SUNDRAY
信锐技术

CLI Reference Guide
命令行手册

SW-5024 v2.0

目录

手册概述

本手册提供 CLI（Command Line Interface,命令行界面）参考信息，适用于 SW-5024 交换机。

各章节内容安排如下：

第 1 章：命令行使用指导

主要介绍 CLI 的使用方法、命令行模式、使用命令行、命令行分级及命令行格式约定。

第 2 章：用户界面

主要介绍用户登录和退出操作模式的相关配置命令。

第 **3 章：IEEE 802.1Q VLAN 配置命令**

主要介绍 IEEE 802.1Q VLAN 的相关配置命令。

第 **4 章：MAC VLAN 配置命令**

主要介绍 MAC VLAN 的相关配置命令。

第 5 章：协议 VLAN 配置命令

主要介绍协议 VLAN 的相关配置命令。

第 **6 章：VLAN-VPN 配置命令**

主要介绍 VLAN-VPN 的相关配置命令。

第 **7 章：Private VLAN 配置命令**

主要介绍 Private VLAN 功能的相关配置命令。

第 8 章：L2PT 配置命令

主要介绍 L2PT 功能的相关配置命令。

第 9 章：GVRP 配置命令

主要介绍 GVRP 的相关配置命令。

第 10 章：语音 VLAN 的配置命令

主要介绍语音 VLAN 的相关配置命令。

第 **11 章：Etherchannel 配置命令**

主要介绍端口汇聚和 LACP 的相关配置命令。

第 **12 章：用户管理配置命令**

主要介绍用户管理信息的相关配置命令。

第 **13 章：HTTP 和 HTTPS 配置命令**

主要介绍交换机 HTTP 和 HTTPS 管理服务的相关配置命令。

第 14 章：ARP 配置命令

主要介绍 ARP 的相关配置命令。

第 15 章：绑定列表配置命令

主要介绍 IPv4-MAC-VID-PORT 四元绑定表的相关配置命令。

第 16 章：IPv6 绑定列表配置命令

主要介绍 IPv6-MAC-VID-PORT 四元绑定表的相关配置命令。

第 17 章：IP 源防护配置命令

主要介绍 IP 源防护的相关配置命令。

第 18 章：IPv6 源防护配置命令

主要介绍 IPv6 源防护的相关配置命令。

第 19 章：ARP 防护配置命令

主要介绍 ARP 防护的相关配置命令。

第 20 章：DoS 防护命令

主要介绍 DoS 防护和攻击检测的相关配置命令。

第 **21 章：IEEE 802.1X 配置命令**

主要介绍 IEEE 802.1X 认证的相关配置命令。

第 **22 章：PPPoE 的 ID 嵌入配置命令**

主要介绍 PPPoE 的 ID 嵌入的相关配置命令。

第 23 章：系统配置命令

主要介绍系统信息、网络参数配置，系统软件复位，系统文件升级，交换机重启及连通性测试等系统相关配置命令。

第 24 章：SSH 配置命令

主要介绍 SSH 配置管理的相关命令。

第 **25 章：地址配置命令**

主要介绍端口安全设置和地址表管理的相关配置命令。

第 **26 章：系统配置命令**

主要介绍系统信息、网络参数配置，系统软件复位，系统文件升级，交换机重启及连通性测试等系统相关配置命令。

第 27 章：IPv6 地址配置命令

主要介绍 IPv6 地址相关配置命令。

第 28 章：以太网配置命令

主要介绍以太网端口的流量控制、协商模式、风暴抑制、带宽限制的相关配置命令。

第 29 章：QoS 配置命令

主要介绍 QoS（服务质量）的相关配置命令。

第 **30** 章：**端口监控配置命令**

主要介绍端口监控的相关配置命令。

第 **31** 章：**端口隔离配置命令**

主要介绍端口隔离的相关配置命令。

第 **32** 章：**环路监测配置命令**

主要介绍环路监测的相关配置命令。

第 33 章：ACL 配置命令

主要介绍访问控制的相关配置命令。

第 **34** 章：**MSTP 配置命令**

主要介绍生成树配置的相关配置命令。

第 **35** 章：**Ethernet OAM 配置命令**

主要介绍 Ethernet OAM 的相关配置命令。

第 **36** 章：**DLDP 配置命令**

主要介绍 DLDP 的相关配置命令。

第 37 章：IGMP 侦听配置命令

主要介绍 IGMP 侦听、组播地址表管理、组播过滤等组播管理相关配置命令。

第 38 章：MLD 侦听配置命令

主要介绍 MLD 侦听的相关配置命令。

第 **39** 章：**SNMP 配置命令**

主要介绍 SNMP（简单网络管理协议）配置、通知管理、RMON（远程网络监视）等 SNMP 相关配置命令。

第 **40** 章：**LLDP 配置命令**

主要介绍链路层发现协议 LLDP 功能的相关配置命令。

第 **41** 章：**sFLow 配置命令**

主要介绍 sFlow（采样流）的相关配置命令。

第 42 章：静态路由配置命令

主要介绍静态路由功能的相关配置命令。

第 43 章：SDM 模板命令

主要介绍 SDM 模板配置命令。

第 44 章：AAA 配置命令

主要介绍 AAA（认证、授权和计费）配置命令。

第 45 章：DHCP 服务器配置命令

主要介绍 DHCP 服务器功能的相关配置命令。

第 46 章：DHCP 中继配置命令

主要介绍 DHCP 中继功能的相关配置命令。

第 47 章：PoE 配置命令

主要介绍 PoE（以太网供电）的相关配置命令。

第 1 章 命令行使用指导

1.1 使用命令行

用户可以通过三种方式登录交换机来使用命令行：

1. 通过 Console 口进行本地登录；
2. 通过以太网端口利用 Telnet 进行本地或远程登录；
3. 通过以太网端口利用 SSH 进行本地或远程登录。

1.1.1 通过 Console 口进行本地登录

➢ Console 端口

交换机有两个 Console 口：一个 RJ-45 口和一个 Micro-USB Console 口。这两种 Console 口可以同时接收从交换机发送来的信息，但不能同时对交换机进行管理。Micro-USB 口的优先级高于 RJ-45 口。当交换机检测到 Micro-USB 口的连接时，会自动不再接收来自 RJ-45 口的命令，转而接收来自 Micro-USB 的命令。当 Micro-USB 口断开连接后，交换机才会开始接收来自 RJ-45 口的命令。

➢ USB Console 驱动

如果用户使用的是 MAC OS X 和 Linux OS 系统上的 USB 口，则没有必要使用 USB 驱动。

但对于 Windows 系统，用户需要安装 USB 驱动才能使用 USB Console 口来管理交换机。在产品 CD 中找到 USB 驱动，并根据安装提示进行安装。

USB Console 驱动程序支持如下 Windows 系统：

- 32-bit Windows XP SP3
- 64-bit Windows XP
- 32-bit Windows 7
- 64-bit Windows 7
- 32-bit Windows 8
- 64-bit Windows 8
- 32-bit Windows 8.1
- 64-bit Windows 8.1

完成安装后，当电脑的 USB 口连接到交换机的 Micro-USB Console 口时，电脑的 USB 口会作为 RS-232 串行端口；而当电脑的 USB 口不再连接到交换机的 Micro-USB 口后，电脑的 USB 会恢复为标准的 USB 口。

➢ 登录

1. 首先，将计算机（或终端）的串口通过配置电缆与以太网交换机的 Console 口连接。
2. 打开计算机的终端仿真程序（如 Hyperterminal 程序）。
3. 在配置终端仿真程序中配置连接 COM 端口。对于 Micro-USB Console 口，可以到如下页面查看哪个端口被分配给了 USB 串行端口。

   进入路径：**控制面板>硬件和声音>设备管理器>端口**。

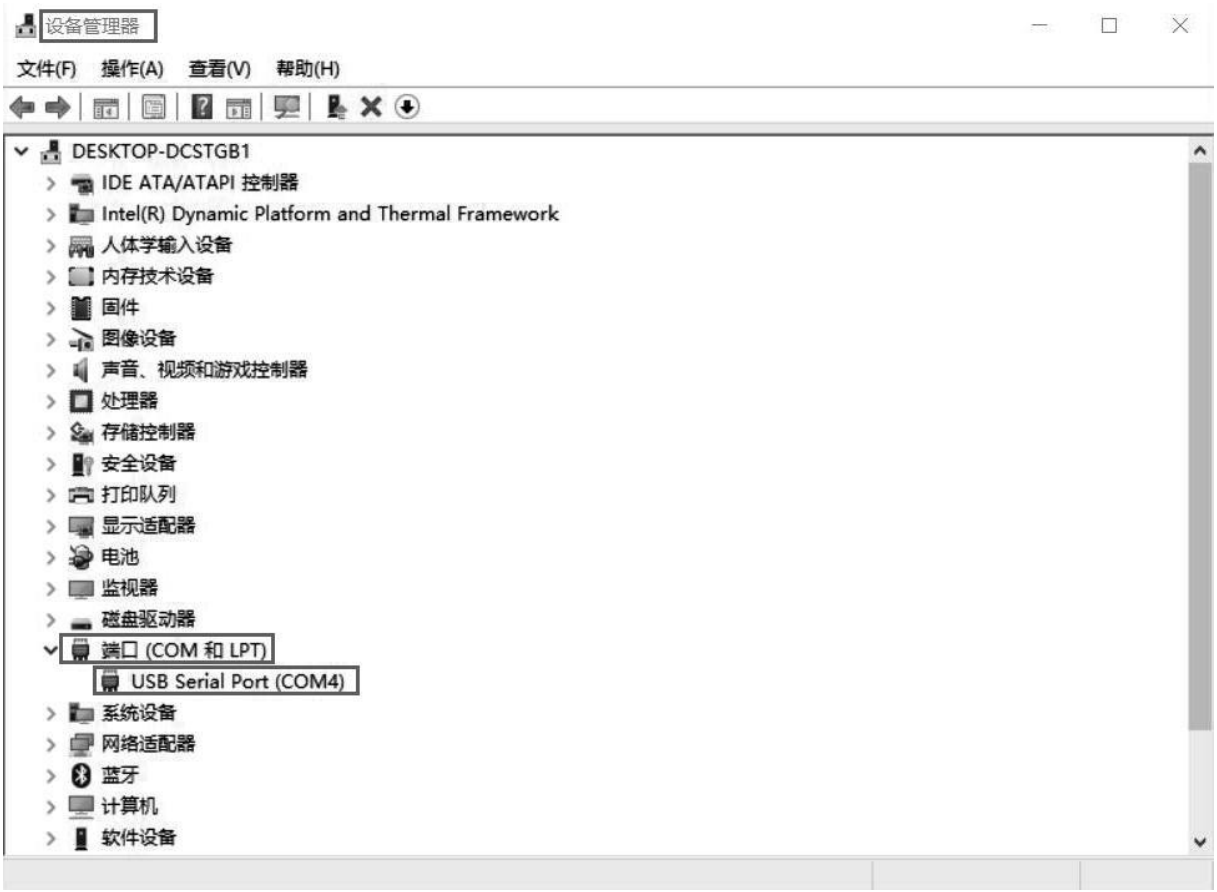

图 1-1 USB 串行端口号

4. 在仿真终端程序中配置如下参数：
   - 波特率：38400bps
   - 数据位：8 位
   - 奇偶校验：无
   - 停止位：1 位
   - 数据流控制：无

5. 在主窗口中输入回车键，可以看到“SW-5024>”的提示符，说明已成功登录交换机。

图 1-2 命令行主窗口

1.1.2 配置特权模式密码

在首次使用 Telnet 或 SSH 进行登录之前，需要先用串口线连接主机及交换机的 Console 口，在超级终端上配置进入特权模式的密码。

按照 **1.1.1 通过 Console 口进行本地登录**所述步骤登录交换机，再照下图所示设置进入特权模式的密码。

图 1-3 设置特权模式密码

1.1.3 通过 Telnet 进行登录

在首次使用 Telnet 进行登录之前，设置好进入特权模式的密码后，还需在超级终端上配置 Telnet 登录模式和登录认证信息。

Telnet 登录模式有两种：Login local 模式和 Login 模式。请根据需要自行选择其中一种模式进行登录。

Login local 模式：需要输入登录用户名和密码，缺省情况下均为 admin。

Login 模式：无需登录用户名和密码，但是需要输入一个连接密码才能建立 Telnet 连接进行访问。

- **Login Local 模式**

如下图所示，首先在超级终端上配置 Telnet 登录模式为“login local”。

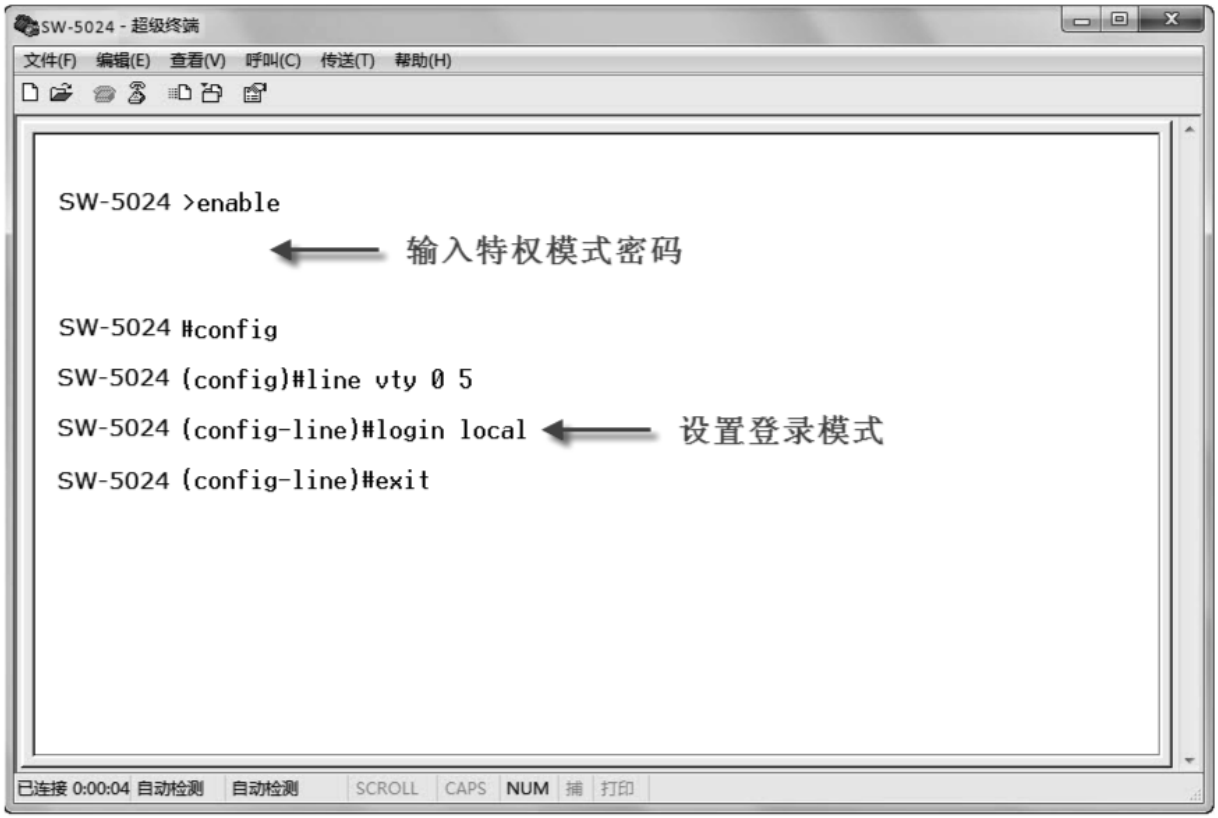

图 1-4 设置 login local 模式

然后便可在 login local 模式下进行 Telnet 登录了：

1. 请先确保本交换机与计算机在同一局域网内。选择开始，在搜索框中输入“cmd”后输入回车键，进入 cmd 窗口。

图 1-5 进入 cmd 窗口

2. 弹出如下图所示的运行窗口，输入 telnet 192.168.0.1，点击确定按钮进入 DOS 界面。

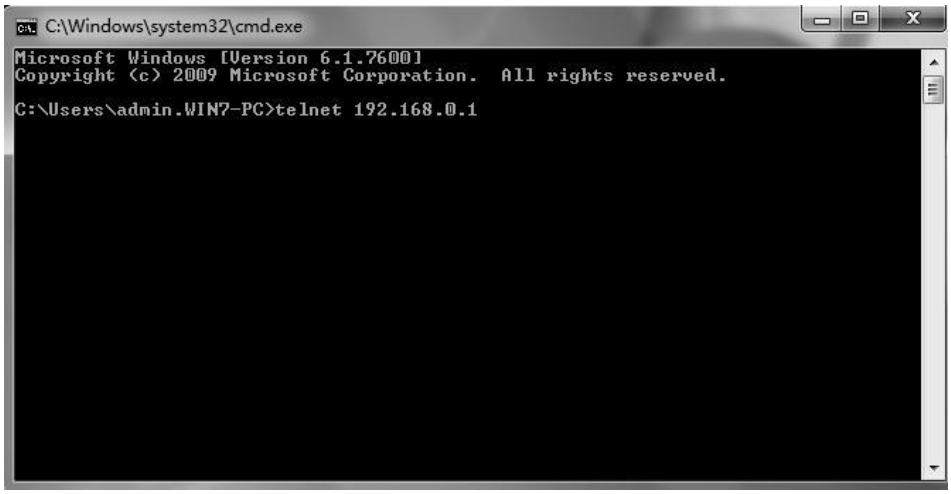

图 1-6 登录交换机

3. 输入登录的用户名和密码（默认值均为“admin”），回车即可进入用户模式，如下图所示。

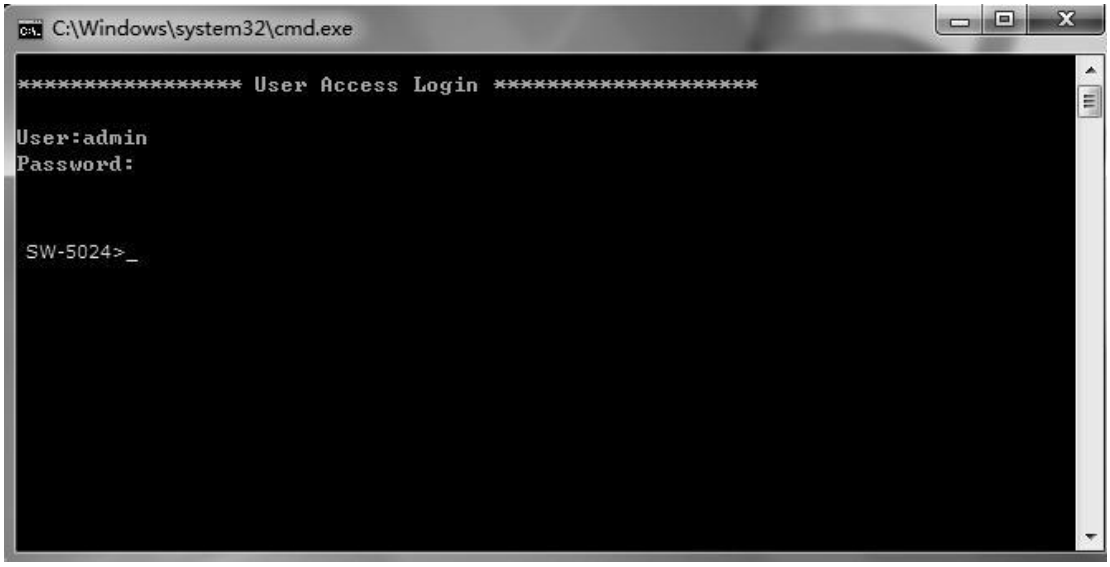

图 1-7 进入用户模式

此时便可在 Telnet 连接中使用 CLI 命令管理交换机了。

4. 可以输入 **enable** 命令进入特权模式。系统会提示输入密码，这里输入我们在终端仿真软件中设置的密码 123。

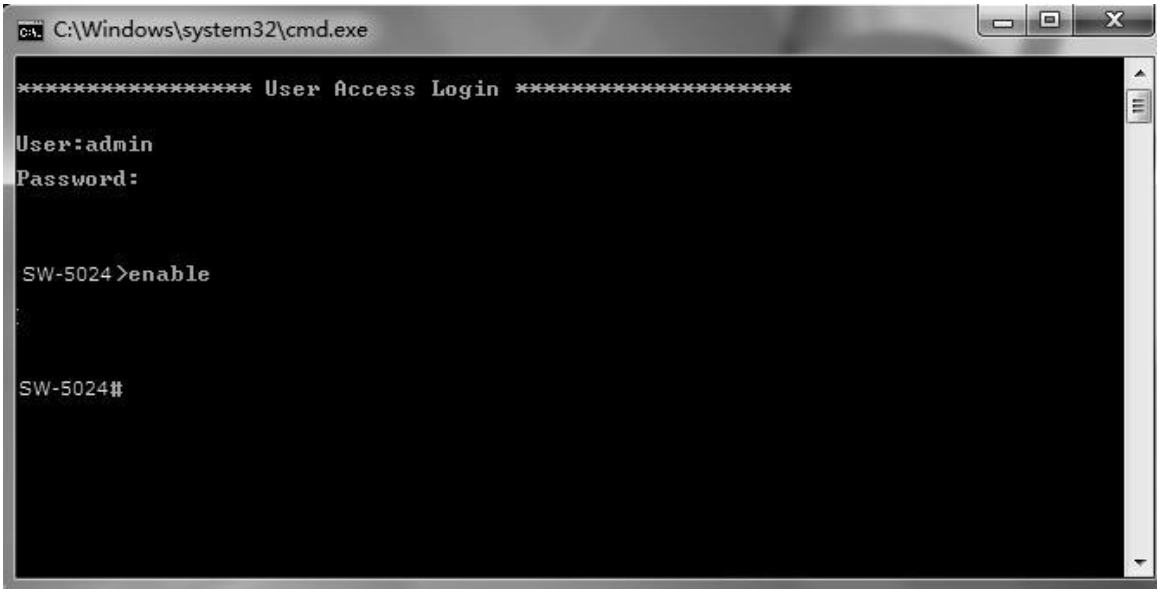

图 1-8 进入特权模式

- **Login 模式**

如下图所示，首先在终端仿真软件上将 Telnet 登录模式配置为“login”，并将连接密码设置为“456”。

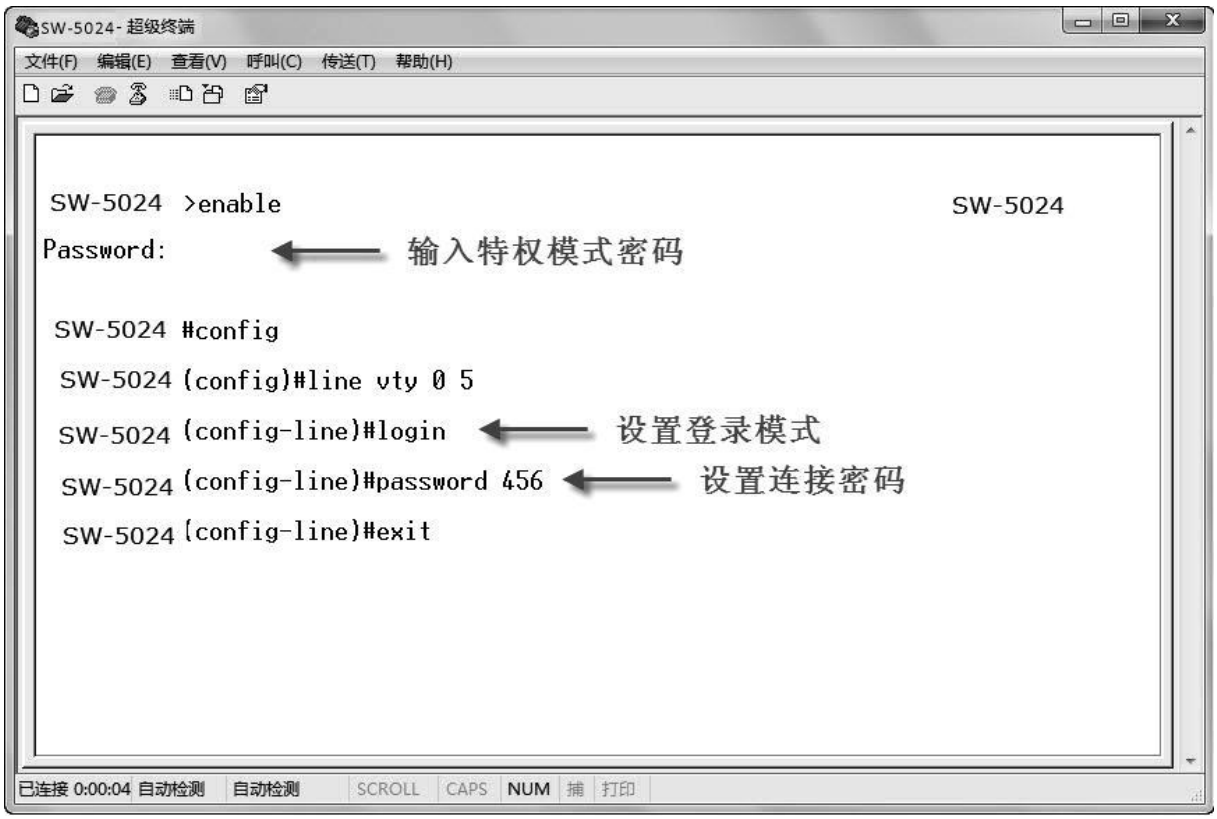

图 1-9 配置 login 模式

此时便可在 login 模式下进行 Telnet 登录了：

1. 在 cmd 窗口中输入 **telnet 192.168.0.1**，按下回车键。

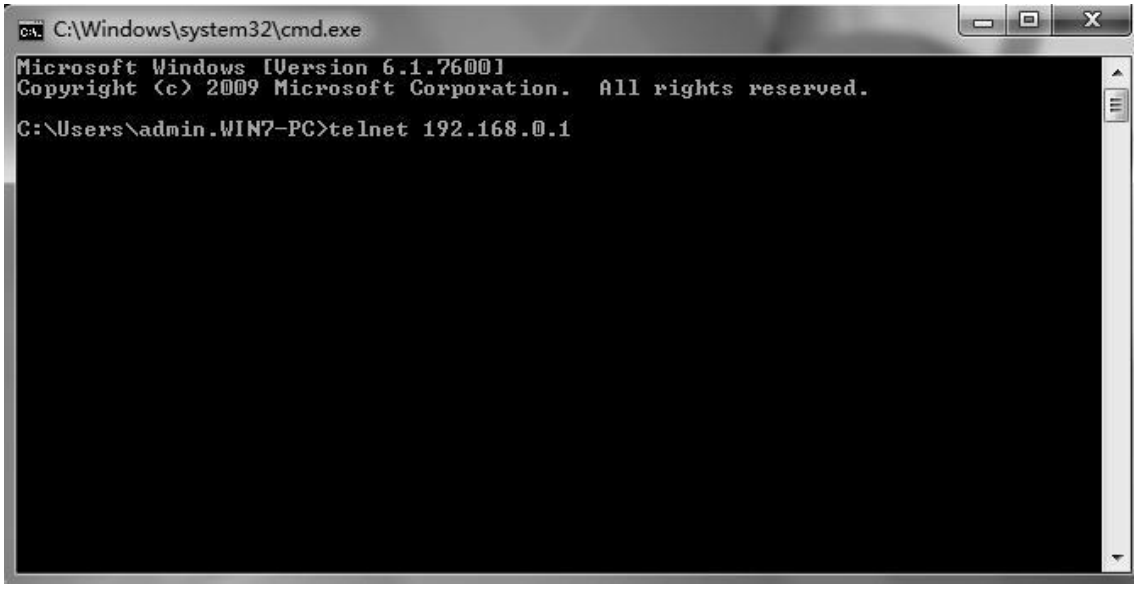

图 1-10 连接交换机

2. 输入已设置的连接密码 **456** 进入用户模式。

图 1-11 进入用户模式

3. 可以输入 **enable** 命令进入特权模式。系统会提示输入密码，这里输入我们在终端仿真软件中设置的密码 123。

图 1-12 进入特权模式

1.1.4 通过 SSH 进行登录

推荐使用第三方客户端软件 PuTTY 来建立 SSH 连接。在首次使用 SSH 进行登录之前请先设置好进入特权模式的密码。SSH 登录有两种认证模式：

密码认证模式：需要登录输入用户名和密码，默认值均为 admin。

密钥认证模式：无需登录用户名和密码，但是需要先通过 Putty 密钥生成器生成一对公钥和私钥，将公钥导入交换机，私钥导入客户端软件进行认证。

进行 SSH 登录之前，请按照下图所示步骤在超级终端中开启交换机的 SSH 功能。

图 1-13 开启 SSH 功能

➢ **密码认证模式**

1. 打开软件，登录 PuTTY 的主界面。在“Host Name”处填写交换机的 IP 地址；“Port”保持默认的 **22**；“Connection type”处选择 **SSH** 的接入方式。如下图所示。

图 1-14 登录 PuTTY 主界面

2. 点击<Open>按键，即可登录到交换机。操作方法与 Telnet 相同，输入登录用户名和登录密码，即可继续进行配置操作。如下图所示。

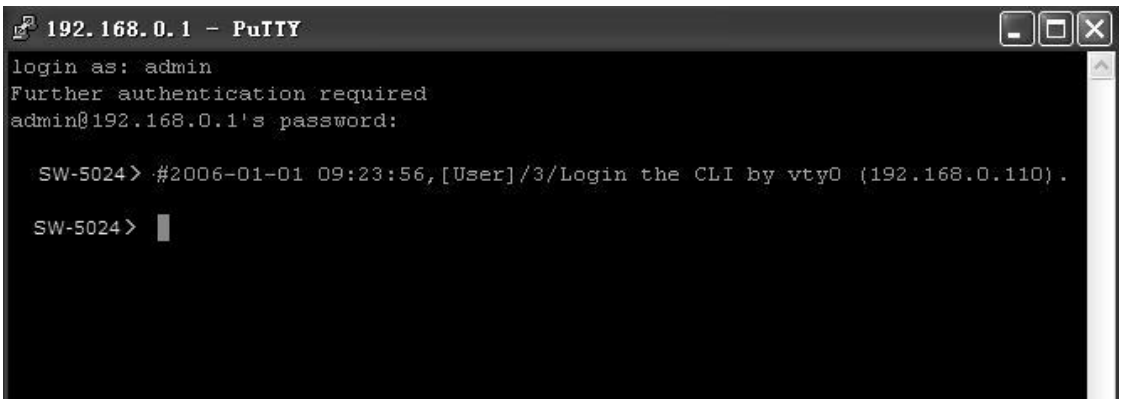

图 1-15 登录交换机

➢ **密钥认证模式**

1. 选择密钥类型和密钥长度，并生成 SSH 密钥。如下图所示。

图 1-16 选择密钥类型和密钥长度

注意:

- 密钥长度的范围为 256 至 3072 比特。
- 生成密钥的过程中，在软件的空白处快速的随意晃动鼠标，产生随机数据，可以加快密钥生成的速度。

2. 密钥生成后，将公钥和私钥文件保存在主机上。如下图所示。

图 1-17 保存公钥和私钥

3. 在超级终端上，将保存至 TFTP 服务器上的公钥文件导入交换机中。

图 1-18 导入公钥文件至交换机

注意:

- 密钥类型要与密钥文件的类型保持一致。
- 载入 SSH 密钥的过程不能被中断。

4. 打开 PuTTY 的主界面，输入 IP 地址并选择连接类型为 SSH，如下图所示。

图 1-19 打开 PuTTY 的主界面

5. 点击左边的目录栏进入 SSH 目录下的 Auth 菜单，将私钥文件导入至 SSH 客户端软件中，再点击<open>按钮与服务器建立连接并进行协商。如下图所示。

图 1-20 导入私钥文件至 SSH 客户端

6. 协商成功后，输入用户名进行登录，如果你不需要输入密码即可登陆成功，表明密钥认证已经成功。如下图所示。

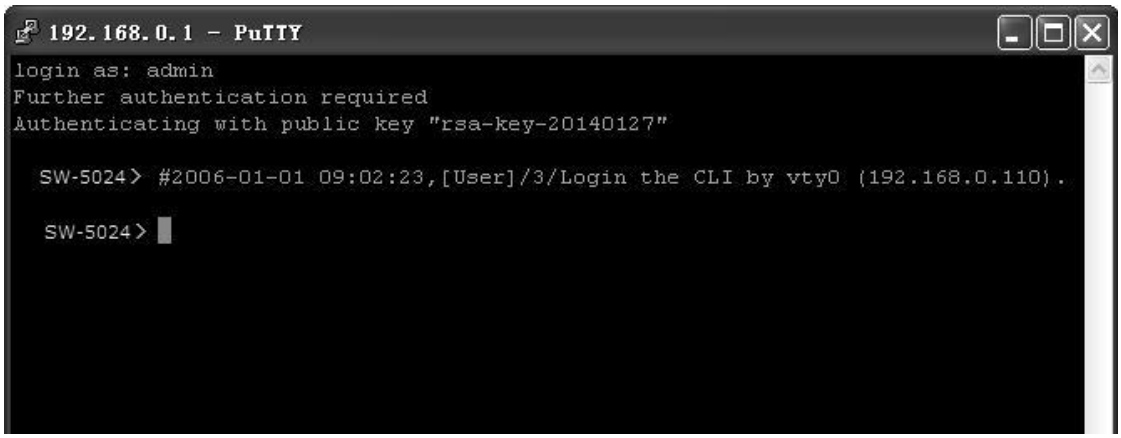

图 1-21 登录交换机

1.2 命令行模式

CLI 按功能划分为以下模式：用户模式、特权模式、全局配置模式、接口配置模式和 VLAN 配置模式，其中接口配置模式又分为以太网端口配置模式和汇聚端口配置模式等等。

下表列出了各模式的访问方法、提示符以及如何离开各模式：

模式	访问方法	提示符	离开或访问下一模式
用户模式	与交换机建立连接即进入该模式	**SW-5024>**	输入 **exit** 命令断开与交换机连接（Console 口接入时无法断开）；输入 **enable** 命令，进入特权模式。
特权模式	在用户模式下，使用 **enable** 命令进入该模式	**SW-5024#**	输入 **exit** 命令，返回用户模式；输入 **configure** 命令，进入全局配置模式。

模式	访问方法	提示符	离开或访问下一模式
全局配置模式	在特权模式下，使用 **configure** 命令进入该模式	**SW-5024(config)#**	输入 **exit** 命令或 **end** 命令，或者键入 Ctrl+Z 组合键，返回特权模式； 输入 **interface gigabitEthernet** *port* 或 **interface range gigabitEthernet** *port-list* 命令，进入接口配置模式； 输入 **vlan** 命令，进入 VLAN 配置模式。
接口配置模式	二层接口： 在全局配置模式下键入 **interface gigabitEthernet** *port* 或 **interface port-channel** *port-channel-id* 或 **interface range gigabitEthernet** *port-list* 进入该模式。 三层接口： 在二层接口配置模式下使用 **no switchport** 命令进入路由端口模式； 在全局配置模式下使用 **interface vlan** *vlan-id* 命令进入 VLAN 接口模式； 在全局配置模式下使用 **interface loopback** *id* 进入环回接口模式。	**SW-5024(config-if)#**或 **SW-5024(config-if-range)#**	使用 **switchport** 命令进入二层接口配置模式； 输入 **end** 命令，或键入 Ctrl+Z 组合键，返回特权模式； 输入 **exit** 或**#**命令，返回全局配置模式。
VLAN 配置模式	在全局配置模式下，使用 **vlan** *vlan-list* 命令进入该模式	**SW-5024(config-vlan)#**	输入 **end** 命令，或键入 Ctrl+Z 组合键返回特权模式； 输入 **exit** 或**#**命令，返回全局配置模式。

说明：

1. 通过 Console 口或 Telnet 方式与交换机建立连接后即进入用户模式。
2. 各个模式都有各自的命令，要进行相应的命令配置必须要先进入对应的模式：

   ●**全局配置模式**：提供全局配置的命令，如：生成树，队列调度模式等；

- **接口配置模式**：分为多个接口，每个接口都有各自相应的命令：
  a) interface gigabitEthernet：配置一个以太网端口的参数，如双工模式，流控状态等。
  b) interface range interface gigabitEthernet：配置多个以太网端口的参数。
  c) interface port-channel：配置汇聚端口的参数，如广播风暴等。
  d) interface range port-channel：配置多个汇聚端口的参数。
  e) interface vlan：配置 VLAN 接口参数。
- **VLAN 配置模式**：创建 VLAN，增加端口到指定 VLAN。

3. 有一些命令是全局的，在所有命令模式下都可执行：
   - **show**：显示交换机各种信息，如：统计信息、端口信息、VLAN 信息等。
   - **history**：显示历史命令。

1.3 命令行安全等级

交换机有四个安全等级：普通用户级、高级用户级、操作级和管理级。可以定义多组用户名和密码，并为每组用户名和密码设置特定的权限级别。不同权限级别可以访问的命令会有所不同，每条命令的“特权要求”部分有具体说明。用户名和密码详细设置方法请参考 user name (password)和 user name (secret)。

在用户模式下，可通过输入命令 **enable** 进入特权模式。默认情况下，不需要密码。在全局配置模式下，可以通过 **enable password** 命令设置管理级密码。设置密码后，需要输入管理级密码才能进入特权模式。

1.4 命令行格式约定

1.4.1 基本格式约定

本文档中对 CLI 命令的叙述遵循以下约定：

- 在中括号 [ ] 中的任何参数都是可选的。
- 在大括号 { } 中的任何参数都是必需的。
- 如果有多个选项，则使用竖线 “|”分隔每个选项。
  例如：**speed** { 10 | 100 | 1000 }
- 关键词（命令中保持不变，必须照输的部分）以粗体形式出现。
  例如：**show logging**
- 常量（枚举量，只能选择其一）以普通字体形式出现。

例如：**mode** { dynamic | static | permanent }

- 变量（命令中必须以实际值进行替代的部分）以斜体形式出现。
  例如：**bridge aging-time** *aging-time*

1.4.2 特殊字符

若变量为字符串形式，输入时请注意：

- ” < > , \ & 这六个字符是不允许输入的。

- 若字符串中包含空格，则字符串首尾需添加单引号’’或双引号””，如’hello world’、”hello world”。此时单/双引号中的两个（或多个）单词会作为一个字符串参数输入；如果不加单/双引号，它们会被解析成两个（或多个）字符串。

1.4.3 参数格式

变量中有些参数是有特定的输入格式的：

- MAC 地址必须以 XX:XX:XX:XX:XX:XX 的格式输入。

- 输入一组端口号(port-list)或一组 VLAN ID(vlan-list)时，可以输入一个或多个值，每个值之间用逗号隔开，连续的一组值可以用连接符-表示。例如 1/0/1,1/0/3-5,1/0/7 表示端口 1/0/1，1/0/3，1/0/4，1/0/5，1/0/7。

第 2 章 用户界面

2.1 enable

描述

该命令用于从用户模式进入特权模式。

命令

enable

模式

用户模式

特权要求

无

示例

设置了从用户模式进入特权模式的密码时：

```
SW-5024>enable
Password:
SW-5024#
```

2.2 service password-encryption

描述

该命令的作用是全局加密，即当配置密码或者写入配置文件时，使用对称算法对密码进行加密。加密功能可以防止配置文件中的密码被读取。它的 no 命令用于禁用全局加密功能。

命令

service password-encryption
no service password-encryption

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

使能全局加密功能：

```
SW-5024(config)# service password-encryption
```

2.3 enable password

描述

该命令用于设置或修改从用户模式切换到特权模式的管理级密码，它的 no 命令用于清空密码。此功能使用对称加密算法。

命令

enable password { [0] *password* | 7 *encrypted-password* }

no enable password

参数

0 —— 加密类型，0 表示接下来输入未经加密的密码。默认的加密类型为 0。

password —— 1～31 位的密码，由字母，数字和符号(!$%'()*,-./[]{|})组成。密码区分大小写。默认情况下密码为空。

7 —— 加密类型，表示接下来需要输入一个固定长度的经过对称加密的密码。

encrypted-password —— 固定长度的经过对称加密的密码，可以从其他交换机的配置文件中复制得到。配置了加密密码之后，当再次进入此模式时，需要输入对应的未经加密的密码。

说明

如果在此配置的密码为未加密的密码，但是通过 **service password-encryption** 命令启用了全局密码加密功能，那么交换机配置文件中的密码将会显示为对称加密格式。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

将用户模式切换到特权模式时的管理级密码设置为不加密密码 admin：

```
SW-5024(config)# enable password admin
```

2.4 enable secret

描述

该命令用于设置或修改从用户模式切换到特权模式的管理级密码，它的 no 命令用于清空密码。此功能使用 MD5 加密算法。

命令

enable secret { [0] *password* | 5 *encrypted-password* }

no enable secret

参数

0 —— 加密类型，0 表示接下来输入未经加密的密码。默认的加密类型为 0。

password —— 1～31 位的密码，由字母，数字和符号(!$%'()*,-./[]{|})组成。密码区分大小写。默认情况下密码为空。此密码在交换机的配置文件中显示为 MD5 加密的格式。

5 —— 加密类型，表示接下来需要输入一个固定长度的经过 MD5 加密的密码。

encrypted-password —— 固定长度的经过对称加密的密码，可以从其他交换机的配置文件中复制得到。配置了加密密码之后，当再次进入此模式时，需要输入对应的未经加密的密码。

说明

如果同时配置了 **enable password** 和 **enable secret**，则必须输入在 **enable secret** 中设置的密码。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

将用户模式切换到特权模式时的管理级密码设置为不加密密码 admin，且此密码在交换机的配置文件中以 MD5 加密的格式显示：

```
SW-5024(config)# enable secret 0 admin
```

2.5 configure

描述

该命令用于从特权模式进入全局配置模式。

命令

configure

模式

特权模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

从特权模式进入全局配置模式：

```
SW-5024# configure
SW-5024(config)#
```

2.6 exit

描述

该命令用于退出当前配置模式返回上一层配置模式。

命令

exit

模式

所有配置模式

特权要求

无

示例

从接口配置模式返回到全局模式，再返回到特权模式：

```
SW-5024 (config-if)# exit
SW-5024 (config)#exit
SW-5024#
```

2.7 end

描述

该命令用于返回特权模式。

命令

end

模式

所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

从接口配置模式直接返回到特权模式：

```
SW-5024(config-if)#end
SW-5024#
```

2.8 history

描述

该命令用于显示系统启动后用户在当前模式下最近输入的 20 条命令。

命令

history

模式

特权模式和所有配置模式

特权要求

无

示例

显示用户之前在当前模式下输入的命令：

```
SW-5024(config)#history
    1 history
```

2.9 history clear

描述

该命令用于清空系统启动后在当前模式下输入过的命令，下一次使用 show history 命令时将不会显示这些被清空的命令。

命令

History clear

模式

特权模式和所有配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

删除用户之前在当前模式下输入的命令：

```
SW-5024(config)#history clear
```

第 3 章 IEEE 802.1Q VLAN 配置命令

VLAN（Virtual Local Area Network，虚拟局域网）是一种在一个物理网络上划分多个逻辑网络的技术，具有控制广播域范围，增强网络安全性，可以灵活创建虚拟工作组等优点。

3.1 vlan

描述

该命令用于进入 VLAN 配置模式并创建 IEEE 802.1Q VLAN，它的 no 命令用于删除 IEEE 802.1Q VLAN。

命令

vlan *vlan-list*

no vlan *vlan-list*

参数

vlan-list —— VLAN ID List，取值范围 2~4094，可以是其中的任意一个值或者一个数值段。格式为 2-3, 5。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建 VLAN 2-10 以及 VLAN 100：

SW-5024(config)# vlan 2-10,100

删除 VLAN 2：

SW-5024(config)# no vlan 2

3.2 interface vlan

描述

该命令用于创建 VLAN 接口并进入 VLAN 接口模式。它的 no 命令用于删除 VLAN 接口。

命令

interface vlan *vlan-id*

no interface vlan *vlan-id*

参数

vlan-id —— VLAN ID，取值范围 1-4094。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建 VLAN 接口 2：

```
SW-5024(config)# interface vlan 2
```

3.3 name

描述

该命令用于配置 IEEE 802.1Q VLAN 描述字符，它的 no 命令用于清空描述字符。

命令

name *descript*

no name

参数

descript —— VLAN 描述字符，长度为 1-16 个字符。

模式

VLAN 配置模式（vlan）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将 VLAN 2 的描述配置为“group1”：

```
SW-5024(config)# vlan 2
SW-5024(config-vlan)# name group1
```

3.4 switchport mode

描述

该命令用于配置以太网端口的链路类型。

命令

switchport mode { access | trunk | general }

参数

access | trunk | general —— 以太网端口链路类型，共支持三种类型。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置以太网端口 3 的链路类型为 trunk：

```
SW-5024 (config)# interface gigabitEthernet 1/0/3
SW-5024 (config-if)# switchport mode trunk
```

3.5 switchport access vlan

描述

该命令用于把 access 类型的端口添加到 IEEE 802.1Q VLAN，它的 no 命令用于把端口从 IEEE 802.1Q VLAN 中移除。

命令

switchport access vlan *vlan-id*

no switchport access vlan

参数

vlan-id —— VLAN ID，取值范围 2-4094。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置以太网端口 3 链路类型为 access 并将其添加到 VLAN2 中：

```
SW-5024 (config)# interface gigabitEthernet 1/0/3
SW-5024 (config-if)# switchport access vlan 2
```

3.6 switchport trunk allowed vlan

描述

该命令用于把 trunk 类型的端口添加到 IEEE 802.1Q VLAN，它的 no 命令用于端口从 IEEE 802.1Q VLAN 中移除。

命令

switchport trunk allowed vlan { *vlan-list* }

no switchport trunk allowed vlan { *vlan-list* }

参数

vlan-list —— 指定 IEEE 802.1Q VLAN ID，取值范围 2-4094，可多选，格式为：2-3, 5。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置以太网端口 2 链路类型为 trunk 并将其添加到 VLAN2 中：

```
SW-5024 (config)# interface gigabitEthernet 1/0/2
SW-5024 (config-if)# switchport mode trunk
SW-5024 (config-if)# switchport trunk allowed vlan 2
```

3.7 switchport general allowed vlan

描述

该命令用于把 general 类型的端口添加到 IEEE 802.1Q VLAN，并配置端口的出口规则。它的 no 命令用于把端口从 IEEE 802.1Q VLAN 中移除。

命令

switchport general allowed vlan *vlan-list* { tagged | untagged }

no switchport general allowed vlan *vlan-list*

参数

vlan-list —— 指定 IEEE 802.1Q VLAN ID，取值范围 2-4094，可多选，格式为：2-3, 5。

tagged | untagged —— 出口规则，tagged 或者 untagged。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置以太网端口 4 链路类型为 general，将其添加到 VLAN2 中，并指定出口规则为 tagged：

```
SW-5024 (config)# interface gigabitEthernet 1/0/4
SW-5024 (config-if)# switchport mode general
SW-5024 (config-if)# switchport general allowed vlan 2 tagged
```

3.8 switchport pvid

描述

该命令用于设置交换机端口的 PVID。

命令

switchport pvid *vlan-id*

参数

vlan-id —— VLAN ID，取值范围 1-4094。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置端口 2 的 PVID 为 2：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# switchport pvid 2
```

3.9 show vlan summary

描述

该命令用于显示 IEEE 802.1Q VLAN 的统计信息。

命令

show vlan summary

模式

特权模式以及所有配置模式

特权要求

无

示例

显示 IEEE 802.1Q VLAN 的统计信息：

```
SW-5024(config)# show vlan summary
```

3.10 show vlan brief

描述

该命令用于显示 IEEE 802.1Q VLAN 的概要信息。

命令

show vlan brief

模式

特权模式以及所有配置模式

特权要求

无

示例

显示 IEEE 802.1Q VLAN 的概要信息：

```
SW-5024(config)# show vlan brief
```

3.11 show vlan

描述

该命令用于显示指定的 IEEE 802.1Q VLAN 的详细信息。

命令

show vlan [**id** *vlan-id*]

参数

vlan-id —— VLAN ID，取值范围为 1-4094。该参数缺省时，显示所有 IEEE 802.1Q VLAN 的信息。

模式

特权模式以及所有配置模式

特权要求

无

示例

显示 VLAN 5 的详细信息：

SW-5024(config)# show vlan id 5

3.12 show interface switchport

描述

该命令用于显示以太网口的信息。

命令

show interface switchport [**gigabitEthernet** port | **port-channel** *port-channel-id*]

参数

port —— 以太网端口号。

port-channel-id —— LAG 号。

模式

特权模式以及所有配置模式

特权要求

无

示例

显示所有端口和 LAG 的详细信息：

SW-5024(config)#show interface switchport

第 4 章 MAC VLAN 配置命令

MAC VLAN 是一种通过 MAC 地址来划分 VLAN 的技术。用户可以配置 MAC 地址和 VLAN ID 一一绑定。当交换机收到 untagged 数据包或 priority-tagged 数据包时，会根据其 MAC 地址为数据包打上相应的 VLAN tag。

4.1 mac-vlan mac-address

描述

该命令用于创建 MAC VLAN 条目，它的 no 命令用于删除 MAC VLAN 条目。

命令

mac-vlan mac-address *mac-addr* **vlan** *vlan-id* [**description** *descript*]

no mac-vlan mac-address *mac-addr*

参数

mac-addr —— 源 MAC 地址，格式为 XX:XX:XX:XX:XX:XX。

vlan-id —— 指定 IEEE 802.1 Q VLAN ID，取值范围 1-4094。

descript —— 给此 MAC VLAN 条目添加一个描述，最多包含 8 个字符。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建 vid=2，MAC 地址为 00:11:11:01:01:12 的 MAC VLAN 条目，命名为 SUNDRAY：

SW-5024(config)# mac-vlan mac-address 00:11:11:01:01:12 **vlan** 2

description SUNDRAY

4.2 mac-vlan

描述

该命令用于启用指定端口的 MAC VLAN 功能，它的 no 命令用于禁用指定端口的 MAC VLAN 功能，缺省时在所有端口上禁用 MAC VLAN 功能。

命令

mac-vlan

no mac-vlan

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启端口 1/0/3 的 MAC VLAN 功能：

```
SW-5024(config)# interface gigabitEthernet 1/0/3

SW-5024(config-if)# mac-vlan
```

4.3 show mac-vlan

描述

该命令用于显示 MAC VLAN 条目信息。可以显示根据 MAC 地址或 VLAN ID 过滤的信息。

命令

show mac-vlan { **all** | **mac-address** *mac-addr* | **vlan** *vlan-id* }

参数

mac-addr ——指定 MAC 地址，格式为 XX:XX:XX:XX:XX:XX。

vlan-id —— 选择 VLAN ID，取值范围 1-4094。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有 MAC VLAN 条目信息：

```
SW-5024(config)# show mac-vlan all
```

4.4 show mac-vlan interface

描述

该命令用于显示 MAC VLAN 的端口使能状态。

命令

show mac-vlan interface

模式

特权模式和所有配置模式

特权要求

无

示例

显示 MAC VLAN 的所有端口使能状态：

```
SW-5024(config)# show mac-vlan interface
```

第 5 章 协议 VLAN 配置命令

协议 VLAN 是按照协议来划分 VLAN 的一种方法。每个协议对应一个 VLAN ID，交换机给端口收到的无 tag 帧和优先级 tag 帧分配此 VLAN ID。

5.1 protocol-vlan template

描述

该命令用于创建协议模板。它的 no 命令用于删除协议模板。

命令

protocol-vlan template name *protocol-name* **frame** { **ether_2 ether-type** *type* | **snap ether-type** *type* | **llc dsap** *dsap_type* **ssap** *ssap_type* }

no protocol-vlan template *template-idx*

参数

protocol-name —— 协议名称，由 1-8 个字符组成。

ether_2 ether-type *type* —— 配置以太网协议类型。

snap ether-type *type* —— 配置以太网协议类型。

llc dsap *dsap_type* **ssap** *ssap_type* —— 配置 DSAP 类型和 SSAP 类型。

template-idx —— 协议模板序号。可用 **show protocol-vlan template** 命令获取各序号对应的模板。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建一个协议类型为 0x2024 的协议模板，并命名为“SUNDRAY”。 **SW-5024(config)# protocol-vlan template name** SUNDRAY **frame ether_2 ether-type** 2024

5.2 protocol-vlan vlan

描述

该命令用于创建协议组条目，它的 no 命令则用于删除协议组条目。

命令

protocol-vlan vlan *vlan-id* **template** *template-idx*

no protocol-vlan vlan *group-idx*

参数

vlan-id —— VLAN ID，取值范围 1-4094。

template-idx —— 协议模板序号。可用 **show protocol-vlan template** 命令获取各序号对应的模板。

group-idx —— 协议组序号。可用 **show protocol-vlan vlan** 命令获取各序号对应的协议组条目。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建 vid=2，协议模板序号为 3 的协议组条目：

```
SW-5024(config)# protocol-vlan vlan 2 template 3
```

5.3 protocol-vlan group

描述

该命令用于在将指定端口加入某协议组，它的 no 命令用于从协议组中删除该端口。

命令

protocol-vlan group *index*

no protocol-vlan group *index*

参数

index —— 协议组序号。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将端口 20 加入到协议组 1：

```
SW-5024(config)# interface gigabitEthernet 1/0/20
SW-5024(config-if)# protocol-vlan group 1
```

5.4 show protocol-vlan template

描述

该命令用于显示协议模板配置信息。

命令

show protocol-vlan template

模式

特权模式和所有配置模式

特权要求

无

示例

显示协议模板配置信息：

```
SW-5024(config)# show protocol-vlan template
```

5.5 show protocol-vlan vlan

描述

该命令用于显示协议组条目信息。

命令

show protocol-vlan vlan

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有的协议组列表里的条目：

SW-5024(config)# show protocol-vlan vlan

第 6 章 VLAN-VPN 配置命令

VLAN-VPN（Virtual Private Network）是一种简单、灵活的二层 VPN 技术，它通过在运营商接入端为用户的私网报文封装外层 VLAN Tag，使报文携带两层 VLAN Tag 穿越运营商网络（公网）。

6.1 dot1q-tunnel

描述

该命令用于全局启用 vlan-VPN 功能，它的 no 命令用于禁用 vlan-VPN 功能。

命令

dot1q-tunnel

no dot1q-tunnel

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局启用 VLAN-VPN 功能：

```
SW-5024(config)#dot1q-tunnel
```

6.2 dot1q-tunnel tpid

描述

该命令用于配置 vlan-VPN 全局 TPID，它的 no 命令用于恢复默认 TPID。

命令

dot1q-tunnel tpid *tpid*

no dot1q-tunnel tpid

参数

tpid —— 全局 TPID。必须为 4 位十六进制整数的形式。默认值为 8100。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 VLAN-VPN 全局 TPID 为 0x9100：

SW-5024(config)#dot1q-tunnel tpid 9100

6.3 dot1q-tunnel mapping

描述

该命令用于全局启用 VLAN 映射功能，它的 no 命令用于禁用 VLAN 映射功能。

命令

dot1q-tunnel mapping

no dot1q-tunnel mapping

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局启用 VLAN 映射功能：

SW-5024(config)#dot1q-tunnel mapping

6.4 switchport dot1q-tunnel mapping

描述

该命令用于在指定端口上添加 VLAN 映射条目，它的 no 命令删除指定端口上的 VLAN 映射条目。

命令

switchport dot1q-tunnel mapping *c-vlan sp-vlan* [*descript*]

no switchport dot1q-tunnel mapping *c-vlan*

参数

c-vlan —— Customer VLAN ID（用户 VLAN ID），取值范围 1-4094。

sp-vlan —— Service Provider VLAN ID（服务商 VLAN ID），取值范围 1-4094。

descript —— VLAN 映射条目的描述信息，可选。最多 15 个字符。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

在端口 3 上添加一条 VLAN 映射条目，C-VLAN 为 2，SP-VLAN 为 3：

SW-5024(config)# interface gigabitEthernet 1/0/3

SW-5024(config-if)#switchport dot1q-tunnel mapping 2 3

6.5 switchport dot1q-tunnel mode

描述

该命令用于设置端口类型，如果为上联口，即与服务商相连的端口，如果为下联口，即与用户端相连的端口。它的 no 命令用于恢复端口为普通端口。

命令

switchport dot1q-tunnel mode { uni/nni }

no switchport dot1q-tunnel mode

参数

uni ——The port connected to the clients.

nni ——The port connected to the ISP.

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置以太网端口 3 作为 VPN NNI 接口：

SW-5024(config)# interface gigabitEthernet 1/0/3 **SW-**

5024(config-if)#switchport dot1q-tunnel mode nni

6.6 show dot1q-tunnel

描述

该命令用于显示 VLAN VPN 全局配置信息。

命令

show dot1q-tunnel

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN VPN 全局配置信息：

```
SW-5024(config)# show dot1q-tunnel
```

6.7 show dot1q-tunnel mapping

描述

该命令用于显示 VLAN 映射条目信息。

命令

show dot1q-tunnel mapping

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN 映射条目：

```
SW-5024(config)# show dot1q-tunnel mapping
```

6.8 show dot1q-tunnel interface

描述

该命令用于显示 VLAN VPN 的端口类型。

命令

show dot1q-tunnel interface

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN VPN 的所有端口类型：

```
SW-5024(config)#show dot1q-tunnel interface
```

第 7 章 Private VLAN 配置命令

Private VLAN（Private Virtual Local Area Network）采用二层 VLAN 结构：Primary VLAN 和 Secondary VLAN。上行设备只需识别 Primary VLAN，而不必关心 Secondary VLAN，从而节省上层设备的 VLAN 资源。通过 MAC 地址复制技术，有效的抑制广播通信方式产生的带宽资源浪费，节省带宽资源。

7.1 private-vlan primary

描述

该命令用于设置指定 VLAN 为 Private VLAN 的 Primary VLAN，no 命令用于删除当前 VLAN 的 Primary VLAN 属性。

命令

private-vlan primary

no private-vlan primary

模式

VLAN 配置模式（VLAN）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置 VLAN 3 为 Private VLAN 的 Primary VLAN：

```
SW-5024(config)#vlan 3
SW-5024(config-vlan)#private-vlan primary
```

7.2 private-vlan community

描述

该命令用于配置 Private VLAN 的 Community VLAN，no 命令用于删除当前的 VLAN 的 Community VLAN 属性。

命令

private-vlan community

no private-vlan community

模式

VLAN 配置模式(VLAN)

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

将 VLAN 3 设置为 Private VLAN 的 Primary VLAN：

```
SW-5024(config)# vlan 3
SW-5024(config-vlan)# private-vlan primary
```

7.3 private-vlan isolated

描述

该命令用于配置 Private VLAN 的 Isolated VLAN，no 命令用于删除当前的 VLAN 的 Isolated VLAN 属性。

命令

private-vlan isolated

no private-vlan isolated

模式

VLAN 配置模式（VLAN）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

将 VLAN 3 设置为 Private VLAN 的 Isolated VLAN：

```
SW-5024(config)# vlan 3
SW-5024(config-vlan)# private-vlan isolated
```

7.4 private-vlan association

描述

该命令用于关联 Primary VLAN 和 Secondary VLAN，no 命令用于取消当前关联。

命令

private-vlan association *vlan_list*

no private-vlan association *vlan_list*

参数

vlan_list —— Secondary VLAN 的 VLAN ID，取值范围 2-4094。

模式

VLAN 配置模式（VLAN）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

关联 Primary VLAN 3 和 Community VLAN 4，使其成为一个 Private VLAN：

```
SW-5024(config)#vlan 3
SW-5024(config-vlan)#private-vlan association 4
```

7.5 switchport private-vlan

描述

该命令用于配置交换机端口的 Private VLAN 属性，no 命令用于删除端口的 Private VLAN 属性。

命令

switchport private-vlan { promiscuous | host }

no switchport private-vlan

参数

promiscuous | host ——配置交换机端口在 Private VLAN 中的端口类型。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

配置端口 3 的 Private VLAN 属性为 host：

```
SW-5024(config)# interface gigabitEthernet 1/0/3
SW-5024(config-if)#switchport private-vlan host
```

7.6 switchport private-vlan host-association

描述

该命令用于将 host 类型端口添加到 Private VLAN，no 命令用于将端口从 Private VLAN 移出。

命令

switchport private-vlan host-association *primary_vlan_id secondary_vlan_id vlantype*

no switchport private-vlan host-association

参数

primary_vlan_id —— 填写端口加入的 Primary VLAN 的 VLAN ID，取值范围 2-4094。

secondary_vlan_id —— 填写端口加入的 Secondary VLAN 的 VLAN ID，取值范围 2-4094。

vlantype ——Private VLAN 类型，可选项为 community 或 isolated。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

将 host 类型的端口 3 添加到 Community 类型的 Private VLAN，其中 Private VLAN 的 primary VLAN 和 secondary VLAN 分别为 VLAN 3 和 VLAN 4：

SW-5024(config)# interface gigabitEthernet 1/0/3 **SW-5024(config-if)#switchport private-vlan host-association** 3 4 community

7.7 switchport private-vlan mapping

描述

该命令用于将 promiscuous 类型端口添加到 Private VLAN，no 命令用于将端口从 Private VLAN 移出。

命令

switchport private-vlan mapping *primary_vlan_id secondary_vlan_id*

no switchport private-vlan mapping

参数

primary_vlan_id —— 填写端口加入的 Primary VLAN 的 VLAN ID，取值范围 2-4094。

secondary_vlan_id —— 填写端口加入的 Secondary VLAN 的 VLAN ID，取值范围 2-4094。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

将 promiscuous 类型的端口 3 添加到 Private VLAN，其中 Private VLAN 的 primary VLAN 和 secondary VLAN 分别为 VLAN 3 和 VLAN 4：

SW-5024(config)# interface gigabitEthernet 1/0/3

SW-5024(config-if)#switchport private-vlan mapping 3 4

7.8 show vlan private-vlan

描述

该命令用于显示设备上已配置的 private-vlan 参数。

命令

show vlan private-vlan

模式

特权模式和所有配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

显示交换机上已配置的 private-vlan 参数：

SW-5024(config)# show vlan private-vlan

7.9 show vlan private-vlan interface

描述

该命令用于显示指定端口的 private-vlan 参数，不指定具体端口显示全部端口的相关配置配置。

命令

show vlan private-vlan interface [**gigabitEthernet** port | **port-channel** *port-channel-id*]

参数

port —— 以太网端口号。

port-channel-id —— 汇聚组号。

模式

特权模式和所有配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

显示交换机上所有端口已配置的 private-vlan 参数：

```
SW-5024(config)#  show vlan private-vlan interface
```

第 8 章 L2TP 配置命令

L2TP (Layer 2 Tunneling Protocol)是一种二层隧道协议。使用 L2TP，服务商可以让用户网络中的数据包在 ISP 网络中进行透明传输。目前我司交换机支持以下二层协议：STP (Spanning Tree Protocol), GVRP (GARP VLAN Registration Protocol)，CDP (Cisco Discovery Protocol)，VTP (VLAN Trunking Protocol)，PAgP (Port Aggregation Protocol)，UDLD (UniDirectional Link Detection) 以及 PVST+(Per VLAN Spanning Tree Plus).

8.1 l2protocol-tunnel

描述

该命令用于全局开启 L2TP 功能。它的 no 命令用于全局关闭 L2TP 功能。

命令

l2protocol-tunnel

no l2protocol-tunnel

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

全局开启 L2TP 功能：

```
SW-5024(config)# l2protocol-tunnel
```

8.2 l2protocol-tunnel type

描述

该命令用于在端口上配置 L2TP 功能。它的 no 命令用于关闭端口的 L2TP 功能。

命令

l2protocol-tunnel type nni

l2protocol-tunnel type uni { 01000ccccccc | 01000ccccccd | gvrp | stp | all }

[**threshold** *threshold*]

no l2protocol-tunnel

参数

nni —— 根据端口所连网络配置端口类型。连接 ISP 网络的端口需配置为 NNI 类型。

uni —— 根据端口所连网络配置端口类型。连接用户网络的端口需配置为 UNI 类型。

01000ccccccc | 01000ccccccd | gvrp | stp | all —— 选择二层协议类型。交换机收到来自用户网络的该协议类型的数据包后，会为其封装上特定的目的 MAC 地址，然后将数据包发送到 ISP 网络。数据包到达对端网络后被解封，交换机根据数据包原本的 MAC 地址发送到用户网络。

- 01000ccccccc: 为目的 MAC 地址为 01000ccccccc 的数据包开启 L2TP 功能。这些数据包类型包括 CDP、VTP、 PAgP 以及 UDLD。
- 01000ccccccd: 为 PVST+类型的数据包开启 L2TP 功能。
- gvrp: 为 GVRP 类型数据包开启 L2TP 功能。
- stp: 为 STP 类型的数据包开启 L2TP 功能
- all: 为所有二层协议数据包开启 L2TP 功能。

threshold —— 配置交换机每秒最多能够封装的数据包数量。当超过这个数值后，数据包会被丢弃。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

将端口 3 配置为 UNI 端口并配置该端口每秒封装的数据包门限值为 1000 个。

SW-5024(config)#interface gigabitEthernet 1/0/3 **SW-5024(config-if)# l2protocol-tunnel type uni** stp **threshold** 1000

8.3 show l2protocol-tunnel global

描述

该命令用于显示全局 L2TP 配置。

命令

show l2protocol-tunnel global

模式

特权模式和所有配置模式

特权要求

无

示例

显示全局 L2TP 配置。

SW-5024(config)# show l2protocol-tunnel global

8.4 show l2protocol-tunnel interface

描述

该命令用于显示特定端口或所有端口上的 L2TP 配置。

命令

show l2protocol-tunnel interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

参数

port —— 以太网端口号。

port-channel-id ——汇聚组号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示以太网端口 1 的 L2TP 配置。

SW-5024(config)#show l2protocol-tunnel interface gigabitEthernet

1/0/1 显示所有端口的 L2TP 配置。

SW-5024(config)#show l2protocol-tunnel interface

第 9 章 GVRP 配置命令

GARP（Generic Attribute Registration Protocol，通用属性注册协议），GVRP 功能是该协议的一种应用，通过在端口动态注册和注销 VLAN 信息来达到创建或删除 VLAN 的目的，并传播该信息到其它交换机中，减少配置 VLAN 时烦琐的手动操作。

9.1 gvrp (global)

描述

该命令用于全局启用 GVRP 功能，它的 no 命令用于禁用 GVRP 功能。

命令

gvrp

no gvrp

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局启用 GVRP 功能：

```
SW-5024(config)# gvrp
```

9.2 gvrp (interface)

描述

该命令用于在指定端口上启用 GVRP 功能，它的 no 命令用于禁用该端口的 GVRP 功能。

命令

gvrp

no gvrp

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用端口 2-6 的 GVRP 功能：

```
SW-5024(config)# interface range gigabitEthernet 1/0/2-6
SW-5024(config-if-range)# gvrp
```

9.3 gvrp registration

描述

该命令用于配置指定端口的 GVRP 注册模式，它的 no 命令用于恢复默认的注册模式。

命令

gvrp registration { normal | fixed | forbidden }

no gvrp registration

参数

normal | fixed | forbidden —— 注册模式，默认的为 normal。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置端口 2-6 的 GVRP 注册模式为 fixed：

```
SW-5024(config)# interface range gigabitEthernet 1/0/2-6
SW-5024(config-if-range)# gvrp registration fixed
```

9.4 gvrp timer

描述

该命令用于配置 GVRP 定时器，它的 no 命令用于恢复默认配置。

命令

gvrp timer { leaveall | join | leave } *value*

no gvrp timer [leaveall | join | leave]

参数

leaveall | join | leave —— 分别表示 leave All、join 和 leave 三个定时器。每个端口启动 GARP 后，同时启动 LeaveAll 定时器，端口将对外循环发送 LeaveAll 消息，以使其它端口重新注册其所有的属性信息。GARP 端口可以将每个 Join 数据包向外发送两次来保证消息的可靠传输，两次发送之间的时间间隔用 Join 定时器来控制。接收到 Leave 数据包的 GARP 端口启动 Leave 定时器，如果在该定时器超时之前没有收到 Join 数据包，则注销相应属性信息。

value —— 定时器值，leave All 的取值范围 1000-30000(厘秒)，默认值为 1000；join 的取值范围 20-1000(厘秒)，默认值为 20；leave 的取值范围 60-3000(厘秒)，默认值为 60。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将端口 6 的 leaveall 定时器设为 2000，并将 join 定时器恢复默认配置：

```
SW-5024(config)# interface gigabitEthernet 1/0/6
SW-5024(config-if)# gvrp timer leaveall 2000
SW-5024(config-if)# no gvrp timer join
```

9.5 show gvrp interface

描述

该命令用于显示以太网端口的 GVRP 配置信息。

命令

show gvrp interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

参数

port —— 以太网端口号。

port-channel-id —— 汇聚组号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示端口 1 的 GVRP 配置信息：

```
SW-5024(config)#show gvrp interface gigabitEthernet
```

1/0/1 显示所有端口的 GVRP 配置信息：

```
SW-5024(config)# show gvrp interface
```

9.6 show gvrp global

描述

该命令用于显示 GVRP 全局状态。

命令

show gvrp global

模式

特权模式和所有配置模式

特权要求

无

示例

显示 GVRP 全局状态：

```
SW-5024(config)# show gvrp global
```

第 10 章语音 VLAN 配置命令

语音 VLAN 是为语音数据流而专门划分的 VLAN。通过划分 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，可以为语音数据流配置 QoS 参数，提高语音数据流的传输优先级、保证通话质量。

10.1 voice vlan

描述

该命令用于开启 Voice VLAN 功能，它的 no 命令用于禁用 Voice VLAN 功能。

命令

voice vlan *vlan-id*

no voice vlan

参数

vlan-id —— VLAN ID，取值范围 2-4094。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启 vid=10 的 Voice VLAN 功能：

```
SW-5024(config)# voice vlan 10
```

10.2 voice vlan aging

描述

该命令用于配置 Voice VLAN 老化时间，它的 no 命令用于恢复默认老化时间。

命令

voice vlan aging *time*

no voice vlan aging

参数

time —— 老化时间，取值范围 1-43200 分钟。默认为 1440 分钟。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 Voice VLAN 老化时间为 2880 分钟：

```
SW-5024(config)# voice vlan aging 2880
```

10.3 voice vlan priority

描述

该命令用于配置语音 VLAN 的优先级，它的 no 命令用于恢复默认优先级。

命令

voice vlan priority *pri*

no voice vlan priority

参数

pri —— 优先级，取值范围 0-7。默认优先级为 6。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置语音 VLAN 的优先级为 5：

```
SW-5024(config)# voice vlan priority 5
```

10.4 voice vlan mac-address

描述

该命令用于创建或删除 Voice VLAN OUI。它的 no 命令用于删除指定的 Voice VLAN OUI。

命令

voice vlan mac-address *mac-addr* **mask** *mask* [**description** *descript*]

no voice vlan mac-address *mac-addr*

参数

mac-addr —— OUI 设备 MAC 地址。格式为 XX:XX:XX:XX:XX:XX。

mask —— MAC 地址掩码。格式为 XX:XX:XX:XX:XX:XX。

descript —— OUI 描述，1-16 个字符。缺省情况下为空。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建 MAC 地址为 00:11:11:11:11:11，掩码为 FF:FF:FF:00:00:00 的 Voice VLAN OUI，将其描述为 Phone：

SW-5024(config)# voice vlan mac-address 00:11:11:11:11:11 **mask** FF:FF:FF:00:00:00 **description** Phone

10.5 switchport voice vlan mode

描述

该命令用于配置以太网端口的 Voice VLAN 成员模式。

命令

switchport voice vlan mode { manual | auto }

参数

manual | auto —— 端口的成员模式。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置以太网端口 3 的 voice vlan 成员模式为 auto：

SW-5024(config)# interface gigabitEthernet 1/0/3 **SW-5024(config-if)# switchport voice vlan mode** auto

10.6 switchport voice vlan security

描述

该命令用于配置以太网端口的 Voice VLAN 安全模式。

命令

switchport voice vlan security

no switchport voice vlan security

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用以太网端口 3 的 Voice VLAN 安全模式：

```
SW-5024(config)# interface gigabitEthernet 1/0/3
SW-5024(config-if)# switchport voice vlan security
```

10.7 show voice vlan

描述

该命令用于显示 Voice VLAN 全局配置。

命令

show voice vlan

模式

特权模式和所有配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

显示 Voice VLAN 全局配置信息：

```
SW-5024(config)# show voice vlan
```

10.8 show voice vlan oui

描述

该命令用于显示 Voice VLAN OUI 配置信息。

命令

show voice vlan oui

模式

特权模式和所有配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

显示 Voice VLAN OUI 配置信息：

SW-5024(config)# show voice vlan oui

10.9 show voice vlan switchport

描述

该命令用于显示以太网端口的 Voice VLAN 配置信息。

命令

show voice vlan switchport [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

参数

port —— 以太网端口。该参数缺省时，显示所有端口的配置信息。

port-channel-id —— 汇聚组号。

模式

特权模式和所有配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

显示所有端口和汇聚组的语音 VLAN 配置信息：

SW-5024(config)# show voice vlan switchport

显示端口 2 的语音 VLAN 中配置信息：

SW-5024(config)# show voice vlan switchport gigabitEthernet 1/0/2

第 11 章 EtherChannel 配置命令

EtherChannel 配置命令用于配置 LAG 和 LACP 功能。

LAG（Link Aggregation Group，端口汇聚组）是将交换机的多个物理端口汇聚成一个逻辑端口的功能，可以增加带宽，提高连接的可靠性。

LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是基于 IEEE 802.3ad 标准用来实现链路动态汇聚的协议。聚合的双方通过协议交互聚合信息，将匹配的链路聚合在一起收发数据，具有很高的灵活性并提供了负载均衡的能力。

11.1 channel-group

描述

该命令用于把端口添加到汇聚组，并设置其模式。它的 no 命令用于将端口从汇聚组移除。

命令

channel-group *num* **mode** { on | active | passive }

no channel-group

参数

num —— 汇聚组组号，取值范围 1-14。

on —— 开启静态 LAG。

active —— 开启主动模式 LACP。

passive —— 开启被动模式 LACP。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

添加端口 2-4 到汇聚组 1，并开启静态 LAG 模式：

```
SW-5024(config)# interface range gigabitEthernet 1/0/2-4

SW-5024(config-if-range)# channel-group 1 mode on
```

11.2 port-channel load-balance

描述

该命令用于选择汇聚组的负载均衡算法 。 它的 no 命令用于恢复默认值，即 src-dst-mac。

命令

port-channel load-balance { src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip }

no port-channel load-balance

参数

src-mac —— 源 MAC 地址。算法将基于源 MAC 地址实现负载均衡。

dst-mac —— 目的 MAC 地址。算法将基于目的 MAC 地址实现负载均衡。

src-dst-mac —— 源目的 MAC 地址。算法将基于源目的 MAC 地址实现负载均衡。

src-ip —— 源 IP 地址。算法将基于源 IP 地址实现负载均衡。

dst-ip —— 目的 IP 地址。算法将基于目的 IP 地址实现负载均衡。. src-dst-ip —— 源目的 IP 地址。算法将基于源目的 IP 地址实现负载均衡。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将 LAG 的负载均衡算法设置为 src-dst-ip：

```
SW-5024(config)# port-channel load-balance src-dst-ip
```

11.3 lacp system-priority

描述

该命令用于配置全局的 LACP 系统优先级，它的 no 命令用于恢复默认值。

命令

lacp system-priority *pri*

no lacp system-priority

参数

pri —— 系统优先级，取值范围 0-65535。默认值为 32768。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 LACP 的系统优先级为 1024：

SW-5024(config)# lacp system-priority 1024

11.4 lacp port-priority

描述

该命令用于配置 LACP 端口优先级，它的 no 命令用于恢复默认值。

命令

lacp port-priority *pri*

no lacp port-priority

参数

pri —— 端口优先级，取值范围 0-65535。默认值为 32768。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将端口 1-3 的端口优先级设置为 1024：

SW-5024(config)# interface range gigabitEthernet 1/0/1-3

SW-5024(config-if-range)# lacp port-priority 1024 将端口

4 的端口优先级设置为 2048：

SW-5024(config)# interface gigabitEthernet 1/0/4

SW-5024(config-if)# lacp port-priority 2048

11.5 show etherchannel

描述

该命令用于显示汇聚组信息。

命令

show etherchannel [*channel-group-num*] { detail | summary }

参数

channel-group-num —— 汇聚组组号，取值范围 1-14。该参数缺省时，显示所有组的信息。

detail —— 详述信息。

summary —— 概述信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示汇聚组 1 的详述信息：

```
SW-5024(config)# show etherchannel 1 detail
```

11.6 show etherchannel load-balance

描述

该命令用于显示 LAG 的负载均衡算法。

命令

show etherchannel load-balance

模式

特权模式和所有配置模式

特权要求

无

示例

显示 LAG 的负载均衡算法：

```
SW-5024(config)# show etherchannel load-balance
```

11.7 show lacp

描述

该命令用于显示特定汇聚组的 LACP 信息。

命令

show lacp [*channel-group-num*] { internal | neighbor }

参数

channel-group-num —— 组号，取值范围 1-14。该参数缺省时，显示所有 LACP 类型组的信息。

internal —— 本端 LACP 信息。

neighbor —— 对端 LACP 信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示汇聚组 1 的本端 LACP 信息：

```
SW-5024(config)# show lacp 1 internal
```

11.8 show lacp sys-id

描述

该命令用于显示 LACP 系统优先级。

命令

show lacp sys-id

模式

特权模式和所有配置模式

特权要求

无

示例

显示 LACP 系统优先级：

```
SW-5024(config)# show lacp sys-id
```

第 12 章用户管理配置命令

用户配置用来管理通过 Web、CLI 或 SSH 方式登录交换机的用户信息，以达到保护交换机配置的目的。

12.1 user name (password)

描述

该命令用于添加一个新用户账户或修改已存在的用户账户的信息，它的 no 命令用于删除已存在的账户。通过此命令可以使用对称加密算法加密用户登录密码。

命令

user name *name* [**privilege** admin | operator | power_user | user] **password** { [0] *password* | 7 *encrypted-password* }

no user name *name*

参数

name —— 用户名，1-16 个字符，只能由数字、英文字母和下划线组成。

admin | operator | power_user | user —— 用户类型，admin：管理员；operator：操作员；power_user：高级用户；user：普通用户。添加用户时，默认为 admin。有关特权要求限制的详细信息，请参阅每个命令中的**特权要求**部分。

0 —— 加密类型，0 表示接下来输入未经加密的密码。默认的加密类型为 0。

password —— 1～31 位的密码，由字母，数字和符号组成。密码区分大小写，可包括数字，英文字母（区分大小写），下划线和十六个特殊字符（!$%'()*,-./[]{|}）。

7 —— 加密类型，表示接下来需要输入一个固定长度的经过对称加密的密码。

encrypted-password —— 固定长度的经过对称加密的密码，可以从其他交换机的配置文件中复制得到。 配置了加密密码之后，当再次进入用户模式时，需要输入对应的未经加密的密码。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

说明

如果在此配置的密码为未加密的密码，但是通过 **service password-encryption** 命令启用了全局密码加密功能，那么交换机配置文件中的密码将会显示为对称加密格式。

示例

添加并启用一个用户名为 SUNDRAY，密码为不加密的 admin 的管理员账户：

SW-5024(config)#user name SUNDRAY **privilege** admin **password** 0 admin

12.2 user name (secret)

描述

该命令用于添加一个新用户账户或修改已存在的用户账户的信息，它的 no 命令用于删除已存在的账户。通过此命令添加的用户，其密码在配置文件中显示为 MD5 加密的格式。

命令

user name *name* [**privilege** admin | operator | power_user | user] **secret** { [0] *password* | 5 *encrypted-password* }

no user name *name*

参数

name —— 用户名，1-16 个字符，只能由数字、英文字母和下划线组成。

admin | operator | power_user | user —— 用户类型。“admin”用户可以编辑、修改和查看不同功能的所有设置。“operator”用户可以编辑、修改和查看大多数不同功能的设置。“power_user”用户可以编辑、修改和查看一些不同功能的设置。“user”用户只能查看一些不同功能的设置，无法编辑或修改。默认用户类型为“admin”。有关特权要求限制的详细信息，请参阅每个命令中的**特权要求**部分。

0 —— 加密类型，0 表示接下来输入未经加密的密码。默认的加密类型为 0。

password —— 1～31 位的密码，由字母，数字和符号组成。密码区分大小写，可包括数字，英文字母（区分大小写），下划线和十六个特殊字符（!$%'()*,-./[]{|}）。此密码在交换机的配置文件中显示为 MD5 加密的格式。

5 —— 加密类型，表示接下来需要输入一个固定长度的经过 MD5 加密的密码。

encrypted-password —— 固定长度的经过对称加密的密码，可以从其他交换机的配置文件中复制得到。 配置了加密密码之后，当再次进入用户模式时，需要输入对应的未经加密的密码。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

说明

如果同时在 **user name** (password)和 **user name** (secret)中配置了密码，则只有最新的配置会生效。

示例

添加并启用一个管理员帐户，用户名为 SUNDRAY，密码为不加密的 admin，此密码在交换机配置文件中以加密格式显示：.

SW-5024(config)#user name SUNDRAY **privilege** admin **secret** 0 admin

12.3 service password-recovery

描述

该命令用于启用账户恢复模式，启用后可以使用默认用户名和密码（都为 admin）通过连接 console 口登陆交换机，删除配置中设置的账户信息。它的 no 命令用于关闭账户恢复模式。

命令

service password-recovery

no service password-recovery

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

开启账户恢复模式：

SW-5024(config)# service password-recovery

12.4 user access-control ip-based

描述

该命令用于启用基于 IP 地址的身份限制，只有处于所设 IP 网段的设备才可以访问本交换机。它的 no 命令用于取消用户身份限制。

命令

user access-control ip-based { *ip-addr ip-mask* } [snmp] [telnet] [ssh] [http] [https] [ping] [all]

no user access-control [**ip-based index** *id*]

参数

ip-addr / ip-mask —— 源 IP 地址和 IP 掩码。只有处于所设 IP 网段的设备才可以访问本交换机。最多可以设置五个条目。

[snmp] [telnet] [ssh] [http] [https] [ping] [all] ——指定访问接口，默认情况下开启。

id ——删除指定条目。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

启用 IP 地址为 192.168.0.148 的身份限制：

SW-5024(config)# user access-control ip-based 192.168.0.148 255.255.255.255

12.5 user access-control mac-based

描述

该命令用于启用基于 MAC 地址的身份限制，只允许所设的 MAC 地址通过 Web 访问交换机。它的 no 命令用于取消用户身份限制。

命令

user access-control mac-based { *mac-addr* } [snmp] [telnet] [ssh] [http] [https] [ping] [all]

no user access-control

参数

mac-addr —— 源 MAC 地址。只有拥有该 MAC 地址的设备才可以访问本交换机。 [snmp] [telnet] [ssh] [http] [https] [ping] [all] ——指定访问接口，默认情
况下开启。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

启用 MAC 地址为 00:00:13:0A:00:01 的身份限制：

SW-5024(config) # user access-control mac-based 00:00:13:0A:00:01

12.6 user access-control port-based

描述

该命令用于启用基于端口的身份限制，只允许连接在所设的端口上的主机通过 WEB 访问交换机。使用 user access-control port-based interface none 命令，可关闭用户身份限制；使用 no user access-control 命令用于取消用户身份限制。

命令

user access-control port-based interface { **gigabitEthernet** *port-list* }
[snmp] [telnet] [ssh] [http] [https] [ping] [all]

no user access-control

参数

port-list —— 以太网端口列表，最多可指定 5 个端口。

[snmp] [telnet] [ssh] [http] [https] [ping] [all] ——指定访问接口，默认情况下开启。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

启用 2-6 五个端口的身份限制：

SW-5024(config)# user access-control port-based interface

gigabitEthernet 1/0/2-6

12.7 line

描述

该命令用于进入 line 配置模式，以配置用户的登录模式及连接密码等参数。

命令

line { **console** *linenum* | **vty** *startlinenum endlinenum* | **ssh** | **telnet** }

参数

linenum ——指定需要配置的 Console 口的端口号，本交换机只有一个 Console 口，故该值为 0。

startlinenum ——指定需要配置的虚拟终端连接的起始序号，取值范围为 0-15。0 表示从第一个通过 Telnet 或 SSH 登录的用户开始，配置生效；1 表示从第二个登录的用户开始，并依次类推。

endlinenum ——指定需要配置的虚拟终端连接的结束序号，取值范围为 0-15，并且不能小于 *startlinenum*。0 表示配置只对第一个通过 Telnet 或 SSH 登录的用户有效；1 表示到第二个登录的用户为止，配置有效，并依次类推。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

进入 Console 端口配置模式以配置 Console 口的连接密码等参数：

SW-5024(config)#line console 0

进入虚拟终端配置模式，配置前 6 个通过 Telnet 或 SSH 连接的用户的登录模式及连接密码等参数：

SW-5024(config)#line vty 0 5

12.8 password

描述

该命令用于配置连接密码，它的 no 命令用于清除密码。

命令

password { [0] *password* | 7 *encrypted-password* }

no password

参数

0 —— 一种加密类型，表示接下来需要输入没有进行加密的密码，0 为默认加密类型。

password —— 配置连接密码，由 1~31 个字符组成，密码区分大小写，允许输入数字、英文字母、下划线和十六种特殊字符（!$%'()*,-./[]{|}）。默认为空。

7 —— 表示使用固定长度的采用对称加密的密码。 *encrypted-password* ——固定长度的进行过对称加密的密码，可以从其他交换机

的配置文件中复制得到。配置了加密密码之后，当要再次进入此模式时，需要输入相应的未加密密码。

模式

line 配置模式

特权要求

只有管理员类型的用户可以使用该命令

说明

如果在此配置的密码为未加密的密码，但通过 **service password-encryption** 命令启用了全局密码加密功能，那么交换机配置文件中的密码将会显示为对称加密格式。

示例

配置 Console 端口 0 的连接密码为不加密密码“SUNDRAY”：

```
SW-5024(config)#line console 0
SW-5024(config-line)#password 0 SUNDRAY
```

配置虚拟终端连接 0-5 的连接密码为不加密密码“SUNDRAY”：

```
SW-5024(config)#line vty 0 5
SW-5024(config-line)#password 0 SUNDRAY
```

12.9 login

描述

该命令用于设置交换机登录模式为 login 模式，即无需输入登录用户名和密码，但是需要输入一个连接密码才能建立 Telnet 连接进行访问。

命令

login

模式

Line 配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置 Console 端口 0 的连接模式为 login：

```
SW-5024(config)#line console 0
SW-5024(config-line)#login
```

配置建立 Telnet 连接的模式为 login：

```
SW-5024(config)#line vty 0 5
SW-5024(config-line)#login
```

12.10 login local

描述

该命令用于设置交换机登录模式为 login local 模式，即输入用户名和密码登录，默认用户名/密码为 admin/admin。

命令

login local

模式

Line 配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置虚拟终端连接的登陆模式 login local：

SW-5024(config)#line vty 0 5

SW-5024(config-line)#login local

配置 Console 端口 0 的连接模式为 login local：

SW-5024(config)#line console 0

SW-5024(config-line)#login local

12.11 media-type rj45

描述

该命令用于提高 RJ45 类型的 Console 口的优先级。交换机配有 RJ45 和 micro-USB 两种类型的 Console 口。默认 Micro-USB 的优先级高于 RJ45，即当两个 Console 口同时连接，将只有 micro-USB 类型的 Console 口生效。它的 no 命令用于恢复默认配置。

命令

media-type rj45

no media-type rj45

模式

Line 配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

启用 RJ45 类型的 Console 口：

```
SW-5024(config)# line console 0
SW-5024(config-line)# media-type rj45
```

优先使用 micro-USB 类型的 Console 口：

```
SW-5024(config)# line console 0
SW-5024(config-line)# no media-type rj45
```

12.12 telnet

描述

该命令用于开启或关闭远程登录功能。默认开启。

命令

telnet enable

telnet disable

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

关闭远程登录功能：

```
SW-5024(config)# telnet disable
```

12.13 serial_port baud-rate

描述

该命令用于配置 Console 口通信的波特率。它的 no 命令用于恢复默认配置。

命令

serial_port baud-rate { 9600 | 19200 | 38400 | 57600 | 115200 }

no serial_port

参数

9600 | 19200 | 38400 | 57600 | 115200 —— 指定 Console 通信的波特率。默认值为 38400bps。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

恢复 Console 口通信波特率为默认值：

```
SW-5024(config)# no serial_port
```

12.14 show password-recovery

描述

该命令用于显示账户恢复模式的状态。

命令

show password-recovery

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示账户恢复模式的状态：

```
SW-5024(config)# show password-recovery
```

12.15 show user account-list

描述

该命令用于显示当前用户账户列表。

命令

show user account-list

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示当前用户账户列表：

```
SW-5024(config)# show user account-list
```

12.16 show user configuration

描述

该命令用于显示用户安全配置，包括身份限制，登录数限制，超时配置等。

命令

show user configuration

模式

特权模式和所有配置模式

特权要求

无

示例

显示用户安全配置：

```
SW-5024(config)# show user configuration
```

12.17 show telnet-status

描述

该命令用于显示远程登录功能的配置信息。

命令

show telnet-status

模式

特权模式和所有配置模式

特权要求

无

示例

显示用户安全配置：

```
SW-5024(config)# show telnet-status
```

第 13 章 HTTP 和 HTTPS 配置命令

在 HTTP（HyperText Transfer Protocol，超文本传输协议）或者 HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer，基于安全套接层的超文本传输协议）帮助下，可以通过一个标准的浏览器管理交换机。HTTP 是用于交换和发送超文本内容的协议。

SSL（Secure Sockets Layer，安全套接层）是一个安全协议，它为基于 TCP 的应用层协议（如 HTTP）提供安全连接。SSL 采用非对称加密技术，用密钥对进行信息的加密/解密，密钥对由一个公钥（包含在证书中）和一个私钥构成。初始时交换机里已有默认的证书（自签名证书）和对应私钥，用户也可以通过证书/密钥导入功能替换默认的密钥对。

13.1 ip http server

描述

该命令用于全局开启 HTTP 服务器功能，它的 no 命令用于禁用该功能。默认情况下启用此功能。HTTP 和 HTTPS 服务器不能同时禁用。

命令

ip http server

no ip http server

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

关闭 HTTP 功能：

```
SW-5024(config)# no ip http server
```

13.2 ip http max-users

描述

该命令用于配置允许连接到 HTTP 服务器的最大用户数，它的 no 命令用于取消限制。

命令

ip http max-users *admin-num guest-num*

no ip http max-users

参数

admin-num —— 以管理员身份登录到 HTTP 服务器的最大数量，范围从 1 到 16。全部用户的总数应该少于 16。

guest-num ——以客人身份登录到 HTTP 服务器的最大数量，范围从 0 到 15。全部用户的总数应小于 16。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

配置管理员和客人登陆到 HTTP 服务器的最大数量为 5 和 3：

SW-5024(config)# ip http max-users 5 3

13.3 ip http session timeout

描述

该命令用于配置 HTTP 服务器的连接超时时间。它的 no 命令可以恢复出厂默认的超时时间，默认的超时时间为 10 分钟。

命令

ip http session timeout *time*

no ip http session timeout

参数

time —— 超时时间，范围从 5 到 30 分钟。默认情况下，该值为 10。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

配置 HTTP 连接超时时间为 15 分钟：

SW-5024(config)# ip http session timeout 15

13.4 ip http secure-server

描述

该命令用于全局开启 SSL 功能，它的 no 命令用于禁用该功能。默认情况下启用此功能。HTTP 和 HTTPS 服务器不能同时禁用。

命令

ip http secure-server

no ip http secure-server

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局关闭 SSL 功能：

SW-5024(config)# no ip http secure-server

13.5 ip http secure-protocol

描述

该命令用于配置 SSL 协议版本，它的 no 命令用于恢复默认 SSL 版本。默认情况下，交换机支持 SSLv3 和 TLSv1。

命令

ip http secure-protocol { [ssl3] [tls1] }

no ip http session

参数

ssl3 ——SSL 3.0 协议。

tls1 ——TLS 1.0 协议。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 SSL 连接使用的协议为 SSL 3.0：

SW-5024(config)# ip http secure-protocol ssl3

13.6 ip http secure-ciphersuite

描述

该命令用于配置交换机支持的 SSL 连接的密码套件，它的 no 命令用于恢复默认密码套件。

命令

ip http secure-ciphersuite { [3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha] }

no ip http secure-ciphersuite

参数

[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha] ——指定 SSL 连接使用的加密算法和摘要算法。

默认情况下，交换机支持所有这些密码套件。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 SSL 连接使用的密码套件为 3des-ede-cbc-sha：

SW-5024(config)# ip http secure-ciphersuite 3des-ede-cbc-sha

13.7 ip http secure-max-users

描述

该命令用于配置允许连接到 HTTPS 服务器的最大用户数，它的 no 命令用于取消限制。

命令

ip http secure-max-users *admin-num guest-num*

no ip secure-max-users

参数

admin-num —— 以管理员身份登录到 HTTPS 服务器的最大数量，范围从 1 到 16。全部用户的总数应该少于 16。

guest-num —— 以客人身份登录到 HTTPS 服务器的最大数量，范围从 0 到 15。全部用户的总数应小于 16。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置管理员和客人登录到 HTTPS 服务器的最大数量为 5 和 3：

```
SW-5024(config)# ip http secure-max-users 5 3
```

13.8 ip http secure-session timeout

描述

该命令用于配置 HTTPS 服务器的连接超时时间。它的 no 命令可以恢复出厂默认的超时时间，默认的超时时间为 10 分钟。

命令

ip http secure-session timeout *time*

no ip http secure-session timeout

参数

minutes ——超时时间，范围从 5 到 30 分钟。默认情况下，该值为 10。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 HTTPS 连接超时时间为 15 分钟：

SW-5024(config)# ip http secure-session timeout 15

13.9 ip http secure-server download certificate

描述

该命令用于通过 TFTP 方式导入 SSL 证书。

命令

ip http secure-server download certificate *ssl-cert* **ip-address** *ip-addr*

参数

ssl-cert —— 选择要导入的 SSL 证书名称，可输入 1~25 个字符。证书必须为 BASE64 编码格式。

ip-addr —— TFTP 服务器的 IP 地址。支持 IPv4 和 IPv6 地址。例如 IPv4 地址 192.168.0.10 或 fe80::1234。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

通过 IP 地址为 192.168.0.146 的 TFTP 服务器导入名为 ssl-cert 的 SSL 证书：

SW-5024(config)# ip http secure-server download certificate ssl-cert **ip-address** 192.168.0.146

通过 IP 地址为 fe80::1234 的 TFTP 服务器导入名为 ssl-cert 的 SSL 证书：

SW-5024(config)# ip http secure-server download certificate ssl-cert **ip-address** fe80::1234

13.10 ip http secure-server download key

描述

该命令用于通过 TFTP 方式导入 SSL 密钥。

命令

ip http secure-server download key *ssl-key* **ip-address** *ip-addr*

参数

ssl-key —— 选择要导入的 SSL 密钥文件名称，可输入 1~25 个字符。密钥必须为 BASE64 编码格式。

ip-addr —— TFTP 服务器的 IP 地址。支持 IPv4 和 IPv6 地址。例如 IPv4 地址 192.168.0.10 或 fe80::1234。

模式

全局配置模式、

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

通过 IP 地址为 192.168.0.146 的 TFTP 服务器导入名为 ssl-key 的 SSL 密钥：

SW-5024(config)# ip http secure-server download key ssl-key **ip-address** 192.168.0.146

通过 IP 地址为 fe80::1234 的 TFTP 服务器导入名为 ssl-key 的 SSL 密钥：

SW-5024(config)# ip http secure-server download key ssl-key **ip-address** fe80::1234

13.11 show ip http configuration

描述

该命令是用来显示的 HTTP 服务器的配置信息，包括状态、会话超时时间、访问控制、最大用户数和空闲超时时间等。

命令

show ip http configuration

模式

特权模式和所有配置模式

特权要求

无

示例

显示 HTTP 服务器的配置信息：

```
SW-5024(config)# show ip http configuration
```

13.12 show ip http secure-server

描述

该命令用于显示 SSL 的全局配置信息。

命令

show ip http secure-server

模式

特权模式和所有配置模式

特权要求

无

示例

显示 SSL 全局配置信息：

```
SW-5024(config)# show ip http secure-server
```

第 14 章 ARP 配置命令

ARP（Address Resolution Protocol，地址解析协议）是将 IP 地址解析为以太网 MAC 地址的协议。交换机维护一个 IP 到 MAC 关系的映射表，该映射表用于转发 IP 数据包时下一跳地址的解析。ARP 映射表包含两种类型的 ARP 表项：动态和静态 ARP 表项。动态 ARP 表项由 ARP 报文自动生成和维护，静态 ARP 表项通过手工配置和维护。

14.1 arp

描述

该命令用于添加静态 ARP 表项。No 命令用于删除 ARP 表项。

命令

arp *ip mac type*

no arp *ip type*

参数

ip —— 静态 ARP 表项的 ip 地址。

mac —— 静态 ARP 表项的 mac 地址。

type —— ARP 的类型，设置为“arpa”。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建一条静态 ARP 表项，其中 IP 地址为 192.168.0.1，MAC 地址为 00:11:22:33:44:55：

SW-5024(config)# arp 192.168.0.1 00:11:22:33:44:55 arpa

14.2 clear arp-cache

描述

该命令用于删除所有的动态 ARP 表项。

命令

clear arp-cache

模式

特权模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

删除所有的动态 ARP 表项：

SW-5024(config)# clear arp-cache

14.3 arp timeout

描述

该命令用于配置三层接口的 ARP 老化时间。

命令

arp timeout *timeout*

no arp timeout

参数

timeout —— 指定老化时间，范围从 1 秒到 3000 秒。默认值为 600 秒。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置接口 1 的 ARP 老化时间为 60 秒：

SW-5024(config)# interface gigabitEthernet 1/0/1

SW-5024(config-if)# arp timeout 60

14.4 show arp

描述

该命令用于显示 ARP 表项。如果没有指定参数，将显示所有的 ARP 表项。

命令

show arp [*ip*] [*mac*]

show ip arp [*ip*] [*mac*]

参数

ip —— 指定需要显示的 ARP 表项的 IP 地址。

mac —— 指定需要显示的 ARP 表项的 MAC 地址。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 IP 地址为 192.168.0.2 的 ARP 表项：

SW-5024(config)# show ip arp 192.168.0.2

14.5 show ip arp (interface)

描述

该命令用于显示指定三层接口的 ARP 表项。

命令

show ip arp { **gigabitEthernet** *port* | **port-channel** *port-channel-id* | **vlan** *id* }

参数

port ——指定端口。

port-channel-id —— 指定端口组 ID。

id ——指定 VLAN ID。

模式

特权模式和所有配置模式

特权要求

无

示例

显示接口 VLAN 2 的 ARP 表项：

```
SW-5024(config)# show ip arp vlan 2
```

14.6 show ip arp summary

描述

该命令用于显示 ARP 表项的条目数。

命令

show ip arp summary

模式

特权模式和所有配置模式

特权要求

无

示例

显示 ARP 表项的条目数：

```
SW-5024(config)# show ip arp summary
```

第 15 章绑定列表配置命令

四元绑定功能可以将局域网中计算机的 IP 地址、MAC 地址、VLAN 和端口进行绑定，IP 源防护功能将使用四元绑定条目对数据包进行过滤。

15.1 ip source binding

描述

该命令用于手动添加 IP-MAC-VID-PORT 四元绑定条目。如果已经掌握了局域网中计算机用户的相关信息，包括 IP 地址、MAC 地址、VLAN 以及连接端口等，可以手动四元绑定。它的 no 命令可将 IP-MAC-VID-PORT 四元绑定条目从列表中删除。

命令

ip source binding *hostname ip-addr mac-addr* **vlan** *vlan-id* **interface gigabitEthernet** *port* { none | arp-detection | ip-verify-source | both } [**forced-source** { arp-scanning | dhcp-snooping }]

no ip source binding index *idx*

参数

hostname —— 需要绑定的主机名，1-20 个字符。

ip-addr —— 源 IP 地址。

mac-addr —— 源 MAC 地址。

vlan-id —— 需要绑定的 VLAN，取值范围 1-4094。

port —— 需要绑定的交换机端口号。

none | arp-detection | ip-verify-source | both —— 该条目执行的 ACL 动作，arp-detection 表示 ARP 防护；ip-verify-source 表示 IP 源防护；both 表示两种防护均生效；none 表示不应用防护。

forced-source —— 可选参数。forced-source 用于强制将新添加条目的来源从 manual 修改为 arp-scanning 或者 dhcp-snooping，以模拟 arp-scan 或 dhcp-snooping 添加绑定条目，使非手动绑定条目可以保存配置。

idx —— 指定要删除的条目序号。可使用命令 **show ip source binding** 获取各条目对应的序号。注意，这里的序号是指该条目在绑定表中的序号，故显示时不一定是按习惯上的从小到大递增的顺序，而是显示该条目在绑定表中的实际序号。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

手动添加一条四元绑定条目，主机名为 host1，IP 地址为 192.168.0.1，MAC 地址为 00:00:00:00:00:01，VID 为 2，端口号为 5，并将该条目同时应用于 IP 源防护：

SW-5024(config)#ip source binding host1 192.168.0.1 00:00:00:00:00:01

vlan 2 **interface gigabitEthernet** 1/0/5 arp-detection

删除 unit1 的绑定表中序号为 5 的 IP-MAC –VID-PORT 条目：

SW-5024(config)#no ip source binding index 5

15.2 ip dhcp snooping

描述

该命令用于全局开启 DHCP 侦听功能，它的 no 命令用于禁用 DHCP 侦听功能。通过 DHCP 侦听功能，交换机可以侦听用户动态申请 IP 地址的过程，并记录局域网中计算机的 IP 地址、MAC 地址、VLAN 以及连接端口等信息，自动进行四元绑定。

命令

ip dhcp snooping

no ip dhcp snooping

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局开启 DHCP 侦听功能：

SW-5024(config)#ip dhcp snooping

15.3 ip dhcp snooping vlan

描述

该命令用于开启 VLAN 中的 DHCP 侦听，使用它的 no 命令可关闭该功能。

命令

ip dhcp snooping vlan *vlan-range*

no ip dhcp snooping vlan *vlan-range*

参数

vlan-range—— 指定 VLAN 开启 DHCP 侦听功能，格式为 1-3,5。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启 VLAN1,4,6-7 的 DHCP 侦听功能：

SW-5024(config)#ip dhcp snooping vlan 1,4,6-7

15.4 ip dhcp snooping information option

描述

该命令用于开启 DHCP 侦听的 Option 82 功能，它的 no 命令用于关闭 Option 82 功能。

命令

ip dhcp snooping information option

no ip dhcp snooping information option

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

在端口 1/0/1 上开启 DHCP 侦听的 Option 82 功能：

```
SW-5024(config)#interface gigabitEthernet 1/0/1 SW-
5024(config-if)#ip dhcp snooping information option
```

15.5 ip dhcp snooping information strategy

描述

该命令用于选择对接收到的包含 Option 82 选项请求报文的配置处理策略，它的 no 命令用于恢复默认选项。

命令

ip dhcp snooping information strategy *strategy*

no ip dhcp snooping information strategy

参数

strategy —— 对接收到的包含 Option 82 选项请求报文的配置处理策略，包括三种类型：

keep：保持该报文中的 Option 82 选项不变并进行转发。默认选项。

replace：按照配置的填充内容填充 Option 82 选项，并替换报文中原有的 Option 82 选项进行转发。

drop：丢弃含有 Option 82 选项的报文。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将接收到的请求报文的 Option 82 选项替换为用户自定义的选项内容，并从 1/0/1 端口转发：

SW-5024(config)#interface gigabitEthernet 1/0/1 **SW-5024(config-if)#ip dhcp snooping information strategy** replace

15.6 ip dhcp snooping information remote-id

描述

该命令用于配置 Option 82 的远程 ID 子选项内容。no 命令用于恢复默认值。

命令

ip dhcp snooping information remote-id *string*

no ip dhcp snooping information remote-id

参数

string —— 用户自定义配置的远程 ID 子选项内容。最多包含 64 个字符。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

在端口 1/0/1 上配置 Option 82 的远程 ID 子选项为 SUNDRAY：

SW-5024(config)#interface gigabitEthernet 1/0/1 **SW-5024(config-if)#ip dhcp snooping information remote-id** SUNDRAY

15.7 ip dhcp snooping information circuit-id

描述

该命令用于配置 Option 82 的电路 ID 子选项内容。no 命令用于恢复默认值。

命令

ip dhcp snooping information circuit-id *string*

no ip dhcp snooping information circuit-id

参数

string —— 用户自定义配置的电路 ID 子选项内容。最多包含 64 个字符。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

在接口 1/0/1 上配置 Option 82 的电路 ID 子选项为 SUNDRAY：

SW-5024(config)#interface gigabitEthernet 1/0/1 **SW-5024(config-if)#ip dhcp snooping information circuit-id** SUNDRAY

15.8 ip dhcp snooping trust

描述

该命令用于配置端口为授信端口，只有授信端口才能接收来自 DHCP 服务器端的消息，它的 no 命令用于取消授信端口配置。

命令

ip dhcp snooping trust

no ip dhcp snooping trust

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用交换机端口 1/0/2 为授信端口：

SW-5024(config)#interface gigabitEthernet 1/0/2

SW-5024(config-if)#ip dhcp snooping trust

15.9 ip dhcp snooping mac-verify

描述

该命令用于启用端口的 MAC 验证功能，它的 no 命令用于禁用 MAC 验证。DHCP 消息中有两个字段存储着客户端的 MAC 地址，MAC 验证功能会对这两个字段进行比较，如果不同，则将消息丢弃。

命令

ip dhcp snooping mac-verify

no ip dhcp snooping mac-verify

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用端口 1/0/2 的 MAC 验证功能：

SW-5024(config)#interface gigabitEthernet 1/0/2

SW-5024(config-if)#ip dhcp snooping mac-verify

15.10 ip dhcp snooping limit rate

描述

该命令用于配置端口的流量控制，超出流量部分的 DHCP 数据包将被丢弃，它的 no 命令用于恢复默认配置。

命令

ip dhcp snooping limit rate *value*

no ip dhcp snooping limit rate

参数

value —— 端口流量控制，可选项为 0、5、10、15、20、25、30，单位 pps（packet per second）。默认值为 0，表示禁用。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将端口 2 的流量控制设为 20pps：

SW-5024(config)#interface gigabitEthernet 1/0/2

SW-5024(config-if)#ip dhcp snooping limit rate 20

15.11 ip dhcp snooping decline rate

描述

该命令用于启用端口的 decline 侦听功能，它的 no 命令用于禁用 decline 侦听。

命令

ip dhcp snooping decline rate *value*

no ip dhcp snooping decline rate

参数

value ——DHCP Decline 包流量控制，可选项为 0、5、10、15、20、25、30，单位 pps（packet per second）。默认值为 0，表示禁用。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用端口 1/0/2 的 decline 侦听功能，并设置包流量控制为 20：

SW-5024(config)#interface gigabitEthernet 1/0/2

SW-5024(config-if)#ip dhcp snooping decline 20

15.12 show ip source binding

描述

该命令用于显示 IP-MAC-VID-PORT 四元绑定表。

命令

show ip source binding

模式

特权模式和所有配置模式

特权要求

无

示例

显示 IP-MAC-VID-PORT 四元绑定表：

```
SW-5024(config)#show ip source binding
```

15.13 show ip dhcp snooping

描述

该命令用于显示 DHCP 侦听的当前状态信息。

命令

show ip dhcp snooping

模式

特权模式和所有配置模式

特权要求

无

示例

显示 DHCP 侦听的当前状态信息：

```
SW-5024#show ip dhcp snooping
```

15.14 show ip dhcp snooping interface

描述

该命令用于显示对应以太网口/链路聚合或所有以太网口/链路聚合的 DHCP 侦听的端口配置信息。

命令

show ip dhcp snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

参数

port —— 交换机端口号，缺省时显示所有端口的配置信息。

port-channel-id —— 端口组的 ID。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口/端口组的 DHCP 侦听配置信息：

SW-5024#show ip dhcp snooping interface

显示端口 1/0/5 的 DHCP 侦听配置信息：

SW-5024#show ip dhcp snooping interface gigabitEthernet 1/0/5

15.15 show ip dhcp snooping information interface

描述

该命令用于显示对应以太网口/链路聚合或所有以太网口/链路聚合的 DHCP 侦听的 option 82 功能的端口配置信息。

命令

show ip dhcp snooping information interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

参数

port —— 交换机端口号，缺省时显示所有端口的配置信息。

port-channel-id —— 端口组的 ID。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口/端口组的 DHCP 侦听的 option 82 功能的配置信息：

SW-5024#show ip dhcp snooping information interface 显

示端口 1/0/5 的 DHCP 侦听的 option 82 功能的配置信息：

SW-5024#show ip dhcp snooping information interface gigabitEthernet

1/0/5

第 16 章 IPv6 绑定列表配置命令

IPv6 四元绑定功能可以将局域网中计算机的 IPv6 地址、MAC 地址、VLAN 和端口进行绑定，邻居检测防护功能以及 IPv6 源防护功能将使用四元绑定条目对数据包进行过滤。

16.1 ipv6 source binding

描述

该命令用于手动添加 IPv6-MAC-VID-PORT 四元绑定条目。如果已经掌握了局域网中计算机用户的相关信息，包括 IPv6 地址、MAC 地址、VLAN 以及连接端口等，可以手动四元绑定。它的 no 命令可将 IP-MAC-VID-PORT 四元绑定条目从列表中删除。

命令

ipv6 source binding *hostname ipv6-addr mac-addr* **vlan** *vlan-id* **interface gigabitEthernet** *port* { none | nd-detection | ipv6-verify-source | both }

no ipv6 source binding index *idx*

参数

hostname —— 需要绑定的主机名，1-20 个字符。

ipv6-addr —— 源 IPv6 地址。

mac-addr —— 源 MAC 地址。

vlan-id —— 需要绑定的 VLAN 的 VID，取值范围 1-4094。

port ——需要绑定的交换机端口号。

none | nd-detection | ipv6-verify-source | both —— 该条目执行的 ACL 动作，nd-detection 表示邻居检测防护；ipv6-verify-source 表示 IPv6 源防护；both 表示两种防护均生效；none 表示不启用防护。

idx —— 指定要删除的条目序号。可以使用命令 **show ipv6 source binding** 获取个条目的对应序号。注意，这里的序号是指该条目在绑定列表中的序号，故显示时不一定是按习惯上的从小到大递增的顺序，而是显示该条目在绑定表中的实际序号。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

手动添加一条四元绑定条目，主机名为 host1，IPv6 地址为 2001::1，MAC 地址为 00:00:00:00:00:01，VID 为 2，端口号为 5，并将该条目同时应用于邻居检测防护：

SW-5024(config)#ipv6 source binding host1 2001::1 00:00:00:00:00:01

vlan 2 **interface gigabitEthernet** 1/0/5 nd-detection

删除绑定列表中序号为 5 的 IPv5-MAC-VID-PORT 条目：

SW-5024(config)#no ipv6 source binding index 5

16.2 ipv6 dhcp snooping

描述

该命令用于全局开启 DHCPv6 侦听功能，它的 no 命令用于禁用 DHCPv6 侦听功能。通过 DHCPv6 侦听功能。交换机可以侦听用户动态申请 IPv6 地址的过程，并记录局域网中极端及的 IPv6 地址、MAC 地址、VLAN 以及连接端口等信息，自动进行四元绑定。

命令

ipv6 dhcp snooping

no ipv6 dhcp snooping

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局开启 DHCPv6 侦听功能：

SW-5024(config)#ipv6 dhcp snooping

16.3 ipv6 dhcp snooping vlan

描述

该命令用于开启 VLAN 中的 DHCPv6 侦听功能，他的 no 命令用于禁用此功能。

命令

ipv6 dhcp snooping vlan *vlan-range*

no ipv6 dhcp snooping vlan *vlan-range*

参数

vlan-range —— 指定开启 DHCPv6 功能的 VLAN 的 VLAN ID，格式为 1-3，5。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

在 VLAN1，4，6，7 中开启 DHCPv6 侦听功能：

SW-5024(config)#ipv6 dhcp snooping vlan 1,4,6-7

16.4 ipv6 dhcp snooping trust

描述

该命令用于配置端口为授信端口，只有授信端口才能接受来自 DHCPv6 服务器的消息，他的 no 命令用于取消授信端口配置。

命令

ipv6 dhcp snooping trust

no ipv6 dhcp snooping trust

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置交换机端口 2 为授信端口：

```
SW-5024(config)#interface gigabitEthernet 1/0/2
SW-5024(config-if)#ipv6 dhcp snooping trust
```

16.5 ipv6 nd snooping

描述

该命令用于全局启用间距检测侦听功能，它的 no 命令用于禁用此功能。通过间距检测侦听功能，交换机可以侦听重复地址检测的过程，并记录局域网中极端及的 IPv6 地址、MAC 地址、VLAN 以及连接端口等信息，自动进行四元绑定。

命令

ipv6 nd snooping

no ipv6 nd snooping

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局开启邻居检测侦听功能：

```
SW-5024(config)#ipv6 nd snooping
```

16.6 ipv6 nd snooping vlan

描述

该命令用于开启 VLAN 中的邻居检测侦听功能，使用它的 no 命令可以关闭该功能。

命令

ipv6 nd snooping vlan *vlan-range*

no ipv6 nd snooping vlan *vlan-range*

参数

vlan-range —— 指定开启邻居检测防护功能的 VLAN 的 VLAN ID，格式为 1-3，5。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

在 VLAN1，4，,6，7 中开启邻居检测侦听功能 **SW-**

5024(config)#ipv6 nd snooping vlan 1,4,6-7

16.7 ipv6 nd snooping max-entries

描述

命令用于设置单个端口允许绑定的邻居检测侦听条目的最大条目数，它的 no 命令用于恢复默认配置。

命令

ipv6 nd snooping max-entries *value*

no ipv6 nd snooping max-entries

参数

value —— 指定端口允许绑定的邻居检测侦听条目的最大条目数。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置端口 2 允许绑定的邻居检测侦听条目的最大条目数为 100：

```
SW-5024(config)#interface gigabitEthernet 1/0/2 SW-
5024(config-if)#ipv6 nd snooping max-entries 100
```

16.8 show ipv6 source binding

描述

该命令用于显示 IPv6-MAC-VID-PORT 四元绑定表。

命令

show ipv6 source binding

模式

特权模式和所有配置模式

特权要求

无

示例

显示 IPv6-MAC-VID-PORT 四元绑定表：

```
SW-5024(config)#show ipv6 source binding
```

16.9 show ipv6 dhcp snooping

描述

该命令用于显示 DHCPv6 侦听的当前状态信息。

命令

show ipv6 dhcp snooping

模式

特权模式和所有配置模式

特权要求

无

示例

显示 DHCPv6 侦听的当前状态信息：

SW-5024#show ipv6 dhcp snooping

16.10 show ipv6 dhcp snooping interface

描述

该命令用于显示对应以太网口/链路聚合或所有以太网口/链路聚合的 DHCPv6 侦听的端口配置信息。

命令

show ipv6 dhcp snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

参数 s

port —— 交换机端口号，缺省时显示所有端口的配置信息。

port-channel-id —— 链路聚合的 ID 号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口的/链路聚合的 DHCPv6 侦听配置信息：

SW-5024#show ipv6 dhcp snooping interface

显示端口 1/0/5 的 DHCPv6 侦听配置信息：

SW-5024#show ipv6 dhcp snooping interface gigabitEthernet 1/0/5

16.11 show ipv6 nd snooping

描述

该命令用于显示 IPv6 邻居检测侦听的当前状态信息。

命令

show ipv6 nd snooping

模式

特权模式和所有配置模式

特权要求

无

示例

显示 IPv6 邻居检测侦听的当前状态信息：

```
SW-5024#show ipv6 nd snooping
```

16.12 show ipv6 nd snooping interface

描述

该命令用于显示对应以太网口/链路聚合或所有以太网口/链路聚合的 IPv6；邻居检测侦听的端口配置信息。

命令

show ipv6 nd snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

参数

port —— 交换机端口号，缺省时显示所有端口的配置信息。

port-channel-id —— 链路聚合的 ID 号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口的/链路聚合的 IPv6 邻居检测侦听配置信息：

```
SW-5024#show ipv6 nd snooping interface
```

显示端口 1/0/5 的 IPv6 邻居检测侦听配置信息：

SW-5024#show ipv6 nd snooping interface gigabitEthernet 1/0/5

第 17 章 IP 源防护配置命令

IP 源防护基于 IP-MAC 绑定条目过滤 IP 数据包，只有满足 IP-MAC 绑定规则的数据报文才能被处理，从而可以提高带宽利用率。

17.1 ip verify source

描述

该命令用于配置特定端口的 IP 源防护模式。它的 **no** 命令用于禁用此功能。

命令

ip verify source { sip+mac }

no ip verify source

参数

sip+mac —— 只处理源 IP 地址、源 MAC 地址和端口均符合四元绑定信息的数据包。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用端口 5-10 的 IP 源防护功能的。配置防护模式为仅处理源 IP 地址，源 MAC 地址和端口号匹配 IP-MAC 绑定规则的数据包：

SW-5024(config)#interface range gigabitEthernet 1/0/5-10

SW-5024(config-if-range)#ip verify source sip+mac

17.2 show ip verify source

描述

该命令用以显示 IP 源防护配置信息。

命令

show ip verify source

模式

特权模式和所有配置模式

特权要求

无

示例

显示 IP 源防护配置信息：

```
SW-5024(config)#show ip verify source
```

17.3 show ip verify source interface

描述

该命令用以显示交换机端口的 IP 源防护配置信息。

命令

show ip verify source interface gigabitEthernet *port*

参数

port —— 交换机端口号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示减缓及端口 5 的 IP 源防护配置信息：

```
SW-5024#show ip verify source interface gigabitEthernet 1/0/5
```

第 18 章 IPv6 源防护配置命令

IPv6 源防护功能是交换机根据 IPv6 四元绑定条目对接收的 IPv6 包进行过滤，只处理数据包相关字段与 IPv6 四元绑定表吻合的数据包，提高交换机带宽资源的利用率。

配置 IPv6 源防护前，需要先将 SDM 模板设置为“enterpriseV6”并保存配置。

18.1 ipv6 verify source

描述

该命令用于启用端口的 IPv6 源防护功能，它的 no 命令用于禁用端口的 IPv6 源防护。

命令

ipv6 verify source { sipv6+mac }

no ipv6 verify source

参数

sipv6+mac —— 防护类型，sipv6+mac 表示只有源 IPv6 地址、MAC 地址和端口号均与 IPv6 四元绑定匹配的数据包才能被交换机处理。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

在端口 5-10 启用 IPv6 源防护并设定只处理 IPv6 地址、MAC 地址和端口号均匹配 IPv6 四元绑定的数据包：

```
SW-5024(config)#interface range gigabitEthernet 1/0/5-10
SW-5024(config-if-range)#ipv6 verify source sipv6+mac
```

18.2 show ipv6 verify source

描述

该命令用于显示 IPv6 源防护的配置信息。

命令

show ipv6 verify source

模式

特权模式和所有配置模式

特权要求

无

示例

显示 IPv6 源防护配置信息：

```
SW-5024(config)#show ipv6 verify source
```

18.3 show ipv6 verify source interface

描述

该命令用于显示指定端口的 IPv6 源防护配置信息。

命令

show ipv6 verify source interface gigabitEthernet *port*

参数

port —— 交换机端口号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示端口 5 的 IPv6 源防护配置信息：

```
SW-5024#show ipv6 verify source interface gigabitEthernet 1/0/5
```

第 19 章 ARP 防护配置命令

防 ARP 欺骗功能可以针对局域网中常见的网关欺骗和中间人攻击等 ARP 欺骗进行防护，有效抑制局域网中的 ARP 欺骗。

19.1 ip arp inspection(global)

描述

该命令用于全局开启 ARP 防护，它的 no 命令用于禁用 ARP 防护功能。

命令

ip arp inspection

no ip arp inspection

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局开启 ARP 防护：

```
SW-5024(config)#ip arp inspection
```

19.2 ip arp inspection trust

描述

该命令用于配置 ARP 防护的信任端口，它的 no 命令用于清空信任端口列表。上联端口、路由端口以及 LAG 端口等特殊端口均应配置为信任端口。在启用防 ARP 欺骗功能之前，应先配置 ARP 信任端口，以免影响正常通信。

命令

ip arp inspection trust

no ip arp inspection trust

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置端口 2-5 为 ARP 防护的信任端口：

```
SW-5024(config)#interface range gigabitEthernet 1/0/2-5
SW-5024(config-if-range)#ip arp inspection trust
```

19.3 ip arp inspection(interface)

描述

该命令用于开启端口的 ARP 防护功能，它的 no 命令用于禁用 ARP 防护功能。

命令

ip arp inspection

no ip arp inspection

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启端口 2-6 的 ARP 防护功能：

```
SW-5024(config)#interface range gigabitEthernet 1/0/2-6
SW-5024(config-if-range)#ip arp inspection
```

19.4 ip arp inspection limit-rate

描述

该命令用于配置端口的 ARP 超速速率，它的 no 命令用于恢复默认超速速率。

命令

ip arp inspection limit-rate *value*

no ip arp inspection limit-rate

参数

value —— 超速速率值，取值范围 10-100，单位 pps（packet/second）。默认值为 15。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将端口 5 的 ARP 超速速率设置为 50pps：

SW-5024(config)#interface gigabitEthernet 1/0/5

SW-5024(config-if)#ip arp inspection limit-rate 50

19.5 ip arp inspection recover

描述

该命令用于将处于 ARP 过滤状态的端口恢复为 ARP 转发状态。

命令

ip arp inspection recover

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将端口 5 恢复为 ARP 转发状态：

SW-5024(config)#interface gigabitEthernet 1/0/5

SW-5024(config-if)#ip arp inspection recover

19.6 show ip arp inspection

描述

该命令用于显示 ARP 防护全局配置，包括启用状态和信任端口列表。

命令

show ip arp inspection

模式

特权模式和所有配置模式

特权要求

无

示例

显示 ARP 防护全局配置：

```
SW-5024(config)#show ip arp inspection
```

19.7 show ip arp inspection interface

描述

该命令用于显示 ARP 防护端口配置信息。

命令

show ip arp inspection interface [**gigabitEthernet** *port*]

参数

port—— 交换机端口号，缺省时显示所有端口的配置信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示端口 1 的 ARP 防护配置信息：

SW-5024(config)#show ip arp inspection interface gigabitEthernet 1/0/1

显示所有端口的 ARP 防护配置信息：

SW-5024(config)#show ip arp inspection interface

19.8 show ip arp inspection statistics

描述

该命令用于显示 ARP 非法报文统计。

命令

show ip arp inspection statistics

模式

特权模式和所有配置模式

特权要求

无

示例

显示 ARP 非法报文统计：

SW-5024(config)#show ip arp inspection statistics

19.9 clear ip arp inspection statistics

描述

该命令用于对 ARP 非法报文统计进行清零。

命令

clear ip arp inspection statistics

模式

特权模式和所有配置模式

特权要求

无

示例

对 ARP 非法报文统计进行清零：

```
SW-5024(config)#clear ip arp inspection statistics
```

第 20 章 DoS 防护命令

DoS 攻击是指网络中攻击者或者恶意程序向目标主机发送大量的服务请求，恶意消耗网络资源。启用 DoS 防护功能后，交换机对收到的特殊数据包的特定字段进行解析，并针对这些信息定义防护措施，从而保护局域网的正常运行。

20.1 ip dos-prevent

描述

该命令用于全局启用 DoS 防护功能，它的 no 命令用于禁用 DoS 防护功能。

命令

ip dos-prevent

no ip dos-prevent

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局启用 DoS 防护功能：

```
SW-5024(config)#ip dos-prevent
```

20.2 ip dos-prevent type

描述

该命令用于选择启用 DoS 攻击防护类型，它的 no 命令用于禁用相应的防护类型。

命令

ip dos-prevent type { land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke }

no ip dos-prevent type { land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke }

参数

land —— Land 攻击。

scan-synfin —— Scan SYNFIN 攻击。

xma-scan —— Xma Scan 攻击。

null-scan —— NULL Scan 攻击。

port-less-1024 —— 源端口小于 1024 的 SYN 报文。

blat —— Blat 攻击。

ping-flood —— Ping flooding 攻击。

syn-flood —— SYN/SYN-ACK flooding 攻击。

win-nuke —— winNuke 攻击。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用 Land 攻击防护功能：

SW-5024(config)#ip dos-prevent type land

20.3 show ip dos-prevent

描述

该命令用于显示 DoS 攻击防护全局配置信息，包括启用状态、攻击防护类型等。

命令

show ip dos-prevent

模式

特权模式和所有配置模式

特权要求

无

示例

显示 DoS 攻击防护全局配置信息：

SW-5024(config)#show ip dos-prevent

第 21 章 IEEE 802.1X 配置命令

IEEE 802.1X 能为局域网计算机提供认证功能，并根据认证结果对受控端口的授权状态进行控制，主要用于解决以太网内认证和安全方面的问题。

21.1 dot1x system-auth-control

描述

该命令用于全局开启 IEEE 802.1X 功能，它的 no 命令用于禁用 IEEE 802.1X 功能。

模式

dot1x system-auth-control

no dot1x system-auth-control

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启 IEEE 802.1X 功能：

```
SW-5024(config)#dot1x system-auth-control
```

21.2 dot1x handshake

描述

802.1x 握手开关。

命令

dot1x handshake

no dot1x handshake

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

使能 802.1x 握手：

```
SW-5024(config)# no dot1x handshake
```

21.3 dot1x auth-method

描述

该命令用于配置 IEEE 802.1X 的认证方法，它的 no 命令用于恢复默认配置。

命令

dot1x auth-method { pap | eap }

no dot1x auth-method

参数

pap | eap —— 认证方法。选择 pap 时，用户端与交换机之间运行 EAP 协议，交换机将 EAP 消息转换为其它认证协议（如 RADIUS），传递用户认证信息给认证服务器系统。选择 eap-md5 时，交换机与认证服务器之间运行 EAP 协议，EAP 帧中继封装认证数据，将该协议承载在其它高层次协议中（如 RADIUS），以便穿越复杂的网络到达认证服务器。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置 IEEE 802.1X 认证方法为 pap：

```
SW-5024(config)#dot1x auth-method pap
```

21.4 dot1x accounting

描述

该命令用于启用计费服务器的计费功能，它的 no 命令用于禁用计费功能。

命令

dot1x accounting

no dot1x accounting

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启 IEEE 802.1X 计费功能：

```
SW-5024(config)#dot1x accounting
```

21.5 dot1x guest-vlan(global)

描述

该命令用于全局开启 Guest VLAN 功能，它的 no 命令用于全局禁用 Guest VLAN 功能。

命令

dot1x guest-vlan *vid*

no dot1x guest-vlan

参数

vid —— 启用 Guest VLAN 的 VLAN ID，取值范围 2~4094。Guest VLAN 中的用户可以访问指定的网络资源。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用 VLAN 5 为 Guest VLAN：

```
SW-5024(config)#dot1x guest-vlan 5
```

21.6 dot1x quiet-period

描述

该命令用于开启 IEEE 802.1X 特性的静默功能，它的 no 命令用于关闭该功能。

命令

dot1x quiet-period [*time*]

no dot1x quiet-period

参数

time —— 静默时长。用户认证失败后，在静默时间内不再处理同一用户的 IEEE 802.1X 认证请求。取值范围 1~999 秒，默认值为 10 秒。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启 IEEE 802.1X 静默功能：

```
SW-5024(config)#dot1x quiet-period
```

开启 IEEE 802.1X 静默功能，静默时长设置为 5 秒：

```
SW-5024(config)#dot1x quiet-period 5
```

21.7 dot1x timeout

描述

该命令用于配置服务器响应超时时长和客户端响应超时时长，它的 no 命令用于恢复默认配置。

命令

dot1x timeout { **server-timeout** *time* | **supplicant-timeout** *time* }

no dot1x timeout { server-timeout | supplicant-timeout }

参数

server-timeout *time* —— 服务器响应超时时长，即交换机等待服务器响应的最大等待时间。弱交换机在设定时间内没有收到服务器的回复，则重发报文。取值范围 1~9（秒），默认值为 3.

supplicant-timeout *time* —— 客户端响应超时时长，即交换机等待客户端响应的最大等待时间。若交换机在设定时间内没有收到客户端的回复，则重发报文。取值范围 1~9（秒），默认值为 3。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置服务器响应超时时长为 5 秒：

```
SW-5024(config)#dot1x timeout server-timeout 5
```

21.8 dot1x max-reauth-req

描述

该命令用于配置客户端请求报文重复发送次数，它的 no 命令用于恢复默认设置。

命令

dot1x max-reauth-req *times*

no dot1x max-reauth-req

参数

times —— 认证报文的最大重复发送次数，取值范围 1~9 次，默认值为 3 次。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置最大重复发送次数为 5：

SW-5024(config)#dot1x max-reauth-req 5

21.9 dot1x

描述

该命令用于开启端口的 IEEE 802.1X 特性，它的 no 命令用于禁用端口的 IEEE 802.1X 特性。

命令

dot1x

no dot1x

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启端口 1/0/1 的 IEEE 802.1X 特性：

SW-5024(config)#interface gigabitEthernet

1/0/1 **SW-5024(config-if)#dot1x**

21.10 dot1x guest-vlan(interface)

描述

该命令用于开启端口的 Guest VLAN 功能，它的 no 命令用于禁用端口的 Guest VLAN 功能。在开启端口的 Guest VLAN 功能前，请确保相应端口的接入控制类型为 port-based。

命令

dot1x guest-vlan

no dot1x guest-vlan

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启端口 2 的 Guest VLAN 功能：

SW-5024(config)#interface gigabitEthernet

1/0/2 **SW-5024(config-if)#dot1x guest-vlan**

21.11 dot1x port-control

描述

该命令用于配置 IEEE 802.1X 在指定端口的接入控制模式，它的 no 命令用于恢复默认配置。

命令

dot1x port-control {auto | authorized-force | unauthorized-force}

no dot1x port-control

参数

auto | authorized-force | unauthorized-force —— 控制模式，有 auto（自动）、authorized-force（强制已认证）、unauthorized-force（强制不认证）三个选项。

选择 auto 时，端口需要进行认证；选择 authorized-force 时，端口不需认证即可访问网络；选择 unauthorized-force 时，端口永远无法通过认证。默认选项为 auto。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置端口 20 的接入控制模式为强制已认证：

SW-5024(config)#interface gigabitEthernet 1/0/20 **SW-**

5024(config-if)#dot1x port-control authorized-force

21.12 dot1x port-method

描述

该命令用于配置 IEEE 802.1X 在指定端口的接入控制类型，它的 no 命令用于恢复默认配置。

命令

dot1x port-method { mac-based | port-based }

no dot1x port-method

参数

mac-based | port-based —— 控制类型，有 mac-based（基于 MAC）和 port-based（基于 Port）两个选项。选择 mac-based 时，该端口连接的所有计算机都需认证；选择 port-based 时，该端口连接的某个用户通过认证后，其他用户均无须认证即可访问网络。默认选项为 mac-based。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置端口 20 的接入控制类型为基于 Port 认证：

```
SW-5024(config)#interface gigabitEthernet 1/0/20
SW-5024(config-if)#dot1x port-method port-based
```

21.13 show dot1x global

描述

该命令用于显示 801.X 全局配置信息。

命令

show dot1x global

模式

特权模式和所有配置模式

特权要求

无

示例

显示 801.X 全局配置信息：

```
SW-5024(config)#show dot1x global
```

21.14 show dot1x interface

描述

该命令用于显示 801.X 端口配置信息。

命令

show dot1x interface [**gigabitEthernet** *port*]

参数

port —— 以太网端口号。缺省时显示所有端口的配置信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示端口 20 的 801.X 配置信息：

```
SW-5024(config)#show dot1x interface gigabitEthernet
```

1/0/20 显示所有端口的 802.1X 配置信息：

```
SW-5024(config)#show dot1x interface
```

第 22 章 PPPoE 的 ID 嵌入配置命令

PPPoE 的 ID 嵌入功能可以在数据报文中插入生产商特殊标签，该标签用于以太网中的认证、授权和计费（AAA）接入请求。生产商特殊标签共有两种，分别为电路 ID 和远程 ID。启用该功能时，交换机将包含独特标识的生产商特殊标签插入 PPPoE 的 discovery 报文中。宽带接入远程服务器（BRAS）收到带有生产商特殊标签的报文后，进行解码，并在 PPP 认证和 AAA 接入请求过程中使用相应的电路 ID 或远程 ID 作为 NAS-Port-ID 属性值。如果接收到的 PPPoE 发现阶段的 PADO 或 PADS 报文包含生产商特殊标签，系统将会移除报文中的该标签。

22.1 pppoe id-insertion(global)

描述

该命令用于全局启用 PPPoE 的 ID 嵌入功能，它的 no 命令用于禁用该功能。

命令

pppoe id-insertion

no pppoe id-insertion

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局启用 PPPoE 的 ID 嵌入功能：

```
SW-5024(config)# pppoe id-insertion
```

22.2 pppoe circuit-id(interface)

描述

该命令用于启用选定端口的 PPPoE 电路 ID 嵌入功能，它的 no 命令用于禁用该功能。

命令

pppoe circuit-id

no pppoe circuit-id

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

在端口 1 启用 PPPoE 电路 ID 嵌入功能：

```
SW-5024 (config)# interface gigabitEthernet 1/0/1
SW-5024 (config-if)# pppoe circuit-id
```

22.3 pppoe circuit-id type

描述

该命令用于设置端口的 PPPoE 电路 ID 类型，默认情况下类型为“IP”。

命令

pppoe circuit-id type { mac | ip | udf [*Value*] | udf-only [*value*] }

参数

mac | ip | udf | udf-only ——PPPoE 电路 ID 类型。

mac：备 MAC 地址将被用于电路 ID 标签的构成内容。

ip：备 IP 地址将被用于电路 ID 标签的构成内容。这是默认选项。

udf：用户自定义的不超过 40 个字符的字符串将被用于电路 ID 标签的构成内容。

udf-only：仅用户自定义的不超过 40 个字符的字符串将被用于电路 ID 标签的构成内容。

value —— 用户自定义的一串不超过 40 个字符的字符串。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置端口 1 的 PPPOE 电路 ID 类型为“mac”：

SW-5024 (config)# interface gigabitEthernet 1/0/1

SW-5024 (config-if)# pppoe circuit-id type mac

22.4 pppoe remote-id

描述

该命令用于启用并配置 PPPoE 远程 ID 嵌入功能。它的 no 命令用于关闭该功能。默认情况下 PPPoE 远程 ID 嵌入功能为关闭的。

命令

pppoe remote-id [*value*]

no pppoe remote-id

参数

value —— 用户自定义的一串不超过 40 个字符的字符串。如果不定义，则默认为 PPPoE 客户端的 MAC 地址。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置端口 1 的 PPPOE 远程 ID 为“1234”：

SW-5024 (config)# interface gigabitEthernet 1/0/1

SW-5024 (config-if)# pppoe remote-id 1234

22.5 show pppoe id-insertion global

描述

该命令用于显示 PPPoE 的 ID 嵌入功能状态。

命令

show pppoe id-insertion global

模式

特权模式和所有配置模式

描述

无

示例

显示 PPPoE 的 ID 嵌入功能状态：

```
SW-5024 # show pppoe circuit-id global
```

22.6 show pppoe id-insertion interface

描述

该命令用于显示端口 PPPoE 的 ID 嵌入功能状态和配置信息。

命令

show pppoe id-insertion interface [**gigabitEthernet** *port*]

参数

port —— 交换机的端口号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口的 PPPoE 的 ID 嵌入功能状态和配置信息：

```
SW-5024# show pppoe id-insertion interface
```

显示端口 1 的 PPPoE 的 ID 嵌入功能状态和配置信息：

SW-5024# show pppoe id-insertion interface gigabitEthernet 1/0/1

第 23 章系统日志配置命令

系统日志信息对交换机的配置和运行进行分类记载，为监控设备的运行状态和诊断设备故障提供支持。

23.1 logging buffer

描述

该命令用于配置将系统日志写入系统日志缓冲区，它的 no 命令用于关闭系统日志缓冲区功能。保存在本设备上的系统日志信息为本地日志，本地日志有两个输出方向（即可以保存到两个不同的地方）：日志缓冲区和日志文件。日志缓冲区是用于保存系统日志的一块内存区域，缓冲区中的信息可通过 **show logging buffer** 命令查看，在断电重启后这些信息将会丢失。本命令用来启用或关闭日志缓冲区。

命令

logging buffer

no logging buffer

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

启用日志缓冲区：

```
SW-5024(config)# logging buffer
```

23.2 logging buffer level

描述

该命令用于配置系统日志缓冲区的信息输入等级，它的 no 命令用于恢复默认的信息输入等级。

命令

logging buffer level *level*

no logging buffer level

参数

level —— 严重级别，共分为 0~7 八个等级，级别值越小，紧急程度越高。只允许级别小于或等于该值的日志信息保存到日志缓冲区。默认值为 6，表示将级别为 0~6 的日志保存到日志缓冲区。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置日志缓冲区的信息输入等级为 5：

```
SW-5024(config)#logging buffer level 5
```

23.3 logging file flash

描述

该命令用于配置将系统日志写入日志文件，它的 no 命令用于关闭系统日志文件功能。日志文件是 Flash 里的一块存储区域。日志文件的信息可通过 **show logging flash** 命令查看，在断电重启后这些信息不会丢失。

命令

logging file flash

no logging file flash

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

启用日志文件功能：

```
SW-5024(config)#logging file flash
```

23.4 logging file flash frequency

描述

该命令用于配置把系统日志从系统日志缓冲区同步写入到系统日志文件的频率，它的 no 命令用于恢复默认频率。

命令

logging file flash frequency { periodic *periodic* **| immediate }**

no logging file flash frequency

参数

periodic —— 系统日志从日志缓冲区同步到系统日志文件的频率，取值范围是 1～48 小时。默认情况下，同步操作每 24 小时执行一次。

immediate —— 系统日志将会立即从日志缓冲区同步到系统日志文件。此操作会减少 flash 的寿命，不推荐使用。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置同步频率为 10 小时：

SW-5024(config)#logging file flash frequency periodic 10

23.5 logging file flash level

描述

该命令用于配置系统日志文件的信息输入等级，等于或小于此等级的系统信息将会被存入系统日志文件。它的 no 命令用于恢复默认的信息等级。

命令

logging file flash level *level*

no logging file flash level

参数

level ——严重级别，共分为 0~7 八个等级，级别值越小，紧急程度越高。只允许级别小于或等于该值的日志信息保存到日志文件中。默认值为 3，表示允许级别为 0~3 的日志信息保存到日志文件中。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

启用日志文件并设置严重级别为 7：

SW-5024(config)#logging file flash level 7

23.6 logging host index

描述

该命令用于配置日志服务器，它的 no 命令用于清空指定日志服务器的配置信息。日志服务器用于接收本交换机发送的系统日志消息，通过查看日志服务器可以对本交换机的配置情况和运行状态进行远程监控。

命令

logging host index *idx host-ip level*

no logging host index *idx*

参数

idx ——日志服务器的序号，取值范围为 1~4。

host-ip ——日志服务器的 IP 地址。

level ——严重级别，共分为 0~7 八个等级，级别值越小，紧急程度越高。只允许级别小于或等于该值的日志信息发送到该服务器。默认值为 6，表示允许级别为 0~6 的日志信息发送到该服务器。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

启用日志服务器 2，并设置该服务器的 IP 地址为 192.168.0.148，严重级别为 5：

SW-5024(config)# logging host index 2 192.168.0.148 5

23.7 logging console

描述

该命令用于开启将系统日志输出到 Console 口功能，它的 no 命令用于关闭此功能。此功能默认开启。

命令

logging console

no logging console

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

开启发送系统日志到 Console 口功能：

SW-5024(config)# logging console

23.8 logging console level

描述

该命令用于限制记录到与 Console 口相连的终端设备的系统信息。小于或等于所设置的等级的系统信息将会输出到 Console 口。它的 no 命令用于恢复默认的信息等级。

命令

logging console level *level*

no logging monitor level

参数

level ——输出到终端设备的日志信息的严重程度。共分为 0~7 八个等级，级别值越小，紧急程度越高。只有具有相同或较小严重级别值的日志将被输出到终端设备。默认值为 5，表示 0~5 六个等级的日志信息将被输出到终端设备。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置将等级为 0~7 的日志信息输出到 Console 口：

```
SW-5024(config)# logging console level 7
```

23.9 logging monitor

描述

该命令用于在终端设备上显示系统日志。它的 no 命令可用于关闭显示。

命令

logging monitor

no logging monitor

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

关闭系统日志记录：

```
SW-5024(config)# no logging monitor
```

23.10 logging monitor level

描述

该命令用于限制记录到终端设备的消息，等级小于或等于所设置阈值的系统日志将显示在终端设备上。它的 no 命令用于恢复阈值水平到默认值。

命令

logging monitor level *level*

no logging monitor level

参数

level ——输出到终端设备的日志信息的严重程度。共分为 0~7 八个等级，级别值越小，紧急程度越高。只有具有相同或较小严重级别值的日志将被输出到终端设备。默认值为 5，表示 0~5 六个等级的日志信息将被输出到终端设备。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置将等级为 0~7 的日志信息输出到终端设备：

```
SW-5024(config)# logging monitor level 7
```

23.11 clear logging

描述

该命令用于清空日志缓冲区或者日志文件中的信息。

命令

clear logging [buffer | flash]

参数

buffer | flash —要清空的输出方向，有 buffer（日志缓冲区）和 flash（日志文件）两个选项，缺省时表示两者的信息都被清空。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

清空交换机当前日志缓冲区中的系统日志信息：

```
SW-5024(config)# clear logging buffer
```

23.12 show logging local-config

描述

该命令用于显示本地日志在日志缓冲区、日志文件、终端设备以及 Console 上的配置信息。

命令

show logging local-config

模式

特权模式和所有配置模式

特权要求

无

示例

显示本地日志配置信息：

```
SW-5024(config)# show logging local-config
```

23.13 show logging loghost

描述

该命令用于显示日志服务器的配置信息。

命令

show logging loghost [*index*]

参数

index ——要显示配置信息的日志服务器序号，取值范围为 1~4。缺省时显示所有日志服务器的配置信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示日志服务器 2 的配置信息：

SW-5024(config)# show logging loghost 2

23.14 show logging buffer

描述

该命令用于显示日志缓冲区中的日志信息，可根据严重级别进行过滤显示。

命令

show logging buffer [**level** *level*]

参数

*leve*l ——严重级别（0~7），只显示级别小于或等于该值的日志信息，缺省时显示日志缓冲区中的所有日志信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示日志缓冲区中级别为 0~5 的日志信息：

SW-5024(config)# show logging buffer level 5

23.15 show logging flash

描述

该命令用于显示日志文件中的日志信息，可根据严重级别进行过滤显示。

命令

show logging flash [**level** *level*]

参数

level ——严重级别（0~7），只显示级别小于或等于该值的日志信息，缺省时显示日志文件中的所有日志信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示日志文件中级别为 0~3 的日志信息：

SW-5024(config)# show logging flash level 3

第 24 章 SSH 配置命令

SSH（Security Shell）采用加密和认证功能，可以为远程登录管理提供安全保障，以保证管理信息的安全。

24.1 ip ssh server

描述

该命令用于启用 SSH 服务器功能，它的 no 命令用于禁用 SSH 服务器功能。

命令

ip ssh server

no ip ssh server

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用 SSH 服务器功能：

```
SW-5024(config)# ip ssh server
```

24.2 ip ssh version

描述

该命令用于启用 SSH 的协议版本，它的 no 命令用于禁用相应的 SSH 协议版本。

命令

ip ssh version { v1 | v2 }

no ip ssh version { v1 | v2 }

参数

v1 | v2 ——要启用的 SSH 协议版本，分别对应 SSH v1 和 SSH v2。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用 SSH v2：

SW-5024(config)# ip ssh version v2

24.3 ip ssh algorithm

描述

该命令用于配置 SSH 功能的算法。它的 no 命令用于禁用指定的算法。

命令

ip ssh algorithm { AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 }

no ip ssh algorithm { AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 }

参数

AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 ——指定 SSH 算法。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

指定 SSH 的算法为 AES128-CBC：

SW-5024(config)# ip ssh algorithm AES128-CBC

24.4 ip ssh timeout

描述

该命令用于设置 SSH 的静默时长，它的 no 命令用于恢复默认配置。

命令

ip ssh timeout *value*

no ip ssh timeout

参数

value ——静默时长，当此时间内客户端未有动作时，连接会自动断开。单位为秒，取值范围为 1~120，默认值为 120。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 SSH 静默时长为 30 秒：

SW-5024(config)# ip ssh timeout 30

24.5 ip ssh max-client

描述

该命令用于配置 SSH 的最大连接数，它的 no 命令用于恢复默认配置。

命令

ip ssh max-client *num*

no ip ssh max-client

参数

num ——SSH 最大连接数，取值范围为 1~5，默认值为 5。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 SSH 最大连接数为 3：

SW-5024(config)# ip ssh max-client 3

24.6 ip ssh download

描述

该命令用于通过 TFTP 方式导入 SSH 密钥文件。

命令

ip ssh download { v1 | v2 } *key-file* **ip-address** *ip-addr*

参数

v1 | v2 ——选择要导入的密钥类型，v1 表示 SSH-1，v2 表示 SSH-2。

key-file ——选择要导入的密钥文件名称，可输入 1~25 个字符。导入的文件必须是密钥长度为 512~3072 比特的 SSH 公钥。

ip-addr ——TFTP 服务器的 IP 地址。可支持 IPv4 和 IPv6 的地址，如 192.168.0.1 或 fe80::1234。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导入名为 ssh-key 的 SSH-1 密钥文件：

SW-5024(config)# ip ssh download v1 ssh-key **ip-address** 192.168.0.148

通过 IP 地址为 fe80::1234 的 TFTP 服务器导入名为 ssh-key 的 SSH-1 密钥文件：

SW-5024(config)# ip ssh download v1 ssh-key **ip-address** fe80::1234

24.7 remove public-key

描述

该命令用于移除交换机中保存的 SSH 公钥。

命令

remove public-key { v1 | v2 }

参数

v1 | v2 ——选择要删除的密钥的类型，v1 表示 SSH-1，v2 表示 SSH-2。

模式

特权模式

特权要求

只有管理员类型的用户可以使用该命令

示例

删除交换机中的 SSH-1 公钥：

```
SW-5024# remove public-key v1
```

24.8 show ip ssh

描述

该命令用于显示 SSH 的全局配置信息。

命令

show ip ssh

模式

特权模式和所有配置模式

特权要求

无

示例

显示 SSH 全局配置信息：

```
SW-5024(config)# show ip ssh
```

第 25 章地址配置命令

地址配置通过端口安全设置和地址表管理来提高网络安全，管理地址信息。

25.1 mac address-table static

描述

该命令用于添加静态地址条目，它的 no 命令用于删除对应条目。静态地址由用户手工添加和删除，不受老化时间的限制。对于网络拓扑相对固定的使用环境来说，使用静态地址绑定可以提高交换机的转发效率，减少网络中的广播流量。

命令

mac address-table static *mac-addr* **vid** *vid* **interface gigabitEthernet** *port*

no mac address-table static { *mac-addr* | **vid** *vid* | *mac-addr* **vid** *vid* |

interface gigabitEthernet *port* }

参数

mac-addr ——要添加的地址条目的 MAC 地址。

vid ——地址条目所属的 VLAN ID，取值范围为 1~4094。

port ——地址条目对应的端口。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

添加静态地址条目，该条目将 MAC 地址 00:02:58:4f:6c:23、VLAN1 和端口 1 绑定：

SW-5024(config)# mac address-table static 00:02:58:4f:6c:23 **vid** 1

interface gigabitEthernet 1/0/1

25.2 mac address-table aging-time

描述

该命令用于配置动态地址老化时间，它的 no 命令用于恢复默认配置。

命令

mac address-table aging-time *aging-time*

no mac address-table aging-time

参数

aging-time ——要设置的地址老化时间，取值范围为 0 或 10~630（秒），为 0 时表示不启用自动老化功能。默认值为 300 秒。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置地址老化时间为 500 秒：

SW-5024(config)# mac address-table aging-time 500

25.3 mac address-table filtering

描述

该命令用于添加过滤地址条目，它的 no 命令用于删除对应条目。通过配置过滤地址，允许交换机对不期望转发的数据帧进行过滤。过滤地址不会被老化，只能手动进行配置和删除。

命令

mac address-table filtering *mac-addr* **vid** *vid*

no mac address-table filtering {[*mac-addr*] [**vid** *vid*]}

参数

mac-addr ——要添加的地址条目的 MAC 地址。

vid ——地址条目所属的 VLAN ID，取值范围为 1~4094。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

添加过滤地址条目，过滤 VLAN1 的 MAC 地址 00:1e:4b:04:01:5d：

SW-5024(config)# mac address-table filtering 00:1e:4b:04:01:5d **vid** 1

25.4 mac address-table notification

描述

该命令用于配置全局 MAC 地址表事件通知功能。

命令

mac address-table notification { [**global-status** enable | disable] [**table-full-status** enable | disable] [**interval** *time*] }

参数

global-status enable | disable —— 全局开启或禁用 MAC 地址表事件通知功能。

table-full-status enable | disable ——开启或禁用“MAC 地址表已满”通知功能。启用后，当 MAC 地址表填满或溢出时交换机会生成一个 SNMP trap 信息并发送到网络管理系统（NMS）。

interval *time* —— 指定交换机发送 SNMP trap 信息到 NMS 的时间间隔。取值范围为 1~1000 秒，默认为 1 秒。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局开启 MAC 地址表事件通知功能和“地址表已满”通知功能，并制定发送 SNMP trap 信息的时间间隔为 2 秒：

SW-5024(config)# mac address-table notification global-status enable

table-full-status enable **interval** 2

25.5 mac address-table max-mac-count

描述

该命令用于设置端口安全参数，它的 no 命令用于恢复默认配置。端口安全通过限制端口的最大学习 MAC 数目，来防范 MAC 地址攻击和控制端口的网络流量。如果端口启用端口安全功能，将自动学习接入设备的 MAC 地址，当学习地址数达到最大值时停止学习。此后，MAC 地址未被学习的网络设备将不能再通过该端口接入网络，保证安全性。

命令

mac address-table max-mac-count { [**max-number** *num*] [**mode** { dynamic | static | permanent }] [**status** { forward | drop | disable }] }

no mac address-table max-mac-count [max-number | mode | status]

参数

num ——端口最多可以学习的 MAC 地址数目，取值范围为 0~64，缺省时为 64。

dynamic | static | permanent ——端口地址学习模式，有 dynamic（动态）、static（静态）和 permanent（永久）三个选项。选择 dynamic 时，MAC 地址学习受老化时间的限制，老化时间过后，所学的 MAC 地址将被删除；选择 static 时，

MAC 地址学习不受老化时间的限制，只能手动进行删除，但交换机重启后学习到的条目将清空；选择 permanent 时，MAC 地址学习不受老化时间的限制，只能手动进行删除，交换机重启后学习到的条目保持不变。缺省时为 dynamic。

status ——指定当端口上学习到的 MAC 地址达到上限后收到目的地址为未知地址的报文时采取的措施。有转发（forward）、丢弃（drop）和禁用（disable）三个选项，默认为禁用。

- forward: 转发该报文但不学习其目的地址。
- drop: 丢弃该报文。
- disable: 禁用此端口上可学习的 MAC 地址数目限制。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用端口 1 的安全功能，并设置学习模式为静态，最大可学习 MAC 地址数为 30。当该端口学习的 MAC 地址数超过 30 时，丢弃后续收到的目的地址为未知地址的报文：

SW-5024(config)# interface gigabitEthernet 1/0/1 **SW-5024(config-if)# mac address-table max-mac-count max-number** 30 **mode** static **status** drop

25.6 mac address-table notification (interface)

描述

该命令用于配置端口上的 MAC 地址相关信息变化通知功能。

命令

mac address-table notification { [**learn-mode-change** enable | disable] [**exceed-max-learned** enable | disable] [**new-mac-learned** enable | disable] }

参数

learn-mode-change enable | disable ——开启或禁用“MAC 地址学习模式改变”通知功能。启用后当端口上的 MAC 地址学习模式发生改变时，交换机会生成 SNMP trap 信息并发送到网络管理系统（NMS）。MAC 地址学习模式可使用 **mac address-table max-mac-count** 命令进行配置。

exceed-max-learned enable | disable —— 开启或禁用端口上的“MAC 地址已超出阈值”通知功能。启用后当端口上学习到的 MAC 地址数超过所设定的阈值时，交换机会生成 SNMP trap 信息并发送到网络管理系统（NMS）。端口可学习的最大 MAC 地址数可使用 **mac address-table max-mac-count** 命令进行配置。

new-mac-learned enable | disable——开启或禁用端口上的“学习新 MAC 地址”通知功能。启用后当端口上学习了新的 MAC 地址时，交换机会生成 SNMP trap 信息并发送到网络管理系统（NMS）。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

在端口 2 上开启“学习新 MAC 地址”通知功能：

SW-5024(config)# mac address-table notification global-status enable

SW-5024(config)# interface gigabitEthernet 1/0/2 **SW-5024(config-if)#**

mac address-table notification learn-mode-change enable

25.7 mac address-table security

描述

该命令用于配置指定 VLAN 中的 MAC 地址表安全功能。

命令

mac address-table security vid *vid* **max-learn** *number* { forward | drop | disable }

参数

vid —— 指定 VLAN ID。

number —— 设置此 VLAN 中最多可学习的 MAC 地址数，取值范围为 0~16383。

forward | drop | disable —— 指定当 VLAN 中已学习的 MAC 地址达到上限后收到目的地址为未知地址的报文时采取的措施。有转发（forward）、丢弃（drop）和禁用（disable）三个选项。

- forward: 转发该报文但不学习其目的地址。
- drop: 丢弃该报文。
- disable: 禁用此 VLAN 上可学习的 MAC 地址数目限制。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置 VLAN 2 中最多可学习的 MAC 地址数为 1000，达到上限后收到目的地址为未知地址的报文时丢弃该报文：

SW-5024(config)# mac address-table security vid 2 **max-learn** 1000 drop

25.8 clear mac address-table

描述

该命令用于删除指定的 MAC 地址条目类型。

命令

clear mac address-table { dynamic | static | filtering }

参数

dynamic | static | filtering —— 需要删除的 MAC 地址条目类型。

模式

特权模式和所有配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

删除所有通过静态配置的 MAC 地址条目：

SW-5024(config)# clear mac address-table static

25.9 show mac address-table

描述

该命令用于显示地址条目信息。

命令

show mac address-table { dynamic | static | filtering }

参数

dynamic | static | filtering ——要显示的地址类型。默认情况下所有类型条目都将被显示。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有地址条目信息：

SW-5024(config)# show mac address-table

25.10 show mac address-table aging-time

描述

该命令用于显示地址老化时间。

命令

show mac address-table aging-time

模式

特权模式和所有配置模式

特权要求

无

示例

显示地址老化时间：

SW-5024(config)# show mac address-table aging-time

25.11 show mac address-table max-mac-count

描述

该命令用于显示端口的安全配置，即端口最大可学习 MAC 地址数和学习模式。

命令

show mac address-table max-mac-count { all **| interface gigabitEthernet** *port* }

参数

all ——显示所有端口的安全配置信息。

port ——要显示安全配置信息的端口号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口的安全配置信息：

SW-5024(config)# show mac address-table max-mac-count all

显示端口 1 的安全配置信息：Display the security configuration of port 1/0/1:

SW-5024(config)# show mac address-table max-mac-count interface

gigabitEthernet 1/0/1

25.12 show mac address-table interface

描述

该命令用于显示端口的地址配置信息。

命令

show mac address-table interface { **gigabitEthernet** *port* | **port-channel** *port-channel-id* }

参数

port ——要显示地址表信息的端口号。

port-channel-id ——要显示地址表信息的汇聚组号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示端口 1/0/1 的地址配置信息：

SW-5024(config)# show mac address-table interface gigabitEthernet 1/0/1

25.13 show mac address-table count

描述

该命令用于显示地址表总数。

命令

show mac address-table count [**vlan** *vlan-id*]

参数

vlan-id ——显示地址表统计信息的 VLAN ID。

模式

特权模式和所有配置模式

特权要求

无

示例

显示交换机地址表数量，按 VLAN 排序：

SW-5024(config)# show mac address-table count

25.14 show mac address-table address

描述

该命令用于显示指定 MAC 地址的信息。

命令

show mac address-table address *mac-addr* [**interface** { **gigabitEthernet** *port* | **port-channel** *port-channel-id* } | **vid** *vlan-id*]

参数

mac-addr ——指定 MAC 地址。

port ——指定端口号。

port-channel-id —— 指定汇聚组号。

vlan-id ——指定端口所属的 VLAN。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN1 中 MAC 地址为 00:00:00:00:23:00 的条目信息：

SW-5024(config)#show mac address-table address 00:00:00:00:23:00 **vid** 1

25.15 show mac address-table vlan

描述

该命令用于显示指定 VLAN 的 MAC 地址配置。

命令

show mac address-table vlan *vid*

参数

vid ——指定 VLAN ID。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN1 的地址配置信息：

SW-5024(config)# show mac address-table vlan 1

25.16 show mac address-table notification

描述

该命令用于显示全局的或端口上的 MAC 地址表事件通知配置信息。

命令

show mac address-table notification { all **| interface gigabitEthernet** *port* }

参数

all —— 显示全局的设置信息以及在所有端口上的配置信息。

port —— 显示指定端口上的配置信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口上的 MAC 地址表事件通知配置信息：

SW-5024(config)# show mac address-table notification all

25.17 show mac address-table security

描述

该命令用于显示全局的或指定 VLAN 的 MAC 地址表事件通知配置信息。

命令

show mac address-table security [**vid** *vid*]

参数

vid ——指定 VLAN ID。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN 1 上的 MAC 地址表事件通知配置信息。 **SW-5024(config)# show mac address-table security vid** 1

第 26 章系统配置命令

系统配置用来配置系统信息、IP 地址，镜像文件和配置文件等信息，并且可以对交换机进行重启、复位、升级系统文件等操作。

26.1 system-time manual

描述

该命令用于手动设置交换机的系统时间。

命令

system-time manual *time*

参数

time ——手动设置交换机的系统时间，格式为 MM/DD/YYYY-HH:MM:SS。年份取值范围为 2000~2037。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置交换机系统时间为 12/20/2010 17:30:35 **SW-5024(config)# system-time manual** 12/20/2010-17:30:35

26.2 system-time ntp

描述

该命令用于设置交换机从网络中 NTP 服务器上获取 UTC 时间。需要保证交换机能正常访问 NTP 服务器。

命令

system-time ntp { *timezone* } { *ntp-server* } { *backup-ntp-server* } { *fetching-rate* }

参数

timezone ——选择交换机所在的时区。以正二时区为例，UTC 时间的格式为：UTC+02:00。取值范围是 UTC-12:00 到 UTC+13:00。

ntp-server ——设置首选 NTP 服务器的 IP 地址。

backup-ntp-server ——设置备选 NTP 服务器的 IP 地址。

fetching-rate ——设置从 NTP 服务器获取时间的频率。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置交换机系统时间获取方式为 NTP，时区为 UTC-12:00，首选 NTP 服务器 IP 地址为 133.100.9.2，备选 NTP 服务器的 IP 地址为 139.78.100.163，获取频率为 11 小时：

SW-5024(config)# system-time ntp UTC-12:00 133.100.9.2 139.79.100.163 11

26.3 system-time dst predefined

描述

该命令用于从预定义的夏令时样式中选择夏令时配置，配置可循环使用。

命令

system-time dst predefined [USA | Australia | Europe | New-Zealand]

no system-time dst

参数

USA | Australia | Europe | New-Zealand ——夏令时样式。有四个可选值，分别为 USA, Australia, Europe, New-Zealand，默认为 Europe。

四个值代表夏令时起止区间如下：

USA：三月第二个周日的 2：00am ~ 十一月第一个周日的 2：00am

Australia：十月第一个周日 2：00am ~ 四月第一个周日 3：00am

Europe：三月最后一个周日 1：00am ~ 十月最后一个周日 1：00am

New-Zealand：九月最后一个周日 2：00am ~ 四月第一个周日 3：00am

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置交换机的夏令时起止时间为 Europe 标准：

SW-5024(config)#system-time dst predefined USA

26.4 system-time dst date

描述

该命令用于设置一次性的夏令时，开始日期的年份默认为当前年份。夏令时起止区间必须小于一年，可跨年设置。它的 no 命令用于禁用夏令时功能。

命令

system-time dst date {*smonth*} {*sday*} {*stime*} {*syear*} {*emonth*} {*eday*} {*etime*} {*eyear*}[*offset*]

no system-time dst

参数

smonth ——开始月，取值如下：Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec。

sday —— 开始日，取值范围 1~31，各月天数不尽相同，请根据实际情况填写。

stime —— 开始时刻，格式为：hh:mm。

emonth —— 结束月，取值如下：Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec。

eday —— 结束日，取值范围 1~31，各月天数不尽相同，请根据实际情况填写。

etime —— 结束时刻，格式为：hh:mm。

offset —— 可选参数，夏令时时间调整大小，取值范围为 1-1440。默认为 60 分钟。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置交换机夏令时的起止时间日期为 2015 年的 4 月 1 日 0 点到 10 月 1 日 0 点，偏移时间为 30 分钟：

SW-5024(config)# system-time dst date Apr 1 00:00 2015 Oct 1 00:00 2015

30

26.5 system-time dst recurring

描述

该命令用于设置可循环的夏令时配置。可以跨年设置。

命令

system-time dst recurring {*sweek*} {*sday*} {*smonth*} {*stime*} {*eweek*} {*eday*} {*emonth*} {*etime*} [*offset*]

参数

sweek——开始周，取值如下：first, second, third, fourth, last。

sday —— 开始日，取值如下： Sun, Mon, Tue, Wed, Thu, Fri, Sat。

smonth ——开始月，取值如下：Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec。

stime —— 开始时刻，格式为：HH:MM。

eweek ——结束周，取值如下：first, second, third, fourth, last。

eday —— 结束日，取值如下：Sun, Mon, Tue, Wed, Thu, Fri, Sat。

emonth -—结束月，取值如下：Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec。

etime ——结束时刻，格式为：HH:MM。

offset ——可选参数，夏令时时间调整大小，取值范围为 1-1440。默认为 60 分钟。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置交换机夏令时的起止时间日期为 5 月的第一个星期天 2:00am 到 10 月最后一个星期天 2:00 am，偏移时间为 45 分钟：

```
SW-5024(config)# system-time dst recurring first Sun May 02:00 last Sun
Oct 02:00 45
```

26.6 hostname

描述

该命令用于设置设备名称，它的 no 命令用于清空设备名称信息。

命令

hostname [*hostname*]

no hostname

参数

hostname ——设备名称，1~32 个字符，默认为设备型号 SW-5024。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置设备名称为 SUNDRAY:

SW-5024(config)# hostname SUNDRAY

26.7 location

描述

该命令用于设置设备位置，它的 no 命令用于清空设备位置信息。

命令

location [*location*]

no location

参数

location ——设备位置，1~32 个字符，默认为 SHENZHEN。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置设备位置为 SHENZHEN:

SW-5024(config)# location SHENSHEN

26.8 contact-info

描述

该命令用于设置联系方法，它的 no 命令用于清空相应信息。

命令

contact-info [*contact_info*]

no contact-info

参数

contact_info ——联系方法，1~32 个字符。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置联系方法为 www.sundray.com：

SW-5024(config)# contact-info www.sundray.com

26.9 ip address

描述

此命令用于配置指定接口的 IP 地址和子网掩码。接口类型包括：路由端口，环回接口和 VLAN 接口。

命令

ip address { *ip-addr* } { *mask* } [**secondary**]

no ip address [*ip-addr*] [*mask*]

参数

ip-addr ——三层接口的 IP 地址。

mask ——三层接口的子网掩码。

secondary ——设置端口的第二个 IP 地址。缺省时，配置的 IP 地址为接口的主地址。

模式

接口配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 VLAN 接口 2 的 IP 地址为 192.168.1.1，子网掩码为 255.255.255.0，第二 IP 地址为 192.168.2.1，子网掩码为 255.255.255.0：

```
SW-5024(config)# interface vlan 2
SW-5024(config-if)# ip address 192.168.1.1 255.255.255.0
SW-5024(config-if)# ip address 192.168.2.1 255.255.255.0 secondary
```

26.10 ip address-alloc

描述

此命令用于使能 DHCP 客户端功能或者使能 BOOTP 协议。使能此功能后，指定的接口可以从 DHCP 服务器或者 BOOTP 服务器获得 IP 地址。若需要在指定接口上关闭此功能，请使用 **no ip address** 命令。本条命令适用于路由端口和 VLAN 接口。

命令

ip address-alloc { dhcp | bootp }

no ip address

参数

dhcp ——指定的三层接口可以从 DHCP 服务器获取 IP 地址。

bootp ——指定的三层接口可以从 BOOTP 服务器获取 IP 地址。

模式

接口配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

使能路由端口 1/0/1 上的 DHCP 客户端功能：

```
SW-5024(config)# interface gigabitEthernet 1/0/1
```

```
SW-5024(config-if)# no switchport
SW-5024(config-if)# ip address-alloc dhcp
```

关闭 VLAN 接口 2 上获取 IP 地址的功能：

```
SW-5024(config)# interface vlan 2
SW-5024(config-if)# no ip address
```

26.11 reset

描述

该命令用于把交换机软件复位，软件复位后，交换机配置将恢复成出厂默认状态，用户配置数据将丢失。

命令

reset

模式

特权模式

特权要求

只有管理员类型的用户可以使用该命令

示例

对交换机进行软件复位：

```
SW-5024# reset
```

26.12 reboot

描述

该命令用于重启交换机。在重启期间，请注意不要关闭设备电源，以免损坏设备。

参数

reboot

模式

特权模式

特权要求

只有管理员类型的用户可以使用该命令

示例

重新启动交换机：

SW-5024# reboot

26.13 reboot-schedule

描述

该命令用于配置交换机定时重启功能。它的 no 命令用于禁用定时重启功能。

命令

reboot-schedule at *time* [*date*] [**save_before_reboot**]

reboot-schedule in *interval* [**save_before_reboot**]

reboot-schedule cancel

参数

time —— 指定交换机重启的时间，格式为：HH:MM。

date —— 指定交换机重启的日期，格式为 DD:MM:YYYY。所指定的日期应该距离交换机系统时间 30 天之内。

save_before_reboot —— 选择是否让交换机在重启之前保存配置。

interval——指定交换机在现在开始的此时间间隔后重启，时间间隔的取值范围为 1~43200 分钟。

cancel ——删除交换机定时重启设置。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

说明

reboot-schedule at *time* [*date*] [**save_before_reboot**]命令中没有指定 date 参数时，若设置的 time 参数晚于命令执行时间，交换机会在当天的 time 参数所指定的时间重启，否则交换机会在第二天的 time 参数所指定的时间重启。

示例

指定交换机在 200 分钟之后重启，并在重启前保存配置：

SW-5024(config)# reboot-schedule in 200 **save_before_reboot**

26.14 copy running-config startup-config

描述

该命令用于保存当前用户配置为启动配置文件。

命令

copy running-config startup-config

模式

特权模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

保存当前配置为启动配置文件：

```
SW-5024# copy running-config startup-config
```

26.15 copy startup-config tftp

描述

该命令用于通过 TFTP 方式导出配置文件。

命令

copy startup-config tftp ip-address *ip-addr* **filename** *name*

参数

ip-addr ——TFTP 服务器的 IP 地址。支持 IPv4 和 IPv6 地址。例如 IPv4 地址 192.168.0.10 和 IPv6 地址 fe80::1234。

name ——指定导出的配置文件名。

模式

特权模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导出配置文件，并将导出的配置文件命名为 config.cfg：

SW-5024# copy startup-config tftp ip-address 192.168.0.148 **filename** config

通过 IP 地址为 fe80::1234 的 TFTP 服务器导出配置文件，并将导出的配置文件命名为 config.cfg：

SW-5024# copy startup-config tftp ip-address fe80::1234 **filename** config

26.16 copy tftp startup-config

描述

该命令用于通过 TFTP 方式导入配置文件。

命令

copy tftp startup-config ip-address *ip-addr* **filename** *name*

参数

ip-addr ——TFTP 服务器的 IP 地址。支持 IPv4 和 IPv6 地址。例如 IPv4 地址 192.168.0.10 和 IPv6 地址 fe80::1234。

name ——要导入的配置文件名。

模式

特权模式

特权要求

只有管理员类型的用户可以使用该命令

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器导入名为 config.cfg 的配置文件：

SW-5024# copy tftp startup-config ip-address 192.168.0.148 **filename** config

通过 IP 地址为 fe80::1234 的 TFTP 服务器导入名为 config.cfg 的配置文件：

SW-5024# copy tftp startup-config ip-address fe80::1234 **filename** config

26.17 boot application

描述

此命令用于保存镜像文件为启动镜像或备份镜像。

命令

boot application filename { image1 | image 2 } { startup | backup }

no boot application

参数

image1 | image2 ——选择要被保存的镜像文件。默认情况下，image.1 是启动镜像，imange.2 是备份镜像。

startup | backup ——选择镜像的属性：启动镜像或者备份镜像。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

将 image2.bin 配置为启动镜像：

```
SW-5024(config)# boot application filename image2 startup
```

26.18 remove backup-image

描述

该命令用于删除备份镜像。

命令

remove backup-image

模式

特权模式

特权要求

只有管理员类型的用户可以使用该命令

示例

删除备份镜像：

```
SW-5024# remove backup-image
```

26.19 firmware upgrade

描述

该命令用于通过 TFTP 方式升级系统备份镜像。导入的固件文件将覆盖系统中的备份镜像文件，导入后可选择是否试用备份镜像重启交换机。

命令

firmware upgrade ip-address *ip-addr* **filename** *name*

参数

ip-addr ——TFTP 服务器的 IP 地址。支持 IPv4 和 IPv6 地址。例如 IPv4 地址 192.168.0.10 和 IPv6 地址 fe80::1234。

name —— 指定需要导入的固件的文件名称。

模式

特权模式

特权要求

只有管理员类型的用户可以使用该命令

示例

通过 IP 地址为 192.168.0.148 的 TFTP 服务器升级交换机的备份镜像文件，升级文件名为 firmware.bin，并使用此附件重启交换机：

SW-5024# firmware upgrade ip-address 192.168.0.148 **filename** firmware.bin

It will only upgrade the backup image. Continue? (Y/N):y

Operation OK!

Reboot with the backup image? (Y/N): y

通过 IP 地址为 fe80::1234 的 TFTP 服务器升级交换机，升级文件名为 firmware.bin，交换机不重启：

SW-5024# firmware upgrade ip-address fe80::1234 **filename** firmware.bin

It will only upgrade the backup image. Continue? (Y/N):y

Operation OK!

Reboot with the backup image? (Y/N): n

26.20 ping

描述

该命令用于检测从交换机到某一网络节点之间的链路是否连通。

命令

ping [ip | ipv6] { *ip_addr* } [**-n** *count*] [**-l** *count*] [**-i** *count*]

参数

ip **——**输入的 IP 地址类型应为 IPv4。

ipv6 ——输入的 IP 地址类型应为 IPv6。

ip_addr ——要检测的目标节点的 IP 地址。如果参数 ip | ipv6 未被选择，输入 IPv4 和 IPv6 地址均可。

-n *count* ——发送报文的次数，取值范围 1~10，默认值为 4。

-l *count* ——发送报文的长度，取值范围 1~1024（字节），默认值为 64。

-i *count* ——发送报文的时间间隔，取值范围 100~1000（毫秒），默认值为 1000。

模式

用户模式和特权模式

特权要求

无

示例

检测交换机与 IP 地址为 192.168.0.131 的网络设备是否连通，其中测试报文的长度为 512 字节，报文每隔 1000 毫秒发送一次，若发送 8 次后没有收到回复，则连接失败：

```
SW-5024# ping 192.168.0.131 –n 8 –l 512
```

检测交换机与 IP 地址为 fe80::1234 的网络设备是否连通，其中测试报文的长度为 512 字节，报文每隔 1000 毫秒发送一次，若发送 8 次后没有收到回复，则连接失败：

```
SW-5024# ping fe80::1234 –n 8 –l 512
```

26.21 tracert

描述

该命令用于检测测试报文从交换机传送到目的设备所经过的网关的连通性。

命令

tracert [ip | ipv6] *ip_addr* [*maxHops*]

参数

ip —— 输入的 IP 地址类型应为 IPv4。

ipv6 —— 输入的 IP 地址类型应为 IPv6。

ip_addr ——要检测的目的设备的 IP 地址。

maxHops ——最大路由跳数，取值范围 1~30，默认值为 4。

模式

用户模式和特权模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

检测交换机与 IP 地址为 192.168.0.131 的网络设备是否连通，若经过 20 跳路由后仍未连通，则连接失败：

SW-5024# tracert 192.168.0.131 20

检测交换机与 IP 地址为 fe80::1234 的网络设备是否连通，若经过 20 跳路由后仍未连通，则连接失败：

SW-5024# tracert fe80::1234 20

26.22 show system-info

描述

该命令用于显示系统描述、系统名称、系统位置、联系方法、硬件版本、软件版本、系统时间和运行时间等信息。

命令

show system-info

模式

特权模式和所有配置模式

特权要求

无

示例

显示系统信息：

```
SW-5024# show system-info
```

26.23 show image-info

描述

该命令用于显示交换机文件系统中的镜像文件信息。

命令

show image-info

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示交换机文件系统中的镜像文件信息：

```
SW-5024# show image-info
```

26.24 show boot

描述

该命令用于显示系统当前的启动配置信息。

命令

show boot

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示交换机的启动配置信息：

```
SW-5024# show boot
```

26.25 show running-config

描述

该命令用于显示系统或一个指定端口的当前操作配置。

命令

show running-config

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示交换机的当前配置信息：

```
SW-5024# show running-config
```

26.26 show startup-config

描述

该命令用于显示当前交换机中的配置信息。这些配置在交换机重启之后仍然有效。

命令

show startup-config

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示交换机的当前配置信息：

```
SW-5024# show startup-config
```

26.27 show system-time

描述

该命令用于显示交换机的系统时间信息。

命令

show system-time

模式

特权模式和所有配置模式

特权要求

无

示例

显示交换机的系统时间信息：

```
SW-5024# show system-time
```

26.28 show system-time dst

描述

该命令用于显示交换机的夏令时配置信息。

命令

show system-time dst

模式

特权模式和所有配置模式

特权要求

无

示例

显示夏令时信息：

```
SW-5024# show system-time dst
```

26.29 show system-time ntp

描述

该命令用于显示当前系统时间的 NTP 配置信息。

命令

show system-time ntp

模式

特权模式和所有配置模式

特权要求

无

示例

显示 NTP 配置信息：

SW-5024# show system-time ntp

26.30 show cable-diagnostics interface gigabitEthernet

描述

该命令用于显示对端口进行线缆检测后的结果。线缆检测功能能够检测与交换机相连的线缆是否有故障以及故障的位置，利用此功能可以辅助日常工程安装诊断。

命令

show cable-diagnostics interface gigabitEthernet *port*

参数

port ——指定进行线缆检测的端口号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示对端口 3 进行线缆检测的结果：

SW-5024# show cable-diagnostics interface gigabitEthernet 1/0/3

26.31 show cpu-utilization

描述

该命令用于显示系统在过去 5 秒/1 分钟/5 分钟内的 CPU 平均使用率。

命令

show cpu-utilization

模式

特权模式和所有配置模式

特权要求

无

示例

显示交换机的 CPU 使用率信息：

```
SW-5024# show cpu-utilization
```

26.32 show memory-utilization

描述

该命令用于显示系统在过去 5 秒/1 分钟/5 分钟内的内存平均使用率。

命令

show memory-utilization

模式

特权模式和所有配置模式

特权要求

无

示例

显示交换机的内存使用率信息：

```
SW-5024# show memory-utilization
```

第 27 章 IPv6 地址配置命令

IPv6 地址配置命令需在接口模式下设置，包括路由接口，LAG 和 VLAN 接口。进入这三层接口的配置模式并配置相关的 IPv6 参数。

27.1 ipv6 enable

描述

该命令用于开启接口的 IPv6 功能，它的 no 命令用于禁用接口的 IPv6 功能。交换机默认只有 VLAN1 开启 IPv6 功能。同一时间内只允许一个三层接口开启 IPv6 功能。

在进行 IPv6 地址配置管理之前，必须先开启 IPv6 功能。禁用 IPv6 功能会卸载掉主机的 IPv6 协议栈，使得先前配置的 IPv6 地址都不生效，任何基于 IPv6 地址的模块都将失效，例如：SSH，SSL，TFTPv6 等。启用 IPv6 功能则重新恢复原先配置的 IPv6 地址。

命令

ipv6 enable
no ipv6 enable

模式

接口配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启 VLAN1 的 IPv6 功能：

```
SW-5024(config)# interface vlan 1

SW-5024(config-if)# ipv6 enable
```

27.2 ipv6 address autoconfig

描述

该命令用于开启 IPv6 链路本地地址的自动配置功能。

交换机每个三层接口只有一个链路本地地址，有自动配置和手动配置两种配置方式。一般的 ipv6 链路地址的前缀为 fe80::/10。IPv6 路由器不能转发含有本地链

路或者外链的数据包。自动配置的 Ipv6 链路地址采用 EUI-64 格式。为了保证链路地址的唯一性，当自动配置的链路本地地址生效后，手动配置的链路本地地址将被删除。

命令

ipv6 address autoconfig

模式

接口配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启 VLAN1 的 IPv6 链路本地地址的自动配置功能：

```
SW-5024(config)# interface vlan 1
SW-5024(config-if)# ipv6 address autoconfig
```

27.3 ipv6 address link-local

描述

该命令用于使用手动配置方式配置交换机的 IPv6 链路本地地址，它的 no 命令用于删除配置的链路本地地址。

命令

ipv6 address *ipv6-addr* **link-local**

no ipv6 address *ipv6-addr* **link-local**

参数

ipv6-addr ——交换机的 IPv6 链路本地地址，该地址必须是以 fe80::/10 为前缀的标准 IPv6 地址，否则该命令无效。

模式

接口配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 VLAN1 的 IPv6 链路本地地址为 fe80::1234：

SW-5024(config)# interface vlan 1 **SW-5024(config-if)# ipv6 address** fe80::1234 **link-local**

27.4 ipv6 address dhcp

描述

该命令用于启用 DHCPv6 Client 功能。该功能开启后，交换机将通过 DHCPv6 服务器获取 IPv6 全球地址。它的 no 命令用于删除 DHCPv6 服务器分配的地址，或禁用 DHCPv6 Client 功能。

命令

ipv6 address dhcp

no ipv6 address dhcp

模式

接口配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启 VLAN1 的 DHCP Client 功能：

SW-5024(config)# interface vlan 1

SW-5024(config-if)# ipv6 address dhcp

27.5 ipv6 address ra

描述

该命令用于通过地址前缀和从接收到的 RA（Router Advertisement）消息中得到的其他配置参数配置交换机的 IPv6 全球地址，它的 no 命令用于禁用该功能。

命令

ipv6 address ra

no ipv6 address ra

模式

接口配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启 VLAN1 的“使用 RA 消息进行全球地址自动配置”功能：

```
SW-5024(config)# interface vlan 1
SW-5024(config-if)# ipv6 address ra
```

27.6 ipv6 address eui-64

描述

该命令用于手动配置 IPv6 全球地址。仅需指定一个地址前缀，系统将自动生成一个全球地址。它的 no 命令用于删除配置的 EUI-64 格式的 IPv6 全球地址。

命令

ipv6 address *ipv6-addr* **eui-64**

no ipv6 address *ipv6-addr* **eui-64**

参数

ipv6-addr ——EUI-64 格式的 IPv6 全球地址的地址前缀，例如 3ffe::1/64。

模式

接口配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置一个 EUI-64 格式的 IPv6 全球地址，该地址的地址前缀为 3ffe::1/64：

```
SW-5024(config)# interface vlan 1 SW-
5024(config-if)# ipv6 address 3ffe::/64 eui-64
```

27.7 ipv6 address

描述

该命令用于手动配置 IPv6 全球地址。它的 no 命令用于删除配置的 IPv6 全球地址。

命令

ipv6 address *ipv6-addr*

no ipv6 address *ipv6-addr*

参数

ipv6-addr ——IPv6 全球地址的地址前缀，例如 3ffe::1/64。

模式

接口配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置一个 VLAN1 的 IPv6 全球地址，该地址的地址前缀为 3001::1/64：

```
SW-5024(config)# interface vlan 1
SW-5024(config-if)# ipv6 address 3001::1/64
```

27.8 show ipv6 interface

描述

该命令用于显示已配置的 IPv6 功能信息，包括 IPv6 功能开启状态、链路本地地址、全球地址和 IPv6 组播组等。

命令

show ipv6 interface

模式

特权模式和所有配置模式

特权要求

无

示例

显示已配置的 IPv6 功能信息：

```
SW-5024(config)# show ipv6 interface
```

第 28 章以太网配置命令

以太网配置用来配置以太网端口的流量控制、协商模式、风暴抑制、带宽限制等。

28.1 interface gigabitEthernet

描述

该命令用于进入接口配置命令模式，对单个千兆以太网端口进行配置。

命令

interface gigabitEthernet *port*

参数

port ——要配置的以太网端口。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

进入接口配置模式，对以太网端口 2 进行配置：

SW-5024(config)# interface gigabitEthernet 1/0/2

28.2 interface range gigabitEthernet

描述

该命令用于进入接口配置命令模式，对多个千兆以太网端口进行同时配置。

命令

interface range gigabitEthernet *port-list*

参数

port-list ——要配置的以太网端口列表。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

说明

在 interface range gigabitEthernet 配置模式下，同一命令会作用到列表中的所有端口上。但各个端口是相互独立的，如果命令在一个端口上执行失败，不会影响其他端口上的执行。

示例

进入接口配置模式，同时对以太网端口 1,2,3,6,7 进行配置：

SW-5024(config)# interface range gigabitEthernet 1/0/1-3,1/0/6-7,1/0/9

28.3 description

描述

该命令用于设置端口描述，它的 no 命令用于清空相应端口的描述。

命令

description *string*

no description

参数

string ——端口描述的内容，可输入 1~16 个字符。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

为端口 1/0/5 添加端口描述 Port_5：

SW-5024(config)# interface gigabitEthernet 1/0/5

SW-5024(config-if)# description Port_5

28.4 shutdown

描述

该命令用于禁用以太网端口，它的 no 命令用于重新启用相应端口。

命令

shutdown

no shutdown

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

关闭以太网端口 1/0/3：

SW-5024(config)# interface gigabitEthernet 1/0/3

SW-5024(config-if)# shutdown

28.5 flow-control

描述

该命令用于启用端口的流量控制，它的 no 命令用于禁用相应端口的流控。启用流控能够同步接收端和发送端的速率，防止因速率不一致而导致的网络丢包。

命令

flow-control

no flow-control

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

开启以太网端口 1/0/3 的流量控制：

```
SW-5024(config)# interface gigabitEthernet 1/0/3
SW-5024(config-if)# flow-control
```

28.6 duplex

描述

该命令用于设置端口的双工模式，它的 no 命令用于恢复默认设置。

命令

duplex { auto | full | half }

no duplex

参数

auto | full | half ——端口双工模式，分别为自协商，全双工模式和半双工模式。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置以太网端口 1/0/3 为全双工模式：

```
SW-5024(config)# interface gigabitEthernet 1/0/3
SW-5024(config-if)# duplex full
```

28.7 jumbo

描述

该命令用于允许巨型帧通过端口，它的 no 命令用于禁用该功能。默认为禁用状态。

命令

jumbo

no jumbo

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

允许巨型帧通过以太网端口 1/0/3：

```
SW-5024(config)# interface gigabitEthernet 1/0/3
SW-5024(config-if)# jumbo
```

28.8 speed

描述

该命令用于设置端口的速率模式，它的 no 命令用于恢复默认设置。

命令

speed { 10 | 100 | 1000 | auto }

no speed

参数

10 | 100 | 1000 | auto ——端口速率模式，分别为 10M、100M、1000M、10000M 和自协商模式。默认为 auto 模式。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置以太网端口 1/0/3 的速率模式为 100M：

```
SW-5024(config)# interface gigabitEthernet 1/0/3
SW-5024(config-if)# speed 100
```

28.9 storm-control pps

描述

该命令用于配置接口上的风暴控制模式为 pps（每秒数据包），它的 no 命令用于关闭该模式。

命令

storm-control pps

no storm-control pps

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

说明

在 pps 模式中启用风暴控制功能和指定详细参数时，该命令应连同 **storm-control** 功能一起使用。

示例

设置端口 1/0/5 的风暴控制模式为 pps：

SW-5024(config)# interface gigabitEthernet 1/0/5

SW-5024(config-if)# storm-control pps

28.10 storm-control

描述

该命令用于启用端口的广播、组播、单播风暴的控制功能并设置阈值，它的 no 命令用于禁用相风暴抑制功能。

命令

storm-control { broadcast | multicast | unicast } { kbps | ratio | pps } { *rate* }

no storm-control { broadcast | multicast | unicast }

参数

broadcast | multicast | unicast ——启用广播/组播/单播风暴控制的接口。

kbps | ratio | pps ——指定风暴控制单位。

kbps: 指定千位每秒的门槛。

ratio: 指定阈值为带宽的百分比。

pps: 指定每秒数据包的阈值。

rate ——指定接收端口上的数据包的带宽。超过带宽的指定包流类型将被丢弃。对于 kbps，速率范围从 1 到 1000000 kbps。对于 ratio，速率范围从 1 到百分之 100。对于 pps，速率范围从 1 到 1488000 每秒。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

说明

在配置风暴控制类型为 kbps 或者 ratio 时，请确认端口不在 pps 模式。

示例

配置广播风暴控制率为 1000 kbps 的端口是 5：

SW-5024(config)# interface gigabitEthernet 1/0/5 **SW-5024(config-if)# storm-control** broadcast kbps 1000

28.11 bandwidth

描述

该命令用于配置以太网端口的出入口带宽限制，它的 no 命令用于禁用端口带宽限制。

命令

bandwidth {[**ingress** *ingress-rate*] [**egress** *egress-rate*]}

no bandwidth { all | ingress | egress }

参数

ingress-rate ——配置入口带宽限制，单位为 kbps。取值范围为 1-1000000Kbps 。

egress-rate ——配置出口带宽限制，单位为 kbps。取值范围为 1-1000000Kbps。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置端口 5 的入口带宽为 5120kbps，出口带宽为 1024kbps：

SW-5024(config)# interface gigabitEthernet 1/0/5 **SW-5024(config-if)# bandwidth ingress** 5120 **egress** 1024

28.12 clear counters

描述

该命令用于清除所有太网端口和 LAG 的统计信息。

命令

clear counters

clear counters interface [**gigabitEthernet** *port*] [**port-channel** *port-channel-id*]

参数

port ——以太网端口。

port-channel-id ——LAG 号。

模式

特权模式和所有配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

清除所有太网端口和 LAG 的统计信息：

```
SW-5024(config)# clear counters
```

28.13 show interface status

描述

该命令用于显示以太网端口和 LAG 的连接状态。

命令

show interface status [**gigabitEthernet** *port*] [**port-channel** *port-channel-id*]

参数

port ——要显示连接状态的以太网端口。

port-channel-id ——LAG 号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有以太网端口和 LAG 的连接状态：

SW-5024(config)# show interface status

显示端口 1/0/1 连接状态：

SW-5024(config)# show interface status gigabitEthernet 1/0/1

28.14 show interface counters

描述

该命令用于显示以太网端口和 LAG 的统计信息。

命令

show interface counters [**gigabitEthernet** *port*] [**port-channel** *port-channel-id*]

参数

port ——要显示统计信息的以太网端口。

port-channel-id ——LAG 号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口和 LAG 的统计信息：

SW-5024(config)# show interface counters

显示以太网端口 2 的统计信息：

SW-5024(config)# show interface counters gigabitEthernet 1/0/2

28.15 show interface configuration

描述

该命令用于显示以太网端口的配置信息，包括端口状态、流量控制、协商模式和端口描述等。

命令

show interface configuration [**gigabitEthernet** *port*] [**port-channel** *port-channel-id*]

参数

port ——要显示配置信息的以太网端口。

port-channel-id ——LAG 号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口和 LAG 的配置信息：

SW-5024(config)# show interface configuration

显示以太网端口 1/0/2 的配置信息：

SW-5024(config)# show interface configuration gigabitEthernet 1/0/2

28.16 show storm-control

描述

该命令用于显示端口的风暴抑制信息。

命令

show storm-control interface [**gigabitEthernet** *port-list*] [**port-channel** *port-channel-id-list*]

参数

port-list —— 要显示风暴抑制信息的端口号/端口列表。

port-channel-id-list ——LAG 列表。

模式

特权模式和所有配置模式

特权要求

无

示例

显示端口 4，5，6，7 的风暴抑制信息：

SW-5024(config)# show storm-control interface gigabitEthernet 1/0/4-7

28.17 show bandwidth

描述

该命令用于显示端口的带宽限制信息。

命令

show bandwidth interface [**gigabitEthernet** *port-list*] [**port-channel** *port-channel-id-list*]

参数

port-list ——要显示带宽限制信息的端口号/端口列表。

port-channel-id-list ——LAG 列表。

模式

特权模式和所有配置模式

特权要求

无

示例

显示端口 1/0/4 的带宽限制信息：

SW-5024(config)# show bandwidth interface gigabitEthernet 1/0/4

第 29 章 QoS 配置命令

QoS（Quality of Service，服务质量）功能用以提高网络传输的可靠性，提供更高质量的网络服务。

29.1 qos

描述

该命令用于设置基于端口的 CoS，它的 no 命令用于恢复某端口的默认 CoS。

命令

qos *cos-id*

no qos

命令

cos-id ——端口对应的优先级等级，可选范围为 0~7，表示 CoS0~CoS7。默认值为 0。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

说明

端口优先级只是端口的一个属性值，在设置了端口优先级后，数据流会根据端口的 CoS 值以及 IEEE 802.1P 中 CoS 到 TC 之间的映射关系来确定数据流的出口队列。

示例

设置端口 5 的优先级等级为 3：

```
SW-5024(config)# interface gigabitEthernet 1/0/5
SW-5024(config-if)# qos 3
```

29.2 qos dscp

描述

该命令用于启用 DSCP 优先级的 DSCP 值和出口队列的映射关系，它的 no 命令用于禁用该映射关系。

命令

qos dscp

no qos dscp

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

说明

DSCP (DiffServ Code Point，区分服务编码点)是 IEEE 对 IP ToS 字段的重定义，利用该字段可以将 IP 报文划分为 64 个优先级。开启 DSCP 优先级后，IP 数据流会根据数据包的 DSCP 值到 TC 队列之间的映射关系来确定数据包的出口队列。

示例

启用 DSCP 优先级的 DSCP 值和出口队列的映射关系：

```
SW-5024(config)# qos dscp
```

29.3 qos queue cos-map

描述

该命令用于设置 IEEE 802.1P 的优先级 tag 和出口队列的映射关系，它的 no 命令用于恢复默认设置。IEEE 802.1P 对 IEEE 802.1Q tag 中的 Pri 字段给予了推荐性的定义，利用该字段可以将数据包划分为 8 个优先级。启用 IEEE 802.1P 优先级后，交换机根据数据包是否带有 IEEE 802.1Q tag 来确定所使用的优先级模式。对于带有 tag 的数据包，应用 IEEE 802.1P 优先级，否则应用基于端口的优先级。

命令

qos queue cos-map { *tag/cos-id* } { *tc-id* }

no qos queue cos-map

参数

tag/cos-id ——IEEE 802.1P 协议里规定的 8 个优先级，取值范围是 CoS 0~CoS 7。

tc-id ——tag 对应的出口队列优先级，可选范围为 0~7，分别对应 8 个不同等级的出口队列 TC0~TC7。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

说明

1. 默认情况下，tag 和出口队列的对应关系是：0-TC2，1-TC0，2-TC1，3-TC3，4-TC4，5-TC5，6-TC6，7-TC7。
2. 优先级等级 TC0、TC1…TC7 中，数字越大，表示优先级越高。

示例

设置 CoS 5 的对应出口队列优先级为 TC2：

```
SW-5024(config)# qos queue cos-map 5 2
```

29.4 qos queue dscp-map

描述

该命令用于设置 DSCP 优先级的 DSCP 值和出口队列的映射关系，它的 no 命令用于恢复默认设置。DSCP（DiffServ Code Point，区分服务编码点）是 IEEE 对 IP ToS 字段的重定义，利用该字段可以将 IP 报文划分为 64 个优先级。启用 DSCP 优先级后，如果转发的数据包是 IP 报文，则交换机应用 DSCP 优先级；如果是非 IP 报文，交换机则根据是否启用了 IEEE 802.1P 优先级以及数据帧是否带有 tag 来决定采用哪种优先级模式。

命令

qos queue dscp-map { *dscp-list* } { *cos-id* }

no qos queue dscp-map

参数

dscp-list ——DSCP 值列表，可选择一个或多个 DSCP 值，连续的一组 DSCP 值可以用“-”符号表示，不连续的值之间、不同组之间需用逗号隔开，如 1,4-7,11 表示选择 1,4,5,6,7,11。DSCP 值的可选范围为 0~63。

cos-id ——DSCP 值对应的 CoS 优先级，可选范围为 0~7，分别对应 CoS0~CoS7。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

说明

默认情况下，DSCP 值 0-7 对应等级 CoS0，DSCP 值 8-15 对应等级 CoS1，DSCP 值 16-23 对应等级 CoS2，DSCP 值 24-31 对应等级 CoS3，DSCP 值 32-39 对

应等级 CoS4，DSCP 值 40-47 对应等级 CoS5，DSCP 值 48-55 对应等级 CoS6， DSCP 值 56-63 对应等级 CoS7。

示例

设置 DSCP 值 10-12 对应的 CoS 优先级为 CoS2：

SW-5024(config)# qos queue dscp-map 10-12 2

29.5 qos queue mode

描述

该命令用于设置出口队列调度模式，它的 no 命令用于恢复默认配置。在网络拥塞时，通常采用队列调度来解决多个数据流同时竞争使用资源的问题。交换机将根据设置的优先级队列和队列调度算法来控制报文的转发次序。本交换机以 TC0、 TC1…TC7 表示不同的优先级队列。

命令

qos queue mode { sp | wrr | spwrr | equ }

no qos queue mode

参数

sp —— 严格优先级模式。在此模式下，高优先级队列会占用全部带宽，只有在高优先级队列为空后，低优先级队列才进行数据转发。

wrr —— 加权轮询优先级模式。在此模式下，所有优先级队列按照预先分配的权重比同时发送数据包。各队列的权重比可通过 **qos queue weight** 命令配置，默认权重比为 1：2：4：8：16：32：64：127。

spwrr —— sp 和 wrr 的混合模式。在此模式下，交换机提供了 sp 和 wrr 两个调度组，其中 sp 组和 wrr 组之间遵循的是严格优先级调度规则，而 wrr 组内部队列遵循的是 wrr 调度规则。在该调度模式下，TC7 以及权重值为 0 的队列属于 sp 组；其他队列属于 wrr 组。各队列的权重值可通过 **qos queue weight** 命令配置，默认情况下，调度的时候首先是 TC7 按照 sp 的调度模式独自占用带宽，然后是 wrr 组的成员 TC0、TC1…TC6 按照权重比 1：2：4：8：16：32：64 的比例占用带宽。

equ —— 无优先级模式，默认选项。在此模式下所有的队列公平地占用带宽，所有队列的权重比是 1：1：1：1：1：1：1：1。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置出口队列的调度模式为加权轮询优先级模式：

```
SW-5024(config)# qos queue mode wrr
```

29.6 qos queue weight

描述

该命令用于配置每个队列权值后的调度方式指定为 WRR 或 SP + WRR。交换机将根据设置的优先级队列和队列调度算法来控制报文的转发次序。本交换机以 TC0、 TC1…TC7 表示不同的优先级队列。

命令

qos queue weight { *tc-id* } { *weight-value* }

参数

tc-id ——TC 队列的 ID，范围从 0 到 7。

weight-value ——配置指定 TC 队列的权重值。

当调度模式被指定为 WRR，权重值的范围从 1 到 127。8 个队列将根据他们的比例占用带宽。TC0, TC1, TC2, TC3, TC4, TC5,TC6 和 TC7 的默认值分比为：1，2，4，8，16，32，64 和 127。

当调度模式被指定为 SP + WRR，权重值的范围从 0 到 127。TC7 和其权重值在 SP 组队列设为 0；在其他队列，具有非零的权重值，属于 WRR 组。在这个 SP + WRR 调度模式，在 SP 组队列优先调度（优先级 TC6>TC5>TC4>TC3>TC2>TC1>TC0）。当没有数据包是在 SP 组发送，在 WRR 队列组会根据每个队列的权重值的预定。TC1、TC2，TC0，TC3、TC4 默认权重值，TC5 和 TC6 是 1，2，4，8，16，分别为 32 和 64，而 7 的值为 0，非可配置。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置出口队列的调度模式为加权轮询优先级模式，TC0，TC1，TC2 和 TC3 的权重值依次为 4，7，15 和 24：

```
SW-5024(config)# qos queue mode wrr
```

```
SW-5024(config)# qos queue weight 0 4
SW-5024(config)# qos queue weight 1 7
SW-5024(config)# qos queue weight 2 15
SW-5024(config)# qos queue weight 3 24
```

29.7 show qos interface

描述

该命令用于显示基于端口优先级的配置信息。

命令

show qos interface [**gigabitEthernet** *port-list*] [**port-channel** *lagid-list*]

参数

port-list ——要显示基于端口优先级配置信息的以太网端口号/端口列表。

lagid-list ——LAG 列表。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口和 LAG 的配置信息：

```
SW-5024# show qos interface
```

显示以太网端口 1/0/1-4 的 QoS 配置信息：

```
SW-5024# show qos interface gigabitEthernet 1/0/1-4
```

29.8 show qos cos-map

描述

该命令用于显示 IEEE 802.1P 优先级的配置信息和 cos-id 之间 tc-id 的映射关系。

命令

show qos cos-map

模式

特权模式和所有配置模式

特权要求

无

示例

显示 IEEE 802.1P 优先级的配置信息和 cos-id 之间 tc-id 的映射关系：

```
SW-5024# show qos cos-map
```

29.9 show qos dscp-map

描述

该命令用于显示 DSCP 优先级的配置信息。

命令

show qos dscp-map

模式

特权模式和所有配置模式

特权要求

无

示例

显示 DSCP 优先级的配置信息：

```
SW-5024# show qos dscp-map
```

29.10 show qos queue mode

描述

该命令用于显示出口队列的调度规则。

命令

show qos queue mode

模式

特权模式和所有配置模式

特权要求

无

示例

显示出口队列的调度规则：

```
SW-5024# show qos queue mode
```

29.11 show qos status

描述

该命令用于显示 IEEE 802.1P 优先级和 DSCP 优先级的启用状态。

命令

show qos status

模式

特权模式和所有配置模式

特权要求

无

示例

显示 IEEE 802.1P 优先级和 DSCP 优先级的启用状态：

```
SW-5024# show qos status
```

第 30 章端口监控配置命令

端口监控是将被监控端口的报文复制到监控端口，在监控端口接入数据分析设备，利用该设备分析经过监控端口的报文，达到网络监控和故障排除的目的。

30.1 monitor session destination interface

描述

该命令用于启用端口监控功能，并设置监控端口。它的 no 命令用于删除某个监控组。

命令

monitor session *session_num* **destination interface gigabitEthernet** *port*

no monitor session *session_num* **destination interface gigabitEthernet** *port* **no monitor session** *session_num*

参数

session_num ——监控组组号。取值仅可为 1。

port ——监控端口号。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置端口 1 为监控组 1 的监控端口：

SW-5024(config)# monitor session 1 **destination interface gigabitEthernet** 1/0/1

删除端口 2 为监控组 1 的监控端口：

SW-5024(config)# no monitor session 1 **destination interface gigabitEthernet** 1/0/2

删除监控组 1：

SW-5024(config)# no monitor session 1

30.2 monitor session source interface

描述

该命令用于设置被监控端口，它的 no 命令用于删除相应的被监控端口。

命令

monitor session *session_num* **source interface gigabitEthernet** *port-list mode*

no monitor session *session_num* **source interface gigabitEthernet** *port-list mode*

参数

session_num ——监控组组号。取值仅可为 1。

port-list ——被监控端口列表，可选择一个或多个端口。

mode ——监控模式。有三种选择：rx，tx 以及 both。rx（入口监控模式），将被监控端口收到的数据复制到监控端口，进行监控。tx（出口监控模式），将被监控端口发出的数据复制到监控端口，进行监控。both，同时进行入口监控和出口监控。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

说明

1. 监控端口对应当前的接口模式。
2. 被监控端口个数不做限制，但它不可以同时为监控端口。
3. 监控端口和被监控端口可以处于同一 VLAN 中，也可以不处于同一 VLAN 中。
4. 监控端口和被监控端口不能为汇聚端口成员。

示例

设置端口 4,5,7 为监控组 1 的被监控端口，并开启入口监控：

```
SW-5024(config)# monitor session 1  source interface gigabitEthernet
1/0/4-5,1/0/7 rx
```

删除端口 4 为监控组 1 的被监控端口，并关闭入口监控：

```
SW-5024(config)# no monitor session 1 source interface gigabitEthernet
1/0/4 rx
```

30.3 show monitor session

描述

该命令用于显示监控组的监控信息。

命令

show monitor session [*session_num*]

参数

session_num ——指定监控组组号，缺省情况下显示所有监控组的监控信息。取值仅可为 1。

模式

特权模式和所有配置模式

特权要求

无

示例

显示监控组 1 的监控配置信息：

```
SW-5024(config)# show monitor session 1
```

第 31 章端口隔离配置命令

端口隔离功能可以严格限制一个端口到另外一组端口的数据转发，从而提高网络的安全性。

31.1 port isolation

描述

该命令用于设置每个端口的端口隔离功能，限制每个端口仅可以向转发端口列表中的端口转发数据包。它的 no 命令用于删除相应设置。

命令

port isolation { [**gi-forward-list** *gi-forward-list*] [**po-forward-list** *po-forward-list*] }

no port isolation

参数

gi-forward-list ——转发端口列表，可选择一个或多个端口。

po-forward-list ——汇聚组列表。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置由端口 5 仅可以向端口 1,2,4 和 LAG2 转发数据包：

```
SW-5024(config)# interface gigabitEthernet 1/0/5
SW-5024(config-if)# port isolation gi-forward-list 1/0/1-2,1/0/4 po-forward-list 2
```

设置由端口 2 可以向任意端口转发数据包，即恢复出厂设置：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# no port isolation
```

31.2 show port isolation interface

描述

该命令用于查看每个端口和 LAG 的转发端口列表。

命令

show port isolation interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

参数

port ——选择希望查看转发端口列表信息的端口号。

port-channel-id ——选择希望查看转发端口列表信息的汇聚组号，取值范围 1-6。

模式

特权模式和所有配置模式

特权要求

无

示例

显示端口 1/0/2 的转发端口列表：

SW-5024# show port isolation interface gigabitEthernet 1/0/2

显示全部端口和 LAG 列表的转发端口列表：

SW-5024# show port isolation interface

第 32 章环路监测配置命令

环路监测功能可以检测出交换机物理端口所连接的网络中是否存在环路，从而降低网络中产生广播风暴的风险。

32.1 loopback-detection(global)

描述

该命令用于启用全局环路监测功能。它的 no 命令用于关闭全局环路监测功能。

命令

loopback-detection

no loopback-detection

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用交换机环路监测功能：

```
SW-5024(config)# loopback-detection
```

32.2 loopback-detection interval

描述

该命令用于配置环路监测的时间间隔，交换机在每个周期内发送一个监测报文来监测网络是否存在环路。

命令

loopback-detection interval *interval-time*

参数

interval-time ——配置环路监测的间隔时间，取值范围 1 到 1000 秒，默认为 30 秒。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置环路监测的间隔时间为 50 秒：

```
SW-5024(config)# loopback-detection interval 50
```

32.3 loopback-detection recovery-time

描述

该命令用于配置端口阻塞后的恢复时间。

命令

loopback-detection recovery-time *recovery-time*

参数

recovery-time ——当端口监测到网络出现环路时，将阻塞端口。在配置的恢复时间后，阻塞的端口将恢复正常属性，并重新监测环路。恢复时间请设置为监测间隔时间的整数倍，取值范围为 1~100 个监测时间间隔，默认为 3。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置环路监测的恢复时间为 3 个监测间隔时间：

```
SW-5024(config)# loopback-detection recovery-time 3
```

32.4 loopback-detection(interface)

描述

该命令用于启用指定端口的环路监测功能。它的 no 命令用于关闭全局环路监测功能。

命令

loopback-detection

no loopback-detection

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用端口 1-3 的环路监测功能：

SW-5024(config)# interface range gigabitEthernet 1/0/1-3

SW-5024(Config-if-range)# loopback-detection

32.5 loopback-detection config

描述

该命令用于配置端口阻塞后的处理模式和恢复模式。

命令

loopback-detection config [**process-mode** { alert | port-based }] [**recovery-mode** { auto | manual }]

参数

process-mode ——选择端口发现环路时的处理模式。有两个选项：

alert：端口上发现环路时只发出报警信息。

port based：端口上发现环路时发出报警信息，同时阻塞端口。

recovery-mode ——选择端口被阻塞后的恢复模式。有两个选项：

auto：端口被阻塞后经过自动恢复时间后会自动解除阻塞。

manual：端口被阻塞后只能手动解除阻塞状态。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置端口 2 的环路监测处理模式为 port-based，恢复模式为 manual：

SW-5024(config)# interface gigabitEthernet 1/0/2 **SW-5024(config-if)#**

loopback-detection config process-mode port-based **recovery-mode**

manual

32.6 loopback-detection recover

描述

该命令用于将指定的阻塞端口恢复为正常状态。

命令

loopback-detection recover

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将端口 2 由阻塞状态恢复为正常状态：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# loopback-detection recover
```

32.7 show loopback-detection global

描述

该命令用于显示环路监测功能的全局配置参数。

命令

show loopback-detection global

模式

特权模式和所有配置模式

特权要求

无

示例

查看环路监测功能的全局配置参数：

```
SW-5024# show loopback-detection global
```

32.8 show loopback-detection interface

描述

该命令用于显示所有端口的环路监测功能配置参数及端口状态。

命令

show loopback-detection interface [**gigabitEthernet** *port*]

参数

port ——指定端口号。

模式

特权模式和所有配置模式

特权要求

无

示例

查看所有端口的环路监测功能配置参数及端口状态：

SW-5024# show loopback-detection interface 查

看端口 5 的环路监测功能配置参数及端口状态：

SW-5024# show loopback-detection interface gigabitEthernet 1/0/5

第 33 章 ACL 配置命令

ACL（Access Control List，访问控制列表），通过配置匹配规则、处理操作以及时间权限来实现对数据包的过滤，提供灵活的安全访问控制策略，为控制网络安全提供方便。

33.1 time-range

描述

该命令用于添加时间段，它的 no 命令用于删除对应的时间段。当用户配置的 ACL 规则需要按时间段进行过滤时，可以先配置时间段，然后在相应的规则下通过时间段名称引用该时间段，这条规则只在该指定的时间段内生效，从而实现基于时间段的 ACL 过滤。

命令

time-range *name*

no time-range *name*

参数

name ——要添加的时间段名称，可输入 1~16 个字符。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

添加一个名为 tSeg1 的时间段：

```
SW-5024(config)# time-range tSeg1
```

33.2 absolute

描述

该命令用于配置时间段为绝对模式，它的 no 命令用于禁用绝对模式。

命令

absolute start *start-date* **end** *end-date*

no absolute

参数

start-date —— 绝对模式下的起始日期，形式为 MM/DD/YYYY，缺省时为 01/01/1970。

end-date —— 绝对模式下的结束日期，形式为 MM/DD/YYYY，缺省时为 12/31/2099。若起始日期和结束日期同时缺省，则禁止绝对模式。

模式

时间段配置模式（time-range create）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置时间段 tSeg1 为绝对模式，时间范围为 2012 年 5 月 5 日至 2012 年 10 月 5 日：

SW-5024(config)# time-range tSeg1 **SW-5024(config-time-range)#**

absolute start 05/05/2012 **end** 10/05/2012

33.3 periodic

描述

该命令用于配置时间段为周期模式，它的 no 命令用于禁用周期模式。

命令

periodic [**week-date** *week-day*] [**time-slice1** *time-slice*] [**time-slice2** *time-slice*] [**time-slice3** *time-slice*] [**time-slice4** *time-slice*]

no periodic

no periodic week-date

no periodic time-slice

参数

week-day —— 周期模式，形式为 1-3，6，也可输入 daily，weekend，weekdays。其中 1-3，6 表示周一、周二、周三和周六；daily 表示每天，即周一到周日；weekend 表示周末，即周六和周日；weekdays 表示工作日，即周一到周五。缺省时禁止周期模式。

模式

时间段配置模式（time-range create）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

编辑已添加的 tSeg1 时间段，时间范围为周末的 08:30-12:00：

SW-5024(config)#time-range tSeg1

SW-5024(config-time-range)#periodic week-date weekend **time-slice1** 08:30-12:00

33.4 holiday

描述

该命令用于在时间段配置模式下将指定时间段配置为假日模式。它的 no 命令用于禁用假日模式。

命令

holiday

no holiday

模式

时间段配置模式（time-range create）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

编辑已添加的 tSeg1 时间段为假日模式：

SW-5024(config)#time-range tSeg1

SW-5024(config-time-range)#holiday

33.5 holiday (global)

描述

该命令用于创建假期模式的节假日，它的 no 命令用于删除相应节假日。

命令

holiday *name* **start-date** *start-date* **end-date** *end-date* **no holiday**

参数

name ——假期模式的节假日，它的 no 命令用于删除相应节假日。

start-date ——节假日的起始日期，格式为 MM/DD，如 05/01。

end-date ——节假日的结束日期，格式为 MM/DD，如 05/03。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

定义节假日国庆节，并设置其起止时间为 10 月 1 日到 10 月 3 日：

SW-5024(config)#holiday nationalday **start-date** 10/01 **end-date** 10/03

33.6 access-list create

描述

该命令用于创建标准 IP ACL、扩展 IP ACL 和 IPv6 ACL。

命令

access-list create *access-list-num*

参数

access-list-num ——ACL ID 号。取值范围为 0 ~ 4499。其中， MAC ACL 的 ACL ID 范围为 0-499；标准 IP 的 ACL ID 范围为 500-1499；扩展 IP 的 ACL ID 范围为 1500-2499；混合 ACL ID 范围为 2500-3499 ； IPv6 ACL ID 范围为 3500-4499。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建一个 ID 号为 523 的标准 IP ACL：

SW-5024(config)# access-list create 523

33.7 mac access-list

描述

该命令用于创建 MAC ACL，它的 no 命令用于删除对应的 MAC ACL。MAC ACL 根据数据包的源 MAC 地址、目的 MAC 地址、VLAN、二层协议类型等二层信息制定匹配规则，对数据包进行相应的分析处理。

命令

mac access-list *access-list-num*

no mac access-list *access-list-num*

参数

access-list-num ——要添加规则的 ACL ID 号，取值范围为 0-499。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建一个 ID 号为 23 的 MAC ACL：

SW-5024(config)# mac access-list 23

33.8 access-list standard

描述

该命令用于添加标准 IP ACL 规则，它的 no 命令用于删除对应规则。标准 IP ACL 可以根据数据包的 IP 地址信息制定匹配规则，对数据包进行相应的分析处理。

命令

access-list standard *acl-id* **rule** *rule-id* { deny | permit } [[**sip** *source-ip*] **smask** *source-ip-mask*] [[**dip** *destination-ip*] **dmask** *destination-ip-mask*] [**tseg** *time-segment*]

no access-list standard *acl-id* **rule** *rule-id*

参数

acl-id ——要添加规则的 ACL ID 号。

rule-id ——当前添加的规则的 ID 号。

deny ——交换机将丢弃满足匹配规则的数据包。

permit ——交换机将丢转发满足匹配规则的数据包。这是交换机的默认处理方式。

source-ip ——规则包含的源 IP 地址。

source-ip-mask ——源 IP 地址的掩码。若您输入了源 IP 地址，则必须输入相应的掩码。

destination-ip ——规则包含的目的 IP 地址。

destination-ip-mask ——目的 IP 地址的掩码。若您输入了目的 IP 地址，则必须输入相应的掩码。

time-segment ——规则生效的时间段的名称，缺省时为无限制。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建一个 ID 号为 520 的标准 IP ACL，为其添加规则 10，其中源 IP 地址为 192.168.0.100，掩码为 255.255.255.0，规则生效的时间段为 tSeg1，对满足此规则的数据包，交换机予以转发：

SW-5024(config)# access-list create 520 **SW-5024(config)# access-list standard** 520 **rule** 10 permit **sip** 192.168.0.100 **smask** 255.255.255.0 **tseg** tSeg1

33.9 access-list extended

描述

该命令用于添加扩展 IP ACL 规则，它的 no 命令用于删除对应规则。

命令

access-list extended *acl-id* **rule** *rule-id* { deny | permit } [[**sip** *source-ip*] **smask** *source-ip-mask*] [[**dip** *destination-ip*] **dmask** *destination-ip-mask*] [**tseg** *time-segment*] [**frag** {disable | enable}] [**dscp** *dscp*] [**s-port** *s-port*] [**d-port** *d-port*] [**tcpflag** *tcpflag*] [**protocol** *protocol*] [**tos** *tos*] [**pre** *pre*]

no access-list extended *acl-id* **rule** *rule-id*

参数

acl-id ——要添加规则的 ACL ID 号。

rule-id ——当前添加的规则的 ID 号。

deny ——交换机将丢弃满足匹配规则的数据包。

permit ——交换机将丢转发满足匹配规则的数据包。这是交换机的默认处理方式。

source-ip ——规则包含的源 IP 地址。

source-ip-mask ——源 IP 地址的掩码。若您输入了源 IP 地址，则必须输入相应的掩码。

destination-ip ——规则包含的目的 IP 地址。

destination-ip-mask ——目的 IP 地址的掩码。若您输入了目的 IP 地址，则必须输入相应的掩码。

time-segment ——规则生效的时间段的名称，缺省时为无限制。

frag —— 开启或关闭分片处理功能。当开启时，该规则将会处理所有的分片，而总是转发报文中的最后一个分片。

dscp ——设置 dscp 的值，范围 0-63。

s-port ——当 IP 协议选择 TCP/UDP 时，此处配置规则包含的 TCP/UDP 源端口号。

d-port ——当 IP 协议选择 TCP/UDP 时，此处配置规则包含的 TCP/UDP 目的端口号。

tcpflag —— 当 IP 协议为 TCP 时指定此规则中 TCP 报文的 flag 值。

protocol ——设置匹配的协议字段的值。

tos ——规则包含的 IP ToS 字段信息。

pre ——规则包含的 IP Precedence 字段信息。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建一个 ID 号为 2220 的扩展 IP ACL，为其添加规则 10，其中源 IP 地址为 192.168.0.100，掩码为 255.255.255.0，规则生效的时间段为 tSeg1，对满足此规则的数据包，交换机予以转发：

SW-5024(config)# access-list create 2220 **SW-5024(config)# access-list extended** 2220 **rule** 10 permit **sip** 192.168.0.100 **smask** 255.255.255.0 **tseg** tSeg1

33.10 access-list combined

描述

该命令用于添加混合 ACL 规则，它的 no 命令用于删除对应规则。混合 ACL 可以基于 MAC 地址信息、IP 地址信息及数据包的其他信息制定一系列匹配规则，对数据包进行相应的分析处理。

命令

access-list combined *acl-id* **rule** *rule-id* { deny | permit } [[**smac** *source-mac*] **smask** *source-mac-mask*] [[**dmac** *destination-mac*] **dmask** *destination-mac-mask*] [**vid** *vlan-id*] [**type** *ethernet-type*] [**pri** *user-pri*] [[**sip** *source-ip*] **sip-mask** *source-ip-mask*] [[**dip** *destination-ip*] **dip-mask** *destination-ip-mask*] [**tseg** *time-segment*]

no access-list combined *acl-id* **rule** *rule-id*

参数

acl-id ——要添加规则的 ACL ID 号。

rule-id ——当前添加的规则的 ID 号。

deny ——交换机将丢弃满足匹配规则的数据包。

permit ——交换机将丢转发满足匹配规则的数据包。这是交换机的默认处理方式。

source-mac ——规则包含的源 MAC 地址。

source-mac-mask ——源 MAC 地址的掩码。若您输入了源 MAC 地址，则必须输入相应的掩码。

destination-mac——规则包含的目的 MAC 地址。

destination-mac-mask ——目的 MAC 地址的掩码。若您输入了目的 MAC 地址，则必须输入相应的掩码。

vlan-id —— 规则包含的 VLAN ID，取值范围为 1~4094。

ethernet-type ——规则包含的以太网类型信息，输入格式为 4 位 16 进制数。

user-pri ——用户优先级，取值范围为 0~7，缺省时为无限制。

source-ip ——规则包含的源 IP 地址。

source-ip-mask ——源 IP 地址的掩码。若您输入了源 IP 地址，则必须输入相应的掩码。

destination-ip ——规则包含的目的 IP 地址。

destination-ip-mask ——目的 IP 地址的掩码。若您输入了目的 IP 地址，则必须输入相应的掩码。

time-segment ——规则生效的时间段的名称，缺省时为无限制。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

说明

将混合 ACL 绑定到某个 VLAN 或端口之前，请先将 SDM 模板设置为 default 或者 enterpriseV4 并保存配置。可使用 **sdm prefer** 命令配置 SDM 模板。

示例

创建一个 ID 号为 2700 的混合 ACL，为其添加规则 10，其中源 MAC 地址为 00:01:3F:48:16:23，掩码为 11:11:11:11:11:00，源 IP 地址为 192.168.0.100，掩码为 255.255.255.0，规则生效的时间段为 tSeg1，对满足此规则的数据包，交换机予以转发：

SW-5024(config)# access-list create 2700 **SW-5024(config)# access-list combined** 2700 **rule** 10 permit **smac** 00:01:3F:48:16:23 **smask** 11:11:11:11:11:00 **sip** 192.168.0.100 **sip-mask** 255.255.255.0 **tseg** tSeg1

33.11 access-list ipv6

描述

该命令用于添加 IPv6 ACL 规则，它的 no 命令用于删除对应规则。

命令

access-list ipv6 *acl-id* **rule** *rule-id* { deny | permit } [**dscp** *dscp-value*] [**flow-label** *flow-label-value*] [[**sip** *source-ip*] **sip-mask** *source-ip-mask*] [[**dip** *destination-ip*] **dip-mask** *destination-ip-mask*] [**s-port** *s-port*] [**d-port** *d-port*] [**tseg** *time-segment*]

no access-list ipv6 *acl-id* **rule** *rule-id*

参数

acl-id ——要添加规则的 ACL ID 号。

rule-id ——当前添加的规则的 ID 号。

deny ——交换机将丢弃满足匹配规则的数据包。

permit ——交换机将丢转发满足匹配规则的数据包。这是交换机的默认处理方式。

dscp-value ——指定 dscp 的值，范围从 0-63。

flow-label-value ——IPv6 流标签，范围从 0-0xfffff。

source-ip ——规则包含的源 IP 地址。

source-ip-mask ——源 IP 地址的掩码。若您输入了源 IP 地址，则必须输入相应的掩码。

destination-ip ——规则包含的目的 IP 地址。

destination-ip-mask ——目的 IP 地址的掩码。若您输入了目的 IP 地址，则必须输入相应的掩码。

s-port ——当 IP 协议选择 TCP/UDP 时，此处配置规则包含的 TCP/UDP 源端口号。

d-port ——当 IP 协议选择 TCP/UDP 时，此处配置规则包含的 TCP/UDP 目的端口号。

time-segment ——规则生效的时间段的名称，缺省时为无限制。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

说明

在将 IPv6 ACL 连接到一个 VLAN 或接口时，请先配置 SDM 模板为“enterprisev6”并保存你的配置。要了解更多 SDM 配置信息，请查看 **sdm prefer**。

示例

创建一个 ID 号为 3600 的扩展 IPv6 ACL，为其添加规则 10，其中源 IP 地址为 3001::1，掩码为 255.255.255.0，对满足此规则的数据包，交换机予以转发：

```
SW-5024(config)# access-list create 3600 SW-5024(config)# access-list
ipv6 3600 rule 10 permit sip 3001::1 sip-mask ffff:ffff:ff00:00ff tseg tSeg1
```

33.12 rule

描述

该命令用于编辑已创建的 MAC ACL 规则，它的 no 命令用于删除相应的规则。

命令

rule *rule-id* { deny | permit } [[**smac** *source-mac*] **smask** *source-mac-mask*] [[**dmac** *destination-mac*] **dmask** *destination-mac-mask*] [**vid** *vlan-id*] [**type** *ethernet-type*] [**pri** *user-pri*] [**tseg** *time-segment*]

no rule *rule-id*

参数

rule-id ——当前规则的 ID 号。

deny ——交换机将丢弃满足匹配规则的数据包。

permit ——交换机将丢转发满足匹配规则的数据包。这是交换机的默认处理方式。

source-mac ——规则包含的源 MAC 地址。

source-mac-mask ——源 MAC 地址的掩码。若您输入了源 MAC 地址，则必须输入相应的掩码。

destination-mac——规则包含的目的 MAC 地址。

destination-mac-mask ——目的 MAC 地址的掩码。若您输入了目的 MAC 地址，则必须输入相应的掩码。

vlan-id —— 规则包含的 VLAN ID，取值范围为 1~4094。

ethernet-type ——规则包含的以太网类型信息，输入格式为 4 位 16 进制数。

user-pri ——用户优先级，取值范围为 0~7，缺省时为无限制。

time-segment ——规则生效的时间段的名称，缺省时为无限制。

模式

MAC Access-list 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

编辑 MAC ACL 20 的规则 10，其中源 MAC 地址为 00:01:3F:48:16:23，掩码为 11:11:11:11:11:00，VLAN ID 为 2，用户优先级为 5，规则生效的时间段为 tSeg1，对满足此规则的数据包，交换机予以转发：

SW-5024(config)# mac access-list 20 **SW-5024(config-mac-acl)# rule**

10 permit **smac** 00:01:3F:48:16:23 **smask** 11:11:11:11:11:00 **vid** 2 **pri** 5

tseg tRange1

33.13 access-list policy name

描述

该命令用于添加 Policy，它的 no 命令用于删除对应的 Policy 条目。Policy 功能将 ACL 和动作组合起来，组成一个访问控制策略，对符合相应 ACL 规则的数据包进行控制，添加的操作包括流镜像、流监控 QoS 重标记和端口重定向。

命令

access-list policy name *name*

no access-list policy name *name*

参数

name ——要添加的 Policy 名称，可输入 1~16 个字符。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

添加一个名为 policy1 的 Policy：

```
SW-5024(config)# access-list policy name policy1
```

33.14 access-list policy action

描述

该命令用于为 Policy 添加 ACL 并进入 Action 配置模式以设置动作，它的 no 命令用于删除相应动作。

命令

access-list policy action *policy-name acl-id*

no access-list policy action *policy-name acl-id*

参数

policy-name ——要设置的 Policy 的名称，可输入 1~16 个字符。

acl-id ——Policy 作用的 ACL 的 ID 号。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

为名为 policy1 的 Policy 添加 ACL 120：

SW-5024(config)# access-list policy action policy1 120

33.15 redirect interface

描述

该命令用于为 Policy 添加重定向动作，设置将匹配了相应 ACL 的数据包转发到指定端口。它的 no 命令用于删除指定端口。

命令

redirect interface { **gigabitEthernet** *port* }

参数

port ——端口重定向的出口端口，即将匹配了相应 ACL 的数据包转发到此处指定的端口。缺省时为所有端口。

模式

Action 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

为名为 policy1 的 Policy 添加动作，对符合 ACL 120 相应规则的数据包，转发到端口 2：

SW-5024(config)#access-list policy action policy1 120 **SW-5024(config-action)#redirect interface gigabitEthernet** 1/0/2

33.16 s-condition

描述

该命令用于为 Policy 添加流监管动作。它的 no 命令用于删除动作。

命令

s-condition rate *rate* **osd** { none | discard }

参数

rate ——流监管的额定速率，取值范围为 1~1000000（kbps）。

osd ——流监管的超速处理，即对超过额定速率的数据包的处理方式，有不处理（none）和丢弃（discard）两个选项。缺省时为不处理。

模式

Action 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

为名为 policy1 的 Policy 添加动作，对符合 ACL 120 相应规则的数据包，若速率超过 1000kbps，交换机将予以丢弃：

```
SW-5024(config)#access-list policy action policy1 120
SW-5024(config-action)#s-condition rate 1000 osd discard
```

33.17 s-mirror

描述

该命令用于为 Policy 添加流镜像动作。它的 no 命令删除镜像动作。

命令

s-mirror interface { **gigabitEthernet** *port* }

参数

port ——流镜像的镜像端口。

模式

Action 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

为名为 policy1 的 Policy 添加动作，将符合 ACL 120 相应规则的数据包复制到端口 2：

```
SW-5024(config)#access-list policy action policy1 120 SW-
5024(config-action)#s-mirror interface gigabitEthernet 1/0/2
```

33.18 qos-remark

描述

该命令用于为 Policy 添加 QoS 重标记动作，它的 no 命令用于删除相应动作。

命令

qos-remark [**dscp** *dscp*] [**priority** *pri*]

no qos-remark

参数

dscp ——QoS 重标记之 DSCP，为匹配了相应 ACL 的数据包指定 DSCP 域。取值范围为 0~63，缺省时为无限制。

pri ——QoS 重标记之本地优先级，为匹配了相应 ACL 的数据包指定优先级。取值范围为 0~7。

模式

Action 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

为名为 policy1 的 Policy 添加动作，对符合 ACL 120 相应规则的数据包，指定 DSCP 域为 30，优先级为 2：

```
SW-5024(config)#access-list policy action policy1 120

SW-5024(config-action)# qos-remark dscp 30 priority 2
```

33.19 access-list bind acl(interface)

描述

该命令用于绑定 ACL 到指定端口，它的 no 命令用于取消绑定。

命令

access-list bind acl *acl-id*

no access-list bind acl *acl-id*

参数

acl-id ——要绑定到端口的 ACL 号。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将 ACL100 绑定到端口 2：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# access-list bind acl 100
```

33.20 access-list bind acl(vlan)

描述

该命令用于绑定 ACL 到指定 VLAN，它的 no 命令用于取消绑定。

命令

access-list bind acl *acl-id*

no access-list bind acl *acl-id*

参数

acl-id ——要绑定到端口的 ACL 号。

模式

接口配置模式（interface vlan）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将 ACL 100 绑定到 VLAN 2：

```
SW-5024(config)# interface vlan 2
SW-5024(config-if)# access-list bind acl 100
```

33.21 access-list bind(interface)

描述

该命令用于绑定 Policy 到指定端口，它的 no 命令用于取消绑定。

命令

access-list bind *policy-name*

no access-list bind *policy-name*

参数

policy-name ——要绑定到端口的 Policy 名称。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将 policy1 绑定到端口 2：

SW-5024(config)# interface gigabitEthernet 1/0/2

SW-5024(config-if)# access-list bind policy1

33.22 access-list bind(vlan)

描述

该命令用于绑定 Policy 到指定 VLAN，它的 no 命令用于取消绑定。

命令

access-list bind *policy-name*

no access-list bind *policy-name*

参数

policy-name ——要绑定到 VLAN 的 Policy 名称。

模式

接口配置模式（interface vlan）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将 policy1 绑定到 VLAN 2：

SW-5024(config)# interface vlan 2

SW-5024(config-if)# access-list bind policy1

33.23 show access-list

描述

该命令用于显示 ACL 配置。

命令

show access-list *acl-id*

参数

acl-id ——要显示配置的 ACL ID 号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 ID 号为 20 的 MAC ACL 的配置：

```
SW-5024(config)# show access-list 20
```

33.24 show access-list policy

描述

该命令用于显示 Policy 配置。

命令

show access-list policy *name*

参数

name ——要显示配置的 policy 的名称。

模式

特权模式和所有配置模式

特权要求

无

示例

显示名为 policy1 的信息：

```
SW-5024(config)# show access-list policy policy1
```

33.25 show access-list bind

描述

该命令用于显示 Policy 绑定配置。

命令

show access-list bind

模式

特权模式和所有配置模式

特权要求

无

示例

显示 Policy 绑定设置：

```
SW-5024(config)# show access-list bind
```

第 34 章 MSTP 配置命令

MSTP（Multiple Spanning Tree Protocol，多生成树协议）是在 STP 和 RSTP 的基础上，根据 IEEE 协会制定的 IEEE 802.1S 标准建立的，用于在局域网中消除数据链路层物理环路的协议。生成树协议的基本思想是通过构造一棵或多棵自然树的方法达到裁剪冗余环路的目的，同时实现链路备份和路径最优化。

34.1 debug spanning-tree

描述

该命令用于开启生成树活动时的调试功能，它的 no 命令用于关闭该功能。

命令

debug spanning-tree { all | bpdu receive | bpdu transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc }

no debug spanning-tree { all | bpdu receive | bpdu transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc }

Parameters

all ——显示生成树的全部调试信息。

bpdu receive ——显示所接收生成树的网桥协议数据单元（BPDU）调试信息。

bpdu transmit ——显示发出的生成树的网桥协议数据单元（BPDU）调试信息。

cmpmsg ——显示消息优先的调试信息。

errors ——显示 MSTP 错误的调试信息。

flush ——显示地址表刷新的调试信息。

init ——显示数据结构初始化的调试信息。

migration ——显示版本迁移的调试信息。

proposals ——显示 MSTP 握手的调试信息。

roles ——显示 MSTP 接口角色切换的调试信息。

state ——显示 MSTP 接口状态变化的调试信息。

tc ——显示 MSTP 拓扑事件的调试信息。

模式

特权模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示生成树的全部调试信息：

```
SW-5024# debug spanning-tree all
```

34.2 spanning-tree(global)

描述

该命令用于全局开启生成树功能，它的 no 命令用于禁用生成树功能。

命令

spanning-tree

no spanning-tree

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启交换机的生成树功能：

```
SW-5024(config)# spanning-tree
```

34.3 spanning-tree (interface)

描述

该命令用于为指定端口开启生成树功能，它的 no 命令用于禁用生成树功能。

命令

spanning-tree

no spanning-tree

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启端口 2 的生成树功能：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# spanning-tree
```

34.4 spanning-tree common-config

描述

该命令用于生成树协议端口配置，它的 no 命令用于恢复默认配置。CIST（Common and Internal Spanning Tree，公共和内部生成树）是连接一个交换网络内所有设备的单生成树。本命令用来配置端口基于 CIST 的参数以及所有实例的共用参数。

命令

spanning-tree common-config [**port-priority** *pri*] [**ext-cost** *ext-cost*] [**int-cost** *int-cost*] [**portfast** { enable | disable }] [**point-to-point** { auto | open | close }]

no spanning-tree common-config

参数

pri ——端口优先级，它是确定端口是否会被对端设备选为根端口的重要依据，同等条件下优先级高的端口将被选为根端口。值越小，表示优先级越高。取值范围 0~240，间隔 16，缺省时为 128。

ext-cost ——外部路径开销。它是在不同 MST 域之间的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高，缺省时为自动。

int-cost ——内部路径开销。它是在 MST 域内的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高，缺省时为自动。

portfast ——是否启用边缘端口，缺省时为禁用（disable）。边缘端口由阻塞状态向转发状态迁移时，可实现快速迁移，无需等待延迟时间。

point-to-point ——点对点链路状态，有自动（auto）、强制开启（open）和强制关闭（close）三个选项，缺省时为自动。以点对点链路相连的两个端口，如果为根端口或者指定端口，则可以快速迁移到转发状态，从而减少不必要的转发延迟时间。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用端口 1 的 STP 功能，并设置其优先级为 64，内、外部路径开销均为 100，开启边缘端口：

```
SW-5024(config)# interface gigabitEthernet 1/0/1 SW-5024(config-
if)# spanning-tree common-config port-priority 64 ext-cost 100
int-cost 100 portfast enable point-to-point open
```

34.5 spanning-tree mode

描述

该命令用于配置生成树的模式，它的 no 命令用于恢复默认配置。

命令

spanning-tree mode { stp | rstp | mstp }

no spanning-tree mode

参数

stp ——默认模式，为生成树兼容模式。

rstp ——快速生成树兼容模式。

mstp ——多重生成树模式。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置生成树模式为 MSTP：

```
SW-5024(config)# spanning-tree mode mstp
```

34.6 spanning-tree mst configuration

描述

该命令用于从全局配置模式下进入 MST 配置模式，它的 no 命令用于将相应的实例恢复为默认配置。

命令

spanning-tree mst configuration

no spanning-tree mst configuration

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

进入 MST 配置模式：

```
SW-5024(config)# spanning-tree mst

configuration SW-5024(Config-mst)#
```

34.7 instance

描述

该命令用于配置 VLAN-MSTP 实例映射，它的 no 命令用于移除映射关系或删除相应的实例。实例被删除后，与该实例有关的映射关系也会被移除。

命令

instance *instance-id* **vlan** *vlan-id*

no instance *instance-id* [**vlan** *vlan-id*]

Parameters

instance-id ——实例 ID，范围为 1~8。

vlan-id ——要加入该实例的 VLAN ID。

模式

MST 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将 VLAN1-100 映射到实例 1：

```
SW-5024(config)# spanning-tree mst
configuration SW-5024(config-mst)# instance 1
```

vlan 1-100 移除实例 1 中的 VLAN1-100 映射：

```
SW-5024(config)# spanning-tree mst configuration
SW-5024(config-mst)# no instance 1
```

将实例 1 的 VLAN1-50 从 VLAN1-100 映射中移除：

```
SW-5024(config)# spanning-tree mst configuration
SW-5024(config-mst)# no instance 1 vlan 1-50
```

34.8 name

描述

该命令用于配置 MST 实例的域名。MSTP 可以将交换网络划分为多个域，有着相同域配置和 VLAN-实例映射关系的交换机被认为属于同一个 MST 域（Multiple Spanning Tree Regions，多生成树域）。域配置包括配置域名和修订级别。

命令

name *name*

Parameters

name ——域名，用于标识 MST 域，可输入 1~32 个字符。

模式

MST 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 MSTP 的域名为 region1：

```
SW-5024(config)# spanning-tree mst
configuration SW-5024(config-mst)# name region1
```

34.9 revision

描述

该命令用于配置 MST 实例的修订级别。

命令

revision *revision*

Parameters

revision —— The revision level for MST region identification, ranging from 0 to 65535.

模式

MST 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 MSTP 的修订级别为 100：

SW-5024(config)# spanning-tree mst

configuration SW-5024(config-mst)# revision 100

34.10 spanning-tree mst instance

描述

该命令用于配置 MST 实例的优先级，它的 no 命令用于恢复对应实例的默认优先级。

命令

spanning-tree mst instance *instance-id* **priority** *pri*

no spanning-tree mst instance *instance-id* **priority**

参数

instance-id ——实例 ID，范围为 1~8。

pri ——MSTI 优先级，它是在对应实例 ID 中，确定交换机是否会被选为根桥的重要依据。取值范围 0~61440，间隔 4096，缺省时为 32768。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用实例 1，并设置 MSTI 优先级为 4096：

```
SW-5024(config)# spanning-tree mst instance 1 priority 4096
```

34.11 spanning-tree mst

描述

该命令用于 MSTP 实例端口配置，它的 no 命令用于恢复对应实例端口的默认配置。端口在不同的生成树实例中可以担任不同的角色，本命令用来配置不同实例 ID 中的端口的参数。

命令

spanning-tree mst instance *instance-id* {[**port-priority** *pri*] | [**cost** *cost*]}

no spanning-tree mst instance *instance-id*

参数

instance-id ——需要配置端口属性的实例 ID 号，取值范围 1~8。

pri ——端口优先级，它是在对应实例 ID 中，确定端口是否会被对端设备选为根端口的重要依据。取值范围 0~240，间隔 16，缺省时为 128。

cost ——路径开销。路径开销是在 MST 域内的对应实例中，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。取值范围为 0~200000，其中 0 表示自动。值越小，表示优先级越高，缺省时为自动。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置实例 1 的端口 1 优先级为 64，路径开销为 2000：

```
SW-5024(config)# interface gigabitEthernet 1/0/1 SW-5024(config-if)#

spanning-tree mst instance 1 port-priority 64 cost 2000
```

34.12 spanning-tree priority

描述

该命令用于配置桥优先级，它的 no 命令用于恢复默认配置。

命令

spanning-tree priority *pri*

no spanning-tree priority

参数

pri ——桥优先级。取值范围 0~61440，缺省时为 32768。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置桥优先级为 4096：

SW-5024(config)# spanning-tree priority 4096

34.13 spanning-tree tc-defend

描述

该命令用于配置生成树的全局 TC 保护，它的 no 命令用于恢复默认配置。设备在接收到 TC 报文（网络拓扑发生变化的通知报文）后，会执行地址表项的删除操作。当设备受到恶意的 TC 报文攻击时，频繁地删除操作会给设备带来很大负担，给网络的稳定带来很大隐患。TC 保护可以限制一定周期内交换机接收 TC 报文的最大数目，从而控制地址表项的删除操作。

命令

spanning-tree tc-defend threshold *threshold* **period**

period **no spanning-tree tc-defend**

参数

threshold ——TC 保护阀值，取值范围 1~100（数据包），缺省时为 20。TC 保护阀值是在 TC 保护周期内，交换机收到 TC 报文的最大数目。超过该数目后，交换机在该周期内不再进行删除地址表的操作。

period ——TC 保护周期，取值范围 1~10（秒），缺省时为 5。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置 TC 保护阀值为 30 数据包，TC 保护周期为 10 秒：

SW-5024(config)# spanning-tree tc-defend threshold 30 **period** 10

34.14 spanning-tree timer

描述

该命令用于配置生成树的联络时间、老化时间、传输延时，它的 no 命令用于恢复默认配置。

命令

spanning-tree timer {[**forward-time** *forward-time*] [**hello-time** *hello-time*] [**max-age** *max-age*]}

no spanning-tree timer

参数

forward-time ——传输延时，即在网络拓扑改变后，交换机的端口状态迁移的延时时间，取值范围为 4~30（秒），默认值为 15，并且 2×（传输延时-1）≥老化时间。

hello-time ——联络时间，即交换机发送协议报文的周期，用于检测链路是否存在故障，取值范围为 1~10（秒），默认值为 2，并且 2×（联络时间+1）≤老化时间。

max-age ——老化时间，即协议报文在交换机中能够保存的最大生命期，取值范围为 6~40（秒），默认值为 20。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置生成树的传输延时为 16 秒，联络时间为 3 秒，老化时间为 22 秒：

SW-5024(config)# spanning-tree timer forward-time 16 **hello-time**

3 **max-age** 22

34.15 spanning-tree hold-count

描述

该命令用于设置生成树流量限制，它的 no 命令用于恢复默认配置。

命令

spanning-tree hold-count *value*

no spanning-tree hold-count

参数

value ——流量限制，即在每个联络时间内，端口最多能够发送的协议报文的速度。取值范围为 1~20（pps），默认值为 5。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置生成树流量限制为 8pps：

```
SW-5024(config)# spanning-tree hold-count 8
```

34.16 spanning-tree max-hops

描述

该命令用于设置生成树协议报文被转发的最大跳数，它的 no 命令用于恢复默认配置。

命令

spanning-tree max-hops *value*

no spanning-tree max-hops

参数

value ——最大跳数，即协议报文被转发的最大跳数，它限制了生成树的规模，取值范围为 1~40（跳），默认值为 20。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置最大跳数为 30：

```
SW-5024(config)# spanning-tree max-hops 30
```

34.17 spanning-tree bpdufilter

描述

该命令用于为指定端口开启 BPDU 过滤功能，启用了 BPDU 报文过滤功能的端口，将不再接收和转发任何 BPDU 报文，但是会向外发送自身的 BPDU 报文，从而防止交换机受到 BPDU 报文的攻击，保证 STP 计算的正确性。它的 no 命令用于禁用该功能。

命令

spanning-tree bpdufilter

no spanning-tree bpdufilter

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

为端口 2 开启 BPDU 过滤功能：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# spanning-tree bpdufilter
```

34.18 spanning-tree bpduguard

描述

该命令用于为指定端口开启 BPDU 保护功能，启用了 BPDU 保护功能后，如果端口收到了 BPDU 报文，MSTP 就将这些端口关闭，同时通知网管这些端口被 MSTP 关闭，被关闭的端口只能由网络管理人员来恢复。它的 no 命令用于禁用该功能。

命令

spanning-tree bpduguard

no spanning-tree bpduguard

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

为端口 2 开启 BPDU 保护功能：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# spanning-tree bpduguard
```

34.19 spanning-tree guard loop

描述

该命令用于启用环路保护功能，它的 no 命令用于禁用该功能。环路保护可以防止由于链路拥塞或者单向链路故障，导致下游设备重新计算生成树，从而产生的网络环路现象。

命令

spanning-tree guard loop

no spanning-tree guard loop

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启端口 2 的环路保护：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# spanning-tree guard loop
```

34.20 spanning-tree guard root

描述

该命令用于启用根桥保护，它的 no 命令用于禁用该功能。根桥保护可以防止当前合法根桥失去根桥地位，从而引起的网络拓扑结构的错误变动。

命令

spanning-tree guard root

no spanning-tree guard root

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启端口 2 的根桥保护：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# spanning-tree guard root
```

34.21 spanning-tree guard tc

描述

该命令用于启用 TC 保护，它的 no 命令用于禁用该功能。启用 TC 保护功能后，交换机在“TC 保护周期”内，收到 TC-BPDU 的最大数目为“TC 保护阈值”处所设的数目，超过该数目后，交换机在该周期内不再进行地址表删除操作。这样就可以避免频繁地删除转发地址表项。

命令

spanning-tree guard tc

no spanning-tree guard tc

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启端口 2 的 TC 保护：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# spanning-tree guard tc
```

34.22 spanning-tree mcheck

描述

该命令用于启用协议迁移。

命令

spanning-tree mcheck

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用端口 2 的协议迁移：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# spanning-tree mcheck
```

34.23 show spanning-tree active

描述

该命令用于显示生成树的当前运行状态信息。

命令

show spanning-tree active

模式

特权模式和所有配置模式

特权要求

无

示例

显示生成树当前运行状态信息：

```
SW-5024(config)# show spanning-tree active
```

34.24 show spanning-tree bridge

描述

该命令用于显示生成树的参数配置信息。

命令

show spanning-tree bridge [forward-time | hello-time | hold-count | max-age | max-hops | mode | priority | state]

模式

特权模式和所有配置模式

特权要求

无

示例

显示生成树参数配置信息：

```
SW-5024(config)# show spanning-tree bridge
```

34.25 show spanning-tree interface

描述

该命令用于显示生成树的端口配置信息。

命令

show spanning-tree interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*] [edge | ext-cost | int-cost | mode | p2p | priority | role | state | status]

参数

port ——要显示配置信息的端口号。

port-channel-id ——LAG 号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口的生成树信息：

```
SW-5024(config)# show spanning-tree
```

interface 显示端口 20 的生成树信息：

```
SW-5024(config)# show spanning-tree interface gigabitEthernet
```

1/0/2 显示端口 20 的生成树模式：

```
SW-5024(config)# show spanning-tree interface gigabitEthernet
```

```
1/0/2 mode
```

34.26 show spanning-tree interface-security

描述

该命令用于显示生成树的端口安全配置信息。

命令

show spanning-tree interface-security [**gigabitEthernet** *port* | **port-channel** *port-channel-id*] [bpdufilter | bpduguard | loop | root | tc | tc-defend]

参数

port ——要显示配置信息的端口号。

port-channel-id ——LAG 号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口的安全配置信息：

```
SW-5024(config)# show spanning-tree interface-
```

security 显示端口 1 的安全配置信息：

```
SW-5024(config)# show spanning-tree interface-security
```

```
gigabitEthernet 1/0/1
```

显示接口 bpdu 过滤器的安全配置信息：

SW-5024(config)# show spanning-tree interface-security bpdufilter

34.27 show spanning-tree mst

描述

该命令用于显示 MST 实例的相关信息。

命令

show spanning-tree mst { **configuration** [**digest**] | **instance** *instance-id*

[**interface** [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]] }

参数

instance-id ——要显示配置信息的实例 ID，取值范围 1~8。

port ——要显示配置信息的端口号。

port-channel-id ——LAG 号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN 和 MST 实例的区域信息和配置信息：

SW-5024(config)#show spanning-tree mst

configuration 显示 MST 实例 1 的相关信息：

SW-5024(config)#show spanning-tree mst instance

1 显示 MST 实例 1 的所有端口信息：

SW-5024(config)#show spanning-tree mst instance 1 **interface**

第 35 章 Ethernet OAM 配置命令

Ethernet OAM (Operation, Administration, Maintenance)是一种用于网络监控和排错的二层协议。OAM 实体之间会进行数据包交互，并将网络状态上报给网络管理员。Enternet OAM 是一种慢速协议，只会占用极少的端口带宽，因此几乎不会影响端口之间的数据传输。

35.1 ethernet-oam

描述

该命令用于开启端口的 Ethernet OAM 功能。它的 no 命令用于禁用端口的 Ethernet OAM 功能。

命令

ethernet-oam

no ethernet-oam

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

在端口 2 上开启 Ethernet OAM 功：” **SW-**

```
5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)#ethernet-oam
```

35.2 ethernet-oam mode

描述

该命令用于配置端口的 OAM 模式。它的 no 命令用于将端口的 OAM 模式恢复为默认配置。默认配置为 active。

命令

ethernet-oam mode { passive | active }

no ethernet-oam mode

参数

passive ——配置 OAM 模式为 passive。

active ——配置 OAM 模式为 active。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

将端口 2 的 OAM 模式配置为 passive：

SW-5024(config)# interface gigabitEthernet 1/0/2

SW-5024(config-if)#ethernet-oam mode passive

35.3 ethernet-oam link-monitor symbol-period

描述

该命令用于配置 error symbol period 链路事件的相关 OAM 参数。它的 no 命令用于恢复默认值。

命令

ethernet-oam link-monitor symbol-period { **threshold** *threshold* | **window** *window* | **notify** { disable | enable }}

no ethernet-oam link-monitor symbol-period { threshold | window | notify }

参数

threshold —— 配置 error symbol period 链路事件产生的阈值。当 window 时间内交换机收到的 symbol error 数量超过这个阈值，则会产生 error symbol period 链路事件。参数范围为 1- 4294967295，默认值为 1。

window —— 配置 window 值。参数范围为 10-600，默认值为 10。该参数的单位是（*100 毫秒），比如配置 window 值为 20，表示 20*100 毫秒，即 2000 毫秒。

notify —— 配置是否让端口上报该类型事件。默认为开启。

threshold | window | notify ——选择需要恢复为默认值的参数。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

在端口 2 上配置 error symbol-period 链路事件的 threshold 值为 5、window 值为 3 秒（3000 毫秒）：

SW-5024(config)# interface gigabitEthernet 1/0/2 **SW-5024(config-if)#**

ethernet-oam link-monitor symbol-period threshold 5 **window** 30

35.4 ethernet-oam link-monitor frame

描述

该命令用于配置 error frame 链路事件的相关 OAM 参数。它的 no 命令用于恢复默认值。

命令

ethernet-oam link-monitor frame { [**threshold** *threshold*] [**window** *window*] [**notify** { disable | enable }] }

no ethernet-oam link-monitor frame { threshold | window | notify }

参数

threshold —— 配置 error frame 链路事件产生的阈值。当 window 时间内交换机收到的 error frame 数量超过这个阈值，则会产生 error frame 链路事件。参数范围为 1- 4294967295，默认值为 1。

window —— 配置 window 值。参数范围为 10-600，默认值为 10。该参数的单位是（*100 毫秒），比如配置 window 值为 20，表示 20*100 毫秒，即 2000 毫秒。

notify —— 配置是否让端口上报该类型事件。默认为开启。

threshold | window | notify ——选择需要恢复为默认值的参数。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

在端口 3 上配置 error frame 链路事件的 threshold 值为 6、window 值为 9 秒（9000 毫秒）：

```
SW-5024(config)# interface gigabitEthernet 1/0/3 SW-5024(config-if)#

ethernet-oam link-monitor frame threshold 6 window 90
```

35.5 ethernet-oam link-monitor frame-period

描述

该命令用于配置 error frame period 链路事件的相关 OAM 参数。它的 no 命令用于恢复默认值。

命令

ethernet-oam link-monitor frame-period { [**threshold** *threshold*] [**window** *window*] [**notify** { disable | enable }] }

no ethernet-oam link-monitor frame-period { threshold | window | notify }

参数

threshold —— 配置 error frame period 链路事件产生的阈值。当 window 个帧内交换机收到的 error frame period 数量超过这个阈值，则会产生 error frame period 链路事件。参数范围为 1- 4294967295，默认值为 1。

window —— 配置 window 值。参数范围为 148810-89286000，单位为帧个数。对于百兆端口，默认值为 148810；对于千兆端口，默认值为 1488100。

notify —— 配置是否让端口上报该类型事件。默认为开启。

threshold | window | notify ——选择需要恢复为默认值的参数。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

在端口 4 上配置 error frame period 链路事件的 threshold 值为 6、window 值为 150000 个帧：

SW-5024(config)# interface gigabitEthernet 1/0/4 **SW-5024(config-if)#**

ethernet-oam link-monitor frame-period threshold 6 **window** 150000

35.6 ethernet-oam link-monitor frame-seconds

描述

该命令用于配置 error frame seconds 链路事件的相关 OAM 参数。它的 no 命令用于恢复默认值。

命令

ethernet-oam link-monitor frame-seconds { [**threshold** *threshold*] [**window** *window*] [**notify** { disable | enable }] }

no ethernet-oam link-monitor frame-seconds { threshold | window | notify }

参数

threshold —— 配置 error frame seconds 链路事件产生的阈值。当 window 时间内交换机检测到的 error frame seconds 数量超过这个阈值，则会产生 error frame 链路事件。参数范围为 1-900，默认值为 1。

window —— 配置 window 值。参数范围为 100-9000，默认值为 600。该参数的单位是（*100 毫秒），比如配置 window 值为 600，表示 600*100 毫秒，即 60000 毫秒。

notify —— 配置是否让端口上报该类型事件。默认为开启。

threshold | window | notify ——选择需要恢复为默认值的参数。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

在端口 5 上配置 error frame seconds 链路事件的 threshold 值为 8、window 值为 30 秒（30000 毫秒）：

```
SW-5024(config)# interface gigabitEthernet 1/0/5 SW-5024(config-if)#

ethernet-oam link-monitor frame-seconds threshold 8 window 300
```

35.7 ethernet-oam remote-failure

描述

该命令用于配置交换机是否上报 dying gasp 链路事件和 critical 链路事件。它的 no 命令用于恢复默认值。

命令

ethernet-oam remote-failure { dying-gasp | critical-event } **notify** { disable | enable }

no ethernet-oam remote-failure { dying-gasp | critical-event } **notify**

参数

dying-gasp —— 配置 dying gasp 链路事件是否会被上报。该链路事件是指诸如断电等不可恢复的事件。

critical-event ——配置 dying gasp 链路事件是否会被上报。该链路事件是指没有被定义的严重链路事件。

notify ——配置是否让端口上报该类型事件。默认为开启。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

配置端口 7 不上报 dying gasp 链路事件：

SW-5024(config)# interface gigabitEthernet 1/0/7 **SW-5024(config-if)#**

ethernet-oam remote-failure dying-gasp **notify** disable

35.8 ethernet-oam remote-loopback received-remote-loopback

描述

该命令用于配置端口对接收到的 remote loopback 请求的处理方式。它的 no 命令用于恢复默认配置。

命令

ethernet-oam remote-loopback received-remote-loopback { process | ignore }

no ethernet-oam remote-loopback received-remote-loopback

参数

process —— 处理收到的 remote loopback 请求。

ignore —— 不对收到的 remote loopback 请求进行处理。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

配置端口 1 收到 remote loopback 请求后对其进行处理：

SW-5024(config)# interface gigabitEthernet 1/0/1

SW-5024(config-if)# ethernet-oam remote-loopback received

-remote-loopback process

35.9 ethernet-oam remote-loopback

描述

该命令用于请求对端开启或禁用 remote loopback 模式。

命令

ethernet-oam remote-loopback { start | stop }

参数

start —— 请求对端开启 remote loopback 模式。

stop ——请求端口禁用 remote loopback 模式。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

在端口 3 上请求对端开启 remote loopback 模式：

SW-5024(config)# interface gigabitEthernet 1/0/3 **SW-**

5024(config-if)# ethernet-oam remote-loopback start

35.10 clear ethernet-oam statistics

描述

该命令用于清除 Ethernet OAM 数据。

命令

clear ethernet-oam statistics [**interface gigabitEthernet** *port*]

参数

port ——配置需要清除 Ethernet OAM 数据的以太网端口号。缺省情况下，所有端口上的 Ethernet OAM 数据都会被清除。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

清除端口 3 的 Ethernet OAM 数据：

```
SW-5024(config)# clear ethernet-oam statistics interface gigabit Ethernet
1/0/3
```

35.11 clear ethernet-oam event-log

描述

该命令用于清除 Ethernet OAM 链路事件记录。

命令

clear ethernet-oam event-log [**interface gigabitEthernet** *port*]

参数

port ——配置需要清除 Ethernet OAM 链路事件记录的以太网端口号。缺省情况下，所有端口上的 Ethernet OAM 链路事件记录都会被清除。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

清除端口 3 上的 Ethernet OAM 链路事件记录：

```
SW-5024(config)# clear ethernet-oam event-log interface gigabitEthernet
1/0/3
```

35.12 show ethernet-oam configuration

描述

该命令用于显示 Ethernet OAM 配置信息。

命令

show ethernet-oam configuration [**interface gigabitEthernet** *port*]

参数

port ——配置需要显示的以太网端口号。缺省情况下，所有端口的 Ethernet OAM 配置都会显示。

模式

特权模式以及所有配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

显示端口 2 的 Ethernet OAM 配置信息：

SW-5024(config)# show ethernet-oam configuration interface

gigabitEthernet 1/0/2

35.13 show ethernet-oam event-log

描述

该命令用于显示 Ethernet OAM 链路事件记录。

命令

show ethernet-oam event-log [**interface gigabitEthernet** *port*]

参数

port —— 配置需要显示的以太网端口号。缺省情况下，所有端口的 Ethernet OAM 链路事件记录都会显示。

模式

特权模式以及所有配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

显示端口 2 的 Ethernet OAM 链路事件记录：

```
SW-5024(config)# show ethernet-oam event-log interface gigabitEthernet
1/0/2
```

35.14 show ethernet-oam statistics

描述

该命令用于显示 Ethernet OAM 数据。

命令

show ethernet-oam statistics [**interface gigabitEthernet** *port*]

参数

port ——配置需要显示的以太网端口号。缺省情况下，所有端口的 Ethernet OAM 数据都会显示。

模式

特权模式以及所有配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

显示端口 2 的 Ethernet OAM 数据：

```
SW-5024(config)# show ethernet-oam statistics interface gigabitEthernet
1/0/2
```

35.15 show ethernet-oam status

描述

该命令用于显示本地和对端的 Ethernet OAM 状态。

命令

show ethernet-oam status [**interface gigabitEthernet** *port*]

参数

port —— 配置需要显示的以太网端口号。缺省情况下，所有端口的本地和对端 Ethernet OAM 状态都会显示。

模式

特权模式以及所有配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

显示端口 2 的本地和对端 Ethernet OAM 状态：

```
SW-5024(config)# show ethernet-oam status interface gigabitEthernet
1/0/2
```

第 36 章 DLDP 配置命令

DLDP (Device Link Detection Protocol，设备链路检测协议)可以用来监控光纤或双绞线的链路状态，并检测设备之间是否存在单向链路。当两个设备之间检测存在单向链路时，DLDP 可以根据用户配置，自动或通知用户手动关闭相关端口，以防止网络问题的发生。

36.1 dldp(global)

描述

该命令用于全局启用 DLDP 功能，它的 no 命令用于禁用该功能。

命令

dldp

no dldp

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

全局启用 DLDP 功能：

```
SW-5024(config)# dldp
```

36.2 dldp interval

描述

该命令用于设置 DLDP 的通告间隔。

命令

dldp interval *interval-time*

参数

interval-time —— 设置 DLDP 通告间隔，范围为 1—30 秒，默认为 5 秒。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置 DLDP 通告间隔为 10 秒：：

```
SW-5024(config)# dldp interval 10
```

36.3 dldp shut-mode

描述

该命令用于设置当检测到单向链路时 DLDP 的关闭模式。

命令

dldp shut-mode { auto | manual }

参数

auto —— 当检测到单向链路时自动关闭相应端口。默认使用该模式。

manual —— 当检测到单向链路时交换机显示警告，提醒管理员手动关闭端口。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置关闭模式为手动关闭：

```
SW-5024(config)# dldp shut-mode manual
```

36.4 dldp reset(global)

描述

该命令用于全局重置所有单向链路状态，并重新开始链路检测过程。

命令

dldp reset

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

全局重置 DLDP 功能：

```
SW-5024(config)# dldp reset
```

36.5 dldp(interface)

描述

该命令用于启用端口的 DLDP 功能，它的 no 命令用于禁用该功能。

命令

dldp

no dldp

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

开启端口 2-4 的 DLDP 功能：

```
SW-5024 (config)# interface range gigabitEthernet 1/0/2-4
SW-5024 (config-if-range)# dldp
```

36.6 dldp reset(interface)

描述

该命令用于重置端口单向链路状态，并重新开始链路检测过程。

命令

dldp reset

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

重置端口 2-4 的 DLDP 功能：

```
SW-5024 (config)# interface range gigabitEthernet 1/0/2-4

SW-5024 (config-if-range)# dldp reset
```

36.7 show dldp

描述

该命令用于显示 DLDP 功能的全局配置信息,如 DLDP 全局状态、DLDP 通告间隔和关闭模式。

命令

show dldp

模式

特权模式和所有配置模式

特权要求

无

示例

显示 DLDP 功能的全局配置信息：

```
SW-5024# show dldp
```

36.8 show dldp interface

描述

该命令用于显示端口的 DLDP 功能配置信息，缺省情况下显示所有端口的配置和状态。

命令

show dldp interface [**gigabitEthernet** *port*]

参数

port —— The Gigabit Ethernet port number.

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口的配置和状态：

```
SW-5024# show dldp interface
```

显示端口 5 的配置和状态：

```
SW-5024# show dldp interface gigabitEthernet 1/0/5
```

第 37 章 IGMP 侦听配置命令

IGMP Snooping（Internet Group Management Protocol Snooping，IGMP 侦听）是运行在二层交换机上的组播约束机制，用于管理和控制组播组。启用 IGMP 侦听功能可以有效地避免组播数据在网络中广播。

37.1 ip igmp snooping(global)

描述

该命令用于全局开启 IGMP 侦听功能，它的 no 命令用于禁用该功能。

命令

ip igmp snooping

no ip igmp snooping

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启 IGMP 全局配置:

```
SW-5024(config)# ip igmp snooping
```

37.2 ip igmp snooping(interface)

描述

该命令用于为指定端口配置 IGMP 侦听功能，它的 no 命令用于禁用该功能。

命令

ip igmp snooping

no ip igmp snooping

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启端口 3 的 IGMP 侦听功能：

```
SW-5024(config)# interface gigabitEthernet 1/0/3
SW-5024(config-if)# ip igmp snooping
```

37.3 ip igmp snooping rtime

描述

该命令用于全局设置 IGMP 侦听路由器端口老化时间，它的 no 命令用于恢复默认值。

命令

ip igmp snooping rtime *rtime*
no ip igmp snooping rtime

参数

rtime ——指定的老化时间秒数，取值范围 60-600 秒。默认的老化时间是 300 秒。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局设置 IGMP 侦听路由器端口老化时间为 100 秒：

```
SW-5024(config)# ip igmp snooping rtime 100
```

37.4 ip igmp snooping mtime

描述

该命令用于全局设置 IGMP 侦听成员端口的老化时间，它的 no 命令用于恢复默认值。默认的老化时间是 260 秒。

命令

ip igmp snooping mtime *mtime*
no ip igmp snooping mtime

参数

mtime ——指定的老化时间秒数，取值范围 60-600 秒。默认的老化时间是 260 秒。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置 IGMP 侦听全局成员端口时间为 100 秒：

```
SW-5024(config)# ip igmp snooping mtime 100
```

37.5 ip igmp snooping report-suppression

描述

该命令用于开启 IGMP Report 报文抑制功能。启用时，对于每个组播组，只有第一个 IGMP 报告消息转发到 3 层设备，随后接收到相同组播组的 IGMP 报告报文将被丢弃。它的 no 命令用于禁用该功能，默认处于关闭状态。

命令

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启 IGMP Report 报文抑制：

```
SW-5024(config)# ip igmp snooping report-suppression
```

37.6 ip igmp snooping immediate-leave

描述

该命令用于开启端口的快速离开功能，它的 no 命令用于禁用该功能。

命令

ip igmp snooping immediate-leave

no ip igmp snooping immediate-leave

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启端口 3 的快速离开功能：

```
SW-5024(config)# interface gigabitEthernet 1/0/3 SW-
5024(config-if)# ip igmp snooping immediate-leave
```

37.7 ip igmp snooping drop-unknown

描述

该命令用于开启未知组播报文丢弃功能，它的 no 命令用于禁用该功能。

命令

ip igmp snooping drop-unknown

no ip igmp snooping drop-unknown

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启未知组播报文丢弃功能：

```
SW-5024(config)# ip igmp snooping drop-unknown
```

37.8 ip igmp snooping last-listener query-inteval

描述

该命令用于指定发送特定组查询报文的间隔时间，它的 no 命令用于恢复默认值。默认的间隔是 1 秒。

命令

ip igmp snooping last-listener query-inteval *interval*

no ip igmp snooping last-listener query-inteval

参数

interval —— 指定发送特定组查询报文的间隔秒数，从 1 到 5。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置发送特定组查询报文的间隔时间为 3s：

SW-5024(config)# ip igmp snooping last-listener query-inteval 3

37.9 ip igmp snooping last-listener query-count

描述

该命令用于指定发送特定组查询报文的次数，它的 no 命令用于恢复默认值。默认的次数是 2 次。

命令

ip igmp snooping last-listener query-count *num*

no ip igmp snooping last-listener query-count

参数

num —— 指定发送特定组查询报文的次数，从 1 到 5。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置发送特定组查询报文的次数为 3：

SW-5024(config)# ip igmp snooping last-listener query-count 3

37.10 ip igmp snooping vlan-config

描述

该命令用于启用指定 VLAN 的 IGMP 侦听功能，并修改其 IGMP 参数以及创建静态组播地址条目。它的 no 命令用于禁用指定 VLAN 的 IGMP 侦听功能。IGMP 侦听所建立的组播组是基于 VLAN 广播域的，不同的 VLAN 可以设置不同的 IGMP 参数，本命令用于配置每个 VLAN 的 IGMP 侦听参数。

命令

ip igmp snooping vlan-config *vlan-id-list* [**rtime** *router-time* | **mtime** *member-time* | **rport interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }]

ip igmp snooping vlan-config *vlan-id-list* **static** *ip* **interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }

no ip igmp snooping vlan-config *vlan-id list* [**rtime** *router-time* | **mtime** *member-time* | **rport interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }]

no ip igmp snooping vlan-config *vlan-id-list* **static** *ip* **interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }

参数

vlan-id-list —— 需要修改 IGMP 参数的 VLAN ID 列表，取值范围 1~4094，格式为 1-3，5。

router-time —— 路由器端口时间。在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。取值范围 60~600（秒），默认值为 0。

member-time —— 成员端口时间。在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。取值范围 60~600（秒），默认值为 0。

port-list —— 成员端口列表。

port-channel-id —— LAG 号。

ip —— 静态组播 IP 地址。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用 VLAN 1-3 的 IGMP 侦听功能，将它们的路由器端口时间设置为 300 秒、成员端口时间设置为 200 秒，并将 VLAN1-2 的路由端口号设为 1：

SW-5024(config)# ip igmp snooping vlan-config 1-3 **rtime** 300

SW-5024(config)# ip igmp snooping vlan-config 1-3 **mtime** 200

SW-5024(config)# ip igmp snooping vlan-config 1-2 **rport interface**

gigabitEthernet 1/0/1

在 VLAN 2 中添加静态组播地址条目，组播 IP 为 225.0.0.1，转发端口为端口 1-3：

SW-5024(config)# ip igmp snooping vlan-config 2 **static** 225.0.0.1 **interface**

gigabitEthernet 1/0/1-3

37.11 ip igmp snooping vlan-config (router-port-forbidden)

描述

该命令用于禁止在指定 VLAN 中的指定端口成为路由端口。它的 no 命令用于删除被禁用的路由端口。

命令

ip igmp snooping vlan-config *vlan-id-list* **router-port-forbidd interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }

no ip igmp snooping vlan-config *vlan-id-list* **router-port-forbidd interface** [**gigabitEthernet** *port-list* | **port-channel** *port-channel-id*]

参数

vlan-id-list —— 需要修改 IGMP 参数的 VLAN ID 列表，取值范围 1~4094，格式为 1-3，5。

port-list —— 禁止成为路由端口的端口列表。该端口将丢弃收到的组播组报文。

port-channel-id ——禁止成为路由端口的 LAG。该 LAG 将丢弃收到的组播组报文。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

禁止 VLAN 1 中的端口 1-3 成为路由端口：

SW-5024(config)# ip igmp snooping vlan-config 1 **router-port-forbidd interface gigabitEthernet** 1/0/1-3

37.12 ip igmp snooping multi-vlan-config

描述

该命令用于创建组播 VLAN，它的 no 命令用于删除相应的组播 VLAN。

命令

ip igmp snooping multi-vlan-config [*vlan-id*] [**rtime** *router-time* | **mtime** *member-time* | **rport interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }]

no ip igmp snooping multi-vlan-config [**rtime** *router-time* | **mtime** *member-time* | **rport interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }]

参数

vlan-id —— 需要修改配置的 VLAN ID，取值范围 2~4094。如果没有配置该参数，将会选择默认的组播 VLAN。

router-time —— 路由端口老化时间。在所设时间内，如果交换机没有从路由端口接收到 IGMP 查询报文，就认为该路由器端口失效。取值范围 60~600（秒），默认值为 0 且会使用全局路由老化时间。

member-time —— 成员端口老化时间。在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。取值范围 60~600（秒），默认值为 0 且会使用全局成员端口老化时间。

port-list —— 成员端口列表。

port-channel-id —— LAG 号。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

开启组播 VLAN 功能，并设置 VLAN 3 的路由端口老化时间为 100 秒、成员端口老化时间为 100 秒，端口 1/0/3 为静态路由端口：

SW-5024(config)# ip igmp snooping multi-vlan-config 3 **rtime** 100 **SW-5024(config)# ip igmp snooping multi-vlan-config** 3 **mtime** 100 **SW-5024(config)# ip igmp snooping multi-vlan-config** 3 **rport interface gigabitEthernet** 1/0/3

37.13 ip igmp snooping multi-vlan-config (router-port-forbidden)

描述

该命令用于禁止在指定组播 VLAN 中的指定端口成为路由端口。它的 no 命令用于删除被禁用的路由端口。

命令

ip igmp snooping multi-vlan-config [*vlan-id*] **router-port-forbidd interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }

no ip igmp snooping multi-vlan-config router-port-forbidd [**interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }]

参数

vlan-id —— 组播 VLAN ID。

port-list —— 禁止成为路由端口的端口列表。该端口将丢弃收到的组播组报文。

port-channel-id ——禁止成为路由端口的 LAG。该 LAG 将丢弃收到的组播组报文。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

禁止 VLAN 1 中的端口 1-3 成为路由端口：

SW-5024(config)# ip igmp snooping multi-vlan-config 1 **router-port-forbidd interface gigabitEthernet** 1/0/1-3

37.14 ip igmp snooping multi-vlan-config (source-ip-replace)

描述

该命令用于替换指定组播 VLAN 中 IGMP 报文的源 IP 地址。它的 no 命令用于禁止替换源 IP 地址。

命令

ip igmp snooping multi-vlan-config [*vlan-id*] **replace-sourceip** *ip*

no ip igmp snooping multi-vlan-config replace-sourceip

参数

vlan-id —— 组播 VLAN ID。

ip —— 指定替换的 IP 地址。该 IP 地址将替换掉 IGMP 报文中的源 IP 地址。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

将组播 VLAN 1 中的 IGMP 报文的源 IP 地址替换为 192.168.0.112：

SW-5024(config)# ip igmp snooping multi-vlan-config 1 **replace-sourceip** 192.168.0.112

37.15 ip igmp snooping querier vlan

描述

该命令用于在指定 VLAN 中使能 IGMP 侦听查询器功能，它的 no 命令用于禁用指定 VLAN 中的 IGMP 侦听查询器功能。

命令

ip igmp snooping querier vlan *vlan-id*

no ip igmp snooping querier vlan *vlan-id*

参数

vlan-id —— VLAN ID，范围为 1-4094。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

在 VLAN1 中使能 IGMP 侦听查询器功能：

```
SW-5024(config)#ip igmp snooping querier vlan 1
```

37.16 ip igmp snooping querier vlan (general query)

描述

该命令用于配置 IGMP 侦听查询器的通用查询报文参数，它的 no 命令用于恢复默认配置。

命令

ip igmp snooping querier vlan *vlan-id* { **query-interval** *interval* | **max-response-time** *response-time* | **general-query source-ip** *ip-addr* }

no ip igmp snooping querier vlan *vlan-id* { **query-interval** | **max-response-time** | **general-query source-ip** }

参数

vlan-id —— VLAN ID，范围为 1-4094。

interval —— 发送通用查询报文的时间间隔，取值范围从 10-300 秒，默认值为 60 秒。

response-time —— 指定客户收到通用查询报文后的最大响应时间，取值范围 1 到 25 秒，默认值为 10 秒。

ip-addr —— IGMP 侦听查询器所发送的通用查询报文的源 IP，不能为组播或广播地址。默认值为 192.18.0.1。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

在 VLAN2 中使能 IGMP 侦听查询器的通用查询报文的发送间隔为 200 秒，最大响应时间为 20 秒：

SW-5024(config)#ip igmp snooping querier vlan 2 **query-interval** 200 **SW-5024(config)#ip igmp snooping querier vlan** 2 **max-response-time** 20

37.17 ip igmp snooping max-groups

描述

ip igmp snooping max-groups 用于配置一个端口最多能够加入到组播组数量； **ip igmp snooping max-groups action** 用于配置当一个端口所加入到组播组数量达到限定值时，对收到的新 IGMP 报告报文的处理动作。**no ip igmp snooping max-groups** 用于清除指定端口的最大组播组限制，恢复其默认的无限制状态；

no ip igmp snooping max-groups action 用于恢复端口所加入到组播组达到上限时，对 IGMP 报文的默认操作，即丢弃操作。这些命令只对动态组播组有效。

命令

ip igmp snooping max-groups [*maxgroup*]

ip igmp snooping max-groups action { drop | replace }

no ip igmp snooping max-groups

no ip igmp snooping max-groups action

参数

maxgroup —— 设定某端口能加入的最大组播组的数量，范围是 1 到 1000，默认值是 1000。

drop —— 当端口所加入到动态组播组超过了设定的 maxgroup，端口将不会加入到任何新的组播组中。

replace ——当端口所加入到动态组播组超过了设定的 maxgroup，新加入的组播组条目会选择组播组 IP 最小的旧组播条目进行替换。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设定端口 1/0/2-5 最多能加入到动态组播组数量为 10 个，若达到 10 个后有新的组播组加入，新加入的组播组条目会选择组播组 IP 最小的旧组播条目进行替换：

SW-5024(config)#interface range gigabitEthernet 1/0/2-5

SW-5024(config-if-range)#ip igmp snooping max-groups 10 **SW-5024(config-if-range)#ip igmp snooping max-groups action** replace

37.18 ip igmp snooping authentication

描述

该命令用于配置对想要加入组播组的用户进行认证。它的 no 命令用于关闭组播认证。

命令

ip igmp snooping authentication

no ip igmp snooping authentication

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

说明

只有在 AAA 功能已经开启并且配置了 RADIUS 服务器的情况下，IGMP 认证才会生效。对于 AAA 和 RADIUS 服务器的配置，请参考 aaa enable 和 radius-server 命令。

示例

在端口 3 上开启 IGMP 认证：

SW-5024(config)# interface gigabitEthernet 1/0/3 **SW-5024(config-if)# ip igmp snooping authentication**

37.19 ip igmp snooping accounting

描述

该命令用于全局开启 IGMP 计费功能。它的 no 命令用于关闭 IGMP 计费。

命令

ip igmp snooping accounting

no ip igmp snooping accounting

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局开启 IGMP 计费功能：

```
SW-5024(config)# ip igmp snooping accounting
```

37.20 ip igmp profile

描述

该命令用于创建 IGMP profile 文件，它的 no 命令用于删除指定的 profile 文件。

命令

ip igmp profile *id*

no ip igmp profile *id*

参数

id —— 指定 profile 文件的 ID，范围为 1-999。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建 profile 1：

```
SW-5024(config)# ip igmp profile 1
```

37.21 deny

描述

该命令用于配置 profile 的过滤模式为 deny。

命令

deny

模式

Profile 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 profile 1 的过滤模式为 deny：

```
SW-5024(config)# ip igmp profile 1
SW-5024(config-igmp-profile)#deny
```

37.22 permit

描述

该命令用于配置 profile 的过滤模式为 permit。

参数

permit

模式

Profile 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 profile 1 的过滤模式为 permit：

```
SW-5024(config)# ip igmp profile 1
SW-5024(config-igmp-profile)#permit
```

37.23 range

描述

该命令用于配置 IGMP profile 的过滤组播地址的范围，它的 no 命令用于删除指定的组播地址。一个 profile 最多可以包含 16 个 IP 地址范围条目。

命令

range *start-ip end-ip*

no range *start-ip end-ip*

参数

start-ip —— 起始过滤组播 IP 地址。

end-ip —— 结束过滤组播 IP 地址。

模式

Profile 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 profile 1 中一条过滤组播地址的范围为 225.1.1.1 到 226.3.2.1：

SW-5024(config)# ip igmp profile 1 **SW-5024(config-igmp-profile)#range** 225.1.1.1 226.3.2.1

37.24 ip igmp filter

描述

该命令用于绑定一个 profile 到指定的以太网端口，它的 no 命令用于删除指定的 profile-端口绑定条目。

命令

ip igmp filter *profile-id*

no ip igmp filter

参数

profile-id —— 需要绑定的 profile ID。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

绑定 profile 1 到交换机的端口 1/0/2：

```
SW-5024(config)# interface gigabitEthernet 1/0/2

SW-5024(config-if)# ip igmp filter 1
```

37.25 clear ip igmp snooping statistics

描述

该命令用于清除 IGMP 侦听的报文统计信息。

命令

clear ip igmp snooping statistics

模式

特权模式和所有配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

清除 IGMP 报文统计信息：

```
SW-5024(config)# clear ip igmp snooping statistics
```

37.26 show ip igmp snooping

描述

该命令用于显示 IGMP 全局配置信息。

参数

show ip igmp snooping

模式

特权模式和所有配置模式

特权要求

无

示例

显示 IGMP 全局配置信息：

```
SW-5024# show ip igmp snooping
```

37.27 show ip igmp snooping interface

描述

该命令用于显示 IGMP 端口配置信息。

命令

show ip igmp snooping interface [**gigabitEthernet** [*port* | *port-list*]] { basic-config | max-groups | packet-stat }

show ip igmp snooping interface [**port-channel** [*port-channel-id*]] { basic-config | max-groups }

参数

port / *port-list* —— 要显示配置信息的端口号/端口列表。

basic-config | max-groups | packet-stat —— 选择要显示的相关配置信息。

port-channel-id —— 要显示配置信息的 LAG 号/LAG 列表。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口和 LAG 的 IGMP 基本配置信息：

SW-5024# show ip igmp snooping interface basic-config

显示端口 2 的 IGMP 基本配置信息：

SW-5024# show ip igmp snooping interface gigabitEthernet 1/0/2 basic-config

显示端口 1-4 的 IGMP 报文统计信息：

SW-5024# show ip igmp snooping interface gigabitEthernet 1/0/1-4 packet-stat

37.28 show ip igmp snooping vlan

描述

该命令用于显示 IGMP VLAN 配置信息。

命令

show ip igmp snooping vlan [*vlan-id*]

参数

vlan-id —— 要显示 VLAN 号。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN 2 的 IGMP Snooping 配置信息：

```
SW-5024# show ip igmp snooping vlan 2
```

37.29 show ip igmp snooping multi-vlan

描述

该命令用于显示组播 VLAN 配置信息。

命令

show ip igmp snooping multi-vlan

模式

特权模式和所有配置模式

特权要求

无

示例

显示组播 VLAN 配置信息：

```
SW-5024# show ip igmp snooping multi-vlan
```

37.30 show ip igmp snooping groups

描述

该命令用于显示所有组播组信息。可以在后面添加扩展参数以显示指定 VLAN 的动态组播和静态组播配置信息。

参数

show ip igmp snooping groups [**vlan** { *vlan-id* }] [*multicast_addr* | count | dynamic | dynamic count | static | static count]

命令

vlan-id —— 需要显示组播信息的 VLAN 号。

multicast_addr—— 需要显示组播地址

count —— 显示所有组播组的数目。

dynamic —— 查看所有的动态组播组信息。

dynamic count —— 显示动态组播组的数目。

static —— 查看所有的静态组播组信息。

static count —— 显示静态组播组的数目。

模式

特权模式和所有配置模式

特权要求

无

示例

显示组播组信息列表：

SW-5024# show ip igmp snooping groups

显示 VLAN 5 的所有组播组条目：

SW-5024(config)# show ip igmp snooping groups vlan

5 显示 VLAN 5 中的组播组条目个数：

SW-5024(config)# show ip igmp snooping groups vlan 5 count

显示动态组播组信息列表：

SW-5024(config)# show ip igmp snooping groups vlan 5 dynamic

显示静态组播组信息列表：

SW-5024(config)# show ip igmp snooping groups vlan 5

static 显示 VLAN 5 中的动 态组播组条目个数：

SW-5024(config)# show ip igmp snooping groups vlan 5 dynamic

count 显示 VLAN 5 中的静态组播组条目个数：

SW-5024(config)# show ip igmp snooping groups vlan 5 static count

37.31 show ip igmp snooping querier

描述

该命令用于显示 VLAN 中 IGMP 侦听查询器的信息。

命令

show ip igmp snooping querier [**vlan** *vlan-id*]

参数

vlan-id —— 要显示查询器信息的 VLAN ID，取值范围 1-4094。若不指定，则显示所有 VLAN 中的查询器配置。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 IGMP 侦听查询器的信息：

```
SW-5024(config)# show ip igmp snooping querier
```

37.32 show ip igmp profile

描述

该命令用于显示 profile 的配置信息。

命令

show ip igmp profile [*id*]

参数

id —— 指定需要显示的配置信息的 profile ID，范围 1-999。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有 profile 的配置信息：

```
SW-5024(config)# show ip igmp profile
```

第 38 章 MLD 侦听配置命令

MLD Snooping（Multicast Listener Discover Snooping，MLD 侦听）是运行在交换机上的 IPv6 组播约束机制，用于管理和控制组播组。启用 MLD 侦听功能可以有效地避免组播数据在网络中广播。

38.1 ipv6 mld snooping(global)

描述

该命令用于开启 MLD 侦听全局配置，它的 no 命令用于禁用该功能。

命令

ipv6 mld snooping
no ipv6 mld snooping

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

开启 MLD 侦听全局配置：

```
SW-5024(config)# ipv6 mld snooping
```

38.2 ipv6 mld snooping(interface)

描述

该命令用于为指定端口配置 MLD 侦听功能，它的 no 命令用于禁用该功能。

参数

ipv6 mld snooping
no ipv6 mld snooping

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

开启端口 2 的 MLD 侦听功能：

SW-5024(config)# interface gigabitEthernet 1/0/2

SW-5024(config-if)# ipv6 mld snooping

38.3 ipv6 mld snooping rtime

描述

该命令用于设置 MLD 侦听全局路由器端口老化时间，它的 no 命令用于恢复默认值。默认的老化时间是 300 秒。

命令

ipv6 mld snooping rtime *rtime*

no ipv6 mld snooping rtime

参数

rtime —— 指定的老化时间秒数，取值范围 60-600 秒。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置 MLD 侦听全局路由器端口老化时间为 100 秒：

SW-5024(config)# ipv6 mld snooping rtime 100

38.4 ipv6 mld snooping mtime

描述

该命令用于 MLD 侦听成员端口时间，它的 no 命令用于恢复默认值。默认的老化时间是 260 秒。.

命令

ipv6 mld snooping mtime *mtime*

no ipv6 mld snooping mtime

参数

mtime —— 指定的老化时间秒数，取值范围 60-600 秒。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置 MLD 侦听全局成员端口时间为 100 秒：

```
SW-5024(config)# ipv6 mld snooping mtime 100
```

38.5 ipv6 mld snooping report-suppression

描述

该命令用于 MLD Report 报文抑制。启用时，对于每个组播组，只有第一个 MLD 报告消息转发到 3 层设备，随后接收到相同组播组的 MLD 报告报文将被丢弃。它的 no 命令用于禁用该功能，默认处于关闭状态。

命令

ipv6 mld snooping report-suppression
no ipv6 mld snooping report-suppression

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

开启 MLD Report 报文抑制：

```
SW-5024(config)# ipv6 mld snooping report-suppression
```

38.6 ipv6 mld snooping immediate-leave

描述

该命令用于配置端口的快速离开功能，它的 no 命令用于禁用该功能。

命令

ipv6 mld snooping immediate-leave

no ipv6 mld snooping immediate-leave

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

开启端口 3 的快速离开功能：

```
SW-5024(config)# interface gigabitEthernet 1/0/3 SW-
5024(config-if)# ipv6 mld snooping immediate-leave
```

38.7 ipv6 mld snooping drop-unknown

描述

该命令用于开启未知组播报文丢弃功能，它的 no 命令用于禁用该功能。

命令

ipv6 mld snooping drop-unknown
no ipv6 mld snooping drop-unknown

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

开启未知组播报文丢弃功能：

```
SW-5024(config)# ipv6 mld snooping drop-unknown
```

38.8 ipv6 mld snooping last-listener query-inteval

描述

该命令用于指定发送特定组查询报文的间隔时间，它的 no 命令用于恢复默认值。默认的间隔是 1 秒。

命令

ipv6 mld snooping last-listener query-inteval *interval*
no ipv6 mld snooping last-listener query-inteval

参数

interval —— 指定发送特定组查询报文的间隔秒数，从 1 到 5。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置发送特定组查询报文的间隔时间为 3s：

SW-5024(config)# ipv6 mld snooping last-listener query-inteval 3

38.9 ipv6 mld snooping last-listener query-count

描述

该命令用于指定发送特定组查询报文的次数，它的 no 命令用于恢复默认值。默认的次数是 2 次。

命令

ipv6 mld snooping last-listener query-count *num*

no ipv6 mld snooping last-listener query-count

参数

num —— 指定发送特定组查询报文的次数，从 1 到 5。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置发送特定组查询报文的次数为 3：

SW-5024(config)# ipv6 mld snooping last-listener query-count 3

38.10 ipv6 mld snooping vlan-config

描述

该命令用于启用指定 VLAN 的 MLD 侦听功能，并修改其 MLD 参数以及创建静态组播地址条目。它的 no 命令用于禁用指定 VLAN 的 MLD 侦听功能。MLD 侦听

所建立的组播组是基于 VLAN 广播域的，不同的 VLAN 可以设置不同的 MLD 参数，本命令用于配置每个 VLAN 的 MLD 侦听参数。

命令

ipv6 mld snooping vlan-config *vlan-id-list* [**rtime** *router-time* | **mtime** *member-time* | **rport interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }]

ipv6 mld snooping vlan-config *vlan-id-list* **static** *ip* **interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }

no ipv6 mld snooping vlan-config *vlan-id-list* [**rtime** *router-time* | **mtime** *member-time* | **rport interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }]

no ipv6 mld snooping vlan-config *vlan-id-list* **static** *ip* **interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }

参数

vlan-id-list —— 需要修改 MLD 参数的 VLAN ID 列表，取值范围 1~4094，格式为 1-3，5。

router-time —— 路由器端口时间。在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。取值范围 60~600（秒），默认值为 0 且会使用全局路由老化时间。

member-time —— 成员端口时间。在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。取值范围 60~600（秒），默认值为 0 且会使用全局成员老化时间。

port-list —— 成员端口列表。

port-channel-id —— LAG 号。

ip —— 静态组播 IPv6 地址。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

启用 VLAN 1-3 的 MLD 侦听功能，将它们的路由器端口时间设置为 300 秒、成员端口时间设置为 200 秒：

SW-5024(config)# ipv6 mld snooping vlan-config 1-3 **rtime** 300

SW-5024(config)# ipv6 mld snooping vlan-config 1-3 **mtime** 200

在 VLAN 2 中添加静态组播地址条目，组播 IP 为 225.0.0.1，转发端口为端口 1-3：

SW-5024(config)# ipv6 mld snooping vlan-config 2 **static**

ff01::1234:01 **interface gigabitEthernet** 1/0/1-3

38.11 ip mld snooping vlan-config (router-port-forbidden)

描述

该命令用于禁止在指定 VLAN 中的指定端口成为路由端口。它的 no 命令用于删除被禁用的路由端口。

命令

ipv6 mld snooping vlan-config *vlan-id-list* **router-port-forbidd interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }

no ipv6 mld snooping vlan-config *vlan-id-list* **router-port-forbidd interface** [**gigabitEthernet** *port-list* | **port-channel** *port-channel-id*]

参数

vlan-id-list —— 需要修改 MLD 参数的 VLAN ID 列表，取值范围 1~4094，格式为 1-3，5。

port-list —— 禁止成为路由端口的端口列表。该端口将丢弃收到的组播组报文。

port-channel-id ——禁止成为路由端口的 LAG。该 LAG 将丢弃收到的组播组报文。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

禁止 VLAN 1 中的端口 1-3 成为路由端口：

SW-5024(config)# ipv6 mld snooping vlan-config 1 **router-port-**

forbidd interface gigabitEthernet 1/0/1-3

38.12 ipv6 mld snooping multi-vlan-config

描述

该命令用于创建组播 VLAN，它的 no 命令用于删除相应的组播 VLAN。

命令

ipv6 mld snooping multi-vlan-config [*vlan-id*] [**rtime** *router-time* | **mtime** *member-time* | **rport interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }]

no ipv6 mld snooping multi-vlan-config [**rtime** *router-time* | **mtime** *member-time* | **rport interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }]

参数

vlan-id —— 需要修改配置的 VLAN ID，取值范围 2~4094。

router-time —— 路由器端口时间。在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。取值范围 60~600（秒），默认值为 0 且将使用全局路由端口时间。

member-time —— 成员端口时间。在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。取值范围 60~600（秒），默认值为 0 且将使用全局成员端口时间。

port-list —— 成员端口列表。

port-channel-id —— LAG 号。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

开启组播 VLAN 功能，并设置 VLAN 3 的路由器端口时间为 100 秒、成员端口时间为 100 秒，静态路由端口为端口 1/0/3：

SW-5024(config)# ipv6 mld snooping multi-vlan-config 3 **rtime** 100 **SW-5024(config)# ipv6 mld snooping multi-vlan-config** 3 **mtime** 100 **SW-5024(config)# ipv6 mld snooping multi-vlan-config** 3 **rport interface gigabitEthernet** 1/0/3

38.13 ipv6 mld snooping multi-vlan-config (router-port-forbidden)

描述

该命令用于禁止在指定组播 VLAN 中的指定端口成为路由端口。它的 no 命令用于删除被禁用的路由端口。

命令

ipv6 mld snooping multi-vlan-config [*vlan-id*] **router-port-forbidd interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }

no ipv6 mld snooping multi-vlan-config router-port-forbidd [**interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-id* }]

参数

vlan-id —— 组播 VLAN ID。

port-list —— 禁止成为路由端口的端口列表。该端口将丢弃收到的组播组报文。

port-channel-id ——禁止成为路由端口的 LAG。该 LAG 将丢弃收到的组播组报文。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

禁止 VLAN 1 中的端口 1-3 成为路由端口：

```
SW-5024(config)# ipv6 mld snooping multi-vlan-config
1 router-port-forbidd interface gigabitEthernet 1/0/1-3
```

38.14 ipv6 mld snooping multi-vlan-config (source-ip-replace)

描述

该命令用于替换指定组播 VLAN 中 MLD 报文的源 IP 地址。它的 no 命令用于禁止替换源 IP 地址。

命令

ipv6 mld snooping multi-vlan-config [*vlan-id*] **replace-sourceip** *ip*

no ipv6 mld snooping multi-vlan-config replace-sourceip

参数

vlan-id —— 组播 VLAN ID。

ip —— 指定替换的 IPv6 地址。该 IP 地址将替换掉 MLD 报文中的源 IPv6 地址。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

将组播 VLAN 1 中的 MLD 报文的源 IP 地址替换为 fe80::02ff:ffff:fe00:0001：

```
SW-5024(config)# ipv6 mld snooping multi-vlan-config 1 replace-
sourceip fe80::02ff:ffff:fe00:0001
```

38.15 ipv6 mld snooping querier vlan

描述

该命令用于在指定 VLAN 中使能 MLD 侦听查询器功能，它的 no 命令用于禁用指定 VLAN 中的 MLD 侦听查询器功能。

命令

ipv6 mld snooping querier vlan *vlan-id*

no ipv6 mld snooping querier vlan *vlan-id*

参数

vlan-id —— VLAN ID，范围为 1-4094。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

在 VLAN1 中使能 MLD 侦听查询器功能：

```
SW-5024(config)# ipv6 mld snooping querier vlan 2
```

38.16 ipv6 mld snooping querier vlan (general query)

描述

该命令用于配置 MLD 侦听查询器的通用查询参数，它的 no 命令用于恢复默认配置。

命令

ipv6 mld snooping querier vlan *vlan-id* { **query-interval** *interval* | **max-response-time** *response-time* | **general-query source-ip** *ip-addr* }

no ipv6 mld snooping querier vlan *vlan-id* { **query-interval** | **max-response-time** | **general-query source-ip** }

参数

vlan-id —— VLAN ID，范围为 1-4094。

interval —— 发送通用查询报文的时间间隔，取值范围从 10-300 秒，默认值为 60 秒。

response-time —— 指定客户收到通用查询报文后的最大响应时间，取值范围 1 到 25 秒，默认值为 10 秒。

ip-addr —— MLD 侦听查询器所发送的通用查询报文的源 IP，不能为组播或广播地址。默认值为 192.18.0.1。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

在 VLAN 2 中使能 MLD 侦听查询器的通用查询报文的发送间隔为 200 秒，最大响应时间为 20 秒：

SW-5024(config)#ipv6 mld snooping querier vlan 2 **query-interval** 200

SW-5024(config)#ipv6 mld snooping querier vlan 2 **max-response-time** 20

38.17 ipv6 mld snooping max-groups

描述

用于配置一个端口最多能够加入到组播组数量； **ipv6 mld snooping max-groups action** 用于配置当一个端口所加入到组播组数量达到限定值时，对收到的新 MLD 报告报文的处理动作。**no ipv6 mld snooping max-groups** 用于

清除指定端口的最大组播组限制，恢复其默认的无限制状态；**no ipv6 mld snooping max-groups action** 用于恢复端口所加入到组播组达到上限时，对 MLD 报文的默认操作，即丢弃操作。这些命令只对动态组播组有效。.

命令

ipv6 mld snooping max-groups [*maxgroup*]

ipv6 mld snooping max-groups action { drop | replace }

no ipv6 mld snooping max-groups

no ipv6 mld snooping max-groups action

参数

maxgroup —— 设定某端口能加入的最大组播组的数量，范围是 1 到 1000，默认值是 1000。

drop —— 当端口所加入到动态组播组超过了设定的 maxgroup，端口将不会加入到任何新的组播组中。

replace ——当端口所加入到动态组播组超过了设定的 maxgroup，新加入的组播组条目会选择组播组 IP 最小的旧组播条目进行替换。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设定端口 1/0/2-5 最多能加入到动态组播组数量为 10 个，若达到 10 个后有新的组播组加入，新加入的组播组条目会选择组播组 IP 最小的旧组播条目进行替换：

```
SW-5024(config)#interface range gigabitEthernet 1/0/2-5
SW-5024(config-if-range)#ipv6 mld snooping max-groups 10
SW-5024(config-if-range)#ipv6 mld snooping max-groups action replace
```

38.18 ipv6 mld profile

描述

该命令用于创建 MLD profile 文件，它的 no 命令用于删除指定的 profile 文件。

命令

ipv6 mld profile *id*

no ipv6 mld profile *id*

参数

id —— 指定 profile 文件的 ID，范围为 1-999。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

创建 profile 1：

```
SW-5024(config)# ipv6 mld profile 1
```

38.19 deny

描述

该命令用于配置 profile 的过滤模式为 deny。

命令

deny

模式

Profile 配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

配置 profile 1 的过滤模式为 deny：

```
SW-5024(config)# ipv6 mld profile 1
SW-5024(config-igmp-profile)#deny
```

38.20 permit

描述

该命令用于配置 profile 的过滤模式为 permit。

命令

permit

模式

Profile 配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

配置 profile 1 的过滤模式为 permit：

```
SW-5024(config)# ipv6 mld profile 1
SW-5024(config-igmp-profile)#permit
```

38.21 range

描述

该命令用于配置 MLD profile 的过滤组播地址的范围，它的 no 命令用于删除指定的组播地址。

命令

range *start-ip end-ip*

no range *start-ip end-ip*

参数

start-ip —— 起始组播 IP 地址。

end-ip —— 结束组播 IP 地址。

模式

Profile 配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

配置 profile 1 中一条过滤组播地址的范围为 225.1.1.1 到 226.3.2.1：

```
SW-5024(config)# ipv6 mld profile 1 SW-5024(config-
igmp-profile)#range ff80::1234 ff80::1235
```

38.22 ipv6 mld filter

描述

该命令用于绑定一个 profile 到指定的以太网端口，它的 no 命令用于删除指定的 profile-端口绑定条目。

命令

ipv6 mld filter *profile-id*

no ipv6 mld filter

参数

profile-id —— 需要绑定的 profile ID。

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

绑定 profile 1 到交换机的端口 1/0/1：

```
SW-5024(config)# interface gigabitEthernet 1/0/2

SW-5024(config-if)# ipv6 mld filter 1
```

38.23 clear ipv6 mld snooping statistics

描述

该命令用于清除 MLD 侦听的报文统计信息。

命令

clear ipv6 mld snooping statistics

模式

特权模式和所有配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

清除 MLD 报文统计信息：

```
SW-5024(config)# clear ipv6 mld snooping statistics
```

38.24 show ipv6 mld snooping

描述

该命令用于显示 MLD 全局配置信息。

命令

show ipv6 mld snooping

模式

特权模式和所有配置模式

特权要求

无

示例

显示 MLD 全局配置信息：

```
SW-5024(config)# show ipv6 mld snooping
```

38.25 show ipv6 mld snooping interface

描述

该命令用于显示 MLD 端口配置信息。

命令

show ipv6 mld snooping interface [**gigabitEthernet** [*port* | *port-list*]]
{ basic-config | max-groups | packet-stat }
show ipv6 mld snooping interface [**port-channel** [*port-channel-id*]]
{ basic-config | max-groups }

参数

port-list —— 要显示配置信息的端口号/端口列表。

basic-config | packet-stat | max-groups —— 选择要显示的相关配置信息。

lag-list —— 要显示配置信息的 LAG 号/LAG 列表。

模式

特权模式和所有配置模式

特权要求

无

示例

显示端口 2 的 MLD 基本配置信息：

SW-5024# show ipv6 mld snooping interface gigabitEthernet 1/0/2

basic-config

显示端口 1-4 的 MLD 报文统计信息：

SW-5024# show ipv6 mld snooping interface gigabitEthernet 1/0/1-4

packet-stat

38.26 show ipv6 mld snooping vlan

描述

该命令用于显示 MLD VLAN 配置信息。

命令

show ipv6 mld snooping vlan [*vlan-id*]

参数

vlan-id —— The VLAN ID selected to display, ranging from 1 to 4094.

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN 2 的 MLD Snooping 配置信息：

SW-5024(config)# show ipv6 mld snooping vlan

38.27 show ipv6 mld snooping multi-vlan

描述

The **show ipv6 mld snooping multi-vlan** command is used to display the Multicast VLAN configuration.

命令

show ipv6 mld snooping multi-vlan

模式

特权模式和所有配置模式

特权要求

无

示例

显示组播 VLAN 配置信息：

```
SW-5024# show ipv6 mld snooping multi-vlan
```

38.28 show ipv6 mld snooping groups

描述

该命令用于显示所有组播组信息。可以在后面添加扩展参数以显示指定 VLAN 的动态组播和静态组播配置信息。

命令

show ipv6 mld snooping groups [**vlan** { *vlan-id* }] [*ipv6_multicast_addr* | count | dynamic | dynamic count | static | static count]

参数

vlan-id —— 需要显示组播信息的 VLAN 号。

ipv6_multicast_addr —— 组播组的 IPv6 地址。

count —— 显示所有组播组的数目。

dynamic —— 查看所有的动态组播组信息。

dynamic count —— 显示动态组播组的数目。

static —— 查看所有的静态组播组信息。

static count —— 显示静态组播组的数目。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有组播组信息列表：

```
SW-5024(config)# show ipv6 mld snooping groups
```

38.29 show ipv6 mld snooping querier

描述

该命令用于显示 VLAN 中 MLD 侦听查询器的信息。

命令

show ipv6 mld snooping querier [**vlan** *vlan-id*]

参数

vlan-id —— 要显示查询器信息的 VLAN ID，取值范围 1-4094。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN2 中 MLD 侦听查询器的信息：

SW-5024(config)# show ipv6 mld snooping querier

38.30 show ipv6 mld profile

描述

该命令用于显示 profile 的配置信息。

命令

show ipv6 mld profile [*id*]

参数

id —— 指定需要显示的配置信息的 profile ID。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有 profile 的配置信息：

SW-5024(config)# show ipv6 mld profile

第 39 章 SNMP 配置命令

SNMP（Simple Network Management Protocol，简单网络管理协议）功能用于管理网络设备，实现与众多产品的无障碍连接，以便于网络管理员对网络节点的监控和操作。

39.1 snmp-server

描述

该命令用于启用 SNMP 功能，它的 no 命令用于禁用 SNMP 功能。SNMP 功能默认是被禁用的。

命令

snmp-server

no snmp-server

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

开启 SNMP 功能：

```
SW-5024(config)# snmp-server
```

39.2 snmp-server view

描述

该命令用于添加视图，它的 no 命令用于删除对应视图。在 SNMP 报文中使用管理变量（OID）来描述交换机中的管理对象，MIB（Management Information Base，管理信息库）是所监控网络设备的管理变量的集合。视图用来控制管理变量是如何被管理的。

命令

snmp-server view *name mib-oid* { include | exclude }

no snmp-server view *name mib-oid*

参数

name —— 要添加的视图条目的名称，可输入 1~16 个字符。一个视图可以有多个同名的视图条目。

mib-oid —— MIB 子树 OID，即该视图条目的管理变量（OID）。可输入 1~61 个字符。

include | exclude —— 视图类型，有包括（include）和排除（exclude）两个选项。选择包括时，该 OID 可以被管理软件管理；选择排除时，该 OID 不能被管理软件管理。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

添加视图 view1，并设置其 OID 为 1.3.6.1.6.3.20，该 OID 可以被管理软件管理：

SW-5024(config)# snmp-server view view1 1.3.6.1.6.3.20 include

39.3 snmp-server group

描述

该命令用于添加组管理配置，它的 no 命令用于删除对应的组。SNMP v3 提供了 VACM（View-based Access Control Model，基于视图的访问控制模型）及 USM（User-based Security Model，基于用户的安全模型）的认证机制。组内的用户通过读、写、通知视图来达到访问控制的目的。同时通过有无认证和有无加密等功能组合，为管理软件和被管理设备之间的通信提供更高的安全性。

命令

snmp-server group *name* [**smode** { v1 | v2c | v3 }] [**slev** { noAuthNoPriv | authNoPriv | authPriv }] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*]

no snmp-server group *name* **smode** { v1 | v2c | v3 } **slev** { noAuthNoPriv | authNoPriv | authPriv }

参数

name —— 要添加的组名，可输入 1~16 个字符。组名与“安全模式”和“安全级别”共同组成该组的标识，三项均相同才被认为是同一组。

smode —— 安全模式，有 v1、v2c 和 v3 三个选项，分别表示 SNMP v1、SNMP v2c 和 SNMP v3。

slev —— SNMP v3 的组安全级别，有 noAuthNoPriv（不认证不加密）、authNoPriv

（认证不加密）和 authPriv（认证加密）三个选项，缺省时为 noAuthNoPriv。SNMP v1 和 SNMP v2c 安全模式下不需设置此项。

read-view —— 关联的只读视图名称。只读视图只能被查看不能被编辑。

write-view —— 关联的只写视图名称。只写视图只能被编辑不能被查看。若要对某视图进行读写操作，则需同时将该视图添加为只读视图和只写视图。

notify-view —— 关联的通知视图名称。管理软件可以接收到通知视图发送的异常报警信息。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

添加组 group1，并设置其安全模式为 SNMP v3，组安全级别为 authNoPriv，组内的用户可对视图 viewDefault 进行读写操作，管理软件可以接收到视图 viewDefault 发送的异常报警信息：

SW-5024(config)# snmp-server group group1 **smode** v3 **slev** authNoPriv **read** viewDefault **write** viewDefault **notify** viewDefault 删除组 group1：

SW-5024(config)# no snmp-server group group1 **smode** v3 **slev** authNoPriv

39.4 snmp-server user

描述

该命令用于添加用户，它的 no 命令用于删除对应的用户。管理软件可以通过用户的方式对交换机进行管理。用户建立在组之下，与其所属的组具有相同的安全级别和访问控制特权要求。

命令

snmp-server user *name* { local | remote } *group-name* [**smode** { v1 | v2c | v3 }] [**slev** { noAuthNoPriv | authNoPriv | authPriv }] [**cmode** { none | MD5 | SHA }] [**cpwd** *confirm-pwd*] [**emode** { none | DES }] [**epwd** *encrypt-pwd*]

no snmp-server user *name*

参数

name —— 要添加的用户名，可输入 1~16 个字符。

local | remote —— 用户类型，分本地（local）和远程（remote）两种。本地用户即建立在本地引擎下的用户，远程用户即建立在远程引擎下的用户。

group-name —— 关联的组名。通过“组名”、“安全模式”和“安全级别”来确定用户所属的组。

smode —— 安全模式，有 v1、v2c 和 v3 三个选项，缺省时为 v1。用户的安全模式
必须和其所属组的安全模式相同。

slev —— SNMP v3 的组安全级别，有 noAuthNoPriv（不认证不加密）、authNoPriv（认证不加密）和 authPriv（认证加密）三个选项，缺省时为 noAuthNoPriv。用户的安全级别必须和其所属组的安全级别相同。

cmode —— SNMP v3 用户的认证模式，有 none、MD5 和 SHA 三个选项。其中 none 表示不认证；MD5 为信息摘要算法；SHA 为安全散列算法，比 MD5 的安全性更高。缺省时为 none。

confirm-pwd —— 认证密码，可输入 1~16 个字符，不允许输入问号和空格。此密码在配置文件中将以对称加密的形式显示。

emode —— SNMP v3 用户的加密模式，有 none 和 DES 两个选项。其中 none 表示不加密，DES 为数据加密标准。缺省时为 none。

encrypt-pwd —— 加密密码，可输入 1~16 个字符，不允许输入问号和空格。此密码在配置文件中将以对称加密的形式显示。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

将本地用户 admin 添加到组 group2，输入组的安全模式 v3、安全级别 authPriv，并设置用户的认证模式为 MD5、认证密码为 11111、加密模式为 DES、加密密码为 22222：

SW-5024(config)# snmp-server user admin local group2 **smode** v3 **slev**

authPriv **cmode** MD5 **cpwd** 11111 **emode** DES **epwd** 22222

39.5 snmp-server community

描述

该命令用于添加团体，它的 no 命令用于删除对应的团体。SNMP v1 和 SNMP v2c 采用团体名（Community Name）认证，团体名起到了类似于密码的作用。

命令

snmp-server community *name* { read-only | read-write } *mib-*

view **no snmp-server community** *name*

参数

name —— 要添加的团体名称，可输入 1~16 个字符。

read-only | read-write —— 团体对相应视图的特权要求，有 read-only（只读）和 read-write（读写）两个选项。

mib-view —— MIB 视图，即团体可访问的视图。默认为 viewDefault。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

添加团体 public，此团体对视图 viewDefault 具有读写特权要求：

SW-5024(config)# snmp-server community public read-write viewDefault

39.6 snmp-server host

描述

该命令用于添加通知管理条目，它的 no 命令用于删除对应条目。通知管理功能是交换机主动向管理软件报告某些视图的重要事件，便于管理软件对交换机的某些事件进行及时监控和处理。

命令

snmp-server host *ip udp-port user-name* [**smode** { v1 | v2c | v3 }] [**slev**

{ noAuthNoPriv | authNoPriv | authPriv }] [**type** { trap | inform }] [**retries** *retries*]

[**timeout** *timeout*]

no snmp-server host *ip user-name*

参数

ip —— 管理主机的 IP 地址。

udp-port —— UDP 端口号，即管理主机上开启供通知过程使用的 UDP 端口号，与 IP 地址共同作用。取值范围为 1~65535，默认值为 162。

user-name —— 配置管理软件的团体名/用户名。

smode —— 用户的安全模式，有 v1、v2c 和 v3 三个选项。缺省时为 v1。

slev —— SNMP v3 的组安全级别，有 noAuthNoPriv（不认证不加密）、authNoPriv（认证不加密）和 authPriv（认证加密）三个选项，缺省时为 noAuthNoPriv。

type —— 通知报文的类型，有 trap 和 inform 两个选项，缺省时为 trap。选择 trap 时，以 Trap 方式发送通知；选择 inform 时，以 Inform 方式发送通知。Inform 具有更高的可靠性，并且需要设置重传次数（retries）和超时时间（timeout）。v1 安全模式下只能选择 Trap 方式。

retries —— Inform 报文的重传次数，取值范围 1~255。交换机发送 Inform 报文后，若经过超时时间仍没有收到 Inform 回应报文，则会重发 Inform 报文。超过重传次数后，将不再重发 Inform 报文。

timeout —— 超时时间，即交换机等待 Inform 回应报文的时间。超过该时间后，将重新发送 Inform 报文。取值范围为 1~3600（秒）。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

添加通知管理条目，其中管理主机的 IP 地址为 192.168.0.146，其 UDP 端口号为 162，管理软件的用户名为 admin，用户安全模式为 v2c，通知报文以 Inform 的方式发送，Inform 报文的超时时间为 1000 秒，重传次数 100 次：

```
SW-5024(config)# snmp-server host 192.168.0.146 162 admin smode
v2c type inform retries 100 timeout 1000
```

添加通知管理条目，其中管理主机的 IP 地址为 fe80::1234，其 UDP 端口号为 162，管理软件的用户名为 admin，用户安全模式为 v2c，通知报文以 Inform 的方式发送，Inform 报文的超时时间为 1000 秒，重传次数 100 次：

```
SW-5024(config)# snmp-server host fe80::1234 admin smode v2c type
inform retries 100 timeout 1000
```

39.7 snmp-server engineID

描述

该命令用于配置交换机本地和远程的引擎 ID，它的 no 命令用于恢复默认的配置。

命令

snmp-server engineID { [**local** *local-engineID*] [**remote** *remote-engineID*] }

no snmp-server engineID

参数

local-engineID —— 本地引擎 ID，即本地 SNMP 实体的引擎 ID。本地用户建立在本地引擎之下。可输入 10~64 个十六进制字符，且字符的个数必须为偶数。

remote-engineID —— 远程引擎 ID，即 SNMP 管理端的引擎 ID。远程用户建立在远程引擎之下。可输入 10~64 个十六进制字符，且字符个数必须是偶数。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置交换机 SNMP 的本地引擎 ID 为 1234567890，远程引擎 ID 为 abcdef123456：

SW-5024(config)# snmp-server engineID local 1234567890 **remote**

abcdef123456

39.8 snmp-server traps snmp

描述

该命令用于开启所有的标准 traps。它的 no 命令用于关闭标准 traps。SNMP 的标准 traps 共有 4 种：linkup，linkdown，warmstart 和 coldstart。

命令

snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

no snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

参数

linkup —— 当端口由断开状态转变为连接状态时，发送 linkup 类型 trap。默认开启。给端口插上连接线可触发此类型 trap。

linkdown —— 当端口由连接状态转变为断开状态时，发送 linkdown 类型 trap。默认开启。断开端口的连接线可触发此类型 trap。

warmstart —— 表示交换机的 SNMP 被重初始化，且该实体的配置没有发生改变。在交换机全局 SNMP 功能开启并设置好团体名及通知条目的情况下，先关闭再重新开启全局 SNMP 功能可触发此类型 trap。

coldstart —— 表示因交换机系统的重初始化而导致 SNMP 实体发生初始化。默认开启。重启交换机即可触发此类型 trap。

Auth-failure —— 开启因认证失败而触发的 trap..

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

开启交换机的 SNMP 标准 traps 的 linkup 功能：

```
SW-5024(config)# snmp-server traps snmp linkup
```

39.9 snmp-server traps link-status

描述

该命令用于开启指定端口的 SNMP 标准 traps 的端口连接状态监控功能。它的 no 命令用于关闭该功能。

命令

snmp-server traps link-status

no snmp-server traps link-status

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员类型的用户可以使用该命令

示例

开启端口 3 的 SNMP 标准 traps 的连接状态监控功能：

```
SW-5024(config)# interface gigabitEthernet 1/0/3

SW-5024(config-if)# snmp-server traps link-status
```

39.10 snmp-server traps

描述

该命令用于开启交换机的扩展 traps 功能。 它的 no 命令用于关闭交换机的扩展 traps 功能。

命令

snmp-server traps { bandwidth-control | cpu | flash | lldp | loopback-detection | storm-control | spanning-tree | memory }

no snmp-server traps { bandwidth-control | cpu | flash | lldp | loopback-detection | storm-control | spanning-tree | memory }

参数

bandwidth-control —— 用于监控端口的速率是否超过了设定的带宽速率。在端口的带宽控制功能开启情况下，以大于所设定速率的速率往该端口发送数据包时，系统会触发此类型 trap。

cpu —— 用于监控 cpu 的负载状况。当 cpu 使用率超过设定的最高阈值时系统会触发此类型 trap。我司交换机的 cpu 使用率最高阈值默认为 80%。

flash —— 用于监控 flash 是否被修改。当 flash 被修改时，如进行保存配置、恢复出厂设置、升级、导入配置等操作时，系统会触发此类型 trap。

lldp —— 用于 LLDP 监测。当相邻端口发生变化时，系统会触发此类型 trap。

loopback-detection —— 用于环路监测。交换机监测到环路时，或是环路被清除时，系统都会触发此类 trap。

storm-control —— 用于监控网络风暴的情况。当广播或者组播的速率达到风暴控制的设定值时，系统会触发此类型 trap。

spanning-tree —— 用于监控生成树系统的拓扑状况。以下几种情况会触发此类型 trap： a). 交换机端口从非转发态变为转发态或者从转发态变为非转发态；b). 交换机端口接收到带 TC flag 的报文或 TCN 报文。

memory —— 用于内存监控。当内存使用率超过 80%时，系统会触发此类型 trap。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

开启交换机的 SNMP 扩展 traps 的带宽监控功能：

SW-5024(config)# snmp-server traps bandwidth-control

39.11 snmp-server traps vlan

描述

该命令用于统一开启交换机中与 VLAN 相关的扩展 traps 功能。它的 no 命令用于统一关闭交换机中与 VLAN 相关的扩展 traps 功能。与 VLAN 相关的 trap 有 vlan create 和 vlan delete 两种，可以在后面扩展参数以单独开启其中某一项功能。

命令

snmp-server traps vlan [create | delete]

no snmp-server traps vlan [create | delete]

参数

create —— 当新的 VLAN 被创建成功时系统会触发此类型 trap。

delete —— 当已有 VLAN 被删除成功时系统会触发此类型 trap。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

统一开启交换机中与 vlan 相关的扩展 traps 功能：

SW-5024(config)# snmp-server traps vlan

单独开启交换机 SNMP 扩展 traps 中的 vlan create 功能：

SW-5024(config)# snmp-server traps vlan create

39.12 rmon history

描述

该命令用于配置历史采样条目，它的 no 命令用于恢复默认配置。RMON（Remote Monitoring，远程网络监视）基于 SNMP 体系结构，用于监视和管理远程网络设备。历史组是 RMON 的一个组，利用 RMON 的历史采样控制功能，交换机会周期性地收集网络统计信息，从而监视网络的使用情况。

命令

rmon history *index* **interface gigabitEthernet** *port* [**interval** *seconds*]

[**owner** *owner-name*] [**buckets** *number*]

no rmon history *index*

参数

index —— 采样条目的序号，取值范围 1~12，可输入多条，格式为 1-3,5。

port —— 采样端口。

seconds —— 采样间隔，即端口采样的时间间隔，单位为秒，取值范围 10~3600，默认值为 1800。

owner-name —— 条目的创建者，可输入 1~16 个字符。缺省时为 monitor。

number —— 显示当前历史控制表项所能够保存的采样数据条目的最大数目。范围为 1-130，默认值为 50。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置条目 1-3 的采样端口为端口 2，采样间隔为 100 秒，创建者为 owner1：

```
SW-5024(config)# rmon history 1-3 interface gigabitEthernet 1/0/2
interval 100 owner owner1
```

39.13 rmon event

描述

该命令用于配置 SNMP-RMON 事件条目，它的 no 命令用于恢复默认配置。事件组是 RMON 一个组，用来定义事件及其类型，此处定义的事件主要用于在警报配置中触发报警。

命令

rmon event *index* [**user** *user-name*] [**description** *descript*] [**type** { none | log | notify | log-notify }] [**owner** *owner-name*]

no rmon event *index*

参数

index —— 条目序号，取值范围 1~12，每条命令只能输入一个条目。

user-name —— 事件所属的用户名，可输入 1~16 个字符。缺省时为 public。

descript —— 对事件的描述信息，可输入 1~16 个字符，默认为空。

type —— 事件类型，选择 none 时，不做任何操作；选择 log 时，交换机将事件记录在日志表中；选择 notify 时，交换机向管理主机发送报警信息；选择 both 时，交换机将事件记录在日志表中并向管理主机发送报警信息。

owner-name —— 条目的创建者，可输入 1~16 个字符。缺省时为 monitor。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

设置条目 1、2、3、4 的用户名为 user1，事件描述为 description1，事件类型为 log，创建者为 owner1：

SW-5024(config)# rmon event 1-4 **user** user1 **description** description1

type log **owner** owner1

39.14 rmon alarm

描述

该命令用于配置 SNMP-RMON 警报管理信息，它的 no 命令用于恢复默认配置。警报组是 RMON 的一个组，警报配置是对指定的警报变量进行监视，一旦计数器超过阈值则触发警报，报警方式将按照事件的类型进行相应的处理。

命令

rmon alarm *index* { **stats-index** *sindex* } [**alarm-variable** { revbyte | revpkt | bpkt | mpkt | crc-lign | undersize | oversize | jabber | collision | 64 | 65-127 | 128-511 | 512-1023 | 1024-10240 }] [**s-type** { absolute | delta}] [**rising-threshold** *r-hold*] [**rising-event-index** *r-event*] [**falling-threshold** *f-hold*] [**falling-event-index** *f-event*] [**a-type** {rise | fall | all}] [**owner** *owner-name*] [**interval** *interval*]

no rmon alarm *index*

参数

index —— 警报管理条目的序号，取值范围 1~12，可输入多条，格式为 1-3,5。

sindex —— 指定统计数据的序号。

port —— 端口号。

alarm-variable —— 警报变量，缺省时为 drop。

s-type —— 样例类型，即为警报变量选择取样，并将取样值与阈值进行比较的方法，有 absolute（绝对值）和 delta（增量）两个选项。选择 absolute，则在一个取样周期结束时将取样结果直接与阈值进行比较；选择 delta，则将目前值减去上一次取样值之后的增量与阈值进行比较。默认选项为 absolute。

r-hold —— 触发警报的上升阈值，取值范围 1~65535，默认值为 100。

r-event —— 上升事件，即触发上升阈值警报的事件的序号，取值范围 1~12。

f-hold —— 触发警报的下降阈值，取值范围 1~65535，默认值为 100。

f-event —— 下降事件，即触发下降阈值警报的事件的序号，取值范围 1~12。

a-type —— 警报触发的方式，有 rise（上升）、fall（下降）和 all（全部）三个选项。选择 rise，则只在触发上升阈值后触发警报；选择 fall，则只在触发下降阈值后触发警报；选择 all，则触发上升和下降阈值均触发警报。默认选项为 all。 *owner-name* —— 条目的创建者，可输入 1~16 个字符，缺省时为 monitor。 *interval* —— 时间间隔，取值范围 10~3600，单位为秒，默认值为 1800。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

设置条目 1、2、3 与数据条目 2 绑定，创建者为 owner1，时间间隔为 100 秒：

SW-5024(config)#rmon alarm 1-3 **stats-index** 2 **owner** owner1 **interval** 100

39.15 rmon statistics

描述

此命令用于配置 SNMP-RMON 统计组信息，它的 no 命令用于删除指定条目。支持的最大统计组条目数为 1000。

命令

rmon statistics *index* **interface gigabitEthernet** *port* [**owner** *owner-name*]

[**status** { underCreation | valid }]

no rmon statistics *index*

参数

index —— 统计条目的序号，取值范围 1 到 65535，格式如 1-3,5。

port —— 统计条目的端口号，格式如 1/0/1。

owner-name —— 条目创建者，最多包含 16 个字符。默认为“monitor”。

status —— 条目状态，包括“valid”和“underCreation”。“valid”是指条目创建后立即生效，“underCreation”表示条目创建后不会工作，直至被设定为生效。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置数据条目 1-3 的端口为 1/0/3，创建者 为 owner1，状态为“valid”：

```
SW-5024(config)#rmon statistics 1-3 interface gigabitEthernet 1/0/1 owner
owner1 status valid
```

39.16 show snmp-server

描述

该命令用于显示 SNMP 全局配置信息。

命令

show snmp-server

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示 SNMP 全局配置信息：

```
SW-5024# show snmp-server
```

39.17 show snmp-server view

描述

该命令用于显示视图列表。

命令

show snmp-server view

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示视图列表：

```
SW-5024# show snmp-server view
```

39.18 show snmp-server group

描述

该命令用于显示组列表。

命令

show snmp-server group

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示组列表：

```
SW-5024# show snmp-server group
```

39.19 show snmp-server user

描述

该命令用于显示用户列表。

命令

show snmp-server user

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示用户列表：

```
SW-5024# show snmp-server user
```

39.20 show snmp-server community

描述

该命令用于显示团体列表。

命令

show snmp-server community

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示团体列表：

```
SW-5024# show snmp-server community
```

39.21 show snmp-server host

描述该命令用于显示目的主机列表。

命令

show snmp-server host

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示目的主机列表：

```
SW-5024# show snmp-server host
```

39.22 show snmp-server engineID

描述

该命令用于显示 SNMP 的引擎 ID 信息。

命令

show snmp-server engineID

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示 SNMP 的引擎 ID 信息：

```
SW-5024# show snmp-server engineID
```

39.23 show rmon history

描述

该命令用于显示历史采样条目的配置信息。

命令

show rmon history [*index*]

参数

index —— 要显示配置信息的采样条目序号，取值范围 1~12，可输入多条，格式为 1-3,5。缺省时显示所有历史采样条目的配置信息。

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示所有历史采样条目的配置信息：

```
SW-5024# show rmon history
```

39.24 show rmon event

描述

该命令用于显示 SNMP-RMON 事件配置信息。

命令

show rmon event [*index*]

参数

index —— 要显示事件配置信息的条目序号，取值范围 1~12，可输入多条，格式为 1-3，5。缺省时显示所有条目的事件配置信息。

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示条目 1-4 的事件配置信息：

```
SW-5024# show rmon event 1-4
```

39.25 show rmon alarm

描述

该命令用于显示警报管理条目的配置信息。

命令

show rmon alarm [*index*]

参数

index —— 要显示配置信息的警报管理条目序号，取值范围 1~12，可输入多条，格式为 1-3，5。缺省时显示所有警报管理条目的配置信息。

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示警报管理条目 1-2 的配置信息：

SW-5024# show rmon alarm 1-2

39.26 show rmon statistics

描述

该命令用于显示统计组条目的配置信息。

命令

show rmon statistics [*index*]

参数

index —— 要显示配置信息的统计组条目序号，取值范围 1~65535，可输入多条，格式为 1-3，5。缺省时显示所有统计组条目的配置信息。

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示统计组条目 1 的配置信息：

SW-5024#show rmon statistics 1

第 40 章 LLDP 配置命令

链路层发现协议 LLDP（Link Layer Discovery Protocol）允许网络设备周期性的向处于同一局域网的邻居设备通告自己的设备信息。邻居设备收到信息后将其以标准的 MIB（Management Information Base，管理信息库）形式保存起来，使得网络管理系统可以通过管理协议 SNMP（Simple Network Management Protocol，简单网络管理协议）获取到这些信息。

40.1 lldp

描述

该命令用于全局开启 LLDP 功能，它的 no 命令用于禁用 LLDP 功能。

命令

lldp

no lldp

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

使能 LLDP 功能：

```
SW-5024(config)#lldp
```

40.2 lldp hold-multiplier

描述

该命令用于设置 TTL 乘数。TTL 乘数用以控制本地设备发送的 LLDPDU 中 TTL 字段的值，TTL 即为本地信息在邻居设备上的存活时间。TTL=TTL 乘数*发送间隔。它的 no 命令用于恢复默认设置。

命令

lldp hold-multiplier *multiplier*

no lldp hold-multiplier

参数

multiplier —— TTL 乘数，范围为 2~10。默认值为 4。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置 TTL 乘数值为 5：

```
SW-5024(config)#lldp hold-multiplier 5
```

40.3 lldp timer

描述

该命令用于设置发送报文的各项时间参数。它的 no 命令用于恢复默认设置。

命令

lldp timer { **tx-interval** *tx-interval* | **tx-delay** *tx-delay* | **reinit-delay** *reinit-delay* | **notify-interval** *notify-interval* | **fast-count** *fast-count* }

no lldp timer { tx-interval | tx-delay | reinit-delay | notify-interval | fast-count }

参数

tx-interval—— 本地设备向邻居设备发送 LLDPDU 的时间间隔，取值范围为 5-32768，默认值为 30 秒。

tx-delay ——本地设备向邻居设备发送 LLDPDU 的延迟时间。当本地配置发生变化时，将延迟指定时间再发送 LLDPDU 通知邻居设备，从而可以避免由于本地配置频繁变化而导致 LLDPDU 的频繁发送。取值范围为 1-8192，默认值为 2 秒。

reinit-delay ——初始化延迟时间。当端口 LLDP 工作模式改变时，将延迟一段时间再进行初始化，以避免端口 LLDP 工作模式频繁改变导致端口不断执行初始化。取值范围为 1-10，默认值为 3 秒。

notify-interval ——本地设备向网络管理系统发送 Trap 信息的时间间隔。通过调整该时间间隔，可以避免由于邻居信息频繁变化而导致 Trap 信息的频繁发送。取值范围为 5-3600，默认值为 5 秒。

fast-count ——当端口 LLDP 工作模式从禁用（或只接收）切换为发送接收（或只发送）时，为了让其它设备尽快发现本设备，将启用快速发送机制，即将 LLDP 报文的发送周期缩短为 1 秒，并连续发送指定数量的 LLDPDU 后再恢复为正常的发送周期。取值范围为 1-10，默认值为 3 个。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置 LLDPDU 的发送间隔为 45 秒，向网络管理系统发送 trap 信息的发送时间间隔为 120 秒：

SW-5024(config)#lldp timer tx-interval 45 **SW-**

5024(config)#lldp timer notify-interval 120

40.4 lldp receive

描述

该命令用于开启指定端口的 LLDPDU 接收功能。它的 no 命令用于禁用该功能。

命令

lldp receive

no lldp receive

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启端口 1 的 LLDPDU 接收功能：

SW-5024(config)#interface gigabitEthernet

1/0/1 **SW-5024(config-if)#lldp receive**

40.5 lldp transmit

描述

该命令用于开启指定端口的 LLDPDU 发送功能。它的 no 命令用于禁用该功能。

命令

lldp transmit

no lldp transmit

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

开启端口 1 的 LLDPDU 发送功能：

```
SW-5024(config)# interface gigabitEthernet 1/0/1
SW-5024(config-if)#lldp transmit
```

40.6 lldp snmp-trap

描述

该命令用于启用端口的 SNMP 通知功能。启用此功能时，如果发生 trap 事件，本地设备将会通知 SNMP 服务器。它的 no 命令用于禁用端口的 SNMP 通知功能。

命令

lldp snmp-trap

no lldp snmp-trap

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用端口 1 的 SNMP 通知功能：

```
SW-5024(config)#interface gigabitEthernet
1/0/1 SW-5024(config-if)#lldp snmp-trap
```

40.7 lldp tlv-select

描述

该命令用于配置发送的 LLDPDU 中包含的 TLV 类型。LLDPDU 必须顺序包含三个必须的 TLV，然后是可选的 TLV，最后是必须的 END TLV。可以在此页面选择

端口发送 LLDPDU 时包含的可选 TLV 类型。它的 no 命令用于删除 LLDPDU 中包含的相关 TLV 类型。默认情况下，LLDPDU 中包含所有的 TLV 类型。

命令

lldp tlv-select { [port-description] [system-capability] [system-description] [system-name] [management-address] [port-vlan] [protocol-vlan] [vlan-name] [link-aggregation] [mac-phy-cfg] [max-frame-size] [power] [all] }

no lldp tlv-select { [port-description] [system-capability] [system-description] [system-name] [management-address] [port-vlan] [protocol-vlan] [vlan-name] [link-aggregation] [mac-phy-cfg] [max-frame-size] [power] [all] }

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

从端口 1 发送的 LLDPDU 中包含的 TLV 类型中不包含管理地址 TLV 和端口 VLAN ID TLV：

SW-5024(config)# interface gigabitEthernet 1/0/1 **SW-5024(config-if)# no lldp tlv-select** management-address port-vlan

40.8 lldp med-fast-count

描述

该命令用于设置 LLDP-MED 快速发送机制时发送的 LLDP-MED 帧的数目。当 LLDP-MED 的快速发送机制启动时，会连续发送指定个数的包含 LLDP-MED 信息的 LLDPDU，其默认值为 4。它的 no 命令用于恢复默认设置。

命令

lldp med-fast-count *count*

no lldp med-fast-count

参数

count —— 快速发送报文个数，取值范围为 1~10，默认值为 4。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置快速发送报文个数为 5：

```
SW-5024(config)# lldp med-fast-count 5
```

40.9 lldp med-status

描述

该命令用于启用端口的 LLDP-MED 状态。启用端口的 LLDP-MED 功能后，端口的 LLDP 状态会被设置为发送接收。它的 no 命令用于禁用端口的 LLDP-MED 功能。

命令

lldp med-status

no lldp med-status

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用端口 2 的 LLDP-MED 功能：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# lldp med-status
```

40.10 lldp med-tlv-select

描述

该命令用于选择发送的 LLDPDU 中包含的 LLDP-MED 的 TLV 类型。默认情况下， LLDPDU 中包含所有的 TLV 类型。它的 no 命令用于删除选中的 TLV 类型。

命令

lldp med-tlv-select { [inventory-management] [location] [network-policy] [power-management] [all] }

no lldp med-tlv-select { [inventory-management] [location] [network-policy] [power-management] [all] }

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

从端口 1 发送的 LLDPDU 中包含的 TLV 类型中不包含网络策略 TLV 和设备地址 TLV：

SW-5024(config)# interface gigabitEthernet 1/0/2 **SW-5024(config-if)# no lldp med-tlv-select** network-policy inventory-management

40.11 lldp med-location

Description

该命令用于设置端口发送的 LLDPDU 中包含的设备地址 TLV 的信息。

命令

lldp med-location { **emergency-number** *identifier* | **civic-address** [[language *language*] [province-state *province-state*] [county *county*] [city *city*] [street *street*] [house-number *house-number*] [name *name*] [postal-zipcode *postal-zipcode*] [room-number *room-number*] [post-office-box *post-office-box*] [additional *additional*] [country-code *country-code*] [what { dhcp-server | endpoint | switch }]] }

参数

emergency-number —— 紧急号码是紧急呼叫服务使用的号码，用以呼叫 CAMA 或者 PSAP，字符长度介于 10 到 25 之间。

civic-address —— 普通地址使用 IETF 规定的地址信息格式。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置端口 2 发送的 LLDPDU 中设备地址 TLV 类型中的普通地址，设置语言为英语，城市为伦敦：

```
SW-5024(config)# interface gigabitEthernet 1/0/2 SW-5024(config-if)# lldp

med-location civic-address language English city London
```

40.12 show lldp

描述

该命令用于显示 LLDP 的全局配置信息。

命令

show lldp

模式

特权模式和所有配置模式

特权要求

无

示例

显示 LLDP 的全局配置信息：

```
SW-5024#show lldp
```

40.13 show lldp interface

描述

该命令用于显示端口的 LLDP 配置信息。

命令

show lldp interface [**gigabitEthernet** *port*]

Parameters

port —— 端口号

模式

特权模式和所有配置模式

特权要求

无

示例

显示端口 1 的 LLDP 配置信息：

SW-5024#show lldp interface gigabitEthernet 1/0/1

40.14 show lldp local-information interface

描述

该命令用于显示端口的 LLDP 信息。

命令

show lldp local-information interface [**gigabitEthernet** *port*]

参数

port —— 要显示 LLDP 信息的端口号，缺省显示所有端口的 LLDP 信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示端口 1 的 LLDP 信息：

SW-5024#show lldp local-information interface gigabitEthernet 1/0/1

40.15 show lldp neighbor-information interface

描述

该命令用于显示连接到该端口的邻居信息。

命令

show lldp neighbor-information interface [**gigabitEthernet** *port*]

参数

port —— 要显示邻居信息的本地端口号，缺省显示所有端口的邻居信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示连接到端口 1 的邻居信息：

SW-5024#show lldp neighbor-information interface gigabitEthernet 1/0/1

40.16 show lldp traffic interface

描述

该命令用于显示连接到该端口的本地设备和邻居设备的 LLDP 统计信息。

命令

show lldp traffic interface [**gigabitEthernet** *port*]

参数

port —— 端口号.

模式

特权模式和所有配置模式

特权要求

无

示例

显示连接到端口 1 的 LLDP 统计信息：

SW-5024#show lldp traffic interface gigabitEthernet 1/0/1

第 41 章 sFlow 配置命令

sFlow（Sampled Flow）协议用于精确监控高速的网络流量。sFlow 监控系统包含了 sFlow 代理（嵌入在交换机、路由器或独立探测器中）和中央 sFlow 采集器。sFlow 代理是使用采样技术从被监控设备中抓取流量统计信息的虚拟实体。sFlow 收集器可以是从 sFlow 代理接收 sFlow 数据报的主机。

sFlow 功能实现如下：sFlow 收集器采集流量统计的样本，并将 sFlow 数据报发送到 sFlow 代理进行处理。sFlow 代理将 sFlow 数据报转发到 sFlow 收集器进行分析。 分析结果可以显示在 sFlow 收集器上。

41.1 sflow address

描述

该命令用于设置 sFlow 代理的 IP 地址，它的 no 命令用于删除 sFlow 代理的 IP 地址。

命令

sflow address { *ipv4-addr* }

no sflow address { *ipv4-addr* }

参数

ipv4-addr —— sFlow 代理的 IP 地址。IP 类型需为 IPv4。例如，可以将交换机的管理 IP 设为 sFlow 代理的地址。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置 sFlow 代理的 IP 地址为 192.168.0.1：

```
SW-5024(config)#sflow address 192.168.0.1
```

41.2 sflow enable

描述

该命令用于开启 sFlow 功能，它的 no 命令用于关闭 sFlow 功能。

命令

sflow enable

no sflow enable

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

说明

在开启 sFlow 之前，请先为交换机中的 sFlow 实体分配一个有效的 IP 地址。

示例

全局开启 sFlow 代理：

```
SW-5024(config)#sflow enable
```

41.3 sflow collector collector-ID

描述

该命令用于设置 sFlow 采集器的参数。

命令

sflow collector collector-ID *value* { [**descript** *descript*] | [**ip** *ip*] | [**port** *port*] | [**maxData** *maxData*] | [**timeout** *timeout*] }

参数

value —— sFlow 收集器的 ID。取值范围为 1-14。

descript —— 输入 sFlow 收集器描述。最多可输入 16 个字符。

ip —— sFlow 收集器的 IP 地址。该 IP 类型需为 IPv4。

port —— sFlow 收集器使用的 UDP 端口。

maxData —— 设置在一个采样数据中最多可以包含的字节数。取值范围为 300-1400，默认值为 300。

timeout —— 设置 sFlow 收集器的老化时间，取值范围为 0-2000000（秒）。0 表示收集器的收集周期是无限的。

模式

全局配置模式

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置端口 1 位 sFlow 的采样器：设置 collector ID 为 1，入口采样速率为 1024：

```
SW-5024(config)# sflow collector collector-ID 1 ip 192.168.0.100

SW-5024(config)# sflow collector collector-ID 1 port 3000
```

41.4 sflow sampler

描述

该命令用于设置 sFlow 采样器的参数。

命令

sflow sampler { [**collector-ID** *value*] | [**ingRate** *ingress-rate*] [**egRate** *egress-rate*] | [**maxHeader** *maxHeader*] }

参数

value —— 接收 sFlow 采样器发送的数据的 sFlow 收集器的 ID。取值范围为 0-14。

0 表示未选中 sFlow 收集器。

ingress-rate —— sFlow 采样器的入口数据的采样频率。该值表示两个采样数据之间会间隔多少个数据包。取值范围为 1024-65535，默认值为 0 表示对数据包不进行采样。

egress-rate —— sFlow 采样器的出口数据的采样频率。该值表示两个采样数据之间会间隔多少个数据包。取值范围为 1024-65535，默认值为 0 表示对数据包不进行采样。

maxHeader—— 从一个样本数据中复制的最大字节数。取值范围 18-256，默认值为 128 字节。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

只有管理员和操作员类型的用户可以使用该命令

示例

设置 sFlow 收集器 1 的 IP 地址为 192.168.0.100，使用的 UDP 端口为 3000：

```
SW-5024(config)#interface gigabitEthernet 1/0/1
```

```
SW-5024(config-if)#sflow sampler collector-ID 1
SW-5024(config-if)#sflow sampler ingRate 1024
```

41.5 show sflow global

描述

该命令用于显示 sFlow 全局配置信息。

命令

show sflow global

模式

特权模式和所有配置模式

特权要求

无

示例

显示 sFlow 采集器的全局配置信息：

```
SW-5024#show sflow global
```

41.6 show sflow collector

描述

该命令用于显示 sFlow 采集器的全局配置信息。

命令

show sflow collector

模式

特权模式和所有配置模式

特权要求

无

示例

显示 sFlow 采集器的全局配置信息：

```
SW-5024#show sflow collector
```

41.7 show sflow sampler

描述

该命令用于显示 sFlow 采样器的全局配置信息。

命令

show sflow sampler

模式

特权模式和所有配置模式

特权要求

无

示例

显示 sFlow 采样器的全局配置信息：

```
SW-5024#show sflow sampler
```

第 42 章静态路由配置命令

在本交换机上，可以配置静态路由条目。当交换机收到数据包时，可以通过数据包的目的地址查找最佳路由转发路径，然后快速将数据包转发到下一网络节点。静态路由通常由网络管理员手动配置，不随着网络拓扑的改变而自动变化，多用于网络规模较小，拓扑结构固定的网络中。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。

42.1 interface vlan

描述

该命令用于创建 VLAN 接口，它的 no 命令用于删除 VLAN 接口。

命令

interface vlan { *vid* }

no interface vlan { *vid* }

参数

vid —— VLAN ID。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建 VLAN 接口 2：

```
SW-5024(config)# interface vlan 2
```

42.2 interface loopback

描述

该命令用于创建环回接口，它的 no 命令用于删除环回接口。

命令

interface loopback { *id* }

no interface loopback { *id* }

参数

id ——环回接口 ID，取值范围：1-64。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建环回接口 1：

SW-5024(config)# interface loopback 1

42.3 switchport

描述

此命令用于从三层接口模式切换到二层端口模式，它的 no 命令用于从二层端口切换到三层路由端口。

命令

switchport

no switchport

模式

接口配置模式 (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

进入端口 1/0/9 的路由端口模式：

SW-5024(config)# interface gigabitEthernet 1/0/9

SW-5024(config-if)# no switchport

42.4 interface range port-channel

描述

该命令用于创建多个端口通道接口。

命令

interface range port-channel *port-channel-list*

参数

port-channel-list ——端口通道接口列表，取值范围为 1～14，格式为 1-3，5。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建端口通道接口 1,3,4 和 5：

SW-5024(config)# interface port-channel 1,3-5

42.5 description

描述

此命令用于给指定的路由接口添加描述，类型包括路由端口，环回接口和 VLAN 接口。它的 no 命令用于删除指定的路由接口的描述。

命令

description *string*

no description

参数

string ——长度为 1-16 位的描述字符串。

模式

接口配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

添加路由端口 1/0/9 的描述为 system-if：

```
SW-5024(config)# interface gigabitEthernet 1/0/9
SW-5024(config-if)# no switchport
SW-5024(config-if)# description system-if
```

42.6 shutdown

描述

此命令用于关闭指定的路由接口，类型包括路由端口，环回接口和 VLAN 接口。它的 no 命令用于开启指定的路由接口。

命令

shutdown

no shutdown

模式

接口配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

关闭路由端口 1/0/9：

```
SW-5024(config)# interface gigabitEthernet 1/0/9
SW-5024(config-if)# no switchport
SW-5024(config-if)# shutdown
```

42.7 interface port-channel

描述

该命令用于创建端口通道接口。要删除指定的端口通道接口，请使用它的 no 命令。

命令

interface port-channel { *port-channel-id* }

no interface port-channel { *port-channel-id* }

参数

port-channel-id ——端口通道接口的 ID，取值范围为 1～14。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建端口通道接口 1：

SW-5024(config)# interface port-channel 1

42.8 ip route

描述

该命令用于创建静态路由条目，no 命令用于删除静态路由条目。

命令

ip route { *dest-address* } { *mask* } { *next-hop-address* } [*distance*]

no ip route { *dest-address* } { *mask* } { *next-hop-address* }

参数

dest-address —— 配置路由条目能够到达的目标网络地址。

mask —— 配置路由条目能够到达的目标网络的子网掩码。

next-hop-address —— 通往目标网络的路由路径上下一个网络节点的 IP 地址。

distance —— 路由条目的度量值，度量值越小，优先级越高。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建目的 IP 地址为 192.168.2.0，子网掩码为 255.255.255.0，下一跳地址为 192.168.0.2 的静态路由：

SW-5024(config)# ip route 192.168.2.0 255.255.255.0 192.168.0.2

42.9 ipv6 routing

描述

该命令用于全局开启 IPv6 路由，它的 no 命令用于关闭 IPv6 路由。

命令

ipv6 routing

no ipv6 routing

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局开启 IPv6 路由：

SW-5024(config)# ipv6 routing

42.10 ipv6 route

描述

该命令用于配置 IPv6 静态路由，它的 no 命令用于删除 IPv6 静态路由。

命令

ipv6 route { *ipv6-dest-address* } { *next-hop-address* } [*distance*]

no ipv6 route { *ipv6-dest-address* } { *next-hop-address* }

参数

ipv6-dest-address/mask length —— 配置路由条目能够到达的目标 IPv6 地址。

next-hop-address —— 下一跳的 IPv6 地址。

distance —— 此路由的距离度量，范围从 1 到 255.距离越小，优先级越高。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建目的网络 IP 地址为 3200 :: / 64，下一跳地址为 3100 :: 1234 的静态路由：

SW-5024(config)# ipv6 route 3200::/64 3100::1234

42.11 show interface vlan

描述

该命令用于显示指定 VLAN 接口的信息。

命令

show interface vlan *vid*

Parameter

vid —— The VLAN ID.

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN 接口 2 的信息：

SW-5024(config)#show interface vlan 2

42.12 show ip interface

描述

该命令用于显示特定三层接口的详细信息。

命令

show ip interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id* | **loopback** *id* | **vlan** *vlan-id*]

参数

port —— 端口号。

port-channel-id —— 端口通道的 ID。此端口通道中的成员端口都应为路由端口。

id —— 环回接口 ID。

vlan-id —— VLAN 接口 ID。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN 接口 2 的详细信息：

```
SW-5024(config)# show ip interface vlan 2
```

42.13 show ip interface brief

描述

该命令用于显示三层接口的汇总信息。

命令

show ip interface brief

模式

特权模式和所有配置模式

特权要求

无

示例

显示三层接口的汇总信息：

```
SW-5024(config)# show ip interface brief
```

42.14 show ip route

描述

该命令用于显示设备上指定类型的路由条目。

命令

show ip route [static | connected]

参数

static | connected | rip —— 指定路由类型。如果未指定，将显示所有类型的路由条目。

static：显示设备上的静态路由信息。

connected：显示设备上的直连网络的路由信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示静态路由信息：

SW-5024(config)# show ip route static

42.15 show ip route specify

描述

该命令用于显示到指定 IP 地址或者网段的有效路由信息。

命令

show ip route specify { *ip* } [*mask*] [**longer-prefixes**]

参数

ip —— 指定目标 IP 地址。

mask ——指定目标 IP 地址和参数 ip。

longer-prefixes ——指定由 ip 和 mask 参数确定的匹配网段的目标子网。

模式

特权模式和所有配置模式

特权要求

无

示例

查找到 192.168.0.100 的最短路径：

SW-5024(config)# show ip route specify 192.168.0.100

查找到目的网段为 192.168.0.0/24 的路由条目是否存在：

SW-5024(config)# show ip route specify 192.168.0.0 255.255.255.0

查找目的网段为 192.168.0.0/16 所包含所有子网的路由信息：

SW-5024(config)# show ip route specify 192.168.0.0 255.255.0.0 **longer-prefixes**

42.16 show ip route summary

描述

该命令用于显示路由统计信息。

命令

show ip route summary

模式

特权模式和所有配置模式

特权要求

无

示例

显示交换机上的路由统计信息：

SW-5024(config)# show ip route summary

42.17 show ipv6 interface

描述

该命令用于显示管理接口配置的 IPv6 信息，包括 ipv6 的功能状态，链路本地地址和全局地址，IPv6 组播组等。

Syntax

show ipv6 interface

模式

特权模式和所有配置模式

特权要求

无

示例

显示管理接口的 IPv6 信息：

```
SW-5024(config)# show ipv6 interface
```

42.18 show ipv6 route

描述

该命令用于显示设备上指定类型的 IPv6 路由条目。

命令

show ipv6 route [static | connected]

参数

static | connected —— 指定路由类型。如果未指定，将显示所有类型的路由条目。

static：静态路由。

connected：显示设备上的直连网络的路由信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 IPv6 静态路由：

SW-5024(config)# show ipv6 route static

42.19 show ipv6 route summary

描述

该命令用于显示设备上指定类型的 IPv6 路由条目。

命令

show ipv6 route summary

模式

特权模式和所有配置模式

特权要求

无

示例

显示 IPv6 路由项的汇总信息：

SW-5024(config)# show ipv6 route summary

第 43 章 SDM 模板配置命令

本章介绍如何配置交换机数据库管理（SDM，Switch Database Management）模板，以便为交换机分配不同用途的硬件资源。

43.1 sdm prefer

描述

该命令用于配置 SDM 模板。SDM 模板用于分配系统资源，以最好地支持应用程序中使用的功能。要返回使用默认模板，请使用 sdm prefer default 命令。模板更改将在重新启动后生效。

命令

sdm prefer { default | enterpriseV4 | enterpriseV6 }

参数

default —— 将交换机中使用的 SDM 模板指定为“默认”。

enterpriseV4 —— 将交换机中使用的 SDM 模板指定为“enterpriseV4”。

enterpriseV6 —— 将交换机中使用的 SDM 模板指定为“enterpriseV6”。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

将交换机中使用的 SDM 模板指定为“enterpriseV4”：

```
SW-5024(config)# sdm prefer enterpriseV4
```

43.2 show sdm prefer

描述

该命令用于显示正在使用的当前 SDM 模板或可以使用的 SDM 模板的资源分配。

命令

show sdm prefer { used | default | enterpriseV4 | enterpriseV6 }

参数

used ——显示当前使用及重启后生效的模板的资源分配。

default ——显示默认模板的资源分配。

enterpriseV4 ——显示 enterpriseV4 模板的资源分配。

enterpriseV6 ——显示 enterpriseV6 模板的资源分配。

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示当前使用及重启后生效的模板的资源分配：

SW-5024(config)#show sdm prefer used

第 44 章 AAA 配置命令

AAA 是认证、授权和计费（Authentication、Authorization、Accounting）的简称。主要用于对试图访问交换机或者获得访问特权要求的用户进行认证，管理具有访问权的用户可以获得哪些服务，如何对正在使用网络资源的用户进行计费。具体功能表现为：

1. 认证(Authentication)：认证用户是否可以获得访问特权要求；
2. 授权(Authorization)：授权用户可以使用哪些服务；
3. 计费(Accounting)：记录用户使用网络资源的情况。

44.1 aaa enable

描述

该命令用于 AAA 全局配置，它的 no 命令用于禁用该功能。

命令

aaa enable no

aaa enable

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

开启 AAA 全局配置功能：

```
SW-5024(config)# aaa enable
```

44.2 tacacas-server host

描述

该命令用于配置一个新的 TACACS+ 服务器，它的 no 命令用于删除特定 TACACS+服务器。

命令

tacacs-server host *ip-address* [**port** *port-id*] [**timeout** *time*] [**key** { [0] *string* | 7 *encryped-string* }]

no tacacs-server host *ip-address*

参数

ip-address ——指定 TACACS+服务器的 IP 地址。

port-id ——指定 AAA 服务器的端口号。默认情况下是 49。

time ——指定超时范围内等待服务器响应的时间。时间范围从 1 到 9 秒，默认为 5 秒。

[0] *string* | 7 *encrypted-string* ——0 和 7 是加密类型。0 表示遵循一个非加密密钥。7 表示遵循一个固定长度的对称加密密钥。默认情况下，加密类型为 0。“字符串”是交换机和身份认证服务器的共享密钥，它最多可以交换包含 31 个字符的信息。问号和空格是不允许的。“加密字符串”是一个具有固定长度的对称加密密钥，可以从另一个交换机的配置文件中复制过来。配置的密钥或加密密钥将以加密形式显示。请将配置密钥始终作为该命令的最后一项。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

说明

配置的 TACACS+服务器将默认添加到“tacacs”服务器组中。

示例

配置 TACACS+服务器的 IP 地址为 1.1.1.1，TCP 端口为 1500，超时为 6 秒，未加密密钥串为 12345。

SW-5024(config)# tacacs-server host 1.1.1.1 **port** 1500 **timeout** 6 **key** 12345

44.3 show tacacs-server

描述

该命令用于显示 TACACS+服务器的配置信息。

命令

show tacacs-server

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示所有 TACACS+服务器信息：

```
SW-5024(config)# show tacacs-server
```

44.4 radius-server host

描述

该命令用于配置新的 RADIUS 服务器，删除特定 RADIUS 服务器，请使用它的 no 命令。

命令

radius-server host *ip-address* [**auth-port** *port-id*] [**acct-port** *port-id*]

[**timeout** *time*] [**retransmit** *number*] [**key** { [0] *string* | 7 *encrypted-string* }]

no radius-server host *ip-address*

参数

ip-address ——指定 RADIUS 服务器的 IP 地址。 **auth-port** *port-id* ——为认证请求指定 UDP 目的端口。默认情况下是 1812。 **acct-port** *port-id* ——为计费要求指定 UDP 目的端口。默认情况下是 1813。 *time* ——指定超时范围内等待服务器响应的时间。时间范围从 1 到 9 秒，默认为
5 秒。

number ——如果服务器没有及时响应，指定 RADIUS 请求的次数。默认情况下是 2 次。

[0] *string* | 7 *encrypted-string* ——0 和 7 是加密类型。0 表示遵循一个非加密密钥。7 表示遵循一个固定长度的对称加密密钥。默认情况下，加密类型为 0。“字符串”是交换机和身份认证服务器的共享密钥，它最多可以交换包含 31 个字符的信息。问号和空格是不允许的。“加密字符串”是一个具有固定长度的对称加密密

钥，可以从另一个交换机的配置文件中复制过来。配置的密钥或加密密钥将以加密形式显示。请将配置密钥始终作为该命令的最后一项。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

说明

配置的 RADIUS 服务器将默认添加到“radius”服务器组中。

示例

配置 RADIUS 服务器的 IP 地址为 1.1.1.1，认证端口为 1200，超时 6 秒，重传次数为 3，未加密的密钥串为 12345。

```
SW-5024(config)# radius-server host 1.1.1.1 auth-port 1200 timeout 6
retransmit 3 key 12345
```

44.5 show radius-server

描述

该命令用于显示 RADIUS 服务器的配置信息。

命令

show radius-server

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示所有 RADIUS 服务器信息：

```
SW-5024(config)# show radius-server
```

44.6 aaa group

描述

该命令用于新建服务器组，将用于认证的 TACACS+/RADIUS 服务器成组管理，使用该命令进入服务器组配置模式，删除相应 AAA 服务器组，请使用它的 no 命令。

命令

aaa group { radius | tacacs } *group-name* **no**

aaa group { radius | tacacs } *group-name*

参数

radius | tacacs —— 指定服务器组的类型为 RADIUS 或 TACACS+。

group-name —— 指定服务器组的名称。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

创建一个名为 radius1 的 RADIUS 服务器组：

SW-5024(config)# aaa group radius radius1

44.7 server

描述

该命令用于在已定义服务器组中添加现有的服务器，从服务器组删除相应服务器，请使用它的 no 命令。

命令

server *ip-address*

no server *ip-address*

参数

ip-address ——指定服务器的 IP 地址。

模式

服务器组配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

创建 RADIUS 服务器 1.1.1.1 到 RADIUS 服务器组“Radius1”中：

```
SW-5024(config)# aaa group radius radius1
SW-5024(aaa-group)# server 1.1.1.1
```

44.8 show aaa group

描述

该命令用于显示 AAA 服务器组的信息，若指定组名，则此组中的所有服务器都将被列出。

命令

show aaa group [*group-name*]

参数

group-name ——定义服务器组的名称

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示所有服务器组的信息：

```
SW-5024(config)# show aaa group
```

44.9 aaa authentication login

描述

该命令用于配置一个登录身份认证方法列表。该方法列表描述了对用户进行身份认证的方法和序列，删除指定认证方法列表，请使用它的 no 命令。

命令

aaa authentication login { *method-list* } { *method1* } [*method2*] [*method3*] [*method4*]

no authentication login *method-list*

参数

method-list ——指定方法列表的名称。

method1, method2, method3, method4 —— 定义认证方法的序号。如果前面的方法不响应，则尝试下一个身份认证方法，如果失败，则不进行。

预设的方法包括 radius、tacacs、local 和 none。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置一个优先级 1 为 radius，优先级 2 为 local 的登录认证方法列表：

SW-5024(config)# aaa authenticaiton login list1 radius local

44.10 aaa authentication enable

描述

该命令用于配置特权要求认证方法列表，该方法列表描述了提升用户特权要求的身份认证方法和顺序。删除指定身份认证方法列表，请使用它的 no 命令。

命令

aaa authentication enable { *method-list* } { *method1* } [*method2*] [*method3*] [*method4*]

no authentication enable *method-list*

参数

method-list —— 指定方法列表的名称。

method1, method2, method3, method4 ——定义认证方法的序号。如果前面的方法不响应，则尝试下一个身份认证方法，如果失败，则不进行。

预设的方法包括 radius、tacacs、local 和 none。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置一个优先级 1 为 radius，优先级 2 为 local 的特权要求认证方法列表：

SW-5024(config)# aaa authenticaiton enable list2 radius local

44.11 aaa authentication dot1x default

描述

该命令用于配置 802.1x 认证方法列表。该方法列表描述了 802.1x 用户登录认证方法。删除默认身份认证方法列表，请使用它的 no 命令。

命令

aaa authentication dot1x default { *method* }

no aaa authentication dot1x default

参数

method ——指定方法名称。只支持 RADIUS 服务器组时，默认方法是服务器组。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置默认的 802.1x 认证方式为“radius1”：

SW-5024(config)# aaa authentication dot1x default radius1

44.12 aaa accounting dot1x default

描述

该命令用于配置 802.1X 计费方法列表，删除默认计费方法列表，请使用它的 no 命令。

命令

aaa accounting dot1x default { *method* }

no aaa accounting dot1x default

参数

method ——指定方法名称。只支持 RADIUS 服务器组时，默认方法是服务器组。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置默认的 802.1x 计费方式为“radius1”：

SW-5024(config)# aaa accounting dot1x default radius1

44.13 show aaa authentication

描述

该命令用于显示身份认证登录信息，启用 dot1x 方法列表。

命令

show aaa authentication [login | enable | dot1x]

参数

login | enable | dot1x ——指定方法列表的类型。

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示所有认证方法列表的信息：

SW-5024(config)# show aaa authentication

44.14 show aaa accounting

描述

该命令用于显示计费方法列表的配置信息。

命令

show aaa accounting [dot1x]

参数

dot1x ——指定方法列表的类型。

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示默认 802.1X 计费方法列表的信息：

SW-5024(config)# show aaa accounting

44.15 line console

描述

该命令用来进入串口配置模式并配置 console 用户的认证列表。

命令

line console { *linenum* }

参数

linenum —— 允许通过 console 口登录的用户数量。其值一般为 0，因为 console 输入值在同一时刻只能在一个 console 口生效。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

进入串口配置模式并配置 console 接口 0：

```
SW-5024(config)#line console 0
```

44.16 login authentication(console)

描述

该命令用于配置 console 用户使用的 Login 方法列表。它的 no 命令用于恢复默认的 Login 方法列表。

命令

login authentication { *method-list* }

no login authentication

参数

method-list ——设置 console 用户使用的 Login 方法列表。默认 Login 列表为 default，且方法一默认为 local。

模式

Line Configuration Mode

特权要求

只有管理员类型的用户可以使用该命令

示例

配置 console 用户使用的 Login 方法列表为“list1”：

```
SW-5024(config)# line console 0
```

SW-5024(config-line)# login authentication list1

44.17 enable authentication(console)

描述

该命令用于配置 console 用户使用的 Enable 方法列表。它的 no 命令用于恢复默认的 Enable 方法列表。

命令

enable authentication { *method-list* }

no enable authentication

参数

method-list ——设置 console 用户使用的 Enable 方法列表。默认 Enable 列表为 default，且方法一默认为 none。

模式

Line Configuration Mode

特权要求

只有管理员类型的用户可以使用该命令

示例

配置 console 用户使用的 Enable 方法列表为“list2”：

SW-5024(config)# line console 0 **SW-**

5024(config-line)# enable authentication list2

44.18 line telnet

描述

该命令用来进入 telnet 配置模式。

命令

line telnet

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

进入 telnet 配置模式：

```
SW-5024(config)#line telnet
```

44.19 login authentication(telnet)

描述

该命令用于配置 telnet 用户使用的 Login 方法列表。它的 no 命令用于恢复默认的 Login 方法列表。

命令

login authentication { *method-list* }

no login authentication

参数

method-list —— 设置 telnet 用户使用的 Login 方法列表。默认 Login 列表为 default，且方法一默认为 local。

模式

Line 配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置 telnet 用户使用的 Login 方法列表为“list1”：

```
SW-5024(config)#line telnet SW-5024(config-
line)# login authentication list1
```

44.20 enable authentication(telnet)

描述

该命令用于配置 telnet 用户使用的 Enable 方法列表。它的 no 命令用于恢复默认的 Enable 方法列表。

命令

enable authentication { *method-list* }

no enable authentication

参数

method-list —— 设置 telnet 用户使用的 Enable 方法列表。默认 Enable 列表为 default，且方法一默认为 none。

模式

Line 配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置 telnet 用户使用的 Enable 方法列表为“list2”：

```
SW-5024(config)#line telnet SW-5024(config-
line)# enable authentication list2
```

44.21 line ssh

描述

该命令用来进入 ssh 配置模式并配置 ssh 用户的认证列表。

命令

line ssh

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

进入 ssh 配置模式：

```
SW-5024(config)#line ssh
```

44.22 login authentication(ssh)

描述

该命令用于配置 ssh 用户使用的 Login 方法列表。它的 no 命令用于恢复默认的 Login 方法列表。

命令

login authentication { *method-list* }

no login authentication

参数

method-list —— 设置 ssh 用户使用的 Login 方法列表。默认 Login 列表为 default，且方法一默认为 local。

模式

Line 配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置 ssh 用户使用的 Login 方法列表为“list1”：

```
SW-5024(config)# line ssh SW-5024(config-
line)# login authentication list1
```

44.23 enable authentication(ssh)

描述

该命令用于配置 ssh 用户使用的 Enable 方法列表。它的 no 命令用于恢复默认的 Enable 方法列表。

命令

enable authentication { *method-list* }

no enable authentication

参数

method-list —— 设置 ssh 用户使用的 Enable 方法列表。默认 Enable 列表为 default，且方法一默认为 none。

模式

Line 配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

配置 ssh 用户使用的 Enable 方法列表为“list2”：

```
SW-5024(config)# line ssh SW-5024(config-
line)# enable authentication list2
```

44.24 ip http login authentication

描述

该命令用来配置 http 用户的 Login 方法列表。它的 no 命令用于恢复默认的 Login 方法列表。

命令

ip http login authentication { *method-list* }

no ip http login authentication

参数

method-list ——设置 http 用户使用的 Login 方法列表。默认 Login 列表为 default，且方法一默认为 local。

模式

全局配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

设置 http 用户使用的 Login 方法列表为“list1”：

```
SW-5024(config)# ip http login authentication list1
```

44.25 ip http enable authentication

描述

该命令用来配置 http 用户的 Enable 方法列表。它的 no 命令用于恢复默认的 Login 方法列表。

命令

ip http enable authentication { *method-list* }

no ip http enable authentication

参数

method-list —— 设置 http 用户使用的 Enable 方法列表。默认 Enable 列表为 default，且方法一默认为 none。

模式

Line 配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

设置 http 用户使用的 Enable 方法列表为“list2”：

```
SW-5024(config)# ip http enable authentication list2
```

44.26 show aaa global

描述

该命令用于显示 AAA 功能的全局配置信息和各应用模块（console, telnet, ssh 和 HTTP）的 Login/Enable 方法列表。

命令

show aaa global

模式

特权模式和所有配置模式

特权要求

只有管理员类型的用户可以使用该命令

示例

显示 AAA 功能的全局配置信息和各应用模块（console, telnet, ssh 和 HTTP）的 login/Enable 方法列表：

```
SW-5024(config)# show aaa global
```

第 45 章 DHCP 服务器配置命令

本交换机可以配置为 DHCP 服务器，为网络中的多个 VLAN 指定地址池，实现不同 VLAN 的设备获得不同网段的 IP 地址。

45.1 service dhcp server

描述

该命令用于全局使能 DHCP 服务功能，包括 DHCP 服务器和 DHCP 中继功能。它的 no 命令用于关闭 DHCP 服务功能。

命令

service dhcp server

no service dhcp server

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局启用 DHCP 服务功能：

```
SW-5024(config)# service dhcp server
```

45.2 ip dhcp server extend-option capwap-ac-ip

描述

该命令用于设置远程 DHCP 服务器的 IP 地址，它的 no 命令用于删除指定的远程 DHCP 服务器地址。

命令

ip dhcp server extend-option capwap-ac-ip *ip-address*

no ip dhcp server extend-option capwap-ac-ip

参数

ip-address ——设置远程 DHCP 服务器的 IP 地址。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置远程 DHCP 服务器的 IP 地址为 192.168.3.1：

SW-5024(config)# ip dhcp server extend-option capwap-ac-ip 192.168.3.1

45.3 ip dhcp server extend-option vendor-class-id

描述

该命令用于设置来自不同网段的 DHCP 服务器的数据包类 ID，它的 no 命令用于删除该设置。

命令

ip dhcp server extend-option vendor-class-id *class-id* **no ip dhcp server extend-option vendor-class-id**

参数

class-id ——设置来自其它网段的 DHCP 数据包类 ID。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置来自其它网段的 DHCP 数据包类 ID 为 34：

SW-5024(config)# ip dhcp server extend-option vendor-class-id 34

45.4 ip dhcp server exclude-address

描述

该命令用于为每个网段保留特定的 IP 地址不做分配，如网关地址、网段广播地址、服务器地址等均需要进行配置保留。no 命令用于取消某段保留地址。

命令

ip dhcp server exclude-address *start-ip-address end-ip-address*
no ip dhcp server exclude-address *start-ip-addr end-ip-address*

参数

start-ip-address —— 设置预留 IP 地址段的起始地址。

end-ip-address —— 设置预留 IP 地址段的结束地址。当结束 IP 地址和起始 IP 地址一致时，表示只预留一个 IP 地址。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 192.168.10.10 为保留地址不做分配：

SW-5024(config)# ip dhcp server exclude-address 192.168.1.1 192.168.1.9

45.5 ip dhcp server pool

描述

该命令用于创建地址池并进入 DHCP 配置模式，它的 no 命令用于删除指定的地址池。

命令

ip dhcp server pool *pool-name*
no ip dhcp server pool *pool-name*

参数

pool-name ——设置地址池名称，1-8 个字符，由数字、英文字母，中文字符和下划线组成。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

创建地址池“POOL1”并进入 DHCP 配置模式：

```
SW-5024(config)# ip dhcp server pool POOL1
```

45.6 ip dhcp server ping timeout

描述

此命令用于指定 ping 的超时时间，它的 no 命令用于恢复默认值。DHCP 使用 ping 操作来确认指定的 IP 地址是否存在。

命令

ip dhcp server ping timeout *value*

no ip dhcp server ping timeout

参数

value —— 设置 ping 超时时间，范围是 100-10000ms，默认值为 100ms。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置 ping 超时时间为 200ms：

```
SW-5024(config)# ip dhcp server ping timeout 200
```

45.7 ip dhcp server ping packets

描述

此命令用于配置发出 ping 数据包的个数，如果设置为 0，则不进行 ping 操作。

命令

ip dhcp server ping packets *num*

参数

num ——设置发送 ping 包的数量，范围是 0 到 10。默认值为 1。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置 ping 包的发送数量为 2：

SW-5024(config)# ip dhcp server ping packets 2

45.8 network

描述

该命令用于配置地址池的网络地址。

命令

network *network-address subnet-mask*

参数

network-address —— 配置此地址池的网络地址，同一网段中的地址除了预留地址以及特殊地址外均可以作为可分配地址。

subnet-mask —— 配置此地址池的子网掩码。当客户端从此地址池获取 IP 地址时，其子网掩码以此参数为准。

模式

DHCP 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

为地址池“product”配置网络地址及子网掩码：

SW-5024(config)# ip dhcp server pool product **SW-**

5024(config-dhcp)# network 192.168.1.0 255.255.255.0

45.9 lease

描述

该命令用于配置地址池中的 IP 地址可供分配的租期。

命令

lease *lease-time*

参数

lease-time ——配置此地址池中的 IP 地址可供分配的租期时间长度，最长为 2880 分钟。默认值为 120 分钟。

模式

DHCP 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将地址池“product”的租期设置为 10 分钟：

SW-5024(config)# ip dhcp server pool product

SW-5024(config-dhcp)# lease 10

45.10 address hardware-address

描述

该命令用于为特定 MAC 地址的设备预留地址池中指定的 IP 地址，它的 no 命令用于删除预留的绑定关系。

命令

address *ip-address* **hardware-address** *hardware-address* **hardware-type** { ethernet | ieee802 }

no address *ip-address*

参数

ip-address —— 配置需要预留的 IP 地址。

hardware-address —— 输入特定设备的 MAC 地址。

ethernet | ieee802 —— 输入特定设备的硬件类型，包括 Ethernet 或者 IEEE802 类型。

模式

DHCP 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将地址池“product”中的地址 192.168.10.50 为设备 00:19:66:20:d4:1a 预留，该设备的硬件类型为 Ethernet：

SW-5024(config)# ip dhcp server pool product **SW-5024(config-dhcp)#**

address 192.168.0.50 **hardware-address** 00:19:66:20:d4:1a **hardware-type**

ethernet

45.11 address client-identifier

描述

该命令用于为特定客户端 ID 设备预留地址池中指定的 IP 地址，它的 no 命令用于删除预留的绑定关系。

命令

address *ip-address* **client-identifier** *client-id* [**ascii**]

no address *ip-address*

参数

ip-address —— 配置需要预留的地址。

client-id —— 配置客户端 ID，格式为 16 进制。

ascii —— 客户端 ID 的格式为 ASCII 码。

模式

DHCP 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

为 ASCII 码为 abc 的客户端 ID 保留地址池 product 中的 IP 地址 192.168.0.10：

SW-5024(config)# ip dhcp pool product **SW-5024(dhcp-config)#**

address 192.168.0.10 **client-identifier** abc **ascii**

45.12 default-gateway

描述

该命令用于配置地址池的缺省网关。

命令

default-gateway *gateway-list*
no default-gateway

参数

gateway-list ——配置此地址池的默认网关，最多可以为地址池配置 8 个网关，相互之间以逗号间隔。默认情况下，也可以以 VLAN 接口 IP 地址作为默认网关。

模式

DHCP 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

为地址池“product”配置两个网关，分别为 192.168.10.1 和 192.168.10.2：

SW-5024(config)# ip dhcp server pool product **SW-5024(dhcp-config)# default-gateway** *192.168.0.1,192.168.1.1*

45.13 dns-server

描述

该命令用于配置地址池的 DNS 服务器，它的 no 命令用于删除 DNS 服务器。

命令

dns-server *dns-list*
no dns-server

参数

dns-server-list —— 配置此地址池的 DNS 服务器，最多可以为地址池配置 8 个 DNS 服务器地址，相互之间以逗号间隔。

模式

DHCP 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将 DNS 服务器 192.170.10.10 配置为地址池“product”的 DNS 服务器：

SW-5024(config)# ip dhcp server pool product **SW-5024(config-dhcp)# dns-server 192.168.0.1,192.168.1.1**

45.14 netbios-name-server

描述

该命令用于设置 Netbios 服务器的 IP 地址，它的 no 命令用于删除 Netbios 服务器。

命令

netbios-name-server *NBNS-list*
no netbios-name-server

参数

NBNS-list ——设置 Netbios 服务器的地址列表，最多可以为 Netbios 服务器设置 8 个地址，相互之间以逗号间隔。

模式

DHCP 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置 Netbios 服务器的 IP 地址为 192.168.0.1 和 192.168.1.1：

SW-5024(config)# ip dhcp server pool product **SW-5024(config-dhcp)# netbios-name-server** 192.168.0.1,192.168.1.1

45.15 netbios-node-type

描述

该命令用于设置 Netbios 服务器的节点类型，它的 no 命令用于删除该设置。

命令

netbios-node-type *type*
no netbios-node-type

参数

type ——设置 Netbios 服务器的节点类型，可选项有：b-node，h-node，m-node 和 p-node。

模式

DHCP 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置 Netbios 服务器的节点类型为 b-node：

```
SW-5024(config)# ip dhcp server pool product SW-
5024(config-dhcp)# netbios-node-type b-node
```

45.16 next-server

描述

该命令用于设置引导过程的下一个服务器地址，它的 no 命令用于删除该设置。

命令

next-server *ip-address*
next-server

参数

ip-address ——设置下一服务器地址。

模式

DHCP 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置下一服务器地址为 192.168.2.1：

```
SW-5024(config)# ip dhcp server pool product
```

```
SW-5024(config-dhcp)# next-server 192.168.2.1
```

45.17 domain-name

描述

该命令用于设置客户端域名，它的 no 命令用于删除该设置。

命令

domain-name *domainname*
no domain-name

参数

domainname ——设置客户端域名。

模式

DHCP 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置客户端域名为 edu：

```
SW-5024(config)# ip dhcp server pool product
SW-5024(config-dhcp)# domain-name edu
```

45.18 bootfile

描述

该命令用于设置引导过程中用到的镜像文件名，它的 no 命令用于删除该设置。

命令

bootfile *file-name*
no bootfile

参数

file-name ——设置启动文件名。

模式

DHCP 配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

设置启动文件名为 boot1：

```
SW-5024(config)# ip dhcp server pool product
SW-5024(config-dhcp)# bootfile boot1
```

45.19 show ip dhcp server status

描述

该命令用于查看 DHCP 服务的全局配置信息。

命令

show ip dhcp server status

模式

特权模式和所有配置模式

特权要求

无

示例

查看 DHCP 服务的全局配置信息：

```
SW-5024(config)# show ip dhcp server status
```

45.20 show ip dhcp server statistics

描述

该命令用于查看 DHCP Server 模块接收报文和发送报文的统计信息。

命令

show ip dhcp server statistics

模式

特权模式和所有配置模式

特权要求

无

示例

查看当前 DHCP Server 模块接收报文和发送报文的统计信息：

```
SW-5024(config)# show ip dhcp server statistics
```

45.21 show ip dhcp server extend-option

描述

该命令用于查看远程 DHCP 服务器配置。

命令

show ip dhcp server extend-option

模式

特权模式和所有配置模式

特权要求

无

示例

查看远程 DHCP 服务器配置：

```
SW-5024(config)# show ip dhcp server extend-option
```

45.22 show ip dhcp server pool

描述

该命令用于查看地址池配置信息。

命令

show ip dhcp server pool

模式

特权模式和所有配置模式

特权要求

无

示例

查看地址池配置信息：

```
SW-5024(config)# show ip dhcp server pool
```

45.23 show ip dhcp server excluded-address

描述

该命令用于查看每个地址池保留不做分配的 IP 地址。

命令

show ip dhcp server excluded-address

模式

特权模式和所有配置模式

特权要求

无

示例

查看每个地址池保留不做分配的 IP 地址信息：

```
SW-5024(config)# show ip dhcp server excluded-address
```

45.24 show ip dhcp server manual-binding

描述

该命令用于查看进行静态绑定的 IP 地址信息。

命令

show ip dhcp server manual-binding

模式

特权模式和所有配置模式

特权要求

无

示例

查看进行静态绑定的 IP 地址信息：

```
SW-5024(config)# show ip dhcp server manual-binding
```

45.25 show ip dhcp server binding

描述

该命令用于查看指定 IP 或者所有 IP 地址的绑定条目。

命令

show ip dhcp server binding [**ip** *ip-address*]

参数

ip-address ——指定 IP 以查看该 IP 地址的绑定条目。.

模式

特权模式和所有配置模式

特权要求

无

示例

查看所有 IP 地址的绑定条目：

```
SW-5024(config)# show ip dhcp server binding
```

45.26 clear ip dhcp server statistics

描述

此命令用于清除 DHCP 报文的统计信息。

命令

clear ip dhcp server statistics

模式

特权模式和所有配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

清除 DHCP 报文的统计信息：

```
SW-5024(config)# clear ip dhcp server statistics
```

45.27 clear ip dhcp server binding

描述

此命令用于清除绑定信息。

命令

clear ip dhcp server binding [*ip-address*]

参数

ip-address —— 输入进行绑定的 IP 地址。

模式

特权模式和所有配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

删除所有进行 IP 地址绑定的条目：

```
SW-5024(config)# clear ip dhcp server binding
```

第 46 章 DHCP 中继配置命令

DHCP 中继是在客户端和服务器之间转发 DHCP 数据包的三层设备。当客户端和服务器不在同一物理子网上时，DHCP 中继转发请求和应答。

46.1 service dhcp relay

描述

该命令用于全局启用 DHCP 中继功能。 要禁用 DHCP 中继功能，请使用它的 no 命令。

命令

service dhcp relay

no service dhcp relay

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

全局启用 DHCP 中继功能：

```
SW-5024(config)# service dhcp relay
```

46.2 ip helper-address

描述

该命令用于向三层接口添加 DHCP 服务器地址。要删除服务器地址，请使用它的 no 命令。

命令

ip helper-address *ip-address*

no ip helper-address [*ip-address*]

参数

ip-address ——DHCP 服务器地址。

模式

接口配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

将 DHCP 服务器地址 192.168.2.1 添加到接口 VLAN 1：

```
SW-5024(config)# interface vlan 1 SW-
5024(config-if)# ip helper-address 192.168.2.1
```

46.3 ip dhcp relay information

描述

该命令用于在 DHCP 中继中启用 Option 82 选项功能，no 命令用于禁用 Option 82 选项功能。

命令

ip dhcp relay information
no ip dhcp relay information

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用 Option 82 选项功能：

```
SW-5024(config)# ip dhcp relay information
```

46.4 ip dhcp relay information policy

描述

该命令用于指定来自主机的 DHCP 请求报文中 Option 82 字段的操作。要恢复到默认选项，请使用它的 no 命令。

命令

ip dhcp relay information policy { drop | keep | replace }

no ip dhcp relay information policy

参数

drop | keep | replace ——来自主机的 DHCP 请求报文中 Option 82 字段的操作。默认操作是 keep。

drop —— 丢弃包含 Option 82 字段的数据包。

keep —— 保留数据包中的 Option 字段信息。

replace —— 替换数据包中的 Option 字段信息，替换为交换机自定义的系统选项内容。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置交换机在收到含有 Option 82 字段的 DHCP 请求报文时，将 Option 82 字段的内容替换为本地参数后转发：

```
SW-5024(config)# ip dhcp relay information policy replace
```

46.5 ip dhcp relay information custom

描述

该命令用于配置 Option 82 选项自定义功能，no 命令用于关闭自定义功能。

命令

ip dhcp relay information custom
no ip dhcp relay information custom

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

启用 Option 82 选项自定义功能：

```
SW-5024(config)# ip dhcp relay information custom
```

46.6 ip dhcp relay information circuit-id

描述

该命令用于在启用 Option 82 自定义功能时指定自定义电路 ID。 要清除电路 ID，请使用它的 no 命令。

命令

ip dhcp relay information circuit-id *circuitID*
no ip dhcp relay information circuit-id

参数

circuitID ——指定电路 ID，取值范围为 1～64 个字符。

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 Option 82 字段中的电路 ID 子选项内容为“SUNDRAY”:

SW-5024(config)# ip dhcp relay information circuit-id SUNDRAY

46.7 ip dhcp relay information remote-id

描述

该命令用于在启用 Option 82 自定义功能时指定自定义远程 ID。要清除远程 ID，请使用它的 no 命令。

命令

ip dhcp relay information remote-id *remoteID*
no ip dhcp relay information remote-id

参数

remoteID —— Specify the remote ID, ranging from 1 to 64 characters.

模式

全局配置模式

特权要求

只有管理员、操作员和高级用户类型的用户可以使用该命令

示例

配置 Option 82 字段中的远程 ID 子选项内容为“SUNDRAY”:

```
SW-5024(config)# ip dhcp relay information remote-id SUNDRAY
```

46.8 show ip dhcp relay

描述

该命令用于显示 DHCP 中继的全局状态和 Option 82 配置。

参数

show ip dhcp relay

模式

特权模式和所有配置模式

特权要求

无

示例

查看 DHCP 中继功能的配置参数：

```
SW-5024(config)# show ip dhcp relay
```

第 47 章 PoE 配置命令

PoE（Power over Ethernet，以太网供电，又称远程供电）是指设备通过以太网线对外接 PD（Powered Device，受电设备）设备（如 IP 电话、无线 AP、网络摄像机等）进行远程供电。

47.1 power inline consumption (global)

描述

该命令用于配置 PoE 交换机所能提供的最大功率。

命令

power inline consumption *power-limit*

参数

power-limit ——PoE 交换机所能提供的最大功率，取值范围为 1W-384W，默认为 384W。

模式

全局配置模式

特权要求

无

示例

配置 PoE 交换机所能提供的最大功率为 160W：

SW-5024(config)# power inline consumption 160

47.2 power inline disconnect-method

描述

该命令用于当负载功率超出限定功率时的处理方法，保持交换机提供系统的功率在可用的水平。

命令

power inline disconnect-method {deny-next-port|deny-low-priority}

参数

deny-next-port——当负载功率超过限制时，连在下一个端口的 PD 设备将被断开。

deny-next-priority——当负载功率超过限制时，连在端口上优先级较低的 PD 设备将被断开。

模式

全局配置模式

特权要求

无

示例

配置当负载功率超过限制时，处理方法为 deny-next-port：

```
SW-5024(config)# power inline disconnect-method deny-next-port
```

47.3 power profile

描述

该命令用于创建一个新的 PoE profile 文件。它的 no 命令用于删除已配置的 PoE profile 文件。PoE profile 文件用于对具有相同属性的 PoE 接口进行批量配置，以简化用户的操作。在 PoE profile 文件中，配置了端口的三个 PoE 属性：状态、优先级、最大功率。创建一个 PoE profile 文件，然后将其应用于相应的端口，可简化配置过程。

命令

power profile *name* [**supply** {enable | disable} [**priority** {low | middle | high} [**consumption** { *power-limit* | auto | class1 | class2 | class3 | class4 }]]]

no power profile *name*

参数

name——profile 文件的名称，可输入 1-16 个字符。如果文件的名称包含空格，请将该名称放在双引号中，如“File 2”。

supply——profile 文件中设置的端口 PoE 状态。

priority——profile 文件中设置的端口 PoE 优先级。

consumption——profile 文件中设置的端口 PoE 最大功率。有 *power-limit*，auto，class1，class2，class3 和 class4 五个可选项。*power-limit* 表示可手动输入具体数值，取值范围为 1-300，功率上限为输入值乘以 0.1W。例如，要设置某端口最大供电功率为 5W，则此处应输入 50。auto 表示由系统自动指定端口的 PoE 最大功率。class1 表示 4W。class2 表示 7W。class3 表示 15.4W。class4 表示 30W。

模式

全局配置模式

特权要求

无

示例

创建一个 PoE profile 文件。profile 文件的名称是 IP Camera，PoE 状态为开启，PoE 优先级为低，最大功率为 5W：

SW-5024(config)# power profile “IP Camera” **supply** enable **priority** low **consumption** 50

47.4 power time-range

描述

该命令用于添加时间段并进入 PoE 时间段设置模式。在 PoE 时间段设置模式下可进一步通过 holiday，absolute 或 periodic 命令具体配置该时间段。它的 no 命令用于删除相应的时间段。当用户需要某些端口在特定时间段供电时，可以先配置时间段，然后将其应用于这些端口即可。这些端口将只在指定的时间段内供电。

命令

power time-range *name*

no power time-range *name*

参数

name ——要添加的时间段名称。可输入 1-16 个字符。

模式

全局配置模式

特权要求

无

示例

添加一个名为 tRange1 的时间段：

SW-5024(config)# power time-range tRange1

47.5 power holiday

描述

该命令用于创建 **power time-range** 假期模式的节假日，它的 no 命令用于删除相应节假日。

命令

power holiday *name* **start-date** *start-date* **end-date** *end-date*

no power holiday *name*

参数

name —— 节假日名称，可输入 1~16 个字符。

start-date —— 节假日的起始日期，格式为 MM/DD，如 05/01。

end-date —— 节假日的结束日期，格式为 MM/DD，如 05/03。

模式

全局配置模式

特权要求

无

示例

定义节假日国庆节，并设置其起止时间为 10 月 1 日到 10 月 3 日：

SW-5024(config)# power holiday NationalDay **start-date** 10/01 **end-date** 10/03

47.6 absolute

描述

该命令用于配置已创建的时间段的绝对起始日期，设置后交换机将只在该起始日期期间为受电设备供电。它的 no 命令用于取消配置的绝对时间。

命令

absolute start *start-date* **end** *end-date*

no absolute

参数

start-date ——起始日期，格式为 MM/DD/YYYY，如 01/01/2012。

end-date —— 结束日期，格式为 MM/DD/YYYY，如 12/31/2013。

模式

PoE 时间段设置模式（power time-range）

特权要求

无

示例

配置时间段 tRange1 为从 2012 年 5 月 5 日至 2012 年 10 月 5 日：

SW-5024(config)# power time-range tRange1 **SW-5024(config-pwr-time-range)# absolute start** 05/05/2012 **end** 10/05/2012

47.7 periodic

描述

该命令用于以周期模式配置已创建的时间段，即可让交换机在一周中的某几天为受电设备供电。它的 no 命令用于取消配置的周期时间。

命令

periodic { [**week-date** *week-day*] [**time-slice1** *time-slice*] [**time-slice2** *time-slice*] [**time-slice3** *time-slice*] [**time-slice4** *time-slice*] }

no periodic [week-date | time-slice]

参数

week-day ——周期模式，形式为 1-3，6，也可输入 daily，off-day，working-day。

其中 1-3，6 表示周一、周二、周三和周六；daily 表示每天，即周一到周日；off-day 表示周末，即周六和周日；working-day 表示工作日，即周一到周五。缺省时禁止周期模式。.

time-slice —— 创建时间片段，格式为 HH:MM-HH:MM，如 08:30-12:00。

week-date | time-slice——取消配置的周期时间中的周期模式或时间片段。

模式

PoE 时间段设置模式（power time-range）

特权要求

无

示例

配置时间段 tRange2 为每周末的 08:30-12:00：

SW-5024(config)# power time-range tRange2 **SW-5024(config-pwr-time-range)# periodic week-date** off-day **time-slice1** 08:30-12:00

47.8 holiday

描述

该命令用于配置已创建的时间段是否包含 PoE 节假日。PoE 节假日可通过 power holiday 命令定义。

命令

holiday { exclude | include }

参数

exclude ——不包含 PoE 节假日，即 PoE 节假日期间交换机不为受电设备供电。

include —— 包含节假日，即 PoE 节假日期间交换机交换机仍为受电设备供电。默认选择该项。

模式

PoE 时间段设置模式（power time-range）

特权要求

无

示例

将配置时间段 tRange3 为不包含节假日：

```
SW-5024(config)# power time-range tRange3 SW-
5024(config-pwr-time-range)# holiday exclude
```

47.9 power inline consumption(interface)

描述

该命令用于配置端口供电功率上限。

命令

power inline consumption { *power-limit* | auto | class1 | class2 | class3 | class4 }

参数

power limit——相应端口能提供的最大供电功率。取值范围为 1-300。功率上限为输入值乘以 0.1W。例如，要设置某端口最大供电功率为 5W，则此处应输入 50。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

无

示例

配置端口 2 的最大供电功率为 5W：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# power inline consumption 50
```

47.10 power inline priority

描述

该命令用于为相应的端口配置 PoE 优先级。

命令

power inline priority { low | middle | high }

参数

priority——当剩余功率不够时，与供电管理方式一起决定对新接入的 PD 的供电方式，优先级等级包括低（low）、中（middle）、高（high）三种。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

无

示例

配置端口 2 的 PoE 优先级为低：

```
SW-5024(config)# interface gigabitEthernet 1/0/2
SW-5024(config-if)# power inline priority low
```

47.11 power inline supply

描述

该命令用于启用或禁用相应端口的 PoE 功能。

命令

power inline supply { enable | disable }

参数

enable | disable ——启用或禁用相应端口的 PoE 功能。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

无

示例

启用端口 2 的 PoE 功能：

SW-5024(config)# interface gigabitEthernet 1/0/2

SW-5024(config-if)# power inline supply enable

47.12 power inline profile

描述

该命令用于将 PoE profile 文件应用于所选的端口。它的 no 命令用于取消应用 PoE profile 文件。

命令

power inline profile *name*

no power inline profile

参数

name ——已配置的 profile 文件的名称，可输入 1-16 个字符。如果文件的名称包含空格，请将该名称放在双引号中，如“File 2”。

模式

接口配置模式（interface gigabitEthernet / interface range gigabitEthernet）

特权要求

无

示例

将名为 IP Camera 的 PoE profile 文件应用于端口 2：

SW-5024(config)# interface gigabitEthernet 1/0/2 **SW-**

5024(config-if)# power inline profile “IP Camera”

47.13 power inline time-range

描述

该命令用于为端口配置供电的时间段。它的 no 命令用于取消已选的时间段。

命令

power inline time-range *name*

no power inline time-range

参数

name ——已创建的时间段的名称。

模式

接口配置模式

特权要求

无

示例

选择时间段 tRange2 作为端口 2 的供电时间段：

```
SW-5024(config)# interface gigabitEthernet 1/0/2 SW-
5024(config-if)# power inline time-range tRange2
```

47.14 show power inline

描述

该命令用于显示系统 PoE 信息。

命令

show power inline

模式

特权模式和所有配置模式

特权要求

无

示例

显示系统 PoE 信息：

```
SW-5024# show power inline
```

47.15 show power inline configuration interface

描述

该命令用于显示某端口的 PoE 配置信息。

命令

show power inline configuration interface [**gigabitEthernet** *port*]

参数

port ——要显示 PoE 配置信息的端口号，缺省显示所有端口的 PoE 信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口的 PoE 配置信息：

```
SW-5024# show power inline configuration interface
```

47.16 show power inline information interface

描述

该命令用于显示某端口的 PoE 信息。

命令

show power inline information interface [**gigabitEthernet** port]

参数

port ——要显示 PoE 信息的端口号，缺省显示所有端口的 PoE 信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口的 PoE 信息：

```
SW-5024# show power inline information interface
```

47.17 show power profile

描述

该命令用于显示已定义的 PoE profile 文件。

命令

show power profile

模式

特权模式和所有配置模式

特权要求

无

示例

显示已定义的 PoE profile 文件：

```
SW-5024# show power profile
```

47.18 show power holiday

描述

该命令用于显示已定义的节假日。

命令

show power holiday

模式

特权模式和所有配置模式

特权要求

无

示例

显示已定义的节假日：

```
SW-5024# show power holiday
```

47.19 show power time-range

描述

该命令用于显示时间段配置信息。

命令

show power time-range

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有的时间段 PoE 信息：

```
SW-5024# show power time-range
```