TP-LINK®

全万兆三层网管交换机

命令行手册

REV1.1.0
1910040765

声明

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TP-LINK TL-ST5416/ TL-ST5016F 全万兆三层网管交换机。

鉴于三层网管交换机功能相近，本手册以TL-ST5416为例介绍。

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：语音 VLAN 的配置命令

主要介绍语音 VLAN 的相关配置命令。

第 8 章：P-rivate VLAN 配置命令

主要介绍 Private VLAN 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：Etherchannel 配置命令

主要介绍端口汇聚和 LACP 的相关配置命令。

第 11 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 12 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 13 章：绑定列表配置命令

主要介绍 IP-MAC-VID-PORT 四元绑定表的相关配置命令。

第 14 章：ARP 防护配置命令

主要介绍 ARP 防护的相关配置命令。

第 15 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 16 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 17 章：系统日志配置命令

主要介绍系统日志的查看、输出，日志服务器的相关配置命令。

第 18 章：SSH 配置命令

主要介绍 SSH 配置管理的相关命令。

第 19 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 20 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 21 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 22 章：IPv6 地址配置命令

主要介绍 IPv6 地址相关配置命令。

第 23 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 24 章：QoS 配置命令

主要介绍 QoS（服务质量）的相关配置命令。

第 25 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 26 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 27 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 28 章：ACL 配置命令

主要介绍访问控制的相关配置命令。

第 29 章：MSTP 配置命令

主要介绍生成树配置的相关配置命令。

第 30 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 31 章：MLD 侦听配置命令

主要介绍 MLD 侦听的相关配置命令。

第 32 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 33 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 34 章：ARP 配置命令

主要介绍 ARP 配置命令。

第 35 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 36 章：SDM 模板命令

主要介绍 SDM 模板配置命令。

第 37 章：AAA 配置命令

主要介绍 AAA 配置命令。

第 38 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 39 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 40 章：代理 ARP 配置命令

主要介绍代理 ARP 功能的相关配置命令。

第 41 章：RIP 配置命令

主要介绍 RIP 功能的相关配置命令。

第 42 章：管理口配置命令

主要介绍管理口的相关配置命令。

第 43 章：U 盘开局配置命令

主要介绍 U 盘开局功能的相关配置命令。

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

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），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
3. 在主窗口中输入回车键，可以看到“TL-ST5416>”的提示符，说明已成功登录交换机。

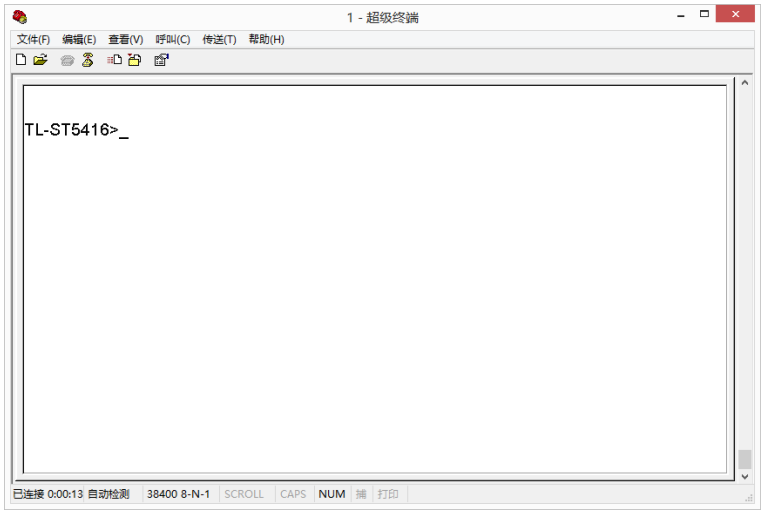


图 1-1 命令行主窗口

说明：

若计算机使用Windows XP系统，可在**开始>所有程序>附件>通讯>超级终端**，打开超级终端，配置如上所需参数，也可登录交换机

1.1.2. 通过Telnet进行登录

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。

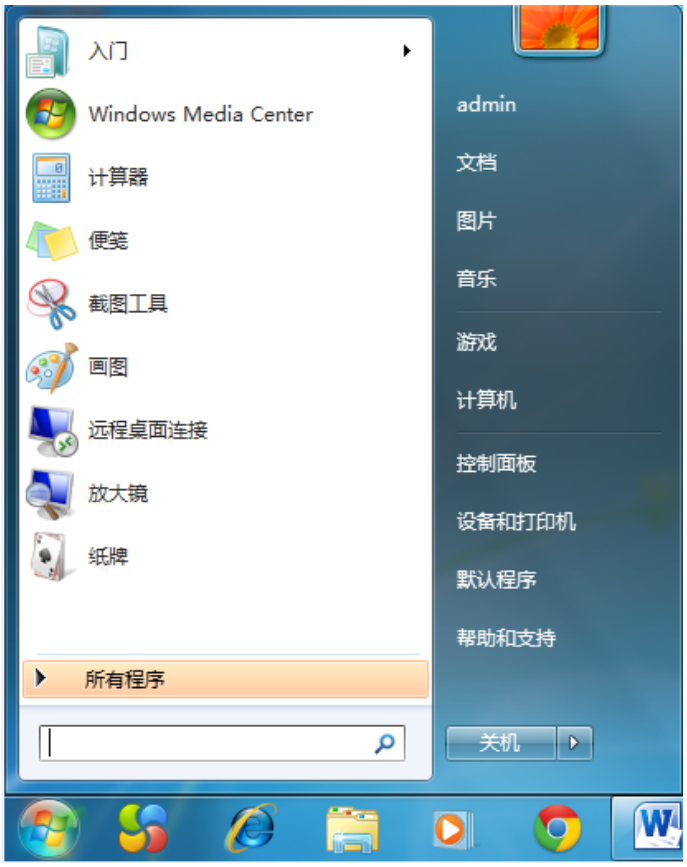


图 1-2 进入cmd窗口

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。

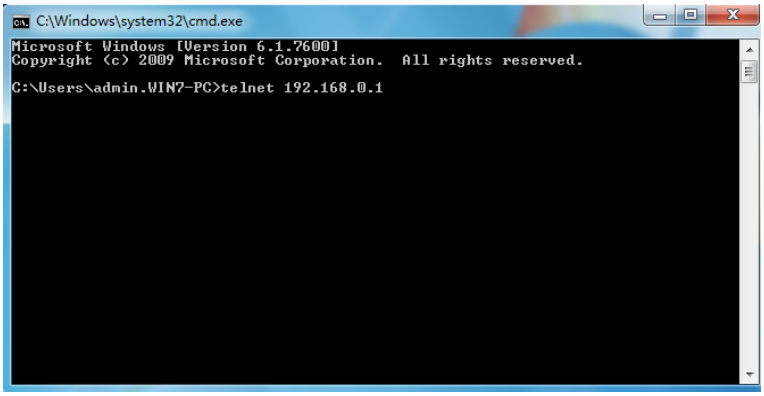


图 1-3 登录交换机

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。

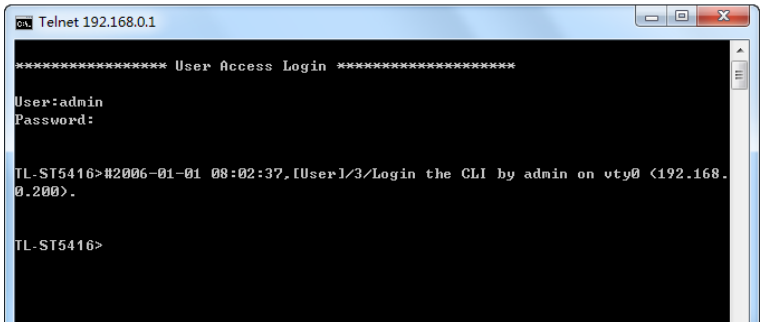


图 1-4 进入用户模式

4. 输入**enable**命令进入特权模式。

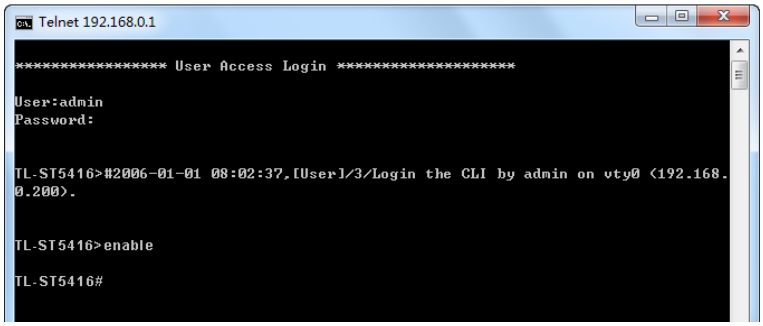


图 1-5 进入特权模式

1.1.3. 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开启交换机的 SSH 功能。

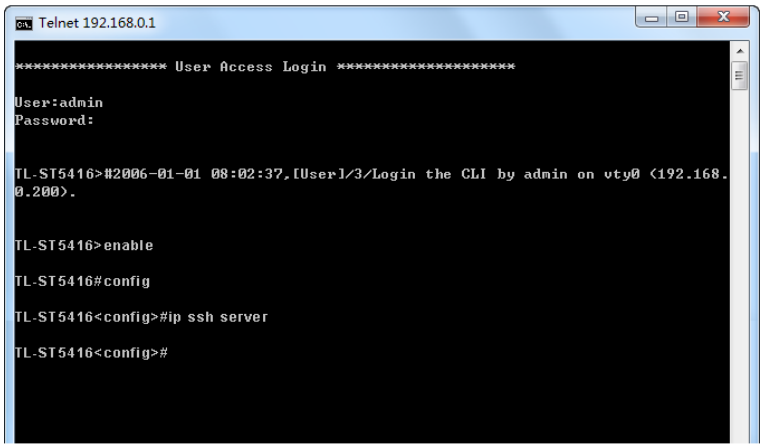


图 1-6 开启SSH功能

➢ **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 1-7 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。

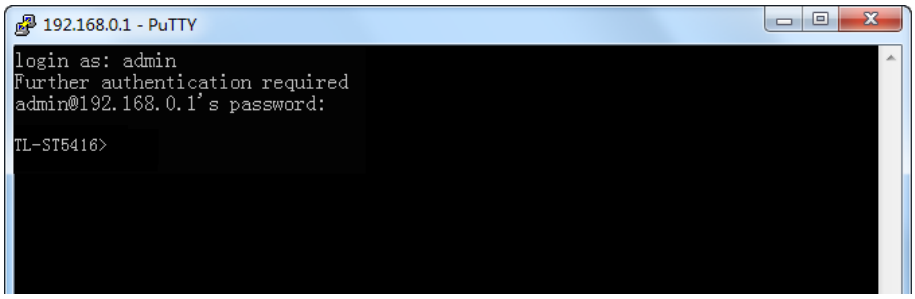


图 1-8 登录交换机

➢ **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 1-9 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。

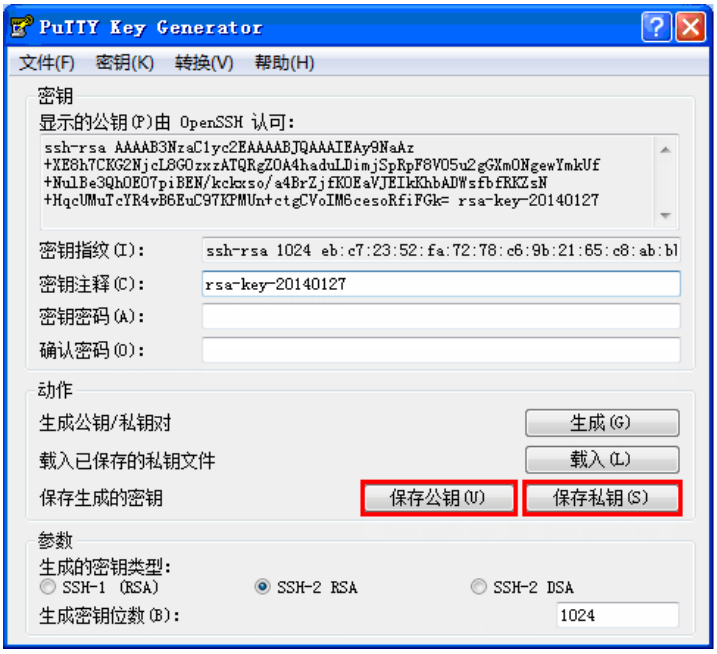


图 1-10 保存公钥和私钥

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。

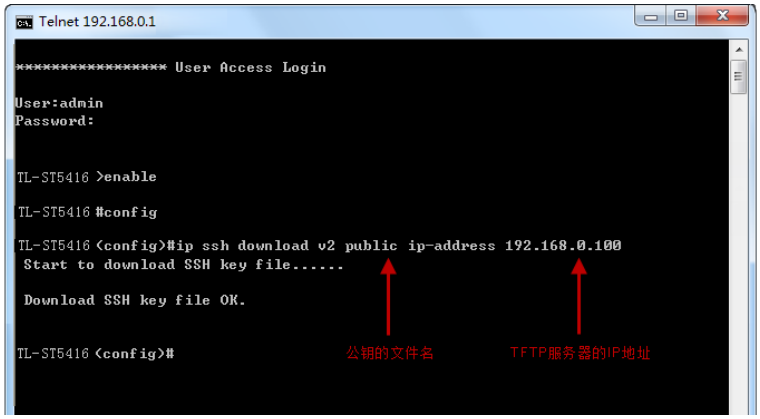


图 1-11 导入公钥文件至交换机

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 1-12 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。

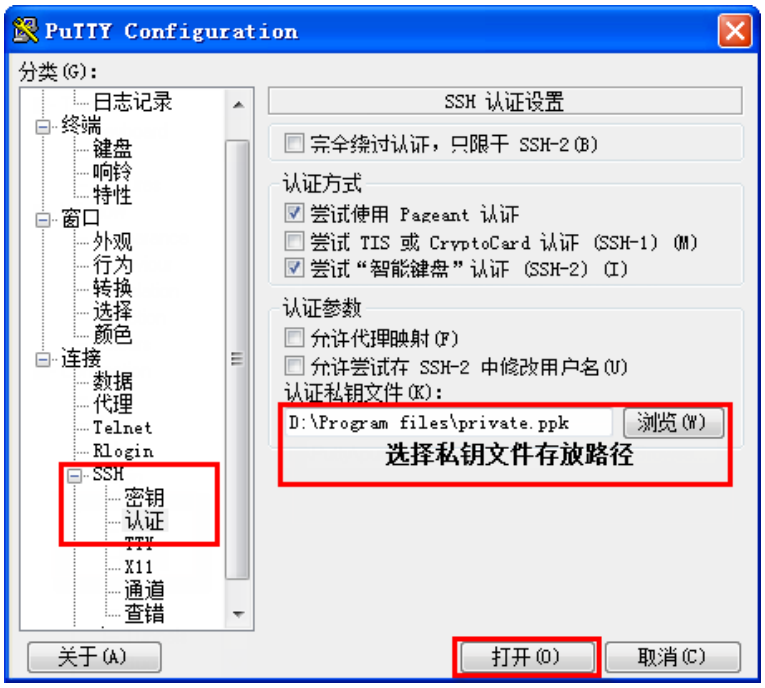


图 1-13 导入私钥文件至SSH客户端

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。

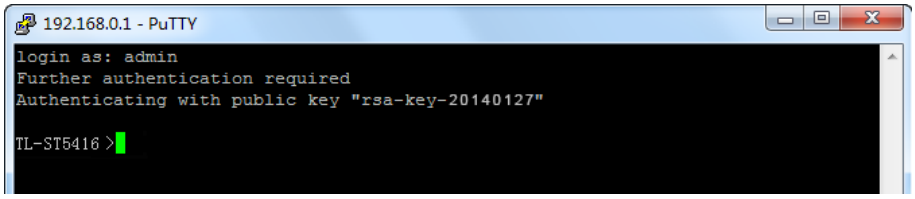
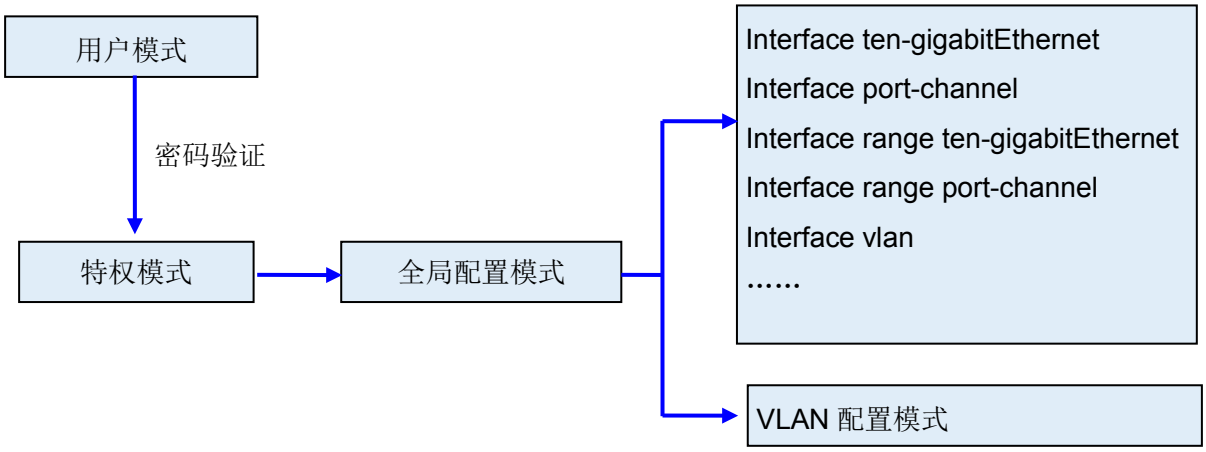


图 1-14 登录交换机

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，如下图：



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	**TL-ST5416>**	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	**TL-ST5416#**	输入**disable**命令或**exit**命令，返回用户模式； 输入**configure**命令，进入全局配置模式。
全局配置模式	在特权模式下，使用**configure**命令进入该模式	**TL-ST5416(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** *type number*命令，进入接口配置模式； 输入**vlan**命令，进入VLAN配置模式。

模式	访问方法	提示符	离开或访问下一模式
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	**TL-ST5416(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。
接口配置模式	二层接口： 在全局配置模式下键入**interface ten-gigabitEthernet** *port*或**interface port-channel** *lagid* 或 **interface range ten-gigabitEthernet** *port-list* 或 **interface port-channel** *lag-list*进入该模式。	**TL-ST5416(config-if)#** 或 **TL-ST5416(config-if-range)#**	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； 在**interface**命令中必须指明要进入哪一个接口配置子模式。
	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。		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 ten-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 ten-gigabitEthernet：包含的命令跟interface ten-gigabitEthernet基本一样，配置多个以太网端口的参数。
     c) Interface port-channel：配置一个以太网通道的参数。
     d) Interface range port-channel：包含的命令跟Interface port-channel基本一样，配置多个以太网通道的参数。
     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：**switchport type** { access | trunk | general }
- 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

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：

```
TL-ST5416>enable
Password:
TL-ST5416#
```

2.2 service password-encryption

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：

```
TL-ST5416(config)# service password-encryption
```

2.3 enable password

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，无视起始空格并且不能包含问号。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

1. 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。
2. 如果同时配置了 **enable password** 和 **enable secret**，则只有最新的配置会生效。

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

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：

```
TL-ST5416(config)# enable password admin
```

2.4 enable secret

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，无视起始空格并且不能包含问号。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**，则只有最新的配置会生效。

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

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：

```
TL-ST5416(config)# enable secret 0 admin
```

2.5 configure

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：

```
TL-ST5416# configure
TL-ST5416(config)#
```

2.6 exit

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：

```
TL-ST5416 (config-if)# exit
TL-ST5416 (config)#exit
TL-ST5416#
```

2.7 end

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：

```
TL-ST5416(config-if)#end
TL-ST5416#
```

2.8 history

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：

```
TL-ST5416(config)#history
    1 history
```

2.9 history clear

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**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：

```
TL-ST5416(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

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。

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：

```
TL-ST5416(config)# vlan 2-10,100
```

删除VLAN 2：

```
TL-ST5416(config)# no vlan 2
```

3.2 interface vlan

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：

```
TL-ST5416(config)# interface vlan 2
```

3.3 name

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vid=2的VLAN描述成“VLAN002”：

```
TL-ST5416(config)# vlan 2
TL-ST5416(config-vlan)# name VLAN002
```

3.4 switchport mode

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# switchport mode trunk
```

3.5 switchport access vlan

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# switchport mode access
TL-ST5416(config-if)# switchport access vlan 2
```

3.6 switchport trunk allowed vlan

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# switchport mode trunk
TL-ST5416(config-if)# switchport trunk allowed vlan 2
```

3.7 switchport general allowed vlan

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/4
TL-ST5416(config-if)# switchport mode general
TL-ST5416(config-if)# switchport general allowed vlan 2 tagged
```

3.8 switchport pvid

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 ten-gigabitEthernet / interface range ten-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3的PVID为1：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# switchport pvid 1
```

3.9 show vlan summary

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：

```
TL-ST5416(config)# show vlan summary
```

3.10 show vlan brief

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：

```
TL-ST5416(config)# show vlan brief
```

3.11 show vlan

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

显示所有VLAN的详细信息：

```
TL-ST5416(config)# show vlan
```

显示vid=2的VLAN的详细信息：

```
TL-ST5416(config)# show vlan id 2
```

3.12 show interface switchport

该命令用于显示以太网口的信息。

命令

show interface switchport [**ten-gigabitEthernet** *port* | **port-channel** *lagid*]

参数

port —— 以太网端口号。

lagid —— LAG号。

模式

特权模式以及所有配置模式

特权要求

无

示例

显示所有端口详细信息：

```
TL-ST5416(config)#show interface switchport
```

第4章 MAC VLAN配置命令

4.1 mac-vlan mac-address

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 RD：

```
TL-ST5416(config)# mac-vlan mac-address 00:11:11:01:01:12 vlan 2 description RD
```

4.2 mac-vlan

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 ten-gigabitEthernet / interface range ten-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 3 的 MAC VLAN 功能：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3

TL-ST5416(config-if)# mac-vlan
```

4.3 show mac-vlan

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：

```
TL-ST5416(config)# show mac-vlan all
```

4.4 show mac-vlan interface

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：

```
TL-ST5416(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

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。

type —— 以太网协议类型，由 4 位十六进制数组成。

dsap —— 目的服务访问点，由两位十六进制组成。

ssap —— 源服务访问点，由两位十六进制组成。

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“TP”。

```
TL-ST5416(config)# protocol-vlan template name TP frame ether_2 ether-type 2024
```

5.2 protocol-vlan vlan

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：

TL-ST5416(config)# protocol-vlan vlan 2 **template** 3

5.3 protocol-vlan group

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 ten-gigabitEthernet / interface range ten-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加入到协议组1：

TL-ST5416(config)# interface ten-gigabitEthernet 1/0/5

TL-ST5416(config-if)# protocol-vlan group 1

5.4 show protocol-vlan template

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：

```
TL-ST5416(config)# show protocol-vlan template
```

5.5 show protocol-vlan vlan

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：

```
TL-ST5416(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

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：

```
TL-ST5416(config)#dot1q-tunnel
```

6.2 dot1q-tunnel tpid

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 *num*

no dot1q-tunnel tpid

参数

num —— 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8200：

```
TL-ST5416(config)#dot1q-tunnel tpid 8200
```

6.3 dot1q-tunnel mapping

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：

TL-ST5416(config)#dot1q-tunnel mapping

6.4 switchport dot1q-tunnel mapping

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 16 个字符。

模式

接口配置模式(interface ten-gigabitEthernet / interface range ten-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 上添加一条 VLAN 映射条目，C-VLAN 为 2，SP-VLAN 为 3：

TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2

TL-ST5416(config-if)#switchport dot1q-tunnel mapping 2 3

6.5 switchport dot1q-tunnel mode

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 ten-gigabitEthernet / interface range ten-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

配置以太网端口3作为VPN NNI接口：

TL-ST5416(config)#interface ten-gigabitEthernet 1/0/3

TL-ST5416(config-if)#switchport dot1q-tunnel mode nni

6.6 show dot1q-tunnel

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：

TL-ST5416(config)# show dot1q-tunnel

6.7 show dot1q-tunnel interface

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的端口类型：

```
TL-ST5416(config)#show dot1q-tunnel interface
```

6.8 show dot1q-tunnel mapping

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：

```
TL-ST5416(config)# show dot1q-tunnel mapping
```

第7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。

7.1 voice vlan

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：

```
TL-ST5416(config)# voice vlan 10
```

7.2 voice vlan aging

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，默认值为1440分钟。

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。

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：

TL-ST5416(config)# voice vlan aging 2880

7.3 voice vlan priority

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。语音VLAN的默认优先级为6。

命令

voice vlan priority *pri*

no voice vlan priority

参数

pri —— 优先级，取值范围0-7。

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：

TL-ST5416(config)# voice vlan priority 5

7.4 voice vlan mac-address

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TP- Phone：

TL-ST5416(config)# voice vlan mac-address 00:11:11:11:11:11 **mask** FF:FF:FF:00:00:00 **description** TP- Phone

7.5 switchport voice vlan mode

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 ten-gigabitEthernet / interface range ten-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manual：

TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3

TL-ST5416(config-if)# switchport voice vlan mode manual

7.6 switchport voice vlan security

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# switchport voice vlan security
```

7.7 show voice vlan

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：

```
TL-ST5416(config)# show voice vlan
```

7.8 show voice vlan oui

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：

```
TL-ST5416(config)# show voice vlan oui
```

7.9 show voice vlan switchport

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 [**ten-gigabitEthernet** *port* | **port-channel** *lagid*]

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。

lagid —— LAG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

显示语音VLAN中所有端口的配置信息：

```
TL-ST5416(config)# show voice vlan switchport
```

第8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。

8.1 private-vlan primary

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：

```
TL-ST5416(config)#vlan 3
TL-ST5416(config-vlan)#private-vlan primary
```

8.2 private-vlan community

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 4 设置为 Private VLAN 的 Community VLAN：

```
TL-ST5416(config)# vlan 4
TL-ST5416(config-vlan)# private-vlan community
```

8.3 private-vlan isolated

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 4 设置为 Private VLAN 的 Isolated VLAN：

```
TL-ST5416(config)# vlan 4
TL-ST5416(config-vlan)# private-vlan isolated
```

8.4 private-vlan association

该命令用于关联Primary VLAN和Community 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 —— Community 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：

```
TL-ST5416(config)#vlan 3
TL-ST5416(config-vlan)#private-vlan association 4
```

8.5 switchport private-vlan

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 { promiscuous | host }

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 ten-gigabitEthernet / interface range ten-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

配置端口3的Private VLAN属性为host：

```
TL-ST5416(config)#interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)#switchport private-vlan host
```

8.6 switchport private-vlan host-association

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 ten-gigabitEthernet / interface range ten-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

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：

TL-ST5416(config)#interface ten-gigabitEthernet 1/0/3

TL-ST5416(config-if)#switchport private-vlan host-association 3 4 community

8.7 switchport private-vlan mapping

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 *primary_vlan_id secondary_vlan_id*

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 ten-gigabitEthernet / interface range ten-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

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

TL-ST5416(config)#interface ten-gigabitEthernet 1/0/4

TL-ST5416(config-if)#switchport private-vlan mapping 3 4

8.8 show vlan private-vlan

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：

```
TL-ST5416(config)# show vlan private-vlan
```

8.9 show vlan private-vlan interface

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 [**ten-gigabitEthernet** *port*]

参数

port —— 以太网端口号。

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：

```
TL-ST5416(config)#   show vlan private-vlan 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)

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：

```
TL-ST5416(config)# gvrp
```

9.2 gvrp (interface)

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 ten-gigabitEthernet / interface range ten-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2-6的GVRP功能：

```
TL-ST5416(config)# interface range ten-gigabitEthernet 1/0/2-6
```

TL-ST5416(config-if-range)# gvrp

9.3 gvrp registration

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 ten-gigabitEthernet / interface range ten-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2-6的GVRP注册模式为fixed：

TL-ST5416(config)# interface range ten-gigabitEthernet 1/0/2-6

TL-ST5416(config-if-range)# gvrp registration fixed

9.4 gvrp timer

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 ten-gigabitEthernet / interface range ten-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6的leaveall定时器设为2000，并将join定时器恢复默认配置：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/6
TL-ST5416(config-if)# gvrp timer leaveall 2000
TL-ST5416(config-if)# no gvrp timer join
```

9.5 show gvrp global

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：

```
TL-ST5416(config)# show gvrp global
```

9.6 show gvrp interface

该命令用于显示以太网端口的GVRP配置信息。

命令

show gvrp interface [**ten-gigabitEthernet** *port*]

参数

port —— 以太网端口号，缺省时显示所有端口的GVRP配置信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口的GVRP配置信息：

```
TL-ST5416(config)# show gvrp interface
```

第10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。

10.1 channel-group

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1-32。

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 ten-gigabitEthernet / interface range ten-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

添加端口2-4到汇聚组1，并开启静态LAG模式：

```
TL-ST5416(config)# interface range ten-gigabitEthernet 1/0/2-4
TL-ST5416(config-if-range)# channel-group 1 mode on
```

10.2 port-channel load-balance

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-mac：

```
TL-ST5416(config)# port-channel load-balance src-dst-mac
```

10.3 lacp system-priority

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：

TL-ST5416(config)# lacp system-priority 1024

10.4 lacp port-priority

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 ten-gigabitEthernet / interface range ten-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1的端口优先级设置为1024：

TL-ST5416(config)# interface ten-gigabitEthernet 1/0/1

TL-ST5416(config-if)# lacp port-priority 1024

10.5 show etherchannel

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1-32。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：

```
TL-ST5416(config)# show etherchannel 1 detail
```

10.6 show etherchannel load-balance

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：

```
TL-ST5416(config)# show etherchannel load-balance
```

10.7 show lacp

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：

```
TL-ST5416(config)# show lacp 1 internal
```

10.8 show lacp sys-id

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：

```
TL-ST5416(config)# show lacp sys-id
```

第11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。

11.1 user name (password)

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

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

guest | admin —— 用户类型，guest：受限用户，admin：管理员。添加用户时，默认为admin。

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tplink，密码为不加密的admin的管理员账户：

```
TL-ST5416 (config)#user name tplink privilege admin password 0 admin
```

11.2 user name (secret)

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tplink，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：

TL-ST5416 (config) #user name tplink **privilege** admin **secret** 0 admin

11.3 user access-control ip-based

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

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。

[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IP地址为192.168.0.148的身份限制：

TL-ST5416 (config) # user access-control ip-based 192.168.0.148 255.255.255.255

11.4 user access-control mac-based

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：

TL-ST5416 (config) # user access-control mac-based 00:00:13:0A:00:01

11.5 user access-control port-based

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 { **ten-gigabitEthernet** *port-list* } [snmp] [telnet] [ssh] [http] [https] [ping] [all]

user access-control port-based interface none

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：

TL-ST5416 (config) # user access-control port-based interface ten-gigabitEthernet 1/0/2-6

11.6 telnet

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：

```
TL-ST5416 (config)# telnet disable
```

11.7 show user account-list

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：

```
TL-ST5416 (config)# show user account-list
```

11.8 show user configuration

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：

```
TL-ST5416 (config)# show user configuration
```

11.9 show telnet-status

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：

```
TL-ST5416 (config)# show telnet-status
```

第12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。

12.1 ip http server

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：

```
TL-ST5416 (config)# no ip http server
```

12.2 ip http max-users

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 operator-num powerusr-num user-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。

operator-num —— 以操作员身份登录到 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。

powerusr-num —— 以高级用户身份登录到 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。

user-num —— 以普通用户身份登录到 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、操作员、高级用户和普通用户登录到 HTTP 服务器的最大数量为 5、3、2 和 3：

```
TL-ST5416 (config)# ip http max-users 5 3 2 3
```

12.3 ip http session timeout

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 *minutes*

no ip http 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：

```
TL-ST5416 (config)# ip http session timeout 15
```

12.4 ip http secure-server

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：

```
TL-ST5416 (config)# no ip http secure-server
```

12.5 ip http secure-protocol

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 secure-protocol

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：

```
TL-ST5416 (config)# ip http secure-protocol ssl3
```

12.6 ip http secure-ciphersuite

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：

TL-ST5416 (config)# ip http secure-ciphersuite 3des-ede-cbc-sha

12.7 ip http secure-max-users

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 operator-num powerusr-num user-num*

no ip http 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。

operator-num ——以操作员身份登录到 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。

powerusr-num ——以高级用户身份登录到 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。

user-num ——以普通用户身份登录到 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、操作员、高级用户和普通用户登录到 HTTPS 服务器的最大数量为 5、3、2 和 3：

```
TL-ST5416 (config)# ip http secure-max-users 5 3 2 3
```

12.8 ip http secure-session timeout

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 *minutes*

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：

```
TL-ST5416 (config)# ip http secure-session timeout 15
```

12.9 ip http secure-server download certificate

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 192.168.0.148 的 TFTP 服务器导入名为 ssl.cert 的 SSL 证书：

TL-ST5416 (config)# ip http secure-server download certificate ssl.cert **ip-address** 192.168.0.148

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

TL-ST5416 (config) # ip http secure-server download certificate ssl.cert **ip-address** fe80::1234

12.10 ip http secure-server download key

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 192.168.0.148 的 TFTP 服务器导入名为 ssl.key 的 SSL 密钥：

TL-ST5416 (config)# ip http secure-server download key ssl.key **ip-address** 192.168.0.148

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

TL-ST5416 (config)# ip http secure-server download key ssl.key **ip-address** fe80::1234

12.11 show ip http configuration

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：

```
TL-ST5416 (config)# show ip http configuration
```

12.12 show ip http secure-server

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：

```
TL-ST5416 (config)# show ip http secure-server
```

第13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。

13.1 ip source binding

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 ten-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：

TL-ST5416 (config)# ip source binding host1 192.168.0.1 00:00:00:00:00:01 **vlan** 2 **interface ten-gigabitEthernet** 1/0/5 ip-verify-source

删除unit1的绑定表中序号为5的IP-MAC –VID-PORT条目：

TL-ST5416 (config)# no ip source binding index 5

13.2 ip dhcp snooping

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：

TL-ST5416 (config)# ip dhcp snooping

13.3 ip dhcp snooping vlan

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：

TL-ST5416 (config) #ip dhcp snooping vlan 1,4,6-7

13.4 ip dhcp snooping information option

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 ten-gigabitEthernet / interface range ten-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上开启DHCP侦听的Option 82功能：

TL-ST5416 (config)# interface ten-gigabitEthernet 1/0/1

TL-ST5416 (config)# ip dhcp snooping information option

13.5 ip dhcp snooping information strategy

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 ten-gigabitEthernet / interface range ten-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：

TL-ST5416 (config) # interface ten-gigabitEthernet 1/0/1

TL-ST5416 (config)# ip dhcp snooping information strategy replace

13.6 ip dhcp snooping information remote-id

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。长度为1-32个字符。

模式

接口配置模式(interface ten-gigabitEthernet / interface range ten-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上配置Option 82的远程ID子选项为tplink：

TL-ST5416 (config) # interface ten-gigabitEthernet 1/0/1

TL-ST5416 (config)# ip dhcp snooping information remote-id tplink

13.7 ip dhcp snooping information circuit-id

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。长度为1-32个字符。

模式

接口配置模式(interface ten-gigabitEthernet / interface range ten-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tplink:

TL-ST5416 (config)# interface ten-gigabitEthernet 1/0/1

TL-ST5416 (config)# ip dhcp snooping information circuit-id tplink

13.8 ip dhcp snooping trust

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 ten-gigabitEthernet / interface range ten-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2为授信端口：

TL-ST5416 (config)# interface ten-gigabitEthernet 1/0/2

TL-ST5416 (config-if)# ip dhcp snooping trust

13.9 ip dhcp snooping mac-verify

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 ten-gigabitEthernet / interface range ten-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MAC验证功能：

TL-ST5416 (config)# interface ten-gigabitEthernet 1/0/2

TL-ST5416 (config-if)# ip dhcp snooping mac-verify

13.10 ip dhcp snooping limit rate

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416 (config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416 (config-if)# ip dhcp snooping limit rate 20
```

13.11 ip dhcp snooping decline rate

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 ten-gigabitEthernet / interface range ten-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decline侦听功能：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if) #ip dhcp snooping decline rate 20
```

13.12 show ip source binding

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：

```
TL-ST5416 (config)# show ip source binding
```

13.13 show ip dhcp snooping

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：

```
TL-ST5416 (config)# show ip dhcp snooping
```

13.14 show ip dhcp snooping interface

该命令用于显示对应千兆网口/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 [**ten-gigabitEthernet** *port* | **port-channel** *lagid*]

参数

port —— 交换机端口号，缺省时显示所有端口的配置信息。

lagid —— 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/链路聚合的DHCP侦听配置信息：

```
TL-ST5416# show ip dhcp snooping interface
```

显示端口5的DHCP侦听配置信息：

TL-ST5416# show ip dhcp snooping interface ten-gigabitEthernet 1/0/5

13.15 show ip dhcp snooping information interface

该命令用于显示对应千兆网口/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 [**ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

参数

port —— 交换机端口号。

port-channel-id —— 端口通道的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/链路聚合的DHCP侦听的option 82功能的配置信息：

TL-ST5416#show ip dhcp snooping information interface

第14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。

14.1 ip arp inspection vlan

该命令用于根据 VLAN 开启 ARP 防护功能，它的 no 命令用于禁用 ARP 防护功能。

命令

ip arp inspection vlan *vlan-list* [**logging**]

no ip arp inspection vlan

参数

vlan-list —— 要开启 ARP 防护功能的 vlan，可使用“-”表示区间，并用“,”隔开，例如：vlan 3-5，8。

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 vlan 3-5 上的 ARP 过滤，并开启 log 功能：

```
TL-ST5416(config-if-range)#ip arp inspection vlan 3-5 logging
```

14.2 ip arp inspection validate

该命令用于开启 ARP 报文检查功能，它的 no 命令用于关闭该功能。

命令

ip arp inspection validate { src-mac | dst-mac | ip }

no ip arp inspection validate

参数

src-mac | dst-mac | ip —— 选择要开启的防护类型。包括报文中的 send mac 与 src mac 不符合，dst mac 与 dest mac 不符合，或者 IP 字段非法。

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

开启 Src Mac 检查：

```
TL-ST5416(config)#ip arp inspection validate src-mac
```

14.3 ip arp inspection trust

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 ten-gigabitEthernet / interface range ten-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 为 ARP 防护的信任端口：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# ip arp inspection trust
```

14.4 ip arp inspection limit-rate

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* [**burst-interval** *seconds*] | **none** }

no ip arp inspection limit-rate

参数

value —— 超速速率值，取值范围 1-300，单位 pps（packet/second）。默认值为 15。

seconds —— 设置端口可超速的时间，取值范围 1-15。

模式

接口配置模式(interface ten-gigabitEthernet / interface range ten-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 5 不限速：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/5
TL-ST5416(config-if)# ip arp inspection limit-rate none
```

14.5 ip arp inspection recover

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/5
TL-ST5416(config-if)# ip arp inspection recover
```

14.6 show ip arp inspection

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：

```
TL-ST5416(config)# show ip arp inspection
```

14.7 show ip arp inspection interface

该命令用于显示 ARP 防护端口配置信息。

命令

show ip arp inspection interface [**ten-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

显示所有端口的 ARP 防护配置信息：

TL-ST5416(config)# show ip arp inspection interface

显示端口 2 的配置：

TL-ST5416(config)# show ip arp inspection interface ten-gigabitEthernet 1/0/2

14.8 show ip arp inspection statistics

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：

TL-ST5416(config)# show ip arp inspection statistics

14.9 clear ip arp inspection statistics

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

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

对 ARP 非法报文统计进行清零：

```
TL-ST5416(config)# clear ip arp inspection statistics
```

第15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。

15.1 ip verify source

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 ten-gigabitEthernet / interface range ten-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：

TL-ST5416(config)#interface range ten-gigabitEthernet 1/0/5-10

TL-ST5416(config-if-range)#ip verify source sip+mac

15.2 show ip verify source

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：

```
TL-ST5416(config)#show ip verify source
```

第16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。

16.1 ip dos-prevent

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：

```
TL-ST5416 (config)# ip dos-prevent
```

16.2 ip dos-prevent type

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Ping flooding攻击防护功能：

```
TL-ST5416 (config)# ip dos-prevent type ping-flood
```

16.3 show ip dos-prevent

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：

```
TL-ST5416 (config)# show ip dos-prevent
```

第17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。

17.1 logging buffer

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：

```
TL-ST5416 (config)# logging buffer
```

17.2 logging buffer level

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7，表示所有日志信息都保存到日志缓冲区。

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6：

```
TL-ST5416 (config)# logging buffer leverl 6
```

17.3 logging file flash

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：

```
TL-ST5416 (config)# logging file flash
```

17.4 logging file flash frequency

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：

```
TL-ST5416 (config)# logging file flash frequency 10
```

17.5 logging file flash level

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*

no logging file flash

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2，表示允许级别为0~2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：

```
TL-ST5416 (config)# logging file flash 7
```

17.6 logging host index

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：

```
TL-ST5416 (config)# logging host index 2 192.168.0.148 5
```

17.7 logging monitor

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：

```
TL-ST5416 (config)# # no logging monitor
```

17.8 logging monitor level

该命令用于限制登录到终端设备的消息，系统日志不高于设置阈值电平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。

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 0~8 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

设置严重级别为 7：

```
TL-ST5416 (config)# logging monitor level 7
```

17.9 clear logging

该命令用于清空指定unit或者整个堆叠的日志缓冲区或日志文件中的信息。

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

清空堆叠中所有交换机的当前日志缓冲区中的系统日志信息：

```
TL-ST5416 (config)# clear logging buffer
```

17.10 show logging local-config

该命令用于显示本地日志（包括日志缓冲区和日志文件）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：

```
TL-ST5416 (config)# show logging local-config
```

17.11 show logging loghost

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，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：

```
TL-ST5416 (config)# show logging loghost 2
```

17.12 show logging buffer

该命令用于显示某堆叠成员或者整个堆叠的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*] [**unit** *unit-id*]

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，缺省时显示日志缓冲区中的所有日志信息。

unit-id —— 指定堆叠成员以显示它的日志缓冲区中的日志信息。缺省时，整个堆叠的交换机的日志缓冲区中的日志信息都将被显示。

模式

特权模式和所有配置模式

特权要求

无

示例

显示堆叠中unit2的日志缓冲区中级别为0-5的日志信息：

```
TL-ST5416 (config)# show logging buffer level 5 unit 2
```

17.13 show logging flash

该命令用于显示某堆叠成员或者整个堆叠的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*] [**unit** *unit-id*]

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。

unit-id —— 指定堆叠成员以显示它的日志文件中的日志信息。缺省时，整个堆叠的交换机的日志文件中的日志信息都将被显示。

模式

特权模式和所有配置模式

特权要求

无

示例

显示堆叠中unit2的日志文件中级别为0~3的日志信息：

```
TL-ST5416 (config)# show logging flash level 3 unit 2
```

第18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。

18.1 ip ssh server

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：

```
TL-ST5416 (config)# ip ssh server
```

18.2 ip ssh version

该命令用于启用SSH的协议版本，它的no命令用于禁用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：

TL-ST5416 (config)# ip ssh version v2

18.3 ip ssh algorithm

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 } ——指定的 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：

TL-ST5416 (config)# ip ssh algorithm AES128-CBC

18.4 ip ssh timeout

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：

TL-ST5416 (config)# ip ssh timeout 30

18.5 ip ssh max-client

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：

TL-ST5416 (config)# ip ssh max-client 3

18.6 ip ssh download

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256~3072比特的SSH公钥。

ip-addr —— TFTP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

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：

TL-ST5416 (config)# ip ssh download v1 ssh-key **ip-address** 192.168.0.148

18.7 remove public-key

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

删除交换机中的SSH-1公钥：

TL-ST5416# remove public-key v1

18.8 show ip ssh

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：

TL-ST5416 (config)# show ip ssh

第19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。

19.1 dot1x system-auth-control

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。

命令

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：

```
TL-ST5416 (config)# dot1x system-auth-control
```

19.2 dot1x handshake

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：

```
TL-ST5416(config)# dot1x  handshake
```

19.3 dot1x auth-method

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：

```
TL-ST5416 (config)# dot1x auth-method pap
```

19.4 dot1x accounting

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：

```
TL-ST5416 (config)# dot1x accounting
```

19.5 dot1x guest-vlan (global)

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：

```
TL-ST5416 (config)# dot1x guest-vlan 5
```

19.6 dot1x quiet-period

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

模式

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：

```
TL-ST5416 (config)# dot1x quiet-period
```

开启IEEE 802.1X静默功能，静默时长设置为5秒：

TL-ST5416 (config)# dot1x quiet-period 5

19.7 dot1x timeout supplicant-timeout

该命令用于配置静默时长、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 supplicant-timeout *time*

no timeout supplicant-timeout

参数

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

配置客户端响应超时时长为 9 秒：

TL-ST5416 (config)# dot1x timeout supplicant-timeout 9

19.8 dot1x max-reauth-req

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：

```
TL-ST5416 (config)# dot1x max-reauth-req 5
```

19.9 dot1x

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 ten-gigabitEthernet / interface range ten-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IEEE 802.1X特性：

```
TL-ST5416 (config)# interface ten-gigabitEthernet 1/0/1
TL-ST5416(config-if)# dot1x
```

19.10 dot1x guest-vlan (interface)

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，详见**dot1x port-method**。

命令

dot1x guest-vlan

no dot1x guest-vlan

模式

接口配置模式(interface ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416 (config)# interface ten-gigabitEthernet 1/0/2
```

TL-ST5416(config-if)# dot1x guest-vlan

19.11 dot1x port-control

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 ten-gigabitEthernet / interface range ten-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5的接入控制模式为强制已认证：

TL-ST5416 (config)# interface ten-gigabitEthernet 1/0/5

TL-ST5416(config-if)# dot1x port-control authorized-force

19.12 dot1x port-method

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 ten-gigabitEthernet / interface range ten-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5的接入控制类型为基于Port认证：

```
TL-ST5416 (config)# interface ten-gigabitEthernet 1/0/5
TL-ST5416(config-if)# dot1x port-method port-based
```

19.13 show dot1x global

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：

```
TL-ST5416 (config)# show dot1x global
```

19.14 show dot1x interface

该命令用于显示801.X端口配置信息。

命令

show dot1x interface [**ten-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801.X端口配置信息：

TL-ST5416 (config)# show dot1x interface

显示端口5的802.1X配置信息：

TL-ST5416 (config)# show dot1x interface ten-gigabitEthernet 1/0/5

第20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。

20.1 mac address-table static

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 ten-gigabitEthernet** *port*

no mac address-table static { *mac-addr* | **vid** *vid* | *mac-addr* **vid** *vid* | **interface ten-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：

TL-ST5416 (config)# mac address-table static 00:02:58:4f:6c:23 **vid** 1 **interface ten-gigabitEthernet** 1/0/1

20.2 mac address-table aging-time

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：

TL-ST5416 (config)# mac address-table aging-time 500

20.3 mac address-table filtering

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：

TL-ST5416 (config)# mac address-table filtering 00:1e:4b:04:01:5d **vid** 1

20.4 mac address-table notification

该命令用于MAC地址表通知的全局设置。

命令

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

参数

global-status enable | disable ——打开/关闭全局通知功能。

table-full-status enable | disable —— 打开/关闭MAC阈值通知。打开此功能时，当达到或超过交换机地址阈值时，会产生一条SNMP通知并发送至网络管理系统。

interval *time* —— 设置两个通知之间的间隔时间，可设置1-1000秒。默认值为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

启用全局MAC地址通知和地址表满载通知，设置通知发送间隔为2秒：

TL-ST5416 (config) # mac address-table notification global-status enable **table-full-status** enable **interval** 2

20.5 mac address-table notification (interface)

该命令用于配置基于端口的MAC地址更改通知。

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 —— 打开/关闭学习模式变化通知功能。打开此功能时，当端口的学习模式发生变化，会产生一条SNMP通知并发送至网络管理系统。

exceed-max-learned enable | disable —— 打开/关闭超过最大地址学习数通知功能。打开此功能时，当端口上的MAC地址达到或超过最大地址学习数时，会产生一条SNMP通知并发送至网络管理系统。

new-mac-learned enable | disable —— 打开/关闭新地址学习通知功能。打开此功能时，当端口学习到一条新的MAC地址时，会产生一条SNMP通知并发送至网络管理系统。

模式

接口配置模式(interface ten-gigabitEthernet / interface range ten-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

启用全局MAC地址通知，同时启用端口2的学习模式变化通知功能：

```
TL-ST5416 (config) # mac address-table notification global-status enable
TL-ST5416 (config) # interface ten-gigabitEthernet 1/0/2
TL-ST5416 (config) # mac address-table notification learn-mode-change enable
```

20.6 mac address-table max-mac-count

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。它的no命令用于恢复默认配置。

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0~1024，缺省时为1024。

mode —— 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 —— 是否启用端口安全功能，包括三种模式，默认为禁用（disable）：

- forward：当已学习的MAC地址数到达阈值时，数据包将向前传递，但是不会被学习。
- drop：当已学习的MAC地址数到达阈值时，数据包将被丢弃。
- disable：禁用该端口端口安全功能。

模式

接口配置模式(interface ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/1
TL-ST5416(config-if)# mac address-table max-mac-count max-number 30 mode static status forward
```

20.7 mac address-table security

该命令用于对指定VLAN的最大地址学习数目进行配置。它的no命令用于恢复默认配置。

命令

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

no mac address-table security vid *vid*

参数

vid —— 设置需要配置MAC地址表的VLAN ID。

number —— 配置MAC地址表阈值，取值范围0~16383。

forward | drop | disable —— 选择当学习的MAC地址超过设定阈值时，对于新数据包的处理模式：

- forward: 当已学习的MAC地址数到达阈值时，数据包可以被转发，但是不会被学习。
- drop: 当已学习的MAC地址数到达阈值时，数据包将被丢弃。
- disable: 关闭VLAN安全功能。

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的最大MAC地址学习数目为1000，当该VLAN学习到的MAC地址数量达到1000个时，新的数据包将被丢弃：

```
TL-ST5416 (config) # mac address-table security vid 2 max-learn 1000 drop
```

20.8 show mac address-table

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：

```
TL-ST5416 (config)# show mac address-table
```

20.9 clear mac address-table

该用于清除指定的地址项。

命令

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

参数

dynamic | static | filtering —— 所选择的条目类型

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

清除所有静态地址项的信息：

```
TL-ST5416 (config)# clear mac address-table static
```

20.10 show mac address-table aging-time

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：

```
TL-ST5416 (config)# show mac address-table aging-time
```

20.11 show mac address-table max-mac-count

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 ten-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

显示端口5的安全配置信息：

```
TL-ST5416 (config)# show mac address-table max-mac-count interface ten-gigabitEthernet 1/0/5
```

20.12 show mac address-table interface

该命令用于显示端口的地址配置信息。

命令

show mac address-table interface { **ten-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的地址配置信息：

```
TL-ST5416 (config)# show mac address-table interface ten-gigabitEthernet 1/0/1
```

20.13 show mac address-table count

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

显示整个堆叠中的地址表数量，按VLAN排序：

```
TL-ST5416 (config)# show mac address-table count
```

20.14 show mac address-table address

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 { ten-gigabitEthernet** port | **port-channel** *lagid* } | **vid** *vlan-id*]

参数

mac-addr —— 指定MAC地址。

port —— 指定端口号。

lagid —— 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：

TL-ST5416 (config)#show mac address-table address 00:00:00:23:00:00 **vid** 1

20.15 show mac address-table vlan

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的地址表信息：

TL-ST5416 (config)# show mac address-table vlan 1

20.16 show mac address-table notification

该命令用于显示全局或某一端口的MAC通知。

命令

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

参数

all —— 显示所有端口的通知信息。

port —— 显示指定端口的通知信息。

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有端口的通知信息：

TL-ST5416 (config) # show mac address-table notification all

20.17 show mac address-table security

该命令用于显示指定VLAN的MAC地址安全配置信息。

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的MAC地址安全配置：

TL-ST5416 (config) # show mac address-table security vid 1

第21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。

21.1 system-time manual

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。

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03/20/2013 17:30:35：

TL-ST5416 (config)# system-time manual 03/20/2013-17:30:35

21.2 system-time ntp

该命令用于设置交换机从网络中NTP服务器上获取UTC时间。

命令

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

参数

time-zone —— 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：

TL-ST5416 (config)# system-time ntp UTC-12:00 133.100.9.2 139.79.100.163 11

21.3 system-time dst predefined

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]

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：

TL-ST5416 (config)# system-time dst predefined Europe

21.4 system-time dst date

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。

命令

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

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4月1日0点到10月1日0点：

TL-ST5416 (config)# system-time dst date Apr 1 00:00 Oct 1 00:00

21.5 system-time dst recurring

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：

TL-ST5416 (config)# system-time dst recurring first Sun May 02:00 last Sun Oct 02:00

21.6 hostname

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，1~17 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

设置设备名称为 TP-LINK：

TL-ST5416 (config)# hostname TP-LINK

21.7 location

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 GUANGZHOU：

```
TL-ST5416 (config)# location GUANGZHOU
```

21.8 contact-info

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，默认为 www.tp-link.com.cn。

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.tp-link.com：

```
TL-ST5416 (config)# contact-info www.tp-link.com
```

21.9 reset

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：

```
TL-ST5416# reset
```

21.10 reboot

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。

命令

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：

```
TL-ST5416# reboot
```

21.11 reboot-schedule

该命令用于设置交换机在指定时间重启。使用 reboot-schedule cancel 命令可删除设置。

命令

reboot-schedule at *time* [*date*] [**save_before_reboot**]

reboot-schedule in *interval* [**save_before_reboot**]

reboot-schedule cancel

参数

time—— 指定交换机重启时间。

date—— 指定交换机重启日期，必须在 30 天以内。

save_before_reboot —— 在交换机重启前保存配置文件。

interval—— 指定交换机在一段时间之后重启。可设置 1-43200 分钟。

cancel—— 删除交换机重启的相关设置。

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

用户指南

在**reboot-schedule at** *time* [*date*] [**save_before_reboot**]命令中，如果date缺省，那么如果time在此条命令执行之前，则交换机会在第二天指定的time时间重启，如果time在此条命令执行之后，则交换机会在稍后时间到达time时重启。

示例

重新启动交换机：

```
TL-ST5416# reboot
```

21.12 copy running-config startup-config

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

保存堆叠系统中 unit1 的当前配置为启动配置文件：

TL-ST5416# copy running-config startup-config

21.13 copy startup-config tftp

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：

TL-ST5416# 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：

TL-ST5416# copy startup-config tftp ip-address fe80::1234 **filename** config

21.14 copy tftp startup-config

该命令用于通过 TFTP 方式导入配置文件。

命令

copy tftp startuup-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：

TL-ST5416# 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：

TL-ST5416# copy tftp startup-config ip-address fe80::1234 **filename** config

21.15 boot application

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 | image2 } { 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，image.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 配置为堆叠中所有成员的启动镜像：

TL-ST5416 (config)# boot application filename image2 startup

21.16 remove backup-image

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

删除堆叠系统中所有成员的备份镜像：

```
TL-ST5416# remove backup-image
```

21.17 firmware upgrade

该命令用于通过 TFTP 方式升级系统文件。

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 —— 指定升级文件的名称。

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 服务器升级堆叠系统的所有成员，升级文件名为 firmware.bin，重启交换机：

```
TL-ST5416# 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 服务器升级堆叠系统的所有成员，升级文件名为 firmware.bin，交换机不重启：

```
T1700X-16TS# 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
```

21.18 ping

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IPv4。

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：

TL-ST5416# 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：

TL-ST5416# ping fe80::1234 **–n** 8 **–l** 512

21.19 tracert

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_address* [*maxHops*]

参数

ip_address —— 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：

```
TL-ST5416# 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：

```
TL-ST5416# tracert fe80::1234 20
```

21.20 show system-info

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：

```
TL-ST5416# show system-info
```

21.21 show image-info

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 [*unitid*]

参数

unitid —— 可选参数，用于指定需要显示系统镜像文件信息的堆叠成员。若不指定，则显示所有堆叠成员的镜像文件信息。

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

显示堆叠系统中所有成员的文件系统中的镜像文件信息：

```
TL-ST5416 (config)# show image-info
```

21.22 show running-config

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

显示堆叠系统所有成员的当前配置信息：

```
TL-ST5416# show running-config
```

21.23 show startup-config

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

显示堆叠系统所有成员的当前配置信息：

```
TL-ST5416# show startup-config
```

21.24 show system-time

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：

```
TL-ST5416# show system-time
```

21.25 show system-time dst

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：

```
TL-ST5416# show system-time dst
```

21.26 show system-time ntp

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：

```
TL-ST5416# show system-time ntp
```

21.27 show cable-diagnostics interface ten-gigabitEthernet

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 ten-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：

```
TL-ST5416# show cable-diagnostics interface ten-gigabitEthernet 1/0/3
```

21.28 show cpu-utilization

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

显示堆叠系统所有成员的CPU使用率信息：

```
TL-ST5416#show cpu-utilization
```

21.29 show memory-utilization

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

显示堆叠系统所有成员的内存使用率信息：

```
TL-ST5416#show memory-utilization
```

第22章 IPv6 地址配置命令

IPv6 地址配置命令需在接口模式下设置，包括端口，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。

22.1 ipv6 enable

该命令用于开启全局 IPv6 功能，它的 no 命令用于禁用全局 IPv6 功能。

在进行 IPv6 地址配置管理之前，必须先开启 IPv6 功能，交换机默认开启 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：

```
TL-ST5416 (config)# interface vlan 1

TL-ST5416 (config-if)# ipv6 enable
```

22.2 ipv6 address autoconfig

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：

```
TL-ST5416(config)# interface vlan 1
TL-ST5416(config-if)# ipv6 address autoconfig
```

22.3 ipv6 address dhcp

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：

```
TL-ST5416(config)# interface vlan 1
TL-ST5416(config-if)# ipv6 address dhcp
```

22.4 ipv6 address link-local

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：

```
TL-ST5416(config)# interface vlan 1
TL-ST5416(config-if)# ipv6 address fe80::1234 link-local
```

22.5 ipv6 address ra

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：

```
TL-ST5416(config)# interface vlan 1
TL-ST5416(config-if)# ipv6 address ra
```

22.6 ipv6 address

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：

```
TL-ST5416(config)# interface vlan 1
TL-ST5416(config-if)# ipv6 address 3001::1/64
```

22.7 ipv6 address eui-64

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：

```
TL-ST5416(config)# interface vlan 1
TL-ST5416(config-if)# ipv6 address 3ffe::/64 eui-64
```

22.8 show ipv6 interface

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：

```
TL-ST5416(config)# show ipv6 interface
```

第23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。

23.1 interface ten-gigabitEthernet

该命令用于进入接口配置命令模式，对单个万兆以太网端口进行配置。

命令

interface ten-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：

TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2

23.2 interface range ten-gigabitEthernet

该命令用于进入接口配置命令模式，对多个万兆以太网端口进行同时配置。

命令

interface range ten-gigabitEthernet *port-list*

参数

port-list —— 要配置的万兆以太网端口列表。

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 ten-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：

TL-ST5416(config)# interface ten-gigabitEthernet interface range ten-gigabitEthernet 1/0/1-3,1/0/6-7,1/0/9

23.3 description

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 ten-gigabitEthernet / interface range ten-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5添加端口描述Port_5：

TL-ST5416(config)# interface ten-gigabitEthernet 1/0/5

TL-ST5416(config-if)# description Port_5

23.4 shutdown

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 ten-gigabitEthernet / interface range ten-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3：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# shutdown
```

23.5 flow-control

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 ten-gigabitEthernet / interface range ten-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3的流量控制：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# flow-control
```

23.6 duplex

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。缺省时，万兆口为自协商模式。

模式

接口配置模式（interface ten-gigabitEthernet / interface range ten-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3为全双工模式：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# duplex full
```

23.7 jumbo

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 ten-gigabitEthernet / interface range ten-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3：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# jumbo
```

23.8 speed

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 { 100 | 1000 | 10000 | auto }

no speed

参数

100 | 1000 | 10000 | auto —— 端口速率模式，分别为100M、1000M、10000M和自协商模式。缺省时万兆口工作在自协商模式。

模式

接口配置模式（interface ten-gigabitEthernet / interface range ten-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3的速率模式为1000M：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# speed 1000
```

23.9 storm-control pps

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 ten-gigabitEthernet / interface range ten-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5的风暴控制模式为pps：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/5
```

TL-ST5416(config-if)# storm-control pps

23.10 storm-control

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 } { *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 10000000 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 14880000 每秒。

模式

接口配置模式（interface ten-gigabitEthernet / interface range ten-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：

TL-ST5416(config)# interface ten-gigabitEthernet 1/0/5

TL-ST5416(config-if)# storm-control broadcast kbps 1000

23.11 bandwidth

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1-10000000kbps。

egress-rate —— 配置出口带宽限制，单位为kbps。取值范围为1-10000000kbps。

模式

接口配置模式（interface ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/5
TL-ST5416(config-if)# bandwidth ingress 5120 egress 1024
```

23.12 clear counters

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 [**ten-gigabitEthernet** *port*] [**port-channel** *lagid*]

参数

port —— 以太网端口。

lagid —— 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：

```
TL-ST5416(config)# clear counters
```

23.13 show interface status

该命令用于显示以太网端口和LAG的连接状态。

命令

show interface status [**ten-gigabitEthernet** *port*] [**port-channel** *lagid*]

参数

port —— 要显示连接状态的以太网端口。

lagid —— 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：

```
TL-ST5416(config)# show interface status
```

显示端口1连接状态：

```
TL-ST5416(config)# show interface status ten-gigabitEthernet 1/0/1
```

23.14 show interface counters

该命令用于显示以太网端口和LAG的统计信息。

命令

show interface counters [**ten-gigabitEthernet** *port*] [**port-channel** *lagid*]

参数

port —— 要显示统计信息的以太网端口。

lagid —— 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：

```
TL-ST5416(config)# show interface counters
```

显示以太网端口2的统计信息：

TL-ST5416(config)# show interface counters ten-gigabitEthernet 1/0/2

23.15 show interface configuration

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 [**ten-gigabitEthernet** *port*] [**port-channel** *lagid*]

参数

port —— 要显示配置信息的以太网端口。

lagid —— 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：

TL-ST5416(config)# show interface configuration

显示以太网端口2的配置信息：

TL-ST5416# show interface configuration ten-gigabitEthernet 1/0/2

23.16 show storm-control

该命令用于显示端口的风暴抑制信息。

命令

show storm-control interface [**ten-gigabitEthernet** *port-list*] [**port-channel** *lagid-list*]

参数

port-list —— 要显示风暴抑制信息的端口号/端口列表。

lagid-lsit —— 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：

```
TL-ST5416(config)# show storm-control interface ten-gigabitEthernet 1/0/4-7
```

23.17 show bandwidth

该命令用于显示端口的带宽限制信息。

命令

show bandwidth interface [**ten-gigabitEthernet** *port-list*] [**port-channel** *lagid-list*]

参数

port-list —— 要显示带宽限制信息的端口号/端口列表。

lagid-lsit —— 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的带宽限制信息：

```
TL-ST5416(config)# show bandwidth interface ten-gigabitEthernet 1/0/4
```

第24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。

24.1 qos

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

参数

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/5
TL-ST5416(config-if)# qos 3
```

24.2 qos dscp

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：

```
TL-ST5416(config)# qos dscp
```

24.3 qos queue cos-map

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-TC1，1-TC0，2-TC2，3-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：

```
TL-ST5416(config)# qos queue cos-map 5 2
```

24.4 qos queue dscp-map

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-pri* }

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-pri —— 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：

```
TL-ST5416(config)# qos queue dscp-map 10-12 2
```

24.5 qos queue mode

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。TC0到TC7的权重比值是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属于sp组；TC0到TC6属于wrr组，权重比是1：2：4：8：16：32：64。这样在调度的时候首先是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：

```
TL-ST5416(config)# qos queue mode wrr
```

24.6 qos queue weight

该命令用于调度方式指定为 WRR 或 SP + WRR 后配置每个队列的权值。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 和权重值为 0 的队列属于 SP 组；非 0 权重值的队列属于 WRR 组。在 SP + WRR 调度模式中，SP 组队列

优先调度（优先级 TC7>TC6>TC5>TC4>TC3>TC2>TC1>TC0）。当 SP 组没有数据包发送，WRR 组会根据每个队列的权重值的比例占用带宽。TC0、TC1、TC2、TC3、TC4、TC5 和 TC6 默认权重值分别为 1、2、4、8、16、 32 和 64，而 TC 7 的权重值为 0，不可配置。

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：：

```
TL-ST5416(config)# qos queue mode wrr
TL-ST5416(config)# qos queue weight 0 4
TL-ST5416(config)# qos queue weight 1 7
TL-ST5416(config)# qos queue weight 2 15
TL-ST5416(config)# qos queue weight 3 24
```

24.7 show qos interface

该命令用于显示基于端口优先级的配置信息。

命令

show qos interface [**ten-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-lsit —— 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：

```
TL-ST5416# show qos interface
```

显示以太网端口1-4的QoS配置信息：

```
TL-ST5416# show qos interface ten-gigabitEthernet 1/0/1-4
```

24.8 show qos cos-map

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：

```
TL-ST5416# show qos cos-map
```

24.9 show qos dscp-map

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：

```
TL-ST5416# show qos dscp-map
```

24.10 show qos queue mode

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：

```
TL-ST5416# show qos queue mode
```

24.11 show qos status

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：

```
TL-ST5416# show qos status
```

第25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。

25.1 monitor session destination interface

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 ten-gigabitEthernet** *port*

no monitor session *session_num* **destination interface ten-gigabitEthernet** *port*

no monitor session *session_num*

参数

session_num —— 监控组组号。取值范围1-4。

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：

```
TL-ST5416(config)# monitor session 1 destination interface ten-gigabitEthernet 1/0/1
```

删除端口2为监控组1的监控端口：

```
TL-ST5416(config)# no monitor session 1 destination interface ten-gigabitEthernet 1/0/2
```

删除监控组1：

```
TL-ST5416(config)# no monitor session 1
```

25.2 monitor session source interface

该命令用于设置被监控端口和LAG，它的no命令用于删除相应的被监控端口和LAG。

命令

monitor session *session_num* **source interface** { **ten-gigabitEthernet** *port-list* | **port-channel** *lagid-list* } *mode*

no monitor session *session_num* **source interface** { **ten-gigabitEthernet** *port-list* | **port-channel** *lagid-list* } *mode*

参数

session_num —— 监控组组号。取值范围1-4。

port-list —— 被监控端口列表，可选择一个或多个端口。

lagid-list —— 汇聚组列表，可选择一个或多个汇聚组。

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：

```
TL-ST5416(config)# monitor session 1 source interface ten-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：

```
TL-ST5416(config)# no monitor session 1 source interface ten-gigabitEthernet 1/0/4 rx
```

25.3 show monitor session

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。取值范围1-4。

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：

```
TL-ST5416# show monitor session 1
```

第26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。

26.1 port isolation

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 { [**te-forward-list** *te-forward-list*] [**po-forward-list** *po-forward-list*] }

no port isolation

参数

te-forward-list —— 万兆转发端口列表，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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/5
TL-ST5416(config-if)# port isolation te-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# no port isolation
```

26.2 show port isolation interface

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 [**ten-gigabitEthernet** *port* | **port-channel** *lagid*]

参数

port —— 选择希望查看转发端口列表信息的端口号。

lagid —— 选择希望查看转发端口列表信息的汇聚组号，取值范围1-14。

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的转发端口列表：

TL-ST5416# show port isolation interface ten-gigabitEthernet 1/0/2

显示全部端口和LAG列表的转发端口列表：

TL-ST5416# show port isolation interface

第27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。

27.1 loopback-detection (global)

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：

```
TL-ST5416(config)# loopback-detection
```

27.2 loopback-detection interval

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：

TL-ST5416(config)# loopback-detection interval 50

27.3 loopback-detection recovery-time

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：

TL-ST5416(config)# loopback-detection recovery-time 3

27.4 loopback-detection (interface)

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 ten-gigabitEthernet / interface range ten-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：

TL-ST5416(config)# interface range ten-gigabitEthernet 1/0/1-3

TL-ST5416(config-if-range)# loopback-detection

27.5 loopback-detection config

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# loopback-detection config process-mode port-based recovery-mode manual
```

27.6 loopback-detection recover

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# loopback-detection recover
```

27.7 show loopback-detection global

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：

```
TL-ST5416# show loopback-detection global
```

27.8 show loopback-detection interface

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 [**ten-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：

```
TL-ST5416# 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：

```
TL-ST5416# show loopback-detection interface ten-gigabitEthernet 1/0/5
```

第28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。

28.1 time-range

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：

```
TL-ST5416(config)# time-range tSeg1
```

28.2 absolute

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 01/01/2000。

end-date —— 绝对模式下的结束日期，形式为 MM/DD/YYYY，缺省时为 01/01/2000。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：

```
TL-ST5416(config)# time-range tSeg1
TL-ST5416(config-time-range)# absolute start 05/05/2012 end 10/05/2012
```

28.3 periodic

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

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 —— 添加时间片段，形式为 HH:MM-HH:MM。

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：

```
TL-ST5416(config)# time-range tSeg1
TL-ST5416(config-time-range)# periodic week-date off-day time-slice1
08:30-12:00
```

28.4 holiday

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：

```
TL-ST5416(config)# time-range tSeg1
TL-ST5416(config-time-range)# holiday
```

28.5 holiday(global)

该命令用于创建 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

holiday *name* **start-date** *start-date* **end-date** *end-date*

no 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

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：

```
TL-ST5416(config)# holiday nationalday start-date 10/01 end-date 10/03
```

28.6 access-list create

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。

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：

TL-ST5416(config)# access-list create 523

28.7 access-list bind acl

该命令之前用于将 ACL 直接绑定在端口或者 VLAN 上。

命令

access-list bind acl *acl-id*

no access-list bind acl *acl-id*

参数

acl id ——要绑定到 VLAN 的 access-list 名称。

模式

接口模式

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

在端口 2 上直接绑定 ACL 100

TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2

TL-ST5416(config-if)# access-list bind acl 100

28.8 mac access-list

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：

```
TL-ST5416(config)# mac access-list 23
```

28.9 access-list standard

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。

op —— 交换机对满足匹配规则的数据包的处理方式。其中 *deny* 表示丢弃数据包；permit 表示转发数据包。缺省时为 permit。

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 120 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：

TL-ST5416(config)# access-list create 120

TL-ST5416(config)# access-list standard 120 **rule** 10 permit **sip** 192.168.0.100 **smask** 255.255.255.0 **tseg** tSeg1

28.10 access-list extended

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*] [**dscp** *dscp*] [**s-port** *s-port*] [**d-port** *d-port*] [**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。

op —— 交换机对满足匹配规则的数据包的处理方式。其中 ***deny*** 表示丢弃数据包；permit 表示转发数据包。缺省时为 permit。

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。

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。

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 220 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：

TL-ST5416(config)# access-list create 220

TL-ST5416(config)# access-list extended 220 **rule** 10 permit **sip** 192.168.0.100 **smask** 255.255.255.0 **tseg** tSeg1

28.11 access-list ipv6

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*]

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 —— 丢弃数据包。

permit —— 转发数据包。此为缺省值。

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。

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：

```
TL-ST5416(config)# access-list create 3600
TL-ST5416(config)# access-list ipv6 3600 rule 10 permit sip 3001::1 sip-mask ffff:ffff:ff00:00ff
```

28.12 rule

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 —— 当前添加的规则的 ID 号。

op —— 交换机对满足匹配规则的数据包的处理方式。其中 deny 表示丢弃数据包；permit 表示转发数据包。缺省时为 permit。

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 号，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：

```
TL-ST5416(config)# mac access-list 20
TL-ST5416(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 tSeg1
```

28.13 access-list policy name

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：

```
TL-ST5416(config)# access-list policy name policy1
```

28.14 access-list policy action

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：

TL-ST5416(config)# access-list policy action policy1 120

28.15 redirect interface

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 { **ten-gigabitEthernet** *port* }

no redirect interface { **ten-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：

TL-ST5416(config)# access-list policy action policy1 120

TL-ST5416(config-action)# redirect interface ten-gigabitEthernet 1/0/2

28.16 s-condition

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 }

no **s-condition**

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：

TL-ST5416(config)# access-list policy action policy1 120

TL-ST5416(config-action)# s-condition rate 1000 **osd** discard

28.17 s-mirror

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 { **ten-gigabitEthernet** *port* }

no s-mirror interface { **ten-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：

TL-ST5416(config)# access-list policy action policy1 120

TL-ST5416(config-action)# s-mirror interface ten-gigabitEthernet 1/0/2

28.18 qos-remark

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 0~3。

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：

TL-ST5416(config)# access-list policy action policy1 120

TL-ST5416(config-action)# qos-remark dscp 30 **priority** 2

28.19 access-list bind acl(interface)

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# access-list bind acl 100
```

28.20 access-list bind acl(vlan)

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：

```
TL-ST5416(config)# interface vlan 2
TL-ST5416(config-if)# access-list bind acl 100
```

28.21 access-list bind (interface)

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 ten-gigabitEthernet / interface range ten-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policy1绑定到端口2：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# access-list bind policy1
```

28.22 access-list bind (vlan)

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：

```
TL-ST5416(config)# interface vlan 2
TL-ST5416(config-if)# access-list bind policy1
```

28.23 show time-range

该命令用于显示所有时间段的配置。

命令

show time-range

模式

特权模式和所有配置模式

特权要求

无

示例

显示所有时间段配置：

```
TL-ST5416# show time-range
```

28.24 show holiday

该命令用于显示所有已定义的节假日。

命令

show holiday

模式

特权模式和所有配置模式

特权要求

无

示例

显示节假日设置：

```
TL-ST5416# show holiday
```

28.25 show access-list

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：

TL-ST5416# show access-list 20

28.26 show access-list policy

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的描述。

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：

TL-ST5416# show access-list policy policy1

28.27 show access-list bind

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：

TL-ST5416# show access-list bind

第29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。

29.1 debug spanning-tree

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 }

参数

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：

```
TL-ST5416(config)# debug spanning-tree all
```

29.2 spanning-tree (global)

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：

```
TL-ST5416(config) # spanning-tree
```

29.3 spanning-tree mode

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：

```
TL-ST5416(config)# spanning-tree mode mstp
```

29.4 spanning-tree mst configuration

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：

```
TL-ST5416(config)# spanning-tree mst configuration
TL-ST5416(config-mst)#
```

29.5 spanning-tree mst instance

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：

```
TL-ST5416(config)# spanning-tree mst instance 1 priority 4096
```

29.6 spanning-tree priority

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：

```
TL-ST5416(config)# spanning-tree priority 4096
```

29.7 spanning-tree tc-defend

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：

```
TL-ST5416(config)# spanning-tree tc-defend threshold 30 period 10
```

29.8 spanning-tree hold-count

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：

```
TL-ST5416(config)# spanning-tree hold-count 8
```

29.9 spanning-tree timer

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：

```
TL-ST5416(config)# spanning-tree timer forward-time 16 hello-time 3 max-age 22
```

29.10 spanning-tree max-hops

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：

```
TL-ST5416(config)# spanning-tree max-hops 30
```

29.11 instance

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*]

参数

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：

```
TL-ST5416(config)# spanning-tree mst configuration
TL-ST5416(config-mst)# instance 1 vlan 1-100
```

移除实例1中的VLAN1-100映射：

```
TL-ST5416(config)# spanning-tree mst configuration
TL-ST5416(config-mst)# no instance 1
```

将实例1的VLAN1-50从VLAN1-100映射中移除：

```
TL-ST5416(config)# spanning-tree mst configuration
TL-ST5416(config-mst)# no instance 1 vlan 1-50
```

29.12 name

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*

参数

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：

```
TL-ST5416(config)# spanning-tree mst configuration
TL-ST5416(config-mst)# name region1
```

29.13 revision

该命令用于配置MST 实例的修订级别。

命令

revision *revision*

参数

revision —— 修订级别，范围为0~65535。

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：

```
TL-ST5416(config)# spanning-tree mst configuration
TL-ST5416(config-mst)# revision 100
```

29.14 spanning-tree (interface)

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config) # interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# spanning-tree
```

29.15 spanning-tree common-config

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/1
TL-ST5416(config-if)# spanning-tree common-config port-priority 64 ext-cost 100
int-cost 100 portfast enable point-to-point open
```

29.16 spanning-tree mst

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。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 ten-gigabitEthernet / interface range ten-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：

TL-ST5416(config)# interface ten-gigabitEthernet 1/0/1

TL-ST5416(config-if)# spanning-tree mst instance 1 **port-priority** 64 **cost** 2000

29.17 spanning-tree bpdufilter

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 ten-gigabitEthernet / interface range ten-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：

TL-ST5416 (config)# interface ten-gigabitEthernet 1/0/2

TL-ST5416(config-if)# spanning-tree bpdufilter

29.18 spanning-tree bpduguard

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# spanning-tree bpduguard
```

29.19 spanning-tree guard loop

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# spanning-tree guard loop
```

29.20 spanning-tree guard root

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# spanning-tree guard root
```

29.21 spanning-tree guard tc

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# spanning-tree guard tc
```

29.22 spanning-tree mcheck

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# spanning-tree mcheck
```

29.23 show spanning-tree active

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：

```
TL-ST5416# show spanning-tree active
```

29.24 show spanning-tree bridge

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：

```
TL-ST5416# show spanning-tree bridge
```

29.25 show spanning-tree interface

该命令用于显示生成树的端口配置信息。

命令

show spanning-tree interface [**ten-gigabitEthernet** *port* | **port-channel** *lagid*] [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。

lagid —— 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：

TL-ST5416# show spanning-tree interface

显示端口20的生成树信息：

TL-ST5416# show spanning-tree interface ten-gigabitEthernet 1/0/20

显示端口20的生成树模式：

TL-ST5416# show spanning-tree interface ten-gigabitEthernet 1/0/2 mode

29.26 show spanning-tree interface-security

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 [**ten-gigabitEthernet** *port* | **port-channel** *lagid*] [bpdufilter | bpduguard | loop | root | tc | tc-defend]

参数

port —— 要显示配置信息的端口号。

lagid —— 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：

TL-ST5416(config)# show spanning-tree interface-security

显示端口1的安全配置信息：

TL-ST5416(config)# show spanning-tree interface-security ten-gigabitEthernet 1/0/1

显示接口bpdu过滤器的安全配置信息：

TL-ST5416(config)# show spanning-tree interface-security bpdufilter

29.27 show spanning-tree mst

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** [**ten-gigabitEthernet** *port* | **port-channel** *lagid*]] }

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。

lagid —— 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：

TL-ST5416(config)# show spanning-tree mst configuration

显示MST实例1的相关信息：

TL-ST5416(config)# show spanning-tree mst instance 1

显示MST实例1的所有端口信息：

TL-ST5416(config)# show spanning-tree mst instance 1 **interface**

第30章 IGMP侦听配置命令

IGMP Snooping（Internet Group Management Protocol Snooping，IGMP侦听）是运行在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。

30.1 ip igmp snooping(global)

该命令用于IGMP全局配置，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：

```
TL-ST5416(config)# ip igmp snooping
```

30.2 ip igmp snooping (interface)

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# ip igmp snooping
```

30.3 ip igmp snooping rtime

该命令用于设置 IGMP 侦听全局路由器端口时间，它的 no 命令用于恢复默认值。默认的老化时间是 300 秒。

命令

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。

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令

示例

设置 IGMP 侦听全局路由器端口时间为 100 秒：

```
TL-ST5416(config-if-range)# ip igmp snooping rtime 100
```

30.4 ip igmp snooping mtime

该命令用于 IGMP 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

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。

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 IGMP 侦听全局成员端口时间为 100 秒：

```
TL-ST5416(config-if-range)# ip igmp snooping mtime 100
```

30.5 ip igmp snooping report-suppression

该命令用于 IGMP Report 报文抑制。启用时，对于每个组播组，只有第一个 IGMP 报告消息转发到第 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：

```
TL-ST5416(config-if-range)# ip igmp snooping report-suppression
```

30.6 ip igmp snooping immediate-leave

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

ip igmp snooping immediate-leave

no ip igmp snooping immediate-leave

模式

接口配置模式（interface ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# ip igmp snooping immediate-leave
```

30.7 ip igmp snooping drop-unknown

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：

```
TL-ST5416(config)# ip igmp snooping drop-unknown
```

30.8 ip igmp snooping last-listener query-inteval

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：

```
TL-ST5416(config-if-range)# ip igmp snooping last-listener query-inteval 3
```

30.9 ip igmp snooping last-listener query-count

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：

```
TL-ST5416(config-if-range)# ip igmp snooping last-listener query-count 5
```

30.10 ip igmp snooping vlan-config

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 { ten-gigabitEthernet port**-*list* | **port-channel** *lagid* }]

ip igmp snooping vlan-config *vlan-id* **static** *ip* **interface { ten-gigabitEthernet** *port-list* | **port-channel** *lagid* }

no ip igmp snooping vlan-config *vlan-id list* **[rtime** *router-time* | **mtime** *member-time* | **rport interface { ten-gigabitEthernet port**-*list* | **port-channel** *lagid* }]

no ip igmp snooping vlan-config *vlan-id* **static** *ip* **interface { ten-gigabitEthernet** *port-list* | **port-channel** *lagid* }

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300。

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260。

leave-time —— 离开滞后时间，即主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。取值范围1~30（秒），默认值为1。

port-list —— 成员端口列表。

lagid —— 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：

```
TL-ST5416(config)# ip igmp snooping vlan-config 1-3 rtime 300
TL-ST5416(config)# ip igmp snooping vlan-config 1-3 mtime 200
TL-ST5416(config)# ip igmp snooping vlan-config 1-2 rport interface
ten-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：

```
TL-ST5416(config)# ip igmp snooping vlan-config 2 static 225.0.0.1 interface
ten-gigabitEthernet 1/0/1-3
```

30.11 ip igmp snooping vlan-config (router-ports-forbidden)

该命令用于禁止指定端口作为指定 VLAN 中的路由器端口。要删除禁止的路由器端口，请使用它的 no 命令。

命令

Ip igmp snooping vlan-config *vlan-id-list* **router-ports-forbidden interface { ten-gigabitEthernet port-***list* **| port-channel** *port-channel-id* **}**

no ip igmp snooping vlan-config *vlan-id-list* **router-ports-forbidden interface [ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **]**

参数

vlan-id-list —— 用于修改配置的 VLAN 的 ID 列表，范围从 1 到 4094，格式为 1-3,5。

port-list —— 禁止指定的端口作为路由器端口。 从组播路由器发送到这些端口的数据包将被丢弃。

port-channel-id —— 禁止指定的端口通道作为路由器端口。从组播路由器发送到这些端口通道的数据包将被丢弃。

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

禁止以太网端口 1/0 / 1-3 作为 VLAN 1 中的路由器端口：

```
TL-ST5416(config)# ip igmp snooping vlan-config 1 router-ports-forbidden
interface ten-gigabit Ethernet 1/0/1-3
```

30.12 ip igmp snooping multi-vlan-config

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 { ten-gigabitEthernet port**-*list* | **port-channel** *lagid* }]

no ip igmp snooping multi-vlan-config [**rtime** *router-time* | **mtime** *member-time* | **rport interface { ten-gigabitEthernet port**-*list* | **port-channel** *lagid* }]

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300。

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260。

port-list —— 成员端口列表。

lagid —— LAG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

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3：

```
TL-ST5416(config)# ip igmp snooping multi-vlan-config 3 rtime 100
TL-ST5416(config)# ip igmp snooping multi-vlan-config 3 mtime 100
TL-ST5416(config)# ip igmp snooping multi-vlan-config 3 rport interface
ten-gigabitEthernet 1/0/3
```

30.13 ip igmp snooping multi-vlan-config (router-ports-forbidden)

该命令用于禁止指定的端口作为指定组播 VLAN 中的路由器端口。 要删除禁止的路由器端口，请使用它的 no 命令。

命令

ip igmp snooping multi-vlan-config [*vlan-id*] **router-ports-forbidden interface { ten-gigabitEthernet port**-*list* | **port-channel** *port-channel-id* }

no ip igmp snooping multi-vlan-config router-ports-forbidden [**interface { ten-gigabitEthernet port**-*list* | **port-channel** *port-channel-id* }]

参数

vlan-id——组播 VLAN 的编号，取值范围为 2～4094。

port-list ——禁止指定的端口作为路由器端口。 从组播路由器发送到这些端口的数据包将被丢弃。

port-channel-id ——禁止指定的端口通道作为路由器端口。 从组播路由器发送到这些端口通道的数据包将被丢弃。

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

禁止以太网端口 1/0 / 1-3 作为组播 VLAN 2 中的路由器端口：

TL-ST5416(config)# ip igmp snooping multi-vlan-config 2 **router-ports-forbidden interface ten-gigabitEthernet** 1/0/1-3

30.14 ip igmp snooping multi-vlan-config (source-ip-replace)

该命令用于替换指定组播 VLAN 中 IGMP 报文的组播源 IP 地址。它的 no 命令用于关闭该功能。

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 的编号，取值范围为 2～4094。

ip ——指定 IP 地址。 交换机将使用此 IP 地址替换 IGMP 数据包的源 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

替换组播 VLAN 2 中 IGMP 报文的源 IP 地址为 192.168.0.112：

TL-ST5416(config)# ip igmp snooping multi-vlan-config 2 **replace-sourceip** 192.168.0.112

30.15 ip igmp snooping querier vlan

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：

TL-ST5416(config)# ip igmp snooping querier vlan 1

30.16 ip igmp snooping querier vlan (general query)

该命令用于配置IGMP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

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：

TL-ST5416(config)#ip igmp snooping querier vlan 2 **query-interval** 200

TL-ST5416(config)#ip igmp snooping querier vlan 2 **max-response-time** 20

30.17 ip igmp snooping max-groups

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 1024，默认值是 1024。

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 ten-gigabitEthernet / interface range ten-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 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：

```
TL-ST5416(config)#interface range ten-gigabitEthernet 1/0/2-5
TL-ST5416(config-if-range)#ip igmp snooping max-groups 10
TL-ST5416(config-if-range)#ip igmp snooping max-groups action replace
```

30.18 ip igmp snooping authentication

该命令用于对要加入有限多播源的用户进行身份验证，它的 no 命令用于关闭该功能。

命令

ip igmp snooping authentication

no ip igmp snooping authentication

模式

接口配置模式（interface ten-gigabitEthernet / interface range ten-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AAA功能开启并且配置好RADIUS服务器时，IGMP认证功能才会生效。关于如何开启AAA功能和配置RADIUS服务器，请参考aaa enable和radius-server host。

示例

在端口 3 中开启 IGMP 认证功能：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if-range)# ip igmp snooping authentication
```

30.19 ip igmp snooping accounting

该命令用于开启 IGMP 的全局计数功能，它的 no 命令用于关闭该功能。

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

开启全局计数功能：

```
TL-ST5416(config-if-range)#ip igmp snooping accounting
```

30.20 ip igmp profile

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：

```
TL-ST5416(config)# ip igmp profile 1
```

30.21 deny

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：

```
TL-ST5416(config)# ip igmp profile 1
TL-ST5416(config-igmp-profile)# deny
```

30.22 permit

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、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：

```
TL-ST5416(config)# ip igmp profile 1
TL-ST5416(config-igmp-profile)# pemit
```

30.23 range

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。

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、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：

```
TL-ST5416(config)# ip igmp profile 1
TL-ST5416(config-igmp-profile)#range 225.1.1.1 226.3.2.1
```

30.24 ip igmp filter

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 ten-gigabitEthernet / interface range ten-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 2：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# ip igmp filter 1
```

30.25 clear ip igmp snooping statistics

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：

```
TL-ST5416# clear ip igmp snooping statistics
```

30.26 show ip igmp snooping

该命令用于显示IGMP全局配置信息。

命令

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：

TL-ST5416# show ip igmp snooping

30.27 show ip igmp snooping interface

该命令用于显示IGMP端口配置信息。

命令

show ip igmp snooping interface [ten-gigabitEthernet [*port* | *port-list*]] { basic-config | max-groups | packet-stat }

show ip igmp snooping interface [**port-channel** [*lagid*]] { basic-config | max-groups }

参数

port —— 要显示配置信息的端口号。

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。

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：

TL-ST5416# show ip igmp snooping interface basic-config

显示端口2的IGMP基本配置信息：

TL-ST5416# show ip igmp snooping interface ten-gigabitEthernet 1/0/2 basic-config

显示端口1-4的IGMP报文统计信息：

TL-ST5416# show ip igmp snooping interface ten-gigabitEthernet 1/0/1-4 packet-stat

30.28 show ip igmp snooping vlan

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：

```
TL-ST5416# show ip igmp snooping vlan 2
```

30.29 show ip igmp snooping multi-vlan

该命令用于显示组播VLAN配置信息。

命令

show ip igmp snooping multi-vlan

模式

特权模式和所以配置模式

特权要求

无

示例

显示组播VLAN配置信息：

```
TL-ST5416# show ip igmp snooping multi-vlan
```

30.30 show ip igmp snooping groups vlan

该命令用于显示组播组信息。

命令

show ip igmp snooping groups vlan *vlan-id* [*multicast_addr*]

参数

vlan-id ——选择要显示的 VLAN ID。

multicast_addr ——组播组地址。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN 5 中的所有组播表项：

```
TL-ST5416# show ip igmp snooping groups vlan 5
```

在 VLAN 5 中显示地址为 225.1.1.1 的组播组信息：

```
TL-ST5416# show ip igmp snooping groups vlan 5 225.1.1.1.1
```

30.31 show ip igmp snooping groups

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 ip igmp snooping groups [**vlan** *vlan-id*] [count | dynamic | dynamic count | static | static count]

参数

vlan-id —— 需要显示组播信息的VLAN号。

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

特权模式及所有配置模式

特权要求

无

示例

显示组播组信息列表：

```
TL-ST5416# show ip igmp snooping groups
```

显示VLAN 5的所有组播组条目：

```
TL-ST5416(config)# show ip igmp snooping groups vlan 5
```

显示VLAN 5中的组播组条目个数：

```
TL-ST5416(config)# show ip igmp snooping groups vlan 5 count
```

显示动态组播组信息列表：

TL-ST5416(config)# show ip igmp snooping groups vlan 5 dynamic

显示静态组播组信息列表：

TL-ST5416(config)# show ip igmp snooping groups vlan 5 static

显示VLAN 5中的动 态组播组条目个数：

TL-ST5416(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：

TL-ST5416(config)# show ip igmp snooping groups vlan 5 static count

30.32 show ip igmp snooping querier

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：

TL-ST5416(config)# show ip igmp snooping querier

30.33 show ip igmp profile

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：

```
TL-ST5416(config)# show ip igmp profile
```

第31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。

31.1 ipv6 mld snooping(global)

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：

```
TL-ST5416(config)# ipv6 mld snooping
```

31.2 ipv6 mld snooping (interface)

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。

命令

ipv6 mld snooping

no ipv6 mld snooping

模式

接口配置模式（interface ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
```

```
TL-ST5416(config-if)# ipv6 mld snooping
```

31.3 ipv6 mld snooping rtime

该命令用于设置 MLD 侦听全局路由器端口时间，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时间为 100 秒：

```
TL-ST5416(config-if-range)# ipv6 mld snooping rtime 100
```

31.4 ipv6 mld snooping mtime

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：

```
TL-ST5416(config-if-range)# ipv6 mld snooping mtime 100
```

31.5 ipv6 mld snooping report-suppression

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 报告消息转发到第 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：

```
TL-ST5416(config-if-range)# ipv6 mld snooping report-suppression
```

31.6 ipv6 mld snooping immediate-leave

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# ipv6 mld snooping immediate-leave
```

31.7 ipv6 mld snooping drop-unknown

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：

```
TL-ST5416(config)# ipv6 mld snooping drop-unknown
```

31.8 ipv6 mld snooping last-listener query-inteval

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 mtime

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 5s：

```
TL-ST5416(config-if-range)# ipv6 mld snooping last-listener query-inteval 5
```

31.9 ipv6 mld snooping last-listener query-count

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 mtime

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 5：

TL-ST5416(config-if-range)# ipv6 mld snooping last-listener query-count 5

31.10 ipv6 mld snooping vlan-config

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** { **ten-gigabitEthernet** *port* }]

ipv6 mld snooping vlan-config *vlan-id* **static** *ip* **interface** { **ten-gigabitEthernet** *port* }

no ipv6 mld snooping vlan-config *vlan-id list*

no ipv6 mld snooping vlan-config *vlan-id* **static** *ip*

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300。

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260。

port —— 交换机成员端口号。

vlan-id —— 组播IP的VLAN ID，取值范围1 ~ 4094。

ip —— 静态组播IP地址。

port-list —— 成员端口列表。

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：

TL-ST5416(config)# ipv6 mld snooping vlan-config 1-3 **rtime** 300

TL-ST5416(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：

TL-ST5416(config)# ipv6 mld snooping vlan-config 2 **static** 225.0.0.1 **interface ten-gigabitEthernet** 1/0/1-3

31.11 ipv6 mld snooping vlan-config (router-ports-forbidden)

该命令用于禁止指定端口作为指定 VLAN 中的路由器端口。要删除禁止的路由器端口，请使用它的 no 命令。

命令

ipv6 mld snooping vlan-config *vlan-id-list* **router-ports-forbidden interface { ten-gigabitEthernet port-***list* **| port-channel** *port-channel-id* **}**

no ipv6 mld snooping vlan-config *vlan-id-list* **router-ports-forbidden interface [ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **]**

参数

vlan-id-list —— 用于修改配置的 VLAN 的 ID 列表，范围从 1 到 4094，格式为 1-3,5。

port-list —— 禁止指定的端口作为路由器端口。 从组播路由器发送到这些端口的数据包将被丢弃。

port-channel-id —— 禁止指定的端口通道作为路由器端口。从组播路由器发送到这些端口通道的数据包将被丢弃。

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

禁止以太网端口 1/0 / 1-3 作为 VLAN 1 中的路由器端口：

```
TL-ST5416(config)# ipv6 mld snooping vlan-config 1 router-ports-forbidden
interface ten-gigabit Ethernet 1/0/1-3
```

31.12 ipv6 mld snooping multi-vlan-config

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** { **ten-gigabitEthernet** *port* } }

no ipv6 mld snooping multi-vlan-config

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300。

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260。

port —— 交换机成员端口号。

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3：

```
TL-ST5416(config)# ipv6 mld snooping multi-vlan-config 3 rtime 100
TL-ST5416(config)# ipv6 mld snooping multi-vlan-config 3 mtime 100
TL-ST5416(config)# ipv6 mld snooping multi-vlan-config 3 rport interface
ten-gigabitEthernet 1/0/3
```

31.13 ipv6 mld snooping multi-vlan-config (router-ports-forbidden)

该命令用于禁止指定的端口作为指定组播 VLAN 中的路由器端口。 要删除禁止的路由器端口，请使用它的 no 命令。

命令

ipv6 mld snooping multi-vlan-config [*vlan-id*] **router-ports-forbidden interface { ten-gigabitEthernet port-***list* | **port-channel** *port-channel-id* }

no ipv6 mld snooping multi-vlan-config router-ports-forbidden [**interface { ten-gigabitEthernet port-***list* | **port-channel** *port-channel-id* }]

参数

vlan-id——组播 VLAN 的编号，取值范围为 2～4094。

port-list ——禁止指定的端口作为路由器端口。 从组播路由器发送到这些端口的数据包将被丢弃。

port-channel-id ——禁止指定的端口通道作为路由器端口。 从组播路由器发送到这些端口通道的数据包将被丢弃。

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

禁止以太网端口 1/0 / 1-3 作为组播 VLAN 2 中的路由器端口：

```
TL-ST5416(config)# ipv6 mld snooping multi-vlan-config 2 router-ports-forbidden
interface ten-gigabitEthernet 1/0/1-3
```

31.14 ipv6 mld snooping multi-vlan-config (source-ip-replace)

该命令用于替换指定组播 VLAN 中 MLD 报文的组播源 IP 地址。它的 no 命令用于关闭该功能。

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 的编号，取值范围为 2～4094。

ip ——指定 IP 地址。交换机将使用此 IP 地址替换 MLD 数据包的源 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

替换组播 VLAN 2 中 MLD 报文的源 IP 地址为 fe80 :: 02ff：ffff：fe00：0001：

```
TL-ST5416(config)# ipv6 mld snooping multi-vlan-config 2 replace-sourceip
fe80::02ff:ffff:fe00:0001
```

31.15 ipv6 mld snooping querier vlan

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：

```
TL-ST5416(config)# ipv6 mld snooping querier vlan 1
```

31.16 ipv6 mld snooping querier vlan (general query)

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VLAN2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：

TL-ST5416(config)#ipv6 mld snooping querier vlan 2 **query-interval** 200

TL-ST5416(config)#ipv6 mld snooping querier vlan 2 **max-response-time** 20

31.17 ipv6 mld snooping max-groups

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 1024，默认值是 1024。

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 ten-gigabitEthernet / interface range ten-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 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：

```
TL-ST5416(config)#interface range ten-gigabitEthernet 1/0/2-5
TL-ST5416(config-if-range)#ipv6 mld snooping max-groups 10
TL-ST5416(config-if-range)#ipv6 mld snooping max-groups action replace
```

31.18 ipv6 mld profile

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：

```
TL-ST5416(config)# ipv6 mld profile 1
```

31.19 deny

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：

```
TL-ST5416(config)# ipv6 mld profile 1
TL-ST5416(config-mld-profile)# deny
```

31.20 permit

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：

```
TL-ST5416(config)# ipv6 mld profile 1
TL-ST5416(config-mld-profile)# pemit
```

31.21 range

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：

```
TL-ST5416(config)# ipv6 mld profile 1
TL-ST5416(config-mld-profile)#range 225.1.1.1 226.3.2.1
```

31.22 ipv6 mld filter

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 *profile-id*

参数

profile-id —— 需要绑定的 profile ID。

模式

接口配置模式(interface ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/1
TL-ST5416(config-if)# ipv6 mld filter 1
```

31.23 clear ipv6 mld snooping statistics

该命令是用于清除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：

```
TL-ST5416# clear ipv6 mld snooping statistics
```

31.24 show ipv6 mld snooping

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：

```
TL-ST5416# show ipv6 mld snooping
```

31.25 show ipv6 mld snooping interface

该命令用于显示MLD端口配置信息。

命令

show ipv6 mld snooping interface [**ten-gigabitEthernet** *port*] { basic-config | packet-stat | max-groups }

参数

port —— 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。

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：

```
TL-ST5416# show ipv6 mld snooping interface ten-gigabitEthernet 1/0/2
basic-config
```

显示端口1-4的MLD报文统计信息：

```
TL-ST5416# show ipv6 mld snooping interface ten-gigabitEthernet 1/0/1-4
packet-stat
```

31.26 show ipv6 mld snooping vlan

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 —— 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MLD Snooping配置信息：

```
TL-ST5416# show ipv6 mld snooping vlan 2
```

31.27 show ipv6 mld snooping multi-vlan

该命令用于显示组播VLAN配置信息。

命令

show ipv6 mld snooping multi-vlan

模式

特权模式和所以配置模式

特权要求

无

示例

显示组播VLAN配置信息：

```
TL-ST5416# show ipv6 mld snooping multi-vlan
```

31.28 show ipv6 mld snooping groups vlan

该命令用于显示组播组信息。

命令

show ipv6 mld snooping groups vlan *vlan-id* [*ipv6_multicast_addr*]

参数

vlan-id ——选择要显示的 VLAN ID。

ipv6_multicast_addr ——组播组的 IPv6 地址。

模式

特权模式和所有配置模式

特权要求

无

示例

显示 VLAN 5 中的所有组播表项：

```
TL-ST5416#show ipv6 mld snooping groups vlan 5
```

在 VLAN 5 中显示 IPv6 地址为 ff80 :: 1234 的组播组信息：

```
TL-ST5416#show ipv6 mld snooping groups vlan 5 ff80::1234
```

31.29 show ipv6 mld snooping groups

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*] [count | dynamic | dynamic count | static | static count]

参数

vlan-id —— 需要显示组播信息的VLAN号。

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

特权模式及所有配置模式

特权要求

无

示例

显示组播组信息列表：

TL-ST5416# show ipv6 mld snooping groups

显示VLAN 5的所有组播组条目：

TL-ST5416(config)# show ipv6 mld snooping groups vlan 5

显示VLAN 5中的组播组条目个数：

TL-ST5416(config)# show ipv6 mld snooping groups vlan 5 count

31.30 show ipv6 mld snooping querier

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：

TL-ST5416(config)# show ipv6 mld snooping querier vlan 2

31.31 show ipv6 mld profile

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：

```
TL-ST5416(config)# show ipv6 mld profile
```

第32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。

32.1 snmp-server

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：

```
TL-ST5416(config)# snmp-server
```

32.2 snmp-server view

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：

```
TL-ST5416(config)# snmp-server view view1 1.3.6.1.6.3.20 include
```

32.3 snmp-server group

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。其中SNMP v1和SNMP v2c采用团体名（详见命令**snmp-server community**）认证，SNMP v3采用USM认证。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。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：

TL-ST5416(config)# snmp-server group group1 **smode** v3 **slev** authNoPriv **read** viewDefault **write** viewDefault **notify** viewDefault

删除组group1：

TL-ST5416(config)# no snmp-server group group1 **smode** v3 **slev** authNoPriv

32.4 snmp-server user

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：

TL-ST5416(config)# snmp-server user admin local group2 **smode** v3 **slev** authPriv **cmode** MD5 **cpwd** 11111 **emode** DES **epwd** 22222

32.5 snmp-server community

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：

TL-ST5416(config)# snmp-server community public read-write viewDefault

32.6 snmp-server host

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：

TL-ST5416(config)# snmp-server host 192.168.0.146 162 admin **smode** v2c **type** inform **retries** 100 **timeout** 1000

32.7 snmp-server engineID

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** l*ocal-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：

TL-ST5416(config)# snmp-server engineID local 1234567890 **remote** abcdef123456

32.8 snmp-server traps snmp

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 }

no snmp-server traps snmp { linkup | linkdown | warmstart | coldstart }

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。

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：

TL-ST5416(config)# snmp-server traps snmp linkup

32.9 snmp-server traps link-status

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/3
TL-ST5416(config-if)# snmp-server traps link-status
```

32.10 snmp-server traps

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 | ipaddr-change | lldp | loopback-detection | storm-control | spanning-tree | memory }

no snmp-server traps { bandwidth-control | cpu | flash | ipaddr-change | 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。

ipaddr-change —— 用于监控交换机的IP是否更改。当交换机的IP地址被修改时，如进行手动修改IP地址或通过DHCP获取到新的IP地址时，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：

```
TL-ST5416(config)# snmp-server traps bandwidth-control
```

32.11 snmp-server traps vlan

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：

TL-ST5416(config)# snmp-server traps vlan

单独开启交换机SNMP扩展traps中的 vlan create功能：

TL-ST5416(config)# snmp-server traps vlan create

32.12 rmon history

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）完全基于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** { **ten-gigabitEthernet** *port* } [**interval** *seconds*] [**owner** *owner-name*]

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。

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：

TL-ST5416(config)# rmon history 1-3 **interface ten-gigabitEthernet** 1/0/2 **interval** 100 **owner** owner1

32.13 rmon event

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：

```
TL-ST5416(config)# rmon event 1-4 user user1 description description1 type log
owner owner1
```

32.14 rmon alarm

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：

TL-ST5416(config)# rmon alarm 1-3 **stats-index** 2 **owner** owner1 **interval** 100

32.15 rmon statistics

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** { **ten-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“生效”和“未生效”。“生效”是指条目创建后立即生效，“未生效”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“生效”：

```
TL-ST5416(config)#rmon statistics 1-3 interface ten-gigabitEthernet 1/0/1 owner owner1 status valid
```

32.16 show snmp-server

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：

```
TL-ST5416# show snmp-server
```

32.17 show snmp-server view

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：

```
TL-ST5416# show snmp-server view
```

32.18 show snmp-server group

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：

```
TL-ST5416# show snmp-server group
```

32.19 show snmp-server user

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：

```
TL-ST5416# show snmp-server user
```

32.20 show snmp-server community

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：

```
TL-ST5416# show snmp-server community
```

32.21 show snmp-server host

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：

```
TL-ST5416# show snmp-server host
```

32.22 show snmp-server engineID

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：

```
TL-ST5416# show snmp-server engineID
```

32.23 show rmon history

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：

```
TL-ST5416# show rmon history
```

32.24 show rmon event

该命令用于显示SNMP-RMON事件配置信息。

命令

show snmp-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：

```
TL-ST5416# show rmon event 1-4
```

32.25 show rmon alarm

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：

```
TL-ST5416# show rmon alarm 1-2
```

32.26 show rmon statistics

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：

```
TL-ST5416# show rmon alarm 1-2
```

第33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。

33.1 lldp

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：

```
TL-ST5416(config)# lldp
```

33.2 lldp hold-multiplier

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：

```
TL-ST5416(config)# lldp hold-multiplier 5
```

33.3 lldp timer

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：

```
TL-ST5416(config)# lldp timer tx-interval 45
TL-ST5416(config)# lldp timer notify-interval 120
```

33.4 lldp receive

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/1
TL-ST5416(config-if)# lldp receive
```

33.5 lldp transmit

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/1
TL-ST5416(config-if)# lldp transmit
```

33.6 lldp snmp-trap

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/1
TL-ST5416(config-if)# lldp snmp-trap
```

33.7 lldp tlv-select

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-id] [protocol-vlan-id] [vlan-name] [link-aggregation] [mac-phy] [max-frame-size] [power] [all] }

no lldp tlv-select { [port-description] [system-capability] [system-description] [system-name] [management-address] [port-vlan-id] [protocol-vlan-id] [vlan-name] [link-aggregation] [mac-phy] [max-frame-size] [power] [all] }

参数

port-description —— 使LLDPDU包含端口描述TLV，以向邻居发布本端口的IEEE 802局域网工作站规定的端口描述。

system-capability —— 使LLDPDU包含系统能力TLV，以向邻居发布本地设备支持的功能和这些功能是否允许的信息。

system-description —— 使LLDPDU包含系统描述TLV，用以向邻居发布本地设备包含系统硬件、软件版本等系统信息的描述。

system-name —— 使LLDPDU包含系统名称TLV，以向邻居发布本地设备的系统名称。

management-address —— 使LLDPDU包含管理地址TLV，以向邻居发布本地设备的管理地址，网络管理协议可以通过该地址对本地设备进行管理。

port-vlan-id —— 使LLDPDU包含端口VLAN ID TLV，以向邻居发布本端口所处802.1Q VLAN的ID。

protocol-vlan-id —— 使LLDPDU包含协议VLAN ID TLV，以向邻居发布本端口所处协议VLAN的ID。

vlan-name —— 使LLDPDU包含VLAN名称TLV，以向邻居发布本端口所处VLAN被指派的名称。

link-aggregation —— 使LLDPDU包含链路聚合TLV，以向邻居发布本端口当前的链路聚合信息，包括本端口是否具有链路聚合能力、是否处于聚合状态以及处于链路聚合状态时的端口ID。

mac-phy —— 使LLDPDU包含MAC/PHY TLV，以向邻居发布本端口的端口属性，包括端口支持的速率双工、当前工作的速率双工以及是手工设置还是自动协商而得到的速率双工。

max-frame-size —— 使LLDPDU包含最大帧长度TLV，以向邻居发布本端口的MAC和PHY支持的最大帧长度。

power —— 使LLDPDU包含供电能力TLV，以向邻居发布本端口的基本供电信息。

all —— 使LLDPDU包含以上所有的TLV类型。

模式

接口配置模式（interface ten-gigabitEthernet / interface range ten-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类型中删除管理地址TLV和端口VLAN ID TLV：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/1
TL-ST5416(config-if)# no lldp tlv-select management-address port-vlan-id
```

33.8 lldp med-fast-count

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：

```
TL-ST5416(config)# lldp med-fast-count 5
```

33.9 lldp med-status

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 ten-gigabitEthernet / interface range ten-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：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# lldp med-status
```

33.10 lldp med-tlv-select

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]}

参数

inventory-management —— 使 LLDPDU 包含资产信息 TLV，资产信息中包含七种基本的资产信息 TLV，分别为硬件版本 TLV、固件版本 TLV、软件版本 TLV、序列号 TLV、制造厂商名称 TLV、模块名称 TLV 和资产跟踪 ID TLV。

location —— 使 LLDPDU 包含设备地址 TLV，设备地址 TLV 提供了向相邻设备发布本地设备物理地址信息的能力。

network-policy ——使 LLDPDU 包含网络策略 TLV，网络策略 TLV 允许网络连接设备和终端设备发布本端口的 VLAN 配置与二层和三层属性。

power-management ——使 LLDPDU 包含扩展供电能力 TLV，扩展供电能力 TLV 允许 LLDP-MED 连接设备和终端设备之间交互详细的供电信息，例如供电优先级、供电状态等。

all —— 使 LLDPDU 包含以上所有的 TLV 类型。

模式

接口配置模式（interface ten-gigabitEthernet / interface range ten-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 类型中删除网络策略 TLV 和设备地址 TLV：

TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2

TL-ST5416(config-if)# no lldp med-tlv-select network-policy inventory- management

33.11 lldp med-location

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 ten-gigabitEthernet / interface range ten-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：

TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2

TL-ST5416(config-if)# lldp med-location civic-address language English city London

33.12 show lldp

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：

```
TL-ST5416# show lldp
```

33.13 show lldp interface

该命令用于显示端口的LLDP配置信息。

命令

show lldp interface [**ten-gigabitEthernet** *port*]

参数

port —— 要显示LLDP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

显示端口1的LLDP配置信息：

```
TL-ST5416# show lldp interface ten-gigabitEthernet 1/0/1
```

33.14 show lldp local-information interface

该命令用于显示端口的LLDP信息。

命令

show lldp local-information interface [ten-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

特权模式和所有命令模式

特权要求

无

示例

显示端口1的LLDP信息：

TL-ST5416# show lldp local-information interface ten-gigabitEthernet 1/0/1

33.15 show lldp neighbor-information interface

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 [ten-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

特权模式和所有命令模式

特权要求

无

示例

显示连接到端口1的邻居信息：

TL-ST5416# show lldp neighbor-information interface ten-gigabitEthernet 1/0/1

33.16 show lldp traffic interface

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 [ten-gigabitEthernet *port*]

参数

port —— 要显示本地设备和邻居设备的LLDP统计信息的端口号，缺省表示显示所有端口的统计信息。

模式

特权模式和所有命令模式

特权要求

无

示例

显示连接到端口1的LLDP统计信息：

```
TL-ST5416# show lldp traffic interface ten-gigabitEthernet 1/0/1
```

第34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。

34.1 arp

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：

```
TL-ST5416(config)# arp 192.168.0.1 00:11:22:33:44:55 arpa
```

34.2 clear arp-cache

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

删除所有的动态 ARP 表项：

```
TL-ST5416(config)# clear arp-cache
```

34.3 arp timeout

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

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 VLAN 1 的 ARP 老化时间为 60 秒：

```
TL-ST5416(config)# interface vlan 1
TL-ST5416(config-if)# arp timeout 60
```

34.4 show arp

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：

```
TL-ST5416(config)# show ip arp 192.168.0.2
```

34.5 show ip arp(interface)

该命令用于显示指定三层接口的 ARP 表项。

命令

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

参数

port —— 指定端口。

lagid —— 指定 LAG 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：

```
TL-ST5416(config)# show ip arp vlan 2
```

34.6 show ip arp summary

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：

```
TL-ST5416(config)# show ip arp summary
```

第35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。

35.1 ip address

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，环回借口和 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 地址为借口的主地址。

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：

```
TL-ST5416 (config)# interface vlan 2
TL-ST5416(config-if)# ip address 192.168.1.1 255.255.255.0
TL-ST5416(config-if) # ip address 192.168.2.1 255.255.255.0 secondary
```

35.2 ip address-alloc

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 上的 DHCP 客户端功能：

```
TL-ST5416 (config)# interface ten-gigabitEthernet 1/0/1
TL-ST5416(config-if)# no switchport
TL-ST5416(config-if)# ip address-alloc dhcp
```

关闭 VLAN 接口 2 上获取 IP 地址的功能：

```
TL-ST5416 (config)# interface vlan 2
TL-ST5416(config-if)# no ip address
```

35.3 interface vlan

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：

```
TL-ST5416(config)# interface vlan 2
```

35.4 interface loopback

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

Vid —— 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：

```
TL-ST5416(config)# interface loopback 1
```

35.5 switchport

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 ten-gigabitEthernet / interface range ten-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 9 的路由端口模式：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/9
TL-ST5416(config-if)# no switchport
```

35.6 interface range port-channel

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，操作员和高级用户级别的用户才能访问这些命令。

示例

创建端口通道接口 1,3,4 和 5：

```
TL-ST5416(config)# interface port-channel 1,3-5
```

35.7 description

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(interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

特权要求

只有管理员，操作员和高级用户级别的用户才能访问这些命令。

示例

添加路由端口 9 的描述为 system-if：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/9
TL-ST5416(config-if)# no switchport
TL-ST5416(config-if)# description system-if
```

35.8 shutdown

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(interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

特权要求

只有管理员，操作员和高级用户级别的用户才能访问这些命令。

示例

关闭路由端口 9：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/9
TL-ST5416(config-if)# no switchport
TL-ST5416(config-if)# shutdown
```

35.9 interface port-channel

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，操作员和高级用户级别的用户才能访问这些命令。

示例

创建端口通道接口 1：

TL-ST5416(config)# interface port-channel 1

35.10 ip route

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，操作员和高级用户级别的用户才能访问这些命令。

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：

TL-ST5416(config)# ip route 192.168.2.0 255.255.255.0 192.168.0.2

35.11 ipv6 routing

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，操作员和高级用户级别的用户才能访问这些命令。

示例

全局开启 IPv6 路由：

TL-ST5416(config)# ipv6 routing

35.12 ipv6 route

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/mask length* } { *next-hop-address* } [*distance*]

no ipv6 route { *ipv6-dest-address/mask length* } { *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，操作员和高级用户级别的用户才能访问这些命令。

示例

创建目的网络的 IP 地址为 3200 :: / 64，下一跳地址为 3100 :: 1234 的静态路由：

TL-ST5416(config)# ipv6 route 3200::/64 3100::1234

35.13 show interface vlan

该命令用于显示指定VLAN接口的信息。

命令

show interface vlan *vid*

参数

vid ——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：

TL-ST5416(config)# show interface vlan 2

35.14 show ip interface

该命令用于显示特定三层接口的详细信息。

命令

show ip interface [**ten-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：

```
TL-ST5416(config)# show ip interface vlan 2
```

35.15 show ip interface brief

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：

```
TL-ST5416(config)# show ip interface brief
```

35.16 show ip route

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 | rip]

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。

rip：显示设备上的RIP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：

TL-ST5416(config)# show ip route static

35.17 show ip route specify

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：

TL-ST5416(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：

TL-ST5416(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：

TL-ST5416(config)# show ip route specify 192.168.0.0 255.255.0.0 **longer-prefixes**

35.18 show ip route summary

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：

```
TL-ST5416(config)# show ip route summary
```

35.19 show ipv6 interface

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。

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

显示管理接口的 IPv6 信息：

```
TL-ST5416(config)# show ipv6 interface
```

35.20 show ipv6 route

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

特权模式以及所有配置模式

特权要求

无

示例

显示 IPv6 静态路由：

```
TL-ST5416# show ipv6 route static
```

35.21 show ipv6 route summary

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

特权模式以及所有配置模式

特权要求

无

示例

显示 IPv6 路由项的汇总信息：

```
TL-ST5416# show ipv6 route summary
```

第36章 SDM 模板命令

本章介绍如何配置交换机数据库管理（SDM）模板，以便为交换机分配不同用途的硬件资源。

36.1 sdm prefer

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 | enterpriseV6 }

参数

default —— 将交换机中使用的 SDM 模板指定为“默认”。

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

只有管理员级别的用户才能访问这些命令。

示例

将交换机中使用的 SDM 模板指定为“enterpriseV6”：

```
TL-ST5416(config)# sdm prefer enterpriseV6
```

36.2 show sdm prefer

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 | 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。

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

只有管理员级别的用户才能访问这些命令。

示例

显示当前使用及重启后生效的模板的资源分配：

TL-ST5416(config)#show sdm prefer used

第37章 AAA 配置命令

AAA 是认证、授权和计费（Authentication、Authorization、Accounting）三个英文单词的简称。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。

37.1 aaa enable

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

只有管理员级别的用户才能访问这些命令。

示例

开启 AAA 全局配置功能：

```
TL-ST5416(config)# aaa enable
```

37.2 tacacas-server host

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。请始终将配置密钥作为该命令的最后一项。

模式

全局配置模式

特权要求

只有管理员级别的用户才能访问这些命令。

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。

```
TL-ST5416(config)# tacacs-server host 1.1.1.1 port 1500 timeout 6 key 12345
```

37.3 show tacacs-server

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

只有管理员级别的用户才能访问这些命令。

示例

显示所有 TACACS+服务器信息：

```
TL-ST5416(config)# show tacacs-server
```

37.4 radius-server host

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。请始终将配置密钥作为该命令的最后一项。

模式

全局配置模式

特权要求

只有管理员级别的用户才能访问这些命令。

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。

```
TL-ST5416(config)# radius-server host 1.1.1.1 auth-port 1200 timeout 6 retransmit 3 key 12345
```

37.5 show radius-server

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

只有管理员级别的用户才能访问这些命令。

示例

显示所有 RADIUS 服务器信息：

```
TL-ST5416(config)# show radius-server
```

37.6 aaa group

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

只有管理员级别的用户才能访问这些命令。

示例

创建一个名为 Radius1 的 RADIUS 服务器组：

```
TL-ST5416(config)# aaa group radius radius1
```

37.7 server

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

只有管理员级别的用户才能访问这些命令。

示例

创建 RADIUS 服务器 1.1.1.1 到 RADIUS 服务器组“Radius1”中：

```
TL-ST5416(config)# aaa group radius radius1
TL-ST5416(aaa-group)# server 1.1.1.1
```

37.8 show aaa group

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

只有管理员级别的用户才能访问这些命令。

示例

显示所有服务器组的信息：

TL-ST5416(config)# show aaa group

37.9 aaa authentication login

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

只有管理员级别的用户才能访问这些命令。

示例

配置一个优先方法 1 为 radius，优先方法 2 为 local 的登录认证方法列表：

TL-ST5416(config)# aaa authenticaiton login list1 radius local

37.10 aaa authentication enable

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

只有管理员级别的用户才能访问这些命令。

示例

配置一个优先方法 1 为 radius，优先方法 2 为 local 的特权要求认证方法列表：

TL-ST5416(config)# aaa authenticaiton enable list2 radius local

37.11 aaa authentication dot1x default

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

只有管理员级别的用户才能访问这些命令。

示例

配置默认的 802.1x 认证方式为“radius1”：

TL-ST5416(config)# aaa authentication dot1x default radius1

37.12 aaa accounting dot1x default

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

只有管理员级别的用户才能访问这些命令。

示例

配置默认的 802.1x 计费方式为“radius1”：

TL-ST5416(config)# aaa accounting dot1x default radius1

37.13 show aaa authentication

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

只有管理员级别的用户才能访问这些命令。

示例

显示所有认证方法列表的信息：

```
TL-ST5416(config)# show aaa authentication
```

37.14 show aaa accounting

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

只有管理员级别的用户才能访问这些命令。

示例

显示默认 802.1X 计费方法列表的信息：

```
TL-ST5416(config)# show aaa accounting
```

37.15 line telnet

该命令用于进入线路配置模式，配置应用于 telnet 终端线路的认证方法列表。

命令

line telnet

模式

全局配置模式

特权要求

只有管理员级别的用户才能访问这些命令。

示例

进入 telnet 终端线路配置模式：

```
TL-ST5416(config)#line telnet
```

37.16 login authentication(telnet)

该命令用于在 Telnet 终端线路上应用登录认证方法列表，若要还原为默认登录方法列表，请使用它的 no 命令。

命令

login authentication { *method-list* }

no login authentication

参数

method-list —— 指定 telnet 终端线上的登录方法列表。默认情况下是“默认”，包含方法“local”。

模式

线路配置模式

特权要求

只有管理员级别的用户才能访问这些命令。

示例

配置 telnet 终端线上的登录认证方法列表为“list1”：

```
TL-ST5416(config)#line telnet
```

```
TL-ST5416(config-line)# login authentication list1
```

37.17 line ssh

该命令用于进入线路配置模式，配置应用于 ssh 终端线路的认证方法列表。

命令

line ssh

模式

全局配置模式

特权要求

只有管理员级别的用户才能访问这些命令。

示例

进入 ssh 终端线路配置模式：

```
TL-ST5416(config)#line ssh
```

37.18 login authentication(ssh)

该命令用于在 ssh 终端线路上应用登录认证方法列表，若要还原为默认登录方法列表，请使用它的 no 命令。

命令

login authentication { *method-list* }

no login authentication

参数

method-list —— 指定 ssh 终端线上的登录方法列表。默认情况下是“默认”，包含方法“local”。

模式

线路配置模式

特权要求

只有管理员级别的用户才能访问这些命令。

示例

配置 ssh 终端线上的登录认证方法列表为“list1”：

```
TL-ST5416(config)# line ssh
TL-ST5416(config-line)# login authentication list1
```

37.19 enable authentication(telnet)

该命令用于在 Telnet 终端线路上应用特权认证方法列表，若要还原为默认登录方法列表，请使用它的 no 命令。

命令

enable authentication { *method-list* }

no enable authentication

参数

method-list —— 指定 telnet 终端线路上的启用方法列表。默认情况下是“默认”，包含方法“none”。

模式

线路配置模式

特权要求

只有管理员级别的用户才能访问这些命令。

示例

配置 telnet 终端线路上的启用认证方法列表为“list2”：

```
TL-ST5416(config)#line telnet
TL-ST5416(config-line)# enable authentication list2
```

37.20 enable authentication(ssh)

该命令用于在 ssh 终端线路上应用特权认证方法列表，若要还原为默认登录方法列表，请使用它的 no 命令。

命令

enable authentication { *method-list* }

no enable authentication

参数

method-list ——指定 ssh 终端线上的启用方法列表。默认情况下是“默认”，包含方法“none”。

模式

线路配置模式

特权要求

只有管理员级别的用户才能访问这些命令。

示例

配置 ssh 终端线上的启用方法列表为“list2”：

```
TL-ST5416(config)# line ssh
TL-ST5416(config-line)# enable authentication list2
```

37.21 ip http login authentication

该命令用于配置对通过 HTTP 进行访问的用户进行认证所使用的认证方法列表，还原默认登录方法列表，请使用它的 no 命令。

命令

ip http login authentication { *method-list* }

no ip http login authentication

参数

method-list —— 指定 HTTP 访问的登录方法列表，默认情况下为“默认”，包含方法“local”。

模式

全局配置模式

特权要求

只有管理员级别的用户才能访问这些命令。

示例

配置 HTTP 访问上的登录认证方法列表为“list1”：

```
TL-ST5416(config)# ip http login authentication list1
```

37.22 ip http enable authentication

该命令用于配置对通过 HTTP 进行访问的用户进行认证所使用的认证方法列表，还原默认登录方法列表，请使用它的 no 命令。

命令

ip http enable authentication { *method-list* }

no ip http enable authentication

参数

method-list —— 指定 HTTP 访问上的启用方法列表，默认情况下为“默认”，包含“none”。

模式

线路配置模式

特权要求

只有管理员级别的用户才能访问这些命令。

示例

配置 HTTP 访问上的认证方法列表为“list2”：

```
TL-ST5416(config)# ip http enable authentication list2
```

37.23 show aaa global

该命令用于显示 AAA 功能的全局配置和通过不同终端模式（console、telnet、SSH 和 HTTP）进行访问的认证/授权方法列表。

命令

show aaa global

模式

特权模式和所有配置模式

特权要求

只有管理员级别的用户才能访问这些命令。

示例

显示 AAA 功能的全局定位和每个应用的方法列表：

```
TL-ST5416(config)# show aaa global
```

第38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。

38.1 service dhcp server

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：

```
TL-ST5416(config)# service dhcp server
```

38.2 ip dhcp server extend-option capwap-ac-ip

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：

TL-ST5416(config)# ip dhcp server extend-option capwap-ac-ip 192.168.3.1

38.3 ip dhcp server extend-option vendor-class-id

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：

TL-ST5416(config)#ip dhcp server extend-option vendor-class-id 34

38.4 ip dhcp server excluded-address

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 excluded-address *start-ip-address end-ip-address*

no ip dhcp server excluded-address *start-ip-address 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：

```
TL-ST5416(config)# ip dhcp server excluded-address 192.168.10.10 192.168.10.10
```

38.5 ip dhcp server pool

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 *name*

no ip dhcp server pool *name*

参数

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“product”并进入DHCP配置模式：

```
TL-ST5416(config)# ip dhcp server pool product
```

38.6 ip dhcp ping timeout

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：

```
TL-ST5416(config)# ip dhcp server ping timeout 200
```

38.7 ip dhcp ping packets

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*

no ip dhcp server ping packets

参数

num —— 设置发送ping包的数量，范围是0到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

设置ping包的发送数量为2：

```
TL-ST5416(config)# ip dhcp server ping packets 2
```

38.8 network

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：

```
TL-ST5416(config)# ip dhcp server pool product
TL-ST5416(dhcp-config)#network 192.168.10.0 255.255.255.0
```

38.9 lease

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20分钟：

```
TL-ST5416(config)# ip dhcp server pool product
TL-ST5416(dhcp-config)# lease 20
```

38.10 address hardware-address

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：

TL-ST5416(config)# ip dhcp server pool product

TL-ST5416(dhcp-config)# address 192.168.10.50 **hardware-address**

00:19:66:20:d4:1a **hardware-type** ethernet

38.11 address client-identifier

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：

TL-ST5416(config)# ip dhcp pool product

TL-ST5416(dhcp-config)# address 192.168.0.10 **client-identifier** abc **ascii**

38.12 default-gateway

该命令用于配置地址池的缺省网关。

命令

default-gateway *gateway-list*

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：

```
TL-ST5416(config)# ip dhcp server pool product
TL-ST5416(dhcp-config)# default-gateway 192.168.10.1,192.168.10.2
```

38.13 dns-server

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-server-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：

TL-ST5416(config)# ip dhcp server pool product

TL-ST5416(dhcp-config)# dns-server 192.170.10.10

38.14 netbios-name-server

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：

TL-ST5416(config)# ip dhcp server pool product

TL-ST5416(config-dhcp)# netbios-name-server 192.168.0.1,192.168.1.1

38.15 netbios-node-type

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：

```
TL-ST5416(config)# ip dhcp server pool product
TL-ST5416(config-dhcp)# netbios-node-type b-node
```

38.16 next-server

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：

```
TL-ST5416(config)# ip dhcp server pool product
TL-ST5416(config-dhcp)# next-server 192.168.2.1
```

38.17 domain-name

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：

```
TL-ST5416(config)# ip dhcp server pool product
TL-ST5416(config-dhcp)# domain-name edu
```

38.18 bootfile

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：

```
TL-ST5416(config)# ip dhcp server pool product
TL-ST5416(config-dhcp)# bootfile boot1
```

38.19 show ip dhcp server status

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：

```
TL-ST5416(config)# show ip dhcp server status
```

38.20 show ip dhcp server statistics

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：

```
TL-ST5416(config)# show ip dhcp server statistics
```

38.21 show ip dhcp server extend-option

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：

```
TL-ST5416(config)# show ip dhcp server extend-option
```

38.22 show ip dhcp server pool

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：

```
TL-ST5416(config)# show ip dhcp server pool
```

38.23 show ip dhcp server excluded-address

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：

```
TL-ST5416(config)# show ip dhcp server excluded-address
```

38.24 show ip dhcp server manual-binding

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：

```
TL-ST5416(config)# show ip dhcp server manual-binding
```

38.25 show ip dhcp server binding

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：

```
TL-ST5416(config)# show ip dhcp server binding
```

38.26 clear ip dhcp server statistics

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：

```
TL-ST5416(config)# clear ip dhcp server statistics
```

38.27 clear ip dhcp server binding

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：

```
TL-ST5416(config)# clear ip dhcp server binding
```

第39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。

39.1 service dhcp relay

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，操作员和高级用户级别的用户才能访问这些命令。

示例

全局启用 DHCP 中继功能：

```
TL-ST5416(config)# service dhcp relay
```

39.2 ip helper-address

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，操作员和高级用户级别的用户才能访问这些命令。

示例

将 DHCP 服务器地址 192.168.2.1 添加到接口 VLAN 1：

```
TL-ST5416(config)# interface vlan 1
TL-ST5416(config-if)# ip helper-address 192.168.2.1
```

39.3 ip dhcp relay information

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，操作员和高级用户级别的用户才能访问这些命令。

示例

启用Option 82选项功能：

```
TL-ST5416(config)# ip dhcp relay information
```

39.4 ip dhcp relay information policy

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，操作员和高级用户级别的用户才能访问这些命令。

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：

```
TL-ST5416(config)# ip dhcp relay information policy replace
```

39.5 ip dhcp relay information custom

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，操作员和高级用户级别的用户才能访问这些命令。

示例

启用Option 82选项自定义功能：

```
TL-ST5416(config)# ip dhcp relay information custom
```

39.6 ip dhcp relay information circuit-id

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

circuit-id —— 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，操作员和高级用户级别的用户才能访问这些命令。

示例

配置Option 82字段中的电路ID子选项内容为“TP-LINK”：

TL-ST5416(config)# ip dhcp relay information circuit-id TP-LINK

39.7 ip dhcp relay information remote-id

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，操作员和高级用户级别的用户才能访问这些命令。

示例

配置Option 82字段中的远程ID子选项内容为“TP-LINK”：

TL-ST5416(config)# ip dhcp relay information remote-id TP-LINK

39.8 show ip dhcp relay

该命令用于显示DHCP中继的全局状态和Option 82配置。

命令

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：

```
TL-ST5416(config)# show ip dhcp relay
```

第40章 代理ARP配置命令

代理ARP是ARP协议的一种应用。通常应用于网关在连接不同网络时，为不同网络中的计算机提供ARP代理服务。网关收到源计算机向目标网络计算机发送的ARP请求时，使用自己的MAC地址与目标计算机的IP地址对源计算机进行ARP应答，使得不同网络中的计算机能够正常通信而不必关心网络的划分。本交换机的代理ARP功能可以为交换机直连网络提供代理ARP服务。

40.1 ip proxy-arp

该命令用于使能不同接口的代理ARP服务，no命令用于关闭相应接口的代理ARP服务。

命令

ip proxy-arp

no ip proxy-arp

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VLAN接口2的代理ARP服务：

```
TL-ST5416(config)# interface vlan 2
TL-ST5416(config-if)# ip proxy-arp
```

40.2 ip local-proxy-arp

该命令用于使能本地代理 ARP 功能在指定的 VLAN 接口或路由端口。no 命令用于禁用接口的本地代理 ARP 功能。

命令

ip local-proxy-arp

no ip local-proxy-arp

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VLAN接口2的本地代理ARP服务：

```
TL-ST5416(config)# interface vlan 2
TL-ST5416(config-if)# ip local-proxy-arp
```

使能路由端口2的本地代理ARP服务：

```
TL-ST5416(config)# interface ten-gigabitEthernet 1/0/2
TL-ST5416(config-if)# no switchport
TL-ST5416(config-if)# ip local-proxy-arp
```

40.3 show ip proxy-arp

该命令用于显示设备上的代理ARP功能配置信息。

命令

show ip proxy-arp

模式

特权模式和所有配置模式

特权要求

无

示例

查看所有三层接口的代理ARP功能使能信息：

```
TL-ST5416(config)# show ip proxy-arp
```

40.4 show ip local-proxy-arp

该命令用于显示设备上的本地代理ARP功能配置信息。

命令

show ip local-proxy-arp

模式

特权模式和所有配置模式

特权要求

无

示例

查看所有三层接口的本地代理ARP功能使能信息：

```
TL-ST5416(config)# show ip local-proxy-arp
```

第41章 RIP配置命令

RIP（Routing Information Protocol，路由信息协议）是最早的内部网关协议（Interior Gateway Protocol）之一，主要用于规模较小的网络中，比如校园网以及结构较简单的地区性网络。RIP 是一种距离向量路由协议，使用广播 UDP 报文来交换路由信息。RIP 当前存在 RIPv1 和 RIPv2 两个版本。

41.1 router rip

该命令用于使能 RIP 并进入路由配置模式。它的 no 命令用于关闭 RIP 功能。

命令

router rip

no router rip

模式

全局配置模式

特权要求

无

示例

使能 RIP，并进入 RIP 的路由配置模式：

```
TL-ST5416(config)# router rip
TL-ST5416(config) (config-router)#
```

41.2 network

该命令用于使能指定网段的接口的 RIP 功能，它的 no 命令用于关闭该网段接口的 RIP 功能。

命令

network *network_ip*

no network *network_ip*

参数

network_ip —— 交换机直连网段的 IP 地址，格式如 192.168.0.0。

模式

路由配置模式

特权要求

无

示例

使能所有属于网段 192.168.0.0 的交换机接口的 RIP 功能：

```
TL-ST5416(config)# router rip
TL-ST5416 (config-router)# network 192.168.0.0
```

41.3 version

该命令用于全局配置 RIP 的版本，它的 no 命令用于恢复默认配置。默认情况下，交换机发送 RIPv1 报文，同时接收 RIPv1 和 RIPv2 报文。

命令

version { 1 | 2 }

no version

参数

1 —— 交换机发送和接收 RIPv1 报文。

2 —— 交换机发送和接收 RIPv2 报文。

模式

路由配置模式

特权要求

无

示例

配置 RIP 使用版本 RIPv2：

```
TL-ST5416(config)# router rip
TL-ST5416 (config-router)# version 2
```

41.4 timer basic

该命令用于配置 RIP 协议的计时器。

命令

timer basic { **update** *update-value* | **timeout** *timeout-value* | **garbage-collect** *garbage-collect-value* }

参数

update-value —— 路由更新计时器，取值范围为 1 到 100 秒，默认值为 30 秒。

timeout-value —— 路由老化计时器，取值范围为 1 到 300 秒，默认值为 180 秒。

garbage-collect-value —— 垃圾回收计时器，即从路由条目失效或者标记为不可达，到把它从路由表中删除所经历的时间。取值范围为 1 到 500 秒，默认值为 120 秒。

模式

路由配置模式

特权要求

无

示例

配置 RIP 路由更新计时器为 80 秒：

```
TL-ST5416 (config)# router rip
TL-ST5416 (config-router)# timer basic update 80
```

41.5 distance

该命令用于配置 RIP 的路由管理距离。

命令

distance *distance-value*

参数

distance-value —— RIP 的管理距离，取值范围为 1 到 255，默认值是 120。

模式

路由配置模式

特权要求

无

示例

配置 RIP 的管理距离为 20：

```
TL-ST5416 (config)# router rip
TL-ST5416 (config-router)# distance 20
```

41.6 auto-summary

此命令用于配置 RIPv2 在网络边界上自动汇聚子网路由条目为主网路由，以减少总路由条目的数量。默认情况下，RIPv2 自动汇聚功能关闭。它的 no 命令用于关闭自动汇聚功能。另外，RIPv1 的自动汇聚功能总是开启的。

命令

auto-summary

no auto-summary

模式

路由配置模式

特权要求

无

示例

关闭 RIP 协议版本 2 的自动汇聚功能：

```
TL-ST5416 (config)# router rip
TL-ST5416 (config-router)# version 2
TL-ST5416 (config-router)# no auto-summary
```

41.7 default-metric

此命令用于配置 RIP 协议引入路由的缺省度量值，它的 no 命令用于恢复默认值。

命令

default-metric *metric*

no default-metric

参数

metric —— 缺省度量值，取值范围 1 到 15，默认值为 1。

模式

路由配置模式

特权要求

无

示例

配置 RIP 引入路由的缺省度量值为 5：

```
TL-ST5416 (config)# router rip
TL-ST5416 (config-router)# default-metric 5
```

41.8 redistribute

此命令用于配置 RIP 重发布外部路由，它的 no 命令用于恢复默认配置。默认情况下，RIP 重发布外部路由的功能是关闭的。

命令

redistribute static **metric** *metric-value*

no redistribute static **metric**

参数

static —— 引入外部静态路由条目到 RIP 协议。

metric-value —— 配置引入的外部路由的度量值。

模式

路由配置模式

特权要求

无

示例

配置 RIP 协议引入外部静态路由条目，度量值为 5：

TL-ST5416 (config)# router rip

TL-ST5416 (config-router)# redistribute static metric 5

41.9 passive-interface

此命令用于配置接口工作在抑制状态，不发送路由更新报文。它的 no 命令用于恢复默认配置，即使能接口发送路由更新报文。

命令

passive-interface interface { *interface-type* } { *interface-number* }

no passive-interface interface { *interface-type* } { *interface-number* }

参数

interface-type —— 接口类型，包括 ten-gigabitEthernet，loopback 和 VLAN 接口。

interface-number —— 接口号。

模式

路由配置模式

特权要求

无

示例

配置 VLAN 接口 1 工作在抑制状态：

TL-ST5416 (config)# router rip

TL-ST5416 (config-router)# passive-interface interface vlan 1

41.10 ip rip receive version

此命令用于配置指定接口可以接收的 RIP 报文版本，它的 no 命令用于恢复默认配置。若不配置接口的 RIP 接收版本，RIP 将使用全局配置的版本（见 **version** 命令）。

命令

ip rip receive version [1|2]

no ip rip receive version

参数

1 | 2 —— 配置 RIP 接收报文的版本。若此处不配置参数，则同时接收版本 1 和版本 2 的数据包。

模式

接口配置模式

特权要求

无

示例

配置 VLAN 接口 2 只接收 RIP 版本 1 的数据包：

```
TL-ST5416 (config)# interface vlan 2
TL-ST5416 (config-if)# ip rip receive version 1
```

41.11 ip rip send version

此命令用于配置指定接口发送 RIP 报文的版本，它的 no 命令用于恢复默认配置。若不配置接口的 RIP 发送版本，RIP 将使用全局配置的版本（见 **version** 命令）。

命令

ip rip send version {1 | 2}

no ip rip send version

参数

1 | 2 —— 接口发送数据包的 RIP 协议版本。默认情况下，接口发送 RIP 版本 1 的数据包。

模式

接口配置模式

特权要求

无

示例

配置 VLAN 接口 2 只发送 RIP 版本 2 的数据包：

```
TL-ST5416 (config)# interface vlan 2
TL-ST5416 (config-if)# ip rip send version 2
```

41.12 ip rip v2-broadcast

该命令用于配置接口的 RIP 协议版本 2 的发送报文为广播类型，no 命令用于恢复默认配置。默认情况下，RIP 协议版本 2 的发送报文为组播类型，组播地址为 224.0.0.9。

命令

ip rip v2-broadcast

no ip rip v2-broadcast

模式

接口配置模式

特权要求

无

示例

配置 VLAN 接口 2 发送 RIP 版本 2 的报文类型为广播报文：

```
TL-ST5416 (config)# interface vlan 2
TL-ST5416 (config-if)# ip rip v2-broadcast
```

41.13 ip rip authentication-mode

该命令用于配置 RIP 协议认证模式。默认情况下，RIP 协议不使用认证。

命令

ip rip authentication-mode { simple | md5 *key-id* } { [0] *password* | 7 *encrypted-password* }

ip rip authentication-mode none

参数

simple | md5 *key-id* —— 设置 RIP 的认证模式。simple 表示认证使用文本密码；md5 表示认证使用文本密码和 MD5 算法加密。若使用 md5 加密还需要设置 key ID 值，取值范围为 1 到 255。

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 —— 1～16 位的密码，由字母，数字和符号组成。密码区分大小写，不能包含空格和问号。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。

none —— 不使用加密。

模式

接口配置模式

特权要求

无

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

配置 VLAN 接口 2 的 RIP 认证模式为 simple，密码为 123：

```
TL-ST5416 (config)# interface vlan 2
TL-ST5416 (config-if)# ip rip authentication-mode simple 123
```

41.14 ip rip poison-reverse

该命令用于在指定 RIP 接口上使能毒性逆转功能，它的 no 命令用于关闭毒性逆转功能。

命令

ip rip poison-reverse

no ip rip poison-reverse

模式

接口配置模式

特权要求

无

示例

在 VLAN 接口 2 上开启 RIP 毒性逆转功能：

```
TL-ST5416 (config)# interface vlan 2
TL-ST5416 (config-if)# ip rip poison-reverse
```

41.15 ip rip split-horizon

该命令用于在指定 RIP 接口上开启水平分割功能，它的 no 命令用于关闭水平分割功能。

命令

ip rip split-horizon

no ip rip split-horizon

模式

接口配置模式

特权要求

无

示例

在 VLAN 接口 2 上使能水平分割功能：

```
TL-ST5416 (config)# interface vlan 2
TL-ST5416 (config-if)# ip rip split-horizon
```

41.16 show ip rip

此命令用来显示 RIP 配置信息。

命令

show ip rip [**interface** | **database** [**specify** *ip-address mask*]]

参数

interface —— 显示 RIP 接口的基本信息。

database —— 显示 RIP 路由表信息。

specify *ip-address mask* —— 显示指定 IP 地址的 RIP 路由信息。*ip-address* 为指定的目的网段 IP，mask 为其掩码。

模式

特权模式以及所有配置模式

特权要求

无

示例

显示目的网段为 192.168.1.0/24 的 RIP 路由信息：

```
TL-ST5416(config)# show ip rip database specify 192.168.1.0 255.255.255.0
```

第42章 管理口配置命令

说明:

本功能仅 TL-ST5016F 有。

管理端口是专用于设备带外管理的以太网端口，该端口的流量与交换机用户端口隔离，不会被交换或路由到用户端口所在网络中。为管理口配置 IP 地址后，将能通过该端口访问交换机 Web 页面进行交换机的管理。

42.1 negotiation auto

该命令用于开启管理口的自动协商功能，它的 no 命令用于关闭管理口的自动协商功能。默认开启。

命令

negotiation auto

no negotiation auto

模式

管理接口配置模式（interface meth）

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

开启管理口的自动协商功能：

```
TL-ST5016F(config)# interface meth 1/0/1

TL-ST5016F(config-if)# negotiation auto
```

42.2 speed

该命令只在关闭管理口的自动协商功能时才生效，用于强制设置管理口的工作速率，它的no命令用于恢复默认设置，默认为100M。

命令

speed { 10 | 100 | 1000 }

no speed

参数

10 | 100 | 1000 —— 端口速率模式，分别为10M、100M和1000M。

模式

管理接口配置模式（interface meth）

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

设置管理口的速率为1000M：

```
TL-ST5016F(config)# interface meth 1/0/1
TL-ST5016F(config-if)# no negotiation auto
TL-ST5016F(config-if)# speed 1000
```

42.3 duplex

该命令只在关闭管理口的自动协商功能时才生效，用于强制设置管理口的双工模式，它的no命令用于恢复默认设置，默认为全双工。

命令

duplex { full | half }

no duplex

参数

full | half —— 端口双工模式，分别为全双工模式和半双工模式。

模式

管理接口配置模式（interface meth）

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

设置管理口的双工模式为半双工：

```
TL-ST5016F(config)# interface meth 1/0/1
TL-ST5016F(config-if)# no negotiation auto
TL-ST5016F(config-if)# duplex half
```

42.4 ip address

该命令用于配置管理接口的 IP 地址和子网掩码，它的 no 命令用于删除管理接口的 IP 地址。

命令

ip address { *ip-addr* } { *mask* }

no ip address

参数

ip-addr —— 管理接口的 IP 地址。

mask —— 管理接口的子网掩码。

模式

管理接口配置模式（interface meth）

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

配置管理接口的 IP 地址为 192.168.1.1，子网掩码为 255.255.255.0：

```
TL-ST5016F(config)# interface meth 1/0/1

TL-ST5016F(config-if)# ip address 192.168.1.1 255.255.255.0
```

42.5 show interface meth

该命令用于显示管理口的工作状态。

命令

show interface meth { *port* }

参数

port —— 管理端口号，该机型管理口为 1/0/1。

模式

管理接口配置模式（interface meth）

特权要求

无

示例

显示管理口的工作状态：

```
TL-ST5016F(config)# show interface meth 1/0/1
```

第43章 U 盘开局配置命令

说明：

本功能仅 TL-ST5016F 有。

U 盘开局是指设备在开局部署时，用户预先将开局文件存储在 U 盘中，然后将 U 盘插入设备，通过从 U 盘下载开局文件来对设备实现目标版本以及相关业务的部署。

43.1 set device usb-deployment

该命令用于使能/禁用 U 盘开局功能。设备默认使能 U 盘开局功能。

命令

set device usb-deployment { enable | disable }

参数

enable | disable —— 使能/禁用 U 盘开局功能。

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

使能设备的 U 盘开局功能：

TL-ST5016F(config)# set device usb-deployment enable

43.2 set device usb-deployment password

该命令用于配置 U 盘开局的认证密码。它的 no 命令用于删除 U 盘开局的认证密码。

命令

set device usb-deployment password *password*

no set device usb-deployment password

参数

password —— U 盘开局认证密码。该参数为字符串类型，长度范围为 1 ~ 64。

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

设置设备 U 盘开局认证密码为 admin：

TL-ST5016F(config)# set device usb-deployment password *admin*

43.3 set device usb-deployment config-file password

该命令用于配置 U 盘开局时用于对配置文件进行加密的密码。它的 no 命令用于删除 U 盘开局时对配置文件进行加密的密码。

命令

set device usb-deployment config-file password *password*

no set device usb-deployment config-file password

参数

password —— U 盘开局时对配置文件进行加密的密码。该参数为字符串类型，长度范围为 1 ~ 64。

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

设置设备 U 盘开局时用于对配置文件进行加密的密码为 admin：

TL-ST5016F(config)# set device usb-deployment config-file password *admin*

43.4 set device usb-deployment hmac

该命令用于使能 U 盘开局时对配置文件的 HMAC 校验功能。它的 no 命令用于禁用 U 盘开局时对配置文件的 HMAC 校验功能。

命令

set device usb-deployment hmac

no set device usb-deployment hmac

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 U 盘开局的 HMAC 校验功能：

```
TL-ST5016F(config)# set device usb-deployment hmac
```

43.5 show device usb-deployment configuration

该命令用于显示 U 盘开局功能的配置信息。

命令

show device usb-deployment configuration

模式

全局配置模式

特权要求

无

示例

显示 U 盘开局功能的配置信息：

```
TL-ST5016F(config)# show device usb-deployment configuration
```