUI 接口

根据以下任一模式， QoS 属性可根据端口分配给语音数据包：

- 全部 — 设置给语音 VLAN 的 QoS 值可应用到端口接收到以及分类给此语音 VLAN 的所有传入帧。
- 电话源 **MAC** 地址（**SRC**）— 设置给语音 VLAN 的 QoS 值仅可应用到任意分类给此语音 VLAN 且其源 MAC 地址中包含的 OUI 与设定的电话 OUI 条目匹配的传入帧。

使用 “电话 OUI 接口”页面可根据 OUI ID 将一个接口分配给语音 VLAN，并设置语音 VLAN 的 QoS 模式。

设置电话 OUI 接口的步骤：

步骤 1 单击 “**VLAN** 管理” > “语音 **VLAN**” > “电话 **OUI** 接口”。

步骤 2 选择接口类型 （端口或 LAG），单击 “确定”。

步骤 3 如需将一个端口设置为基于电话 OUI 的语音 VLAN 的候选端口，选择此端口，然后单击 “编辑”。

步骤 4 设定以下参数：

- 接口 — 选择要设置的端口或 LAG。
- 电话 **OUI VLAN** 成员关系 — 勾选 “启用”，此端口将作为电话 OUI 语音 VLAN 的一个候选端口。当数据包匹配设定的电话 OUI 接收的一个数据包时，此端口被添加到语音 VLAN。
- 电话 **OUI** 模式 — 选择电话 OUI 模式。可选项如下：
  - *自动* — 端口被定义为语音 VLAN 的候选端口。当端口发现数据包带有用来识别远程设备为语音设备的一个源 OUI MAC 地址时，端口将加入语音 VLAN 并且成为一个已标记的成员端口。如果最后一个电话的 MAC 地址过期的时间超出自动成员关系过期时间，此端口将从语音 VLAN 移除。
  - *手动* — 手动将端口分配给语音 VLAN。
- 电话 **OUI QoS** 模式 — QoS 属性可按照以下方法分配给语音数据包：
  - *电话源 MAC 地址* — QoS 属性仅应用到来自 IP 电话的数据包。

- *全部* — QoS 属性可应用到归类为语音 VLAN 的所有数据包。

步骤 5 单击 “应用”。设置电话 OUI 接口，并更新交换机的当前配置。

12

设置生成树协议

默认情况下，系统会启用生成树协议 （Spanning Tree Protocol, STP）（IEEE802.1D 和 IEEE802.1Q），并将其设置为传统 STP 模式。

本章介绍如何设置生成树协议功能，包含以下内容：

- **STP** 模式
- 定义 **STP** 状态和全局设置
- 定义 **STP** 接口设置
- 定义 **RSTP** 接口设置
- 设置 **MSTP**

STP 模式

STP 通过选择性地将链路设置为待机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。在待机模式下，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，从而造成流量增加和网络效率降低。

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

交换机支持以下 STP 模式：

- 传统 **STP**（**Classic STP**） — 可在任意两个终端工作站之间提供单一路径，从而避免和消除环路。
- 快速 **STP**（**Rapid STP**， **RSTP**）— RSTP 会检测网络拓扑，以提供更快的生成树聚合。 RSTP 在网络拓扑本身为树状结构且可以实现快速聚合的情况下最有效。

- 多 **STP**（**Multiple STP**，**MSTP**）— MSTP 以 RSTP 为基础。它会检测二层网络环路，并且试图通过阻止所涉及的端口传输流量来缓解环路造成的影响。由于环路可能会存在于以 VLAN 为基础的二层域内，会出现 VLAN A 中存在环路，而 VLAN B 中没有环路的情况。如果两个 VLAN 的流量都会通过某个指定的造成环路的端口且 STP 希望缓解环路造成的影响，系统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，以便可以在每个实例中分别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。

定义 STP 状态和全局设置

使用 “STP 状态和全局设置”页面可启用或禁用 STP 功能并设定 STP 模式。您可以使用 “STP 接口设置”页面、“RSTP 接口设置”页面和 “MSTP 属性”页面分别设置各个 STP 模式的参数。

查看 STP 状态和定义全局设置的步骤：

步骤 1 单击 “生成树” > “**STP** 状态和全局设置”。

“指定根”区域显示以下信息：

- 网桥 **ID** — 网桥优先级与交换机的 MAC 地址串联在一起。
- 根网桥 **ID** — 根网桥优先级与根网桥的 MAC 地址串联在一起。
- 根端口 — 可提供从该网桥到根网桥的最低成本路径的端口。这在网桥不为根网桥的情况下很有意义。
- 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经过的时间间隔。显示格式为日 / 小时 / 分钟 / 秒。

步骤 2 在 “全局设置”区域，设定以下参数：

- 生成树状态 — 在交换机上启用或禁用 STP。
- **STP** 运行模式 — 选择 STP 模式，如 Classic STP、 RSTP 或 MSTP 。

- **BPDU** 处理 — 选择在交换机上禁用 STP 时如何管理 BPDU 数据包。BPDU 用于传输生成树信息。可选项如下：
  - *过滤* — 禁用生成树时，过滤 BPDU 数据包。
  - *泛洪* — 禁用生成树时，转发 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。分配给端口的默认路径成本根据所选择的方式而变化。可选项如下：
  - *短* — 端口路径成本为 1 到 65535 范围。
  - *长* — 端口路径成本为 1 到 200000000 范围。

步骤 **3** 在 “网桥设置” 区域，设定以下参数：

- 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。范围为 1 到 10 秒，默认为 2 秒。
- 最大老化时间 — 设置交换机在尝试重新定义其自身配置之前，可用来等待接收配置消息的时间间隔，以秒为单位。范围为 6 到 40 秒，默认为 20 秒。
- 转发时间 — 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。范围为 4 到 30 秒，默认为 15 秒。

步骤 **4** 单击 “应用”。设定 STP 全局设置，并更新交换机的当前配置。

定义 **STP** 接口设置

使用 “STP 接口设置” 页面可针对每个接口配置 STP 以及查看该协议获取的信息，例如指定的网桥。在本页面上输入的配置对于任何 STP 模式均有效。

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** 选择接口类型 （端口或 LAG），单击 “确定”。

步骤 **3** 选择一个接口并单击 “编辑”。

步骤 **4** 设定以下参数：

- 接口 — 选择要设置的端口或 LAG。
- 边缘端口 — 在端口上启用或禁用快速链路。如果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置于转发状态。快速链路属性会优化 STP 协议收敛时间。
- **BPDU** 防护 — 在端口上启用或禁用 BPDU 防护功能。当端口接收到一个 BPDU 消息时，启用此功能，端口会被关闭。
- **BPDU** 过滤 — 在端口上启用或禁用 BPDU 过滤功能。启用此选项，端口将不会发送和接收 BPDU 数据包。
- 路径成本 — 选择 “用户定义”手动设置端口产生的根路径成本，或选择 “使用默认设置”使用系统生成的默认路径成本。
- 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。优先级范围为 0 到 240，设置增量为 16。
- 端口状态 — 显示端口当前是否启用或禁用 STP 及其工作模式。
  - *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，无法转发除 BPDU 数据除外的流量或学习 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。端口可以转发流量及学习新的 MAC 地址。
- 指定网桥 **ID** — 显示指定网桥的网桥优先级和 MAC 地址。
- 指定端口 **ID** — 显示所选端口的优先级值和端口号。
- 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。

步骤 **5** 单击 “应用”。定义 STP 接口设置，并更新交换机的当前配置。

定义 **RSTP** 接口设置

RSTP 可实现链路快速收敛而不会形成转发环路。

使用 “RSTP 接口设置”页面可针对每个接口设置 RSTP。当全局 STP 模式设置为 RSTP 或 MSTP 时，在此页面上完成的任何配置均有效。

定义接口的 RSTP 设置的步骤：

步骤 **1** 单击 “生成树” > “**STP** 状态和全局设置”。

步骤 **2** 将 STP 运行模式设为 RSTP。

步骤 **3** 单击 “生成树” > “**RSTP** 接口设置”。

步骤 **4** 选择接口类型 （端口或 LAG），单击 “确定”。

步骤 **5** 选择一个接口，并单击 “编辑”。

步骤 **6** 设定以下参数：

- 接口 — 选择要设置的端口或 LAG。
- 点到点管理状态 — 定义点到点链路状态。可选项如下：
  - *启用* — 选择此选项，该端口对应的链路为点对点。
  - *禁用* — 选择此选项，该端口对应的链路为共享链路。
  - *自动* — 选择此选项，将根据实际连接的单双工模式决定链路类型。全双工时为点对点链路，半双工时为共享链路。
- 点到点运行状态 — 显示点到点链路的当前运行状态。
- 角色 — 显示由 STP 指定的端口角色，以提供 STP 路径。可选项如下：
  - *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。
  - *替换* — 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。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，则会出现备份端口。如果 LAN 具有两条或更多条至一个共享网段的连接，也会出现备份端口。
  - *已禁用* — 端口不会加入生成树。
- 快速链路运行状态 — 显示端口是否启用或禁用快速链路 （边缘端口）功能。
- 端口状态 — 显示端口的 RSTP 状态。可选项为：
  - *已禁用* — 目前在端口上禁用 RSTP。
  - *阻塞* — 端口目前被阻塞，其无法转发流量或学习 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。端口可以转发流量及学习新的 MAC 地址。

步骤 7 单击 “应用”。定义接口的 RSTP 设置，并更新交换机的当前配置。

步骤 8 如果所选接口连接到一个被测试的网桥伙伴，“激活协议迁移”按钮将被激活。当使用 STP 协议发现了一个链路伙伴，单击 “激活协议迁移”可执行协议迁移测试。此测试可以确定使用 STP 的链路伙伴是否仍然存在，并且如果存在，可确定该链路伙伴是否已迁移到 RSTP 或 MSTP。如果其仍作为 STP 链路存在，则设备将继续使用 STP 与其进行通信。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。

设置 MSTP

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 实例中将此端口置于转发状态。

设置 MSTP 的步骤：

步骤 1 将 STP 运行模式设为 MSTP。详见 “定义 **STP** 状态和全局设置”。

步骤 2 全局设置 MSTP 参数。详见 “设置 **MSTP** 属性”。

步骤 3 设置 MSTP 实例。每个 MSTP 实例会计算和构建一个无环路拓扑，从而映射到此实例的 VLAN 桥接数据包。详见 “设置 **MSTP** 实例”。

步骤 4 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 相关连。详见 “映射 **VLAN** 到 **MSTP** 实例”。

设置 MSTP 属性

使用 “MSTP 属性”页面设置全局 MSTP 参数。 MSTP 为每一个 VLAN 设置一个单独的生成树，并且在每一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 （Multiple Spanning Tree Instance）的 MSTP 区域。多个 MSTP 区域和其他 STP 网桥可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 网桥可以将一个 MSTP BPDU 解析为一个 RSTP BPDU。这不仅可实现在不更改配置的情况下与 RSTP 网桥兼容，还会导致 MSTP 区域之外的所有 RSTP 网桥将该区域视为一个 RSTP 网桥，而不管在该区域内存在多少个 MSTP 网桥。

对于将在同一个 MSTP 区域内的两台或更多台交换机，它们必须具有相同的 VLAN 到 MSTP 实例映射、相同的配置修订编号以及相同的区域名称。此映射可以在 “VLAN 到 MSTP 实例”页面中完成。

将在同一个 MSTP 区域内的交换机永远不会被另一个 MSTP 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。

设置全局 MSTP 属性的步骤：

步骤 1 单击 “生成树” > “**MSTP** 属性”页面。

步骤 2 设定以下参数：

- 区域名称 — 输入 MSTP 区域名称。
- 版本 — 输入一个无符号的 16 位数字，用来标识目前 MSTP 配置的修订版本。设置范围为 0 到 65535。
- 最大步跳数 — 设置丢弃 BPDU 之前特定区域内可发生的跃点总数。一旦丢弃 BPDU 后，端口信息即过期。设置范围为 1 到 40，默认为 20。

步骤 3 单击 “应用”。设置 MSTP 属性，并更新交换机的当前配置。

映射 VLAN 到 MSTP 实例

使用 “VLAN 到 MSTP 实例”页面可将 VLAN 映射到 MSTP 实例。对于要在同一区域中的设备，它们必须具有相同的 VLAN 到 MSTP 实例映射。

注释 同一个 MSTP 实例可以与多个 VLAN 进行映射，但每个 VLAN 只能与一个 MSTP 实例关联。

交换机最多可定义 16 个 MSTP 实例。对于那些未明确映射到某个 MSTP 实例的 VLAN，交换机会自动将其映射到 CIST （Core and Internal Spanning Tree）实例。CIST 实例为 MSTP 实例 0。

将 VLAN 映射到 MSTP 实例的步骤：

步骤 1 单击 “生成树” > “**VLAN** 到 **MSTP** 实例”。

步骤 2 选择一个 MSTP 实例并单击 “编辑”。

步骤 3 设定以下参数：

- **MSTP** 实例 **ID** — 选择一个 MSTP 实例。
- **VLAN** — 选择要映射到该 MSTP 实例的 VLAN。
- 操作 — 选择 “添加” 将指定的 VLAN 映射到该 MSTP 实例，或选择 “移除” 取消指定的 VLAN 与此 MSTP 实例的映射。

步骤 4 单击 “应用”。设置 VLAN 到 MSTP 实例映射，并更新交换机的当前配置。

设置 MSTP 实例

使用 “MSTP 实例设置” 页面可设定和查看每个 MSTP 实例配置。

设置 MSTP 实例的步骤：

步骤 1 单击 “生成树” > “**MSTP** 实例设置”。

步骤 2 设定以下参数：

- 实例 **ID** — 选择要查看或设定的 MSTP 实例。
- 包含的 **VLAN** — 显示映射到此 MSTP 实例的 VLAN。默认为将所有 VLAN 映射到 CIST 实例 （MSTP 实例 0）。
- 优先级 — 为所选 MSTP 实例设置网桥优先级。
- 指定根网桥 **ID** — 显示 MSTP 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** — 显示所选实例的此交换机的网桥优先级和 MAC 地址。
- 剩余的步跳数 — 显示保留到下个目标的跃点数。

步骤 3 单击 “应用”。设置 MSTP 实例，并更新交换机的当前配置。

设置 MSTP 接口配置

使用 “MSTP 接口设置”页面可定义每个端口的 MSTP 实例设置，以及查看协议目前已学习到的信息，例如每个 MSTP 实例的指定网桥。

定义接口的 MSTP 实例配置的步骤：

步骤 1 单击 “生成树” > “**MSTP** 接口设置”。

步骤 2 选择要设置的 MSTP 实例和接口类型 （端口和 LAG），单击 “确定”。

步骤 3 选择一个接口，单击 “编辑”。

步骤 4 设定以下参数：

- 实例 **ID** — 选择要配置的 MSTP 实例。
- 接口 — 选择要为其定义 MSTP 实例的端口或 LAG。
- 路径成本 — 设置端口产生的根路径成本。选择 “使用默认设置”使用默认值或选择 “用户定义”手动输入根路径成本。根路径成本是交换机至指定 MSTP 实例的根网桥的成本。
- 优先级 — 设置指定接口和 MSTP 实例的优先级。
- 端口状态 — 显示端口的 MSTP 状态，如：
  - *禁用* — 端口当前禁用 MSTP。
  - *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。
  - *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。端口可以转发流量及学习新的 MAC 地址。
- 端口角色 — 显示每个实例的端口角色 （由 MSTP 算法指定以提供 STP 路径），如：
  - *Master* — Master 端口提供一个 MSTP 域到总根的连接。
  - *根* — 通过此端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 MSTP 实例的根网桥的最低根路径成本。
- *替换* — 该端口提供从根接口到根设备的备用路径。
- *备份* — 该端口提供指向生成树叶节点的指定端口路径的备份路径。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，则会出现备份端口。如果 LAN 具有两条或更多条至一个共享网段的连接，也会出现备份端口。
- *已禁用* — 端口不会加入生成树。

▪ 模式 — 显示端口目前的 STP 模式。

- *STP* — 在端口上启用传统 STP。
- *RSTP* — 在端口上启用 RSTP。
- *MSTP* — 在端口上启用 MSTP。

▪ 类型 — 显示端口的 MSTP 类型。

- *边界* — 边界端口可将MSTP网桥连接至边缘区域中的LAN。如果端口为边界端口，它还会指出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。

▪ 指定网桥 **ID** — 显示将链路或共享 LAN 连接到根的网桥 ID 号。

▪ 指定端口 **ID** — 显示指定网桥上将链路或共享 LAN 连接到根的端口 ID 号。

▪ 剩余的步跳数 — 显示保留到下个目标的跃点。

步骤 **5** 单击 “应用”。定义端口的 MSTP 实例配置，并更新交换机的当前配置。

13

管理 MAC 地址表

本章介绍如何添加 MAC 地址到交换机，包括以下内容：

- MAC 地址类型
- 设置静态 MAC 地址
- 设置静态 MAC 地址过滤
- 设置动态 MAC 地址过期时间
- 查询动态 MAC 地址
- 设置保留的 MAC 地址

MAC 地址类型

MAC 地址有两种类型，分别为静态 MAC 地址和动态 MAC 地址。根据其类型，MAC 地址与 VLAN 和端口信息一起保存在静态地址表或动态地址表中。

静态地址由用户配置，因此不会过期。在到达交换机的帧中出现的新的源 MAC 地址会被添加到动态地址表中并被保留一段时间。如果这段时间过去之后没有具有相同源 MAC 地址的其他帧到达交换机，则会从动态地址表中删除该条目。

当帧到达交换机时，交换机会搜索与静态或动态地址表条目相匹配的 MAC 地址。如果找到匹配项，则会根据对地址表的搜索结果将此帧标记为通过特定端口输出。如果帧的目标 MAC 地址不在这两个地址表中，则会将这些帧转发到相应 VLAN 上的所有端口。这些帧叫做未知单播帧。

设置静态 MAC 地址

静态地址可以分配给交换机上的特定接口和 VLAN。这些地址与所分配的接口绑定在一起。如果在其他接口看到静态地址，会将其忽略而不会写入地址表。交换机最多可设置 256 个静态 MAC 地址。

设置静态 MAC 地址的步骤：

步骤 1 单击 “**MAC** 地址表” > “静态地址”。

步骤 2 单击 “添加”，添加静态 MAC 地址。

步骤 3 设定以下参数：

- **VLAN ID** — 选择一个 VLAN。
- **MAC** 地址 — 输入 MAC 地址。此 MAC 地址被视为一个静态 MAC 地址，并分配给指定的 VLAN 和接口。
- 接口 — 选择 MAC 地址要绑定到哪个端口或 LAG。
- 状态 — 选择静态 MAC 地址的处理方式。可选项如下：
  - *永久* — 该静态 MAC 地址在地址表中永不过期，如果将其保存在启动配置中，交换机重新启动后，该地址仍然存在。
  - *重置即删除* — 交换机重置后该地址将被删除。
  - *超时即删除* — 当该 MAC 地址过期时将其删除。
  - *安全* — 当接口处于传统锁定模式时，该 MAC 地址是安全的。

步骤 4 单击 “应用”。设置静态 MAC 地址，并更新交换机的当前配置。

设置静态 MAC 地址过滤

使用 “静态地址过滤”页面可设置静态 MAC 过滤规则，使特定的静态 MAC 地址不会被分配给交换机的特定 VLAN。

设置静态 MAC 地址过滤规则的步骤：

步骤 1 单击 “**MAC** 地址表” > “静态地址过滤”。

步骤 2 单击 “添加”，添加静态 MAC 地址过滤规则。

步骤 3 设定以下参数：

- **MAC** 地址 — 输入一个 MAC 地址。
- **VLAN ID** — 选择一个 VLAN。设定的静态 MAC 地址将不会分配给此 VLAN。

步骤 4 单击 “应用”。设置静态 MAC 地址过滤规则，并更新交换机的当前配置。

设置动态 MAC 地址过期时间

动态地址表包含通过监控进入交换机的流量的源地址而获得的 MAC 地址。为了防止动态地址表溢出并为新地址腾出空间，如果在特定的时间段内没有从动态 MAC 地址接收到任何流量，系统会将该地址从动态地址表中删除。该时间段为过期时间。

设置动态 MAC 地址的过期时间的步骤：

步骤 1 单击 “**MAC** 地址表” > “动态地址设置”。

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

步骤 3 单击 “应用”。设置动态 MAC 地址过期时间，并更新交换机的当前配置。

查询动态 MAC 地址

使用 “动态地址”页面可根据接口类型、 MAC 地址和 VLAN ID 来查询动态 MAC 地址表中的条目。此页面显示系统动态获取的 MAC 地址。您可以清除动态地址表中的动态 MAC 地址，也可以根据指定的查询标准显示该表的子集。例如，只显示在特定接口上获取的 MAC 地址。如果没有设定查询条件，将显示全部动态 MAC 地址条目。

查询动态 MAC 地址的步骤：

步骤 1 单击 “**MAC** 地址表” > “动态地址”。

步骤 2 设定以下查询标准：

- **VLAN ID** — 勾选此选项并输入要查询的 VLAN ID。
- **MAC** 地址 — 勾选此选项并输入要查询的 MAC 地址。

- 接口 — 勾选此选项并选择要查询的端口或 LAG。

步骤 3 单击 “确定”。将对动态 MAC 地址表进行查询并显示查询结果。

步骤 4 如有必要，从 “动态地址表排序关键字”下拉框中选择一个关键字，所有查询结果将按照接口、 VLAN 或 MAC 地址的先后顺序进行排列。

步骤 5 单击 “清除表”，清除动态 MAC 地址表中的数据。

设置保留的 MAC 地址

如果交换机收到目标 MAC 地址在保留地址范围 （根据 IEEE 标准的规定）内的帧，可以选择丢弃或桥接此帧。

使用 “保留的 MAC 地址”页面可定义保留哪些 MAC 地址已经处理帧的方法。

保留一个 MAC 地址的步骤：

步骤 1 单击 “**MAC** 地址表” > “保留的 **MAC** 地址”。

步骤 2 单击 “添加”。

步骤 3 设定以下参数：

- **MAC** 地址 — 选择要保留的 MAC 地址（MAC 地址为用户手动添加的静态 MAC 地址或者系统获取的动态 MAC 地址）。
- 操作 — 选择如何处理符合所选标准的到达数据包。可选项如下：
  - *网桥* — 将数据包转发给所有 VLAN 成员。
  - *丢弃* — 删除数据包。
  - *对等* — 根据协议丢弃或继续处理数据包。

步骤 4 单击 “应用”。保留设定的 MAC 地址，并更新交换机的当前配置。

14

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。

本章介绍如何设置组播转发功能，包括以下内容：

- 组播转发
- 设置组播属性
- 设置 **IP** 组播组地址
- 设置 **IGMP** 侦听
- 设置 **MLD** 侦听
- 查询 **IGMP/MLD IP** 组播组
- 设置组播路由器端口
- 设置全部转发端口
- 设置最大 **IGMP/MLD** 组播组
- 设置组播过滤

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，节点和路由器必须都能进行组播。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 IGMP 监听功能或 MLD 监听的交换机以及要接收组播流的组播客户端。在此设置中，路由器会定期发送 IGMP 查询。

注释 针对 IPv6 的 MLD 衍生自针对 IPv4 的 IGMPv2。虽然本节中主要介绍的是 IGMP，但也涵盖了对 MLD 的隐含介绍。

这些查询会访问交换机，交换机转而会将查询泛洪到 VLAN，并且也会学习其中包含的组播路由器端口。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 侦听的交换机会分析加入消息，并了解到必须将主机所请求的组播流转发到此特定端口。然后，交换机会只将 IGMP 加入转发到组播路由器。同样地，当组播路由器接收到 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。组播路由器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。

当交换机启用 IGMP 和 MLD 侦听并接收组播流的帧时，它会将组播帧转发到经过注册可使用 IGMP 加入消息接收组播流的所有端口。

交换机仅可以根据组播 MAC 组地址转发组播数据流。可以为每个 VLAN 设置组播转发。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 MLD 协议侦听可以静态地配置或动态地学习组播组及其进行接收的端口。

组播注册

组播注册是监听组播注册协议并对其作出响应的程序。提供的协议有针对 IPv4 的 IGMP 和针对 IPv6 的 MLD 协议。当在 VLAN 上启用交换机中的 IGMP/MLD 侦听时，交换机会分析其接收的所有 IGMP/MLD 数据包 （来自连接到交换机的 VLAN 和网络中的组播路由器）。

当交换机了解到主机正在使用 IGMP/MLD 消息进行注册以接收组播流时 （或者从特定源进行接收），交换机会在其组播转发数据库中添加注册。

IGMP/MLD 侦听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 侦听的交换机只会将组播流量转发给对需要该流量的主机。这种组播流程的减少还会减少交换机上处理的数据包，也会减少终端主机上的工作负荷，这是因为它们不必接收和过滤网络中生成的所有组播流量。

交换机可支持以下版本：

- IGMP v1/v2/v3
- MLD v1/v2
- 简单的 IGMP 侦听查询器

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。

交换机可被配置为一个 IGMP 查询器，用作备份查询器或者在不存在常规 IGMP 查询器时使用。此交换机不是全功能 IGMP 查询器。

如果交换机作为 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）的 1/4 查询间隔时间后启动。如果存在其他 IGMP 查询器，则交换机可能会 （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

将一个 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。在标准情况下，前 9 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。它会将最多 32 个 IP 组播组地址映射至同一第 2 层地址。
- 通过取得 IPv6 组播地址中的低 32 位并添加前缀 33:33 来组成 2 层组播地址。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。

设置组播属性

使用 “属性”页面可全局启用或禁用 IGMP 侦听和 MLD 侦听功能，并设置组播转发方法。

设置组播属性的步骤：

步骤 1 单击 “组播” > “属性”。

步骤 2 设定以下参数：

- **IGMP Snooping** — 全局启用或禁用 IGMP 侦听功能（默认为启用）。全局启用 IGMP 侦听时，监控网络流量的设备将决定哪些主机已请求接收组播流量，而交换机仅执行 IGMP 侦听。
- **MLD Snooping**— 全局启用或禁用 MLD 侦听 （默认为禁用）。
- 未知组播操作 — 选择如何处理未知组播数据包。可选项如下：
  - *丢弃* — 丢弃未知组播数据包。
  - *泛洪* — 将未知组播数据包泛洪出去。
  - *转发到路由器端口* — 将未知组播数据包转发到路由器端口。

步骤 3 单击 “应用”。设置组播属性，并更新交换机的当前配置。

设置 IP 组播组地址

使用 “IP 组播组地址”页面可查询和添加 IP 组播组地址。

设置 IP 组播组的步骤：

步骤 1 单击 “组播” > “**IP** 组播组地址”。

步骤 2 设定以下查询条件：

- **VLAN ID** — 输入 IP 组播组所属的 VLAN ID。
- **IP** 版本 — 选择 IP 版本 （IPv6 或 IPv4）。
- **IP** 组播组地址 — 输入要查询的 IP 组播组的 IP 地址。

步骤 3 单击 “确定”。

“IP 组播组地址表”中将列出符合条件的 IP 组播组地址及其详细信息，包括 VLAN ID、 IP 组播组地址和成员端口。

步骤 4 单击 “添加”，添加 IP 组播组地址。

步骤 5 设定以下参数：

- **VLAN ID** — 选择一个 VLAN，将此 IP 组播组添加到此 VLAN。
- **IP** 版本 — 选择 IP 地址类型：IPv4 或 IPv6。
- **IP** 组播组地址 — 输入 IP 组播组的 IP 地址。

步骤 6 选择接口类型 （端口或 LAG），然后单击 “确定”。

步骤 7 设置端口或 LAG 与 IP 组播组的成员关系，包括：

- 静态 — 选择此按钮将此端口或 LAG 添加到 IP 组播组，作为一个静态成员端口。
- 无 — 选择此按钮表示此端口或 LAG 当前不是 IP 组播组的一个成员。

步骤 8 单击 “应用”。添加 IP 组播组，并更新交换机的当前配置。

设置 IGMP 侦听

要支持 IPv4 组播转发，必须全局和在每个相关 VLAN 上都启用 IGMP 侦听功能。

默认情况下，交换机会将组播帧转发到相关 VLAN 的所有端口，实质上似乎是将帧作为广播进行处理。而使用 IGMP 侦听功能，交换机会将组播帧转发到已注册组播客户端的端口。

注释 交换机在静态和动态 VLAN 上均支持 IGMP 侦听。

当全局和在相应 VLAN 上都启用 IGMP 侦听后，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
- 哪些端口连接到了生成 IGMP 查询的组播路由器
- 哪些端口正在接收 PIM、 DVMRP 或 IGMP 查询协议

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

则第 2 层组播域中应仅存在一个 IGMP 查询器。当域中存在多个 IGMP 查询器时，交换机将支持基于标准的 IGMP 查询器选择。

设置 IGMP 侦听的步骤：

步骤 1 单击 “组播” > “**IGMP Snooping**”。

步骤 2 设定以下全局参数：

- **IGMP Snooping** 版本 — 选择交换机使用的 IGMP 侦听版本 （IGMPv2 或 IGMPv3）。
- 报告抑制 — 选择启用或禁用报告抑制功能。禁用此功能，会将所有 IGMP 报告转发给组播路由器。

  注　只有当组播查询有 IGMPv1 和 IGMPv2 报告时才会支持 IGMP 报告抑制功能。当组播查询包含 IGMPv3 报告时，不支持此功能。

  交换机使用 IGMP 报告抑制功能将每个组播路由器查询的一个 IGMP 报告转发给组播设备。当启用 IGMP 报告抑制功能时，交换机会将来自一个组播组的所有主机的第一个 IGMP 报告发送给所有组播路由器。交换机不会发送组播组剩余的 IGMP 报告给组播路由器。此功能可防止重复的报告被发送到组播设备。

  不论组播路由器查询是否也包含 IGMPv3 报告，交换机始终只会将来自一个组播组的所有主机的第一个 IGMPv1 或 IGMPv2 报告发送给所有组播路由器。

步骤 3 单击 “应用”。保存全局 IGMP 侦听设置，并更新交换机的当前配置。

步骤 4 选择一个 VLAN，然后单击 “编辑”。

步骤 5 设定以下参数：

- **VLAN ID** — 选择要设置的 VLAN。
- **IGMP Snooping** 状态 — 选择启用或禁用 IGMP 侦听功能。IGMP 侦听可监控网络流量以确定哪些主机已要求接收组播流量。
- 组播路由器端口自动学习 — 选择启用或禁用是否自动获取组播路由器所连接的端口。
- 查询健壮性 — 输入当此交换机是选择的查询器时要使用的健壮性变量值。
- 查询间隔 — 输入当此交换机是选择的查询器时要使用的普通查询的时间间隔。

- 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。
- 最后成员查询计数值 — 如果交换机是选择的查询器且假定此组播组没有任何成员端口时，输入发送的特定 IGMP 组的查询数。
- 最后成员查询周期 — 如果交换机无法从由选择的查询器发送的特定组查询中读取最大响应时间值，在此字段输入要使用最大响应延迟。
- 立即离开 — 当在成员端口上接收到一个 IGMP 组离开消息时，启用此功能可减少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。

  网络中只有一个 IGMP 查询器。交换机支持基于标准的 IGMP 查询器选择。此此表格的某些运行参数的值由选择的查询器发送，而其他值则来自于交换机本身。
- **IGMP** 查询器版本 — 当交换机成为选择的查询器时，选择要使用的 IGMP 版本。如果在 VLAN 中存在执行特定源 IP 组播转发的交换机和 / 或组播路由器时，请选择 IGMPv3。

步骤 6 单击 “应用”。定义 VLAN 的 IGMP 侦听设置，并更新交换机的当前配置。

设置 MLD 侦听

要支持 IPv6 组播转发，必须全局和在每个相关 VLAN 上都启用 MLD 侦听。交换机支持在静态和动态 VLAN 上都支持 MLD 侦听。

主机使用 MLD 协议来报告组播会话中这些主机的参与情况，交换机使用 MLD 侦听功能来构建组播成员关系列表。交换机会使用这些列表来转发组播数据包到其中存在作为组播组成员的主机节点的交换机端口。交换机不支持 MLD 查询器。

交换机支持两种 MLD 侦听版本：

- MLDv1 侦听检测 MLDv1 控制数据包并根据 IPv6 目的组播地址设置流量桥接。
- MLDv2 侦听使用 MLDv2 控制数据包，根据目的地址转发流量。MLDv2 侦听支持解析 MLDv2 控制数据包的能力。

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 侦听的方法，在交换机将 MLD 帧从多个工作站转发到一个上行组播路由器时侦听这些帧，反之亦然。此设备可使交换机能够推断以下信息：

- 想要加入特定组播组的工作站位于哪些端口上
- 发送组播帧的组播路由器位于哪些端口上

这些信息用于从传入组播帧的转发集中排除不相关的端口 （这些端口上没有经过注册可接收特定组播组的工作站）。

除手动配置的组播组之外，如果您还启用了 MLD 侦听，则结果是衍生自手动设置和通过 MLD 侦听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。

设置 MLD 侦听的步骤：

步骤 1 单击 “组播” > “ **MLD Snooping**”。

步骤 2 设定以下参数：

- **MLD Snooping** 版本 — 选择交换机支持的 MLD 侦听版本 （MLDv1 或 MLDv2）。
- 报告抑制 — 选择启用或禁用 IPv6 MLD 侦听报告抑制功能。禁用此功能将所有 MLDv1 报告转发给所有组播路由器。

步骤 3 单击 “应用”。设置 MLD 侦听全局参数，并更新交换机的当前配置。

步骤 4 选择一个 VLAN，然后单击 “编辑”。

步骤 5 设定以下参数：

- **VLAN ID** — 选择要设置的 VLAN。
- **MLD Snooping** 状态 — 选择在 VLAN 上启用或禁用 MLD 侦听功能。交换机会监控网络流量以确定哪些主机已要求接收组播流量。只有全局和在每个相关 VLAN 上都启用 MLD 侦听功能，交换机才会执行 MLD 侦听操作。
- 组播路由器端口自动学习 — 选择启用或禁用自动获取组播路由器端口功能。
- 查询健壮性 — 输入要使用的健壮性变量值 （如果该交换机无法从所选查询器发送的消息获取此值）。
- 查询间隔 — 输入交换机要使用的查询间隔值 （如果该交换机无法从所选查询器发送的消息获取此值）。
- 查询最大响应间隔 — 输入要使用的查询最大响应延迟时间 （如果交换机无法从所选查询器发送的普通查询读取最大响应时间值）。
- 最后成员查询计数器 — 输入要使用的最后成员查询次数 （如果交换机无法从所选查询器发送的消息获取此值）。

- 最后成员查询周期 — 输入要使用的最大响应延迟时间 （如果交换机无法从所选查询器发送的特定组的查询读取最大响应时间值）。
- 立即离开 — 启用此功能，将减少用来阻止发送到交换机端口的多余 MLD 流量的时间。

步骤 6 单击 “应用”。定义 VLAN 的 MLD 侦听设置，并更新交换机的当前配置。

查询 IGMP/MLD IP 组播组

使用 “IGMP/MLD IP 组播组”页面显示交换机从侦听的 IGMP/MLD 消息获取的 IPv4 和 IPv6 组地址。

查询 IGMP/MLD IP 组播组的步骤：

步骤 1 单击 “组播” > “**IGMP/MLD IP** 组播组”。

步骤 2 设定以下查询条件：

- **VLAN ID** — 按照设定的 VLAN 过滤侦听获取的 IP 组播组地址。
- **IP** 版本 — 按照选择的 IP 版本（IPv6 或 IPv4）过滤侦听获取的 IP 组播组地址。
- **IP** 组播组地址 — 按照设定的 IP 组播组地址过滤侦听获取的 IP 组播组地址。

步骤 3 单击 “确定”。

“IGMP/MLD IP 组播组表”中将列出符合条件的 IP 组播组地址及其详细信息，包括：

- **VLAN ID** — 组播流量的来源 VLAN。
- **IP** 组播组地址 — 组播组的 IP 地址。
- 成员端口 — 相应组播流被转发到哪些端口。
- 类型 — 组播组的类型，如静态或动态。
- 有效时间 — 动态组播组的有效时间。

设置组播路由器端口

组播路由器 （Multicast Rrouter，Mrouter）端口是指连接至一个组播路由器的端口。当交换机转发组播流和 IGMP/MLD 注册消息时，该交换机将包含组播路由器端口。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。

使用 “组播路由器端口”页面可以静态配置或动态检测哪些端口连接到组播路由器。

设置组播路由器端口的步骤：

步骤 1 单击 “组播” > “组播路由器端口”。

步骤 2 设置以下查询条件：

- **VLAN ID**— 选择组播流量的来源 VLAN。
- **IP** 版本 — 选择组播路由器支持的 IP 版本。
- 接口类型 — 选择端口或 LAG。

步骤 3 单击 “确定”。

步骤 4 为每个端口选择其关联类型。可选项如下：

- 静态 — 将端口静态配置为组播路由器端口。
- 动态 — 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功能，请分别在 “IGMP Snooping”页面和 “MLD Snooping”页面设置。
- 已禁止 — 不将此端口配置为组播路由器端口，即使此端口上接收到 IGMP 或 MLD 查询。
- 无 — 端口当前不是组播路由器端口。

步骤 5 单击 “应用”。设置组播路由器端口，并更新交换机的当前配置。

设置全部转发端口

使用 “全部转发”页面可设置要从特定 VLAN 接收组播流的端口或 LAG。

如果连接到端口的设备不支持 IGMP/MLD，您可以手动将该端口静态设置为全部转发端口。

注释 此配置仅影响所选 VLAN 的所有成员端口。

设置全部转发端口的步骤：

步骤 1 单击 “组播” > “全部转发”。

步骤 2 分别选择组播流量来自哪个 VLAN 和接口类型 （端口或 LAG），然后单击 “确定”。

步骤 3 设置端口是否要接收来自指定 VLAN 的所有组播流：

- 静态 — 端口接收所有注册的组播流。
- 已禁止 — 端口无法接收任何注册的组播流，即使 IGMP/MLD 侦听已指定端口加入组播组。
- 无 — 端口当前不是全部转发端口。

步骤 4 单击 “应用”。设置全部转发端口，并更新交换机的当前配置。

设置最大 IGMP/MLD 组播组

使用 “最大组播组数”页面可设置每个接口允许的最大组播组以及当超过上限时采取何种动作。

设置最大组播组的步骤：

步骤 1 单击 “组播” > “最大组播组数”。

步骤 2 选择接口类型 （端口或 LAG），单击 “确定”。

步骤 3 选择一个接口，然后单击 “编辑”。

步骤 4 设定以下参数：

- 接口 — 选择要限制组播组数量的端口或 LAG。
- **IGMP** 最大组播组 — 设置允许的最大 IGMP 组播组。
- **IGMP** 超出操作 — 选择当达到上限时拒绝或替换组播组。
- **MLD** 最大组播组 — 设置允许的最大 **MLD** 组播组。
- **MLD** 超出操作 — 选择当达到上限时拒绝或替换组播组。

步骤 5 单击 “应用”。设置端口的最大组播组，并更新交换机的当前配置。

设置组播过滤

您可以添加一个组播过滤模板，当加入组符合特定 IP 组播组范围时，允许或拒绝交换机学习到的一定范围的组播组，并将此组播过滤模板绑定到一个接口。此组播过滤设置将应道选择的接口。

设置组播过滤模板

使用组播过滤模板，当加入组播组匹配过滤模板设定的 IP 组播范围时，可允许或拒绝学习到的一定范围内的组播组。

设置组播过滤模板的步骤：

步骤 1 单击 “组播” > “组播过滤 ” > “模板”。

步骤 2 单击 “添加”，添加组播过滤模板。

步骤 3 设定以下参数：

- 模板索引 — 输入组播过滤模板的编号。
- **IP** 版本 — 选择组播的 IP 版本：IPv4 或 IPv6。
- 组播起始地址 — 输入起始的组播组地址。
- 组播结束地址 — 输入结束的组播组地址。
- 操作 — 选择允许或拒绝设定的组播组地址。

步骤 4 单击 “应用”。设置组播过滤模板，并更新交换机的当前配置。

设置接口组播过滤

使用 “过滤器设置”页面可绑定一个组播过滤模板到一个接口。

设置接口的组播过滤的步骤：

步骤 1 单击 “组播” > “组播过滤 ” > “过滤器设置”。

步骤 2 选择 IP 版本 （IPv4 或 IPv6）和接口类型 （端口或 LAG），然后单击 “确定”。

步骤 3 选择一个端口，单击 “编辑”。

步骤 4 设定以下参数：

- 接口 — 选择要设置组播过滤的端口或 LAG。
- 过滤器 — 选择启用或禁用此接口的组播过滤功能。
- 过滤模板索引 — 选择要采用的组播过滤模板，允许或拒绝设定的组播组地址。

步骤 5 单击 “应用”。定义接口的组播过滤设置，并更新交换机的当前配置。

15

配置 IP 信息

接口的 IP 地址可由用户手动配置或由 DHCP 服务器自动配置。

本章介绍如何手动或由 DHCP 服务器自动配置交换机 IP 地址，包括以下内容：

- IP 寻址
- 设置 IPv4 管理接口
- 设置 IPv6 管理接口
- 设置域名系统

IP 寻址

交换机的管理 VLAN 中拥有一个 IPv4 地址和一个 IPv6 接口。此 IP 地址及其默认网关可以手动配置也可以通过 DHCP 自动分配。静态 IP 地址和默认网管分别在 “IPv4 接口”和 “IPv6 接口”页面设定。交换机使用设定的默认网管与不在交换机同一 IP 子网内的其他设备进行通讯。默认情况下， VLAN1 是交换机的管理 VLAN。用户也可以修改默认的管理 VLAN。交换机只能通过其管理 VLAN 的特定 IP 地址被访问到。

IPv4 地址配置的出厂默认设置为 DHCPv4。这表示交换机作为一个 DHCPv4 客户端，在启动期间会发出 DHCPv4 请求以获取一个 IPv4 地址。

如果交换机收到 DHCPv4 服务器使用 IPv4 地址发送的 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 IP 地址正在使用中，则交换机会向提供 IP 地址的 DHCP 服务器发送一条 DHCPDECLINE 消息，并发送另一个重新启动该过程的 DHCPDISCOVER 数据包。

如果交换机在 60 秒内仍然未收到 DHCPv4 响应，它会继续发送 DHCPDISCOVER 查询并采用出厂默认的 IP 地址 192.168.1.254/24。

如果同一 IP 子网内的多个设备使用同一 IP 地址，则会发生 IP 地址冲突。地址冲突需要对与交换机发生冲突的 DHCP 服务器和 / 或设备执行管理操作。

将 VLAN 配置为使用动态 IP 地址时，交换机会发出 DHCPv4 请求直到 DHCPv4 服务器为其分配 IPv4 地址。只有管理 VLAN 可以使用静态或动态 IP 地址进行配置。

交换机的 IP 地址分配规则如下：

- 除非使用静态 IP 地址配置交换机，否则交换机会发出 DHCPv4 请求，直到收到 DHCP 服务器的响应。
- 交换机收到来自 DHCP 服务器的新的唯一 IP 地址时，系统状态指示灯会显示为绿色常亮。如果已设置静态 IP 地址，则系统状态指示灯也会显示为绿色常亮。如果交换机正获取 IP 地址并且当前正在使用出厂默认 IP 地址 192.168.1.254，则系统指示灯会闪烁。
- 如果DHCP客户端必须在其IP到期之前通过发送 DHCPREQUEST消息续租IP地址，则相同的规则也适用。
- 如果没有静态定义的 IP 地址或 DHCP 分配的 IP 地址可用，交换机会使用出厂默认的 IP 地址。有其他 IP 地址可用时，交换机会自动使用这些地址。默认 IP 地址始终在管理 VLAN 上。

如需通过基于 Web 的管理界面访问和管理交换机，交换机的管理 IP 地址必须被定义且为用户所知。在交换机从 DHCP 服务器获取一个 IP 地址之前，默认使用其出厂设置 192.168.1.254。您也可以手动设置此管理 IP 地址。

设置 IPv4 管理接口

要使用基于 Web 的管理界面管理交换机，您必须定义并知道交换机的管理 IPv4 地址。交换机管理 IPv4 地址可以手动配置，也可以从 DHCP 服务器自动获得。

设置交换机管理 IPv4 地址的步骤：

步骤 1 单击 “管理” > “管理接口” > “**IPv4** 接口”。

步骤 2 设定以下参数：

- 管理 **VLAN** — 选择通过 Telnet 或基于 Web 的管理界面来访问交换机的管理 VLAN。 VLAN1 为默认的管理 VLAN。
- **IP** 地址类型 — 选择 IP 地址的类型。可选项如下：
  - *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。

如果使用静态 IP 地址类型，请设定以下字段：

- **IP** 地址— 输入 IP 地址。
- 掩码 — 设定 IP 地址掩码或前缀长度。可选项如下：

- *网络掩码*— 选择此选项，手动输入 IP 地址掩码。
- *前缀长度* — 选择此选项，输入 IP 地址的前缀长度。

- 指定默认网关— 选择 “用户定义”并输入默认网关 IP 地址，或选择 “无”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 IP 地址。

注　　如果交换机为设置默认网关地址，则它无法与同一 IP 子网内的其他设备进行通信。

如果选择从 DHCP 服务器获取一个动态 IP 地址，设定以下字段：

- **DHCP** 强制自动配置 — 启用此功能，可强制交换机执行自动配置操作，即交换机将从一台 DHCP 服务器自动获取一个新的 IP 地址。在 DHCP 服务器动态分配了一个 IP 地址后，交换机可以选择在任何时间更新其动态 IP 地址。根据您的 DHCP 服务器配置，交换机可能会在 IP 地址更新后收到新的 IP 地址，从而导致与基于 Web 的管理界面的连接中断。
- 通过 **DHCP** 进行自动配置 — 显示交换机当前是否启用或禁用自动配置功能。您可以从 “管理” > “文件管理” > “DHCP 自动配置”页面设定此功能。

步骤 3　单击 “应用”。保存 IPv4 接口设置，并更新交换机的当前配置。

设置 IPv6 管理接口

交换机支持一个 IPv6 接口。除默认链路本地地址和组播地址外，交换机也可以根据接口接收到的路由广播将全局地址添加到接口。每个地址必须是使用冒号分隔的 16 位值以十六进制格式指定的有效 IPv6 地址。

设置 IPv6 接口的 IPv6 地址的步骤：

步骤 1　单击 “管理” > “管理接口” > “**IPv6** 接口”。

步骤 2　勾选 “**IPv6** 地址自动配置”选项，则交换机由 DHCPv6 服务器自动分配 IP 地址。

步骤 3　勾选 “**DHCPv6**”选项，启用 DHCPv6 服务器功能。

步骤 4　如您禁用以上两个选项，需手动设定以下参数：

- **IPv6** 地址— 输入交换机的 IPv6 地址。
- 前缀长度— 输入交换机的全局 IPv6 前缀长度。

- **IPv6** 网关— 输入默认路由器的链接本地 IPv6 地址。
- 链路本地地址— 显示交换机的链路本地 IPv6 地址。
- 正在使用的 **IPv6** 地址— 显示交换机当前使用的 IPv6 地址。
- 正在使用的 **IPv6** 网关— 显示交换机当前使用的 IPv6 网关地址。

步骤 5 如需将此接口作为一个 DHCPv6 客户端，使得交换机可以接收来自 DHCPv6 服务器的配置信息，设定以下参数：

- 无状态— 启用或禁用此接口作为一个无状态的 DHCPv6 客户端。
- 最小信息刷新时间— 选择 “无限期”或选择 “用户定义”手动设置一个值。“无限期”表示除非服务器发送此选项，否则不会刷新信息。此值用于给刷新时间值一个最低保证。如果服务器发送一个低于此设定值的刷新时间选项，那么此设定值将被采用。
- 信息刷新时间— 选择 “无限期”或选择 “用户定义”手动设置一个值。“无限期”表示除非服务器发送此选项，否则不会刷新信息。此值表示交换机多久时间更新一次从 DHCPv6 服务器接收到信息。如果没有从 DHCPv6 服务器接收到此选项，将使用此设定值。

步骤 6 单击 “应用”。设定 IPv6 接口配置，并更新交换机的当前配置。

设置域名系统

域名系统 (Domain Name System， DNS) 会将用户定义的域名转换为 IP 地址，以找到这些对象并对其进行寻址。作为一个 DNS 客户端，交换机可通过一个或对多个配置的 DNS 服务器将域名解析为 IP 地址。

定义 DNS 设置

使用 “DNS 设置”页面可启用或禁用 DNS 功能，设置 DNS 服务器以及交换机使用的默认域名。

设置 DNS 服务器的步骤：

步骤 1 单击 “**IP** 配置” > “域名系统” > “**DNS** 设置”。

步骤 2 选择启用或禁用 “**DNS**”选项。如启用 DNS，交换机将作为一个 DNS 客户端，并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。

步骤 3 如启用 DNS，在 “默认域名”字段输入默认 DNS 域名。交换机会对非完全限定的域名 （NFQDN）进行追加，以将其转换为 FQDN。

注释 请不要输入包含域名 （例如 cisco.com）中用来分割非限定名的初始句号。

步骤 4 单击 “应用”。设置 DNS 参数，并更新交换机的当前配置。

步骤 5 单击 “DHCP 域搜索列表”字段的 “详情”链接，可查看交换机上设定的 DNS 服务器的详细信息，包括用户定义的静态 DNS 服务器以及所有从 DHCPv4 和 DHCPv6 服务器收到的动态 DNS 服务器。

步骤 6 单击 “添加”，可手动添加一个 DNS 服务器。

步骤 7 设定以下参数：

- **IP** 版本— 选择定义 DNS 服务器 IP 地址的格式版本。
- **DNS** 服务器 **IP** 地址 — 输入 DNS 服务器的 IP 地址。
- 偏好 — 选择 DNS 服务器的偏好值。每一个 DNS 服务器都有一个偏好值，较低的偏好值表示较高的被使用的机会。

步骤 8 单击 “应用”。添加 DNS 服务器，并更新交换机的当前配置。

搜索 DNS 列表

域名搜索列表包含由用户定义的唯一静态域名和从 DHCPv4 和 DHCPv6 服务器接收到的所有动态域名。

如需查看交换机上设定的 DNS 域名，单击 “**IP** 配置” > “域名系统” > “搜索列表”。

显示以下信息：

- 源— 此域名所对应的服务器来源。其中：
  - 静态表示用户自定义
  - DHCPv4 表示来自于 DHCPv4 服务器
  - DHCPv6 表示来自于 DHCPv6 服务器
- 偏好— 域名使用的从低到高的偏好值。偏好值可以更有效地判断 DNS 查询期间按什么顺序完成的非限定名的查询。
- 域名— 交换机可使用的域名地址。

映射 DNS 主机

交换机会将所有主机名和 IP 地址的映射保存到主机映射表 （DNS 缓存）中。 DNS 缓存包含了手动添加的静态映射条目。域名解析始终从检查这些静态映射条目开始，然后继续向外部 DNS 服务器发送请求。

每个主机最多可关联 8 个 IP 地址。目前交换机仅支持关联的第一个 IP 地址与主机的映射关系可用。

添加域名及其 IP 地址的步骤：

步骤 1 击 “**IP** 配置” > “域名系统” > “主机映射”。

显示以下字段：

- 主机名— 用户定义的域名或完全限定名 （FQDN）。
- **IP** 地址— 主机的 IP 地址。
- **IP** 版本— 主机 IP 地址的版本。
- 类型— DNS 缓存中的静态条目。
- 状态— 访问此主机的尝试结果 （静态条目始终显示为 OK）。

步骤 2 单击 “添加”，添加一个主机映射规则。

步骤 3 设定以下参数：

- **IP** 版本— 选择主机 IP 地址的版本。
- 主机名— 输入一个域名或完全限定名 （FQDN）。
- **IP** 地址— 输入最多 8 个关联的 IP 地址。

步骤 4 单击 “应用”。添加一个主机映射规则，并更新交换机的当前配置。

16

设置安全性

交换机可处理多种类型的安全性，某些功能可用于多种类型的安全性或控制。例如，管理交换机的权限，保护交换机 CPU 不受攻击、控制终端用户通过交换机对网络的访问，保护其他网路用户不受攻击 （这些攻击通过交换机进行，而非针对交换机本身）。

本章介绍如何设置交换机的安全功能，包括以下内容：

- 设置用户帐号
- 设置 **TACACS+** 服务器
- 设置 **RADIUS** 服务器
- 管理访问方法
- 设置密码强度规则
- 管理访问验证
- 设置 **TCP/UDP** 服务
- 设置风暴控制
- 设置端口安全性
- 设置 **802.1X**
- 设置 **DoS** 防护
- 设置 **DHCP** 侦听
- 设置 **IP** 源防护
- 设置动态 **ARP** 检测

设置用户帐号

交换机默认的用户名和密码均为 **cisco**。首次登录交换机或者交换机密码过期时，系统会要求您设置一个新的管理密码。交换机默认启用密码强度检测机制。

使用 “用户帐号”页面可添加新的用户帐号或者修改用户密码。

系统默认管理员帐号不能被删除。

设置用户帐号的步骤：

步骤 1 单击 “管理” > “用户帐号”。

步骤 2 单击 “添加”，添加一个新用户；或选择一个用户并单击 “编辑”，修改用户参数。

步骤 3 设定以下参数：

- 用户名 — 输入新用户名。
- 密码 — 输入新密码 （用户密码必须满足密码强度规则的要求）。
- 确认密码 — 再次输入密码。
- 密码强度计 — 显示新密码的强度。有关设置密码强度规则的详细信息，请参考 “设置密码强度规则”。
- 用户等级 — 选择用户的权限等级。可选项如下：
  - *只读CLI访问(1)* — 用户只能访问交换机的命令行管理接口并执行不修改交换机配置的命令。用户不能访问交换机的基于 Web 的管理界面。
  - *读/写管理访问(15)* — 用户可访问交换机的基于Web的管理界面并设置交换机参数。

步骤 4 单击 “应用”。添加用户帐号，并更新交换机的当前配置。

设置 TACACS+ 服务器

一个机构可建立一个终端访问控制器访问控制系统 （Terminal Access Controller Access-Control System Plus, TACACS+）服务器，为所有设备提供集中的安全保护。通过这种方式，针对此机构的所有设备的认证和授权都可以在一台单一服务器上处理。

交换机可作为 TACACS+ 客户端，通过 TACACS+ 服务器来提供以下服务：

- 验证 — 对使用用户名和用户定义的密码登录到交换机的管理员进行验证。
- 授权 — 在登录时执行此服务。验证会话完成之后，将使用经过验证的用户名开始一个授权会话，然后 TACACS+ 服务器将检查用户权限。

TACACS+ 协议可通过加密协议在设备与 TACACS+ 服务器之间的交换来确保网络的完整性。

TACACS+ 仅支持 IPv4。

某些 TACACS+ 服务器只支持单一连接，使得设备接收单一连接的所有信息。如果 TACACS+ 服务器支持此功能，那么设备会恢复多个连接。

使用 “TACACS+”页面可设置 TACACS+ 服务器，设置用来与所有 TACACS+ 服务器进行通信的默认参数。您必须在 TACACS+ 服务器上配置用户，才有权授予该用户管理交换机的权限。

设置默认 TACACS+ 参数和添加 TACACS+ 服务器的步骤：

步骤 1 单击 “安全” > “**TACACS+**”。

步骤 2 设置以下默认 TACACS+ 参数：

- 密钥字符串 — 以明文或加密方式输入默认密钥字符串。此密钥字符串是用于与 TACACS+ 服务器进行通信的验证和加密密钥。如果您未在此字段中设定密钥字符串，则在添加 TACACS+ 服务器页面上设定的密钥必须与 TACACS+ 服务器所使用的加密密钥相匹配。如果您在此处设定了密钥字符串，并且为单个 TACACS+ 服务器也设定了密钥字符串，则单个 TACACS+ 服务器所配置的密钥字符串优先级较高。
- 应答超时 — 输入交换机与 TACACS+ 服务器之间的连接超时之前经过的时间量。如果单个 TACACS+ 服务器没有设定此值，则会使用此默认值。

步骤 3 单击 “应用”。设置 TACACS+ 默认参数，并更新交换机的当前配置。

步骤 4 单击 “添加”，添加 TACACS+ 服务器。

步骤 5 设定以下参数：

- 服务器定义 — 选择按 IP 地址或主机名来定义 TACACS+ 服务器。
- **IP** 版本 — 选择支持的 IP 格式。
- 服务器 **IP** 地址 / 名称 — 输入 TACACS+ 服务器的 IP 地址或主机名。
- 优先级 — 输入使用此 TACACS+ 服务器的优先级。 0 表示优先级最高的 TACACS+ 服务器，也就是第一个要使用的服务器。如果交换机无法建立与优先级最高的服务器的会话，交换机将尝试使用下一个优先级最高的服务器。
- 密钥字符串 — 密钥字符串使用 MD5 来加密通信。您可以选择 “使用默认设置”使用全局设定的密钥字符串默认值，也可以选择以加密模式或明文模式手动输入此密钥。此密钥必须与 TACACS+ 服务器上所配置的加密密钥相匹配。如果您没有来自其他设备的加密的密钥字符串，可以以明文形式输入此值。单击 “应用”后系统将生成和显示一个加密的密钥字符串。
- 应答超时 — 选择 “用户定义”手动输入交换机与 TACACS+ 服务器之间的连接超时之前经过的时间，或选择 “使用默认设置”使用全局设定的应答超时默认值。
- 验证 **IP** 端口 — 输入通过其进行 TACACS+ 会话的端口号。默认端口号为 49。

步骤 **6** 单击 “应用”。添加 TACACS+ 服务器，并更新交换机的当前配置。

设置 RADIUS 服务器

一个机构可以建立一台远程授权拨入用户服务 （Remote Authorization Dial-In User Service，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。

交换机作为 RADIUS 客户端，可使用 RADIUS 服务器来提供集中的安全保护、授权和用户验证。如需使用 RADIUS 服务器，您必须首先在 RADIUS 服务器上为交换机开通一个帐号，并使用在 “RADIUS”页面上设置的参数设置 RADIUS 服务器。

注释 如果设置有多台 RADIUS 服务器，那么交换机会根据可用 RADIUS 服务器的优先级来选择使用哪台 RADIUS 服务器。

设置 RADIUS 服务器的步骤：

步骤 **1** 单击 “安全” > “**RADIUS**”。

步骤 **2** 设定以下默认 RADIUS 参数：

注释 这些默认参数适用于所有 RADIUS 服务器。如果没有为特定 RADIUS 服务器输入相应的值，则交换机将使用这些默认值。

- 重试次数 — 输入在认为已发生故障之前发送到 RADIUS 服务器的传输请求的次数。
- 应答超时 — 输入交换机在重试查询或切换到下一个服务器之前等待从 RADIUS 服务器中返回响应的时间，单位为秒。
- 密钥字符串 — 选择以加密模式或明文模式输入使用 MD5 加密交换机和 RADIUS 服务器之间的通信的密钥字符串。此密钥必须与在 RADIUS 服务器上配置的密钥相匹配。如果您没有一个加密的密钥字符串，可以选择以明文形式输入。

步骤 **3** 单击 “应用”。设置默认 RADIUS 参数，并更新交换机的当前配置。

步骤 **4** 单击 “添加”，添加一台 RADIUS 服务器。

步骤 **5** 设置以下参数：

- 服务器定义 — 选择按 IP 地址或名称定义 RADIUS 服务器。
- **IP** 版本 — 选择支持的 IP 格式。
- 服务器 **IP** 地址 / 名称 — 输入 RADIUS 服务器的 IP 地址或主机名。
- 优先级 — 输入 RADIUS 服务器的优先级。优先级可确定交换机尝试联系服务器以验证用户的顺序。交换机将首先从优先级最高的 RADIUS 服务器开始。 0 代表最高优先级。
- 密钥字符串 — 选择 “用户定义”以明文或加密形式输入用于验证和加密交换机与 RADIUS 服务器之间通信的密钥字符串。此密钥必须与在单个 RADIUS 服务器上配置的密钥相匹配。您也可以选择 “使用默认设置”使用全局设定的默认值。
- 应答超时 — 选择 “用户定义”手动输入交换机在重试查询或转换到下一个服务器之前等待从 RADIUS 服务器中返回响应的秒数，或选择 “使用默认设置”使用全局设定的默认值。
- 验证 **IP** 端口 — 输入用于验证请求的 RADIUS 服务器的 UDP 端口号。默认为 1812。
- 重试次数 — 选择 “用户定义”手动输入在认为已发生故障之前发送到 RADIUS 服务器的请求次数，或选择 “使用默认设置”使用全局设定的默认值。
- 用途类型 — 选择 RADIUS 服务器的验证类型。可选项如下：
  - *登录* — RADIUS 服务器用于验证希望管理交换机的用户。
  - *802.1X* — RADIUS 服务器用于 802.1X 访问控制方面的验证。

- *全部* — RADIUS 服务器用于验证想要管理交换机的用户或 802.1X 访问控制方面的验证。

步骤 6 单击 “应用”。添加 RADIUS 服务器，并更新交换机的当前配置。

管理访问方法

管理访问验证设置用于验证和授权使用不同管理访问方法的用户的验证方法。详情可参考 “管理访问验证”一节的说明。管理访问模板限制特定源对交换机的管理访问。

只有通过活动的访问模板和管理访问验证的用户才会获得对交换机的管理访问权限。

访问模板规则、过滤器和元素

访问模板由允许访问交换机的规则组成。每个访问模板均可由一个或多个规则组成。交换机按照访问模板中规则的优先级顺序 （从上到下）来执行这些规则。

规则由包括以下元素的过滤器组成：

- 访问方法 — 访问和管理交换机的方法。包括：
  - Telnet
  - SSH
  - HTTP
  - HTTPS
  - SNMP
  - 以上全部
- 动作 — 允许或拒绝访问某一接口或特定源地址。
- 接口 — 可通过哪些端口或 LAG 访问交换机。
- 源地址 — IP 地址或子网。不同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 会话来访问交换机模块，而另一个用户组却能够使用 HTTPS 会话和 Telnet 会话来访问交换机。

活动的访问模板

“访问模板”页面显示了交换机上配置的所有访问模板，并允许您选择一个活动访问模板。交换机上只有一个访问模板可处于活动状态，并且任何访问交换机的尝试都必须符合活动的访问模板中的规则。

当一个用户试图使用某一访问方法访问交换机时，交换机会检查活动的访问模板是否允许通过此方法对交换机进行管理访问。如果没有找到匹配的规则，则该用户访问将被拒绝。

如果一个仅通过控制台访问模板被激活，则将其禁用的唯一方式就是从管理站直接连接到交换机上的物理控制台端口。

设置访问配置模板之后，可使用 “模板规则”页面添加或编辑其他规则。

设置访问模板

使用 “访问模板”页面可创建访问模板并添加一条规则。如果此访问模板仅包含一条规则，那么此访问模板的配置就完成了。如需添加多条规则，您必须在 “模板规则”页面继续添加。

设置访问模板和选择活动的访问模板的步骤：

步骤 1 单击 “安全” > “管理访问方法” > “访问模板”。

步骤 2 如需修改交换机的活动的访问模板，请从 “当前选中的访问模板”下拉框中选择一个访问模板。

步骤 3 单击 “应用”。选择的访问模板将成为活动的访问模板。

注释 如果您选择了 “仅控制台”并继续，则系统会立即断开您与基于 Web 的管理界面的连接，并且您只能通过控制台端口访问交换机。

注释 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相应的告警消息，提醒您系统可能会断开您与基于 Web 的管理界面的连接。

步骤 4 单击 “添加”，添加一个访问配置模板并定义一条规则。

步骤 5 设定以下参数：

- 访问模板名称 — 输入访问模板的名称。
- 规则优先级 — 输入规则优先级。当数据包与规则相匹配时，系统会允许或拒绝用户组访问交换机。由于根据首次匹配原则对数据包进行匹配，因此在将数据包与规则进行匹配时，规则优先级至关重要。 1 代表最高优先级。

- 管理方法 — 选择此规则定义的管理方法。使用此访问模板的用户只能使用选择的管理方法访问交换机。可选项如下：
  - *全部* — 将所有管理方法分配给规则。
  - *Telnet* — 只有通过 Telnet 方法访问交换机的用户才会被允许或拒绝访问。
  - *安全 Telnet（SSH）* — 只有通过 SSH 方法访问交换机的用户才会被允许或拒绝访问。
  - *HTTP* — 只有通过 HTTP 方法访问交换机的用户才会被允许或拒绝访问。
  - *安全HTTPS* — 只有使用HTTPS方法访问交换机的用户才会被允许或拒绝访问。
  - *SNMP* — 只有使用 SNMP 方法访问交换机的用户才会被允许或拒绝访问。
- 操作 — 选择用户访问匹配此规则时采用的操作。可选项如下：
  - *允许* — 如果用户与访问模板中的设置相匹配，则允许该用户访问交换机。
  - *拒绝* — 如果用户与访问模板中的设置相匹配，则拒绝该用户访问交换机。
- 应用到接口 — 选择将访问模板应用到接口。可选项如下：
  - *全部* — 选择此选项，此访问模板可应用到所有端口。
  - *用户定义* — 选择此选项，此访问模板仅应用到某一特定端口或 LAG。
- 接口 — 选择此访问模板要应用在哪个特定端口或 LAG 上。
- 应用到源 **IP** 地址 — 选择此访问模板应用的源 IP 地址类型。可选项如下：
  - *全部* — 选择此选项，此访问模板可应用到所有源 IP 地址。
  - *用户定义* — 选择此选项，此访问模板仅应用到特定源 IP 地址类型。
- **IP** 版本 — 选择 IP 地址版本。
- **IP** 地址 — 输入源 IP 地址。
- 掩码 — 选择源 IP 地址的子网掩码的格式并设定相应的值。
  - *网络掩码* — 输入源 IP 地址所属的子网和子网掩码。
  - *前缀长度* — 输入组成源 IP 地址前缀的位数。

步骤 **6** 单击 “应用”。添加访问模板和访问规则，并更新交换机当前配置。

设置访问规则

访问模板可包含多个访问规则，以确定有权管理和访问交换机的用户以及可使用的访问方法。

访问模板中的每个规则均包含要匹配的操作和标准 （一个或多个参数）。每个规则均具有优先级且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，您可以限制除 IP 管理中心的 IP 地址之外的所有 IP 地址访问交换机。通过此方式，交换机仍然可以被管理且获得了其他层次的安全保护。

设置访问模板的规则的步骤：

步骤 1 单击 “安全” > “管理访问方法” > “模板规则”。

步骤 2 选择一个访问模板并单击 “确定”。

步骤 3 单击 “添加”，添加一个规则到选择的访问模板。

步骤 4 设定以下参数：

- 访问模板名称 — 输入访问模板的名称。
- 规则优先级 — 输入规则优先级。当数据包与规则相匹配时，系统会允许或拒绝用户组访问交换机。由于根据首次匹配原则对数据包进行匹配，因此在将数据包与规则进行匹配时，规则优先级至关重要。
- 管理方法 — 选择此规则定义的管理方法。使用此访问模板的用户只能使用选择的管理方法访问交换机。可选项如下：
  - *全部* — 将所有管理方法分配给规则。
  - *Telnet* — 只有通过 Telnet 方法访问交换机的用户才会被允许或拒绝访问。
  - *安全 Telnet（SSH）* — 只有通过 SSH 方法访问交换机的用户才会被允许或拒绝访问。
  - *HTTP* — 只有通过 HTTP 方法访问交换机的用户才会被允许或拒绝访问。
  - *安全HTTPS* — 只有使用HTTPS方法访问交换机的用户才会被允许或拒绝访问。
  - *SNMP* — 只有使用 SNMP 方法访问交换机的用户才会被允许或拒绝访问。
- 操作 — 选择用户访问匹配此规则时采用的操作。可选项如下：
  - *允许* — 如果用户与访问模板中的设置相匹配，则允许该用户访问交换机。

- *拒绝* — 如果用户与访问模板中的设置相匹配，则拒绝该用户访问交换机。

- 应用到接口 — 选择将访问模板应用到接口。可选项如下：
  - *全部* — 选择此选项，此访问模板可应用到所有端口。
  - *用户定义* — 选择此选项，此访问模板仅应用到某一特定端口或 LAG。
- 接口 — 选择此访问模板要应用在哪个特定端口或 LAG 上。
- 应用到源 **IP** 地址 — 选择此访问模板应用的源 IP 地址类型。可选项如下：
  - *全部* — 选择此选项，此访问模板可应用到所有源 IP 地址。
  - *用户定义* — 选择此选项，此访问模板仅应用到特定源 IP 地址类型。
- **IP** 版本 — 选择 IP 地址版本。
- **IP** 地址 — 输入源 IP 地址。
- 掩码 — 选择源 IP 地址的子网掩码的格式并设定相应的值。
  - *网络掩码* — 输入源 IP 地址所属的子网和子网掩码。
  - *前缀长度* — 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，并更新交换机的当前配置。

设置密码强度规则

密码用于验证访问交换机的用户。简单密码可能有潜在的安全风险。因此，交换机默认强制启用密码复杂性要求。用户也可以修改密码复杂性设置。

使用 “密码强度”页面可修改最低密码复杂性要求并设置密码过期时间。

设置最低密码复杂性要求的步骤：

步骤 **1** 单击 “安全” > “密码强度”。

步骤 **2** 设定以下参数：

- 密码过期 — 选择启用或禁用密码过期功能。启用此功能时，当密码使用时间超过上限时，系统将提示用户更改密码。
- 密码过期时间 — 输入用户必须更改密码之前可经过的天数。默认为 180 天。

注　密码过期时间也适用于空密码。

- 密码复杂性设置 — 选择启用或禁用密码的最低复杂性要求 （默认为启用）。默认的密码复杂性要求如下：
  - 不能与当前密码相同
  - 不能与当前用户名相同
  - 必须包含至少三种字符类型 （可用的字符类型包括小写字母、大写字母、数字或特殊字符）
  - 不能包含连续 3 次的字符
  - 最低 8 个字符长度

步骤 3　您也可以在以下字段修改默认的密码复杂性设置：

- 最短密码长度 — 输入密码所需的最小字符数。
- 允许的字符重复 — 设置最多可连续输入多少个相同字符。
- 最少字符类别数 — 输入密码必须包含的字符类别：小写字母、大写字母、数字或特殊字符。
- 新密码必须与当前密码不同 — 勾选 “启用”，则新密码不能与当前密码相同。
- 新密码必须与当前用户名不同 — 勾选 “启用”，则新密码不能与当前用户名相同。

步骤 4　单击 “应用”。设置密码复杂性要求，并更新交换机的当前配置。

管理访问验证

您可以为不同的管理访问方法（如 SSH、Console、Telnet、HTTP 和 HTTPS）分配验证方法。可以在本地或外部服务器 （如 TACACS+ 或 RADIUS 服务器）上执行此验证。

如需通过 RADIUS 服务器授权对基于 Web 的管理界面的访问，则 RADIUS 服务器必须返回 cisco-avpair = shell:priv-lvl=15。

用户验证按照选择的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”，并且按照优先级顺序查询所有配置的 RADIUS 服务器而这些服务器并不做出回复，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不足，则系统会拒绝用户访问交换机。换句话说，如果验证因验证方法而失败，则交换机会停止验证尝试。交换机不会继续进行验证也不会尝试使用下一个验证方法。

为访问方法分配验证方法的步骤：

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 将 “可选方法”列表中的方法移动到 “选定的方法”列表。排第一位的方法将是首先要使用的验证方法。可选项如下：

- **RADIUS** — 在 RADIUS 服务器上验证用户。您必须已配置一个或多个 RADIUS 服务器。
- **TACACS+** — 在 TACACS+ 服务器上验证用户。您必须已配置一个或多个 TACACS+ 服务器。
- 无 — 允许用户在不经过验证的情况下访问交换机。
- 本地 — 根据存储在本地交换机上的数据检查用户名和密码。这些用户名和密码对是您在 “用户帐号”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关联，并更新交换机的当前配置。

设置 TCP/UDP 服务

使用 “TCP/UDP 服务”页面可在交换机上启用或禁用 TCP/UDP 服务和查看当前所有活跃的 TCP 和 UDP 连接的状态。

设置 TCP/UDP 服务的步骤：

步骤 1 单击 “安全” > “**TCP/UDP** 服务”。

“**TCP** 服务表”显示所有当前活跃的 TCP 连接的详细信息，包括：

- 服务名称 — 显示交换机提供此服务的方法。
- 类型 — 显示服务采用的 IP 协议。
- 本地 **IP** 地址 — 显示交换机提供此服务的本地 IP 地址。
- 本地端口 — 显示交换机提供此服务的本地 TCP 端口号。
- 远程 **IP** 地址 — 显示请求此服务的远程设备的 IP 地址。
- 远程端口 — 显示请求此服务的远程设备的 TCP 端口号。
- 状态 — 显示服务当前状态。下面列出不同状态的说明：
  - *ESTABLISHED* — 套接字已建立连接。
  - *SYN_SENT* — 套接字正在积极地试图建立连接。
  - *SYN_RECV* — 已接收到来自网络的连接请求。
  - *FIN_WAIT1* — 套接字已关闭，正在断开连接。
  - *FIN_WAIT2* — 连接已关闭，正在等待远程终端中断套接字。
  - *TIME_WAIT* — 套接字在关闭后正在等待处理仍然在网络中的数据包。
  - *CLOSED* — 套接字没有被使用。
  - *CLOSE_WAIT* — 远程终端已中断，正在等待套接字关闭。
  - *LAST_ACK* — 远程终端已中断且套接字已关闭，正在等待确认 。
  - *LISTEN* — 套接字正在监听传入连接。
  - *CLOSING* — 两个套接字均已中断，但仍然没有传输完所有数据。
  - *UNKNOWN* — 套接字状态为未知。

“**UDP** 服务表”显示所有当前活跃的 UDP 连接的详细信息，包括：

- 服务名称 — 显示交换机提供此服务的方法。
- 类型 — 显示服务采用的 IP 协议。
- 本地 **IP** 地址 — 显示交换机提供此服务的本地 IP 地址。
- 本地端口 — 显示交换机提供此服务的本地 UDP 端口号。

步骤 **2** 如有必要，启用或禁用以下 TCP 和 UDP 服务：

- **HTTP** 服务 （默认为启用）
- **HTTPS** 服务 （默认为启用）
- **SNMP** 服务 （默认为禁用）
- **Telnet** 服务 （默认为禁用）
- **SSH** 服务 （默认为禁用）

步骤 **3** 单击 “应用”。设置 TCP/UDP 服务，并更新交换机的当前配置。

设置风暴控制

交换机接收到广播帧、组播帧或未知单播帧后，会对它们进行复制，并将副本发送到所有可能的输出端口。也就是说实际上已将它们发送到属于相关 VLAN 的所有端口。通过这种方式，一个传入帧会转变为多个传入帧，从而使风暴的实现成为可能。

您可以通过风暴保护来限制进入交换机的帧数，并设置计入此限制的帧类型。

当广播帧、未知组播帧或未知单播帧的速率超过用户定义的阈值时，系统会丢弃达到阈值之后的接收到的帧或者关闭端口。

设置风暴控制的步骤：

步骤 **1** 单击 “安全” > “风暴控制”。

步骤 **2** 设置以下全局参数：

- 帧配置 — 选择在对广播帧、未知组播帧或未知单播帧进行风暴控制时计数 preamble 和 IFG 20Bytes。
- 风暴控制速率阈值模式 — 选择定义速率阈值的单位，如千位 / 秒或者数据包 / 秒。

步骤 3 单击 “应用”。

步骤 4 如需编辑端口的风暴控制设置，选择一个端口然后单击 “编辑”。

步骤 5 设定以下参数：

- 接口 — 选择要设置的端口。
- 风暴控制 — 在此端口上启用或禁用风暴控制功能。
- 未知单播 — 在此端口上启用或禁用针对未知单播流量的风暴控制。
- 风暴控制速率阈值 — 输入未知单播风暴控制的速率阈值。
- 未知组播 — 在此端口上启用或禁用针对未知组播流量的风暴控制。
- 风暴控制速率阈值 — 输入未知组播风暴控制的速率阈值。
- 广播 — 在此端口上启用或禁用针对广播流量的风暴控制。
- 风暴控制速率阈值 — 输入广播风暴控制的速率阈值。
- 操作 — 选择当超过设定的风暴控制速率阈值时采取何种动作。可选项如下：
  - *丢弃* — 丢弃接收到的数据包。
  - *关闭* — 关闭此端口。

步骤 6 单击 “应用”。设置端口的风暴控制参数，并更新交换机的当前配置。

设置端口安全性

限制特定 MAC 地址的用户对某一端口的访问可以增强网络安全性。 MAC 地址可以由系统自动学习或者用户手动配置。

端口安全性功能可监控接收到的和学习到的数据包。只允许通过特定 MAC 地址访问的锁定的端口。

端口安全性具有两种模式：

- 传统锁定 — 端口上所有学习到的 MAC 地址均被锁定且交换机可学习到此端口所允许的最大 MAC 地址数。学习的地址不会过期或无需重新学习。
- 有限动态锁定 — 交换机学习的 MAC 地址数不能超过配置的允许地址数上限。达到上限后，交换机不会学习其他地址。在这种模式下，地址会过期且无需重新获取。

当端口收到具有新 MAC 地址的未授权帧 （可能是此端口启用了传统锁定模式且此帧的 MAC 地址已被学习到另一个启用了传统锁定的端口上，或者此端口已被传统锁定或动态锁定且已超过了允许地址的最大数量）时，交换机会调用保护机制，并且可能会执行以下操作之一：

- 丢弃帧
- 转发帧
- 丢弃帧并且生成一个 SYSLOG 消息
- 关闭端口

当在另一个端口上发现安全 MAC 地址时，将会根据指定的操作处理此帧，并且该端口将不会学习此 MAC 地址。

使用 “端口安全”页面可设置端口的安全参数。

配置端口安全性的步骤：

步骤 1 单击 “安全” > “端口安全”。

步骤 2 选择一个端口，然后单击 “编辑”。

步骤 3 设定以下参数：

- 接口 — 选择要设置的端口。
- 接口状态 — 选择锁定或不锁定此端口。
- 学习模式 — 选择锁定端口的模式。此字段只有在 “接口状态”被设为锁定时才可用。如需修改端口的学习模式，锁定接口必须先解除锁定。修改学习模式之后，锁定接口可以重新恢复。可选项如下：
  - *传统锁定* — 立即锁定端口。启用此功能前，如果此端口已学习的 MAC 地址数超过了允许的最大地址数量，那么所有学习的地址将被清除。
  - *有限动态锁定* — 通过删除关联到此端口的当前动态 MAC 地址来锁定端口。端口最多可学习所允许的最大地址数。此时， MAC 地址的重新学习和过期机制都将被启用。
- 允许的最大地址数量 — 当端口处于有限动态锁定模式时，输入此端口可学习的最大 MAC 地址数。设置范围为 1 至 256，默认为 1。
- 违反规则响应措施 — 如果端口被锁定，选择对到达锁定端口的数据包所应采用的操作。可选项如下：
  - *丢弃* — 丢弃来自任何未知源的数据包。
  - *转发* — 转发来自任何未知源的数据包，无需学习 MAC 地址。

- *丢弃并记录* — 丢弃来自任何未获取源的数据包，关闭端口，记入系统日志以及发送 Trap 到指定的接收器。
- *关闭* — 丢弃来自任何未获取源的数据包并关闭端口，关闭端口，记入系统日志，并发送 Trap 到指定的接收器。在重新激活端口或重新启动交换机之前，该端口将始终保持关闭状态。

▪ **Trap** 频率 — 输入发送两个 Trap 通知之间的最短时间间隔，以秒为单位。当锁定端口接收到数据包时，交换机会启用发送 Trap 通知功能。

步骤 4 单击 “应用”。修改端口安全性设置，并更新交换机的当前配置。

设置 802.1X

基于端口的访问控制可在交换机端口上创建两种类型的访问。其中一个访问点启用非受控通信，而不考虑授权状态 （非受控端口）。另一个访问点对主机与交换机之间的通信进行授权。

802.1X 是一种 IEEE 标准，适用于基于端口的网络访问控制。 802.1X 框架可使设备（请求方）请求从其连接到的远程设备 （验证方）进行端口访问。仅当请求进行端口访问的请求方已经过验证和授权时，才允许请求方将数据发送到端口。否则，验证方会丢弃请求方数据，除非已将数据发送至访客 VLAN。

验证方通过外部的 RADIUS 服务器对请求方执行验证，并监控验证的结果。

按照 802.1X 标准，一台设备可以同时作为端口的请求方和验证方，既可以请求访问端口，也可以授权端口访问。但是，此设备只能是验证方，并且不会充当请求方的角色。

访客 VLAN

访客 VLAN 可提供对不需要进行 802.1X 或基于 MAC 的验证和授权的订阅设备或端口的服务的访问权限。

访客 VLAN 是具有以下特性的静态 VLAN：

▪ 必须根据现有的静态 VLAN 手动定义

▪ 仅可自动用于未经授权的设备或连接的已启用访客 VLAN 的设备的端口

- 如果端口已启用访客 VLAN，当端口未经授权时交换机会自动将其添加为访问 VLAN 的未添加标签的成员，并且当端口的第一个请求方被授权时交换机会从访客 VLAN 删除此端口。
- 访客 VLAN 不能用作语音 VLAN

802.1X 工作流程

如需设置 802.1X 功能，请执行以下操作：

- 在交换机上全局启用基于端口的验证。如有必要，启用并设置访客 VLAN。详见 “设置 802.1X 属性”。
- 在每个端口上设置 802.1X 端口验证。详见 “设置 802.1X 端口验证”。
- 查看 已验证主机的详细信息。详见 “查看已验证的主机”。

设置 802.1X 属性

使用 “属性”页面可在交换机上全局启用 或禁用 802.1X。必须全局启用和在每个端口上都启用 802.1X。

设置 802.1X 属性的步骤：

步骤 1 单击 “安全” > “**802.1X**” > “属性”。

步骤 2 设定以下参数：

- 基于端口的验证 — 全局启用或禁用基于端口的 802.1X 验证。
- 访客 **VLAN** — 勾选 “启用”，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设定的访客 VLAN。如果稍后对端口进行授权，则会从访客 VLAN 中删除该端口。
- 访客 **VLAN ID** — 从 VLAN 列表选择访客 VLAN。

步骤 3 单击 “应用”。设置 802.1X 属性，并更新交换机的当前配置。

设置 802.1X 端口验证

使用 “端口验证”页面可设置每个端口的 802.1X 功能。因为只有当端口处于强制授权状态时，某些配置更改才有可能实现，例如验证方法。因此，我们建议您在更改端口的 802.1X 设置之前，先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。

注释 启用了 802.1X 验证的端口不能成为 LAG 的成员端口。

设置端口的 802.1X 验证的步骤：

步骤 1 单击 “安全” > “**802.1X**” > “端口验证”。

步骤 2 选择一个端口，然后单击 “编辑”。

步骤 3 设定以下参数：

- 接口 — 选择要设置的端口。
- 用户名 — 显示用户名。
- 管理端口控制 — 选择端口控制管理方法。可选项如下：
  - *已禁用* — 不验证用户。
  - *强制未授权* — 通过将端口设为未经授权状态来拒绝端口访问。交换机不会为通过此端口的客户端提供验证服务。
  - *自动* — 在交换机上启用基于端口的验证和授权。端口根据交换机与客户端之间的验证交换在已授权状态或未经授权状态之间自动转变。
  - *强制授权* — 无需验证即对端口进行授权。
- 访客**VLAN** — 选择在此端口启用或禁用访客VLAN功能。如果启用访问VLAN功能，那么未经授权的端口将自动加入到访客 VLAN。

  在验证尝试失败后切如果指定的端口全局启用了访问 VLAN 功能，那么所有未授权的端口会被自动分配给访客 VLAN 的未添加标签的成员。
- 定期重新验证 — 勾选 “启用”，在指定的重新验证时间段之后尝试重新验证端口。
- 重新验证间隔 — 输入所选端口被重新验证的时间间隔，单位为秒。
- 验证方状态 — 显示设置的端口授权状态。可选项如下：
  - *初始化* — 处在恢复连接的过程中。
  - *强制授权* — 控制的端口状态被设为强制授权 （转发流量）。

- *强制未授权* — 控制的端口状态被设为强制未授权 （丢弃流量）。

  注　　如果端口不是处于强制授权或强制未授权状态，那么它将工作在自动模式下且其验证方将会显示正在进行的验证状态。在端口被验证之后，状态将显示为已验证。

- 静默期 — 输入当验证交换失败时交换机保持静默状态的时间。
- 请求方超时 — 输入在重新发送 EAP 请求给请求方之前的失效时间。
- 最大 **EAP** 请求数 — 输入最大可发送的 EAP 请求数。如果在超时后仍没有收到相应信息，重新开始验证过程。
- 请求方超时 — 输入在 EAP 请求被重新发送给请求方之前的超时时间。

步骤 **4** 单击 “应用”。设置端口 802.1X 验证，并更新交换机的当前配置。

查看已验证的主机

“已验证的主机”页面显示已验证的用户的详细信息。这些信息包括用于验证用户的用户名、工作站 MAC 地址和用户已登录的时间长度。

如需查看已验证用户的详细信息，单击 “安全” > “**802.1X**” > “已验证的主机”。

此页面显示以下字段：

- 用户名 — 在每个端口上已验证的请求方名称。
- 端口 — 端口号。
- 会话时间 — 请求方在端口上保持已登录状态的时间。
- 验证方法 — 显示验证上一个会话所使用的方法。
- **MAC** 地址 — 显示请求方的 MAC 地址。

设置 DoS 防护

拒绝服务 （Denial of Service， DoS）攻击是指造成某台设备无法为用户提供服务的攻击。拒绝服务攻击通过外部通信请求渗透到设备，使得设备无法对合法的流量进行响应。这些攻击通常会导致设备 CPU 过载。

DoS 防护功能是一组保护网络不受攻击的预先定义的规则的组合。而安全套件设置使得用户可以激活已设定的安全防护功能。

安全核心技术 (SCT)

交换机防范拒绝服务攻击的一种方法是使用 SCT 技术。交换机默认启用 SCT，且不能禁用此功能。

思科交换机是一种高级交换机，除终端用户流量之外，还处理管理流量、协议流量和侦听流量。交换机使用 SCT 功能，可以确保交换机无论接收的总流量是多少，都能够接收并处理管理和协议流量。

SCT 功能与其他功能间没有交互。

SCT 可在 “安全” > “拒绝服务” > “安全套件设置”页面中进行监控 （单击 “详情”按钮）。

默认设置

默认情况下， DoS 防护功能具有以下特性：

- 默认在所有端口上禁用 DoS 防护功能
- 默认在安全套件中启用 DoS 防护功能
- 默认启用 SYN-FIN 和 SYN-RST 防护
- SYN 防护的默认保护模式为 “阻塞并报告”。默认的 SYN 保护阈值为 60 SYN 数据包每秒。默认的端口恢复周期为 60 秒。

定义拒绝服务安全套件设置

使用 “安全套件设置”页面可以启用流量过滤功能。这样可以保护网络不受 DoS 和 DDoS 攻击。

注释 在激活 DoS 防护功能之前，您必须解除所有 ACL 或者高级 QoS 策略与端口的绑定。也就是说，当端口具有 DoS 防护功能时， ACL 和高级 QoS 策略不可用。

设置全局 DoS 防护功能并监控 SCT 的步骤：

步骤 1 单击 “安全” > “拒绝服务” > “安全套件设置”。

“**CPU** 保护机制”字段显示交换机当前是否启用了安全核心技术 （始终显示为已启用）。

步骤 2 单击 “**CPU** 使用率”字段的 “详情”按钮，可转到 “CPU 利用率”页面查看交换机当前的 CPU 使用情况。

步骤 3 单击 “**TCP SYN** 保护”字段的 “编辑”按钮，可转到 “SYN 保护”页面查看和设置 SYN 保护功能。

步骤 4 在 “拒绝服务防护”区域，列出了交换机可支持的安全套件。您可以选择启用或禁用此套件中一个或多个拒绝服务防护功能并设置相应的触发阈值 （如有必要）。交换机安全套件包括以下拒绝服务防护功能：

- DA 等于 SA （默认为启用）
- ICMP 分片数据包 （默认为启用）
- ICMP Ping 最大长度 （默认为启用，默认的阈值为 512）
  - 启用 ICMPv4
  - 启用 ICMPv6
- IPv6 最小分片长度 （默认为启用，默认阈值为 1240）
- Land （默认为启用）
- Null 扫描 （默认为启用）
- POD （默认为启用）
- Smurf 子网掩码 （默认为启用，默认阈值为 0）
- 低于 1024 的 TCP 源端口 （默认为启用）
- TCP Blat （默认为启用）
- 最小 TCP Frag-Off 检查 （默认为启用）
- TCP Herder 最小长度 （默认为启用，默认阈值为 20）
- UDP Blat （默认为启用）
- XMA （默认为启用）

步骤 5 单击 “应用”。设置拒绝服务防护功能，并更新交换机的当前配置。

定义 DoS 接口设置

使用 “接口设置”页面可针对每个端口启用或禁用 DoS 防护功能和 IP Gratuitous ARP 防护功能。在安全套件设置中启用的 DoS 防护功能将会作用到启用了 DoS 防护功能的端口。

设置端口的 DoS 防护和 IP Gratuitous ARP 防护功能的步骤：

步骤 1 单击 “安全” > “拒绝服务” > “接口设置”。

步骤 2 选择接口类型 （端口或 LAG），然后单击 “确定”。

显示以下信息：

- 接口 — 显示接口编号。
- **DoS** 防护 — 显示当前接口是否启用或禁用 DoS 防护功能。
- **IP Gratuitous ARPs**防护— 显示当前接口是否启用或禁用IP Gratuitous ARP功能。

步骤 3 如需修改接口的 DoS 设置，选择一个接口然后单击 “编辑”。

步骤 4 设置以下参数：

- 接口 — 选择要设置的端口或 LAG。
- **DoS** 防护 — 选择是否在此端口上启用或禁用 DoS 防护功能。
- **IP Gratuitous ARPs**防护— 选择是否在此端口上启用或禁用IP Gratuitous ARP功能。

步骤 5 单机 “应用”。在端口上启用或禁用 DoS 防护功能，并更新交换机的当前配置。

设置 SYN 保护

网络端口可能被黑客利用 SYN 攻击来消耗交换机的 TCP 资源和 CPU 功率。

因为 CPU 使用 SCT 功能进行保护，因此流向 CPU 的 TCP 流量会受到限制。但是，如果当一个或多个端口被高速率的 SYN 数据包攻击时， CPU 就只能接收来自黑客的数据包，造成交换拒绝提供服务。

使用 SYN 保护功能时， CPU 会统计每秒钟来自每一个端口的 SYN 数据包的数量。如果 SYN 数据包数超出了指定的阈值，那么一条拒绝 SYN 数据包的规则会被应用到相应的端口。端口会在每个用户定义的间隔时间之后解除绑定此规则。

设置 SYN 保护的步骤：

步骤 1 单击 “安全” > “拒绝服务” > “**SYN** 保护”。

“SYN 保护接口表”显示以下信息：

- 接口 — 显示接口编号。
- 当前状态 — 显示当前此接口是否受到 SYN 攻击。
- 上一个攻击 — 显示此接口检测到的上一次 SYN 攻击的时间。

步骤 2 设定以下全局参数：

- 阻塞 **SYN-RST** 数据包 — 选择是否阻塞 SYN-RST 数据包功能。启用此功能，在启用了 DoS 防护的端口上将丢弃所有带有 SYN 和 RST 标记的 TCP 数据包。
- 阻塞 **SYN-FIN** 数据包 — 选择是否阻塞 SYN-FIN 数据包。启用此功能，在启用了 DoS 防护的端口上将丢弃带有 SYN 和 FIN 标记的 TCP 数据包。
- **SYN** 保护模式 — 选择此端口采用的 SYN 保护模式。可选项如下：
  - 禁用 — 在此端口上禁用 SYN 保护功能。
  - 报告 — 创建一条 SYSLOG 消息，报告交换机受到 SYN 服务攻击。当超出了设定的阈值时，此端口的状态将修改为受到攻击。
  - 阻塞并报告 — 当一个 TCP SYN 攻击被识别时，发送到系统的 TCP SYN 数据包将被丢弃，且端口的状态将更改为已阻塞。
- **SYN** 保护阈值 — 输入触发 SYN 保护的阈值（默认为 60 数据包 / 秒）。此值表示在 SYN 数据包被阻塞之前的检测到每秒收到的 SYN 数据包数。当超出此阈值时，将应用一条拒绝 SYN 规则到此端口。
- **SYN** 保护期限 — 输入 SYN 保护的间隔周期（默认为 60 秒）。此值表示在不阻塞 SYN 数据包之前的时间。将不会在此端口上继续应用拒绝 SYN 规则。

步骤 3 单击 “应用”。设置 SYN 保护功能，并更新交换机的当前配置。

设置 DHCP 侦听

DHCP 侦听 （DHCP Snooping）通过过滤非信任的 DHCP 信息、建立和维护 DHCP 侦听绑定数据库来保护网络安全。 DHCP 侦听在非信任主机和 DHCP 服务器之间起到防火墙的作用。 DHCP 侦听区分连接到最终用户的非信任接口和连接到 DHCP 服务器或其他交换机的信任接口之间 DHCP 信息。

注释 DHCP 侦听功能仅在销售往中国大陆地区的交换机型号上支持。

设置 DHCP 侦听属性

“属性”页面可在交换机上启用或禁用 DHCP 侦听功能并设置 DHCP 侦听参数。

设置 DHCP 侦听属性的步骤：

步骤 1 单击 “安全” > “**DHCP Snooping**” > “属性”。

步骤 2 设定以下参数：

- **DHCP Snooping** 状态 — 在交换机上全局启用或禁用 DHCP 侦听功能。
- 验证 **MAC** 地址 — 勾选“启用”，在非信任端口上验证第 2 层头文件中的源 MAC 地址是否与出现在 DHCP 头文件中的客户端硬件地址一致。取消勾选禁用此功能 （默认为禁用）。
- **Option 82** 状态 — 在交换机上全局启用或禁用插入 Option 82 功能。
- 远程 **ID**— 如果启用插入 Option 82，选择 “用户定义”手动输入远程 ID，或选择 “使用默认设置”使用默认值。

步骤 3 在 “备份数据库”栏，设定以下参数：

- 备份数据库类型 — 选择备份 DHCP 侦听数据库代理的类型。可选项如下：
  - *无* — 禁用 DHCP 侦听数据库代理功能。
  - *闪存* — 将 DHCP 侦听绑定数据库保存到交换机的闪存。
  - *TFTP*— 将 DHCP 侦听绑定数据库保存到一台 TFTP 服务器。
- 文件名 —（仅限 TFTP 代理模式）输入要保存到 TFTP 服务器中的 DHCP 侦听配置的文件名称。
- 服务器 **IP** 地址 —（仅限 TFTP 代理模式）输入远程 TFTP 服务器的 IP 地址或主机名。

- 写入延迟 — 输入在更改 DHCP 侦听绑定数据库之后传输应延迟多长时间，单位为秒。设置范围为 15 到 86400 秒，默认为 300 秒。
- 超时 — 输入在更改 DHCP 侦听绑定数据库之后停止数据库传输进程的时间。设置范围为 0 到 86400 秒，默认为 300 秒。设为 0 表示无限期。

步骤 4 单击 “应用”。设置 DHCP 侦听属性，并更新交换机的当前配置。

定义 DHCP 侦听 VLAN 设置

使用 “VLAN 设置”页面可在 VLAN 上启用或禁用 DHCP 侦听功能。您必须在交换机上全局启用以及在每个 VLAN 上启用 DHCP 侦听功能。

在 VLAN 上启用或禁用 DHCP 侦听的步骤：

步骤 1 单击 “安全” > “**DHCP Snooping**” > “**VLAN** 设置”。

步骤 2 从 “可用的 **VLAN**”列表中将要启用 DHCP 侦听功能的 VLAN 添加到 “已启用的 **VLAN**”列表。

步骤 3 单击 “应用”。定义 DHCP 侦听 VLAN 设置，并更新交换机的当前配置。

设置 DHCP 侦听信任接口

使用 “接口设置”页面可设置 DHCP 侦听的信任接口。交换机转发所有的 DHCP 请求到信任接口。

设置 DHCP 侦听的信任接口的步骤：

步骤 1 单击 “安全” > “**DHCP Snooping**” > “接口设置”。

步骤 2 选择接口类型 （端口或 LAG），然后单击 “确定”。

步骤 3 从列表中选择一个接口，然后单击 “编辑”。

步骤 4 设定以下参数：

- 接口 — 选择要设置信任接口的端口或 LAG。
- 信任接口 — 选择信任或不信任此接口。

  注　连接到一台 DHCP 服务器或其他交换机或路由器的端口通常被设为信任接口，而连接到 DHCP 客户端的端口通常被设为非信任接口。

- 速率限制 — 启用 DHCP 速率限制功能并设置此接口所允许的速率上限。

步骤 5 单击 “应用”。设置 DHCP 侦听信任接口，并更新交换机的当前配置。

查询 DHCP 侦听绑定数据库

使用 “绑定数据库”页面可查询 DHCP 侦听绑定数据库的条目。

查询 DHCP 侦听绑定数据库的步骤：

步骤 1 单击 “安全”> “**DHCP Snooping**”> “绑定数据库”。

步骤 2 设定以下查询条件：

- **VLAN ID** — 勾选此选项，输入要查询的 VLAN ID。
- **MAC** 地址 — 勾选此选项，输入要查询的 MAC 地址。
- **IP** 地址 — 勾选此选项，输入要查询的 IP 地址。
- 接口 — 勾选此选项，选择要查询的端口或 LAG。

步骤 3 单击 “确定”。

“绑定数据库表”将显示所有符合条件的 DHCP 侦听绑定数据库条目的以下信息：

- **VLAN ID** — DHCP 侦听绑定数据中 IP 地址所属的 VLAN。
- **MAC** 地址 — 查询到的条目的 MAC 地址。
- **IP** 地址 — 查询到的条目的 MAC 地址。
- 接口 — 连接到此地址的接口。
- 类型 — IP 地址绑定类型。可选项如下：
  - *静态* — 此 IP 地址为静态 IP 地址。
  - *动态* — 此 IP 地址在数据库中被定义为一个动态 IP 地址。
- 租用时间 — DHCP 侦听数据库保存此条目的时间。当某一地址的租用时间过期时，将从数据库中删除。

查看 Option 82 统计信息

查看 DHCP 侦听 Option 82 统计信息的步骤：

步骤 1 单击 “安全” > “**DHCP Snooping**” > “统计信息”。

步骤 2 选择接口类型 （端口或 LAG），并单击 “确定”。

“统计信息表”显示以下信息：

- 接口 — 接口编号。
- 转发 — 转发的数据包总数。
- 已丢弃 **Chaddr** 检查 — Chaddr 检查所丢弃的数据包总数。
- 已丢弃不信任端口 — 不信任端口所丢弃的数据包总数。
- 已丢弃具有**Option82**的不信任端口— 启用了Option 82的不信任端口所丢弃的数据包总数。
- 丢弃无效 — 因无效而丢弃的数据包总数。

步骤 3 单击 “刷新”刷新统计信息表，或单击 “清除表”清除统计信息表。

定义 Option 82 接口设置

使用 “Option 82 接口设置”页面可设置如何处理不信任接口收到的带有 Option 82 信息的 DHCP 数据包。

定义 Option 82 接口设置的步骤：

步骤 1 单击 “安全” > “**DHCP Snooping**” > “**Option82** 接口设置”。

步骤 2 选择接口类型 （端口或 LAG），然后单击 “确定”。

步骤 3 选择一个接口，然后单击 “编辑”。

步骤 4 设定以下参数：

- 接口 — 选择要设置的端口或 LAG。
- 允许不信任 — 选择当不信任端口接收到 DHCP 数据包时所采取的动作。可选项如下：
  - *保留* — 保留带 Option 82 的 DHCP 数据包。

- *丢弃* — 丢弃带 Option 82 的 DHCP 数据包。
- *取代* — 替换带 Option 82 的 DHCP 数据包。

步骤 5 单击 “应用”。修改 Option82 端口设置，并更新交换机的当前配置。

定义 Option 82 接口 CID 设置

“Option 82 端口 CID 设置”页面可设置特定的 CID （Circuit ID）以便在 DHCP 服务器接收到报文后作相应地处理。

定义 Option82 接口 CID 设置的步骤：

步骤 1 单击 “安全” > “**DHCP Snooping**” > “**Option82** 端口 **CID** 设置”。

步骤 2 单击 “添加”。

步骤 3 设定以下参数：

- 接口 — 选择要设置的端口或 LAG。
- **VLAN**状态 — 选择在特定VLAN上使用电路ID，或禁止在所有VLAN上使用电路ID。
- **VLAN ID**— 选择要使用 CID 的 VLAN。
- 电路 **ID**— 输入要使用的 CID。

步骤 4 单击 “应用”。设置 Option 82 接口 CID 设置，并更新交换机的当前配置。

设置 IP 源防护

IP 源防护限制客户端 IP 流量到 IP 源防护绑定数据中定义的源 IP 地址。例如，IP 源防护可帮助阻止因一台主机试图使用其邻居的 IP 地址时造成的流量攻击。

注释 IP 源防护功能仅在销售给中国大陆地区的交换机型号上支持。

定义 IP 源防护接口设置

“接口设置”页面可在接口上启用或禁用 IP 源防护功能。

在接口上启用或禁用 IP 源防护功能的步骤：

步骤 1 单击 “安全” > “IP 源防护” > “接口设置”。

步骤 2 选择接口类型 （端口或 LAG），单击 “确定”。

步骤 3 选择一个接口，然后单击 “编辑”。

步骤 4 设定以下参数：

- 接口 — 选择要设置的端口或 LAG。
- IP 源防护 — 选择在此接口上启用或禁用 IP 源防护功能。
- 验证源 — 选择要验证的来源流量类型。可以只验证 IP 流量，也可以选择同时验证 MAC 和 IP 流量。
- 最大条目— 输入此端口所允许的最大IP源绑定规则数。设置范围为0到50。0表示无限之。

步骤 5 单击 “应用”。定义 IP 源防护接口设置，并更新交换机的当前配置。

查询 IP 源绑定数据库

使用 “绑定数据库”页面可查询和查看 IP 源防护数据库中记录的非攻击地址的详细信息，以及设置 IP/MAC 地址绑定规则。

查询 IP 源绑定数据库的步骤：

步骤 1 单击 “安全” > “IP 源防护” > “绑定数据库”。

步骤 2 设定以下查询条件：

- VLAN ID— 输入用来查询的 VLAN ID。
- MAC 地址 — 输入用来查询的 MAC 地址。
- IP 地址 — 输入用来查询的 IP 地址。
- 接口 — 选择要查询的端口或 LAG。

步骤 3 单击 “确定”。查询结果显示以下信息：

- **VLAN ID**— IP 地址关联的 VLAN。
- **MAC** 地址 — 接口的 MAC 地址。
- **IP** 地址 — 接口的 IP 地址。
- 接口 — 接口编号。
- 类型 — IP 地址类型，如：
  - *动态* — 表示 IP 地址是动态学习的 IP 地址。
  - *静态* — 表示 IP 地址是一个静态 IP 地址。
- 租用时间 — 表示此 IP 地址的可用时间。租用时间到期之后，IP 地址将从数据库中删除。

步骤 **4** 单击 “添加”，可添加 IP 源绑定规则。

步骤 **5** 设定以下参数：

- 接口 — 选择要设置的端口和 LAG。
- **VLAN ID**— 选择 IP 地址要关联到哪个 VLAN。
- **MAC** 地址 — 输入来源流量的 MAC 地址。
- **IP** 地址 — 输入来源流量的 IP 地址。

步骤 **6** 单击 “应用”。添加 IP 源绑定规则，并更新交换机的当前配置。

设置动态 ARP 检测

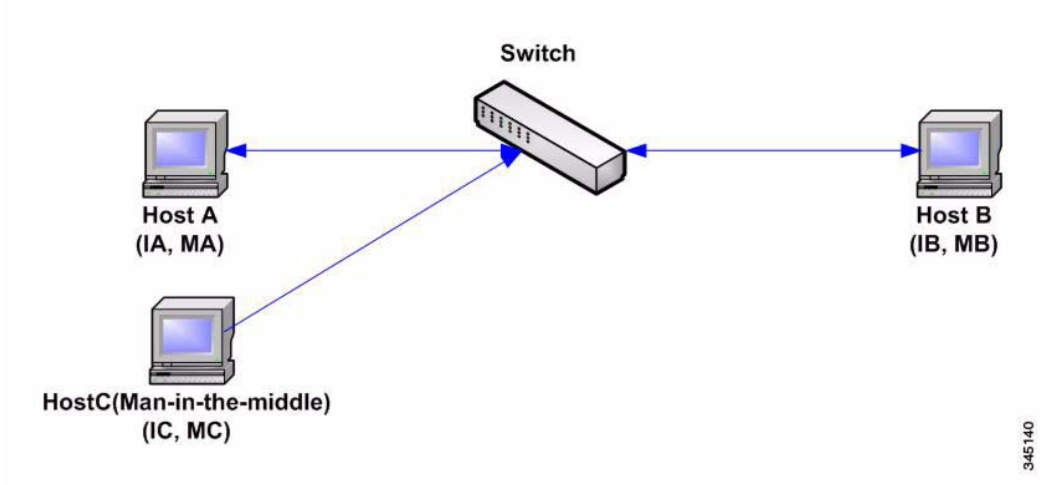
地址解析协议 （Address Resolution Protocol， ARP）是一个 TCP/IP 协议，用来将 IP 地址解析为 MAC 地址。

注释 ARP 检测功能仅在销售往中国大陆地区的交换机型号上支持。

ARP 缓存污染

恶意用户可以通过污染连接至子网的系统 ARP 缓存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 缓存污染示例：



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，污染交换机、主机 A 和主机 B 的 ARP 缓存。使用已污染 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 如何预防缓存污染

ARP 检测功能与接口相关联。

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。

- 如果未找到数据包的 IP 地址，且该数据包的 VLAN 已启用 DHCP 侦听，则在 DHCP 侦听绑定数据库中搜索该数据包的 <VLAN - IP 地址 > 对。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 侦听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。

如果在 “属性”页面启用了 ARP 数据包验证，将执行额外的验证检查：

- 源 **MAC** — 比较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。此检查针对 ARP 请求和响应都执行。
- 目的 **MAC** — 比较以太网报头中该数据包的目的 MAC 地址与目的接口 MAC 地址。此检查仅针对 ARP 响应执行。
- **IP** 地址 — 比较 ARP 正文，以找出无效和意外 IP 地址。一般包括 0.0.0.0、255.255.255.255 和所有 IP 组播地址。

系统将记录使用无效 ARP 检测绑定的数据包，并将其丢弃。

ARP 检测与 DHCP 侦听之间的交互

如果已启用 DHCP 侦听，则 ARP 检测除了使用 ARP 访问控制规则之外，还使用 DHCP 侦听绑定数据库。如果未启用 DHCP 侦听，则只使用 ARP 访问控制规则。

下表列出了 ARP 检测的默认设置：

选项	默认状态
动态 ARP 检测	禁用
ARP 数据包验证	禁用
在 VLAN 上启用 ARP 检测	禁用
日志缓存间隔	默认针对丢弃的数据包记录到系统日志，间隔时间为 5 秒。

ARP 检测工作流程

如需设置 ARP 检测功能，请执行以下操作：

步骤 1 在 “属性”页面启用 ARP 检测功能并设置各种参数。详见 “设置 **ARP** 检测属性”。

步骤 2 在 “接口设置”页面设置 ARP 检测的信任端口和非信任端口。详见 “设置 **ARP** 检测信任接口”。

步骤 3 在 “VLAN 设置”页面在 VLAN 上启用或禁用 ARP 检测功能。详见 “应用 **ARP** 检测到 **VLAN**”。

步骤 4 在 “统计信息”页面查看 ARP 检测统计信息。详见 “查看 **ARP** 检测统计信息”。

设置 ARP 检测属性

使用 “属性”页面可全局启用或禁用动态 ARP 检测功能并设置相关参数。

设置 ARP 检测属性的步骤：

步骤 1 单击 “安全”> “**ARP** 检测”> “属性”。

步骤 2 设定以下参数：

- **ARP** 检测状态 — 在交换机上全局启用或禁用动态 ARP 检测功能。
- **ARP** 数据包验证 — 选择 ARP 检测哪些数据包。可选项如下：
  - *源 MAC* — 在 ARP 请求和响应中验证源 MAC 地址。
  - *目的 MAC* — 在 ARP 响应中验证目的 MAC 地址。
  - *IP 地址* — 在 ARP 请求和响应中验证 IP 地址。
  - *允许全零IP地址*— 如果IP地址验证被启用，勾选此选项可允许全零IP地址。

步骤 3 单击 “应用”。设置 ARP 检测属性，并更新交换机的当前配置。

设置 ARP 检测信任接口

“接口设置”页面可设置 ARP 检测的信任或不信任接口以及设定接口允许的速率上限。 ARP 检测信任接口设置与 DHCP 侦听中定义的信任接口设置相互独立。 ARP 检测仅在不信任的接口上启用。

设置 ARP 检测信任接口的步骤：

步骤 1 单击 “安全” > “**ARP** 检测” > “接口设置”。

步骤 2 选择接口类型 （端口或 LAG），单击 “确定”。

步骤 3 选择一个接口，然后单击 “编辑”。

步骤 4 设定以下参数：

- 接口 — 选择要设置的端口或 LAG。
- 信任接口 — 选择是否信任此接口。如信任此接口，对通过此接口发送和接收的 ARP 请求或响应均不执行 ARP 检测。如不信任此接口，对通过此接口发送和接收的 ARP 请求或响应均执行 ARP 检测。
- 速率限制 — 设置此接口允许的最大速率。设置范围为 1 到 300 pps，默认为 15。

步骤 5 单击 “应用”。定义 ARP 检测接口设置，并更新交换机的当前配置。

查看 ARP 检测统计信息

“统计信息”页面显示 ARP 检测的统计信息。

查看 ARP 检测统计信息的步骤：

步骤 1 单击 “安全” > “**ARP** 检测” > “统计信息”。

“统计信息表”显示以下 ARP 检测统计信息：

- **VLAN ID**— VLAN 编号。
- 转发 — 此 VLAN 转发的 ARP 数据包总数。
- 源 **MAC** 故障 — 包含错误的源 MAC 地址的 ARP 数据包总数。
- 目的 **MAC** 故障 — 包含错误的目的 MAC 地址的 ARP 数据包总数。
- 源 **IP** 验证失败 — 源 IP 地址验证失败的 ARP 数据包总数。

- 目的 **IP** 验证失败 — 目的 IP 地址验证失败的 ARP 数据包总数。
- **IP** 与 **MAC** 不匹配故障 — IP 地址和 MAC 地址不匹配的 ARP 数据包总数。

步骤 2 单击 “刷新” 刷新 ARP 检测统计信息，或单击 “清除” 清除 ARP 检测统计信息。

应用 ARP 检测到 VLAN

使用 “VLAN 设置” 页面可在 VLAN 上启用 ARP 检测。当 VLAN 上启用了 ARP 检测时，用户将分配静态 ARP 检测列表给此 VLAN。当数据包通过一个启用了 ARP 检测的不信任接口时，交换机依次执行以下检测：

- 判断数据包的 IP 地址和 MAC 地址是否已存在于静态 ARP 检测表。如果已存在，数据包顺利通过此接口。
- 如果交换机没有发现匹配的 IP 地址，但是此 VLAN 上启用了 DHCP 侦听，则交换机会检测 DHCP 侦听数据验证此 IP 地址和 VLAN 是否相互匹配。如果在 DHCP 侦听数据库发现此条目，则数据包顺利通过接口。
- 如果数据包的 IP 地址既不在 ARP 检测列表也不在 DHCP 侦听数据库内，交换机会拒绝数据包。

应用 ARP 检测到 VLAN 的步骤：

步骤 1 单击 “安全” > “**ARP** 检测” > “**VLAN** 设置”。

步骤 2 从 “可用的 **VLAN**” 列表中将 VLAN 并添加到 “已启用的 **VLAN**” 列表，应用 ARP 检测到所选择的 VLAN。

步骤 3 单击 “应用”。应用 ARP 检测到 VLAN，并更新交换机的当前配置。

17

设置访问控制

访问控制列表（Access Control List， ACL）功能是安全机制的一部分。 ACL 定义可用于定义为特定服务质量 （QoS）提供的流量。有关 QoS 的详情，请参考 “设置服务质量”章节的介绍。

ACL 使得网络管理员可为入站流量设定模型 （包括过滤器和操作）。交换机棵接受或拒绝在具有活动 ACL 的端口或 LAG 上进入交换机的数据包。

本章主要介绍如何设置 ACL 规则，包含以下内容：

- 访问控制列表
- 设置基于 **MAC** 的 **ACL**
- 设置基于 **MAC** 的 **ACE**
- 设置基于 **IPv4** 的 **ACL**
- 设置基于 **IPv4** 的 **ACE**
- 设置基于 **IPv6** 的 **ACL**
- 设置基于 **IPv6** 的 **ACE**
- 设置 **ACL** 绑定

访问控制列表

访问控制列表是分类过滤器和操作的排序列表。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 （Access Control Element， 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 可包含一个或多个 ACE，这些 ACE 会与传入帧的内容进行匹配，并将一个拒绝或允许操作应用到内容与过滤器匹配的帧。

交换机最多可支持 512 条 ACL。每个 ACL 可支持最多 128 条 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。如果在一个 ACL 的所有 ACE 中都找不到匹配项，且存在另一个 ACL，则会在另一个 ACL 上执行相似的操作。

注释 如果在所有 ACL 的任意 ACE 中都找不到匹配项，那么此数据包将会被丢弃 （默认操作）。因此执行此默认丢弃操作，因此您必须将明确地将 ACE 添加到 ACL 以允许包括管理流量在内的所有流量。管理流量表示指向该交换机本身的 Telnet、 HTTP 或 SNMP 流量。例如，您不想丢弃所有与一个 ACL 中所有规则都不相匹配的数据包，那么您必须添加一个允许所有流量的 ACE 规则，并将其优先级设为最低。

如果绑定了一条 ACL 的端口上启用了 IGMP/MLD 侦听，那么必须在 ACL 中添加 ACE 过滤规则以转发 IGMP/MLD 数据包到交换机。否则 IGMP/MLD 侦听将无法作用到此端口上。

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 （例如允许或拒绝特定的流量），也可用于在 QoS 高级模式下进行流量分类和优化。

注释 既可以使用 ACL 也可以使用高级 QoS 策略保护端口安全，但不能同时使用这两种方法。

每个端口只能有一个 ACL （有可能同时将一个基于 IPv4 的 ACL 和一个基于 IPv6 的 ACL 关联到同一个端口）。

如需将一个或多个 ACL 绑定到一个端口，此端口必须使用一个或多个类映射的高级 QoS 策略。详见 “设置 **QoS** 策略”。

交换机可以定义以下类型的 ACL （具体取决于检查的帧报头部分）：

- 基于 MAC 的 ACL — 只检查第 2 层字段。详见 “设置基于 **MAC** 的 **ACL**”。
- 基于 IPv4 的 ACL — 检查 IP 帧的第 3 层。详见 “设置基于 **IPv4** 的 **ACL**”。
- 基于 IPv6 的 ACL — 检查 IPv4 帧的第 3 层。详见 “设置基于 **IPv6** 的 **ACL**”。

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 QoS 高级模式中，可以使用此流量名称代指这些帧，并将 QoS 应用于这些帧。详见 “设置 **QoS** 高级模式”。

创建 ACL 工作流程

要创建 ACL 并将其关联到一个接口，请执行以下操作：

步骤 1 创建以下类型的一个或多个 ACL：

- 创建基于 MAC 的 ACL 和基于 MAC 的 ACE。详见“设置基于 **MAC** 的 **ACL**”和“设置基于 **MAC** 的 **ACE**”。
- 创建基于 IPv4 的 ACL 和基于 IPv4 的 ACE。详见“设置基于 **IPv4** 的 **ACL**”和“设置基于 **IPv4** 的 **ACE**”。
- 创建基于 IPv6 的 ACL 和基于 IPv6 的 ACE。详见“设置基于 **IPv6** 的 **ACL**”和“设置基于 **IPv6** 的 **ACE**”。

步骤 2 在 “ACL 绑定”页面将创建的 ACL 与接口相关联。详见 “设置 **ACL** 绑定”。

修改 ACL 工作流程

只有在未使用 ACL 时，才可以对其进行修改。如需解除接口绑定的 ACL 并修改 ACL 设置，请按照顺序执行以下操作：

- 如果 ACL 不属于类映射 （QoS 高级模式），但已将其与一个接口相关联，可直接在在 “ACL 绑定”页面解除其与该接口的绑定。详见 “设置 **ACL** 绑定”。
- 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。
- 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，则您必须执行解除绑定的一系列操作：
  - 在 “策略绑定”页面解除包含类映射的策略与该接口的绑定。详见 “设置策略绑定”。
  - 从策略中删除包含 ACL 的类映射。详见 “设置 **QoS** 策略”。
  - 删除包含 ACL 的类映射。详见 “设置类映射”。

只有在执行这些操作后，才可以按本章中的各节所述修改 ACL。

设置基于 MAC 的 ACL

使用 “基于 MAC 的 ACL”页面可创建基于 MAC 的 ACL。基于 MAC 的 ACL 会检查所有帧，看是否有匹配项。

设置基于 MAC 的 ACL 的步骤：

步骤 1 单击 “访问控制” > “基于 **MAC** 的 **ACL**”。

步骤 2 单击 “添加”。

步骤 3 在 “**ACL** 名称”字段中输入基于 MAC 的 ACL 的名称。 ACL 名称区分大小写。

步骤 4 单击 “应用”。添加基于 MAC 的 ACL，并更新交换机的当前配置。

步骤 5 单击 “基于 **MAC** 的 **ACE** 表”可转到 “基于 MAC 的 ACE”页面为此 ACL 添加相应的规则 （ACE）。

设置基于 MAC 的 ACE

为基于 MAC 的 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 选择要添加规则的 ACL，然后单击 “确定”。

步骤 3 单击 “添加”。

步骤 4 设定以下参数：

- **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。交换机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。可选项如下：
  - *允许* — 转发符合此 ACE 标准的数据包。
  - *拒绝* — 丢弃符合此 ACE 标准的数据包。
  - *关闭* — 丢弃符合此 ACE 标准的数据包，并禁用接收这些数据包的端口。您可以在 “错误恢复设置”页面重新激活这类端口。

- 目的 **MAC** 地址 — 选择 “任意” 接受所有目标地址，或选择 “用户定义” 手动输入一个目标地址或目标地址范围。
  - *目的 MAC 地址值* — 输入目标 MAC 地址要匹配的 MAC 地址及其掩码（如相关）。
  - *目的 MAC 地址掩码* — 输入定义 MAC 地址范围的掩码。此掩码与其他用途的掩码 （如子网掩码）不同。在此处，设置为 1 表示不掩盖，设置为 0 表示掩盖该值。例如，值 “FFFFFF000000” 表示只会与目标 MAC 地址的前三个字节进行匹配。

  注　使用掩码 0000 0000 0000 0000 0000 0000 1111 1111 1111 1111 1111 1111，您可以选择匹配那些值为 0 的比特位，而不匹配那些值为 1 的比特位。您需要将 “1” 的数字转换为十六进制整数，并且每四个 0 要写成 0。在此示例中，因为 1111 1111 = FF，因此该掩码将写成：00000FFFFFF。
- 源 **MAC** 地址 — 选择 “任意” 接受所有源地址，或选择 “用户定义” 手动输入一个源地址或输入源地址范围。
  - *源 MAC 地址值* — 输入要源 MAC 地址要匹配的 MAC 地址及其掩码 （如相关）。
  - *源 MAC 地址掩码* — 输入定义 MAC 地址范围的掩码。
- **VLAN ID** — 输入 VLAN 标签中要匹配的 VLAN ID。
- **802.1p** — 如需使用 802.1p，勾选此选项并设定以下字段：
  - *802.1p 值* — 输入要添加到 VPT 标签的 802.1p 值。
  - *802.1p 掩码* — 输入要应用于 VPT 标签的掩码。
- 以太网类型 — 输入要匹配的帧以太网类型。

步骤 **5** 单击 “应用”。添加基于 MAC 的 ACE，并更新交换机的当前配置。

设置基于 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，如 ARP。

基于 IPv4 的 ACL 将匹配以下字段：

- IP 协议 （按照已知协议的名称或直接按照值）
- 源 IP 地址 / 目标 IP 地址 （包括掩码）

- TCP/UDL 流量的源端口 / 目标端口
- TCP 帧的标签值
- DSCP 值或 IP 优先级值
- ICMP 和 ICMP 类型和代码

注释 ACL 也可以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。详见 “设置 QoS 高级模式”。

使用 “基于 IPv4 的 ACL”页面创建基于 IPv4 的 ACL。使用 “基于 IPv4 的 ACE”页面添加相应的规则 （ACE）。

使用 “基于 IPv6 的 ACL”页面创建基于 IPv6 的 ACL。使用 “基于 IPv6 的 ACE”页面添加相应的规则 （ACE）。

设置基于 IPv4 的 ACL 的步骤：

步骤 1 单击 “访问控制” > “基于 **IPv4** 的 **ACL**”。

步骤 2 单击 “添加”。

步骤 3 在 “**ACL** 名称”字段中输入 ACL 名称。名称区分大小写。

步骤 4 单击 “应用”。添加基于 IPv4 的 ACL，并更新交换机的当前配置。

步骤 5 如需删除基于 IPv4 的 ACL，选择相应的条目并单击 “删除”。

步骤 6 单击 “基于 **IPv4** 的 **ACE** 表”可转到 “基于 IPv4 的 ACE”页面查看并设置相应的规则 （ACE）。

设置基于 IPv4 的 ACE

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 选择要添加规则的 ACL，然后单击 “确定”。显示此 ACL 相关的所有基于 IPv4 的 ACE。

步骤 3 单击 “添加”。

步骤 4 设定以下参数：

- **ACL** 名称 — 显示要添加规则的 ACL 的名称。
- 优先级 — 输入 ACE 的优先级。交换机会先处理优先级较高的 ACE。1 表示最高优先级。
- 操作 — 选择当数据包与 ACE 匹配时应采取的操作。可选项如下：
  - *允许* — 转发符合此 ACE 标准的数据包。
  - *拒绝* — 丢弃符合此 ACE 标准的数据包。
  - *关闭* — 丢弃符合此 ACE 标准的数据包，并禁用要处理数据包的端口。您可以从 “错误恢复设置” 页面重新激活此端口。
- 协议 — 选择根据根据哪个特定协议或协议 ID 来创建此 ACE。可选项如下：
  - *任意 (IP)* — 可接受所有 IP 协议
  - *从列表中选择* — 从下拉列表中选择以下协议之一：

    ICMP — 互联网控制消息协议

    IP in IP — IP-in-IP 封装协议

    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

    IPV6 — IPv6-over-IPv4 隧道协议

    IPV6:ROUT — 与属于通过一个网关的 IPv6-over-IPv4 路由的数据包进行匹配

    IPV6:FRAG — 与属于 IPv6-over-IPv4 分片报头的数据包进行匹配

    RSVP — 保留协议

    IPV6:ICMP — 互联网控制消息协议

    OSPF — 开放式最短路径优先

    PIM — 协议独立组播

    L2TP — 第 2 层隧道协议

- *要匹配的协议 ID* — 选择此选项，输入要匹配的协议 ID。

- 源 **IP** 地址 — 选择 “任意”接受所有源地址，或选择 “用户定义”手动输入一个源地址或输入源地址范围。
  - *源 IP 地址值* — 输入源 IP 地址将要匹配的 IP 地址。
  - *源 IP 地址掩码* — 输入定义 IP 地址范围的掩码。此掩码与其他用途的掩码（如子网掩码）不同。设置为 1 表示不掩盖，设置为 0 表示掩盖此值。
- 目的 **IP** 地址 — 选择 “任意”接受所有目标地址，或选择 “用户定义”手动输入一个目标地址或输入目标地址范围。
  - *目的 IP 地址值* — 输入目标 IP 地址要匹配的 IP 地址。
  - *目的 IP 地址掩码* — 输入定义 IP 地址范围的掩码。
- 源端口 — 请选择以下选项之一：
  - *任意* — 与所有源端口匹配。
  - *单个* — 输入数据包要匹配的单独 TCP/UDP 源端口。此字段只有在 “协议”下拉框中选择了 TCP 或 UDP 才可用。
  - *范围为* — 选择要将数据包与其相匹配的 TCP/UDP 源端口的范围。可配置八个不同的端口范围 （源端口与目标端口共享）。 TCP 和 UDP 协议各有八个端口范围。
- 目的端口 — 与上述 “源端口”字段相同，选择要匹配的目的端口。

  注　　您必须为 ACE 规则指定要匹配的 IP 协议，才能设置源端口和 / 或目标端口。
- **TCP** 标签 — 选择要用来过滤数据包的一个或多个 TCP 标签。过滤的数据包会被转发或直接丢弃。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。
  - *已设置* — 表示匹配此 TCP 标签。
  - *未设置* — 表示不匹配此 TCP 标签。
  - *忽略* — 忽略此 TCP 标签。
- 服务类型 — 选择 IP 数据包的服务类型。可选项如下：
  - *任意* — 任意服务类型。
  - *要匹配的 DSCP* — 输入要匹配的 DSCP 值。
  - *要匹配的 IP 优先级* — 输入要匹配的 IP 优先级值。

- **ICMP** — 如果 ACL 的 IP 协议为 ICMP，选择用于过滤的 ICMP 消息类型。可选项如下：
  - *任意 (IP)* — 可接受所有消息类型。
  - *从列表中选择* — 从下拉框中选择用于过滤用途的消息类型名称。
  - *要匹配的 ICMP 类型* — 输入用于过滤用途的 ICMP 消息类型编号。
- **ICMP** 代码 — ICMP 消息有一个代码字段，指示如何处理消息。选择 “任意” 接受所有 ICMP 代码，或选择 “用户定义” 手动输入用于过滤的 ICMP 代码。

步骤 5 单击 “应用”。添加基于 IPv4 的 ACE，并更新交换机的当前配置。

设置基于 IPv6 的 ACL

使用 “基于 IPv6 的 ACL” 页面可创建基于 IPv6 的 ACL。基于 IPv6 的 ACL 会检查单纯基于 IPv6 的流量，它不会检查 IPv6-over-IPv4 或 ARP 数据包。

设置基于 IPv6 的 ACL 的步骤：

步骤 1 单击 “访问控制” > “基于 **IPv6** 的 **ACL**”。

步骤 2 单击 “添加”。

步骤 3 在 “**ACL** 名称” 字段中输入 ACL 名称。名称区分大小写。

步骤 4 单击 “应用”。添加基于 IPv6 的 ACL，并更新交换机的当前配置。

步骤 5 单击 “基于 **IPv6** 的 **ACE** 表” 可转到 “基于 IPv6 的 ACE” 页面为其添加相应的规则（ACE）。详见 “设置基于 **IPv6** 的 **ACE**”。

设置基于 IPv6 的 ACE

为基于 IPv6 的 ACL 添加规则 （ACE）的步骤：

步骤 1 单击 “访问控制” > “基于 **IPv6** 的 **ACE**”。

步骤 2 选择要添加规则的 ACL，然后单击 “确定”。显示此 ACL 相关的所有基于 IPv6 的 ACE。

步骤 3 单击 “添加”。

步骤 4 设定以下参数：

- **ACL** 名称 — 显示要添加 ACE 的 ACL 名称。
- 优先级 — 输入 ACE 的优先级。交换机会先处理优先级较高的 ACE。1 表示最高优先级。
- 操作 — 选择如何处理匹配此 ACE 规则的数据包。可选项如下：
  - *允许* — 转发符合此 ACE 标准的数据包。
  - *拒绝* — 丢弃符合此 ACE 标准的数据包。
  - *关闭* — 丢弃符合此 ACE 标准的数据包，并禁用此数据包发送的端口。您可以从 “错误恢复设置”页面重新激活此端口。
- 协议 — 选择根据一个特定协议或协议 ID 来创建此 ACE。可选项如下：
  - *任意 (IP)* — 可接受所有 IP 协议。
  - *从列表中选择* — 从下拉列表中选择一个协议名称。其中：

    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 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 — 选择 “任意”接受所有源地址，或选择 “用户定义”手动输入一个源地址或输入源地址范围。
  - *源 IP 地址值* — 输入源 IP 地址要匹配的 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 — 选择 “任意”接受所有目的地址，或选择 “用户定义”手动输入一个目的地址或输入目的地址范围。
  - *目的 IP 地址值* — 输入要目的 IP 地址要匹配的 IP 地址及其掩码 （如果相关）。
  - *目的 IP 前缀长度* — 输入目的 IP 地址的前缀长度。
- 源端口 — 选择以下选项之一：
  - *任意* — 与所有源端口匹配。
  - *单个* — 输入数据包要匹配的一个单独的 TCP/UDP 源端口。此字段只有当“协议”字段被设为 TCP 或 UDP 时才可用。
  - *范围* — 选择数据包要匹配的 TCP/UDP 源端口的范围。
- 目的端口 — 与源端口设置相似，选择要匹配的目的端口或目的端口范围。

  注　　您必须为此 ACE 选择一个 IPv6 协议才能设置源端口和目的端口。
- **TCP** 标签 — 选择用来过滤数据包的一个或多个 TCP 标签。过滤的数据包会被转发或直接丢弃。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。
  - *已设置* — 匹配此 TCP 标签。
  - *未设置* — 不匹配此 TCP 标签。
  - *忽略* — 忽略 此 TCP 标签。
- 服务类型 — 选择 IP 数据包的服务类型。可选项如下：
  - *任意* — 任意服务类型。
  - *要匹配的 DSCP* — 选择要匹配的 DSCP 值。
  - *要匹配的 IP 优先级* — 选择要匹配 IP 优先级值。
- **ICMP** — 如果 ACL 基于 ICMP，选择用于过滤的 ICMP 消息类型。可选项如下：
  - *任意 (IP)* — 可接受所有消息类型。
  - *从列表中选择* — 从下拉列表中选择一个 ICMP 消息类型的名称。
  - *要匹配的 ICMP 类型* — 输入用于过滤的 ICMP 消息类型的编号。

- **ICMP** 代码 — ICMP 消息可能有一个代码字段，指示如何处理消息。选择 “任意”接受所有代码，或选择 “用户定义”手动输入用于过滤的 ICMP 代码。

步骤 5 单击 “应用”。添加基于 IPv6 的 ACE，并更新交换机的当前配置。

设置 ACL 绑定

将一个 ACL 与一个接口绑定后，此 ACL 的所有 ACE 规则将应用到所有到达此接口的数据包。与此 ACL 中任何 ACE 都不匹配的数据包将会与默认规则进行匹配，而默认规则将丢弃不匹配的数据包。

尽管一个接口只能与一个 ACL 绑定，但是多个接口可以与同一个 ACL 绑定。方法是将包含多个接口的 LAG 绑定到一个策略映射，从而实现将策略映射与多个接口绑定。

一旦将 ACL 绑定到接口后，便无法编辑、修改或删除此 ACL，直到将其从它绑定的或使用的所有接口中移除。

注释 接口既可以与一个 QoS 策略绑定，也可以与 ACL 绑定，但不同同时与它们进行绑定。

将 ACL 绑定到接口的步骤：

步骤 1 单击 “访问控制” > “**ACL** 绑定”。

步骤 2 选择接口类型 （端口或 LAG），单击 “确定”。

根据选择的接口类型，显示该类型的所有接口及其 ACL 绑定规则：

- 接口 — 接口编号。
- **MAC ACL** — 与接口绑定的基于 MAC 的 ACL （如果有）。
- **IPv4 ACL** — 与接口绑定的基于 IPv4 的 ACL （如果有）。
- **IPv6 ACL** — 与接口绑定的 基于 IPv6 的 ACL （如果有）。

步骤 3 要解除 ACL 与某接口的绑定关系，选择该接口并单击 “清除”。

步骤 4 要将某一 ACL 绑定到接口，选择接口并单击 “编辑”。

步骤 5 设定以下参数：

- 选择基于 **MAC** 的 **ACL** — 勾选此选项并选择要与该接口绑定的基于 MAC 的 ACL。

- 选择基于 **IPv4** 的 **ACL** — 勾选此选项并选择要与该接口绑定的基于 IPv4 的 ACL。
- 选择基于 **IPv6** 的 **ACL** — 勾选此选项并选择要与该接口绑定的基于 IPv6 的 ACL。

步骤 **6** 单击 “应用”。设置接口绑定的 ACL，并更新交换机的当前配置。

注释 如果不选择任何 ACL，则会解除之前与该接口绑定的 所有 ACL。

18

设置服务质量

在整个网络中应用服务质量 （quality of service, QoS）功能，可确保根据所需的标准设置网络流量的优先级，从而优先处理所需的流量。

本章介绍如何设置交换机的 QoS 功能，包含以下内容：

- **QoS** 功能和组件
- 设置 **QoS** 的工作流程
- 设置 **QoS** 基本模式
- 设置 **QoS** 高级模式

QoS 功能和组件

QoS 功能主要用于优化网络性能。 QoS 根据以下属性将传入流量分为不同的流量类型：

- 设备配置
- 传入接口
- 数据包内容
- 以上属性的组合

QoS 包括以下几个方面的特性：

- 流量分类 — 根据数据包内容和 / 或接口，将每个传入数据包分类为特定数据流。分类操作由 ACL 来完成，并且仅对符合 ACL 标准的流量进行 CoS 或 QoS 分类。
- 分配到硬件队列 — 将传入数据包分配给转发队列。数据包所属流量类别所具有的功能会将数据包发送到特定的队列进行处理。详见 “设置 **QoS** 队列”。
- 其他流量分类处理属性 — 将 QoS 机制应用到各种类别，包括带宽限制。

思科 220 交换机支持以下 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 （class of service， CoS）。

  将对相同类别的所有流量进行相同的处理。这是根据传入帧中指定的 QoS 值来确定出站接口上的出站队列的单一 QoS 操作。在 QoS 基本模式下，交换机信任此外部分配的 QoS 值。数据包的外部分配 QoS 值将决定其流量类别和 QoS。

- 高级模式 — 每数据流服务质量 （QoS）。

  在 QoS 高级模式中，每数据流 QoS 由一个类映射和一个策略器组成：

  - 类映射定义数据流中的流量类型和包含一个或多个 ACL。与 ACL 匹配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 配置通常由出站队列、DSCP 或 CoS/802.1p 值以及对超限流量执行的操作组成。

- 禁用模式 — 在此模式下，交换机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。

注释 在一个时刻只能有一种模式处于活动状态。如果交换机工作在 QoS 高级模式下，则 QoS 基本模式的设置将处于非活动状态，反之亦然。

更改 QoS 模式时将发生以下情况：

- 如果从 QoS 高级模式更改为任何其他模式，将会删除 QoS 策略和类映射。直接绑定到接口的 ACL 仍然会保持绑定状态。
- 如果从 QoS 基本模式更改为 QoS 高级模式，将不保留基本模式下的 QoS 信任模式配置。
- 如果禁用 QoS，会将整形和队列设置 （带宽限制设置）将重置为默认值。
- 所有其他用户配置将保持不变。

设置 QoS 的工作流程

请执行以下操作设置基本的 QoS 参数：

步骤 1 设置交换机的 QoS 模式 （如基本模式、高级模式或禁用模式，详见 “ 设置 QoS 属性”）。

以下步骤假定您启用了 QoS 功能。

步骤 2 为出口队列指定调度方法 （严格优先级或 WRR）以及分配给 WRR 的带宽权重。详见 “设置 QoS 队列”。

步骤 3 为每一个 CoS/802.1p 值指定一个出口队列。如果交换机处于 CoS/802.1p 信任模式，则会根据传入数据包的 CoS/802.1p 优先级将传入数据包放入指定的出口队列。详见 “映射 CoS/802.1P 到队列”。

步骤 4 为每一个 IP 优先权指定一个出口队列。详见 “映射 IP 优先权到队列”。

步骤 5 为每一个 DSCP 值指定一个出口队列。如果交换机处于 DSCP 信任模式，则会根据传入数据包的 DSCP 值将传入数据包放入出口队列。详见 “映射 DSCP 到队列”。

步骤 6 重新标记接口的传入流量的 CoS/802.1p 优先级、 IP 优先权和 / 或 DSCP 值。可同时重新标记 CoS/802.1p 优先级和 IP 优先权值，或者同时标记 DSCP 值和 CoS/802.1p 优先级值，但不能同时重新标记 IP 优先权值和 DSCP 值。详见 “设置接口重新标记”。

- 重新标记来自每个队列的传出流量的 CoS/802.1p 优先级。详见 “映射队列到 CoS/802.1p”。
- 重新标记来自每个队列的传出流量的 IP 优先权。详见 “映射队列到 IP 优先权”。
- 重新标记来自每个队列的传出流量的 DSCP 值。详见 “映射队列到 DSCP”。

步骤 7 设定带宽和速率限制：

- 设置每接口的入口速率限制和出口整形速率。详见 “设置带宽限制”。
- 设置每队列的出口整形。详见 “设置每队列出口整形”。
- 设置 VLAN 入口速率限制。详见 “设置 VLAN 入口速率限制”。

步骤 8 根据选择的 QoS 模式，然后执行以下操作：

- 设置 QoS 基本模式参数。详见 “设置 QoS 基本模式”。
- 设置 QoS 基本模式参数。详见 “ 设置 QoS 高级模式”。

步骤 9 激活 TCP 拥塞避免算法。详见 “设置 TCP 拥塞避免算法”。

设置 QoS 属性

使用 “QoS 属性”页面可设置交换机的 QoS 模式，并定义每个接口默认的 CoS 优先级。

设置 QoS 属性的步骤：

步骤 1 单击 “服务质量” > “一般” > “QoS 属性”。

步骤 2 选择交换机的 QoS 工作模式 （禁用模式、基本模式或高级模式）。

步骤 3 单击 “应用”。

步骤 4 在 “接口 QoS 配置表”栏，选择接口类型 （端口或 LAG），单击 “确定”。

“接口 QoS 配置表”中将显示所有接口的默认 CoS 优先级。

步骤 5 如需修改接口的默认 CoS 优先级，选择一个接口并单击 “编辑”。

步骤 6 设定以下参数：

- 接口 — 选择要设置的端口或 LAG。
- 默认 CoS — 选择分配给不包含 VLAN 标签的传入数据包的 CoS 值。设置范围为 0-7，默认为 0。

  此默认值仅在交换机工作在 QoS 基本模式且在信任模式设为 CoS/802.1p 的情况下有效。

步骤 7 单击 “应用”。设置接口的默认 CoS 值并更新交换机的当前配置。

步骤 8 如需将接口的 CoS 优先级设置恢复到出厂默认设置，勾选相应的接口然后单击 “恢复默认配置 ”。

设置 QoS 队列

交换机在每个接口支持 8 个队列。队列 8 为最高优先级队列，而队列 1 为最低优先级队列。

交换机支持两种处理队列中流量的方式：严格优先级 （Strict Priority， SP）和加权轮询 （Weighted Round Robin， WRR）。

- 严格优先级 — 最先传输最高优先级队列中的出站流量。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，从而为队列 8 提供最高的流量处理优先级。
- **WRR**— 在 WRR 模式下，从队列发送的数据包数量与队列权重成正比。权重越高，发送的帧越多。

使用 “队列”页面中可设置排队模式。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 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个优先级的队列。如果排队模式为 WRR，则会按照配额处理队列，在一个队列的配额用尽后开始处理另一个队列。

也可以将部分较低优先级的队列指定为 WRR 模式，同时保持部分较高优先级的队列为严格优先级模式。在这种情况下，严格优先级队列中的流量会始终先于 WRR 队列中的流量发送。仅当严格优先级队列中的流量发送完毕后才会转发 WRR 队列中的流量。每个 WRR 队列的相对配额取决于其权重。

设置队列优先级的步骤：

步骤 1 单击 “服务质量” > “一般” > “队列”。

步骤 2 设定以下参数：

- 队列 — 显示队列编号。
- 调度方法 — 选择以下选项之一：
  - *严格优先级* — 针对所选队列及所有更高优先级队列的流量调度将严格遵循队列优先级。
  - *WRR* — 针对所选队列的流量调度将遵循 WRR。在不为空的 WRR 队列（表示队列具有要输出的描述符）之间划分时段。仅当严格优先级队列为空时，才会采用此方法。
  - *WRR 权值* — 如果选择了 WRR，设置分配给队列的 WRR 权重。
  - *WRR 带宽百分比* — 显示已为队列分配的带宽百分比。这些值表示 WRR 权重的百分比。系统将根据 WRR 权值自动计算其 WRR 带宽百分比。

步骤 3 单击 “应用”。设置队列优先级，并更新交换机的当前配置。

映射 CoS/802.1P 到队列

使用 “CoS/802.1p 到队列”页面可将 802.1p 优先级映射到出口队列。交换机将根据传入数据包的 VLAN 标签中的 802.1p 优先级来确定数据包的出口队列。对于未添加标签的传入数据包， 802.1p 优先级将使用指定给入口接口的默认 CoS/802.1p 优先级。

802.1p 值 （0 到 7， 7 表示最高 802.1p 优先级）	队列 （8 个队列， 8 表示最高优先级队列）	备注
0	2	后台
1	1	尽力服务
2	3	最大努力
3	4	关键应用 LVS 电话 SIP
4	5	视频
5	6	语音思科 IP 电话默认
6	7	交互操作控制 LVS 电话 RTP
7	8	交互操作控制

通过更改 CoS/802.1p 到队列映射、队列调度方法和带宽分配，可以在网络中实现预期的服务质量。

仅当存在以下条件之一时， CoS/802.1p 到队列映射才可用：

- 交换机工作在 QoS 基本模式且信任模式设为 CoS/802.1p。
- 交换机工作在 QoS 高级模式且数据包属于 CoS/802.1p 信任数据流。

将 802.1p 优先级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 设定以下参数：

- **802.1p** — 显示要指定给出口队列的 802.1p 优先级值，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。交换机支持 8 个出口队列，其中队列 8 优先级最高，队列 1 优先级最低。

步骤 3 单击 “应用”。将 802.1p 优先级映射到队列并更新交换机的当前配置。

步骤 4 单击 “恢复默认设置”，将 802.1p 优先级与队列的映射设置恢复到出厂默认设置。

映射 IP 优先权到队列

使用 “IP 优先权到队列”页面可将 IP 优先权映射到出口队列。

将 IP 优先权映射到队列的步骤：

步骤 1 单击 “服务质量” > “一般” > “**IP** 优先权到队列”。

步骤 2 选择 IP 优先权所映射的输出队列 （流量转发队列）。

步骤 3 单击 “应用”。将 IP 优先权映射到队列，并更新交换机的当前配置。

步骤 4 单击 “恢复默认设置”，将 IP 优先权与队列的映射设置恢复到出厂默认设置。

映射 DSCP 到队列

使用 “DSCP 到队列”页面可将 DSCP 值映射到输出队列。交换机可根据传入 IP 数据包的 DSCP 值确定数据包的输出队列。数据包的原始 VPT （VLAN 优先级标签）不会发生更改。

通过更改 DSCP 到队列映射、队列调度方法和带宽分配，即可在网络中实现预期的服务质量。

在以下任意情况下， DSCP 到队列映射可应用于 IP 数据包：

- 交换机工作在 QoS 基本模式且信任模式设为 DSCP。
- 交换机工作在 QoS 高级模式且数据包属于 DSCP 信任的数据流。

注释 交换机始终将非 IP 数据包分类为尽力服务队列。

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”。

“入口 **DSCP**”字段显示传入数据包中的 DSCP 值及其关联类别。

步骤 2 选择 DSCP 值所映射的输出队列 （流量转发队列）。

步骤 3 单击 “应用”。将 DSCP 值映射到队列并更新交换机的当前配置。

步骤 4 单击 “恢复默认设置”，将 DSCP 到队列映射设置恢复到出厂默认设置。

映射队列到 CoS/802.1p

“队列到 CoS/802.1p”页面可重新标记每个队列的输出数据的 CoS/802.1p 优先级。

将队列映射到 CoS/802.1p 的步骤：

步骤 1 单击 “服务质量” > “一般” > “队列到 **CoS/802.1p**”。

步骤 2 为每个队列的输出流量选择重新标记的 CoS/802.1p 优先级值。

步骤 3 单击 “应用”。将队列映射到 CoS/802.1p 优先级，并更新交换机的当前配置。

步骤 4 单击 “恢复默认设置”，将队列到 CoS/802.1p 优先级映射设置还原为出厂默认设置。

映射队列到 IP 优先权

使用 “队列到 IP 优先权”页面可针对每个队列的输出数据重新标记其 IP 优先权。

将队列映射到 IP 优先权的步骤：

步骤 1 单击 “服务质量” > “一般” > “队列到 **IP** 优先权”。

步骤 2 为每个队列的输出流量选择重新标记的 IP 优先权值。

步骤 3 单击 “应用”。将队列映射到 IP 优先权，并更新交换机的当前配置。

步骤 4 单击 “恢复默认设置”，将队列到 IP 优先权映射设置还原为出厂默认设置。

映射队列到 DSCP

使用 “队列到 DSCP”页面可针对每个队列的输出数据重新标记其 DSCP 值。

将队列映射到 DSCP 值的步骤：

步骤 1 单击 “服务质量” > “一般” > “队列到 **DSCP**”。

步骤 2 为每个队列的输出流量选择重新标记的 DSCP 值。

步骤 3 单击 “应用”。将队列映射到 DSCP 值，并更新交换机的当前配置。

步骤 4 单击 “恢复默认设置 ”，将队列到 DSCP 值映射设置还原为出厂默认设置。

设置接口重新标记

“重新标记接口设置”页面可启用或禁用每个端口的重新标记功能。您可以同时重新标记 CoS/802.1p 和 IP 优先权值，或同时重新标记 DSCP 和 CoS/802.1p 值，但不能同时重新标记 IP 优先权和 DSCP 值。

设置接口的重新标记功能的步骤：

步骤 1 单击 “服务质量” > “一般” > “重新标记接口设置”。

步骤 2 选择接口类型 （端口或 LAG），单击 “确定”。

步骤 3 如需编辑接口的重新标记设置，选择一个接口然后单击 “编辑”。

步骤 4 设定以下参数：

- 接口 — 选择要设置的端口或 LAG。
- 重新标记 **CoS** — 在此接口上启用或禁用重新标记 CoS/802.1p 功能。每个队列的输出数据应重新标记的 CoS/802.1p 值可在 “队列到 CoS/802.1p”页面设置。
- 重新标记 **IP** 优先权 — 在此接口上启用或禁用重新标记 IP 优先权功能。每个队列的输出数据应重新标记的 IP 优先权值可在 “队列到 IP 优先权”页面设置。
- 重新标记 **DSCP** — 在此接口上启用或禁用重新标记 DSCP 功能。每个队列的输出数据应重新标记的 DSCP 值可在 “队列到 DSCP”页面设置。

  注 不能同时启用 “重新标记 IP 优先权”和 “重新标记 DSCP”选项。

步骤 5 单击 “应用”。设置接口的重新标记功能，并更新交换机的当前配置。

设置带宽限制

使用 “带宽”页面可设置端口的入口速率限制和出口整形速率，以确定系统可以接收和发送多少流量。

入口速率限制是指传入端口每秒能够接收的位数。超过此限制的带宽将被丢弃。

此功能要求交换机工作在 QoS 基本模式或 QoS 高级模式下。

设置带宽限制的步骤：

步骤 1 单击 “服务质量” > “一般” > “带宽”。

步骤 2 选择一个端口，然后单击 “编辑”。

步骤 3 设定以下参数：

- 接口 — 选择要限制带宽的端口。
- 入口速率限制 — 在此端口上启用或禁用入口速率限制功能。
- 入口速率限制 — 如启用入口速率限制功能，在此字段输入此端口所传入的最大带宽。
- 出口整形速率 — 在此端口上启用或禁用出口整形速率功能。
- 承诺的信息传输速率 **(CIR)**— 如启用出口整形速率功能，在此字段输入此端口可输出的最大带宽。

步骤 4 单击 “应用”。设置接口的带宽限制，并更新交换机的当前配置。

设置每队列出口整形

除限制每接口的传输速率 （在 “带宽”页面中完成）之外，交换机还可以在每队列每接口基础上，限制所选出口帧的传输速率。

交换机将限制除管理帧以外的所有帧。在速率计算中将忽略所有未限制的帧，表示其大小不包括在总限制之内。

每队列出口整形速率可被禁用。此功能要求交换机工作在 QoS 基本模式或 QoS 高级模式下。

设置每队列出口整形的步骤：

步骤 1 单击 “服务质量” > “一般” > “每队列出口整形”。

步骤 2 选择一个端口，然后单击 “编辑”。

步骤 3 设定以下参数：

- 接口 — 选择要设置的端口。
- 启用 — 在所选队列上启用或禁用出口整形功能。
- 承诺的信息传输速率 **(CIR)** — 如启用此功能，输入每队列所允许的最大带宽。CIR 是能够发送的平均最大数据量。

步骤 4 单击 “应用”。设置每队列出口整形功能，并更新交换机的当前配置。

设置 VLAN 入口速率限制

VLAN 入口速率限制可实现在 VLAN 上的流量限制。而 QoS 速率限制 （在 “策略表”页面中配置）的优先级高于 VLAN 入口速率限制。例如，如果数据包同时受到 QoS 速率限制和 VLAN 入口速率限制，且这两种速率限制发生了冲突，在这种情况下将优先使用 QoS 速率限制。

如果配置了 VLAN 入站速率限制，它将限制从交换机上的所有接口汇总的流量。

VLAN 入站速率限制功能在设备层面配置，而 QoS 速率限制将分别应用到网络中的每台设备。如果系统中存在多台设备，则配置的 VLAN 入站速率限制值将分别应用到这两台设备上。

VLAN 入口速率限制功能要求交换机工作在 QoS 基本模式或 QoS 高级模式下。

设置 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”。

步骤 2 单击 “添加”。

步骤 3 设定以下参数：

- **VLAN ID** — 选择要限制传入流量的 VLAN。
- 承诺的信息传输速率 **(CIR)**— 输入在此 VLAN 上所能接受的平均最大数据量。

步骤 4 单击 “应用”。添加 VLAN 入口速率限制规则，并更新交换机的当前配置。

设置 VLAN 端口入口速率限制

使用 “VLAN 端口入口速率限制”页面可限制某特定 VLAN 的所有端口的传入速率。 VLAN 端口入站速率限制可限制从交换机上特定端口上汇总的流量。

此功能要求交换机工作在 QoS 基本模式或 QoS 高级模式下。

同时启用带宽限制和 VLAN 端口入口速率限制功能时，速率限制值较小的设置生效。

限制 VLAN 端口入口速率的步骤：

步骤 1 单击 “服务质量” > “一般” > “**VLAN** 端口入口速率限制”。

步骤 2 单击 “添加”。

步骤 3 设定以下参数：

- **VLAN ID** — 选择要限制入站流量的 VLAN。
- 承诺的信息传输速率 **(CIR)** — 输入此 VLAN 上特定端口可接受的平均最大数据量。
- 接口 — 输入要限制入站流量的端口或端口范围。这些端口必须是所选 VLAN 的成员端口。

步骤 4 单击 “应用”。添加 VLAN 端口入口速率限制规则，并更新交换机的当前配置。

设置 TCP 拥塞避免算法

使用 “TCP 拥塞避免”页面可激活一个 TCP 拥塞避免算法。此算法可破除或避免拥塞节点 （拥塞由众多发送具有相同字节数的数据包的源引起）中的 TCP 全局同步。

设置 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 选择启用或禁用 TCP 拥塞避免算法。

步骤 3 单击 “应用”。

设置 QoS 基本模式

QoS 基本模式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输出队列。最初的数据包分类和对这些字段的标记是在信任域的传入流量中完成的。

要设置 QoS 基本模式，请执行以下操作：

步骤 1 将交换机的 QoS 工作模式设为基本模式。详见 “设置 **QoS** 属性”。

步骤 2 选择 QoS 信任模式。交换机支持 CoS/802.1p 信任模式、DSCP 信任模式、IP 优先权信任模式和 CoS/802.1p-DSCP 信任模式。详见 “设置基本 **QoS** 信任模式”。

步骤 3 如果出现有某接口不信任传入 CoS 标记的例外，则应在 “接口设置”页面禁用该接口的 QoS 功能。详见 “设置接口 **QoS** 功能”。

在 “接口设置”页面可针对端口启用或禁用所选的全局信任模式。如果某端口禁用信任模式，则此端口的所有传入数据包将被转发到尽力服务队列。如果某端口传入数据包的 CoS/802.1p 和 / 或 DSCP 值不值得信任，那么我们建议您禁用此端口的信任模式。否则，它可能会给您的网络性能带来负面影响。

设置基本 QoS 信任模式

“全局设置”页面可选择 QoS 基本模式下的全局信任模式。进入 QoS 域的数据包将在 QoS 域的边缘进行分类。

设置 QoS 基本模式下的信任模式的步骤：

步骤 1 单击 “服务质量” > “**QoS** 基本模式” > “全局设置”。

步骤 2 当交换机工作在 QoS 基本模式下，选择 QoS 信任模式。如果一个数据包的 CoS 优先级和 DSCP 标记被映射到不同的队列，那么信任模式将决定此数据包被分配给哪个队列。可选项如下：

- **CoS/802.1p** — 根据VLAN标签中的VPT字段或根据每端口的默认CoS/802.1p值 （如果传入数据包中没有 VLAN 标签）将流量映射到队列。其实际的 VPT 到队列映射可以在 “CoS/802.1p 到队列”页面中配置。
- **DSCP** — 根据 IP 报头中的 DSCP 字段将所有 IP 流量映射到队列。其实际的 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。

- **IP** 优先权 — 根据 IP 优先权将流量映射到队列。实际的 IP 优先权到队列映射可以在 “IP 优先权到队列” 页面中配置。
- **CoS/802.1p-DSCP** — 为所有非IP流量使用信任CoS模式；为所有IP数据流量使用信任 DSCP 模式。

步骤 3 单击 “应用”。设置 QoS 基本模式的信任模式，并更新交换机的当前配置。

设置接口 QoS 功能

“接口配置” 页面可在交换机的每个接口上启用或禁用 QoS。

- **QoS** 状态已禁用 — 接口的所有传入流量将被映射到尽力服务队列，且不会对流量进行分类或优化。
- **QoS** 状态已启用 — 接口将根据系统全局设定的信任模式，优化传入流量。

启用或禁用接口的 QoS 功能的步骤：

步骤 1 单击 “服务质量” > “**QoS** 基本模式” > “接口设置”。

步骤 2 选择接口类型 （端口或 LAG），单击 “确定”。

步骤 3 选择一个接口并单击 “编辑”。

步骤 4 设定以下参数：

- 接口 — 选择要设置的端口或 LAG。
- **QoS** 状态 — 在该接口上启用或禁用 QoS 功能。

步骤 5 单击 “应用”。启用或禁用接口的 QoS 功能，并更新交换机的当前配置。

设置 QoS 高级模式

与 ACL 匹配并被允许进入的帧将使用允许其进入的 ACL 名称进行隐式标记。系统将应用 QoS 高级模式中定义的操作到这些数据流。

在 QoS 高级模式中，交换机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 QoS 策略包含一个或多个类映射。

- 类映射通过一个或多个关联的 ACL 来定义数据流。只有符合带许可 （转发）操作的类映射中的 ACL 规则 （ACE）的数据包才能被被视为属于同一个数据流，并遵循相同的服务质量。因此， QoS 策略包含了一个或多个数据流，且每个数据流都有一个用户定义的 QoS。
- 类映射的 QoS 由关联的策略器强制执行。交换机支持单策略器和集合策略器。每种策略器都设置有一个 QoS 规格。单策略器可将 QoS 应用到单个类映射，从而应用到单个数据流。而集合策略器将 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。
- 通过将策略绑定至特定端口可将每数据流 QoS 应用到数据流。一个策略及其类映射可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。

设置 QoS 高级模式时，请注意以下事项：

- 不论策略为何，都可以将一个 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。
- 当使用单策略器的类映射被绑定至多个端口时，每个端口都有其自己的单策略器实例。每个实例在相互独立的端口上分别对该类映射应用 QoS。
- 不论策略和端口为何，集合策略器会将 QoS 应用到集合的所有数据流上。

QoS 高级模式设置由三部分组成：

- 要匹配的规则。与单组规则匹配的所有帧将被视为一个数据流。
- 要每个数据流中匹配规则的所有帧所采取的操作。
- 将规则和操作的组合绑定至一个或多个端口。

因此，请执行以下步骤置 QoS 高级模式：

步骤 1 使用 “QoS 属性”页面将交换机的 QoS 工作模式设置为高级模式。详见 “设置 QoS 属性”。

步骤 2 使用 “全局设置”页面选择 QoS 高级模式下的全局信任模式。详见 “设置高级 QoS 信任模式”。

步骤 3 按 “创建 ACL 工作流程”中所述创建 ACL。

步骤 4 如果定义了 ACL，使用 “类映射”页面创建类映射并将 ACL 与创建的类映射相关联。详见 “设置类映射”。

步骤 5 使用 “策略表”页面创建策略。详见 “设置 QoS 策略”。

步骤 6 使用 “策略类映射”页面将策略与一个或多个类映射相关联。详见 “设置策略类映射”。

步骤 7 如有必要，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 “策略类映射”页面和 “类映射”页面创建一个策略，将类映射与单策略器进行关联。
- 集合策略器 — 首先使用 “集合策略器”页面针对每个数据流创建一个 QoS 操作 （即将所有匹配的帧发送到同一个策略器，详见 “设置集合策略器”），然后使用 “策略类映射”页面创建一个策略，将类映射与此集合策略器进行关联。

步骤 8 使用 “策略绑定”页面将策略绑定至端口。详见 “设置策略绑定”。

设置高级 QoS 信任模式

使用 “全局设置”页面可设置 QoS 高级模式下的信任模式和默认信任状态。

设置 QoS 高级模式下的信任模式的步骤：

步骤 1 单击 “服务质量” > “**QoS** 高级模式” > “全局设置”。

步骤 2 设定以下参数：

- 信任模式 — 选择QoS高级模式下的信任模式。如果一个数据包的CoS优先级和 DSCP 标记被映射到不同的队列，那么信任模式将决定此数据包分配给哪个队列。可选项如下：
  - *CoS/802.1p* — 根据 VLAN 标签中的 VPT 字段或每端口默认的 CoS/802.1p 值 （如果传入数据包中没有 VLAN 标签）将流量映射到队列。实际的 CoS/802.1p 到队列映射可以在 “CoS/802.1p 到队列”页面中配置。
  - *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。
  - *IP* 优先权 — 根据 IP 优先权将流量映射到队列。实际的 IP 优先权到队列映射可以在 “IP 优先权到队列”页面中配置。
  - *CoS/802.1p-DSCP* — 非 IP 流量将使用信任 CoS 模式，而 IP 流量将使用 DSCP 信任模式。
- 默认信任状态 — 选择所有端口上默认的信任模式 （信任或不信任）。默认信任状态可在高级 QoS 模式下提供最基本的 QoS 功能，因此您在 QoS 高级模式下默认信任 CoS/DSCP，而无需创建一个策略。

在 QoS 高级模式下，如果默认信任状态被设为不信任，那么接口上设置的默认 QoS 值可能被用来优化到达此接口的流量。

如果在接口上设置有一个 QoS 策略且默认模式不相关，那么将根据 QoS 策略设置来采取相应的操作，且任何不匹配的流量会被丢弃。

步骤 3 单击 “应用”。设置 QoS 高级模式的信任模式，并更新交换机的当前配置。

设置类映射

类映射使用 ACL 定义数据流。基于 MAC 的 ACL、基于 IPv4 的 ACL 和基于 IPv6 的 ACL 都可以绑定到一个类映射。类映射被设置为匹配数据包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。

注释 设置类映射不会对 QoS 产生任何影响。这是一个过渡性步骤，其目的是为了使得类映射在稍后被使用。

如果需要更复杂的规则集合，可以将多个类映射分组为一个超级组，该组称为策略。详见 “设置 QoS 策略”。

设置类映射的步骤：

步骤 1 单击 “服务质量” > “QoS 高级模式” > “类映射”。

步骤 2 单击 “添加”，添加一个类映射。

步骤 3 设定以下参数：

- 类映射名称 — 输入类映射的名称。
- 匹配 **ACL** 类型 — 为了将数据包划分到此类映射中定义的数据流中，选择数据包必须匹配的规则，即与 ACL 匹配的数据包将视为同一个数据流。可选项如下：
  - *IP* — 数据包必须与类映射中定义的基于IPv4的ACL或基于IPv6的ACL相匹配。
  - *MAC* — 数据包必须与类映射中定义的基于 MAC 的 ACL 相匹配。
  - *MAC or IP*— 数据包必须与类映射中定义的基于IP的ACL或基于MAC的ACL相匹配。
- **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**— 选择数据包先与基于 IP 的 ACL 还是基于 MAC 的 ACL 进行匹配。

步骤 4 单击 “应用”。添加类映射，并更新交换机的当前配置。

QoS 策略

您可以测量与一组预先设定的规则相匹配的流量的速率并强制执行速率限制，例如限制某端口的文件传输的速率。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。

一个策略设置有一个 QoS 规范。交换机支持两种类型的策略器：

- 单策略器 — 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，每个端口都具有其各自的单策略器实例。每个实例在相互独立的端口上对该类映射应用 QoS。单策略器在 “策略类映射”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。集合策略器可支持来自不同策略的类映射。不管策略和端口为何，集合策略器会将 QoS 应用到其汇总的所有数据流上。集合策略器可在 “策略类映射”页面创建。

每一个策略器都定义有各自的 QoS 规范且包含以下参数：

- 允许的最大速率，称为承诺信息速率 （CIR），单位为 kbps。
- 对超出限制的帧 （称为超出预约带宽的流量）采取的操作。这些帧可以继续传输或被丢弃。

将一个类映射添加到一个策略可实现将一个策略器指定给一个类映射。如果此策略器是一个集合策略器，那么您必须先在 “集合策略器”页面创建此策略器。

设置集合策略器

一个集合策略器将 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。一个集合策略器可支持来自不同策略的类映射。不管策略和端口为何，集合策略器将 QoS 应用到其汇总的所有数据流。

设置集合策略器的步骤：

步骤 1 单击 “服务质量” > “**QoS** 高级模式” > “集合策略器”。

步骤 2 单击 “添加”。

步骤 3 设定以下参数：

- 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)** — 输入所允许的最大带宽，单位为千位 / 秒。
- 超出操作 — 选择要对超出 CIR 的传入数据包执行的操作。可选项如下：
  - *转发* — 转发超出 CIR 值的数据包。
  - *丢弃* — 丢弃超出 CIR 值的数据包。

步骤 4 单击 “应用”。添加集合策略器，并更新交换机当前配置。

设置 QoS 策略

使用 “策略表”页面可设置 QoS 策略。只有绑定到接口的策略才有效 （详见 “设置策略绑定”）。

每一个策略有以下部分组成：

- 一个或多个 ACL 类映射 （在策略中定义数据流）
- 一个或多个集合 （将 QoS 应用到策略中定义的数据流）

添加策略后，在 “策略类映射”页面将类映射关联到此策略。

设置 QoS 策略的步骤：

步骤 1 单击 “服务质量” > “**QoS** 高级模式” > “策略表”。

步骤 2 单击 “添加”。

步骤 3 在 “新策略名称”字段中输入策略名称。

步骤 4 单击 “应用”。添加 QoS 策略，并更新交换机的当前配置。

步骤 5 单击 “策略类映射表”，转到 “策略类映射”页面查看或设置策略类映射。

设置策略类映射

可以在一个策略中添加一个或多个类映射。策略类映射定义属于同一个数据流的数据包的类型。

在策略中添加类映射的步骤：

步骤 1 单击 “服务质量” > “**QoS** 高级模式” > “策略类映射”。

步骤 2 选择一个 QoS 策略，然后单击 “确定”。显示关联到此策略的所有类映射。

步骤 3 单击 “添加”，添加策略类映射。

步骤 4 设定以下参数：

- 策略名称 — 显示要添加类映射的策略。
- 类映射名称 — 选择要与该策略关联的类映射。
- 操作类型 — 根据所有匹配的数据包的入口CoS/802.1p值和/或DSCP值选择如下操作：
  - *使用默认信任模式*— 忽略入口CoS/802.1p和/或DSCP值。所有匹配的数据包将转发至尽力服务队列。
  - *始终信任* — 交换机将始终信任匹配数据包的 CoS/802.1p 和 DSCP 值。如果为 IP 数据包，交换机会根据数据包的 DSCP 值及 DSCP 到队列映射关系将数据包发送至输出队列。否则，将根据数据包的 CoS/802.1p 值及 CoS/802.1p 到队列映射关系将数据包发送至输出队列。
  - *设置* — 手动设置所有匹配数据包的输出队列。如选择此选项，从下拉框中选择 “队列” 并输入队列编号。
- 监察类型 — 选择此策略的策略器类型。可选项如下：
  - *无* — 不使用任何策略。
  - *单个* — 策略器为单策略器。
  - *集合* — 策略器为集合策略器。
- 集合策略器 — 如果监察类型为 “集合”，选择一个预先定义的集合策略器。
- 入口承诺的信息传输速率 **(CIR)** — 如果监察类型为 “单个”，输入所允许的最大带宽。
- 超出操作 — 选择对超出 CIR 的传入数据包执行何种操作。可选项如下：
  - *无* — 不采取任何操作。

- *丢弃* — 丢弃超出 CIR 值的数据包。

步骤 5 单击 “应用”。添加策略类映射，并更新交换机的当前配置。

设置策略绑定

使用 “策略绑定”页面将策略绑定到特定接口。如果一个策略被绑定到某一接口，则该策略仅在此接口有效。一个接口只能配置一个策略，但一个策略可以绑定至多个接口。

将策略绑定至接口后，该策略会过滤传入流量并应用 QoS 到属于此策略定义的数据流的传入流量。此策略不会应用到同一接口的输出流量。

注释 如需编辑一个策略，必须先将它从所绑定的所有接口中移除，即解除其接口绑定关系。

设置策略绑定的步骤：

步骤 1 单击 “服务质量” > “**QoS** 高级模式” > “策略绑定”。

步骤 2 选择一个策略和接口类型 （端口或 LAG），单击 “确定”。

步骤 3 勾选此策略要绑定的接口。

步骤 4 单击 “应用”。将策略绑定到接口，并更新交换机的当前配置。

步骤 5 单击 “显示每个端口的策略绑定”，在单个页面显示每个端口绑定的策略详细信息。

步骤 6 单击 “上一步”，返回到 “策略绑定”页面。

19

设置 SNMP

本章介绍如何设置提供管理网络设备方法的简单网络管理协议 （Simple Network Management Protocol， SNMP），包括以下内容：

- SNMP 版本和工作流程
- 支持的 MIB
- 对象 ID
- 设置 SNMP 引擎 ID
- 设置 SNMP 视图
- 设置 SNMP 组
- 设置 SNMP 用户
- 设置 SNMP 社团
- 设置 SNMP 通知接收设备

SNMP 版本和工作流程

思科 220 交换机可作为 SNMP 代理，并且支持 SNMP v1、 v2 和 v3。思科 220 交换机还可以使用其支持的管理信息库 （Management Information Base， MIB）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，系统会定义一系列 SNMP 社团。每个 SNMP 社团由一个社团字符串及其访问权限组成。系统只对包含正确的许可权限和操作的社团的 SNMP 消息作出响应。

SNMP 代理会维护用于管理交换机的变量列表。这些变量在 MIB 中定义。 MIB 中包含由代理控制的变量。请参考 “支持的 MIB”一节查看所有交换机支持的 MIB 信息。

注释 SNMPv2 协议具有已知的安全性漏洞，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 Trap 机制应用到 SNMPv1 和 SNMPv2 PDU。 SNMPv3 还可定义一个用户安全模式 （User Security Model，USM），该模式包括：

- 认证 — 提供数据完整性和数据源验证。
- 隐私 — 防止消息内容泄露。使用密码块链接技术 （Cipher Block-Chaining，CBC）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。
- 时间性 — 防止消息延迟或反演攻击。SNMP 代理会比较传入消息的时间戳与消息的到达时间。
- 密钥管理 — 定义密钥生成、密钥更新和密钥使用。交换机支持基于对象 ID （Object ID，OID）的 SNMP 通知过滤器。交换机使用对象 ID 来管理设备的功能。

SNMP 工作流程

出于安全考虑，默认情况下交换机禁用 SNMP 服务。在通过 SNMP 设置交换机之前，请先在交换机上启用 SNMP 服务 （详见 “设置 TCP/UDP 服务”）。

如果决定使用 SNMPv1 或 v2，请执行以下操作：

步骤 1 如有必要，设置 SNMP 视图。详见 “设置 SNMP 视图”。

步骤 2 设置 SNMP 组，并将 SNMP 视图绑定到 SNMP 组。详见 “设置 SNMP 组”。

步骤 3 设置 SNMP 社团。可以将 SNMP 社团与访问权限和 SNMP 视图相关联 （在基本模式下），也可以将其与 SNMP 组相关联 （在高级模式下）。详见 “设置 SNMP 社团”。

- 基本模式 — 可以将 SNMP 社团的访问权限设置为只读或读写。此外，还可以将 SNMP 社团的访问权限限制为只能通过视图访问特定的 MIB 对象。
- 高级模式 — SNMP 社团的访问权限由 SNMP 组来定义。可以使用特定的安全模式来设置 SNMP 组。 SNMP 组的访问权限包括读取、写入和通知。

步骤 4 设置 SNMPv1,2 通知接收器。详见 “设置 SNMPv1,2 通知接收设备”。

如果决定使用 SNMPv3，请执行以下操作：

步骤 1 设置 SNMP 引擎 ID。您既可以创建一个新的 SNMP 引擎 ID，也可以选择使用默认引擎 ID。详见 “设置 SNMP 引擎 ID”。

步骤 2 如有必要，设置 SNMP 视图。 SNMP 视图可限定在 SNMP 社团或 SNMP 组上可用的对象 ID。详见 “设置 SNMP 视图”。

步骤 3 设置 SNMP 组，并将 SNMP 视图绑定到 SNMP 组。详见 “设置 SNMP 组”。

步骤 4 设置 SNMP 用户，并将 SNMP 用户与 SNMP 组相关联。详见 “设置 SNMP 用户”。

步骤 5 设置 SNMPv3 通知接收器。详见 “设置 SNMPv3 通知接收设备”。

支持的 MIB

思科 220 交换机支持以下 MIB：

- RFC1213 MIB-II
- RFC1215 Generic-Traps MIB
- RFC1493 (4188) Bridge MIB
- RFC2618 RADIUS Client MIB
- RFC2674 Bridge MIB Extension
- RFC2737 Entity MIB
- RFC2819 RMON
- RFC2863 The Interface Group MIB
- RFC3164 Syslog MIB
- RFC3621 PoE MIB (仅适用于支持 PoE 功能的交换机型号)
- RFC3635 EtherLike MIB
- SNMP-COMMUNITY MIB
- SNMP-MIB
- LLDP-MIB

- LLDP-EXT-MED-MIB
- IEEE802.3 Annex 30C MIB
- CISCO-CDP-MIB
- CISCO-ENVMON-MIB
- CISCO-PORT-SECURITY-MIB
- CISCO-IMAGE-MIB

对象 ID

下别列出了不同交换机型号的对象 ID：

交换机型号	OID
SF220-24	1.3.6.1.4.1.9.6.1.84.24.1
SF220-24P	1.3.6.1.4.1.9.6.1.84.24.2
SF220-48	1.3.6.1.4.1.9.6.1.84.48.1
SF220-48	1.3.6.1.4.1.9.6.1.84.48.2
SG220-26	1.3.6.1.4.1.9.6.1.84.26.1
SG220-26P	1.3.6.1.4.1.9.6.1.84.26.2
SG220-50	1.3.6.1.4.1.9.6.1.84.50.1
SG220-50P	1.3.6.1.4.1.9.6.1.84.50.2
SG220-28	1.3.6.1.4.1.9.6.1.84.28.5
SG220-28MP	1.3.6.1.4.1.9.6.1.84.28.3
SG220-52	1.3.6.1.4.1.9.6.1.84.52.5

设置 SNMP 引擎 ID

SNMP 引擎 ID 仅由 SNMPv3 实体用来唯一标识其自身。 SNMP 代理被视为权威 SNMP 引擎。也就是说， SNMP 代理会响应传入消息 （Get、 GetNext， GetBulk 和 Set）并发送 Trap 消息给一个管理员。

每一个 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。 SNMP 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。

本地信息一般存储在四个只读的 MIB 变量 （snmpEngineId、 snmpEngineBoots、snmpEngineTime 和 snmpEngineMaxMessageSize）中。

设置 SNMP 引擎 ID 的步骤：

步骤 1 单击 “**SNMP**” > “引擎 **ID**”。

步骤 2 在 “本地引擎 **ID**”字段，设置本地引擎 ID：

- 使用默认设置 — 选择此选项，将使用设备生成的引擎 ID。默认的引擎 ID 以交换机 MAC 地址为基础，并且根据以下标准进行定义：
  - *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，表示随后的 MAC 地址。
  - *后 6 个八位字节* — 交换机的 MAC 地址。
- 用户定义 — 选择此选项，手动输入本地设备引擎 ID。此字段是一个十六进制字符串 （范围为 10 到 64 个字符）。十六进制字符串的每个字节都由两个十六进制数字表示。

步骤 3 单击 “应用”。设置本地设备引擎 ID，并更新交换机的当前配置。

步骤 4 “远程引擎 **ID** 表”列出了交换机支持的所有远程引擎 ID。单击 “添加”，添加一个远程引擎 ID。

步骤 5 设定以下参数：

- 服务器定义 — 选择按 IP 地址还是按名称来定义远程服务器。
- **IP** 版本 — 选择支持的 IP 格式。
- 服务器 **IP** 地址 / 名称 — 输入接收 Trap 的远程服务器的 IP 地址或域名。
- 引擎 **ID** — 输入远程 SNMP 引擎 ID。

步骤 6 单击 “应用”。添加远程引擎 ID，并更新交换机的当前配置。

设置 SNMP 视图

SNMP 视图是 MIB 树的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 定义。您既可以使用已知名称来指定所需子树的根节点，也可以输入对象 ID。

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”页面可设置 SNMP 视图。默认视图不能被修改。在 “组”页面可将视图绑定到 SNMP 组，或者在 “社团”页面将视图绑定到使用基本访问模式的 SNMP 社团。

设置 SNMP 视图的步骤：

步骤 1 单击 “**SNMP**” > “视图”。

步骤 2 单击 “添加”，添加一个 SNMP 视图。

步骤 3 设定以下参数：

- 视图名称 — 输入 SNMP 视图名称。
- 对象**ID**子树 — 定义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。此节点的子节点会全部包括在该视图中或排除在该视图之外。
  - *从列表中选择* — 从列表中选择一个已定义好的对象 ID。
  - *用户定义的* — 手动输入列表中未提供的对象 ID。
- 包含在视图中 — 勾选此选项，将输入的对象 ID 子树包括在视图中。取消勾选此选项，将输入的对象 ID 子树排除在视图之外。

步骤 4 单击 “应用”。添加 SNMP 视图，并更新交换机的当前配置。

设置 SNMP 组

在 SNMPv1 和 SNMPv2 中，一个社团字符串会随 SNMP 帧一起发送。社团字符串将作为访问 SNMP 代理的密码。但是，帧和社团字符串均未加密。因此 SNMPv1 和 SNMPv2 不安全。

在 SNMPv3 中，可以配置以下两种安全性机制：

- 验证 — 交换机会检查 SNMP 用户是否为已授权的系统管理员。该验证会分别针对每个帧进行。
- 隐私 — SNMP 帧可以传输加密数据。

SNMPv3 可提供三个安全性级别：

- 无验证 （不验证且无隐私）
- 验证 （验证但无隐私）
- 验证和隐私 （指定的 SNMP 组的安全等级须为隐私）

SNMPv3 通过将 SNMP 用户与 SNMP 组关联的方式，控制获得授权和经过验证的 SNMP 用户可以读取和写入的内容以及他们可以收到哪些通知。 SNMP 组可定义读取和写入权限以及安全级别，但仅在与 SNMP 用户或 SNMP 社团关联时才起作用。

注释 如需将非默认 SNMP 视图关联到 SNMP 组，首先必须在 “视图”页面创建此视图。

创建 SNMP 组的步骤：

步骤 1 单击 “**SNMP**” > “组”。

步骤 2 单击 “添加”，添加一个 SNMP 组。

步骤 3 设定以下参数：

- 组名称 — 输入 SNMP 组的名称。
- 安全模式 — 选择要应用到该组的 SNMP 版本 （SNMPv1、 SNMPv2 或 SNMPv3）。

您可以为 SNMP 组定义三种拥有不同安全性级别的 SNMP 视图。针对每一种安全性级别，通过设定以下参数来分别指定其读取、写入和通知视图：

- 启用 — 勾选此选项，启用相应的安全性级别。安全性级别仅适用于 SNMPv3。
- 安全等级 — 勾选 “启用”将选中的安全等级应用此 SNMP 组。 SNMPv1 和 SNMPv2 既不支持验证也不支持隐私。因此，如果安全模式为 SNMPv3，您需要选择以下任意选项：

- *不验证且无隐私* — 既不为组指定 “验证”安全性级别，也不为其指定 “隐私”安全性级别。
- *验证且无隐私* — 验证 SNMP 消息，并确保 SNMP 消息源经过验证，但不对消息加密，表示消息可以拦截和读取。
- *验证和隐私* — 验证 SNMP 消息，并确保 SNMP 消息源经过验证，同时加密 SNMP 消息。

▪ 视图 — 分别为读取、写入和通知等访问权限选择一个预先定义好的 SNMP 视图。将 SNMP 视图关联到 SNMP 组的读取、写入和通知访问权限可以限制该 SNMP 组拥有读取、写入和通知访问权限的 MIB 树的范围。

- *读取* — 所选视图的管理访问权限为只读。在创建 SNMP 组时必须指定一个读取视图。
- *写入* — 所选视图的管理访问权限为可写。如不设定写入视图，则与该组关联的 SNMP 用户或 SNMP 社团将能够写入除控制 SNMP 本身的 MIB 之外的所有 MIB。
- *通知* — 仅接收包含通知选择的 SNMP 视图内容的 Trap。如不设定通知视图，将不对 Trap 内容进行限制。通常不需要为 SNMP 组选择通知视图。

步骤 4 单击 “应用”。设置 SNMP 组，并更新交换机的当前配置。

设置 SNMP 用户

SNMP 用户由登录凭证 （用户名、密码和认证方法）及其工作 （通过与 SNMP 组合引擎 ID 关联实现）的环境和范围来定义。

SNMP 用户具有其 SNMP 组的属性，并具有在关联的视图中设置的访问权限。

SNMP 组使得网络管理员可以将访问权限授权给整组用户而非单个用户。一个 SNMP 用户只能成为一个 SNMP 组的成员。

创建一个 SNMPv3 用户前，必须在 “组”页面先创建一个 SNMPv3 组。

设置 SNMP 用户的步骤：

步骤 1 单击 “**SNMP**” > “用户”。

步骤 2 单击 “添加”，添加一个 SNMP 用户。

步骤 3 设定以下参数：

- 用户名 — 输入 SNMP 用户的名称。
- 组名称 — 选择该 SNMP 用户所属的 SNMP 组。

  注　　如选择一个已经删除的 SNMP 组，那么关联到此组的用户仍然会保留，但这些 SNMP 用户不可用。
- 验证方法 — 选择验证 SNMP 用户的方法。可选项如下：
  - *无* — 不验证 SNMP 用户。
  - *MD5* — 使用 MD5 密码或密钥进行验证。
  - *SHA* — 使用 SHA （安全散列算法）密码或密钥进行验证。
- 验证密码 — 选择 “加密模式”输入一个加密的验证密码，或选择 “明文模式”以明文的形式输入验证密码。验证密码用于根据 MD5 或 SHA 验证算法生成一个密钥。
- 隐私方法 — 选择 “无”或 “DES”作为隐私方法。
- 隐私密码 — 选择 “加密模式”输入一个加密的隐私密码，或选择 “明文模式”以明文的形式输入隐私密码。隐私密码用于根据 DES 方法生成一个密钥。

步骤 4　单击 “应用”。添加 SNMP 用户，并更新交换机的当前配置。

设置 SNMP 社团

SNMPv1 和 SNMPv2 的访问权限由在 “社团”页面定义 SNMP 社团进行管理。社团字符串是在 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 面向用户而非社团，因此社团只能在 SNMPv1 和 SNMPv2 中定义。SNMP 用户属于具有访问权限的 SNMP 组。

使用 “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 SNMP 组进行关联 （高级模式）。

- 基本模式 — 社团的访问权限可以设定为只读或读写。此外，还可以将社团的访问权限限制为只能通过所选视图访问特定的 MIB 对象。
- 高级模式 — 社团的访问权限由 SNMP 组来定义。可以使用特定的安全等级来设置 SNMP 组。 SNMP 组的访问权限为读取、写入和通知。

设置 SNMP 社团的步骤：

步骤 1 单击 “**SNMP**” > “社团”。

步骤 2 单击 “添加”，添加一个 SNMP 社团。

步骤 3 设定以下参数：

- 社团字符串 — 输入用于验证设备管理站点的社团名称 （密码）。
- 基本 — 在基本模式下，不存在到任何 SNMP 组的连接。您可以选择社团的访问级别 （“只读”、“读写”或 “SNMP 管理”），或者进一步授予社团对特定视图的访问权限。默认情况下，基本模式会应用到整个 MIB。如果选择基本模式，设定以下字段：
  - *访问模式* — 选择社团的访问权限。可选项如下：

    只读 — 将管理访问权限限制为只读。不能更改社团。

    读写 — 管理访问权限为可读写。可以对设备配置进行更改，但不能更改社团。

    SNMP 管理 — 管理访问权限为可读写。可以对设备的所有配置进行更改，因此其相应的读写视图为 “all”，即全部。
  - 视图名称 — 选择社团关联的 SNMP 视图（要授予其访问权限的 MIB 子树集合）。
- 高级 — 高级模式下，社团的访问权限由 SNMP 组来定义。选择此模式，您需要从下拉框中选择一个用来确定访问权限的 SNMP 组。

步骤 4 单击 “应用”。添加 SNMP 社团，并更新交换机的当前配置。

设置 SNMP 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）是接收交换机发送的 Trap 消息的网络节点。系统会定义一系列 Trap 接收器作为 Trap 消息的接收设备。每个 Trap 接收器中包含的节点 IP 地址和 SNMP 凭证与 Trap 消息中将要包括的节点 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 “通知接收方表”上所列的每个节点。

使用 “通知接收设备 SNMPv1,2”和 “通知接收设备 SNMPv3”页面可设置 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）。

SNMP 通知是指交换机向 SNMP 管理站点发送的消息。在其中说明发了某个事件，例如链路连接或中断。

设置 SNMPv1,2 通知接收设备

设置 SNMPv1,2 通知接收设备的步骤：

步骤 1 单击 “**SNMP**” > “通知接收设备 **SNMPv1,2**”。

步骤 2 单击 “添加”，添加一个 SNMPv1,2 通知接收设备。

步骤 3 设定以下参数：

- 服务器定义 — 选择按 IP 地址或按名称来定义通知接收设备。
- **IP** 版本 — 选择支持的 IP 格式。
- 接收方 **IP** 地址 / 名称 — 输入通知接收设备的 IP 地址或主机名。
- **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 还是发送通知给接收设备。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 Trap 或通知之前交换机等待的时间（以秒为单位）。默认为 15 秒。
- 重试次数 — 输入重新发送通知请求的次数。默认为 3。
- 社团字符串 — 选择 Trap 管理器的 SNMP 社团。
- 通知版本 — 选择 Trap 的 SNMP 版本。SNMPv1 和 SNMPv2 均可作为 Trap 版本使用，但一个时刻只能启用一个版本。

步骤 4 单击 “应用”。添加 SNMPv1,2 通知接收设备，并更新交换机的当前配置。

设置 SNMPv3 通知接收设备

设置 SNMPv3 通知接收设备的步骤：

步骤 1 单击 “**SNMP**” > “通知接收设备 **SNMPv3**”。

步骤 2 单击 “添加”，添加一个 SNMPv3 通知接收设备。

步骤 3 设定以下参数：

- 服务器定义 — 选择按 IP 地址或按名称来定义通知接收设备。
- **IP** 版本 — 选择支持的 IP 格式。
- 接收方 **IP** 地址 / 名称 — 输入通知接收设备的 IP 地址或主机名称。
- **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 还是发送通知给接收设备。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 Trap 或通知之前交换机等待的时间（以秒为单位）。默认为 15 秒。
- 重试次数 — 输入设备重新发送通知请求的次数。默认为 3。
- 用户名 — 选择接收 SNMP 通知的用户。要接收 SNMP 通知，必须在 “用户” 页面定义此用户，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。可选项如下：
  - *不验证* — 表示既不对数据包进行验证，也不对其加密。
  - *验证* — 表示对数据包进行验证，但不对其加密。
  - *隐私* — 表示既要对数据包进行验证，又要对其加密。

  注　安全等级取决于选择的用户名。如果选择的用户被设定为*无验证*，那么此处的安全等级将设为*不验证*。但是，如果选择的用户被设定为*验证且隐私*，那么此处的安全等级可以设为*不验证*、*验证*或者*隐私*。

步骤 4 单击 “应用”。添加 SNMPv3 通知接收设备，并更新交换机的当前配置。

A

快速索引

思科为您提供了丰富完整的文档资料，帮助您和您的客户获取关于思科 220 系列智能增强型交换机的完整信息。

资源	地址
思科 220 交换机主页	www.cisco.com/go/cn/220switches
思科客户支持中心	www.cisco.com/web/CN/smallbusiness
思科产品渠道合作伙伴中心（需登录）	www.cisco.com/web/CN/partners/smb_kr/index.html
软件下载	www.cisco.com/web/CN/solutions/industry/segment_sol/small/index.html#small_down
思科开放源许可通知	www.cisco.com/go/cn/220switches
思科产品兼容性和安全提示	www.cisco.com/go/cn/220switches
思科产品保修条款	www.cisco.com/web/CN/solutions/industry/segment_sol/small/index.html#~service
思科产品服务热线	8008888168 （固定电话） 4006282616 （移动电话）