

管理型交换机 用户手册 **Version 0.0.1**

2022年5月

支持

感谢您选择万兆交换机(L2+)产品。

请与您的服务提供商联系以获得技术支持

修订历史

出版发布编号	发布日期	备注
2022-0528-01	2022年5月	第一次发布

目录

1. 开始	8
1.1. 理解用户界面	10
1.2. Web管理界面概述	11
1.3. 使用Web浏览器访问交换机并登录	11
1.4. 使用 SNMP	14
2. 系统管理	16
2.1. 基本管理	17
2.1.1. 系统信息管理	17
2.1.2. 硬件模块信息	19
2.1.3. 设备信息及状态	20
2.1.4. 交换机计数统计	20
2.1.5. CPU系统资源	22
2.1.6. 网络接口管理	24
2.1.7. 时间	26
2.2. 内置服务	35
2.2.1. DHCP 服务器	35
2.2.2. DHCP L2中继代理	42
2.2.3. IP Relay Agent	44
2.2.4. DHCPv6 Server	48
2.2.5. DHCPv6 Relay	54
2.3. DNS	55
2.3.1. DNS客户端配置	55
2.3.2. 主机名称配置	56
2.4. SNMP管理	57
2.4.1. SNMP V1/V2	57
2.4.2. SNMP V3	58
2.4.3. Trap消息配置	59
2.4.4. MIBS支持列表	61
2.5. LLDP管理	62
2.5.1. 全局配置	62
2.5.2. 端口配置	63
2.5.3. LLDP报文统计	64
2.5.4. 本地设备信息	65
2.5.5. LLDP远端设备信息	66
2.5.6. LLDP远端设备信息	67
2.5.7. LLDP-MED	68
2.6. POE	73
2.7. ISDP管理	76
2.7.1. 基本管理	76
2.7.2. 高级管理信息	77
2.8. 定时计划管理	80

3. L2交换机管理	82
3.1. 端口管理	83
3.1.1. 端口物理连接配置	83
3.1.2. 配置端口描述	84
3.2. 链接聚合组	85
3.2.1. 配置LAG设置	85
3.2.2. LACP	89
3.3. 配置 VLAN	90
3.3.1. 配置基本VLAN设置	91
3.3.2. 配置高级VLAN	92
3.3.3. 协议VLAN	100
3.3.4. 802.1Q双标记	104
3.3.5. 配置语音VLAN	105
3.4. MAC 地址表	106
3.4.1. 配置MAC地址表	106
3.4.2. 设置动态地址老化间隔	107
3.4.3. 配置静态MAC地址	107
3.5. 生成树协议	108
3.5.1. 配置基本STP设置	108
3.5.2. 配置高级STP设置	110
3.5.3. 配置CST设置	112
3.5.4. 配置CST端口设置	114
3.5.5. 查看CST端口状态	116
3.5.6. 配置MST设置	118
3.5.7. 查看生成树MST端口状态	119
3.5.8. 查看STP统计信息	121
3.6. 组播	123
3.6.1. 查看MFDB表	123
3.6.2. 查看MFDB统计信息	123
3.6.3. IGMP Snooping	124
3.6.4. 配置 MLD Snooping	132
3.7. MVR	137
3.7.1. 配置基本MVR设置	137
3.7.2. 配置高级MVR设置	138
3.7.3. 配置MVR组	139
3.7.4. 配置MVR接口	140
3.7.5. 配置MVR组成员	141
3.7.6. 查看MVR统计信息	141
3.8. Auto-VoIP	142
3.8.1. 配置基于协议的端口设置	143
3.8.2. 配置 Auto-VoIP 基于OUI-Based 的属性	143
3.8.3. 基于OUI的端口设置	144
3.8.4. 配置OUI表	145
3.8.5. 查看 Auto-VoIP 状态	146
3.9. UDLD管理	146
3.9.1. 系统配置	146

3.9.2. 端口配置	147
3.10. 环路保护	148
3.11. ERPS	150
4. QoS管理	152
4.1. CoS管理	152
4.1.1. 基本管理	152
4.1.2. 802.1p 优先级映射表	153
4.1.3. DSCP 优先级映射表	154
4.1.4. 端口队列配置	155
4.1.5. Configure CoS Drop Precedence Settings	156
4.2. 差分服务质量管理	159
4.2.1. 差分服务质量管理	159
4.2.2. 高级管理	159
4.3. 接口带宽管理	163
5. 设备安全管理	165
5.1. 管理安全设置	166
5.1.1. 配置用户	166
5.1.2. 添加新用户	167
5.1.3. 配置用户密码设定参数	168
5.1.4. 配置特权密码	169
5.1.5. 配置线路密码	170
5.1.6. RADIUS 概述	171
5.1.7. 配置全局RADIUS服务器设置	172
5.1.8. 配置RADIUS服务器	173
5.1.9. 配置RADIUS记帐服务器	175
5.2. TACACS 概述	177
5.2.1. 配置全局TACACS设置	177
5.2.2. 配置TACACS服务器设置	178
5.2.3. 配置登录身份验证列表	179
5.2.4. 配置启用特权身份验证列表	181
5.2.5. 配置Dot1x身份验证列表	182
5.2.6. 配置HTTP身份验证列表	183
5.2.7. 配置HTTPS身份验证列表	184
5.2.8. 查看登录会话	185
5.3. 配置管理访问权限	186
5.3.1. 配置HTTP服务器设置	186
5.3.2. HTTPS 配置	188
5.3.3. 管理证书	189
5.3.4. 下载证书	190
5.3.5. 配置SSH设置	192
5.3.6. 管理服务密钥	193
5.3.7. 下载服务密钥	195
5.3.8. 配置Telnet设置	196
5.3.9. 配置Telnet身份验证列表	197

5.3.10. 配置控制台端口	199
5.3.11. 配置访问控制配置文件	200
5.3.12. 查看访问控制统计	202
5.3.13. 配置DoS拒绝服务设置	202
5.4. 端口身份验证	205
5.4.1. 配置全局802.1X设置	205
5.4.2. Configure 802.1X Settings	207
5.4.3. 配置端口身份验证	208
5.4.4. 查看端口信息	210
5.4.5. 查看客户端信息	213
5.5. 流量控制	214
5.5.1. 配置MAC筛选	214
5.5.2. MAC筛选器摘要	216
5.6. 端口安全	217
5.6.1. 配置全局端口安全模式	217
5.6.2. 配置端口安全接口	218
5.6.3. 将学到的MAC地址转换为静态地址	219
5.6.4. 配置静态MAC地址	220
5.6.5. 配置保护端口	221
5.6.6. 配置私有VLAN	223
5.6.7. 配置私有VLAN关联设置	224
5.6.8. 配置私有VLAN端口模式	225
5.6.9. 配置私有VLAN主机接口	226
5.6.10. 配置私有VLAN混杂接口	227
5.6.11. 风暴控制	228
5.6.12. 配置全局风暴控制设置	229
5.6.13. 配置风暴控制界面	230
5.7. DHCP Snooping	231
5.7.1. 配置DHCP侦听全局设置	231
5.7.2. 配置DHCP侦听接口	232
5.7.3. 配置DHCP侦听绑定	233
5.7.4. 配置窥探持久设置	234
5.7.5. 查看DHCP窥探统计信息	235
5.7.6. 配置IP源保护接口	236
5.7.7. 配置IP源保护绑定设置	238
5.7.8. 配置动态ARP检查	239
5.7.9. 配置 DAI VLAN	240
5.7.10. 配置DAI接口	241
5.7.11. 配置 DAI ACL	242
5.7.12. 配置DAI ACL规则	243
5.7.13. 查看DAI统计数据	244
5.8. 配置访问控制列表ACL	246
5.8.1. 配置基本 MAC ACL	246
5.8.2. 配置MAC ACL规则	247
5.8.3. 配置MAC ACL绑定	251
5.8.4. 查看或删除MAC绑定表中的MAC ACL绑定	253

5.8.5. 配置 IP ACL	254
5.8.6. 为IP ACL配置规则	255
5.8.7. 为扩展IP ACL配置规则	258
5.8.8. 配置 IPv6 ACL	263
5.8.9. 配置IPv6规则	264
5.8.10. 配置IP ACL接口绑定	269
5.8.11. 在IP ACL绑定表中查看或删除IP ACL绑定	271
6. 系统监控	273
6.1. 查看端口统计信息	274
6.1.1. 查看详细的端口统计信息	275
6.1.2. 查看EAP统计信息	281
6.1.3. 执行电缆测试	282
6.2. 管理日志	285
6.2.1. View Buffered Logs	285
6.2.2. 配置缓冲日志	286
6.2.3. 消息日志格式	287
6.2.4. 启用或禁用命令日志	287
6.2.5. 启用或禁用控制台日志记录	288
6.2.6. 配置Syslog日志主机设置	289
6.2.7. 查看Trap日志	291
6.2.8. 查看事件日志	292
6.2.9. 配置持久日志	293
6.3. 配置多端口镜像	294
6.3.1. 配置 RSPAN VLAN	296
6.3.2. 配置RSPAN源交换机	297
6.3.3. 配置RSPAN目标交换机	299
6.4. 配置 sFlow	300
6.4.1. 配置基本sFlow代理信息	300
6.4.2. 配置sFlow代理高级设置	301
6.4.3. Configure an sFlow Receiver	302
6.4.4. 配置sFlow接口	304
7. 维护	306
7.1. 保存配置	307
7.2. 重新启动交换机	307
7.3. 将交换机重置为出厂默认设置	308
7.3.1. 将所有用户密码重置为其默认设置	309
7.4. 从交换机下载文件	309
7.4.1. 将文件从交换机复制到TFTP服务器:	310
7.4.2. HTTP文件上载	312
7.4.3. 将文件从交换机保存到USB设备	312
7.5. 将文件上传保存到交换机	314
7.5.1. 上传文件	314
7.5.2. 使用HTTP将文件下载到交换机	316
7.5.3. 从USB设备下载文件	318

7.6. 文件管理	319
7.6.1. 复制映像	319
7.6.2. 配置双映像设置	320
7.7. 故障排除	321
7.7.1. Ping IPv4	321
7.7.2. Ping IPv6	323
7.7.3. Traceroute IPv4	325
7.7.4. Traceroute IPv6	327
8. 默认设置	330
9. 配置例子参考	333
9.1. 虚拟局域网 (VLANs)	334
9.1.1. VLAN配置示例	334
9.2. Access Control Lists (ACLs)	334
9.2.1. MAC ACL Sample Configuration	335
9.2.2. Standard IP ACL Sample Configuration	336
9.2.3. DiffServ Example Configuration	337
9.3. 802.1X	338
9.3.1. 802.1X Example Configuration	339
9.4. MSTP	340
9.4.1. MSTP Example Configuration	341
10. 缩略语	344

1. 开始

本章概述了如何启动交换机 以及如何通过用户界面访问管理。本章包括以下章节内容：

- 有效的文档手册和而在线帮助
- 理解用户管理界面接口
- **Web** 管理界面接口概述
- 通过 **Web** 浏览器访问和登录交换机
- 使用 **SNMP**

提示: 有关本手册所涵盖主题的更多信息, 请访问支持网站 *****.com**

提示: 具有新功能和错误修复的固件更新可能随时发布, 请及时通过供应商获取。有些产品可以定期检查站点并下载新固件, 或者您可以手动检查

并下载新固件。如果产品的功能或行为与本指南中描述的不匹配，则可能需要更新固件。

1.1.理解用户界面

管理型交换机软件包括一套综合管理功能，可以使用以下方法之一配置和监控系统：

- Web网络用户界面
- 简单网络管理协议（SNMP）
- 命令行界面（CLI）

每种基于标准的管理方法都允许您配置和监视管理型交换机软件的功能组件。您用于管理系统的方法取决于您的网络大小和要求，以及您的偏好。

管理型用户手册 (本文档) 介绍了如何使用基于web的界面来管理和监控系统。

1.2.Web管理界面概述

管理型交换机包含一个嵌入式web服务器和管理软件，用于管理和监视交换机的各个功能。此管理型交换机在不使用管理软件的情况下可以作为简单交换机运行。但是您可以使用管理软件配置更高级的功能，以提高交换机效率和整体网络性能。

基于Web的管理方式允许您使用标准Web浏览器远程监视、配置和控制交换机，而不是使用昂贵而复杂的SNMP软件产品。通过web浏览器，您可以监视交换机的性能并优化其网络配置。您可以使用基于web的管理界面配置绝大部分的交换机功能，例如VLAN、QoS和ACL。

使用Web界面的软件要求

要使用web浏览器访问交换机，此交换机支持常见的浏览器，浏览器必须满足以下软件要求：

- HTML 版本 4.0, 或更高版本
- HTTP 版本 1.1, 或更高版本

1.3.使用Web浏览器访问交换机并登录

您可以使用web浏览器访问交换机并登录配置。您必须能够从管理系统成功地ping到管理型交换机管理接口的IP地址，才能开始使用web访问。

要使用基于浏览器的访问权限登录交换机，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址，

交换机的默认IP地址为192.168.10.12。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为admin，默认管理员密码为空，即不要输入密码。
6. 单击登录按钮。

将显示web管理界面页面。

Web界面按钮和用户定义字段

下表显示了在web界面的整个屏幕中使用的命令按钮：

表1. Web界面命令按钮

按钮	功能
增加	单击“增加”按钮可添加在表格标题行中配置的新项。
应用	单击“应用”按钮将更新的配置发送到交换机，配置更改立即生效。
取消	单击“取消”按钮取消屏幕上的配置，并将屏幕上的数据重置为交换机的先前值。
删除	单击“删除”按钮可删除所选项目。
更新	单击“更新”按钮可加载设备的最新信息刷新当前屏幕。.
注销	单击“注销”按钮结束会话。

用户定义的字段可以包含1到159个字符，除非在配置web屏幕上另有说明。除以下字符外，可以使用所有字符（除非在中针对该功能特别注明）：

用户定义的字段无效字符	
\	<
/	>
*	
?	

接口命名的约定

管理型交换机支持多种物理和逻辑接口，接口由其类型和接口编号标识。物理端口是千兆接口，在前面板上由对应的编号。您可以使用软件配置这些逻辑接口。

下表描述了交换机上所有可用接口的命名约定。

表2. 接口的命名约定

接口	描述	例子
物理端口	物理端口是千兆、万兆以太网接口，从一个数字开始按顺序编号。	0/1, 0/2, 0/3, 等等
链路聚合组(LAG)	LAG 接口是逻辑接口类型，仅用于桥接功能的逻辑接口。	LAG 1, LAG 2, IAG 3, 等等
CPU 管理接口	这是负责对应交换机基本MAC地址的内部交换机接口。此接口不可配置，始终列在MAC地址表中。	5/1
VLAN 路由接口	这是一个用于路由功能的接口。	VLAN 1, VLAN 2, VLAN 3, 等等

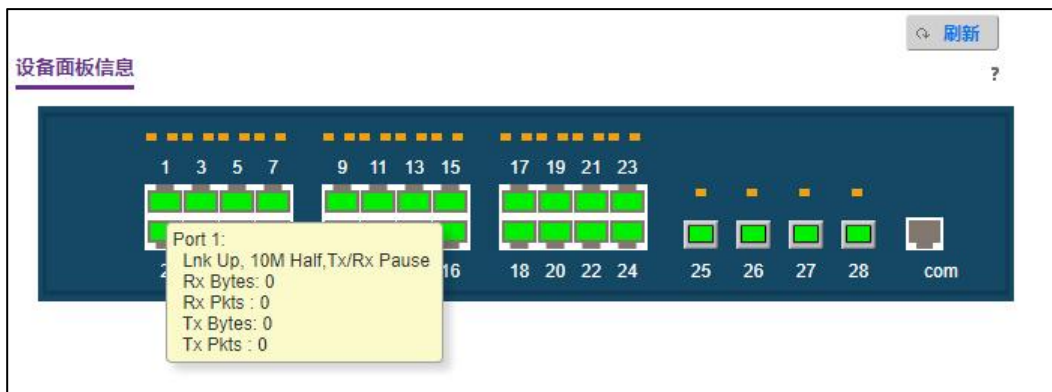
要使用设备视图，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址，
交换机的默认IP地址为192.168.10.12 。
此时将显示登录屏幕。
5. 输入用户名和密码。
默认管理员用户名为admin，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
7. 单击 **系统管理 > 设备面板**。



端口颜色指示端口当前是否处于活动状态。绿色表示端口已启用；橙色表示端口上发生错误，或链接已禁用。

移动光标到端口可以查看显示端口的统计信息，或单击端口以跳转查看端口的详细统计信息。



1.4. 使用 SNMP

管理型交换机软件支持配置SNMP组和用户，以管理SNMP代理生成的Trap消息。

此管理型交换机使用标准公共MIB实现标准功能，同时使用支持其它交换机功能的专用MIB。所有专用MIB都以“-”前缀开头。接口配置的主要对象是 -SWITCHING-MIB，它是一个私有MIB。某些接口配置还涉及公共MIB（IF-MIB）中的对象。

SNMP模块的默认配置是启用的，系统信息屏幕（登录时显示的屏幕）显示配置SNMP管理器以访问交换机所需的信息。

任何用户都可以使用SNMP v1/2/3协议连接到交换机。但对于身份验证和加密，交换机可以支持多个用户，因此可以单独创建或修改多个配置文件，对应于不同的 MIB 和权限。

要为SNMP v3管理配置文件配置身份验证和加密设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址，
交换机的默认IP地址为192.168.10.12 。
此时将显示登录屏幕。
5. 输入用户名和密码。
默认管理员用户名为admin，默认管理员密码为空，即不要输入密码。
6. 单击**登录**按钮。
7. 单击 **系统管理 > SNMP管理 > SNMP v3 > 用户名管理** 。
此时将显示SNMPv3用户信息配置页面。
8. 要启用身份验证，请选择一个 **认证协议** 选项，即 **MD5** 或 **SHA**。
9. 要启用加密，请在 **加密模式** 列表中选择 **DES** 选项，然后在**密钥值** 和 **确认密钥值** 字段中输入八个或更多字母数字字符的加密代码。
10. 单击 **增加** 按钮，您的设置将生效。

要访问SNMP V1或SNMP V2的配置信息，请选择 **系统 > SNMP管理 > SNMPv1/v2**，然后根据屏幕显示的信息继续配置。

2. 系统管理

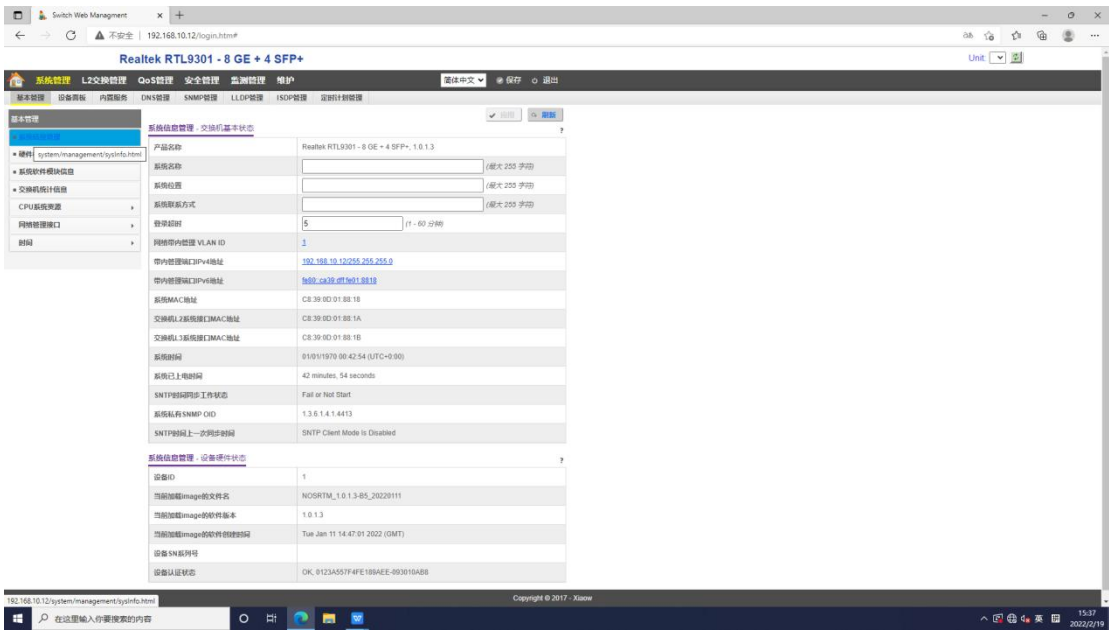
本章涵盖以下主题：

- 基本管理
- 内置服务
- *DNS* 管理
- *SNMP* 管理
- *LLDP* 管理
- *ISDP* 管理
- 定时表

2.1.基本管理

2.1.1.系统信息管理

系统管理 > 基本管理 > 系统信息管理



1. 在 **系统名称** 字段，键入用于标识此交换机的名称。
您最多可以使用255个字符的名称，出厂默认值为空。
2. 在 **系统位置** 字段，键入描述交换机的位置信息。
您最多可以使用255个字符的名称，出厂默认值为空。
3. 输入 **系统联系方式**，即此交换机的联系人信息或其它类似的信息
您最多可以使用255个字符的联系人信息，出厂默认值为空
4. 输入**登录超时**，即此交换机的登录时间限制
配置范围是1-60分钟，出厂默认值5分钟
5. 单击 **应用** 按键
更新的配置将发送到交换机，配置更改立即生效。

下表描述了系统信息屏幕显示的状态信息。

表3. 系统信息

字段	描述
产品名称	此交换机的产品名称标示。
网络带内管理 VLAN ID	交换机的管理VLAN ID。单击显示的管理VLAN ID值跳转到配置屏幕。
带内管理端口IPv4地址	分配给管理VLAN接口的IPv4地址和掩码。
带内管理端口IPv6地址	分配给管理VLAN接口的IPv6前缀和前缀长度。
系统MAC地址	通用分配的网络MAC地址。
交换机L2系统接口MAC地址	用于 L2层交换网段上本交换机通信的MAC地址。
交换机L3系统接口MAC地址	用于 L3层路由模式上交换机通信的MAC地址。
系统时间	交换机内当前工作的日期时间。
系统已上电时间	自上次交换机重新启动以来的时间（以天、小时和分钟为单位）。
SNTP时间同步工作状态	当前交换机内 SNTP 客户端的同步状态。
系统私有SNMP OID	交换机的私有MIB的基本 OID。
SNTP时间上一次同步时间	SNTP 客户端上一次成功同步的时间。

系统信息管理 - 设备硬件状态	
设备ID	1
当前加载image的文件名	NOSRTM_1.0.1.0-B5_20210720
当前加载image的软件版本	1.0.1.0
当前加载image的软件创建时间	Tue Jul 20 06:40:48 2021 (GMT)
设备SN序列号	
设备认证状态	OK, 0123613A959F05F2EE-09301013D

下表介绍了显示的信息。

2.1.2. 硬件模块信息

系统管理 > 基本管理 > 硬件模块信息

系统管理 L2交换管理 路由管理 QoS管理 安全管理 监测管理 维护													
基本管理 设备面板 内置服务 DNS管理 SNMP管理 LLDP管理 ISDP管理 定时计划管理	简体中文 保存 退出												
基本管理	硬件模块信息 - 机型信息												
- 系统信息管理 - 硬件模块信息 - 设备信息及状态 - 交换机计数统计 - CPU系统资源 - 网络管理接口 - 时间	自动刷新: 3秒 刷新 <table> <tr> <td>硬件类别</td><td>Realtek RTL9301 - 24 GE + 4 SFP+</td></tr> <tr> <td>硬件型号</td><td>RTL9301-28</td></tr> <tr> <td>设备版本</td><td>09301013D</td></tr> <tr> <td>制造商代号</td><td>0x8001</td></tr> <tr> <td>设备Boot引导程序版本</td><td>U-Boot 2011.12.(3.6.5.55070) (Jul 20 2021 - 14:47:08)</td></tr> <tr> <td>硬件设计版本</td><td></td></tr> </table>	硬件类别	Realtek RTL9301 - 24 GE + 4 SFP+	硬件型号	RTL9301-28	设备版本	09301013D	制造商代号	0x8001	设备Boot引导程序版本	U-Boot 2011.12.(3.6.5.55070) (Jul 20 2021 - 14:47:08)	硬件设计版本	
硬件类别	Realtek RTL9301 - 24 GE + 4 SFP+												
硬件型号	RTL9301-28												
设备版本	09301013D												
制造商代号	0x8001												
设备Boot引导程序版本	U-Boot 2011.12.(3.6.5.55070) (Jul 20 2021 - 14:47:08)												
硬件设计版本													

表4. 硬件模块信息

字段	描述
硬件类别	交换机硬件模块内部名称标识。
硬件型号	交换机硬件模块内部型号
设备版本	交换机硬件内部编号
制造商代号	交换机硬件生产商编码
设备Boot引导程序版本	本交换机 boot引导加载程序的软件版本编号。
硬件设计版本	本交换机硬件设计版本编号。

下表不可配置，描述了系统的温度状态信息。

硬件模块信息 - 温度传感器状态

传感器	当前温度	最大温度
System	33°C	33°C

表5. 温度状态信息

字段	描述
传感器	温度传感器的所属的模块信息
当前温度 (°C)	显示当前传感器的温度，单位为摄氏度。
最大温度 (°C)	显示当前传感器在工作周期内测量到最高的温度。

2.1.3. 设备信息及状态

系统管理 > 基本管理 > 设备信息及状态

系统管理 L2交换管理 路由管理 QoS管理 安全管理 监测管理 维护 简体中文 保存 退出			
基本管理 设备面板 内置服务 DNS管理 SNMP管理 LLDP管理 ISDP管理 定时计划管理			
基本管理			
■ 系统信息及管理			
■ 系统初始设置			
■ 硬件模块信息			
■ 交换机计数统计			
CPU系统资源			
网络管理接口			
■ Loopback IP环路接口			
时间			
设备信息及状态			
产品名称	Broadcom 53346 - 24 GE + 4 SFP+, 1.0.2.1	系统MAC地址	02:00:00:00:00:00
系统名称		管理接口IP地址	0.0.0.0
系统位置		管理接口MASK	0.0.0.0
系统联系方式		Gateway	0.0.0.0
引导程序版本		管理接口VLAN ID	1
当前加载image的软件版本	Unknown, 1.0.2.1	登录超时(分钟)	5
硬件设计版本		系统时间	08/11/2021 12:37:25 (UTC+0:00)
设备SN序列号		认证状态	OK, 123ABC
系统管理软件模块状态			
SNTP	Disabled Setting	LAG	Disabled Setting
Spanning Tree	Enabled Setting	IGMP Snooping	Disabled Setting
SNMP	Enabled Setting	MLD Snooping	Disabled Setting
System Log	Disabled Setting	802.1X	Disabled Setting
SSL	Disabled Setting	SSH	Disabled Setting
GVRP	Disabled Setting	Port Mirror	Disabled Setting
Telnet	Enabled Setting	CLI Paging	Enabled Setting
Web	Enabled Setting	DHCP Snooping	Disabled Setting
DHCP Server	Disabled Setting	DHCP Relay	Disabled Setting
UDP Relay	Disabled Setting	DNS Resolver	Enabled Setting
Routing	Enabled Setting	BFD	Disabled Setting
RIP	Enabled Setting	OSPF	Enabled Setting
BGP	Enabled Setting	VRRP	Disabled Setting
PIM	Not support	DVMRP	Not support

要刷新屏幕信息，请单击 刷新 按钮。

2.1.4. 交换机计数统计

系统管理 > 基本管理 > 交换机计数统计

交换机计数统计 ?	
CPU端口索引号	65
CPU端口接收字节数	0
CPU端口接收单播帧数量	0
CPU端口接收组播帧数量	0
CPU端口接收广播帧数量	0
CPU端口接收丢弃帧数量	-
CPU端口发送字节数	18656079
CPU端口接收正确帧数量	156774
CPU端口发送单播帧数量	0
CPU端口发送组播帧数量	156774
CPU端口发送广播帧数量	0
CPU端口发送端丢弃帧数量	-
最大地址占用数量	1
已使用地址数量	1
VLAN最大可使用数量	4094
VLAN最大使用数量	1
静态VLAN数量	1
动态VLAN数量	0
删除VLAN数量	0
上次清除计数的间隔时间	2 day 3 hr 52 min 44 sec

要清除所有计数器，将所有交换机摘要和详细统计信息重置为默认值，请单击 **清除** 按钮。无法清除丢弃的数据包计数。

下表介绍了交换机统计信息。

表6. 交换机统计信息

字段	描述
端口索引号	此交换机的处理器关联的接口表项的 内部索引值 。
端口接收字节数	处理器接收的数据的字节总数（不包括帧位，但包括FCS字节）。
接收单播帧数量	传送到更高层协议的子网单播数据包数。
接收组播帧数量	接收到的定向到组播地址的数据包总数。此号码不包括指向广播地址的数据包。
接收广播帧数量	接收到的定向到广播地址的数据包总数，这不包括组播数据包。
接收丢弃帧数量	即使未检测到错误也被丢弃的入站数据包的数量，以防止其可传递到更高层协议。丢弃数据包的一个可能原因是释放缓冲区空间，或者不符合协议要求。

发送字节数	从接口传输的字节总数，包括帧字符
接收正确帧数量	从接口向外传输的数据包总数。
发送单播帧数量	高级协议请求传输到子网单播地址的数据包总数，包括被丢弃或未发送的数据包。
发送组播帧数量	高级协议请求传输到组播地址的数据包总数，包括被丢弃或未发送的数据包。
发送广播帧数量	高级协议请求传输到广播地址的数据包总数，包括被丢弃或未发送的数据包。
发送端丢弃帧数量	即使未检测到错误也被丢弃的出站数据包数，以防止其可传递到更高层协议。丢弃数据包的一个可能原因是释放缓冲区空间。
最大地址占用数量	自最近一次重新启动以来，此交换机学习及存储的转发地址表项的最大数目。
已使用地址数量	此交换机的当前学习及存储的转发地址表中的数目，包括静态条目数。
VLAN最大可使用数量	此交换机上支持的允许最大 VLAN 数量。
VLAN最大使用数量	自上次重新启动以来此交换机上活动的最大VLAN数。
静态VLAN数量	当前时间下，此交换机上静态创建的活动VLAN条目数。
动态VLAN数量	通过GVRP注册创建的此交换机上当前活动的VLAN条目数统计值。
删除VLAN数量	自上次重新启动以来在此交换机上创建并删除的VLAN数统计值。
上次清除计数的间隔时间	自上次清除此交换机的统计信息以来经过的时间，以天、小时、分钟和秒为单位。

2.1.5. CPU系统资源

2.1.5.1. CPU系统资源

系统管理 > 基本管理 > CPU系统资源> CPU系统资源

CPU系统资源 - 内存状态	
系统内存大小	246 MBytes
剩余内存大小	68 MBytes

CPU系统资源 - CPU使用率

PID	Name	5 Secs	60 Secs	300 Secs
3	(ksoftirqd/0)	0.00%	0.01%	0.00%
129	rtkRxTask	0.00%	0.03%	0.04%
133	cpuUtilMonitorTask	0.41%	0.54%	0.56%
139	tap_monitor_task	0.00%	0.04%	0.04%
145	nim_t	0.00%	0.00%	0.02%
146	httpd	0.00%	0.21%	0.07%
151	emlWeb	0.00%	0.00%	0.01%
153	dtlTask	0.00%	0.03%	0.03%
165	hapiBroadBfdCtrlTas	0.00%	0.00%	0.01%
175	SNMPTask	0.20%	0.04%	0.01%
220	openrTask	0.00%	0.00%	0.02%
258	RMONTask	0.00%	0.24%	0.36%
Total CPU Utilization		0.61%	1.18%	1.27%

您可以查看CPU利用率信息，其中包含内存信息、任务相关信息以及每个任务的CPU利用率百分比。

下表介绍了CPU内存状态信息。

表7. CPU内存状态信息

字段	描述
系统内存大小	交换机的总内存（以KB为单位）。
剩余内存大小	交换机的剩余可用内存空间（KB）。

2.1.5.2. CPU利用率阈值

系统管理 > 基本管理 > CPU系统资源 > CPU利用率阈值

基本管理

系统信息管理

硬件模块信息

设备信息及状态

交换机计数统计

CPU系统资源

CPU系统资源

CPU利用率阈值

网络管理接口

时间

CPU利用率阈值 - 报警配置

上升阈值

0

(0 - 100, 单位: 百分比)

上升阈值检测间隔时间

0

(5 - 86400, 单位: 秒)

下降阈值

0

(0 - 100, 单位: 百分比)

下降阈值检测间隔时间

0

(5 - 86400, 单位: 秒)

剩余内存检测阈值

0

(0 - 3037172, 单位: KB, 千字节)

应用

刷新

1. 配置 上升阈值 参数

在配置的时间段内，当CPU总利用率超过此阈值时，将生成通知。范围是1到100。

2. 配置 上升阈值检测间隔时间 参数

此利用率监控时间段可配置为5到86400秒，以5秒的倍数表示。

3. 配置 下降阈值 参数

当总CPU利用率在配置的时间段内低于此水平时，将触发通知。

下降的利用率阈值必须等于或小于上升的阈值。仅当先前已完成阈值上升通知时，才会发出利用率阈值下降通知。配置下降利用率阈值和时间段是可选的。如果未配置下降的CPU利用率参数，则其值与上升的CPU利用率参数值相同。范围是1到100。

4. 配置 下降阈值检测间隔时间 参数

利用率监控时间段可配置为5秒到86400秒，以5秒的倍数表示。

5. 配置 CPU 剩余内存检测阈值，单位是 KB。

要更新屏幕数据，请单击 刷新 按钮。

2.1.6. 网络接口管理

2.1.6.1. IPV4网络管理接口

系统管理 > 基本管理 > 网络接口管理 > IPV4网络管理接口

1. 指定交换机的管理VLAN ID。

管理VLAN用于管理交换机。 VLAN ID 可以是1到4093之间的任何值，此VLAN ID必须先创建于交换机内。

基本管理

系统信息管理

硬件模块信息

设备信息 & 状态

交换机计数统计

CPU系统资源

网络管理接口

IPV4网络管理接口

IPV6网络管理接口

IPV6网络邻居

时间

基本管理

设备面板

内置服务

DNS管理

SNMP管理

LLDP管理

ISDP管理

定时计划管理

IPv4网络管理接口 - 带内接口

网络带内管理 VLAN ID

1

当前网络IP地址配置模式

☒ 手动配置

☐ Bootp

☐ DHCP

管理接口IP地址

192.168.10.12

管理接口MASK值

255.255.255.0

缺省网关地址

0.0.0.0

已烧录内置的MAC地址

C8:39:0D:01:5B:E0

指定的管理接口MAC地址

00:00:00:00:00:00

MAC地址选择

☒ 系统内置

☐ 指定的

DHCP供应商类别标识符

☐ 关闭

☒ 启用

指定的DHCP供应商类别标识符

带内管理接口状态

Up

应用

刷新

表8. IPv4管理VLAN配置

字段	描述
内置的MAC地址	使用已烧录的MAC地址分配给VLAN 管理接口。
指定的管理接口MAC地址	指定一个单播的的MAC地址分配给VLAN 管理接口。

MAC地址选择	选择VLAN 管理接口的MAC 地址使用何种分配方式。
DHCP供应商类别标识符	当IP地址为DHCP模式，是否发送标识符给 dhcp 服务器。
指定的DHCP供应商类别标识符	手动指定一个DHCP供应商类别标识符。
接口状态	指示链路工作状态是 up 或 down 。

2. 选择 IPv4地址分配 单选按钮。

这指定获取服务端口的IPv4网络参数（IPv4地址和网络掩码）的方法。可能的选项有 **DHCP**, **BootP**, 或 **Static** 。默认值是静态设置IPv4地址。

- **BootP**. 在下一个引导周期中，设备上的BootP客户端广播BootP请求，试图从网络上的BootP服务器获取信息。
- **DHCP**. 在下一个引导周期中，设备上的DHCP客户端广播DHCP请求，试图从网络上的DHCP服务器获取信息。
- **None**. 设备不会尝试动态获取网络信息，可以手动设定一个IPv4地址。

3. 指定服务端口的 IP地址 。

出厂默认值为 192.168.10.12 。

4. 指定服务端口的 子网掩码 值。

这也称为子网/网络掩码，定义了用于标识连接网络的接口IP地址部分。出厂默认值为 255.255.255.0 。

5. 指定服务端口IPv4地址的 默认网关。

默认值为 0.0.0.0 (空) 。

2.1.6.2. IPV6网络管理接口

系统管理 > 基本管理 > 网络管理接口 > IPv6 网络管理接口

The screenshot displays the 'IPv6 Network Management Interface' configuration page. The left sidebar shows a navigation menu with 'Network Management Interface' selected. The main content area is divided into two sections: 'IPv6 Network Management Interface - Global Parameter Configuration' and 'IPv6 Network Management Interface - Interface Parameter Configuration'.

Global Parameter Configuration:

- IPv6 protocol enablement: Radio buttons for 'Disable' (关闭) and 'Enable' (启用). 'Enable' is selected.
- IPv6 address automatic management: Radio buttons for 'Disable' (关闭) and 'Enable' (启用). 'Disable' is selected.
- Current network IP address configuration mode: Radio buttons for 'Manual configuration' (手动配置) and 'DHCPv6'. 'Manual configuration' is selected.
- IPv6 default gateway: A text input field.

Interface Parameter Configuration:

- IPv6 address/Prefix length: A text input field.
- Use EUI64 format: A dropdown menu.

1. 单击IPv6协议使能单选项中的 关闭 或 启用 按钮

这将启用或禁用交换机上管理VLAN IPv6 接口的管理模式。

- 单击IPv6地址自动管理单选项中的 **关闭** 或 **启用** 按钮
 提示: 只有在全局禁用单播路由时,“地址自动配置模式”选项才可用。
- 单击网络IP地址配置模式单选项中的 **手动配置**或 **DHCPV6** 按钮
- 在表项 IPv6地址/Prefix长度 字段中, 指定要从管理VLAN接口添加或删除的IPv6地址。
- 单击 **EUI46** 选项中的 **True** (启用) IPv6地址的扩展通用标识符 (EUI) 。
- 单击 **增加** 按钮
 新的IPv6地址将添加到管理VLAN 中
- 要删除选定的IPv6地址, 请单击 **删除** 按钮。
- 单击 **应用** 按键

更新的配置参数将发送到交换机, 配置更改将立即生效。

2.1.6.3. IPv6 网络邻居

系统管理 > 基本管理 > 网络管理接口 > IPv6 网络邻居

IPv6网络邻居 - 列表				
IPv6地址	系统MAC地址	是否路由设备	缓存条目状态	最近确认时间

下表显示IPv6网络接口邻居表信息。

表9. IPv6网络接口邻居表信息

字段	描述
IPv6地址	网络接口可见的邻居交换机的IPv6地址。
MAC 地址	邻居交换机或设备的MAC地址。
是否路由设置	true (1) 如果邻居机器是路由器, false (2) 否则为其它。 .
缓存条目状态	相邻交换机的状态: reachable (1). 通过此交换机可以访问邻居。 stale (2). 已计划删除有关邻居的信息。 delay (3). 延迟期间未收到邻居的任何信息。 . probe (4). 交换机正在尝试探测此邻居。 unknown (6). 未知状态。
最近确认时间	此邻居上次更新的系统正常运行时间。

2.1.7. 时间

2.1.7.1. 系统时间配置

系统管理 > 基本管理 > 时间 > 系统时间配置

1. 单击时间源选择中的单选 **手动配置** 或 **SNTP** 按钮

默认值是手动配置，即使用交换机本地的时钟源。只有满足以下两个条件，才能将本地时钟设置为SNTP：

- 已配置SNTP服务器。
 - SNTP上次尝试状态为成功。
2. 在 手动配置模式，可以选择 **自动从浏览器获取时间** 选项，从浏览器中获取时间，然后在设定为交换机的本地时间。
3. 在 **日期** 字段中，以月、日和年为单位指定当前日期。
4. 在 **时间** 字段中，以小时、分钟和秒为单位指定当前时间。
5. 使用 **时区名称** 字段配置时区，指定小时数以及（GMT）与UTC的分钟数之差，以及 **偏移小时数** 和 **偏移分钟数**。

时区会影响当前系统时间的显示，默认值为UTC。当使用SNTP/NTP时间服务器更新交换机时钟时，从服务器接收到的时间数据是基于UTC (Coordinated Universal time)的，即与GMT (Greenwich Mean time)相同，这可能不是交换机所在的时区。

6. 使用 **时区偏移小时** 字段指定与UTC的时差数。允许的范围为-12到13。默认值为0。
7. 使用 **时区偏移分钟** 字段指定与UTC相差的分钟数。允许的范围为0到59。默认值为0。
8. 使用**预定义的时区选择** 字段，可以选择内部预定义的时区参数更新前面的时间偏移值。
9. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

要更新屏幕信息，请单击 **刷新** 按钮。

2.1.7.2. SNTP全局管理

系统管理 > 基本管理 > 时间 > SNTP全局管理

选择 **SNTP** 选项作为时钟源时，**SNTP**全局状态显示在**SNTP**全局配置部分下方。

1. 单击 **客户端工作模式** 单选按钮以指定SNTP客户端的操作模式：

- **关闭**. SNTP无法运行。不会从客户端发送SNTP请求，也不会处理收到的SNTP消息。
- **单播**. SNTP以点对点的方式运行。单播客户机在其单播地址向指定的服务器发送请求，并期望得到一个应答，从中可以确定时间以及（可选）相对于服务器的往返延迟和本地时钟偏移。
- **广播**. 以与**组播**模式相同的方式运行，但使用本地广播地址而不是**组播**地址。广播地址具有单个子网范围，而**组播**地址具有Internet范围。

默认值为关闭。

2. 在 **协议端口号** 字段中，指定SNTP客户端在其上接收服务器数据包的本地UDP端口。

允许的范围为1025到65535，或为123。默认值为123。配置默认值时，SNTP数据包中使用的实际客户端端口值由操作系统分配。

3. 单击 **源接口选择** 用于选择SNTP客户端连接的IP接口。

可能的值如下所示：

- None
- VLAN 1
- Routing interface
- Routing VLAN
- Routing loopback interface
- Tunnel interface
- Service port

默认情况下，VLAN 1 用作源接口。

4. 指定单播查询间隔 .

这是在单播模式下配置时，以二次幂表示的单播轮询请求之间的秒数。允许的范围为6到10。默认值为6。

5. 指定广播查询间隔 .

这是在广播模式下配置时，广播轮询请求之间的秒数，表示为2的幂。在此间隔到期之前接收的广播将被丢弃。允许的范围为6到10。默认值为6。

6. 指定单播查询超时 .

这是在单播模式下配置时等待SNTP响应的秒数。允许的范围为1到30。默认值为5。

7. 指定单播查询重试次数 .

这是在单播模式下配置时，在尝试使用下一个配置的服务器之前，在第一次超时后重试对SNTP服务器的请求的次数。允许的范围为0到10。默认值为1。

8. 单击 应用 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

要更新屏幕信息，请单击 刷新 按钮。

选择SNTP选项作为时钟源时，SNTP全局状态显示在SNTP全局配置部分下方。

SNTP全局管理 - 工作状态		?
服务端版本	4	
Supported Mode		
最近更新时间	Not Synchronized	
最近成功通讯时间		
最近成功通讯状态	Other	
服务器地址		
服务器地址类别	unknown	
服务器信息	0	
服务器参考时间ID		
服务器工作模式	Reserved	
单播最大尝试次数	3	
单播查询服务器次数统计	0	
广播查询次数统计	0	

下表显示了不可配置的SNTP全局状态信息。

表10. SNTP全局工作状态

字段	描述
支持版本	客户端支持的SNTP版本。
Supported mode	客户端支持的SNTP模式，一个客户端可以支持多种模式。

最近更新时间	SNTP客户端上次更新系统时钟的本地日期和时间（UTC）。
最近成功通讯时间	上次SNTP请求或收到未经请求的消息的本地日期和时间（UTC）。
最近成功通讯状态	单播和广播模式下最后一个SNTP请求或未经请求的消息的状态。如果未收到来自服务器的消息，则显示“其他”状态。这些值适用于所有操作模式。 • Other. 以下枚举状态值均不存在。 • Success. SNTP操作成功，系统时间已更新。 • Request Timed Out. 定向SNTP请求在未收到SNTP服务器响应的情况下超时。 • Bad Date Encoded. SNTP服务器提供的时间无效。 • Version Not Supported. 服务器支持的SNTP版本与客户端支持的版本不兼容。 • Server Unsynchronized. SNTP服务器与其对等服务器不同步。这通过SNTP消息上的leap指示符字段指示。 • Server Kiss Of Death. SNTP服务器表示不会向该服务器发送进一步的查询。这由从服务器接收的消息中等于0的层字段表示。
服务器地址	服务器最后收到的有效数据包的 IP 地址。如果没有从任何服务器接收消息，则显示一个空字符串。
服务器地址类别	最后收到的有效数据包的 SNTP 服务器地址类型的地址类型。
服务器信息	服务器的最后一个已收到的有效数据包的声明层数据。
服务器参考时间ID	服务器上一个已收到的有效数据包的参考时钟标识符。
服务器工作模式	最后收到有效数据包的服务器模式。
单播服务器最大条目数	可在此客户端上配置的单播服务器条目的最大数量。
单播查询服务器次数统计	为此客户端配置的当前有效单播服务器条目的数量。
广播查询次数统计	自上次重新启动以来SNTP客户端接收和处理的未经请求的广播SNTP消息数。

2.1.7.3. SNTP服务器配置

系统管理 > 基本管理 > 时间 > SNTP服务器配置



1. 在 **服务器类别** 列表中，选择配置的SNTP服务器地址的地址类型。
可能的值如下所示：

- IPv4
- IPv6
- DNS

默认值为 IPv4。

2. 在 **服务器地址** 字段中，指定SNTP服务器的地址。

这是一个最多64个字符的文本字符串，包含SNTP服务器的编码单播IP地址或主机名。单播SNTP请求被发送到此地址。如果此地址是DNS主机名，则每次向其发送SNTP请求时，该主机名都会解析为IP地址。

3. 在 **协议端口号** 字段中输入其向SNTP服务器发送请求的目的端口号。

有效范围为1到 65535，默认值为123。

4. 在 **优先级** 字段中，输入一个数值，确定向其发送SNTP请求的服务器顺序。

客户端继续向不同的服务器发送请求，直到收到成功的响应，或者所有服务器都已耗尽。优先级指示查询服务器的顺序。优先级为1的服务器条目在优先级为2的服务器之前查询，依此类推。如果多个服务器具有相同的优先级，则请求顺序遵循此表中条目的字典顺序。有效范围为1到3。默认值为1。

5. 在 **支持版本** 字段中，指定在服务器上运行的SNTP软件的版本。

范围为1到4。默认值为4。

6. 单击 **增加** 按钮

此操作将添加SNTP服务器条目。这会将更新的配置发送到交换机，配置更改立即生效。

7. 重复前面的步骤以添加其他SNTP服务器。

您最多可以配置三台SNTP服务器。

8. 要更改现有SNTP服务器的设置，请选中已配置服务器旁边的复选框，并在可用字段中输入新值。

9. 要删除SNTP服务器条目，请选中要删除的已配置服务器旁边的复选框，然后单击 **删除** 按钮。

已选条目将删除，并更新设备数据。

10. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

要更新屏幕信息，请单击 **刷新** 按钮。

SNTP服务器状态表显示交换机上配置的SNTP服务器的状态信息。下表显示了SNTP服务器状态信息。

表11. SNTP服务器状态

字段	描述
服务器地址	所有现有的服务器地址。如果不存在服务器配置，屏幕上将闪烁一条消息，说明不存在SNTP服务器。
最近更新时间	此服务器的响应用于更新系统时钟的本地日期和时间（UTC）。
最近成功通讯时间	上次查询此SNTP服务器的本地日期和时间（UTC）。
最近成功通讯状态	向此服务器发出的上一个S9 NTP请求的状态。如果没有从该服务器接收到数据包，则显示Other状态。 • Other. 以下枚举值均不存在。 • Success. SNTP操作成功，系统时间已更新。 • Request Timed Out. 定向SNTP请求在未收到SNTP服务器响应的情况下超时。 • Bad Date Encoded. SNTP服务器提供的时间无效。 • Version Not Supported. 服务器支持的SNTP版本与客户端支持的版本不兼容。 • Server Unsynchronized. The SNTP服务器与其对等服务器不同步。这通过SNTP消息上的leap指示符字段指示。 • Server Kiss Of Death. SNTP服务器表示不会向该服务器发送进一步的查询。这由从服务器接收的消息中等于0的层字段表示。
查询次数	自上次代理重新启动以来对此服务器发出的SNTP请求数。
查询失败次数	自上次重新启动以来对此服务器发出的失败SNTP请求数。

SNTP确保精确的网络设备时钟时间同步高达毫秒。时间同步由网络SNTP服务器执行。本交换机的软件系统仅作为SNTP客户端运行，不能向其他系统提供时间服务。

时间来源由阶层确定。层定义参考时钟的准确性。阶层越高（零是最高的），时钟就越准确。该设备从层 1 及以上接收时间，因为它本身就是一个层 2 设备。

以下是阶层示例：

- **Stratum 0.** 实时时钟用作时间源，例如GPS系统。
- **Stratum 1.** 使用直接链接到0层时间源的服务器。第1层时间服务器提供主要的网络时间标准。
- **Stratum 2.** 时间源通过网络路径与第1层服务器保持距离。例如，第2层服务器通过NTP通过网络链路从第1层服务器接收时间。

根据时间级别和服务器类型评估从SNTP服务器接收的信息。

SNTP时间定义由以下时间级别进行评估和确定：

- **T1.** 客户端发送原始请求的时间。
- **T2.** 服务器接收原始请求的时间。
- **T3.** 服务器发送回复的时间。
- **T4.** 客户端收到服务器回复的时间。

设备可以轮询服务器时间内的单播服务器类型。

轮询单播信息用于轮询IP地址已知的服务器。设备上配置的SNTP服务器是唯一轮询同步信息的服务器。T1到T4用于确定服务器时间。这是同步设备时间的首选方法，因为它是最安全的方法。如果选择此方法，则仅从使用SNTP服务器配置屏幕的设备上定义的SNTP服务器接受SNTP信息。

设备通过主动请求信息或在每个轮询间隔检索同步信息。

您可以查看和修改有关添加和修改简单网络时间协议SNTP服务器的信息。

2.1.7.4. 夏令时配置

系统管理 > 基本管理 > 时间 > 夏令时配置

夏令时配置 - 参数配置

夏令时(DST)工作模式: ☒ Disable ☐ Recurring ☐ Recurring EU ☐ Recurring USA ☐ Non Recurring

调整时间(单位: 分钟): (1 - 1440)

时区名称: (最大 31 个字符)

夏令时配置 - 工作状态

夏令时(DST)工作模式: Disabled

夏令时(DST)生效状态:

1. 单击 夏令时(DST)工作模式选中的单选按钮。

- **Disable.** 禁用夏令时。
- **Recurring.** 启用周期性夏令时。

- **Recurring EU.** 启用周期性EU夏令时。
- **Recurring USA.** 启用周期性美国夏令时。
- **Non Recurring.** 配置非周期性夏令时。

2. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

下表中的字段仅在夏令时制设定为 **Recurring** 或 **Recurring EU** 或 **Recurring USA** 可见。

表12. 夏令时-周期性使用

字段	描述
起始时间	这些字段用于配置日期和时间的开始值。 • Week. 配置开始周。 • Day. 配置开始日期。 • Month. 配置开始月份。 • Hours. 配置开始时间。 • Minutes. 配置开始分钟数。
结束时间	这些字段用于配置日期和时间的结束值。 • Week. 配置结束时的周数。 • Day. 配置结束时的日期。 • Month. 配置结束时的月份 • Hours. 配置结束时的小时数 • Minutes. 配置结束时的分钟数
调整时间	以分钟为单位配置周期性偏移量，有效范围为1-1440分钟。
时区名称	配置时区名称

下表中的字段仅在夏令时设定为 **Non Recurring** 时可见。

表13. 夏令时- Non Recurring

字段	描述
起始时间	这些字段用于配置日期和时间的开始值。 • Week. 配置开始周。 • Day. 配置开始日期。 • Month. 配置开始月份。 • Hours. 配置开始时间。 • Minutes. 配置开始分钟数。
结束时间	这些字段用于配置日期和时间的结束值。 • Week. 配置结束时的周数。 • Day. 配置结束时的日期。 • Month. 配置结束时的月份 • Hours. 配置结束时的小时数 • Minutes. 配置结束时的分钟数

调整时间	以分钟为单位配置周期性偏移量，有效范围为1-1440分钟。
时区名称	配置时区名称

夏令时配置 - 工作状态 ?

夏令时(DST)工作模式	Disabled
夏令时(DST)生效状态	

要更新屏幕信息，请单击 **刷新** 按钮。

表显示了启用夏令时（DST）状态信息。

表14. 夏令时状态

字段	描述
夏令时(DST)工作模式	显示夏令时的工作模式。
夏令时(DST)生效状态	显示当前时间夏令时是否有效。

2.2. 内置服务

2.2.1. DHCP 服务器

2.2.1.1. DHCP 服务器配置

系统管理 > 内置服务 > DHCP 服务器 > DHCP 服务器配置

The screenshot shows the 'DHCP 服务器配置' (DHCP Server Configuration) page. The left sidebar lists various services, with 'DHCP 服务器' (DHCP Server) selected. The main content area has tabs for '基本管理' (Basic Management), '设备面板' (Device Panel), and '内置服务' (Built-in Services). Under '内置服务', 'DHCP 服务器' is selected. The configuration fields include:

- 工作模式 (Work Mode):** Radio buttons for '关闭' (Disabled) and '启用' (Enabled). '关闭' is selected.
- Ping包文确认次数 (Ping Packet Confirmation Count):** A text input field with the value '2'. A note indicates the range is '(2-10, 0 to disable)'.
- 冲突地址LOG记录模式 (Conflict Address Log Recording Mode):** Radio buttons for '关闭' (Disabled) and '启用' (Enabled). '启用' is selected.
- Bootp自动模式 (Bootp Automatic Mode):** Radio buttons for '关闭' (Disabled) and '启用' (Enabled). '关闭' is selected.
- DHCP服务器配置 - 可分配地址排除列表 (DHCP Server Configuration - Assignable Address Exclusion List):** A table with two columns: '排除地址起始地址' (Exclusion Address Start Address) and '排除地址结束地址' (Exclusion Address End Address). There is one empty row for adding an exclusion.

1. 单击 工作模式 选项中， **关闭** 或 **启用** 单选按钮

这指定是启用还是禁用DHCP服务。默认值为禁用。

2. 在 **Ping包文确认次数** 字段中输入数值，指定服务器发送到池地址的包数，以检查是否存在重复IP地址，这是Ping操作的一部分

默认值为2。有效范围为0，2到10。将该值设置为0将禁用该功能。

3. 单击 **冲突地址LOG记录模式** 选项中的 **关闭 或 启用** 单选按钮
这指定是启用还是禁用DHCP服务器上的冲突日志记录。默认值为 启用。
4. 单击 **BootP 自动模式**选项中的 **关闭 或 启用** 单选按钮
这指定是启用还是禁用动态池的BootP。默认值为禁用。
5. 要排除不分配IP地址，请执行以下操作：
 - a. 在字段 **排除地址起始地址** 中，输入范围内的最低地址或要排除的单个地址。
 - b. 在字段**排除地址结束地址** 中，请输入范围中的最高地址。要排除单个地址，请输入与“排除地址起始地址”字段中指定的相同IP地址，或将其保留为0.0.0.0。
6. 单击 **增加** 按钮
排除地址或地址范围将添加到交换机中
7. To delete the exclude address from the switch, 请单击 **删除** 按钮
8. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效

2.2.1.2. DHCP 地址池配置

系统管理 > 内置服务 > DHCP 服务器 > DHCP 地址池配置

DHCP地址池配置 ?

地址池列表	Create ▾
地址池名称	(1 到 31 个字母数字字符)
地址分配方式	未分配 ▾
网络地址	
地址掩码	
客户名称	(0 到 31 个字母数字字符)
硬件地址	
硬件地址类型	▾
客户ID	(长度为0 to 255, 类似于 xx:xx:.....:xx:xx)
主机号	
主机掩码	
Host Prefix Length	(1-32)
租约期限	无限时间 ▾
天	(0 to 59)
小时	(0 to 23)
分钟	(0 to 59)
<u>缺省路由地址</u> ▸	
<u>DNS服务器地址</u> ▸	
<u>NetBIOS域名服务器地址</u> ▸	
NetBIOS节点类型	▾
下一个服务器地址	
域名服务器名称	(长度为0 到 255 个字符)
Bootfile文件名	(长度为0 到 128 个字符)

1. 单击 **增加** 按钮
- 添加新的地址池配置。
2. 要删除地址池，请单击 **删除** 按钮
3. 单击 **应用** 按键
- 更新的配置参数将发送到交换机，配置更改将立即生效。
- 下表介绍了DHCP池配置字段。

表15. DHCP池配置

字段	描述
地址池列表	对于具有读/写权限的用户，此字段显示所有现有池的名称以及附加选项 Create 。当用户选择“创建”时，会出现另一个文本框“池名称”，用户可以在其中输入要创建的池的名称。对于具有只读权限的用户，此字段仅显示现有池的名称。
地址池名称	要创建的池的名称。当具有读写权限的用户在池名称列表*中选择“创建”时，此字段出现。池名称的长度最多可以为 31 个字符。
地址分配方式	池的绑定类型： •未分配 •动态分配 •手动指定
网络地址	动态池的 DHCP 地址的子网地址。
地址掩码	动态池的 DHCP 地址的子网号。可以将网络掩码或前缀长度配置为指定子网掩码，但不能同时指定两者。
客户名称	DHCP 手动池的客户端名称。
硬件地址	DHCP 客户端硬件平台的 MAC 地址。
硬件地址类型	DHCP 客户端硬件平台的协议。有效类型为以太网和 ieee802 。默认值为以太网。
客户ID	DHCP 手动池的客户端标识符。
主机号	手动绑定到 DHCP 客户端的 IP 地址。仅当指定了 f 客户端标识符或硬件地址时，才能设置主机。删除主机将删除手动池的客户端名称、客户端 ID 和硬件地址，并将池类型设置为未分配。
主机掩码	手动绑定到 DHCP 客户端的子网掩码。可以将主机掩码或前缀长度配置为指定子网掩码，但不能同时指定两者。
Host Prefix Length	手动绑定到 DHCP 客户端的子网掩码。可以将主机掩码或前缀长度配置为指定子网掩码，但不能同时指定两者。有效范围为 0 到 32 。
租约期限	可以选择“无限”以将租赁时间指定为“无限”，也可以选择“指定持续时间”以输入特定租赁期。在动态绑定的情况下，无限意味着 60 天的租赁期，在手动绑定的情况下，无限意味着无限的租赁期。默认值是指定的持续时间。
租约期限，天数	租赁期的天数。仅当用户将指定的持续时间指定为租赁时间时，此字段才会显示。默认值为 1 。有效范围为 0 到 59 。
租约期限，小时数	租赁期的小时数。仅当用户将指定的持续时间指定为租赁时间时，此字段才会显示。有效范围为 0 到 22 。

租约期限，分钟数	租赁期的分钟数。仅当您将指定的持续时间指定为租赁时间时，此字段才会显示。有效范围为0到86399。
缺省路由地址	池的默认路由器地址列表。单击字段名称旁边的箭头以展开屏幕并显示一个表格，在该表格中，您最多可以按首选项的顺序指定八个默认路由器地址。
DNS服务器地址	池的DNS服务器地址列表。单击字段名称旁边的箭头以展开屏幕并显示一个表，在该表中，您最多可以按首选项的顺序指定八个DNS服务器地址。
NetBIOS域名服务器地址	池的NetBIOS名称服务器地址列表。单击字段名称旁边的箭头以展开屏幕并显示一个表，在该表中，您最多可以按首选项的顺序指定八个NetBIOS名称服务器地址。
NetBIOS节点类型	DHCP客户端的NetBIOS节点类型： •b节点广播 •p节点点对点 •m节点混合 •h节点混合
下一个服务器地址	池的下一个服务器地址。
域名服务器名称	DHCP客户端的域名。域名的长度最多可以为255个字符。
Bootfile文件名	DHCP客户端的默认启动映像的名称。文件名的长度最多为128个字符。

2.2.1.3. DHCP Options配置

系统管理 > 内部服务 > DHCP 服务器 > DHCP Options配置

1. 在列表 **地址池名称** 选项中，选择需要修改的地址池名称。
2. 在 **Option 值** 字段中，输入所选池配置的选项代码。
3. 在 **Option 类别** 字段中，根据为选定池配置的选项代码指定选项类型：
 - ASCII 字符串

- Hex 16进制数
 - IP 地址
4. 在 **Option 值内容** 字段内，输入为选定池配置的选项代码指定值。
5. 单击 **增加** 按钮
- 将为所选地址池添加Option代码。.
6. 要删除所选地址的 Option 代码，请单击 **删除** 按钮

2.2.1.4. DHCP服务器计数统计

系统管理 > 内置服务> DHCP 服务器 > DHCP服务器计数统计

DHCP服务器计数统计 - 地址绑定计数		?
自动绑定地址计数	0	
过期的绑定地址计数	0	
不完整消息计数	0	
DHCP服务器计数统计 - 接收报文		?
DHCPDISCOVER	0	
DHCPREQUEST	0	
DHCPDECLINE	0	
DHCPRELEASE	0	
DHCPINFORM	0	
DHCP服务器计数统计 - 发送报文		?
DHCPOFFER	0	
DHCPACK	0	
DHCPNAK	0	

下表介绍了DHCP服务器统计信息字段。

表16. DHCP服务器统计信息

字段	描述
自动绑定地址计数	DHCP服务器上的自动绑定数。
过期的绑定地址计数	DHCP服务器上过期的绑定数。
不完整消息计数	格式不完整或错误的消息数。
DHCPDISCOVER	DHCP服务器接收的DHCPDISCOVER消息数。
DHCPREQUEST	DHCP服务器接收的DHCPREQUEST消息数。
DHCPDECLINE	DHCP服务器接收的DHCPDecend消息数。

DHCPRELEASE	DHCP服务器接收的DHCPRELEASE消息数。
DHCPINFORM	DHCP服务器接收的DHCPInfo消息数。
DHCPOFFER	DHCP服务器发送的DHCPOFFER消息数。
DHCPACK	DHCP服务器发送的DHCPACK消息数。
DHCPNAK	DHCP服务器发送的DHCPNAK消息数。

2.2.1.5. DHCP地址分配信息

系统管理 > 内置服务 > DHCP 服务器 > DHCP地址分配信息



1. 要显示DHCP绑定信息，请选择以下单选按钮之一：

- 所有动态绑定的地址. 指定要显示或删除的所有动态绑定
- 指定的动态地址. 指定要显示或删除的特定动态绑定。

下表介绍了DHCP绑定信息字段。

表17. DHCP绑定信息

字段	描述
IPv4地址	客户端的IP地址。
硬件地址	客户端的硬件地址。
剩余租约时间	剩余的租赁时间以天、小时和分钟为单位dd:hh:mm格式。
类别	绑定类型：动态或手动。

2.2.1.6. DHCP地址冲突信息

系统管理 > 内置服务 > DHCP 服务器 > DHCP地址冲突信息



1. 要显示DHCP冲突信息，请选择以下单选按钮之一：

- 所有的冲突地址. 指定要删除的所有地址冲突。
- 指定的冲突地址. 指定要删除的特定动态绑定。

下表介绍了DHCP冲突信息字段。

表18. DHCP冲突信息

字段	描述
IPv4地址	DHCP服务器上记录的主机IP地址。
硬件地址	客户端的硬件地址。
侦测模式	在DHCP服务器上找到主机IP地址的方式。
侦测的时间	相对于系统启动时间，以N天NNh:NNm:NNs格式检测到冲突的时间。

2.2.2. DHCP L2中继代理

2.2.2.1. DHCP 中继全局配置

系统管理 > 内部服务 > DHCP L2中继代理 > DHCP 中继全局配置



1. 单击选项 工作模式 中， 关闭 或 启用 单选按钮

对于全局配置，这将启用或禁用交换机上的DHCP L2中继。默认设置为禁用。

2. 对于VLAN配置，VLAN ID 表栏显示交换机上配置的VLAN ID。

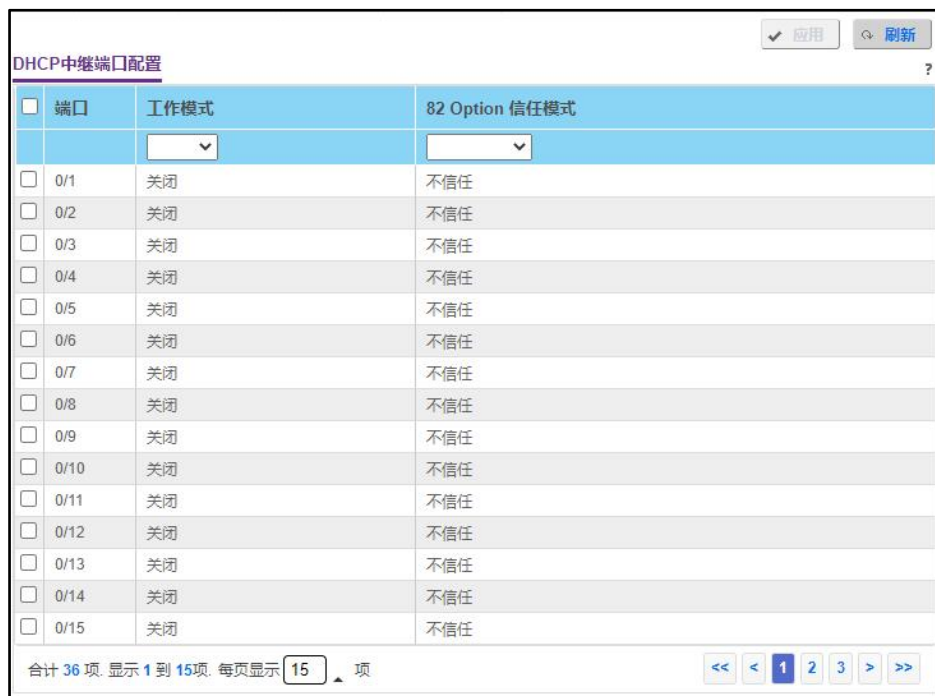
- 在表格中 工作模式 项中， 选择启用或禁用选定VLAN上的DHCP L2中继。
- 在表格中 **Circuit ID 模式** 项中， 选择启用或禁用DHCP的 Option-82
- 在表格中 Remote ID 模式 及 Remote ID 字符串 中，启用远程 ID 模式然后再设定远程 ID数值。

3. 单击 应用 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

2.2.2.2. DHCP中继端口配置

系统管理 > 内部服务 > DHCP L2中继代理 > DHCP中继端口配置



1. 在表格的 **工作模式** 选项中，选择启用或禁用所选接口上的DHCP L2中继。
默认设置为禁用。
2. 在表格的 **82 Option 信任模式** 选项中，选择是否信任接收到的DHCP L2中继 (Option2) 。

2.2.2.3. DHCP中继端口包文统计

系统管理 > 内部服务 > DHCP L2中继代理 > DHCP中继端口包文统计

DHCP中继端口包文统计					
☐	端口	携带Opt82信息, 非信任服务端	携带Opt82信息, 非信任客户端	未携带Opt82信息, 信任服务端	未携带Opt82信息, 信任客户端
☐	0/1	0	0	0	0
☐	0/2	0	0	0	0
☐	0/3	0	0	0	0
☐	0/4	0	0	0	0
☐	0/5	0	0	0	0
☐	0/6	0	0	0	0
☐	0/7	0	0	0	0
☐	0/8	0	0	0	0
☐	0/9	0	0	0	0
☐	0/10	0	0	0	0
☐	0/11	0	0	0	0
☐	0/12	0	0	0	0
☐	0/13	0	0	0	0
☐	0/14	0	0	0	0
☐	0/15	0	0	0	0
合计 36 项. 显示 1 到 15项. 每页显示 15 项				<< < 1 2 3 > >>	

下表介绍了DHCP L2中继接口统计字段。

表19. DHCP L2中继接口统计信息

字段	描述
端口	显示接收DHCP消息的接口。
携带Opt82信息, 非信任服务端	显示从不受信任的服务器接收的带有option82的DHCP消息数。
携带Opt82信息, 非信任客户端	显示从不受信任的客户端接收的带有option82的DHCP消息数。
未携带Opt82信息, 信任服务端	显示从受信任服务器接收的不带option82的DHCP消息数。
未携带Opt82信息, 信任客户端	显示从受信任客户端接收的不带option82的DHCP消息数。

2.2.3. IP Relay Agent

2.2.3.1. DHCP L3中继代理

系统管理 > 内部服务 > IP Relay Agent > DHCP L3中继代理



- 1. 在字段 **最大Hop数限制** 中，输入客户端请求在被丢弃之前可以进行的最大跃点数。范围是（1到16）。默认值为4。
- 2. 单击 **工作模式** 选择项中， **关闭** 或 **启用** 单选按钮
当您选择"启用"时，DHCP 请求将转发到您在"服务器地址"字段中输入的 IP 地址。
- 3. 在字段**最小等待时间** 中，输入最小等待时间（以秒为单位）。
此值与客户请求包中的时间戳进行比较，该时间戳表示客户端通电以来的时间。仅当时间戳超过最短等待时间时，才会转发数据包。范围是（0到100）。
- 4. 单击 **Circuit ID Option** 携带模式 选项中的， **关闭** 或 **启用** 单选按钮
如果您选择"启用"，则中继代理选项在转发到服务器之前会添加到请求中，并在回复转发给客户之前将其删除。

2.2.3.2. UDP 广播代理全局配置

系统管理 > 内部服务 > IP Relay Agent > UDP 广播代理全局配置



- 1. 单击选项 **工作模式** 中的， **关闭** 或 **启用** 单选按钮

这将启用或禁用交换机上的全局UDP中继功能。默认值为禁用。

2. 在表格中 **服务器地址** 项目中，指定x.x.x.x格式的UDP中继服务器地址。
3. 在表格中 **UDP 端口号** 项目中，指定UDP目标端口。

支持以下端口：

- **DefaultSet.** 中继UDP端口0数据包。如果在创建中继服务器时未选择UDP端口，则指定此选项。
 - **dhcp.** 中继DHCP（UDP端口67）数据包。
 - **domain.** 中继DNS（UDP端口53）数据包。
 - **isakmp.** 中继ISAKMP（UDP端口500）数据包。
 - **mobile-ip.** 中继移动IP（UDP端口434）数据包。
 - **nameserver.** 中继IEN-116名称服务（UDP端口42）数据包。
 - **netbios-dgm.** 中继NetBIOS数据报服务器（UDP端口138）数据包。
 - **netbios-ns.** 中继NetBIOS名称服务器（UDP端口137）数据包。
 - **ntp.** 中继网络时间协议（UDP端口123）数据包。
 - **pim-auto-rp.** 中继 pim-auto-rp（UDP端口496）数据包。
 - **rip.** 中继路由映像协议（RIP）（UDP端口520）数据包
 - **tacacs.** 中继TACACS（UDP端口49）数据包
 - **tftp.** 中继TFTP（UDP端口69）数据包
 - **time.** 中继时间服务（UDP端口37）数据包
 - **Other.** 如果选择此选项，则启用UDP端口其他值。此选项允许您在UDP端口其他值中输入自己的UDP端口。
4. 在表格中 **UDP 端口数值** 项目中，输入指定介于0和65535之间的UDP目标端口。
 5. 单击 **增加** 按钮

这将在具有指定配置的UDP中继表中创建一个条目。

6. 要从UDP中继表中删除所有条目或指定条目，请单击 **删除** 按钮

7. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

要更新屏幕信息显示，请单击 **刷新** 按钮。

2.2.3.3. UDP 广播代理端口配置

系统管理 > 内部服务 > IP Relay Agent > UDP 广播代理端口配置

+ 增加
- 删除
↻ 刷新

UDP 广播代理端口配置 ?

☐ 端口	服务器地址	UDP 端口号	UDP 端口数值	丢弃数	响应次数
v		v		v	

1. 在表格中 **端口** 项目中，选择要为UDP中继启用的接口。
2. 在表格中 **服务器地址** 项目中，指定x.x.x.x格式的UDP中继服务器地址。
3. 在表格中 **UDP 端口号** 项目中，指定UDP目标端口。

支持以下端口：

- **DefaultSet.** 中继UDP端口0数据包。如果在创建中继服务器时未选择UDP端口，则指定此选项。
- **dhcp.** 中继DHCP（UDP端口67）数据包。
- **domain.** 中继DNS（UDP端口53）数据包。
- **isakmp.** 中继ISAKMP（UDP端口500）数据包。
- **mobile-ip.** 中继移动IP（UDP端口434）数据包。
- **nameserver.** 中继IEN-116名称服务（UDP端口42）数据包。
- **netbios-dgm.** 中继NetBIOS数据报服务器（UDP端口138）数据包。
- **netbios-ns.** 中继NetBIOS名称服务器（UDP端口137）数据包。
- **ntp.** 中继网络时间协议（UDP端口123）数据包。
- **pim-auto-rp.** 中继 pim-auto-rp（UDP端口496）数据包。
- **rip.** 中继路由映像协议（RIP）（UDP端口520）数据包
- **tacacs.** 中继TACACS（UDP端口49）数据包
- **tftp.** 中继TFTP（UDP端口69）数据包
- **time.** 中继时间服务（UDP端口37）数据包
- **Other.** 如果选择此选项，则启用UDP端口其他值。此选项允许您在UDP端口其他值中输入自己的UDP端口。

4. 在表格中 **UDP 端口数值** 项目中，输入指定介于0和65535之间的UDP目标端口。
5. 在表格中 **丢弃** 项目中，选择是否删除匹配的数据包。
 仅当用户输入0.0.0.0 IP地址时才能选择启用。当用户添加具有非零IP地址的新条目时，可以将放弃模式设置为禁用。

6. 单击 **增加** 按钮
 这将在具有指定配置的UDP中继表中创建一个条目。

7. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

要从UDP中继接口配置表中删除所有条目或指定条目，请单击 **删除** 按钮。

表项 **响应次数** 中显示命中UDP端口的UDP数据包数。

要更新屏幕信息，请单击 **刷新** 按钮。

2.2.4. DHCPv6 Server

2.2.4.1. DHCPv6 Server Configuration

系统管理 > 内部服务 > DHCPv6 Server > DHCPv6 Server Configuration



1. 单击选项 工作模式 中的，**关闭** 或 **启用** 单选按钮

这指定是启用还是禁用DHCPv6服务管理模式。默认值为关闭。

2. 在 **DHCPv6 Server DUID** 字段中，显示定DHCPv6服务器的DHCP唯一标识符（DUID）。
3. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

2.2.4.2. DHCPv6 Pool Configuration

系统管理 > 内部服务 > DHCPv6 Server > DHCPv6 Pool Configuration



地址池选择 字段显示所有现有池的名称和 **Create** 选项。

提示： 如果您以具有只读权限的用户身份登录，则“池名称”字段仅显示现有池名称。要创建池，必须使用具有读/写权限的管理员用户名登录。

- 1. 要创建新的地址池，请选择 **Create** 项目，并输入标识要创建的DHCPv6服务器池的唯一名称。名称的长度最多可为31个字母数字字符。
- 2. 在字段 **DNS服务器地址** 中，指定池的默认DNS服务器地址列表。用户可以按首选顺序指定最多 8 个默认DNS服务器地址。
- 3. 在字段 **域名服务器名称** 中，指定此地址池的DHCPv6客户端域名数据。

域名的长度可达 255 个字母数字字符。

要删除交换机上的选定池，请单击 **删除** 按钮

- 4. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

2.2.4.3. DHCPv6 Pool Configuration

系统管理 > 内部服务 > DHCPv6 Server > DHCPv6 Pool Configuration



- 1. 在表项 **地址池名称** 中，单击选择需要修改的地址池。
- 2. 在表项 **Prefix/Prefix Length** 中，指定委派的IPv6前缀。
- 3. 在表项 **DUID** 中，指定用于标识客户端唯一DUID值的DUID标识符。
- 4. 在表项 **客户名称** 中，指定客户名称标识，这仅对日志记录或跟踪有用。名称最多可包含31个字母数字字符。
- 5. 在表项 **生存期时间** 中，指定委派地址的秒数。有效值为0到4294967295。
- 6. 在表项 **优先生存期** 中，指定委派地址的优先生存期。效值为0到4294967295。
- 7. 单击 **增加** 按钮

将为所选地址池添加分配前缀。

- 8. 要删除选定地址池的分配前缀，请单击 **删除** 按钮
- 9. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

2.2.4.4. DHCPv6 Interface Configuration

系统管理 > 内部服务 > DHCPv6 Server > DHCPv6 Interface Configuration

DHCPv6 Interface Configuration ?

☐	端口	Admin mode	地址池名称	Rapid Commit	优先权
☐					
☐	0/1	关闭			
☐	0/2	关闭			
☐	0/3	关闭			
☐	0/4	关闭			
☐	0/5	关闭			
☐	0/6	关闭			
☐	0/7	关闭			
☐	0/8	关闭			
☐	0/9	关闭			
☐	0/10	关闭			
☐	0/11	关闭			
☐	0/12	关闭			
☐	0/13	关闭			
☐	0/14	关闭			
☐	0/15	关闭			

合计 28 项. 显示 1 到 15 项. 每页显示 15 项

<< < 1 2 > >>

- 1. 在表格中 **Admin mode** 项目中，选择启用或禁用DHCPv6模式以配置服务器功能。

DHCPv6服务器和DHCPv6中继功能是互斥的。
- 2. 在表格中**地址池名称** 选项中，指定端口对应的包含无状态和/或前缀委派参数的DHCPv6池。
- 3. 在表格中 **Rapid Commit** 选项中，指定快速提交可选参数。在快速提交列表中，选择启用以允许在客户端和服务器之间进行简短的交换。
- 4. 在表格中 **Preference** 选项中，指定客户端用于确定DHCPv6服务器之间的首选项的首选项值。

有效值为0到4294967295。默认值为0。

- 5. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

2.2.4.5. DHCPv6 Bindings Information

系统管理 > 内部服务 > DHCPv6 Server > DHCPv6 Bindings Information



要更新屏幕信息，请单击 **刷新** 按钮。

下表描述了显示的不可配置字段。

表20. DHCPv6绑定信息

字段	描述
Client Address	与绑定关联的客户端的IPv6地址。
Client Interface	发生客户端绑定的接口号。
Client DUID	客户端的DHCPv6唯一标识符（DUID）。DUID是客户端硬件地址和客户端标识符的组合。
Prefix	与此绑定关联的委派前缀的IPv6地址。
Prefix Length	与此绑定关联的委派前缀的IPv6掩码长度。
Prefix Type	与此绑定关联的IPv6前缀的类型。
Expiry Time	与绑定关联的前缀过期之前的秒数。
Valid Lifetime	允许客户端使用前缀的最长时间（秒）。
Prefer Lifetime	允许客户端使用前缀的首选时间量（秒）。

2.2.4.6. DHCPv6 Server Statistics

系统管理 > 内部服务 > DHCPv6 Server > DHCPv6 Server Statistics

DHCPv6 Interface Selection

Interface

ALL ▼

Messages Received

Total DHCPv6 Packets Received	0
DHCPv6 Solicit Packets Received	0
DHCPv6 Request Packets Received	0
DHCPv6 Confirm Packets Received	0
DHCPv6 Renew Packets Received	0
DHCPv6 Rebind Packets Received	0
DHCPv6 Release Packets Received	0
DHCPv6 Decline Packets Received	0
DHCPv6 Inform Packets Received	0
DHCPv6 Relay-forward Packets Received	0
DHCPv6 Relay-reply Packets Received	0
DHCPv6 Malformed Packets Received	0
Received DHCPv6 Packets Discarded	0

Messages Sent

Total DHCPv6 Packets Sent	
DHCPv6 Advertisement Packets Transmitted	0
DHCPv6 Reply Packets Transmitted	0
DHCPv6 Reconfig Packets Transmitted	0
DHCPv6 Relay-forward Packets Transmitted	0
DHCPv6 Relay-reply Packets Transmitted	0

- 要查看界面的详细DHCPv6统计信息，请从 **Interface** 列表中选择要显示其数据的条目。
如果选择“ALL”，则显示所有接口的数据。

要重置一个或多个接口的DHCPv6计数器，请选择具有要重置的统计信息的每个接口，然后单击 **清除** 按钮。

要更新屏幕信息，请单击 **刷新** 按钮。

下表描述了显示的不可配置字段的数据。

表21. DHCPv6服务器统计信息

字段	描述
Messages Received	已接收消息的所有接口级统计信息的集合。

Total DHCPv6 Packets Received	在接口上接收的DHCPv6消息数。从DHCP v6客户端发送到DHCP v6服务器的DHCPv6消息包括请求、请求、确认、续订、重新绑定、释放、拒绝和信息请求消息。此外，DHCP v6中继代理可以将中继消息转发到DHCP v6服务器。
DHCPv6 Solicit Packets Received	在接口上接收的DHCPv6请求消息数。此类型的消息由客户端发送以定位DHCPv6服务器。
DHCPv6 Request Packets Received	请求的数量。
DHCPv6 Confirm Packets Received	在接口上接收的DHCPv6确认消息数。此类型的消息由客户端发送到所有DHCPv6服务器，以确定其配置是否对所连接的链路有效。
DHCPv6 Renew Packets Received	在接口上接收的DHCPv6续订消息数。此类型的消息由客户端发送，以扩展和更新DHCPv6服务器提供的配置信息。
DHCPv6 Rebind Packets Received	在接口上接收的DHCPv6重新绑定消息数。当客户端没有收到对续订消息的响应时，它会将此类消息发送到任何DHCPv6服务器。
DHCPv6 Release Packets Received	在接口上接收的DHCPv6发布消息数。这种类型的消息由客户端发送，以表明它不再需要指定的地址。
DHCPv6 Decline Packets Received	在接口上接收的DHCPv6拒绝消息数。这种类型的消息由客户端发送到DHCPv6服务器，以指示分配的地址已在链路上使用。
DHCPv6 Inform Packets Received	在接口上接收的DHCP v6信息请求消息数。此类型的消息由客户端发送，以请求IP地址分配以外的配置信息。
DHCPv6 Relay-forward Packets Received	在接口上接收的DHCPv6中继转发消息数。这种类型的消息由中继代理发送，以将消息转发到服务器。
DHCPv6 Relay-reply Packets Received	在接口上接收的DHCP v6中继回复消息数。此类型的消息由服务器发送到DHCP v6中继代理，并包含中继代理要传递到客户端的消息。
DHCPv6 Malformed Packets Received	在接口上接收但由于格式错误而被丢弃的DHCPv6消息数。
Received DHCPv6 Packets Discarded	丢弃的数据包数。
Messages Sent	已发送消息的所有接口级统计信息的集合。
Total DHCPv6 Packets Sent	接口发送的DHCPv6消息数。从DHCPv6服务器发送到DHCPv6客户端的DHCPv6消息包括播发、回复、重新配置和中继回复消息。
DHCPv6 Advertisement Packets Transmitted	接口发送的DHCPv6播发消息数。此类型的消息由服务器发送到DHCPv6客户端，以响应请求消息，并指示该消息可用于服务。

DHCPv6 Reply Packets Transmitted	为响应请求、请求、续订、重新绑定、信息请求、确认、发布或拒绝消息，从接口发送到DHCPv6客户端的DHCPv6回复消息数。
DHCPv6 Reconfig Packets Transmitted	接口发送的DHCPv6重新配置消息数。这种类型的消息由服务器发送到DHCPv6客户机，通知客户机服务器有新的或更新的信息。然后，客户机通常与服务器发起续订/回复或信息请求/回复事务，以接收更新的信息。
DHCPv6 Relay-forward Packets Transmitted	接口发送的DHCPv6中继转发消息数。这种类型的消息由中继代理发送，以将消息转发到服务器。
DHCPv6 Relay-reply Packets Transmitted	接口发送的DHCPv6中继回复消息数。此类型的消息由服务器发送到DHCPv6中继代理，并包含中继代理要传递到客户端的消息。

2.2.5. DHCPv6 Relay

系统管理 > 内部服务 > DHCPv6 Relay

DHCPv6 Relay Configuration

☐	端口	工作模式	Relay Interface	Destination IP Address	Remote ID
☐	0/1	关闭			
☐	0/2	关闭			
☐	0/3	关闭			
☐	0/4	关闭			
☐	0/5	关闭			
☐	0/6	关闭			
☐	0/7	关闭			
☐	0/8	关闭			
☐	0/9	关闭			
☐	0/10	关闭			
☐	0/11	关闭			
☐	0/12	关闭			
☐	0/13	关闭			
☐	0/14	关闭			
☐	0/15	关闭			

合计 28 项. 显示 1 到 15 项. 每页显示 15 项

<< < 1 2 > >>

- 在表格中 **工作模式** 字段，指定DHCPv6模式（启用或禁用），以配置DHCPv6中继功能。
默认设置为禁用。DHCPv6服务器和DHCPv6中继功能是互斥的。
- 在表格中 **Relay Interface** 字段，选择要连接中继服务器的接口。
- 在表格中 **Destination IP Address** 字段，指定要到达中继服务器的IPv6地址。

- 在表格中 **Remote ID** 字段，指定中继代理信息选项。

远程ID来自DHCPv6服务器DUID和中继接口号，也可以指定为用户定义的字符串。

- 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

2.3.DNS

2.3.1. DNS客户端配置

系统管理 > 基本管理 > DNS管理 > DNS客户端配置

The screenshot shows the 'DNS Client Configuration' page. It includes a sidebar with 'DNS Client Configuration' selected. The main area has two sections: 'DNS Client Configuration' and 'DNS Client Configuration - DNS Server Configuration'. The first section has fields for 'DNS Client Mode' (radio buttons for 'Enabled' and 'Disabled'), 'DNS Default Name' (text input), 'Retries' (text input), 'Response Timeout (unit: seconds)' (text input), and 'Source Port' (dropdown menu). The second section is a table for adding DNS servers with columns for 'Serial Number', 'DNS Server Address', and 'Priority'.

- 单击 **DNS工作模式** 选项中的 **关闭** 或 **启用** 单选按钮

- 启用. 允许交换机向DNS服务器发送DNS查询以解析DNS域名。默认值为启用。
- 关闭. 阻止交换机发送DNS查询。

- 在 **DNS默认名称** 表项中输入字符，为要包含在DNS查询中的域。

当系统对不合格的主机名执行查找时，此字段将提供域名（例如，如果默认域名为abc.com，并且用户输入test，则test将更改为test.abc.com以解析名称）。名称的长度不得超过255个字符。

- 使用 **重试次数** 字段，指定向DNS服务器发送DNS查询的重试次数。

此数字的范围为0到100。默认值为2。

- 使用 **响应超时** 字段，指定DNS查询等待响应的时间量（秒）。

此超时范围为0到3600。默认值为3。

- 使用 **查询的源端口** 要用于DNS的查询的源接口。

可能的值如下所示：

- None
- VLAN 1
- Routing interface
- Routing VLAN

- Routing loopback interface
- Tunnel interface
- Service port

默认情况下，VLAN 1用作源接口。

6. 要设定交换机向其发送DNS查询的DNS服务器，请在 **DNS服务器地址** 字段中以标准IPv4点符号输入IP地址，然后 单击 **增加** 按钮

服务器将显示在列表中。您最多可以指定八个DNS服务器。优先级是按照创建的顺序设置的。

7. 要从列表中删除DNS服务器，请选中其复选框并单击 **删除** 按钮。

8. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

要更新屏幕信息，请单击 **刷新** 按钮。

下表显示DNS服务器配置信息。

表22. DNS服务器配置

字段	描述
系列号	DNS服务器的序列号。
优先权	显示查询 DNS 服务器的优先首选项。首选项由输入的顺序决定。

2.3.2. 主机名称配置

系统管理 > 基本管理 > DNS管理 > 主机名称配置

主机名称配置 - DNS主机配置 ?

☐ 主机名称
 IPv4地址

主机名称配置 - 动态主机映射表 ?

主机名称	总数	经过时间	类别	IP地址

1. 在 **主机名称** 字段，输入要添加的静态主机名。其长度不能超过255个字符，并且是必填字段。

2. 在 **IPv4地址** 字段中，以标准IPv4点表示法输入与主机名关联的IP地址。

3. 单击 **增加** 按钮

该条目出现在屏幕上的列表中。

4. 在表格 **访问模式** 选项中，选择 **只读模式** 或 **读写模式** 或 **超级模式**

这将指定此团体的访问级别。.

5. 在表格 **状态** 字段中，显示此团体是否有效的状态。

6. 单击 **增加** 按钮

这会将所选团体数据添加到交换机。.

7. 要删除选定的团体名称， 请单击 **删除** 按钮

2.4.2. SNMP V3

2.4.2.1. 用户名配置

系统管理 > SNMP管理 > SNMP V3 >用户名配置

+ 增加- 删除刷新

用户名配置 - SNMP V3?

Engine ID 选择

☒ 本地值☐ 远程用户

Engine ID

8000113D03020000000000

用户名

本地组名称

(Local group:)

认证协议

无

密码

确认密码

加密模式

None

密钥值

确认密钥值

用户名配置 - SNMPv3 用户安全模式列表?

☐ 用户名本地组名称Engine ID认证模式加密模式

1. 在选项 **Engine ID 选择** 中，选择指定创建的用户是本地的还是 **traps**访问登录时所用的。
2. 在表项 **用户名** 中，输入用户帐户名称。

在**本地组名称** 字段中，输入对应的 Group 组，指示用户帐户的SNMPv3访问权限。管理员帐户具有读/写权限，所有其他帐户都被分配为只读权限。

3. 在列表选项 **认证协议** 中，选择此用户对应的认证协议。

有效的身份验证协议为 **None**, **MD5** 或 **SHA**:

- 如果选择 **None**, 用户将没有身份认证，此用户仅可以用于**SNMP v1/2** 协议。
- 如果选择 **MD5** 或 **SHA**, 用户登录密码将用作**SNMPv3**身份验证密码，因此必须指定密码，密码长度必须为8个字符。

这指定所选用户帐户的**SNMPv3**身份验证协议设置。

- 单击 **加密模式** 单选按钮，这将指定所选用户帐户的SNMPv3加密协议设置。

有效的加密协议为 **None or DES**:

- 如果选择**DES**协议，则必须在加密密钥字段中输入密钥。
- 如果没有为协议指定加密密钥，则忽略加密密钥。

- 如果选择了**加密模式** 选项中的 **DES**，请在 **密钥值/确认密钥值** 字段中输入DES密钥。

如果未选择DES，则忽略此字段。有效密钥的长度为0到15个字符。.

- 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

2.4.3. Trap消息配置

2.4.3.1. SNMP V1/V2 Trap 消息

系统管理 > SNMP管理 > Trap消息配置> SNMP V1/V2 Trap 消息

团体名称	消息版本	通知类别	协议	主机名称/IP地址	Filter	重试次数	超时	UDP端口

- 要添加接收SNMP Traps 的远程主机，请执行以下步骤：

- 团体名称.** 输入要发送到Traps管理器的SNMP Traps数据包的中团体字符串。此名称最多可包含16个字符，区分大小写。

- 消息版本.** 选择接收器要使用的SNMP版本：

- SNMP V1.** 使用SNMP V1向接收器发送 Traps 。
- SNMP V2.** 使用SNMP V2向接收器发送Traps 。

- 协议.** 选择接收器要使用的IP地址协议。

单击**IPv4** 选择接收方IP地址为**IPv4地址**，或者如果接收方地址为IPv6，则选择IPv6。

- 主机地址.** 输入x.x.x.x格式的IPv4地址或 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx中的IPv6地址，或 一个dns 主机名，以从此设备接收SNMP Traps。地址的长度不能超过39个字符。

- Filter.** 此管理器对应的 filter 表项。

- 重试次数,** 输入一个数值，当 traps 主机访问不成功时，重试的次数。

- 超时,** 输入一个数值，当 traps 主机访问时最大的等待相依时间。

h. **UDP端口**，输入1-65535的目的端口数值，访问traps 主机的目的 UDP端口号。

i. 单击 **增加** 按钮

2. 要修改现有SNMP Traps 接收的信息，请选中该 Traps 的复选框，然后更改所需字段。.

3. 要删除接收 traps ，请选中该traps的复选框，请单击 **删除** 按钮

4. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

2.4.3.2. Trap 消息类别

系统管理 > SNMP管理 > Trap消息配置> Trap 消息类别

Trap 消息类别 - SNMP Trap		?
交换机身份验证	☐ 关闭 ☒ 使能	
交换机端口状态	☐ 关闭 ☒ 使能	
Multiple Users	☐ 关闭 ☒ 使能	
生成树消息	☐ 关闭 ☒ 使能	
ACL消息	☒ 关闭 ☐ 使能	
Captive Portal	☒ 关闭 ☐ 使能	
DVMRP消息	☒ 关闭 ☐ 使能	
PIM消息	☒ 关闭 ☐ 使能	
电源模块状态消息	☐ 关闭 ☒ 使能	
温度报警消息	☐ 关闭 ☒ 使能	
风扇状态消息	☐ 关闭 ☒ 使能	
BGP消息	☒ 关闭 ☐ 使能	

1. 单击 交换机身份验证 选项中， **关闭 或 启用** 单选按钮

这将启用或禁用身份验证失败Traps的激活。出厂默认设置为启用。

2. 单击 交换机端口状态 选项中， **关闭 或 启用** 单选按钮

这将启用或禁用链路状态Traps的激活。出厂默认值为启用。

3. 单击 Multiple Users 选项中， **关闭 或 启用** 单选按钮

这将启用或禁用多个用户Traps的激活。出厂默认值为启用。当同一用户ID同时多次登录交换机（通过Telnet或串行端口）时，会触发此Traps。

4. 单击 生成树消息 选项中， **关闭 或 启用** 单选按钮

这将启用或禁用生成树Traps的激活。出厂默认设置为启用。

5. 单击 ACL消息 选项中， **关闭 或 启用** 单选按钮

这将启用或禁用ACL Trpas的激活。出厂默认设置为禁用。.

6. 单击 PoE消息 选项中， 关闭 或 启用 单选按钮
- 这将启用或禁用PoE Traps的激活。出厂默认设置为启用。指示是否发送PoE Traps 消息。
7. 单击 应用 按键
- 更新的配置参数将发送到交换机，配置更改将立即生效。

2.4.4. MIBS支持列表

系统管理 > SNMP管理 > MIBS支持列表

MIBS支持列表 - 列表	
Name	Description
RFC 1907 - SNMPv2-MIB	The MIB module for SNMPv2 entities
HC-RMON-MIB	The original version of this MIB, published as RFC3273.
HCNUM-TC	A MIB module containing textual conventions for high capacity data types.
SNMP-COMMUNITY-MIB	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3.
SNMP-MPD-MIB	The MIB for Message Processing and Dispatching
SNMP-TARGET-MIB	The Target MIB Module
SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-based Access Control Model for SNMP.
SFLOW-MIB	sFlow MIB
FASTPATH-ISDP-MIB	Industry Standard Discovery Protocol MIB
FASTPATH-BOXSERVICES-PRIVATE-MIB	The Broadcom Private MIB for FASTPATH Box Services Feature.
IANA-ADDRESS-FAMILY-NUMBERS-MIB	The MIB module defines the AddressFamilyNumbers textual convention.
FASTPATH-DHCPCLIENT-PRIVATE-MIB	The Broadcom Private MIB for FASTPATH DHCP Client
FASTPATH-DENIALOFSERVICE-PRIVATE-MIB	The Broadcom Private MIB for FASTPATH Denial of Service.
LLDP-MIB	Management Information Base module for LLDP configuration, statistics, local system data and remote systems data components.
LLDP-EXT-MED-MIB	The LLDP Management Information Base extension module for TIA-TR41.4 Media Endpoint Discovery information.
合计 49 项, 显示 1 到 15项, 每页显示 15 项	

下表介绍了SNMP支持的MIB状态字段。

表24. SNMP支持的MIB

字段	描述
Name	RFC编号（如适用）和MIB的名称。
Description	RFC标题或MIB说明。

系统管理 > LLDP > Global Configuration

全局配置 - LLDP全局参数配置

发送间隔时间

30

(5 - 32768 秒)

发送包文中TTL倍数

4

(2 - 10)

重新初始化延迟时间

2

(1 - 10 秒)

通告时间间隔

5

(5 - 3600 秒)

1. 在 发送间隔时间 字段中，以秒为单位输入传输LLDP帧的间隔。
- 范围为5到32768秒。默认值为30秒。

2. 在 **发送包文中TTL倍数** 字段中，输入传输间隔上的乘数以分配TTL。

The range is from 2 to 10 secs. The default value is 4.

3. 在 **重新初始化延迟** 字段中，输入重新初始化前的延迟。

The range is from 1 to 10 secs. The default value is 2 seconds.

4. 在 **通告间隔** 字段中，输入以秒为单位的通告传输间隔。

范围为5到3600秒。默认值为5秒。

5. 单击 **应用** 按键

更新的配置将发送到交换机。更改将立即生效，但除非执行保存，否则不会在整个电源循环中保留更改。

2.5.LLDP管理

IEEE 802.1AB 定义的标准链接层发现协议（LLDP），允许 802 局域网上的站点发布其对应的主要功能和物理描述。网络管理器可以查看此信息以识别系统拓扑并检测局域网上的不良配置。

LLDP 是单向协议，没有数据请求/响应序列。信息由执行传输功能的站点进行通告发送消息，由执行接收功能的站点接收和处理接收的消息。每个端口可分别启用/禁用传输和接收功能。默认情况下，所有端口上的传输和接收均禁用。该应用程序负责根据端口的配置状态和运行状态，独立的启动每个传输和接收状态机。

链路层发现协议媒体端点发现（LLDP-MED）是对LLDP的增强，具有以下功能：

- 自动发现LAN策略（如VLAN、第2层优先级和区分服务设置），支持即插即用网络。
- 用于创建位置数据库的设备位置发现。
- 通过以太网端点扩展和自动电源管理。
- 库存管理，使网络管理员能够跟踪其网络设备并确定其特征（制造商、软件和硬件版本、序列号/资产编号）。

2.5.1. 全局配置

系统管理 > LLDP管理 > 全局配置

全局配置 - LLDP全局参数配置

发送间隔时间	30 (5 - 32768 秒)
发送包文中TTL倍数	4 (2 - 10)
重新初始化延迟时间	2 (1 - 10 秒)
通告时间间隔	5 (5 - 3600 秒)

1. 发送间隔，默认30s，范围5-32768秒。
2. 发送报文中TTL倍数，默认4，范围2-4。
3. 重新初始化延迟时间，默认2s，范围1-10秒
4. 通告时间间隔，默认5秒，范围5-3600秒。.

2.5.2. 端口配置

系统管理 > LLDP管理 > 端口配置

端口配置 - LLDP管理

端口	发送包文	接收报文	通告报文	发送设备管理信息	TLV(s)可选参数				
					系统名称	系统描述	系统兼容特性	端口名称描述	Port ID
☐ 0/1	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/2	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/3	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/4	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/5	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/6	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/7	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/8	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/9	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/10	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/11	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/12	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/13	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/14	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name
☐ 0/15	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Disable	Port Name

合计 28 项. 显示 1 到 15 项. 每页显示 15 项

5. 在最左侧的多选项中选择端口，指定可以配置的LLDP - 802.1AB的端口列表项。
6. 使用 发送报文 为所选接口指定LLDP-802.1AB传输模式。
7. 使用 接收报文 为所选接口指定LLDP-802.1AB接收模式。.
8. 使用 通告报文 为所选接口指定LLDP-802.1AB通知模式。.
9. 可选 TLV 信息：

- 使用端口描述在LLDP帧中包括端口描述TLV。
- 使用系统名称在LLDP帧中包括系统名称TLV。
- 使用系统兼容特性将系统描述TLV包含在LLDP框架中。
- 使用端口名称描述将端口名称描述信息TLV包括在LLDP框架中。
- 选择使用Port ID将端口名称或MAC地址信息TLV包括在LLDP框架中。

10. 使用 发送设备管理信息 指定是否在所选接口的LLDP帧中传输管理地址。

2.5.3. LLDP报文统计

系统管理 > LLDP > Statistics.

LLDP报文统计 - LLDP管理

最近更新信息时间	0 days 00:00:00
远端设备记录数据统计	0
删除远端设备记录统计	0
丢弃远端设备记录统计	0
远端设备记录时效过期删除数统计	0

LLDP报文统计 - LLDP端口信息

端口	发送报文数	接收报文数	丢弃报文数	错误报文数	时效过期条目	TLV丢弃数	无法识别TLV数	TLV MED数	TLV 802.1数	TLV 802.3数
0/1	0	0	0	0	0	0	0	0	0	0
0/2	0	0	0	0	0	0	0	0	0	0
0/3	0	0	0	0	0	0	0	0	0	0
0/4	0	0	0	0	0	0	0	0	0	0
0/5	0	0	0	0	0	0	0	0	0	0
0/6	0	0	0	0	0	0	0	0	0	0
0/7	0	0	0	0	0	0	0	0	0	0
0/8	0	0	0	0	0	0	0	0	0	0

下表介绍了LLDP统计字段显示信息。

表25. LLDP Statistics

字段	描述
最近更新信息时间	在与远程系统关联的表中创建、修改或删除条目的时间。
远端设备记录数据统计	特定MAC服务接入点（MSAP）发布的完整信息集插入与远程系统相关联的表的次数。
删除远端设备记录统计	从与远程系统关联的表中删除特定MAC服务访问点（MSAP）公布的完整信息集的次数。
丢弃远端设备记录统计	由于资源不足，特定MAC服务访问点（MSAP）播发的完整信息集无法输入到与远程系统关联的表中的次数。
远端设备记录时效过期删除数统计	由于信息及时性间隔已过期，特定MAC服务接入点（MSAP）播发的完整信息集从与远程系统相关联的表中删除的次数。
端口	接口的单元/插槽/端口。

发送报文数	LLDP代理在相应端口上传输的LLDP帧数。
接收包文数	启用LLDP代理时，此LLDP代理在相应端口上接收的有效LLDP帧数。
丢弃包文数	相应端口上LLDP代理出于任何原因丢弃的LLDP TLV数。
错误包文数	启用LLDP代理时，LLDP代理在相应端口上接收的无效LLDP帧数。
时效过期条目	给定端口上发生的过期数。过时是指由于信息时效性间隔过期，特定MAC服务访问点（MSAP）播发的完整信息集从与远程条目相关联的表中删除的次数。
TLV丢弃数	相应端口上LLDP代理出于任何原因丢弃的LLDP TLV数。
无法识别TLV数	在本地端口上接收的LLDP TLV的数量，这些端口未被相应端口上的LLDP代理识别。
TLV MED数	在本地端口上接收的LLDP-MED TLV总数。
TLV 802.1	在802.1类型的本地端口上接收的LLDP TLV总数。
TLV 802.3	在802.3类型的本地端口上接收的LLDP TLV总数。

2.5.4. 本地设备信息

系统管理 > LLDP > 本地设备信息

LLDP本地设备信息 - 选择LLDP端口 ?

Interface: 0/1

LLDP本地设备信息 - LLDP管理 ?

工作状态	Transmit Receive
Chassis ID 信息类别	MAC Address
Chassis ID 数据	02:00:00:00:00:00
Port ID 信息类别	Interface Name
Port ID 数据	0/1
系统名称	
系统描述	Broadcom 53346 - 24 GE + 4 SFP+, 1.0.2.1
端口名称描述	
本地设备支持的系统能力	bridge, router
本地设备启用的系统能力	bridge
本地设备管理地址	02:00:00:00:00:00
本地设备管理地址的类别	802

1. 在接口列表中，选择可以发送LLDP-802.1AB帧的端口的本地发送信息。

下表介绍了LLDP本地设备信息字段。

表26. LLDP本地设备信息

字段	描述
Chassis ID信息类别	描述机箱标识符来源的字符串。
Chassis ID	用于标识与本地系统关联的机箱组件的字符串值。
Port ID信息类别	描述端口标识符源的字符串。
Port ID	描述端口标识符源的字符串。
系统名称	本地系统的系统名称。
系统描述	与本地系统关联的选定端口的说明。
端口名称描述	与本地系统关联的选定端口的说明。
本地设备支持的系统能力	本地系统的系统功能。
本地设备启用的系统能力	支持和启用的本地系统的系统功能。
本地设备管理地址	管理地址的类型。
本地设备管理地址的类别	本地系统的公布管理地址。

2.5.5. LLDP远端设备信息

系统管理 > LLDP管理 > LLDP远端设备信息

LLDP远端设备信息 - 选择LLDP端口 ?

Interface:

0/1 ▼

1. 使用接口选择允许接收LLDP帧的本地端口，对应的远端设备信息。

下表介绍了LLDP远端设备信息字段。

表27. LLDP远端设备信息

字段	描述
Remote ID	The remote ID.
Chassis ID数据	与远程系统关联的机箱组件。
Chassis ID 信息类别	机箱标识符的源。
Port ID 数据	与远程系统关联的端口组件。
Port ID 信息类别	端口标识符的源。
系统名称	远程系统的系统名称。
系统描述	与远程系统关联的给定端口的说明。
端口名称描述	与远程系统关联的给定端口的说明。
本地设备支持的系统能力	远程系统的系统功能。
本地设备启用的系统能力	支持和启用的远程系统的系统功能。
接收到的远程条目的生存时间值 (秒)	接收到的远程条目的生存时间值（以秒为单位）。
本地设备管理地址	管理地址的类型。
本地设备管理地址的类别	•管理地址。远程系统的播发管理地址。 •类型。管理地址的类型。

2.5.6. LLDP远端设备信息

系统管理 > LLDP管理 > LLDP远端设备统计表

LLDP远端设备统计表 - LLDP管理 ?

端口	远端设备ID	本地设备管理地址	远端设备MAC地址	系统名称	远端设备Port ID

下表介绍了LLDP远端设备资源清单字段信息。

表28. LLDP远端设备清单

字段	描述
端口	启用LLDP帧的所有端口的列表。
远端设备 ID	远程设备ID。
本地设备管理地址	远程系统的播发管理地址。
远端设备MAC地址	与远程系统关联的MAC地址。
系统名称	指定远程设备的型号名称。
远端设备Port ID	与远程系统关联的端口组件。

2.5.7. LLDP-MED

2.5.7.1. 全局配置

系统管理 > LLDP管理 > LLDP-MED >全局配置

全局配置 - LLDP-MED ?

发送PDU包文重复次数	3 (1 to 10)
本地设备的MED分类	Network Connectivity

1. 在 发送PDU包文重复次数 字段中，输入协议启用时传输的LLDP PDU数量。
范围为（1到10）。快速重复计数的默认值为3。
- 设备类别字段指定本地设备的MED分类。有四种不同类型的设备，其中三种代表实际端点（分类为I类通用[IP通信控制器等]、II类媒体[会议桥等]、III类通信[IP电话等]）。第四个设备是网络连接设备，它通常是LAN交换机/路由器、IEEE 802.1网桥、IEEE 802.11无线接入点等。

2.5.7.2. 端口配置

系统管理 > LLDP管理 > LLDP-MED > 端口配置

端口配置 - LLDP-MED											
☐	端口	连接状态	MED模式	MED工作状态	通告模式	发送TLV数据选择					
						MED能力	网络策略	本地信息	扩展PSE	扩展PD	设备清单信息
☐	0/1	Detach	Enable	Disabled	Disable	Enable	Enable	Disable	Disable	Disable	Disable
☐	0/2	Detach	Enable	Disabled	Disable	Enable	Enable	Disable	Disable	Disable	Disable
☐	0/3	Detach	Enable	Disabled	Disable	Enable	Enable	Disable	Disable	Disable	Disable
☐	0/4	Detach	Enable	Disabled	Disable	Enable	Enable	Disable	Disable	Disable	Disable
☐	0/5	Detach	Enable	Disabled	Disable	Enable	Enable	Disable	Disable	Disable	Disable
☐	0/6	Detach	Enable	Disabled	Disable	Enable	Enable	Disable	Disable	Disable	Disable
☐	0/7	Detach	Enable	Disabled	Disable	Enable	Enable	Disable	Disable	Disable	Disable
☐	0/8	Detach	Enable	Disabled	Disable	Enable	Enable	Disable	Disable	Disable	Disable
☐	0/9	Detach	Enable	Disabled	Disable	Enable	Enable	Disable	Disable	Disable	Disable
☐	0/10	Detach	Enable	Disabled	Disable	Enable	Enable	Disable	Disable	Disable	Disable
☐	0/11	Detach	Enable	Disabled	Disable	Enable	Enable	Disable	Disable	Disable	Disable

链路状态字段显示端口的链路状态（连接Up 或 断开Down）。

MED工作状态字段显示LLDP-MED TLV是否在此接口上传输。

1. 使用接口指定选择需要配置LLDP-MED-802.1AB的端口列表。
2. 使用 **MED 模式** 指定在此接口上启用还是禁用LLDP-MED模式
3. 使用 **通告模式** 指定接口的LLDP-MED拓扑通知模式。
4. 使用 **发送TLV数据选择** 中指定在选定接口的LLDP PDU帧中传输LLDP-MED中的哪些可选类型长度值（TLV）：
 - **MED 能力.** 在LLDP帧中传输 MED 信息.
 - **网络策略.** 在LLDP帧中传输 网络策略信息
 - **本地信息.** 在LLDP帧中传输 本地信息
 - **扩展 MDI - PSE.** 在LLDP帧中传输扩展PSE信息
 - **扩展MDI - PD.** 在LLDP帧中传输扩展PD信息
 - **设备清单信息.** 在LLDP帧中传输设备清单信息

2.5.7.3. LLDP-MED本地设备信息

系统管理 > LLDP管理 > LLDP-MED > LLDP-MED本地设备信息

LLDP-MED本地设备信息 - 选择LLDP-MED端口 ?

端口

0/1 ▾

LLDP-MED本地设备信息 - 网络策略信息 ?

发送的媒体信息	VLAN ID	Priority	DSCP	Unknown bit Status	Tagged Bit Status
---------	---------	----------	------	--------------------	-------------------

LLDP-MED本地设备信息 - 设备清单信息 ?

硬件版本	
固件版本	
应用软件版本	
序列号	
制造商	
设备型号	
指定的设备ID	

LLDP-MED本地设备信息 - 定位信息 ?

信息类别	定位信息内容
------	--------

LLDP-MED本地设备信息 - 扩展PoE信息 ?

1. 使用接口选择允许传输LLDP-MED帧的端口。

下表介绍了LLDP-MED本地设备信息字段

表29. LLDP-MED本地设备信息

字段	描述
网络策略信息：指定LLDP帧中是否存在网络策略TLV。	
发送的媒体信息	应用程序类型。应用程序类型的类型未知：语音信号、来宾语音、来宾语音信号、软电话语音、视频会议、流媒体视频、视频信号。 接收到的每个应用程序类型都具有VLAN ID、优先级、DSCP、标记位状态和未知位状态。一个端口可以接收一个或多个这样的应用程序类型。 如果传输了网络策略TLV，则仅此信息才会显示。
资产信息：指定资产信息TLV是否存在于LLDP帧中	
硬件版本	指定硬件版本。

固件版本	指定固件版本。
应用软件版本	指定软件版本。
序列号	指定序列号。
制造商	指定制造商名称。
设备型号	指定模型名称。
指定的设备ID	指定资产ID。
位置信息：指定LLDP帧中是否存在位置TLV。.	
信息类别	指定位置信息的类型。
定位信息内容	位置信息作为给定类型的位置ID的字符串显示。

2.5.7.4. LLDP-MED远端设备信息

系统管理 > LLDP管理 > LLDP-MED > LLDP-MED远端设备信息

LLDP-MED远端设备信息 - 选择LLDP-MED端口
?

端口
0/1

LLDP-MED远端设备信息 - 系统能力
?

远端设备支持的系统能力
远端设备启用的系统能力
本地设备的MED分类

LLDP-MED远端设备信息 - 网络策略信息
?

发送的媒体信息
VLAN ID
Priority
DSCP
Unknown bit Status
Tagged Bit Status

LLDP-MED远端设备信息 - 设备清单信息
?

硬件版本
固件版本
应用软件版本
序列号
制造商
设备型号
指定的设备ID

LLDP-MED远端设备信息 - 定位信息
?

信息类别
Location Information

LLDP-MED远端设备信息 - 扩展PoE信息
?

1. 使用接口选择启用LLDP-MED功能的端口，显示其接收到对端设备的信息。

下表介绍了LLDP-MED远程设备信息字段。

表30. LLDP-MED远程设备信息

字段	描述
性能支持信息：此端口上的MED TLV中接收到的受支持和启用的功能。	
支持的功能	指定在此端口上在MED TLV中接收到的受支持功能。
启用的功能	指定在此端口上在MED TLV中接收到的已启用功能。
设备类	指定远程连接到端口的设备播发的设备类别。
网络策略信息：指定此端口上的LLDP帧中是否接收到网络策略TLV。.	
媒体应用程序类型	应用程序类型。应用程序类型的类型未知：语音信号、来宾语音、来宾语音信号、软电话语音、视频会议、流媒体视频、视频信号。接收到的每个应用程序类型都具有VLAN ID、优先级、DSCP、标记位状态和未知位状态。一个端口可以接收一个或多个这样的应用程序类型。如果在此端口上接收到网络策略TLV，则只会显示此信息。
VLAN Id	与特定策略类型关联的VLAN ID。
Priority	与特定策略类型关联的优先级。
DSCP	与特定策略类型关联的DSCP。
Unknown Bit Status	与特定策略类型关联的未知位。
Tagged Bit Status	与特定策略类型关联的标记位。
资产信息：指定是否在此端口上的LLDP帧中接收资产TLV。	
硬件修订	指定远程设备的硬件版本。
固件版本	指定远程设备的固件版本。
软件修订	指定远程设备的软件版本。
序列号	指定远程设备的序列号。
制造商名称	指定远程设备的制造商名称。
型号名称	指定远程设备的型号名称。
资产ID	指定远程设备的资产ID。
位置信息：指定是否在此端口上的LLDP帧中接收位置TLV。	
子类型	指定位置信息的类型。
位置信息	位置信息作为给定类型的位置ID的字符串显示。
扩展POE：指定远程设备是否为POE设备。	
设备类型	指定连接到此端口的远程设备的PoE设备类型。
扩展POE PSE：指定是否在此端口上的LLDP帧中接收扩展PSE TLV	

Available	远程端口的功率值以十分之一瓦为单位。
Source	远程端口是电源。
Priority	远程端口具有电源优先级。
扩展POE PD：指定是否在此端口上的LLDP帧中接收扩展PD TLV。	
Required	远程端口的PD电源要求。
Source	远程端口的PD电源。
Priority	远程端口的PD电源优先级。

2.5.7.5. LLDP-MED远端设备统计表

系统管理 > LLDP管理 > LLDP-MED > LLDP-MED远端设备统计表

LLDP-MED远端设备统计表 - LLDP-MED				
端口	远程设备名称	指定的设备ID	设备型号	应用软件版本

下表介绍了LLDP-MED远端设备清单字段。

表31. LLDP-MED远端设备清单

字段	定义
端口	启用LLDP-MED的所有端口的列表。
远程设备名称	远程系统的设备名称。
指定的设备ID	与远程系统关联的设备ID值。
设备型号	指定远程设备的型号名称。
应用软件版本	指定远程设备的软件版本。

2.6.POE

系统管理 > PoE > Basic > PoE Configuration

PoE Configuration

1 All

	Unit	Model	Host	Status	Firmware Version	Power Status	Total Power (Main AC) Watt	Total Power (RPS) Watt	Power Source	Threshold Power mW	Consumed Power mW	System Usage Threshold (1% to 99%)
	1		XCM8948						PD (0/2)			90

1 All

Unit Selection 字段显示当前PoE单元。

1. 如果需要修改PoE单元，请在列表中选择其他单元。
2. 设置系统管理**Usage Threshold**,输入一个数字从1到99。
如果消耗的功率大于阈值功率，则设置发送trap的阈值水平。
3. 电源管理模式描述 **Power Management mode**或控制电源管理算法，PSE使用该算法向请求的pd下发电源。
单击静态表明权力分配给每个端口的类型取决于功率阈值配置的端口。单击动态表明每个端口上的功耗测量和实时计算。
4. 如果需要设置trap，选择“**Enable**”，激活PoE trap。
单击**Disable**,禁用PoE trap。默认设置为启用。
5. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

“PoE配置”不可配置字段说明如下表所示。

表32. PoE Configuration nonconfigurable Fields

字段	描述
Units	当前PoE单元。您可以通过选择此处列出的其他单元号来更改PoE单元。
Firmware Version	PoE控制器的FW镜像版本。
Power Status	电源状态。
Total Power (Main AC)	主交流电源提供的总功率。
Total Power (RPS)	由冗余电源提供的总功率。
Power Source	系统电源的电流来源(主交流或RPS)。
Threshold Power	系统管理可以启动一个端口,如果消耗功率小于这个权力。功耗可以在“标称功率”和“阈值功率”之间。阈值功率值是影响通过改变系统管理使用阈值。
Consumed Power	当前所有端口供电的总功率。

系统管理 > PoE > **高级管理** > PoE Port Configuration

PoE Port Configuration

1 All

Go To Port

☐	Port	Admin Mode	High Power	Max Power (mW)	Port Priority	High Power Mode	Power Limit Type	Power Limit (mW)	Detection Type	Class	Timer Schedule	Output Voltage (Volts)	Output Current (mA)	Output Power (mW)	Temperature	Status	Fault Status
☐																	

1 All

Go To Port

1. 单击**Admin mode (Enable or Disable)** 来确定端口提供电力的能力。

2. “端口优先级”用于确定当系统总供电功率超过阈值时，哪些端口可以供电。

如果交换机不能为所有连接的设备供电，则优先级决定哪些端口可以供电。具有相同端口优先级设置的最低编号的端口具有更高的优先级。从下面的列表单击优先顺序：

- Low**。低优先级

- Medium**。中优先级

- High**。高优先级

- Critical**。关键的优先级

3. 单击高功率模式从以下选项：

- Disabled**表示端口在IEEE 802.3af模式下通电。

- Legacy**表示该端口使用高涌流供电，由Legacy PD使用，从上电开始功率要求大于15W。

- “Pre-802.3at”**表示端口最初是在IEEE 802.3af模式下供电，在75msec之前切换到大功率的IEEE 802.3at模式。如果PD没有执行第2层分类或PSE正在执行2-事件第1层分类，则必须选择此模式。

- “802.3at”**表示端口供电模式为“IEEE 802.3at”。例如，如果PSE检测到的类不是class4，则PSE端口不会启动PD。

4. “功率限制类型”用于描述或控制端口所能提供的最大功率。从下面的列表单击类型：

- Class**表示端口的功率限制等于所附PD的等级。

- “User”**表示端口的功率限制等于“power limit”的值。

- 无表示端口在低功耗模式下达到0类最大功率，在高功率模式下达到4类最大功率。

5. 单击功率极限定义的最大力量(瓦),可以由一个端口。

6. 检测类型描述PSE端口执行的PD检测机制。

- pre-ieee**。只进行遗留检测。

- ieee**。4点电阻检测完成。

- 汽车**。4点电阻检测，然后是遗留检测。

- 4point and Legacy**表示使用电阻式4点检测方案，当检测到连接的PD失败时，使用Legacy电容检测方案。

7. 定时器时间表定义了分配给端口的定时器时间表。单击没有删除定时器安排任务。

8. 单击“重置”，强制重置PSE端口。

9. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

“PoE配置”不可配置字段说明如下表所示。

表33. PoE Configuration

字段	描述
Port	显示或配置数据的接口。
High Power	当特定端口支持高功率模式时启用
Max Power	端口所能提供的最大功率，单位为瓦。
Class	类定义了PD从系统中获得的功率范围。类定义： 0 - 0.44-12.95(瓦) 1 - 0.44-3.83(瓦) 2 - 0.44-6.48(瓦) 3 - 0.44-12.95(瓦) 4- 0.44-25.5(瓦)
Output Voltage	传送到装置上的电流电压以伏特为单位。
Output Current	电流以毫安单位被输送到设备。
Output Power	输送到设备的电流单位为瓦。
Status	状态为端口PD检测的运行状态。 • Disabled 。没有能量被传递。 • DeliveringPower 。电力正在被设备吸收。 • Fault 。表示端口有问题。 • Test 。端口处于测试模式。 • otherFault 。告警解释错误导致端口空闲。 Searching 。端口不是上述状态之一。
Fault Status	描述PSE端口处于故障状态时的错误描述。 • No Error 。PSE端口没有任何错误状态。 • MPS Absent 。PSE端口检测到主电源缺失。 • Short 。PSE端口检测到短路情况。 • Overload 。连接到PSE端口的PD试图提供超过硬件允许的功率。 • Power Denied 。由于电力不足或行政行为，PSE港口被拒绝供电。

2.7.ISDP管理

2.7.1. 基本管理

系统管理 > ISDP管理 > 基本管理 > 全局配置

全局配置 - ISDP	
工作模式	☐ 关闭 ☒ 启用
发送间隔时间	30 (5 - 254 秒)
保持时间	180 (10 - 255 秒)
发送Version 2包文	☐ 关闭 ☒ 启用
对端最近更新数据时间	0 days 00:00:00
设备ID	BCM-53346-28
支持的设备ID类别	Serial Number, Host Name
使用中的设备ID	Serial Number

1. 选择 **工作模式** 中， **关闭** 或 **启用** 单选按钮
这指定是启用还是禁用ISDP服务。默认值已禁用。
2. 使用 **发送间隔时间** 指定发送新ISDP数据包之间的时间段。
范围为5到254秒。默认值为30秒。
3. 使用 **保持时间** 指定交换机传输的ISDP数据包的保持时间。
保持时间指定接收设备在丢弃ISDP数据包之前必须存储ISDP数据包中发送的信息的时间。
范围为10到255秒。默认值为180秒。
4. 选择 **发送Version 2包文** 中的， **关闭** 或 **启用** 单选按钮
这将启用或禁用从设备发送ISDP版本2数据包。默认值已启用。

下表描述了ISDP基本全局配置字段。

表34. ISDP基本全局配置

字段	描述
对端最近更新数据时间	指定是否
设备ID	此交换机的设备ID。
支持的设备ID类别	设备ID格式功能。
使用中的设备ID	设备ID格式。

2.7.2. 高级管理信息

系统管理 > ISDP管理 > 高级管理信息 > 端口配置



1. 使用端口选择配置管理模式的端口。
2. 使用管理模式启用或禁用端口上的ISDP。

默认值为关闭。

系统管理 > ISDP管理 > 高级管理信息 > ISDP 邻居列表



下表介绍了ISDP邻居显示的字段信息。

表35. ISDP邻居

字段	描述
设备ID	ISDP邻居的设备ID。
端口	在其上发现邻居的接口。
地址数据	邻居的地址。
支持性	邻居的能力。这个字段支持包含的设备类型： • Router • Trans Bridge • Source Route • Switch • Host • IGMP • Repeater

平台	邻居的模型类型(0至32)
端口ID	邻居上的端口ID。
保持时间	邻居发送的ISDP数据包的保持时间。
包文版本	从邻居发送的ISDP版本。
条目最近更新时间	自上次输入以来的时间已更改。
软件版本	邻居上的软件版本。

系统管理 > ISDP管理 > 高级管理信息 > ISDP包文统计

ISDP包文统计 - ISDP包文统计	
接收到的ISDP数据包	0
发送的ISDP数据包	0
接收到的ISDPv1 数据包	0
发送的ISDPv1 数据包	0
接收到的ISDPv2 数据包	0
发送的ISDPv2 数据包	0
接收到的ISDP数据包错误头标记统计	0
接收到的ISDP数据包校验值错误统计	0
ISDP Transmission Failure	0
接收到的ISDP数据包无效格式统计	0
接收ISDP数据表溢出统计	0
接收ISDP数据表中IP表溢出统计	0

下表介绍了ISDP统计字段。

表36. ISDP统计

字段	描述
接收到的ISDP数据包	接收的ISDP数据包包括ISDPv1和ISDPv2数据包。
传输的ISDP数据包	传输的ISDP数据包包括ISDPv1和ISDPv2数据包。
接收到ISDPv1数据包	已接收ISDPv1数据包。
发送的ISDPv1数据包	ISDPv1数据包被传输。
接收到ISDPv2数据包	已接收ISDPv2数据包。
发送的ISDPv2数据包	ISDPv2数据包被传输。
接收到的ISDP数据包错误头标记统计	接收到的ISDP坏数据包。

接收到的ISDP数据包校验值错误统计	校验和错误的编号。
ISDP传输故障	变速箱故障的编号。
接收到的ISDP数据包无效格式统计	接收到的无效格式ISDP数据包数。
接收ISDP数据表溢出统计	ISDP表的表大小。
接收ISDP数据表中IP表溢出统计	ISDP IP地址表的表大小。

2.8. 定时计划管理

系统管理 > 定时计划管理 > 高级管理信息 > 全局配置

1. 选择 **工作模式** 中，**关闭** 或 **启用** 单选按钮

这指定是启用还是禁用定时任务模块, 默认值已禁用。

2. 在列表项中 **定时器进度名称** 中，指定需要创建的计时器计划任务的名称。
3. 单击 **增加** 按钮

添加了新的计时器任务，任务的时间需要继续配置，配置更改立即生效。

4. 要删除选定的计时器计划，请单击“**删除**”按钮。

删除配置更改立即生效。

系统管理 > 定时计划管理 > 高级管理信息 > 定时计划列表

1. 在“计时器计划名称”列表中，选择计时器计划。

2. 在计时器计划类型列表中，选择绝对或周期。
3. 在计时器计划条目列表中，选择要配置或添加的计时器计划条目的数量。
如果要添加条目，请选择“新建”。
4. 在时间开始字段中，以格式（HH:MM）输入计划操作开始时的一天时间。
此字段必填。如果未指定时间，则计划不会开始运行。
5. 在“时间结束”字段中，以格式（HH:MM）输入计划操作终止时一天的时间。
6. 使用“开始日期”设置计划开始日期。
如果未指定日期，计划将立即开始运行。
7. 使用“日期停止”设置计划终止日期。
如果未选择结束日期，计划将无限期运行。
8. 使用重复模式显示事件重复的时间段。
如果不需要重复（计时器计划必须只触发一次），则将日期停止设置为等于日期开始。有以下可能的重复值：
 - **Daily.** 计时器计划使用每日重复日模式。
Daily mode. 选择意味着从周一到周五每天都会触发日程安排。“每天”选择表示计划每定义一天触发一次。如果未指定天数，则每天都会触发计划。
 - **Weekly.** 计时器计划每周重复运行
Every Week(s). 定义触发计划的周数。如果未指定周数，则每周触发计划。
WeekDay. 指定计划运行的星期几。
 - **Monthly.** 计时器计划使用每月重复
Monthly mode. 显示触发计划的月份的哪一天。字段“每月”表示计划每定义一个月触发一次
9. 单击 **应用** 按钮
更新的配置将发送到交换机，配置更改立即生效。

3. L2交换机管理

本章涵盖以下主题：

- 配置 VLANs
- 自动VoIP
- 生成树协议
- 二层组播
- 配置 MVR
- MAC地址表
- 端口设置
- 链接聚合组
- 多重注册协议（MRP）概述

3.1.端口管理

您可以查看和监视交换机上可用端口的物理端口信息。

3.1.1. 端口物理连接配置

您可以在交换机上配置物理接口。

L2交换管理 > 端口管理 > 端口物理连接配置

系统管理L2交换管理路由管理QoS管理安全管理监测管理维护

端口管理

端口物理连接配置

端口协议配置

端口名称描述

端口物理连接配置 - Port Configuration

Port	Port Type	Admin Mode	Auto-negotiation	Ability(all,10,100,1G,or 10G,etc.)	Force Speed	Maximum Frame Size	Flow Control	Link Status	CLI Name
☐ 0/1	Normal	Enable	Enable	All		1518	Disable	N/A	0/1
☐ 0/2	Normal	Enable	Enable	All		1518	Disable	N/A	0/2
☐ 0/3	Normal	Enable	Enable	All		1518	Disable	N/A	0/3
☐ 0/4	Normal	Enable	Enable	All		1518	Disable	N/A	0/4
☐ 0/5	Normal	Enable	Enable	All		1518	Disable	N/A	0/5
☐ 0/6	Normal	Enable	Enable	All		1518	Disable	N/A	0/6
☐ 0/7	Normal	Enable	Enable	All		1518	Disable	N/A	0/7
☐ 0/8	Normal	Enable	Enable	All		1518	Disable	N/A	0/8
☐ 0/9	Normal	Enable	Enable	All		1518	Disable	N/A	0/9
☐ 0/10	Normal	Enable	Enable	All		1518	Disable	N/A	0/10
☐ 0/11	Normal	Enable	Enable	All		1518	Disable	N/A	0/11

1. 使用端口选择接口。

2. 在 **Admin Mode** 列表中，选择启用或禁用。

这将设置端口控制管理模式。要使端口参与网络，必须选择启用。出厂默认设置为启用。

3. 从自动协商列表中，选择启用或禁用。

这将指定此端口的自动协商模式。默认值为**Enable**。
- 提示：** 更改自动协商模式后，在新设置生效的几秒钟内，交换机可能无法访问。
4. 从“Ability”列表中，输入本地端口自动协商时支持的不同速率。

可能的字段值如下所示：
- **Auto.** 所有支持的速度。
 - **100.** 100Mbps/秒
 - **10G.** 10Gbit/秒.
- 自协商属性可以包含多种速度的组合，用于设置不同速度值的分隔符字符是逗号（，）、句点（.）和空格（ ）。要设置自动协商速度，必须将自动协商模式设置为启用。仅支持自协商的端口才允许修改此属性，否则修改无效。默认设置为自动。
- 提示：** 更改速度值后，在新设置生效的几秒钟内，交换机可能无法访问。
5. 从“Force Speed”列表中，选择所选端口的强制速度值。
- 83

可能的字段值如下所示：

- **100 Half.** 100Mbps/秒，半双工速率
- **1000 Full，** 1000Mbps/秒，全双工速率

默认设置为 自协商模式或最高速率。

设置端口的强制速率时，必须先关闭端口的自协商功能（支持自协商）。

提示： 更改双工模式后，在新设置生效的几秒钟内，交换机可能无法访问。

6. 使用帧大小指定接口支持或配置为使用的最大以太网帧大小，包括以太网标头、CRC和有效负载。

范围为1518到12288。默认最大帧大小为1518。

7. 从流量控制列表中，选择以启用或禁用IEEE 802.3流量控制。

默认为“禁用”。如果端口缓冲区满了，交换机不发送暂停帧。当端口不能跟上被交换的帧数时，流量控制有助于防止数据丢失。当启用时，如果端口上的包使用的内存数量超过预先配置的阈值，并响应伙伴设备的暂停请求，交换机可以发送一个暂停帧来停止端口上的流量。暂停端口在暂停帧指定的一段时间内不转发数据包。当暂停帧时间过去，或利用率返回到指定的低阈值时，交换机允许端口再次发送帧。说明对于LAG接口，由于不适用流量控制，流量控制方式显示为空白。

8. 单击 **应用** 按钮

交换机会根据输入的值进行更新。要使交换机在整个电源周期中保留新值，您必须保存配置。

下表描述了显示的不可配置数据。

表37. 端口配置

字段	描述
Media Type	The media type.
Port Type	对于正常端口，此字段是正常的。否则，可能的值如下所示： • Mirrored. 该端口是一个镜像端口，其上的所有通信量都复制到探测端口。 • Probe. 使用此端口可监视镜像端口 • Trunk Member. 该端口是链路聚合组的成员。
Link Status	指示链路是否正常。
CLI Name	与该端口关联的接口索引，在CLI中显示 unit/port 编号。

3.1.2. 配置端口描述

要配置和显示设备中所有端口的描述，请执行以下操作：

L2交换管理 > 端口管理 > 端口名称描述



1. 使用端口描述输入要附加到端口的描述字符串。
它的长度最多可以是64个字符。

下表描述了屏幕上显示的不可配置信息。

表38. 端口描述

字段	描述
端口	选择要为其显示或配置数据的界面。
MAC地址	指定接口的物理地址。
PortList表项中索引	在SNMP中使用MIB对象类型PortList进行管理时，对应于端口的位偏移量值。
CLI中名称	与该端口关联的接口索引，在CLI中显示 unit/port 编号。

3.2. 链接聚合组

链路聚合组(Link aggregation group, lag)，也称为端口通道(port-channels)，可以将多个全双工以太网链路组合成一个逻辑链路。网络设备将聚合视为单个链路，这增加了容错性并提供了负载共享。创建LAG VLAN后，才能指定VLAN的成员。缺省情况下，LAG成为管理VLAN的成员。

LAG接口可以是静态的，也可以是动态的，但不能两者兼而有之。一个LAG的所有成员必须参与相同的协议。静态端口-通道接口不需要伙伴系统能够聚合其成员端口。

支持静态LAG，端口作为静态成员加入LAG时，既不发送lacpdu报文，也不接收lacpdu报文。

3.2.1. 配置LAG设置

可以将一个或多个需要汇聚的全双工以太网链路分组，形成链路聚合组，也称为端口-通道。

交换机将LAG视为一个单一的链接。

3.2.1.1. 汇聚组管理

要配置LAG设置，请执行以下操作：

L2交换管理 > 汇聚组管理 > 基本管理信息 > 汇聚组管理

汇聚名称	ID	使能模式	Hash 模式	最小连接数	STP模式	静态模式	连接状态 Trap	配置的物理端口	有效的物理端口	工作状态
☐ ch1	1	Enable	Src/Dest MAC, VLAN, EtherType	1	Enable	Enable	Disable			Down
☐ ch2	2	Enable	Src/Dest MAC, VLAN, EtherType	1	Enable	Enable	Disable			Down
☐ ch3	3	Enable	Src/Dest MAC, VLAN, EtherType	1	Enable	Enable	Disable			Down
☐ ch4	4	Enable	Src/Dest MAC, VLAN, EtherType	1	Enable	Enable	Disable			Down
☐ ch5	5	Enable	Src/Dest MAC, VLAN, EtherType	1	Enable	Enable	Disable			Down
☐ ch6	6	Enable	Src/Dest MAC, VLAN, EtherType	1	Enable	Enable	Disable			Down
☐ ch7	7	Enable	Src/Dest MAC, VLAN, EtherType	1	Enable	Enable	Disable			Down
☐ ch8	8	Enable	Src/Dest MAC, VLAN, EtherType	1	Enable	Enable	Disable			Down

1. 使用 LAG 名称输入要分配给 LAG 的名称。

您可以输入最多 15 个字母数字字符的任何字符串。必须指定一个有效名称，以便您创建 LAG。

2. 使用管理模式选择启用或禁用。

当 LAG 被禁用时，不会丢弃流量和 LACP PDUs，但不会释放形成 LAG 的链接。工厂默认值是启用。

3. 使用哈希模式选择端口通道上使用的负载平衡模式（LAG）。

通过选择要传输特定数据包的通道中的一个链路，在端口通道（LAG）上平衡通信量。通过从数据包中的选定字段创建二进制模式，并将该模式与特定链接关联来选择链接：

- **Src MAC, VLAN, EType, incoming port.** 报文关联的源MAC、VLAN、EtherType和入端口。
- **Dest MAC, VLAN, EType, incoming port.** 目的MAC、VLAN、EtherType和报文关联的入端口
- **Src/Dest MAC, VLAN, EType, incoming port.** 报文关联的源/目的MAC、VLAN、EtherType和入端口。
- **Src IP and Src TCP/UDP Port .** 报文的源IP字段、源TCP/UDP字段。
- **Dest IP and Dest TCP/UDP Port .** “目的IP”、“目的TCP/UDP端口”字段。
- **Src/Dest IP and TCP/UDP Port.** 报文的源/目的IP、源/目的TCP/UDP端口字段。
 - 对于L2包，使用源MAC地址和目的MAC地址进行哈希计算。
 - L3报文使用源IP地址、目的IP地址、TCP/UDP端口。

4. 使用STP Mode开启或关闭与LAG相关联的生成树协议管理模式。

可能的值如下所示：

- **Disable.** 生成树在此LAG中被禁用。
- **Enable.** 在这个LAG中启用了生成树。

5. 使用静态模式选择启用或禁用。

当LAG启用时，它不会发送或处理接收到的LACPDU，也就是说，成员端口不会发送LACPDU，并且它可以接收的所有LACPDU都会被丢弃。出厂默认设置为禁用。

6. 使用链接Trap指定在链接状态更改时是否发送Trap。

出厂默认值为**Enable**，这会导致Trap被发送。

7. 单击 **应用** 按钮

交换机会根据输入的值进行更新。配置更改立即生效。

下表描述了屏幕上显示的不可配置信息。

表39. LAG配置

字段	描述
LAG 描述	输入要附加到LAG的描述字符串。它的长度最多可以是64个字符。
LAG ID	LAG的识别。
LAG 状态	指示链路是否正常。
配置的物理端口	指示配置此汇聚组成员的物理端口
有效的物理端口	表示已经加入汇聚组工作的端口。

3.2.1.2. 配置LAG成员

您可以选择两条或多条全双工以太网链路进行汇聚，形成链路聚合组(link aggregation group, LAG)，也称为端口-通道。交换机可以将端口-通道视为单个链路。

要配置LAG成员，请执行以下操作：

L2交换管理 > 汇聚组管理 > 基本管理信息 > 汇聚成员

1. 使用LAG ID选择LAG的标识。
2. 使用“汇聚名称”输入要分配给LAG的名称。

您可以输入不超过15个字母数字字符的任意字符串。要创建LAG，必须指定一个有效的名称。

3. 使用“汇聚描述”输入要附加到LAG的描述字符串。

它可以长达 64 个字符。

4. 使用管理模式选择启用或禁用。

当 LAG 被禁用时，不会丢弃流量和 LACP PDUs，但不会释放形成 LAG 的链接。工厂默认值是启用。

5. 使用哈希模式选择端口通道上使用的负载平衡模式（LAG）。

通过选择要传输特定数据包的通道中的一个链路，在端口通道（LAG）上平衡通信量。通过从数据包中的选定字段创建二进制模式，并将该模式与特定链接关联来选择链接：

- **Src MAC, VLAN, EType, incoming port.** 报文关联的源MAC、VLAN、EtherType和入端口。
- **Dest MAC, VLAN, EType, incoming port.** 目的MAC、VLAN、EtherType和报文关联的入端口
- **Src/Dest MAC, VLAN, EType, incoming port.** 报文关联的源/目的MAC、VLAN、EtherType和入端口。
- **Src IP and Src TCP/UDP Port .** 报文的源IP字段、源TCP/UDP字段。
- **Dest IP and Dest TCP/UDP Port .** “目的IP”、“目的TCP/UDP端口”字段。
- **Src/Dest IP and TCP/UDP Port.** 报文的源/目的IP、源/目的TCP/UDP端口字段。
 - 对于L2包，使用源MAC地址和目的MAC地址进行哈希计算。

- L3报文使用源IP地址、目的IP地址、TCP/UDP端口。
6. 使用STP Mode开启或关闭与LAG相关联的生成树协议管理模式。

可能的值如下所示：

- **Disable.** 生成树在此LAG中被禁用。
 - **Enable.** 在这个LAG中启用了生成树。
7. 使用静态模式选择启用或禁用。

当LAG启用时，它不会发送或处理接收到的LACPDU，也就是说，成员端口不会发送LACPDU，并且它可以接收的所有LACPDU都会被丢弃。出厂默认设置为禁用。

8. 使用链接Trap指定在链接状态更改时是否发送Trap。

出厂默认值为Enable，这会导致Trap被发送。

9. 使用端口选择表选择端口作为LAG的成员。

3.2.2. LACP

3.2.2.1. LACP系统属性

L2交换管理 > 汇聚组管理 > LACP > LACP系统属性

The screenshot shows the 'LACP系统属性管理 - LACP' configuration page. The top navigation bar includes '系统管理', 'L2交换管理', '路由管理', 'QoS管理', '安全管理', '监测管理', and '维护'. The left sidebar shows '汇聚组管理' with sub-items like '基本管理信息', 'LACP', 'LACP系统属性管理', 'LACP组属性管理', and '端口的LACP属性管理'. The main content area has a title 'LACP系统属性管理 - LACP' and a search icon. Below the title is a form with a label 'LACP系统优先级' and a text input field containing '32768'. To the right of the input field is a hint '(0-65535)'. At the top right of the form area are buttons for '应用' (Apply) and '刷新' (Refresh).

1. lacp系统优先级，默认值32768，范围是0-65535

3.2.2.2. LACP组属性管理

L2交换管理 > 汇聚组管理 > LACP > LACP组属性管理

VLAN的流量，但它只能支持一个默认VLAN ID。

您可以定义存储在VLAN成员资格表中的VLAN组。每个交换机最多支持4094个VLAN。VLAN 1是默认创建的，是所有端口都是其成员的默认VLAN。

3.3.1. 配置基本VLAN设置

内部VLAN由基于端口的路由接口保留，对最终用户不可见。一旦这些内部VLAN由基于端口的路由接口分配，就不能将它们分配给路由VLAN接口。

要配置内部VLAN设置，请执行以下操作：

L2交换管理 > VLAN管理 > 基本管理信息 > VLAN 配置

VLAN ID (例如: 2, 5-10)	VLAN 名称(最大长度: 64 字符)	VLAN类别	静态模式
1	default	Default	关闭

1. 要将 VLAN 设置重置到其默认值，请选择重置配置复选框。

工厂默认值如下：

- 所有端口都分配给默认VLAN 1。
- 所有端口的PVID均为1。
- 所有端口配置为允许所有帧的可接受帧类型值。
- 所有端口均配置为禁用入口过滤。
- 所有端口配置为仅传输未标记的帧。
- 在所有端口上禁用GVRP，并清除所有动态条目。

2. 指定内部VLAN设置。

内部VLAN配置部分显示内部VLAN的分配基础和分配模式。

a. 使用内部VLAN分配基数指定路由接口的VLAN分配基数。

内部VLAN的默认基本范围为1到4093。

b. 选择内部VLAN分配策略升序或降序单选按钮。

这指定了内部VLAN分配的策略。

3. 使用VLAN ID为新VLAN指定VLAN标识符。

VLAN ID的范围为1到4093。

4. 使用可选的VLAN名称字段指定VLAN的名称。

VLAN名称最多可包含32个字母数字字符，包括空格。默认值为空。VLAN ID 1始终使用默认名称。

VLAN类型字段标识您正在配置的VLAN的类型。无法更改默认VLAN（VLAN ID=1）的类型：它始终是默认类型。使用此屏幕创建VLAN时，其类型始终为静态。通过GVRP注册创建的VLAN最初使用一种动态类型。配置动态VLAN时，可以将其类型更改为静态。

5. 单击 **增加** 按钮

VLAN已添加到交换机。

6. 要从交换机中删除选定的VLAN，请单击删除按钮。

7. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

3.3.2. 配置高级VLAN

要配置高级VLAN，请执行以下操作：

L2交换管理 > VLAN管理 > 高级管理 > VLAN 配置

端口 - vian复位

恢复默认Vlan配置

☐

端口 - 内部VLAN配置

内部VLAN分配基准值

4093

内部VLAN分配方式

☒ 降序 ☐ 升序

端口 - 端口

☐	VLAN ID (例如: 2, 5-10)	VLAN 名称(最大长度: 64 字符)	VLAN类别	静态模式
☐	1	default	Default	关闭

1. **恢复默认Vlan配置** - 如果选择此按钮并在下一屏幕上确认选择。

所有VLAN配置参数将重置为出厂默认值。此外，所有VLAN（默认VLAN除外）都将被删除。出厂默认值如下所示：

- 所有端口都分配给默认VLAN 1。
- 所有端口的PVID均为1。
- 所有端口配置为允许所有帧的可接受帧类型值。
- 所有端口均配置为禁用入口过滤。
- 所有端口配置为仅传输未标记的帧。
- 在所有端口上禁用GVRP，并清除所有动态条目。

配置内部VLAN

内部VLAN部分显示内部VLAN的分配基础和分配模式。内部VLAN由基于端口的路由接口保留，对最终用户不可见。一旦这些内部VLAN由基于端口的路由接口分配，就不能将它们分配给路由VLAN接口。

3.3.2.1. VLAN 管理

要配置内部VLAN，请执行以下操作：

L2交换管理 > VLAN管理 > 高级管理 > VLAN 管理

1. 在内部VLAN分配基数字段中，指定路由接口的VLAN分配基数。
您可以输入1到4093之间的值。
2. 选择内部VLAN分配策略升序或降序单选按钮。

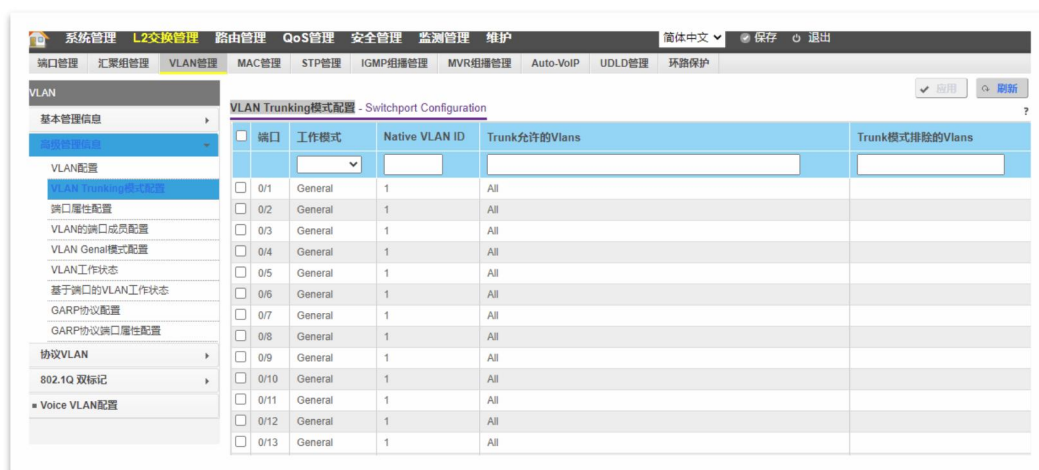
这指定了内部VLAN分配的策略。

3.3.2.2. 配置 VLAN Trunking

您可以在接口上配置switchport模式设置。switchport模式根据端口连接的设备类型定义端口的用途，并相应地限制端口的VLAN配置。分配适当的switchport模式有助于简化VLAN配置并最小化错误。

要配置VLAN Trunking，请执行以下操作：

L2交换管理 > VLAN管理 > 高级管理 > VLAN Trunking模式配置



1. 单击端口选择要配置数据的接口。
2. 在 工作模式 列表中，选择以下选项之一：
 - **Access.** 此模式适用于连接到终端站或终端用户的端口。访问端口仅参与一个VLAN。它们接受标记和未标记的数据包，但总是传输未标记的数据包。
 - **Trunk.** 此模式适用于连接到其他交换机的端口。中继端口可以参与多个VLAN，并接受标记和未标记的数据包。
 - **General.** 自定义端口配置模式。使用 **VLAN General模式配置** 界面上的设置，可以配置通用端口VLAN属性，如成员、PVID、标签、入口过滤器等。缺省情况下，所有端口的初始配置模式为“General”
3. 从列表中选择以配置本机VLAN ID。

这是端口的本机VLAN，仅当端口switchport模式为Trunk时才有效。
4. 配置允许的中继VLAN。

这是一组VLAN，在中继模式下配置时，端口可以是其成员。默认情况下，此列表包含所有可能的VLAN，即使它们尚未创建。VLAN ID的范围为1到4093。请使用连字符（-）指定范围，或使用逗号（，）分隔列表中的VLAN ID。空间是不允许的。零值清除允许的VLAN。All值设置范围（1到4093）内的所有VLAN。
5. 单击 应用 按钮

更新的配置将发送到交换机。配置更改将立即生效。

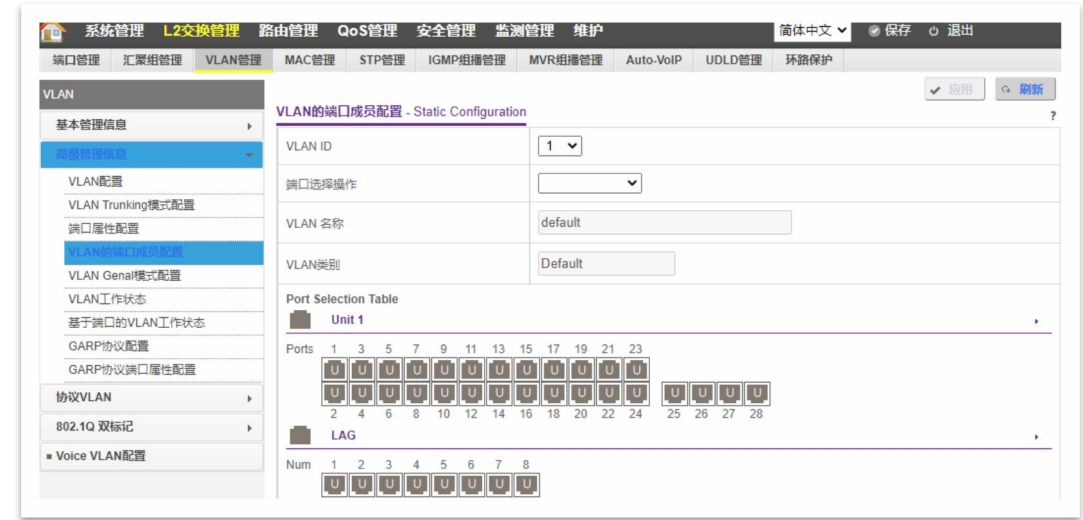
本机VLAN标记字段显示已启用或已禁用：

- 启用VLAN标记时，如果中继端口接收到未标记的帧，它将在没有VLAN标记的本机VLAN上转发这些帧。
- 禁用VLAN标记时，如果中继端口接收到未标记的帧，则在转发时会在VLAN标记中包含本机VLAN ID

3.3.2.3. 配置VLAN成员

要配置VLAN成员，请执行以下操作：

L2交换管理 > VLAN管理 > 高级管理 > VLAN的端口成员配置



- 1. 在VLAN ID列表中，选择VLAN ID。
- 2. 在 端口选择操作组操作列表中，选择所有端口并配置它们：
 - **Untag All.** 所有为此 VLAN 传输的所有帧的端口均未标记。所有端口都包含在 VLAN 中。
 - **Tag All.** 选择为此 VLAN 传输的所有帧的端口。所有端口都包含在 VLAN 中。
 - **Remove All.** 所有可以通过 GVRP 在此 VLAN 中动态注册的端口。此选择将所有端口排除在所选 VLAN 之外。
- 3. 在端口显示中，选择端口编号以将其添加到此 VLAN 中。Each 端口可以使用三种模式之一：
 - **T (Tagged).** 单击此 VLAN 传输的所有帧的端口。所选端口包含在 VLAN 中。
 - **U (Untagged).** 单击此 VLAN 传输的所有帧未标记的端口。所选端口包含在 VLAN 中。
 - **BLANK (Autodetect).** 单击可通过 GVRP 在此 VLAN 中动态注册的端口。此选择将端口排除在所选 VLAN 中。

下表描述了屏幕上显示的不可配置信息。

表40. 高级VLAN成员

字段	Definition
VLAN名称	所选VLAN的名称。它最多可以是32个字母数字字符，包括空格。 VLAN ID 1始终使用默认名称。

VLAN类型	所选VLAN的类型： • Default (VLAN ID = 1). 始终存在。 • Static. 您手动配置的 VLAN • Dynamic. GVRP 注册创建的 VLAN，您没有转换为静态，因此 GVRP 可以删除
--------	---

3.3.2.4. 查看VLAN状态

您可以查看所有当前配置的VLAN的状态。

要查看VLAN状态，请执行以下操作：

L2交换管理 > VLAN管理 > 高级管理 > VLAN 工作状态



下表描述了屏幕上显示的不可配置信息。

表41. VLAN状态

字段	Definition
VLAN ID	VLAN的VLAN标识符（VID）。VLAN ID的范围为1到4093。
VLAN 名称	VLAN的名称。VLAN ID 1始终命名为“默认”。
VLAN类别	VLAN类型： • Default (VLAN ID = 1). 始终存在 • Static. 您手动配置创建的VLAN • Dynamic. 由GVRP注册创建的VLAN，您没有将其转换为静态，因此GVRP可以删除该VLAN
路由接口	如果已为此VLAN配置VLAN路由，则与VLAN关联的接口。

输出Untagged的端口	VLAN中包含的端口，从此端口输出包含此 VLAN ID的数据，将不携带 VLAN ID标记。
输出Tag的端口	VLAN中包含的端口，从此端口输出包含此 VLAN ID的数据，将携带此 VLAN ID标记。
禁止分配Vlan的端口	由GVRP注册创建的动态VLAN，不会包含的端口列表。

3.3.2.5. 配置端口PVID设置

您可以将端口VLAN ID（PVID）分配给接口。PVID有某些要求：

- 必须为所有端口定义PVID。
- 如果未指定其他值，则使用默认VLAN PVID。
- 要更改端口的默认PVID，必须首先创建一个VLAN，将端口作为成员包含在内。
- 使用端口 VLAN ID（PVID）配置屏幕在端口上配置虚拟 LAN。

要配置PVID设置，请执行以下操作：

L2交换管理 > VLAN管理 > 高级管理 > 端口属性配置

1. 选择接口

选中接口旁边的接口复选框。您可以选择多个接口。要选择所有接口，请选中标题行中的接口复选框。

2. 在PVID字段中，指定要分配给此端口上接收的未标记或优先级标记帧的VLAN ID。

出厂默认值为1。

3. 在“可接受的帧类型”列表中，指定可在此端口上接收的帧类型。

选项为 **VLAN only** 或 **Admit All**：

- 当设置为仅**VLAN only**时，此端口上接收的未标记帧或优先标记帧将被丢弃。

- 当设置为 **Admit All** 时，接受此端口上接收的未标记帧或优先标记帧，并为其分配端口VLAN ID的值。无论使用哪种选项，VLAN标记的帧都会根据802.1Q VLAN规范进行转发。
4. 在配置的入口过滤字段中，选择启用或禁用。
 - 启用时，如果此端口不是与此帧关联的VLAN的成员，则丢弃该帧。在标记帧中，VLAN由VLAN标识标签中的ID。在未标记的帧中，VLAN是为接收此帧的端口指定的端口VLAN ID。
 - 禁用时，将根据802.1Q VLAN网桥规范转发所有帧。出厂默认设置已禁用。
 5. 在端口优先级字段中，指定为到达端口的未标记数据包分配的默认802.1p优先级。
您可以输入0到7之间的数字。

3.3.2.6. 配置GARP交换机设置

提示： GARP配置更改可能需要10秒钟才能生效。

要配置GARP交换机设置，请执行以下操作：

L2交换管理 > VLAN管理 > 高级管理 > GARP协议配置



1. 选择GVRP模式禁用或启用单选按钮。
这将为交换机选择GARP VLAN注册协议管理模式。出厂默认设置为禁用。
2. 选择GMRP模式禁用或启用单选按钮。
这将为交换机选择GARP组播注册协议管理模式。出厂默认设置为禁用。

3.3.2.7. 配置GARP端口

提示： GARP配置更改可能需要10秒钟才能生效。

要配置GARP端口，请执行以下操作：

L2交换管理 > VLAN管理 > 高级管理 > GARP协议端口属性配置

端口	端口GVRP工作模式	端口GMRP工作模式	加入时间(百分秒)	离开时间(百分秒)	离开全部时间(百分秒)
☐ 0/1	关闭	关闭	20	60	1000
☐ 0/2	关闭	关闭	20	60	1000
☐ 0/3	关闭	关闭	20	60	1000
☐ 0/4	关闭	关闭	20	60	1000
☐ 0/5	关闭	关闭	20	60	1000
☐ 0/6	关闭	关闭	20	60	1000
☐ 0/7	关闭	关闭	20	60	1000
☐ 0/8	关闭	关闭	20	60	1000
☐ 0/9	关闭	关闭	20	60	1000
☐ 0/10	关闭	关闭	20	60	1000
☐ 0/11	关闭	关闭	20	60	1000
☐ 0/12	关闭	关闭	20	60	1000

1. 使用接口选择要为其显示或配置数据的物理接口。
2. 在端口GVRP模式字段中，选择启用或禁用。

这指定端口的GARP VLAN注册协议管理模式。如果选择“禁用”，则该协议不处于活动状态，且加入时间、离开时间和离开所有时间均无效。出厂默认设置为禁用。

3. 在端口GMRP模式字段中，选择启用或禁用

这指定端口的GARP组播注册协议管理模式。如果选择“禁用”，则协议不处于活动状态，并且“加入时间”、“离开时间”和“离开所有时间”都不起作用。出厂默认设置为禁用。

4. 在“加入时间(百分之一秒)”字段中，指定GARP pdu注册(或重新注册)VLAN或组播组成员的传输间隔时间，单位为百分之一秒。

输入一个介于10到100(0.1到1.0秒)之间的数字。默认值是20厘秒(0.2秒)。对于每个端口的每个GARP参与者，都存在这个定时器的实例。

5. 在“离开时间(百分之一秒)”字段中，指定在收到VLAN或组播组的注销请求后，在删除相关表项之前需要等待的时间，单位为百分之一秒。

这就允许另一个站点有时间断言注册相同的属性，以保持不间断的服务。输入一个20到600之间的数字(0.2到6.0秒)。默认值是60厘秒(0.6秒)。对于每个端口的每个GARP参与者，都存在这个定时器的实例。

6. 使用Leave All Time（厘米秒）控制生成LeaveAll PDU的频率。

Leave All PDU表示所有的注册将很快被注销。为了保持注册，参与者必须重新加入。

leave all period定时器设置为一个随机值，取值范围为LeaveAllTime ~

1.5*LeaveAllTime。定时器以厘秒为单位指定。请输入200 ~ 6000之间的数字(2 ~ 60

秒)。默认值是1000厘秒(10秒)。对于每个端口的每个GARP参与者，都存在这个定时器

的实例。

3.3.3. 协议VLAN

3.3.3.1. 配置基于MAC的VLAN

基于 MAC 的 VLAN 功能允许将传入的未标记数据包分配到 VLAN，从而根据数据包的源 MAC 地址对流量进行分类。

您通过在 MAC 到 VLAN 表中配置条目来定义 MAC 到 VLAN 映射。条目通过源 MAC 地址和所需的 VLAN ID 进行指定。MAC 到 VLAN 配置在设备的所有端口之间共享（即有一个系统范围的表，其中 MAC 地址为 VLAN ID 映射）。

当untagged或priority -tagged报文到达交换机时，如果MAC到VLAN表中存在表项，则查找该报文的源MAC地址。如果找到相应的表项，则为报文分配相应的VLAN ID。如果数据包已经被标记为优先级，它将保持这个值;否则，优先级设置为零。分配的VLAN ID根据VLAN表进行验证，如果VLAN有效，则继续对报文进行入接口处理;否则报文将被丢弃。这意味着允许用户对系统中未创建的VLAN配置MAC地址映射。.

要配置基于MAC的VLAN，请执行以下操作：

L2交换管理 > VLAN管理 > 协议VLAN > 基于MAC地址的VLAN



1. 在MAC地址字段中，键入要绑定到VLAN ID的有效MAC地址。
仅当创建基于MAC的VLAN时，此字段才可配置。
2. 在VLAN ID字段中，指定范围为1到4093的VLAN ID。
3. 单击 **增加** 按钮
MAC地址被添加到VLAN映射中。
4. 要从VLAN映射中删除MAC地址, 请单击 **删除** 按钮

3.3.3.2. 基于以太网包文类别的VLAN

通过基于协议的VLAN，可以为未带标签的报文定义过滤条件。缺省情况下，如果没有配置基于

端口(IEEE 802.1Q)或基于协议的VLAN，则将不带标签的报文分配到VLAN 1中。您可以通过定义基于端口的vlan或基于协议的vlan，或两者同时定义来覆盖这种行为。带标签的报文通常按照IEEE 802.1Q标准进行处理，不包含在基于协议的vlan中。

如果为特定的协议将端口分配到基于协议的VLAN，则该端口接收到的该协议的untagged帧将被分配基于协议的VLAN ID。端口接收到的其他协议的Untagged帧被分配端口VLAN ID，要么是缺省的PVID(1)，要么是使用端口VLAN配置界面指定给端口的PVID。

通过创建组来定义基于协议的VLAN。每个组与VLAN ID是一一对应的关系，可以包含一到三个协议定义，可以包含多个端口。当您创建一个组时，需要指定了一个名称，并自动分配了一个组ID。

要配置基于协议的VLAN组，请执行以下操作：

L2交换管理 > VLAN管理 > 协议VLAN > 基于以太网报文类别的VLAN

分组ID	分组名称	帧协议	指定值	VLAN ID	Ports

1. 在“组名”字段中，键入新组的名称。

最多可以输入16个字符。

2. 在协议字段中，选择要与组关联的协议。

有三种可配置的协议：

- **IP.** IP是一种网络层协议，为数据传输提供无连接服务。
- **ARP.** 地址解析协议（ARP）是一种低级协议，它将网络层地址动态映射到物理介质访问控制（MAC）地址。
- **IPX.** 网络间数据包交换（IPX）是一种无连接数据报网络层协议，通过网络转发数据。

3. 在VLAN ID字段中，选择VLAN ID。

它可以是1到4093之间的任何数字。组中的所有端口都将此VLAN ID分配给为此组中包含的协议接收的未标记数据包。

4. 单击 **增加** 按钮

将基于协议的VLAN组添加到交换机。

5. 要删除由组ID字段中的值标识的基于协议的VLAN组，请单击 **删除** 按钮

下表描述了屏幕上显示的不可配置信息。

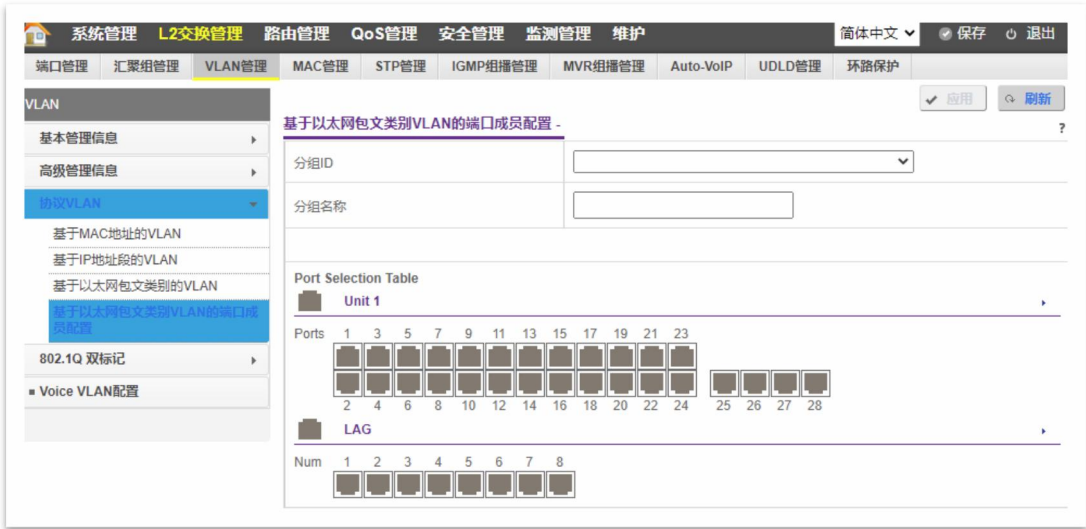
表42. 基于协议的VLAN组

字段	描述
组ID	用于标识用户创建的组的数字。当用户创建组时，会自动分配组ID。
Ports	显示属于该组的所有成员端口。

3.3.3.3. 基于以太网包文类别VLAN的端口成员配置

要配置基于协议的VLAN组成员，请执行以下操作：

L2交换管理 > VLAN管理 > 协议VLAN > 基于以太网包文类别VLAN的端口成员配置



- 1. 在组ID列表中，选择基于协议的VLAN组ID。
- 2. 选择端口号（1、2、3等）以选择要添加到此基于协议的VLAN组的端口。

对于给定的协议，接口只能属于一个组。如果已将端口添加到IP的组中，则无法将其添加到另一个也包含IP的组中，尽管可以将其添加到IPX的新组中。

下表描述了屏幕上显示的不可配置信息。

表43. 基于协议的VLAN组成员

字段	描述
组名	此字段标识所选基于协议的VLAN的名称。它最多可以是32个字母数字字符，包括空格。
成员	单击此按钮可显示所选基于协议的VLAN组中的当前编号。

3.3.3.4. 配置基于IP子网的VLAN

IP子网到VLAN映射是通过在IP子网到VLAN表中配置一个表项来定义的。该表项通过源IP地址、掩码和VLAN ID指定。IP子网到VLAN的配置在设备的所有端口上共享

要配置基于IP子网的VLAN，请执行以下操作：

L2交换管理 > VLAN管理 > 协议VLAN > 基于IP地址段的VLAN

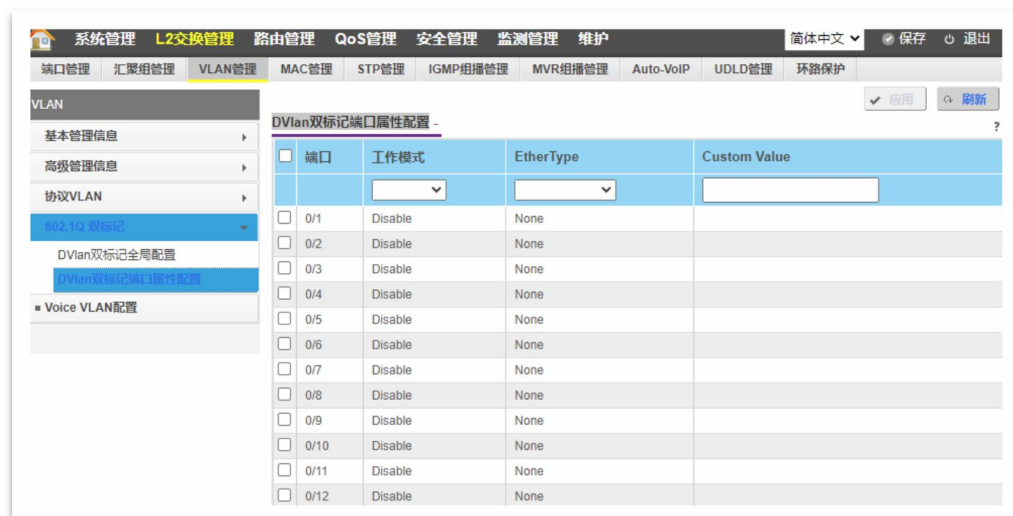


1. 在IP地址字段中，指定绑定到VLAN ID的有效IP地址。
以点十进制表示法输入IP地址。
2. 在子网掩码字段中，指定IP地址的有效子网掩码。
以点十进制表示法输入子网掩码。
3. 在VLAN ID字段中，指定范围为（1到4093）的VLAN ID。
4. 单击 **增加** 按钮
添加了基于IP子网的VLAN。
5. 要删除选定的基于IP子网的VLAN，请单击 **删除** 按钮

3.3.4. 802.1Q双标记

要配置端口DVLAN，请执行以下操作：

L2交换管理 > VLAN管理 > 802.1Q双标记 > DVlan双标记端口属性配置



1. 选择接口复选框以选择物理接口。
要选择所有端口，请选中列顶部的接口复选框。
2. 在管理模式字段中，选择启用或禁用。
这指定了可以启用或禁用双VLAN分配的管理模式。此项的默认值已禁用。
3. 在全局EtherType字段中，指定DVLAN标记的前16位。
 - **802.1Q Tag**. 表示0x8100的常用标记
 - **vMAN Tag**. 表示0x88A8的常用标记
 - **Custom Tag**. 在0到65535之间的任意范围内配置EtherType

3.3.5. 配置语音VLAN

配置语音VLAN的相关参数。只有具有读写访问权限的用户才能更改此屏幕上的数据。

要配置语音VLAN，请执行以下操作：

L2交换管理 > VLAN管理 > Voice VLAN配置

端口	工作模式	指定的VLAN ID/Priority值	CoS重修改模式	当前工作状态
☐ 0/1	Disable		Disable	Disabled
☐ 0/2	Disable		Disable	Disabled
☐ 0/3	Disable		Disable	Disabled
☐ 0/4	Disable		Disable	Disabled
☐ 0/5	Disable		Disable	Disabled
☐ 0/6	Disable		Disable	Disabled

1. 选择管理模式禁用或启用单选按钮。
这指定交换机语音VLAN的管理模式。默认设置为禁用。
2. 使用接口选择物理接口。
3. 使用接口模式为所选接口选择语音VLAN模式：
 - **Disable**. 这是默认值。
 - **None**. 允许IP话机使用自己的配置发送不带标签的语音流量。
 - **VLAN ID**. 配置话机发送带标签的语音流量。
 - **dot1p**, 为语音流量配置语音VLAN 802.1p优先级标记。选择此选项后，在值字段中输入dot1p值。
 - **Untagged**. 将话机配置为发送未标记的语音通信。
4. 使用值输入VLAN ID或dot1p值。

- 仅当选择VLAN ID或dot1p作为接口模式时，才会启用此选项。
- 在CoS覆盖模式字段中，选择禁用或启用。
- 默认设置为禁用。

3.4.MAC 地址表

您可以查看或配置MAC地址表。该表包含交换机具有转发或过滤信息的单播表项信息。透明桥接函数使用这个信息来决定如何传播接收到的帧。

3.4.1. 配置MAC地址表

要配置MAC地址表，请执行以下操作：

L2交换管理 > MAC管理 > 基本管理信息 > MAC地址列表



- 使用"搜索"按 MAC 地址、VLAN ID 或端口搜索 MAC 地址：
 - Searched by MAC Address.** 选择"MAC Address"，输入以冒号分隔的6字节16进制MAC地址，例如:01:23:45:67:89:AB。然后单击Go按钮。如果该地址存在，该表项显示为第一个表项，后面跟着剩余的(更大的)MAC地址。需要完全匹配。
 - Searched by VLAN ID.** 选择VLAN ID，输入VLAN ID，例如100。然后单击Go按钮。如果该地址存在，则该条目将显示为第一个条目，后跟其余（更大）MAC地址。
 - Searched by Port.** 以单元/插槽/端口格式输入端口ID，例如2/1/1。然后单击Go按钮。如果该地址存在，则该条目将显示为第一个条目，后跟其余（更大）MAC地址。

下表描述了屏幕上显示的不可配置信息。

表44. 基本地址表

字段	描述
MAC表地址总数量:	显示学习或配置的MAC地址总数。

MAC地址	交换机具有转发和/或过滤信息的单播MAC地址。该格式是一个由冒号分隔的6字节MAC地址，例如01:23:45:67:89:AB。
VLAN ID	与MAC地址关联的VLAN ID。
接口	学习此地址的端口。
状态	此条目的状态。这些值的含义如下： • Static. 相应实例的值是由系统或用户添加的，无法重新学习。 • Learned. 已学习到对应实例的值，并正在使用。 • Management. 对应实例的值是系统管理用。

3.4.2. 设置动态地址老化间隔

您可以为指定的转发数据库设置地址老化间隔。

要设置地址老化间隔：

L2交换管理 > MAC管理 > 高级管理 > 动态MAC地址配置

1. 使用地址老化超时（秒）指定老化动态学习的转发信息的超时时间（秒）。

802.1D-1990建议默认值为300秒。该值可以指定为10到1000000秒之间的任何数字。出厂默认值为300。

3.4.3. 配置静态MAC地址

要配置静态MAC地址，请执行以下操作：

L2交换管理 > MAC管理 > 高级管理 > 静态MAC地址管理

1. 使用接口选择物理接口/汇聚组。
2. 在静态MAC地址字段中，键入MAC地址。
3. 选择与MAC地址关联的VLAN ID。
4. 单击 增加 按钮
5. 静态MAC地址被添加到交换机中。
6. 要从交换机中删除现有静态MAC地址，请单击删除按钮。

3.5.生成树协议

生成树协议(STP)为桥的任何安排提供了树状拓扑结构。STP还提供了网络端站之间的一条路径，消除了环路。支持的生成树版本包括传统STP、多 STP和快速 STP。

经典STP在终端站之间提供单一路径，避免和消除环路。有关配置通用STP的信息，请参阅第236页的。*配置CST端口设置*

MSTP (Multiple Spanning Tree Protocol)支持多个生成树实例，在不同的接口上有效地通道VLAN流量。生成树的每个实例都按照IEEE 802.1w快速生成树(RSTP)中规定的方式进行操作，只是在工作上略有修改，而不是结束效果(主要的效果是端口快速过渡到转发)。RSTP与传统STP (IEEE 802.1D)的区别在于，RSTP能够配置和识别与端站相连的全双工连接和端口，从而使端口快速过渡到Forwarding状态，并抑制拓扑变化通知。这些特征由点和边端口参数表示。MSTP同时兼容RSTP和STP。它对STP和RSTP桥具有适当的行为。MSTP桥可以配置为完全作为RSTP桥或STP桥。

提示： 对于位于同一区域的两个网桥，强制版本必须为802.1s，并且它们的配置名称、摘要密钥和修订级别必须匹配。有关区域及其对网络拓扑的影响的更多信息，请参阅IEEE 802.1Q标准。

3.5.1. 配置基本STP设置

要配置STP基本设置，请执行以下操作：

L2交换管理 > STP管理 > 基本信息管理 > 生成树管理

MST ID	VID	FID
0	1	1

1. 选择生成树管理模式禁用或启用单选按钮。

这指定是否在交换机上启用生成树操作。

2. 使用Force Protocol Version为交换机指定Force Protocol Version参数。

这些选项包括IEEE 802.1d、IEEE 802.1w、IEEE 802.1s、PVST和RPVST。

3. 使用配置名称指定用于标识当前正在使用的配置的标识符。

它最多可以是32个字母数字字符。

4. 使用配置修订级别指定用于标识当前使用的配置的标识符。

允许的值介于0和65535之间。默认值为0。

5. 单击 转发BPDU帧， 在关闭 STP 时，是否启用或禁用。

这指定在交换机上禁用生成树时是否转发生成树BPDU。

6. 选择BPDU防护禁用或启用单选按钮。

这指定是否启用BPDU防护功能。STP BPDU guard允许网络管理员强制执行STP域边界，并保持活动拓扑的一致性和可预测性。启用STP BPDU保护的边缘端口后面的交换机不会影响整个STP拓扑。在接收BPDU时，BPDU保护操作将禁用使用此选项配置的端口，并将端口转换为禁用状态。这将导致端口的管理禁用。

7. 选择BPDU过滤器禁用或启用单选按钮。

这指定是否启用BPDU筛选器功能。STP BPDU过滤适用于所有操作边缘端口。处于运行状态的边缘端口应连接到通常丢弃BPDU的主机。如果操作边缘端口接收到BPDU，它将立即失去其操作状态。在这种情况下，如果在此端口上启用了BPDU过滤，则会删除在此端口上接收的BPDU。

8. 选择e Fast主干模式禁用或启用单选按钮(仅限PVSTP)。

当间接链接失败时，使用此选项选择新的间接链接。系统不会像802.1d中那样忽略劣质BPDU。相反，系统使用BPDU在接收BPDU的端口上老化。稍后，系统在其他非指定端口上发送根链接查询。根据回复，如果至少有一个回复是肯定的，它会选择一个新的间接链接。默认情况下禁用快速主干模式。

9. 选择快速上行模式禁用或启用单选按钮(仅限PVSTP)。

当主根端口关闭时，此选项可缩短选择新根端口的恢复时间。默认情况下禁用快速上行模式。

10. 使用最大更新速率字段配置快速上行链路最大更新速率。

启用快速上行链路模式时，此字段用于配置。允许的值为每秒0到32000个数据包。默认值为150。

11. 单击 应用 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

下表描述了不可配置的字段。

表45. STP配置

字段	描述
配置中的数字Key值	用于标识当前正在使用的配置的标识符。
STP Status	
MST ID	由MST实例（包括CST）和与其相关联的相应VLAN ID组成的表。
VID ID	由VLAN ID和与其相关联的相应FID组成的表。
FID ID	由FID和与其相关的相应VLAN ID组成的表。

3.5.2. 配置高级STP设置

要配置高级STP设置，请执行以下操作：

L2交换管理 > STP管理 > 高级管理 > 生成树管理

MST ID	VID	FID
0	1	1

1. 选择生成树管理模式禁用或启用单选按钮。

这指定是否在交换机上启用生成树操作。

2. 使用Force Protocol Version为交换机指定Force Protocol Version参数。

这些选项包括IEEE 802.1d、IEEE 802.1w、IEEE 802.1s、PVST和RPVST。

3. 使用配置名称指定用于标识当前正在使用的配置的标识符。

它最多可以是32个字母数字字符。

4. 使用配置修订级别指定用于标识当前使用的配置的标识符。

允许的值介于0和65535之间。默认值为0。

5. 单击 转发BPDU帧， 在关闭 STP 时，是否启用或禁用。

这指定在交换机上禁用生成树时是否转发生成树BPDU。

6. 选择BPDU防护禁用或启用单选按钮。

这指定是否启用BPDU防护功能。STP BPDU guard允许网络管理员强制执行STP域边界，并保持活动拓扑的一致性和可预测性。启用STP BPDU保护的边缘端口后面的交换机不会影响整个STP拓扑。在接收BPDU时，BPDU保护操作将禁用使用此选项配置的端口，并将端口转换为禁用状态。这将导致端口的管理禁用。

7. 选择BPDU过滤器禁用或启用单选按钮。

这指定是否启用BPDU筛选器功能。STP BPDU过滤适用于所有操作边缘端口。处于运行状态的边缘端口应连接到通常丢弃BPDU的主机。如果操作边缘端口接收到BPDU，它将立即失去其操作状态。在这种情况下，如果在此端口上启用了BPDU过滤，则会删除在此端口上接收的BPDU。

8. 选择e Fast主干模式禁用或启用单选按钮(仅限PVSTP)。

当间接链接失败时，使用此选项选择新的间接链接。系统不会像802.1d中那样忽略劣质BPDU。相反，系统使用BPDU在接收BPDU的端口上老化。稍后，系统在其他非指定端口上发送根链接查询。根据回复，如果至少有一个回复是肯定的，它会选择一个新的间接链接。默认情况下禁用快速主干模式。

9. 选择快速上行模式禁用或启用单选按钮(仅限PVSTP)。

当主根端口关闭时，此选项可缩短选择新根端口的恢复时间。默认情况下禁用快速上行模式。

10. 使用最大更新速率字段配置快速上行链路最大更新速率。

启用快速上行链路模式时，此字段用于配置。允许的值为每秒0到32000个数据包。默认值为150。

11. 单击 应用 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

下表描述了不可配置的字段。

表46. STP配置

字段	描述
配置中的数字Key值	用于标识当前正在使用的配置的标识符。
STP Status	
MST ID	由MST实例（包括CST）和与其相关联的相应VLAN ID组成的表。
VID ID	由VLAN ID和与其相关联的相应FID组成的表。
FID ID	由FID和与其相关的相应VLAN ID组成的表。

3.5.3. 配置CST设置

您可以在交换机上配置公共生成树（CST）和内部生成树。

要配置CST设置，请执行以下操作：

L2交换管理 > STP管理 > 高级管理 > CST 树管理

系统管理 L2交换管理 路由管理 QoS管理 安全管理 监测管理 维护 简体中文 保存 退出

端口管理 汇聚组管理 VLAN管理 MAC管理 STP管理 IGMP组播管理 MVR组播管理 Auto-VoIP UDLD管理 环路保护

STP管理

基本管理信息

高级管理信息

生成树管理

CST树管理

CST树端口属性管理

CST树端口状态

MST树管理

MST树VLAN管理

MST树端口属性管理

MST树端口状态

生成树包文统计

CST树管理 - 配置

网桥优先级	32768	(0 to 61440)
BPDU报文消息生存的最长时间(秒)	20	(6 to 40)
定时发送BPDU 报文的时间间隔(秒)	2	(1 to 10)
端口状态改变的时间间隔(秒)	15	(4 to 30)
BPDU 帧的最大跳数	20	(0 to 127)
每秒钟最多发送的 BPDU个数	6	(1 to 10)

CST树管理 - 工作状态

网桥标识号	80:00:02:00:00:00:00
最近拓扑路径更改时间	2 day 15 hr 44 min 20 sec
拓扑路径更改次数	0
拓扑路径改变标记	False
指派根桥	80:00:02:00:00:00:00
根路径开销	0
根端口的标识号	80:00
Max Age (secs)	20
Forward Delay (秒)	15
Hold Time (秒)	6
CST根桥	80:00:02:00:00:00:00
CST根桥路径	0

1. 在适当领域指定 CST 值:

- **Bridge Priority.** 当交换机或网桥运行STP时，每个交换机或网桥都被分配一个优先级。交换bpdud后，优先级最低的交换机成为根桥。CST (Common and Internal Spanning Tree)的桥优先级。有效范围是0-61440。桥优先级是4096的倍数。如果指定的优先级不是4096的倍数，则该优先级将自动设置为下一个最低的4096倍数。例如，如果试图将优先级设置为0到4095之间的任何值，则将其设置为0。默认优先级为32768。
- **Bridge Max Age (secs).** 公共和内部生成树（CST）的网桥最长使用时间，表示网桥在实现拓扑更改之前等待的时间（以秒为单位）。有效范围为6-40，该值必须小于或等于（2*网桥前向延迟）-1且大于或等于2*（网桥问候时间+1）。默认值为20。
- **Bridge Hello Time (secs).** 生成树（CST），表示根网桥在配置消息之间等待的时间（秒）。该值固定为2秒。该值必须小于或等于（网桥最大使用年限/2）-1。默认问候时间值为2。
- **Bridge Forward Delay (secs).** 表示网桥在转发数据包之前处于侦听和学习状态的时间量（秒）。该值必须大于或等于（桥接器最大使用年限/2）+1。时间范围为4秒到30秒。默认值为15秒。
- **Spanning Tree Maximum Hops.** 特定CST实例的信息可以在被丢弃之前传播。有效范围为6-40。默认值为20跳。

- **Spanning Tree Tx Hold Count.** 配置在hello时间窗口内允许网桥发送的最大BPDU数。有效范围为1–10。默认值为6。

2. 单击 应用 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表描述了显示的CST状态信息。

表47. STP高级CST配置

字段	描述
网桥标识符	CST的网桥标识符。它由网桥优先级和网桥的基本MAC地址组成。
拓扑更改后的时间	自上次更改CST拓扑以来的时间（秒）。
拓扑更改计数	为CST更改拓扑的次数。
拓扑变化	交换机拓扑更改参数的值，指示分配给CST的任何端口上是否正在进行拓扑更改。如果为True或False，则接受一个值。
指定根	根网桥的网桥标识符。它由网桥优先级和网桥的基本MAC地址组成。
Root Path Cost	CST指定根目录的路径成本。
Root Port Identifier	用于访问CST的指定根目录的端口。
Max Age(secs)	CST指定根目录的路径成本。
Forward Delay(secs)	根端口网桥前向延迟参数的派生值。
Hold Time(secs)	传输配置BPDU之间的最短时间。
CST区域根	CST区域根的优先级和基MAC地址。
CST路径成本	CST树区域根的路径成本。

3.5.4. 配置CST端口设置

您可以在交换机的特定端口上配置公共生成树（CST）和内部生成树。

当DOT1S遇到严重的错误情况时，端口可以变成诊断禁用(D-Disable)。最常见的原因是DOT1S软件发生BPDU泛洪。泛洪标准是DOT1S在3秒间隔内接收到超过15个bpdu。DOT1S D-Disable的其他原因非常罕见。

要配置CST端口设置，请执行以下操作：

L2交换管理 > STP管理 > 高级管理 > CST树端口属性管理

接口	端口优先级 (0-240, 16为步进单位)	Admin Edge模式	端口路径开销 (0-200000000, 0:自动配置)	路径开销自动配置模式	Hello Timer	External Port Path Cost	Auto Calculated External Port Path Cost	BPDU Filter	BPDU Flood	BPDU Guard Effect	Auto Edge	Root Guard	Loop Guard	TCN Guard	STP工作模式	端口转发状态
☐ 0/1	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/2	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/3	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/4	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/5	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/6	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/7	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/8	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/9	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/10	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/11	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/12	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/13	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled
☐ 0/14	128	关闭	0	启用	2	0	启用	关闭	关闭	Disabled	Disable	关闭	关闭	Disable	启用	Disabled

1. 选择一个接口。

您可以选择与CST关联的VLAN关联的物理或端口通道接口。

2. 使用端口优先级指定CST内特定端口的优先级。

端口优先级以16的倍数设置。例如，如果尝试将优先级设置为0到15之间的任何值，则将其设置为0。如果尝试将其设置为16到（2*16-1）之间的任何值，则将其设置为16，依此类推。默认值为128。

3. 使用Admin Edge Port指定端口是否为CIST内的边缘端口，使用菜单选择禁用或启用。

默认值为禁用。

4. 使用端口路径成本将路径成本设置为公共生成树和内部生成树中指定端口的新值。

它的取值范围为1到2000000000。默认值为0。

5. 使用外部端口路径成本将外部路径成本设置为生成树中指定端口的新值。

它的取值范围为1到2000000000。默认值为0。

6. 使用BPDU筛选器配置BPDU筛选器，当在该端口上启用STP时，该筛选器将筛选该端口上的BPDU流量。

可能的值为启用或禁用。默认值为禁用。

7. 使用BPDU Flood配置BPDU Flood，在端口关闭STP协议的情况下，对到达端口的BPDU流量进行泛洪处理。

可能的值为启用或禁用。默认值为禁用。

8. 使用“自动边缘”配置端口的自动边缘模式，使端口在一段时间内没有看到bpdud报文时成为边缘端口。

可能的值为启用或禁用。默认值为Enable。

9. 使用Root Guard配置Root Guard模式，该模式将端口设置为丢弃端口接收到的任何高级信息，从而防止设备的Root发生变化。

端口进入丢弃状态，不转发任何数据包。可能的值为启用或禁用。默认值为禁用。

10. 使用环路保护功能可以在端口上开启或关闭环路保护功能，对二层转发环路进行保护。

如果使能环路保护功能，端口将进入STP环路不一致阻塞状态，而不是侦听/学习/转发状态。默认值为“禁用”

11. 使用TCN Guard配置端口的TCN守卫，以限制端口传播通过该端口接收到的任何拓扑更改信息。

可能的值为启用或禁用。默认值为禁用。

12. 使用“端口模式”启用或禁用与端口或端口通道关联的生成树协议管理模式。

可能的值为启用或禁用。默认值为禁用。

13. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表描述了屏幕上显示的不可配置信息。

表48. CST端口配置

字段	描述
自动计算端口路径成本	显示路径成本是否自动计算（启用）或未计算（禁用）。如果端口路径成本的配置值为零，则根据端口的链路速度计算路径成本。
Hello Timer	CST的参数值。
Auto Calculated External Port Path Cost	显示外部路径成本是否自动计算（启用）或未计算（禁用）。如果外部端口路径成本的配置值为零，则根据端口的链接速度计算外部路径成本。
BPDU Guard Effect	显示BPDU保护效果，它将禁用接收BPDU数据包的边缘端口。可能的值为启用或禁用。
端口转发状态	此端口的转发状态。

3.5.5. 查看CST端口状态

您可以查看交换机上特定端口上的公共生成树（CST）和内部生成树。

要查看CST端口状态，请执行以下操作：

L2交换管理 > STP管理 > 高级管理 > CST树端口状态

CST端口状态 - 工作状态									
接口	Port ID	端口转发状态	Port Role	指派根桥	Designated Cost	Designated Bridge	Designated Port	Topology Change Acknowledge	Edge Port
0/1	80:01	Disabled	Disabled	80:00:02:00:00:00:00	0	80:00:02:00:00:00:00	00:00	False	False
0/2	80:02	Disabled	Disabled	80:00:02:00:00:00:00	0	80:00:02:00:00:00:00	00:00	False	False
0/3	80:03	Disabled	Disabled	80:00:02:00:00:00:00	0	80:00:02:00:00:00:00	00:00	False	False
0/4	80:04	Disabled	Disabled	80:00:02:00:00:00:00	0	80:00:02:00:00:00:00	00:00	False	False
0/5	80:05	Disabled	Disabled	80:00:02:00:00:00:00	0	80:00:02:00:00:00:00	00:00	False	False
0/6	80:06	Disabled	Disabled	80:00:02:00:00:00:00	0	80:00:02:00:00:00:00	00:00	False	False
0/7	80:07	Disabled	Disabled	80:00:02:00:00:00:00	0	80:00:02:00:00:00:00	00:00	False	False
0/8	80:08	Disabled	Disabled	80:00:02:00:00:00:00	0	80:00:02:00:00:00:00	00:00	False	False
0/9	80:09	Disabled	Disabled	80:00:02:00:00:00:00	0	80:00:02:00:00:00:00	00:00	False	False
0/10	80:0A	Disabled	Disabled	80:00:02:00:00:00:00	0	80:00:02:00:00:00:00	00:00	False	False

Point-to-Point MAC	CST根桥	CST根桥路径	Port Up Time Since Counters Last Cleared	Loop Inconsistent State	Transitions Into Loop Inconsistent State	Transitions Out Of Loop Inconsistent State
False	80:00:02:00:00:00:00	0	2 day 16 hr 24 min 5 sec	False	0	0
False	80:00:02:00:00:00:00	0	2 day 16 hr 24 min 5 sec	False	0	0
False	80:00:02:00:00:00:00	0	2 day 16 hr 24 min 5 sec	False	0	0
False	80:00:02:00:00:00:00	0	2 day 16 hr 24 min 5 sec	False	0	0
False	80:00:02:00:00:00:00	0	2 day 16 hr 24 min 5 sec	False	0	0
False	80:00:02:00:00:00:00	0	2 day 16 hr 24 min 5 sec	False	0	0
False	80:00:02:00:00:00:00	0	2 day 16 hr 24 min 5 sec	False	0	0
False	80:00:02:00:00:00:00	0	2 day 16 hr 24 min 5 sec	False	0	0
False	80:00:02:00:00:00:00	0	2 day 16 hr 24 min 5 sec	False	0	0
False	80:00:02:00:00:00:00	0	2 day 16 hr 24 min 5 sec	False	0	0
False	80:00:02:00:00:00:00	0	2 day 16 hr 24 min 5 sec	False	0	0

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表描述了屏幕上显示的CST状态信息。

表49. CST端口状态

字段	描述
接口	识别与CST关联的VLAN关联的物理或端口通道接口。
Port ID	CST内指定端口的端口标识符。它由端口优先级和端口的接口号组成。
端口转发状态	此端口的转发状态。
Port Role	每个启用的MST桥接端口为每棵生成树分配一个端口角色。端口角色是以下值之一：根端口、指定端口、备用端口、备份端口、主端口或禁用端口。
Designated Root	CST的根桥。它由网桥优先级和网桥的基本MAC地址组成。

Designated Cost	指定端口提供给LAN的路径成本。
Designated Bridge	具有指定端口的网桥的网桥标识符。它由网桥优先级和网桥的基本MAC地址组成。
Designated Port	为LAN提供最低成本的指定网桥上的端口标识符。它由端口优先级和端口的接口号组成。
Topology Change Acknowledge	标识是否要为此端口传输的下一个BPDU设置拓扑更改确认标志。这不是真的就是假的。
Edge port	指示端口是否作为边缘端口启用。它采用启用或禁用的值。
Point-to-point MAC	点到点状态的派生值。
CST根桥	CST区域根的网桥标识符。它由网桥优先级和网桥的基本MAC地址组成。
CST根桥路径	CST区域根的路径成本。
Port Up Time Since Counters Last Cleared	自上次清除计数器以来的时间，以天、小时、分钟和秒为单位显示。
Loop Inconsistent State	此参数标识端口是否处于循环不一致状态。
Transitions Into Loop Inconsistent State	此接口转换为循环不一致状态的次数。
Transitions Out Of Loop Inconsistent State	此接口转换为循环外不一致状态的次数。

3.5.6. 配置MST设置

您可以在交换机上配置多个生成树（MST）。

要配置MST实例，请执行以下操作：

L2交换管理 > STP管理 > 高级管理 > MST 树管理



1. 配置MST值：

- **MST ID.** 指定要创建的MST的ID。该值的有效值为1到4094。只有在选中MST ID选

择框的选择选项时，此值才可见。

- **Priority.** MST的网桥优先级值。当交换机或网桥运行STP时，每个交换机或网桥都被分配一个优先级。交换BPDU后，具有最低优先级值的交换机成为根网桥。网桥优先级是4096的倍数。如果指定的优先级不是4096的倍数，则会自动将优先级设置为下一个最低优先级，即4096的倍数。例如，如果尝试将优先级设置为0到4095之间的任何值，设置为0。默认优先级为32768。有效范围为0–61440。
- **VLAN ID.** 这将给出交换机上每个VLAN的组合框。可以选择或取消选择这些选项，以便重新配置VLAN与MST实例的关联。

2. 单击添加按钮。

This creates the new MST that you configured.

3. To modify an MST instance:

- a. 选中实例旁边的复选框（您可以选择多个复选框以将相同设置应用于所有选定端口）。
- b. 更新值
- c. 单击应用按钮。

4. 要删除MST实例，请选中该实例的复选框，然后单击“删除”按钮。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

对于每个配置的实例，下表中描述的信息将显示在屏幕上。

表50. MST配置

字段	描述
网桥标识号	所选MST实例的网桥标识符。它由网桥优先级和网桥的基本MAC地址组成。
最近拓扑路径更改时间	所选MST实例的拓扑上次更改后的n秒时间。
拓扑路径更改次数	为所选MST实例更改拓扑的次数。
拓扑路径改变标记	交换机拓扑更改参数的值，指示分配给所选MST实例的任何端口上是否正在进行拓扑更改。如果为True或False，则接受一个值。
指派根桥	根网桥的网桥标识符。它由网桥优先级和网桥的基本MAC地址组成
根路径开销	此MST实例的指定根目录的路径开销。
根端口的标识号	用于访问此MST实例的指定根目录的端口。

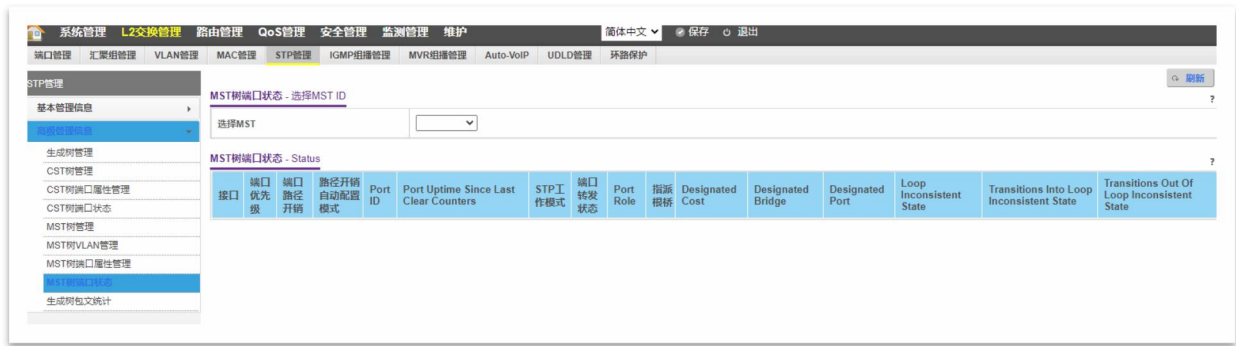
3.5.7. 查看生成树MST端口状态

您可以在交换机的特定端口上配置和显示多生成树（MST）设置。

当DOT1S遇到严重的错误情况时，端口可以变成诊断禁用(D-Disable)。最常见的原因是DOT1S软件发生BPDU泛洪。泛洪标准是DOT1S在3秒间隔内接收到超过15个bpdu。DOT1S D-Disable的其他原因非常罕见。

要查看生成树MST端口状态，请执行以下操作：

L2交换管理 > STP管理 > 高级管理 > MST树端口属性管理



提示： 如果交换机上未配置MST实例，屏幕将显示no MST Available（无MST可用）消息，并且不会显示下面的字段描述表中显示的字段。

- 1. 使用MST ID从现有MST实例中选择一个MST实例。
- 2. 使用接口选择与所选MST实例关联的VLAN关联的物理或端口通道接口之一。
- 3. 使用端口优先级指定所选MST实例中特定端口的优先级。

端口优先级以16的倍数设置。例如，如果尝试将优先级设置为0到15之间的任何值，则将其设置为0。如果尝试将其设置为16到（2*16-1）之间的任何值，则将其设置为16，依此类推。

- 4. 使用端口路径成本将路径成本设置为所选MST实例中指定端口的新值。
它的取值范围为1到2000000000。

- 5. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

下表描述了生成树CST配置屏幕上显示的只读MST端口配置信息。

表51. MST端口状态

字段	描述
路径开销自动配置模式	显示是否自动计算路径成本（启用）或未计算路径成本（禁用）。如果端口路径成本的配置值为零，则根据端口的链路速度计算路径成本。
Port ID	所选MST实例中指定端口的端口标识符。它由端口优先级和端口的接口号组成。

Port Uptime Since Last Clear Counters	自上次清除计数器以来的时间，以天、小时、分钟和秒为单位显示。
STP工作模式	与端口或端口通道关联的生成树协议管理模式。可能的值为启用或禁用。
端口转发状态	此端口的转发状态。
Port Role	每个启用的MST桥接端口为每棵生成树分配一个端口角色。端口角色是以下值之一：根端口、指定端口、备用端口、备份端口、主端口或禁用端口。
指派根桥	所选MST实例的根网桥。它由网桥优先级和网桥的基本MAC地址组成。
Designated Cost	指定端口提供给LAN的路径成本。
Designated Bridge	具有指定端口的网桥的网桥标识符。它由网桥优先级和网桥的基本MAC地址组成。
Designated Port	为LAN提供最低成本的指定网桥上的端口标识符。它由端口优先级和端口的接口号组成。

3.5.8. 查看STP统计信息

您可以查看关于每个端口上传输和接收的网桥协议数据单元（BPDU）的数量和类型的信息。

要查看生成树统计信息，请执行以下操作：

L2交换管理 > STP管理 > 高级管理 > 生成树包文统计

接口	STP BPDUs 接收统计	STP BPDUs 发送统计	RSTP BPDUs 接收统计	RSTP BPDUs 发送统计	MSTP BPDUs 接收统计	MSTP BPDUs 发送统计
0/1	0	0	0	0	0	0
0/2	0	0	0	0	0	0
0/3	0	0	0	0	0	0
0/4	0	0	0	0	0	0
0/5	0	0	0	0	0	0
0/6	0	0	0	0	0	0
0/7	0	0	0	0	0	0
0/8	0	0	0	0	0	0
0/9	0	0	0	0	0	0
0/10	0	0	0	0	0	0
0/11	0	0	0	0	0	0
0/12	0	0	0	0	0	0

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表介绍了STP统计屏幕上的可用信息。

表52. STP统计数据

字段	描述
----	----

接口	选择交换机的一个物理或端口通道接口。
STP BPDUs 接收统计	在所选端口接收的STP BPDU数。
STP BPDUs 发送统计	从所选端口传输的STP BPDU数。
RSTP BPDUs 接收统计	在所选端口接收的RSTP BPDU数。
RSTP BPDUs 发送统计	从所选端口传输的RSTP BPDU数。
MSTP BPDUs 接收统计	在所选端口接收的MSTP BPDU数。
MSTP BPDUs 发送统计	从所选端口传输的MSTP BPDU数。

3.6.组播

组播IP流量是指向主机组的流量。主机组由D类IP地址标识，范围为224.0.0.0 ~ 239.255.255.255。

3.6.1. 查看MFDB表

组播转发数据库保存所有活动组播地址表项的端口成员信息。该表项的key由VLAN ID和MAC地址对组成。条目可以包含多个协议的数据。

要查看MFDB表，请执行以下操作：

L2交换管理 > 组播管理 > MFDB > 组播地址表



表53. MFDB表

字段	描述
MAC 地址	为其请求数据的组播MAC地址。
VLAN ID	与组播MAC地址相关的VLAN ID。
类别	这将显示条目的类型。静态条目是由最终用户配置的条目。动态条目作为学习过程或协议的结果添加到表中。
所属组件	这是负责组播转发数据库中此项的组件。可能的值为IGMP窥探、GMRP、静态过滤和MLD窥探。
描述	此组播表项的文本说明。可能的值包括管理配置、网络配置和网络辅助。
转发接口	通过组合所有转发接口并删除列为静态筛选接口的接口，可以导出生成的转发列表。

3.6.2. 查看MFDB统计信息

要查看MFDB统计信息，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。

- 4. 在web浏览器地址字段中输入交换机的IP地址。
交换机的默认IP地址为 192.168.10.12 。
此时将显示登录屏幕。
- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **L2交换管理 > 组播管理 > MFDB > 组播地址表统计**



下表介绍了 MFDB 统计字段。

表54. MFDB统计数据

字段	描述
系统支持的最大组播地址表项数量	组播转发数据库表可以容纳的最大条目数。
系统曾经分配的最大的组播表项数量	自上次重置以来，组播转发数据库表中存在的最大条目数。该值也称为MFDB高水位线。
当前分配的表项数量	组播转发数据库表中的当前条目数。

3.6.3. IGMP Snooping

IGMP snooping (Internet Group Management Protocol snooping)是一种允许交换机在交换机上智能转发组播流量的功能。组播IP流量是指向主机组的流量。主机组由D类IP地址标识，范围为224.0.0.0 ~ 239.255.255.255。通过IGMP查询报文和IGMP报告报文，交换机只将流量转发到请求组播流量的端口。这将防止交换机将流量广播到所有端口，并可能影响网络性能。

这种方法适用于希望所有连接节点都能看到或处理的广播包。然而，在多播包的情况下，这种方法可能导致网络带宽的使用效率较低，特别是当包仅用于少数节点时。数据包被淹没到没有节点接收数据包的网段中。虽然节点很少会产生任何处理开销来过滤指向非请求组地址的包，但在多播包被淹没的一段时间内，它们无法将新的包传输到共享媒体上。浪费带宽的问题在不共享局域网段时更加严重，例如在全双工链路中。

允许交换机窥探IGMP数据包是解决这个问题的一项创造性努力。当IGMP报文在整个网络中

被转发时，交换机使用其中的信息来确定哪些网段接收到定向到组地址的报文。

3.6.3.1. 配置 IGMP Snooping

配置IGMP snooping的相关参数，IGMP snooping用于组播流量建立转发列表。

提示： 您必须以管理员用户身份登录，管理员具有读/写访问权限才能更改此屏幕上的数据。

要配置IGMP snooping，请执行以下操作：

L2交换管理 > 组播管理 > IGMP Snooping > 配置



1. 单击the Admin mode **Enable** or **Disable** radio button
This specifies the administrative mode for IGMP snooping for the switch. The default is Disable.
2. Use the **Validate IGMP IP header** option to **Enable** or **Disable** header validation for all IGMP versions.
If Validate IGMP IP Header is enabled, then IGMP IP header checks for Router Alert option, ToS and TTL. The default value is Enable.
3. 单击the Proxy Querier Mode **Enable** or **Disable** 单选按钮
This enables or disables IGMP proxy querier on the system. If disabled, then the IGMP proxy query with source IP 0.0.0.0 is not sent in response to IGMP leave packet. the default value is Enable.
4. 单击 **应用** 按键
更新的配置参数将发送到交换机，配置更改将立即生效。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表在屏幕上显示有关全局IGMP snooping状态和统计信息的信息。

表55. IGMP snooping配置

字段	描述
已处理组播控制帧数量统计	CPU处理的组播控制帧数。
已启用IGMP Snooping功能的端口	当前为IGMP snooping启用的所有接口的列表。
已启用IGMP Snooping功能的VLAN列表	Displays VLAN IDs enabled for IGMP snooping.

3.6.3.2. 接口配置IGMP snooping

要为接口配置IGMP snooping，请执行以下操作：

L2交换管理 > 组播管理 > IGMP Snooping > 端口配置

接口	工作模式	成员端口的老化时间(2-3600秒)	最大响应时间(1-25秒)	连接组播路由器接口等待过期时间(0-3600秒)	快速离开模式
☐ 0/1	关闭	260	10	0	关闭
☐ 0/2	关闭	260	10	0	关闭
☐ 0/3	关闭	260	10	0	关闭
☐ 0/4	关闭	260	10	0	关闭
☐ 0/5	关闭	260	10	0	关闭
☐ 0/6	关闭	260	10	0	关闭
☐ 0/7	关闭	260	10	0	关闭
☐ 0/8	关闭	260	10	0	关闭

屏幕列出了所有物理、LAG接口。

1. 使用接口复选框选择接口。
2. 在管理模式字段中，选择禁用或启用。

这为交换机的IGMP snooping指定所选接口的接口模式。默认设置为禁用。

3. 使用组成员资格间隔可指定交换机在从组中删除特定接口之前，等待特定接口上特定组的报告的时间量。

输入一个介于1到3600秒之间的值。默认值为260秒。

4. 使用“最大响应时间”（Max Response Time）指定交换机在接口上发送查询后等待的时间量，因为它没有在该接口上收到特定组的报告。

输入大于或等于1且小于组成员资格间隔（以秒为单位）的值。默认值为10秒。配置的值必须小于组成员资格间隔。

5. 使用“当前过期时间”指定交换机在从连接了组播路由器的接口列表中删除查询之前等待接收接口查询的时间量。

输入一个介于0和3600秒之间的值。默认值为0秒。值为零表示无限超时，即无过期。

6. 使用快速离开管理模式为特定界面选择快速离开模式。

默认设置为禁用。

7. 使用代理查询器模式为特定接口选择代理查询器模式。

如果禁用，则不会发送源IP为0.0.0.0的IGMP代理查询以响应IGMP离开数据包。默认值为Enable。

8. 单击 **应用** 按钮

这些设置将应用于开关。配置更改立即生效。

3.6.3.3. VLAN配置IGMP snooping

要为VLAN配置IGMP snooping设置，请执行以下操作：

L2交换管理 > 组播管理 > IGMP 组播 > 组播VLAN配置

VLAN ID	工作模式	未知组播报文转发模式	快速离开模式	成员端口的老化时间(2-3600 秒)	最大响应时间(1-25 秒)	组播路由接口等待过期时间(0-3600 secs)	Report 报文抑制
☐ 1	关闭	Flooding	关闭	260	10	0	关闭

1. 要在VLAN上启用IGMP snooping，请输入VLAN ID并配置IGMP snooping值：

- **工作模式** - 使用管理模式启用或禁用指定VLAN ID的IGMP snooping。
- **快速离开模式** - 使用快速离开管理模式启用或禁用指定VLAN ID的IGMP snooping快速离开模式。
- **成员端口的老化时间** - 使用组成员资格间隔设置的组成员资格间隔值，IGMP snooping指定的VLAN ID。有效范围为最大响应时间+1到3600秒。
- **最大响应时间** - 使用最大响应时间设置指定VLAN ID的IGMP snooping的最大响应时间值。有效范围为1到组成员资格间隔-1。其值必须大于组成员资格间隔值。
- **组播路由接口等待过期时间** - 使用组播路由器到期时间为指定VLAN ID设置IGMP snooping的组播路由器到期时间值。有效范围为0到3600秒。
- **Report 报文抑制** - 使用报告抑制模式启用或禁用指定VLAN ID的IGMP snooping报告抑制模式。IGMP snooping报告抑制允许通过构建第3层成员表抑制组播主机发送的IGMP报告，从而仅将非常需要的报告发送到IGMP路由器以接收组播通信量。结果，发送到IGMP路由器的组播报告通信量减少。

2. 要修改VLAN的IGMP snooping设置，请执行以下操作：

- a. 选中VLAN ID旁边的复选框
- b. 更新参数设定值
- c. 单击 **应用** 按钮

设置被发送到交换机。

3.6.3.4. 配置组播路由器

可以将该接口配置为组播路由器的接口。交换机侦听到的所有IGMP报文都将从该接口转发到可达的组播路由器。大多数情况下不需要配置，因为交换机会自动检测组播路由器，并相应地转发IGMP报文。在复杂的网络中，只有当组播路由器总是能接收到来自交换机的IGMP报文时，才需要配置。

要配置组播路由器，请执行以下操作：

L2交换管理 > 组播管理 > IGMP Snooping > 组播路由端口配置



- 1. 使用接口选择需要配置的接口。
- 2. 在组播路由器字段中，选择启用或禁用。
- 3. 单击 应用 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

3.6.3.5. 配置组播路由器VLAN

配置接口只将来自VLAN ID 的IGMP报文转发给该接口下的组播路由器。由于交换机会自动检测组播路由器并转发IGMP报文，所以大多数情况下不需要配置。在复杂的网络环境中，只有当组播路由器需要始终接收到交换机发来的IGMP报文时，才需要配置组播路由。

要配置组播路由器VLAN，请执行以下操作：

L2交换管理 > 组播管理 > IGMP Snooping > 组播路由VLAN配置



1. 使用“Interface”选择接口。
2. 使用VLAN ID选择VLAN ID。
3. 在组播路由器字段中，选择启用或禁用。
4. 单击 应用 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

3.6.3.6. IGMP snooping查询器概述

IGMP snooping要求一个中央交换机或路由器定期查询网络上的所有终端设备，以宣布它们的组播成员身份。该中心设备是IGMP查询器。IGMP查询响应，即IGMP报告，以端口对端口的方式更新交换机的当前组播组成员。如果交换机没有及时收到更新的成员信息，则停止向终端设备所在端口转发组播。

您可以在网络上以及VLAN上分别配置和显示有关IGMP snooping查询器的信息。

3.6.3.7. 配置IGMP snooping查询器

您可以为IGMP snooping查询器配置参数。只有具有读/写访问权限的用户才能更改此屏幕上的数据。

要配置IGMP snooping查询器设置，请执行以下操作：

L2交换管理 > 组播管理 > IGMP Snooping > 查询器配置



1. 使用Querier管理模式为交换机的IGMP snooping选择管理模式。
默认设置为禁用。
2. 在 **Querier 全局IP地址** 字段中，键入IP地址。
这指定在定期IGMP查询中用作源地址的侦听查询器地址。在发送查询的VLAN上未配置地址时，使用此地址。
3. 使用IGMP版本指定定期IGMP查询中使用的IGMP协议版本。
范围为1到2。默认值为2。
4. 使用查询间隔（秒）指定窥探查询器发送的定期查询之间的时间间隔（秒）。
查询间隔必须是介于1和1800之间的值。默认值为60。
5. 使用查询器到期时间间隔（秒）指定删除最后一个查询器信息后的时间间隔（秒）。
查询器到期时间间隔必须是介于60和300之间的值。默认值为125。
6. 单击 **应用** 按钮
更新的配置参数将发送到交换机，配置更改将立即生效。
屏幕显示为IGMP snooping查询器启用的VLAN ID。

3.6.3.8. VLAN配置IGMP snooping查询器

可以将IGMP查询器配置为与网络上的VLAN一起使用。

要配置查询器VLAN设置，请执行以下操作：

L2交换管理 > 组播管理 > IGMP Snooping > 查询器VLAN配置

1. 要为IGMP snooping创建新的VLAN ID，请从VLAN ID字段中选择新条目，并填写以下字段。

您还可以设置预先配置的窥探查询器参数。

- **VLAN ID.** 要为修改查询器配置参数的VLAN ID。
- **工作模式** 启用或禁用VLAN上的IGMP snooping查询器。
- **Querier 选举模式.** 启用或禁用查询器参与模式。
 - **Disabled.** 当在VLAN中看到相同版本的查询程序时，侦听查询程序将转移到非查询程序状态。
 - **Enabled.** 侦听查询程序参与查询程序选举，其中最小的IP地址作为该VLAN中的查询程序运行。另一个查询程序转到非查询程序状态。
- **在VLAN上Querier的IP地址.** 指定在指定VLAN上发送的定期IGMP查询中用作源地址的侦听查询器IP地址。

2. 单击 **应用** 按钮

这些设置将应用于交换机，配置更改立即生效

下表描述了屏幕上显示的不可配置信息。

表56. Querier VLAN配置

字段	描述
工作状态	VLAN上IGMP snooping查询器的操作状态。它可以处于以下任一状态： • Querier: 这个snooping交换机是VLAN内的查询器。侦听开关发送周期性查询的时间间隔等于配置的查询器查询的时间间隔。如果在VLAN中发现更好的查询器，则切换到非查询器模式。 • Non-Querier: VLAN内的snooping模式为innNon-querier。如果查询器超时时间过长，则切换到查询器模式。 • Disabled: 侦听查询器在VLAN上不起作用。当VLAN上没有IGMP snooping功能，或者没有配置查询器地址或没有配置网管地址时，将切换到去使能模式。
工作的版本	查询器的可操作IGMP协议版本。

上一次查询的地址	在VLAN上窥探查询的最后一个查询器的IP地址。
上一次查询的版本	在VLAN上窥探查询的最后一个查询器的IGMP协议版本。
工作时最大的响应时间	显示窥探查询器发送的查询中使用的最大响应时间。

3.6.4. 配置 MLD Snooping

配置MLD snooping的参数，MLD snooping用于组播流量建立转发列表。只有具有读写访问权限的用户才能更改此屏幕上的数据。

要配置MLD snooping，请执行以下操作：

L2交换管理 > 组播管理 > MLD Snooping > IPv6组播全局配置.



1. 使用MLD snooping管理模式为交换机选择MLD snooping的管理模式。
默认设置为禁用。
2. 选择代理查询器模式启用或禁用单选按钮。
这将启用或禁用系统上的MLD代理查询器。如果禁用，则不会发送源IP为0::0的MLD代理查询来响应MLD LEVE数据包。如果启用，则发送MLD代理查询。默认值为Enable。
3. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表描述了不可配置的MLD snooping配置字段。

表57. MLD snooping配置

字段	Definition
已处理组播控制帧数量统计	CPU处理的组播控制帧数。

已启用MLD Snooping的接口	当前为MLD snooping启用的所有接口的列表。
已启用MLD Snooping的VLAN列表	显示为MLD snooping启用的VLAN ID。

3.6.4.1. 配置MLD snooping接口

要配置MLD snooping接口，请执行以下操作：

L2交换管理 > 组播管理 > MLD Snooping > 端口配置

将显示所有物理、LAG接口。

1. 使用界面复选框选择界面。
2. 使用管理模式为所选接口选择接口模式，以便对交换机进行MLD snooping。

默认设置为禁用。

3. 使用组成员资格间隔（秒）指定交换机在从组中删除某个接口之前，等待该接口上某个特定组的报告的时间量。

有效范围为2到3600秒。配置的值必须大于最大响应时间。默认值为260秒。

4. 使用最大响应时间（秒）指定交换机在接口上发送查询后等待的时间量，因为它没有在该接口上收到特定组的报告。

输入大于或等于1且小于组成员资格间隔（以秒为单位）的值。默认值为10秒。配置的值必须小于组成员资格间隔。

5. 使用“当前过期时间”指定交换机在从连接了组播路由器的接口列表中删除查询之前等待接收接口查询的时间量。

输入一个介于0和3600秒之间的值。默认值为0秒。值为零表示无限超时，即无过期。

6. 使用快速离开管理模式为特定界面选择快速离开模式。默认设置为禁用。

7. 选择代理查询器模式以启用或禁用系统上的MLD代理查询器。

如果禁用，则不会发送源IP为0::0的MLD代理查询来响应MLD LEVE数据包。如果启用，则发

送MLD代理查询。默认值为Enable。

3.6.4.2. 配置MLD VLAN设置

要配置MLD VLAN设置，请执行以下操作：

L2交换管理 > 组播管理 > MLD Snooping > IPv6组播VLAN配置

VLAN ID	工作模式	未知组播报文转发模式	快速离开模式	成员端口的老化时间(2-3600 秒)	最大响应时间(1-25 秒)	组播路由接口等待过期时间(0-3600 secs)	Report 报文抑制
☐ 1	关闭	Flooding	关闭	260	10	0	关闭

1. 使用VLAN ID设置启用MLD snooping的VLAN ID。
2. 使用管理模式为指定的VLAN ID启用MLD侦听。
3. 使用快速离开管理模式启用或禁用指定VLAN ID的MLD snooping快速离开模式。
4. 使用组成员身份间隔为指定VLAN ID的MLD snooping的组成员身份间隔设置值。
有效范围为（最大响应时间+1）到3600。
5. 使用最大响应时间设置指定VLAN ID的MLD侦听的最大响应时间值。
有效范围为1到（组成员资格间隔-1）。其值必须小于组成员资格间隔值。
6. 使用组播路由器到期时间为指定VLAN ID的MLD snooping设置组播路由器到期时间的值。
有效范围为0到3600。
7. 单击 **应用** 按钮
更新的配置将发送到交换机。

3.6.4.3. 在接口上启用或禁用组播路由器

要在接口上启用或禁用组播路由器，请执行以下操作：

L2交换管理 > 组播管理 > MLD Snooping > 组播路由端口配置



1. 接口: 单击选择需要修改的接口
2. 使用组播路由器在所选接口上启用或禁用组播路由器。
3. 单击 应用 按钮

更新的配置将发送到交换机。

3.6.4.4. 配置组播路由器VLAN设置

要配置组播路由器VLAN设置，请执行以下操作：

L2交换管理 > 组播管理 > MLD Snooping > 组播路由VLAN配置



1. 接口: 单击选择需要修改的接口
2. 使用VLAN ID选择VLAN ID。
3. 使用组播路由器启用或禁用VLAN ID的组播路由器。
4. 单击 应用 按钮

更新的配置将发送到交换机。

3.6.4.5. 配置MLD snooping查询器

您可以为MLD snooping查询器配置参数。只有具有读/写访问权限的用户才能更改此屏幕上的数据。

要配置MLD snooping查询器，请执行以下操作：

L2交换管理 > 组播管理 > MLD Snooping > 查询器配置

- 1. 使用Querier Admin Mode为交换机的MLD snooping选择管理模式。
默认设置为禁用。
 - 2. 使用查询器地址指定在定期MLD查询中用作源地址的侦听查询器地址。
在发送查询的VLAN上未配置地址时，使用此地址。支持的IPv6格式为x:x:x:x:x:x:x和x::x。
 - 3. 使用MLD版本指定定期MLD查询中使用的MLD协议版本。
 - 4. 使用查询间隔（秒）指定snooping查询器发送的定期查询之间的时间间隔（秒）。
查询间隔必须是1到1800之间的值。默认值为60。
 - 5. 使用查询器到期时间间隔（秒）指定删除最后一个查询器信息后的时间间隔（秒）。
查询器到期时间间隔必须是介于60到300之间的值。默认值为60。
- 屏幕显示为MLD snooping查询器启用的VLAN ID。

3.6.4.6. 配置MLD snooping查询器VLAN设置

要配置MLD snooping查询器VLAN设置：

L2交换管理 > 组播管理 > MLD Snooping > 查询器VLAN配置

1. 使用VLAN ID选择管理上启用MLD snooping查询器且VLAN数据库中存在VLAN的VLAN ID。
2. 使用Querier选举参与模式启用或禁用MLD snoopingQuerier参与选举模式。
禁用此模式时，在VLAN中检测到另一个相同版本的查询器时，snooping查询器将移动到非查询器状态。启用此模式时，snooping查询器将参与查询器选择，其中最低IP地址将赢得查询器选择，并作为该VLAN中的查询器运行。另一个查询器移动到非查询器状态。
3. 使用查询器VLAN地址指定snooping查询器地址，该地址将用作在指定VLAN上发送的定期MLD查询中的源地址。

下表描述了屏幕上显示的不可配置信息。

表58. 查询器VLAN配置

字段	描述
工作状态	VLAN上MLD snooping查询器的操作状态。它可以处于以下任一状态： • Querier: 这个Snooping交换机是VLAN内的查询器。侦听开关发送周期性查询的时间间隔等于配置的查询器查询的时间间隔。如果侦听交换机在VLAN中看到更好的查询器，则切换到非查询器模式。 • Non-Querier: VLAN内的Snooping交换机为非查询模式。如果查询器超时时间超时，则切换到查询器模式。 • Disabled: VLAN上不能使用侦听查询器。当VLAN上没有MLD snooping，或者没有配置查询器地址或没有配置网管地址时，查询器将移到去使能模式。
工作的版本	查询器的操作MLD协议版本。
上一次查询的地址	在VLAN上snooping查询的最后一个查询器的IP地址。
上一次查询的版本	在VLAN上snooping查询的最后一个查询器的MLD协议版本。
工作时最大的响应时间	显示snooping查询器发送的查询中使用的最大响应时间。

3.7.MVR

您可以配置MVR模块的基本、高级、组、接口或组成员身份设置。

3.7.1. 配置基本MVR设置

要配置基本MVR设置，请执行以下操作：

L2交换管理 > MVR > 基本管理> MVR 协议配置.

The screenshot shows the 'MVR Group Management' configuration page. On the left, there's a sidebar with 'MVR Group Management' and sub-items like 'Basic Management Information', 'MVR Protocol Configuration', and 'Advanced Management Information'. The main area is titled 'MVR Protocol Configuration' and contains several rows of settings:

- MVR Global Mode:** Radio buttons for 'Off' (selected) and 'On'.
- Specify VLAN for receiving MVR data:** A text box containing '1' with a range '(1 - 4094)'.
- Maximum number of MVR groups supported by the system:** A fixed value of '256'.
- Currently allocated MVR groups:** A fixed value of '0'.
- MVR Global Query Response Time:** A text box containing '5' with a range '(1 - 100 秒)'.
- MVR Operation Mode:** Radio buttons for 'compatible' (selected) and 'dynamic'.

At the top right, there are buttons for 'Apply' (应用) and 'Refresh' (刷新).

1. 使用MVR Running启用或禁用MVR功能。
出厂默认设置为禁用。
2. 使用MVR组播VLAN指定接收MVR组播数据的VLAN。
所有源端口都属于此VLAN。该值可以设置在1到4093的范围内。默认值为1。
3. 使用MVR全局查询响应时间设置在接收器端口上等待IGMP报告成员身份的最长时间。
此时间仅适用于接收方端口离开处理。当从接收器端口发送IGMP查询时，交换机将等待IGMP组成员资格报告的默认或配置的MVR查询时间，然后再从组播组成员资格中删除该端口。该值等于十分之一秒。范围从十分之一到十分之一百。出厂默认值为十分之五或一半。
4. 使用MVR模式指定MVR操作模式。
可能的值是兼容的或动态的。出厂默认值是兼容的。
5. 单击 应用 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表描述了屏幕上显示的不可配置信息。

表59. MVR配置

字段	Definition
系统中MVR支持的最大组播组数	MVR支持的最大组播组数。
当前已分配的MVR组播组数	显示分配的MVR组的当前数目。

3.7.2. 配置高级MVR设置

要配置高级MVR设置，请执行以下操作：

L2交换管理 > MVR > 高级管理 > MVR协议配置

The screenshot displays the 'MVR Protocol Configuration' page. On the left, a sidebar lists navigation options: 'Basic Management Information', 'Advanced Management Information', 'MVR Protocol Configuration' (selected), 'MVR Group Configuration', 'MVR Port Attribute Configuration', 'MVR Group Member Configuration', and 'MVR Protocol Packet Statistics'. The main area contains the following configuration items:

- MVR Global Mode:** Radio buttons for 'Disabled' (selected) and 'Enabled'.
- Designated VLAN for Receiving MVR Data:** A text box containing '1' with a range '(1 - 4094)'.
- Maximum MVR Groups Supported:** A read-only field showing '256'.
- Current MVR Groups:** A read-only field showing '0'.
- MVR Global Query Response Time:** A text box containing '5' with a range '(1 - 100 s)'.
- MVR Operation Mode:** Radio buttons for 'compatible' (selected) and 'dynamic'.

Buttons for 'Apply' and 'Refresh' are located at the top right of the configuration area.

8. 使用MVR Running启用或禁用MVR功能。
出厂默认设置为禁用。
9. 使用MVR组播VLAN指定接收MVR组播数据的VLAN。
所有源端口都属于此VLAN。该值可以设置在1到4093的范围内。默认值为1。
10. 使用MVR全局查询响应时间设置在接收器端口上等待IGMP报告成员身份的最长时间。
此时间仅适用于接收方端口离开处理。当从接收器端口发送IGMP查询时，交换机将等待IGMP组成员资格报告的默认或配置的MVR查询时间，然后再从组播组成员资格中删除该端口。该值等于十分之一秒。范围从十分之一到十分之一百。出厂默认值为十分之五或一半。
11. 使用MVR模式指定MVR操作模式。
可能的值是兼容的或动态的。出厂默认值是兼容的。
12. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表描述了屏幕上显示的不可配置信息。

表60. MVR配置

字段	Definition
系统中MVR支持的最大组播组数	MVR支持的最大组播组数。
当前已分配的MVR组播组数	显示分配的MVR组的当前数目。

3.7.3. 配置MVR组

要配置MVR组，请执行以下操作：

L2交换管理 > MVR > 高级管理 > MVR组配置

The screenshot shows the 'MVR组配置' (MVR Group Configuration) page. The sidebar on the left has 'MVR组配置' selected under 'MVR组管理'. The main area has a table with the following columns: 'MVR Group IP', '状态' (Status), '参与MVR组的端口' (Ports participating in MVR group), and '创建连续的组数(1-256)' (Create continuous groups (1-256)). There are buttons for '+ 增加' (Add), '- 删除' (Delete), and '刷新' (Refresh) at the top right of the table area.

1. 使用MVR组IP指定新MVR组的IP地址。
2. 使用计数指定连续MVR组的数量。

这有助于通过单击Add按钮创建多个MVR组。如果字段为空，则单击按钮仅创建一个新组。对于每个特定组，该字段显示为空。范围从1到256。

3. 单击 增加 按钮

添加MVR组。

4. 要删除选定的MVR组，请单击 删除 按钮

下表描述了屏幕上显示的不可配置信息。

表61. MVR组配置

字段	Definition
状态	特定MVR组的状态。
参与MVR组的端口	参与特定MVR组的端口列表。

3.7.4. 配置MVR接口

要配置MVR接口，请执行以下操作：

L2交换管理 > MVR > 高级管理 > MVR端口属性配置

The screenshot shows the 'MVR端口属性配置' (MVR Port Attribute Configuration) page. The sidebar on the left has 'MVR端口属性配置' selected under 'MVR组管理'. The main area has a table with the following columns: '接口' (Interface), '工作模式' (Work Mode), '类别' (Category), '立即离开模式' (Immediate Leave Mode), and '状态' (Status). The table lists interfaces from 0/1 to 0/10, all with '关闭' (Closed) status. There are buttons for '应用' (Apply) and '刷新' (Refresh) at the top right of the table area.

每个端口的状态显示。

1. 使用接口选择接口。
2. 使用管理模式启用或禁用端口上的MVR。
出厂默认设置为禁用。
3. 使用类型将端口配置为MVR接收器端口或源端口。
默认端口类型为“无”。
4. 使用立即休假可启用或禁用端口上MVR的立即休假功能。
出厂默认设置为禁用。
5. 单击 应用 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

3.7.5. 配置MVR组成员

要配置MVR组成员身份，请执行以下操作：

L2交换管理 > MVR > 高级管理 > MVR组成员配置



1. 使用组IP指定MVR组的IP组播地址。
2. 使用端口列表查看所选MVR组成员的配置列表。
您可以使用此端口列表将所选端口添加到此MVR组。
3. 单击 应用 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

3.7.6. 查看MVR统计信息

要查看MVR统计信息，请执行以下操作：

L2交换管理 > MVR > 高级管理 > MVR协议包文统计



要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表描述了屏幕上显示的不可配置信息。

表62. MVR统计数据

字段	Definition
接收到的IGMP查询包文数	收到的IGMP查询数。
接收到的IGMP Report V1包文统计数	收到的IGMP报告数V1。
接收到的IGMP Report V1包文统计数	接收到的IGMP报告数V2。
接收到的IGMP Leave包文统计数	收到的IGMP叶数。
发送IGMP Query包文统计数	传输的IGMP查询数。
发送IGMP Report V1包文统计数	传输的IGMP报告数V1。
发送IGMP Report V2包文统计数	传输的IGMP报告数V2。
发送IGMP Leave包文统计数	传输的IGMP叶数。
接收IGMP报文失败统计数	IGMP数据包接收失败的次数。
IGMP报文发送失败统计数	IGMP数据包传输失败的次数。

3.8.Auto-VoIP

您可以配置基于协议的端口设置和OUI设置。

3.8.1. 配置基于协议的端口设置

要配置基于协议的端口设置，请执行以下操作：

L2交换管理 > Auto-VoIP > 基本配置 > 端口属性配置

系统管理

L2交换管理

路由管理

QoS管理

安全管理

监测管理

维护

端口管理

汇聚组管理

VLAN管理

MAC管理

STP管理

IGMP组播管理

MVR组播管理

Auto-VoIP

UDLD管理

环路保护

Auto-VoIP

基本配置

端口属性配置

OUI-based

应用

刷新

端口属性配置 - 全局配置

指定优先级的处理类型

Traffic Class

重新分配的CoS值

7

端口属性配置 - 端口配置

Interface	Auto VoIP工作模式	当前工作状态
☐ 0/1	关闭	Down
☐ 0/2	关闭	Down
☐ 0/3	关闭	Down
☐ 0/4	关闭	Down
☐ 0/5	关闭	Down
☐ 0/6	关闭	Down
☐ 0/7	关闭	Down
☐ 0/8	关闭	Down
☐ 0/9	关闭	Down
☐ 0/10	关闭	Down
☐ 0/11	关闭	Down
☐ 0/12	关闭	Down

1. 在“优先级类型”字段中，选择“Traffic Class”或“Remark”。

这将指定优先级的类型。

2. 在“重新分配的CoS值”列表中，指定启用备注CoS时要为语音VLAN上接收的数据包重新分配的CoS标记值。

3. 单击 应用 按钮

交换机会根据输入的值进行更新。要使交换机在整个电源循环中保留新值，您必须执行保存。

3.8.2. 配置 Auto-VoIP 基于OUI-Based 的属性

要配置基于OUI的Auto-VoIP属性，请执行以下操作：

L2交换管理 > Auto-VoIP > OUI-based > 属性配置



1. 在VoIP VLAN ID字段中，键入交换机的VoIP VLAN ID。
自动VoIP没有默认VLAN，您必须先为其创建VLAN。
2. 在基于OUI的优先级列表中，选择交换机基于OUI的优先级。

默认值为7。

3. 单击 **应用** 按钮

交换机会根据输入的值进行更新。要使交换机在整个电源循环中保留新值，您必须执行保存。

3.8.3. 基于OUI的端口设置

要配置基于OUI的Auto-VoIP 端口设置，请执行以下操作：

L2交换管理 > Auto-VoIP > OUI-based > 端口属性配置



当前工作状态字段表示各接口当前的运行状态。

1. 使用接口复选框选择接口。

2. 在 **Auto VoIP工作模式** 字段中, 选择 **关闭** 或 **启用** .默认情况下禁用自动VoIP。

3. 单击 **应用** 按钮

交换机会根据输入的值进行更新。要使交换机在整个电源循环中保留新值, 您必须执行保存。

3.8.4. 配置OUI表

要配置OUI表, 请执行以下操作:

L2交换管理 > Auto-VoIP > OUI-based > OUI表配置

The screenshot shows the 'OUI表配置 - Configuration' page. The left sidebar has a menu with 'Auto-VoIP' selected. The main area contains a table with the following data:

☐	Telephony OUI前缀地址值 (xx:xx:xx)	描述 (0-32 字符)
☐		
☐	00:01:E3	SIEMENS
☐	00:03:6B	CISCO1
☐	00:12:43	CISCO2
☐	00:0F:E2	H3C
☐	00:60:B9	NITSUKO
☐	00:D0:1E	PINTEL
☐	00:E0:75	VERILINK
☐	00:E0:BB	3COM
☐	00:04:0D	AVAYA1
☐	00:1B:4F	AVAYA2
☐	00:04:13	SNOM

1. 在“**Telephony OUI**”中输入要添加的VoIP OUI字冠, 格式为AA:BB:CC。
最多可配置128个OUI。

2. 在描述字段中, 输入OUI的描述。

描述的最大长度为32个字符。默认情况下, 配置中存在以下OUI:

- 00:01:E3 - SIEMENS
- 00:03:6B - CISCO1
- 00:12:43 - CISCO2
- 00:0F:E2 - H3C
- 00:60:B9 - NITSUKO
- 00:D0:1E - PINTEL
- 00:E0:75 - VERILINK
- 00:E0:BB - 3COM
- 00:04:0D - AVAYA1

- 00:1B:4F - AVAYA2

3. 单击 **增加** 按钮

将添加电话OUI条目。

4. 要删除已创建的条目，请单击“删除”按钮。

3.8.5. 查看 Auto-VoIP 状态

要查看 auto-VoIP 状态，请执行以下操作：

L2交换管理 > Auto-VoIP > OUI-based > Auto-VoIP工作状态



要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表描述了不可配置的自动VoIP状态信息。

表63. Auto-VoIP 状态

字段	描述
Auto-VoIP使用的VLAN ID	自动VoIP VLAN ID。
系统支持的最大语音通道数	支持的最大语音频道数。
检测到已使用的语音通道数	已成功设置VoIP通道优先级的数量。

3.9.UDLD管理

3.9.1. 系统配置

L2交换管理 > UDLD管理 > 系统配置

端口管理

汇聚组管理

VLAN管理

MAC管理

STP管理

IGMP组播管理

MVR组播管理

Auto-VoIP

UDLD管理

环路保护

UDLD管理

UDLD系统配置

UDLD端口属性配置

UDLD系统配置 - UDLD

全局工作模式

☒ 关闭
☐ 启用

消息发送间隔时间

(7-90 秒)

超时时间

(5-60 秒)

应用

刷新

- 全局模式。
关闭与启用。
- 发送间隔时间默认15s。
- 超时时间默认5s。

3.9.2. 端口配置

L2交换管理 > UDLD管理 > 端口配置

28 口交换机

系统管理

L2交换管理

路由管理

QoS管理

安全管理

监测管理

维护

简体中文

保存

退出

端口管理

汇聚组管理

VLAN管理

MAC管理

STP管理

IGMP组播管理

MVR组播管理

Auto-VoIP

UDLD管理

环路保护

UDLD管理

UDLD系统配置

UDLD端口属性配置

应用

Reset Port

刷新

UDLD端口属性配置 - UDLD端口属性配置

	Interface	Global Admin Mode	UDLD工作方式	UDLD 当前工作状态
☐	0/1	关闭	Normal	Not Applicable
☐	0/2	关闭	Normal	Not Applicable
☐	0/3	关闭	Normal	Not Applicable
☐	0/4	关闭	Normal	Not Applicable
☐	0/5	关闭	Normal	Not Applicable
☐	0/6	关闭	Normal	Not Applicable
☐	0/7	关闭	Normal	Not Applicable
☐	0/8	关闭	Normal	Not Applicable
☐	0/9	关闭	Normal	Not Applicable
☐	0/10	关闭	Normal	Not Applicable
☐	0/11	关闭	Normal	Not Applicable

- 全局管理（关闭与开启）。
- UDLD工作方式。

3.10. 环路保护

L2交换管理 > 环路保护 > 基本管理>工作状态

系统管理

L2交换管理

路由管理

QoS管理

安全管理

监测管理

维护

简体中文

保存

退出

端口管理

汇聚组管理

VLAN管理

MAC管理

STP管理

IGMP组播管理

MVR组播管理

Auto-VoIP

UDLD管理

环路保护

环路保护

基本管理信息

高级管理信息

应用

Clear Counters

刷新

工作状态 - 环路保护

环路保护全局工作模式	Disable
接收到的环路保护包文统计数	0
接收到的环路保护无效格式包文统计数	0
接收到的环路保护包文中属于其它设备发送的统计数	0
发送的环路保护包文统计数	0
发送失败的环路保护包文统计数	0
环路保护动作的统计数	0
最近的保护动作时间	No action even
当前检测到环路的状态	

L2交换管理 > 环路保护 > 高级管理信息>全局配置

系统管理

L2交换管理

路由管理

QoS管理

安全管理

监测管理

维护

简体中文

保存

退出

端口管理

汇聚组管理

VLAN管理

MAC管理

STP管理

IGMP组播管理

MVR组播管理

Auto-VoIP

UDLD管理

环路保护

环路保护

基本管理信息

高级管理信息

应用

刷新

全局配置 - 环路保护

全局工作模式	☒ 关闭 ☐ 启用
发送消息包文的间隔时间	5 (1-10 秒)
保护端口动作前需要接收到Pdu包文数	1 (1-10 包文)
从保护状态中自动恢复模式	☒ 关闭 ☐ 启用
自动恢复模式下超时时间	300 (30-86400 秒)

- 1. 全局管理（关闭与开启）。
- 2. 发送间隔。

L2交换管理 > 环路保护 > 高级管理信息>端口属性配置

系统管理

L2交换管理

路由管理

QoS管理

安全管理

监测管理

维护

简体中文

保存

退出

端口管理

汇聚组管理

VLAN管理

MAC管理

STP管理

IGMP组播管理

MVR组播管理

Auto-VoIP

UDLD管理

环路保护

环路保护

基本管理信息

高级管理信息

全局配置

端口属性配置

协议包文统计

端口工作状态

应用

Reset Port

刷新

端口属性配置 - 环路保护

Interface	工作模式	主动发送Pdu消息	动作模式	端口工作模式	端口环路保护状态
☐ 0/1	关闭	启用	Shutdown, Trap	Disable	---
☐ 0/2	关闭	启用	Shutdown, Trap	Disable	---
☐ 0/3	关闭	启用	Shutdown, Trap	Disable	---
☐ 0/4	关闭	启用	Shutdown, Trap	Disable	---
☐ 0/5	关闭	启用	Shutdown, Trap	Disable	---
☐ 0/6	关闭	启用	Shutdown, Trap	Disable	---
☐ 0/7	关闭	启用	Shutdown, Trap	Disable	---
☐ 0/8	关闭	启用	Shutdown, Trap	Disable	---
☐ 0/9	关闭	启用	Shutdown, Trap	Disable	---
☐ 0/10	关闭	启用	Shutdown, Trap	Disable	---
☐ 0/11	关闭	启用	Shutdown, Trap	Disable	---
☐ 0/12	关闭	启用	Shutdown, Trap	Disable	---

1. 工作模式（关闭与开启）。
2. 动作模式。

L2交换管理 > 环路保护 >高级管理信息>协议报文

系统管理

L2交换管理

路由管理

QoS管理

安全管理

监测管理

维护

简体中文

保存

退出

端口管理

汇聚组管理

VLAN管理

MAC管理

STP管理

IGMP组播管理

MVR组播管理

Auto-VoIP

UDLD管理

环路保护

环路保护

基本管理信息

高级管理信息

全局配置

端口属性配置

协议包文统计

端口工作状态

应用

Clear Counters

刷新

协议包文统计 - 环路保护

环路保护全局工作模式	Disable
接收到的环路保护包文统计数	0
接收到的环路保护无效格式包文统计数	0
接收到的环路保护包文中属于其它设备发送的统计数	0
发送的环路保护包文统计数	0
发送失败的环路保护包文统计数	0
环路保护动作的统计数	0
最近的保护动作时间	No action even
当前检测到环路的状态	

L2交换管理 > 环路保护 >高级管理信息>端口工作状态

28 口交换机

系统管理 **L2交换管理** 路由管理 QoS管理 安全管理 监测管理 维护

端口管理 汇聚组管理 VLAN管理 MAC管理 STP管理 IGMP组播管理 MVR组播管理 Auto-VoIP UDLD管理 **环路保护**

简体中文 保存 退出

环路保护

基本管理信息

高级管理信息

全局配置

端口属性配置

协议包文统计

端口工作状态

端口工作状态 - Loop Protect

Interface	工作模式	端口工作模式	连接状态	环路保护状态	环路保护工作计数	最近端口状态变化时间
0/1	Disable	Disable	Down		0	
0/2	Disable	Disable	UP		0	
0/3	Disable	Disable	Down		0	
0/4	Disable	Disable	Down		0	
0/5	Disable	Disable	Down		0	
0/6	Disable	Disable	Down		0	
0/7	Disable	Disable	Down		0	
0/8	Disable	Disable	Down		0	
0/9	Disable	Disable	Down		0	
0/10	Disable	Disable	Down		0	
0/11	Disable	Disable	Down		0	
0/12	Disable	Disable	Down		0	
0/13	Disable	Disable	Down		0	
0/14	Disable	Disable	Down		0	
0/15	Disable	Disable	Down		0	

合计 36 项, 显示 1 到 15 项, 每页显示 15 项

3.11. ERPS

L2交换管理 > ERPS > 基本管理>ERPS Ring Status

系统管理 **L2交换管理** 路由管理 QoS管理 安全管理 监测管理 维护

端口管理 汇聚组管理 VLAN管理 MAC管理 STP管理 IGMP组播管理 MVR组播管理 Auto-VoIP UDLD管理 环路保护 **ERPS**

刷新

ERPS

基本管理信息

ERPS Ring Status

高级管理信息

ERPS Ring Status - ERPS

环本地ID cc:52:91:0c:01:f8

ERPS Ring Status - ERPS Ring List

Ring ID	域 ID	域拓扑类型	环类型	节点类型	控制及协议 VLAN	RPL Port	RPL 端口状态	RL Port	RL 端口状态	环状态
1	1	None-Interconnection	major-ring	ring node	3001	0/26,Down	blocking	0/25,Down	blocking	protection

L2交换管理 > ERPS > 高级管理>ERPS Ring Status

系统管理 L2交换管理 路由管理 QoS管理 安全管理 监测管理 维护 简体中文 保存 退出

端口管理 汇聚组管理 VLAN管理 MAC管理 STP管理 IGMP组播管理 MVR组播管理 Auto-VoIP UDLD管理 环路保护 **ERPS**

ERPS

基本管理信息

高级管理信息

New ERPS Ring

ERPS Rings View

ERPS Ring Configuration

ERPS Ring Status

New ERPS Ring - Create New ERPS Ring

域 ID

ERPS 域拓扑类型

None-Interconnection Interconnection

Ring ID

New ERPS Ring - ERPS Ring List

Ring ID	域 ID	域拓扑类型	环类型	节点类型	控制及协议VLAN	环状态
1	1	None-Interconnection	major-ring	ring node	3001	protection

L2交换管理 > ERPS >高级管理>ERPS Ring View

系统管理 L2交换管理 路由管理 QoS管理 安全管理 监测管理 维护 简体中文 保存 退出

端口管理 汇聚组管理 VLAN管理 MAC管理 STP管理 IGMP组播管理 MVR组播管理 Auto-VoIP UDLD管理 环路保护 **ERPS**

ERPS

基本管理信息

高级管理信息

New ERPS Ring

ERPS Rings View

ERPS Ring Configuration

ERPS Ring Status

ERPS Rings View - ERPS Ring Configuration

Ring ID	域 ID	域拓扑类型	节点类型	节点类型	控制及协议VLAN	环状态
1	1	none-interconnection	major-ring	ring node	3001	protection

L2交换管理 > ERPS >高级管理>ERPS Ring Configuration

系统管理 L2交换管理 路由管理 QoS管理 安全管理 监测管理 维护 简体中文 保存 退出

端口管理 汇聚组管理 VLAN管理 MAC管理 STP管理 IGMP组播管理 MVR组播管理 Auto-VoIP UDLD管理 环路保护 **ERPS**

ERPS

基本管理信息

高级管理信息

New ERPS Ring

ERPS Rings View

ERPS Ring Configuration

ERPS Ring Status

ERPS Ring Configuration - ERPS Ring Configuration

Ring ID	域 ID	域拓扑类型	节点类型	节点类型	控制及协议VLAN	环状态
1	1	none-interconnection	major-ring	ring node	3001	protection

L2交换管理 > ERPS >高级管理>ERPS Ring Status

4. QoS管理

4.1. CoS管理

4.1.1. 基本管理

设置全局CoS

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。

- 7. 单击**QoS 管理> CoS管理>基本管理 > CoS 配置**

Cos管理

基本管理信息

CoS配置

高级管理信息

Cos配置 - 配置

☒ 全局配置

☐ 端口

All

全部端口的Trust模式

trust dot1p

应用

刷新

Cos配置 - 端口CoS配置

端口	Trust模式
☐ 0/1	trust dot1p
☐ 0/2	trust dot1p
☐ 0/3	trust dot1p
☐ 0/4	trust dot1p
☐ 0/5	trust dot1p
☐ 0/6	trust dot1p
☐ 0/7	trust dot1p
☐ 0/8	trust dot1p
☐ 0/9	trust dot1p
☐ 0/10	trust dot1p
☐ 0/11	trust dot1p
☐ 0/12	trust dot1p
☐ 0/13	trust dot1p
☐ 0/14	trust dot1p
☐ 0/15	trust dot1p

合计 62 项, 显示 1 到 15 项, 每页显示 15 项

<<

<

1

2

3

4

5

>

>>

提示： QoS 管理> CoS管理 >高级管理 > CoS 配置

8. 使用Global指定所有CoS可配置接口。
选项Global表示最近的全局配置设置。
9. 使用Interface指定基于每个接口的CoS配置。
10. 使用全局信任模式指定是否信任入口的特定数据包标记。全局信任模式可以是以下方式之一：

- untrusted
- trust dot1p
- trust ip-dscp

The default value is trust dot1p.

11. 使用接口信任模式来指定是否信任入口的特定数据包标记。“接口信任”模式可以是：

- untrusted
- trust dot1p
- trust ip-dscp

The default value is untrusted.

12. 单击 **应用** 按钮

更新后的配置信息发送到交换机。

4.1.2. 802.1p 优先级映射表

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

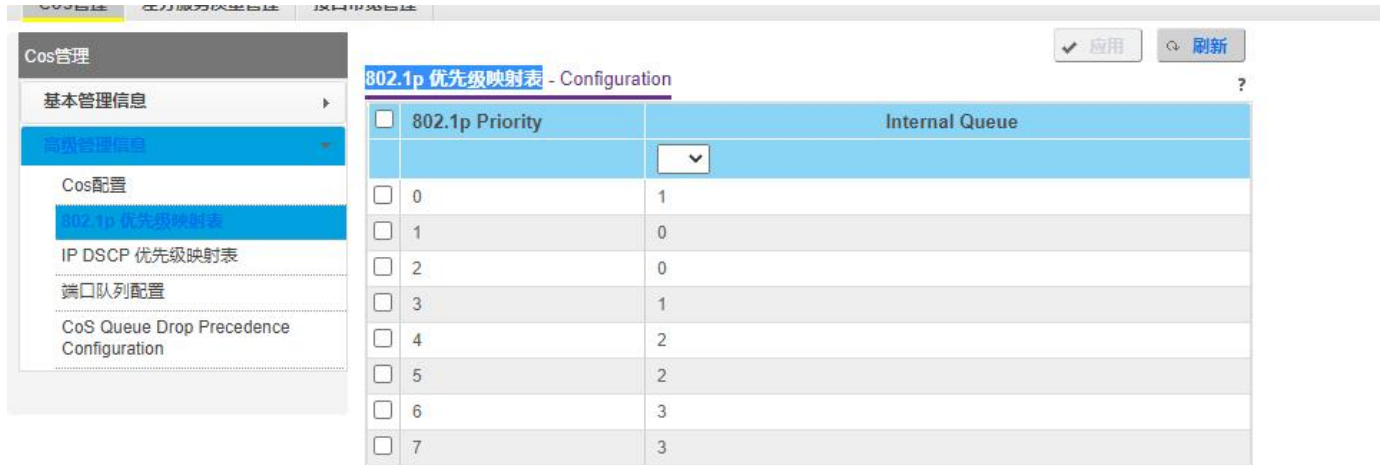
5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击**QoS > CoS > 高级管理 > 802.1p 优先级映射表**



8. “802.1p to Queue Mapping”屏幕还显示“Current 802.1p Priority Mapping”表。

将802.1p优先级映射到队列:

使用“Interface”选择接口。

您可以为每个接口或所有可配置的接口指定CoS配置。

9. 指定要映射对应的802.1p值的内部流类。

队列号取决于特定的硬件。802.1p优先级行包含要映射的8个802.1p优先级中的每一个的流量分类选择器。优先级从low(0)到high(3)。例如，优先级为0的流量代表大多数数据流量，并且使用最大努力发送。具有较高优先级(如3)的流量可能是时间敏感的流量，如语音或视频。

每个列表中的值表示流量类。流量类是端口的硬件队列。较高的流分类值表示较高的队列位置。低队列的流量发送前，必须等待高队列的流量发送。

10. 单击 **应用** 按钮

The updated configuration is sent to the switch.

4.1.3. DSCP 优先级映射表

您可以指定哪个内部流类映射对应的DSCP值。

将DSCP值映射到队列:

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **QoS > CoS > 高级管理 > IP DSCP 优先级映射表**。

IP DSCP to Queue Mapping							
IP DSCP	Queue	IP DSCP	Queue	IP DSCP	Queue	IP DSCP	Queue
0	1 ▾	16	0 ▾	32	2 ▾	48	3 ▾
1	1 ▾	17	0 ▾	33	2 ▾	49	3 ▾
2	1 ▾	18	0 ▾	34	2 ▾	50	3 ▾
3	1 ▾	19	0 ▾	35	2 ▾	51	3 ▾
4	1 ▾	20	0 ▾	36	2 ▾	52	3 ▾
5	1 ▾	21	0 ▾	37	2 ▾	53	3 ▾

The **IP DSCP** field displays an IP DSCP value from 0 to 63.

8. 对于每个DSCP值，指定哪个内部流类映射对应的IP DSCP值。

队列号取决于特定的硬件。

9. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

4.1.4. 端口队列配置

接口整形速率可以应用于所有接口，也可以应用于特定的接口。

设置接口的CoS值。

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。

2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。

3. 启动web浏览器。

4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击QoS > CoS> 高级管理 > 端口队列配置

✓ 应用

↻ 刷新

端口队列配置 - 端口选择

指定的端口

ALL

端口队列配置 - 配置

Queue ID	分配的最小保证带宽(0 - 100)%	调度模式	队列深度管理方式
0	0	Weighted	TailDrop
1	0	Weighted	TailDrop
2	0	Weighted	TailDrop
3	0	Weighted	TailDrop
4	0	Weighted	TailDrop
5	0	Weighted	TailDrop
6	0	Weighted	TailDrop
7	0	Weighted	TailDrop

4.1.5. Configure CoS Drop Precedence Settings

To configure CoS Drop Precedence settings:

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

- 单击 **登录** 按钮。
将显示web管理界面菜单。
- 单击QoS > CoS> 高级管理 > CoS Queue Drop Precedence Configuration

IMSG24T24F6WF

系统管理

L2交换管理

路由管理

QoS管理

安全管理

监测管理

维护

CoS管理

差分服务质量管理

接口带宽管理

Cos管理

基本管理信息

高级管理信息

Cos配置

802.1p 优先级映射表

IP DSCP 优先级映射表

端口队列配置

CoS Queue Drop Precedence Configuration

应用

刷新

CoS Queue Drop Precedence Configuration - CoS Interface Queue Drop Precedence Configuration

端口

Global

Queue ID

0

Drop Precedence Level

1

WRED Minimum Threshold

40

(0 to 100)

WRED Maximum Threshold

100

(0 to 100)

WRED Drop Probability Scale

10

(0 to 100)

CoS Queue Drop Precedence Configuration - CoS Interface Queue Drop Precedence Status

端口	Queue ID	Drop Precedence Level	WRED Minimum Threshold	WRED Maximum Threshold	WRED Drop Probability Scale
Global	0	1	40	100	10
Global	0	2	30	90	10
Global	1	1	40	100	10
Global	1	2	30	90	10
Global	2	1	40	100	10
Global	2	2	30	90	10
Global	3	1	40	100	10
Global	3	2	30	90	10
Global	4	1	40	100	10
Global	4	2	30	90	10
Global	5	1	40	100	10
Global	5	2	30	90	10
Global	6	1	40	100	10
Global	6	2	30	90	10
Global	7	1	40	100	10

合计 16 项. 显示 1 到 15 项. 每页显示 15 项

<<

<

1

2

>

>>

- 使用Interface指定所有CoS可配置的接口。
- 使用Queue ID指定所有可用的队列。取值范围为0 ~ 6。默认为0。
- 使用删除优先级指定所有可用的删除优先级。取值范围为1 ~ 4。缺省值为1。
- 使用WRED最小阈值指定当前丢弃优先级的加权RED最小队列阈值，低于该阈值不会丢弃任何数据包。
取值范围为0 ~ 100。默认为40。
- 使用WRED Maximum Threshold指定当前丢弃优先级中加权的RED最大队列阈值，超过该阈值所有报文将被丢弃。

取值范围为0 ~ 100。默认值为100。

13. 使用WRED丢弃概率尺度来确定当前丢弃优先级的数据包丢弃概率。

取值范围为0 ~ 100。默认为10。

14. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

The following table describes the nonconfigurable data that is displayed.

Table 198. CoS Interface Queue Drop Precedence Status

字段	描述
Interface	interface可配置CoS的接口。
Queue ID	Queue ID队列ID。
Drop Precedence Level	Drop Precedence level删除优先级。
WRED Minimum Threshold	WRED Minimum threshold加权的RED最小队列阈值。
WRED Maximum Threshold	WRED Maximum threshold加权的RED最大队列阈值。
WRED Drop Probability Scale	WRED Drop Probability scale丢包概率。

4.2.差分服务质量管理

4.2.1. 差分服务质量管理

QoS > 差分服务质量管理> 基本管理>差分服务质量管理

差分服务质量管理 - Configuration

Diffserv Admin Mode

☐ Disable

☒ Enable

差分服务质量管理 - 状态

MIB Table	Current Size	Max Size
Class Table Size	0	32
Class Rule Table Size	0	416
Policy Table Size	0	64
Policy Instance Table Size	0	1792
Policy Attribute Table Size	0	5376
Service Table Size	0	72

4.2.2. 高级管理

QoS > 差分服务质量管理> 高级管理>差分服务质量管理

CoS管理 差分服务质量管理 接口带宽管理

差分服务质量管理

基本管理信息

高级管理信息

差分服务质量管理

Class View

Class Detail Configuration

IPv6 Class View

IPv6 Class Detail Configuration

Policy View

Policy Detail Configuration

Service Interface Configuration

Service Statistics

差分服务质量管理 - Configuration

Diffserv Admin Mode

☐ Disable

☒ Enable

差分服务质量管理 - 状态

MIB Table	Current Size	Max Size
Class Table Size	0	32
Class Rule Table Size	0	416
Policy Table Size	0	64
Policy Instance Table Size	0	1792
Policy Attribute Table Size	0	5376
Service Table Size	0	72

QoS > 差分服务质量管理> 高级管理>Class View

CoS管理 差分服务质量管理 接口带宽管理

差分服务质量管理

基本管理信息

高级管理信息

差分服务质量管理

Class View

Class Detail Configuration

IPv6 Class View

IPv6 Class Detail Configuration

Policy View

Policy Detail Configuration

Service Interface Configuration

Service Statistics

IPv6 Class View - IPv6 Class Name

+ 增加 - 删除 ✓ 应用 ↻ 刷新

Class Name	Class Type

QoS > 差分服务质量管理> 高级管理>IPv6 Class Detail Configuration

CoS管理 差分服务质量管理 接口带宽管理

差分服务质量管理

基本管理信息

高级管理信息

差分服务质量管理

Class View

Class Detail Configuration

IPv6 Class View

IPv6 Class Detail Configuration

Policy View

Policy Detail Configuration

Service Interface Configuration

Service Statistics

IPv6 Class Detail Configuration - IPv6 Class Name

+ 增加 - 删除 ✓ 应用 ↻ 刷新

Class Name	Class Type

QoS > 差分服务质量管理> 高级管理>Policy View

系统管理 L2交换管理 路由管理 **QoS管理** 安全管理 监测管理 维护 简体中文 保存 退出

CoS管理 差分服务质量管理 接口带宽管理

差分服务质量管理

基本管理信息

高级管理信息

差分服务质量管理

Class View

Class Detail Configuration

IPv6 Class View

IPv6 Class Detail Configuration

Policy View

Policy Detail Configuration

Service Interface Configuration

Service Statistics

Policy View - Configuration

+ 增加 - 删除 ✓ 应用 ↺ 刷新

☐	Policy Name	Policy Type	Member Class

QoS > 差分服务质量管理> 高级管理>Policy Detail Configuration

IMSG24T24F6WF

系统管理 L2交换管理 路由管理 **QoS管理** 安全管理 监测管理 维护 简体中文 保存 退出

CoS管理 差分服务质量管理 接口带宽管理

差分服务质量管理

基本管理信息

高级管理信息

差分服务质量管理

Class View

Class Detail Configuration

IPv6 Class View

IPv6 Class Detail Configuration

Policy View

Policy Detail Configuration

Service Interface Configuration

Service Statistics

Policy Detail Configuration - Configuration

+ 增加 - 删除 ✓ 应用 ↺ 刷新

☐	Policy Name	Policy Type	Member Class

QoS > 差分服务质量管理> 高级管理>Service Interface Configuration

CoS管理

差分服务质量管理

接口带宽管理

差分服务质量管理

基本管理信息

高级管理信息

差分服务质量管理

Class View

Class Detail Configuration

IPv6 Class View

IPv6 Class Detail Configuration

Policy View

Policy Detail Configuration

Service Interface Configuration

Service Statistics

Service Interface Configuration - Configuration

☐	Interface	Policy In Name	Policy Out Name	Direction	Operational Status
☐	0/1				
☐	0/2				
☐	0/3				
☐	0/4				
☐	0/5				
☐	0/6				
☐	0/7				
☐	0/8				
☐	0/9				
☐	0/10				
☐	0/11				
☐	0/12				
☐	0/13				
☐	0/14				
☐	0/15				

合计 62 项, 显示 1 到 15 项, 每页显示 15 项

<<

<

1

2

3

4

5

>

>>

QoS > 差分服务质量管理> 高级管理>Service Statistics

CoS管理

差分服务质量管理

接口带宽管理

差分服务质量管理

基本管理信息

高级管理信息

差分服务质量管理

Class View

Class Detail Configuration

IPv6 Class View

IPv6 Class Detail Configuration

Policy View

Policy Detail Configuration

Service Interface Configuration

Service Statistics

Service Statistics - Service Statistics

Interface	Direction	Policy Name	Operational Status	Member Classes	Offered Octets/Packets	Discarded Octets/Packets
-----------	-----------	-------------	--------------------	----------------	------------------------	--------------------------

4.3.接口带宽管理

QoS > 接口带宽管理>接口带宽管理

CoS管理

差分服务质量管理

接口带宽管理

BandWidth Limit

端口输入带宽管理

端口输出带宽管理

应用

刷新

端口输入带宽管理 - 配置

☐	端口	限速工作模式	限速方式选择	限速值设定	突发数据最大值(K字节)
☐	0/1	关闭	端口速率百分比	0	0
☐	0/2	关闭	端口速率百分比	0	0
☐	0/3	关闭	端口速率百分比	0	0
☐	0/4	关闭	端口速率百分比	0	0
☐	0/5	关闭	端口速率百分比	0	0
☐	0/6	关闭	端口速率百分比	0	0
☐	0/7	关闭	端口速率百分比	0	0
☐	0/8	关闭	端口速率百分比	0	0
☐	0/9	关闭	端口速率百分比	0	0
☐	0/10	关闭	端口速率百分比	0	0
☐	0/11	关闭	端口速率百分比	0	0
☐	0/12	关闭	端口速率百分比	0	0
☐	0/13	关闭	端口速率百分比	0	0
☐	0/14	关闭	端口速率百分比	0	0
☐	0/15	关闭	端口速率百分比	0	0

合计 54 项, 显示 1 到 15 项, 每页显示 15 项

<<

<

1

2

3

4

>

>>

QoS > 接口带宽管理>端口输出带宽管理

CoS管理

差分服务质量管理

接口带宽管理

BandWidth Limit

端口输入带宽管理

端口输出带宽管理

应用

刷新

端口输出带宽管理 - 配置

☐	端口	限速工作模式	限速方式选择	限速值设定	突发数据最大值(K字节)
☐	0/1	关闭	端口速率百分比	0	0
☐	0/2	关闭	端口速率百分比	0	0
☐	0/3	关闭	端口速率百分比	0	0
☐	0/4	关闭	端口速率百分比	0	0
☐	0/5	关闭	端口速率百分比	0	0
☐	0/6	关闭	端口速率百分比	0	0
☐	0/7	关闭	端口速率百分比	0	0
☐	0/8	关闭	端口速率百分比	0	0
☐	0/9	关闭	端口速率百分比	0	0
☐	0/10	关闭	端口速率百分比	0	0
☐	0/11	关闭	端口速率百分比	0	0
☐	0/12	关闭	端口速率百分比	0	0
☐	0/13	关闭	端口速率百分比	0	0
☐	0/14	关闭	端口速率百分比	0	0
☐	0/15	关闭	端口速率百分比	0	0

合计 54 项, 显示 1 到 15 项, 每页显示 15 项

<<

<

1

2

3

4

>

>>

164

5. 设备安全管理

本章涵盖以下主题：

- 管理安全设置
- **TACACS** 概述
- 配置管理访问权限
- 端口身份验证
- 流量管制
- 端口安全
- **DHCP Snooping**
- 配置访问控制列表 (ACL)

5.1.管理安全设置

您可以配置登录密码、远程授权拨入用户服务（RADIUS）设置、终端访问控制器访问控制系统（TACACS）设置和身份验证列表。

5.1.1. 配置用户

默认情况下，存在两个用户帐户：

- admin, 管理员，具有读/写权限
- guest, 来宾，具有只读权限

默认情况下，这两个帐户的密码均为空。名称不区分大小写。

如果您登录到一个具有读写权限的用户帐户(admin)，您可以为默认帐户分配密码和设置安全参数，并可以添加和删除帐户(除了admin)，最多6个。只有具有读写权限的用户才能修改web界面屏幕上的数据，且只能创建一个具有读写权限的帐户

要配置用户，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 系统访问管理 > 本地交换机用户 > 用户管理**



8. 在 **用户名称** 字段中，选择需要修改的帐户。
直接单击用户名可以进入指定用户的密码和权限修改页面。
9. 锁定状态”字段表示用户帐户是否被锁定(TRUE或FALSE)。
10. Password Expiration Date字段表示当前密码的截止日期。
11. 要删除选定的用户帐户，请单击 **删除** 按钮

您不能删除管理员(admin)读/写用户。

5.1.2. 添加新用户

要添加用户，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。
交换机的默认IP地址为 192.168.10.12 。
此时将显示登录屏幕。
5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
将显示web管理界面菜单。
7. 单击 **安全管理 > 系统访问管理 > 本地交换机用户 > 添加新用户**



8. 在 **用户名称** 字段中，输入新帐户的名称。
只有在创建帐户时才能输入新的用户名。用户名长度最多为64个字符，不区分大小写。有效字符包括所有字母数字字符以及连字符(-)和下划线(_)字符。默认用户名无效。用户名一旦创建，就不能再修改。
9. 在 **密码** 字段中，输入帐户的密码。
字符在键入时不显示;只有星号(*)显示。密码长度不超过64个字母数字字符，区分大小写。
10. 在“**确认密码**”字段中，再次输入密码，以确认您输入的密码正确。
该字段不显示输入的密码，但显示星号(*)。需要保证和 “密码” 字段中的字符串相同。
11. **访问操作权限** 字段， 显示用户的访问方式。**admin**帐户始终具有读/写访问权限，所有其他帐户被分配为只读访问权限。
12. 单击 **增加** 按钮
完成用户的添加。

5.1.3. 配置用户密码设定参数

要配置用户密码设定参数，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。
交换机的默认IP地址为 192.168.10.12 。
此时将显示登录屏幕。
5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 系统访问管理 > 本地交换机用户 > 用户密码安全性管理**

用户密码安全性管理 - 配置	
密码最小长度要求	8 (0, or 8 to 64)
密码有效期(日)	0 (0, 1 to 365)
保留旧密码的条目数	0 (0 to 10)
锁定用户前,认证失败尝试次数	0 (0 to 5)

8. 在密码最小长度字段中，键入所有新本地用户密码的最小字符长度。

9. 在密码老化（天）字段中，键入用户密码自设置密码起的最长有效时间（天）。

密码过期后，用户必须在密码过期后首次登录后输入新密码。值**0**表示密码永不过期。

10. 在“密码历史记录”字段中，键入以前要存储的密码数，以防止密码重复使用。

这确保了每个用户不会经常重复使用密码。值为**0**表示未存储以前的密码。

11. 在锁定尝试字段中，指定锁定用户帐户之前允许的失败本地身份验证尝试次数。

值**0**表示从不锁定用户帐户。

5.1.4. 配置特权密码

您可以更改特权EXEC密码。密码最多为**64**个字母数字字符。密码区分大小写。

要启用特权密码配置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 **192.168.10.101**。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 **192.168.10.12**。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > 系统访问管理 > Enable认证密码配置**



- 8. 在密码字段中，键入密码。
密码最多为64个字母数字字符。
- 9. 在确认密码字段中，再次键入密码，以确认您输入的密码正确。
- 10. 如果需要清除特权密码， 可以勾选 **“删除密码”**。
- 11. 字段 **“工作状态”** 显示当前是否已经配置启用特权密码。

5.1.5. **配置线路密码**

要配置线路密码，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。
交换机的默认IP地址为 192.168.10.12 。
此时将显示登录屏幕。
- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > 系统访问管理 > Line登录密码管理**

8. 在控制台密码字段中，输入控制台密码。
密码最多为64个字母数字字符。
9. 在确认控制台密码字段中，再次键入密码以确认键入的密码正确。
10. 在Telnet密码字段中，键入Telnet密码。
密码最多为64个字母数字字符。
11. 在确认Telnet密码字段中，再次键入密码以确认输入正确。
12. 在SSH密码字段中，键入SSH密码。
密码最多为64个字母数字字符。
13. 在确认SSH密码字段中，再次键入密码，以确认输入正确。

5.1.6. RADIUS 概述

RADIUS服务器为网络提供了额外的安全性。RADIUS服务器维护一个用户数据库，其中包含每个用户的身份验证信息。交换机将信息传递给已配置的RADIUS服务器，该服务器可以在授权使用网络之前验证用户名和密码。RADIUS服务器为以下各项提供集中身份验证方法：

- Web 访问
- 访问控制端口 (802.1X)

5.1.7. 配置全局RADIUS服务器设置

您可以添加有关网络上一个或多个RADIUS服务器的信息。

要配置全局RADIUS服务器设置，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。

- 7. 单击 **安全管理 > 系统访问管理 > RADIUS > Radius属性配置**



如果未配置服务器，则当前服务器IP地址字段为空（参见配置RADIUS服务器）。交换机最多支持三台配置的RADIUS服务器。如果配置了多个RADIUS服务器，则当前服务器是主服务器。如果未将任何服务器配置为主服务器，则当前服务器是最近添加的RADIUS服务器。

- 8. 请求报文重传到服务器的最大次数，指定请求数据包重传到RADIUS服务器的最大次数。

有效范围为1–15。默认值为4。

考虑配置RADIUS最大重发和RADIUS超时时的最大延迟时间。如果配置了多个RADIUS服务器，则在尝试下一个服务器之前，每个服务器上的最大重新传输值都将耗尽。在该服务器上配置的超时值未通过RADIUS服务器的响应之前，不会发生重新传输。因此，从RADIUS应用程序接收响应的最大延迟等于所有已配置服务器的重新传输时间和超时时间。如果RADIUS请求是由用户登录尝试生成的，则会阻止所有用户界面，直到RADIUS应用程序返回响应为止。

9. 请求重传的超时值，以秒为单位指定请求重新传输的超时值。

有效范围为1–30。默认值为5。

考虑配置RADIUS最大重发和RADIUS超时时的最大延迟时间。如果配置了多个RADIUS服务器，则在尝试下一个服务器之前，每个服务器上的最大重新传输值都将耗尽。在该服务器上配置的超时值未通过RADIUS服务器的响应之前，不会发生重新传输。因此，从RADIUS应用程序接收响应的最大延迟等于所有已配置服务器的重新传输时间和超时时间。如果RADIUS请求是由用户登录尝试生成的，则会阻止所有用户界面，直到RADIUS应用程序返回响应为止。

10. 单击 开启Accounting模式， 关闭 或 启用 单选按钮

这指定在当前服务器上启用还是禁用RADIUS记帐模式。

11. 单击 支持Radius Attribute 4模式， 关闭 或 启用 单选按钮

启用或禁用RADIUS Attribute 4。默认值为“禁用”。Radius Attribute 4值是可选字段，只有启用Radius Attribute 4模式时才能看到。IP地址的格式为xx.xx.xx.xx。

表64. Radius 配置

字段	描述
当前工作的服务器地址	当前服务器的地址。如果未配置服务器，则此字段为空。
配置的认证服务器个数	已配置的身份验证RADIUS服务器的数量。该值的范围从0到32。
配置的计费服务器个数	配置的RADIUS记帐服务器数。该值的范围从0到32。
已配置的命名RADIUS服务器认证组的个数	已配置的命名RADIUS服务器身份验证组数。
已配置的RADIUS命名计费组的个数	已配置的命名RADIUS服务器记帐组数。

5.1.8. 配置RADIUS服务器

要配置RADIUS服务器，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

- 6. 单击 **登录** 按钮。

将显示web管理界面菜单。

- 7. 单击 **安全管理 > 系统访问管理 > RADIUS > 服务器管理**



- 8. 要添加RADIUS服务器，请指定以下设置：

- 在Radius服务器IP地址字段中，指定Radius服务器的IP地址。
- 在Radius服务器名称字段中，指定服务器名称。
- 使用端口指定此服务器使用的UDP端口。有效范围为0–65535。
- **配置密钥**， 仅当此选项为“是”时，才会应用此机密。如果选项为“否”，则在“机密”字段中输入的任何内容都无效，并且不会保留。
- 使用 **密钥值** 指定此服务器的共享机密。
- **Primary Server**， 使用主服务器将所选服务器设置为主服务器或辅助服务器。
- **消息验证启用**， 使用消息验证器启用或禁用所选服务器的消息验证器属性。

- 9. 单击 **增加** 按钮，

服务器已添加到交换机。

只有使用具有读写权限的管理员用户名登录时，此按钮才可用。除非执行保存，否则

在整个电源循环中不会保留这些更改。

10. 要从配置中删除所选服务器，请单击删除按钮。

只有使用具有读写权限的管理员用户名登录时，此按钮才可用。除非执行保存，否则

在整个电源循环中不会保留这些更改。

当前字段指示此服务器当前是否用作身份验证服务器。要将身份验证服务器和RADIUS统计信息重置为其默认值，请单击屏幕底部的“清除计数器”按钮。

下表介绍了屏幕上显示的RADIUS服务器统计信息。

表65. RADIUS 统计

字段	描述
Radius 服务器	RADIUS服务器的地址或显示统计信息的RADIUS服务器的名称。
Round Trip 间隔时间	最近的访问应答/访问质询与来自此RADIUS身份验证服务器的与其匹配的访问请求之间的时间间隔（百分之一秒）。
发送Access-Request报文数	发送到此服务器的RADIUS访问请求数据包数。这个数字不包括重新传输。
重发Access-Request报文数	重新传输到此服务器的RADIUS访问请求数据包数。
Access Accept报文数	从此服务器接收的RADIUS access accept数据包数，包括有效和无效数据包。
Access Rejects报文数	从该服务器接收的RADIUS访问拒绝数据包数，包括有效和无效数据包。
Access Challenges报文数	从该服务器接收的RADIUS访问质询数据包的数量，包括有效和无效数据包。
错误的Access Response报文数	从此服务器接收的格式错误的RADIUS访问响应数据包数。格式错误的数据包包括长度无效的数据包。格式错误的访问响应中不包括错误的身份验证程序、签名属性或未知类型。
无效的Authenticator报文数	从该服务器接收的包含无效身份验证程序或签名属性的RADIUS访问响应数据包数。
未处理Request报文数	发送到此服务器但尚未超时或未收到响应的RADIUS访问请求数据包数。
验证超时次数	此服务器的身份验证超时数。
未知类型报文数	在身份验证端口上从此服务器接收的未知类型的RADIUS数据包数。
丢弃的报文数	在身份验证端口上从此服务器接收并由于其他原因丢弃的RADIUS数据包数。

5.1.9. 配置RADIUS记帐服务器

要配置RADIUS记帐服务器，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 系统访问管理 > RADIUS > Accounting 服务器管理**



- 8. 在记帐服务器IP地址字段中，指定RADIUS记帐服务器的IP地址。
- 9. 在记帐服务器名称字段中，输入记帐服务器的名称。
- 10. 在端口字段中，指定服务器用于验证RADIUS记帐服务器的UDP端口号。
有效范围为0–65535。如果用户具有只读访问权限，则会显示该值，但无法更改。
- 11. 从机密配置列表中，选择“是”以在下一个字段中添加RADIUS机密。
添加RADIUS记帐服务器后，此字段指示是否配置了此服务器的共享机密。
- 12. 在“机密”字段中，键入要与指定的记帐服务器一起使用的共享机密。
- 13. 从记帐模式列表中，启用或禁用RADIUS记帐模式。
- 14. 要删除已配置的RADIUS记帐服务器，请单击“删除”按钮。

要清除记帐服务器统计信息，请单击“清除计数器”按钮。

下表介绍了屏幕上可用的RADIUS accounting server统计信息。

表66. RADIUS记帐服务器统计数据

字段	描述
Accounting Server 服务器	与统计信息关联的记帐服务器。
间隔时间	最近的记帐响应与来自此RADIUS记帐服务器的与其匹配的记帐请求之间的时间间隔（百分之一秒）。
Accounting Requests	发送的RADIUS记帐请求数据包数，不包括重传。
重发Accounting Request报文数	重新传输到此RADIUS记帐服务器的RADIUS记帐请求数据包数。
接收Accounting服务器报文数	记帐端口上从此服务器接收的RADIUS数据包数。
错误的Accounting Response报文数	从此服务器接收的格式错误的RADIUS记帐响应数据包数。格式错误的数据包包括长度无效的数据包。错误的身份验证程序和未知类型不包括在格式错误的记帐响应中。
无效的Authenticator报文数	从此记帐服务器接收的包含无效身份验证程序的RADIUS记帐响应数据包数。
未处理Request报文数	发送到此服务器但尚未超时或未收到响应的RADIUS记帐请求数据包数。
验证超时次数	此服务器的记帐超时数。
未知类型报文数	在记帐端口上从此服务器接收的未知类型的RADIUS数据包数。
丢弃的报文数	在记帐端口上从此服务器接收并由于其他原因丢弃的RADIUS数据包数。

5.2.TACACS 概述

TACACS提供了一个集中的用户管理系统，同时仍然保持与RADIUS和其他身份验证过程的一致性。TACACS提供以下服务：

- **Authentication.** 在登录期间以及通过用户名和用户定义的密码提供身份验证。
- **Authorization.** 在登录时执行。身份验证会话完成后，将使用经过身份验证的用户名启动授权会话。TACACS服务器检查用户权限。

TACACS协议通过设备和TACACS服务器之间的加密协议交换确保网络安全。

5.2.1. 配置全局TACACS设置

您可以为交换机和通过带内管理端口配置的TACACS服务器之间的通信配置TACACS设置。

要配置全局TACACS设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。

- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > 系统访问管理 > TACACS > TACACS 属性配置**

The screenshot shows the 'TACACS+ 属性配置 - 配置' page. The left sidebar has a tree view with 'TACACS+' selected. The main content area has a table with the following fields:

密钥配置状态	Not Configured
清除密钥	☐
新的密钥值	(最长 128 字符)
密钥确认值	
服务器连接最大超时时间	5 (1 to 30)

- 8. 在密钥字符串字段中，为交换机和TACACS服务器之间的TACACS通信指定身份验证和加密密钥。
有效范围为0–128。密钥必须与TACACS服务器上配置的密钥匹配。
- 9. 在连接超时字段中，指定在托管交换机和TACACS服务器之间建立TCP连接所允许的最大秒数。
- 10. 单击 **应用** 按键
更新的配置参数将发送到交换机，配置更改将立即生效。

5.2.2. 配置TACACS服务器设置

您可以配置多台TACACS服务器，交换机可以与之通信。

要配置TACACS服务器设置，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。

- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。
交换机的默认IP地址为 192.168.10.12 。
此时将显示登录屏幕。
- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > 系统访问管理 > TACACS > TACACS 服务器管理**

TACACS+服务器管理 - 配置?

☐	TACACS+ 服务器地址	顺序优先级 (0-65535)	服务器端口号 (0-65535)	Key Reconfig	新的密钥值	服务器连接超时 时间(1-30秒)

- 8. 使用TACACS服务器配置TACACS服务器IP地址。
- 9. 使用优先级指定TACACS服务器的使用顺序。
有效范围为0–65535。
- 10. 使用端口指定身份验证端口。它必须在0–65535范围内。
- 11. 使用密钥字符串为设备和TACACS服务器之间的TACACS通信指定身份验证和加密密钥。
有效范围为0–128。密钥必须与TACACS服务器上使用的密钥匹配。
- 12. 使用连接超时指定设备与TACACS服务器之间的连接超时之前经过的时间量。
范围为1-30。
- 13. 单击 **增加** 按钮
服务器已添加到交换机。

此按钮仅对读/写用户可用。除非执行保存，否则在整个电源循环中不会保留这些更改。
- 14. 要从配置中删除所选服务器，请单击删除按钮。

5.2.3. 配置登录身份验证列表

登录列表指定用于验证与列表关联的用户的交换机或端口访问权限的身份验证方法。预配置的用户 **admin** 和 **guest** 被分配到名为 **defaultList** 的预配置列表中，您无法删除该列表。所有新创建的用户也将分配给 **defaultList**，直到您专门将其分配给其他列表。

存在两个默认列表：DefaultList和networkList。

要配置登录身份验证列表，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
将显示web管理界面菜单。
7. 单击 **安全管理 > 系统访问管理 > 登录认证列表 > 终端登录认证管理**



8. 要创建新的登录列表，请在列表名称字段中输入名称。
该名称最多可包含15个字母数字字符，不区分大小写。
9. 在编号列表（1、2、3、4、5）中，选择要首先出现在所选身份验证启用列表中的方法。

方案如下：

- **Enable.** 特权EXEC密码用于身份验证。
- **Line.** 线路密码用于身份验证。
- **None.** 无法对用户进行身份验证。
- **RADIUS.** 使用RADIUS服务器而不是本地服务器对用户名和密码进行身份验证。

- **TACACS.** 使用TACACS服务器对用户名和密码进行身份验证。
- **Deny.** 身份验证总是失败。

10. 单击 **增加** 按钮

登录列表将添加到交换机中。

11. 要从配置中删除选定的身份验证登录列表，请单击删除按钮。

如果将所选登录列表分配给任何系统登录用户（包括默认用户），则删除失败。只有以具有读/写访问权限的管理员用户身份登录时，才能使用此按钮。除非执行保存，否则在整个电源循环中不会保留更改。

5.2.4. 配置启用特权身份验证列表

启用列表指定验证方法，以验证与该列表关联的用户的特权EXEC访问。预配置的用户admin和guest被分配到名为defaultList的预配置列表中，您无法删除该列表。所有新创建的用户也将分配给defaultList，直到您专门将其分配给其他列表。存在两个默认列表：**enableList**和**enableNetList**。

要配置启用特权身份验证列表，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 系统访问管理 > 登录认证列表 > Enable 级认证管理**

Enable Authentication List						
☐	List Name	1	2	3	4	5
☐						
☐	enableList	Enable	None	N/A	N/A	N/A
☐	enableNetList	Enable	None	N/A	N/A	N/A

8. 要创建新的启用列表，请在列表名称字段中输入名称。

它最多可包含15个字母数字字符，不区分大小写。

9. 在编号列表（1、2、3、4、5）中，选择要首先出现在所选身份验证启用列表中的方法。

方案如下：

- **Enable.** 特权EXEC密码用于身份验证。
- **Line.** 线路密码用于身份验证。
- **None.** 无法对用户进行身份验证。
- **RADIUS.** 使用RADIUS服务器而不是本地服务器对用户名和密码进行身份验证。
- **TACACS.** 使用TACACS服务器对用户名和密码进行身份验证。
- **Deny.** 身份验证总是失败。

10. 单击 **增加** 按钮

登录列表将添加到交换机中。

11. 要从配置中删除选定的身份验证启用列表，请单击删除按钮。

仅当您具有读/写访问权限时，才能使用此按钮。除非执行保存，否则在整个电源循环中不会保留更改。

5.2.5. 配置Dot1x身份验证列表

您可以配置dot1x列表。dot1x列表指定验证与列表关联的用户端口访问权限的身份验证方法。只能支持一种dot1x方法。

默认列表是dot1xList。

要配置dot1x身份验证列表，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
将显示web管理界面菜单。
7. 单击 **安全管理 > 系统访问管理 > 登录认证列表 > Dot1x认证管理**



8. 在列表名称字段中，选择dot1x列表名称。
9. 选择要首先显示在所选身份验证登录列表中的方法。

方案如下：

- **IAS.** 内部身份验证服务器数据库中的用户ID和密码用于身份验证。
- **Local.** 用户本地存储的ID和密码用于身份验证。
- **RADIUS.** 用户的ID和密码使用RADIUS服务器而不是本地进行身份验证。
- **None.** 用户未使用用户名和密码进行身份验证。

5.2.6. 配置HTTP身份验证列表

您可以配置HTTP列表。HTTP列表指定通过HTTP验证交换机或端口访问的身份验证方法。

要配置HTTP身份验证列表，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 安全管理 > 系统访问管理 > 登录认证列表 > HTTP 认证管理



8. 使用列表名称选择HTTP列表名称。
9. 在编号列表（1、2、3、4）中，选择要首先出现在所选身份验证启用列表中的方法。
- 方案如下：

- **Enable.** 特权EXEC密码用于身份验证。
- **None.** 无法对用户进行身份验证。
- **RADIUS.** 使用RADIUS服务器而不是本地服务器对用户名和密码进行身份验证。
- **TACACS.** 使用TACACS服务器对用户名和密码进行身份验证。

5.2.7. 配置HTTPS身份验证列表

您可以配置HTTPS列表。登录列表指定身份验证方法，以验证与列表关联的用户通过HTTPS访问交换机或端口的权限。默认列表是httpsList。

要配置HTTPS身份验证列表，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 系统访问管理 > 登录认证列表 > HTTPS 认证管理**

	1	2	3	4
☐ 默认会话列表				
☐ HttpsListName	Local			

8. 选中HTTPS列表名称的列表名称复选框。

9. 在编号列表（1、2、3、4）中，选择要首先出现在所选身份验证启用列表中的方法。

方案如下：

- **Enable.** 特权EXEC密码用于身份验证。
- **None.** 无法对用户进行身份验证。
- **RADIUS.** 使用RADIUS服务器而不是本地服务器对用户名和密码进行身份验证。
- **TACACS.** 使用TACACS服务器对用户名和密码进行身份验证。

5.2.8. 查看登录会话

要查看登录会话，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。
- 将显示web管理界面菜单。
7. 单击 **安全管理 > 系统访问管理 > 登录会话状态**



表67. 登录会话

字段	描述
ID	标识此行的ID。
用户名称	会话已打开的用户名。
登录访问端地址	与用户连接的机器。
会话空闲时间	空闲会话时间。
会话已登录时间	总会话时间。
会话模式	会话类型：Telnet、Serial、SSH 或 HTTP， HTTPS

5.3.配置管理访问权限

您可以配置对交换机管理界面的HTTP和安全HTTP访问。

5.3.1. 配置HTTP服务器设置

要使用web浏览器访问交换机，必须首先使用IP信息（IP地址、子网掩码和默认网关）对其进行配置。您可以使用以下任一选项配置IP信息：

- BOOTP
- DHCP
- 通过EIA-232端口的终端接口

建立带内连接后，可以使用基于web的管理更改IP信息。

要配置HTTP服务器设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 会话属性管理 > HTTP > HTTP 登录配置**

The screenshot shows a web management interface with a sidebar on the left containing menu items like '系统管理', 'L2交换管理', '路由管理', 'QoS管理', '安全管理', '监测管理', and '维护'. The '安全管理' (Security Management) menu is expanded, showing '会话属性管理' (Session Attribute Management) and 'HTTP' configuration. The main content area is titled 'HTTP登录配置 - 配置' (HTTP Login Configuration - Configuration). It contains a table with the following settings:

配置项 (Configuration Item)	值 (Value)	范围 (Range)
HTTP服务工作模式 (HTTP Service Mode)	☒ 启用 (Enabled)	
HTTP 会话不活动超时(分钟) (HTTP Session Inactivity Timeout (minutes))	5	(1 to 60)
HTTP 会话强制超时(小时) (HTTP Session Forced Timeout (hours))	24	(1 to 168)
允许的HTTP 会话最大数量 (Maximum Allowed HTTP Sessions)	32	(0 to 32)
登录认证列表 (Login Authentication List)	HttpListName	

8. 选择HTTP访问禁用或启用单选按钮。

这指定是否可以从web浏览器访问交换机。如果启用web模式，则可以从web浏览器管理切换。出厂默认设置为启用。

9. 在HTTP端口字段中，输入HTTP端口号。

有效范围为80和1025至65535。默认值为80。

10. 在HTTP会话软超时（分钟）字段中，设置HTTP会话的非活动超时。

该值必须在1到60分钟的范围内。默认值为5分钟。显示当前配置的值。

11. 在HTTP会话硬超时（小时）字段中，设置HTTP会话的硬超时。

此超时不受会话活动级别的影响。该值必须在1到168小时的范围内。默认值为24小时。将显示当前配置的值。

12. 在最大HTTP会话数字段中，设置允许的最大HTTP会话数。

该值必须在0到16之间。默认值为16。将显示当前配置的值。

“身份验证列表”字段显示HTTP正在使用的列表。

5.3.2. HTTPS 配置

安全HTTP支持通过加密的安全套接字层（SSL）或传输层安全性（TLS）连接传输HTTP。当您使用web界面管理交换机时，安全HTTP可以帮助确保管理系统和交换机之间的通信受到保护，免受窃听者和中间人攻击。

您可以配置管理站和交换机之间HTTPS通信的设置。

要配置HTTPS设置，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。

- 7. 单击 **安全管理 > 会话属性管理 > HTTPS > HTTPS 登录配置**



- 8. 选择HTTPS管理模式禁用或启用单选按钮。
这将启用或禁用安全HTTPS的管理模式。将显示当前配置的值。默认值为禁用。只有在禁用HTTPS管理模式时，才能下载SSL证书。仅当设备上存在证书时，才能启用HTTPS管理模式。
- 9. 选择SSL版本3禁用或启用单选按钮。

这将启用或禁用安全套接字层版本3.0。将显示当前配置的值。默认值为启用。

10. 选择TLS版本1禁用或启用单选按钮。

这将启用或禁用传输层安全版本1.0。将显示当前配置的值。默认值为启用。

11. 在HTTPS端口字段中，键入HTTPS端口号。

该值必须在1025到65535之间。端口443是默认值。将显示当前配置的值。

12. 在HTTPS会话软超时（分钟）字段中，输入HTTPS会话的非活动超时。

该值必须在1到60分钟的范围内。默认值为5分钟。将显示当前配置的值。

13. 在HTTPS会话硬超时（小时）字段中，设置HTTPS会话的硬超时。

此超时不受会话活动级别的影响。该值必须在1到168小时的范围内。默认值为24小时。将显示当前配置的值。

14. 在最大HTTPS会话数字段中，输入允许的最大HTTPS会话数。

该值必须在0到16之间。默认值为16。将显示当前配置的值。

身份验证列表字段显示HTTPS的身份验证列表。

5.3.3. 管理证书

您可以生成或删除证书。

要管理证书，请执行以下操作：

- 1.** 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2.** 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3.** 启动web浏览器。
- 4.** 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5.** 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

- 6.** 单击 **登录** 按钮。

将显示web管理界面菜单。

- 7.** 单击 **安全管理 > 会话属性管理 > HTTPS > 证书管理**



证书存在字段显示设备上是否存在证书。

8. 选择以下单选按钮之一：

- **None.** 在证书管理方面没有什么可以做的。这是默认选择。
- **Generate Certificates.** 开始生成证书文件。
- **Delete Certificates.** 删除相应的证书文件（如果存在）。

证书生成状态字段显示SSL证书生成状态。

5.3.4. 下载证书

您可以将证书文件传输到交换机。

要使交换机上的web服务器接受来自管理站的HTTPS连接，web服务器需要公钥证书。您可以在外部（例如，脱机）生成证书并将其下载到交换机。

将文件下载到交换机之前，必须满足以下条件：

- 要从TFTP服务器下载的文件位于相应目录中的服务器上。
- 文件格式正确。
- 交换机具有到TFTP服务器的路径。

下载证书：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 会话属性管理 > HTTPS > 上传证书操作**



8. 在“文件类型”列表中，指定要传输的文件类型：

- **SSL Trusted Root Certificate PEM File.** SSL受信任根证书文件（PEM编码）
- **SSL Server Certificate PEM File.** SSL服务器证书文件（PEM编码）
- **SSL DH Weak Encryption Parameter PEM File.** SSL Diffie-Hellman弱加密参数文件（PEM编码）
- **SSL DH Strong Encryption Parameter PEM File.** SSL Diffie-Hellman强加密参数文件（PEM编码）

9. 在传输模式列表中，指定用于传输文件的协议：

- **TFTP.** 普通文件传输协议
- **SFTP.** 安全文件传输协议
- **SCP.** 安全复制协议

10. 在服务器地址类型列表中，指定IPv4、IPv6或DNS以指示TFTP/SFTP/SCP服务器地址字段的格式。

出厂默认值为IPv4。

11. 在服务器地址字段中，根据服务器地址类型指示的格式键入服务器的IP地址或DNS主机名。

出厂默认值为IPv4地址0.0.0.0。

12. 在远程文件路径字段中，输入要下载的文件的路径。

13. 最多可以输入96个字符。出厂默认值为空。

最多可以输入32个字符。出厂默认值为空。

5.3.5. 配置SSH设置

您可以查看和修改设备上的Secure Shell（SSH）服务器设置。SSH是一种网络协议，可通过在远程管理系统上使用SSH客户端访问CLI管理界面。SSH是一种比Telnet更安全的访问方法，因为它加密了管理系统和设备之间的通信。您可以下载或生成SSH主机密钥，以实现基于CLI的安全管理。

要配置SSH设置，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。

- 7. 单击 **安全管理 > 会话属性管理 > SSH > SSH登录配置**



- 8. 选择SSH管理模式禁用或启用单选按钮。
这将启用或禁用SSH服务器管理模式。启用此模式后，可以使用远程系统上的SSH客户端访问设备。将显示当前配置的值。默认值为禁用。
- 9. 选择SSH版本1禁用或启用单选按钮。
这将启用或禁用SSH的协议级别1。选择启用后，设备上的SSH服务器可以使用SSH协议级别

1（SSH-1）接受来自SSH客户端的连接。选择“禁用”时，设备不允许使用SSH-1协议从客户端进行连接。将显示当前配置的值。默认值为Enable。

10. 选择SSH版本2禁用或启用单选按钮。

这将启用或禁用SSH的协议级别2。选择启用后，设备上的SSH服务器可以使用SSH协议级别2（SSH-2）接受来自SSH客户端的连接。选择“禁用”时，设备不允许使用SSH-2协议从客户端进行连接。将显示当前配置的值。默认值为Enable。

11. 使用SSH会话超时为交换机的传入SSH会话配置SSH会话非活动超时值。

在这段时间内未显示任何SSH活动的已连接用户将自动断开与设备的连接。该字段的可接受范围为1-5分钟。

12. 使用最大SSH会话数配置可同时连接到设备的最大入站SSH会话数。

将显示当前配置的值。此字段的可接受范围为0-5。

13. 使用登录身份验证列表选择身份验证列表。

此列表用于验证尝试登录交换机的用户。

14. 使用“启用身份验证列表”选择身份验证列表。

此列表用于验证尝试获取启用级别权限的用户。

15. 使用SSH端口输入从1到65535的端口范围。

默认值为22。

16. 单击应用按钮。

更新的配置将发送到交换机。配置更改立即生效。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

表68. SSH配置

字段	描述
当前SSH会话数	远程SSH客户端和设备上SSH服务器之间的活动SSH会话数。
密钥证书状态	显示设备上是否存在以下密钥中的一个或两个（如果有）： - SSH-1 Rivest-Shamir-Adelman (RSA) 密钥文件或 SSH-2 RSA 密钥文件（PEM编码） - SSH-2数字签名算法 (DSA) 密钥文件（PEM编码）

5.3.6. 管理服务密钥

您可以生成或删除RSA和DSA密钥。

要管理服务密钥，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。

4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 会话属性管理 > SSH > 服务密钥管理**



8. 选择RSA密钥管理单选按钮：

- **空操作** 这是默认选择。
- **生成新的RSA密钥**. 开始生成RSA主机密钥。要生成SSH密钥文件，必须在管理上禁用SSH，并且不能有活动的SSH会话。
- **删除RSA密钥**. 删除相应的DSA密钥文件（如果存在）。

9. 选择DSA密钥管理单选按钮：

- **空操作**. 这是默认选择。
- **生成新的DSA密钥**. 开始生成DSA主机密钥。

要生成SSH密钥文件，必须在管理上禁用SSH，并且不能有活动的SSH会话。

- **删除DSA密钥**. 删除相应的DSA密钥文件（如果存在）。

10. 单击 **应用** 按键

主机密钥文件开始下载。要下载SSH密钥文件，必须在管理上禁用SSH，并且不能有活动的SSH会话。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

表69. RSA密钥管理

字段	描述
密钥存在状态	显示设备上存在以下哪个键或两个键（如果有）： - SSH-1 Rivest Shamir Adelman（RSA）密钥文件或SSH-2 RSA密钥文件（PEM编码） - SSH-2数字签名算法（DSA）密钥文件（PEM编码）
自动生成密钥的状态	显示正在生成的密钥（如果有）、RSA、DSA或无。

5.3.7. 下载服务密钥

您可以将SSH-1 RSA、SSH-2 RSA或SSH-2 DSA密钥文件从远程系统下载到设备。

要下载服务密钥，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 会话属性管理 > SSH > 服务密钥操作**



8. 在“文件类型”列表中，选择要传输的文件类型：
 - **SSH-1 RSA Key File.** SSH-1 Rivest Shamir Adelman (RSA) 密钥文件
 - **SSH-2 RSA Key PEM File.** SSH-2 Rivest Shamir Adelman (RSA) 密钥文件 (PEM编码)。
 - **SSH-2 DSA Key PEM File.** SSH-2 数字签名算法 (DSA) 密钥文件 (PEM编码)
9. 在传输模式列表中，选择用于传输文件的协议：
 - **TFTP.** 普通文件传输协议
 - **SFTP.** 安全文件传输协议
 - **SCP.** 安全复制协议
10. 在服务器地址类型字段中，指定IPv4、IPv6或DNS。

这指定TFTP/SFTP/SCP服务器地址字段的格式。出厂默认值为IPv4。
11. 在服务器地址字段中，根据服务器地址类型指示的格式输入服务器的IP地址或DNS主机名。

出厂默认值为IPv4地址0.0.0.0。
12. 在远程文件路径字段中，输入要下载的文件的路径。

最多可以输入96个字符。出厂默认值为空。
13. 在远程文件名字段中，输入TFTP服务器上要下载的文件名。

最多可以输入32个字符。出厂默认值为空。
14. 单击应用按钮。

主机密钥文件开始下载。要下载SSH密钥文件，必须在管理上禁用SSH，并且不能有活动的SSH会话。

5.3.8. 配置Telnet设置

要配置Telnet设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。
5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。

将显示web管理界面菜单。
7. 单击 **安全管理 > 会话属性管理 > Telnet.**



5.3.9. 配置Telnet身份验证列表

您可以选择登录并启用可用的身份验证列表。登录列表指定用于验证与列表关联的用户的交换机或端口访问权限的身份验证方法。启用列表指定用于验证与列表关联的用户的特权EXEC访问权限的身份验证方法。可以通过“管理安全”下的“身份验证列表”链接创建这些列表。

要配置Telnet身份验证列表，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 会话属性管理 > Telnet**。



8. 使用登录身份验证列表指定要通过Telnet登录的身份验证列表。

默认值为networkList。

9. 使用“启用身份验证列表”指定进入特权EXEC模式时使用的身份验证列表。

默认值为enableNetList。

10. 要配置带内管理端口的Telnet设置，请指定以下内容：

- 选择Telnet服务器管理模式禁用或启用单选按钮。

这将启用或禁用Telnet服务器的管理模式。默认值已启用。

- 这将启用或禁用Telnet服务器的管理模式。默认值已启用。

这指定是启用还是禁用新的入站Telnet会话。默认值已启用，以便可以建立新的入站Telnet会话，直到没有更多可用会话为止。如果禁用，则不会建立新的入站Telnet会话。在会话结束或异常网络错误结束会话之前，已建立的会话将保持活动状态。

- 使用会话超时指定在注销会话之前Telnet会话上发生不活动的分钟数。
- 您可以输入1到160之间的任意数字。出厂默认值为5分钟。
- 使用最大会话数指定允许同时进行多少Telnet会话。最大值为5，这也是出厂默认值。

“当前会话数”字段显示当前会话数。

11. 要配置带外端口的Telnet设置，请指定以下内容：

- 选择Telnet服务器管理模式禁用或启用单选按钮。

这将启用或禁用Telnet服务器的管理模式。默认值已启用。

- 这将启用或禁用Telnet服务器的管理模式。默认值已启用。

这指定是启用还是禁用新的入站Telnet会话。默认值已启用，以便可以建立新的入站Telnet会话，直到没有更多可用会话为止。如果禁用，则不会建立新的入站Telnet会话。在会话结束或异常网络错误结束会话之前，已建立的会话将保持活动状态。

- 使用会话超时指定在注销会话之前Telnet会话上发生不活动的分钟数。
- 您可以输入1到160之间的任意数字。出厂默认值为5分钟。
- 使用最大会话数指定允许同时进行多少Telnet会话。最大值为5，这也是出厂默认值。

“当前会话数”字段显示当前会话数。

5.3.10. 配置控制台端口

要配置控制台端口，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 会话属性管理 > 串口终端配置**



8. 在串行端口登录超时（分钟）字段中，指定在交换机关闭连接之前，串行端口连接上发生不活动的分钟数。

输入一个介于0和160之间的数字。出厂默认值为5。输入0将禁用超时。

9. 在波特率（bps）列表中，选择串行端口连接的默认波特率。

您可以选择1200、2400、4800、9600、19200、38400、57600和115200波特。出厂默认值为115200波特。

10. 在“登录身份验证列表”列表中，选择通过Telnet登录时要使用的身份验证列表。

默认值为defaultList。在“启用身份验证列表”列表中，选择进入特权EXEC模式时要使用的身份验证列表。

默认值为enableList

下表描述了显示的不可配置数据。

表70. 控制台端口

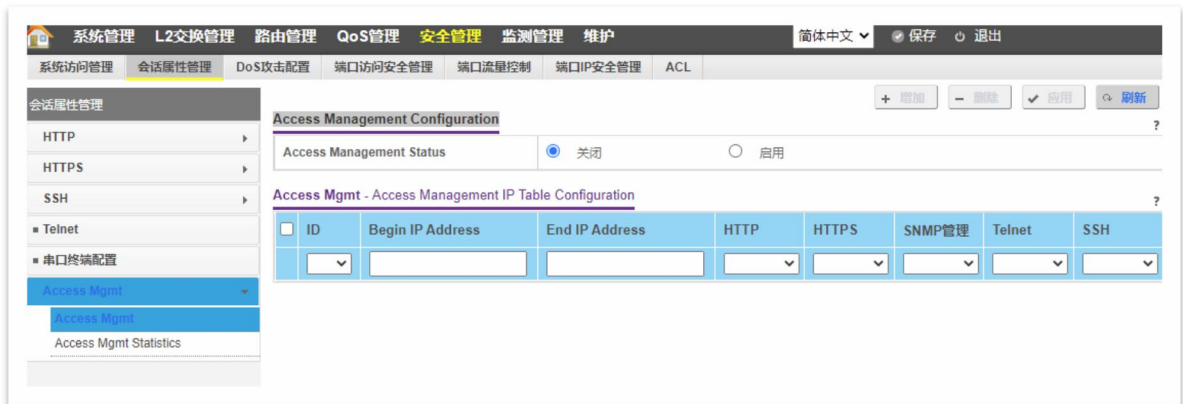
字段	描述
字符大小（位）	字符中的位数。这总是8。
流量控制	是否启用或禁用硬件流控制。它总是被禁用的。
停止位	每个字符的停止位数。它总是1。
奇偶校验	串行端口上使用的奇偶校验方法。总是没有。

5.3.11. 配置访问控制配置文件

要配置访问配置文件设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。

4. 在web浏览器地址字段中输入交换机的IP地址。
- 交换机的默认IP地址为 192.168.10.12 。
- 此时将显示登录屏幕。
5. 输入用户名和密码。
- 默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
- 将显示web管理界面菜单。
7. 单击 **安全管理 > 会话属性管理 > Access Mgmt > Access Management Configuration**



只有当访问配置文件处于非激活状态时，才能对访问规则应用更改。

提示： 确保在添加规则之前已创建访问配置文件。

8. 从“规则类型”列表中，选择以在所选规则匹配时允许或拒绝访问。

可能的管理方法如下：

- HTTP
- HTTPS (SSL)
- Secure Telnet (SSH)
- SNMP
- Telnet

9. 输入允许管理通信的客户端的起始源IP地址。

10. 输入允许管理通信的客户端的结束源IP地址。

在起始和结束IP地址范围之间的 IP地址，将允许对应的管理类型访问。

11. 单击 **增加** 按钮

将添加访问规则。

12. 要删除选定的访问规则，请单击“删除”按钮。

更新的配置将发送到交换机。配置更改立即生效。

5.3.12. 查看访问控制统计

要配置访问配置文件设置，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。

将显示web管理界面菜单。

- 7. 单击 **安全管理 > 会话属性管理 > Access Mgmt > Access Management Statistics**



要使用交换机上的最新信息刷新屏幕，请单击更新按钮。
下表描述了显示的表格中的数据。

表71. 访问统计

领域	描述
访问操作权限	网络管理的访问类型。
Receive	接收到的 IP 报文数量。
Allow	接收到的 IP 报文中允许访问的数量。
Discard	接收到的 IP 报文中丢弃的数量。

5.3.13. 配置DoS拒绝服务设置

要配置DoS拒绝服务设置，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > DoS攻击配置 > DoS攻击配置**

The screenshot shows the 'DoS攻击配置 - 配置' (DoS Attack Configuration - Configuration) page. The left sidebar has a 'DOS' menu with 'DoS攻击配置' selected. The main content area contains a table of settings:

Setting Name	Value / Option	Range / Note
Denial of Service First Fragment	☒ 关闭 ☐ 启用	
Denial of Service Min TCP Header Size	20	(0 to 255)
Denial of Service ICMP	☒ 关闭 ☐ 启用	
Denial of Service Max ICMPv4 Size	512	(0 to 16384)
Denial of Service ICMPv6	☒ 关闭 ☐ 启用	
Denial of Service Max ICMPv6 Size	512	(0 to 16384)
Denial of Service ICMP Fragment	☒ 关闭 ☐ 启用	
Denial of Service SIP=DIP	☒ 关闭 ☐ 启用	
Denial of Service SMAC=DMAC	☒ Disable ☐ Enable	
Denial of Service TCP FIN&URG&PSH	☒ 关闭 ☐ 启用	
Denial of Service TCP Flag&Sequence	☒ 关闭 ☐ 启用	
Denial of Service TCP Fragment	☒ 关闭 ☐ 启用	
Denial of Service TCP Offset	☒ 关闭 ☐ 启用	
Denial of Service TCP Port	☒ 关闭 ☐ 启用	
Denial of Service TCP SYN	☒ 关闭 ☐ 启用	
Denial of Service TCP SYN&FIN	☒ 关闭 ☐ 启用	
Denial of Service UDP Port	☒ 关闭 ☐ 启用	

- 8. 在拒绝服务最小TCP标头大小字段中，指定允许的最小TCP标头大小。
如果启用DoS TCP片段，交换机将丢弃以下数据包：
 - 具有TCP负载的第一个TCP片段：IP_负载长度-IP_头大小<最小TCP_头大小。
 - 其范围为0到255。默认值为20。

9. 选择拒绝服务ICMPv4禁用或启用单选按钮。

启用ICMPv4 DoS防护会导致交换机丢弃类型设置为ECHO_REQ (ping) 且大小大于配置的ICMPv4数据包大小的ICMPv4数据包。出厂默认设置为禁用。

10. 指定拒绝服务最大ICMPv4数据包大小。

这是允许的最大ICMPv4 Pkt大小。如果启用了ICMPv4 DoS防护，交换机将丢弃大小大于配置的最大ICMPv4数据包大小的IPv4 ICMP ping数据包。其范围为0到16376。默认值为512。

11. 使用拒绝服务ICMPv6启用ICMPv6 DoS预防。

这会导致交换机丢弃类型设置为ECHO_REQ (ping) 且大小大于配置的ICMPv6 Pkt大小的ICMPv6数据包。出厂默认设置为禁用。

12. 使用拒绝服务最大ICMPv6数据包大小指定允许的最大IPv6 ICMP数据包大小。

如果启用了ICMPv6 DoS防护，交换机将丢弃大小大于配置的最大ICMPv6数据包大小的IPv6 ICMP ping数据包。其范围为0到16376。默认值为512。

13. 选择拒绝服务第一片段禁用或启用单选按钮。

这将启用第一个片段DoS预防，这将导致交换机在接收片段IP数据包时检查第一个片段IP数据包上的DoS选项。否则，交换机将忽略第一个片段IP包。出厂默认值为禁用。

14. 选择拒绝服务ICMP片段禁用或启用单选按钮。

启用ICMP碎片DoS预防会导致交换机丢弃ICMP碎片数据包。出厂默认设置为禁用。

15. 选择拒绝服务SIP=DIP Disable或Enable单选按钮。

Enable SIP=DIP DoS预防导致交换机丢弃源IP地址等于目标IP地址的数据包。出厂默认设置为禁用。

16. 选择拒绝服务SMAC=DMAC禁用或启用单选按钮。

启用SMAC=DMAC DoS防护会导致交换机丢弃源MAC地址等于目标MAC地址的数据包。出厂默认设置为禁用。

17. 选择拒绝服务TCP FIN&URG&PSH禁用或启用单选按钮。

启用TCP FIN&URG&PSH DoS防护将导致交换机丢弃带有TCP标志FIN、URG和PSH set, TCP序列号=0。出厂默认值为Disable。

18. 选择拒绝服务TCP标志和序列禁用或启用单选按钮。

启用TCP标志DoS防护会导致交换机丢弃TCP控制标志设置为0且TCP序列号设置为0的数据包。出厂默认值为禁用。

19. 选择拒绝服务TCP片段禁用或启用单选按钮。

启用TCP片段DoS预防会导致交换机丢弃数据包，如下所示：

具有TCP负载的第一个TCP片段： $IP_负载长度 - IP_头大小 < 最小TCP_头大小$ 。

出厂默认设置为禁用。

20. 选择拒绝服务TCP偏移禁用或启用单选按钮。

启用TCP偏移量DoS预防会导致交换机丢弃TCP标头偏移量为1的数据包。出厂默认值为禁用。

21. 选择拒绝服务TCP端口禁用或启用单选按钮。

启用TCP端口DoS预防会导致交换机丢弃TCP源端口等于TCP目标端口的数据包。出厂默认设置为禁用。

22. 选择拒绝服务TCP SYN Disable或Enable单选按钮。

启用TCP SYN DoS预防会导致交换机丢弃设置了TCP标志SYN的数据包。出厂默认设置为禁用。

23. 选择拒绝服务TCP SYN&FIN Disable或Enable单选按钮。

启用TCP SYN和FIN DoS预防将导致交换机丢弃设置了TCP标志SYN和FIN的数据包。出厂默认设置为禁用。

24. 选择拒绝服务UDP端口禁用或启用单选按钮。

启用UDP端口DoS防护会导致交换机丢弃UDP源端口等于UDP目标端口的数据包。出厂默认设置为禁用。

5.4.端口身份验证

在基于端口的身份验证中，当在端口上全局启用802.1X时，对连接到该端口的任何一个请求方的成功身份验证将导致所有用户能够不受限制地使用该端口。在任何给定时间，仅允许一个请求者在此模式下尝试对端口进行身份验证。此模式下的端口受双向控制。这是默认的身份验证模式。

802.1X网络有三个组件：

- **Authenticators.** 在允许系统访问之前经过身份验证的端口。
- **Suplicants.** 连接到请求访问系统服务的已验证端口的主机。
- **Authentication Server.** 外部服务器，例如，代表验证器执行身份验证并指示用户是否有权访问系统服务的RADIUS服务器。

5.4.1. 配置全局802.1X设置

要配置全局802.1X设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口访问安全管理 > 基本管理 > 802.1X 配置**



8. 选择管理模式禁用或启用单选按钮。

这将启用或禁用交换机上的**802.1X**管理模式。

- **启用**. 允许在交换机上进行基于端口的身份验证。

如果启用**802.1X**，则由**RADIUS**服务器执行身份验证。这意味着主身份验证方法必须是**RADIUS**。要设置方法，请选择**安全>管理安全>身份验证列表**，然后选择**RADIUS**作为**defaultList**的方法1。有关更多信息，请参见“配置登录身份验证列表”。

- **关闭**. 在允许任何端口上的通信之前，交换机不会检查**802.1X**身份验证，即使端口配置为仅允许经过身份验证的用户。默认值。

9. 选择**VLAN**分配模式禁用或启用单选按钮。

默认值为禁用。

10. 选择**EAPOL**整体模式禁用或启用单选按钮。

默认值为禁用。

11. 使用**动态VLAN**创建模式选择禁用或启用。

默认值为禁用。

12. 使用**监视器**模式选择禁用或启用。

默认值为禁用。该功能监视**dot1x**身份验证过程，并帮助诊断身份验证失败案例。

13. 使用**用户**为**802.1x**端口安全性的所选登录列表选择用户名。

14. 使用**Login**选择要应用于指定用户的登录列表。

将显示所有配置的登录列表。身份验证列表字段显示**802.1X**使用的身份验证列表。

5.4.2. Configure 802.1X Settings

配置802.1X设置

要配置802.1X设置，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > 端口访问安全管理 > 高级管理 > 802.1X 配置**



- 8. 选择管理模式禁用或启用单选按钮。
默认值为禁用。
- 9. 选择VLAN分配模式禁用或启用单选按钮。
默认值为禁用。
- 10. 选择EAPOL整体模式禁用或启用单选按钮。
默认值为禁用。
- 11. 使用动态VLAN创建模式选择禁用或启用。

默认值为禁用。

12. 使用监视器模式选择禁用或启用。

默认值为禁用。该功能监视dot1x身份验证过程，并帮助诊断身份验证失败案例。

13. 使用用户为802.1x端口安全性的所选登录列表选择用户名。

14. 使用Login选择要应用于指定用户的登录列表。

将显示所有配置的登录列表。“身份验证列表”字段显示802.1X使用的列表。

5.4.3. 配置端口身份验证

您可以在一个或多个端口上启用和配置端口访问控制。

要为端口配置802.1X设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 登录 按钮。

将显示web管理界面菜单。

7. 单击 安全管理 > 端口访问安全管理 > 高级管理 > 端口认证-身份验证模式配置

提示： 使用屏幕底部的水平滚动条查看所有字段。

端口	控制方式	MAB	静默周期	发送周期	Guest VLAN ID	Guest VLAN认证定时器	未经认证的VLAN ID	Supplicant超时时间	服务器超时时间	最大请求数	PAE功能	允许重新认证	重新认证周期	最大用户数
☐ 0/1	Auto	关闭	60	30	0	90	0	30	30	2	Authenticator	关闭	3600	48
☐ 0/2	Auto	关闭	60	30	0	90	0	30	30	2	Authenticator	关闭	3600	48
☐ 0/3	Auto	关闭	60	30	0	90	0	30	30	2	Authenticator	关闭	3600	48
☐ 0/4	Auto	关闭	60	30	0	90	0	30	30	2	Authenticator	关闭	3600	48
☐ 0/5	Auto	关闭	60	30	0	90	0	30	30	2	Authenticator	关闭	3600	48
☐ 0/6	Auto	关闭	60	30	0	90	0	30	30	2	Authenticator	关闭	3600	48
☐ 0/7	Auto	关闭	60	30	0	90	0	30	30	2	Authenticator	关闭	3600	48
☐ 0/8	Auto	启用	60	30	0	90	0	30	30	2	Authenticator	启用	3600	48

8. 选中要配置的端口旁边的复选框。

您还可以选择多个复选框将相同的设置应用于选定的端口，或者选择标题行中的复选框将相同的设置应用于所有端口。

9. 对于所选端口，请指定以下设置：

- **控制方式.** 为控制模式选择一个选项。仅当端口的链路状态为链路接通时，才设置控制模式。方案如下：
 - **Force unauthorized.** 强迫未经授权，验证器端口访问实体（PAE）无条件地将受控端口设置为未经授权。
 - **Force authorized.** 验证器PAE无条件地将受控端口设置为“已授权”。
 - **Auto.** 认证器PAE设置受控端口模式以反映请求者、认证器和认证服务器之间的认证交换的结果。
 - **MAC Based.** 验证器PAE设置受控端口模式，以反映在每个验证者的基础上，请求者、验证者和认证服务器之间的验证交换的结果。
- **MAB,** 使用MAB启用或禁用基于MAC的。默认选择为禁用。认证器PAE设置受控端口模式，以反映请求者、认证器和认证服务器之间基于每个请求者的认证交换的结果。
- **静默周期.** 此输入字段允许您为所选端口配置静默期。此命令设置此端口上验证器状态机使用的计时器的秒值，以定义它不尝试获取请求者的时间段。静默期是在与请求方的身份验证交换失败后，身份验证方不尝试获取请求方的期间。静默期必须是介于0和65535之间的数字。静默期值为0表示验证器状态机从未获取请求者。默认值为60。在单击“应用”按钮之前，更改该值不会更改配置。
- **发送周期.** 此输入字段允许您配置所选端口的传输周期。传输周期是验证器状态机在指定端口上用于确定何时向请求方发送EAPOL EAP请求/标识帧的计时器的值（以秒为单位）。传输周期必须是一个介于1和65535之间的数字。默认值为30。在单击“应用”按钮之前，更改该值不会更改配置。
- **GuestVLAN ID.** 此字段允许您在接口上配置来宾VLAN ID。有效范围为0–4093。默认值为0。在单击“应用”按钮之前，更改该值不会更改配置。输入0以清除接口上的来宾VLAN ID。
- **Guest VLAN 认证定时器.** 此输入字段允许用户输入所选端口的来宾VLAN周期。来宾VLAN周期是来宾VLAN身份验证计时器的值（以秒为单位）。来宾VLAN超时必须是1到300之间的值。默认值为90。在单击“应用”按钮之前，更改该值不会更改配置。
- **未经认证的VLAN ID.** 输入所选端口的未经验证的VLAN ID。有效范围为0–4093。默认值为0。在单击“应用”按钮之前，更改该值不会更改配置。输入0以清除接口上未经验证的VLAN ID。
- **Supplicant 超时时间.** 输入所选端口的请求超时。请求方超时是此端口上的身份验证程序状态机用于超时请求方的计时器的值（以秒为单位）。请求超时必须在1到65535的范围内。默认值为30。在单击“应用”按钮之前，更改该值不会更改配置。
- **服务器超时时间.** 输入所选端口的服务器超时。服务器超时是此端口上的身份验证程序用于超时身份验证服务器的计时器的值（以秒为单位）。服务器超时必须在1到65535的范围内。默认值为30。在单击“应用”按钮之前，更改该值不会更改配置。
- **最大请求数.** 输入所选端口的最大请求数。**maximum requests**值是此端口上的身份验证程序状态机在超时请求者之前重新传输EAPOL EAP请求/标识的最大次数。最大请求值必须

在1到10之间。默认值为2。在单击“应用”按钮之前，更改该值不会更改配置。

- **PAE 功能.** 选择所选端口的端口访问实体（PAE）功能。可能的值是验证器或请求者。
- **允许重新认证.** 启用或禁用指定端口的请求者的重新身份验证。可选值为启用或禁用。如果该值为**Enable**，则会进行重新身份验证。否则，不允许重新验证。默认值为禁用。在单击应用按钮之前，更改选择不会更改配置。
- **重新认证周期.** 输入所选端口的重新验证周期。重新验证周期是此端口上验证器状态机的计时器值（以秒为单位），用于确定何时对请求者进行重新验证。重新身份验证周期必须是介于1到65535之间的值。默认值为**3600**。在单击“应用”按钮之前，更改该值不会更改配置。
- **最大用户数.** 输入指定接口上请求者数量的限制。

10. 要在所选端口上开始初始化序列，请单击“初始化”按钮。

只有在控制模式为“自动”时，才能单击此按钮。如果按钮不可用，则该按钮将灰显。单击此按钮后，操作立即生效。无需单击“应用”按钮即可执行操作。

11. 单击“重新验证”按钮。

重新验证序列从所选端口开始。

只有在控制模式为“自动”时，才能单击此按钮。如果按钮不可用，则该按钮将灰显。单击此按钮后，操作立即生效。无需单击“应用”按钮即可执行操作。

5.4.4. 查看端口信息

您可以查看有关特定端口上的端口访问控制设置的信息。

要查看端口摘要，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口访问安全管理 > 高级管理 > 端口状态**

系统管理 L2交换管理 路由管理 QoS管理 安全管理 监测管理 维护 简体中文 保存 退出																																																																																																																																																															
系统访问管理 会话属性管理 DoS攻击配置 端口访问安全管理 端口流量控制 端口IP安全管理 ACL																																																																																																																																																															
PortAuthentication 基本管理信息 802.1X 配置 端口认证-身份验证模式配置 端口认证-服务模式配置 IAS用户配置 Dot1x认证管理 802.1X 配置 客户端状态																																																																																																																																																															
端口状态 - 状态 <table> <tr> <th>Port</th><th>控制方式</th><th>实际运行的控制模式</th><th>允许重新认证</th><th>控制方向</th><th>协议版本</th><th>PAE功能</th><th>PAE状态机的当前状态</th><th>后端身份验证状态机的状态</th><th>分配的VLAN ID</th><th>分配VLAN ID的原因</th><th>启用密钥传输</th><th>会话超时时间</th><th>会话终止动作</th><th>端口工作状态</th><th>端口工作模式</th></tr> <tr> <td>0/1</td><td>auto</td><td>N/A</td><td>False</td><td>both</td><td>1</td><td>Authenticator</td><td>Initialize</td><td>Initialize</td><td>0</td><td>Not Assigned</td><td>False</td><td>0</td><td>Default</td><td>N/A</td><td>Port based</td></tr> <tr> <td>0/2</td><td>auto</td><td>N/A</td><td>False</td><td>both</td><td>1</td><td>Authenticator</td><td>Initialize</td><td>Initialize</td><td>0</td><td>Not Assigned</td><td>False</td><td>0</td><td>Default</td><td>N/A</td><td>Port based</td></tr> <tr> <td>0/3</td><td>auto</td><td>N/A</td><td>False</td><td>both</td><td>1</td><td>Authenticator</td><td>Initialize</td><td>Initialize</td><td>0</td><td>Not Assigned</td><td>False</td><td>0</td><td>Default</td><td>N/A</td><td>Port based</td></tr> <tr> <td>0/4</td><td>auto</td><td>N/A</td><td>False</td><td>both</td><td>1</td><td>Authenticator</td><td>Initialize</td><td>Initialize</td><td>0</td><td>Not Assigned</td><td>False</td><td>0</td><td>Default</td><td>N/A</td><td>Port based</td></tr> <tr> <td>0/5</td><td>auto</td><td>N/A</td><td>False</td><td>both</td><td>1</td><td>Authenticator</td><td>Initialize</td><td>Initialize</td><td>0</td><td>Not Assigned</td><td>False</td><td>0</td><td>Default</td><td>N/A</td><td>Port based</td></tr> <tr> <td>0/6</td><td>auto</td><td>N/A</td><td>False</td><td>both</td><td>1</td><td>Authenticator</td><td>Initialize</td><td>Initialize</td><td>0</td><td>Not Assigned</td><td>False</td><td>0</td><td>Default</td><td>N/A</td><td>Port based</td></tr> <tr> <td>0/7</td><td>auto</td><td>N/A</td><td>False</td><td>both</td><td>1</td><td>Authenticator</td><td>Initialize</td><td>Initialize</td><td>0</td><td>Not Assigned</td><td>False</td><td>0</td><td>Default</td><td>N/A</td><td>Port based</td></tr> <tr> <td>0/8</td><td>auto</td><td>N/A</td><td>False</td><td>both</td><td>1</td><td>Authenticator</td><td>Initialize</td><td>Initialize</td><td>0</td><td>Not Assigned</td><td>False</td><td>0</td><td>Default</td><td>N/A</td><td>Port based</td></tr> </table>																Port	控制方式	实际运行的控制模式	允许重新认证	控制方向	协议版本	PAE功能	PAE状态机的当前状态	后端身份验证状态机的状态	分配的VLAN ID	分配VLAN ID的原因	启用密钥传输	会话超时时间	会话终止动作	端口工作状态	端口工作模式	0/1	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based	0/2	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based	0/3	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based	0/4	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based	0/5	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based	0/6	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based	0/7	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based	0/8	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based
Port	控制方式	实际运行的控制模式	允许重新认证	控制方向	协议版本	PAE功能	PAE状态机的当前状态	后端身份验证状态机的状态	分配的VLAN ID	分配VLAN ID的原因	启用密钥传输	会话超时时间	会话终止动作	端口工作状态	端口工作模式																																																																																																																																																
0/1	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based																																																																																																																																																
0/2	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based																																																																																																																																																
0/3	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based																																																																																																																																																
0/4	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based																																																																																																																																																
0/5	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based																																																																																																																																																
0/6	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based																																																																																																																																																
0/7	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based																																																																																																																																																
0/8	auto	N/A	False	both	1	Authenticator	Initialize	Initialize	0	Not Assigned	False	0	Default	N/A	Port based																																																																																																																																																

下表介绍了端口摘要屏幕上的字段。

表72. 端口汇总表

字段	描述
Port	其设置显示在当前表行中的端口。
控制方式	此字段表示端口配置的控制模式。可能的值如下所示： Force Unauthorized. 验证器端口访问实体（PAE）无条件地将受控端口设置为未经授权。 Force Authorized. 验证器PAE无条件地将受控端口设置为“已授权”。 Auto. 认证器PAE设置受控端口模式以反映请求者、认证器和认证服务器之间的认证交换的结果。 MAC Based. 验证器PAE设置受控端口模式以反映每个请求者、验证器和认证服务器之间的认证交换的结果。
Operating Control Mode	端口实际运行的控制模式。可能的值如下： - ForceUnauthorized - ForceAuthorized - Auto - MAC Based - N/A: 如果端口处于分离状态，则无法参与端口访问控制。
允许重新认证	此字段显示是否允许重新验证指定端口的请求者。可能的值为True和False。如果该值为True，则会进行重新身份验证。否则，不允许重新验证。
控制方向	指定端口的控制方向。控制方向指示请求者和认证者之间协议交换的程度。这会影响未经授权的受控端口是在两个方向（禁用传入和传出帧）还是仅在传入方向（仅禁用传入帧的接收）上对通信进行控制。

协议版本	与所选端口关联的协议版本。唯一可能的值是1，对应于802.1x规范的第一个版本。此字段不可配置。
PAE 能力	所选端口的端口访问实体（PAE）功能。可能的值是验证器或请求者。此字段不可配置。
PAE状态机的当前状态	验证器PAE状态机的当前状态。可能的值如下所示： • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • ForceAuthorized • ForceUnauthorized
后端身份验证状态机的状态	后端身份验证状态机的当前状态。可能的值如下所示： • Request • Response • Success • Fail • Timeout • Initialize • Idle
分配的VLAN ID	由验证器分配给所选接口的VLAN ID。仅当所选接口的端口控制模式不是基于MAC时，才会显示此字段。
VLAN分配原因	验证器分配给所选接口的VLAN ID的原因。仅当所选接口的端口控制模式不是基于MAC时，才会显示此字段。此字段不可配置。可能的值如下所示： • Radius • Unauth • Default • Not Assigned
启用密钥传输	此字段显示所选端口上是否启用了密钥传输。 这不是一个可配置的字段。可能的值为True和False。如果该值为False，则不会发生密钥传输。否则，所选端口支持密钥传输。
会话超时	RADIUS服务器为所选端口设置的会话端口。仅当所选端口的端口控制模式不是基于MAC时，才会显示此字段。

会话终止动作	RADIUS服务器为所选端口设置的终止操作。仅当所选端口的端口控制模式不是基于MAC时，才会显示此字段。可能的值如下所示 • Default • Reauthenticate 如果终止操作设置为默认，则在会话结束时，初始化客户端详细信息。否则，将尝试重新验证。
端口工作状态	指定端口的授权状态。可能的值为授权值、未授权值和不适用值。如果端口处于分离状态，则该值为N/A，因为该端口无法参与端口访问控制。

5.4.5. 查看客户端信息

要查看客户端摘要，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
7. 将显示web管理界面菜单。
8. 单击 **安全管理 > 端口访问安全管理 > 高级管理 > 客户端状态**



表73. 客户概要

字段	描述
端口	要显示的端口。

用户名	表示请求方设备标识的用户名。
请求者Mac地址	请求者的设备MAC地址。
会话开始时间	自请求者登录以来的时间，以秒为单位。
过滤器ID	身份验证程序分配给请求方设备的策略筛选器ID。
VLAN ID	验证器分配给请求方设备的VLAN ID。
分配的VLAN ID	验证器分配给请求方设备的VLAN ID的原因。
会话超时时间	RADIUS服务器向请求方设备设置的会话超时。
终止行动	RADIUS服务器向请求方设备设置的终止操作。

5.5.流量控制

您可以配置MAC筛选器、风暴控制、端口安全和受保护的端口设置。

5.5.1. 配置MAC筛选

您可以创建MAC筛选器，以限制允许进出系统上指定端口的流量。

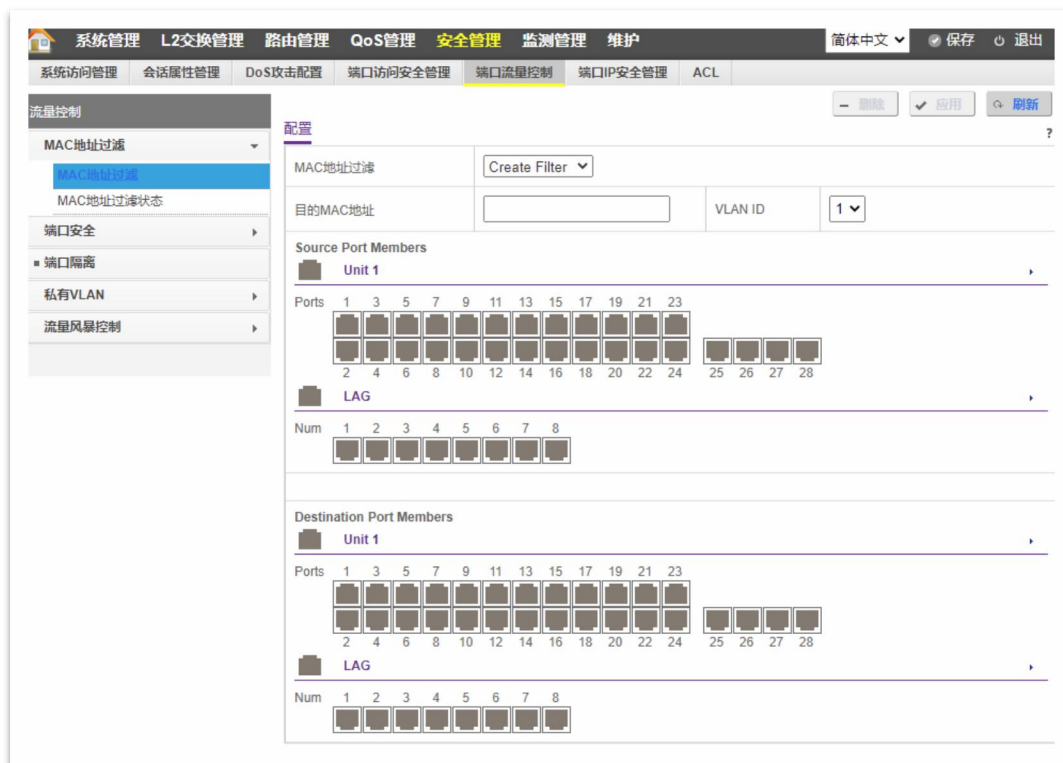
要配置MAC筛选器设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
将显示web管理界面菜单。
7. 单击 **安全管理 > 端口流量控制 > MAC 地址过滤**



这是所有已配置筛选器的MAC地址和VLAN ID对的列表。

8. 要更改现有筛选器的端口掩码，请选择条目。
9. 要添加新筛选器，请从MAC筛选器列表中选择创建筛选器。
10. 从VLAN ID列表中，选择要与MAC地址一起使用的VLAN，以完全标识要过滤的数据包。

仅当从MAC筛选器列表中选择“创建筛选器”时，才能更改此字段。

11. 在MAC地址字段中，以00:01:1A:B2:53:4D格式指定筛选器的MAC地址。

选择“创建过滤器”选项时，可以更改此字段。

无法为以下MAC地址定义筛选器：

- 00:00:00:00:00:00
- 01:80:C2:00:00至01:80:C2:00:00:0F
- 01:80:C2:00:00:20至01:80:C2:00:21
- FF:FF:FF:FF:FF:FF

12. 使用源端口成员列出要包括在入站筛选器中的端口。

如果在不在列表中的端口上接收到具有所选MAC地址和VLAN ID的数据包，则会丢弃该数据包。

13. 使用目标端口成员列出要包括在出站筛选器中的端口。

具有您选择的MAC地址和VLAN ID的数据包仅从列表中的端口传输。目标端口只能包含在组播筛选器中。

- 14. 要删除已配置的MAC筛选器，请选择它，然后单击删除按钮。
- 15. 单击应用按钮。

更新的配置将发送到交换机。配置更改立即生效。

5.5.2. MAC筛选器摘要

要查看MAC筛选器摘要，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
- 7. 将显示web管理界面菜单。
- 8. 单击 **安全管理 > 端口流量控制 > MAC地址过滤 > MAC地址过滤状态**



下表描述了屏幕上显示的信息。

表74. MAC过滤器摘要

字段	描述
MAC 地址	过滤器的MAC地址格式为00:01:1A:B2:53:4D。
VLAN ID	与筛选器关联的VLAN ID。
源端口成员	用于筛选入站数据包的端口列表。
目的端口成员	用于筛选出站数据包的端口列表。

5.6.端口安全

您可以配置端口安全设置。

5.6.1.配置全局端口安全模式

您可以锁定系统上的一个或多个端口。当端口被锁定时，只能转发具有允许的源MAC地址的数据包。所有其他数据包都将被丢弃。

要配置全局端口安全模式，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > 端口流量控制 > 端口安全 > 端口安全配置**



- 8. 选择端口安全模式禁用或启用单选按钮。

“端口安全冲突”表显示了有关为端口安全启用的端口上发生的冲突的信息。下表介绍了端口安全冲突表中的字段。

表75. 违反端口安全规定

字段	描述
端口	物理接口。
丢弃的最后一个报文的源MAC地址	在锁定端口丢弃的最后一个数据包的源MAC地址。
VLAN ID	与上次违反MAC地址对应的VLAN ID。

5.6.2. 配置端口安全接口

MAC地址可以通过两种方法之一定义为允许的：动态或静态。当端口被锁定时，这两种方法同时使用。

动态锁定实现了端口安全的第一到达机制。您可以指定在锁定的端口上可以读入多少地址。如果未达到限制，则学习并正常转发具有未知源MAC地址的数据包。当达到限制时，端口上不再读入地址。任何带有源MAC地址但尚未读入的数据包都将被丢弃。通过将允许的动态条目数设置为零，可以有效地禁用动态锁定。

静态锁定允许您指定端口上允许的MAC地址列表。数据包的行为与动态锁定相同：只能转发具有允许的源MAC地址的数据包。

要配置端口安全设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。

- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。
交换机的默认IP地址为 192.168.10.12 。
此时将显示登录屏幕。
- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > 端口流量控制 > 端口安全 > 端口配置**



- 8. 选中要配置的端口或延迟旁边的复选框。
选中多个复选框可将相同设置应用于所有选定接口。选中标题行中的复选框，将相同的设置应用于所有接口。
- 9. 指定以下设置：
 - **安全模式**. 启用或禁用所选接口的端口安全功能。
 - **最大允许动态学习MAC**. 设置所选接口上动态学习的MAC地址的最大数目。
 - **最大允许静态锁定MAC**. 设置所选接口上静态锁定MAC地址的最大数量。
 - **违规后动作模式**. 启用或禁用发送新的违规消息。

5.6.3. 将学到的MAC地址转换为静态地址

您可以将动态学习的MAC地址转换为静态锁定的地址。

要转换学习的MAC地址，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。

- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > 端口流量控制 > 动态地址 > 动态地址**



- 8. 使用端口列表选择物理接口
- 9. 使用 **转换动态地址为静态** 复选框将动态读入的MAC地址转换为静态锁定的地址。
动态MAC地址项按数字升序转换为静态MAC地址项，直到达到静态限制。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表显示了MAC地址及其在所选端口上识别的相关VLAN。使用端口列表菜单选择接口。

表76. 动态MAC地址

字段	描述
学习到的动态MAC地址的个数	特定端口上动态学习的MAC地址数。
VLAN ID	与MAC地址对应的VLAN ID。
MAC 地址	在特定端口上学习的MAC地址。

5.6.4. 配置静态MAC地址

要配置静态MAC地址，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > 端口流量控制 > 端口安全 > 静态MAC地址管理**



- 8. 使用接口选择物理接口。
- 9. **静态MAC地址**. 接受要添加的MAC地址的用户输入。
- 10. 使用VLAN ID选择与要添加的MAC地址对应的VLAN ID。
- 11. 单击添加按钮。
静态MAC地址被添加到交换机中。
- 12. 要从交换机中删除现有静态MAC地址，请单击删除按钮。

5.6.5. 配置保护端口

如果端口配置为受保护，则它不会将流量转发到交换机上的任何其他受保护端口，但会将流量转发到未受保护的端口。您可以将端口配置为受保护或不受保护。您需要具有读写访问权限才能修改配置。

要配置受保护的端口，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口流量控制 > 端口隔离**



8. 在“组ID”列表中，选择一组可组合到逻辑组中的受保护端口。

流量可以在属于不同组的受保护端口之间流动，但不能在同一组内流动。该列表包括当前平台支持的所有可能的受保护端口组ID。Group ID的有效范围为0到2。

9. 使用可选组名称字段将名称与受保护端口组关联（用于标识目的）。

它最多可以是32个字母数字字符，包括空格。默认值为空。此字段是可选的。

10. 单击橙色栏以显示可用端口。

11. 选中每个端口下方的复选框，将其配置为受保护的端口。

选择列表由物理端口（受保护和未受保护）组成。受保护的端口被勾选以区分它们。两个受保护端口之间不可能进行流量转发。如果未配置，则默认状态为未受保护。

12. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

5.6.6. 配置私有VLAN

私有VLAN包含不能相互通信但可以访问另一个网络的交换机端口。这些端口称为专用端口。每个私有VLAN包含一个或多个专用端口和一个上行端口或上行聚合组。请注意，私有端口之间的所有流量在所有层都被阻止，不仅是第2层流量，还包括FTP、HTTP和Telnet等流量。

要配置私有VLAN类型，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。

- 7. 单击 **安全管理 > 端口流量控制 > 私有VLAN > 私有VLAN类别配置**



- 8. 使用私有VLAN类型选择私有VLAN的类型。The factory 出厂默认值为未配置。
- 9. 单击 **应用** 按钮
更新的配置参数将发送到交换机，配置更改将立即生效。
VLAN ID字段指定正在为其设置私有VLAN类型的VLAN ID。出厂默认值为未配置。

5.6.7. 配置私有VLAN关联设置

要配置私有VLAN关联，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。

将显示web管理界面菜单。

- 7. 单击 **安全管理 > 端口流量控制 > 私有VLAN > VLAN关联配置**



- 8. 使用主VLAN选择域的主VLAN ID。
这用于将辅助VLAN与域关联。
- 9. 使用辅助VLAN显示所有静态创建的VLAN（不包括主VLAN和默认VLAN）。
此控件用于将VLAN与选定的主VLAN关联。
- 10. 要从交换机中删除基于IP子网的VLAN，请单击删除按钮。
- 11. 单击应用按钮。

更新的配置将发送到交换机。配置更改立即生效。

下表描述了屏幕上显示的不可配置信息。

表77. 私有VLAN关联

字段	描述
Isolated VLAN	与所选主VLAN关联的隔离VLAN。
Community VLAN(s)	与所选主VLAN关联的社区VLAN列表。

5.6.8. 配置私有VLAN端口模式

要配置私有VLAN端口模式，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口流量控制 > 私有VLAN > 端口模式配置**



8. 使用交换机端口模式选择交换机端口模式。
 - **General:** 在通用模式下设置端口。
 - **Host:** 在主机模式下设置端口。用于私有VLAN配置。

- **Promiscuous:** 将端口设置为混杂模式。用于私有VLAN配置。

9. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

5.6.9. 配置私有VLAN主机接口

要配置私有VLAN主机接口，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口流量控制 > 私有VLAN > 主机接口配置**



8. 在主机主VLAN字段中，设置主机关联模式的主VLAN ID。

VLAN ID的范围为2–4093。

9. 使用主机辅助VLAN为主机关联模式设置辅助VLAN ID。

VLAN ID的范围为2–4093。

10. 要从交换机中删除基于IP子网的VLAN，请单击删除按钮。

11. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

下表描述了屏幕上显示的不可配置信息。

表78. 私有VLAN主机接口配置

字段	描述
Interface	选择物理接口或汇聚组。
Operational VLAN(s)	包含的工作 VLANs.

5.6.10. 配置私有VLAN混杂接口

要配置私有VLAN混杂接口，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口流量控制 > 私有VLAN > 端口混杂模式配置**



8. 使用混杂主VLAN为混杂关联模式设置主VLAN ID。

VLAN ID的范围为2–4093。

9. 使用混杂次要VLAN ID设置混杂关联模式的次要VLAN ID列表。

此字段可以接受单个VLAN ID或VLAN ID范围，或以“，”分隔的顺序接受两者的组合。您可以指定单个VLAN ID，例如10。您可以指定用连字符分隔的VLAN范围值，例如10-13。您可以指定用逗号分隔的两者的组合，例如：12,15,40–431000–10052000。VLAN ID的范围为2–4093。

提示： 该控件中给出的VLAN ID List替换关联中已配置的辅助VLAN列表。

10. 单击删除按钮从交换机中删除基于IP子网的VLAN。

11. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

下表描述了屏幕上显示的不可配置信息。

表79. 私有VLAN混杂接口配置

字段	描述
接口	选择物理或LAG接口
Operational VLAN(s)	包含的工作 VLANs

5.6.11. 风暴控制

广播风暴是由单个端口通过网络同时传输的广播消息过多造成的。转发的消息响应

可能会使网络资源过载和/或导致网络超时。

交换机测量每个端口的传入广播/组播/未知单播数据包速率，并在速率超过定义值时丢弃数据包。通过定义数据包类型和数据包传输速率，每个接口都可以启用风暴控制。

5.6.12. 配置全局风暴控制设置

要配置全局风暴控制设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口流量控制 > 流量风暴控制 > 流量风暴全局配置**



以下三个控件提供了一种简单的方法，可以以全局方式在每个端口上启用或禁用每种类型的数据包的速率限制。通过进入端口配置屏幕，可以查看每个端口的有效风暴控制状态。

8. 选择广播风暴控制全部禁用或启用单选按钮。

这将启用或禁用所有端口上的广播风暴恢复模式。当您指定启用且任何以太网端口上的广播流量超过配置的阈值时，交换机将阻止（丢弃）广播流量。出厂默认设置为启用。

9. 选择组播风暴控制全部禁用或启用单选按钮。

这将在所有端口上启用或禁用组播风暴恢复模式。当您指定启用，并且任何以太网端口上的组播流量超过配置的阈值时，交换机将阻止（丢弃）组播流量。出厂默认设置为禁用。

10. 选择未知单播风暴控制全部禁用或启用单选按钮。

这将在所有端口上启用或禁用单播风暴恢复模式。当您指定启用，并且任何以太网端口上的单播通信量超过配置的阈值时，交换机将阻止（丢弃）单播通信量。出厂默认设置为禁用。

5.6.13. 配置风暴控制界面

要配置风暴控制界面，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

- 6. 单击 **登录** 按钮。

将显示web管理界面菜单。

- 7. 单击 **安全管理 > 端口流量控制 > 流量风暴控制 > 端口配置**



下表描述了屏幕上显示的不可配置信息。

表80. 风暴控制接口配置

字段	描述
广播风暴恢复模式	通过在下拉输入字段中选择相应的行来启用或禁用此选项。当您为广播风暴恢复指定启用且指定以太网端口上的广播流量超过配置的阈值时，交换机将阻止（丢弃）广播流量。出厂默认设置为启用。
广播风暴恢复级别类型	将广播风暴恢复级别指定为链路速度的百分比或每秒的数据包数。

广播风暴恢复水平	指定风暴控制激活的阈值。对于pps类型，出厂默认值为端口速度的5%。
广播风暴控制行动	提供在广播风暴恢复功能的配置阈值被突破时关闭端口的配置能力。选择关机或速率限制模式选项。默认值为RateLimit。
组播风暴恢复模式	通过选择列表中的相应行来启用或禁用此选项。当您指定启用组播风暴恢复，并且指定以太网端口上的组播流量超过配置的阈值时，交换机将阻止（丢弃）组播流量。出厂默认设置为禁用。
组播风暴恢复级别类型	将组播风暴恢复级别指定为链路速度的百分比或每秒的数据包数。
组播风暴恢复级别	指定风暴控制激活的阈值。对于pps类型，出厂默认值为端口速度的5%。
单播风暴恢复模式	启用或禁用此选项。当您为单播风暴恢复指定启用且指定以太网端口上的单播流量超过配置的阈值时，交换机将阻止（丢弃）单播流量。出厂默认设置为禁用。
单播风暴恢复级别类型	将单播风暴恢复级别指定为链路速度的百分比或每秒的数据包数。
单播风暴恢复级别	指定风暴控制激活的阈值。对于pps类型，出厂默认值为端口速度的5%。

5.7.DHCP Snooping

您可以配置DHCP侦听全局和接口设置。

5.7.1. 配置DHCP侦听全局设置

配置DHCP侦听全局设置

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口IP安全管理 > DHCP Snooping > 全局配置**



8. 选择DHCP窥探模式禁用或启用单选按钮。

出厂默认设置为禁用。

9. 选择MAC地址验证禁用或启用单选按钮。

这将启用或禁用DHCP窥探发送方MAC地址的验证。出厂默认设置为启用。

10. 使用VLAN ID输入要启用DHCP侦听模式的VLAN。

11. 使用DHCP窥探模式为输入的VLAN启用或禁用DHCP窥探功能。

出厂默认设置为禁用。

12. 单击应用按钮。

更新的配置将发送到交换机。除非执行保存配置，否则在整个电源循环中不会保留这些更改。

5.7.2. 配置DHCP侦听接口

要配置DHCP侦听接口，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口IP安全管理 > DHCP Snooping > 端口配置**



8. 使用界面复选框选择界面。

9. 如果启用了信任模式，DHCP侦听应用程序会将端口视为受信任的端口。

出厂默认设置为禁用。

10. 如果启用了无效数据包，DHCP侦听应用程序将在此接口上记录无效数据包。

出厂默认设置为禁用。

11. 使用速率限制（pps）指定用于DHCP侦听的速率限制值。

如果DHCP数据包的传入速率在连续的突发间隔秒内超过此值，则端口将关闭。如果该值为N/A，则突发间隔没有意义，因此它被禁用。默认值为不适用。可将其设置为值-1，表示不适用。利率限制范围为0至300。

12. 使用突发间隔（秒）为此接口上的速率限制目的指定突发间隔值。

如果速率限制为N/A，则突发间隔没有意义，它是N/A。默认值为不适用。可设置为-1，表示不适用。突发间隔的范围是1到15。

5.7.3. 配置DHCP侦听绑定

要配置侦听绑定，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > 端口IP安全管理 > DHCP Snooping > 地址绑定管理**



- 8. 要配置静态绑定，请指定以下内容：
 - a. 使用界面复选框选择界面。
 - b. 使用MAC地址指定要添加的绑定项的MAC地址。这是绑定数据库的密钥。
 - c. 使用VLAN ID从绑定规则的列表中选择VLAN。VLAN ID的范围为1到4093。
 - d. 使用IP地址为绑定规则指定有效的IP地址。
 - e. 单击 **增加** 按钮
DHCP侦听绑定条目将添加到数据库中。
 - f. 要从数据库中删除选定的静态条目，请单击“删除”按钮。
- 9. 要配置动态绑定，请指定以下内容：
 - a. 使用界面复选框选择界面。
 - b. 使用MAC地址在绑定数据库中显示绑定的MAC地址。
 - c. 使用VLAN ID在绑定数据库中显示绑定项的VLAN。VLAN ID的范围为1到4093。
 - d. **IP Address.** 显示绑定数据库中绑定项的IP地址。
 - e. **租赁时间.** 动态条目的剩余租用时间。
 - f. 要删除所有DHCP侦听绑定项，请单击清除按钮。

5.7.4. 配置窥探持久设置

要配置窥探持久设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
将显示web管理界面菜单。
7. 单击 **安全管理 > 端口IP安全管理 > DHCP Snooping > 地址表保存配置**



8. 选择存储本地或远程单选按钮。
选择“本地”将禁用远程字段“远程文件名”和“远程IP地址”。
9. 如果选择“远程”，请执行以下操作：
 - a. 在远程IP地址字段中，键入用于存储窥探数据库的远程IP地址。
 - b. 在远程文件名字段中，输入要存储数据库的远程文件名。
10. 在写入延迟字段中，输入将数据库写入本地或远程的最长写入时间。
范围是15到86400。

5.7.5. 查看DHCP窥探统计信息

要查看DHCP窥探统计信息，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > 端口IP安全管理 > DHCP Snooping > 包文统计**。



要清除所有接口统计信息，请单击“清除”按钮。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表介绍了DHCP侦听统计信息。

表81. DHCP侦听统计信息

字段	描述
不受信任的端口	要显示其统计信息的不受信任且支持窥探的界面。
MAC地址验证而丢弃的报文数	由于找不到匹配的DHCP窥探绑定项而被DHCP窥探丢弃的数据包数。
不匹配而丢弃的报文数	根据源MAC地址和客户端HW地址验证丢弃的DHCP消息数。
不受信任端口上丢弃的服务器消息的数量	在不受信任的端口上丢弃的服务器消息数。

5.7.6. 配置IP源保护接口

您可以在每个接口上配置IP源代码保护（IPSG）。IPSG是一种基于源ID过滤IP数据包的安全功能。此功能有助于保护网络免受使用IP地址欺骗来危害或破坏网络的攻击。源ID可以是源IP地址，也可以是源IP地址和源MAC地址对。DHCP窥探绑定数据库以及数据库中的IPSG条

目标标识授权的源ID。如果在禁用DHCP侦听或启用DHCP侦听但该端口受信任的端口上启用IPSG，则根据管理员配置的IPSG条目，该端口上接收的所有IP通信都将被丢弃。此外，IPSG与端口安全性（也称为端口MAC锁定）交互，以在接收到的数据包中强制执行源MAC地址。端口安全性控制第2层转发数据库（MAC地址表）中的源MAC地址学习。当接收到具有先前未学习的源MAC地址的帧时，端口安全性查询IPSG功能以确定MAC地址是否属于有效绑定。

要配置IP源保护接口设置，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > 端口IP安全管理 > IPSG 管理 > 端口配置**



- 8. 使用接口复选框选择接口。
- 9. 在IPSG模式列表中，选择禁用或启用。

这将在界面上设置IPSG的管理模式。启用IPSG模式时，将根据DHCP侦听绑定数据库验证此接口上的发送方IP地址。如果启用IPSG，则如果发送方IP地址不在DHCP侦听绑定数据库中，则不会转发数据包。出厂默认设置为禁用。

10. 在IPSG端口安全列表中，选择禁用或启用。

这将启用或禁用所选接口上IPSG端口安全性的管理模式。启用此选项后，如果发送方MAC地址不在转发数据库（FDB）表或DHCP侦听绑定数据库中，则不会转发数据包。要根据MAC地址实施过滤，其他所需配置如下：

- 全局启用端口安全。
- 在接口级别启用端口安全性。

如果禁用IPSG，则无法启用IPSG端口安全性。出厂默认设置为禁用。

11. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

5.7.7. 配置IP源保护绑定设置

要配置IP保护静态绑定设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口IP安全管理 > IPSG管理 > 地址绑定管理**

接口	MAC地址	VLAN ID	IP 地址	Filter Type
0/1		1		

接口	MAC地址	VLAN ID	IP 地址	Filter Type
----	-------	---------	-------	-------------

8. 使用“接口”复选框选择接口。
9. 在MAC地址字段中，键入绑定的MAC地址。
10. 在VLAN ID列表中，选择绑定规则的VLAN。

11. 在IP地址字段中，为绑定规则指定有效的IP地址。

12. 单击添加按钮。

IPSG静态绑定条目被添加到数据库中。

13. 要从数据库中删除选定的静态条目，请单击“删除”按钮。

要清除所有动态绑定条目，请单击“清除”按钮。

下表描述了显示的不可配置的IP源代码保护动态绑定配置信息。

表82. IP源保护动态绑定配置

字段	描述
接口	要向IPSG数据库中添加绑定的接口。
MAC地址	绑定项的MAC地址。
VLAN ID	绑定项的VLAN。
IP 地址	显示绑定项的有效IP地址。
Filter Type	接口上使用的筛选器类型。一种是源IP地址筛选器类型，另一种是源IP地址和MAC地址筛选器类型。

5.7.8. 配置动态ARP检查

要配置动态ARP检查（DAI），请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口IP安全管理 > 动态ARP检验 > DAI 配置**



8. 选择验证源MAC禁用或启用单选按钮。

这指定交换机的DAI源MAC验证模式。如果选择启用，则启用ARP数据包的发送方MAC验证。出厂默认设置为禁用。

9. 选择验证目标MAC禁用或启用单选按钮

这指定交换机的DAI目标MAC验证模式。如果选择启用，则启用ARP响应数据包的目标MAC验证。出厂默认设置为禁用。

10. 选择验证IP禁用或启用单选按钮。

这将指定交换机的DAI IP验证模式。如果选择启用，则启用ARP数据包的IP地址验证。出厂默认设置为禁用。

5.7.9. 配置 DAI VLAN

要配置DAI VLAN，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口IP安全管理 > 动态ARP检验 > DAI保护VLAN配置**



8. 使用VLAN ID复选框选择支持DAI的VLAN。

9. 在管理模式列表中，选择启用或禁用。

这表示是否在此VLAN上启用了动态ARP检查。如果设置为启用，则启用动态ARP检查。如果设置为禁用，则禁用动态ARP检查。默认设置为禁用。

10. 使用无效数据包指示是否在此VLAN上启用了动态ARP检查日志记录。

如果设置为启用，将记录无效的ARP数据包信息。如果设置为禁用，则禁用动态ARP检查日志记录。默认值为Enable。

11. 使用ARP ACL名称为ARP访问列表指定名称。

VLAN可以配置为使用此包含规则的ARP ACL作为ARP数据包验证的筛选器。名称最多可包含31个字母数字字符。如果指定不适用，则会删除ARP ACL名称。

12. 在ARP ACL规则不匹配的情况下，使用静态标志确定ARP数据包是否需要使用DHCP侦听数据库进行验证。

如果该标志已启用，则仅通过ARP ACL规则验证ARP数据包。如果该标志被禁用，则ARP数据包需要使用DHCP侦听条目进行进一步验证。出厂默认设置为禁用。

13. 单击应用按钮。

更新的配置将发送到交换机。配置更改立即生效。

5.7.10. 配置DAI接口

要配置DAI接口，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

- 单击 **登录** 按钮。

将显示web管理界面菜单。

- 单击 **安全管理 > 端口IP安全管理 > 动态ARP检验 > DAI端口配置**



- 使用接口复选框选择物理接口。

- 使用信任模式指示接口是否受信任以进行动态ARP检查。

如果将其设置为启用，则该接口受信任。到达该接口的ARP数据包在不进行检查的情况下被转发。如果设置为禁用，则该接口不受信任。到达该接口的ARP数据包将接受ARP检查。出厂默认设置为禁用。

- 使用速率限制（pps）指定用于动态ARP检查的速率限制值。

如果ARP数据包的传入速率在连续的突发间隔秒内超过该值，ARP数据包将被丢弃。如果该值为N/A，则没有限制。该值可设置为-1，表示不适用。范围为0-300。出厂默认值为15 pps（每秒数据包）。

- 使用突发间隔（秒）为此接口上的速率限制目的指定突发间隔值。如果速率限制为“无”，则“突发间隔”没有意义，显示为N/A。出厂默认值为1秒。

5.7.11. 配置 DAI ACL

要配置DAI ACL，请执行以下操作：

- 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 启动web浏览器。
- 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > 端口IP安全管理 > 动态ARP检验 > 创建 ACL**



8. 使用“**ACL名称**”为DAI创建ARP ACL。

9. 单击 **增加** 按钮

DAI ACL被添加到交换机配置中。

10. 要从交换机配置中删除当前选定的DAI ACL，请单击删除按钮。

5.7.12. 配置DAI ACL规则

要配置DAI ACL规则，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 安全管理 > 端口IP安全管理 > 动态ARP检验 > ACL规则管理



- 8. 在ACL名称字段中，选择DAI ARP ACL。
- 9. 单击添加按钮。
规则将添加到所选ACL。
- 10. 要从选定的ACL中删除当前选定的规则，请单击“删除”按钮。

下表描述了屏幕上显示的不可配置信息。

表83. DAI ACL规则配置

字段	描述
源IP地址	这表示DAI ARP ACL的发送方IP地址匹配值。
源MAC地址	这表示DAI ARP ACL的发送方MAC地址匹配值。

5.7.13. 查看DAI统计数据

要查看DAI统计信息，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 登录 按钮。
将显示web管理界面菜单。

7. 单击 安全管理 > 端口IP安全管理 > 动态ARP检验 > DAI包文统计



要清除DAI统计信息，请单击清除按钮。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表描述了屏幕上显示的不可配置信息。

表84. DAI统计数据

字段	描述
VLAN	要显示其统计信息的已启用VLAN ID。
无匹配的表项而被丢弃的报文数	由于找不到匹配的DHCP窥探绑定项，DAI丢弃的ARP数据包数。
匹配表项而转发的报文数	由于找到匹配的DHCP窥探绑定项，DAI转发的ARP数据包数。
没有匹配ACL规则而被丢弃的报文数	DAI丢弃的ARP数据包数，因为没有为此VLAN找到匹配的ARP ACL规则，并且在此VLAN上设置了静态标志。
匹配ACL规则而允许的报文数	DAI允许的ARP数据包数，因为找到了与此VLAN匹配的ARP ACL规则。
源MAC地址不匹配而被丢弃的报文数	由于ARP数据包中的发送方MAC地址与以太网报头中的源MAC地址不匹配，DAI丢弃的ARP数据包数。
目的MAC地址不匹配而被丢弃的报文数	由于ARP应答数据包中的目标MAC地址与以太网报头中的目标MAC地址不匹配，DAI丢弃的ARP数据包数。
IP地址不合法而丢弃的报文数	由于ARP数据包中的发送方IP地址或ARP应答数据包中的目标IP地址无效，DAI丢弃的ARP数据包数。无效地址包括0.0.0.0、255.255.255.255、IP组播地址、E类地址（240.0.0.0/4）、环回地址（127.0.0.0/8）。
转发的有效ARP报文数	DAI转发的有效ARP数据包数。
丢弃的ARP报文数	DAI丢弃的无效ARP数据包数。

5.8.配置访问控制列表ACL

访问控制列表（ACL）确保只有授权用户才能访问特定资源，同时阻止任何不必要的访问网络资源的尝试。ACL用于提供流量控制、限制路由更新的内容、决定转发或阻止哪种类型的流量，最重要的是为网络提供安全性。本管理交换机的软件支持IPv4、IPv6和MAC ACL。

首先创建基于IPv4、基于IPv6或基于mac的ACL ID。然后，创建规则并将其分配给唯一的ACL ID。接下来，定义规则，这些规则可以识别协议、源和目的IP和MAC地址，以及其他包匹配条件。最后，使用ID号将ACL分配给端口或LAG。

5.8.1. 配置基本 MAC ACL

MAC ACL由一组规则组成，这些规则按顺序与数据包匹配。当数据包满足规则的匹配条件时，将执行指定的规则操作（允许/拒绝），并且不会检查其他规则是否匹配。使用MAC ACL规则配置屏幕指定/创建MAC ACL的规则。

定义MAC ACL并将其应用于交换机涉及多个步骤：

1. 创建ACL名称。
2. 为ACL创建规则(Rules)。
3. 按名称将ACL分配给端口。
4. （可选）使用屏幕查看配置。 *查看或删除MAC绑定表中的MAC ACL绑定*

要配置MAC ACL，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
将显示web管理界面菜单。
7. 单击 **安全管理 > ACL > 基本信息 > MAC ACL表**



MAC ACL界面显示当前交换机上配置的ACL数量和可配置的最大ACL数量。当前acl数量等于已配置的IPv4 acl和IPv6 acl的数量加上已配置的MAC acl的数量。

8. 在名称字段中，指定MAC ACL的名称。

名称字符串只能包含字母、数字、连字符、下划线或空格字符。名称必须以字母字符开头。

每个配置的ACL显示以下信息：

- **Rules.** 当前为MAC ACL配置的规则数。
- **Direction.** 受MAC ACL影响的数据包通信的方向，可以是入站或空白。

9. 单击 增加 按钮

MAC ACL将添加到交换机配置中。

10. 要更改MAC ACL的名称，请在名称字段中更新名称，然后单击应用按钮。

11. 要删除选定的MAC ACL， 请单击 删除 按钮

5.8.2. 配置MAC ACL规则

您可以为基于MAC的ACL定义规则。访问列表定义包括指定符合条件的流量是正常转发还是丢弃的规则。默认的拒绝所有规则是每个列表的最后一个规则。

要配置MAC ACL规则，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > ACL> Basic > MAC Rules**.



- 8. 要增加新的规则，直接单击“增加”按钮，进入规则新增编辑页面。
 - 9. 单击“ID”列表中的ID数字，直接进入指定规则的编辑页面。
 - 10. 要删除规则，请选中与该规则关联的复选框，然后单击“删除”按钮。
- 更新的配置参数将发送到交换机，配置更改将立即生效。

编辑MAC ACL规则

要配置MAC ACL规则，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。
交换机的默认IP地址为 192.168.10.12 。
此时将显示登录屏幕。
- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **安全管理 > ACL> Basic > ACL匹配规则编辑**

系统管理

L2交换管理

路由管理

QoS管理

安全管理

监测管理

维护

简体中文

保存

退出

系统访问管理

会话属性管理

DoS攻击配置

端口访问安全管理

端口流量控制

端口IP安全管理

ACL

ACL

基本管理信息

MAC ACL表

ACL匹配规则列表

ACL匹配规则编辑

ACL绑定端口配置

ACL绑定列表

高级管理信息

ACL匹配规则编辑 - MAC ACL Rule Configuration

ACL Name

abc

Rule ID

121

Action

☒ Permit
☐ Deny

Match Every

☐ False
☒ True

Destination MAC

Destination MAC Bit Mask

EtherType Key

EtherType User Value

(1536-65535, or 0x600-0xFFFF)

Source MAC

Source MAC Bit Mask

VLAN

CoS

Mirror Interface

Redirect Interface

Rate Limit Conform Data Rate

(1 - 4294967295)Kbps

Rate Limit Burst Size

(1 - 128)Kbytes

Assign QueueId

Logging

☒ 关闭
☐ 启用

Time Range

Time Range Status

仅当存在规则或进入新增规则时，此页面才可见编辑。

8. 使用ID输入1到2147483647之间的整数以标识规则。
9. 使用Action指定如果数据包符合规则的条件，将采取什么操作。
选择是允许还是拒绝。使用Assign Queue ID指定用于处理与此ACL规则匹配的所有数据包的硬件出口队列标识符。
10. 队列ID的有效范围为0到7。
11. 镜像接口指定特定出口接口，在该接口中，除了由设备正常转发外，还复制匹配的业务流。
如果已为ACL规则配置重定向接口，则无法设置此字段。此字段对于许可操作可见。
12. 使用重定向接口指定强制匹配流量流的特定出口接口，绕过设备通常执行的任何转发决策。
如果已为ACL规则配置镜像接口，则无法设置此字段。
13. 使用Match Every指定与每个第2层MAC数据包匹配的指示。
有效值如下所示：
 - **True.** 表示每个数据包都被视为与所选ACL规则匹配
 - **False.** 示并非每个数据包都必须匹配所选ACL规则。
14. 使用CoS指定要与以太网帧进行比较的802.1p用户优先级。
值的有效范围为0到7。

15. 使用目标MAC指定要与以太网帧进行比较的目标MAC地址。有效格式为xx:xx:xx:xx:xx:xx。可以使用目标MAC地址01:80:C2:xx:xx:xx指定BPDU关键字。
16. 使用目标MAC掩码指定目标MAC地址掩码，指定目标MAC中要与以太网帧进行比较的位。有效格式为xx:xx:xx:xx:xx:xx。BPDU关键字可以使用目标MAC掩码00:00:00:ff:ff:ff指定。
17. 使用EtherType键指定要与以太网帧进行比较的EtherType值。
有效值如下所示：
- Appletalk
 - ARP
 - IBM SNA
 - IPv4
 - IPv6
 - IPX
 - MPLS multicast
 - MPLS unicast
 - NetBIOS
 - Novell
 - PPPoE
 - Reverse ARP
 - User Value
18. 使用EtherType用户值指定用户定义的自定义EtherType值，当您选择用户值作为EtherType键时，将使用该值与以太网帧进行比较。
值的有效范围为0x0600到0xFFFF。
19. 使用源MAC指定要与以太网帧进行比较的源MAC地址。
有效格式为xx:xx:xx:xx:xx:xx。
20. 使用源MAC掩码指定源MAC地址掩码，指定源MAC中要与以太网帧进行比较的位。
有效格式为xx:xx:xx:xx:xx:xx。
21. 使用VLAN指定要与以太网帧进行比较的VLAN ID。
值的有效范围为1到4095。可以配置VLAN范围或VLAN。
22. 使用日志记录启用或禁用日志记录。
设置为启用时，将为此ACL规则启用日志记录（取决于设备中的资源可用性）。如果还启用了访问列表陷阱标志，则会生成周期性陷阱，指示在当前报告间隔期间命中此规则的次数。整个系统使用固定的5分钟报告间隔。如果当前间隔的ACL规则命中计数为零，则不会发出陷阱。仅拒绝操作支持此字段。
23. 使用“速率限制符合数据速率”指定MAC ACL规则的符合数据速率的值。
有效值为1到4294967295，单位为Kbps。
24. 使用速率限制突发大小指定MAC ACL规则的突发大小。
有效值为1到128 KB。
25. 使用时间范围输入与MAC ACL规则关联的时间范围的名称。

规则状态显示ACL规则是活动的还是非活动的。如果此字段为空，则不向规则分配计时器计划。

26. 要更改规则，请选中与规则关联的复选框并更改所需字段。

27. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

5.8.3. 配置MAC ACL绑定

将ACL绑定到接口时，定义的所有规则都将应用于所选接口。使用MAC绑定配置屏幕将MAC ACL列表分配给ACL优先级和接口。

要配置MAC ACL绑定，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

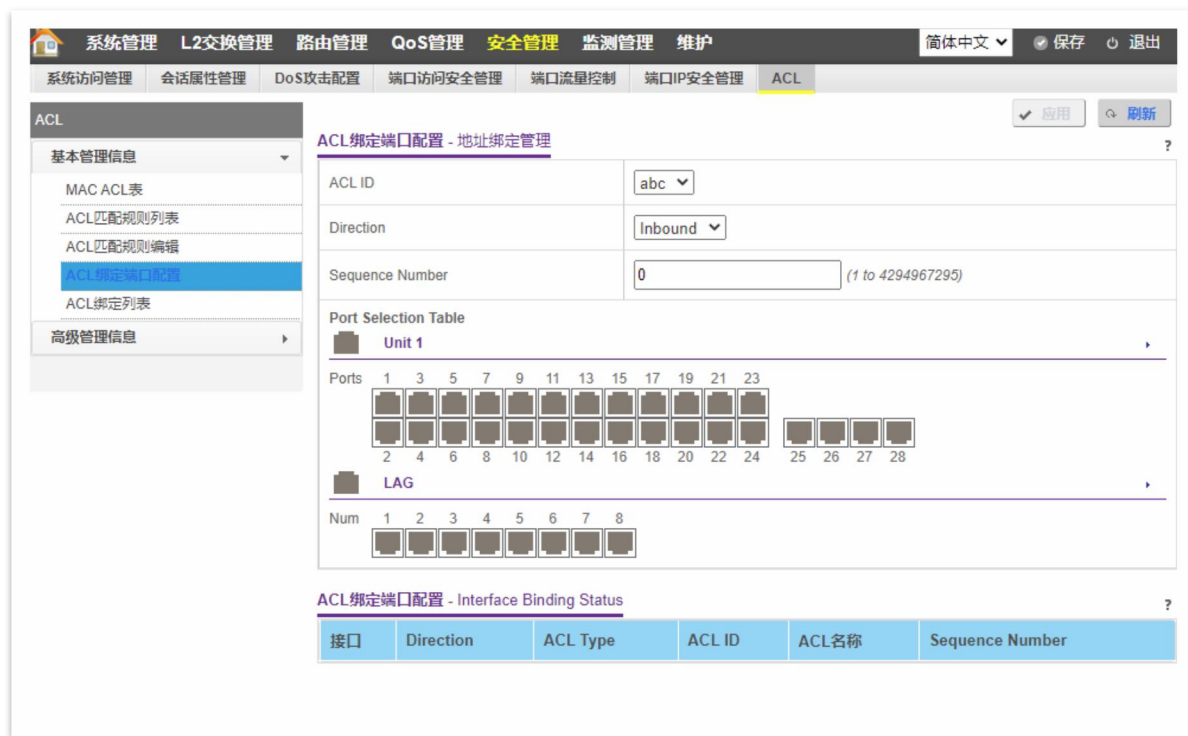
5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > ACL > 基本管理 > ACL绑定端口配置**



8. 在ACL ID列表中选择“MAC ACL”。

您可以选择一个并将其绑定到接口。

ACL的数据包过滤方向为Inbound，这意味着MAC ACL规则应用于进入端口的流量。

9. 指定可选序列号，以指示此访问列表相对于已分配给此接口和方向的其他访问列表的顺序。

较小的数字表示优先级较高。如果此接口和方向已使用序列号，则指定的访问列表将使用该序列号替换当前附加的访问列表。如果未指定序列号，则使用比当前用于此接口和方向的最高序列号大一的序列号。有效范围为1–4294967295。

10. 端口选择表提供了用于ACL绑定的所有可用有效接口的列表。列出了所有非路由物理接口VLAN接口和参与LAG的接口。

- 若要将所选ACL添加到端口或LAG中，请单击端口或LAG编号下方的复选框，使复选框中出现X。
- 若要从端口或LAG中删除所选ACL，请单击端口或LAG编号下方的复选框。其中X表示该ACL应用到该接口。

11. 单击应用按钮保存对运行配置的任何更改。

下表描述了界面绑定状态中显示的信息。

表85. 接口绑定状态

字段	描述
接口	分配的ACL的接口。

方向	显示ACL的选定数据包过滤方向。
ACL类型	分配给选定接口和方向的ACL类型。
ACL ID	ACL编号（对于IP ACL）或ACL名称（对于MAC ACL），标识分配给所选接口和方向的ACL。
序列号	序列号，表示指定ACL相对于分配给选定接口和方向的其他ACL的顺序。

5.8.4. 查看或删除MAC绑定表中的MAC ACL绑定

您可以在MAC绑定表中查看或删除MAC ACL绑定。

要查看或删除MAC ACL绑定，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
将显示web管理界面菜单。

7. 单击 **安全管理 > ACL > Basic > ACL绑定列表**



要删除MAC ACL到接口绑定，请选中接口旁边的复选框，然后单击删除按钮。

下表描述了 MAC 绑定表中显示的信息。

表86. MAC绑定表

字段	描述
接口	分配的ACL的接口。
Direction	为ACL选择的数据包过滤方向。
ACL Type	分配给选定接口和方向的ACL类型。
ACL ID	ACL名称，标识分配给选定接口和方向的ACL。
Sequence Number	序列号，表示指定ACL相对于分配给选定接口和方向的其他ACL的顺序。

5.8.5. 配置 IP ACL

IP或IPv6 ACL由一系列规则组成，这些规则依次对报文进行匹配。当报文满足规则的匹配条件时，将采取规则的动作(允许/禁止)，不检查附加的规则是否匹配。必须指定应用IP ACL的接口，以及是否应用于流入流量或流出流量。IP ACL的规则可以通过“IPv6 ACL规则配置”界面指定或创建。

要配置IP ACL，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > ACL > 高级管理 > IPv4 ACL表**



IP ACL屏幕显示ACL表的当前大小和表的最大大小ACL表。当前大小等于配置的IPv4和IPv6 ACL的数量加上配置的MAC ACL的数量。最大尺寸为100。

“当前的ACL条目数” 字段显示交换机上配置的所有ACL的当前数量。

“系统支持的最大ACL条目数” 显示交换机上可配置的最大IP ACL数，具体取决于硬件。

8. 在IP ACL字段中，指定ACL ID或IP ACL名称，这取决于IP ACL类型。

IP ACL ID是以下范围内的整数：

- **1–99:** 创建IP基本ACL，允许您允许或拒绝来自源IP地址的流量。
- **100–199:** 允许您允许或拒绝从源IP地址到目标IP地址的特定类型的第3层或第4层通信。这种类型的ACL比标准IP ACL提供更多的粒度和过滤功能。
- **IP ACL Name:** 创建长度最多包含31个字母数字字符的IPv4 ACL名称字符串。名称必须以字母字符开头。

每个配置的ACL显示以下信息：

- **Rules.** 当前为IP ACL配置的规则数。
- **Type.** 将ACL标识为基本IP ACL（ID为1到99）、扩展IP ACL（ID为100到199）或命名IP ACL。

9. 要删除IP ACL，请选中IP ACL ID字段旁边的复选框，然后单击删除按钮。

10. 单击 增加 按钮

IP ACL将添加到交换机配置中。

11. 单击 应用 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

5.8.6. 为IP ACL配置规则

您可以显示所创建的IP访问控制列表（ACL）的规则。此屏幕上显示的内容因规则配置过程中的当前步骤而异。

提示： 在ACL列表的末尾有一个隐式的deny all规则。这意味着，如果一个ACL应用于一个数据包，如果没有一个显式规则匹配，那么将应用最终的隐式拒绝所有规则，数据包将被丢弃。

要配置IP ACL的规则，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > ACL > 高级管理 > IPv4 规则列表**.



The screenshot displays the 'IPv4 Rule Configuration' window. On the left is a sidebar with a tree view containing '基本管理信息', '高级管理信息', 'IPv4 ACL表', 'IPv4 规则列表', 'IPv4 规则编辑' (selected), 'IPv4 扩展规则列表', 'IP Extend Rule Edit', 'IPv6 ACL表', 'IPv6 规则列表', 'IPv6 规则编辑', 'IP Binding Configuration', and 'ACL绑定列表'. The main area is titled 'IPv4 规则编辑 - Standard ACL Rule Configuration(1-99)'. It contains a form with the following fields: 'ACL ID' (dropdown with '1'), 'Rule ID' (dropdown), 'Action' (radio buttons for 'Permit' and 'Deny'), 'Egress Queue' (dropdown), 'Logging' (radio buttons for '关闭' and '启用'), 'Mirror Interface' (dropdown), 'Redirect Interface' (dropdown), 'Match Every' (radio buttons for '关闭' and '启用'), '源IP地址' (text input), 'Source Wildcard Mask' (text input), 'Rate Limit Conform Data Rate' (text input with a range '(1 - 4294967295)Kbps'), 'Rate Limit Burst Size' (text input with a range '(1 - 128)Kbytes'), and 'Time Range' (dropdown). At the top right of the form area are buttons for '应用' and '刷新'.

8. 要添加IP ACL规则，请选择ACL ID，填写以下列表中描述的字段，然后单击添加按钮。
(仅显示从1到99的ACL ID。)

- **Rule ID.** 输入1到1023之间的整数，用于标识规则。每个IP ACL最多可以包含128条规则。
- **Action.** 指定如果数据包符合规则的条件，将采取什么操作。选择是允许还是拒绝。
- **Logging.** 设置为启用时，将为此ACL规则启用日志记录（取决于设备中的资源可用性）。如果还启用了访问列表陷阱标志，则会生成周期性陷阱，指示在当前报告间隔期间命中此规则的次数。整个系统使用固定的5分钟报告间隔。如果当前间隔的ACL规则命中计数为零，则不会发出陷阱。此字段对于拒绝操作可见。
- **Assign Queue ID.** 用于处理与此IP ACL规则匹配的所有数据包的硬件出口队列标识符。队列ID的有效范围为0到6。选择“允许”作为操作时，此字段可见。
- **Match Every.** 选择真或假。True表示所有数据包必须与选定的IP ACL和规则匹配，并且是允许的或拒绝的。在这种情况下，由于所有数据包都与规则匹配，因此不提供配置其他匹配条件的选项。要为该规则配置特定的匹配条件，请删除该规则并重新创建它，或者将match Every重新配置为False以使其他匹配条件可见。
- **Mirror Interface.** 其中除了由设备正常转发外，还复制匹配的业务流。如果已为ACL规则配置重定向接口，则无法设置此字段。此字段对于许可操作可见。
- **Redirect Interface.** 其中强制匹配业务流，绕过设备通常执行的任何转发决策。如果已为ACL规则配置镜像接口，则无法设置此字段。此字段为许可操作启用
- **Source IP Address.** 输入IP地址(点分十进制格式)，将与报文的源IP地址进行比较，作为所选IP ACL规则的匹配条件。
- **Source IP Mask.** 指定与“源IP地址”值一起使用的点分十进制格式的IP掩码。
- **Rate Limit Conform Data Rate.** 速率限制一致数据速率的值指定IP ACL规则的一致数

据速率。有效值为1到4294967295，单位为Kbps。

- **Rate Limit Burst Size.** 速率限制突发大小的值指定IP ACL规则的突发大小。有效值为1到128 KB。
- **Time Range.** 与IP ACL规则关联的时间范围的名称。
- **Rule Status.** 显示ACL规则是活动的还是非活动的。空白表示没有为规则分配计时器计划。

9. 要删除IP ACL规则，请选中规则复选框，然后单击删除按钮。

10. 要更新IP ACL规则，请选中规则复选框，更新所需字段，然后单击应用按钮。

无法修改现有IP规则的规则ID。

11. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

12. 要修改现有的IP扩展ACL规则，请单击规则ID。

该编号是指向扩展ACL规则配置屏幕的超链接。

5.8.7. 为扩展IP ACL配置规则

您可以查看所创建的IP访问控制列表的规则。此屏幕上显示的内容因规则配置过程中的当前步骤而异。

提示： 在ACL列表的末尾有一个隐式的deny all规则。这意味着，如果一个ACL应用于一个数据包，如果没有一个显式规则匹配，那么将应用最终的隐式拒绝所有规则，数据包将被丢弃。

要为扩展IP ACL配置规则，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

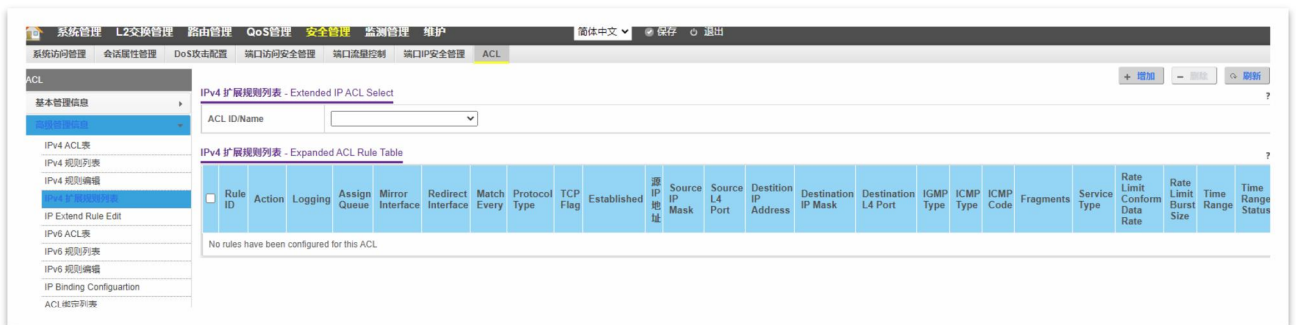
5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **安全管理 > ACL > 高级管理 > IPv4 扩展规则列表**



系统管理 L2交换管理 路由管理 QoS管理 安全管理 监测管理 维护 简体中文 保存 退出

系统访问管理 会话属性管理 DoS攻击配置 端口访问安全管理 端口流量控制 端口IP安全管理 ACL

ACL

基本管理信息

高级管理信息

IPv4 ACL表

IPv4 规则列表

IPv4 规则编辑

IPv4 扩展规则列表

IP Extend Rule Edit

IPv6 ACL表

IPv6 规则列表

IPv6 规则编辑

IP Binding Configuration

ACL绑定列表

IP Extend Rule Edit - Extended ACL Rule Configuration(100-199)

ACL ID/Name 100

Rule ID (1 - 2147483647)

Action ☒ Permit ☐ Deny

Egress Queue

Logging ☒ 关闭 ☐ 启用

Mirror Interface

Redirect Interface

Match Every ☒ 关闭 ☐ 启用

Protocol Type Other (0 to 255)

TCP Flag URG Ignore ACK Ignore PSH Ignore RST Ignore SYN Ignore FIN Ignore

Established

Src IP Address

Src IP Wildcard Mask

Src L4 Port ☒ Port None domain (0 to 65535) ☐ Range Start Port domain End Port domain (0 to 65535)

Dst IP Address

Dst IP Wildcard Mask

Dst L4 Port ☒ Port None domain (0 to 65535) ☐ Range Start Port domain End Port domain (0 to 65535)

IGMP Type (0 to 255)

ICMP ☐ Type (0 to 255) Code (0 to 65535) ☐ Message echo

Fragments ☐ 关闭 ☐ 启用

Service Type ☐ IP DSCP Other (0 to 63) ☐ IP Precedence (0 to 7)

8. **ACL ID/Name** - 选择要为其创建或更新规则的IP ACL。
9. **Rule ID** 输入1到 2147483647 范围内的整数，用于标识规则。
一个IP ACL最多可以包含128条规则。
10. **Action** - 指定如果数据包符合规则的条件，则要采取的操作。

选择是允许还是拒绝。

11. Logging - 将日志记录设置为启用。

这将启用此ACL规则的日志记录(取决于设备中的资源可用性)。如果访问列表trap标志也被启用,这将导致产生周期性的trap,指示在当前报告间隔期间命中该规则的次数。整个系统使用固定的5分钟报告间隔。在当前时间间隔内,如果ACL规则命中次数为零,则不会发出告警。该字段对于Deny操作是可见的。

12. Assign Queue ID -, 在分配队列ID中,指定用于处理与此IP ACL规则匹配的所有数据包的硬件出口队列标识符。

队列ID的有效范围为0到6。

13. Mirror Interface 指定特定出口接口,在该接口中,除了由设备正常转发外,还复制了匹配的业务流。

如果已为ACL规则配置重定向接口,则无法设置此字段。此字段对于许可操作可见。

14. Redirect Interface - 使用重定向接口字段指定强制匹配业务流的特定出口接口,绕过设备通常执行的任何转发决策。

如果ACL规则已经配置了镜像接口,则不能设置该字段。此字段为Permit (允许动作)时启用。

15. Match Every - 选择True或False。

True表示所有数据包必须与选定的IP ACL和规则匹配,并且是允许的或拒绝的。在这种情况下,由于所有数据包都与规则匹配,因此不提供配置其他匹配条件的选项。要为该规则配置特定的匹配条件,请删除该规则并重新创建它,或者将match Every重新配置为False以使其他匹配条件可见。

16. Protocol Type - 使用协议类型字段指定数据包的IP协议是所选IP ACL规则的匹配条件。

可能的值是ICMP、IGMP、IP、TCP、UDP、EIGRP、GRE、IPINIP、OSPF和PIM。

17. TCP Flag - 指定数据包的TCP标志是所选IP ACL规则的匹配条件。

TCP标志值为URG、ACK、PSH、RST、SYN和FIN。每个TCP标志都可以单独设置。可能的值如下所示:

- **Ignore.** 无论是否设置了此数据包中的TCP标志,数据包都与此ACL规则匹配。
- **Set (+).** 如果设置了此数据包中的TCP标志,则数据包与此ACL规则匹配。
- **Clear (-).** 如果未设置此数据包中的TCP标志,则数据包与此ACL规则匹配。

18. Established - 当指定“已建立”时,如果在TCP标头中设置了RST或ACK指定位,则会发生匹配。这些字段仅在选择TCP协议时启用。

19. Src - 在Src字段中,使用点十进制表示法输入要与数据包的源IP地址进行比较的源IP地址,作为所选IP ACL规则的匹配条件:

a. 选择IP地址选项并输入一个带有相关通配符掩码的IP地址以应用此条件。如果此字段留空,则表示任何。

b. 选择主机选项时,通配符掩码配置为0.0.0.0。如果此字段留空,则表示任何。

通配符掩码确定使用哪些位以及忽略哪些位。通配符掩码为0.0.0.0表示所有位都不重要。通配符255.255.255.255表示所有位都很重要。

20. Source L4 Port Action - 使用源L4端口为当前扩展ACL规则中的L4端口号指定相关匹配条件的操作:

- **Equal.** 只有当四层源端口号与指定的端口号相等时, 才能匹配IP ACL规则。
- **Less Than.** 如果第4层源端口号小于指定的端口号, 则IP ACL规则匹配。
- **Greater Than.** 如果第4层源端口号大于指定的端口号, 则IP ACL规则匹配。
- **Not Equal.** IP ACL规则仅在第4层源端口号不等于指定的端口号时匹配

21. Src L4 Port 和 Src L4 Range - 只有当协议设置为TCP或UDP时, Src L4范围选项才可用。选择端口选项时, 请从列表中选择端口键或自己输入端口号。

- 源IP TCP端口名为bgp、域、echo、ftp、ftpdata、http、smtp、snmp、Telnet、www、pop2、pop3。
- 源IP UDP端口名为域、echo、ntp、rip、snmp、tftp、time、who。

这些值中的每一个都转换为其等效端口号, 该端口号用作端口范围的开始和结束。

只有在端口键列表中选择“Other”时, 才能输入自己的端口号。如果将另一个字段留空, 则表示有。

22. Range - 选择范围选项时, IP ACL规则仅在第4层端口号在指定的端口范围内时匹配。

起始端口和结束端口参数标识属于端口范围的第一个和最后一个端口。它们的值可以在0到65535之间。

只有在端口键列表中选择“Other”时, 才可以输入自己的端口号。起始端口、结束端口以及两者之间的所有端口都是第4层端口范围的一部分。如果这些字段留空, 则表示有。

通配符掩码确定使用哪些位以及忽略哪些位。通配符掩码为0.0.0.0表示所有位都不重要。通配符255.255.255.255表示所有位都很重要。

23. Dst - 在Dst字段中, 使用点十进制表示法和相关的通配符掩码指定目标IP地址。

这将与数据包的目标IP地址进行比较, 作为所选扩展IP ACL规则的匹配条件。

24. IP Address - 选择IP地址选项并输入一个带有相关通配符掩码的IP地址以应用此条件。

如果这些字段为空, 则表示任何字段。

25. Host - 选择主机选项时, 通配符掩码配置为0.0.0.0。

如果此字段留空, 则表示任何。

26. Destination IP Mask - 在目标IP掩码字段中, 以点十进制表示法指定要与目标IP地址值一起使用的IP掩码。

27. Dst L4 Port 和 Dst L4 Range - 指定所选扩展IP ACL规则的第4层目标端口匹配条件。

仅当协议设置为TCP或UDP时, 这些选项才可用。

只有在端口键列表中选择“Other”时, 才能输入自己的端口号。如果Other字段为空, 则表示any。

- 目标IP TCP可能的端口名为bgp、域、echo、ftp、ftp数据、http、smtp、Telnet、www、pop2、pop3。
- 目标IP UDP可能的端口名为域、echo、ntp、rip、snmp、tftp、时间、who。

这些值中的每一个都转换为其等效端口号, 该端口号用作端口范围的开始和结束。这是一

个可选配置。

28. Destination L4 Port Action - 使用目标L4端口操作作为当前扩展ACL规则中的L4端口号指定相关匹配条件:

- **Equal.** IP ACL规则仅在第4层源端口号等于指定的端口号时匹配。
- **Less Than.** 如果第4层源端口号小于指定的端口号, 则IP ACL规则匹配。
- **Greater Than.** 如果第4层源端口号大于指定的端口号, 则IP ACL规则匹配。
- **Not Equal.** IP ACL规则仅在第4层源端口号不等于指定的端口号时匹配。

29. Range - 选择范围选项时, IP ACL规则仅在第4层端口号在指定的端口范围内时匹配。

起始端口和结束端口参数标识属于端口范围的第一个和最后一个端口。它们的值可以在0到65535之间。

只有在端口键列表中选择“Other”时, 才可以输入自己的端口号。目标L4起始端口、目标L4结束端口以及两者之间的所有端口都是第4层端口范围的一部分。如果这些字段留空, 则表示有。

30. IGMP Type - 指定IGMP类型时, IP ACL规则与指定的IGMP消息类型匹配。

可能的值在0到255之间。如果此字段为空, 则表示任意值。

31. ICMP Type 和 ICMP Code - 仅当协议为ICMP时, 才会启用ICMP类型和ICMP代码字段。使用ICMP类型和ICMP代码字段指定ICMP数据包的匹配条件:

- 选择“ICMP类型”时, IP ACL规则匹配指定的ICMP报文类型。可能的类型数字的范围是0到255。
- 配置“ICMP报文码”选项时, IP ACL规则匹配指定的ICMP报文码。Code的可能值可以在0到255之间。
- 如果这些字段为空, 则表示any。
- 选择Message选项时, 需要选择ICMP报文的类型, 以匹配所选的IP ACL规则。指定Message意味着同时指定ICMP类型和ICMP代码。ICMP报文被解码为相应的ICMP类型和该ICMP类型内的ICMP代码。IPv4 ICMP消息类型有: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, time-exceeded, ttl-exceeded, and unreachable。

32. Service Type - 为扩展IP ACL规则选择服务类型匹配条件。

IP DSCP、IP precedence、IP TOS是对IP报头中相同服务类型字段指定匹配条件的替代方式;然而, 每一种都使用不同的用户符号。在进行选择之后, 可以指定适当的值。

- **IP DSCP.** 指定IP区分服务代码点(DSCP)字段。DSCP定义为IP报头中服务类型八位字节的高阶6位。这是一个可选配置。输入0到63之间的整数。要选择IP DSC, 请从列表选择一个DSCP关键字。如果要通过指定数值来选择某个值, 请选择“Other”, 并显示一个字段, 您可以在其中输入DSCP的数值。
- **IP Precedence.** 数据包中的IP优先级字段定义为IP报头中服务类型八位字节的高三位。这是一个可选配置。输入0到7之间的整数。

- **IP TOS.** 数据包中的IP TOS字段定义为IP报头中服务类型八位字节的所有8位。TOS位值是从00到09、从aa到ff的十六进制数。ToS掩码值是从00到FF的十六进制数。ToS掩码表示ToS Bits值中的位位置，用于与数据包中的IP ToS字段进行比较。例如，要检查设置了位7和5且位1清除的IP ToS值，其中位7最为有效，请使用ToS位值0xA0和ToS掩码0xFF。这是一个可选配置。

33. Rate Limit Conform Data Rate - 指定IP ACL规则的符合数据速率。

有效值为1到4294967295，单位为Kbps。

34. Rate Limit Burst Size - 指定IP ACL规则的突发大小。有效值为1到128 KB。

35. Time Range - 与IP扩展ACL规则关联的时间范围的名称。

Rule Status 字段显示ACL规则是活动的还是非活动的。空白表示没有为规则分配计时器计划。

36. 要修改现有的IP扩展ACL规则，请单击规则ID。

该编号是指向扩展ACL规则配置100-199屏幕的超链接。单击IP扩展规则屏幕上的添加按钮。

37. 要删除IP ACL规则，请选中该规则的复选框，然后单击删除按钮。

5.8.8. 配置 IPv6 ACL

IP或IPv6 ACL由一系列规则组成，这些规则依次对报文进行匹配。当报文满足规则的匹配条件时，将采取规则的动作(允许/禁止)，不检查附加的规则是否匹配。在该界面中，需要指定应用IP ACL的接口，以及是否应用于入方向或出方向的流量。

要配置IPv6 ACL，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。
交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
将显示web管理界面菜单。
7. 单击 **安全管理 > ACL > 高级管理 > IPv6 ACL表**



8. 指定 **IPv6 ACL**.
这是IPv6 ACL名称字符串，最多只包含31个字母数字字符。名称必须以字母字符开头。
9. 单击 **增加** 按钮
IPv6 ACL将添加到交换机配置中。
10. 要从交换机配置中删除当前选定的IPv6 ACL，请单击**删除**按钮。
11. 单击 **应用** 按键
更新的配置参数将发送到交换机，配置更改将立即生效。
下表描述了屏幕上显示的不可配置信息。

表87. IPv6 ACL

字段	描述
当前的ACL条目数	交换机上配置的IP ACL的当前数目。
系统支持的最大ACL条目数	可在交换机上配置的最大IP ACL数，具体取决于硬件。
Rules	与IP ACL关联的规则数。
Type	类型为IPv6 ACL。

5.8.9. 配置IPv6规则

使用这些屏幕显示使用IPv6访问控制列表配置屏幕创建的IPv6访问控制列表的规则。默认情况下，任何IPv6 ACL规则都没有有效的特定值。

配置ACL IPv6规则：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。

- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。

- 7. 单击 **安全管理 > ACL > 高级管理 > IPv6 规则列表**



The screenshot displays the 'IPv6 Rule Configuration' page. On the left is a sidebar with a tree view under 'ACL' containing items like 'Basic Management Information', 'Advanced Management Information', 'IPv4 ACL Table', 'IPv4 Rule List', 'IPv4 Rule Edit', 'IPv4 Extended Rule List', 'IP Extend Rule Edit', 'IPv6 ACL Table', 'IPv6 Rule List', 'IPv6 Rule Edit' (highlighted), 'IP Binding Configuration', and 'ACL Binding List'. The main area contains the configuration form for 'IPv6 Rule Edit - IPv6 ACL Rule Configuration'. The form includes fields for:

- ACL Name: IPv6-0
- Rule ID: (empty)
- Action: ☒ Permit, ☐ Deny
- Egress Queue: (empty)
- Logging: ☒ Disabled, ☐ Enabled
- Mirror Interface: (empty)
- Redirect Interface: (empty)
- Match Every: ☒ Disabled, ☐ Enabled
- Protocol Type: Other (0 to 255)
- TCP Flag: URG, ACK, PSH, RST, SYN, FIN (all set to Ignore)
- Established: (empty)
- Src IPv6 Address: (empty)
- Prefix Len: (empty)
- Src L4 Port: Port (0 to 65535)
- Dst IPv6 Address: (empty)
- Prefix Len: (empty)
- Dst L4 Port: Port (0 to 65535)
- ICMPv6: Type (0 to 255), Code (0 to 65535), Message: echo-reply
- Fragments: ☐ Disabled, ☐ Enabled
- Routing: ☐ Disabled, ☐ Enabled
- Flow Label: (0 to 1048575)
- IPv6 DSCP Service: Other (0 to 63)

 Buttons for 'Apply' and 'Refresh' are at the top right.

8. **Rule ID** - 使用规则ID输入1到2147483647 范围内的整数，用于标识规则。
一个IP ACL最多可以包含有128条规则。
9. **Action** - 指定如果数据包符合规则的条件，将采取什么操作。选择是允许还是拒绝。
10. **Logging** - 使用日志记录启用此ACL规则的日志记录（取决于设备中的资源可用性）。

如果访问列表trap标志也被启用，这将导致产生周期性的trap，指示在当前报告间隔期间命中该规则的次数。整个系统使用固定的5分钟报告间隔。在当前时间间隔内，如果ACL规则命中次数为零，则不会发出告警。该字段对于Deny操作是可见的。

11. **Assign Queue ID** - 使用Assign Queue ID指定用于处理与此IPv6 ACL规则匹配的所有数据包的硬件出口队列标识符。
队列id的有效范围是0到7。此字段对于Permit操作是可见的。

12. Mirror Interface - 使用镜像接口指定特定出口接口，在该接口中，除了由设备正常转发外，还复制匹配的业务流。

如果已为ACL规则配置重定向接口，则无法设置此字段。此字段对于许可操作可见。

13. Redirect Interface - 指定强制匹配流量流的出接口，从而绕过设备正常情况下的转发决策。

如果已为ACL规则配置镜像接口，则无法设置此字段。此字段对于许可操作可见。

14. Match Every - 在匹配每个字段中，选择True或False。

True表示所有报文必须匹配所选的IPv6 ACL和规则，允许或拒绝。在这种情况下，由于所有报文都匹配该规则，因此不提供配置其他匹配条件的选项。若要为该规则配置特定的匹配条件，请删除该规则并重新创建它，或将match Every重新配置为False，以使其他匹配条件可见。

15. Protocol Type - 有两种方法可以配置IPv6协议类型：

- 选择协议关键字**other**后，指定一个介于1到255之间的整数。这个数字代表IP协议。
- 从现有的Internet协议（IPv6）、传输控制协议（TCP）、用户数据报协议（UDP）和Internet控制消息协议（ICMPv6）列表中选择协议的名称。

16. TCP Flag - 使用TCP标志指定数据包的TCP标志是选定IPv6 ACL规则的匹配条件。

TCP标志值为URG、ACK、PSH、RST、SYN、FIN。每个TCP标志都可以单独设置。可能的值如下所示：

- **Ignore**. 无论是否设置了此数据包中的TCP标志，数据包都与此ACL规则匹配。
- **Set (+)**. 如果设置了此数据包中的TCP标志，则数据包与此ACL规则匹配。
- **Clear (-)**. 如果未设置此数据包中的TCP标志，则数据包与此ACL规则匹配。
- 当指定Established时，如果TCP报头中设置了RST或ACK指定位，就会匹配。
- 仅当选择TCP协议时，才会启用以下字段：
 - **Protocol**. 配置IPv6协议有两种方法。
选择协议关键字**other**后，指定一个介于1到255之间的整数。这个数字代表IP协议。
从现有的Internet协议（IPv6）、传输控制协议（TCP）、用户数据报协议（UDP）和Internet控制消息协议（ICMPv6）列表中选择协议名称。
 - **Src**. 指定与所选IPv6 ACL规则匹配的源IPv6地址。
选中“IPv6地址”单选按钮时，需要输入带前缀长度的IPv6地址，以匹配IPv6 ACL规则。如果这些字段为空，则表示任何字段。
选中“主机”单选按钮时，输入主机源IPv6地址与指定的IPv6地址匹配。如果该字段为空，则表示任意。

该源IPv6地址参数必须采用RFC 2373中记录的格式，其中地址以冒号之间的16位值的十六进制形式指定。

17. Src L4 Port - 仅对TCP或UDP协议启用选项：

- 源L4 TCP端口名为bgp、domain、echo、ftp、ftpdata、http、smtp、Telnet、www、pop2、pop3。

- 源L4 UDP端口名为domain、echo、ntp、rip、snmp、tftp、time、who。

选择端口选项后，从列表中选择端口键或输入端口号。只有在端口密钥列表中选择了“Other”时，才能输入自己的端口号。如果此字段留空，则表示任何。

18. Src L4 Port Action - 指定当前扩展规则中第4层端口号的相关匹配条件：

- **Equal.** IPv6 ACL规则仅在第4层源端口号等于指定的端口号时匹配。
- **Less Than.** 如果第4层源端口号小于指定的端口号，则IPv6 ACL规则匹配。
- **Greater Than.** 如果第4层源端口号大于指定的端口号，则IPv6 ACL规则匹配。
- **Not Equal.** IPv6 ACL规则仅在第4层源端口号不等于指定的端口号时匹配。

19. Dst L4 Port - 选项仅对TCP或UDP协议启用：

- 目的L4 TCP端口名称为bgp、domain、echo、ftp、ftpdata、http、smtp、Telnet、www、pop2、pop3。
- 目的L4 UDP端口名称为domain、echo、ntp、rip、snmp、tftp、time、who。

当选择端口选项时，请从列表中选择端口键或输入端口号。只有在端口键列表中选择“Other”时，才能输入自己的端口号。如果该字段为空，则表示任意。

20. Destination L4 Port Action - 指定当前扩展ACL规则中第4层端口号的相关匹配条件：

- **Equal.** IPv6 ACL规则仅在第4层目的端口号等于指定的端口号时匹配。
- **Less Than.** 如果第4层目的端口号小于指定的端口号，则IPv6 ACL规则匹配。
- **Greater Than.** 如果第4层目的端口号大于指定的端口号，则IPv6 ACL规则匹配。
- **Not Equal.** IPv6 ACL规则仅在第4层目的端口号不等于指定的端口号时匹配。

21. Fragments - 匹配非初始分片(分片位断言)的数据包的规则。

该选项对匹配L4信息(如TCP端口号)的规则无效，因为该信息是在初始包中携带的。

22. Routing - 匹配包含路由扩展头的数据包的规则。

23. ICMPv6 Type - 指定ICMP数据包的条件。

选中“Type”单选按钮时，表示IPv6 ACL规则匹配指定的ICMPv6消息类型。可能的类型数字的范围是0到255。当指定ICMPv6消息码时，IP ACL规则匹配指定的ICMPv6消息码。取值范围为0 ~ 255。如果该字段为空，则表示任意。

24. 选中“Message”单选按钮时，需要选择与所选IPv6 ACL规则匹配的ICMPv6消息类型。

指定Message表示同时指定ICMPv6类型和ICMPv6代码。ICMPv6消息被解码成相应的ICMPv6类型和该ICMPv6类型内的ICMPv6代码。IPv6 ICMPv6消息类型包括destination-unreachable、echo-reply、echo-request、header、hop-limit、mld-query、mld-reduction、mld-report、nd-na、nd-ns、next-header、no-admin、no-route、packet-too-big、port-unreachable、router-solicitation、router-advertisement、router-renumbered、time-exceeded和unreachable。

提示： 只有当协议为ICMPv6时，才会启用以下字段。

25. Flow Label - 流标签是IPv6数据包特有的20位数字，由终端站用于表示路由器中的服务处理质量。

可以在0到1048575范围内指定流量标签。

26. IPv6 DSCP Service - 使用IPv6 DSCP服务指定IP区分服务代码点（DSCP）字段。

DSCP定义为IPv6报头中服务类型八位字节的高阶六位。这是一个可选配置。输入0到63之间的整数。要选择IPv6 DSCP，请选择一个DSCP关键字。如果要通过指定数值来选择某个值，请选择“其他”，此时会出现一个字段，您可以在其中输入DSCP的数值。

27. Rate Limit Conform Data Rate - 符合数据速率的速率限制. 指定IPv6 ACL规则的一致性数据速率。

有效值为1到4294967295，单位为Kbps。

28. Rate Limit Burst Size - 速率限制突发大小. 指定IPv6 ACL规则的突发大小。

有效值为1到128 KB。

29. Time Range - 时间范围. 与IPv6 ACL规则关联的时间范围的名称。

30. Rule Status - 规则地位. 显示ACL规则是活动的还是非活动的。

空白表示没有为规则分配计时器计划。

31. 要修改IP扩展ACL规则，请单击规则ID。

该号码是指向扩展IPv6 ACL规则配置（100-199）屏幕的超链接。单击IP扩展规则屏幕上的添加按钮。

32. 对于标准ACL规则配置（1-99），请单击IPv6规则屏幕上的添加按钮。

33. 要删除规则，请选中其复选框并单击“删除”按钮。

5.8.10. 配置IP ACL接口绑定

将ACL绑定到接口时，定义的所有规则都将应用于所选接口。您可以将ACL列表分配给ACL优先级和接口。

要配置IP ACL接口绑定，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

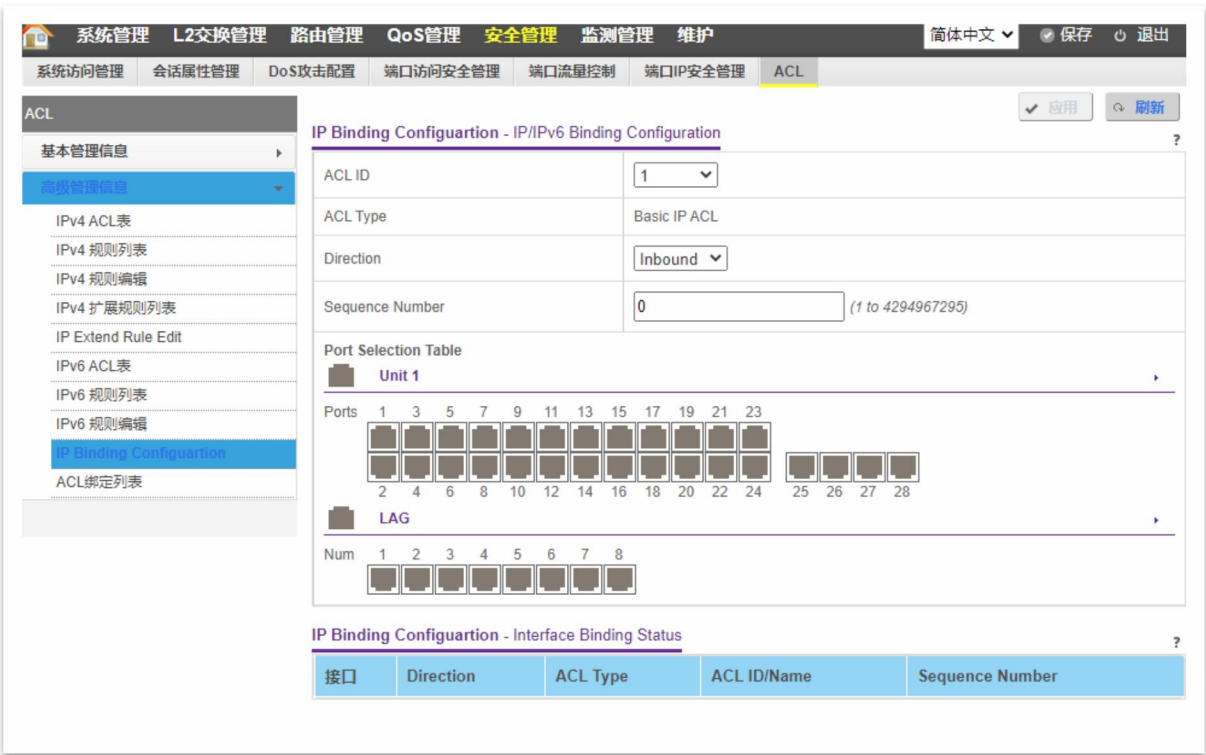
交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。
- 将显示web管理界面菜单。
7. 单击 **安全管理 > ACL > 高级管理 > IP Binding Configuration**



8. 在ACL ID菜单中，选择一个IP ACL。

提示： 当系统没有资源绑定新ACL时，将ACL绑定到接口失败。IPv4 ACL和IPv6 ACL不能同时绑定到接口。

9. 选择ACL的数据包过滤方向。
- 有效方向为入站或出站。**ACL**的数据包过滤方向为**Inbound**，这意味着**IP ACL**规则应用于进入端口的流量。
10. 指定可选序列号，以指示此访问列表相对于已分配给此接口和方向的其他访问列表的顺序。
- 较小的数字表示优先级较高。如果此接口和方向已使用序列号，则指定的访问列表将使用该序列号替换当前附加的访问列表。如果未指定序列号（表示该值为0），则将使用比当前用于此接口和方向的最高序列号大一的序列号。有效范围为**1–4294967295**。
11. 端口选择表列出了**ACL**映射的所有可用有效接口。
- 列出了所有非路由物理接口以及参与**LAG**的接口。单击适当的设备名称以显示可用端口或LAG：
- 要将所选**ACL**添加到端口或LAG，请单击端口或LAG编号正下方的框，以便框中显示**X**。

- 若要从端口或LAG中删除所选ACL，请单击端口或LAG编号下方的复选框。其中X表示该ACL应用到该接口。

12. 单击应用按钮保存对运行配置的任何更改。

下表描述了屏幕上显示的不可配置信息。

表88. IP绑定配置

字段	描述
接口	显示选定的接口。
Direction	显示ACL的选定数据包过滤方向。
ACL Type	分配给所选接口和方向的ACL类型。
ACL ID/Name	标识分配给选定接口和方向的ACL的ACL编号（对于IP ACL）或ACL名称（对于命名的IP ACL和IPv6 ACL）。
Sequence Number	序列号，表示指定ACL相对于分配给选定接口和方向的其他ACL的顺序。

5.8.11. 在IP ACL绑定表中查看或删除IP ACL绑定

要查看或删除IP ACL绑定，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
将显示web管理界面菜单。
7. 单击 **安全管理 > ACL > 高级管理 > ACL绑定列表**



8. 要删除IP ACL到接口绑定，请选中接口旁边的复选框，然后单击删除按钮。

下表描述了IP ACL绑定表中显示的信息。

表89. IP ACL绑定表

字段	描述
接口	显示选定的接口。
Direction	显示ACL的选定数据包过滤方向。
ACL Type	分配给所选接口和方向的ACL类型。
ACL ID/Name	标识分配给选定接口和方向的ACL的ACL号（对于IP ACL）或ACL名称（对于命名的IP ACL和IPv6 ACL）。
Sequence Number	序列号，表示指定ACL相对于分配给选定接口和方向的其他ACL的顺序。

6. 系统监控

本章涵盖以下主题：

- 查看端口统计信息
- 管理日志
- 配置多端口镜像
- 配置 RSPAN VLAN
- 配置 sFlow

6.1.查看端口统计信息

您可以查看交换机上每端口流量统计信息的摘要。

要查看端口统计信息，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **监测管理 > Ports > 端口统计信息**

The screenshot shows a web management interface with a top navigation bar containing '系统管理', 'L2交换管理', '路由管理', 'QoS管理', '安全管理', '监测管理', and '维护'. Below this is a sub-navigation bar with 'Ports', '镜像管理', 'sFlow管理', and 'Log管理'. The main content area is titled '端口统计信息 - 状态' and contains a table with 12 columns: '端口', '接收无错误帧', '接收错误帧', '接收广播帧', '接收端丢弃帧', '发送无错误帧', '发送端丢弃帧', '发送输出错误统计', '碰撞帧', '端口Link down事件', '链路抖动计数', and '最近清除计数时间'. The table lists ports from 0/1 to 0/15, all showing zero counts for most metrics and a '02 day 5 hr 41 min 52 sec' time for the last cleared counter.

端口	接收无错误帧	接收错误帧	接收广播帧	接收端丢弃帧	发送无错误帧	发送端丢弃帧	发送输出错误统计	碰撞帧	端口Link down事件	链路抖动计数	最近清除计数时间
0/1	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/2	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/3	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/4	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/5	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/6	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/7	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/8	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/9	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/10	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/11	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/12	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/13	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/14	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec
0/15	0	0	0	0	0	0	0	0	0	0	02 day 5 hr 41 min 52 sec

使用屏幕上部的按钮执行以下操作：

- 要清除交换机上所有端口的所有计数器，请选中顶部行标题中的复选框，然后单击 **清除** 按钮。
- 要清除特定端口的计数器，请选中该端口的复选框，然后单击 **清除** 按钮。
- 要使用交换机上的最新信息刷新屏幕，请单击 **刷新** 按钮。

下表介绍了屏幕上显示的每端口统计信息。

表90. 端口计数统计

字段	描述
----	----

接口	此对象表示适配器上与此端口关联的接口表项的接口。
接收无错误帧	接收到的没有错误的数据包总数。
接收错误帧	包含错误的入站数据包的数量，这些错误会阻止它们传递到更高层协议。
接收广播帧	接收到的定向到广播地址的正确数据包总数。这不包括组播数据包。
发送无错误帧	此端口传输到其段的帧数。
发送帧出错统计	由于错误而无法传输的出站数据包数。
碰撞帧	此以太网段上冲突总数的最佳估计。
端口Link down事件	物理端口上的链路断开事件总数。
链路摆动计数	在解抖动时间内，从链路断开到链路接通事件（使一个链路抖动）的总发生次数。
最近清除计数时间	自上次清除此端口的统计信息以来经过的时间（以天、小时、分钟和秒为单位）。

6.1.1. 查看详细端口统计信息

您可以查看各种每个端口的流量统计信息。

要查看详细端口统计信息，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **监测管理 > Ports > 端口详细统计信息**

下图显示了Port Detailed Statistics（端口详细统计信息）屏幕上的部分（但不是全部）字段。

端口详细统计信息 - 端口详细统计信息?

端口	0/1
MST ID	CST
ifIndex	1
端口类别	Normal
端口的汇聚模式	Disable
Port Role	
STP模式	Enabled
STP State	
使能模式	Enabled
LACP模式	Enabled
端口PHY工作模式	Auto-negotiate
端口PHY连接状态	
连接状态	Detach
连接状态Trap	Enable
接收和发送长度在64字节内的帧数	0
接收和发送长度在65-127字节范围内的帧数	0
接收和发送长度在128-255字节范围内的帧数	0
接收和发送长度在256-511字节范围内的帧数	0
接收和发送长度在512-1023字节范围内的帧数	0
接收和发送长度在1024-1518字节范围内的帧数	0
接收和发送长度在1519-1522字节范围内的帧数	
接收和发送长度在1523-2047字节范围内的帧数	0
接收和发送长度在2048-4095字节范围内的帧数	0
接收和发送长度在4096-9216字节范围内的帧数	0
接收的总字节数	0

使用屏幕上部的按钮执行以下操作：

- 要清除所有计数器，请单击 **清除** 按钮。这会将此端口的所有统计信息重置为默认值。
- 要使用交换机上的最新信息刷新屏幕，请单击 **刷新** 按钮。

下表描述了屏幕上显示的详细端口信息。要查看有关不同端口的信息，请从界面菜单的端口列表中选择需要显示的端口号。

表91. 端口详细统计

字段	描述
MST ID	显示与接口关联的MST实例。
ifIndex	此对象表示适配器上与此端口关联的接口表项的ifIndex。
端口类别	对于正常端口，此字段是正常的。否则，可能的值如下所示： • Mirrored. 此端口作为镜像端口参与端口镜像。有关更多信息，请查看端口镜像屏幕。 • Probe. 此端口作为探测端口参与端口镜像。有关更多信息，请查看端口镜像屏幕。 • Trunk Member. 该端口是链路聚合中继的成员。查看汇聚端口屏幕了解更多信息。

端口的汇聚模式	如果端口是汇聚端口的成员，则会显示端口通道的接口ID和名称。否则，将显示 Disable 。
Port Role	为每个生成树为每个启用的MST网桥端口分配一个端口role。端口角色是以下值之一：根、指定、备用、备份、主或禁用。
STP Mode	与端口或端口通道关联的生成树协议管理模式。可能的值如下所示： • Enable. 已为此端口启用生成树。 • Disable. 已为此端口禁用生成树。
STP State	端口的当前生成树状态。此状态控制端口在接收帧时采取的操作。如果网桥检测到故障端口，它会将该端口置于断开状态。这些状态在IEEE 802.1D中定义： • Disabled • Blocking • Listening • Learning • Forwarding • Broken
使能模式	端口的工作激活状态。必须启用该端口才能允许其进入网络。出厂默认值已启用。
LACP Mode	指示链路聚合控制协议管理状态。必须启用该模式，端口才能参与链路聚合。
端口PHY工作模式	指示端口速度和双工模式。在自动协商模式下，通过自动协商过程设置双工模式和速度。
端口PHY连接状态	指示端口速度和双工模式。
Link Status	指示链接是 成功连接 或 连接断开。
Link Trap	指示链路状态更改时端口是否发送 trap 。
Packets RX and TX 64 Octets	接收或传输长度为64个字节（不包括帧位，但包括FCS字节）的数据包（包括坏数据包）总数。
Packets RX and TX 65-127 Octets	接收或传输的数据包（包括坏数据包）总数，其长度在65到127个字节之间（不包括帧位，但包括FCS字节）。
Packets RX and TX 128-255 Octets	接收或传输的数据包（包括坏数据包）总数，其长度在128到255个字节之间（不包括帧位，但包括FCS字节）。
Packets RX and TX 256-511 Octets	接收或传输的数据包（包括坏数据包）总数，其长度在256到511个字节之间（不包括帧位，但包括FCS字节）。
Packets RX and TX 512-1023 Octets	接收或传输的数据包（包括坏数据包）总数，其长度介于512和1023个字节之间（不包括帧位，但包括FCS字节）。
Packets RX and TX 1024-1518 Octets	接收或传输的数据包（包括坏数据包）总数，其长度在1024到1518个字节之间（不包括帧位，但包括FCS字节）。
Packets RX and TX 1519-2047 Octets	接收或传输的数据包（包括坏数据包）总数，其长度在1519到2047个字节之间（不包括帧位，但包括FCS字节）。

Packets RX and TX 2048-4095 Octets	接收或传输的数据包（包括坏数据包）总数，其长度在2048到4095个字节之间（不包括帧位，但包括FCS字节）。
Packets RX and TX 4096-9216 Octets	接收或传输的数据包（包括坏数据包）总数，其长度介于4096和9216个字节之间（不包括帧位，但包括FCS字节）。
Octets Received	网络上接收的数据（包括坏数据包中的数据）的字节总数（不包括帧位，但包括FCS字节）。该对象可作为以太网利用率的合理估计。如果需要更高的精度，则必须在公共间隔前后对etherStatsPkts和etherStatsOctets对象进行采样。
Packets Received 64 Octets	接收到的长度为64个字节（不包括帧位，但包括FCS字节）的数据包总数（包括坏数据包）。
Packets Received 65-127 Octets	接收的数据包总数（包括坏数据包），其长度在65到127个字节之间（不包括帧位，但包括FCS字节）。
Packets Received 128-255 Octets	接收的数据包总数（包括坏数据包），其长度在128到255个字节之间（不包括帧位，但包括FCS字节）。
Packets Received 256-511 Octets	接收的数据包总数（包括坏数据包），其长度在256到511个字节之间（不包括帧位，但包括FCS字节）。
Packets Received 512-1023 Octets	接收的数据包（包括坏数据包）总数，其长度介于512和1023个字节之间（不包括帧位，但包括FCS字节）。
Packets Received 1024-1518 Octets	接收的数据包总数（包括坏数据包），其长度在1024到1518个字节之间（不包括帧位，但包括FCS字节）。
Packets Received > 1518 Octets	接收到的长度超过1518个字节（不包括帧位，但包括FCS字节）且格式良好的数据包总数。
Total Packets Received Without Errors	接收到的没有错误的数据包总数。
Unicast Packets Received	传送到更高层协议的子网单播数据包数。
Multicast Packets Received	接收到的定向到组播地址的正确数据包总数。此号码不包括指向广播地址的数据包。
Broadcast Packets Received	接收到的定向到广播地址的正确数据包总数。这不包括组播数据包。
Receive Packets Discarded	即使未检测到错误也被丢弃的入站数据包的数量，以防止它们被传递到更高层协议。丢弃数据包的一个可能原因是释放缓冲区空间。
Total Packets Received with MAC Errors	包含错误的入站数据包的总数，这些错误使它们无法传递到更高层协议。
Jabbers Received	接收的数据包总数超过1518个字节（不包括帧位，但包括FCS字节），并且具有具有整数个字节（FCS错误）的坏帧检查序列（FCS）或具有非整数个字节（对齐错误）的坏FCS。jabber的定义不同于IEEE-802.3第8.2.1.5节（10BASE5）和第10.3.1.4节（10BASE2）中的定义。这些文件将jabber定义为任何数据包超过20 ms的情况。允许检测jabber的范围在20 ms和150 ms之间。

Fragments Received	接收的长度小于64个字节且带有错误CRC的数据包总数（不包括帧位，但包括FCS字节）。
Undersize Received	接收的长度小于64个字节且CRC良好的数据包总数（不包括帧位，但包括FCS字节）。
Alignment Errors	接收的数据包总数，其长度（不包括帧位，但包括FCS字节）介于64到1518个字节之间（包括64到1518个字节），但具有非整数个字节的坏帧检查序列（FCS）。
Rx FCS Errors	接收的数据包总数，其长度（不包括帧位，但包括FCS字节）介于64到1518个字节之间（包括64到1518个字节），但具有整数个字节的坏帧检查序列（FCS）。
Overruns	由于此端口因传入数据包过载而丢弃的帧总数，并且无法跟上流入。
Total Received Packets Not Forwarded	接收到的被转发进程丢弃（即过滤）的有效帧的计数。
802.3x Pause Frames Received	在此接口上接收的MAC控制帧计数，操作码指示暂停操作。当接口在半双工模式下工作时，此计数器不递增。
Unacceptable Frame Type	由于是不可接受的帧类型而从此端口丢弃的帧数。
Total Packets Transmitted (Octets)	在网络上传输的数据（包括坏数据包中的数据）的字节总数（不包括帧位，但包括FCS字节）。该对象可作为以太网利用率的合理估计。如果需要更高的精度，则必须在公共间隔前后对etherStatsPkts和etherStatsOctets对象进行采样。
Packets Transmitted 64 Octets	接收到的长度为64个字节（不包括帧位，但包括FCS字节）的数据包总数（包括坏数据包）。
Packets Transmitted 65-127 Octets	接收的数据包总数（包括坏数据包），其长度在65到127个字节之间（不包括帧位，但包括FCS字节）。
Packets Transmitted 128-255 Octets	接收的数据包总数（包括坏数据包），其长度在128到255个字节之间（不包括帧位，但包括FCS字节）。
Packets Transmitted 256-511 Octets	接收的数据包总数（包括坏数据包），其长度在256到511个字节之间（不包括帧位，但包括FCS字节）。
Packets Transmitted 512-1023 Octets	接收的数据包（包括坏数据包）总数，其长度介于512和1023个字节之间（不包括帧位，但包括FCS字节）。
Packets Transmitted 1024-1518 Octets	接收的数据包总数（包括坏数据包），其长度在1024到1518个字节之间（不包括帧位，但包括FCS字节）。
Packets Transmitted > 1518 Octets	传输的数据包总数超过1518个字节（不包括帧位，但包括FCS字节），并且格式良好。此计数器以10 Mb/s的速度每秒递增815个计数。
Maximum Frame Size	接口支持或配置为使用的最大以太网帧大小，包括以太网报头、CRC和有效负载(1518至9216)。默认的最大帧大小为1518。

Total Packets Transmitted Successfully	此端口传输到其段的帧数。
Unicast Packets Transmitted	高级协议请求传输到子网单播地址的数据包总数，包括被丢弃或未发送的数据包。
Multicast Packets Transmitted	高级协议请求传输到组播地址的数据包总数，包括被丢弃或未发送的数据包。
Broadcast Packets Transmitted	高级协议请求传输到广播地址的数据包总数，包括被丢弃或未发送的数据包。
Total Transmit Errors	单个、多个和过度碰撞的总和。
Total Transmit Packets Discarded	丢弃的单个碰撞帧、多个碰撞帧和多余帧的总和。
Single Collision Frames	在某一特定接口上成功传输的帧数的一种计数，该接口的传输被一次冲突所禁止。
Multiple Collision Frames	在一个特定接口上成功传输的帧数的计数，其中传输被一个以上的冲突所禁止。
Excessive Collision Frames	由于过度冲突，特定接口上传输失败的帧计数。
STP BPDUs Received	在所选端口接收的STP BPDU数。
STP BPDUs Transmitted	从所选端口传输的STP BPDU数。
RSTP BPDUs Received	在所选端口接收的RSTP BPDU数。
RSTP BPDUs Transmitted	从所选端口传输的RSTP BPDU数。
MSTP BPDUs Received	在所选端口接收的MSTP BPDU数。
MSTP BPDUs Transmitted	从所选端口传输的MSTP BPDU数。
802.3x Pause Frames Transmitted	在此接口上传输的MAC控制帧计数，带有指示暂停操作的操作码。当接口在半双工模式下工作时，此计数器不递增。
GVRP PDUs Received	在GARP层中接收的GVRP PDU计数。
GVRP PDUs Transmitted	从GARP层传输的GVRP PDU计数。
GVRP Failed Registrations	尝试的GVRP注册无法完成的次数。
GMRP PDUs Received	从GARP层接收的GMRP PDU计数。
GMRP PDUs Transmitted	从GARP层传输的GMRP PDU计数。
GMRP Failed Registrations	无法完成尝试的GMRP注册次数。
接收到的EAPOL帧	此验证器接收的任何类型的有效EAPOL帧数。
传输的EAPOL帧	此验证器传输的任何类型的EAPOL帧数。
自上次清除计数器以来的时间	自上次清除此端口的统计信息以来经过的时间（以天、小时、分钟和秒为单位）。

6.1.2. 查看EAP统计信息

您可以显示有关在特定端口上接收的EAP数据包的信息。

要查看EAP统计信息，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。

将显示web管理界面菜单。

- 7. 单击 **监测管理 > Ports > 端口EAP包文统计信息**

端口EAP包文统计信息 - ?														
☐	端口	PAE功能	EAPOL							EAP				
			接收帧数	发送帧数	接收的认证帧数	接收的高线帧数	接收EAPOL帧中的协议版本号	最近接收EAPOL帧中的MAC源地址	接收的无效帧数	接收中长度错误的帧数	接收的Response/ID帧数	接收的Response帧数	发送的Request/ID帧数	发送的Request帧数
☐	0/1	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/2	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/3	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/4	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/5	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/6	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/7	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/8	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/9	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/10	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/11	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/12	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/13	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
☐	0/14	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0

使用屏幕上部的按钮执行以下操作：

- 要清除交换机上所有端口的所有EAP计数器，请选中行标题栏中的复选框，然后单击 **清除** 按钮。单击按钮将所有端口的所有统计信息重置为默认值。
- 要清除特定端口的计数器，请选中与端口关联的复选框，然后单击 **清除** 按钮。
- 用交换机上上的最新信息刷新屏幕。

下表描述了屏幕上显示的EAP统计信息，单击 **刷新** 按钮。

表92. EAP统计数据

字段	描述
Port	选择要显示的端口。更改选择时，屏幕更新会导致更新新选择端口的所有字段。所有物理接口都是有效的。
PAE Capabilities	这将显示所选端口的PAE功能。
EAPOL Frames Received	这将显示此验证器接收的任何类型的有效EAPOL帧数。
EAPOL Frames Transmitted	这将显示此验证器传输的任何类型的EAPOL帧数。
EAPOL Start Frames Received	这将显示此验证器接收的EAPOL开始帧数。
EAPOL Logoff Frames Received	这将显示此验证器接收到的EAPOL注销帧数。
EAPOL Last Frame Version	显示最近接收到的EAPOL帧中携带的协议版本号。
EAPOL Last Frame Source	显示最近接收到的EAPOL帧中携带的源MAC地址。
EAPOL Invalid Frames Received	这将显示此验证器接收的未识别帧类型的EAPOL帧数。
EAPOL Length Error Frames Received	这将显示此验证器接收的未识别帧类型的EAPOL帧数。
EAP Response/ID Frames Received	这将显示此验证器接收的EAP响应/标识帧的数量。
EAP Response Frames Received	这将显示此验证器接收的有效EAP响应帧数（resp/ID帧除外）。
EAP Request/ID Frames Transmitted	这将显示此验证器传输的EAP请求/标识帧的数量。
EAP Request Frames Transmitted	这将显示此验证器传输的EAP请求帧（请求/标识帧除外）的数量。

6.1.3. 执行电缆测试

要执行电缆测试，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
- 默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
- 将显示web管理界面菜单。
7. 单击 **监测管理 > Ports > 端口电缆测试**

端口电缆测试 - ?				
☐	端口	电缆检测状态	电缆检测长度	电缆失效定位点
☐	0/1	UNTESTED		
☐	0/2	UNTESTED		
☐	0/3	UNTESTED		
☐	0/4	UNTESTED		
☐	0/5	UNTESTED		
☐	0/6	UNTESTED		
☐	0/7	UNTESTED		
☐	0/8	UNTESTED		
☐	0/9	UNTESTED		
☐	0/10	UNTESTED		
☐	0/11	UNTESTED		
☐	0/12	UNTESTED		

8. **端口**. 指示要测试的电缆所连接的接口。仅RJ45端口，使用双绞线的接口才能使用端口电缆测试功能。
9. 单击 **应用** 按键

在所选接口上执行电缆测试。电缆测试可能需要超过十秒钟以上才能完成。如果端口具有活动链路，则电缆状态始终正常。如果PHY当前链路速度支持此功能，则该命令将返回电缆长度估计值。请注意，如果链路断开且电缆连接到10/100以太网适配器，则电缆状态可能为开路或短路，因为某些以太网适配器未使用的线对未端接或接地。

下表描述了屏幕上显示的不可配置信息。

表93. 电缆测试

字段	描述
电缆检测状态	这个表项将显示电缆状态为正常、开路或短路。. • Normal: 电缆工作正常。 • Open: 电缆断开或接头有故障。 • Short: 电缆中存在电气短路。 • Cable Test Failed: 无法确定电缆状态。事实上，电缆可能正在工作。 • Untested: 电缆尚未能测试。 • Invalid cable type: 不支持该电缆类型。
电缆检测长度	电缆的估计长度（以米为单位）。长度显示为最短估计长度和最长估计长度之间的范围。如果无法确定电缆长度，则显示Unknown。仅当电缆状态正常时，才会显示电缆长度。

电缆失效定位点	从电缆末端到故障位置的估计距离（米）。仅当电缆状态为开路或短路时，才会显示故障位置。
---------	--

查看端口外部收发器模块信息

您可以查看机箱中所有光纤端口的收发器信息。

要查看端口收发器外置模块信息，请执行以下操作：

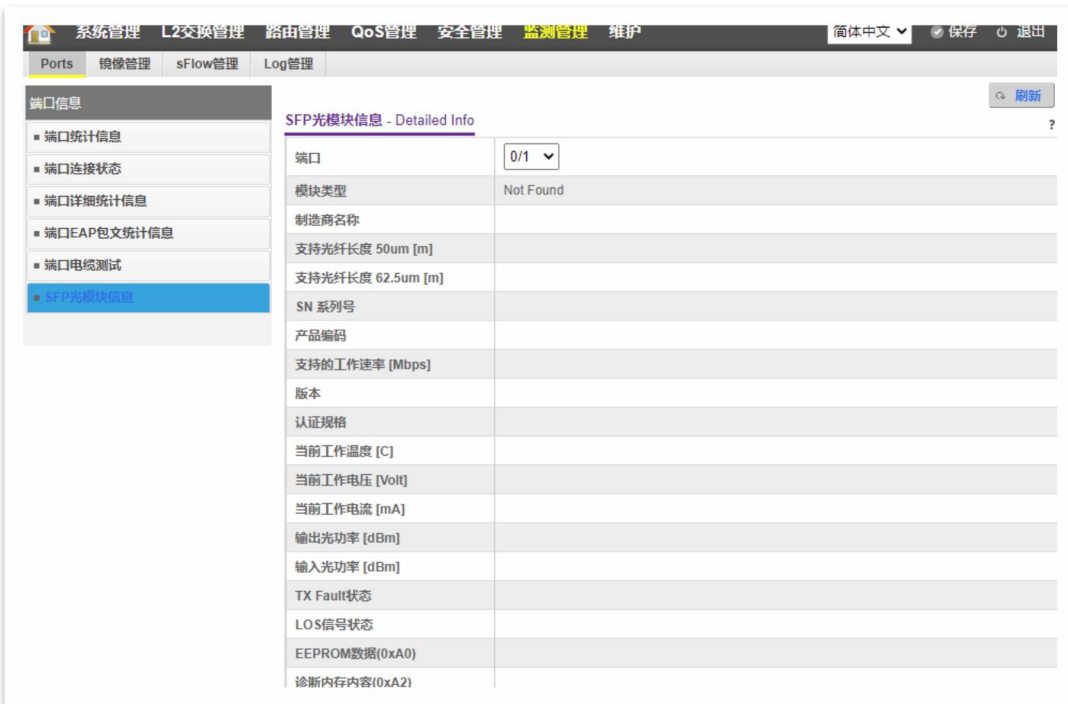
1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
将显示web管理界面菜单。

7. 单击 **监测管理 > Ports > SFP光模块信息**



8. 选择 端口 以显示所选设备的物理端口，没有检测到外部SFP模块的端口，可能不会出现在列表中。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

以下描述显示的不可配置数据。

表94. 端口收发器信息

字段	描述
Port	The interface for which data is to be displayed.
Vendor Name	Vendor name of the SFP.
Link Length 50 μm	Link length supported for 50 μm fiber.
Link Length 62, 5 μm	Link length supported for 62, 5 μm fiber.
Serial Number	Serial number of the SFP.
Part Number	Part number of the SFP.
Nominal Bit Rate	Nominal signalling rate for SFP.
Revision	Vendor revision of the SFP.
Compliance	Compliance of the SFP.

6.2.管理日志

交换机生成多种消息以响应平台上发生的事件、故障或错误以及配置更改或其他事件。这些消息存储在本地，可以转发到一个或多个集中收集点，以进行监视或长期存档存储。记录功能的本地和远程配置包括根据严重性和生成组件过滤记录或转发的消息。

6.2.1. View Buffered Logs

To view buffered logs:

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **监测管理> Log管理 > 临时log信息**。

临时log信息 - Configuration

工作模式

☐ 关闭

☒ 启用

缓冲区工作模式

覆盖擦写

记录消息级别

Debug

临时log信息 - Status

记录号	消息级别	时间	Description
NaN	Debug	Aug 15 22:42:22	[httpd]: nim_intf_map_api.c(530) 987 %% NIM: out of bounds usp used U=1, S=10 P=1 - port too large
NaN	Debug	Aug 15 22:42:21	_WEB[httpd]: boa_get.c(207) 986 %% HTTP Server: can't find file '/top_logo.png'.
NaN	Debug	Aug 15 22:42:21	[httpd]: nim_intf_map_api.c(530) 985 %% NIM: out of bounds usp used U=1, S=10 P=1 - port too large
NaN	Debug	Aug 15 22:42:20	_WEB[httpd]: boa_get.c(207) 984 %% HTTP Server: can't find file '/system/deviceView/deviceview_GS3028XFC.js'.
NaN	Debug	Aug 15 22:42:20	_WEB[httpd]: boa_request.c(738) 983 %% Peer 192.168.5.1 login success!
NaN	Info	Aug 15 22:42:20	R_MGR[httpd]: user_mgr_util.c(1612) 982 %% HTTP Session 111 started for user admin connected from 192.168.5.1
NaN	Notice	Aug 15 22:42:09	P_CLI[osapiTimer]: dhcp_prot.c(791) 981 %% Failed to acquire an IP address on Service Port; DHCP Server did not respond.

6.2.2. 配置缓冲日志

此日志根据消息组件和严重性的设置将消息存储在内存中，断电或系统重启后Log信息将被丢弃而刷新。

要配置缓冲日志，请执行以下操作：

1. 单击 **工作模式** 选项中，**启用** 或 **关闭** 单选按钮。
- 禁用的日志不会记录消息。
2. 在 **缓冲区工作模式** 选项中，指定日志已满时的行为。日志空间已满时，它可以环绕或停止。
3. 单击 **记录消息级别** 选项中，选择消息的过滤器。

日志记录的消息等于或高于配置消息的级别阈值。消息级别如下：

- **Emergency (0).** 紧急情况消息，系统无法使用。
- **Alert (1).** 警报消息，必须立即采取行动
- **Critical (2).** 临界状态消息
- **Error (3).** 错误条件消息。
- **Warning (4).** 警告条件消息。
- **Notice (5).** 正常但重要的情况消息。
- **Informational (6).** 信息性消息。
- **Debug (7).** 调试级消息。

要使用交换机上的最新信息刷新屏幕，请单击 **刷新** 按钮。

4. 单击 **清除** 按钮清除内存中的缓冲日志。

5. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

6.2.3. 消息日志格式

本主题适用于为消息日志、持久日志或控制台日志显示的所有已记录消息的格式。

通过syslog记录到收集器或中继的消息使用相同的格式：

- <15>Aug 24 05:34:05 0.0.0.0-1 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry.

此示例消息表示消息级别为7 (15 mod 8) (调试) 的消息，该消息由MSTP_api.c文件的第318行在线程ID 2110中运行的组件MSTP在8月24日05:34:05生成。这是使用系统IP 0.0.0.0和任务ID 1记录的第237条消息。

- <15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry.

此示例消息表示消息级别为7 (调试) 的用户级消息（1），该消息由MSTP_api.c文件第318行在线程ID 2110中运行的组件MSTP在8月24日05:34:05生成。这是记录的第237条消息。通过syslog记录到收集器或中继的消息使用与前一条消息相同的格式。

6.2.4. 启用或禁用命令日志

要启用或禁用命令日志，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **监测管理 > Log管理 > 操作Log记录配置**



8. 在 **工作模式** 选项中，使用管理模式启用/禁用CLI命令日志记录的操作。

6.2.5. 启用或禁用控制台日志记录

这允许将登录到连接到主机的任何串行设备的记录到Log。

要启用或禁用控制台日志记录，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **监测管理> Log管理 > CLI命令Log记录配置**



8. 单击 **工作模式** 选项中， **关闭** 或 **启用** 单选按钮。

禁用的日志不会记录消息。

9. **记录消息级别** 日志记录的消息等于或高于配置的消息级别阈值。通过在下拉输入字段中选择相应的行来选择消息级别选项。

这些消息级别可用：

- **Emergency (0)**. 紧急情况消息，系统无法使用。
- **Alert (1)**. 警报消息，必须立即采取行动
- **Critical (2)**. 临界状态消息
- **Error (3)**. 错误条件消息。
- **Warning (4)**. 警告条件消息。

- **Notice (5).** 正常但重要的情况消息。
- **Informational (6).** 信息性消息。
- **Debug (7).** 调试级消息。

6.2.6. 配置Syslog日志主机设置

要配置日志 Syslog系统，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **监测管理 > Log管理 > Sys Log 服务端配置**

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Ports	Logs	Mirroring	sFlow					

• Buffered Logs

• Command Log Configuration

• Console Log Configuration

• **Syslog Configuration**

• Trap Logs

• Event Logs

Syslog Configuration

Admin Status

☒ Disable
☐ Enable

Local UDP Port

514 (1 to 65535)

Source Interface

vlan 1

Messages Received

5925

Messages Relayed

0

Messages Ignored

0

Host Configuration

IP Address Type	Host Address	Status	Port	Severity Filter

The **Status** field displays whether the host was configure to be actively logging or not.

8. 单击 工作模式 中的， **关闭 或 启用** 单选按钮
这将启用或禁用对已配置的系统日志主机的日志记录。将此设置为禁用会停止对所有 **syslog**主机的日志记录，从而不会向任何收集器或中继发送任何消息。启用意味着使用为每个收集器或中继设备配置的值将消息发送到配置的收集器或中继器。
9. 使用本地UDP端口指定本地主机上发送syslog消息的端口。
默认端口是514。

10. 指定要用于syslog的源接口。

可能的值如下所示：

- None
- Routing interface
- Routing VLAN
- Routing loopback interface
- Tunnel interface
- Service port

默认情况下，VLAN 1用作源接口。

11. 使用IP地址类型指定主机的地址类型。

它可以是以下内容之一：

- IPv4
- IPv6
- DNS

12. 主机地址-这是为系统日志配置的主机的地址。

13. 在端口字段中，指定主机上向其发送系统日志消息的端口。

默认端口是514。

14. 在消息级别过滤器列表中选择消息级别选项。

日志记录等于或高于配置的消息级别阈值的消息。这些消息级别程度可用：

- **Emergency (0).** 紧急情况消息，系统无法使用。
- **Alert (1).** 警报消息，必须立即采取行动
- **Critical (2).** 临界状态消息
- **Error (3).** 错误条件消息。
- **Warning (4).** 警告条件消息。
- **Notice (5).** 正常但重要的情况消息。
- **Informational (6).** 信息性消息。
- **Debug (7).** 调试级消息。

下表描述了不可配置的数据。

表95. 系统日志配置

字段	描述
收到的信息	日志进程接收的消息数。这包括被删除或忽略的消息。
转发的消息	中继的系统日志消息的计数。
忽略消息	忽略系统日志消息的计数。

6.2.7. 查看Trap日志

您可以查看Trap日志中的条目。信息可以作为文件检索。

查看Trap日志：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。

- 7. 单击 **监测管理> Log管理 > Trap Log消息**



屏幕还显示有关发送的Trap信息。

单击“清除”按钮以清除所有计数器。这会将Trap日志的所有统计信息重置为默认值。

下表描述了屏幕上显示的Trap日志信息。

表96. Trap消息

字段	描述
上一次复位后接收的Trap消息数	自交换机上次重新启动以来发生的陷阱数。
Trap消息保存的容量	日志中存储的陷阱的最大数量。如果陷阱数量超过容量，则条目将覆盖最旧的条目。

自上次查看日志以来的trap数目	自上次显示陷阱以来发生的陷阱数。通过任何方法（终端界面显示、web显示、从交换机上载文件等）显示陷阱都会使此计数器清除为0。
Log	此陷阱的序列号。
消息发生时间	自上次重新启动交换机以来发生此陷阱的时间，以天、小时、分钟和秒表示。
Trap消息内容	识别陷阱的信息。

6.2.8. 查看事件日志

您可以查看事件日志，其中包含来自系统的错误消息。系统重置时不会清除事件日志。

要查看事件日志，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **监测管理> Log管理 > Event Log消息**

Event Logs						
Entry	Type	Filename	Line	Task ID	Code	Time
1	EVENT>	bootos.c	192	0	AAAAAAAA	0 0 0 28
2	EVENT>	unitmgr.c	6462	0	00000000	0 16 25 54
3	EVENT>	bootos.c	192	0	AAAAAAAA	0 0 0 28
4	EVENT>	unitmgr.c	6462	0	00000000	0 8 49 34
5	EVENT>	bootos.c	192	0	AAAAAAAA	0 0 0 28

使用屏幕上部的按钮执行以下操作：

- 要从事件日志中清除消息，请单击 **清除** 按钮。
- 要使用交换机上的最新信息刷新屏幕，请单击 **刷新** 按钮。

表97. 事件日志

字段	描述
Entry	事件的序列号。
Type	事件的类型。
File Name	事件起源的文件。
Line	事件的行号。
Task Id	事件的任务ID。
Code	事件的序列号。
Time	事件的类型。

6.2.9. 配置持久日志

持久性日志是存储在持久性存储中(Flash文件系统)的日志。持久性存储可以跨平台重新启动。第一种日志类型是系统启动日志。系统启动日志存储系统重新启动后收到的前N条消息。第二种日志类型是系统操作日志。系统操作日志存储系统操作期间收到的最后N条消息。

要配置持久日志，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

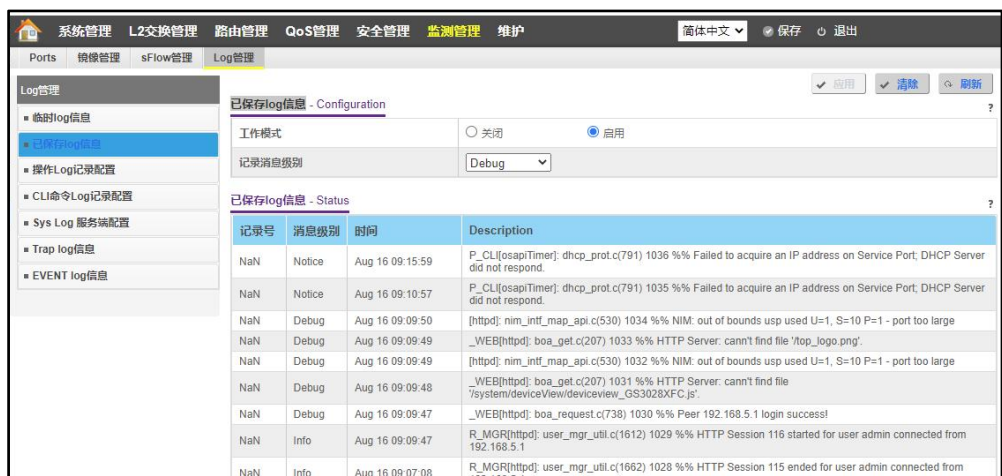
交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **监测管理 > Log管理 > 已保存log信息**



禁用的日志不会记录消息。

8. 单击 **工作模式** 选项中的，**关闭** 或 **启用** 单选按钮

9. 在“**记录消息级别**”列表中，选择消息级别。

日志记录的消息等于或高于配置的消息级别阈值。这些消息级别可用：

- **Emergency (0).** 紧急情况消息，系统无法使用。
- **Alert (1).** 警报消息，必须立即采取行动
- **Critical (2).** 临界状态消息
- **Error (3).** 错误条件消息。
- **Warning (4).** 警告条件消息。
- **Notice (5).** 正常但重要的情况消息。
- **Informational (6).** 信息性消息。
- **Debug (7).** 调试级消息。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

6.3.配置多端口镜像

端口镜像选择网络流量供网络分析器分析。这是针对交换机的特定端口完成的。因此，许多交换机端口配置为源端口，一个交换机端口配置为目标端口。您可以配置如何在源端口上镜像流量。在源端口上接收、在端口上传输或同时接收和传输的数据包可以镜像到目标端口。

复制到目标端口的数据包与线路上的原始数据包格式相同。这意味着，如果镜像正在复制接收到的数据包，则复制的数据包在源端口上接收时会被VLAN标记或未标记。如果镜像正在复制传输的数据包，则复制的数据包在源端口上传输时会被VLAN标记或未标记。

要全局配置多端口镜像，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。

- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

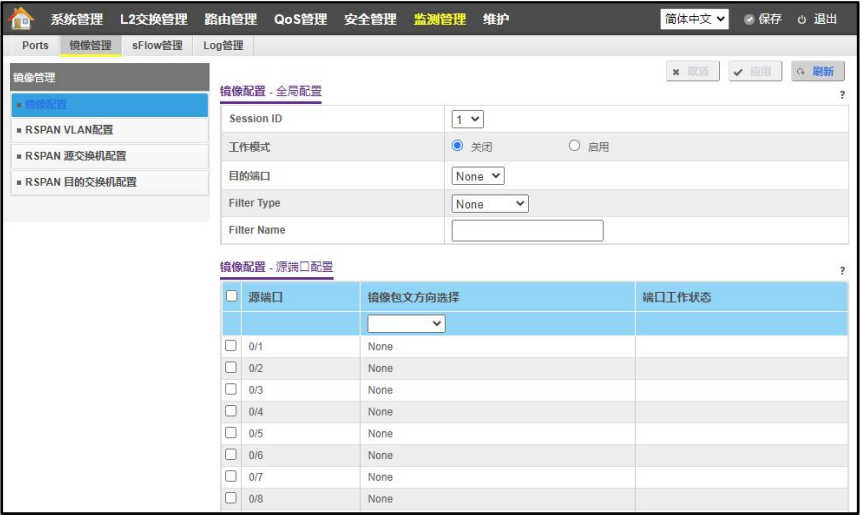
交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。

- 7. 单击 **监测管理 > 镜像管理 > 镜像配置**



- 8. 从会话ID列表中选择会话的编号。
- 9. 单击 工作模式中的， 关闭 或 启用 单选按钮
选择 启用 选项为所选会话启用管理模式。启用特定会话时，任何进入或离开会话源端口的流量都会复制（镜像）到相应的目标端口或远程交换端口分析器（RSPAN）VLAN上。默认情况下，管理模式被禁用。
- 10. 从目标端口列表中，选择要将端口通信复制到的目标接口。
您只能在系统上配置一个目标端口。它充当探测端口，并从配置的镜像端口接收所有流量。如果未配置该值，则显示为无。默认值为“无”。
- 11. 从筛选器类型列表中，选择可以镜像与许可证规则匹配的流量的IP或MAC ACL。

可能的值如下所示：

- **None.** 没有为会话配置筛选器。
- **IP ACL.** 配置IP ACL。
- **MAC ACL.** 配置MAC ACL。

默认值为“无”。

12. 在筛选器名称字段中，输入筛选器的名称（如果已为会话配置）。

13. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

14. 在“源接口配置”部分中，配置的端口指定为镜像端口。配置端口的通信量被发送到探测端口。

15. 在方向字段中，指定要从配置的镜像端口镜像的通信量的方向。

如果未配置该值，则显示为无。默认值为“无”。方向选项如下：

- **None.** 未配置该值。
- **Tx and Rx.** 监视发送和接收的数据包。
- **Tx.** 仅监视传输的数据包。
- **Rx.** 只监视接收到的数据包。

16. 单击 **应用** 按钮

这些设置将应用于系统。如果端口配置为源端口，则镜像端口字段值将被镜像。

状态字段指示接口状态。

6.3.1. 配置 RSPAN VLAN

您可以将VLAN配置为使用远程交换端口分析器（RSPAN）VLAN。RSPAN允许您从不同网络设备的多个源端口（或VLAN成员的所有端口）镜像流量，并将镜像流量发送到远程设备上的目标端口（连接到网络分析仪的探测端口）。镜像流量使用RSPAN VLAN ID进行标记，并通过中的中继端口进行传输 RSPAN VLAN。

要配置RSPAN VLAN，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **监测管理 > 镜像管理 > RSPAN VLAN**



VLAN ID列列出设备上的所有VLAN。

8. 选择要用作RSPAN VLAN的VLAN。
9. 在管理模式列表中，选择启用或禁用相应VLAN上的RSPAN支持。
默认值为禁用。

10. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

6.3.2. 配置RSPAN源交换机

要配置RSPAN源交换机，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **监测管理 > 镜像管理 > RSPAN 源交换机配置**

RSPAN 源交换机配置 - 交换机配置

Session ID: 1

工作模式: ☐ 启用 ☒ 关闭

RSPAN 目的VLAN: None

RSPAN Reflector 端口: None

Filter Type: None

Filter Name:

RSPAN 源交换机配置 - 端口配置

源端口	镜像包文方向选择	端口工作状态
☐ 0/1	None	
☐ 0/2	None	
☐ 0/3	None	
☐ 0/4	None	
☐ 0/5	None	
☐ 0/6	None	
☐ 0/7	None	
☐ 0/8	None	
☐ 0/9	None	
☐ 0/10	None	

8. 从列表中选择会话ID号。

9. 单击 工作模式中的， 关闭 或 启用 单选按钮

启用特定会话时，任何进入或离开会话源端口的流量都会复制（镜像）到相应的目标端口或远程交换端口分析器（RSPAN）VLAN上。默认情况下，管理模式为禁用。

10. 从可用VLAN ID列表中选择RSPAN目标VLAN。

11. 从反射器端口接口列表中选择RSPAN反射器端口。

12. 从筛选器类型列表中选择以配置可以镜像与许可证规则匹配的流量的IP或MAC ACL。

可能的值如下所示：

- None.
- **IP ACL.** 配置IP ACL。
- **MAC ACL.** 配置MAC ACL。

13. 如果为会话配置了筛选器，请输入筛选器名称。

14. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

要配置RSPAN源接口，请执行以下操作：

1. 在接口列表中，选择一个接口以将配置的端口指定为镜像端口。

配置端口的通信量被发送到探测端口。

2. 从“方向”列表中选择以指定要从配置的镜像端口镜像的通信量的方向。

如果未配置该值，则显示“无”。默认值为“无”。

- **None.** 未配置该值。 .

- **Tx and Rx.** 监视发送和接收的数据包。
- **Tx.** 仅监视传输的数据包。
- **Rx.** 仅监视接收到的数据包。

状态字段指示接口状态。

6.3.3. 配置RSPAN目标交换机

要配置RSPAN目标交换机，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **监测管理 > 镜像管理 > RSPAN 目的交换机配置**

The screenshot shows the 'RSPAN 目的交换机配置' (RSPAN Destination Switch Configuration) page. The left sidebar contains a tree view with '镜像管理' (Mirror Management) expanded, showing sub-items: '镜像配置' (Mirror Configuration), 'RSPAN VLAN配置' (RSPAN VLAN Configuration), 'RSPAN 源交换机配置' (RSPAN Source Switch Configuration), and 'RSPAN 目的交换机配置' (RSPAN Destination Switch Configuration), which is currently selected. The main content area has a title bar with 'RSPAN 目的交换机配置 -' and a question mark icon. Below the title bar are buttons for '取消' (Cancel), '应用' (Apply), and '刷新' (Refresh). The configuration fields include: 'Session ID' (dropdown menu showing '1'), '工作模式' (Work Mode) with radio buttons for '启用' (Enable) and '关闭' (Disable), 'RSPAN 源VLAN' (dropdown menu showing 'None'), 'RSPAN 目的端口' (dropdown menu showing 'None'), 'Filter Type' (dropdown menu showing 'None'), and 'Filter Name' (text input field).

8. 从会话ID列表中，选择会话ID。

9. 为所选会话选择管理模式 **启用** 或 **禁用** 单选按钮。

启用特定会话时，任何进入或离开会话源端口的流量都会复制（镜像）到相应的目标端口或远程交换端口分析器（RSPAN）VLAN上。默认情况下，管理模式处于禁用状态。

10. 从可用VLAN ID列表中选择RSPAN源VLAN。

11. 从目标接口列表中选择RSPAN目标VLAN。

12. 配置过滤器类型。

符合ACL规则的IP或MAC ACL镜像流量。可能的值如下所示：

- **None.** 没有为会话配置筛选器。
- **IP ACL.** 配置IP ACL。
- **MAC ACL.** 配置MAC ACL。

13. 输入筛选器名称（如果已为会话配置）。

14. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

6.4.配置 sFlow

您可以配置基本或高级sFlow设置。

6.4.1. 配置基本sFlow代理信息

要配置基本sFlow代理信息，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **监测管理 > sFlow管理 > 基本信息 > sFlow Agent**

The screenshot shows the 'sFlow Agent' configuration page. The top navigation bar includes '系统管理', 'L2交换管理', '路由管理', 'QoS管理', '安全管理', '监测管理', and '维护'. The '监测管理' tab is active, and the 'sFlow管理' sub-tab is selected. The left sidebar shows 'sFlow管理' with '基本信息' and '高级管理信息' options. The main content area is divided into two sections: 'sFlow Agent - Source Interface' and 'sFlow Agent - Information'. The 'Source Interface' section has a 'Source Interface' dropdown menu currently set to 'None'. The 'Information' section displays 'Agent Version' as '1.3;Broadcom Corp.;1.0.2.1' and 'Agent Address' as '0.0.0.0'. There are '应用' (Apply) and '刷新' (Refresh) buttons at the top right of the configuration area.

8. 在“源接口”列表中，选择用于sFlow代理的管理接口。

可能的值如下所示：

- None
- Routing interface
- Routing VLAN
- Routing loopback interface
- Tunnel interface
- Service port

默认情况下，VLAN 1用作源接口。

9. 单击 **应用** 按键

更新的配置参数将发送到交换机，配置更改将立即生效。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表描述了不可配置的信息。

表98. sFlow Basic Agent Information

字段	描述
Agent Version	唯一标识此MIB的版本和实现。版本字符串必须使用以下结构：MIB版本；组织机构；软件版本，其中： • MIB 版本: 例如，1.3，此MIB的版本 • 机构: Broadcom Inc. • 修订版: 1.0.2.1
Agent Address	与此代理关联的IP地址。.

6.4.2. 配置sFlow代理高级设置

要配置sFlow agent高级设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **监测管理 > sFlow管理 > 高级管理信息 > sFlow Agent.**

System	Switching	Routing	QoS	Security	Monitoring
Ports	Logs	Mirroring	sFlow		
sFlow		sFlow Agent Source Interface			
• Basic • Advanced • sFlow Agent Information • sFlow Receiver Configuration • sFlow Interface Configuration		Source Interface: vlan 1			
		sFlow Agent Information			
		Agent Version: 1.3;Netgear Inc.;Q.2.15.1 Agent Address: 10.130.84.23			

11. 在“源接口”列表中，选择用于sFlow代理的管理接口。

可能的值如下所示：

- None
- Routing interface
- Routing VLAN
- Routing loopback interface
- Tunnel interface
- Service port

默认情况下，VLAN 1用作源接口。

12. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

要使用交换机上的最新信息刷新屏幕，请单击更新按钮。

下表描述了不可配置的信息。

表99. sFlow Basic Agent Information

字段	描述
Agent Version	唯一标识此MIB的版本和实现。版本字符串必须使用以下结构：MIB版本；组织机构；软件版本，其中： • MIB 版本: 例如，1.3，此MIB的版本 • 机构: Broadcom Inc. • 修订版: 1.0.2.1
Agent Address	与此代理关联的IP地址。

6.4.3. Configure an sFlow Receiver

To configure an sFlow receiver:

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。

- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **监测管理 > sFlow > 高级管理 > sFlow Receiver Configuration.**

sFlow Receiver Configuration - ?								
☐	Receiver Index	Receiver Owner	No Timeout	Receiver Timeout	Maximum Datagram Size	Receiver Address	Receiver Port	Datagram Version
☐	1		True	0	1400	0.0.0.0	6343	5
☐	2		True	0	1400	0.0.0.0	6343	5
☐	3		True	0	1400	0.0.0.0	6343	5
☐	4		True	0	1400	0.0.0.0	6343	5
☐	5		True	0	1400	0.0.0.0	6343	5
☐	6		True	0	1400	0.0.0.0	6343	5
☐	7		True	0	1400	0.0.0.0	6343	5
☐	8		True	0	1400	0.0.0.0	6343	5

- 8. 指定接收方所有者
这是使用sFlowRcvrTable表项的实体。空字符串表示条目当前未声明，接收方配置被重置为默认值。希望声明sFlowRcvrTable条目的实体必须确保该条目在尝试声明之前是未声明的。通过设置所有者字符串声明条目。在对其他采样器对象进行任何更改之前，必须声明该条目。
- 9. 接收器超时-释放取样器并停止取样前剩余的时间（秒） 。
希望保持对采样器控制的管理实体负责在旧值过期之前设置新值。有效范围为0到2147483647。值为零将所选接收器配置设置为其默认值。
- 10. 使用“无超时”选择 **True** 或 **False** ， 设置接收器的无超时采样。
在选择的“无超时”条目为真之前，不会停止采样。默认值为False。
- 11. **Maximum Datagram Size** - 单个样本数据报中可发送的最大数据字节数。
设置此值以避免sFlow数据报的碎片。默认值： 1400。允许的范围为200到9116。
- 12. **Receiver Address.** sFlow收集器的IP地址。
如果设置为0.0.0.0， 则不发送sFlow数据报。
- 13. **Receiver Port.** sFlow数据报的目标端口。
允许的范围为1到65535。

Receiver Datagram Version（接收器数据报版本）字段显示要发送的sFlow数据报的版本。

6.4.4. 配置sFlow接口

sFlow agent对交换流进行基于统计包的采样，并将其发送给配置的接收者。配置为收集流示例的数据源称为采样器。sFlow agent还收集基于时间的网络接口统计数据采样，并将它们发送给配置好的sFlow接收器。配置为收集计数器样本的数据源称为轮询器。

要配置sFlow接口，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **监测管理 > sFlow > 高级管理信息 > sFlow Interface Configuration.**

sFlow Interface Configuration - ?						
☐	Interface	Poller		Sampler		
		Receiver Index	Poller Interval	Receiver Index	Sampling Rate	Maximum Header Size
☐						
☐	0/1					
☐	0/2					
☐	0/3					
☐	0/4					
☐	0/5					
☐	0/6					
☐	0/7					
☐	0/8					
☐	0/9					
☐	0/10					
☐	0/11					

- 8. **Interface** 显示此流量轮询器和采样器的界面。
此代理仅支持物理端口。
- 9. **Poller Receiver Index** 使用轮询器接收器索引指定与此计数器轮询器关联的sFlow接收器的允许范围。
允许的范围是1到8。

10. Poller Interval 使用轮询器间隔指定与此数据源关联的计数器连续采样之间的最大秒数。

采样间隔为0将禁用计数器采样。允许的范围为0到86400秒。

11. Sampler Receiver Index 使用采样器接收器索引指定此流量采样器的sFlow接收器。

只能设置活动接收器。如果接收器过期，则与接收器关联的所有采样器也将过期。允许的范围是1到8。

12. Sampling Rate 使用采样率为此源的数据包采样指定统计采样率。

采样率为1统计所有数据包。采样率为0将禁用采样。允许的范围是1024到65536。

13. Maximum Header Size 使用最大标头大小指定要从采样数据包复制的最大字节数。

允许的范围是20到256。

7. 维护

本章涵盖以下主题：

- 保存配置
- 重新启动交换机
- 将交换机重置为出厂默认设置
- 将所有用户密码重置为其默认设置
- 从交换机上载文件
- 将文件下载到交换机
- 文件管理
- 故障排除

7.1.保存配置

保存配置后，将存储所做的设置更改，直到交换机下一次重新启动时加载使用。您可以手动保存配置。

要保存配置，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
- 6. 单击 **登录** 按钮。
将显示web管理界面菜单。
- 7. 单击 **维护 > 保存配置 > 保存操作**



- 8. 单击勾选 复选框
- 9. 单击 **应用** 按键

您所做的配置更改将在系统重新启动时保存。交换机保留自上次保存或系统重新启动以来提交的所有更改。

7.2.重新启动交换机

要重新启动交换机，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **维护 > 重启设备 > 重启操作**



8. 选择一个单选按钮：

- 保存当前配置并重新启动交换机。
- 交换机将在不保存当前配置的情况下重新启动。

9. 单击 **应用** 按键

如果选择了“保存”选项，则会保存当前的配置。交换机重新启动。

7.3.将交换机重置为出厂默认设置

提示： 如果将交换机重置为默认配置，则IP地址将重置为 192.168.10.12 .

要将交换机重置为出厂默认设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **维护 > 重启设备 > 恢复出厂设备**



8. 选中该复选框。

9. 单击 **应用** 按钮

将显示一个确认信息提示。

10. 单击“是”确认。

所有配置参数均重置为出厂默认值。即使您发出了保存命令，您所做的所有更改都是无效的。

7.3.1. 将所有用户密码重置为其默认设置

要将所有用户密码重置为其默认设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击**维护 > 重启设备 > 密码清除**



8. 选中该复选框。

9. 单击 **应用** 按钮

所有用户密码均重置为出厂默认值。

7.4.从交换机下载文件

您可以将配置（ASCII）、日志（ASCII）和映像（二进制）文件从交换机上拷贝到TFTP服务器。

7.4.1. 将文件从交换机复制到TFTP服务器：

要将文件从交换机上复制到TFTP服务器，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **维护>下载配置文件 > 保存文件下载**.

文件类别	Running Configuration ▼
传输用的协议	TFTP ▼
服务端的地址选择	IPv4 ▼
服务端的地址值	
保存在服务端的文件名	

8. 使用“文件类别”指定要复制拷贝的文件类型：

- **Archive.** 保存在FLASH 中指定的存档加载运行的代码
- **CLI Banner.** 指定的CLI标题文件.
- **Startup Configuration.** 在文本模式下，交换机启动时加载的配置文件
- **Running Configuration.** 在文本模式下，当前交换机运行的配置文件
- **Script File.** 特定的脚本配置文件
- **Error Log.** 指定的系统错误（持续）日志，有时称为事件日志。
- **Trap Log.** 指定Traps事件日志。
- **Buffered Log.** 指定的缓冲区（内存中）记录日志.
- **Crash Logs.** 指定系统崩溃记录日志。工厂默认值为存档.

9. Image Name字段仅在选定的文件类型为存档时可见。

如果要上载交换机映像（存档），请使用映像名称列表选择交换机上要上载到管理系统的软件映像：

- 选择image1以上载image1。
- 选择image2以上载image2。.

10. 使用传输模式指定要用于传输文件的协议：

- **TFTP.** 普通文件传输协议
- **SFTP.** 安全文件传输协议
- **SCP.** 安全复制协议
- **FTP.** 文件传输协议

11. 使用服务器地址类型指定IPv4、IPv6或DNS以指示服务器地址字段的格式。出厂默认值为IPv4。

12. 根据服务器地址类型，输入服务器地址类型对应格式的输入服务器的IP地址。.

出厂默认值为IPv4地址0.0.0.0。

13. 使用远程文件路径输入上载文件的路径。

文件路径只能包含字母、数字、正斜杠、点或下划线字符。最多可以输入160个字符。出厂默认值为空。

14. 使用远程文件名输入要从服务器下载的文件名称。最多可以输入32个字符。

出厂默认值为空。

15. 使用本地文件名指定要上载的本地脚本文件名。

仅当文件类型为脚本文件时，此字段才可见。

16. 使用用户名输入远程登录到发送文件的SFTP/SCP服务器的用户名。

仅当选择SFTP或SCP传输模式时，此字段才可见。

17. 使用密码输入远程登录到发送文件的SFTP/SCP服务器的密码。

仅当选择SFTP或SCP传输模式时，此字段才可见。

表格的下端的状态框用于显示有关文件传输进度的信息。

7.4.2. HTTP文件上载

要使用HTTP 文件上载，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **维护>下载配置文件 > HTTP 文件下载**



8. 使用“文件类别”指定要复制拷贝的文件类型：
 - **Archive.** 保存在FLASH 中的存档加载运行的代码
 - **CLI Banner.** 指定的CLI标题文件.
 - **Startup Configuration.** 在文本模式下，交换机启动时加载的配置文件
 - **Running Configuration.** 在文本模式下，当前交换机运行的配置文件
 - **Script File.** 特定的脚本配置文件
 - **Error Log.** 指定的系统错误（持续）日志，有时称为事件日志。
 - **Trap Log.** 指定Traps事件日志。
 - **Buffered Log.** 指定的缓冲区（内存中）记录日志.
 - **Crash Logs.** 指定系统崩溃记录日志。工厂默认值为存档.
9. 使用本地文件名指定要上载的本地脚本文件名。

7.4.3. 将文件从交换机保存到USB设备

要使用将文件从交换机上载到**USB**设备，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

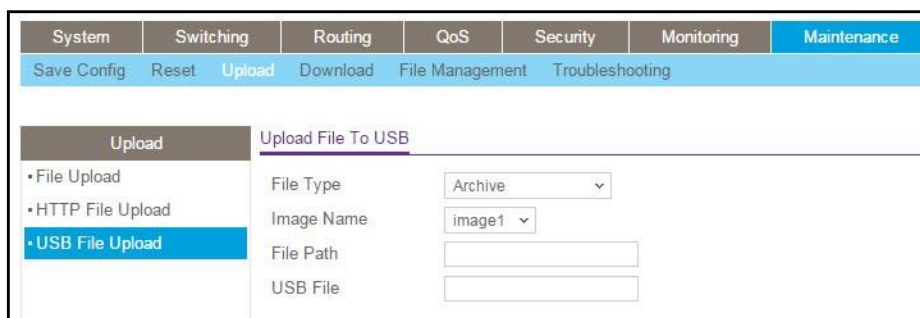
5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **维护>下载配置文件 > USB文件下载**。



System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Save Config	Reset	Upload	Download	File Management	Troubleshooting	

Upload

Upload File To USB

• File Upload

• HTTP File Upload

• **USB File Upload**

File Type

Archive

Image Name

image1

File Path

USB File

8. 使用“文件类型”指定要上载的文件类型：
 - **Archive.** 保存在FLASH 中的存档加载运行的代码
 - **Text Configuration.** 文本模式下的的配置文件。
9. Image Name字段仅在选定的文件类型为存档时可见。
 - 选择image1以上载image1。
 - 选择image2以上载image2。 .
10. 在文件路径字段中，输入要上载的文件的路径。

最多可以使用146个字符。默认值为空。

11. 使用USB文件指定要上载的文件的名称和路径。

最多可以输入32个字符。出厂默认值为空。

12. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

7.5.将文件上传保存到交换机

交换机支持使用TFTP或HTTP将系统文件从远程系统下载到交换机的Flash文件系统。

7.5.1. 上传文件

要上传文件，请执行以下操作：

- 1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
- 2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
- 3. 启动web浏览器。
- 4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

- 5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

- 6. 单击 **登录** 按钮。

将显示web管理界面菜单。

- 7. 单击 **维护> 更新设备文件 > 文件上传**

文件上传 - 上传文件然后保存到交换机中

文件类别

Startup Configuration

传输用的协议

TFTP

服务端的地址选择

IPv4

服务端的地址值

保存在服务端的文件名

- 8. 使用“文件类型”指定要传输的文件类型。

- **Archive.** 存档映像代码，用于升级闪存中的加载运行代码。
- **Startup Configuration.** 在文本模式下，交换机启动时加载的配置文件
- **Running Configuration.** 在文本模式下，当前交换机运行的配置文件
- **SSH-1 RSA Key File.** SSH-1 Rivest Shamir Adelman (RSA) 密钥文件。
- **SSH-2 RSA Key PEM File.** SSH-2 Rivest Shamir Adelman (RSA) 密钥文件 (PEM编码)。
- **SSH-2 DSA Key PEM File.** SSH-2 数字签名算法 (DSA) 密钥文件 (PEM编码)。
- **SSL Trusted Root Certificate PEM File,** 使用SSL可信根证书PEM文件指定SSL可信根证书文件 (PEM编码)。
- **SSL Server Certificate PEM File,** 使用SSL服务器证书PEM文件指定SSL服务器证书文件 (PEM编码)。
- **SSL DH Weak Encryption Parameter PEM File,** 使用SSL DH弱加密参数PEM文件指定SSL Diffie-Hellman弱加密参数文件 (PEM编码)。
- **Use SSL DH Strong Encryption Parameter PEM File,** 使用SSL DH强加密参数PEM文件指定SSL Diffie-Hellman强加密参数文件 (PEM编码)。
- **Script File,** 脚本配置文件。
- **CLI Banner,** 如果要在登录提示之前显示标题，请指定CLI标题。
- **IAS Users,** 使用IAS用户指定内部身份验证服务器用户数据库文件。

提示： 要下载SSH密钥文件，必须在管理上禁用SSH，并且不能有活动的SSH会话。

提示： 要下载SSL PEM文件，必须以管理方式禁用SSL，并且不能有活动的SSH会话。

仅当选择“**Archive**”时，“**Image Name**”字段才可见。

9. 使用 “**Image Name**” 从列表选择一个图像：
 - **Image1.** 选择image1以更新image1 固件代码。
 - **Image2.** 选择image2以更新image2 固件代码。
10. 使用传输模式指定要用于传输文件的协议：
 - **TFTP.** 普通文件传输协议
 - **SFTP.** 安全文件传输协议
 - **SCP.** 安全复制协议
 - **FTP.** 文件传输协议
11. 使用 **服务端的地址选择** 选项指定IPv4、IPv6或DNS以指示TFTP/SFTP/SCP服务器地址字段的

格式。

出厂默认值为IPv4。

12. 在 **服务器地址** 字段中，根据服务器地址类型指示的格式输入服务器的 IP 地址，例如 x.x.x.x.x 格式中的 IP 地址。

默认值为IPv4地址0.0.0.0。

13. 使用远程文件路径输入要下载的文件的路径。

文件路径不能包含以下符号：“\: *? "<>|“。最多可输入160个字符。出厂默认值为空。

14. 使用远程文件名输入要从服务器下载的文件名称。

文件路径不能包含以下符号：“\: *? "<>|“。最多可以输入32个字符。出厂默认值为空。

15. 使用用户名输入文件所在的SFTP/SCP服务器的远程登录用户名。

仅当选择SFTP或SCP传输模式时，此字段才可见。

16. 使用密码输入远程登录到文件所在的SFTP/SCP服务器的密码。

仅当选择SFTP或SCP传输模式时，此字段才可见。

表的最后一栏显示有关文件传输进度的信息。它仅在流程开始后显示。屏幕将自动刷新，直到文件传输完成。

17. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

7.5.2. 使用HTTP将文件下载到交换机

您可以使用HTTP会话（例如，通过web浏览器）将各种类型的文件下载到交换机。

要使用HTTP将文件下载到交换机，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

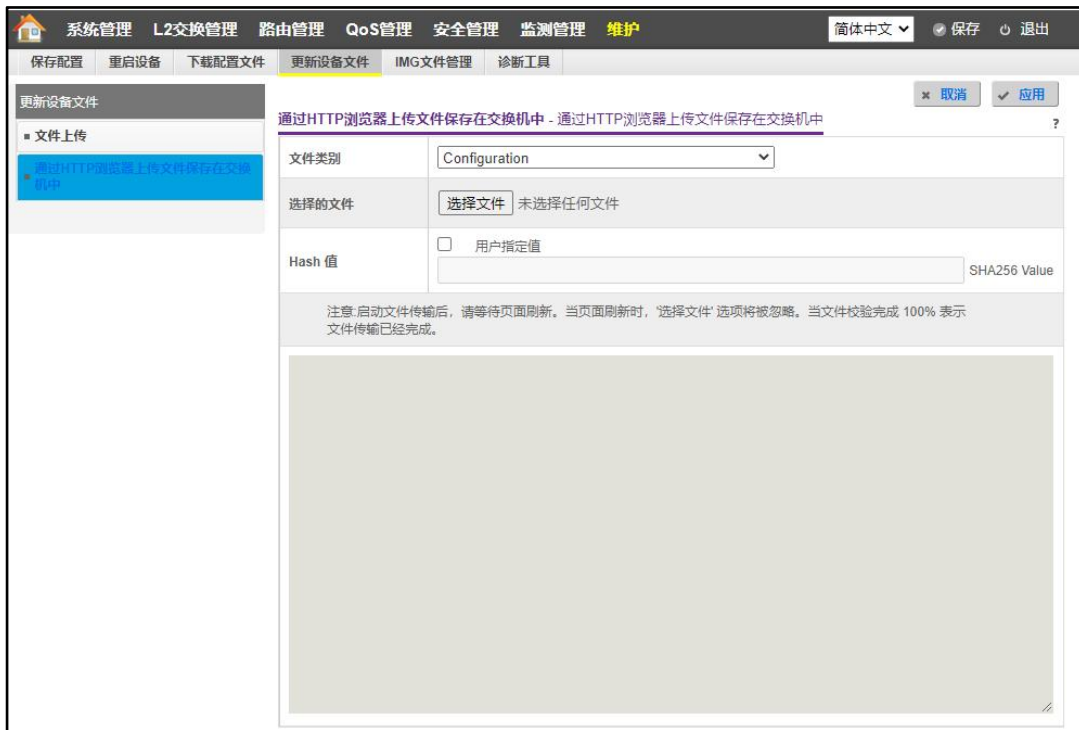
5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **维护> 更新设备文件 > HTTP上传**



8. 使用“文件类型”指定要传输的文件类型。

- **Archive.** 存档映像代码，用于升级闪存中的加载运行代码。
- **Startup Configuration.** 在文本模式下，交换机启动时加载的配置文件
- **Running Configuration.** 在文本模式下，当前交换机运行的配置文件
- **SSH-1 RSA Key File.** SSH-1 Rivest Shamir Adelman (RSA) 密钥文件。
- **SSH-2 RSA Key PEM File.** SSH-2 Rivest Shamir Adelman (RSA) 密钥文件 (PEM编码)。
- **SSH-2 DSA Key PEM File.** SSH-2数字签名算法 (DSA) 密钥文件 (PEM编码)。
- **SSL Trusted Root Certificate PEM File,** 使用SSL可信根证书PEM文件指定SSL可信根证书文件 (PEM编码)。
- **SSL Server Certificate PEM File,** 使用SSL服务器证书PEM文件指定SSL服务器证书文件 (PEM编码)。
- **SSL DH Weak Encryption Parameter PEM File,** 使用SSL DH弱加密参数PEM文件指定SSL Diffie-Hellman弱加密参数文件 (PEM编码)。
- **Use SSL DH Strong Encryption Parameter PEM File,** 使用SSL DH强加密参数PEM文件指定SSL Diffie-Hellman强加密参数文件 (PEM编码)。
- **Script File,** 脚本配置文件。
- **CLI Banner,** 如果要在登录提示之前显示标题，请指定CLI标题。

- **IAS Users**，使用IAS用户指定内部身份验证服务器用户数据库文件。

提示： 要下载SSH密钥文件，必须在管理上禁用SSH，并且不能有活动的SSH会话。

提示： 要下载SSL PEM文件，必须以管理方式禁用SSL，并且不能有活动的SSH会话。

9. 使用“**选择文件**”在浏览器中浏览并输入要下载的文件名称和路径。

最多可以输入80个字符。出厂默认值为空。

10. 在 Hash 值选项中，可以输入文件的 SHA256 校验值，以方便检查文件是否完整无误。

默认不启用 Hash 校验。

11. 单击 **应用** 按键，开始下载。

下载状态字段显示将文件传输到交换机期间的状态。

提示： 启动文件传输后，等待屏幕刷新。当屏幕刷新自动刷新信息时，传输完成后，会弹出一提示框。文件传输中请不要切换到其它操作页面，以免中断文件传输。

7.5.3. 从USB设备下载文件

要从USB设备下载文件，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **维护> 更新设备文件 > USB File Download.**

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Save Config	Reset	Upload	Download	File Management	Troubleshooting	
Download - File Download - HTTP File Download USB File Download Download File From USB File Type: Archive Image Name: image1 File Path: USB File:						

8. 使用“文件类型”指定要传输的文件类型。
 - **Archive.** 存档映像代码，用于升级闪存中的加载运行代码
 - **Text Configuration.** 在文本模式下，交换机启动时加载的配置文件(Startup-config).
如果文件有错误，更新将停止。出厂默认设置为存档。
9. 使用“Image Name”从列表选择一个映像：
 - **Image1.** 单击image1 to download to image1.
 - **Image2.** 单击image2 to download to image2.

仅当选择“文件类型存档”时，**Image Name**字段才可见。
10. 使用文件路径字段提供要下载的文件的路径。

最多可以输入146个字符。默认值为空。
11. 使用USB文件指定要下载的文件名称和路径。

最多可以输入32个字符。出厂默认值为空。
12. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

下载状态显示文件传输到交换机的状态。表的最后一行用于显示有关文件传输进度的信息。它仅在流程开始后显示。屏幕将自动刷新，直到文件传输完成。

7.6.文件管理

系统在永久存储器(Flash)中维护两个版本的加载运行映像固件。一个映像是活动映像，第二个映像是备份映像。在随后的交换机重新启动期间加载活动映像。升级或降级固件软件时，此功能可缩短交换机关机时间。

7.6.1. 复制映像

要复制映像，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。

3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
将显示web管理界面菜单。
7. 单击 **维护> IMG文件管理 > 文件复制**



8. 使用源映像选择image1或 image2 作为 源映像文件（要复制的映像）。
9. 使用目标映像文件选择 Image1 或 Image2 作为目标映像。
10. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

7.6.2. 配置双映像设置

双映像功能允许交换机在永久存储器中保留两个映像。管理员可以将image1或image2指定为活动映像，以便在随后的交换机重新启动期间加载。升级或降级软件映像时，此功能可缩短交换机关闭时间，方便交换机固件维护。

要配置双映像设置，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin**，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **维护> IMG文件管理 > 双固件管理**



8. 使用“**下一次启动时的选择文件**”使所选映像成为此交换机续重新启动的时加载运行的下一个活动映像。

9. 在 **Image 描述** 字段中，可以输入对此Image映像的字符串描述。

10. 单击 **应用** 按钮

更新的配置参数将发送到交换机，配置更改将立即生效。

提示： 激活映像后，必须执行交换机系统的重新启动才可以运行新代码。

下表描述了屏幕上显示的不可配置信息。

表247.双映像配置

字段	描述
Image Name	这将显示选定单元的映像名称。
启用时加载的文件	启动时，设备的加载活动映像与否。
版本	image代码文件的版本。

7.7.故障排除

您可以使用Ping或Traceroute，并且可以执行内置程序。

7.7.1. Ping IPv4

您可以告诉交换机向指定的IP地址发送ping请求。您可以检查交换机是否可以与特定IP站通信。单击应用按钮时，**交换机**将发送指定数量的ping请求，并显示结果。

如果未收到对ping的回复，将显示以下消息：

```
Tx = Count, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec
```

如果收到对ping的回复，将显示以下消息：

```
Reply From a.b.c.d: icmp_seq = 0. time= xyz usec.  
Reply From a.b.c.d: icmp_seq = 1. time= abc usec.  
Reply From a.b.c.d: icmp_seq = 2. time= def usec.  
Tx = count, Rx = count Min/Max/Avg RTT = xyz/abc/def msec
```

设置并ping网络上的主机，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。
将显示web管理界面菜单。
7. 单击 **维护 > 诊断工具 > Ping IPv4**。

The screenshot shows a web management interface with a top navigation bar containing '系统管理', 'L2交换管理', '路由管理', 'QoS管理', '安全管理', '监测管理', and '维护'. Below this is a sub-navigation bar with '保存配置', '重启设备', '下载配置文件', '更新设备文件', 'IMG文件管理', and '诊断工具'. The '诊断工具' section is expanded, showing a sidebar with 'Ping IPv4', 'Ping IPv6', 'Traceroute IPv4', and 'Traceroute IPv6'. The main content area is titled 'Ping IPv4 -' and contains a form with the following fields: '目的IP地址或主机名称' (text input, placeholder '(Max 255 characters/x.x.x.x)'), '次数' (text input, value 3, range '(1 to 15)'), '间隔(秒)' (text input, value 1, range '(1 to 60)'), '包文数据段长度' (text input, value 0, range '(0 to 65507)'), and '选择源接口' (dropdown menu, value 'None'). At the bottom of the form is a 'Ping 结果:' section. There are '取消' and '应用' buttons at the top right of the form area.

8. 使用IP地址/主机名输入切换到ping的站点的IP地址或主机名。
初始值为空。
9. 在计数字段中，输入要发送的回显请求数。
默认值为3。范围为1到15。
10. 输入ping数据包之间的间隔（以秒为单位）。
默认值为3秒。范围是1到60。

11. 输入ping数据包的数据报大小。

默认值为0字节。范围是0到65507。

12. 输入发送回显请求数据包时要使用的源IP地址或接口。

如果不需要源，请选择“无”作为源选项。可能的值如下所示：

- **None.** ping数据包的源地址将是默认传出接口的地址。
- **IP Address.** 发送回显请求数据包时要使用的源IP地址。当选择IP地址作为源选项时，将显示此字段。
- **Interface.** 发送回显请求数据包时要使用的接口。当选择接口作为源选项时，将显示此字段。

提示： 此屏幕上字段中配置的值不会保存到交换机。因此刷新屏幕会将这些字段设置为默认值

13. 单击 **应用** 按钮

ping被发送到指定的地址。交换机发送计数字段中指定的ping数，结果显示在结果区域的可配置数据下方。

要取消屏幕上的操作并将屏幕上的数据重置为交换机的最新值，请单击取消按钮。

7.7.2. Ping IPv6

此屏幕用于向指定的主机名或IPv6地址发送ping请求。您可以使用此选项检查交换机是否可以与特定IPv6站点通信。单击应用按钮时，交换机发送指定数量的ping请求，结果显示在可配置数据下方。

输出显示以下内容：

Send count=n, Receive count=n from (IPv6 Address). Average round triptime = n ms.

要使用Ping IPv6，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **维护 > 诊断工具 > Ping IPv6**。

8. 从列表中选择**Ping类型**。可能的

值如下所示：

- **Global**. Ping全局IPv6地址。
- **Link Local**. 通过指定接口Ping链路本地IPv6地址。当选择接口作为ping选项时，将显示此字段。

9. 使用IPv6地址/主机名输入要切换到ping的站点的IPv6地址或主机名。

初始值为空。格式为xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx，最大字符数为255。

10. 使用Count输入发送的回显请求数。

范围为1到15。默认值为3。

11. 输入ping数据包之间的间隔（以秒为单位）。

范围为1到60。默认值为3。

12. 使用数据报大小输入数据报大小。

有效范围为0到13000。默认值为0字节。

13. 输入发送回显请求数据包时要使用的源IP地址或接口。

如果不需要源，请选择“无”作为源选项。可能的值如下所示：

- **None**. ping数据包的源地址将是默认传出接口的地址。
- **IPv6 Address**. 发送回显请求数据包时要使用的源IPv6地址。选择IPv6地址作为源选项时，将显示此字段。
- **Interface**. 发送回显请求数据包时要使用的接口。当选择接口作为源选项时，将显

示此字段。

提示： Values configured in the fields in this screen are not saved to the switch. As a result, refreshing the screen sets these fields to the default values.

14. 单击 **应用** 按钮

此屏幕中字段中配置的值不会保存到交换机。因此刷新屏幕会将这些字段设置为默认值。

7.7.3. Traceroute IPv4

使用此屏幕告知交换机向指定的IP地址或主机名发送跟踪路由请求。您可以使用它来发现数据包到远程目标的路径。单击**Apply**按钮后，交换机将发送**traceroute**，结果显示在可配置数据下方。

如果收到对跟踪路由的回复，将显示以下消息：

```
1 e.f.g.h 9869 usec 9775 usec 10584 usec
2 0.0.0.0 0 usec * 0 usec * 0 usec *
3 0.0.0.0 0 usec * 0 usec * 0 usec *
Hop Count = j Last TTL = k Test attempt = m Test Success = n.
```

要配置跟踪路由并发送探测数据包以发现到网络上主机的路由，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。

默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。

6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **维护 > 诊断工具 > Traceroute IPv4**.

系统管理 L2交换管理 路由管理 QoS管理 安全管理 监测管理 维护

保存配置 重启设备 下载配置文件 更新设备文件 IMG文件管理 诊断工具

诊断工具

- Ping IPv4
- Ping IPv6
- Traceroute IPv4
- Traceroute IPv6

Traceroute IPv4

目的IP地址或主机名称 (Max 255 characters/x.x.x.x)

Probes Per Hop (1-10)

Max TTL (1-255)

Init TTL (1-255)

Max Fail (1-255)

间隔(秒) (1-60)

端口号 (1 to 65535)

数据包长度 (0 to 39936)

选择源接口

输出结果:

8. 使用IP地址/主机名输入要查找路径的站点的IP地址或主机名。

默认值为空。

9. 输入每个跃点的探测数。

默认值为3。范围为1到10。

10. 输入目标的最大TTL。

默认值为30。范围为1到255。

11. 输入要使用的初始TTL。

默认值为1。范围为1到255。

12. 输入会话中允许的最大失败次数。

默认值为5。范围为1到255。

13. 以秒为单位输入探测之间的时间。

默认值为3。范围为1到60。

14. 在探测数据包中输入UDP目标端口。

默认值为33434。范围为1-65535。

15. 输入探测数据包的大小。

默认值为0。范围为0到39936。

16. 输入发送回显请求数据包时要使用的源IP地址或接口。

如果不需要源，请选择“无”作为源选项。可能的值如下所示：

- **None.** ping数据包的源地址将是默认传出接口的地址。

- **IP Address.** 发送回显请求数据包时要使用的源IP地址。当选择IP地址作为源选项时，将显示此字段。
- **Interface.** 发送回显请求数据包时要使用的接口。当选择接口作为源选项时，将显示此字段。

提示： 此屏幕中字段中配置的值不会保存到交换机。因此刷新屏幕会将这些字段设置为默认值。

17. 单击 **应用** 按钮

跟踪路由请求被发送到指定的IP地址或主机名。结果显示在跟踪路由结果区域的可配置数据下方。

结果字段显示交换机向指定的IP地址或主机名发送跟踪路由请求后的跟踪路由IPv4结果。

7.7.4. Traceroute IPv6

使用此屏幕告知交换机向指定的IPv6地址或主机名发送跟踪路由请求。您可以使用它来发现数据包到远程目标的路径。单击“应用”按钮后，交换机将发送一个跟踪路由，结果显示在可配置数据下方。

如果收到对跟踪路由的回复，将显示以下消息：

```
1 a:b:c:d:e:f:g 9869 usec 9775 usec 10584 usec
2 0:0:0:0:0:0:0:0 0 usec * 0 usec * 0 usec *
Hop Count = p Last TTL = q Test attempt = r Test Success = s.
```

要使用Traceroute IPv6，请执行以下操作：

1. 使用192.168.10.0子网中的静态IP地址准备您的计算机，例如 192.168.10.101。
2. 将以太网电缆从计算机上的以太网端口连接到交换机上的以太网端口。
3. 启动web浏览器。
4. 在web浏览器地址字段中输入交换机的IP地址。

交换机的默认IP地址为 192.168.10.12 。

此时将显示登录屏幕。

5. 输入用户名和密码。
默认管理员用户名为 **admin** ，默认管理员密码为空，即不要输入密码。
6. 单击 **登录** 按钮。

将显示web管理界面菜单。

7. 单击 **维护 > 诊断工具 > Traceroute IPv6**

Traceroute IPv6 -	
目的IPv6地址或主机名称	(IPv6 address/Max 255 characters)
Probes Per Hop	(1-10)
MaxTTL	(1-255)
InitTTL	(1-255)
MaxFail	(1-255)
间隔(秒)	(1-60)
端口号	(1 to 65535)
数据包长度	(0 to 39936)
选择源接口	None ▼
输出结果:	

8. 在IPv6地址/主机名字段中，输入希望交换机查找路径的站点的IPv6地址或主机名。

初始值为空。您输入的IPv6地址或主机名不会在整个上电工作周期内保留。

9. **Probes Per Hop**，输入每跳的探测数。

默认值为3。范围为1到10。

10. **Maximum TTL**，输入目标的最大TTL。

默认值为30。范围为1到255。您输入的MaxTTL不会在整个电源循环中保留。

11. **Initial TTL**，输入要使用的初始TTL。

默认值为1。范围为1到255。您输入的InitTTL不会在整个电源循环中保留。

12. **Maximum Failures**，输入会话中允许的最大失败次数。

默认值为5。范围为1到255。您输入的MaxFail不会在整个电源循环中保留。

13. **间隔（秒）**-以秒为单位输入探测之间的时间。

默认值为3。范围为1到60。您输入的间隔不会在整个电源循环中保留。

14. 在探测数据包中输入UDP目标端口。

默认值为33434。范围为1-65535。您输入的端口不会在整个电源循环中保留。

15. 输入探测数据包的大小。

默认值为0。范围为0到39936。您输入的大小不会在整个电源循环中保留。

16. 输入发送回显请求数据包时要使用的源IP地址或接口。

如果不需要源，请选择“无”作为源选项。可能的值如下所示：

- **None.** ping数据包的源地址将是默认传出接口的地址。
- **IP Address.** 发送回显请求数据包时要使用的源IP地址。当选择IP地址作为源选项时，将显示此字段。

- **Interface.** 发送回显请求数据包时要使用的接口。当选择接口作为源选项时，将显示此字段。

提示： 此屏幕中字段中配置的值不会保存到交换机。因此刷新屏幕会将这些字段设置为默认值。

17. 单击 **应用** 按钮

traceroute 开始运行，结果显示在跟踪路由区域中。

结果字段显示交换机向指定的IP地址或主机名发送跟踪路由请求后的跟踪路由IPv6结果。

8. 默认设置

此附录描述了管理型交换机软件功能中常用参数的默认设置。

表100. 默认设置

Feature	Default
IP address	192.168.10.12
Subnet mask	255.255.255.0
Default gateway	0.0.0.0
Protocol	DHCP
Management VLAN ID	1
Minimum password length	Eight characters
IPv6 management Mode	None
SNTP client	Disabled
SNTP server	Not configured
Global logging	Enabled
CLI command logging	Disabled
Console logging	Enabled (Severity level: debug and above)
RAM logging	Enabled (Severity level: debug and above)
Persistent (FLASH) logging	Disabled
DNS	Enabled (No servers configured)
SNMP	Enabled (SNMPv1/SNMPv2, SNMPv3)
SNMP Traps	Enabled

表101. 默认设置

Feature	Default
sFlow	Disabled
ISDP	Disabled(Versions 1 and 2)
RMON	Enabled
TACACS	Not configured
RADIUS	Not configured
SSH/SSL	Disabled
Telnet	Enabled
Denial of Service Protection	Disabled
Captive Portal	Disabled
Dot1x Authentication (IEEE 802.1X)	Disabled
MAC-based port security	All ports are unlocked
Access control lists (ACL)	None configured
IP source guard (IPSG)	Disabled
DHCP snooping	Disabled
Dynamic ARP inspection	Disabled
Protected ports	None
Private groups	None
Flow control support (IEEE 802.3x)	Disabled
Head of line blocking prevention	Disabled
Maximum frame size	1518 bytes
Auto-MDI/MDIX support	Enabled
Auto-negotiation	Enabled
Advertised port speed	Maximum Capacity
Broadcast storm control	Disabled
Port mirroring	Disabled
LLDP	Disabled
LLDP-MED	Disabled
MAC table address aging	300 seconds (dynamic addresses)

表102. 默认设置

Feature	Default
DHCP Layer 2 relay	Disabled
Default VLAN ID	1
Default VLAN name	Default
GVRP	Disabled
GARP timers	Leave: 60 centiseconds Leave All: 1000 centiseconds Join: 20 centiseconds
Voice VLAN	Disabled
Guest VLAN	Disabled
RADIUS-assigned VLANs	Disabled
Double VLANs	Disabled
Spanning Tree Protocol (STP)	Enabled
STP operation mode	IEEE 802.1s RSTP
Optional STP features	Disabled
STP bridge priority	32768
Multiple Spanning Tree	Disabled
Link aggregation	No Link Aggregation Groups (LAGs) configured
LACP system priority	1
Routing mode	Disabled
IP helper and UDP relay	Disabled
Tunnel and loopback interfaces	None
DiffServ	Enabled
Auto VoIP	Disabled
Auto VoIP traffic class	6
MLD snooping	Disabled
IGMP snooping	Disabled
IGMP snooping querier	Disabled
GMRP	Disabled

9. 配置例子参考

本附录包含有关如何配置以下功能的信息：

- *Virtual Local Area Networks (VLANs)*
- *Access Control Lists (ACLs)*
- *Differentiated Services (DiffServ)*
- *802.1X*
- *MSTP*

9.1. 虚拟局域网 (VLANs)

9.1.1. VLAN配置示例

这个例子演示了VLAN使用的几个场景，并描述了交换机如何处理带标签和不带标签的流量。

在本例中，创建了两个新的VLAN，将端口的隶属关系修改为缺省的VLAN 1，并为两个VLAN分配端口成员：

1.在“Basic VLAN Configuration”界面(参见195页的“Configure VLANs”)，新建以下VLAN：

- VLAN ID为10。

- VLAN ID为20。

2.在“VLAN Membership”界面(参见201页的“Configure VLAN Membership”)中指定VLAN的成员关系，如下所示：

- 对于VLAN ID为1的缺省VLAN，需要指定7 (U)和8 (U)两个成员端口。

- VLAN ID为10的VLAN，需指定以下成员：端口1 (U)、端口2 (U)、端口3 (T)。

- VLAN ID为20的VLAN，指定4 (U)口、5 (T)口、6 (U)口为成员。

3.在“Port PVID Configuration”界面(参见204界面的“Configure Port PVID Settings”)，设置g1、g4端口的PVID，使进入这些端口的报文带有该端口的VLAN ID标记：

- 端口g1: PVID 10

- 端口g4: PVID 20

4.通过配置VLAN，会出现如下两种情况：

- 如果不带tag的报文进入端口1，则交换机将其标记为VLAN ID 10。报文可以访问端口2和端口3。发送的数据包被剥去标记，以离端口2作为一个无标记的数据包。对于端口3，出方向报文为tagged报文，VLAN ID为10。

- 如果VLAN ID为10的报文进入端口3，则该报文可以访问端口1和端口2。如果数据包离端口1或端口2，它的标签被剥离，作为一个untagged数据包离开交换机。

- 如果不带tag的报文进入端口4，则交换机将其标记为VLAN ID 20。报文可以访问端口5和端口6。传出的数据包在离端口6时去掉它的标记，成为一个untagged数据包。对于端口5，发送VLAN ID为20的tag报文。

9.2. Access Control Lists (ACLs)

acl确保只有授权的用户可以访问特定的资源，同时阻止任何不正当的尝试访问网络资源。

acl的作用是对流量进行控制，限制路由更新的内容，决定哪些类型的流量可以转发或阻止，为网络提供安全保障。acl通常用于位于内部网络和外部网络(如Internet)之间的防火墙路由器。它们也可以用于位于网络的两个部分之间的路由器，以控制进入或流出内部网络的特定部分的流

量。ACL特性需要增加的报文处理不会影响交换机性能。也就是说，ACL处理以线速进行。

访问列表是允许和拒绝条件的顺序集合。这些条件集合被称为过滤条件，应用于交换机或路由器处理的每个包。数据包的转发或丢弃取决于数据包是否匹配指定的条件。

流量过滤需要以下两个基本步骤：

1. 创建一个访问列表定义。

访问列表定义包括指定符合条件的流量是正常转发还是丢弃的规则。此外，您可以将符合条件的流量分配到特定队列，或将流量重定向到特定端口。默认的deny all规则是每个列表的最后一条规则。

2. 在入方向应用访问列表。

支持acl绑定物理端口和lag。交换机软件支持MAC acl和IP acl。

9.2.1. MAC ACL Sample Configuration

下面的示例展示了如何创建基于mac的ACL，允许来自Sales部门的以太网流量通过指定端口，并拒绝这些端口上的所有其他流量。

1. 在MAC ACL屏幕上，为您的网络的销售部门创建一个名为Sales_ACL的ACL(参见第649页上的Configure a Basic MAC ACL)。

默认情况下，该ACL在入方向上绑定，这意味着交换机将在进入端口时检查流量。

2. 在MAC Rules屏幕中，使用以下设置为Sales_ACL创建一个规则：

- ID: 1
- Action: Permit
- Assign Queue ID: 0
- Match Every: False
- CoS: 0
- Destination MAC: 01:02:1A:BC:DE:EF
- Destination MAC Mask: 00:00:00:00:FF:FF
- EtherType User Value:
- Source MAC: 02:02:1A:BC:DE:EF
- Source MAC Mask: 00:00:00:00:FF:FF
- VLAN ID: 2

有关MAC ACL规则的更多信息，请参见651页的“配置MAC ACL规则”。

3. 在MAC Binding Configuration屏幕中，将Sales_ACL分配给接口千兆端口6、7和8，然后单击Apply按钮。(请参见配置MAC绑定

654页。)

如果已经为该接口和方向分配了访问列表，可以分配一个可选的序号来指示该访问列表相对于

其他访问列表的顺序。

4.“MAC绑定表”显示接口和MAC ACL绑定信息(请参见655页“MAC绑定表”中的“查看或删除MAC ACL绑定信息”)。

名为Sales_ACL的ACL查找规则中定义的目标、源MAC地址和MAC掩码的以太网帧。此外，框架必须使用VLAN ID 2进行标记，这是销售部门的VLAN。帧的CoS值必须为0，为以太网帧的缺省值。符合此条件的帧被允许在接口6、7和8上，并被分配给硬件出口队列0，这是默认队列。在这些接口上显式拒绝所有其他流量。如果需要允许更多的流量进入这些端口，则需要在接口6、7、8上添加一条新的permit规则，并匹配相应的匹配条件。

9.2.2. Standard IP ACL Sample Configuration

以创建基于IP的ACL为例，在与其他部门关联的端口上不允许来自Finance部门的IP流量。来自财务部门的流量由每个包的网路IP地址识别。

1. 在“IP ACL”界面中，创建一个新的IP ACL, IP ACL ID为1(参见656页的“Configure an IP ACL”)。
2. 在“IP规则”界面中，创建ACL 1的规则，设置如下：
 - Rule ID: 1
 - Action: Deny
 - Assign Queue ID: 0 (optional: 0 is the default value)
 - Match Every: False
 - Source IP Address: 192.168.187.0
 - Source IP Mask: 255.255.255.0

关于IP ACL规则的更多信息，请参见658页的“配置IP ACL规则”。

3. 单击 **增加** 按钮
4. 在“IP规则”界面中，使用以下设置为IP ACL 1创建第二条规则：
 - Rule ID: 2
 - Action: Permit
 - Match Every: True
5. 单击 **增加** 按钮
6. 在“IP Binding Configuration”界面中，为千兆端口2、3、4分配ACL号1，并分配序号1(参见671页的“Configure IP ACL interface Bindings”)。

缺省情况下，该IP ACL在入方向绑定，因此在流量进入交换机时进行检测。

7. 单击 **应用** 按钮
8. 使用“IP Binding Table”界面可以查看接口和IP ACL绑定信息

在673页的“IP ACL绑定表”中查看或删除IP ACL绑定。

本例中的IP ACL匹配财务部门网络的源IP地址和子网掩码，并在交换机的以太网接口2、3、4上deny源IP地址和子网掩码。第二条规则允许端口上的所有非金融流量。第二个规则是必需的，因为有一个显式的deny all规则作为优先级最低的规则。

9.2.3. DiffServ Example Configuration

要创建一个DiffServ类/策略并将其附加到交换机接口，请遵循以下步骤：

1. 在QoS Class Configuration屏幕中，使用以下设置创建一个新类：

- Class Name: Class1
- Class Type: All

有关此屏幕的更多信息，请参见第526页的配置DiffServ类。

2. 单击Class1超链接以查看该类的DiffServ Class Configuration屏幕。

3. 对Class1进行以下设置：

- Protocol Type: UDP
- Source IP Address: 192.12.1.0
- Source Mask: 255.255.255.0
- Source L4 Port: Other, and enter 4567 as the source port value
- Destination IP Address: 192.12.2.0
- Destination Mask: 255.255.255.0
- Destination L4 Port: Other, and enter 4568 as the destination port value

有关此屏幕的更多信息，请参见第526页的配置DiffServ类。

4. 单击 **应用** 按钮

5. 在Policy Configuration界面中，使用以下设置创建一个新策略：

- Policy Selector: Policy1
- Member Class: Class1

有关此屏幕的更多信息，请参见第533页的Configure DiffServ Policy。

6. 单击 **增加** 按钮

The policy is added.

7. 单击Policy1超链接，查看该策略的“Policy Class Configuration”界面。

8. 配置策略属性如下：

- Assign Queue: 3
- Policy Attribute: Simple Policy
- Color Mode: Color Blind
- Committed Rate: 1000000 Kbps
- Committed Burst Size: 128 KB
- Confirm Action: Send
- Violate Action: Drop

有关此屏幕的更多信息，请参见第533页的Configure DiffServ Policy。

9. 在Service Configuration屏幕中，选择接口g7和g8旁边的复选框，将策略附加到这些接口，

然后单击**Apply**按钮。(参见536页配置DiffServ业务接口)

所有的UDP包流向192.12.2.0网络与IP源地址从

包括该交换机端口7和8上的源端口4567和目的端口4568的第4层192.12.1.0网络被分配给硬件队列3。

在这个网络中，来自流应用程序的流量使用UDP端口4567作为源，4568作为目的。这个实时流量是时间敏感的，所以它被分配给

高优先级硬件队列。默认情况下，数据流量使用硬件队列0，该队列被指定为最佳努力队列。

对该流确认的动作是发送承诺速率为1000000 Kbps、突发大小为128kb的数据包。违反承诺速率和突发大小的数据包将被丢弃。

9.3.802.1X

局域网(Local Area network, LAN)通常部署在这样的环境中:允许未经授权的设备在物理上连接到LAN基础设施，或允许未经授权的用户试图通过已经连接的设备访问LAN。在这种环境中，您可能希望将对LAN提供的服务的访问限制为允许使用这些服务的用户和设备。

出口网络访问控制利用物理特性的局域网基础设施提供身份验证和授权的设备连接到一个局域网端口,点对点的连接特点和防止访问端口的情况下,身份验证和授权过程失败。在这种情况下，端口是一个连接到局域网的单一点，例如IEEE 802.11无线局域网中MAC桥和站之间的关联或接入点的端口。

IEEE 802.11标准描述了一个体系结构框架，在该框架内进行身份验证和相应的操作。它还建立了验证者(向验证服务器传递验证请求的系统)和被验证者(请求验证的系统)之间以及验证者和验证服务器之间的协议需求。

被管理交换机支持guest VLAN，允许未经认证的用户访问网络资源。

提示： 通过QoS特性对guest VLAN进行限速，限制guest VLAN提供的网络资源。

802.1X的另一个特性是配置端口来启用/禁用EAPoL报文转发支持。当设备802.1X未启用时，可以启用或禁用EAPoL转发功能。

802.1X身份验证交换机的端口提供了一种方式，使其能够向通过局域网可达的其他系统提供服务。基于端口的网络访问控制允许对交换机端口的操作进行控制，以确保对其服务的访问只被授权的系统允许。

端口访问控制提供了一种防止请求者对系统提供的服务进行未经授权的访问的方法。当您限制对公共可访问的桥接端口的访问或限制对部门局域网的访问时，控制对交换机和所连接的局域网的访问是可取的。

访问控制是通过强制验证附加到验证者的受控端口的请求者的身份验证来实现的。身份验证过程的结果决定了请求者是否被授权访问该受控制端口上的服务。

端口访问实体(PAE)能够在访问控制交互中采用两个不同的角色之一：

1. **Authenticator:**在允许访问通过该端口可用的服务之前强制进行身份验证的端口。
2. **Supplicant:** 试图访问验证者提供的服务的端口的端口。此外，还有第三个角色：
3. **Authentication server:**

代表验证方执行必要的验证功能，以检查被验证方的凭证。

您需要这三个角色才能完成身份验证交换。

被管理交换机只支持**Authenticator**角色，其中PAE负责与被管理交换机的通信。验证者PAE还负责将从被验证者接收到的信息提交给验证服务器，以便检查凭据，这将确定端口的授权状态。

Authenticator PAE根据基于radius的认证过程的结果控制被控端口的授权/未授权状态。

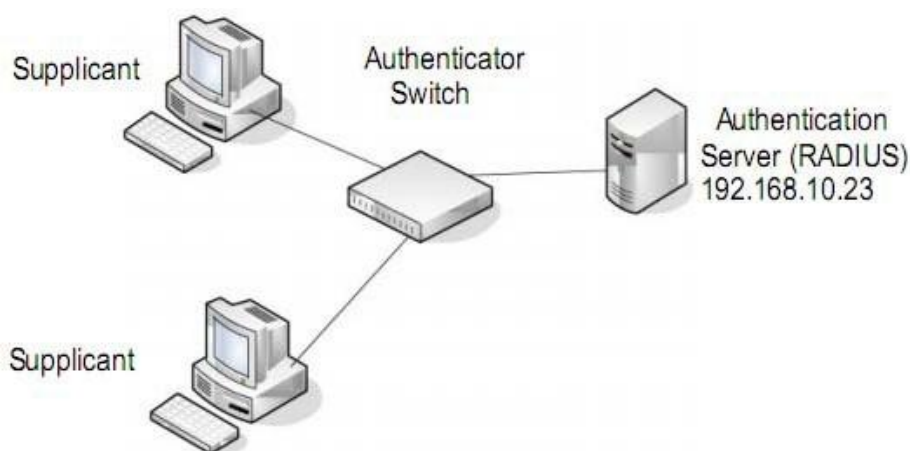


Figure 1. 802.1X Authentication Roles

9.3.1. 802.1X Example Configuration

本举例以企业会议室(1/0/5 ~ 1/0/8)为例，通过交换机配置实现端口802.1 x认证。这些端口对访问者是可用的，在授予对网络的访问权之前必须进行身份验证。认证由外部RADIUS服务器处理。访问者认证通过后，流量自动分配到guest VLAN。本例中假设VLAN ID为150,VLAN Name为Guest。

1.在“Port Authentication”界面中，选择端口1/0/5、1/0/6、1/0/7和1/0/8。

2.从“端口控制”菜单中选择“未授权”。

不需要身份验证的所有其他端口的端口控制设置应该是授权的。当“端口控制”设置为“授权”时，该端口将无条件地处于强制授权状态，不需要任何身份验证。当“Port Control”设置为“Auto”时，验证方PAE设置被控制端口模式

3.在1/0/5—1/0/8端口的Guest VLAN字段中，输入150，将该端口加入到Guest VLAN中。

您可以配置额外的设置来控制通过端口对网络的访问。有关设置的信息，请参见598页的配置端口安全接口。

1. 单击 **应用** 按钮
2. 在802.1X配置界面，将Port Based Authentication State和Guest VLAN模式设置为Enable，然后Apply按钮(参见第597页的Configure the Global Port Security mode)。

本例使用端口身份验证设置的默认值，但是您还可以配置其他几个设置。例如，EAPOL Flood Mode字段可以在设备禁用802.1X时使能EAPOL帧的转发。

3. 在“RADIUS服务器配置”界面中，可以进行以下设置：

- Server Address: 192.168.10.23
- Secret Configured: Yes
- Secret: secret123
- Active: Primary

要了解更多信息，请参见第545页的RADIUS概述。

4. 单击 **增加** 按钮

5. 在“认证列表”界面，配置默认列表，使用RADIUS作为第一种认证方式(参见第555页的“配置登录认证列表”)。

本例以L2+交换机为例，开启802.1 x端口安全，提示g5-g8端口连接的主机进行802.1 x认证为例。交换机将认证信息传递给配置好的RADIUS服务器。

9.4.MSTP

生成树协议STP (Spanning Tree Protocol)运行在网桥网络上，有助于消除环路。如果发生桥接环路，网络可能会被流量淹没。IEEE 802.1 MSTP (Multiple Spanning Tree Protocol)支持通过生成树的多个实例，在不同的接口上高效地引导VLAN流量。生成树的每个实例都按照IEEE 802.1w，快速生成树中规定的方式运行，在工作中有微小的变化，但没有结束效应(主要的影响是端口快速过渡到转发状态)。

RSTP与传统STP (IEEE 802.1D)的区别在于能够配置和识别全双工连接和连接到端站的端口，从而导致端口快速过渡到转发状态，并抑制拓扑变化通知。这些特征由参数pointtpoint和edgeport表示。MSTP兼容RSTP和STP两种协议。它的行为适合于STP和RSTP桥。

MSTP桥可以配置为完全像RSTP桥或STP桥那样运行。因此，IEEE 802.1桥接本身也支持IEEE 802.1w和IEEE 802.1D。

MSTP算法和协议为在一个由任意互连的网络设备组成的桥接局域网(每个运行的MSTP、STP或RSTP)中分配给任何给定VLAN的帧提供简单和完整的连接。MSTP允许分配给不同vlan的帧在由局域网和MSTP桥组成的MST (Multiple Spanning Tree)区域内沿着不同的路径运行，每个路径基于一个独立的MSTI (Multiple Spanning Tree Instance)。这些区域与其他网桥和局域网连接到一个单一的公共生成树(CST)。[IEEE P802.1s草案/ D13]

MSTP用一棵公共和内部生成树(CIST)连接所有的网桥和局域网。CIST支持自动确定每个MST区域，选择其最大可能范围。为CIST计算的连通性提供了这些区域之间互连的CST，以及每个区域内的内部生成树IST (Internal Spanning Tree)。MSTP确保帧与给定的VLAN ID分配给一个且只有一个MSTIs或者是地区内的分配是一致的在所有的网络设备在该地区的稳定连接每个MSTI和坚持的边界地区春秋国旅的匹配。根据IEEE DRAFT P802.1s/D13，尽管属于不同VLAN的帧可以在任何区域内采取不同的路径，但桥接局域网的稳定活跃拓扑结构可以将始终属于任何给定VLAN的帧简单而完整地连接整个网络中的所有LAN和网络设备。

所有的网桥，无论是使用STP、RSTP还是MSTP，都通过bpdu (Bridge Protocol Data unit)以配置消息的形式发送信息，以一个或多个生成树为基础，分配端口角色，决定每个端口在全连接

和简单连接的活动拓扑中的参与程度。所传递的信息称为生成树优先级向量。这些不同协议的BPDU结构是不同的。MSTP桥将根据从特定端口接收到的BPDU类型传输相应的BPDU。

一个MST域由一个或多个MSTP桥组成，这些桥具有相同的MST配置标识符，使用相同的msti，并且没有连接任何不能接收和发送MSTP bpdu的桥。MST配置标识符由以下组成：

1. 配置标识符格式选择器
2. 配置名称
3. 配置修订版本
4. 配置摘要:从MST配置表创建的HMAC-MD5类型的16字节签名(VLAN ID到MSTID的映射)

由于存在生成树的“多实例”，所以存在一种基于每个端口、每个实例的MSTP状态(或者基于每个端口、每个VLAN的状态:任何VLAN都可以且只能存在于一个MSTI或CIST中)。例如，端口A可以转发实例1，而丢弃实例2。端口状态自IEEE 802.1D规范以来发生了变化。

为了支持多生成树，MSTP桥必须为生成树分配明确的VLAN id (vid)。这是通过：

1. 确保将vid分配给fid是明确的。
2. 确保Bridge支持的每个FID都被分配给一个生成树实例。

VID到FID再到FID到MSTI的组合，定义了一个VID到生成树实例的映射，由MST配置表表示。

通过这种分配，我们确保每个VLAN被分配给一个且仅一个MSTI。CIST也是生成树的实例，MSTID为0。

一个实例可能没有分配vid，但是每个VLAN必须分配给生成树的其他实例之一。

连接同一MST域内任意两个网桥的活跃网络拓扑只穿越该区域内的MST网桥和局域网，而不穿越该区域以外的任何类型的网桥，也就是说，区域内的连接是独立于外部连接的。

9.4.1. MSTP Example Configuration

本例介绍如何在L2+交换机交换机上创建一个MSTP实例。示例网络中有三个不同的交换机，它们服务于网络中的不同位置。在本例中，端口1/0/1 ~ 1/0/5连接到主站点，因此这些链路不受网络环路的影响。端口1/0/6 ~ 1/0/8分别连接交换机1、2、3。

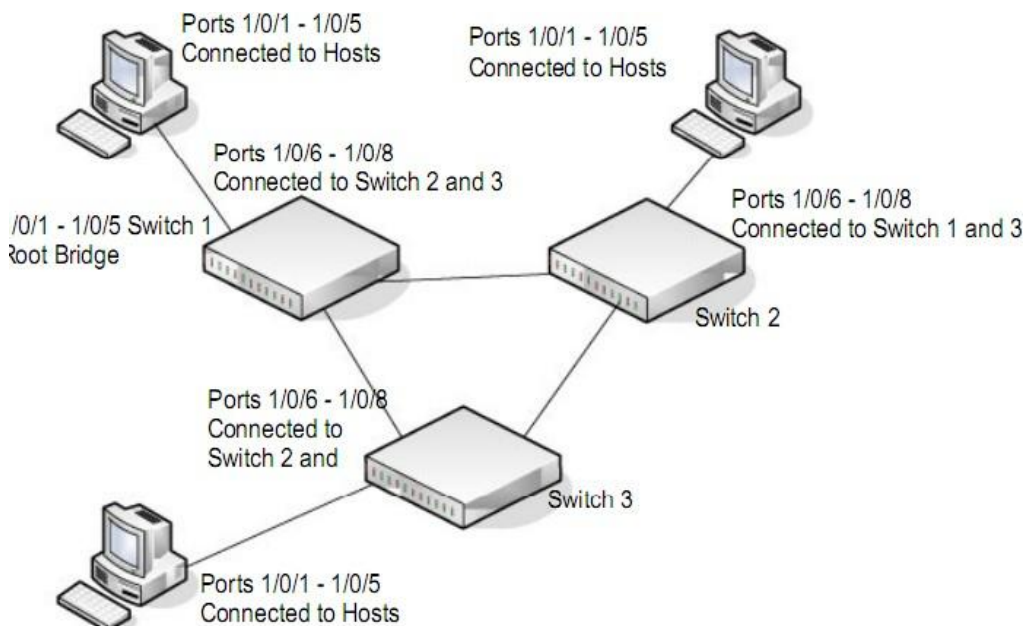


Figure 2. MSTP sample configuration

Perform the following procedures on each switch to configure MSTP:

1. 通过“VLAN Configuration”界面创建VLAN 300和VLAN 500(参考195页的“Configure Basic VLAN Settings”)。
2. 使用VLAN Membership界面将端口1/0/1 /0/8包括为tagged (T)或untagged (U) VLAN 300和VLAN 500的成员(参见195页的“配置基本VLAN设置”)。
3. 在“STP Configuration”界面中, 启用生成树状态选项(参见231页的“Configure Advanced STP Settings”)。

其余配置请使用缺省值。缺省情况下, STP的“操作模式”为“MSTP”, “配置名称”为交换机的MAC地址。

4. 在CST Configuration界面, 设置三个交换机的Bridge Priority值, 强制Switch 1为根桥:
 - Switch 1: 4096
 - Switch 2: 12288
 - Switch 3: 20480

提示: Bridge priority values are multiples of 4096.

如果不指定根桥, 且所有交换机具有相同的桥优先级, 则MAC地址最低的交换机将被选为根桥(参见234页的“配置CST设置”)。

5. 在“CST Port Configuration”界面中选择端口1/0/1 ~ 1/0/8, 并在“STP Status”菜单中选择“Enable”(参见236页的“Configure CST Port Settings”)。
6. 单击 **应用** 按钮
7. 单击港口1/0/1-1/0/5(边缘端口),从快速链接菜单中选择启用。

由于边缘端口没有网络环路的风险, 启用了Fast Link的端口直接过渡到Forwarding状态。

8. 单击 **应用** 按钮

通过“CST端口状态”界面, 可以查看各端口的生成树信息。

9. 在MST Configuration界面中, 使用以下设置创建MST实例:
 - MST ID: 1
 - Priority: Use the default (32768)
 - VLAN ID: 300

For more information, see *Configure MST Settings* on page 240.

10. 单击 **增加** 按钮
11. Create a second MST instance with the following settings
 - MST ID: 2
 - Priority: 49152

- VLAN ID: 500

12. 单击 **增加** 按钮

假设交换机1已经成为MST实例1的根桥，交换机2已经成为MST实例2的根桥。Switch 3在销售部门(端口1/0/1、1/0/2和1/0/3)和HR部门(端口1/0/4和1/0/5)中都有主机。交换机1和2还包括销售和人力资源部门的主机。交换机2上连接的主机使用VLAN 500、MST实例2直接与交换机3上的主机通信。同样，交换机1上的主机使用VLAN 300，即MST实例1直接与交换机3上的主机通信。

主机使用不同的MSTP实例来有效地使用交换机之间的链路。同样的概念可以扩展到其他交换机和更多的MSTP实例。

10. 缩略语

在大多数情况下，缩写词和缩写在本文档中首次使用时进行定义。下表还定义了缩写词和缩写。

表103. 缩略语

Acronym	Definition
802.1x	IEEE 802.1x Authentication Protocol Standard
ACE	Access Control Entry
ACL	Access Control List
API	Application Programming Interface
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
CLI	Command Line Interface
CoS	Class of Service
Default Gateway	The IP address of a router that a host can use as its first hop when the host does not know a more specific route to a given destination.
Default Route	A manually configured (<i>static</i>) route whose destination is 0.0.0.0/0.0.0.0 and therefore matches every packet's destination. A router uses a default route to forward packets that do not match a more specific route.
DHCP	Dynamic Host Configuration Protocol (RFC 2131, RFC3315). A mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DHCP Server	Dynamic Host Configuration Protocol Servers are servers that grant the address and do parameter assignment to requested clients in the network. Current interest is that these servers provide TFTP server and boot file information.
DLL	Data Link Layer
DNS Server	Domain Name 系统管理 servers that provide the IP address mapping to the name of the hosts.
DSCP	Differentiated Services Code Point

表104. 缩略语

Acronym	Definition
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
ECMP	Equal Cost Multiple Paths
EEE	Energy Efficient Ethernet (from the IEEE 802.3az Energy Efficient Ethernet Task Force and IEEE 802.3az Energy Efficient Ethernet Study Group).
Host Interface	An IP interface that is not a routing interface. Only locally-originated packets are sent on a host interface. Only packets with a local destination are received. Host interfaces do not participate in dynamic routing protocols.
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internal Authentication Server
IGMP	Internet Group Management Protocol
In-band Interface	An IP interface that could be used for in-band management. Any IP interface other than the Out-of-Band port.
IP	Internet Protocol
IP Address Owner	The VRRP router that has the virtual router's IP address(es) as real interface address(es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, and so on
IP Interface	An interface configured as an IP interface rather than a Layer 2 switching interface. An IP interface must be assigned one or more IP addresses. Also called a <i>Layer 3 interface</i> .
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISDP	Industry Standard Discovery Protocol
ISID	Initiator-defined session identifier
L2	Layer 2 (networking)
L3	Layer 3 (networking)
LAG	Link Aggregation Group (IEEE standard)
LLDP	Link Layer Discovery Protocol
Local Route	A route to an attached subnet. A router creates a local route for each active, locally-configured IP address and uses the local route to reach other stations on the attached subnet.
LPI	Low-power Idle
MAB	MAC Authentication Bypass

表105. 缩略语

Acronym	Definition
MAC	Media Access Control
Management Interface	An external IP interface used to send and receive IP packets to configure and monitor the device.
Management VLAN	A VLAN configured to be used for management rather than control or data traffic.
MFDB	Multicast Forwarding Database
MIB	Management Information Base
MLAG	Multi-chassis Link Aggregation
MPLS	Multiprotocol Label Switching: A standard involving IP quality.
MVR	Multicast VLAN Registration
N/A	not applicable
NSF	Nonstop Forwarding
PAE	Port Access Entity
PDU	Protocol Data Unit
PIM-DM	Protocol-Independent Multicast Dense mode
PIM-SM	Protocol-Independent Multicast Sparse mode
Primary IP Address	An IP address selected from the set of real interface addresses. One possible selection algorithm is to always select the first address. VRRP advertisements are always sent using the primary IP address as the source of the IP packet.
PoE	Power over Ethernet. Corresponds to the IEEE 802.3AF standard which supports power delivery of up to 15.4W per port.
PoE+	Power over Ethernet Plus. Corresponds to the IEEE 802.3AT standard which supports power delivery of up to 34.2W per port.
PSE	Power Sourcing Equipment
QoS	Quality of Service
RADIUS	Remote Authentication Dial-in User Service
Routing Interface	An IP interface whose physical ports are front panel ports and associated with a VLAN. Packets received on a routing interface can be transmitted on a different VLAN than they were received on.
SDM	Switch Database Management
Service Port	An IP interface on an Ethernet interface that is separate from the front panel ports. The service port is dedicated to management. The service port has its own independent interface to the IP stack. The service port is a host interface.
SM	state machine

表106. 缩略语

Acronym	Definition
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
TFTP	Trivial File Transfer Protocol
TFTP Server	Trivial File Transfer Protocol Servers are servers that hold the requested configuration and/or image files for requested clients.
TLV	Type-Length-Value
UDLD	Uni-Directional Link Detection
UI	User Interface
UPoE	Universal Power over Ethernet. No IEEE standard exists yet for UPoE. NETGEAR UPoE supports power delivery of up to 60W per port.
USB	Universal Serial Bus
Virtual Router	An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a virtual router identifier and a set of associated IP address(es) across a common LAN. A VRRP router can backup one or more virtual routers
Virtual Router Backup	The set of VRRP routers available to assume forwarding responsibility for a virtual router if the current Master fails.
Virtual Router Master	The VRRP router that is assuming the responsibility of forwarding packets sent to the IP address(es) associated with the virtual router, and answering ARP requests for these IP addresses. Note that if the IP address owner is available, then it will always become the Master.
VLAN	Virtual Local Area Network
VRRP Router	A router running the Virtual Router Redundancy Protocol. It can participate in one or more virtual routers.