ZJ-IES-900
交换机命令行手册

Version 1.0

版本记录	建立时间	文档内容
V1.0	2023.09.06	建立命令行手册正式版文档

中芯数通量子科技（无锡）有限公司

目　　录

一、 命令行管理模式概述

ZJ-IES-900

1.1 命令行简介

ZJ-IES-900 网络交换机支持基于命令行的管理模式。用户可以通过在命令行中配置相应的命令来实现对交换机的监测、控制和管理。

Switch 提供的命令行具有如下特点：

- 全部命令具有帮助信息，帮助用户理解命令的使用方法和功能。
- 具有命令历史记录功能。
- 支持用户权限控制功能。
- 支持通过 telnet、SSH 的方式远程登录设备的命令行。

1.2 命令行的基础操作

1.2.1 命令行模式

ZJ-IES-900 网络交换机提供的命令行根据命令实现的功能，以及对应的操作权限，将命令安装在不同的模式下。

具体每种模式的权限和功能描述信息见下表。

模式	模式描述	进入方法	命令行标识	退出方法
普通用户模式	该模式下用户可以配置交换机的基本信息，显示参数等等	登录交换机，输入用户和密码。	administrator>	exit 退出当前模式
特权用户模式	该模式下，用户可以配置交换机的基本信息，如系统时间，交换机名称等，不可以配置交换机的运行信息	在普通用户模式下输入 **enable** 及相关密码。	administrator#	exit 退出当前模式
全局配	该模式下，用户可以配	在特权用户模式	administrator(	exit

置模式	置交换机所有运行参数	下，输入 **config**。	config)#	退出当前模式
物理层接口配置模式	在该模式下，用户可以配置交换机以太物理接口的参数	在全局模式下，输入 **ifconfig ethernet-port** *port-number* 命令。	administrator(port[]S)#	exit 退出当前模式
物理层接口批量配置模式	在该模式下，用户可以批量配置交换机以太物理接口的参数	在全局模式下，输入 **ifconfig port-range** *port-list* 命令。	administrator(port-range[])#	Exit 退出当前模式

1.2.2 命令行帮助信息

ZJ-IES-900 网络交换机提供的命令行支持多种帮助方式，帮助用户快速理解命令的含义和使用方法。

帮助信息的获取方法见下表。

命令	功能描述
abbreviated-command-entry**?**	获得一个以特定字符串（abbreviated-command-entry）开头的所有的命令列表。 例如： administrator> **i**? ifconfig Interface configuration mode igmp IGMP configuration ip IP setting
abbreviated-command-entry<**Tab**>	补全一个不完全输入的命令。 例如： administrator#**display f**<Tab> administrator#**display fdb**
?	列出该模式下所有的命令。 例如： administrator#**?**
command **?**	列出某一个命令的所有关键字和可选项，及其简短的帮助信息。

	administrator#**display** ?

1.2.3 命令行快捷键

ZJ-IES-900 网络交换机提供的命令行支持一系列快捷键，目前支持的快捷键及其含义见下表。

命令	功能描述
up arrow	上一条输入的命令
down arrow	下一条输入的命令
left arrow	光标向左移动一个字符
right arrow	光标向右移动一个字符
backspace	删除光标所在位置的前一个字符
Ctrl+d	删除光标所在位置的后一个字符
Ctrl+a	将光标移动到行首
Ctrl+e	将光标移动到行尾
Ctrl+k	将光标以后的字符全部删除
Ctrl+x	将光标左边的字符全部删除
Ctrl+z	从非特权用户模式退到特权用户模式

1.2.4 命令行错误提示

下表中列举了命令行中可能出现的错误提示，以及出现该问题可能的原因。

错误信息	信息描述	获取帮助
命令未知，不准确：例如： administrator# display co * " co " No matched command.	重新查看需要输入的命令	
命令未被证实：例如： administrator# display a * " a " Ambiguous input.	输入命令中某个名称不足以使交换机识别所输入的命令	在命令后面添加“？”获得相关命令和注释，例如：administrator# display a aggregation Ports

		aggregation arp ARP table information
命令不完整，例如： administrator# display * " display " Incompleted command.	输入命令不能使交换机判定所要执行的任务，需要可以使交换机识别其操作的命令	在命令后面添加“？”获得相关命令和注释，例如：administrator# display a aggregation Ports aggregation arp ARP table information

二、 系统功能配置

2.1 文件管理

2.1.1 系统软件管理

ZJ-IES-900 网络交换机运行过程中所需要的文件(如:系统软件、配置文件等)均保存在设备的存储设备中。为了方便用户对存储设备进行有效的管理，设备以文件系统的方式对这些文件进行管理。

文件系统功能主要包括目录的创建和删除、文件的拷贝和显示等。缺省情况下，对于有可能丢失数据的命令（比如删除文件、覆盖文件等命令），文件系统将提示用户进行确认。

ZJ-IES-900 网络交换机允许用户从远程服务器中下载新版本系统软件，同时也支持将设备上现存的系统软件上传至远端服务器上备份。

2.1.2 配置文件管理

ZJ-IES-900 网络交换机允许用户将配置信息以文件的形式存储在设备中，系统默认的配置文件名称为 startup_config.conf。一旦配置文件被存储，当下一次系统重新启动的时候，配置文件中的信息会自动被重新配置到交换机中。

配置信息文件可以使用命令 update 或 backup 实现文件上传/下载的功能。

执行命令 display startup-config 可以显示系统存储的配置信息；执行命令 display current-config 则可以显示系统当前的配置信息。

命令	功能描述
save	将配置文件写入到flash文件系统中，当下一次系统重新启动的时候，存储的配置信息会自动被配置
display startup-config	显示存储的配置信息
display current-config	显示当前系统的配置信息

2.2 用户管理

ZJ-IES-900 网络交换机采用多用户管理的方式。用户在登录时需要输入用户名和密码，系统拥有缺省用户 administrator，密码为 admin。

用户可以按照下述配置步骤增加一个新的用户，并为其分配操作权限。

步骤	命令	描述
第 1 步	**user name** *USERNAME* **password** *PASSWORD*	用户登录： *USERNAME*：用户名； *PASSWORD*：密码信息（密码至少由 8 位组成，其中包括数字、大写字母、小写字母或符号）
第 2 步	**user name** *USERNAME* **privilege** *<1-15>*	用户登录权限： *USERNAME*：用户名； *<1-15>*：用户权限等级；
第 3 步	**save**	保存配置信息
第 4 步	**display user**	设置 Telnet 服务

2.3 Ping 诊断功能

2.3.1 Ping 功能简介

Ping 是最常使用的故障诊断与排除命令，常用于测试两台主机间是否存在连接。ping 功能一般用 ICMP ECHO 报文组实现。它由一组 ICMP 回应请求报文组成，如果网络正常运行将返回一组回应应答报文。

ZJ-IES-900 网络交换机支持 ping 功能。在使用 ping 功能之前，请确认交换机已经配置了正确的 IP 地址。

2.3.2 Ping 相关命令

用户可以按照下述配置步骤，进行一次完整的 ping 操作。

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ip address** *A.B.C.D* [*A.B.C.D*] *vlan-id*	配置交换机的 ip 地址 *A.B.C.D*：IP 地址； [*A.B.C.D*]：子网掩码； *vlan-id*：vlan 的 ID，范围<1-4094>；
第 3 步	**exit**	退出全局配置模式进入特权用户模式
第 4 步	**ping** *A.B.C.D* **[count** *<1-65535>***]** **[size** *<64-4096>***]**	测试远程主机是否可达 *A.B.C.D* ：测试主机 IP 地址 <*1-65535*>：ICMP packet size <64-*4096*>： Packet send number

2.3.3 典型配置举例

配置示例 2-3：

如下图所示，主机通过网线与交换机相连接。用户可以通过 ping 命令确认主机是否与交换机连接成功，交换机也可以通过 ping 命令与主机进行数据的传递。

图 2-2 ping 配置示例拓扑图

设置交换机的 IP 地址为 20.0.0.10，连接 PC 机的 IP 地址为 10.168.0.221，发送报数为 3 ，报文大小 100 ，由于目的 IP 地址与 PC 机的 IP 不符，所以未连接通。

配置过程：

```
administrator#config
administrator(config)#ip address 20.0.0.10 1
administrator(config)#exit
administrator#ping 10.168.0.221 size 100 count 3
```

ping: sendto: Network is unreachable

配置示例 2-4：

在图 2-2 的基础上，设置交换机的 IP 地址为 10.168.0.222，显示连接成功

配置过程：

administrator**#config**

administrator(config)**#ip address 10.168.0.222 1**

administrator(config)**#exit**

administrator**#ping 10.168.0.221 size 100 count 3**

```
PING 10.168.0.221 (10.168.0.221): 100 data bytes
108 bytes from 10.168.0.221: seq=0 ttl=128 time=1.673 ms
108 bytes from 10.168.0.221: seq=1 ttl=128 time=0.500 ms
108 bytes from 10.168.0.221: seq=2 ttl=128 time=0.572 ms

 --- 10.168.0.221 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
```

2.4 Telnetd 功能

2.4.1 Telnetd 原理介绍

Telnet 是进行远程登录的标准协议和主要方式，它为用户提供了在本地计算机上完成远程主机工作的能力。telnetd 模块实现 telnet 服务器功能，即允许 telnet 客户端远程登录到设备，从而实现被 telnet 客户端远程登录和管理的功能。

ZJ-IES-900 网络交换机支持用户在远端通过 Telnet 协议登录到设备的命令行上。登录成功后，用户可以通过 Telnet 远端执行该用户权限支持的全部命令行操作。

2.4.2 Telnetd 缺省配置

Telnetd 功能缺省配置值如下表所示：

功能	缺省值

telnet 服务器连接上限	5
telnet 服务器连接物理端口	所有端口

2.4.3 Telnetd 功能配置

关闭 Telnetd 服务：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**telnetd session** <0-4 > off	关闭指定会话号的 telnet 服务器
第 3 步	**exit**	返回特权模式
第 4 步	**display telnetd**	显示 telnet server 当前配置

三、 系统日志配置

3.1 系统日志功能概述

ZJ-IES-900 网络交换机支持系统日志功能。可以依据用户配置的日志级别，将交换机中的系统消息或调试信息发送到用户期望的目的地。

- 支持将日志消息输送到本地日志文件、控制台或者日志主机上。当输送到本地日志文件时，设备掉电重启不会导致日志信息的丢失。

用户可以通过配置指定系统日志的消息格式。默认的日志格式为："timestamp module-level- Message content."。

3.2 系统日志功能配置

3.2.1 系统日志缺省配置

ZJ-IES-900 网络交换机的系统日志功能缺省配置如下表所示。

功能	缺省值
设置日志消息输出到控制台	该功能默认情况下是开启的，输出等级为 informational。
设置日志信息输出到文件	默认关闭
设置日志主机	没有日志主机的配置信息
设置日志输出到 monitor	默认关闭
系统日志的启动和关闭	日志功能启动
日志速率的配置	不限制日志的发送速率
日志信息的时间戳设置	使用标准时间

3.2.2 系统日志源配置

系统日志的启动和关闭

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**syslog on**	启动系统日志
第 3 步	**exit**	返回特权模式
第 4 步	**display syslog**	显示配置情况

日志信息的时间戳设置

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**syslog timestamp-mode (date-time| relative-start | null)**	设置时间戳： date-time：标准时间 mm-dd-yyyy hh-mm-ss，例如“FEB-22-2005 14:27:33”； relative-start：交换机启动时间 hh-mm-ss，例如“29:40:6”表示 29 小时 40 分 6 秒； null：日志消息中没有时间戳；
第 3 步	**exit**	返回特权模式
第 4 步	**display syslog**	显示配置情况

日志速率的配置

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**syslog interval** *<1-1000>*	*<1-1000>*：设置每秒发送的日志数目；
第 3 步	**exit**	返回特权模式

3.2.3 系统日志目的配置

设置日志消息输出到控制台

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**[no] syslog console-level (<0-7> | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings)**	配置和启动将日志信息输出到 console 以及参数信息，no 形式命令关闭该日志输出方向； <0-7> 日志等级 alerts 需要立即动作 (等级=1) critical 严重状态 (等级=2) debugging 调试消息 (等级=7) emergencies 系统不可以使用 （等级=0) errors 错误的条件 (等级=3) informational 通告事件 (等级=6) notifications 正常的处于关键性条件的事件(等级=5) warnings 警告条件 (等级=4)
第 3 步	**exit**	返回特权模式
第 4 步	**display syslog**	显示配置情况

设置日志主机

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**[no] syslog host** *A.B.C.D* **(<0-7> | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings)**	配置和启动将日志信息输出到日志主机以及参数信息，no 形式命令关闭该日志输出方向。 *A.B.C.D*：日志主机的 ip <0-7> 日志等级

		alerts 需要立即动作 (等级=1) critical 严重状态 (等级=2) debugging 调试消息 (等级=7) emergencies 系统不可以使用 (等级=0) errors 错误的条件 (等级=3) informational 通告事件 (等级=6) notifications 正常的处于关键性条件的事件(等级=5) warnings 警告条件 (等级=4)
第 3 步	**exit**	返回特权模式
第 4 步	**display syslog**	显示配置情况

设置日志信息到文件

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**[no] syslog file <0-7>**	配置和启动将日志信息记录到 flash 中的文件中，no 形式命令关闭该日志输出方向。 <0-7> 日志等级 alerts 需要立即动作 (等级=1) critical 严重状态 (等级=2) debugging 调试消息 (等级=7) emergencies 系统不可以使用 (等级=0) errors 错误的条件 (等级=3) informational 通告事件 (等级=6) notifications 正常的处于关键性条件的事件(等级=5) warnings 警告条件 (等级=4)
第 3 步	**exit**	返回特权模式

第 4 步	**display syslog file**	显示配置情况

3.2.4 监控与维护

用户通过使用下表命令可以实现对日志功能的监控与维护。

命令	描述
display syslog	显示配置情况
display syslog file	显示日志文件内容

3.2.5 典型配置举例

配置示例 3-1：

如图 3-1 所示，配置交换机，将 Warnning 级别之上的全部日志信息发送至日志主机 10.0.0.102。

图 3-1 配置示例图

配置过程：

administrator#**config**

administrator(config)# **ip address 10.0.0.60 255.0.0.0 1**

administrator(config)#**syslog on**

administrator(config)#**syslog timestamp-mode date-time**

administrator(config)# **syslog interval 2**

administrator(config)#**syslog host 10.0.0.102 warings**

administrator(config)#**exit**

administrator#**display syslog**

```
Syslog        :  enable
Interval      :  2 messages per second
Time stamp    :  date-time
Dest      Status    Level
---------------------------------
console   enable    informational(6)
file      disable   warnings(4)
Syslog host:
Target Address     Port      Level
---------------------------------
10.0.0.102         0         warnings(4)
```

交换机日志文件显示信息：

```
Syslog in file  :
1970-01-01,23:12:05 SYSTEM-6-:fastethernet1/0/8 Link Down.
1970-01-01,23:12:05 MIB-2-3-LINK_DOWN:port8 Link Down
1970-01-01,23:12:05 SYSTEM-6-:port8 Link Down.
1970-01-01,23:13:29 SYSTEM-6-:fastethernet1/0/8 Link Up.
1970-01-01,23:13:29 MIB-2-3-LINK_UP:port8 Link UP
1970-01-01,23:13:29 SYSTEM-6-:port8 Link Up.
```

四、 SNMP 功能配置

4.1 SNMP 原理介绍

4.1.1 SNMP 基本概念

SNMP，全称 Simple Network Management Protocol，是当前计算机网络中应用最为广泛的网络管理协议。它也是管理互联网的标准协议之一。

在结构上，SNMP 可以分为代理（agent）和网络管理系统（Network Management Station，NMS）两部分。即 SNMP 采用的是代理/管理站模式。

其中，NMS 是运行客户端程序的工作站，Agent 是指运行在网络设备如交换机上的服务器端软件。Agent 中负责维护管理信息库（management information base ，MIB）。

当 SNMP Agent 收到 NMS 发出的关于 MIB 变量的查询报文 Get-Request、Get-Next-Request、Get-Bulk-Request 或 Set-Request 时，Agent 根据报文类型对 NMS 所请求的 MIB 变量进行 Get 或 Set 操作，然后根据操作结果生成 Response 报文，并作为响应发送给 NMS。

另一方面，当 SNMP Agent 收到有关设备本身状态变化，如冷/热启动或异常事件时，就生成一个 Trap 报文并主动发送到 NMS 以报告这些重要的事件。

ZJ-IES-900 网络交换机的 SNMP Agent 同时支持 SNMPv1、SNMPv2 和 SNMPv3 这三个版本。

4.1.2 SNMP V1/V2 介绍

SNMPV1 是一种简单的请求 / 响应协议。网络管理系统发出一个请求，管理器则返回一个响应。这一行为的实现是通过使用四种协议操作中的其中任一种完成的。这四种操作分别是 GET、GETNEXT、SET 和 TRAP 。 NMS 通过 GET 操作，从 SNMP 代理处得到一个或更多的对象（实例）值。如果代理处不能提供请求列表中所有的对象（实例）值，它也就不提供任何值。 NMS 使用 GETNEXT 操作请求代理从请求列表或对象列表中取出下一个对象实例值。 NMS 通过 SET

操作向 SNMP 代理发送命令，要求对对象值重新配置。 SNMP 代理通过 TRAP 操作不定时的通知 NMS 所发生的特定事件。

与 SNMPv1 单纯的集中式管理模式不同，SNMPv2 支持分布式/分层式的网络管理结构，在 SNMPv2 管理模型中有些系统可以同时具有管理器和代理的功能，作为代理，它可以接收上一级管理系统的命令，访问其存储的本地信息，也可以提供它所负责的管理域中其他代理的信息摘要，向上级管理器发送 Trap 信息。

4.1.3 SNMP V3 介绍

SNMPv3 采用基于用户的安全模型（user-based security model）。无论是 NMS 向 SNMP Agent 发查询报文，还是 SNMP Agent 向 NMS 发 Trap 报文，NMS 和 SNMP Agent 之间都是以某个用户的名义进行通信。SNMP NMS 和代理双方都维护一张本地 SNMP 用户表，用户表记录用户名字、用户关联的引擎 ID、是否需要鉴别以及鉴别密钥等信息。SNMP 网管和代理中任何一方收到对方发送的消息时，接收方查找该用户表获取该用户的鉴别和加密信息，从而对消息的内容进行正确解析，并做出适当回应。SNMP 用户的配置就是通过命令行中的口令信息生成密钥，并在交换机的本地 SNMP 用户表中添加一个用户。

4.2 SNMP V1/V2/V3 管理配置

4.2.1 SNMP V1/V2 配置

SNMP Agent 为了保护自身及其管理的 MIB 不受到未被授权的访问，提出了团体的概念。在某一个团体内的管理站必须在所有对 agent 的 Get 和 Set 操作中使用该团体的名字，否则其请求不被受理。

团体名是用不同的字符串来标识不同的 SNMP 团体。不同的团体可以具有只读（read-only）或读写（read-write）访问权限。具有只读权限的团体只能对设备信息进行查询，而具有读写权限的团体除了可以对设备信息进行查询之外还可以对设备进行配置。

当 SNMPv1 和 SNMPv2 采用团体名认证方案时，与设备认可的团体名不符合

的 SNMP 报文将被丢弃。完整的配置（包括用户的配置）过程如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
(可选)	**snmp view** *view-name oid-tree* [*mask*] **(included | excluded)**	定义视图及其包含的 MIB 树范围 *view-name*：视图名，长度不超过 32 字符的字符串； *oid-tree*：OID 树，深度与视图名长度之和不超过 62； *mask*：OID 树的掩码，深度不超过 128，格式为 OID 的形式，OID 的每项只能为 0 或者 1； included：包含 oid-tree； excluded：不包含 oid-tree；
第 2 步	**snmp community** *community-name* **[view** *view-name* **] (ro | rw)**	设置团体名、其对应的视图和访问权限 *community-name*：指定团体名，类型为字符串，长度必须不超过 32； *view-name*：视图名，长度必须不超过 32； ro：只读； rw：读写；
第 3 步	**exit**	返回特权模式
第 4 步	**display snmp community**	显示团体信息

⚠注意：

SNMPv1 和 SNMPv2 都采用团体名认证方案，与设备认可的团体名不符的 SNMP 报文将被丢弃。

4.2.2 SNMP V3 配置

SNMPV3 采用 usm(user-based security model)基于用户的安全模型。usm 提出

了访问组（group）的概念：一个或多个用户对应于一个访问组，每个访问组设定相应的读、写、通告视图，访问组中的用户拥有在该视图内的权限。发送 Get 和 Set 等请求的用户所在的访问组必须具有和其请求相应的权限，否则请求不被受理。

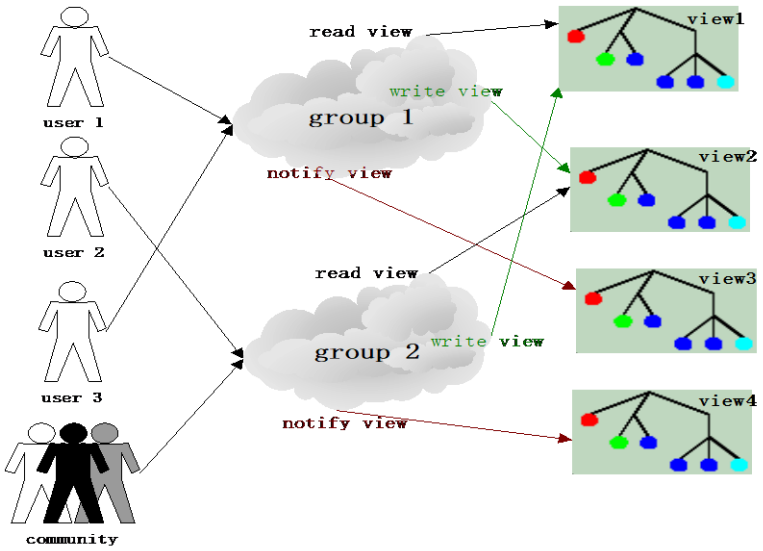


图 4-1 SNMPv3 组概念图

由上图可以看出，NMS 对交换机正常的访问，除了需要配置好用户以外，还需要确定该用户属于哪个访问组，访问组拥有的视图权限，以及各个视图。完整的配置（包括用户的配置）过程如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**snmp view** *view-name oid-tree* [*mask*] **(included | excluded)**	定义视图及其包含的 MIB 树范围 *view-name*：视图名，长度不超过 32 字符的字符串； *oid-tree*：OID 树，深度与视图名长度之和不超过 62； *mask*：OID 树的掩码，深度不超过 128，格式为 OID 的形式，OID 的每项只能为 0 或者 1； included：包含 oid-tree； excluded：不包含 oid-tree；

第 3 步	**snmp user** *username* **[remote** *engineid***] [authentication (md5 | sha)** *authpassword* **] [authkey]**	以口令形式增加一个 SNMP 用户 *username*：用户名； *engineid*：用户关联的 SNMP 引擎 ID，命名必须以偶数字节来命名； *authpassword*：鉴别口令；
第 4 步	**snmp access** *groupname* ［**read** *readview*］［**write** *writeview*］［**notify** *notifyview*］［**context** *contextname* **(exact | prefix)**］ **usm (noauthnopriv | authnopriv| authpriv)**	增加一个 SNMP 访问组 *groupname*：组名，长度不超过 32 字符的字符串； *readview*：读视图名，长度不超过 32 字符的字符串； *writeview*：写视图名，长度不超过 32 字符的字符串； *notifyview*：通告视图名，长度不超过 32 字符的字符串； *contextname*：上下文名字或者前缀，长度不超过 32 字符的字符串； noauthnopriv：不需认证不需加密； authnopriv：需认证不需加密； authpriv ：需认证需加密；
第 5 步	**snmp group** *groupname* **user** *username* **usm**	确定用户属于哪个访问组 *groupname*：组名，长度不超过 32 字符的字符串； *username*：用户名，长度不超过 32 字符的字符串；
第 6 步	**exit**	返回特权模式
第 7 步	**display snmp group** **display snmp access** **display snmp view** **display snmp user**	显示访问组表中所有表项

4.2.3 SNMP V1/V2 TRAP 配置

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ip address** *A.B.C.D* [*A.B.C.D*] *<1-4094>*	配置交换机的 ip 地址 *A.B.C.D*：IP 地址； [*A.B.C.D*]：子网掩码； *vlan-id*：vlan 的 ID，范围<1-4094>；
第 3 步	**snmp host** *A.B.C.D* **version (1|2c)** *NAME* [**udpport** *<1-65535>*]	配置 SNMPv1/v2 Trap 目标主机 *A.B.C.D*：NMS IP 地址 *NAME*：SNMPv1/v2c 团体名 *<1-65535>*： 目标主机接收 trap 的端接收端口号，缺省设置为 162；
第 4 步	**exit**	返回特权模式
第 5 步	**display snmp host**	显示配置情况

4.2.4 SNMP V3 TRAP 配置

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ip address** *A.B.C.D* [*A.B.C.D*] *vlan-id*	配置交换机的 ip 地址 *A.B.C.D*：IP 地址； [*A.B.C.D*]：子网掩码； *vlan-id*：vlan 的 ID，范围<1-4094>；
第 3 步	**snmp host** *A.B.C.D* **version** 3 **(noauthnopriv | authnopriv|authpriv)** *NAME* **[udpport** *<1-65535>*]	配置 SNMPv3 Trap 目标主机 *A.B.C.D*： HOST IP 地址； *NAME*：SNMPv3 用户名； *<1-65535>*： 目标主机接收端口号，缺省设置为 162；

		noauthnopriv：不需认证不需加密； authnopriv：需认证不需加密； authpriv ：需认证需加密；
第 4 步	**exit**	返回特权模式
第 5 步	**display snmp host**	显示配置情况

4.2.5 SNMP 其他配置

sysContact 配置：

网管人员的标识及联系方法 sysContact 是 MIB system 组的一个变量，其作用是设置管理交换机的相关网管人员的标识及联系方法。

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**snmp contact** *STRING*	设置网管人员的标识及联系方法 *STRING*：指定网管人员的标识与联系方法，类型为字符串；
第 3 步	**exit**	返回特权模式
第 4 步	**display snmp config**	显示配置情况

TRAP 全局开关：

Trap 主要用于向网管工作站（NMS）提供某些交换机本身的重要事件。如当收到一个含有错误团体名的请求并被设置允许发送 snmp trap 时交换机就会向 NMS 发送一个认证失败的 trap 消息。

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**snmp traps (on | off)**	允许/禁止交换机发送 trap
第 3 步	**exit**	返回特权模式
第 4 步	**display snmp config**	显示配置情况

设备位置信息配置：

设备位置信息 sysLocation 是 MIB system 组的一个变量，用于描述交换机放置的物理位置。

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**snmp location** *STRING*	设置交换机位置 *STRING*：指定交换机放置的物理位置，类型为字符串；
第 3 步	**exit**	返回特权模式
第 4 步	**display snmp config**	显示配置情况

4.2.6 监控与维护

命令	描述
display snmp community	显示所有的团体名，对应的视图名，及权限
display snmp host	显示所有 trap 目标主机的 IP 地址
display snmp config	显示本地 SNMP 引擎 ID，网管人员的标识及联系方法，交换机所在位置，TRAP 开关
display snmp view	显示所有视图名，和视图范围
display snmp access	显示所有访问组名，和访问组的属性
display snmp group	显示用户到访问组的所有映射关系
display snmp user	显示所有用户，和用户所采用的鉴别加密协议
display snmp statistics	显示 SNMP 包统计信息

4.2.7 典型配置举例

配置示例 4-1：

设置本地交换机 IP 地址为 20.0.0.10，用户 guestuser1，采用 md5 鉴别算法，鉴别口令为 Switch，来访问 mib2 的视图。视图范围包括 1.3.6.1.x.1 下的所有 MIB 变量,创建 guestgroup 的访问组，安全模式安全模型为 usm，安全等级为鉴别但不加密，可读视图名为 mib2，这样可以完成安全等级为 usm 的 guestuser1 用户映射到访问组 guestgroup 的过程，并显示结果。

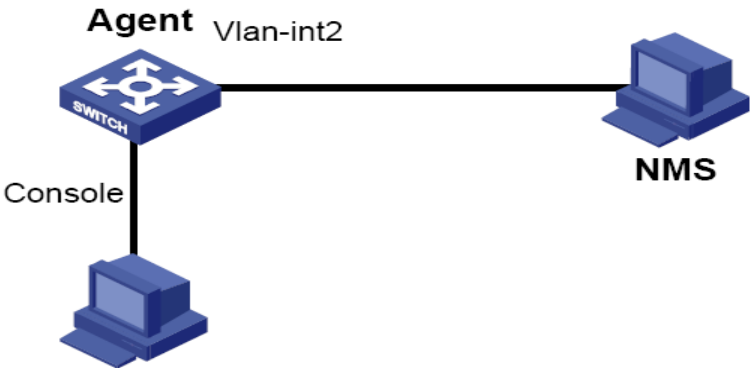


图 4-2 V3 访问控制配置举例图

配置过程：

administrator#**config**

administrator(config)#**ip address 20.0.0.10 1**

administrator(config)#**snmp view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included**

administrator(config)#**snmp user guestuser1 authentication md5 Switch**

administrator(config)#**snmp access guestgroup read mib2 usm authnopriv**

administrator(config)#**snmp group guestgroup user guestuser1 usm**

administrator(config)#**exit**

administrator# **display snmp access**

```
  Index:          0
  Group:          initial
  Security Model: usm
  Security Level: authnopriv
  Context Prefix: --
  Context Match:  exact
  Read View:      internet
  Write View:     internet
  Notify View:    internet

  Index:          1
```

```
  Group:          gusetgroup
  Security Model: usm
  Security Level: authnopriv
  Context Prefix: --
  Context Match:  exact
  Read View:      mib2
  Write View:     --
  Notify View:    internet

  Index:          2
  Group:          initialnone
  Security Model: usm
  Security Level: noauthnopriv
  Context Prefix: --
  Context Match:  exact
  Read View:      system
  Write View:     --
  Notify View:    internet
```

```
administrator# display snmp group

Index    GroupName         UserName              SecModel
-------------------------------------------------------
0        initialnone        one                    usm
1        initial           md5nopriv              usm
2        initial           shanopriv              usm
3        guestgroup         guestuserl             usm
```

配置示例 **4-2**：

Trap 是 Agent 主动向 NMS 发送的信息，用于报告一些紧急的重要事件。如下图所示，配制交换机的 IP 地址为 20.0.0.10，NMS 主机的 IP 地址配置为 20.0.0.221，用户名 Switch，SNMP 版本 v3，鉴别但不加密。

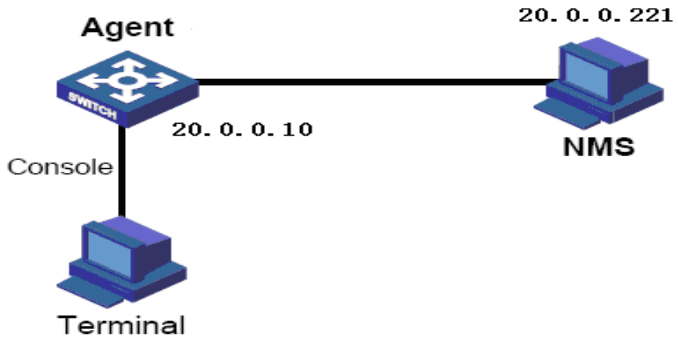


图 4-3　SNMPv3Trap 配置示例图

administrator#**config**

administrator(config)#**ip address 20.0.0.10 1**

administrator(config)#**snmp host 20.0.0.221 version 3 authnopriv　Switch**

administrator(config)#**exit**

administrator# **display snmp host**

```
Index:          0
IP family:      IPv4
IP address:     20.0.0.221
Port:           162
User Name:      Switch
SNMP Version:   v3
Security Level:   authnopriv
TagList:        bridge config interface rmon snmp ospf
```

五、 时间管理功能配置

5.1 时间管理介绍

ZJ-IES-900 网络交换机提供两种系统时间设置方法：

- 使用 SNTP 协议使交换机系统时间与 SNTP 服务器的时间同步。
- 手动设置系统时间。

当使用 SNTP 协议方式获取时间时，同步的时间为格林威治时间。此时设备会根据系统时区的设置来转化成本地时间。

5.2 时间配置功能

5.2.1 时间配置缺省配置

功能	缺省值
缺省时间	2000-01-01 08:00:00.000
缺省时钟模式	系统时钟
缺省时区偏移	+08:00

⚠注意：

如果是支持时钟芯片的设备，则采用时钟芯片的缺省时间

5.2.2 时间设置功能配置

步骤	命令	描述
第 1 步	time set <0-23> <0-59> <0-59> <2000-2099> <1-12> <1-31>	设置系统时间，依次是：小时，分钟，秒，年，月，日；
第 2 步	**display time**	显示系统时间及配置情况

5.2.3 时区管理功能配置

步骤	命令	描述

第 1 步	**time timezone** {+|-} <0-11> <0-59> *TIMEZONE*	设置系统时区： • + 东半球时区 • - 西半球时区 • <0-11> 时区偏移小时 • <0-59> 时区偏移分钟 默认为北京时间，即东半球 8 小时整 *TIMEZONE*： 时区名称；
第 2 步	**time set** <0-23> <0-59> <0-59> <2000-2099> <1-12> <1-31>	设置系统时间，依次是：小时，分钟，秒，年，月，日；
第 3 步	**display time**	显示系统时间及配置情况

5.2.4 监控与维护

命令	描述
display time	显示时间信息

⚠注意：

如果是支持时钟芯片的设备，则采用时钟芯片的缺省时间

5.2.5 典型配置举例

配置示例 5-1：

配置交换机的时区和当前系统时间。

配置过程：

```
administrator#time timezone + 8 00 beijing
administrator#time set 13 34 20 2017 07 04
administrator#display time
Clock display mode: default
Current system time: 2017-07-04,13:34:25.849
Timezone offset: +08:00-beijing
```

5.3 SNTP 功能配置

5.3.1 SNTP 协议缺省配置

表 5-2 SNTP 功能缺省配置表

功能	缺省值
SNTP 服务器地址	不存在

5.3.2 SNTP 协议功能配置

配置 SNTP 服务器地址后，设备将每隔 10 秒钟尝试一次从 SNTP 服务器获取时钟信息，并且每次从 SNTP 获取时钟信息的最大超时时间为 10 秒。

配置 SNTP 服务器地址的配置方法如下：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**sntp server** *A.B.C.D*	配置 SNTP 服务器地址 *A.B.C.D*：服务器的 ip 地址；
第 3 步	**exit**	返回特权模式
第 4 步	**display sntp**	显示配置情况

5.3.3 监控与维护

命令	描述
display time	显示时间信息

5.3.4 典型配置举例

配置示例 5-2：

配置交换机通过 SNTP 协议从服务器中同步系统时间。

网络拓扑如图 5-1 所示：

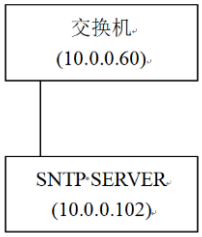


图 5-1 SNTP 时间同步拓扑示例

配置过程：

administrator(config)#**display time**

```
Clock display mode:  default
Current system time:  2017-07-04,13:35:25.860
Timezone offset: +08:00-yazhou
```

administrator#**config**

administrator(config)#ip address 10.0.0.60 1

administrator(config)#**sntp server 10.0.0.102**

administrator(config)#**exit**

administrator#**display sntp**

```
SNTP server address:10.0.0.102
SNTP Server        Stratum   Version   Synchronize Time.
-------------------------------------------------------
10.0.0.102          10         1       2017-07-04, 17:15:48
```

administrator#**display time**

```
Clock display mode:  default
Current system time:  2017-07-04,13:37:35.572
Timezone offset: +08:00-yazhou
```

六、 告警功能配置指南

6.1 告警功能概述

针对工业环境中高安全性的需求，ZJ-IES-900 网络交换机提供了基于多种事件的告警功能。告警功能主要针对设备的运行环境进行监控，监控的告警事件包括：电源掉电告警、温度超出阈值告警、电压超出阈值告警、端口层次告警等告警事件。

当产生告警时，可以通过多种方式通知用户，如：把告警信息输出到继电器故障灯、发送到 SNMP server、将告警信息发送到系统日志输出。网络管理员由此可以在第一时间得知故障的出现，从而采取相应的措施，排除故障。

6.1.1 监控的告警事件

温度异常告警

ZJ-IES-900 网络交换机可以实时侦测设备的温度值，当温度异常时，设备可以根据用户的配置，以不同的方式发出告警。

用户可以根据环境情况，自行配置低温告警阈值和高温告警阈值。当设备当前温度低于低温阈值时，产生低温告警事件；当设备当前温度高于高温阈值时，产生高温告警事件。

温度异常告警支持继电器输出、Trap 输出、Syslog 输出三种方式。

端口状态告警

ZJ-IES-900 网络交换机提供三种基于端口状态的告警事件：端口 LinkFault 告警、端口 LinkDown 告警以及端口 not-forwarding 告警。任意一种基于端口的告警事件均支持继电器输出、Trap 输出、Syslog 输出这三种告警输出方式。

- LinkFault 告警：表示对端链路信号丢失，此功能只针对光介质端口。
- LinkDown 告警：表示端口处于 Link down 状态。
- Not-forwarding 告警：表示端口在所有 VLAN 中均处于阻塞的状态。

6.1.2 告警输出方式

继电器输出

配置继电器输出开启后，告警信息将同时输出到继电器和故障指示灯。只要设备上仍存在任意一个告警信息，则继电器会输出告警。直到所有告警信息被清除，继电器才会恢复正常输出。

继电器输出没有全局的开关，只在各种告警事件下存在各自的继电器告警输出开关。

Trap 输出

配置 Trap 输出为开启后，告警功能将会以 Trap 的形式把告警信息发送到 SNMP 服务器。Trap 输出有全局的开关，在各种告警事件下也存在各自的 Trap 告警输出子开关，只有当全局开关和监控的告警事件下的子开关同时开启时，才能产生告警信息的 Trap 输出。

Trap 中告警信息的内容包括：

告警状态： asserted（当前正在发生告警）、cleared（告警恢复）或 clearall（清除所有的告警信息）；

告警事件源：全局告警（用 Device 表示）或端口告警（用端口号表示）；

时间戳：告警产生的时间，以绝对时间的形式表示；

告警事件类型：告警事件和描述信息也将记录在 Trap 的内容之中。

Syslog 输出

配置 Syslog 输出为开启后，告警功能将会以系统日志的方式输出。Syslog 输出具有全局的开关，同时在各种告警事件下也存在各自的 Syslog 告警输出子开关，只有当 Syslog 全局开关和告警事件下的子开关同时开启时，才能产生告警信息的 Syslog 输出。

Syslog 中告警信息的内容包括：

Facility（模块名）：env-monitor

Severity（级别）：为 error 级别

Mnemonics（消息名称）：根据事件类型定义

Msg-body（正文）：根据消息不同描述发生的事件内容

6.2 告警功能的配置

6.2.1 缺省配置

功能	缺省值
告警信息全局 syslog 输出功能	关闭
告警信息全局 Trap 发送功能	关闭
电源掉电事件告警输出功能	trap 输出功能开启； syslog 输出功能开启； relay 输出功能开启。
温度告警输出功能	trap 输出功能开启； syslog 输出功能开启； relay 输出功能开启。
配置高温告警阈值	缺省高温阈值由设备属性确定
配置低温告警阈值	缺省低温阈值由设备属性确定
电压告警输出功能	trap 输出功能开启； syslog 输出功能开启； relay 输出功能开启。
配置高电压告警阈值	缺省高电压阈值由设备属性确定
配置低电压告警阈值	缺省低电压阈值由设备属性确定
端口 LinkFault 事件告警输出功能	trap 输出功能关闭； syslog 输出功能关闭； relay 输出功能关闭。
端口 not-forwarding 事件告警输出功能	trap 输出功能关闭； syslog 输出功能关闭； relay 输出功能关闭。
端口 LinkDown 事件告警输出功能	trap 输出功能开启； syslog 输出功能开启；

	relay 输出功能开启。

6.2.2 告警功能配置

配置告警信息全局 syslog 输出功能

缺省告警全局 syslog 输出开关是关闭的，当全局开关和监控的告警事件下的开关同时开启时，告警才能产生 syslog 输出。

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**env-monitor syslog (on | off)**	使能/禁止告警信息全局 syslog 输出
第 3 步	**display env-monitor configure**	查看全局的 env-monitor 配置信息

配置告警信息全局 Trap 发送功能

缺省告警全局 Trap 发送开关是关闭的，当全局 Trap 发送开关和监控的告警事件下的 Trap 发送开关同时开启时，告警才能产生 Trap 输出。

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	env-monitor trap (on | off)	使能/禁止告警信息全局 Trap 发送功能
第 3 步	**display env-monitor configure**	显示全局的 env-monitor 配置信息

配置电源掉电事件告警输出功能

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**env-monitor power-supply (electrical-relay | trap-**	使能/禁止电源掉电事件告警输出功能，可配置的输出方式为：

	notifies | syslog) (on | off)	relay（继电器）输出、trap 输出、syslog 输出
第 3 步	**display env-monitor configure**	显示全局的 env-monitor 配置信息

配置温度告警输出功能

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**env-monitor temperature (electrical-relay | trap-notifies | syslog) (on | off)**	使能/禁止温度告警输出功能，可配置的输出方式为：relay（继电器）输出、trap 输出、syslog 输出
第 3 步	**display env-monitor configure**	显示全局的 env-monitor 配置信息

配置高温告警阈值

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**[no] env-monitor temperature max** <*-20-80*>	no 恢复高温告警阈值为缺省值命令；配置高温告警阈值，设备温度高于设置的高温告警阈值时产生告警信息 <*-20-80*>：温度范围；
第 3 步	**display env-monitor configure**	显示全局的 env-monitor 配置信息

配置低温告警阈值

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**[no] env-monitor temperature min** <*-20-80*>	no 恢复低温告警阈值为缺省值命令；配置低温告警阈值，设备温度

		低于设置的低温告警阈值时产生告警信息 *<-20-80>*：温度范围；
第 3 步	**display env-monitor configure**	显示全局的 env-monitor 配置信息

配置电压告警输出功能

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**env-monitor voltage (electrical-relay | trap-notifies | syslog) (on | off)**	使能/禁止电压告警输出功能，可配置的输出方式为：relay（继电器）输出、trap 输出、syslog 输出
第 3 步	**display env-monitor configure**	显示全局的 env-monitor 配置信息

配置高压告警阈值

设备存在多路电压时，只监控一路电压，具体监控哪路电压由设备属性决定。

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**env-monitor voltage index *<1-5>* max *<12000-12500>***	配置高电压告警阈值，设备电压高于设置的高电压告警阈值时产生告警信息 *<1-5>*：电压路数； *<12000-12500>*：电压参数；
第 3 步	**display env-monitor configure**	显示全局的 env-monitor 配置信息

配置低压告警阈值

设备存在多路电压时，只监控一路电压，具体监控哪路电压由设备属性决定。

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**env-monitor voltage index <*1-5*> min <*11500-12000*>**	配置低压告警阈值，设备电压低于设置的低压告警阈值时产生告警信息 <*1-5*>：电压路数； <*11500-12000*>：电压参数；
第 3 步	**display env-monitor configure**	显示全局的 env-monitor 配置信息

配置端口 LinkFault 告警输出功能

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**[no] env-monitor interface link-fault (electrical-relay | syslog | trap-notifies) port-range** *port-list*	使能/禁止端口 LinkFault 告警输出功能，可配置的输出方式为：relay（继电器）输出、trap 输出、syslog 输出 *port-list*：端口列表，范围<1-28>；
第 3 步	**display env-monitor port-range** *port-list*	显示端口层次告警的信息 *port-list*：端口列表，范围<1-28>；

配置端口 not-forwarding 告警输出功能

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**[no] env-monitor interface not-forwarding (electrical-relay | syslog| trap-notifies) port-range**	使能/禁止端口 not-forwarding 告警输出功能，可配置的输出方式为：relay（继电器）输出、trap 输出、syslog 输出 *port-list*：端口列表，范围<1-28>；

	port-listt	
第 3 步	**display env-monitor port-range** *port-list*	显示端口层次告警的信息 *port-list*：端口列表，范围<1-28>；

配置端口 link-down 告警输出功能

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**[no] env-monitor interface link-down (electrical-relay | syslog | trap-notifies) port-range** *port-list*	使能/禁止端口 link-down 告警输出功能，可配置的输出方式为：relay（继电器）输出、trap 输出、syslog 输出 *port-list*：端口列表，范围<1-28>；
第 3 步	**display env-monitor port-range** *port-list*	显示端口层次告警的信息 *port-list*：端口列表，范围<1-28>；

手动清除全部告警功能

手动清除全部告警功能用于清除当前尚未恢复的所有告警。配置该命令后，清除告警当前表中的所有告警信息，并在历史表中添加一条告警类型为 clear all 的信息。如果告警全局 trap 输出开关打开，把这条告警类型为 clearall 的信息以 trap 形式输出；如果告警全局 syslog 输出开关打开，把这条告警信息以 syslog 形式输出；如果告警全局 relay 输出开关打开，关闭告警灯，设置继电器处于非告警状态。

告警当前表中被清除的告警信息，在故障恢复时不进行任何处理，这些告警信息不会重新显示；只有在故障恢复后，再次发生故障时才产生新的告警信息。

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**reset env-monitor**	手动清除全部告警功能
第 3 步	**display env-monitor port-range** *port-list*	显示端口层次告警的信息 *port-list*：端口列表，范围<1-28>；

第 4 步	**display env-monitor currrent**	显示当前尚未清除的告警信息
第 5 步	**display env-monitor history**	显示历史告警信息

6.3 监控与维护

命令	描述
display env-monitor configure	显示全局的 env-monitor 配置信息
display env-monitor port-range *port-list*	显示端口层次告警的信息 *port-list*：端口列表，范围<1-28>；
display env-monitor currrent	显示当前尚未清除的告警信息
display env-monitor history	显示历史告警信息
display env-monitor [power-supply | temperature | voltage]	显示全局环境相关的统计信息等

6.4 典型配置举例

配置示例 6-1：

配置电源告警功能的继电器输出、syslog 输出和 trap 输出，其中 trap 以 SNMPv2 的规格输出至服务器 20.0.0.6 中。

配置过程：

administrator#**config**

administrator(config)# **env-monitor syslog on**

administrator(config)# **snmp traps on**

administrator(config)# **snmp host 20.0.0.1 version 2c public**

administrator(config)# **ip address 20.0.0.6 1**

administrator(config) # **env-monitor trap on**

administrator(config)# **env-monitor power-supply electrical-relay** on

administrator(config)#**env-monitor power-supply syslog** on

administrator(config)# **env-monitor power-supply trap-notifies** on

配置示例 6-2：

配置温度告警功能的高温阈值为 50 摄氏度，低温阈值为-10 摄氏度。当产生温度异常告警时，输出告警信息至继电器。

配置过程：

administrator#**config**

administrator(config)# **env-monitor temperature electrical-relay** on

administrator(config)# **env-monitor temperature max 50**

administrator(config)# **env-monitor temperature min -10**

配置示例 6-3：

配置以太网端口 3 使能 link-fault 告警，link-down 告警以及 not-forwarding 告警。当端口 3 产生 link-fault 和 link-down 告警事件时，将告警消息输出至 syslog；当端口 3 产生 not-forwarding 告警事件时，将告警输出至继电器。

配置过程：

administrator#**config**

administrator(config)# **env-monitor syslog on**

administrator(config)# **env-monitor interface link-fault syslog port-range 3**

administrator(config)# **env-monitor interface link-down syslog port-range 3**

administrator(config)# **env-monitor interface not-forwarding electrical-relay port-range 3**

administrator(config)# **display env-monitor port-range 3**

```
Port3
Event          Relay     Syslog    Notifies   Current
-------------------------------------------------------
link-down      off       on        off        no
link-fault     off       on        off        no
not-forwarding on        off       off        no
```

七、 物理层接口配置

7.1 物理层接口特性介绍

对于交换机来说，无论连接何种设备都需要通过物理层接口来实现。针对某些特定的应用场合，需要对物理层接口进行相应配置才能有效的接收或转发数据报文。

7.2 物理层接口的缺省配置

在缺省情况下，物理层接口命令配置如下表：

表 7-1 物理层接口缺省配置表

命令	缺省值
速率配置	电口和光口的速率是自动协商的，电口速率缺省 100M，光口默认 1000M（电力行业应用）。
双工模式配置	电口和光口的双工模式是自动协商；
流量控制配置	物理端口的流控功能是关闭的；
端口描述信息	port *port-number*
端口开启/关闭配置	端口是打开状态

7.3 速率和双工模式配置

在电力变电站交换机应用场景，以太网口电口初始化被设置为 100Mbps 和全双工。当速率(双工模式)被设置为自动协商时，双工模式（速率）将被同时设置为自动协商。默认情况下所有的电口和光口都设置为自动协商。

速率和双工模式的配置步骤如下：

步骤	命令	描述
第 1 步	config	进入全局配置模式

第 2 步	**ifconfig ethernet-port** *port-number* **ifconfig port-range** (*port-list* | *all*)	进入物理层接口配置模式或者批量配置模式。 *port-numbe*r：物理端口号； *port-list*：端口列表，可以使用“,”和“-”进行多端口输入；
第 3 步	**speed** (auto | 10| 100 |1000) **duplex** (full | half)	设置端口的速率和双工模式。 auto：速率和双工均为自协商； 10：设置的速率为 10Mbps； 100：设置的速率为 100Mbps； 1000：设置千兆口； full：设置的双工模式为全双工； half：设置的双工模式为半双工；
第 4 步	**exit**	退出物理层接口配置模式进入全局配置模式
第 5 步	**exit**	退出全局配置模式进入特权用户模式
第 6 步	**display interface ethernet** *port-number*	显示端口的状态 *port-numbe*r：物理端口号；

⚠注意：

使用 speed auto 的以太网物理接口配置命令将速率和双工模式恢复为默认情况的自动协商。

不同的端口类型,可配置的速率双工模式不同。100M 电口不能配置为 1000M，100M 光口只能配置为 100M/FD，1000M 光口只能配置为 1000M/FD/auto，子卡端口在子卡不存在时不能进行速率双工配置。

7.4 为端口添加描述

根据需要可以使用命令 description WORD 为物理端口添加描述信息，命令 no description 用来恢复默认配置。

具体配置步骤如下：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number* **ifconfig port-range** *port-list*	进入物理层接口配置模式或者批量配置模式。 *port-numbe*r：物理端口号； *port-list*：端口列表；
第 3 步	**[no] description** *WORD*	添加物理端口描述信息 *WORD*：指定物理端口的描述信息，最大长度为 64 个字符，且不能以空格分开；
第 4 步	**exit**	退出物理层接口配置模式进入全局配置模式
第 5 步	**exit**	退出全局配置模式进入特权用户模式
第 6 步	**display interface ethernet** *port-number* **description**	显示端口详细信息。 *port-numbe*r：物理端口号；

7.5 开启和关闭物理层接口

有时出于某种目的需要关闭物理接口，此时就需要配置接口的开启和关闭。默认情况下所有的端口都是开启的。对于子卡接口，在相应子卡没有插入的情况下，执行物理层接口开启和关闭命令失败。

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number* **ifconfig port-range** *port-list*	进入物理层接口配置模式或者批量配置模式。 *port-numbe*r：物理端口号； *port-list*：端口列表，可以使用“,”和“-”进行多端口输入；
第 3 步	**(shutdown | no shutdown)**	关闭或启用物理接口

		shutdown：关闭物理端口； no shutdown：启用物理端口；
第 4 步	**exit**	退出物理层接口配置模式进入全局配置模式
第 5 步	**exit**	退出全局配置模式进入特权用户模式
第 6 步	**display interface ethernet** *port-number*	显示端口的状态 *port-numbe*r：物理端口号；

7.6 清除端口统计

在缺省端口号下，将清除所有端口下的统计信息

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**reset interface ethernet** [*port-number*] **counters**	清除端口统计 *port-number*：物理端口号，不填是清除所有的端口；

7.7 监控与维护

命令	描述
display interface ethernet *port-number*	显示端口的状态 *port-number*：物理端口号；
display interface ethernet [*port-number*] **description**	显示端口描述信息
display interface ethernet *port-number* **counters**	显示端口统计信息 *port-number*：物理端口号；

7.8 综合配置举例

配置示例 7-1：

设置端口 2 的速率为 100 Mbps，双工模式为全双工，并添加描述信息 this-is-TX。

配置过程：

administrator(config)#ifconfig ethernet-port 2

Switch(port-2)#speed 100

Switch(port-2)#duplex full

Switch(port-2)#description this-is-TX

Switch(port-2)#exit

配置示例 7-2：

关闭端口 3

清除 4 端口下的统计信息

配置过程：

administrator(config)#ifconfig ethernet-port 3

Switch(port-3)#shutdown

Switch(port-3)#exit

administrator(config)#reset interface ethernet 4 counters

八、 VLAN 功能配置

8.1 VLAN 原理介绍

8.1.1 IEEE802.1Q VLAN

VLAN（Virtual Local Area Network）即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段，从而实现虚拟工作组的网络技术。

从功能上看，VLAN 有着和 LAN 一样的特性。但是 VLAN 成员不受物理位置的限制。例如，同一交换机上连接的用户可以属于不同的 VLAN，不同交换机上连接的用户可以属于同一 VLAN。VLAN 的广播域与组播域都是相对于 VLAN 成员而言，组播、广播、单播都不会被传播到其他 VLAN。不同 VLAN 间只有通过三层交换机或者路由器才能实现互通。

VLAN 的上述特性为用户管理网络提供了便利，用户可以根据网络中不同群体的职能划分 VLAN，以提高网络带宽利用率和安全性。

下图为一个典型的 VLAN 网络拓扑图：

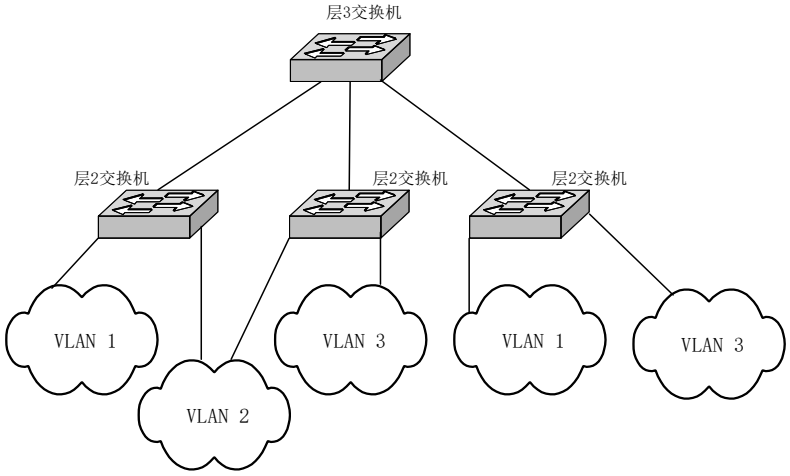


图 8-1 VLAN 典型拓扑示意图

VLAN 是为解决以太网的广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，限制不同工作组间的用户二层互访，每个工作组就是一个虚拟局域网。

IEEE 于 1999 年颁布了用于标准化 VLAN 实现方案的 802.1Q 协议标准草案。不同厂家的交换机只要支持 802.1Q VLAN 就可以跨越交换机，可以统一划分管理。

8.2 交换机 VLAN 功能配置

8.2.1 基于端口的 VLAN

基于端口划分 VLAN 是 VLAN 最简单、最有效的划分方法。它按照设备端口来定义。

VLAN 成员，将指定端口加入指定 VLAN 中之后，端口就可以转发指定 VLAN 的报文。

VLAN 端口模式介绍

成员端口模式	VLAN 成员属性
Access	access 端口模式仅能被用户指定到一个 VLAN 中，从 access 端口转发出的数据包不携带 802.1Q 标记，不同 VLAN 的 access 端口不能互通。access 端口主要用于连接终端用户；缺省情况下,所有端口以 access 模式存在于 vlan 1 中
Trunk	Trunk 端口模式缺省情况存在于所有 VLAN 中，并且从该端口转发的数据包除 Native VLAN 外全部携带 802.1Q 标记。但是，用户可以通过 permit vlans 属性限制 Trunk 端口所能转发的 VLAN 数据包。当交换机端口作为上联 TAG 端口时，可配置为 trunk 模式

VLAN 缺省配置

功能	缺省值
创建静态 VLAN	系统中存在缺省 VLAN，即 VLAN 1，所有端口以 access 模式存在于 VLAN 1 中
VLAN 名称	系统缺省 VLAN（VLAN 1）的名称为“Default”，其他静态 VLAN 的名称为字

	符串“VLAN”加上其 4 位数的 VLAN ID
端口模式	Access
端口 TRUNK 模式时，端口所允许通过的 VLAN 列表	VLAN1
端口 TRUNK 模式时，端口以 UNTAG 形式允许通过的 VLAN 列表	VLAN1（缺省 PVID）
配置 Trunk 端口的 pvid	VLAN1
保护端口	端口不是保护端口
转发端口列表	除自身端口以外的其他所有端口

VLAN 属性配置

VLAN 属性配置包括 VLAN 的创建、删除、名称和活动状态配置。其配置步骤如下：

步骤	命令	命令参数说明
第 1 步	**config**	进入全局配置模式
第 2 步	**vlan create** *vlan-id* **(active | suspend)**	创建 VLAN 并确定是活动状态或挂起状态 active：活动状态； suspend：挂起状态； *vlan-id*：VLAN 的 ID，范围<2-4094>；
第 3 步	**[no] vlan set** *vlan-id* **name** *WORD*	命名 VLAN no：可以删除 VLAN 命名，恢复至缺省名 *vlan-id*：VLAN 的 ID,范围<1-4094>； *WORD*：VLAN 名称，不大于 15 字符
第 4 步	**vlan set** *vlan-id* **state (active | suspend)**	设置 VLAN 的活动状态 active：活动状态；

		suspend：挂起状态； *vlan-id*：VLAN 的 ID，范围<1-4094>；
第 5 步	**exit**	返回全局配置模式
第 6 步	**exit**	返回特权用户模式
第 7 步	**display vlan** *vlan-id*	显示 VLAN 配置情况

使用 vlan delete <2-4094> 可以删除 VLAN。

⚠注意：

默认情况下系统中存在缺省 VLAN（VLAN 1），所有端口为 Access 模式属于缺省 VLAN 中。缺省 VLAN 不允许被删除。

缺省情况下，缺省 VLAN（VLAN 1）的名称为“Default”，其他 VLAN 的名称为字符串“VLAN”加上其 4 位数的 VLAN ID，例如 VLAN 2 的缺省名称为“VLAN0002”、VLAN 4094 的缺省名称为“VLAN4094”。

VLAN 的所有配置仅在该 VLAN 被激活后才会在系统中生效。当 VLAN 的活动状态为 suspend 时，用户仍可对该 VLAN 进行配置，比如删除/添加端口，设置 VLAN 名称等，系统将保留这些配置，一旦该 VLAN 被激活，这些配置将在系统中生效。

端口 VLAN 模式配置

各个模式及其配置如下：

配置端口模式：

步骤	命令	命令参数说明
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入对应物理接口配置模式 *port-number*：物理端口号；
第 3 步	**port link-type (access | trunk)**	设置端口的 VLAN 模式 access：ACCESS 模式，即端口以 UNTAG 形式存在于唯一的 VLAN 中；

		trunk：TRUNK 模式，端口允许多个 VLAN 通过；
第 4 步	**exit**	返回全局配置模式
第 5 步	**exit**	返回特权用户模式
第 6 步	**display interface ethernet vlan** *port-number*	显示端口 VLAN 属性配置 *port-number*： 物理端口号

配置 Trunk 模式下允许通过的 VLAN：

步骤	命令	命令参数说明
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入对应物理接口配置模式 *port-number*：物理端口号；
第 3 步	**port trunk permit vlan (all |** *vlan-id* **| add** *add-vlan-id* **| remove** *remove-vlan-id* **)**	设置 Trunk 端口允许通过的 VLAN 列表 all：允许所有 VLAN 通过； *vlan-id*：允许通过的 VLAN，直接覆盖原有配置，范围<1-4094>； *add-vlan-id*：在原有 VLAN 列表基础上增加新的 VLAN 列表； *remove-vlan-id*：在原有允许 VLAN 基础上删除允许 VLAN；
第 4 步	**[no] port trunk untagged vlan-range (all |** *vlan-id* **| add** *add-vlan-id* **| remove** *remove-vlan-id* **)**	设置 Trunk 端口以 UNTAG 形式允许通过的 VLAN 列表 no ： 恢复 Trunk 端口的 UNTAGGED VLAN 列表为缺省值，即只包含 PVID； all：允许所有 VLAN 通过； *vlan-id*：允许通过的 VLAN，直接覆盖原有配置，范围<1-4094>；

		add-vlan-id：在原有 VLAN 列表基础上增加新的 VLAN 列表； *remove-vlan-id*：在原有允许 VLAN 基础上删除允许 VLAN；
第 5 步	**exit**	返回全局配置模式
第 6 步	**exit**	返回特权用户模式
第 7 步	**display interface ethernet vlan** *port-number*	显示端口 VLAN 属性配置 *port-number*：物理端口号；

当用户设置 TRUNK 模式允许通过的 VLAN 之后，会提示用户“请输入'y'对设置允许 vlan 加以确认：”，用户通过输入“y/Y”或直接输入回车确认配置，配置值才能生效，否则，配置不生效。

配置 Trunk 端口的 PVID：

步骤	命令	命令参数说明
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入对应物理接口配置模式 *port-number*：物理端口号；
第 3 步	**[no] port trunk pvid vlan** *vlan-id*	设置 Trunk 端口的 pvid no：恢复 Trunk 端口的 pvid 为缺省值，即 VLAN1； *vlan-id*：VLAN 的 ID，范围<1-4094>；
第 4 步	**exit**	返回全局配置模式
第 5 步	**exit**	返回特权用户模式
第 6 步	**display interface ethernet vlan** *port-number*	显示端口 VLAN 属性配置

监控与维护

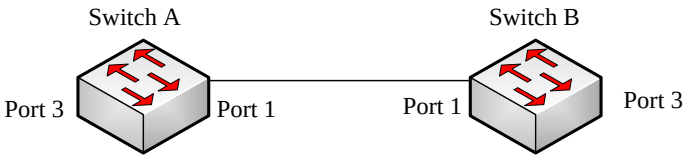
命令	命令参数说明
display interface ethernet vlan	显示端口 VLAN 属性配置

port-number	*port-number*：物理端口号；
display vlan	显示端口 VLAN 属性配置

典型配置举例

配置示例 7-1：

如下图拓朴结构所示，交换机 SwitchA 和 SwitchB 使用 Port1(SwitchA)和 Port1(SwitchB)相连，两个设备的 Port1 配置为 Trunk 端口，允许 VLAN1-VLAN100 通过，Port3(SwitchA)和 Port3(SwitchB)为 Access 端口，Access VLAN 为 VLAN6。SwitchA 与 SwitchB 的配置完全相同，此处仅说明 SwitchA 的配置方法。



配置过程：

administrator#**config**

administrator(config)# **vlan create 6 active**

administrator(config)#**ifconfig ethernet-port 1**

Switch(port-1)#**port link-type trunk**

Switch(port-1)#**port trunk permit vlan 1-100 confirm**

Switch(port-1)# **exit**

administrator(config)#**ifconfig ethernet-port 3**

Switch(port-3)# **port link-type access**

Switch(port-3)# **port access vlan 6**

Switch(port-3)#**exit**

administrator(config)#**exit**

administrator#**display vlan**

VLAN Name State Status Priority Member-Ports

```
    ------------------------------------------------------------
-----------
    1    Default              active  static  --       1-2,4-28
    6    VLAN0006             active  static  --       1,3
```

administrator#**display interface ethernet vlan 1**

```
    Port: port1
    Administrative Mode: trunk
    Operational Mode: trunk
    Access Mode VLAN: 1
    Trunk Native Mode VLAN: 1
    Administrative Trunk Allowed VLANs: 1-100
    Operational Trunk Allowed VLANs: 1,6
    Administrative Trunk Untagged VLANs: 1
    Operational Trunk Untagged VLANs: 1
```

administrator#**display interface ethernet vlan 3**

```
    Port: Port: 3
    Administrative Mode: access
    Operational Mode: access
    Access Mode VLAN: 6
    Trunk Native Mode VLAN: 1
    Administrative Trunk Allowed VLANs: 1-4094
    Operational Trunk Allowed VLANs: 1,6
    Administrative Trunk Untagged VLANs: 1
    Operational Trunk Untagged VLANs: 1
```

九、 QoS 功能配置

9.1 QoS 概述

9.1.1 QOS 简介

QOS 的产生背景：

一般来说，基于存储转发机制的业务实现只为用户提供了“尽力而为（best-effort）”的服务，不能保证数据包传输的实时性、完整性以及到达的顺序性，服务的质量则无法得到保障。但在很多情况下，用户对不同的业务有着不同的服务质量要求，这就要求网络能根据用户的要求分配和调度资源。

网络服务质量（Quality of Service，简称 QoS）的应用，可以优先处理特定的数据流，或对其采取特定的管理调度策略使得网络性能可预测、带宽管理更有效。

服务类别 CoS：

ZJ-IES-900 网络交换机上的 QoS 功能基于 IEEE 802.1P、IEEE 802.1Q 标准，在 2 层报文上进行分类。

Class of Service，简称为 CoS，用于表示业务的服务类别。QoS 要求交换设备可以依据业务的 CoS 值对输出的数据流进行分类，或执行不同的处理。QOS 值的具体含义见下表：

优先级	报文类型	应用
000	Routine	0 级对应于缺省的尽最大努力投递的信息
001	Priority	4～1 级针对多媒体数据或重要的企业级数据信息定义
010	Intermediate	
011	Flash	
100	Flash Override	
101	Critical	6 或 5 级用在对延迟敏感的交互式视频、音频数据中
110	Internet Control	
111	Network Control	最高级 7 级应用于重要的网络数据流如路由信息等

CoS 的承载方法：

IEEE 802.1Q 规定的二层报文数据帧头中，CoS 承载于四字节 VLAN tag 信息中的高三位，取值范围为 0—7。

在三层 IP 报文的 ToS 字段中，高 3 位表示 ToS，高 6 位表示 DSCP，低两位未用。ZJ-IES-900 网络交换机允许用户定义将三层报文的 DSCP 值通过可配置的映射机制转换成 COS 值，从而实现基于三层报文的 QOS 功能。

9.1.2 QoS 缺省配置

	属性	缺省配置
1	QoS 启动	未启动
2	全局 QoS 信任状态	UNTRUST
3	端口 QoS 信任状态	UNTRUST
4	端口缺省 CoS	0
5	端口缺省 DSCP	0
6	端口缺省 CoS 覆盖	Disable
7	端口缺省 DSCP 覆盖	Disable
8	策略信任状态	DSCP
9	队列调度策略	严格优先级调度 SP

COS-DSCP 缺省映射关系为：

CoS 值	0	1	2	3	4	5	6	7
DSCP值	0	8	16	24	32	40	48	56

IP-Precedence-DSCP 缺省映射关系为：

ToS 值	0	1	2	3	4	5	6	7
DSCP 值	0	8	16	24	32	40	48	56

DSCP-COS 缺省映射关系为：

DSCP值	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS 值	0	1	2	3	4	5	6	7

DSCP-to-DSCP-Mutation 缺省映射关系（default-dscp）为：

DSCP值	0	1	2	3	4	5	6	7
0	8	9	10	11	12	13	14	15
1	16	17	18	19	20	21	22	23
2	24	25	26	27	28	29	30	31
3	32	33	34	35	36	37	38	39
5	40	41	42	43	44	45	46	47
6	48	49	50	51	52	53	54	55
7	56	57	58	59	60	61	62	63

内部 COS 到队列缺省映射关系为：

内部CoS值	0	1	2	3	4	5	6	7
队列ID	1	1	2	2	3	3	4	4

9.2 QoS 启动和关闭功能配置

缺省情况下，QoS 在交换机上是关闭的。通过在全局配置模式下执行如下命令，可以将 QoS 置为有效。

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**qos (on | off)**	启动/关闭 QoS
第 3 步	**exit**	返回特权模式
第 4 步	**display qos**	显示 QoS 开关状态

⚠注意：

大部分功能在 QoS 开启前是无效的，但有些功能还是有效的，如端口缺省 COS、端口缺省 DSCP、队列调度模式、CoS 到队列映射等。

建议在启动 QoS 之前，关闭流控功能。

9.3 分类功能配置

配置端口 QoS 信任状态。缺省情况下，交换机的信任状态为 UNTRUST。

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入端口配置模式
第 3 步	**qos trust (** cos | dscp | port-priority)	设置 QoS 信任状态 cos：设置端口为 TRUST cos 状态 dscp：设置端口为 TRUST DSCP 状态 port-priority：设置端口为 port-priority 状态
第 4 步	**exit**	返回全局配置模式
第 5 步	**exit**	返回特权模式
第 6 步	**display qos**	显示 QoS 配置情况

⚠注意：

基于端口信任状态与 ACL/类映射的流分类方式是互斥的，二者遵循后配置生效原则。

全局与端口 QoS 信任状态的配置用于不同的设备，目前，同一设备中，不支持两者共存。

QoS 信任状态的配置与策略信任状态的配置是互斥的，遵循后配置生效原则。

9.4 映射功能配置

9.4.1 CoS-localpriority 映射表配置

CoS-localpriority 映射表将入包的 COS 值映射成一个 localpriority 值，QoS 用其描述数据流的优先级。其缺省映射关系为：

CoS 值	0	1	2	3	4	5	6	7
localpriority值	0	1	2	3	4	5	6	7

修改映射关系：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**qos mapping cos** *cosVal* **to local-pri** *localPrioVal*	设置新的映射关系 *cosVal*：COS 值，范围<0-7>； *localPrioVal*：本地优先级值，范围<0-7>；
第 3 步	**exit**	返回特权模式
第 4 步	**display qos mapping cos**	显示 cos 映射信息

恢复缺省映射关系：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**no qos mapping cos**	恢复到缺省的映射关系
第 3 步	**exit**	返回特权模式
第 4 步	**display qos mapping cos**	显示 cos 映射信息

9.4.2 Dscp-localpriority 映射表配置

dscp-localpriority 映射表将入包的 dscp 值映射成一个 localpriority 值，QoS 用其描述数据流的优先级。其缺省映射关系为：

dscp 值	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
localpriority值	0	1	2	3	4	5	6	7

修改映射关系：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**qos mapping dscp** *dscpVal* **to local-pri** *localPrioVal*	设置新的映射关系 *dscpVal*：dscp值，范围 <0-63>； *localPrioVal*：本地优先级值，范围<0-7>；
第 3 步	**exit**	返回特权模式

第 4 步	**display qos mapping dscp**	显示 dscp 映射信息

恢复缺省映射关系：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**no qos mapping dscp**	恢复到缺省的映射关系
第 3 步	**exit**	返回特权模式
第 4 步	**display qos mapping dscp**	显示 dscp 映射信息

9.5 队列和调度功能模式

目前，设备支持四种队列调度模式：严格优先级（SP）、加权优先级（WRR）、DRR 和 WFQ.缺省设置为严格优先级模式。

SP 模式配置步骤：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**qos queue sched-mode sp**	配置为严格优先级
第 3 步	**exit**	返回特权模式
第 4 步	**display qos queue**	显示 QoS 队列信息

WRR 模式配置步骤：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**qos queue wrr** *<weightVal1>* *<weightVal2>* *<weightVal3>* *<weightVal4>* *<weightVal5>* *<weightVal6>* *<weightVal7>* *<weightVal8>*	设置端口的调度模式为 WRR 模式 *weightVal1-8*：设置队列 1-8 加权权值，范围<1-255>；
第 3 步	**exit**	返回特权模式
第 4 步	**display qos queue**	显示 QoS 队列信息

9.6 维护与监控

命令	描述
display qos	显示 QOS 状态
display qos mapping cos	显示 cos 映射配置信息
display qos mapping dscp	显示 dscp 映射配置信息
display qos mapping local-pri	显示本地优先级到队列映射配置信息
display qos queue	显示队列配置信息

9.7 典型配置举例

配置示例 9-1：

开启全局 QOS 功能。

配置过程：

administrator#**config**

administrator(config)# **qos on**

administrator(config)# **display qos**

```
Qos Status:On
Scheduler Mode:SP
```

配置示例 9-2：

将 CoS 为 5 的业务流，映射到本地优先级 3 的队列中。

配置过程：

administrator#**config**

administrator(config)# **qos on**

administrator(config)# **qos mapping cos 5 to local-pri 3**

administrator(config)#**exit**

administrator# **display qos mapping cos**

```
802.1p CoS to local-priority mapping:
CoS:          0   1   2   3   4   5   6   7
```

```
-----------------------------------------

LocalPriority:0   1   2   3   4   3   6   7
```

配置示例 9-3：

配置 dscp 为 5 localpriority 为 3 的映射：

配置过程：

administrator#**config**

administrator(config)# **qos mapping dscp 5 to local-pri 3**

administrator(config)#**exit**

administrator# **display qos mapping dscp**

```
DSCP to local-priority mapping:

 d1 : d2  0  1  2  3  4  5  6  7  8  9

-------------------------------------------------

     0:  0  0  0  0  0  3  0  0  1  1

     1:  1  1  1  1  1  1  2  2  2  2

     2:  2  2  2  2  3  3  3  3  3  3

     3:  3  3  4  4  4  4  4  4  4  4

     4:  5  5  5  5  5  5  5  5  6  6

     5:  6  6  6  6  6  6  7  7  7  7

     6:  7  7  7  7
```

配置示例 9-4：

设置队列为 WRR 模式，权重分别为 1:2:4:8:3:5:7:9

配置过程：

administrator#**config**

administrator(config)# **qos queue wrr 1 2 4 8 3 5 7 9**

administrator(config)#**exit**

administrator#**display qos queue**

Queue Weight(WRR)

1	**1**
2	**2**
3	**4**
4	**8**
5	**3**
6	**5**
7	**7**
8	**9**

十、 风暴抑制功能配置

10.1 风暴抑制功能概述

当一个端口接收到大量的广播包、组播包或目的寻找失败的包时，将产生一种包风暴。对这些包的转发将造成网络速率下降甚至超时。风暴抑制功能就是为了防止产生这种情况。风暴抑制功能针对整个交换机进行设置，但它针对单个端口生效。

设置的各种数据包的最大包流量必须是相同的，当设置一种数据包的限制数量时，其他数据包的限制数值也将被修改。

10.2 风暴抑制功能缺省配置

默认情况下，广播包的风暴抑制功能是开启的，组播包和对目的寻找失败的单播包风暴抑制功能关闭。

10.3 风暴抑制功能配置

开启或关闭风暴抑制功能：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**storm-suppress** (broadcast | multicast | dlf | all) **(on | off)**	设置对广播包、组播包和目的寻找失败的包的风暴抑制功能启用和关闭 broadcast：目的寻找失败的广播包； multicast：目的寻找失败的组播包； dlf ：目的寻找失败的单播包； all：广播、组播和目的寻找失败单播包；
第 3 步	**exit**	退出全局配置模式进入特权用户模式
第 4 步	**display storm-**	显示风暴抑制的状态。

	suppress	

配置风暴抑制阈值：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**storm-suppress** (broadcast | multicast | dlf | all) **bps** *rate-value*	设置风暴抑制的阈值。 *rate-value*：每秒允许通过的千 bit 数，范围 <64-250000>；
第 3 步	**exit**	退出全局配置模式进入特权用户模式
第 4 步	**display storm-suppress**	显示风暴抑制的状态

10.4 监控与维护

命令	功能描述
display storm-suppress	显示风暴抑制的状态

10.5 典型配置举例

配置示例 10-1：

关闭对广播包的风暴抑制。

配置过程：

administrator#**config**

administrator(config)# **storm-suppress broadcast off**

administrator(config)#**exit**

administrator#**display storm-suppress**

```
Rate: 64 kbps
Broadcast: Off
Multicast: Off
Unicast destination lookup failed(DLF): Off
```

配置示例 10-2：

配置风暴抑制阈值为 200kbps。

配置过程：

administrator#**config**

administrator(config)# **storm-suppress bps 200**

administrator(config)#**exit**

administrator#**display storm-suppress**

```
Rate: 200 kbps
Broadcast: Off
Multicast: Off
Unicast destination lookup failed(DLF): Off
```

十一、 MAC 地址转发表管理配置

11.1 MAC 转发表管理原理介绍

11.1.1 MAC 地址转发表

交换机从它的所有端口接收 Media Access Control (MAC)地址信息，形成 MAC 地址表并维护它。当交换机收到一帧数据时，它将根据自己的 MAC 地址表来决定是将这帧数据进行过滤还是转发。此时，维护的这张 MAC 表就是 FDB 地址表。如果收到数据帧的目的 MAC 地址不在 FDB 地址表中，那么该数据将被发送给除源端口外该数据包所属 VLAN 的其他所有端口。FDB 是以太网节点在运行过程中自我学习到的 MAC 地址表，FDB 能够促进交换策略的选择。

网络交换机的主要功能是在数据链路层对报文进行转发，也就是根据报文的目的 MAC 地址将报文输出到相应的端口。MAC 地址转发表是一张包含了 MAC 地址与转发端口对应关系的二层转发表，是网络交换机实现二层报文快速转发的基础。

MAC 地址转发表的表项中包含如下信息：

- 目的 MAC 地址；
- 端口所属的 VLAN ID；
- 本设备上的转发出端口编号。
- 网络交换机在转发报文时，根据 MAC 地址表项信息，会采取以下两种转发方式：
- 单播方式：当 MAC 地址转发表中包含与报文目的 MAC 地址对应的表项时，交换机直接将报文从该表项中的转发出端口发送；
- 广播方式：当交换机收到目的地址为全 F 的报文，或 MAC 地址转发表中没有包含对应报文目的 MAC 地址的表项时，交换机将采取广播方式将报文向除接收端口外的所有端口转发。

11.1.2 MAC 地址学习

MAC 地址转发表中的表项可以通过两种方式进行更新和维护：

- 手工配置方式；
- MAC 地址学习方式。

手工配置方式：可以通过命令行接口手工增加地址表项到 FDB 地址表中。MAC 地址学习方式:交换机可以根据收到的数据包的源 MAC 地址、端口、VLANID，来自动更新 FDB 地址表。 FDB 地址表数目由产品决定。每一个 FDB 地址表项由 MAC 地址和 VLAN ID 唯一标识。每个 FDB 地址表项都包含以下内容：

MAC 地址 、MAC 地址关联的端口号（Port）、MAC 地址关联的 VLAN 的名称(VLAN name)、FDB 地址表项的标志(Flags)。

通常情况下，多数 MAC 地址表项都是通过 MAC 地址学习功能创建和维护的。网络交换机学习 MAC 地址的过程如下：

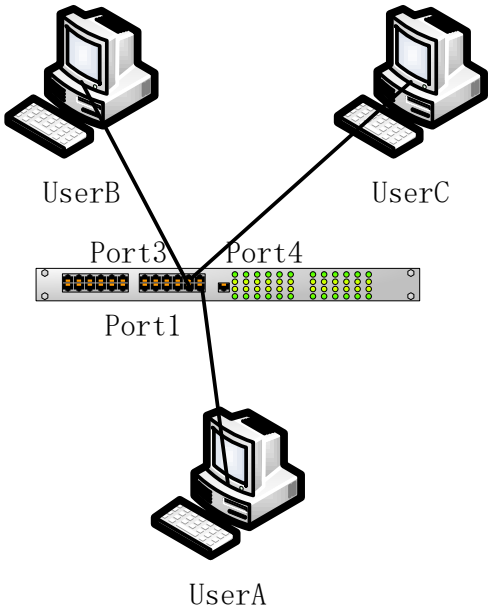


图 11-1 MAC 地址学习示意图

当 UserA 需要与同处在 VLAN1 中的 UserB 通信时，需要将报文发送到交换机的 PORT-1 端口，此时交换机将该报文的源 MAC 地址，即 UserA 的地址“MAC-A”记录到自身的 MAC 地址转发表中。

学习过程完成后，交换机将对该报文进行转发，由于现有的 MAC 地址转发表中没有关于 UserB 的 MAC 地址及端口的对应表项，因此，交换机会如上图所

示将该报文向除 1 之外的所有端口进行转发，以尽最大能力保证 UserB 能够收到该报文。

由于交换机采用广播方式发送报文，UserB 和 UserC 都会收到，但 UserC 不是该报文的目的设备，因此不会进行处理。而正常情况下，UserB 会向 UserA 发送报文进行响应。当该响应报文发送至 PORT-4 端口时，交换机会采取同样的 MAC 地址学习方式将 UserB 的地址和端口对应关系保存到 MAC 地址转发表中。

此时交换机的转发表中应包含两条表项。在转发响应报文时，由于 MAC 地址转发表中已经包含目的为“MAC-A”的表项，因此交换机不会再次采取广播操作，而是直接将报文通过 PORT-1 端口发送至 UserA，完成此次报文交互过程。

11.1.3 MAC 地址表管理

老化机制：

网络交换机的 MAC 地址转发表是有容量限制的，为了最大限度利用地址转发表资源，网络交换机利用老化机制更新 MAC 地址转发表，即：系统在动态创建某条表项的同时，开启老化定时器，如果在老化时间内没有再次收到来自该表项中的 MAC 地址的报文，交换机就会把该 MAC 地址表项删除。

⚠注意：

- 当开启了“目的 MAC 地址更新”功能后，如果交换机在老化时间内对目的为某个 MAC 地址的报文进行了转发，则该 MAC 的表项也将被触发更新，重新开始老化。
- MAC 地址的老化机制只对动态 MAC 地址表项生效。

地址表的分类：

MAC 地址标表的分类与特点：

- 静态 MAC 地址表项：也称为“永久地址”，由用户手工添加和删除，不会随着时间老化。对于一个设备变动较小的网络，手工添加静态地址表项可以减少网络中的广播流量。
- 动态 MAC 地址表项：指可以按照用户配置的老化时间而老化掉的 MAC 地址表项，交换机可以通过 MAC 地址学习机制或通过用户手工建立的

方式添加动态 MAC 地址表项。

11.2 MAC 转发表管理配置

11.2.1 MAC 地址转发表 管理缺省配置

功能	缺省值
MAC 地址老化时间	300s
MAC 地址学习特性	开启

11.2.2 静态单播 MAC 地址配置

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**fdb static unicast** *HHHH.HHHH.HHHH* **vlan** *vlan-id* **ethernet-port** *port-number*	设置静态 MAC 地址 *HHHH.HHHH.HHHH*：要设置的静态单播 MAC 地址，格式为十六进制字符串，每四个字符进行点分； *vlan-id*：VLAN 的 ID，范围<1-4094>； *port-number*：物理端口号；
第 3 步	exit	退出全局配置模式进入特权用户模式
第 4 步	**display fdb address [ethernet-port** *port-number* **]**	显示端口的静态单播地址 *port-number*：物理端口号；

⚠注意：

交换机的 MAC 地址、组播地址、FFFF.FFFF.FFFF 及 0000.0000.0000 不能被配置为静态单播 MAC 地址。

目前支持可配置的静态单播 MAC 地址条目数存在设备差异。

11.2.3 静态组播 MAC 地址配置

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**fdb static multicast** *HHHH.HHHH.HHHH* **vlan** *vlan-id* **port-list** *port-list*	设置静态 MAC 地址 *HHHH.HHHH.HHHH*：要设置的静态多播 MAC 地址，格式为十六进制字符串，每四个字符进行点分； *vlan-id*：VLAN 的 ID，范围<1-4094>；*port-list*：物理端口列表，可以使用“,”“-”关联符号输入端口列表；
第 3 步	exit	退出全局配置模式进入特权用户模式
第 4 步	**display fdb multicast** **display fdb multicast count**	显示 VLAN 的静态多播地址 *vlan-id*：VLAN 的 ID，范围<1-4094>；显示当前的多播地址数量；

⚠注意：

目前支持可配置的静态组播 MAC 地址条目数存在设备差异

11.2.4 MAC 地址老化时间配置

交换机学习到的动态源 MAC 地址在不使用的时候会被老化，可以更改该老化时间，也可以禁止 MAC 地址老化。缺省情况下，老化时间为 300 秒。

步骤	命令	描述
第 1 步	config	进入全局配置模式

第 2 步	[no] fdb aging-time (*0* | *time*)	设置 MAC 地址的老化时间 no：恢复老化时间的缺省值； 0：禁止 MAC 地址老化； *time*：要设置的 MAC 地址老化时间，单位是秒，范围<10-1000000>，缺省值为 300；
第 3 步	**exit**	退出全局配置模式进入特权用户模式
第 4 步	**display fdb aging-time**	显示 MAC 地址老化时间

11.2.5 MAC 学习使能配置

有时需要禁止或打开某个物理端口学习 MAC 地址，可以通过配置对 MAC 地址的学习能力的开关来实现。缺省情况下，每个物理端口都被允许学习 MAC 地址。

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**fdb learning (on | off)** **port-range** (*all* | *port-list*)	设置物理端口MAC地址学习功能的开启和关闭 on：开启学习功能； off：关闭学习功能； *port-list*：物理列表；
第 3 步	**exit**	退出全局配置模式进入特权用户模式
第 4 步	**display interface ethernet** [*port-number*]	显示端口的状态 *port-number*：物理端口号；

11.2.6 MAC 地址转发表清除配置

清除在交换机中的层 2 MAC 地址表，包括动态学到的和静态设置的。该命令在全局配置模式下使用。

命令	描述
reset fdb (all | dynamic | static)	all：清除所有的 2 层 MAC 地址 dynamic：只清除动态学习到的 2 层 MAC 地址 static：只清除静态设置的 2 层 MAC 地址

11.3 监控与维护

命令	描述
display fdb aging-time	显示 MAC 地址老化时间
display fdb static ethernet-port *port-number*	显示在交换机中端口下的 MAC 地址 *port-number*：物理端口号；
display fdb static vlan *vlan-id*	显示在交换机中 VLAN 下的 MAC 地址 *vlan-id*：VLAN 的 ID，范围为<1-4094>；
display fdb multicast count	显示在交换机的动态 MAC 地址数、静态 MAC 地址数、其他 MAC 地址数和 MAC 地址总数 count：统计相关 MAC 地址的个数；
display fdb multicast	显示在交换机中端口下的动态 mac 地址数、静态 mac 地址数、其他 mac 地址数和 mac 地址总数
display fdb static	显示在交换机中的静态 MAC 地址表配置信息

11.4 典型配置举例

配置示例 11-1：

设置静态单播 MAC 地址 1234.1234.1234 在端口 2，vlan10 下，并显示端口的静态单播地址。

配置过程：

```
administrator(config)# ifconfig ethernet-port 2
Switch(port-2)#port access vlan 10
Switch(port-2)#exit
```

administrator(config)#fdb static unicast 1234.1234.1234 vlan 10 ethernet-port 2

administrator(config)#display fdb static ethernet-port 2

```
Port    Vlan    Static MAC
------------------------
port2   10      1234.1234.1234
```

配置示例 11-2：

设置静态组播 MAC 地址 0111.1111.1111 在端口 6，vlan6 下，并显示端口的静态多播地址。

配置过程：

administrator(config)#fdb static multicast 0111.1111.1111 vlan 6 port-list 6

administrator(config)#display fdb multicast

```
Vlan          Multicast address           Ports[Static]
-----------------------------------------------------
 6              0111.1111.1111          port-list 6 [port-list
6]
```

配置示例 11-3：

配置老化时间为 1000s，并显示老化时间。

配置过程：

administrator#**config**

administrator(config)#**fdb aging-time 1000**

administrator(config)#**exit**

administrator#**display fdb aging-time**

```
Aging time: 1000s
```

十二、 链路聚合功能配置

12.1 链路聚合功能原理介绍

链路聚合是将多个物理以太网端口聚合在一起形成一个逻辑上的聚合组，使用链路聚合服务的上层实体把同一聚合组内的多条物理链路视为一条逻辑链路。

链路聚合可以实现出/入负荷在聚合组中各个成员端口之间分担，以增加带宽。同时同一聚合组的各个成员端口之间彼此动态备份，提高了连接可靠性。

在同一个聚合组中，能进行出/入负荷分担的成员端口必须有一致的配置。这些配置主要包括 STP、QoS、VLAN、端口属性、MAC 地址学习等，如下表所示：

分类	具体内容
STP 配置一致	端口的STP 使能/关闭状态、与端口相连的链路属性（如点对点或非点对点）、端口路径开销、STP 优先级、报文发送速率限制、是否配置环路保护、是否配置根保护、是否为边缘端口。
QoS 配置一致	流量监管、流量整形、拥塞避免、端口限速、SP 队列、WRR 队列调度、WFQ 队列、端口优先级、端口信任模式。
VLAN 配置一致	端口上允许通过的VLAN、端口缺省VLAN ID、端口的链路类型（即Trunk、Access 类型）、子网VLAN 配置、协议VLAN 配置、VLAN 报文是否带Tag 配置。
端口属性配置一致	端口是否加入隔离组、端口的速率、双工模式、up/down 状态。

MAC 地址学习配置一致	是否具有MAC 地址学习功能、端口是否具有最大学习MAC 地址个数的限制、MAC 表满后是否继续转发控制。

12.2 链路聚合功能配置

12.2.1 链路聚合功能缺省配置

功能	缺省值
链路聚合功能	开启
链路聚合组	不存在，需手动配置
负载均衡模式	源、目的 MAC 地址逻辑或的结果选择转发端口

12.2.2 链路聚合组配置

步骤	命令	描述
第 1 步	**ifconfig port-range** portlist	进入多端口模式
第 2 步	**[no] aggregation group** *trunk-group-id*	增加一个聚合组； no：删除指定聚合组 *trunk-group-id*：创建的聚合组号，范围<1-8>；
第 3 步	**exit**	退出。进入全局配置模式
第 4 步	**aggregation (on|off)**	使能或禁用链路聚合功能
第 5 步	**exit**	退出全局配置模式进入特权用户模式
第 6 步	display aggregation	显示当前是否启动聚合链路、链路聚合负载均衡模式、当前所有聚合组设置的组成员端口和当前生效的成员端口

12.2.3 负载分担模式配置

聚合链路有 7 种负载分担模式：

- smac 依据源 MAC 地址选择转发端口。
- dmac 依据目的 MAC 地址选择转发端口。
- sxordmac 依据源、目的 MAC 地址逻辑异或的结果选择转发端口。
- sip 依据源 IP 地址选择转发端口。
- dip 依据目的 IP 地址选择转发端口。
- sxordip 依据源、目的 IP 地址逻辑异或的结果选择转发端口。
- sportxorsxordmac 依据源端口、源 MAC 地址、目的 MAC 地址逻辑异或的结果选择转发端口。

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**[no] aggregation load-sharing mode (smac | dmac | sxordmac | sip | dip | sxordip | sportxorsxordmac)**	设置所有聚合链路的负载均衡模式 no：恢复链路聚合负载均衡的缺省模式
第 3 步	**exit**	退出全局配置模式
第 4 步	**display aggregation**	显示当前是否启动聚合链路、链路聚合负载均衡模式、当前所有聚合组设置的组成员端口和当前生效的成员端口

12.3 监控与维护

命令	描述
display aggregation	显示当前是否启动聚合链路、链路聚合负载均衡模式、当前所有聚合组设置的组成员端口和当前生效的成员端口

12.4 典型配置举例

配置示例 12-1：

如下图所示，设备 SwitchA 用 4 个端口聚合接入设备 SwitchB，从而实现出/入负荷在各成员端口中分担。SwitchA 和 SwitchB 的接入端口均为 port1～port4，负载分担模式为基于源 MAC 分担。

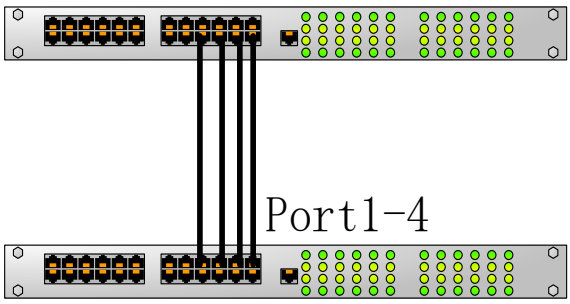


图12-1　链路聚合配置示例图

配置过程：

SwitchA#config

SwitchA(config)# ifconfig port-range 1-4

SwitchA(port-range-1-4)#aggregation group 1

SwitchA(port-range-1-4)# exit

SwitchA(config)# aggregation loadsharing mode smac

SwitchA(config)# aggregation on

SwitchA(config)#exit

SwitchA#display aggregation

```
Link aggregation status: On
Load sharing mode: SMAC
M - Manual    L - Lacp-static
GroupID  Mode Member-Port-List     Efficient-Port-List
------------------------------------------------------------
```

```
----------------------
    1           M                   1-4
    2           M
    3           M
```

SwitchB 的配置方法与 SwitchA 相同，此处不再详细说明。

十三、 端口保护功能配置

13.1 端口保护功能概述

通过端口保护特性，用户可以将需要进行控制的端口加入一个端口保护组中，实现端口保护组内的端口之间二层、三层数据的隔离，既增强了网络的安全性，也为用户提供了灵活的组网方案。

13.2 端口保护功能配置

13.2.1 端口保护功能缺省配置

功能	缺省值
端口保护功能	禁止

13.2.2 端口保护功能配置

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	ifconfig port-range *port-list*	进入多端口配置模式 *port-list*：端口列表；
第 3 步	**port protect**	开启端口保护功能
第 4 步	**display port protected**	查看端口保护配置

⚠注意：

- 配置端口保护后，在端口保护组内的各个端口之间的报文不能互通，端口保护组内端口与端口保护组外的端口以及端口保护组外端口之间的通信不会受影响。
- 端口保护特性与以太网端口所属 VLAN 无关。
- 端口保护特性与 Tint
- RUNK 组或分无关。

13.3 监控与维护

命令	描述
display port protected	查看端口保护配置

13.4 典型配置举例

配置示例 13-1：

应用拓扑如下图所示，Switch A 中端口 1、2、3 分别接小区用户 PC1、PC2、PC3，他们通过 SwitchA 的端口 4 访问外部网络。

要求小区用户 PC1、PC2、PC3 之间两两不能互通。

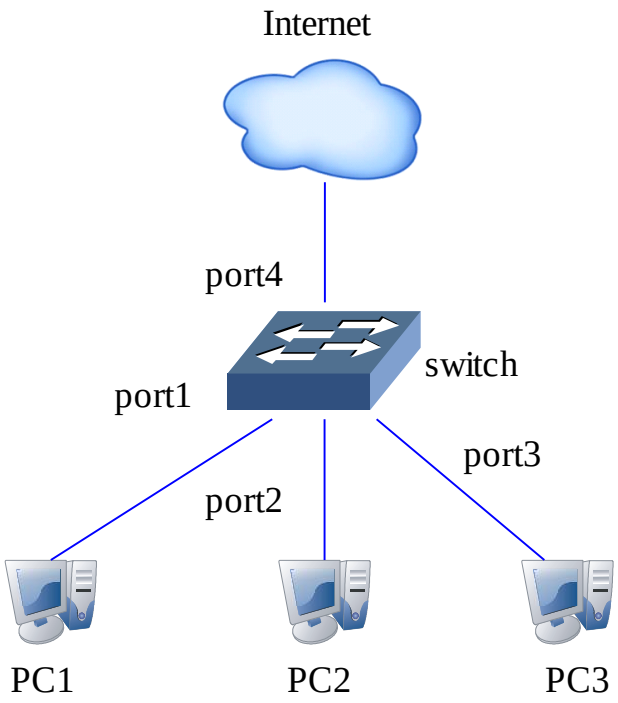


图13-1 端口保护配置示例图

administrator#**config**

administrator(config)# **ifconfig port-range 1-3**

Switch(**port-range-1-3**)# **port protect**

Switch(**port-range-1-3**)#**exit**

administrator(config)# **display port protected**

十四、 端口镜像功能配置

14.1 端口镜像功能概述

端口镜像功能是指将指定的源端口某些报文，镜像到指定的镜像目的端口，而不影响正常报文转发的功能。交换设备用户使用该功能可以监控某个端口的报文接收和发送情况，并分析相关网络状况，或者故障情况。

14.2 端口镜像功能配置

14.2.1 端口镜像功能缺省配置

功能	缺省值
端口镜像功能	禁止
镜像源端口	空
镜像目的端口	端口 1

14.2.2 端口镜像功能配置

镜像端口的报文按照配置的镜像规则复制一份到监视端口，便于监视网络的运行情况。缺省条件下，端口 1 为监视端口。监视端口与镜像端口不能为同一个端口。

镜像功能生效后，出/入镜像端口的报文会被复制一份到监视端口。在配置镜像端口时同时设置了镜像规则：both，ingress 或 egress。同样，设为监视端口后就不能再设为镜像端口。

镜像功能启用后，该功能相关的其他配置才生效。

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**mirroring (on | off)**	开启/关闭镜像功能
第 3 步	**mirroring monitor ethernet-port**	设置镜像功能的监视端口

	port-number	*port-number*：物理端口号；
第 4 步	**[no] mirroring source-port-list (both |ingress| egress) *port-number***	设置镜像功能的镜像源端口，并指定相应的入方向和出方向。 no：可以删除已设置的镜像端口； *port-number*：物理端口号列表，可以使用“,”和“-”进行多端口输入；
第 5 步	**exit**	退出全局配置模式进入特权用户模式
第 6 步	display mirroring	显示镜像配置

使用全局配置命令 no mirroring all 可以删除所有的镜像设置。

⚠注意：

被镜像的报文在镜像目的端口也要遵循该端口的 VLAN 配置规则转发。

镜像端口允许有多个，但监视端口只能有一个。默认情况下未启用镜像功能。

14.3 监控与维护

命令	描述
display mirroring	显示镜像配置

14.4 典型配置举例

配置示例 14-1：

设置端口 26 为监视端口，监控端口 5-8 的入方向流量，监控端口 7-12 的出方向流量。

配置过程：

Switch **#config**

administrator (config)**#mirroring on**

administrator (config)**#mirroring monitor ethernet-port 26**

administrator (config)**#mirroring source-port-list ingress 5-8 egress 7-12**

administrator (config)**#exit**

Switch **#display mirroring**

```
Mirror: On
Monitor port: port26
-----------the ingress mirror rule-----------
Mirrored ports: port-list 5-8
-----------the egress mirror rule-----------
Mirrored ports: port-list 7-12
```

十五、 STP 配置

15.1 STP/RSTP 原理介绍

15.1.1 STP 用途

STP（Spanning Tree Protocol，生成树协议）是根据 IEEE 协会制定的 802.1D 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。运行该协议的设备通过彼此交互报文发现网络中的环路，并有选择地对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构，从而防止报文在环路网络中不断增生和无限循环，避免主机由于重复接收相同的报文造成的报文处理能力下降的问题发生。

STP 包含了两层含义，狭义的 STP 是指 IEEE 802.1D 中定义的 STP 协议，广义的 STP 是指包括 IEEE 802.1D 定义的 STP 协议以及各种在它的基础上经过改进的生成树协议。

15.1.2 STP 报文

STP 采用的协议报文是 BPDU（Bridge Protocol Data Unit，桥协议数据单元），也称为配置消息。

STP 通过在设备之间传递 BPDU 来确定网络的拓扑结构。BPDU 中包含了足够的信息来保证设备完成生成树的计算过程。

BPDU 在 STP 协议中分为两类：

- 配置 BPDU（config BPDU）：用于进行生成树计算和维护生成树拓扑的报文。
- TCN BPDU（Topology Change Notification BPDU）：当拓扑结构发生变化时，用于通知相关设备网络拓扑结构发生变化的报文。

15.1.3 STP 基本概念

跟桥：

树形的网络结构，必须有树根，于是 STP 引入了根桥（Root Bridge）的概念。根桥在全网中只有一个，而且根桥会根据网络拓扑的变化而改变，因此根桥并不是固定的。

网络收敛后，根桥会按照一定的时间间隔产生并向外发送配置 BPDU，其他的设备对该配置 BPDU 进行转发，从而保证拓扑的稳定。

跟端口：

根端口，是指一个非根桥的设备上离根桥最近的端口。根端口负责与根桥进行通信。非根桥设备上有且只有一个根端口，根桥上没有根端口。

指定桥与指定端口：

指定桥与指定端口如下图所示，AP1、AP2、BP1、BP2、CP1、CP2 分别表示设备 Device A、Device B、Device C 的端口。

Device A 通过端口 AP1 向 Device B 转发配置消息，则 Device B 的指定桥就是 Device A，指定端口就是 Device A 的端口 AP1。

与局域网 LAN 相连的有两台设备：Device B 和 Device C，如果 Device B 负责向 LAN 转发配置消息，则 LAN 的指定桥就是 Device B，指定端口就是 DeviceB 的 BP2。

注意：根桥上所有端口都是指定端口。

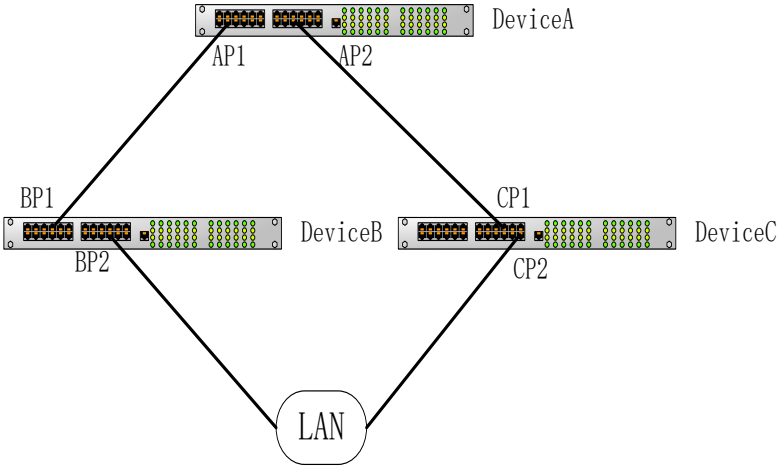


图 16-1 STP 指定桥与指定端口示意图

15.1.4 RSTP 原理介绍

快速生成树协议（RSTP）在普通 STP 协议的基础上增加了端口可以快速由阻

塞状态转变为转发状态的机制，加快了拓扑的收敛速度。在只连接了两个交换端口的点对点链路中，可以通过引入新的 proposal/agreement 机制，指定端口只需与下游网桥进行一次握手就可以无时延地进入转发状态，实现链路的快速切换。直接与终端相连而不是和其他网桥相连的端口定义为边缘端口，边缘端口可以直接进入转发状态不需要任何延时，由于网桥无法知道端口是否是直接与终端相连，所以需要人工配置。

15.1.5 STP 相关协议标准

Switch 内置的 STP/RSTP 协议基于如下标准实现：

- IEEE 802.1D：Spanning Tree Protocol；
- IEEE 802.1w：Rapid Spanning Tree Protocol；
- IEEE 802.1s：Multiple Spanning Tree Protocol。

15.2 STP 配置

15.2.1 STP 缺省配置

功能	缺省值
全局 STP 功能	关闭
端口 STP 功能	开启
生成树协议的端口优先级	128
生成树协议的系统优先级	32768
网络直径	7
端口的开销	一般依据其物理特性，缺省情况如下： • 10Mbps 为 2000000 • 100Mbps 为 200000 • 1000Mbps 为 20000 • 10Gbps 为 2000
每 hello time 内的最大发送包数	3
max-age 定时器	20s

hello-time 定时器	2s
forward-delay 定时器	15s

15.2.2 根桥/备份根桥配置

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**stp root （primary | secondary）**	为生成树设置交换机为根交换机或备份根交换机
第 3 步	**exit**	返回特权用户模式
第 4 步	**display stp**	显示 STP 配置情况

15.2.3 端口优先级配置

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入以太网物理接口模式 *port-number*：物理端口号；
第 3 步	**[no] stp priority** *<0-240>*	为生成树设置端口的优先级 *<0-240>*：端口优先级（16 的倍数）；
第 4 步	**exit**	返回全局配置模式
第 5 步	**exit**	返回特权用户模式
第 6 步	**display stp**	显示 STP 配置情况

15.2.4 交换机优先级配置

步骤	命令	描述

第 1 步	**config**	进入全局配置模式
第 2 步	**[no] stp priority** *<0-61440>*	为生成树设置交换机的优先级 *<0-61440>*：配置交换机优先级（4096 的倍数）；
第 3 步	**exit**	返回特权用户模式
第 4 步	**display stp**	显示 STP 配置情况

15.2.5 端口最大发送速率配置

使用该命令设置 MSTP 每 Hello Time 时间内允许发送的最大 BPDU 数量。此参数是一个相对值，没有单位，该参数被配置得越大，则每个 Hello Time 内允许发送的报文个数就越多，同时也会占用更多的交换机资源。与时间参数相同，只有根交换机的此项配置生效。

缺省情况下，此值为 3。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**[no] stp transmit-limit** *<1-10>*	设置交换机的端口最大发送速率 *<1-10>*：允许发送的最大 BPDU 数量
第 3 步	**exit**	返回特权用户模式
第 4 步	**display stp**	显示 MSTP 配置情况

15.2.6 STP 定时器配置

Hello Time：

交换机定期发送桥配置信息（BPDU）的时间间隔，用于交换机检测链路是否存在故障。交换机每隔 Hello Time 时间，会向周围的交换机发送 hello 报文，以确认链路是否存在故障。

缺省值为 2 秒，用户可以根据网络情况对此值进行调整。当网络中链路出现频繁变化时 ，可以适当缩短该值，来增强生成树协议的健壮性。相反，增大此值则可以降低生成树协议对系统 CPU 资源的占用率。

Forward Delay：

保证交换机状态安全迁移的时间参数。链路故障会引发网络重新进行生成树的计算，生成树的结构将发生相应的变化，不过重新计算得到的新配置消息无法立刻传遍整个网络。如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成暂时性的路径回环。为此协议采用了一种状态迁移的机制：根端口和指定端口重新开始数据转发之前，要经历一个中间状态（学习状态），中间状态经过 Forward Delay 时间的延时后，才能进入转发状态。这个延时保证了新的配置消息已经传遍整个网络。

缺省值为 15 秒，用户可以根据实际情况调整该值，当网络拓扑不频繁变化时可以将该值减小，反之增大。

Max Age：

生成树协议所使用的桥配置信息有生存周期，用来判断配置消息是否过时。交换机会将过时的配置消息丢弃。当桥配置信息过期后，生成树协议将重新计算生成树。

缺省值为 20 秒，该值过小会导致生成树重计算过于频繁，过大则会导致生成树协议不能及时适应网络拓扑结构的变化。

配置步骤：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**[no] stp hello-time** *<1-10>*	设置交换机时间参数 Hello Time *<1-10>*：定期发送 BPDU 的时间间隔
第 3 步	**[no] stp forward-delay** *<4-30>*	设置交换机时间参数 Forward Delay *<4-30>*：安全迁移的时间参数
第 4 步	**[no] stp max-age** *<6-40>*	设置交换机时间参数 Max Age *<6-40>*：BPDU 的生存周期
第 5 步	**exit**	返回特权用户模式

第 6 步	**display stp**	显示 MSTP 配置情况

15.3 边缘端口配置

15.3.1 STP mcheck 操作

在支持 MSTP 的交换机上端口有两种工作模式：STP 兼容模式 MSTP 模式。假设在一个交换网络中运行 MSTP 的交换机的端口连接着运行 STP 的交换机，该端口会自动迁移到 STP 兼容模式下工作。但是此时如果运行 STP 协议的交换机被拆离，该端口不能自动迁移到 MSTP 模式下，仍然会工作在 STP 兼容模式下运行。此时可以通过执行 mcheck 操作迫使其迁移到 MSTP 模式下运行。当然，如果之后，此端口再次收到新的 STP 报文，端口又会回到 STP 兼容模式下。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入以太网物理接口模式 *port-number*：物理端口号；
第 3 步	**stp mcheck**	将端口强制迁移回 MSTP 模式
第 4 步	**exit**	返回全局配置模式
第 5 步	**exit**	返回特权用户模式
第 6 步	**display stp**	显示 MSTP 配置情况

15.3.2 链路类型配置

点对点链路相连的两个端口可以通过传送同步报文快速迁移到转发状态，减少了不必要的转发延迟时间。缺省情况下，MSTP 根据双工状态设定端口的链路类型。全双工端口被认为是点到点链路，半双工被认作共享链路。

用户可以手工强行配置当前以太网端口与点对点链路相连，但是如果该链路不是点到点链路会使系统出现问题，一般情况下建议用户将此配置项设为自动状态，由系统自动发现端口是否与点到点链路相连。 具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入以太网物理接口模式 *port-number*：物理端口号；
第 3 步	**stp link-type (auto | point-to-point | shared)**	设置端口的链路类型
第 4 步	**exit**	返回全局配置模式
第 5 步	**exit**	返回特权用户模式
第 6 步	**display stp**	显示 MSTP 配置情况

15.3.3 统计清除配置

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
	ifconfig ethernet-port *port-number*	进入以太网物理接口模式 *port-number*：物理端口号；
第 2 步	**stp reset counters**	将端口统计信息归零
第 3 步	**exit**	返回全局配置模式
第 4 步	**exit**	返回特权用户模式
第 5 步	**display stp**	显示 MSTP 配置情况

15.3.4 监控与维护

命令	描述
display stp	显示生成树的基本信息
display stp port [*port-list*]	显示生成树端口列表的基本信息
display stp port [*port-list*] detail	显示生成树端口列表的详细信息

15.3.5 典型配置举例

现有三台 Switch 交换机，A、B、C 按设备 MAC 地址递增。通过配置交换机优先级自由选择根桥为 A 或者 B，从而改变拓扑；

组网图：

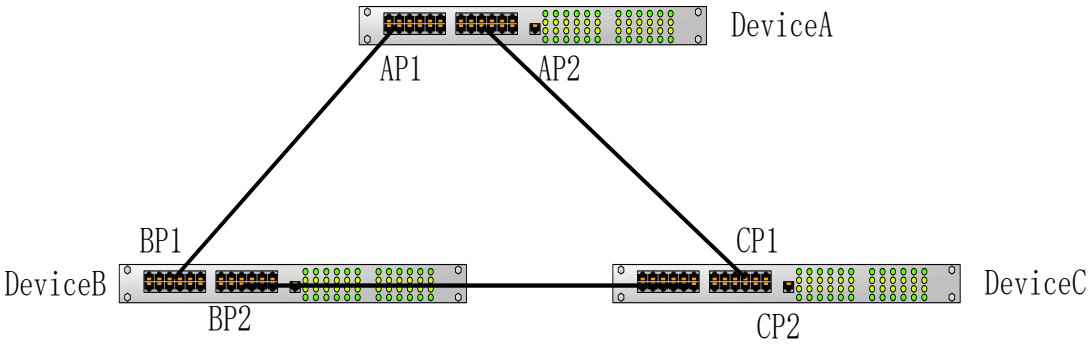


图 13-2：组网图

配置步骤：

开启 A、B、C 全局 STP 协议：

administrator(config)#stp on；

配置端口 AP1、AP2、BP1、BP2、CP1、CP2 的 STP 工作模式为 RSTP；

缺省情况下，查看稳定后的拓扑结构：

administrator#display stp

可以观察到 A 交换机为根桥，交换机 B、C 的指定桥为 A；

查看交换机 A、B、C 的端口 1、2 的生成树配置状态；

administrator#display stp port1-2

A 交换机的 AP1 、AP2 作为指定端口处于正常转发状态；

B 交换机的 BP1 作为根端口处于正常转发状态，BP2 处于阻塞状态；

C 交换机的 CP1 作为根端口处于正常转发状态，CP2 处于阻塞状态；

将 B 的优先级配置为 4096，重新执行上述步骤：

administrator(config)#stp priority 4096

拓扑稳定后根桥变为 B，A、C 之间的端口 AP2、BP1 阻塞。

15.4 MSTP 原理介绍

15.4.1 MSTP 基本概念

MST 域（Multiple Spanning Tree Regions，多生成树域）是由交换网络中的多台交换机以及它们之间的网段构成。这些交换机都启动了 MSTP、具有相同的域名、相同的 VLAN 到生成树映射配置和相同的 MSTP 修订级别配置，并且物理上有链路连通。

MSTI（Multiple Spanning Tree Instance，多生成树实例）是指 MST 域内的生成树。一个 MST 域内可以通过 MSTP 生成多棵生成树，各棵生成树之间彼此独立。

VLAN 映射表是 MST 域的一个属性，用来描述 VLAN 和 MSTI 的映射关系。

IST（Internal Spanning Tree，内部生成树）是 MST 域内的一棵生成树。IST 和 CST（Common Spanning Tree，公共生成树）共同构成整个交换机网络的生成树 CIST Common and Internal Spanning Tree，公共和内部生成树）。IST 是 CIST 在 MST 域内的片段，是一个特殊的多生成树实例。

CST 是连接交换网络内所有 MST 域的单生成树。如果把每个 MST 域看作是一个“交换机”，CST 就是这些“交换机”通过 STP 协议、RSTP 协议计算生成的一棵生成树。

CIST 是连接一个交换网络内所有交换机的单生成树，由 IST 和 CST 共同构成。

域根是指 MST 域内 IST 和 MSTI 的树根。MST 域内各棵生成树的拓扑不同，域根也可能不同。总根（Common Root Bridge）是指 CIST 的树根。

15.5 MSTP 配置

15.5.1 MSTP 缺省配置

功能	缺省值

全局 MSTP 功能	关闭
端口 MSTP 功能	开启
MST 域的最大跳数	20
生成树协议的端口优先级	128
生成树协议的系统优先级	32768
网络直径	7
端口的开销	一般依据其物理特性，缺省情况如下： • 10Mbps 为 2000000 • 100Mbps 为 200000 • 1000Mbps 为 20000 • 10Gbps 为 2000
每 hello time 内的最大发送包数	3
max-age 定时器	20s
hello-time 定时器	2s
forward-delay 定时器	15s
MST 域的修订级别	0

15.5.2 MSTP 域配置

当交换机的运行模式为 MSTP 时，可为交换机设置其归属的域信息。交换机属于哪个 MST 域，是由域名，VLAN 映射表，MSTP 修订级别配置决定的。用户可以通过下面的配置过程将当前交换机划分在一个特定的 MST 域内。

注：在此，配置使用了 MST 域配置视图，配置 MST 域的域名、修订级别及 VLAN 到实例的映射关系时，都必须进入 MST 域视图才可进行。若只配置未激活，则配置信息只记录，不生效。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**stp region-config**	进入 MST 域配置模式
第 3 步	**[no] region-name** *word*	设置 MST 域的名称 *word*：region 的名字；

第 4 步	**[no] revision-level** *level*	设置 MST 域的修订级别 *level*：修订级别，范围<0-65535>，缺省情况为 0
第 5 步	**instance** *instance-id* **vlan-range** *vlan-id*	设置 MST 域的 VLAN 到实例映射关系 *instance-id*：实例号，范围<0-4095>； *vlan-id*：VLAN 的 ID，范围<1-4094>；
第 6 步	**exit**	返回全局配置模式
第 7 步	**stp region-config**	激活 MST 域配置信息
第 8 步	**exit**	返回特权用户模式
第 9 步	**display stp region-operation**	显示 MST 域配置信息

15.5.3 MSTP 域最大跳数配置

MST 域的最大跳数限制了 MST 域的规模。当且仅当配置的交换机为域根时，配置的最大跳数才作为 MST 域的最大跳数，其他非域根交换机配置此项无效。

从域内的生成树的根交换机开始，域内的配置消息（BPDU）每经过一台交换机的转发跳数就被减 1，交换机将丢弃收到的跳数为 0 的配置消息。使处于最大跳数外的交换机无法参与生成树的计算，从而限制了 MST 域的规模。

如：若设置域根交换机的最大跳数为 1，则域中生成树功能无法实现，因为只有这一台交换机参与生成树计算。缺省情况下，最大跳数为 20，即可以从域根沿生成树路径向下跳 19 步。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**[no] stp max-hops** *<1-40>*	设置交换机 MST 域的最大跳数 *<1-40>*：最大跳数；
第 3 步	**exit**	返回特权用户模式
第 4 步	**display stp**	显示 MSTP 配置情况

15.5.4 根桥/备份根桥配置

一方面，MSTP 可以通过配置交换机的优先级，然后经过生成树计算，来确定生成树的根交换机或备份根交换机；另一方面，用户也可以通过此命令来直接指定。要注意的是，如果采用直接指定根交换机的方式，那么在整个网络中，建议用户不能再修改任何交换机的优先级；否则，会造成指定根交换机或备份根交换机无效。

用户可以通过参数 instance instance-id 确定根交换机或备份根交换机生效的实例。如果 instance-id 取值为 0，或者省去参数 instance instance-id 时，当前交换机将被指定为 CIST 的根交换机或备份根交换机。

当前交换机在各实例中的根类型是互相独立的，即它既可以作为一个实例的根交换机或备份根交换机，同时又可以作为其他生成树实例的根交换机或备份根交换机。但在同一棵生成树实例中，同一台交换机不能既作为根交换机，又作为备份根交换机。

用户不能同时为一棵生成树实例指定两个或两个以上的根交换机；相反，用户可以给同一棵生成树指定多个备份树根。一般情况下，建议用户给一棵生成树指定一个树根和多个备份树根。

当根交换机出现故障或被关机时，备份根交换机可以取代根交换机成为相应实例的根交换机。但若此时如果用户设置了新的根交换机，则备份根交换机将不会成为根交换机。如果用户为一棵生成树实例配置了多个备份根交换机，当根交换机失效时，MSTP 将选择 MAC 地址最小的那个备份根交换机作为根交换机。

缺省情况下，交换机既不作为生成树的根交换机，也不作为生成树的备份根交换机。可以使用 no stp [instance instance-id] root 反向命令恢复缺省配置。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**stp [instance** *instance-id* **] root**	为某个生成树实例，设置交换机

	（**primary	secondary**）	为根交换机或备份根交换机 *instance-id*：实例号，范围<0-4095>；
第 3 步	**exit**	返回特权用户模式
第 4 步	**display stp**	显示 MSTP 配置情况

15.5.5 端口优先级配置

生成树协议计算生成树时，需要选举根端口（root port）和指定端口（designated port），在端口路径开销一致的前提下，对端端口 ID 越小的端口越容易被选举为根端口或者指定端口。用户可以通过设置端口优先级，降低端口 ID，继而有目的的控制生成树协议选择特定的端口成为根端口或者指定端口。优先级相同的情况下，端口号小的优先。

与配置交换机的优先级相同，端口优先级在不同实例中的配置相互独立。用户可以通过参数 instance instance-id 确定的配置端口优先级的实例。如果 instance-id 取值为 0，或者省去参数 instance instance-id 时，则是为 CIST 配置的端口优先级。

注：优先级取值必须为 16 的倍数，如 0、16、32、48 等，缺省值为 128。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入以太网物理接口模式 *port-number*：物理端口号；
第 3 步	**[no] stp [instance** *instance-id*] **priority** <*0-240*>	为某个生成树实例，设置端口的优先级 *instance-id*：实例号，范围<0-4095>；<*0-240*>：端口的优先级；
第 4 步	**exit**	返回全局配置模式
第 5 步	**exit**	返回特权用户模式

第 6 步	**display stp**	显示 MSTP 配置情况

15.5.6 交换机优先级配置

交换机 Bridge ID 的大小决定了这台交换机是否能够被选作生成树的根。通过配置较小的优先级，可以得到较小的交换机 Bridge ID，达到指定某台交换机成为生成树树根的目的。优先级相同的情况下，MAC 地址小的为树根。

与配置根与备份根相同，优先级在不同实例中的配置相互独立。用户可以通过参数 instance instance-id 确定配置的优先级的实例。如果 instance-id 取值为 0，或者省去参数 instance instance-id 时，则是为 CIST 配置的桥优先级。

注：优先级取值必须为 4096 的倍数，如 0、4096、8192 等，缺省值为 32768。

具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**[no] stp [instance** *instance-id*] **priority** *<0-61440>*	为某个生成树实例，设置交换机的优先级 *instance-id*：实例号，范围<0-4095>； *<0-61440>*：交换机的优先级
第 3 步	**exit**	返回特权用户模式
第 4 步	**display stp**	显示 MSTP 配置情况

15.5.7 交换网络的网络直径配置

在 RSTP 协议中，网络直径指的是交换网络中交换机个数最多的那条路径上，交换机节点的个数。在 MSTP 协议中，设置网络直径只对 CIST 有效，对 MSTI 实例无效。并且在相同域内，无论路径经过多少节点，只当作一个节点计算。这样实际上，网络直径应定义为跨越域最多的那条路径上，域的个数。如果整个网络只有一个域，那么运行网络直径就为 1。

与 MST 域的最大跳数类似，当且仅当配置的交换机为 CIST 根交换机时，配置生效。

对比 MST 域的最大跳数是用来表征域的规模，网络直径则是表征整个网络规模的一个参数。网络直径越大说明一个网络的规模越大。

当用户配置交换机的网络直径参数时，MSTP 通过计算自动将交换机的 Hello Time，Forward Delay 以及 Max Age 三个时间参数设置为一个较优的值。

缺省情况下网络直径为 7，此时对应的三个时间也分别为它们的缺省值。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**[no] stp bridge-diameter** *<2-7>*	设置交换机网络的网络直径 *<2-7>*：网络直径参数
第 3 步	**exit**	返回特权用户模式
第 4 步	**display stp**	显示 MSTP 配置情况

15.5.8 端口最大发送速率配置

使用该命令设置 MSTP 每 Hello Time 时间内允许发送的最大 BPDU 数量。此参数是一个相对值，没有单位，该参数被配置得越大，则每个 Hello Time 内允许发送的报文个数就越多，同时也会占用更多的交换机资源。与时间参数相同，只有根交换机的此项配置生效。

缺省情况下，此值为 3。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**[no] stp transmit-limit** *<1-10>*	设置交换机的端口最大发送速率 *<1-10>*：允许发送的最大 BPDU 数量
第 3 步	**exit**	返回特权用户模式
第 4 步	**display stp**	显示 MSTP 配置情况

15.5.9 STP 定时器配置

Hello Time：

交换机定期发送桥配置信息（BPDU）的时间间隔，用于交换机检测链路是否存在故障。交换机每隔 Hello Time 时间，会向周围的交换机发送 hello 报文，以确认链路是否存在故障。

缺省值为 2 秒，用户可以根据网络情况对此值进行调整。当网络中链路出现频繁变化时 ，可以适当缩短该值，来增强生成树协议的健壮性。相反，增大此值则可以降低生成树协议对系统 CPU 资源的占用率。

Forward Delay：

保证交换机状态安全迁移的时间参数。链路故障会引发网络重新进行生成树的计算，生成树的结构将发生相应的变化，不过重新计算得到的新配置消息无法立刻传遍整个网络。如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成暂时性的路径回环。为此协议采用了一种状态迁移的机制：根端口和指定端口重新开始数据转发之前，要经历一个中间状态（学习状态），中间状态经过 Forward Delay 时间的延时后，才能进入转发状态。这个延时保证了新的配置消息已经传遍整个网络。

缺省值为 15 秒，用户可以根据实际情况调整该值，当网络拓扑不频繁变化时可以将该值减小，反之增大。

Max Age：

生成树协议所使用的桥配置信息有生存周期，用来判断配置消息是否过时。交换机会将过时的配置消息丢弃。当桥配置信息过期后，生成树协议将重新计算生成树。

缺省值为 20 秒，该值过小会导致生成树重计算过于频繁，过大则会导致生成树协议不能及时适应网络拓扑结构的变化。

整个交换网络中所有的交换机采用 CIST 根交换机上的三个时间参数，因此只有在根交换机上的配置生效。

具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**[no] stp hello-time** *<1-10>*	设置交换机时间参数 Hello Time

		<1-10>：定期发送 BPDU 的时间间隔
第 3 步	**[no] stp forward-delay** *<4-30>*	设置交换机时间参数 Forward Delay *<4-30>*：安全迁移的时间参数
第 4 步	**[no] stp max-age** *<6-40>*	设置交换机时间参数 Max Age *<6-40>*：BPDU 的生存周期
第 5 步	**exit**	返回特权用户模式
第 6 步	**display stp**	显示 MSTP 配置情况

15.5.10 边缘端口配置

边缘端口是指：不直接与任何交换机连接，也不通过端口所连接的网络间接与任何交换机相连的端口。

设置为边缘端口能够使该端口的状态迅速转变为转发状态，而不需要时间等待，对于直接与用户终端相连的以太网端口,为能使其快速迁移到转发状态,应将其设置为边缘端口。

当某个端口设置为边缘端口自动检测（auto）则边缘端口的属性是由实际情况决定的。当某个端口设置为边缘端口（force-true）时，当端口收到 BPDU 后实际运行值会变为非边缘端口。当某个端口设置为非边缘端口（force-false）时，同样，无论其实际情况下为边缘或非边缘端口，此端口会保持为非边缘端口，直到配置改变。

缺省情况下，网络交换机中所有端口均设置为自动检测属性。反向命令 no stp edged-port 恢复边缘端口属性的缺省值。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入以太网物理接口模式 *port-number*：物理端口号；

第 3 步	**stp edged-port (auto | force-true | force-false)**	设置端口的边缘端口属性
第 4 步	**exit**	返回全局配置模式
第 5 步	**exit**	返回特权用户模式
第 6 步	**display stp**	显示 MSTP 配置情况

15.5.11 STP mcheck 操作

在支持 MSTP 的交换机上端口有两种工作模式：STP 兼容模式 MSTP 模式。假设在一个交换网络中运行 MSTP 的交换机的端口连接着运行 STP 的交换机，该端口会自动迁移到 STP 兼容模式下工作。但是此时如果运行 STP 协议的交换机被拆离，该端口不能自动迁移到 MSTP 模式下，仍然会工作在 STP 兼容模式下运行。此时可以通过执行 mcheck 操作迫使其迁移到 MSTP 模式下运行。当然，如果之后，此端口再次收到新的 STP 报文，端口又会回到 STP 兼容模式下。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入以太网物理接口模式 *port-number*：物理端口号；
第 3 步	**stp mcheck**	将端口强制迁移回 MSTP 模式
第 4 步	**exit**	返回全局配置模式
第 5 步	**exit**	返回特权用户模式
第 6 步	**display stp**	显示 MSTP 配置情况

15.5.12 STP/MSTP 模式切换配置

当生成树协议开启时，支持两种生成树运行模式：STP 兼容模式和 MSTP 模式：

STP 兼容模式：不执行替换端口到根端口的快速转换和指定端口快速 forwarding。只发送 STP 配置报文（STP configuration BPDU）和拓扑变化通知（STP

TCN BPDU）。收到 MST BPDU 将丢弃不识别部分；

MSTP 模式：发送 MST BPDU。如果本交换机端口的对端运行 STP 协议，端口将转移到 STP 兼容模式下。如果本交换机端口的对端运行 RSTP 协议，本端口依旧保持 MSTP 协议，仅将其作为域外信息处理。

设置交换机生成树运行模式的步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**stp mode (stp | mstp)**	设置生成树的运行模式
第 3 步	**exit**	返回特权用户模式
第 4 步	**display stp**	显示 MSTP 配置情况

15.5.13 链路类型配置

点对点链路相连的两个端口可以通过传送同步报文快速迁移到转发状态，减少了不必要的转发延迟时间。缺省情况下，MSTP 根据双工状态设定端口的链路类型。全双工端口被认为是点到点链路，半双工被认作共享链路。

用户可以手工强行配置当前以太网端口与点对点链路相连，但是如果该链路不是点到点链路会使系统出现问题，一般情况下建议用户将此配置项设为自动状态，由系统自动发现端口是否与点到点链路相连。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入以太网物理接口模式 *port-number*：物理端口号；
第 3 步	**stp link-type (auto | point-to-point | shared)**	设置端口的链路类型
第 4 步	**exit**	返回全局配置模式
第 5 步	**exit**	返回特权用户模式
第 6 步	**display stp**	显示 MSTP 配置情况

15.5.14 根端口保护配置

当桥收到更高优先级的报文的时候就需要重新选举，重新选举一个是会影响网络的连通性，二来会消耗 CPU 资源。对于开启了 MSTP 功能的网络，如果有人发送高优先级的 BPDU 报文进行攻击，网络就会由于不断的选举而导致不稳定。而一般而言，各个桥的优先级是在网络规划阶段就已经配置好，越是靠近边缘的桥优先级越低，因此下行端口一般不会收到比桥优先级高的报文，除非有人恶意攻击。对于这些端口，可以通过开启根端口保护功能，拒绝处理比桥优先级高的报文，并在收到高优先级报文的时候阻塞端口一段时间，防止攻击源的其他攻击损害更上层的链路。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入以太网物理接口模式 *port-number*：物理端口号；
第 3 步	**stp rootguard (on | off)**	设置端口根端口保护属性
第 4 步	**display stp port detail**	显示 MSTP 配置情况

15.5.15 端口环路保护配置

生成树主要作用有两个：防止环路和链路备份。防止环路就要求必须将拓扑裁剪成树状结构，而如果需要进行链路备份，拓扑中必须有冗余的链路。生成树就是通过阻塞冗余链路来达到防止环路的功能，而在链路发生故障的时候放开冗余链路从而达到链路备份的功能。

生成树模块会周期性交换报文，如果一定时间内没有收到报文即认为发生了链路故障。然后选举，放开备份端口。而在实际应用中，导致收不到报文的原因可能并不是链路故障，如果在这种情况下放开备份端口就有可能导致环路。

环路保护的目的是当端口在一定时间内收不到报文的时候，不进行重新选举，保持端口原来的状态不变。注意：环路保护的功能和链路备份的功能是对立的，也即环路保护是以失去链路备份功能的代价来实现环路避免。具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入以太网物理接口模式 *port-number*：物理端口号；
第 3 步	**stp loopguard (on | off)**	设置端口环路保护属性
第 4 步	**display stp port detail**	显示 MSTP 配置情况

15.5.16 统计清除配置

MSTP 统计每个 MSTP 端口的如下类型 BPDU 报文数量：入 STP 报文、入 RSTP 报文，入 MSTP 报文，出 STP 配置报文、出 RSTP 报文（对于运转 MSTP 模块的交换机，此项将永远为 0）、出 MSTP 报文。

清除 MSTP 端口统计信息的步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入以太网物理接口模式 *port-number*：物理端口号；
第 3 步	**stp reset counters**	将端口统计信息归零
第 4 步	**exit**	返回全局配置模式
第 5 步	**exit**	返回特权用户模式
第 6 步	**display stp**	显示 MSTP 配置情况

15.6 显示与维护

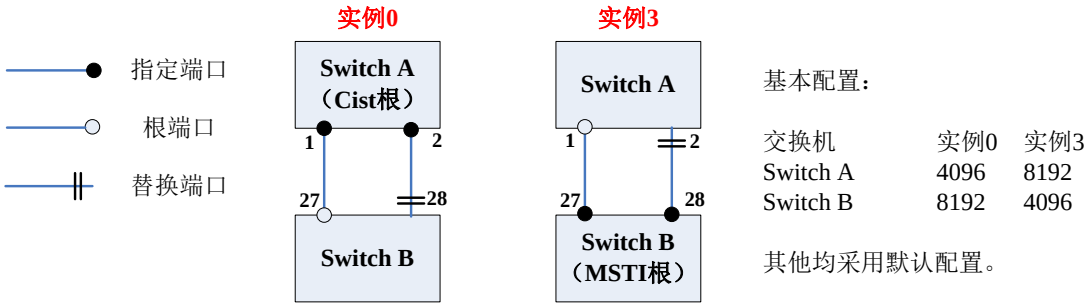
命令	描述
display stp region-operation	显示 MST 域的配置信息
display stp [instance *instance-id*]	显示多生成树实例的基本信息
display stp [instance *instance-id*] port [*port-list*]	显示多生成树实例端口列表的基本信息 *instance-id*：实例号，范围<0-4095>； *port-list*：端口列表，范围<1-28>；

display stp [instance *instance-id*] port [*port-list*] detail	显示多生成树实例端口列表的详细信息 *instance-id*：实例号，范围<0-4095>； *port-list*：端口列表，范围<1-28>；

15.7 典型配置举例

配置示例 15-1：

按照下图的拓扑，通过 STP 协议配置交换机 A 和 B。



基本配置：

交换机	实例0	实例3
Switch A	4096	8192
Switch B	8192	4096

其他均采用默认配置。

图 16-2 STP 配置示例拓扑

配置过程 15-1：

SwitchA:

administrator#config

administrator(config)#**vlan create 11-20 active**

administrator(config)#**ifconfig ethernet-port 1**

Switch(**port-1**)#**port link-type trunk**

Switch(**port-1**)#**port trunk permit vlan 11-20 confirm**

Switch(**port-1**)#**exit**

administrator(config)#**ifconfig ethernet-port 2**

Switch(**port-2**)#**port link-type trunk**

Switch(**port-2**)#**port trunk permit vlan 11-20 confirm**

Switch(**port-2**)#**exit**

administrator(config)#**stp on**

administrator(config)#**stp mode mstp**

administrator(config)#**stp region-config**

Switch(config-region)#**region-name aaa**

Switch(config-region)#**revision-level 2**

Switch(config-region)#**instance 3 vlan-range 11-20**

Switch(config-region)#**exit**

administrator(config)#**stp instance 0 priority 4096**

administrator(config)#**stp instance 3 priority 8192**

SwitchB:

administrator#**config**

administrator(config)#**vlan create 11-20 active**

administrator(config)#**ifconfig ethernet-port 27**

Switch(**port-27**)#**port link-type trunk**

Switch(**port-27**)#**port trunk permit vlan 11-20 confirm**

Switch(**port-27**)#**exit**

administrator(config)#**ifconfig ethernet-port 28**

Switch(**port-28**）#**port link-type trunk**

Switch(**port-28**)#**port trunk permit vlan 11-20 confirm**

Switch(**port-28**)#**exit**

administrator(config)#**stp on**

administrator(config)#**stp mode mstp**

administrator(config)#**stp region-config**

Switch(config-region)#**region-name aaa**

Switch(config-region)#**revision-level 2**

Switch(config-region)#**instance 3 vlan-range 11-20**

Switch(config-region)#**exit**

administrator(config)#**stp instance 0 priority 8192**

administrator(config)#**stp instance 3 priority 4096**

配置示例 15-2：

网络拓扑如下图所示，配置交换机 sw1、sw2、sw3 处于同一个 MST 域 MST1 中，并修改该域的修订级别为 2。将 VLAN1 影射到实例 1，VLAN2 影射到实例 2，其余的 VLAN 影射到 CIST。

配置 MST2、MST3 分别包含 sw4\sw6\sw7,sw5\sw8\sw9，VLAN 影射到实例的对应关系跟 MST1 类似。

配置以 sw3\sw4\sw5 为交换机的 CIST。

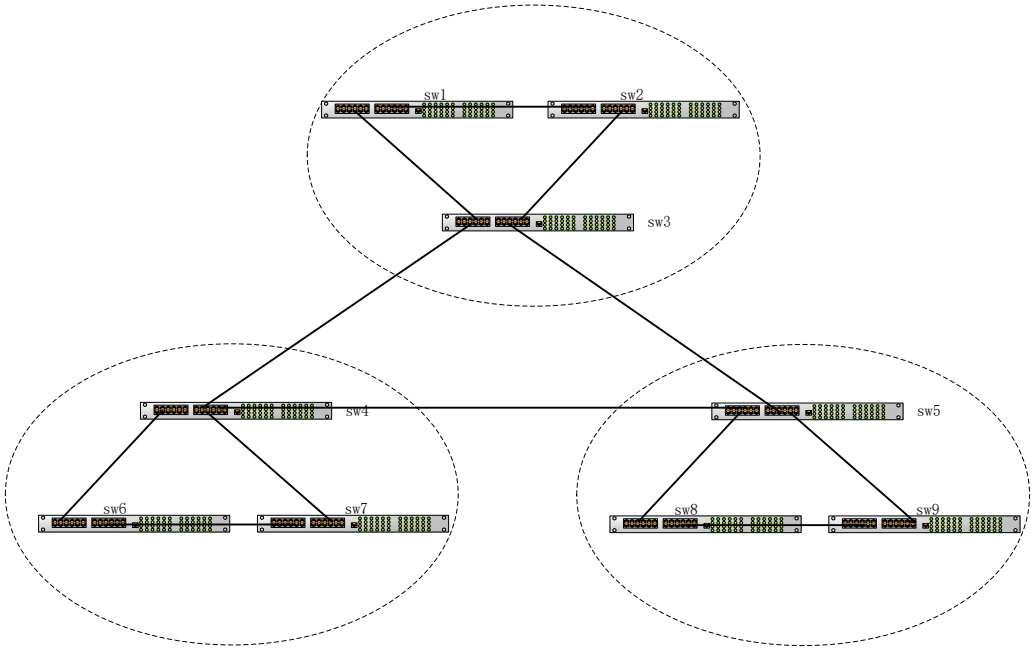


图 15-3 MSTP 配置示例拓扑

配置步骤 15-2：

以下述同样的配置步骤，配置 MST1， MST2 和 MST3。

administrator#**config**

administrator(config)#**stp region-config**

Switch(config-region)# **region-name MST1**

Switch(config-region)#**revision-level 2**

Switch(config-region)#**instance 1 vlan-range 1**

Switch(config-region)#**instance 2 vlan-range 2**

Switch(config-region)#**exit**

administrator(config)#**display stp region-operation**

administrator**#display stp instance 1**

上述步骤完成后，将 MST1、MST2、MST3 域的上电物理端口配置为 VLAN1 的成员端口，此外：

- MST1 域内配置 sw3 的桥优先级分别为 4096，其余交换机桥优先级大于 4096。
- MST2 域内配置 sw4 的桥优先级分别为 8192，其余交换机桥优先级大于 8192。
- MST2 域内配置 sw5 的桥优先级分别为 8192，其余交换机桥优先级大于 8192。

配置结果 15-2：

配置步骤全部完成后，sw3 作为总树的树根，sw4、sw5 间的连接将被阻塞。

MST1\MST2\MST3 域内 MSTI 只有一个，sw3\sw4\sw5 作为根，所以此时的逻辑拓扑图如下：

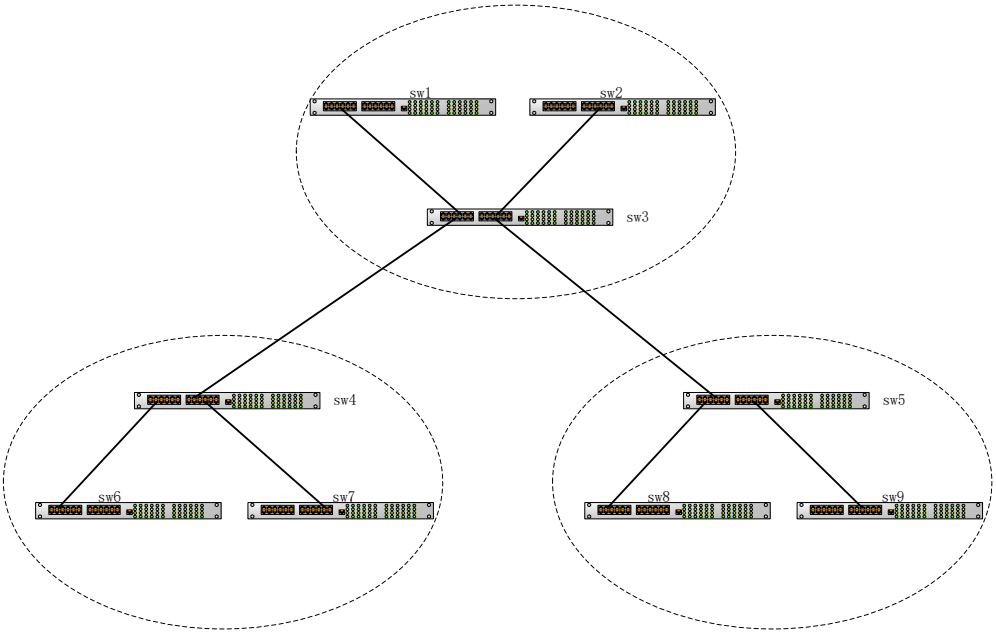


图 15-4　MSTP 配置示例拓扑

十六、 MRP 环网协议配置

16.1 MRP 原理介绍

16.1.1 MRP 用途

MRP（The Media Redundancy Protocol，介质冗余协议），是根据 IEC62439 标准建立的网络恢复协议，用于环形拓扑出现链路异常时，快速恢复网络。

16.1.2 MRP 报文

MRP 采用的协议报文目的地址为 01-15-4E-00-00-01、01-15-4E-00-00-02 的 MRP-PDU。

MRP 通过在设备之间传递 MRP-PDU 来确定网络的链路状态。MRP-PDU 中包含了足够的信息来保证链路异常时快速恢复网络。

MRP-PDU 在 MRP 协议中分为两类：

MC_Test：用于周期性的测试网络状态的报文。

MC_CONTROL：用于控制网络上的设备的报文，有 MRP_LinkUp、MRP_LinkDown、MRP_TopologyChange 3 种类型。

16.1.3 MRP 基本属性

Redundancy domain：

冗余域代表了整个环形网络，由域 ID 来标识，环形网络上的 MRM、MRC 设备都属于冗余域。

MRM：

MRM 全称 Media Redundancy Manager。环形网络中，MRM 用于控制整个环的状态，整个网络中有且只有一个 MRM 设备。

MRC：

MRM 全称 Media Redundancy Client。环形网络中，除 MRM 外的都是 MRC 设备。

主端口和副端口：

冗余域中的设备有两个端口连接到环形网络上，协议为了区分这两个端口分别叫做主端口和副端口。

管理 VLAN：

MRP 协议通过 MRP-PDU 探测网络状态和控制设备，为了不与数据报文相互影响，MRP-PDU 报文在一个特定的 VLAN 中传送，这个 VLAN 就是管理 VLAN。

管理优先级：

MRP 协议要求一个冗余域中只能存在一个 MRM 设备，当配置了两个 MRM 设备时，协议不能正常工作，为了防止这种情况出现，以设备的 MAC 地址+管理优先级进行比较，数值小的优先级大，优先级大的为 MRM，优先级小的会被重新配置为 MRC。

16.2 MRP 配置

16.2.1 MRP 缺省配置

功能	缺省值
冗余域使能	关闭
主端口	无
副端口	无
管理 VLAN	4093
管理优先级（可选配）	65535

⚠注意：

管理 VLAN 是传输 MRP-PDU 的 VLAN，需单独创建并与数据 VLAN 分开。

16.2.2 MRP 设备角色及主副端口配置

具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-*	进入主端口

	number	*port-number*：物理端口号，范围<1-28>；
第 3 步	**mrp domain** *domain-id* *port-number* (**mrm | mrc**)	设置副端口、设备角色 *domain-id*：domain 的 ID，范围<1-8>；
第 4 步	**exit**	返回特权用户模式
第 5 步	**display mrp domain** *domain-id*	显示 MRP 配置情况

⚠注意：

管理 VLAN 是传输 MRP-PDU 的 VLAN，需单独创建并与数据 VLAN 分开。

16.2.3 MRP 管理 VLAN 配置

具体的配置步骤如下：

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**mrp domain** *domain-id* **vlan** *vlan-id*	设置域的管理 VLAN *domain-id*：domain 的 ID，范围<1-8>； *vlan-id*：vlan 的 ID，范围<2-4094>；
第 3 步	**exit**	返回特权用户模式
第 4 步	**display mrp domain** *domain-id*	显示 MRP 配置情况

⚠注意：

配置管理 VLAN 时，要注意与数据 VLAN 分开，例如：数据 VLAN 为 VLAN2，那么管理 VLAN 不可设置为 VLAN2。

16.2.4 MRP 使能状态配置

具体的配置步骤如下：

步骤	命令	描述

第 1 步	**config**	进入全局配置模式
第 2 步	**mrp domain** *domain-id* (**on** | **off**)	设置域的使能 *domain-id*：domain 的 ID，范围<1-8>；
第 3 步	**exit**	返回特权用户模式
第 4 步	**display mrp domain** *domain-id*	显示 MRP 配置情况

16.3 典型配置举例

配置示例：

如下图所示，配置设备 A 为 MRM，配置设备 B 和 C 为 MRC。

MRP 的管理 VLAN 为 VLAN4092。

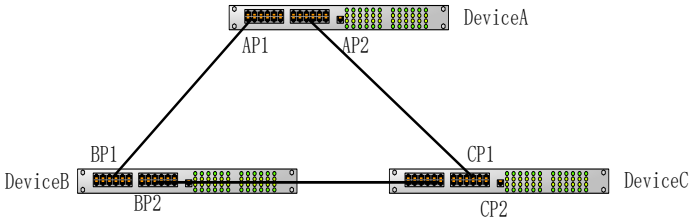


图 16-1 MRP 配置示例拓扑

配置步骤：

[Device A] 配置步骤：

administrator(config)#vlan create 4092 active

administrator(config)#ifconfig port-range 20,22

Switch(port-range-20-22)#port link-type trunk

Switch(port-range-20-22)#exit

administrator(config)#ifconfig ethernet-port 20

Switch(port-20#mrp domain 1 22 mrm

Switch(port-20)#exit

administrator(config)#mrp domain 1 vlan 4092

administrator(config)#mrp domain 1 on

administrator(config)#display mrp domain 1

```
DomainID:                       1
-----------------------------------------
Active:                         On
Primary Port:                    20(Forward)
Secondary Port:                  22(Block)
Manager vlan:                    4092
Manager role:                    MANAGER
Ring state:                      Close
```

[Device B] 配置步骤：

```
administrator(config)#vlan create 4092 active
administrator(config)#ifconfig port-range 20,22
Switch(port-range-20-22)#port link-type trunk
Switch(port-range-20-22)#exit
administrator(config)#ifconfig ethernet-port 20
Switch(port-20)#mrp domain 1 22 mrc
Switch(port-20)#exit
administrator(config)#mrp domain 1 vlan 4092
administrator(config)#mrp domain 1 on
administrator(config)#display mrp domain 1
```

```
DomainID:                       1
-----------------------------------------
Active:                         On
Primary Port:                   20 (Forward)
Secondary Port:                 22 (Block)
Manager vlan:                    4092
Manager role:                    CLIENT
```

```
Ring state:                     Close
```

[Device C] 配置步骤：

```
administrator(config)#vlan create 4092 active
administrator(config)#ifconfig port-range 20,22
Switch(port-range-20-22)#port link-type trunk
Switch(port-range-20-22)#exit
administrator(config)#ifconfig ethernet-port 20
Switch(port-20)#mrp domain 1 22 mrc
Switch(port-20)#exit
administrator(config)#mrp domain 1 vlan 4092
administrator(config)#mrp domain 1 on
administrator(config)#display mrp domain

DomainID:                       1
----------------------------------------
Active:                         On
Primary Port:                    20 (Forward)
Secondary Port:                  22 (Block)
Manager vlan:                    4092
Manager role:                    CLIENT
Ring state:                      Close
```

十七、 LLDP 协议配置

17.1LLDP 原理介绍

17.1.1 LLDP 协议概述

LLDP（Link Layer Discovery Protocol，链路层发现协议）是 IEEE 802.1ab 中定义的第二层发现（Layer 2 Discovery）协议。LLDP 提供了一种标准的链路层发现方式，可以将本端设备的主要能力、管理地址、设备标识、接口标识等信息封装到 LLDP 报文中传递给邻居节点，邻居节点在收到这些信息后将其以标准 MIB（Management Information Base，管理信息库）的形式保存起来，供 NMS（Network Management System，网络管理系统）查询及判断链路的通信状况。

MIB 数据库分成 LLDP Local System MIB 和 LLDP Remote System MIB。

Local System MIB：LLDP 本地 MIB，用来保存本地设备信息，包括设备 ID、接口描述、系统名称、设备能力、网络管理地址等；

Remote System MIB：LLDP 远端 MIB，用来保存相邻设备的信息。

当本地 MIB 库或远端 MIB 库发生变化时，设备向 NMS 发送拓扑变化的告警信息。

17.1.2 报文格式

6 Octets	6 Octets	2 Octets	46-1500 Octets	2 Octets
Destination Mac	Source Mac	EtherType	LLDPDU	FCS

（1） Destination Mac：长度 6 个字节，LLDP 帧的目的 MAC 地址。IEEE 802.1AB 规定可以取如下 3 种值：

- 0x0180-C200-000E：最近网桥（Nearest Bridge）组 MAC 地址。
- 0x0180-C200-0003：最近的非两端口 MAC 中继网桥（Nearest non-TPMR Bridge）组地址。
- 0x0180-C200-0000：最近的客户网桥（Nearest Customer Bridge）组 MAC 地址。

（2） Source Mac：长度 6 个字节，源 MAC 地址，为端口 MAC 地址或设备桥 MAC 地址。

（3） LLDPDU：长度不固定，数据字段，标识帧的负载为 LLDPDU。LLDPDU 就是封装在 LLDP 报文数据部分的数据单元。在组成 LLDPDU 之前，设备先将本地信息封装成 TLV 格式，再由若干个 TLV 组合成一个 LLDPDU 封装在 LLDP 报文的数据部分进行传送。

（4） FCS：4 字节，帧校验序列 FCS（Frame Check Sequence），用于接口判断报文是否传输错误。

17.2 LLDP 配置

17.2.1 LLDP 缺省配置

功能	缺省值
全局 LLDP 功能	关闭
端口 LLDP 功能	开启
LLDP 报文发送间隔	30s
本端信息在邻居节点中保持时间的倍数	4
LLDP 重新使能的延迟时间	2s
发送 LLDP 报文的延迟时间	2s
邻居信息变化告警的延迟时间	5s
LLD 告警使能	开启
LLDP 报文 Destination Mac	0180.C200.000E

17.2.2 LLDP 全局配置

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**lldp (enable | disable)**	LLDP 配置使能

		enable：使能； disable：去使能
第 3 步	**[no] lldp restart-delay** *<1-10>*	配置接口 LLDP 功能重新使能的延迟时间，单位：second
第 4 步	**[no] lldp message-transmission hold-multiplier** *<2-10>*	配置本端信息在邻居节点中保持时间的倍数
第 5 步	**[no] lldp message-transmission interval** *<5-32768>*	配置发送 LLDP 报文的发送间隔，单位：second
第 6 步	**[no] lldp message-transmission delay** *<1-8192>*	配置发送 LLDP 报文的延迟时间，单位：second
第 7 步	**[no] lldp trap-interval** *<5-3600>*	配置邻居信息变化告警的延迟时间，单位：second
第 8 步	**snmp-server lldp-trap (enable | disable)**	配置 LLDP 告警使能

17.2.3 LLDP 接口配置

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入对应物理接口配置模式 *port-number*：物理端口号；
第 3 步	**lldp (enable | disable)**	LLDP 配置使能 enable：使能； disable：去使能
第 4 步	**[no] lldp dest-address** *HHHH.HHHH.HHHH*	配置接口发送的 LLDP 报文目的 Mac 地址

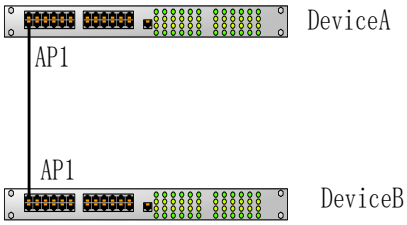
17.2.4 LLDP 信息维护

步骤	命令	描述

第 1 步	**display lldp local config**	查看 LLDP 本地配置
第 2 步	**display lldp local system-data [<*PORT-TYPE*> <*1-MAX_PORT_STR*>]**	查看 LLDP 系统描述信息 *PORT-TYPE*：端口类型 *1-MAX_PORT_STR*：支持的最大端口数
第 3 步	**display lldp remote [<*PORT-TYPE*> <*1-MAX_PORT_STR*>] [detail]**	查看 LLDP 远端信息 *PORT-TYPE*：端口类型 *1-MAX_PORT_STR*：支持的最大端口数
第 4 步	**display lldp statistic**	查看 LLDP 统计
第 5 步	**clear lldp global statistic**	清除 LLDP 全局统计
第 6 步	**clear lldp statistic** <*PORT-TYPE*> <*1-MAX_PORT_STR*>	清除 LLDP 端口统计 *PORT-TYPE*：端口类型 *1-MAX_PORT_STR*：支持的最大端口数
第 7 步	**clear lldp remote-table [**<*PORT-TYPE*> <*1-MAX_PORT_STR*>**]**	清除 LLDP 远端 MIB *PORT-TYPE*：端口类型 *1-MAX_PORT_STR*：支持的最大端口数

17.3 典型配置举例

如下图拓扑结构所示，交换机 SwitchA 和 SwitchB 使用 Port1(SwitchA)和 Port1(SwitchB)相连，SwitchA 设备 Mac 地址 0000.0304.3344，SwitchB 设备 Mac 地址 ec57.8e59.2c4e。



配置步骤：

[Device A] 配置步骤：

administrator(config)#**lldp enable**

administrator(config)#**ifconfig ethernet-port 1**

Switch(port-1)**#lldp enable**

[Device B] 配置步骤：

administrator(config)#**lldp enable**

administrator(config)#**ifconfig ethernet-port 1**

Switch(port-1)**#lldp enable**

SwitchA 上查看远端 LLDP 详细信息：

administrator(config)#display lldp remote port 3 detail

Port ChassisId PortId SysName MgtAddress ExpiredTime

---

port3 0000.0304.3344 port1 SC_DEMO 192.168.2.254 112

port3 has 1 remotes:

Remote 1

ChassisIdSubtype: macAddress

ChassisId: 0000.0304.3344

PortIdSubtype: ifName

PortId: port1

PortDesc: port1

SysName: SC_DEMO

SysDesc: Switch

SysCapSupported: Repeater/Hub,Bridge/Switch

SysCapEnabled: Repeater/Hub,Bridge/Switch

Mgt address: 192.168.2.254

Expired time: 112(s)

LLDPDU TTL: 30720

SwitchB 上查看远端 LLDP 信息：

administrator(config)#display lldp remote

Port ChassisId PortId SysName MgtAddress ExpiredTime

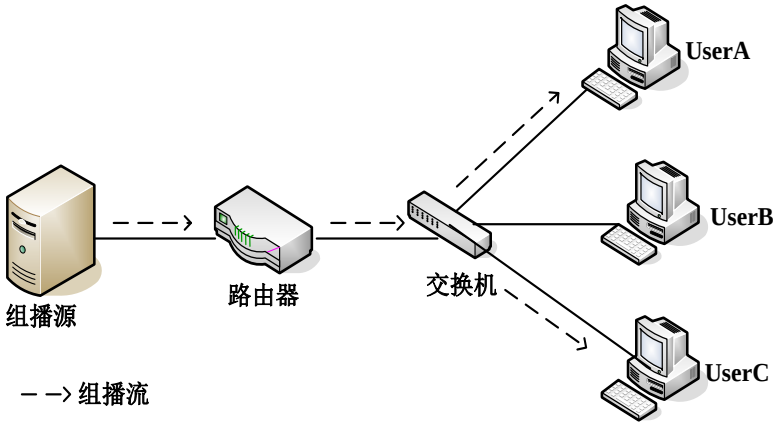
---

port3 0000.0304.3344 port1 SC_DEMO 192.168.2.254 97

十八、 IGMP SNOOPING 功能配置

18.1 IGMP SNOOPING 功能原理介绍

IGMP SNOOPING（Internet Group Management Protocol Snooping，组播侦听）是运行在二层设备上的组播协议，可以通过侦听上游三层组播设备和组播订阅者之间的 IGMP 协议报文来建立并管理设备的二层组播地址表，从而控制组播流的二层转发，避免组播业务数据在近用户端侧局域网内洪泛造成的网络拥塞和带宽浪费。IGMP SNOOPING 工作过测如下图所示：



图中交换机运行 IGMP SNOOPING 功能，使得订阅了组播业务的 UserA 和 UserC 能够接收到组播数据，而没有订阅组播业务的 UserB 接收不到组播数据。

三层组播设备和组播订阅者之间会互发如下 IGMP 协议报文进行信息交互：

- Membership Report（成员关系报告）报文

新增的组播数据订阅者首次加入某个组播组时，会主动向该组播组发送 Membership Report 报文，请求加入该组播组。IGMP SNOOPING 能够处理 IGMPv1、IGMPv2 和 IGMPv3 版本的 Membership Report 报文。运行 IGMP SNOOPING 的设备在收到 Membership Report 报文时进行如下处理：

- 将收到的 Membership Report 报文向所有路由端口转发；
- 解析 Membership Report 报文，如果该收包端口非组播成员端口，则增添对应的组播表项；
- 如果收包端口已经是组播成员端口，则刷新端口的老化定时器；

- 如定时器超时，则老化掉对应的组播表项；

- Leave Group（离开组）报文

当组播数据订阅者退出组播组时，会发送 Leave Group 报文到子网中的所有组播路由器，报文中包含要退出的组播组的地址。运行 IGMP SNOOPING 的设备收到 Leave Group 报文时，会进行如下处理：

- 将收到 Leave Group 报文的端口立即从指定组的转发表项中删除；
- 判断该端口是否是指定组的最后一个成员端口，如果是则将 Leave Group 报文向所有路由端口转发；

- ●Query（查询）报文

IGMP 的 Query 报文有两种，即通用组查询报文和特定组查询报文。

三层设备收到 Group Leave 报文时，会向指定组播组发送特定组查询报文，查询该组播组内是否还有其他组员存在；同时，三层设备还会周期性地向所连接的子网发送通用查询报文来确认组播组内是否还有成员存在，如果 3 次查询后没收 Membership Report 报文就不再向相应子网发送组播数据。运行 IGMP SNOOPING 的设备在收到 Query 报文时，会进行如下处理：

- 将 Query 报文向除接收端口外的所有端口转发；
- 解析 Query 报文并学习路由端口；

18.2 IGMP SNOOPING 管理配置

18.2.1 IGMP SNOOPING 缺省配置

功能	缺省值
IGMP SNOOPING 组播组老化时间	300s
IGMP SNOOPING 特性	关闭
IGMP SNOOPING 操作 vlan	1

18.2.2 IGMP SNOOPING 使能配置

步骤	命令	描述
第 1 步	config	进入全局配置模式

第 2 步	**igmp snooping (on|off)**	使能或禁用 IGMP SNOOPING 功能
第 3 步	**exit**	退出全局配置模式进入特权用户模式
第 4 步	**display igmp snooping**	显示 IGMP SNOOPING 配置

18.2.3 IGMP SNOOPING 操作 vlan 配置

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**[no] igmp snooping vlan** *vlan-list*	设置 IGMP SNOOPING 的操作 vlan 列表 *vlan-list*：VLAN 的范围{1-4094}，no 命令的范围{2-4094}；
第 3 步	**exit**	退出全局配置模式进入特权用户模式
第 4 步	**display igmp snooping**	显示 IGMP SNOOPING 配置

⚠注意：

no 命令的 vlan-list 范围{2-4094}，1 为默认操作 vlan

18.2.4 IGMP SNOOPING 组播组老化时间配置

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**[no] igmp snooping aging <5-3600>**	设置 IGMP SNOOPING 的组播组老化时间；
第 3 步	**igmp snooping aging never**	设置 IGMP SNOOPING 的组播组永不老化；
第 4 步	**exit**	退出全局配置模式进入特权用户

		模式
第 5 步	**display igmp snooping**	显示 IGMP SNOOPING 配置

18.3 监控与维护

命令	描述
display igmp snooping	显示 IGMP SNOOPING 配置
display igmp snooping group [vlan *vlan-id***]**	依据 vlan 显示 IGMP SNOOPING 学习到的组播组 *vlan-id*：VLAN 的 ID，范围为<1-4094>；
display igmp snooping group [port *port-number***]**	依据端口显示 IGMP SNOOPING 学习到的组播组 *port-number*：物理端口号；

18.4 典型配置举例

配置示例 18-1：

开启 IGMP SNOOPING，并配置操作 vlan 为 2，并显示配置。

配置过程：

administrator(config)# **igmp snooping on**

administrator(config)#**igmp snooping vlan 2**

administrator(config)#**display igmp snooping**

```
  IGMP snooping status             :On
  IGMP snooping operational vlans :2
  Multicast group aging time(s)   :300
```

配置示例 18-2：

设置 IGMP SNOOPING 的老化时间为 1000s，并显示配置。

配置过程：

administrator(config)#igmp snooping aging 1000

administrator(config)#display igmp snooping

```
IGMP snooping status           :On
IGMP snooping operational vlans :2
Multicast group aging time(s)   :1000
```

配置示例 18-3：

配置 IGMP SNOOPING 组播组永不老化，并显示。

配置过程：

administrator(config)#igmp snooping aging never

administrator(config)#display igmp snooping

```
IGMP snooping status           :On
IGMP snooping operational vlans :2
Multicast group aging time(s)   :never
```

配置示例 18-4：

显示学习到的组播组信息。

配置过程：

administrator(config)#display igmp snooping group

```
  PORT              VLAN       GROUP           Aging-time
-------------------------------------------------------------
 ethernet-port 2  1          239.1.2.200      300
```

十九、 SNTP 功能配置

19.1 SNTP 功能概述

SNTP(Simple Network Time Protocol 简单网络时间协议)协议，用于跨广域网或局域网同步时间的协议，属于 NTP 的简化版，安全机制较低，但报文格式一致。使用的是 UDP 123 端口，采用客户端/服务器的工作方式。

19.2 SNTP 功能配置

SNTP 客户端配置：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	sntp server A.B.C.D	客户端设置 SNTP 服务器 IP
第 3 步	**display sntp**	显示 sntp 客户端状态。

配置开启 SNTP 服务器模式：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**sntpd （enable|disable）**	开启或者关闭服务器模式

19.3 监控与维护

命令	功能描述
display sntp	显示 sntp 客户端状态

19.4 典型配置举例

配置示例 17-1：

作为 sntp 客户端，申请同 192.168.2.100 进行时间同步。

配置过程：

administrator#**config**

administrator(config)# **sntp server 192.168.2.100**

administrator(config)#**display sntp**

sntp time jump status: normal.

sntp service status: normal.

sntp signal status:normal.

SNTP server address:192.168.2.100

SNTP Server Stratum Version Synchronize Time.

192.168.2.100 9 1 1970-1-1 8:11:22

配置示例 17-2：

配置设备开启 SNTP 服务器模式。

配置过程：

administrator#**config**

administrator(config)# **stpd enable**

administrator(config)#**exit**

二十、 限速功能配置

20.1 限速功能概述

流量限速是一种网络管理技术，旨在通过控制网络流量来确保网络质量。是对不同类型的网络流量进行限制带宽的能力，其典型作用是限制进入某一网络的某一连接的流量与突发。在报文满足一定的条件时，如某个连接的报文流量过大，流量限速就可以采取丢弃报文的动作，进而限制带宽。

基于端口的速率控制，不同的端口，会给定一个发送数据包的不同带宽，其令牌桶的容量也会不同。可以采用 srTCM，trTCM 两种算法。

基于流的速率控制，会根据不同的数据流分配不同的带宽。可以采用 srTCM 和 trTCM 两种算法。

20.2 限速功能配置

20.2.1 限速功能缺省配置

功能	缺省值
端口限速功能	禁止
流限速功能	禁止

20.2.2 限速功能配置

配置基于端口的限速功能：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	ifconfig ethernet-port <1-28>	进入到端口模式下
第 3 步	rate-limit [in-rate <0-16384> in-buffer <8-128000>] [out-rate <0-16384> out-buffer <8-128000>]	配置入方向限速、出方向限速、入出同时限速，限速单位为 62.5(kbps)

第 4 步	rate-limit default	恢复到默认无限速状态，第 3 步命令的反向命令

配置基于流限速的功能：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**rate-limit dest-mac HHHH.HHHH.HHHH mask-len <0-48> rate <0-1000000>**	配置基于 dmac 的限速值
第 3 步	rate-limit (enable|disable)	配置流限速的使能或者去使能
第 4 步	display rate-limit rule	显示流限速的配置
第 5 步	no rate-limit dest-mac HHHH.HHHH.HHHH mask-len <0-48>	删除流限速的规则

20.2.3 监控与维护

命令	功能描述
display rate-limit rule	显示流限速的配置

20.3 典型配置举例

配置示例 20-1：

配置基于端口的限速，入方向限速 50M,出方向限速 20M。

配置过程：

administrator#**config**

administrator(config)# ifconfig ethernet-port 1

administrator (port-1)# **rate-limit in-rate 800 in-buffer 10000 out-rate 320 out-buffer 10000**

反向命令：

administrator (port-1)#rate-limit default

配置示例 20-2：

配置基于 DMAC0000.0001.00AA 的流限速，限速值为 100M。

配置过程：

administrator#**config**

administrator(config)# **rate-limit dest-mac 0000.0001.00aa mask-len 48 rate 100000**

administrator(config)# **rate-limit enable**

administrator (config)#**display rate-limit rule**

rate limit status: enable

Mac: 0000.0001.00AA maskLen: 48 rate: 100000

port: 1

in rate: 800

in buffer: 10000

out rate: 320

out buffer: 10000

port: 2

in rate: 0

in buffer: 0

out rate: 0

out buffer: 0

port: 3

in rate: 0

in buffer: 0

out rate: 0

out buffer: 0

……

port: 27

in rate: 0

in buffer: 0

out rate: 0

out buffer: 0

port: 28

in rate: 0

in buffer: 0

out rate: 0

out buffer: 0

二十一、 Filter 功能配置

21.1 过滤功能概述

报文过滤（Filter）是一种基于规则的报文过滤技术。

针对每个端口输入的数据，可以分别针对源 MAC 地址进行过滤。支持根据源 MAC 地址指定允许接收帧的白名单；

针对每个端口输入的数据，可以分别针对目的 MAC 地址进行过滤。支持根据目的 MAC 地址指定允许转发帧的白名单。

针对特定类型的数据，进行过滤。

21.2 过滤功能配置

21.2.1 过滤功能缺省配置

功能	缺省值
端口 MAC 地址过滤功能	禁止
svpkt 功能	禁止
goosepkt 过滤功能	禁止
Business 过滤功能	禁止

21.2.2 过滤功能配置

配置基于端口的过滤功能：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	ifconfig ethernet-port <*1-28*>	进入到端口模式下
第 3 步	mac-filter rule-id <*0-9*> (dmac|smac) HHHH.HHHH.HHHH mask-len <*0-48*> (drop|forward)	配置 dmac 或 smac 的过滤规则，同时设置动作是丢弃还是转发.

		rule-id:规则 ID,取值<0-9> HHHH.HHHH.HHHH：mac 地址 mask-len ： mac 地址的掩码，取值<*0-48*>
第 4 步	mac-filter (enable | disable)	Mac-filter 配置使能 enable：使能； disable：去使能
第 5 步	no mac-filter rule-id <0-9>	删除指定 macfilter 规则

⚠注意：

配置 mac-filter 规则必须在 mac-filter 功能处于 disable 状态。

配置全局过滤的功能：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	svpkt-filter (enable|disable)	配置 SV 报文过滤功能，如果使能，则端口收到的 SV 报文全部丢弃 enable：使能； disable：去使能
	goosepkt-filte (enable|disable)	配置 Goose 报文过滤功能，如果使能，则端口收到的 Goose 报文全部丢弃 enable：使能； disable：去使能
	business-filter (enable|disable)	配置除 SV 和 Goose 报文之外的业务报文过滤功能，如果使能，则端口收到的所有报文，

		除 SV 和 Goose 报文之外的全部丢弃 enable：使能； disable：去使能

21.2.3 监控与维护

命令	功能描述
display mac-filter enable-status	（端口模式）显示 mac-filter 的配置
display svpkt-filter-enable-status	（Config 模式）显示 svpkt-filter 的配置
display goosepkt-filter-enable-status	（Config 模式）显示 goosepkt-filter 的配置
display businessfilter-enable-status	（Config 模式）显示 businessfilter 的配置

21.3 典型配置举例

配置示例 21-1：

配置基于端口的 mac 过滤，过滤 0000.0000.0001 的 smac,和 0000.0000.0001 的 dmac 两种报文，动作是丢弃。

配置过程：

administrator#**config**

administrator(config)# ifconfig ethernet-port 1

administrator (port-1)#**mac-filter rule-id 0 smac 0000.0000.0000 mask-len 48 drop**

administrator (port-1)#**mac-filter rule-id 1 dmac 0000.0000.0002 mask-len 48 drop**

administrator (port-1)#**mac-filter enable**

反向命令：

administrator (port-1)#no mac-filter rule-id 1

查看配置：

```
administrator(port-1)#display mac-filter enable-status
  port    mac-filter status
---------------------------
    1         enable
    2         disable
    3         disable
    4         disable
    5         disable
    6         disable
    7         disable
    8         disable
    9         disable
    10        disable
    11        disable
    12        disable
    13        disable
    14        disable
    15        disable
    16        disable
    17        disable
    18        disable
    19        disable
    20        disable
    21        disable
    22        disable
    23        disable
    24        disable
```

25 disable

26 disable

27 disable

28 disable

port ruleID mac maskLen action

---

1 0 smac:0000.0000.0001 48 drop

配置示例 21-2：

配置 SV 报文过滤和 GOOSE 报文过滤。

配置过程：

administrator#**config**

administrator(config)#**svpkt-filter enable**

administrator(config)#**goosepkt-filter enable**

administrator (config)#**display svpkt-filter-enable-status**

svpkt-filter-enable-status: enable

administrator(config)#**display goosepkt-filter-enable-status**

goosepkt-filter-enable-status: enable

配置示例 21-3：

配置除 SV 报文和 GOOSE 报文之外的所有业务报文过滤。

配置过程：

administrator#**config**

administrator(config)#**business-filter enable**

administrator (config)#**display business-filter-enable-status**

business-filter-enable-status: enable

二十二、 ACL 功能配置

22.1 ACL 功能概述

访问控制列表(ACL)是一种基于包过滤的访问控制技术,它可以根据设定的条件对接口上的数据包进行过滤，允许其通过或丢弃。访问控制列表被广泛地应用于网络设备，借助于访问控制列表，可以有效地控制用户对网络的访问，从而最大程度地保障网络安全。

22.2 ACL 功能配置

22.2.1ACL 缺省配置

无

22.2.2ACL 功能配置

ACL 条件配置命令如下：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**flow <1-1000> dmac HHHH.HHHH.HHHH HHHH.HHHH.HHHH [vlan <1-4094>] [cos <0-7>] [udf0 RULE-STRING] [udf1 RULE-STRING]**	配置 DMAC 相关条件的下发
	flow <1-1000> smac HHHH.HHHH.HHHH HHHH.HHHH.HHHH [vlan <1-4094>] [udf0 RULE-STRING] [udf1 RULE-STRING]	配置 SMAC 相关条件的下发
	flow <1-1000> ipv4 [dmac HHHH.HHHH.HHHH	配置 IPV4 相关条件的下发

	HHHH.HHHH.HHHH] [smac HHHH.HHHH.HHHH HHHH.HHHH.HHHH] [vlan <1-4094>] [sip A.B.C.D A.B.C.D] [dip A.B.C.D A.B.C.D] \ [dscp <0-63>] [ippro <0-255>] [l4dstport <0-255>] [l4srcport <0-255>] [udf0 RULE-STRING] [udf1 RULE-STRING]	
	flow <1-1000> ipv6 [dmac HHHH.HHHH.HHHH HHHH.HHHH.HHHH] [smac HHHH.HHHH.HHHH HHHH.HHHH.HHHH] [vlan <1-4094>] [sip A:B::C:D/M] [dip A:B::C:D/M] \ [dscp <0-63>] [ippro <0-255>] [l4dstport <0-255>] [l4srcport <0-255>] [udf0 <0xHH>] [udf1 <0xHH>]	配置 IPV6 相关条件的下发
第 3 步	**no flow <1-1000>**	删除流量识别 Id
第 4 步	**display flow <1-1000> config**	显示配置
第 5 步	**flow [udf0-offset <0-64>] [udf1-offset <0-64>]**	配置 UDF 偏移
第 6 步	**clear flow <1-1000> stats**	清除流量统计

配置基于端口下发 ACL 功能：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	ifconfig ethernet-port *<1-28>*	进入到端口模式下
第 3 步	**[no] flow <1-1000> (tsn|forward|drop) [statistics]**	删除/配置 ACL 规则，同时选择设置动作是丢弃、转发、TSN. Tsn:表示流量识别为 Tsn 流量分配 tsnHandle

		Forward:转发 Drop:丢弃
第 4 步	**[no] flow <1-1000> policer <1-1000>**	配置/删除基于流的流量监管规则

⚠注意：

1. 端口下配置 ACL 规则必须在 Flow 规则配置之后。
2. 先配置流量监管的规则，才能在接口下配置基于流的流量监管。

22.2.3 监控与维护

命令	功能描述
display flow <1-1000> config	（Config 模式）显示 flow 规则的配置
display flow <1-1000> stats	（Config 模式）显示基于 flow 规则的命中统计

22.3 典型配置举例

配置示例 22-1：

配置基于端口的 Acl 过滤，过滤 0000.0000.0001 的 dmac, vlan3 cos 3，动作是丢弃并统计

配置过程：

administrator#config

administrator(config)# flow 3 dmac 0000.0000.0001 ffff.ffff.ffff vlan 3 cos 3

administrator(config)# ifconfig ethernet-port 1

administrator (port-1)#flow 3 drop statistics

反向命令：

administrator (port-1)# no flow 3 drop statistics

administrator(config)# no flow 3

查看配置：

administrator(config)#display flow 3 config

flowId: 3

---

dmac: 0.0.0.0.0.1 mask: ff.ff.ff.ff.ff.ff.

vlan: 3

cos: 3

administrator(config)#

administrator(config)#display flow 3 stats

flowId: 3

PktsCnt: 0

BytesCnt: 0

配置示例 22-2：

配置基于端口的 Acl 过滤，匹配 IP 报文，SIP=1.1.1.1 ,DIP 任意，udf0 0x1234 udf10x5678

UDF 偏移 udf0-offset 20 udf1-offset 22，例如打入 UDP 报文，udf 对应 udp 端口号位置。

配置过程：

administrator#**config**

administrator(config)# flow udf0-offset 20 udf1-offset 22

administrator(config)# flow 8 ipv4 sip 1.1.1.1 255.255.255.0 dip 2.2.2.2 0.0.0.0 udf0 1234 udf1 5678

查看配置：

administrator(config)#display flow 8 config

flowId: 8

---

sip: 1.1.1.1 mask: 255.255.255.0

dip: 2.2.2.2 mask: 0.0.0.0

udf0: 0x1234

udf1: 0x5678

administrator(config)# ifconfig ethernet-port 1

administrator (port-1)#flow 8 drop

配置示例 22-3：

配置 ACL 规则，匹配 DMAC，动作是 tsn，相当于基于流分配了 tsnHandle 该 flowId 作为后续 FRER 以及 PSFP 的输入

配置过程：

administrator#**config**

administrator(config)# **flow 12 dmac 0022.0022.0022 ffff.ffff.ffff**

administrator(config)# ifconfig ethernet-port 1

administrator (port-1)#flow 12 tsn

二十三、 FRER 功能配置

23.1 FRER 功能概述

帧复制和帧消除机制(frame replication and elimination for reliability (FRER)，在 IEEE802.1CB 中定义，具体内容包括冗余传输中数据帧的识别以及复制，识别复制帧，以及消除复制帧。为了达到协议中所定义的功能，就需要在终端或者网络桥中实现帧的复制和消除功能。

23.2 FRER 功能配置

23.2.1 FRER 缺省配置

无

23.2.2 FRER 功能配置

FRER 配置命令如下：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	**frer split flow-id <1-1000> egress-port-list {1-28}**	配置基于流的流分裂 Flow-id: ACL 流量识别的 flow Egress-port-list：流分裂的端口
第 3 步	**no frer split flow-id <1-1000> egress-port-list**	删除流分裂
第 4 步	**[no] frer add-rtag flow-id <1-1000>**	删除/配置基于流添加 RTAG 的操作
第 5 步	**[no] frer remove-rtag flow-id <1-1000>**	删除/配置基于流删除 RTAG 的操作

第 6 步	**frer recovery <1-1000> flow-id {1-1000} (individual|merge) algorithm (match|vector) [history-length <0-16>] [accept-no-tag]**	配置基于流的帧恢复功能 **individual：表示成员流** merge:表示复合流 match:表示帧消除时 match 算法 vector:表示帧消除时 vector 算法 history-len:表示 vector 算法下的序列号长度
第 7 步	**no frer recovery <1-1000> flow-id {1-1000}**	删除某条基于流的帧恢复功能

⚠注意：

1. 配置 FRER 时需要先配置 ACL 规则。

22.2.3 监控与维护

命令	功能描述
display frer split flow-id <1-1000>	（Config 模式）显示流复制分裂的配置
display frer recovery <1-1000>	（Config 模式）显示基于流的帧消除配置
display frer recovery <1-1000> [cnt]	（Config 模式）显示基于流的帧消除统计

23.3 典型配置举例

配置 ACL 规则，匹配 DMAC，动作是 tsn，相当于基于流分配了 tsnHandle

基于上述配置，设置流的复制分类，转向 port 3,4，并添加 RTAG

配置过程：

administrator#**config**

administrator(config)# **flow 12 dmac 0022.0022.0022 ffff.ffff.ffff**

administrator(config)# ifconfig ethernet-port 1

administrator (port-1)#flow 12 tsn

administrator(config)#frer split flow-id 12 egress-port-list 3-4

administrator(config)#display frer split flow-id 12

frer split flowId: 12

---

frer split egress-port-bmp: 0xc (注：pbmp:0xc 表示 port 3-4)

administrator(config)#frer add-rtag flow-id 12

配置示例 23-2：

配置 ACL 规则，匹配 DMAC，动作是 tsn，相当于基于流分配了 tsnHandle；

基于上述配置，设置流的帧消除操作，并剥掉 RTAG。

基于上述配置，假设打入报文带 RTAG，并且 RTAG 中序列号相同，仅能转发 1 出来个报文，并且剥掉了 RTAG

配置过程：

administrator#**config**

administrator(config)# **flow 12 dmac 0022.0022.0022 ffff.ffff.ffff**

administrator(config)# ifconfig ethernet-port 1

administrator (port-1)#flow 12 tsn

administrator(config)# frer recovery 1 flow-id 12 merge algorithm match

administrator(config)#display frer recovery 1

frer rcvy rcvy-id: 1

---

frer rcvy streamList: 12

frer rcvy type: megre

frer rcvy alg: match

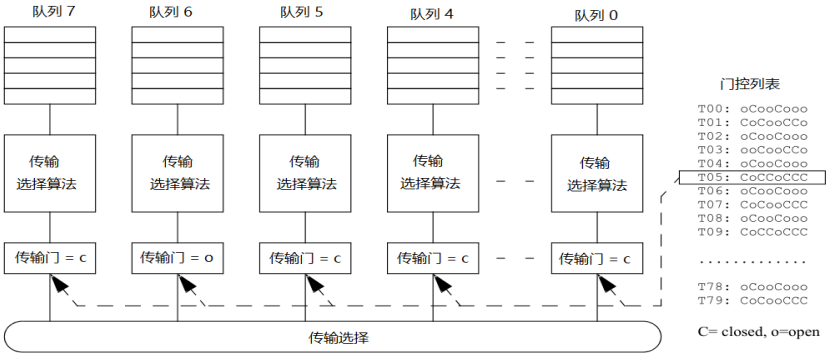
administrator(config)#frer remove-rtag flow-id 12

二十四、 QBV 功能配置

24.1 QBV 功能概述

IEEE 802.1Qbv 是 TSN 系列标准的关键技术之一。为了保障实时性和可靠性，TSN 工作组在 IEEE 802.1Q 的基础上提出了 IEEE 802.1Qbv 标准。

IEEE 802.1Qbv 采用时间感知整形器（Time Awareness Shaper，TAS）调度，通过在报文出队列时增加门控来实现。如下图所示，Qbv 周期性的扫描预先设定好的门控列表，并依据门控列表中各个门的开关状态控制队列的传输。通过控制，预定的时间窗口到期后，预期流量所在队列开门，预期流量被放行；而在同一时间窗口内其他非预期流量所在队列关门，非预期流量被阻止。TAS 调度算法排除了预期流量被非预期流量阻塞的可能性，降低了数据传输时延和抖动。



IEEE802.1Qbv 工作原理

24.2 QBV 功能配置

22.2.1QBV 功能缺省配置

功能	缺省值
端口门控	禁止
剩余报文长度检测	禁止
队列最大 SDU	9216

Base time	0

24.2.2 QBV 功能配置

配置基于端口的 QBV 功能：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	ifconfig ethernet-port <*1-28*>	进入到端口模式下
第 3 步	tsn qbv queue <0-7> max sdu <64-QBV_SDU_MAX>	配置队列支持的最大 SDU，默认值 9216
第 4 步	tsn qbv len-check gate <0-7>	配置队列每次发送时检测剩余时间是否足够发送该包，默认不检测
第 5 步	tsn qbv control-list index <0-127> queue {0-7} cycle-time <64-1000000000> open-time <64-1000000000> cycle-offset <0-1000000000>	配置门控列表。每端口最大支持 128 条门控列表，索引<0-127>；配置控制的队列{0-7}；cycle time 为单次门控执行总时间长度，单位 ns；open time 为此条表项对应门的开门时长，单位 ns；cycle offset 表示此条表项对应门的开门偏移，防止不同门开门时间重叠，单位 ns
第 6 步	tsn qbv control-list index <0-127> queue {0-7} start-delay <0-1000000000>	配置此次实际开门时间相对于配置时间延后值，用于微调时延，单位 ns
第 7 步	tsn qbv control-list index <0-127> queue {0-7} start-ahead <0-1000000000>	配置此次实际开门时间相对于配置时间提前值，用于微调时延，单位 ns
第 8 步	tsn qbv base time seconds <0-1000000000> nanoseconds <0-	配置 base time 值，qbv 使能后，将在 base time 加 2 分钟后的时间生效。默

	1000000000>	认值 0

⚠注意：

如果 base time 不配置，则在 Qbv 使能 2 分钟后，运行门控调度。

配置生效：

步骤	命令	描述
第 1 步	config	进入全局配置模式
第 2 步	ifconfig ethernet-port <*1-28*>	进入到端口模式下
第 2 步	tsn qbv configuration change	触发管理门控列表生效
	tsn qbv (enable|disable)	配置 Qbv 功能使能

⚠注意：

配置 tsn qbv configuration change 为动作性命令，该命令触发管理门控列表变为实际运行的门控列表。

24.2.3 监控与维护

命令	功能描述
display tsn qbv configuration port <1-MAX_PORT_STR>	显示对应端口的 Qbv 功能配置
display tsn qbv administration control-list port <1-MAX_PORT_STR>	显示对应端口的 Qbv 管理门控列表
display tsn qbv operation control-list port <1-MAX_PORT_STR>	显示对应端口的 Qbv 运行门控列表

24.3 典型配置举例

配置示例 24-1：

配置队列 0 最大 SDU 为 1000，检测剩余开门时间。

配置过程：

administrator#**config**

administrator(config)# **ifconfig ethernet-port 1**

administrator (port-1)#**tsn qbv queue 0 max sdu 1000**

administrator (port-1)#**tsn qbv len-check gate 0**

反向命令：

administrator (port-1)#**no tsn qbv queue 0 max sdu**

administrator (port-1)#**no tsn qbv len-check gate 0**

查看配置：

administrator(port-1)#**display tsn qbv configuration port 1**

Enable states :Disable

Supported list max length :128

Config change :No

Config change time :0 seconds, 0 nanoseconds

Config change error times :0

Tick granularity :0

Current time :0 seconds, 0 nanoseconds

Configuration change is in progress :No

Queue	Max Sdu	Transmission Overrun	Gate len-check
0	1000	0	Enable
1	9216	0	Disable
2	9216	0	Disable
3	9216	0	Disable
4	9216	0	Disable
5	9216	0	Disable

6 | 9216 | 0 | Disable

7 | 9216 | 0 | Disable

administrator(port-1)#

配置示例 24-2：

对端口 1 的门 0 和门 1 配置两条门控列表，分别开门 500us。第一条门控列表提前 10ns 开门，第二条门控列表延后 20ns 开门。

配置过程：

administrator#**config**

administrator(config)# ifconfig ethernet-port 1

administrator (port-1)**#tsn qbv control-list index 0 queue 0 cycle-time 1000000 open-time 500000 cycle-offset 0**

administrator (port-1)**#tsn qbv control-list index 0 queue 0 start-ahead 10**

administrator (port-1)**#tsn qbv control-list index 1 queue 1 cycle-time 1000000 open-time 500000 cycle-offset 500000**

administrator (port-1)**#tsn qbv control-list index 1 queue 1 start-delay 20**

反向命令：

administrator (port-1)**#no tsn qbv control-list index 0**

查看配置：

administrator(port-1)**#display tsn qbv administration control-list port 1**

Admin gate states :n/a

Admin GCL length :2

Admin base time :16 hours, 57 minutes, 33 seconds, 1000 nanoseconds

Admin cycle time :1000000

index | gate-state | interval | cycle-offset | start-delay | start-ahead

---

0 | occccccc | 500000 | 0 | 0 | 10

1 | cocccccc | 500000 | 500000 | 20 | 0

配置示例 24-3：

配置 base time 为今天 17 点 23 分 48 秒 1200 纳秒，配置改变触发管理门控列表切换到运行门控列表，Qbv 使能。

配置过程：

administrator#**config**

administrator(config)#**ifconfig ethernet-port 1**

administrator (port-1)#**tsn qbv base time hours 17 minutes 23 seconds 48 nanoseconds 1200**

administrator (port-1)#**tsn qbv configuration change**

administrator (port-1)#**tsn qbv enable**

反向命令：

administrator (port-1)#**tsn qbv disable**

查看配置：

administrator(port-1)#**display tsn qbv operation control-list port 1**

Oper gate states :n/a

Oper GCL length :2

Oper base time :17 hours, 23 minutes, 48 seconds, 1200 nanoseconds

Oper cycle time :1000000

index | gate-state | interval | cycle-offset | start-delay | start-ahead

---

0 | occccccc | 500000 | 0 | 0 | 10

1 | cocccccc | 500000 | 500000 | 20 | 0

administrator(port-1)#

administrator(port-1)#**display tsn qbv configuration port 1**

Enable states :Enable

Supported list max length :128

Config change :Yes

Config change time :Fri Dec 31 16:01:45 2023

Config change error times :0

Tick granularity :0

Current time :Fri Dec 31 16:21:33 2023

Configuration change is in progress :No

Queue	Max Sdu	Transmission Overrun	Gate len-check
0	1000	0	Enable
1	9216	0	Disable
2	9216	0	Disable
3	9216	0	Disable
4	9216	0	Disable
5	9216	0	Disable
6	9216	0	Disable
7	9216	0	Disable

administrator(port-1)#

二十五、 AS 协议配置

25.1AS 原理介绍

25.1.1 AS 协议概述

TSN 时间同步协议 IEEE 802.1AS 简称 gPTP (generalized precision time protocol)，是基于 IEEE 1588 时钟同步协议发展而来的，只在 L2 层工作。gPTP 主要采用两个步骤完成 gPTP 网络中的时间同步：

1. 确定 gPTP 主时钟。主时钟可以默认指定，也可以通过可以通过 BMCA(Best Master Clock Algorithm) 算法动态选取。由主时钟（clock master,CM）向从时钟(clock slave,CS)发布时间同步消息，建立时间同步体系；
2. 从时钟通过计算链路时延、本地时钟与主时钟的时间频率比、本地时间与主时钟的时间偏差等信息，调整本地时间，逐级完成与最佳主时钟的时间同步。

gPTP 协议在时钟同步时要求采用硬件时间戳的方式，在网络 MAC 层给报文标记时间戳，这样可以避免设备的操作系统与协议栈软件处理时间的影响，将同步时间精度从毫秒级提升到微妙级甚至纳秒级。

本产品支持 AS 及 1588 协议，可以通过配置 PTP profile 来选择不同的协议。

25.2 AS 协议配置

25.2.1 AS 缺省配置

功能	缺省值
PTP 协议 profile	AS 协议
全局 PTP 使能	关闭
端口 PTP 使能	关闭

priority1	128
Priority2	128
Domain ID	0
PTP 时钟类型	OC
PTP 一步法/两步法模式	Two-step
logAnnounceInterval	0
logSyncInterval	-3
LogPdelayReqInterval	0

25.2.2 PTP 全局配置

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ptp profile (as |1588)**	PTP 协议选择 as：AS 协议； 1588：1588 协议
第 3 步	**ptp <0-0> clock-type (bc|oc|p2p-tc|e2e-tc)**	PTP 时钟类型： oc：普通时钟； bc： 边界时钟； p2p-tc：P2P-TC； e2e-tc：E2E-TC
第 4 步	**ptp <0-0> step (one-step|two-step)**	PTP 同步模式： one-step：一步法； two-step：两步法
第 5 步	**ptp <0-0> domain <0-255>**	配置 PTP domain Id
第 6 步	**[no] ptp <0-0> domain**	删除 PTP domain Id，恢复默认值
第 7 步	**ptp <0-0> priority1 <0-255>**	配置 PTP 时钟 priority1
第 8 步	**[no] ptp <0-0> priority1**	删除 PTP 时钟 priority1 ，恢复默认值

第 9 步	**ptp <0-0> priority2 <0-255>**	PTP 时钟 priority2
第 10 步	**[no] ptp <0-0> priority2**	删除 PTP 时钟 priority2 ，恢复默认值
第 11 步	**ptp 0 (enable | disable)**	LLDP 配置使能 enable：使能； disable：去使能

25.2.3 PTP 协议接口配置

步骤	命令	描述
第 1 步	**config**	进入全局配置模式
第 2 步	**ifconfig ethernet-port** *port-number*	进入对应物理接口配置模式 *port-number*：物理端口号
第 3 步	**ptp <0-0> sync interval <-4 - 4>**	配置 sync 报文发包间隔，具体发包间隔为以 2 为底的配置值的次数
第 4 步	**no ptp <0-0> sync interval**	恢复 sync 发包间隔为默认值
第 5 步	**ptp <0-0> announce interval <-4 - 4>**	配置 announce 报文发包间隔，具体发包间隔为以 2 为底的配置值的次数
第 6 步	**no ptp <0-0> announce interval**	恢复 announce 发包间隔为默认值
第 7 步	**ptp <0-0> pdelay_req interval <-4 - 4>**	配置 pdelay_req 报文发包间隔，具体发包间隔为以 2 为底的配置值的次数
第 8 步	**no ptp <0-0> pdelay_req interval**	恢复 pdelay_req 发包间隔为默认值
第 9 步	**ptp <0-0> delay-mechanism (e2e|p2p)**	配置链路时延测试模式 e2e：request-response 模式； p2p： peer delay 模式
第 10 步	**ptp 0 (enable | disable)**	PTP 0 端口使能

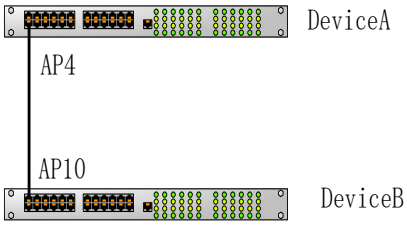
		enable：使能； disable：去使能

25.2.4 PTP 信息查询

步骤	命令	描述
第 1 步	**display ptp profile**	显示当前配置的 PTP profile
第 2 步	**display ptp <0-0> ethernet-port (all|<1-MAX_PORT_STR>) port-ds**	查看端口 PTP 配置与状态
	display ptp <0-0> ethernet-port (all|<1-MAX_PORT_STR>) counters	查看端口 PTP 报文收发统计
第 3 步	**reset ptp <0-0> ethernet-port (all|<1-MAX_PORT_STR>) counters**	清除端口的 PTP 报文统计
第 4 步	**display ptp <0-0> (default-ds |parent-ds |current-ds |time-property-ds)**	查看时钟 PTP 属性 default-ds:默认属性； parent-ds：父节点属性； current-ds：邻居链路比/offset from master 等； time-property-ds：时间属性
第 5 步	**display ptp <0-0> time**	显示当前的 PTP 时间

25.3 典型配置举例

如下图拓扑结构所示，交换机 SwitchA 和 SwitchB 使用 Port4(SwitchA)和 Port10(SwitchB)相连。



25.3.1 AS-twoStep 模式

配置步骤：

[Device A] 配置步骤：

administrator(config)#ptp 0 priority1 200

administrator(config)#ptp 0 enable

administrator(config)#ifconfig ethernet-port 4

administrator(port-4)#ptp 0 enable

[Device B] 配置步骤：

administrator(config)#ptp 0 priority1 100

administrator(config)#ptp 0 enable

administrator(config)#ifconfig ethernet-port 10

administrator(port-10)#ptp 0 enable

SwitchA 上查看 PTP 信息：

查看设备 ptp 默认属性：

administrator(config)#display ptp 0 default-ds

Default Parameter Data

PTP Instance ID: 0 PTP state: enabled

clock type: OC clock Identity:0000ea.fffe.34ebea

priority1: 200 priority2: 128

domain ID: 0 step mode: two-step

查看与主时钟的 offset：

administrator(config)#display ptp 0 current-ds

Current Parameter Data

PTP Instance ID: 0

offset From Master: -3 Neighbor RateRatio: 1.000000

查看端口的 ptp 配置与状态：

administrator(config)#display ptp 0 ethernet-port 4 port-ds

Port Parameter Data

PTP Instance ID: 0 PTP Port: 4

Port Enable: enabled Port State: slave

Sync Interval: 0 Announce Interval: 0

Pdelay interval: -3 Mean Link Delay: 2906

Ptp Vlan: 0 Delay Mechanism: P2P

查看端口 ptp 报文统计：

administrator(config)#display ptp 0 ethernet-port 4 counters

Port Parameter Statistics Data

SYNC : 1032 / 47472 , 22 / 1452

DELAY_REQ : 0 / 0 , 0 / 0

PDELAY_REQ : 133 / 7182 , 133 / 10108

PDELAY_RESP : 133 / 7182 , 133 / 10108

FOLLOW_UP : 1032 / 78432 , 22 / 2156

DELAY_RESP : 0 / 0 , 0 / 0

PDELAY_RESP_FOLLOW_UP : 133 / 7182 , 133 / 10108

ANNOUNCE : 130 / 9880 , 3 / 294

SIGNALING : 0 / 0 , 0 / 0

MANAGEMENT : 0 / 0 , 0 / 0

25.3.2 1588-oneStep 模式

配置步骤：

[Device A] 配置步骤：

```
administrator(config)#ptp profile 1588
administrator(config)#ptp 0 clock-type bc
administrator(config)#ptp 0 domain 1
administrator(config)#ptp 0 step one-step
administrator(config)#ptp 0 priority1 200
administrator(config)#ptp 0 enable
administrator(config)#ifconfig ethernet-port 4
administrator(port-4)#ptp 0 enable
```

[Device B] 配置步骤：

```
administrator(config)#ptp profile 1588
administrator(config)#ptp 0 clock-type bc
administrator(config)#ptp 0 domain 1
administrator(config)#ptp 0 step one-step
administrator(config)#ptp 0 priority1 127
administrator(config)#ptp 0 enable
administrator(config)#ifconfig ethernet-port 10
administrator(port-10)#ptp 0 enable
```

SwitchA 上查看 PTP 信息：

查看设备 ptp 默认属性：

```
administrator(config)#display ptp 0 default-ds
```

Default Parameter Data

PTP Instance ID: 0 PTP state: enabled

clock type: BC clock Identity:0000ea.fffe.34ebea

priority1: 200 priority2: 128

domain ID: 1 step mode: one-step

查看主时钟的属性：

administrator(config)#display ptp 0 parent-ds

Parent Parameter Data

PTP Instance ID: 0

GM.Identity:ec578e.fffe.592c4e

GM.Priority1: 127

GM.Priority2: 128

GM.clockClass: 248

GM.clockAccuracy: 35

GM.offsetScaledLogVar: 17258

查看与主时钟的 offset：

administrator(config)#display ptp 0 current-ds

Current Parameter Data

PTP Instance ID: 0

offset From Master: -39 Neighbor

RateRatio: 1.000000

查看端口的 ptp 配置与状态：

administrator(port-4)#display ptp 0 ethernet-port 4 port-ds

Port Parameter Data

PTP Instance ID: 0 PTP Port: 4

Port Enable: enabled Port State: slave

Sync Interval: 0 Announce Interval: 0

Pdelay interval: -3 Mean Link Delay: 2898

Ptp Vlan: 0 Delay Mechanism: P2P

查看端口 ptp 报文统计：

administrator(port-4)#display ptp 0 ethernet-port 4 counters

Port Parameter Statistics Data

SYNC : 770 / 35420 , 1380 / 91080

DELAY_REQ : 0 / 0 , 0 / 0

PDELAY_REQ : 240 / 12960 , 272 / 20672

PDELAY_RESP : 99 / 5346 , 99 / 7524

FOLLOW_UP : 0 / 0 , 0 / 0

DELAY_RESP : 0 / 0 , 0 / 0

PDELAY_RESP_FOLLOW_UP : 0 / 0 , 0 / 0

ANNOUNCE : 98 / 7448 , 175 / 17150

SIGNALING : 0 / 0 , 0 / 0

MANAGEMENT : 0 / 0 , 0 / 0

查看 PTP 当前时间：

administrator(config)#display ptp 0 time

Current PTP Time : 2021-12-31 18:56:48.553188227