交换机配置指南

本手册对应的软件版本为：Release 7.1.x

文档版本号：V1.08

发布时间：2024.03.25

1. 系统管理

1.1. CLI 命令行模式

设备 CLI 管理界面分成若干不同的模式，用户当前所处的命令模式决定了可以使用的命令。在命令提示符下输入问号键（?）可以列出每个命令模式支持使用的命令。当用户登录到设备上时，首先处于用户模式。

模式名称	提示符	切换模式	模式描述
用户模式	SWITCH>	配置 enable 切换到特权模式	支持设备信息显示、调试命令行等
特权模式	SWITCH#	配置 configure terminal 切换到全局模式；配置 diasble 切换到用户模式	支持网络测试； 支持功能模块信息查看； 支持配置保存、清空等操作
全局模式	SWITCH(config)#	配置 exit 切换到特权模式；配置 interface 切换到接口模式	支持基于全局的配置命令
接口模式	SWITCH(config-if)#	配置 exit 切换到全局模式；配置 end 切换到特权模式	支持接口模式下配置命令，接口包括物理接口、聚合口、SVI 口

1.2. 配置管理 IP

1.2.1. 配置命令

- 配置设备 Ipv4 管理 IP

命令	SWITCH(config)#**management vlan** VLANID **ip address** IPADDR/MASKLEN **gateway** IPADDR SWITCH(config)#**no management vlan**
描述	配置/删除设备 Ipv4 管理 IP

- 配置设备 Ipv4 管理 IP DHCP 动态获取

命令	SWITCH(config)#**management vlan** VLANID **ip address dhcp** SWITCH(config)#**no management vlan**
描述	配置/删除设备 Ipv4 管理 IP

- 配置设备 Ipv6 管理 IP

命令	SWITCH(config)#**management vlan** VLANID **ipv6 address** IPV6ADDR/MASKLEN **gateway** IPV6ADDR SWITCH(config)#**no management vlan**
描述	配置/删除设备 Ipv6 管理 IP

- 配置设备 Ipv6 管理 IP DHCP 动态获取

命令	SWITCH(config)#**management vlan** VLANID **ipv6 address dhcp** SWITCH(config)#**no management vlan**
描述	配置/删除设备 Ipv6 管理 IP

- 查看设备管理 IP 配置

命令	SWITCH#**show management summary**

描述	配置/删除设备 Ipv6 管理 IP

1.2.2. 配置案例

案例需求：管理 VLAN 为 1，管理 IP 为 192.168.64.200/24，网关地址为 192.168.64.1

进入全局模式：

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

配置 Ipv4 管理 IP：

```
SWITCH(config)#management vlan 1 ip address 192.168.64.200/24 gateway
192.168.64.1
```

查看管理 IP 配置信息：

```
SWITCH#show management summary
Management interface with Ipv4:
Type:        Static
Vlan:        1
Ip address:  192.168.64.200/24
Gateway:     192.168.64.1
```

1.3. 配置保存/清除操作

1.3.1. 配置命令

- 配置保存命令

命令	SWITCH#write
描述	保存配置

- 恢复默认配置命令

命令	SWITCH#**copy default-config startup-config** SWITCH#**reload**
描述	恢复系统默认配置，设备重启后生效

- 配置 TFTP 导入

命令	SWITCH#**copy tftp tftp://A.B.C.D/FILE startup-config** SWITCH#**reload**
描述	A.B.C.D：远程 tftp 服务器 ip 地址 FILE：远程服务器下的配置文件 通过 tftp 协议，将远程配置导入到设备中，替换现有配置 设备重启后生效

- 配置 TFTP 导出

命令	SWITCH#**copy startup-config tftp tftp://A.B.C.D/FILE**
描述	A.B.C.D：远程 tftp 服务器 ip 地址 FILE：远程服务器上新建的文件，保存 startup-config 内容

	通过 tftp 协议，配置保存到远程 tftp 服务器指定文件夹中

- 配置 FTP 导入

命令	SWITCH#**copy ftp ftp://A.B.C.D/FILE startup-config** SWITCH#**reload**
描述	A.B.C.D：远程 ftp 服务器 ip 地址 FILE：远程服务器下的配置文件 通过 ftp 协议，将远程配置导入到设备中，替换现有配置 设备重启后生效

- 配置 FTP 导出

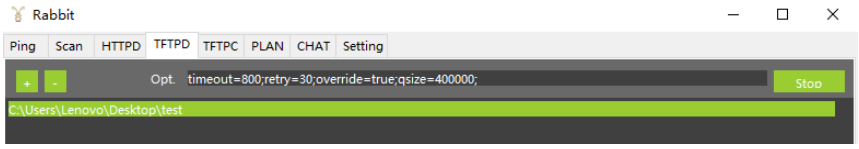
命令	SWITCH#**copy startup-config ftp ftp://A.B.C.D/FILE**
描述	A.B.C.D：远程 ftp 服务器 ip 地址 FILE：远程服务器上新建的文件，保存 startup-config 内容 通过 ftp 协议，配置保存到远程 ftp 服务器指定文件夹中

1.3.2. 配置案例

案例一：将配置导出到远程 tftp 服务器指定的文件夹下，文件名 startup.conf

环境搭建：

远程 PC 端开始 tftp 服务器，并选定 tftp 当前目录



远程 PC 的 ip 地址为 192.168.64.1，配置交换机管理 ip 为 192.168.64.100，可 ping 通远程 PC。

执行配置导出命令：

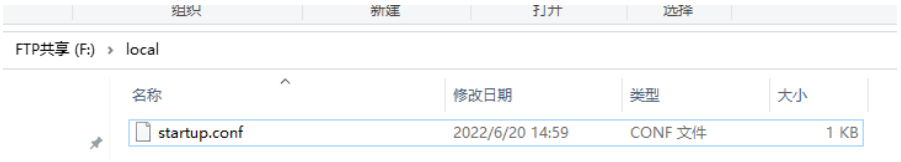
```
SWITCH#
SWITCH# copy startup-config tftp tftp://192.168.64.1/startup.conf
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1230    0     0  100  1230      0   151k --:--:-- --:--:-- --:--:--  240k
100  1230    0     0  100  1230      0   144k --:--:-- --:--:-- --:--:--  144k
Copy Success
```

在远程 PC 的 test 目录下，可查看新建的 startup.conf 文件。

案例二：将远程 ftp 服务器指定的文件夹下配置文件 startup.conf 导入到设备中

环境搭建：

远程 PC 端开始 ftp 服务器，并选定 ftp 当前目录，放置 startup.conf 文件



远程 PC 的 ip 地址为 192.168.64.1，配置交换机管理 ip 为 192.168.64.100，可 ping 通远程 PC

执行配置导入命令：

```
SWITCH#
```

```
SWITCH# #copy ftp ftp://192.168.64.1/startup.conf startup-config
Enter Username:xxxxxx
Enter Password:xxxxxx
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   973  100   973    0     0  42572      0 --:--:-- --:--:-- --:--:-- 48650
Copy Success
```

配置导入后，重启以生效。

1.4. Log 清除命令

- 清除系统 log

命令	SWITCH# **clear logging**
描述	清除系统 log

1.5. 设备热重启操作

- 配置热重启命令

命令	SWITCH#**reload**
描述	设备热重启

1.6. 用户管理

- 新增/删除用户、修改用户密码

命令	SWITCH(config)# **username** NAME **password** LINE SWITCH(config)# **no username** NAME
描述	若用户 NAME 不存在则新增用户，若存在则修改用户的密码； 设备出厂默认自带用户"admin"，密码"admin"，支持修改密码、删除操作； 用户、密码长度为 0-32 字节； 密码显示采用加密方式； 密码字符区分大小写； 删除操作不支持删除用户本身；删除在线用户，需先将该用户踢下线；

1.7. 登录管理

1.7.1. 配置命令

1.7.1.1. 服务使能管理

- 配置使能 WEB 管理

命令	SWITCH(config)# **web-server enable** {**all | http | https**} SWITCH(config)# **no web-server enable**
描述	配置使能 WEB 管理 默认 enable 状态

	支持 Ipv6

- 配置使能 Telnet 管理

命令	SWITCH(config)# **telnet-server enable** SWITCH(config)# **no telnet-server enable**
描述	配置使能 telnet 管理 默认 disable 状态 支持 Ipv6

- 配置使能 SSH 管理

命令	SWITCH(config)# **ssh-server enable** SWITCH(config)# **no ssh-server enable**
描述	配置使能 SSH 管理 默认 disable 状态 支持 Ipv6

1.7.1.2. ACL 应用在服务上

- Ipv4 ACL 应用在服务上

命令	SWITCH(config)# **ip** {**telnet** | **ssh** | **http** | **https**} **access-class** {<1-199> | <1300-2699> | ACLNAME} SWITCH(config)# **no ip** {**telnet** | **ssh** | **http** | **https**} **access-class**
描述	Ipv4 的 ACL 应用在 telnet、ssh、http、https 等服务上 满足 ACL permit 规则的用户允许访问设备，否则用户无法访问设备

- Ipv6 ACL 应用在服务上

命令	SWITCH(config)# **ipv6** {**telnet** | **ssh** | **http** | **https**} **access-class** { ACLNAME } SWITCH(config)# **no ipv6** {**telnet** | **ssh** | **http** | **https**} **access-class**
描述	Ipv6 的 ACL 应用在 telnet、ssh、http、https 等服务上 满足 ACL permit 规则的用户允许访问设备，否则用户无法访问设备

1.7.1.3. ACL 应用在 vty 上

- ACL 应用在 vty 上

命令	SWITCH(config-line)# **access-class** {<1-199> | <1300-2699> | ACLNAME } **in** SWITCH(config-line)# no **access-class** {<1-199> | <1300-2699> | ACLNAME } **in**
描述	ACL 应用在 vty 上 对 vty 上的 telnet、ssh 等服务器均生效

1.7.1.4. 基于 line 的服务管理

- 配置 line vty 上支持的服务

命令	SWITCH(config-line)# **transport input** {**telnet** | **ssh** | **all** | **none**} SWITCH(config-line)# no **transport input**

描述	配置 vty 上支持的服务 telnet：仅支持 telnet 服务 ssh：仅支持 ssh 服务 all：支持 telnet、ssh 服务 none：不支持所有服务 默认支持 telnet、ssh 服务

1.7.1.5. 其他命令

- 踢在线用户下线

命令	SWITCH# **clear line** {**vty	console**} LINE
描述	Vty 表示远程登录用户； Console 表示串口登录用户； LINE 信息可在 show users 命令中查看； 不支持踢用户本身；

- 显示在线用户命令

```
SWITCH#show users
Type        Line    User                    Idle        Host
con         0       admin                   00:00:03    --
vty         0       admin                   00:00:11    192.168.64.1
```

Users 显示要素如下：

字段	说明
Type	console 或 vty
Line	console：固定 0 vty：0-7
User	用户名
Idle	处于 idle 状态时间，超出 timeout 时间，终端自动退出
Host	登录用户 ip 地址

1.7.2. 配置案例

案例一：设备开启 telnet 服务，仅允许 ip 地址为 192.168.64.100 的用户，通过 telnet 访问设备，拒绝其他用户访问。

```
SWITCH(config)#telnet-server enable
SWITCH(config)#ip-access-list standard 1
SWITCH(config-std-acl)#permit host 192.168.64.100
SWITCH(config-std-acl)#exit
SWITCH(config)#ip telnet access-class 1
```

案例二：设备开启 telnet 服务，设备同一时间只允许一个用户通过 telnet 登录设备。

```
SWITCH(config)#telnet-server enable
SWITCH(config)#line vty 1 7
SWITCH(config-line)#transport input none
```

1.8. 配置系统名称

- 配置系统名称

命令	SWITCH(config)# **hostname** WORD

描述	设置系统名称，名称必须由可打印字符组成，长度不能超过63 个字节； 配置即时生效

1.9. 配置系统升级

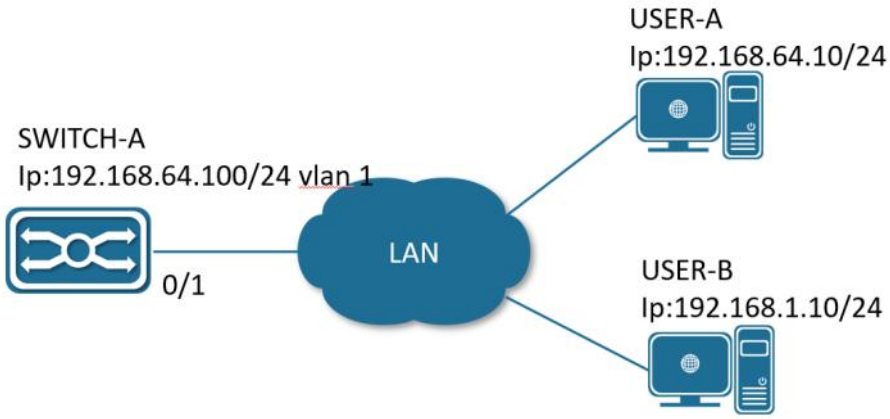
- 配置系统升级

命令	SWITCH# **upgrade firmware tftp://**SERVER**/**FILENAME
描述	固件升级命令，需要在终端搭建TFTP服务器，并确保终端与设备网络双向互连。 SERVER:TFTP服务器IP以及服务器窗口与固件升级文件的相对地址。 FILENAME：固件升级文件。 固件升级过程将耗时5-6分钟，重启设备以完成固件升级。 升级过程中设备请勿下电。

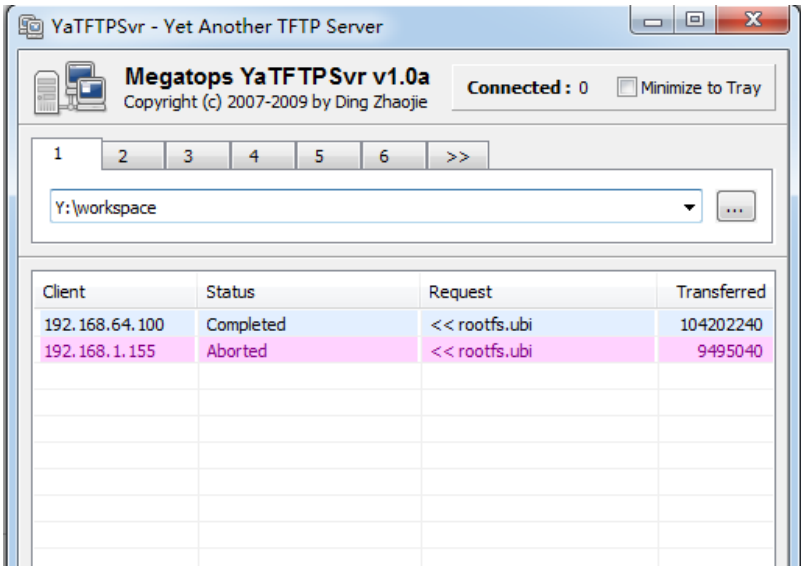
配置案例：

案例需求：远程 telnet 完成对固件的升级操作

1 如下图，SWITCH-A 为待升级设备，打开 telnet 功能；USER-A 为局域网内同网段主机，USER-B 为局域网内管理设备，二者均可 telent 登录 SWITCH-A。



2 选择 USER-B 进行版本升级操作。在 USER-B 上打开 TFTP 服务器，并将升级文件 xcat-release-3.2.0.bin 放在 Y:/workspace 目录下。



3 USER-B telnet 登录 SWITCH-A，在特权模式下执行升级命令。

```
SWITCH#upgrade firmware tftp://192.168.64.1/lite-release-6.2.0.bin
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 82.1M    0 82.1M    0     0  1091k      0 --:--:--  0:01:17 --:--:-- 1093k
100 82.1M    0 82.1M    0     0  1091k      0 --:--:--  0:01:17 --:--:-- 1091k
Un-packet install file, this will last about 60 seconds.
Read configure from config file.
Validation.
Check upgrade file success.
Start erase and write bin to flash, this will last about 120 seconds.
Erasing 128 Kibyte @ d7e0000 -- 100 % complete
Reboot system to finish upgrade? (y/n): 
```

4 升级命令执行结束，选择”y”重启设备，完成升级，选择“n”设备继续运行，升级操作在下次设备重启后完成。

1.10. 配置系统时间

- 手动配置系统时间

命令	SWITCH# **clock set** HH:MM:SS DAY MON YEAR
描述	设置系统时间 例如配置 2017 年 10 月 1 日 15 时 30 分 0 秒： Clock set 15:30:00 1 october 2017

- 配置 ntp 服务器

命令	SWITCH(config)# **ntp server {**A.B.C.D | **ipv6** X.X::X.X }
描述	配置 NTP 服务器的 IP 地址(不支持域名配置)。配置完成后，若设备与服务器保持网络连通，设备将自动从服务器同步时间信息，第一次完成时间同步大概耗时 4-8 分钟。

- 配置系统时区

命令	SWITCH(config)# **clock timezone** ZONE
描述	配置系统时区，默认为世界标准时间 UTC，支持标准的时区配置，如上海时区关键字“Shanghai”，香港时区关键字” Hong_Kong”等。

- 查看系统时间

命令	SWITCH# **show clock**
描述	查看系统时间

2. 配置接口

2.1. 接口类型概述

交换设备的接口，根据业务层面，可分为以下两大类：二层接口与三层接口。

二层接口(L2 interface)，这里包括普通物理口(Switch Port)以及聚合口(Port Channel)。

Switch Port 由设备上的单个物理端口构成，只有二层交换功能。该端口可以是一个 Access Port、Hybrid Port 或一个 Trunk Port，您可以通过 Switch Port 接口配置命令，把一个端口配置为一个 Access Port、Hybrid Port 或者 Trunk Port。

Port Channel 简称 PO，是由多个物理成员端口聚合而成的。我们可以把多个物理链接捆绑在一起形成一个简单的逻辑链接，这个逻辑链接我们称之为一个聚合口。对于二层交换来说聚合口就好像一个高带宽的 Switch port，它可以把多个端口的带宽叠加起来使用，扩展了链路带宽。

三层接口(L3 interface)，这里主要指 SVI(Switch virtual interface)口。

SVI 是交换虚拟接口，用来实现三层交换的逻辑 9 接口。SVI 可以做为本机的管理接口，通过管理接口管理员可管理设备。您可通过 interface vlan 接口配置命令来创建 SVI，然后给 SVI 分配 IP 地址来建立 VLAN 之间的路由。

2.2. 配置命令

- 配置端口 range

命令	SWITCH(config)# **interface** IFNAME_RANGE
描述	IFNAME_RANGE 格式如 gigabitEthernet 0/1-4, gigabitEthernet 0/9-12； 当存在多个 range 组合时，中间用‘,’隔离，不带空格； 最多支持 5 个 range 组合； 当中间某端口配置失败时，配置返回，不再继续后续端口配置

- 配置端口描述符

命令	SWITCH(config-if)# **description** DESC
描述	配置接口描述符，最多 80 个字符

- 配置端口使能

命令	SWITCH(config-if)# **shutdown** SWITCH(config-if)# **no shutdown**
描述	关闭端口或使能端口，默认使能； 仅支持物理口上配置

- 配置端口速率

命令	SWITCH(config-if)# **speed** {**10 | 100 | 1000 | auto**} SWITCH(config-if)# **no speed**
描述	配置端口速率，当配置成 auto 或 no speed 时，端口速率进入自协商模式； 默认端口速率自协商； 不支持在聚合成员口上配置； 不支持在 SVI 口上配置

- 配置端口双工

命令	SWITCH(config-if)# **duplex** {**auto	full	half**} SWITCH(config-if)# **no duplex**
描述	配置端口双工，当配置成 auto 或 no duplex 时，端口双工进入自协商模式； 默认端口双工自协商； 不支持在聚合成员口上配置； 不支持在 SVI 口上配置

说明

✦当速率与双工均退出自协商模式时，端口自协商关闭

- 配置端口流控

当本端交换机和对端交换机都开启了流量控制功能后，如果本端交换机发生拥塞：
本端交换机将向对端交换机发送消息，通知对端交换机暂时停止发送报文或减慢发送报文的速度。
对端交换机在接收到该消息后，将暂停向本端发送报文或减慢发送报文的速度，从而避免了报文丢失现象的发生，保证了网络业务的正常运行。

命令	SWITCH(config-if)# **flowcontrol** {**on	off** }
描述	配置端口流控，默认端口流控自协商； 不支持在聚合成员口上配置； 不支持在 SVI 口上配置

- 配置端口 MTU

当端口进行大吞吐量数据交换时，可能会遇到大于以太网标准帧长度的帧，这种帧被称为 jumbo 帧。用户可以通过设置端口的 MTU 来控制该端口允许收发的最大帧长。 MTU 是指帧中有效数据段的长度，不包括以太网封装的开销。 端口收到或者转发的帧，如果长度超过设置的 MTU，将被丢弃。
因芯片限制，MTU 值仅支持偶数，若用户配置为奇数，设备将自动对齐，如配置 MTU 为 127,实际支持 128 长度报文通过。

命令	SWITCH(config-if)# **mtu** LENGTH SWITCH(config-if)# **no mtu**
描述	配置端口 MTU，允许设置的范围为 46~10222 字节，缺省为 1500 字节 不支持在聚合成员口上配置； 不支持在 SVI 口上配置

- 配置 SFP 端口模式

默认情况下，SFP 端口处于 1000BASE-X 模式下，可以支持遵循 1000BASE-X 的 SFP 模块。有些光模块（某些 1000BASE-T SFP 模块和某些 100BASE-FX SFP 模块）采用的是 SGMII 协议，可以将端口切换为 SGMII 模式以提供支持。可通过配置端口模式 2500BASE-X 提升端口带宽到 2.5G，但仅支持我司提供的特定型号 SFP 模块。

命令	SWITCH(config-if)# **port mode** {**sgmii	2500BASE-X	1000BASE-X}** SWITCH(config-if)# **no port mode**
描述	默认处于 1000BASE-X 模式； Sgmii: 配置 SFP 端口模式为 SGMII 模式； 2500BASE-X：配置端口 2500BASE-X 模式，支持 2.5G 带宽；

	仅支持在物理口上配置

- 配置接口介质类型

如果同一端口可以选择光口和电口两种介质类型，您只能使用其中之一。一旦确定介质类型之后，再配置端口的属性，例如双工、流控和速率等，都是指端口当前选择类型的属性。

命令	SWITCH(config-if)# **medium {copper | fiber | auto prefer {copper | fiber}}** SWITCH(config-if)# **no medium**
描述	配置接口介质类型 默认为 auto 模式，prefer copper Copper：表示选择光口 Fiber：表示选择电口 Auto：表示自适应端口媒介类型，根据接入媒介确定是光口还是电口 Auto prefer copper：自适应媒介类型，当光、电均接入时，优先选择电口 Auto prefer fiber：自适应媒介类型，当光、电均接入时，优先选择光口 No 操作恢复默认电口介质类型

- 配置端口隔离

部分应用环境下，要求设备部分端口间不能互相通讯，可以通过将这些端口设置为隔离口实现。当端口设为隔离口之后，隔离口之间互相无法通讯，隔离口与非隔离口之间可以正常通讯，非隔离口与非隔离口之间可以正常通讯。

命令	SWITCH(config-if)#**switchport isolate** SWITCH(config-if)# **no switchport isolate**
描述	默认端口为非隔离口； 当前不支持在聚合口、vlan 口上配置隔离功能

- 显示端口光/铜缆模块信息

该命令用于显示光口上插入的的光/铜缆模块的信息。

命令	SWITCH#show interface [interface-id] optical-transceiver [info]
描述	不指定 interface-id 则显示所有端口的模块信息 不指定 info 则显示端口模块的 DDM 信息,指定则显示完整模块信息（基本信息，告警信息，厂商信息）

- 配置端口自协商

命令	SWITCH(config-if)# autoneg on SWITCH(config-if)# no autoneg
描述	配置端口自协商开启、关闭 只适用于 1000M 的光口 默认开启 其他端口上配置该命令，提示失败 Show interface brief 可查看 link 端口的自协商状态

2.3. 配置案例

- 进入 gigabitEthernet0/1 口接口配置模式：

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#
```

- 配置端口描述信息为"TEST_A"

```
SWITCH(config-if)#description TEST_A
```

- 打开端口使能

```
SWITCH(config-if)#no shutdown
```

- 强制端口速率 100M，全双工，打开流控功能

```
SWITCH(config-if)#speed 100
SWITCH(config-if)#duplex full
SWITCH(config-if)#flowcontrol on
```

- 配置端口 MTU 值 1024

```
SWITCH(config-if)#mtu 1024
```

2.4. 显示命令

- 显示所有端口简要信息

```
SWITCH#show interface brief

--------------------------------------------------------------------------------
Ethernet   Type  Status  Reason  Speed  Duplex  Flowcontrol  Autoneg  Port
Interface                                                              Ch #
--------------------------------------------------------------------------------
GiE0/1     ETH   down    none    --     --      --           --       --
GiE0/2     ETH   up      none    1000M  FULL    OFF          ON       --
GiE0/3     ETH   down    none    --     --      --           --       --
GiE0/4     ETH   down    none    --     --      --           --       --
GiE0/5     ETH   down    none    --     --      --           --       --
GiE0/6     ETH   down    none    --     --      --           --       --
GiE0/7     ETH   down    none    --     --      --           --       --
GiE0/8     ETH   up      none    100M   FULL    OFF          ON       --
GiE0/9     ETH   down    none    --     --      --           --       --
GiE0/10    ETH   down    none    --     --      --           --       --
GiE0/11    ETH   down    none    --     --      --           --       --
GiE0/12    ETH   down    none    --     --      --           --       --
```

- 显示单端口配置以及状态信息:

```
 SWITCH#show interface gigabitethernet0/1
Interface gigabitethernet0/1
  Hardware is eth  current hw addr: 0050.4c82.89a0
  Physical:0050.4c82.89a0
  Description: test_a
  Index 1 metric 0 mtu 1024 speed-unknown duplex-unknown flowcontrol-unknown
  Port mode is invalid
  <up>
    vrf binding: not bound
  Bandwidth -8
  Input packets 0677, bytes 072690,
  Multicast packets 0327 broadcast packets 0350 fcs error 00 undersizeerrors 00
oversizeerrors 00
```

```
Output packets 00, bytes 00,
Multicast packets 00 broadcast packets 00
```

- 显示端口报文统计信息

```
SWITCH#show interface gigabitEthernet0/1 counters
Interface gigabitEthernet16/1
Good Octets Tx          : 1914949
Good Octets Rx          : 0
Bad Octets Rx           : 0
Mac Tx Err Pkts         : 0
Good Packets Tx         : 1913
Good Packets Rx         : 0
Bad Packets Rx          : 0
Broadcast Packet Tx     : 24
Broadcast Packets Rx    : 0
Multicast Packet Tx     : 55
Multicast Packets Rx    : 0
pkts_64_octets          : 285
pkts_65_127_octets      : 263
pkts_128_255_octets     : 42
pkts_256_511_octets     : 36
pkts_512_1023_octets    : 91
pkts_1024_max_octets    : 1196
Excessive Collisions    : 0
UnRecg MAC Cntl Pkts Rx : 0
Flow Ctrl Pkts Sent     : 0
Flow Ctrl Pkts Recvd    : 0
Drop Events             : 0
Undersized Pkts Recvd   : 0
Fragments Recvd         : 0
Oversized Pkts Recvd    : 0
Jabber Pkts Recvd       : 0
mac_rcv_error           : 0
Bad CRC                 : 0
Collisions              : 0
Late Collisions         : 0
Bad Flow Ctrl Recv      : 0
```

- 显示端口隔离配置信息:

```
SWITCH#show switchport isolate
interface      config
GiE0/1          isolated
GiE0/2          normal
GiE0/3          normal
GiE0/4          normal
GiE0/5          normal
GiE0/6          normal
GiE0/7          normal
GiE0/8          normal
GiE0/9          normal
GiE0/10         normal
```

- 显示端口光模块/铜缆模块 DDM 信息:

DDM 信息显示要素如下:

字段	说明
Temp	模块当前的工作温度, 单位为℃，精确到 1°C。
Voltage	模块当前的工作电压，单位为 V，精确到 0.01V。
Bias	模块当前的工作电流，单位为 mA，精确到 0.01mA。
RX power	模块当前的接收光功率，单位为 dBm，精确到 0.01dBM。
TX power	模块当前的发送光功率，单位为 dBm，精确到 0.01dBM。
OK	正常，无需干预
WARN	告警，表示超过设备允许范围，需要注意。
ALARM	异常，表示严重超过设备允许状态，需要立即干预。
ABSENT	不在位
NA	端口不支持/模块不支持
TIMEOUT	超时
ERR	错误

显示单个端口模块 DDM 信息

```
SWITCH#show interface gigabitEthernet0/9 optical-transceiver
  Port     Temp       Voltage       Bias         RX power      TX power
           [C]          [V]         [mA]          [dBm]         [dBm]
------- ---------- ------------- ------------- ------------- -------------
GiE0/9   40(OK)      3.20(OK)     32.34(OK)     -3.98(OK)      1.70(OK)
```

显示所有端口模块 DDM 信息

```
SWITCH#show interface optical-transceiver
  Port     Temp       Voltage       Bias         RX power      TX power
           [C]          [V]         [mA]          [dBm]         [dBm]
------- ---------- ------------- ------------- ------------- -------------
GiE0/9   42(OK)      3.20(OK)     32.34(OK)     -3.98(OK)      1.64(OK)
GiE0/10  ABSENT      ABSENT       ABSENT        ABSENT         ABSENT
GiE0/11  ABSENT      ABSENT       ABSENT        ABSENT         ABSENT
GiE0/12  ABSENT      ABSENT       ABSENT        ABSENT         ABSENT
SWITCH#
```

- 显示端口光模块/铜缆模块总体信息：

模块总体信息显示要素如下：

操作错误信息

字段	说明
Transceiver absent!	获取信息失败，可能模块不在位
Get transceiver info timeout!	获取信息超时，需要重新获取
Port doesn't support get module info!	端口不支持获取模块信息

基本信息

字段	说明
Transceiver Type	模块类型
Connector Type	接口类型
Wavelength(nm)	波长
Link Length	支持的链路长度
Digital Diagnostic Monitoring	是否支持 DDM 功能
Vendor Serial Number	模块序列号

告警信息

字段	说明

RX Channel loss of signal	接收信号丢失
RX Channel power high	接收光功率高告警
RX Channel power low	接收光功率低告警
TX Channel fault	发送错误
TX Channel bias high	偏置电流高告警
TX Channel bias low	偏置电流低告警
TX Channel power high	发送光功率高告警
TX Channel power low	发送光功率低告警
Temperature high	温度高告警
Temperature low	温度低告警
Voltage high	电压高告警
Voltage low	电压低告警
None	无告警
This module doesn't support getting alarm!	模块不支持获取告警信息

厂商信息

字段	说明
Vendor Name	厂商名称
Vendor OUI	厂商 OUI
Vendor Part Number	厂商部件号
Vendor Revision	厂商版本号
Manufacturing Date	生产日期
Encoding	编码类型

显示单个端口模块总体信息

```
SWITCH#show interface gigabitEthernet0/9 optical-transceiver info
############################################################
                gigabitEthernet0/9
+-------------------------------------------------+
|Transceiver base information:                    |
+-------------------------------------------------+
|Transceiver Type    :  1000BASE-ZX-SFP           |
|Connector Type      :  LC                        |
|Wavelength(nm)      :  1550                      |
|Link Length     :                                |
|    SMF fiber                                    |
|        -- 80km                                  |
|Digital Diagnostic Monitoring  : YES             |
|Vendor Serial Number           : WT1703230031    |
+-------------------------------------------------+
|Transceiver current alarm information:           |
+-------------------------------------------------+
|None                                             |
+-------------------------------------------------+
|Transceiver vendor information:                  |
+-------------------------------------------------+
|Vendor Name         : OEM                        |
|Vendor OUI          : 000000                     |
|Vendor Part Number  : SFP-GE-ZX-SM1550           |
|Vendor Revision     : V2                         |
|Manufacturing Date  : 2017-03-25                 |
```

```
|Encoding           : 8B10B                    |
+----------------------------------------------+
SWITCH#
```

显示所有端口块总体信息

```
SWITCH#show interface optical-transceiver info
#######################################################
                gigabitEthernet0/9
+----------------------------------------------+
|Transceiver base information:                 |
+----------------------------------------------+
|Transceiver Type    :  1000BASE-ZX-SFP        |
|Connector Type      :  LC                     |
|Wavelength(nm)      :  1550                   |
|Link Length     :                             |
|    SMF fiber                                 |
|        -- 80km                               |
|Digital Diagnostic Monitoring  : YES          |
|Vendor Serial Number          : WT1703230031  |
+----------------------------------------------+
|Transceiver current alarm information:        |
+----------------------------------------------+
|None                                          |
+----------------------------------------------+
|Transceiver vendor information:               |
+----------------------------------------------+
|Vendor Name         : OEM                     |
|Vendor OUI          : 000000                  |
|Vendor Part Number  : SFP-GE-ZX-SM1550        |
|Vendor Revision     : V2                      |
|Manufacturing Date  : 2017-03-25              |
|Encoding           : 8B10B                    |
+----------------------------------------------+
#######################################################
                gigabitEthernet0/10
+----------------------------------------------+
|Transceiver base information:                 |
+----------------------------------------------+
|Transceiver Type    :  1000BASE-GT-SFP        |
|Connector Type      :  Unknown or unspecified |
|Wavelength(nm)      :  16652                  |
|Link Length     :                             |
|    Cable Assembly copper                     |
|        -- 100m                               |
|Digital Diagnostic Monitoring  : NO           |
|Vendor Serial Number          : MTC100046     |
+----------------------------------------------+
|Transceiver current alarm information:        |
+----------------------------------------------+
This module doesn't support getting alarm!
|This module doesn't support getting alarm!    |
+----------------------------------------------+
|Transceiver vendor information:               |
+----------------------------------------------+
|Vendor Name         : OEM                     |
```

```
|Vendor OUI          : 000000                    |
|Vendor Part Number  : SFP-T-CBTX                |
|Vendor Revision     : F                         |
|Manufacturing Date  : 2014-10-01                |
|Encoding            : 8B10B                     |
+-----------------------------------------------+
##########################################################
                gigabitEthernet0/11
Get result error(Maybe Transceiver absent)!
##########################################################
                gigabitEthernet0/12
Get result error(Maybe Transceiver absent)!
SWITCH#
```

3. 配置风暴控制

3.1. 风暴控制概述

当 LAN 中存在过量的广播、多播或未知单播数据流时，将导致网络性能下降，甚至网络瘫痪的现象，称为广播风暴。风暴控制针对广播、多播和未知单播数据流进行限速，当交换机端口接收到的广播、未知名多播或未知单播数据流的速率超过所设定的带宽时，设备将只允许通过所设定带宽的数据流，超出带宽部分的数据流将被丢弃，从而避免过量的泛洪数据流进入 LAN 中形成风暴。

3.2. 配置命令

- 配置接口风暴控制策略

命令	SWITCH(config-if)#**storm-control** {**broadcast | multicast | unicast | all | unicast-broadcast | multicast-broadcast**} **level** LINE SWITCH(config-if)#**no storm-control**
描述	配置/删除端口风暴控制策略; 支持在 broadcast/multicast/unicast/all/unicast-broadcast/ multicast-broadcast 中选择配置，选择配置无法共存; 其中 multicast 表示未知名多播报文，unicast 表示未知名单播报文; level 数值为端口带宽百分比，支持自适应端口速率变动

3.3. 配置案例

案例一：配置端口 gigabitEthernet0/1 未知名多播限速为 10%总带宽。

- 进入 gigabitEthernet0/1 口接口配置模式：

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#
```

- 配置接口未知名组播限速策略：

```
SWITCH(config-if)#storm-control multicast level 10
```

3.4. 显示命令

- 显示所有端口风暴控制配置

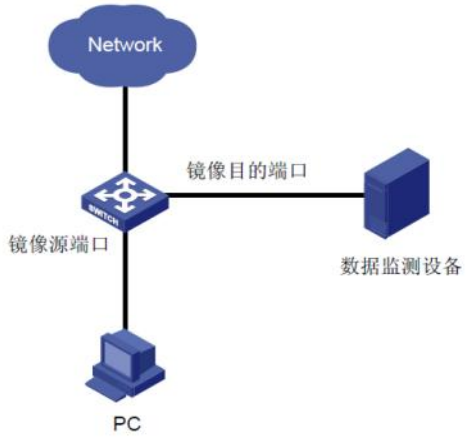
```
SWITCH#show storm-control
Port        BcastLevel     McastLevel     Unicastlevel
GiE0/1      100.00%         10.00%        100.00%
GiE0/2      100.00%        100.00%        100.00%
GiE0/3      100.00%        100.00%        100.00%
GiE0/4      100.00%        100.00%        100.00%
GiE0/5      100.00%        100.00%        100.00%
GiE0/6      100.00%        100.00%        100.00%
GiE0/7      100.00%        100.00%        100.00%
GiE0/8      100.00%        100.00%        100.00%
GiE0/9      100.00%        100.00%        100.00%
GiE0/10     100.00%        100.00%        100.00%
GiE0/11     100.00%        100.00%        100.00%
```

	GiE0/12	100.00%	100.00%	100.00%

4. 配置 SPAN

4.1. SPAN 概述

SPAN（Local Switched Port Analyzer）为本地镜像功能。SPAN 功能将指定端口的报文复制到目的端口，一般 SPAN 目的端口会接入数据检测设，用户利用这些设备分析目的端口接收到的报文，进行网络监控和故障排除。



SPAN 并不影响源端口和目的端口的报文交换，只是将源端口所有进入和输出的报文原样复制了一份到目的端口。当源端口的镜像流量超过目的端口带宽的情况下，例如 100Mbps 目的端口监控 1000Mbps 源端口的流量，可能导致报文被丢弃。

SPAN 基于会话管理，在会话中配置 SPAN 的源端口与目的端口。在一个会话中，只能有一个目的端口，但是可以同时配置多个源端口。

4.2. 配置命令

- 创建会话

命令	SWITCH(config)#**monitor session** SESSION-ID SWITCH(config)#**no monitor session** SESSION-ID
描述	创建/删除会话，创建会话同时进入会话模式； 支持会话数 7 个

- 配置会话描述符

命令	SWITCH(config-monitor)#**description** DESC
描述	配置会话描述符

- 配置源端口

命令	SWITCH(config-monitor)#**source interface** IFNAME {**both	rx	tx**} SWITCH(config-monitor)#**no source interface** IFNAME {**both	rx	tx**}
描述	创建/删除 SPAN 源端口

- 配置目的端口

命令	SWITCH(config-monitor)#**destination interface** IFNAME SWITCH(config-monitor)#**no destination interface** IFNAME
描述	创建/删除 SPAN 目的端口

4.3. 配置案例

案例一：利用端口 gigabitEthernet0/8 监控 gigabitEthernet0/1 口的入口报文以及 gigabitEthernet0/2 的出/入口报文，监控会话名称定义为”TRAFFIC_MONITOR”。

- 进入全局模式，建立会话：

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#monitor session 1
SWITCH(config-monitor)#
```

- 配置会话描述信息为”TRAFFIC_MONITOR”

```
SWITCH(config-monitor)#description TRAFFIC_MONITOR
```

- 配置会话源端口

```
SWITCH(config-monitor)#source interface gigabitEthernet0/1 rx
SWITCH(config-monitor)#source interface gigabitEthernet0/2 both
```

- 配置会话目的端口

```
SWITCH(config-monitor)#destination interface gigabitEthernet0/8
```

4.4. 显示命令

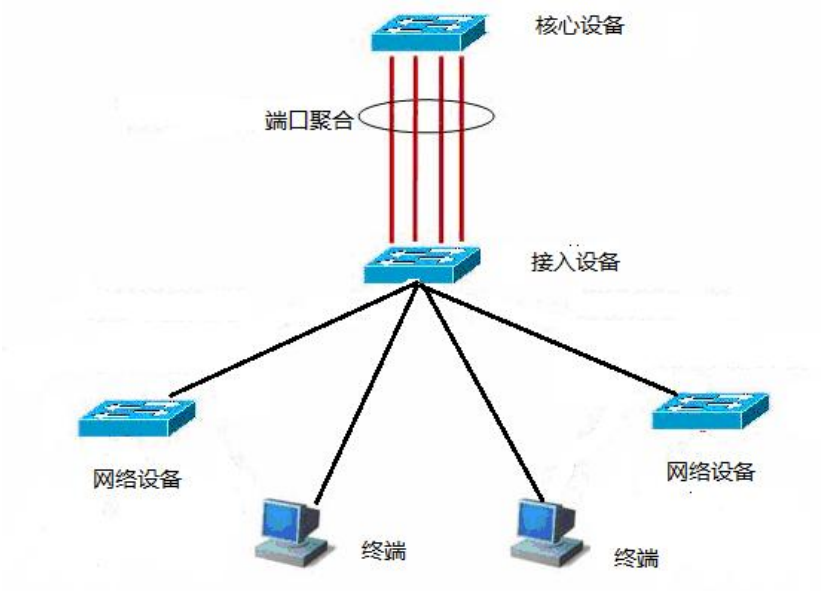
- 显示具体会话

```
SWITCH#show  monitor session 1
session 1
---------------
description       : TRAFFIC_MONITOR
type              : local
source intf       :
    tx            : gigabitEthernet0/2
    rx            : gigabitEthernet0/1  gigabitEthernet0/2
    both          : gigabitEthernet0/2
source VLANs      :
    rx            :
destination ports : gigabitEthernet0/8
Legend: f = forwarding enabled, l = learning enabled
```

5. 配置端口聚合

5.1. 聚合口概述

将多个物理链接捆绑在一起建立一个逻辑链接，这个逻辑链接我们称之为聚合口（port-channel，后者 PO 口），该功能称为端口聚合功能。聚合口功能符合 IEEE802.3ad 标准， 它可以用于扩展链路带宽，提供更高的连接可靠性，常用于端口上联，如下图所示。

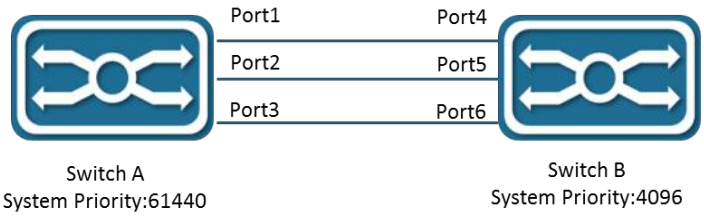


聚合口具备以下几个特性：高带宽，聚合口总带宽为物理成员口带宽总和；支持流量均衡策略，可以根据策略把流量地分配给各成员链路；支持链路备份，当聚合口中的一条成员链路断开时，系统会将该成员链路的流量自动地分配到聚合口中的其它有效成员链路上。

5.2. LACP 概述

基于 IEEE802.3ad 标准的 LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是一种实现链路动态汇聚的协议。如果端口启用 LACP 协议，端口会发送 LACPDU 来通告自己的系统优先级、系统 MAC、端口的优先级、端口号和操作 key 等。相连设备收到对端的 LACP 报文后，根据报文中的系统 ID 比较两端的系统优先级。在系统 ID 优先级较高的一端，将按照端口 ID 优先级从高到低的顺序，设置聚合组内端口处于聚合状态，并发出更新后的 LACP 报文，对端设备收到报文后，也会把相应的端口设置成聚合状态，从而使双方在端口退出或者加入聚合组上达到一致。只有双方的端口都完成动态聚合绑定操作后，该物理链路才能进行数据报文的转发。

LACP 成员口链路绑定之后，还会进行周期性的 LACP 报文交互，在一段时间没有收到 LACP 报文时，就认为收包超时，成员口链路解除绑定，端口重新处于不可转发状态。这里的超时时间有两种模式:长超时模式和短超时模式.在长超时模式下，端口间隔 30 秒发送一个报文，若 90 秒没有收到对端报文，就处于收包超时；在短超时模式下，端口间隔 1 秒发送一个报文，若 3 秒钟没有收到对端报文，就处于收包超时。



如上图所示，交换机 A 和交换机 B 通过 3 个端口连接在一起。设置交换机 A 的系统优先级为 61440，设置交换机 B 的系统优先级为 4096。在交换机 A 和 B 的 3 个直连端口上打开 LACP 链路聚合，设置 3 个端口的聚合模式为主动模式，设置 3 个端口的端口优先级为默认优先级 32768。

在收到对端的 LACP 报文后，交换机 B 发现自己的系统 ID 优先级比较高(交换机 B 的系统优先级比交换机 A 高)，于是按照端口 ID 优先级的顺序(端口优先级相同的情况下，按照端口号从小到大的顺序)设置端口 4、5、6 处于聚合状态。交换机 A 收到交换机 B 更新后的 LACP 报文后，发现对端的系统 ID 优先级比较高，并且把端口设置成聚合状态了，也把端口 1、2、3 设置成聚合状态了。

5.3. 配置命令

- 端口加入/退出聚合口

命令	加入静态聚合口: SWITCH(config-if)#**channel-group** ID **mode manual** 加入动态聚合(LACP): SWITCH(config-if)#**channel-group** ID **mode** {**active** | **passive**} 退出聚合口: SWITCH(config-if)#**no channel-group**
描述	支持 12 个聚合口<1-12>; 一个聚合口要么是静态的，要么是动态的，由加入的第一个成员口加入方式来决定。 Active 聚合模式表示该端口会主动发起 LACP 聚合运算；Passive 聚合模式表示该端口不会主动发起 LACP 聚合运算，但是在接收到邻居的 LACP 报文后会被动参与 LACP 计算。

说明

✦当聚合口（PO 口）未创建，第一个端口加入聚合口时，主动创建 PO 口，且该 PO 口的默认属性为该端口属性;

✦端口加入聚合口，要求与聚合口的以下基本属性相同:

端口的 VLAN 属性配置;

端口隔离配置。

- 配置 LACP 系统优先级

命令	SWITCH(config)#**lacp system-priority** SYSTEM-PRIORITY SWITCH(config)#**no lacp system-priority**
描述	系统优先级范围为<1-65535>，默认为 32768。 一台设备的所有的动态链路组只能有一个 LACP 系统优先级，修改这个值会影响到交换机上的所有聚合组。

- 配置 LACP 端口优先级

命令	SWITCH(config-if)#**lacp port-priority** PORT-PRIORITY

	SWITCH(config-if)#**no lacp port-priority**
描述	端口优先级在接口模式下配置，只支持物理端口配置。 端口优先级范围为<1-65535>，默认为 32768。

- 配置 LACP 超时模式

命令	SWITCH(config-if)#**lacp timeout {long | short}** SWITCH(config-if)#**no lacp timeout**
描述	端口优先级在接口模式下配置，只支持物理端口配置。 默认为 long 模式，LACP 协议报文发送间隔 30S，90S 超时；short 模式，LACP 协议报文发送间隔 1S，3S 超时。

- 配置负载均衡模式

命令	SWITCH(config)#**port-channel load-balance** {**dst-ip | dst-mac | dst-port | src-dst-ip | src-dst-mac | src-dst-port | src-ip | src-mac | src-port**} SWITCH(config)#**no port-channel load-balance**
描述	配置负载均衡模式，默认为 src-dst-mac

5.4. 配置案例

案例需求：配置 gigabitEthernet0/5、gigabitEthernet0/6 口加入 po1；配置负载均衡模式为 src-ip。

- 在接口上配置加入聚合口：

```
SWITCH(config)#interface gigabitEthernet0/5
SWITCH(config-if)#channel-group 1 mode manual
SWITCH(config-if)#exit
SWITCH(config)#interface gigabitEthernet0/6
SWITCH(config-if)#channel-group 1 mode manual
SWITCH(config-if)#exit
SWITCH(config)#port-channel load-balance src-ip
```

5.5. 显示命令

- 显示聚合端口配置及状态信息

```
SWITCH#show port-channel
Load balance: Source and Destination Mac address

Interface po3
  Type: static
  Member:
    gigabitEthernet0/18     link down     Disable

Interface po8
  Type: LACP
  Member:
    gigabitEthernet0/19     link up       Enable
    gigabitEthernet0/17     link up       Enable

SWITCH#show port-channel 8
Interface po8
```

```
  Type: LACP
  Member:
    gigabitEthernet0/19     link up       Enable
    gigabitEthernet0/17     link up       Enable

SWITCH#show port-channel load-balance
Source and Destination Mac address
```

- 显示 LACP 信息

```
SWITCH#show lacp summary
% Aggregator po8 1008
% Aggregator Type: Layer2
% Admin Key: 0008 - Oper Key 0008
%   Link: gigabitEthernet0/17 (17) sync: 1 status: Bundled
%   Link: gigabitEthernet0/19 (19) sync: 1 status: Bundled

SWITCH#show lacp detail
% Aggregator po8 1008
% Aggregator Type: Layer2
%  Mac address: 74:b9:eb:ee:25:46
%  Admin Key: 0008 - Oper Key 0008
%  Actor LAG ID- 0x8000,74-b9-eb-ee-25-46,0x0008
%  Receive link count: 2 - Transmit link count: 2
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x8000,00-01-a0-00-10-10,0x0032
%   Link: gigabitEthernet0/17 (17) sync: 1 status: Bundled
%   Link: gigabitEthernet0/19 (19) sync: 1 status: Bundled

SWITCH#show lacp 8
% Aggregator po8 1008 Admin Key: 0008 - Oper Key 0008
% Partner LAG ID: 0x8000,00-01-a0-00-10-10,0x0032
% Partner Oper Key 0050

SWITCH#show lacp sys-id
% System 8000,74-b9-eb-ee-25-46

SWITCH#show lacp port gigabitEthernet0/19
% LACP link info: gigabitEthernet0/19 - 19
% LAG ID: 0x8000,74-b9-eb-ee-25-46,0x0008
% Partner oper LAG ID: 0x8000,00-01-a0-00-10-10,0x0032
% Actor Port priority: 0x8000 (32768)
% Admin key: 0x0008 (8) Oper key: 0x0008 (8)
% Physical admin key:(1)
% Receive machine state : Current
% Periodic Transmission machine state : Slow periodic
% Mux machine state : Collecting/Distributing
% Oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Partner oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Partner link info: admin port 0
% Partner oper port: 20
% Partner admin LAG ID: 0x0000-00:00:00:00:0000
% Admin state: ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner admin state: ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner system priority - admin:0x0000 - oper:0x8000
```

```
        % Partner port priority - admin:0x0000 - oper:0x8000
        % Aggregator ID: 1008
```

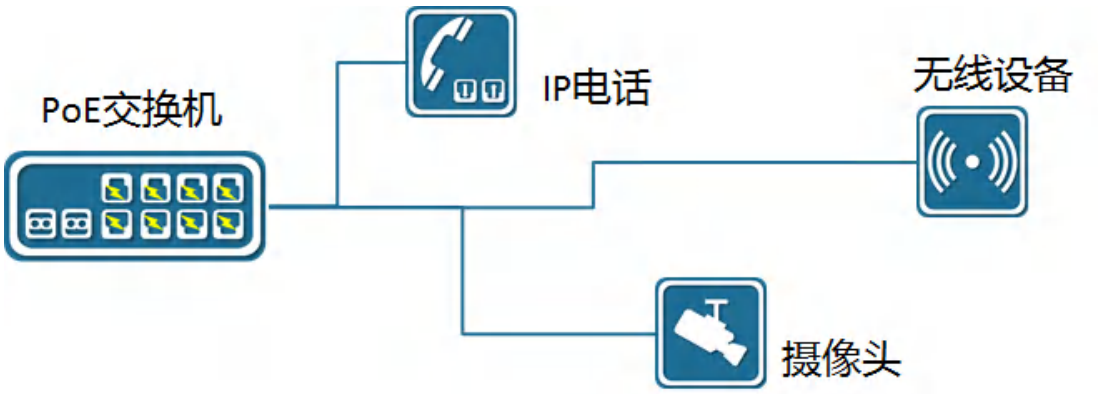
- 显示聚合端口信息

```
        SWITCH#show int po8
        Interface po8
          Hardware is AGG  Current HW addr: 74b9.ebee.2546
          Logical:(not set)
          Port Mode is access
          interface configure:
            medium-fiber mtu 1526 speed-auto duplex-auto flowcontrol-off autonego-
off
          interface status:
            link-up bandwidth-2g
          Aggregate Members:(LACP)
            gigabitEthernet0/19     link up       Enable
            gigabitEthernet0/17     link up       Enable
          input packets:
            Good Octets Rx          : 18986
            Good Packets Rx         : 104
            Broadcast Packets Rx    : 0
            Multicast Packets Rx    : 104
          ouput packets:
            Good Octets Tx          : 38529
            Good Packets Tx         : 359
            Broadcast Packet Tx     : 4
            Multicast Packet Tx     : 355
          un-normal packets:
            Drop Events             : 0
            Undersized Pkts Recvd   : 0
            Oversized Pkts Recvd    : 0
           Bad CRC                 : 0
```

6. 配置 POE

6.1. PoE 概述

Power over Ethernet，简称 PoE，是一个可以在以太网路中通过双绞线与终端进行数据交互同时，提供直流供电的技术。常用对网络电话、WIFI AP、网络摄影机、集线器、电脑等设备进行供电。
按照标准其供电最长距离为 100m。



PSE（Power Sourcing Equipment，供电设备），如上图中 PoE 交换机。PSE 在 PoE 端口的线路上寻找、检测 PD，对 PD 分级，并向其供电。 当检测到 PD 拔出后，PSE 停止供电。PD 是接受 PSE 供电的设备，如上图中 IP 电话、无线设备、摄像头。
PoE 发展经历了两套标准：
IEEE 802.3af(15.4W)是首个 PoE 供电标准，规定了以太网供电标准，是现在 PoE 应用的主流实现标准。它明确规定了远程系统中的电力检测和控制事项，并对路由器、交换机和集线器通过以太网电缆向 IP 电话、安全系统以及无线 LAN 接入点等设备供电的方式进行了规定。IEEE802.3at(25.5W)应大功率终端的需求而诞生，在兼容 802.3af 的基础上，提供更大的供电需求，满足新的需求。根据 IEEE 802.3af 规范，受电设备(PD)上的 PoE 功耗被限制为 12.95W。IEEE 802.3at，它将功率要求高于 12.95W 的设备定义为 Class 4(该级别在 IEEE 802.3af 中有描述，但留作将来使用)，可将功率水平扩展到 25W 或更高。

6.2. 配置命令

- 配置外部电源功率

命令	SWITCH(config)#**poe powersupply** POWER SWITCH(config)#**no poe powersupply**
描述	配置外部电源功率 默认电源功率计算方式：PoE 供电端口数与单端口 15.4W 的乘积 若配置功率小于当前设备消耗功率，则对低优先级端口的 PD 设备下电，端口优先级为端口 ID 小的更高优先级。

- 配置端口供电使能

命令	SWITCH (config-if)#**poe enable** SWITCH (config-if)#**no poe enable**
描述	配置端口使能供电 默认端口供电使能

- 配置端口供电优先级

用户可以配置 PoE 交换机的接口供电优先级。优先级从高到低依次为：high、medium 和 low。在 PoE 交换机整机功率不足的时候，低优先级的端口先掉电。

相同优先级的端口优先级按照端口号顺序排列，端口号小的优先级高，比如端口 0/1 的优先级就比端口 0/2 和 0/3 高。

相同优先级端口，新插入的端口，不会影响到已经处于供电状态的 PD 设备的供电情况。不同优先级的端口不受这个特性影响，高优先级端口可以抢占低优先级的端口。

命令	SWITCH (config-if)#**poe priority (low | medium | high)** SWITCH (config-if)#**no poe priority**
描述	设置端口供电优先级 端口默认优先级为 low

- 配置端口 PD 描述符

命令	SWITCH (config-if)#**poe pd-description** DESC SWITCH (config-if)#**no poe pd-description**
描述	配置接口的 PD 描述符 参数为字符串，最长支持 32 个字符

- 配置端口最大功率

用户可以通过配置端口的最大功率，来限制端口的最大输出功率值。 当端口供电功率超过端口最大功率，端口下电，并显示端口状态异常。

命令	SWITCH (config-if)#**poe max-power** VALUE SWITCH (config-if)#**no poe max-power**
描述	设置端口的最大功率，单位为瓦 对于 AF/AT 端口，端口最大功率范围为 1-30 对于 BT 端口，端口最大功率范围为 1-90

- 配置使能端口兼容模式

命令	SWITCH (config-if))#**poe legacy** SWITCH (config-if))#**no poe legacy**
描述	配置 PoE 接口开启关闭兼容模式 在没有接入 PD 设备的端口上使用这个命令，可能导致对端设备被错误的上电烧毁，请确保端口在接入 PD 设备的时候使用该命令

- 设置端口 PD 自检测模式

PD 自检测功能为解决 PD 负载设备正常受电，但实际工作异常的情况，在检测到 PD 负载异常时，端口停止对外供电，10 秒左右重新对负载上电。PD 自检测有两种方式：

By-flow：端口流量检测，对于供电端口，若长时间无数据交互，则认为负载状态异常。具体时间用户可配置。

By-ping：设备主动发出 ping 请求，若负载正常应答，则认为状态正常，若多次无应答，则认为负载状态异常。

命令	SWITCH (config)#**poe pd-detect mode** (**by-flow | by-ping** IPADDR) SWITCH (config))#**no poe pd-detect mode**
描述	配置使能、关闭端口 PD 自检测功能，配置检测模式 By-flow：基于流的负载检测 By-ping：基于 ping 请求的负载检测 IPADD：by-ping 模式下，PD 负载的 ip 地址

- 设置端口 PD 自检测参数

命令	SWITCH (config)#**poe pd-detect parameter interval** VALUE **times** VALUE SWITCH (config))#**no poe pd-detect parameter**
描述	配置端口 PD 自检测参数 Interval VALUE：检测间隔，范围 5-60 秒，默认 60 秒 Times VALUE：检测次数，范围 3-30 次，默认 5 次

- 设置系统保留功率

考虑 PD 设备消耗功率存在波动，存在 PoE 交换机负载过重导致损坏设备损坏的风险。交换机提供了设置 PoE 系统保留功率的命令来保护 PoE 交换机一直有功率“富裕”，避免该现象的发生。

命令	SWITCH (config)#**poe power-reserved VALUE** SWITCH (config))#**no poe power-reserved**
描述	设置保留功率的占系统总功率的百分比，范围为 0%到 50% 系统的保留功率默认为 0%

- 设置系统功率告警水线

当系统消耗功率大于告警水线功率，系统输出告警 log 信息。

命令	SWITCH (config)#**poe power-alarm VALUE** SWITCH (config))#**no poe power-alarm**
描述	配置系统的功率告警水线，范围为 50-99，单位为百分比，默认为关闭，不支持

6.3. 配置案例

案例一：配置端口 gigabitEthernet0/1 供电使能

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#poe enable
```

6.4. 显示命令

- 显示 PoE 系统供电信息

```
SWITCH#show poe powersupply
  Power supply                : 123.2W
  Power reserved              :  0%
  Power available:            : 123.2W
  Power consume            : 44.1W
  Power management     : energy-saving
  Disconnect mode          : DC
```

```
  Powered ports              : 2
  Power alarm:               : 100%
```

显示的信息含义：

Power supply	电源总功率，单位 W，保留小数点后一位
Power reserved	系统保留功率百分比
Power available	系统可用功率，单位 W，保留小数点后一位
Power consume	系统实际消耗功率，单位 W，保留小数点后一位
Power management	功率管理模式，当前只支持节能模式
Disconnect mode	断连检测模式，目前只支持 DC 检测
Powered ports	上电端口数
Power alarm	系统告警功率百分比

- 显示所有端口供电状态

```
SWITCH#show poe interfaces
Interface   enable  status  reason      class  icut(mA) power(W)
-------------------------------------------------------------------
GiEO/1      YES     OFF     short       4      --       --
GiEO/2      YES     OFF     --          -      --       --
GiEO/3      YES     OFF     --          -      --       --
GiEO/4      YES     OFF     --          -      --       --
GiEO/5      YES     OFF     --          -      --       --
GiEO/6      YES     ON      --          4      270.2    14.0
GiEO/7      YES     OFF     --          -      --       --
GiEO/8      YES     OFF     --          -      --       --
```

显示的信息含义：

Interface	端口名称，采用缩写方式
Enable	端口是否使能对外供电，YES 或 NO
Status	端口供电状态，ON 或 OFF
Reason	端口未正常上电原因： Power management：功率不足 Short：短路
Class	PD 分类登记
Icut	电流值，单位 mA，保留小数点后一位
Power	功率值，单位 W，保留小数点后一位

- 显示单端口 POE 信息

```
SWITCH#show poe interface gigabitEthernet0/1
  Enabled                :  YES
  Status                 :  ON
  Reason:                :  --
  Class                  :  4
  Icut                   :  260.5
  Power                  :  14.2
  Max-power              :  --
  Priority               :  low
  Legacy:                :  Disabled
  Errdis:                :  NO
  Pd-detect mode         :  --
  Pd-detect interval     :  60
```

```
        Pd-detect times        :  5
```

显示的信息含义：

Enabled	端口是否使能对外供电，YES 或 NO
Status	端口供电状态，ON 或 OFF
Reason	端口未正常上电原因： Power management：功率不足 Short：短路
Class	PD 分类登记
Icut	电流值，单位 mA，保留小数点后一位
Power	功率值，单位 W，保留小数点后一位
Max-power	端口最大供电功率，单位 W
Priority	端口供电优先级，Low、Medium、High
Legacy	是否使能非标检测，Enabled、Disabled
Errdis	端口是否触发违例，YES 或 NO
Pd-detect mode	PD 自检测模式，By-flow、By-ping、-- 例如：By-ping（192.168.3.4）
Pd-detect interval	PD 检测间隔
Pd-detect times	PD 检测次数

7. 日志管理

7.1. 日志管理概述

设备在运行过程中，会发生各种状态变化如链路状态 UP、DOWN 等，也会遇到一些事件如处理异常等。系统日志提供一系列服务，在状态变化或发生事件时，将自动生成固定格式的消息，这些消息将记录在设备日志文件上。支持显示在串口、远程登录终端上，也可发送到网络上的 1-3 组日志服务器上，供管理员分析网络情况和定位问题。

为了方便管理员对日志报文的读取和管理，这些日志报文可以被打上时间戳，并按日志信息的优先级进行分级。

7.2. 配置命令

7.2.1. 配置 console 日志等级

命令	SWITCH(config)#**logging console** { **|** <0-7>} SWITCH(config)#**no logging console**
描述	配置串口日志输出等级 默认等级为 6 执行 no 命令时，日志将不在串口输出 执行 logging console，无等级参数，配置为默认等级 6

7.2.2. 配置终端日志输出

- 配置终端日志等级

命令	SWITCH(config)#**logging monitor** { **|** <0-7>} SWITCH(config)#**no logging monitor**
描述	配置终端日志输出等级 默认等级为 6 执行 no 命令时，日志将不在终端输出 执行 logging monitor，无等级参数，配置为默认等级 6

- 使能终端输出日志

命令	SWITCH#**terminal monitor** SWITCH#**terminal no monitor**
描述	日志在终端输出 默认 telnet、ssh 登录，日志不会在终端输出 执行 no 命令后，日志不会在终端输出

7.2.3. 配置远端服务器

- 配置远端服务器

命令	SWITCH(config)#**logging server** { **| second | third**} {A.B.C.D **| ipv6** X.X::X.X} **udp-port** <1-65535> SWITCH(config)#**no logging server** {**| second | third**}

描述	配置远端服务器 最多支持 3 个远端服务器配置 支持远端服务器 UDP 协议端口配置，范围<1-65535> 当没有配置 UDP 端口参数时，默认端口号 514

- 配置送远端服务器日志等级

命令	SWITCH(config)#**logging trap** { **|** <0-7>} SWITCH(config)#**no logging trap**
描述	配置往服务器发送日志等级 默认等级为 6 执行 no 命令时，将不往服务器发送日志 执行 logging trap，无等级参数，配置为默认等级 6

- 配置送服务器日志限速

命令	SWITCH(config)#**logging rate-limit interval** <1-30> **burst** <1-1000> SWITCH(config)#no **logging rate-limit**
描述	配置设备往远端服务器发送日志速率 Interval 为时间范围，默认为 6，范围<1-30>，单位秒 burst 为时间范围内，最大可发送的日志条数，默认 60，范围<1-1000> 默认情况下，每 6 秒内，最多可向服务器发送 60 条 syslog

7.2.4. 配置日志 buffer

命令	SWITCH(config)#**logging buffer** <64-4096> SWITCH(config)#**no logging buffer**
描述	配置本地日志缓存，记录从设备起机开始的 log 默认缓存 1024 条日志 <64 4096>:本地日志缓存最大条数

7.2.5. 清除日志

命令	SWITCH# **clear logging**
描述	清除 syslog

7.3. 配置案例

案例一： 设备 syslog 送远端服务器，设备 ip 为 192.168.1.240， 远端服务器 ip 为 192.168.1.33，UDP 端口号为 10514

在设备上配置远端服务器

```
SWITCH(config)# logging server 192.168.1.33 udp-port 10514
```

设备端产生 syslog 信息

```
*1970 Jan 01 14:19:34 SWITCH %HAL-4: Interface gigabitEthernet0/1 changed state to down
```

在远端服务器器上监控到 syslog 信息：

```
LOCAL.warn: *1970 Jan 1 14:19:34 SWITCH  %HAL-4: Interface
```

```
gigabitEthernet0/1 changed state to down
```

7.4. 显示命令

- 显示日志信息

命令	SWITCH#show logging
描述	显示所有日志信息

- 显示最后特定数量条数日志信息

命令	SWITCH#show logging last <1 4096>
描述	显示最后特定条数日志信息

- 显示日志配置信息

命令	SWITCH#show logging summary
描述	显示日志配置信息

```
SWITCH#show logging summary
Summary of logging configuration:
    Logging console         : 6
    Logging monitor         : 6
    Logging trap            : 6
    Logging buffer          : 1024

    Server:
        Ip address          : 192.168.1.33
        Udp port            : 10514

    Server second           : Disabled

    Server third            : Disabled

    Rate-limit:
        Interval            : 1 seconds
        Burst               : 2
```

字段	说明
Logging console	日志串口输出控制 <0 7>：表示日志等级 Disabled：表示不在串口输出
Logging monitor	日志 vty 输出控制 <0 7>：表示日志等级 Disabled：表示不在 vty 输出
Logging trap	日志 trap 远端服务器输出控制 <0 7>：表示日志等级 Disabled：表示不发送到远端服务器

Logging buffer	本地日志缓存，记录从设备起机开始的 log <64 4096>:本地日志缓存最大条数
Server Server second Server third	服务器，目前支持 3 个服务器配置
Ip address Ipv6 address	Ipv4、ipv6 地址信息
Udp port	UDP 端口信息
Rate-limit	日志送远端服务器限速
Interval	限速有效时间范围
Burst	有效时间内限速值

8. 配置 VLAN

8.1. VLAN 功能概述

VLAN 是虚拟局域网（Virtual Local Area Network）的简称，它是在一个物理网络上划分出来的逻辑网络。这个网络对应于 ISO 模型的第二层网络。VLAN 的划分不受网络端口的 实际物理位置的限制。VLAN 有着和普通物理网络同样的属性，除了没有物理位置的限制，它和普通局域网一样。第二层的单播、广播和多播帧在一个 VLAN 内转发、扩散，而不会直接进入其它的 VLAN 之中。

基于端口的 VLAN 是最简单的一种 VLAN 划分方法。用户可以将设备上的端口划分到不同的 VLAN 中，此后从某个端口接收的报文将只能在相应的 VLAN 内进行传输，从而实现广播域的隔离和虚拟工作组的划分。

以太网交换机的端口链路类型可以分为三种：Access、Trunk、Hybrid。这三种端口在加入 VLAN 和对报文进行转发时会进行不同的处理。

Access 类型：端口只能属于 1 个 VLAN；一般用于交换机与终端用户之间的连接；

Trunk 类型：端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，但是只有 native VLAN 可以不带 VLAN 标记；一般用于交换机之间的连接；

Hybrid 类型：端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，并且可以根据用户的需要配置相关 VLAN 是否带 VLAN 标记；可以用于交换机之间连接，也可以用于连接用户的计算机。

8.2. 配置命令

- 创建删除 VLAN

命令	SWITCH(config)#**vlan** VLAN_RANGE SWITCH(config)#**no vlan** VLAN_RANGE
描述	创建/删除 VLAN

- 配置基于 Access 端口的 VLAN

命令	SWITCH(config)#**interface** IFNAME SWITCH(config-if)#**switchport mode access**
描述	进入以太网端口模式。 配置端口类型为 Access 端口（缺省情况下，端口为 Access 类型）。

命令	SWITCH(config-if)#**switchport access vlan** VLANID SWITCH(config-if)#**no switchport access vlan**
描述	将当前端口加入到指定 VLAN（缺省情况下，所有 Access 端口均属于且只属于 VLAN1），no 命令恢复为缺省。 只有当接口已经配置为 Access 端口后，才能使用如上命令，且指定的 VLAN 必须已经创建。 当配置为非 VLAN1 后，若对应 VLAN 删除，会自动恢复为 VLAN1。

- 配置基于 Trunk 端口的 VLAN

命令	SWITCH(config)#**interface** IFNAME SWITCH(config-if)#**switchport mode trunk**

描述	进入以太网端口模式。 配置端口类型 Trunk 端口。

命令	SWITCH(config-if)#**switchport trunk allowed vlan** { **all** | VLAN_LIST | **none**} SWITCH(config-if)#**no switchport trunk allowed vlan** VLAN_LIST
描述	维护 Trunk 端口的 Allowed VLAN 列表。 只有当接口已经配置为 Trunk 端口后，才能使用如上命令。 All 表示自动模式，自动加入所有已创建的 VLAN，（即使是后续创建，也会自动加入）； None 表示清空 Allowed VLAN 列表，即端口不属于任何 VLAN（包括 native vlan）； VLAN_LIST 表示手动设置 Allowed VLAN 列表，若之前属于 ALL（自动模式），会先清空 Allowed VLAN 列表，再进行 VLAN 列表的添加。VLAN_LIST 支持标准的多 vlan 表示方法(“-”和“,”以及两者组合)； 前面增加 no 关键字时表示从 Allowed VLAN 列表中删除 VLAN_LIST 表示的 VLAN。 设置 all 时，将 Allowed VLAN 列表的维护改为自动模式，其他命令，均修改为手工模式。（缺省情况下，为自动模式，当从其他端口模式切换为 Trunk 端口时，即为自动模式）。 只有已经创建的 VLAN，才能加入 Allowed VLAN 列表；当删除 VLAN 时，Allowed VLAN 列表中对应 VLAN 会自动删除。

命令	SWITCH(config-if)#**switchport trunk native vlan** VLANID SWITCH(config-if)#**no switchport trunk native vlan**
描述	设置 Trunk 端口的 native vlan。（缺省情况下，Trunk 端口的 native VLAN 为 VLAN1），no 命令恢复为缺省。 只有当接口已经配置为 Trunk 端口后，才能使用如上命令。 Native VLAN 的设置跟 Allowed VLAN 是否包含此 VLAN，甚至 VLAN 是否创建没有关系，即 native VLAN 可以设置为一个没有创建的 VLAN。

说明

✦本地设备 Trunk 端口缺省 VLAN ID 和相连的设备的 Trunk 端口的缺省 VLAN ID 必须一致，否则缺省 VLAN 的报文将不能正确传输。

- 配置基于 Hybrid 端口的 VLAN

命令	SWITCH(config)#**interface** IFNAME SWITCH(config-if)#**switchport mode hybrid**
描述	进入以太网端口模式。 配置端口类型 Hybrid 端口。

命令	SWITCH(config-if)#**switchport hybrid allowed vlan** { **all** | VLAN_LIST | **none**} SWITCH(config-if)#**no switchport hybrid allowed vlan** VLAN_LIST
描述	维护 Hybrid 端口的 Allowed VLAN 列表。 只有当接口已经配置为 Hybrid 端口后，才能使用如上命令。 All 表示自动模式，自动加入所有已创建的 VLAN，（即使是后续创建，也会自动加入）；

	None 表示清空 Allowed VLAN 列表，即端口不属于任何 VLAN（包括 native vlan）； VLAN_LIST 表示手动设置 Allowed VLAN 列表，若之前属于 ALL（自动模式），会先清空 Allowed VLAN 列表，再进行 VLAN 列表的添加。VLAN_LIST 支持标准的多 VLAN 表示方法(“-”和“,”以及两者组合)； 前面增加 no 关键字时表示从 Allowed VLAN 列表中删除 VLAN_LIST 表示的 VLAN。 设置 all 时，将 Allowed VLAN 列表的维护改为自动模式，其他命令，均修改为手工模式。（缺省情况下，为自动模式，当从其他端口模式切换为 Trunk 端口时，即为自动模式）。 只有已经创建的 VLAN，才能加入 Allowed VLAN 列表；当删除 VLAN 时，Allowed VLAN 列表中对应 VLAN 会自动删除。

命令	SWITCH(config-if)#**switchport hybrid vlan** VLANID SWITCH(config-if)#**no switchport hybrid vlan**
描述	设置 Hybrid 端口的缺省 VLAN（当端口收到 untagged 报文时，缺省指定的 VLAN；输出时携带缺省 VLAN 的报文，将 untag 输出），（缺省情况下，端口的缺省 VLAN 为 VLAN1），no 命令恢复为缺省情况。 只有当接口已经配置为 Hybrid 端口后，才能使用如上命令。 缺省 VLAN 的设置跟 Allowed VLAN 是否包含此 VLAN，甚至 VLAN 是否创建没有关系，即缺省 VLAN 可以设置为一个没有创建的 VLAN。

命令	SWITCH(config-if)#**switchport hybrid untagged vlan** VLAN_LIST SWITCH(config-if)#**no switchport hybrid untagged vlan** VLAN_LIST
描述	维护 Hybrid 端口的 untagged VLAN 列表。（因为缺省 VLAN 一定是 untag 输出的，因此，不由 untagged VLAN 列表进行维护，缺省情况下，untagged VLAN 列表为空，即除了缺省 VLAN 外，其他 VLAN 均 tagged 输出）。 Untagged VLAN 列表维护的 VLAN 必须在 Hybird 端口的 Allowed VLAN 列表内，因此，当某个 VLAN 从 Allowed VLAN 中删除时，也会对应从 Untagged VLAN 列表中删除。 由于 Untagged VLAN 列表不维护缺省 VLAN，因此，若之前列表中某个 VLAN 被设置为缺省 VLAN，将从 Untagged VLAN 列表中删除，且该过程不可逆。

说明

✦本地设备 Hybrid 端口缺省 VLAN ID 和相连的设备的 Hybrid 端口的缺省 VLAN ID 必须一致，否则缺省 VLAN 的报文将不能正确传输。

8.3. 显示命令

在特权模式下，才可以查看 VLAN 的信息。显示的信息包括 VLAN VID、VLAN 状态、VLAN 成员端口以及 VLAN 配置信息。

- 显示 VLAN

```
VLAN ID  Name        State   H/W Status  Member ports
                                          (u)-Untagged, (t)-Tagged
======= ============ ======= =========== ============================
1       default      ACTIVE  Up          gigabitEthernet0/2(u)
                                             gigabitEthernet0/3(u)
```

9. 配置 QINQ

9.1. QINQ 概述

QinQ 技术〔也称 Stacked VLAN 或 Double VLAN〕。标准出自 IEEE 802.1ad，指在用户报文进入服务提供商网络之前封装上一个服务提供商网络的公网 VLAN Tag，而把用户报文中的私网用户 VLAN Tag 当做数据，使报文带着两层 VLAN Tag 穿越服务提供商网络。

在城域网中需要大量的 VLAN 来隔离用户，IEEE 802.1Q 协议仅支持的 4094 个 VLAN 远远不能满足需求。通过 QinQ 技术双层 Tag 封装，在服务提供商网络中报文只根据公网上分配的唯一外层 VLAN Tag 传播，这样不同的私网用户 VLAN 可以重复使用，扩大了用户可利用的 VLAN Tag 数量，同时提供一种简单的二层 VPN 功能，所以实际上 QINQ 技术是一种 VLAN VPN 技术。

常见的 VLAN VPN 技术除 QINQ 外，还有 VLAN Mapping。两者的区别仅仅在于 QINQ 是对 VLAN 做堆叠（Stacking），VLAN Mapping 是对 VLAN 做映射（Mapping）。

- VLAN Stacking: 从用户网络到提供商网络，单层 tag 变为双层 Tag，C-Tag 保留在报文中，作为内层 Tag；反向，从双层 Tag 变为单层 Tag。
- VLAN Mapping：从用户网络到提供商网络，依然还是单层 Tag，只是 C-Tag 变为 S-Tag；反向，从 S-Tag 变为 C-Tag。

9.2. 配置说明

QINQ 分为三类：

- A 类：基本 QINQ，基于接口开启关闭，当开启基本 QINQ 的接口收到报文时，都当成 untag 报文处理，在原有报文的基础上，增加一层该端口缺省 VLAN 的 VLAN Tag。
- B 类：基于 C-tag 的灵活 QINQ，根据用户侧的 C-VLAN Tag，根据配置的映射策略，在原始报文基础上，增加一层 S-VLAN Tag。该类 QINQ 的配置方式有可选的两种方式，二者只能选择其一。一种方式为接口上直接配置 C-VLAN 和 S-VLAN 的映射关系；一种方式在全局配置 VLAN VPN(其中包含了 C-VLAN 和 S-VLAN 的映射关系)，然后在接口上关联 VPN。对多个接口采用相同映射策略的情况，一般选择后面一种配置方式。对于此类 QINQ，若接口收到的报文为 untag 时，C-tag 为接口的缺省 VLAN Tag。
- C 类：基于 ACL 的灵活 QINQ，根据配置的流策略，来添加外层 Tag。该类 QINQ 的配置放入“QOS”模块中，具体参见“配置 QOS”章节，Policy-map 和 Class-map 的策略对中：“**nest vlan**<1-4094>”即是用于配置基于 ACL 的灵活 QINQ。

如上三类 QINQ 在同一个端口可以同时开启，其优先级关系为：C 类> B 类> A 类。

VLAN Mapping 分为 1:1 VLAN Mapping 和 1:N VLAN Mapping(反向即为 N:1)，当前仅支持 1:1 VLAN Mapping。VLAN Mapping 的配置方式为：在全局配置 VLAN VPN，然后在接口上关联 VPN。VLAN Mapping 只对 tag 报文生效，这跟 QINQ 功能有很大区别。

QINQ 和 VLAN Mapping 功能在配置时有如下一些注意点：

- 仅物理接口支持 QINQ 和 VLAN Mapping 的配置，聚合口不支持。

- VLAN Mapping 只对带 tag 报文生效，上行流，原始报文必须携带 tag，才能实现 CVLAN 到 SVLAN 的映射；对下行流，在下链接口的 VLAN 输出规则，必须是 tag 输出，才能实现 SVLAN 到 CVLAN 的映射。
- QINQ 功能或者 VLAN Mapping 功能使用时，需要和 VLAN 配置配合使用，在输入输出方向，VLAN 的过滤功能，以及 VLAN 是否携带 tag 的规则，均以 VLAN 配置为准。具体要求如下：
  - 涉及到 CVLAN 和 SVLAN 都需要加入到下链接口（连接 Customer 网络）的允许列表，否则流将会被过滤；
  - SVLAN 需要加入到上链接口（连接 Provider 网络）的允许列表，否则流将会被过滤；
  - 对 QINQ，在下链接口，SVLAN 应该配置 untag 输出，以便对 QINQ 下行流剥掉外层 tag；
  - 对 VLAN-Map，由于只对 untag 报文生效，因此，对下链接口，SVLAN 应该配置 tag 输出，否则下行流无法完成 SVLAN 到 CVLAN 的映射。
- 全局配置的 VLAN VPN 要么用于 VLAN Stacking(QINQ),要么用于 VLAN Mapping，不能同时应用于两者。
- VLAN Mapping 由于只支持 1:1 映射，因此，存在 N:1 映射的 VLAN VPN，无法作为 VLAN Mapping 的 VPN 关联到接口上；同样，若已经作为 VLAN Mapping 关联到接口的 VPN，其中的映射关系无法变更为 N:1。
- VLAN Mapping 的映射关系必须全局一致，因此，不同的接口只能关联同一个 VLAN VPN。
- 在同一个接口上，若需要同时应用 VLAN Mapping 与 QINQ，应注意两个功能需控制不同的 CVLAN 和 SVLAN。具体约束如下：
  - 若 VLAN Mapping 和基本 QINQ 一起使用，以基本 QINQ 生效，VLAN Mapping 失效。
  - 若 VLAN Mapping 和灵活 QINQ 一起使用时，若某条流经过 VLAN Mapping 映射后的 SVLAN，同时能作为 CVLAN 命中灵活 QINQ 的映射策略，那么最终的报文将会以灵活 QINQ 生效，添加 SVLAN 作为外层 TAG，内层 TAG 保持不变（而非 VLAN Mapping 映射后的 VLAN）。
  - 介于如上约束，因此在同一个接口上开启两种应用时，需要注意两者进行控制的 VLAN 不要存在交集，若存在交集，命中交集部分的报文，在报文封装时，VLAN Mapping 将失效。
- B 类 QINQ 要么选择在接口下直接配置映射策略，要么选择关联 VPN，不能同时配置。

9.3. 配置命令

- 创建/删除 VLAN VPN

命令	SWITCH(config)#**vlan-vpn** VPN-NAME SWITCH(config)#**no vlan-vpn** VPN-NAME
描述	系统中可以存在多个 VPN，每个 VPN 中维护独立 CVLAN 和 SVLAN 的映射关系。VPN 只有当应用到接口时，才会实际生效。某个 VPN 可以应用于 VLAN Stacking（QINQ），也可以应用于 VLAN Mapping，但只能二选一。

- 添加/删除 VPN 的映射关系

命令	SWITCH(config-vlan-vpn)#**cvlan** VLAN_LIST **svlan** VLANID

	SWITCH(config-vlan-vpn)#**no cvlan** VLAN_LIST SWITCH(config-vlan-vpn)#**no cvlan**
描述	VLAN_LIST 和 VLANID 的有效范围为<1,4094>，VLAN_LIST 支持标准的多 vlan 表示方法(“-”和“,”以及两者组合)。 no cvlan 不带任何参数时，将 VPN 内的所有映射关系全部清除。

- 配置/取消基本 QINQ

命令	SWITCH(config-if)#**switchport vlan-stacking basic** SWITCH(config-if)#**no switchport vlan-stacking basic**
描述	基本 QINQ 开启后，从该接口进入的报文都命中 QINQ 规则，映射的 SVLAN 为接口缺省 VLAN ID。

- 添加/删除接口下 QINQ 的映射关系

命令	SWITCH(config-if)#**switchport vlan-stacking cvlan** VLAN_LIST **svlan** VLANID SWITCH(config-if)#**no switchport vlan-stacking cvlan** VLAN_LIST SWITCH(config-if)#**no switchport vlan-stacking cvlan**
描述	与 VPN 下的映射关系配置类似。只有当接口没有关联 VPN 时，才能直接进行映射关系配置。

- 接口关联/取消关联 QINQ VPN

命令	SWITCH(config-if)#**switchport vlan-stacking vpn** VPN-NAME SWITCH(config-if)#**no switchport vlan-stacking vpn**
描述	一个接口只能关联一个 VPN。只有当接口没有配置映射关系时，才能进行 VPN 关联配置。

- 取消接口的所有 QINQ 配置

命令	SWITCH(config-if)#**no switchport vlan-stacking**
描述	等同于 no switchport vlan-stacking basic no switchport vlan-stacking cvlan no switchport vlan-stacking vpn 三条命令。

- 接口关联/取消关联 VLAN Mapping VPN

命令	SWITCH(config-if)#**switchport vlan-mapping vpn** VPN-NAME SWITCH(config-if)#**no switchport vlan-mapping**
描述	不同接口配置 VLAN Mapping，必须关联同一个 VPN。且对应 VPN 中的映射关系必须是 1:1 的。

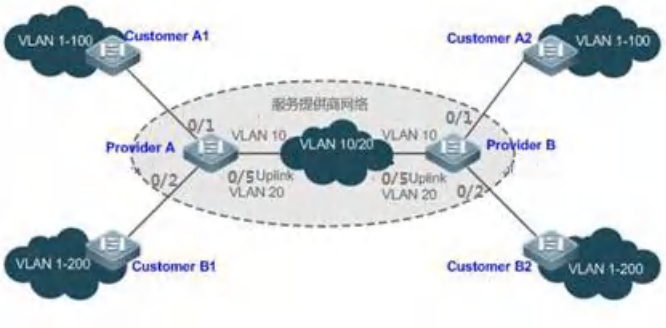
9.4. 配置案例

案例一：基于端口实现二层 VPN 业务

服务提供商为企业 A 和企业 B 提供 VPN：

- 在公网上企业 A 和企业 B 属于不同的 VLAN，各自通过所属的公网 VLAN 通信。

- 企业 A 和企业 B 内的 VLAN 对公网来说是透明的，企业 A 和企业 B 内的用户 VLAN 可以重复使用并且不冲突。
- Tunnel 会对用户数据报文再封装一层 Native VLAN 的 VLAN Tag。在公网中用户数据报文以 Native VLAN 传播，不影响不同企业用户网络的 VLAN 使用，并实现简单的二层 VPN。



图例说明：

- Customer A1 和 Customer A2、Customer B1 和 Customer B2 分别为企业用户 A、企业用户 B 所在网络的边缘设备。Provider A 和 Provider B 为服务提供商网络边缘设备，企业 A 和企业 B 通过提供商边缘设备接入公网。
- 企业 A 使用的办公网络 VLAN 范围为 VLAN 1-100。
- 企业 B 使用的办公网络 VLAN 范围为 VLAN 1-200。

ProviderA 和 ProviderB 完全对称，配置完全一致：

- 配置 VLAN

```
SWITCH(config)#vlan 2-200
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 1-100
SWITCH(config-if)#switchport trunk native vlan 10
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk native vlan 10
SWITCH(config-if)#interface gigabitEthernet0/5
SWITCH(config-if)#switchport mode trunk
```

- 配置基本 QINQ

```
SWITCH(config)#interface gigabitEthernet0/1-2
SWITCH(config-if)#switchport vlan-stacking basic
SWITCH(config-if)#exit
```

案例二：基于 C-Tag 的灵活 QINQ 实现二层 VPN 和业务流管理

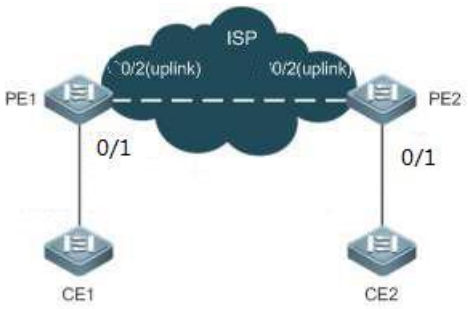
基本 QinQ 只能将用户数据报文封装一层 Native VLAN 的外 Tag，即外层 Tag 的封装依赖于 Tunnel 口的 Native VLAN。灵活 QinQ 提供根据用户报文的 Tag(即 C-Tag)来灵活封装服务提供商(ISP)的外 Tag(即 S-Tag)，以便更灵活实现 VPN 透传和业务流 QOS 策略。

- 宽带上网、IPTV 业务都是城域网的所承载业务的重要部分，城域网服务商网络针对不同业务流划分 VLAN 来区分管理，并提供针对这些 VLAN 设置 QOS 策略服务。可以在服务商边缘设备上运用基于 C-Tag 的 QinQ 将用户的业务流封装相关的 VLAN，在透传的同时利用服务商网络的 QOS 策略进行保障性传输。

- 企业分公司之间实现了统一的 VLAN 规划，重要业务和一般业务分别在不同的 VLAN 范围内，企业网可以利用基于 C-Tag 的灵活 QinQ 透传公司内部的业务，又能利用服务商网络的 QOS 策略优先保障重要业务的数据传输。

如下图所示，城域网内用户端设备通过小区的楼道交换机汇聚，宽带上网、IPTV 业务通过分配不同的 VLAN 进行区分，分别享用不同的 QOS 服务策略。

- 在公网中，宽带上网和 IPTV 的不同业务流以不同的 VLAN 传播，实现用户业务的透传。
- ISP 网络针对 VLAN 设置 QOS 策略，在服务商边缘设备上可以针对用户业务封装对应的 VLAN，使得 IPTV 业务在 ISP 网络中优先传输。



图例说明：

- CE1 和 CE2 为连接用户网络的边缘设备，PE1 和 PE2 为提供商服务网络边缘设备。
- CE1 和 CE2 设备上 VLAN 1-100 为用户宽带上网业务流，VLAN 101-200 为用户 IPTV 业务流。
- PE1 和 PE2 设备为不同业务的 VLAN 封装不同 S-Tag 以区分不同的业务数据。VLAN 1-100 封装 VLAN100，VLAN101-200 封装 VLAN200。

PE1 和 PE2 配置完全一致：

- 配置 VLAN

```
SWITCH(config)#vlan 2-200
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#switchport mode hybrid
SWITCH(config-if)#switchport hybrid untagged vlan 100,200
SWITCH(config-if)#switchport hybrid vlan 100
SWITCH(config-if)#interface gigabitEthernet0/2
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#exit
```

- 配置灵活 QINQ

```
SWITCH(config)#vlan-vpn isp
SWITCH(config-vlan-vpn)# cvlan 1-100 svlan 100
SWITCH(config-vlan-vpn)# cvlan101-200 svlan 200
SWITCH(config-vlan-vpn)# interface gigabitEthernet0/1
SWITCH(config-if)#switchport vlan-stacking vpn isp
SWITCH(config-if)#exit
```

案例三：基于 C-Tag 的 VLAN Mapping 实现二层 VPN 和业务流管理

与案例二类似，区分用户的宽带上网业务和 IPTV 业务，比如宽带上网业务是 VLAN2，IPTV 业务是 VLAN3。在 ISP 网络分别用 VLAN200 和 VLAN300 表示宽带上网业务和 IPTV 业务。PE 设备的 1-10 口全部都有连接 CE 设备,上链接口为 gigabitEthernet0/11

PE1 和 PE2 配置完全一致：

- 配置 VLAN

```
SWITCH(config)#vlan2-3,200,300
SWITCH(config)#interface gigabitEthernet0/1-10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#exit
```

- 配置 VLAN Mapping

```
SWITCH(config)#vlan-vpn isp-map
SWITCH(config-vlan-vpn)#cvlan 2 svlan 200
SWITCH(config-vlan-vpn)#cvlan 3 svlan 300
SWTICH(config-vlan-vpn)#interface gigabitEthernet0/1-10
SWITCH(config-if)#switchport vlan-mapping vpn isp-map
SWITCH(config-if)#exit
```

9.5. 显示命令

- 显示接口下的相关配置

使用 show running-configure 或者 show running-configure interface*IFNAME* 来显示接口下的相关配置。

- 显示 VPN 配置

在特权模式，配置模式，VLAN-VPN 模式，接口模式均支持进行 VPN 配置显示命令

- **show vlan-vpn***VPN-NAME*：查看某个 VPN 信息。

```
SWITCH#show vlan-vpn test
-------------------------------------------------------------
VLAN VPN: test           ==》 VPN 名字。
Class: vlan-stacking     ==》表示 VPN 用于 VLAN-STACKING，若还未关联到任何接口，则为 unknown。
Mapping attributes:      ==》 CVLAN 和 SVLAN 的映射关系，若未配置任何映射关系，则为 empty!
 cvlan 1-25,73,75-80 svlan 3
 cvlan 200 svlan 4
Applied interfaces:      ==》关联此 VPN 的所有接口列表，若还未关联到任何接口，则为 empty!
 gigabitEthernet0/17
 gigabitEthernet0/18
```

2）show vpn-vpn：查看所有 VPN 信息。

```
SWITCH#show vlan-vpn
-------------------------------------------------------------
VLAN VPN: test
Class: vlan-stacking
Mapping attributes:
 cvlan 1-25,73,75-80 svlan 3
 cvlan 200 svlan 4
Applied interfaces:
 gigabitEthernet0/17
 gigabitEthernet0/18
-------------------------------------------------------------
VLAN VPN: test-map1
Class: vlan-mapping
```

```
        Mapping attributes:
         cvlan 100 svlan 1
         cvlan 200 svlan 2
         cvlan 800 svlan 8
         cvlan 900 svlan 9
        Applied interfaces:
         gigabitEthernet0/18
         gigabitEthernet0/19
        ------------------------------------------------------------
        VLAN VPN: test1
        Class: unkown
        Mapping attributes:
         cvlan 800 svlan 8
         cvlan 900 svlan 9
        Applied interfaces:
         empty!
```

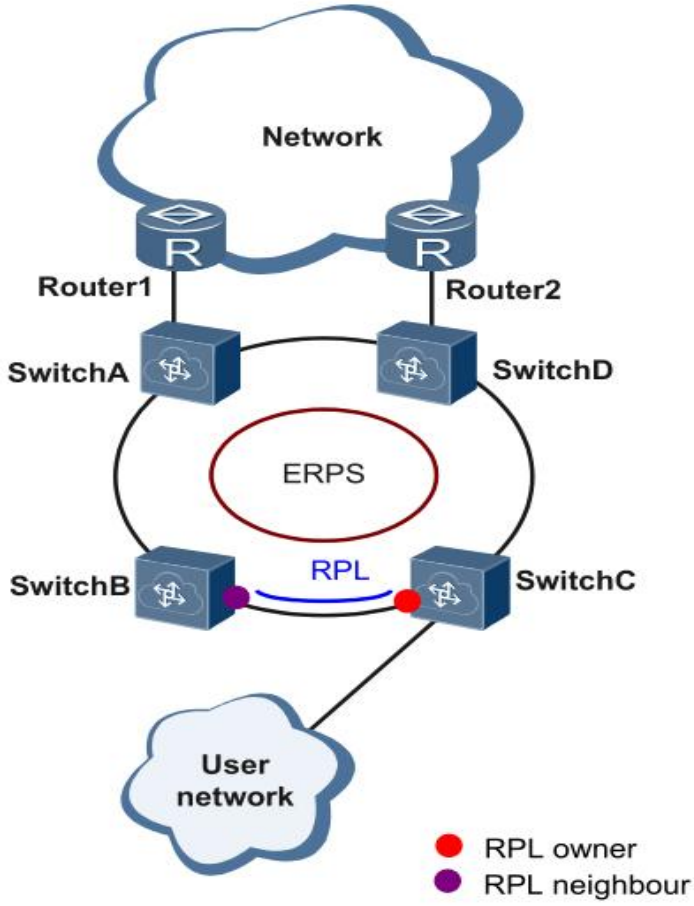
10. 配置 ERPS

10.1. ERPS 功能概述

ERPS（Ethernet Ring Protection Switching，以太环网保护切换协议）为 ITU 开发的一种环网保护协议，也称 G.8032。它是一个专门应用于以太环网的链路层协议。它在以太环网完整时能够防止数据环路引起的广播风暴，而当以太环网上一条链路断开时能迅速恢复环网上各个节点之间的通信。

目前，解决二层网络环路问题的技术还有 STP。STP 应用比较成熟，但其收敛的时间比较长（秒级）。ERPS 是专门应用于以太环网的链路层协议，二层收敛性能达 50ms 以内，具有比 STP 更快的收敛速度。

ERPS 典型组网：



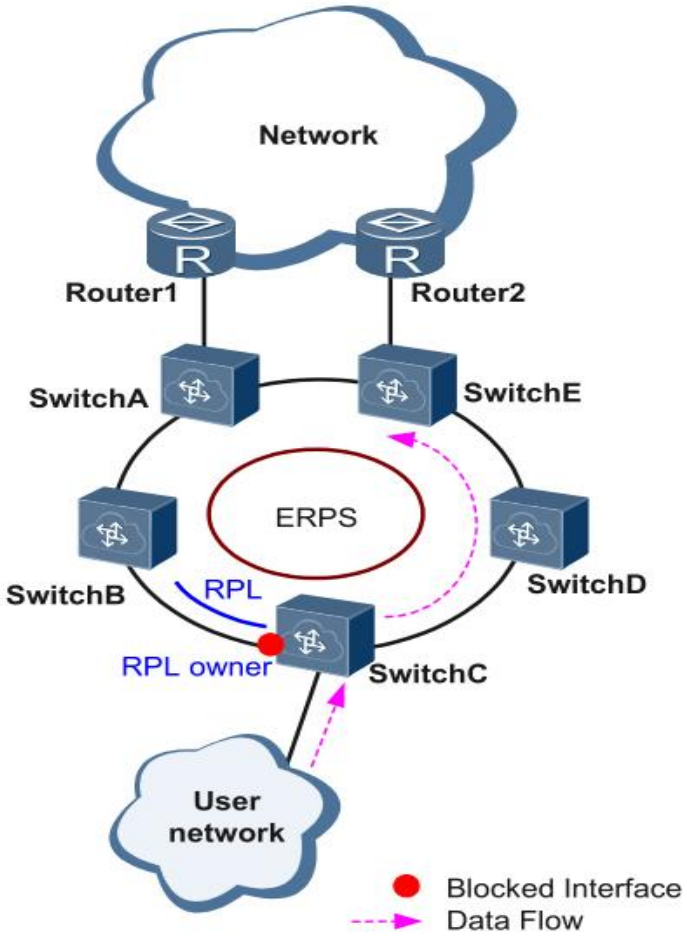
10.2. ERPS 原理简介

ERPS 是一种专用于以太网链路层的标准环网协议，以 ERPS 环为基本单位。每台二层交换设备上只能有两个端口加入同一个 ERPS 环。在 ERPS 环中，为了防止出现环路，可以启动破除环路机制，阻塞 RPL owner 端口，消除环路。当环网发生链路故障时，运行 ERPS 协议的设备可以迅速地放开阻塞端口，进行链路保护倒换，恢复环网上各节点间链路通信。本节主要以示例的形式按照链路正常->链路故障->链路恢复的过程（包括保护倒换操作），介绍基本的单环组网下 ERPS 的实现原理。

链路正常

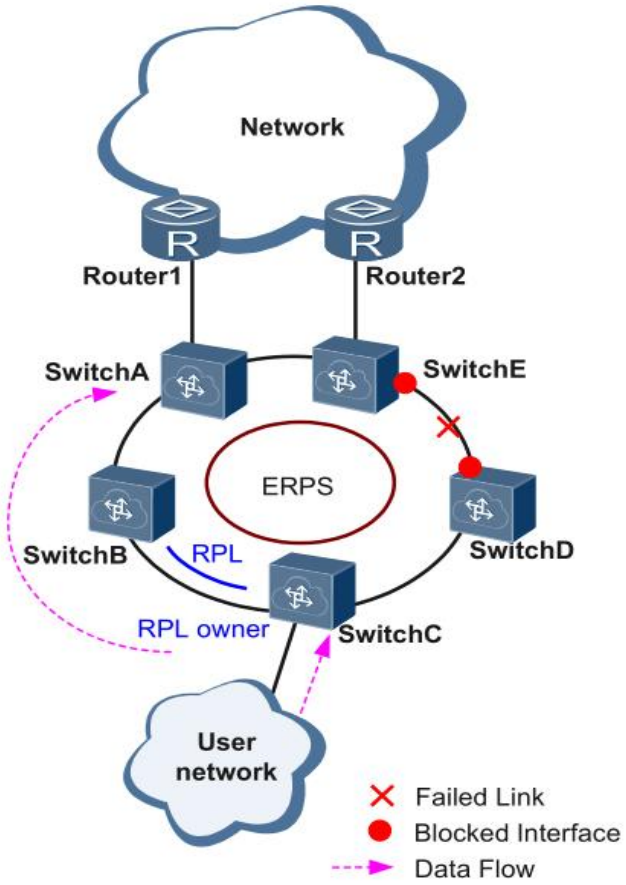
如下图所示，由 SwitchA ~ SwitchE 组成的环路上各设备通信正常。

为防止环路产生，ERPS 首先会阻塞 RPL owner 端口，如果配置了 RPL neighbour 端口，该端口同样会被阻塞，其他端口可以正常转发业务流量。



链路故障

如图所示，当 SwitchD 和 SwitchE 之间的链路发生故障时，ERPS 协议启动保护倒换机制，将故障链路的两端端口阻塞，然后放开 RPL owner 端口，这两个端口重新恢复用户流量的接收和发送，从而保证了流量不中断。



链路恢复

链路恢复正常后，如果 ERPS 环配置的是回切模式，RPL owner 端口所在设备会重新阻塞 RPL 链路上的流量，故障链路重新被用来完成用户流量的传送。

10.3. 配置命令

- 创建环

命令	SWITCH(config)#**erps ring** <1-255> **east-interface** IFNAME **west-interface** IFNAME SWITCH(config)#**no erps ring** <1-255>
描述	创建/删除 ERPS 环； ERPS 环是由一组配置了相同的控制 VLAN 且互连的二层交换设备构成，是 ERPS 协议的基本单位，环中的每台设备上都需要配置。 环编号为 ERPS 环的唯一标识。

- 创建 ERPS 实例

命令	SWITCH(config)#**erps instance** NAME SWITCH(config)#**no erps instance** NAME
描述	创建/删除 ERPS 实例；创建的同时会进入实例配置模式。 对于运行 ERPS 协议的二层设备，传递 ERPS 协议报文和数据报文的 VLAN 必须映射到保护实例中，这样 ERPS 协议才会按照其阻塞原则对这些报文进行转发或阻塞。否则，VLAN 报文可能会在成环的网络中产生广播风暴导致网络不可用。

- 关联 ERPS 实例和环

命令	SWITCH(config-erps-inst)#**ring** <1-255>
描述	配置 ERPS 实例和环的对应关系；

- 配置 ERPS 实例等级

命令	SWITCH(config-erps-inst)#**level** <0-7>
描述	配置 ERPS 实例等级；

- 配置 ERPS 实例中 RPL 角色

命令	SWITCH(config-erps-inst)#**rpl-role** NAME
描述	配置 ERPS 实例 RPL 角色； 一个 ERPS 环只有一个 RPL owner 端口，由用户配置决定，通过阻塞 RPL owner 端口转发用户流量来防止 ERPS 环中产生环路。

- 配置实例保护的管理 VLAN

命令	SWITCH(config-erps-inst)#**vlan** <1-4094> **raps-channel** SWITCH(config-erps-inst)#**no raps-channel**
描述	配置/删除 ERPS 实例的管理 VLAN/数据 VLAN； 每个 ERPS 环必须配置控制 VLAN。不同 ERPS 环不能使用相同 ID 的控制 VLAN。

- 配置实例保护的 MST Instance

命令	SWITCH(config-erps-inst)#**protected-mst-instance** <0-255>
描述	配置 ERPS 实例保护的 MST Instance； 可以在 MST 模式下配置 VLAN 和 Instance 关系，且需要先将 STP 模式设置为 MSTP，详见 STP 配置章节；默认所有 VLAN 属于 Instance 0；默认 id 为 0。 注意：相交环中目前不支持多实例的功能!

- 配置相交子环阻断口

命令	SWITCH(config-erps-inst)#**sub-ring block (east-interface | west-interface)**
描述	配置 ERPS 实例为子环实例，并指定子环阻断口。

- 配置子环虚通道和非虚通道

命令	SWITCH(config-erps-inst)#**virtual-channel attached-to-instance** NAME SWITCH(config-erps-inst)# **non-virtual-channel**
描述	配置 ERPS 相交子环的类型：虚通道并关联主环；或非虚通道类型。 注意：本命令在 showrunning-config 中显示的位置必须在关联实例的显示位置之后。通常只需要确保子环 ID 和实例名称比主环的 ID 和实例名称大即可。

- 配置 ERPS 回切模式

命令	SWITCH(config-erps-inst)#**revertive | non-revertive**

描述	配置 ERPS 自动回切/不回切；

- 配置 ERPS 定时器参数

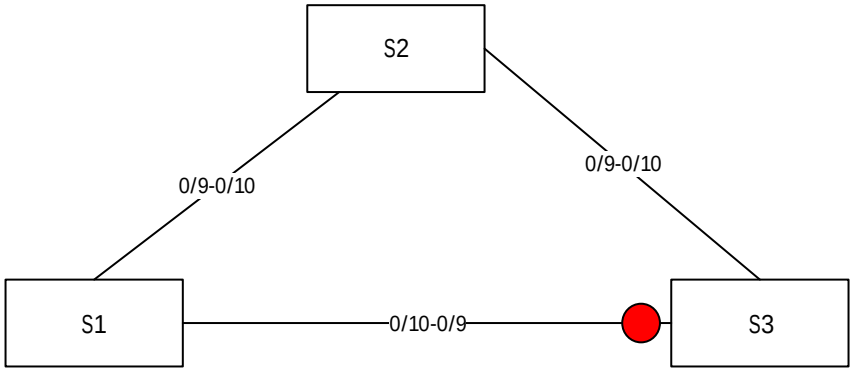
命令	SWITCH(config-erps-inst)#(**wtr-timer** (<1-12> | **default**) | **holdoff-timer** (<0-100> | **default**) | **guard-timer** (<1-200> | **default**))
描述	配置 ERPS 定时器参数； <1-12>: 单位分钟；故障恢复后的回切时间，默认为 5 分钟 <0-100>：单位为 100 毫秒；端口 forward 前的保持时间，默认为 0，直接 forward 不延迟 <1-200>：单位为 10 毫秒；状态变化时的保护窗口，避免收到前一个状态的消息导致协议误判，默认为值 50：500 毫秒 **guard-timer** 参数一定程度上会限制网络规模，保守建议当环网中超过 300 个节点时，直接将该参数配置为最大值，避免因为网络规模过大造成旧报文无法被正常丢弃；300 个以内节点无需特别配置。

- 配置 ERPS 日志

命令	SWITCH(config)#**erps logging** SWITCH(config)#**no erps logging**
描述	开启/关闭 ERPS 日志功能。

10.4. 配置案例

1、单环案例需求：如图所示，配置默认阻断 S1 和 S2 的直连链路，故障时及时恢复链路确保网络可用。其中数据 VLAN 为 1,2 和 3。



S1/S2：

- 进入全局配置模式，创建 ERPS 并设定相关参数，命令参考列表如下：

创建数据 vlan 2,3;vlan 1 默认存在

```
SWITCH(config)#vlan 2,3
```

将接口模式改为 trunk，trunk 模式默认会将所有数据 vlan 和管理 vlan 加入接口转发

```
SWITCH(config)#interface gigabitEthernet0/9-10
SWITCH(config-if)#switchport mode trunk
```

创建 erps 环 1

```
SWITCH(config)#erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
```

创建 erps 实例 1，关联环 1，及相关细节配置

```
SWITCH(config)#erps instance 1
```

```
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role non-owner
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

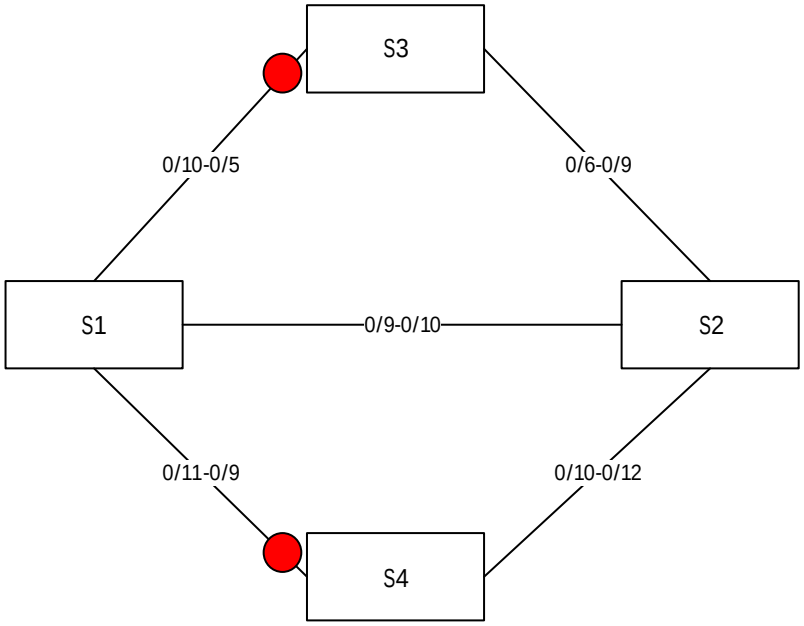
S3:

- 进入全局配置模式，创建 ERPS 并设定相关参数，命令参考列表如下：

```
SWITCH(config)#Vlan 2,3
SWITCH(config)#interface gigabitEthernet0/9,gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
SWITCH(config)#Erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role owner east
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

2、相交环案例需求

如下图拓扑，S1、S2、S3、S4 组成相交环，数据 vlan 为 1、2、3、4，要求每个环中出现单点故障时都能够实现快速收敛；网络中最多可以出现两个故障点(不同环)，而不出现用户断网，达到最优可靠性。



典型配置举例：

S1:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 vlan 1000 raps-channel

Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/11
Erps instance 2
 ring 2
  sub-ring block east-interface
  vlan 1100 raps-channel
  virtual-channel attached-to-instance 1
```

S2:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 vlan 1000 raps-channel

Erps ring 2 east gigabitEthernet0/12 west gigabitEthernet0/10
Erps instance 2
 ring 2
  sub-ring block east-interface
  vlan 1100 raps-channel
  virtual-channel attached-to-instance 1
```

S3:

```
Vlan 2,3,4
interface gigabitEthernet0/5-6
switchport mode trunk
Erps ring 1 east gigabitEthernet0/5 west gigabitEthernet0/6
Erps instance 1
 ring 1
 rpl-role owner east
 vlan 1000 raps-channel
```

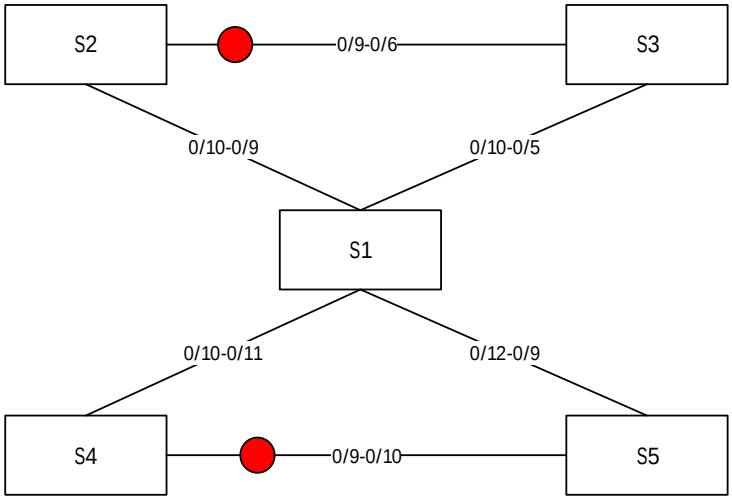
S4:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 2
 ring 2
 rpl-role owner east
 vlan 1100 raps-channel
```

3、相切环案例需求

拓扑图如下所示，S1 位于中心机房，可以被管理员实时监督和维护，具备较高可靠性；S2-S5 分布在各地部署点，为了提高组网的可靠性，避免出现单链路外连的单点故障风险，同时避免双链路外连单机可能出现的单机故障风险，采用双链路外连组成环网的方式。

要求每个环网出现单点故障时均能够快速收敛，避免用户网络中断。



典型配置举例：

S1:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 vlan 1000 raps-channel

Erps ring 2 east gigabitEthernet0/11 west gigabitEthernet0/12
Erps instance 2
 ring 2
  vlan 1100 raps-channel
```

S2:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 rpl-role owner east
 vlan 1000 raps-channel
```

S3:

```
Vlan 2,3,4
interface gigabitEthernet0/5-6
switchport mode trunk
Erps ring 1 east gigabitEthernet0/5 west gigabitEthernet0/6
Erps instance 1
 ring 1
 vlan 1000 raps-channel
```

S4:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 2
 ring 2
 rpl-role owner east
 vlan 1100 raps-channel
```

S5:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 2
 ring 2
 vlan 1100 raps-channel
```

10.5. 显示命令

- 显示 ERPS 环信息

```
SWITCH#show erps ring 1

Ring     : 1
==========
Bridge   : 1
East     : gigabitEthernet0/23
West     : gigabitEthernet0/24
ERP Inst :1, 2,
SWITCH#
```

- 显示 ERPS 实例

```
SWITCH#
SWITCH#show erps instance 1
Name                  : 1
Protected MST Instance: 0
Protected VLANs       : 1
State                 : ERPS_ST_IDLE
Last Priority         : RAPS-NR-RB
Phy Ring              : 1
Role                  : NON-OWNER
East Link             : Link_Unblocked(up)(78-A9-12-12-13-12, 1)
West Link             : Link_Unblocked(up)(78-A9-12-12-13-12, 1)
TCN Propagation       : Disabled
Attached              : -
Attached To           : -
Virtual ID            : -:-
-----------------------------------------------------
     Channel         |       Interface
 (LEVL, VID, RID)    | (east,ver) ,  (west,ver)
=====================================================
 (0, 1000,    1)     | (gigabitEthernet0/23, V=1), (gigabitEthernet0/24,
V=1)
=====================================================
Wait-To-Restore       : 5 mins
Hold Off Timer        : 0 secs
Guard Timer           : 500 ms
Wait-To-Block         : 5500 ms
Protection Type       : Revertive
SWITCH#
```

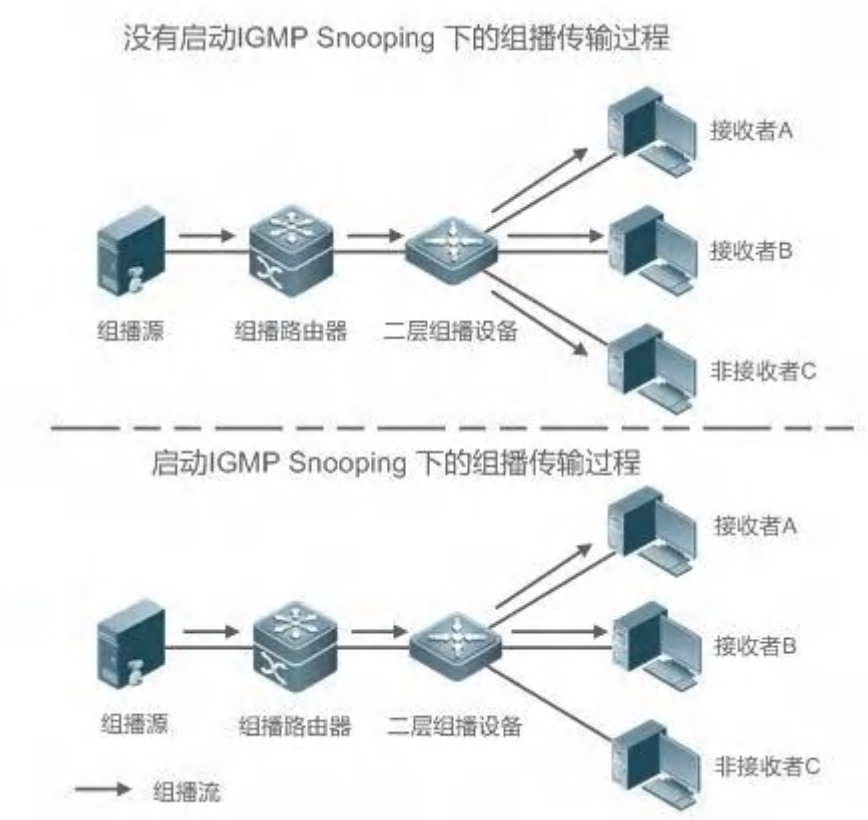
11. 配置 IGMP Snooping

11.1. 概述

IGMP Snooping 是 Internet Group Management Protocol Snooping（互联网组管理协议窥探）的简称，它是运行在二层设备上的组播约束的机制，用于管理和控制组播组。

运行 IGMP Snooping 的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据。当二层设备没有运行 IGMP Snooping 时，组播数据在二层被广播；当二层设备运行了 IGMP Snooping 后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者。

如下图所示，当二层组播设备没有运行 IGMP Snooping 时，IP 组播报文在 VLAN 内被广播；当二层组播设备运行了 IGMP Snooping 后，IP 组播报文只发给组成员接收者。



11.2. 配置命令

- 启用 IGMP Snooping

命令	SWITCH(config)#**igmp snooping** SWITCH(config)#**no igmp snooping**
描述	启用/关闭 IGMP Snooping 功能；默认关闭。 全局模式。

- 配置 IGMP Snooping 上行口

命令	SWITCH(config-if)#**igmp snooping mrouter interface** IFNAME SWITCH(config-if)#**no igmp snooping mrouter interface** IFNAME

描述	配置/删除 IGMP Snooping 上行口；可选配置。 SVI 接口模式。

- 配置 IGMP Snooping 静态组

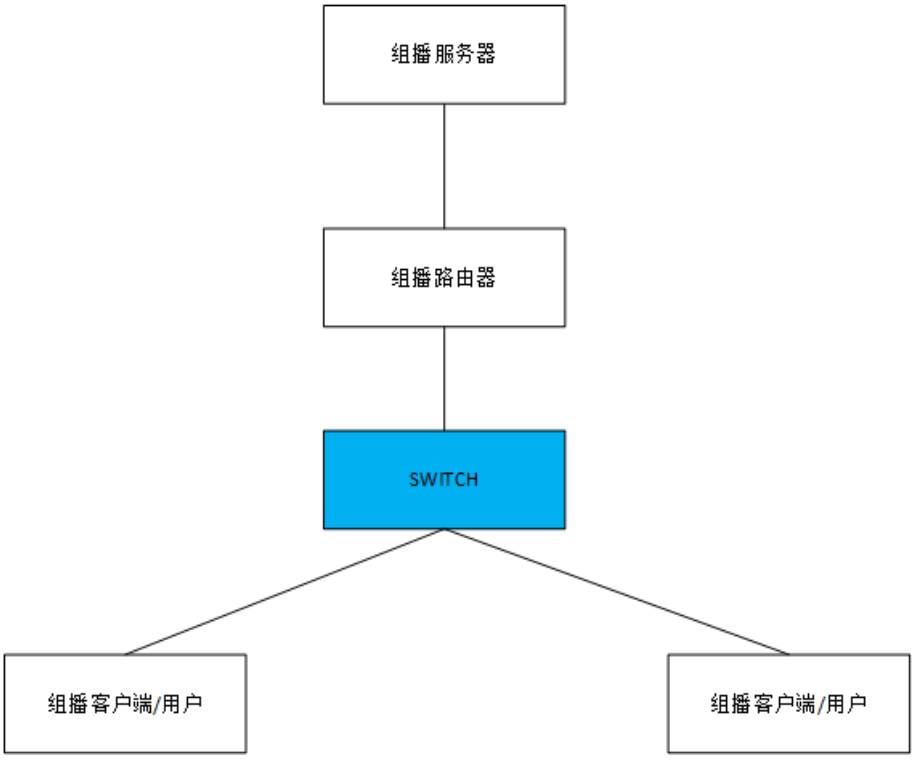
命令	SWITCH(config-if)#**igmp snooping static-group** IPADDR **source** IPADDR **interface** IFNAME SWITCH(config-if)#**no igmp snooping static-group** IPADDR **source** IPADDR **interface** IFNAME
描述	配置/删除 IGMP Snooping 静态组；可选配置。 SVI 接口模式。

- 配置 IGMP Snooping 快速离开

命令	SWITCH(config-if)#**igmp snooping fast-leave** SWITCH(config-if)#**no igmp snooping fast-leave**
描述	配置/删除 IGMP Snooping 快速离开功能；可选配置。 SVI 接口模式。

11.3. 配置案例

简化拓扑：



基本配置/角色：（自上而下）

服务器：

需要启用组播服务，测试时使用了 VLC 作为组播服务器提供组播服务： udp://225.0.0.1:1234，服务器 IP 3.3.3.10

路由器：

运行组播路由协议并启用 IGMP，测试时采用锐捷 S57 三层交换机来模拟，主要配置如下：

开启组播路由

```
ip multicast-routing
```

配置上链口，连接服务器，此处为简单选择 PIM 密集模式，实际网络规模大，组播使用少的建议使用稀疏模式

```
interface GigabitEthernet 0/23
 no switchport
 no ip proxy-arp
 ip pim dense-mode
ip address 3.3.3.3 255.255.255.0
```

配置下链口，此处为简单选择 PIM 密集模式，实际网络规模大，组播使用少的建议使用稀疏模式

```
interface VLAN 1
 no ip proxy-arp
 ip pim dense-mode
ip address 2.2.2.1 255.255.255.0
```

SWITCH：

启用组播即可

```
igmp snooping
```

客户端：

通过 udp://225.0.0.1:1234 来进行观看服务器组播视频，IP 2.2.2.10

11.4. 显示命令

- 查看 IGMP Snooping 组播组

```
SWITCH#show igmp snooping groups
```

- 查看 IGMP Snooping 接口信息

```
SWITCH#show igmp snooping interface {ifname}
示例：
IGMP Snooping information for vlan1
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2 fast-leave is disabled
 IGMPv1/v2 Report suppression enabled
 IGMPv3 Report suppression enabled
 Router port detection using IGMP Queries
 Number of router-ports: 2
 Number of Groups: 2
 Number of Joins: 891
 Number of Leaves: 4
 Active Ports:
  gigabitEthernet0/1
  gigabitEthernet0/2
```

- 查看 IGMP Snooping 路由口信息

```
SWITCH#show igmp snooping mrouter vlan1
示例：
SWITCH#show igmp snooping mrouter vlan1
VLAN    Interface             IP-address    Expires
1       gigabitEthernet0/18(dynamic)         2.2.2.1        00:03:34
       gigabitEthernet0/20(static)           --             --
```

- 查看 IGMP Snooping 接口统计

```
SWITCH#show igmp snooping statistics interface vlan1
IGMP Snooping statistics for vlan1
 Group Count            :  2
 IGMP reports received  :  893
 IGMP leaves received   :  4
 IGMPv1 query warnings  :  0
 IGMPv2 query warnings  :  456
 IGMPv3 query warnings  :  0
```

12. 配置 STP 生成树协议

12.1. 功能介绍

生成树协议是一种二层管理协议，它通过选择性地阻塞网络中的冗余链路来消除二层环路，同时还具备链路备份的功能。

与众多协议的发展过程一样，生成树协议也是随着网络的发展而不断更新的，从最初的 STP（Spanning Tree Protocol，生成树协议）到 RSTP（Rapid Spanning Tree Protocol，快速生成树协议），再到最新的 MSTP（Multiple Spanning Tree Protocol，多生成树协议）。

三种生成树协议的比较：

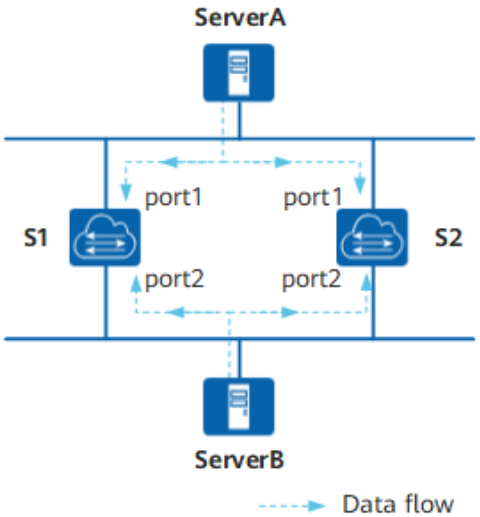
生成树协议	特点	应用场景
STP	形成一棵无环路的树，解决广播风暴并实现冗余备份。 收敛速度较慢。	无需区分用户或业务流量，所有 VLAN 共享一棵生成树。
RSTP	形成一棵无环路的树，解决广播风暴并实现冗余备份。 收敛速度快。	
MSTP	形成一棵无环路的树，解决广播风暴并实现冗余备份。 收敛速度快。 多棵生成树在 VLAN 间实现负载均衡，不同 VLAN 的流量按照不同的路径转发。	需要区分用户或业务流量，并实现负载分担。不同的 VLAN 通过不同的生成树转发流量，每棵生成树之间相互独立。

12.1.1. STP

12.1.1.1. 需求背景

STP 是一个用于局域网中消除环路的协议。运行该协议的设备通过彼此交互信息而发现网络中的环路，并适当对某些端口进行阻塞以消除环路。由于局域网规模的不断增长，生成树协议已经成为了当前最重要的局域网协议之一。

图 12-1 典型局域网络示意图



如图 12-1 所示网络中，会产生如下两种情况：

1. 广播风暴导致网络不可用。

环路产生广播风暴，广播风暴会导致网络不可用。假设交换设备上没有启用 STP 协议。如果 ServerA 发出广播请求，那么广播报文将被其他两台交换设备的端口 port1 接收，并分别从端口 port2 广播出去，然后端口 port2 又收到另一台交换设备发过来的广播报文，再分别从两台交换设备的端口 port1 转发，如此反复，最终导致整个网络资源被耗尽，网络瘫痪不可用。

2. MAC 地址表震荡导致 MAC 地址表项被破坏。

即使是单播报文，也有可能导致交换设备的 MAC 地址表项混乱，以致破坏交换设备的 MAC 地址表。

假设所示的网络中没有广播风暴，ServerA 发送一个单播报文给 ServerB，如果此时 ServerB 临时从网络中移去，那么交换设备上有关 ServerB 的 MAC 地址表项也将被删除。此时 ServerA 发给 ServerB 的单播报文，将被交换设备 S1 的端口 port1 接收，由于 S1 上没有相应的 MAC 地址转发表项，该单播报文将被转发到端口 port2 上，然后交换设备 S2 的端口 port2 又收到从对端 port2 端口发来的单播报文，然后又从 port1 发出去。同时，交换设备 S2 的端口 port1 也会接收 ServerA 发给 ServerB 的单播报文，然后又从 port2 发出去。如此反复，在两台交换设备上，由于不间断地从端口 port1、port2 收到主机 A 发来的单播报文，交换设备会不停地修改自己的 MAC 地址表项，从而引起了 MAC 地址表的抖动。如此下去，最终导致 MAC 地址表项被破坏。

12.1.1.2. 基本概念

- **一个根桥**

对于一个 STP 网络，根桥在全网中只有一个，它是整个网络的逻辑中心，但不一定是物理中心。根桥会根据网络拓扑的变化而动态变化。

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，其他设备仅对该报文进行处理，传达拓扑变化记录，从而保证拓扑的稳定。

- **两种度量**

生成树的生成计算有两大基本度量依据：ID 和路径开销。

ID

ID 又分为：BID（Bridge ID）和 PID（Port ID）。

BID：桥 ID

IEEE 802.1D 标准中规定 BID 是由桥优先级（Bridge Priority）与桥 MAC 地址构成。BID 桥优先级占据高 16 位，其余的低 48 位是 MAC 地址。

在 STP 网络中，桥 ID 最小的设备会被选举为根桥。

PID：端口 ID

PID 由两部分构成的，高 4 位是端口优先级，低 12 位是端口号。

PID 只在某些情况下对选择指定端口有作用。

路径开销

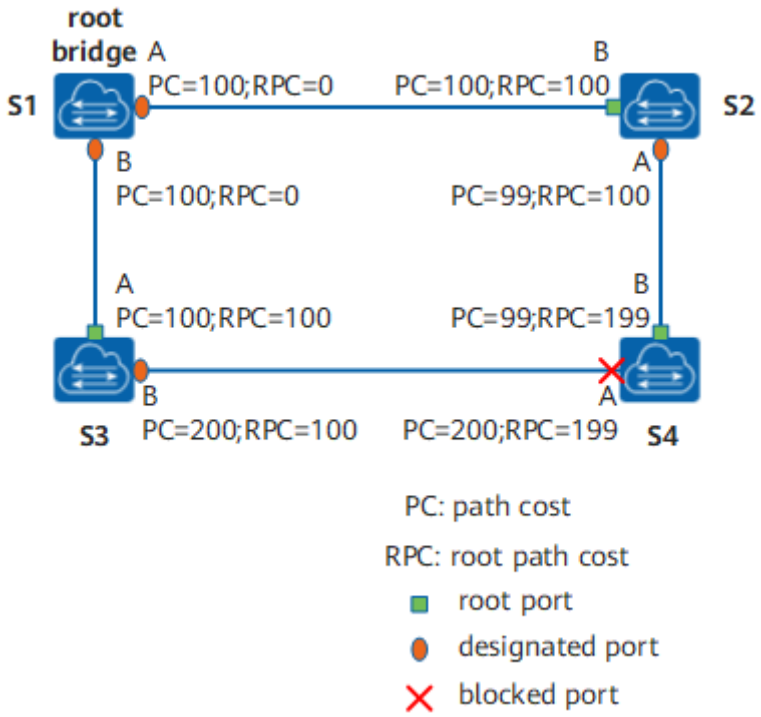
路径开销（Path Cost）是一个端口变量，是 STP 协议用于选择链路的参考值。STP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树形网络结构。

在一个 STP 网络中，某端口到根桥的路径开销就是所经过的各个桥上的出端口的路径开销累加而成，这个值叫做根路径开销（Root Path Cost）。

- **三要素选举**

从环形网络拓扑结构到树形结构，总体来说有三个要素：根桥、根端口和指定端口。以下结合图 12-2 介绍三要素。

图 12-2 STP 网络结构



根桥 RB（Root Bridge）

根桥就是网桥 ID 最小的桥，通过交互配置 BPDU 协议报文选出最小的 BID。

根端口 RP（Root Port）

所谓根端口就是去往根桥路径开销最小的端口，根端口负责向根桥方向转发数据，这个端口的选择标准是依据根路径开销判定。在一台设备上所有使能 STP 的端口中，根路径开销最小者，就是根端口。很显然，在一个运行 STP 协议的设备上根端口有且只有一个，根桥上没有根端口。

指定端口 DP（Designated Port）

指定桥与指定端口的描述见表 12-1。

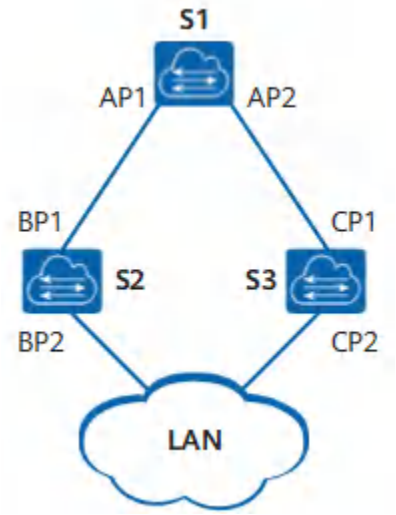
表 12-1 指定桥与指定端口的含义

分类	指定桥	指定端口
对于一台设备而言	与本机直接相连并且负责向本机转发配置消息的设备	指定桥向本机转发配置消息的端口
对于一个局域网而言	负责向本网段转发配置消息的设备	指定桥向本网段转发配置消息的端口

如图 12-3 所示，AP1、AP2、BP1、BP2、CP1、CP2 分别表示设备 S1、S2、S3 的端口。S1 通过端口 AP1 向 S2 转发配置消息，则 S2 的指定桥就是 S1，指定端口就是 S1 的端口 AP1。

与局域网 LAN 相连的有两台设备：S2 和 S3，如果 S2 负责向 LAN 转发配置消息，则 LAN 的指定桥就是 S2，指定端口就是 S2 的 BP2。

图 12-3 指定桥与指定端口示意图



一旦根桥、根端口、指定端口选举成功，则整个树形拓扑建立完毕。在拓扑稳定后，只有根端口和指定端口转发流量，其他的非根非指定端口都处于阻塞（Blocking）状态，它们只接收 STP 协议报文而不转发用户流量。

- **四个比较原则**

STP 选举有四个比较原则，构成消息优先级向量：< 根桥 ID，根路径开销，发送设备 BID，发送端口 PID >。

配置 BPDU 中携带本端口的主要信息如表 12-2 所示。

表 12-2 四个重要信息字段

字段内容	简要说明
根桥 ID	每个 STP 网络中有且仅有一个根。
根路径开销	发送配置 BPDU 的端口到根桥的距离，决定了到根桥的路径开销。
发送设备 BID	发送配置 BPDU 的设备的 BID。
发送端口 PID	发出配置 BPDU 的端口的 PID。

STP 网络中的其他设备收到配置 BPDU 消息后，将比较表中所述的字段，四个基本比较原则如下：

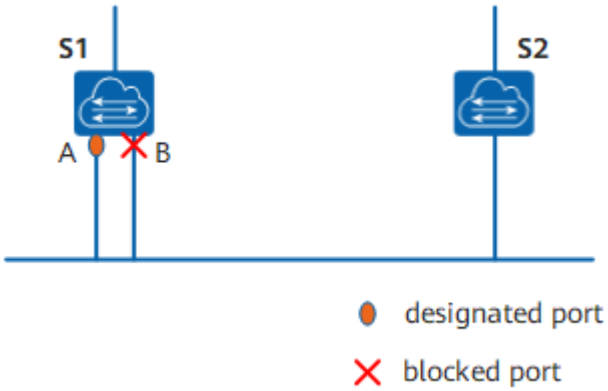
最小 BID：用来选举根桥。运行 STP 协议的设备之间根据根桥 ID 字段选择最小的 BID。

最小根路径开销：用来在非根桥上选择根端口。在根桥上，每个端口到根桥的根路径开销都是 0。

最小发送者 BID：当一台运行 STP 协议的设备要在两个以上根路径开销相等的端口之中选择根端口时，通过 STP 协议计算，将选择接收到的配置消息中发送者 BID 较小的那个端口。如图 12-2 所示，假设 S2 的 BID 小于 S3 的 BID，如果 S4 的 A、B 两个端口接收到的 BPDU 里面的根路径开销相等，那么端口 B 将成为根端口。

最小 PID：用于在根路径开销相同的情况下，不阻塞最小 PID 的端口，而是阻塞 PID 值较大的端口。如图 12-4 所示的情况下 PID 才起作用，S1 的端口 A 的 PID 小于端口 B 的 PID，由于两个端口上收到的 BPDU 中，根路径开销、发送交换设备 BID 都相同，所以消除环路的依据就只有 PID。

图 12-4 应用到 PID 进行比较的拓扑



- **五种端口状态**

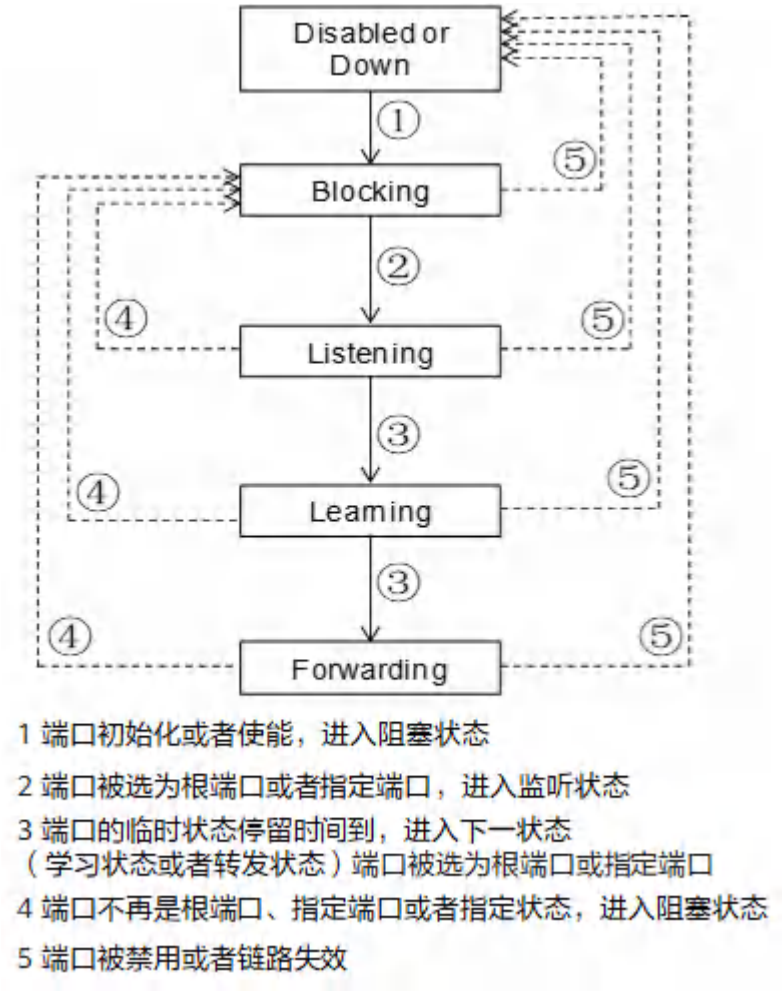
运行 STP 协议的设备上端口状态如表 12-3 所示。

表 12-3 STP 端口状态

端口状态	目的	说明
Forwarding	端口既转发用户流量也处理 BPDU 报文。	只有根端口或指定端口才能进入 Forwarding 状态。
Learning	设备会根据收到的用户流量构建 MAC 地址表，但不转发用户流量。	过渡状态，增加 Learning 状态防止临时环路。
Listening	确定端口角色，将选举出根桥、根端口和指定端口。	过渡状态。
Blocking	端口仅仅接收并处理 BPDU，不转发用户流量。	阻塞端口的最终状态。
Disabled	端口不仅不处理 BPDU 报文，也不转发用户流量。	端口状态为 Down。

端口状态迁移机制如图 12-5 所示。

图 12-5 STP 端口状态迁移图



对于 STP，影响端口状态和端口收敛有以下 3 个参数。

1. Hello Time

运行 STP 协议的设备发送配置消息 BPDU 的时间间隔，用于设备检测链路是否存在故障。设备每隔 Hello Time 时间会向周围的设备发送 hello 报文，以确认链路是否存在故障。
当网络拓扑稳定之后，该计时器的修改只有在根桥修改后才有效。新的根桥会在发出的 BPDU 报文中填充适当的字段以向其他非根桥传递该计时器修改的信息。但当拓扑变化之后，TCN BPDU 的发送不受这个计时器的管理。

2. Forward Delay

设备状态迁移的延迟时间。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，可能会造成临时环路。为此，STP 采用了一种状态迁移机制，新选出的根端口和指定端口要经过 2 倍的 Forward Delay 延时后才能进入转发状态，这个延时保证了新的配置消息传遍整个网络，从而防止了临时环路的产生。
Forward Delay Timer 指一个端口处于 Listening 和 Learning 状态的各自持续时间，默认是 15 秒。即 Listening 状态持续 15 秒，随后 Learning 状态再持续 15 秒。这两个状态下的端口不转发用户流量，这正是 STP 用于避免临时环路的关键。

3. Max Age

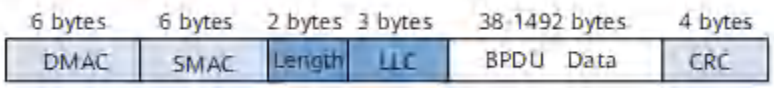
端口的 BPDU 报文老化时间，可在根桥上通过命令人为改动老化时间。

Max Age 通过配置 BPDU 报文的传输，可保证 Max Age 在整网中一致。运行 STP 协议的网络中非根桥设备收到配置 BPDU 报文后，报文中的 Message Age 和 Max Age 会进行比较：
如果 Message Age 小于等于 Max Age，则该非根桥设备继续转发配置 BPDU 报文。
如果 Message Age 大于 Max Age，则该配置 BPDU 报文将被老化。该非根桥设备直接丢弃该配置 BPDU，可认为网络直径过大，导致根桥连接失败。
如果配置 BPDU 是根桥发出的，则 Message Age 为 0。否则，Message Age 是从根桥发送到当前桥接收到 BPDU 的总时间，包括传输延时等。实际实现中，配置 BPDU 报文经过一个桥，Message Age 增加 1。

12.1.1.3. 报文格式

在前面的章节中介绍了桥 ID、路径开销和端口 ID 等信息，所有这些信息都是通过 BPDU 协议报文传输。
配置 BPDU 是一种心跳报文，只要端口使能 STP，则配置 BPDU 就会按照 Hello Time 定时器规定的时间间隔从指定端口发出。
TCN BPDU 是在设备检测到网络拓扑发生变化时才发出。
BPDU 报文被封装在以太网数据帧中，目的 MAC 是组播 MAC：01-80-C2-00-00-00，Length/Type 字段为 MAC 数据长度，后面是 LLC 头，LLC 之后是 BPDU 报文头。以太网数据帧格式如图 12-6 所示。

图 12-6 以太网数据帧格式



- **配置 BPDU**

通常所说的 BPDU 报文多数指配置 BPDU。
在初始化过程中，每个桥都主动发送配置 BPDU。但在网络拓扑稳定以后，只有根桥主动发送配置 BPDU，其他桥在收到上游传来的配置 BPDU 后，才触发发送自己的配置 BPDU。
配置 BPDU 的长度至少要 35 个字节，包含了桥 ID、路径开销和端口 ID 等参数。只有当发送者的 BID 或端口的 PID 两个字段中至少有一个和本桥接收端口不同，BPDU 报文才会被处理，否则丢弃。这样避免了处理和本端口信息一致的 BPDU 报文。
配置 BPDU 在以下 3 种情况下会产生：

1. 只要端口使能 STP，则配置 BPDU 就会按照 Hello Time 定时器规定的时间间隔从指定端口发出。
2. 当根端口收到配置 BPDU 时，根端口所在的设备会向自己的每一个指定端口复制一份配置 BPDU。
3. 当指定端口收到比自己差的配置 BPDU 时，会立刻向下游设备发送自己的 BPDU。

配置 BPDU 报文基本格式如表 12-4 所示。

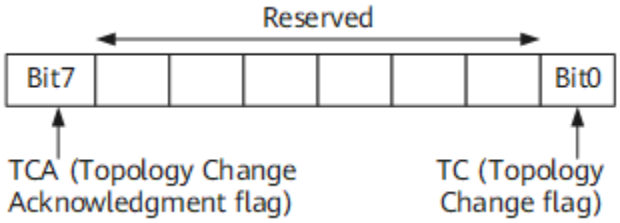
表 12-4 BPDU 报文基本格式

域	字节	说明
Protocol Identifier	2	总是 0。
Protocol Version Identifier	1	总是 0。
BPDU Type	1	当前 BPDU 类型： 0x00：配置 BPDU。

		0x80：TCN BPDU。
Protocol Version Identifier	1	总是 0。
BPDU Type	1	当前 BPDU 类型： 0x00：配置 BPDU。 0x80：TCN BPDU。
Flags	1	网络拓扑变化标志： 最低位=TC（Topology Change，拓扑变化）标志。 最高位=TCA（Topology Change Acknowledgment，拓扑变化确认）标志。
Root Identifier	8	当前根桥的 BID。
Root Path Cost	4	本端口累计到根桥的开销。
Bridge Identifier	8	本交换设备的 BID。
Port Identifier	2	发送该 BPDU 的端口 ID。
Message Age	2	该 BPDU 的消息年龄。 如果配置 BPDU 是根桥发出的，则 Message Age 为 0。否则，Message Age 是从根桥发送到当前桥接收到 BPDU 的总时间，包括传输延时等。实际实现中，配置 BPDU 报文经过一个桥，Message Age 增加 1。
Max Age	2	消息老化年龄。
Hello Time	2	发送两个相邻 BPDU 的时间间隔。
Forward Delay	2	控制 Listening 和 Learning 状态的持续时间。

标志字段如图 12-7 所示，STP 中只使用了其最高位和最低位。

图 12-7 Flags 字段格式



- TCN BPDU

TCN BPDU 内容比较简单，只有表 12-4 中列出的前 3 个字段：协议号、版本和类型。类型字段是固定值 0x80，长度只有 4 个字节。

TCN BPDU 是指在下游拓扑发生变化时向上游发送拓扑变化通知，直到根节点。TCN BPDU 在如下两种情况下会产生：

1. 端口状态变为 Forwarding 状态。
2. 指定端口收到 TCN BPDU，复制 TCN BPDU 并发往根桥。

12.1.1.4. 拓扑计算

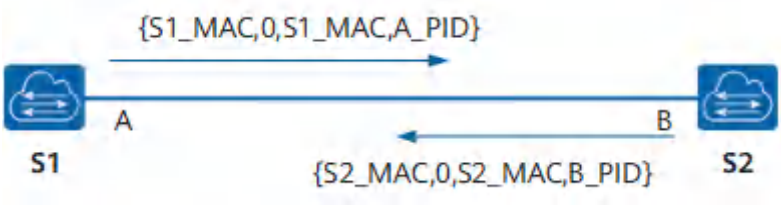
网络中所有的设备使能 STP 协议后，每一台设备都认为自己是根桥。此时，每台设备仅仅收发配置 BPDU，而不转发用户流量，所有的端口都处于 Listening 状态。所有设备通过交换配置 BPDU 后，进行选举工作，选出根桥、根端口和指定端口。

BPDU 报文的交互过程

如图 12-8 所示，用<>标注的四元组表示了由根桥 ID（图中以 S1_MAC 和 S2_MAC 代表两台设备的 BID）、累计根路径开销、发送者 BID、发送端口 PID 构成的有序组。配置 BPDU

会按照 Hello Timer 规定的时间间隔来发送。

图 12-8 初始信息交互



STP 算法实现的基本过程

- 初始状态

由于每个桥都认为自己是根桥，所以在每个端口所发出的 BPDU 中，根桥字段都是用各自的 BID，Root Path Cost 字段是累计的到根桥的开销，发送者 BID 是自己的 BID，端口 PID 是发送该 BPDU 端口的端口 ID。

- 选择根桥

网络初始化时，网络中所有的 STP 设备都认为自己是“根桥”，根桥 ID 为自身的设备 ID。通过交换配置消息，设备之间比较根桥 ID，网络中根桥 ID 最小的设备被选为根桥。

- 选择根端口和指定端口

根端口和指定端口的选择过程如表 12-5 所示。

表 12-5 根端口和指定端口的选择过程

步骤	过程
1	非根桥设备将接收最优配置消息（最优配置消息的选择过程如表 12-6 所示）的那个端口定为根端口
2	设备根据根端口的配置消息和根端口的路径开销，为每个端口计算一个指定端口配置消息： 根桥 ID 替换为根端口的配置消息的根桥 ID； 根路径开销替换为根端口配置消息的根路径开销加上根端口对应的路径开销； 发送者 BID 替换为自身设备的 ID； 发送端口 PID 替换为自身端口 ID。
3	设备将计算出的配置消息与角色待定端口自己的配置消息进行比较： 如果计算出的配置消息更优，则该端口被确定为指定端口，其配置消息也被计算出的配置消息替换，并周期性地向外发送； 如果该端口自己的配置消息更优，则不更新该端口的配置消息并将该端口阻塞。该端口将不再转发数据，且只接收不发送配置消息。

表 12-6 最优配置消息的选择过程

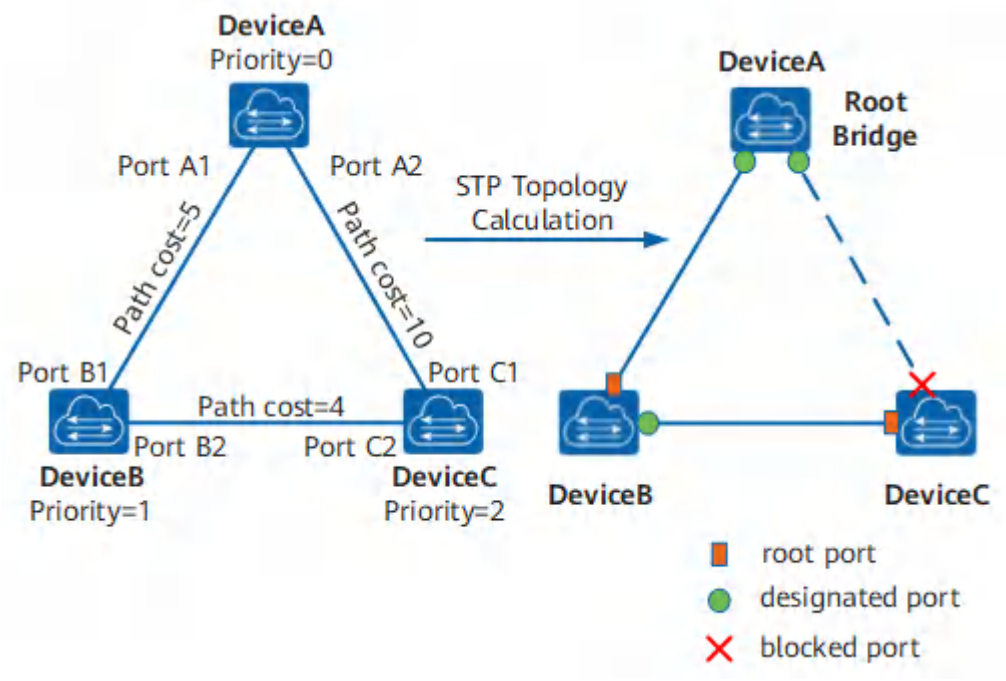
步骤	过程
1	每个端口将收到的配置消息与自己的配置消息进行比较： 如果收到的配置消息优先级较低，则将其直接丢弃，对自己的配置消息不进行任何处理； 如果收到的配置消息优先级较高，则用该配置消息的内容将自己配置消息的内容替换掉。
2	设备将所有端口的配置消息进行比较，选出最优的配置消息。

STP 算法实现举例

一旦根桥、根端口和指定端口选举成功，整个树形拓扑就建立完毕了。下面结合例子说明

STP 算法实现的具体过程。

图 12-9 STP 算法实现过程组网图及计算后的拓扑



如图所示，DeviceA、DeviceB 和 DeviceC 的优先级分别为 0、1 和 2，DeviceA 与 DeviceB 之间、DeviceA 与 DeviceC 之间以及 DeviceB 与 DeviceC 之间链路的路径开销分别为 5、10 和 4。

各设备的初始状态

各设备的初始状态如下表所示。

表 12-7 各设备的初始状态

设备	端口名称	端口的配置消息 <根桥 ID，累计根路径开销，发送者 BID，发送端口 PID>
DeviceA	Port A1	<0，0，0，Port A1>
	Port A2	<0，0，0，Port A2>
DeviceB	Port B1	<1，0，1，Port B1>
	Port B2	<1，0，1，Port B2>
DeviceC	Port C1	<2，0，2，Port C1>
	Port C2	<2，0，2，Port C2>

各设备的比较过程及结果

各设备的比较过程及结果如下表所示。

表 12-8 STP 拓扑计算过程及结果

设备	比较过程	比较后端口的配置消息
DeviceA	Port A1 收到 Port B1 的配置消息<1，0，1，Port B1>，发现自己的配置消息<0，0，0，Port A1>更优，于是将其丢弃。 Port A2 收到 Port C1 的配置消息<2，0，2，Port C1>，发现自己的配置消息<0，0，0，Port A2>更优，于是将其丢弃。	Port A1：<0，0，0，Port A1> Port A2：<0，0，0，Port A2>

	DeviceA 发现自己各端口的配置消息中的根桥和指定桥都是自己，于是认为自己就是根桥，各端口的配置消息都不作任何修改，此后便周期性地向外发送配置消息。	
DeviceB	Port B1 收到 Port A1 的配置消息<0，0，0，Port A1>，发现其比自己的配置消息<1，0，1，Port B1>更优，于是更新自己的配置消息。 Port B2 收到 Port C2 的配置消息<2，0，2，Port C2>，发现自己的配置消息<1，0，1，Port B2>更优，于是将其丢弃。	Port B1：<0，0，0，Port A1> Port B2：<1，0，1，Port B2>
	DeviceB 比较自己各端口的配置消息，发现 Port B1 的配置消息最优，于是该端口被确定为根端口，其配置消息不变。 DeviceB 根据根端口的配置消息和路径开销，为 Port B2 计算出指定端口的配置消息<0，5，1，Port B2>，然后与 Port B2 本身的配置消息<1，0，1，Port B2>进行比较，发现计算出的配置消息更优，于是 Port B2 被确定为指定端口，其配置消息也被替换为计算出的配置消息，并周期性地向外发送。	根端口 Port B1：<0，0，0，Port A1> 指定端口 Port B2：<0，5，1，Port B2>
DeviceC	Port C1 收到 Port A2 的配置消息<0，0，0，Port A2>，发现其比自己的配置消息<2，0，2，Port C1>更优，于是更新自己的配置消息。 Port C2 收到 Port B2 更新前的配置消息<1，0，1，Port B2>，发现其比自己的配置消息<2，0，2，Port C2>更优，于是更新自己的配置消息。	Port C1：<0，0，0，Port A2> Port C2：<1，0，1，Port B2>
	DeviceC 比较自己各端口的配置消息，发现 Port C1 的配置消息最优，于是该端口被确定为根端口，其配置消息不变。 DeviceC 根据根端口的配置消息和路径开销，为 Port C2 计算出指定端口的配置消息<0，10，2，Port C2>，然后与 Port C2 本身的配置消息<1，0，1，Port B2>进行比较，发现计算出的配置消息更优，于是 Port C2 被确定为指定端口，其配置消息也被替换为计算出的配置消息。	根端口 Port C1：<0，0，0，Port A2> 指定端口 Port C2：<0，10，2，Port C2>
	Port C2 收到 Port B2 更新后的配置消息<0，5，1，Port B2>，发现其比自己的配置消息<0，10，2，Port C2>更优，于是更新自己的配置消息。 Port C1 收到 Port A2 周期性发来的配置消息<0，0，0，Port A2>，发现其与自己	Port C1：<0，0，0，Port A2> Port C2：<0，5，1，Port B2>

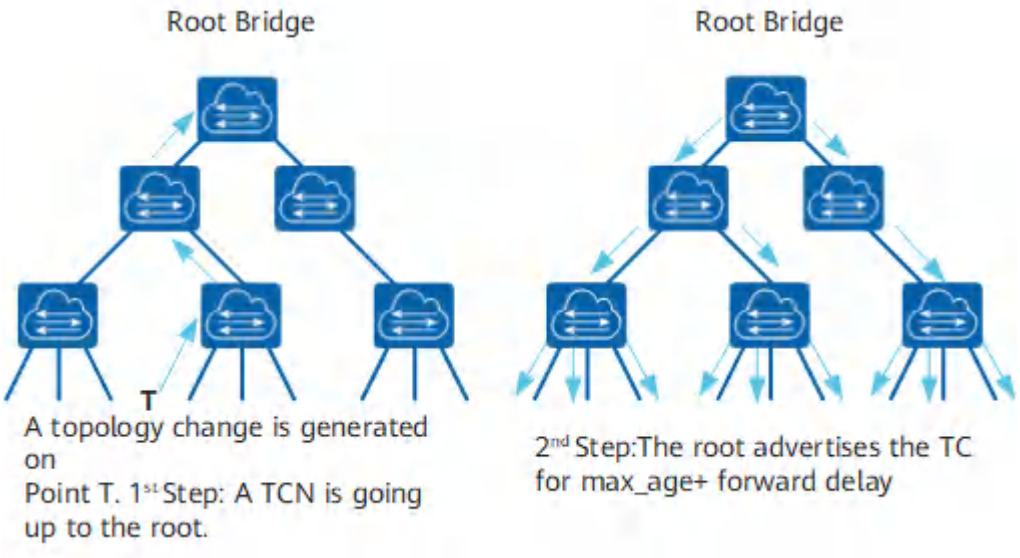
	的配置消息一样，于是将其丢弃。	
	DeviceC 比较 Port C1 的根路径开销 10（收到的配置消息中的根路径开销 0＋本端口所在链路的路径开销 10）与 Port C2 的根路径开销 9（收到的配置消息中的根路径开销 5＋本端口所在链路的路径开销 4），发现后者更小，因此 Port C2 的配置消息更优，于是 Port C2 被确定为根端口，其配置消息不变。 DeviceC 根据根端口的配置消息和路径开销，为 Port C1 计算出指定端口的配置消息<0，9，2，Port C1>，然后与 Port C1 本身的配置消息<0，0，0，Port A2>进行比较，发现本身的配置消息更优，于是 Port C1 被阻塞，其配置消息不变。从此，Port C1 不再转发数据，直至有触发生成树计算的新情况出现，譬如 DeviceB 与 DeviceC 之间的链路 down 掉。	阻塞端口 Port C1：<0，0，0，Port A2> 根端口 Port C2：<0，5，1，Port B2>

拓扑稳定后，根桥仍然按照 Hello Timer 规定的时间间隔发送配置 BPDU 报文，非根桥设备从根端口收到配置 BPDU 报文，通过指定端口转发。如果接收到的优先级比自己高的配置 BPDU，则非根桥设备会根据收到的配置 BPDU 中携带的信息更新自己相应的端口存储的配置 BPDU 信息。

STP 拓扑变化

STP 拓扑变化处理过程如下图所示。

图 12-10 TCN 的发送和 TC 的泛洪



在网络拓扑发生变化后，下游设备会不间断地向上游设备发送 TCN BPDU 报文。

上游设备收到下游设备发来的 TCN BPDU 报文后，只有指定端口处理 TCN BPDU 报文。其它端口也有可能收到 TCN BPDU 报文，但不会处理。

上游设备会把配置 BPDU 报文中的 Flags 的 TCA 位设置 1，然后发送给下游设备，告知下游设备停止发送 TCN BPDU 报文。

上游设备复制一份 TCN BPDU 报文，向根桥方向发送。

重复步骤 1、2、3、4，直到根桥收到 TCN BPDU 报文。
根桥把配置 BPDU 报文中的 Flags 的 TC 和 TCA 位置 1 后发送，通知下游设备直接删除桥 MAC 地址表项。

12.1.2. RSTP

12.1.2.1. 需求背景

IEEE 于 2001 年发布的 802.1w 标准定义了快速生成树协议 RSTP（Rapid Spanning Tree Protocol），该协议基于 STP 协议，对原有的 STP 协议进行了更加细致的修改和补充。

STP 的不足之处

STP 协议虽然能够解决环路问题，但是由于网络拓扑收敛慢，影响了用户通信质量。如果网络中的拓扑结构频繁变化，网络也会随之频繁失去连通性，从而导致用户通信频繁中断，这是用户无法忍受的。

STP 的不足之处如下：

1. STP 没有细致区分端口状态和端口角色，不利于初学者学习及部署。

网络协议的优劣往往取决于协议是否对各种情况加以细致区分。

从用户角度来讲，Listening、Learning 和 Blocking 状态并没有区别，都同样不转发用户流量。

从使用和配置角度来讲，端口之间最本质的区别并不在于端口状态，而是在于端口扮演的角色。

根端口和指定端口可以都处于 Listening 状态，也可能都处于 Forwarding 状态。

2. STP 算法是被动的算法，依赖定时器等待的方式判断拓扑变化，收敛速度慢。

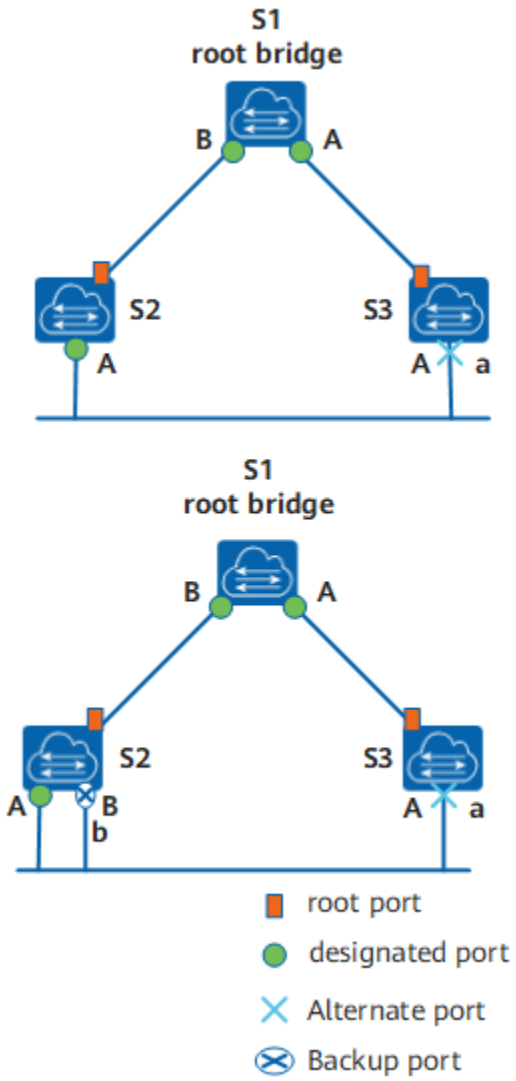
STP 算法要求在稳定的拓扑中，根桥主动发出配置 BPDU 报文，而其他设备进行处理，传遍整个 STP 网络。这也是导致拓扑收敛慢的主要原因之一。

RSTP 对 STP 的改进

根据 STP 的不足，RSTP 删除了 3 种端口状态，新增加了 2 种端口角色，并且把端口属性充分的按照状态和角色解耦；此外，RSTP 还增加了相应的一些增强特性和保护措施，实现网络的稳定和快速收敛。

通过端口角色的增补，简化了生成树协议的理解及部署。

图 12-11 端口角色示意图



如上图所示，RSTP 的端口角色共有 4 种：根端口、指定端口、Alternate 端口和 Backup 端口。

根端口和指定端口的作用同 STP 协议中定义，Alternate 端口和 Backup 端口的描述如下：

从配置 BPDU 报文发送角度来看：

Alternate 端口就是由于学习到其它网桥发送的配置 BPDU 报文而阻塞的端口。

Backup 端口就是由于学习到自己发送的配置 BPDU 报文而阻塞的端口。

从用户流量角度来看：

Alternate 端口提供了从指定桥到根的另一条可切换路径，作为根端口的备份端口。

Backup 端口作为指定端口的备份，提供了另一条从根桥到相应网段的备份通路。

给一个 RSTP 域内所有端口分配角色的过程就是整个拓扑收敛的过程。

端口状态的重新划分

RSTP 的状态规范把原来的 5 种状态缩减为 3 种。根据端口是否转发用户流量和学习 MAC 地址来划分:

如果不转发用户流量也不学习 MAC 地址，那么端口状态就是 Discarding 状态。

如果不转发用户流量但是学习 MAC 地址，那么端口状态就是 Learning 状态。

如果既转发用户流量又学习 MAC 地址，那么端口状态就是 Forwarding 状态。

如表 12-9 所示，新的端口状态与 STP 规定的端口状态比较。端口状态和端口角色是没有必然联系的，表中显示了各种端口角色能够具有的端口状态。

表 12-9 STP 与 RSTP 端口状态角色对应表

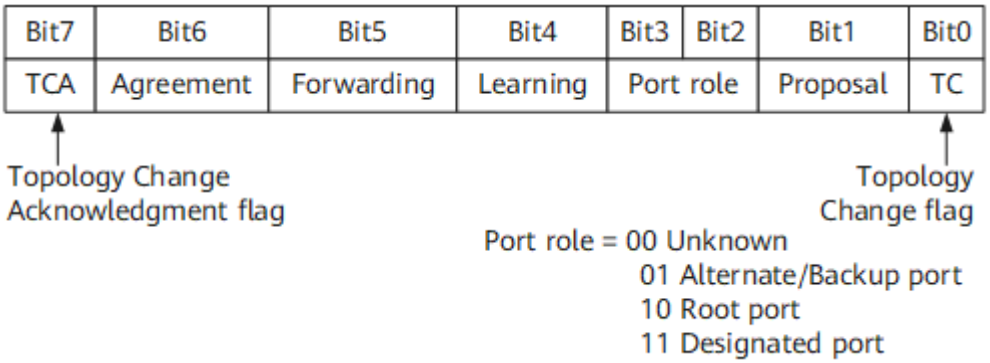
STP 端口状态	RSTP 端口状态	端口在拓扑中的角色
Forwarding	Forwarding	包括根端口、指定端口
Learning	Learning	包括根端口、指定端口
Listening	Discarding	包括根端口、指定端口
Blocking	Discarding	包括 Alternate 端口、Backup 端口
Disabled	Discarding	包括 Disable 端口

配置 BPDU 格式的改变，充分利用了 STP 协议报文中的 Flag 字段，明确了端口角色。

在配置 BPDU 报文的格式上，除了保证和 STP 格式基本一致之外，RSTP 作了一些小变化：Type 字段，配置 BPDU 类型不再是 0 而是 2，所以运行 STP 的设备收到 RSTP 的配置 BPDU 时会丢弃。

Flags 字段，使用了原来保留的中间 6 位，这样改变的配置 BPDU 叫做 RST BPDU，如下图所示。

图 12-12 RSTP Flag 字段格式



- **配置 BPDU 的处理发生变化**
  - 拓扑稳定后，配置 BPDU 报文的发送方式

拓扑稳定后，根桥按照 Hello Timer 规定的时间间隔发送配置 BPDU。其他非根桥设备在收到上游设备发送过来的配置 BPDU 后，才会触发发出配置 BPDU，此方式使得 STP 协议计算复杂且缓慢。RSTP 对此进行了改进，即在拓扑稳定后，无论非根桥设备是否接收到根桥传来的配置 BPDU 报文，非根桥设备仍然按照 Hello Timer 规定的时间间隔发送配置 BPDU，该行为完全由每台设备自主进行。

  - 更短的 BPDU 超时计时

如果一个端口连续 3 个 Hello Time 时间内没有收到上游设备发送过来的配置 BPDU，那么该设备认为与此邻居之间的协商失败。而不像 STP 那样需要先等待一个 Max Age。

  - 处理次等 BPDU

当一个端口收到上游的指定桥发来的 RST BPDU 报文时，该端口会将自身存储的 RST BPDU 与收到的 RST BPDU 进行比较。

如果该端口存储的 RST BPDU 的优先级高于收到的 RST BPDU，那么该端口会直接丢弃收到的 RST BPDU，立即回应自身存储的 RST BPDU。当上游设备收到下游设备回应的 RST BPDU 后，上游设备会根据收到的 RST BPDU 报文中相应的字段立即更新自己存储的 RST BPDU。

由此，RSTP 处理次等 BPDU 报文不再依赖于任何定时器通过超时解决拓扑收敛，从而加快了拓扑收敛。

- 快速收敛
  - Proposal/Agreement 机制

当一个端口被选举成为指定端口之后，在 STP 中，该端口至少要等待一个 Forward Delay（Learning）时间才会迁移到 Forwarding 状态。而在 RSTP 中，此端口会先进入 Discarding 状态，再通过 Proposal/Agreement 机制快速进入 Forward 状态。这种机制必须在点到点全双工链路上使用。

Proposal/Agreement 机制简称 P/A 机制。

  - 根端口快速切换机制

如果网络中一个根端口失效，那么网络中最优的 Alternate 端口将成为根端口，进入 Forwarding 状态。因为通过这个 Alternate 端口连接的网段上必然有个指定端口可以通往根桥。

  - 边缘端口的引入

在 RSTP 里面，如果某一个指定端口位于整个网络的边缘，即不再与其他交换设备连接，而是直接与终端设备直连，这种端口叫做边缘端口。

边缘端口不接收处理配置 BPDU，不参与 RSTP 运算，可以由 Disable 直接转到 Forwarding 状态，且不经历时延，就像在端口上将 STP 禁用。但是一旦边缘端口收到配置 BPDU，就丧失了边缘端口属性，成为普通 STP 端口，并重新进行生成树计算，从而引起网络震荡。

- 保护功能

RSTP 提供的保护功能如下表所示。

表 12-10 保护功能

保护功能	场景	原理
BPDU 保护	在交换设备上，通常将直接与用户终端（如 PC 机）或文件服务器等非交换设备相连的端口配置为边缘端口。 正常情况下，边缘端口不会收到 RST BPDU。如果有人伪造 RST BPDU 恶意攻击交换设备，当边缘端口接收到 RST BPDU 时，交换设备会自动将边缘端口设置为非边缘端口，并重新进行生成树计算，从而引起网络震荡。	交换设备上启动了 BPDU 保护功能后，如果边缘端口收到 RST BPDU，边缘端口将被 error-down，但是边缘端口属性不变，同时通知网管系统。
根保护	由于维护人员的错误配置或网络中的恶意攻击，网络中合法根桥有可能会收到优先级更高的 RST BPDU，使得合法根桥失去根地位，从而引起网络拓扑结构的错误变动。这种不合法的拓扑变化，会导致原来应该通过高速链路的流量被牵	对于启用 Root 保护功能的指定端口，其端口角色只能保持为指定端口。一旦启用 Root 保护功能的指定端口收到优先级更高的 RST BPDU 时，端口状态将进入 Discarding 状态，不再转发报文。在经过一段时间（通常为两倍的 Forward Delay），如果端口一直没有再收到优先级较高

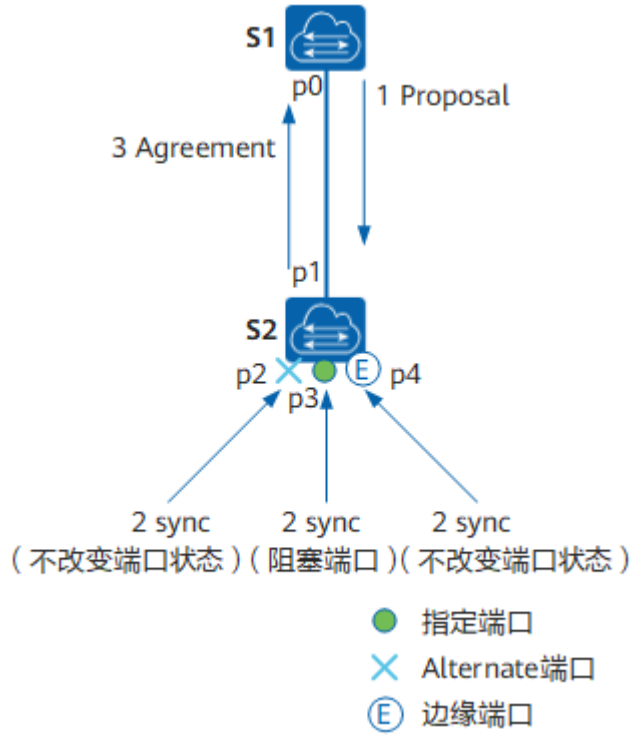
	引到低速链路上，造成网络拥塞。	的 RST BPDU，端口会自动恢复到正常的 Forwarding 状态。 说明: Root 保护功能只能在指定端口上配置生效。

12.1.2.2. 技术原理

Proposal/Agreement 机制

其目的是使一个指定端口尽快进入 Forwarding 状态。如下图所示，根桥 S1 和 S2 之间新添加了一条链路。在当前状态下，S2 的另外几个端口 p2 是 Alternate 端口，p3 是指定端口且处于 Forwarding 状态，p4 是边缘端口。

图 12-13 Proposal/Agreement 过程示意图



新链路连接成功后，P/A 机制协商过程如下:

1. p0 和 p1 两个端口马上都先成为指定端口，发送 RST BPDU。
2. S2 的 p1 口收到更优的 RST BPDU，马上意识到自己将成为根端口，而不是指定端口，停止发送 RST BPDU。
3. S1 的 p0 进入 Discarding 状态，于是发送的 RST BPDU 中把 proposal 置 1。
4. S2 收到根桥发送来的携带 proposal 的 RST BPDU，开始将自己的所有端口进入 sync 变量置位。
5. p2 已经阻塞，状态不变；p4 是边缘端口，不参与运算；所以只需要阻塞非边缘指定端口 p3。
6. p2 和 p3 都进入 Discarding 状态之后，端口的 synced 变量置位，根端口 p1 的 synced 也置位，于是便向 S1 返回 Agreement 位置位的回应 RST BPDU。该 RST BPDU 携带和刚才根桥发过来的 BPDU 一样的信息，除了 Agreement 位置位之外（Proposal 位清零）。

7. 当 S1 判断出这是对刚刚发出的 Proposal 的回应，于是端口 p0 马上进入 Forwarding 状态。下游设备继续执行 P/A 协商过程。

事实上对于 STP，指定端口的选择可以很快完成，主要的速度瓶颈在于：为了避免环路，必须等待足够长的时间，使全网的端口状态全部确定，也就是说必须要等待至少一个 Forward Delay 所有端口才能进行转发。而 RSTP 的主要目的就是消除这个瓶颈，通过阻塞自己的非根端口来保证不会出现环路。而使用 P/A 机制加快了上游端口转到 Forwarding 状态的速度。

RSTP 拓扑变化处理

在 RSTP 中检测拓扑是否发生变化只有一个标准：一个非边缘端口迁移到 Forwarding 状态。一旦检测到拓扑发生变化，将进行如下处理：

为本交换设备的所有非边缘指定端口启动一个 TC While Timer，该计时器值是 Hello Time 的两倍。

在这个时间内，清空所有端口上学习到的 MAC 地址。

同时，由非边缘端口向外发送 RST BPDU，其中 TC 置位。一旦 TC While Timer 超时，则停止发送 RST BPDU。

其他交换设备接收到 RST BPDU 后，清空所有端口学习到 MAC 地址，除了收到 RST BPDU 的端口。然后也为自己所有的非边缘指定端口和根端口启动 TC While Timer，重复上述过程。

如此，网络中就会产生 RST BPDU 的泛洪。

RSTP 与 STP 的互操作

RSTP 可以和 STP 互操作，但是此时会丧失快速收敛等 RSTP 优势。

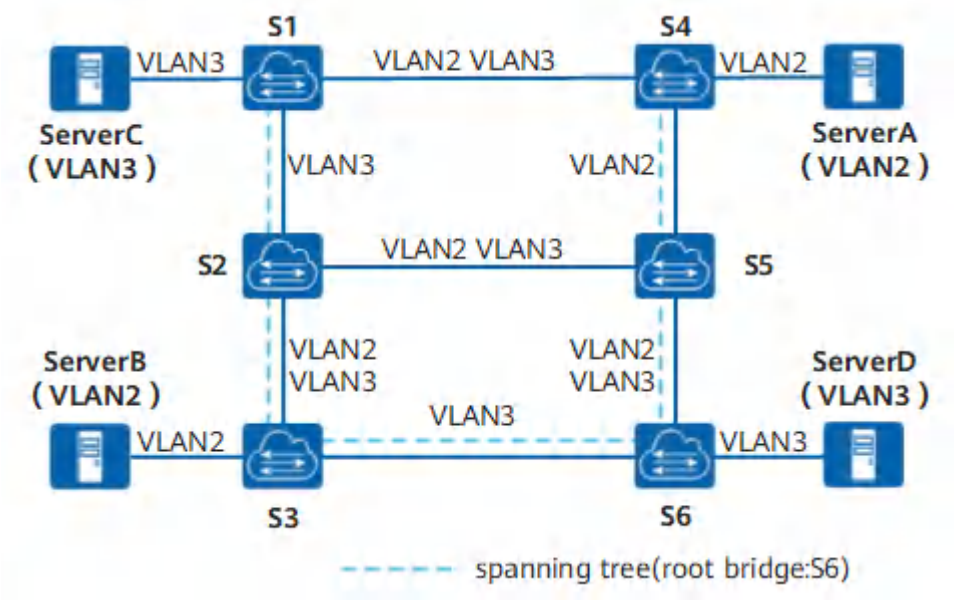
当一个网段里既有运行 STP 的交换设备又有运行 RSTP 的交换设备，STP 交换设备会忽略 RSTP BPDU。运行 RSTP 的交换设备在某端口上接收到运行 STP 的交换设备发出的配置 BPDU，在两个 Hello Time 时间之后，便把自己的端口转换到 STP 工作模式，发送配置 BPDU，从而实现了互操作。

12.1.3. MSTP

12.1.3.1. 需求背景

RSTP 在 STP 基础上进行了改进，实现了网络拓扑快速收敛。但 RSTP 和 STP 还存在同一个缺陷：由于局域网内所有的 VLAN 共享一棵生成树，因此无法在 VLAN 间实现数据流量的负载均衡，链路被阻塞后将不承载任何流量，造成带宽浪费，还有可能造成部分 VLAN 的报文无法转发。

图 12-14 STP/RSTP 的缺陷示意图



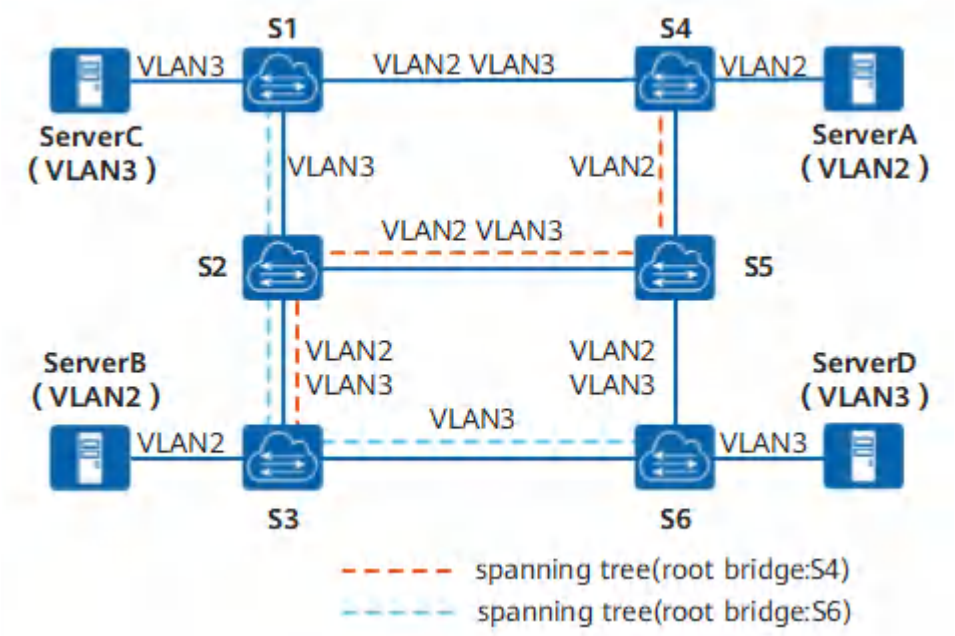
如上图所示网络中，在局域网内应用 STP 或 RSTP，生成树结构在图中用虚线表示，S6 为根交换设备。S2 和 S5 之间、S1 和 S4 之间的链路被阻塞，除了图中标注了“VLAN2”或“VLAN3”的链路允许对应的 VLAN 报文通过外，其它链路均不允许 VLAN2、VLAN3 的报文通过。

ServerA 和 ServerB 同属于 VLAN2，由于 S2 和 S5 之间的链路被阻塞，S3 和 S6 之间的链路又不允许 VLAN2 的报文通过，因此 ServerA 和 ServerB 之间无法互相通讯。

为了弥补 STP 和 RSTP 的缺陷，IEEE 于 2002 年发布的 802.1S 标准定义了 MSTP。MSTP 兼容 STP 和 RSTP，既可以快速收敛，又提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。

通过 MSTP 把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立。每棵生成树叫做一个多生成树实例 MSTI（Multiple Spanning Tree Instance），每个域叫做一个 MST 域（MST Region：Multiple Spanning Tree Region）。

图 12-15 MST 域内的多棵生成树示意图



如上图所示，MSTP 通过设置 VLAN 映射表（即 VLAN 和 MSTI 的对应关系表），把 VLAN 和 MSTI 联系起来。每个 VLAN 只能对应一个 MSTI，即同一 VLAN 的数据只能在一个 MSTI 中传输，而一个 MSTI 可能对应多个 VLAN。

经计算，最终生成两棵生成树：

MSTI1 以 S4 为根交换设备，转发 VLAN2 的报文。

MSTI2 以 S6 为根交换设备，转发 VLAN3 的报文。

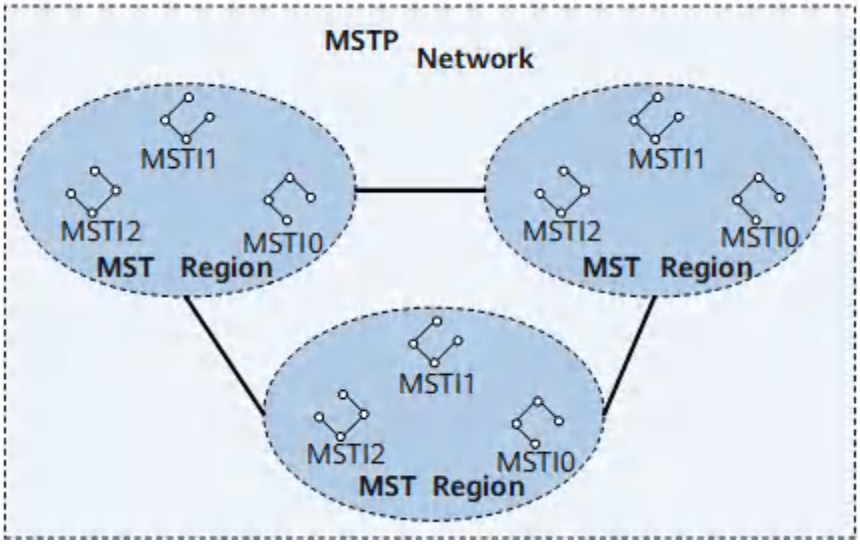
这样所有 VLAN 内部可以互通，同时不同 VLAN 的报文沿不同的路径转发，实现了负载分担。

12.1.3.2. 基本概念

MSTP 网络

如下图所示，MSTP 网络中包含 1 个或多个 MST 域（MST Region），每个 MST Region 中包含一个或多个 MSTI。组成 MSTI 的是运行 STP/RSTP/MSTP 的交换设备，MSTI 是所有运行 STP/RSTP/MSTP 的交换设备经 MSTP 协议计算后形成的树状网络。

图 12-16 MSTP 网络示意图



MST 域（MST Region）

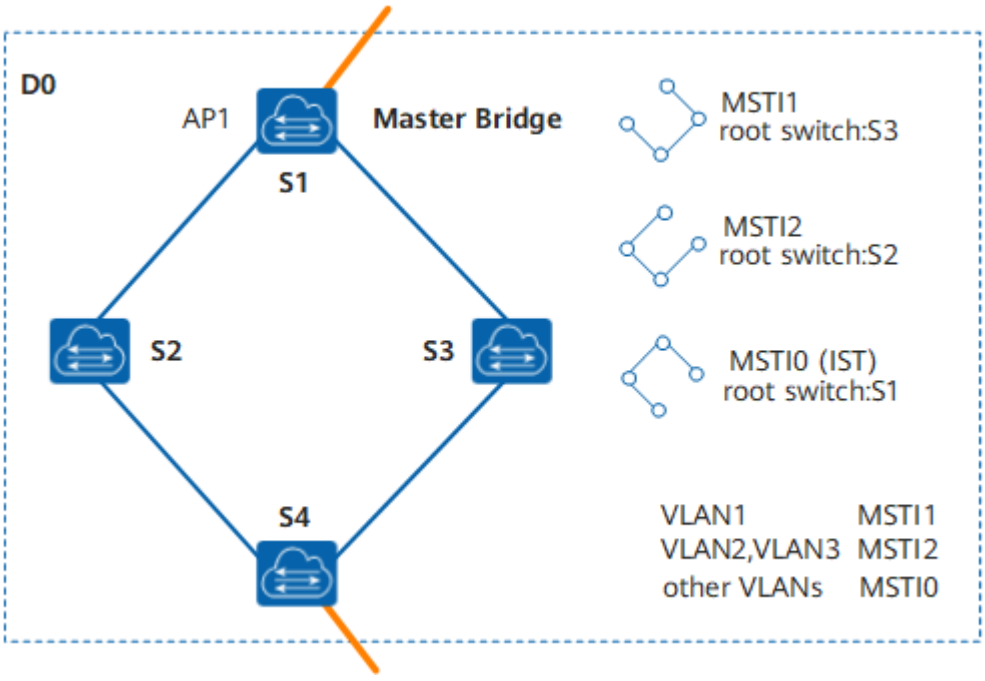
MST 域是多生成树域（Multiple Spanning Tree Region），由交换网络中的多台交换设备以及它们之间的网段所构成。同一个 MST 域的设备具有下列特点：

- 都启动了 MSTP。
- 具有相同的域名。
- 具有相同的 VLAN 到生成树实例映射配置。
- 具有相同的 MSTP 修订级别配置。

一个局域网可以存在多个 MST 域，各 MST 域之间在物理上直接或间接相连。用户可以通过 MSTP 配置命令把多台交换设备划分在同一个 MST 域内。

如下图所示的 MST Region D0 中由交换设备 S1、S2、S3 和 S4 构成，域中有 3 个 MSTI。

图 12-17 MST Region 的基本概念示意图



VLAN 映射表

VLAN 映射表是 MST 域的属性，它描述了 VLAN 和 MSTI 之间的映射关系。

如上图所示，MST 域 D0 的 VLAN 映射表是:

VLAN1 映射到 MSTI1

VLAN2 和 VLAN3 映射到 MSTI2

其余 VLAN 映射到 MSTI0

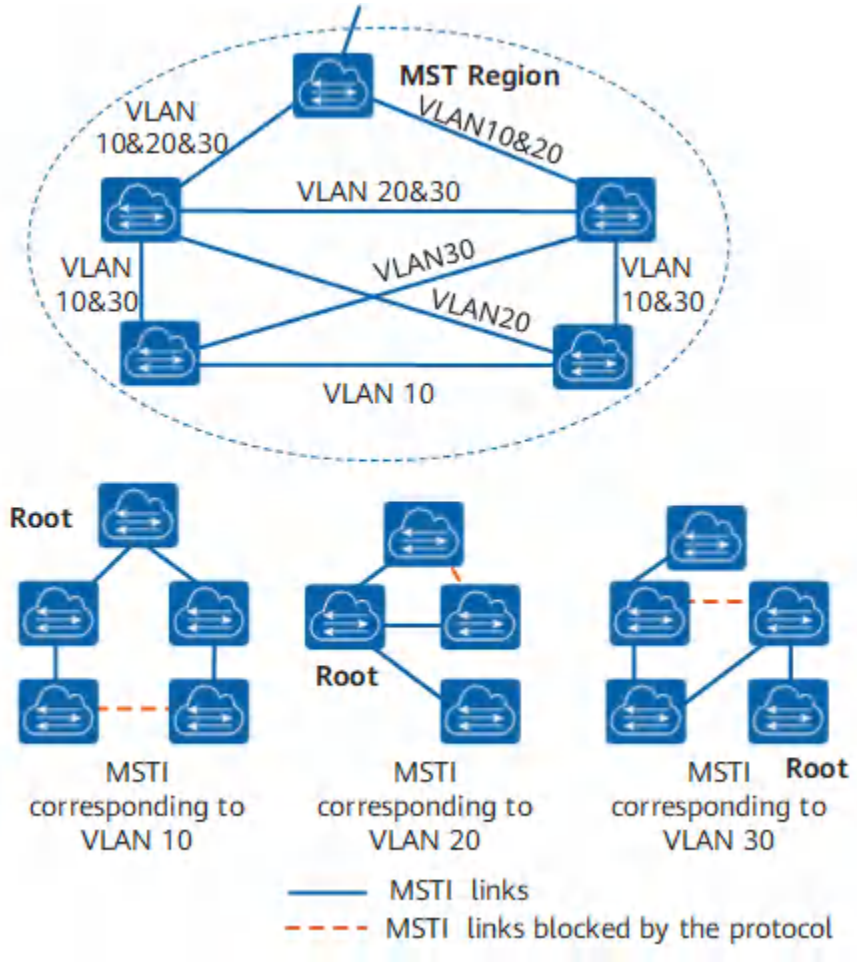
域根

域根（Regional Root）分为 IST（Internal Spanning Tree）域根和 MSTI 域根。

IST 域根如图 12-19 所示，在 B0、C0 和 D0 中，IST 生成树中距离总根（CIST Root）最近的交换设备是 IST 域根。

一个 MST 域内可以生成多棵生成树，每棵生成树都称为一个 MSTI。MSTI 域根是每个多生成树实例的树根。如图 12-18 所示，域中不同的 MSTI 有各自的域根。

图 12-18 MSTI 的基本概念示意图



MSTI 之间彼此独立，MSTI 可以与一个或者多个 VLAN 对应。但一个 VLAN 只能与一个 MSTI 对应。

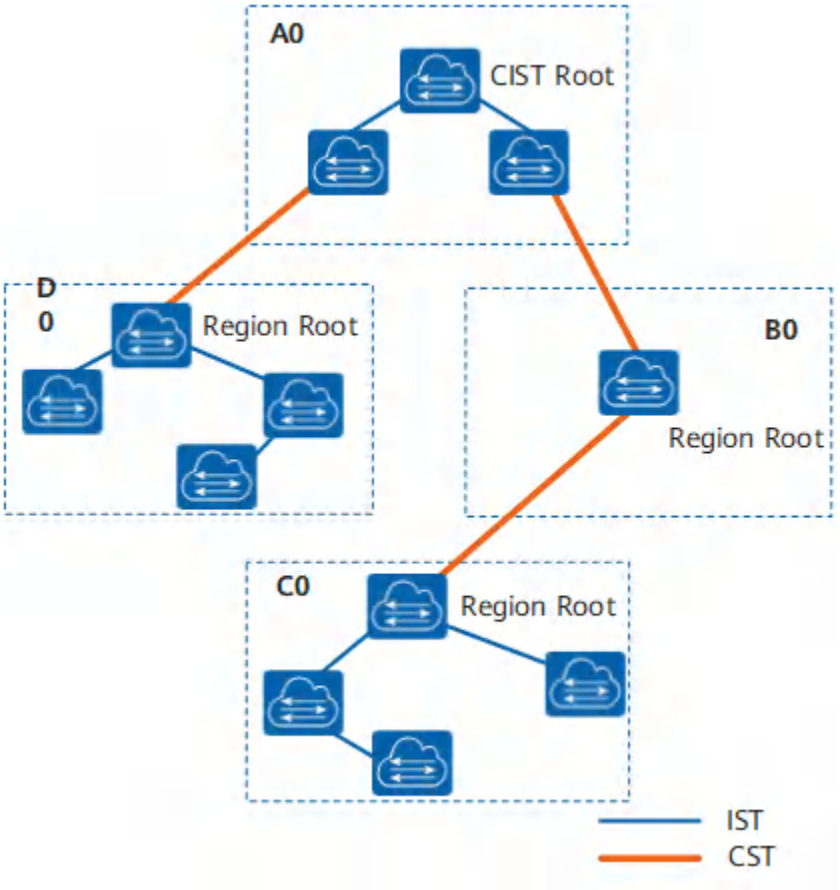
主桥

主桥（Master Bridge）也就是 IST Master，它是域内距离总根最近的交换设备。如图 12-17 中的 S1。

如果总根在 MST 域中，则总根为该域的主桥。

总根

图 12-19 MSTP 网络基本概念示意图



如上图所示，总根是 CIST（Common and Internal Spanning Tree）的根桥。总根是区域 A0 中的某台设备。

CST

公共生成树 CST（Common Spanning Tree）是连接交换网络内所有 MST 域的一棵生成树。如果把每个 MST 域看作是一个节点，CST 就是这些节点通过 STP 或 RSTP 协议计算生成的一棵生成树。

如图 12-19 所示，较粗的线条连接各个域构成 CST。

IST

内部生成树 IST（Internal Spanning Tree）是各 MST 域内的一棵生成树。

IST 是一个特殊的 MSTI，MSTI 的 ID 为 0，通常称为 MSTI0。

IST 是 CIST 在 MST 域中的一个片段。

如图 12-19 所示，较细的线条在域中连接该域的所有交换设备构成 IST。

CIST

公共和内部生成树 CIST 是通过 STP 或 RSTP 协议计算生成的，连接一个交换网络内所有交换设备的单生成树。

如图 12-19 所示，所有 MST 域的 IST 加上 CST 就构成一棵完整的生成树，即 CIST。

SST

构成单生成树 SST（Single Spanning Tree）有两种情况：

运行 STP 或 RSTP 的交换设备只能属于一个生成树。

MST 域中只有一个交换设备，这个交换设备构成单生成树。

如图 12-19 所示，B0 中的交换设备就是一棵单生成树。

端口角色

MSTP 在 RSTP 的基础上新增了 2 种端口，MSTP 的端口角色共有 7 种：根端口、指定端口、Alternate 端口、Backup 端口、边缘端口、Master 端口和域边缘端口。

根端口、指定端口、Alternate 端口、Backup 端口和边缘端口的作用同 RSTP 协议中定义，MSTP 中定义的所有端口角色如下表所示。

表 12-11 端口角色

端口角色	说明
根端口	在非根桥上，离根桥最近的端口是本交换设备的根端口。根交换设备没有根端口。 根端口负责向树根方向转发数据。 如图 12-20 所示，S1 为根桥，CP1 为 S3 的根端口，BP1 为 S2 的根端口。
指定端口	对一台交换设备而言，它的指定端口是向下游交换设备转发 BPDU 报文的端口。 如图 12-20 所示，AP2 和 AP3 为 S1 的指定端口，CP2 为 S3 的指定端口。
Alternate 端口	从配置 BPDU 报文发送角度来看，Alternate 端口就是由于学习到其它网桥发送的配置 BPDU 报文而阻塞的端口。 从用户流量角度来看，Alternate 端口提供了从指定桥到根的另一条可切换路径，作为根端口的备份端口。 如图 12-20 所示，BP2 为 Alternate 端口。
Backup 端口	从配置 BPDU 报文发送角度来看，Backup 端口就是由于学习到自己发送的配置 BPDU 报文而阻塞的端口。 从用户流量角度来看，Backup 端口作为指定端口的备份，提供了另外一条从根节点到叶节点的备份通路。 如图 12-20 所示，CP3 为 Backup 端口。
Master 端口	Master 端口是 MST 域和总根相连的所有路径中最短路径上的端口，它是交换设备上连接 MST 域到总根的端口。 Master 端口是域中的报文去往总根的必经之路。 Master 端口是特殊域边缘端口，Master 端口在 CIST 上的角色是 Root Port，在其它各实例上的角色都是 Master 端口。 如图 12-21 所示，交换设备 S1、S2、S3、S4 和它们之间的链路构成一个 MST 域，S1 交换设备的端口 AP1 在域内的所有端口中到总根的路径开销最小，所以 AP1 为 Master 端口。
域边缘端口	域边缘端口是指位于 MST 域的边缘并连接其它 MST 域或 SST 的端口。 进行 MSTP 计算时，域边缘端口在 MSTI 上的角色和 CIST 实例的角色保持一致。即如果边缘端口在 CIST 实例上的角色是 Master 端口（域和总根相连的所有路径中最短路径上的端口），则它在域内所有 MSTI 上的角色也是 Master 端口。 如图 12-21 所示，MST 域内的 AP1、DP1 和 DP2 都和其它域直接相连，它们都是本 MST 域的域边缘端口。 域边缘端口在生成树实例上的角色与在 CIST 的角色保持一致。如图 12-21，AP1 是域边缘端口，它在 CIST 上的角色是 Master 端口，则 AP1 在 MST 域内所有生成树实例上的角色都是 Master 端口。

边缘端口	如果指定端口位于整个域的边缘，不再与任何交换设备连接，这种端口叫做边缘端口。 边缘端口一般与用户终端设备直接连接。 端口使能 MSTP 功能后，会默认启用边缘端口自动探测功能，当端口在（2 × Hello Timer + 1）秒的时间内收不到 BPDU 报文，自动将端口设置为边缘端口，否则设置为非边缘端口。

图 12-20 根端口、指定端口、Alternate 端口和 Backup 端口示意图

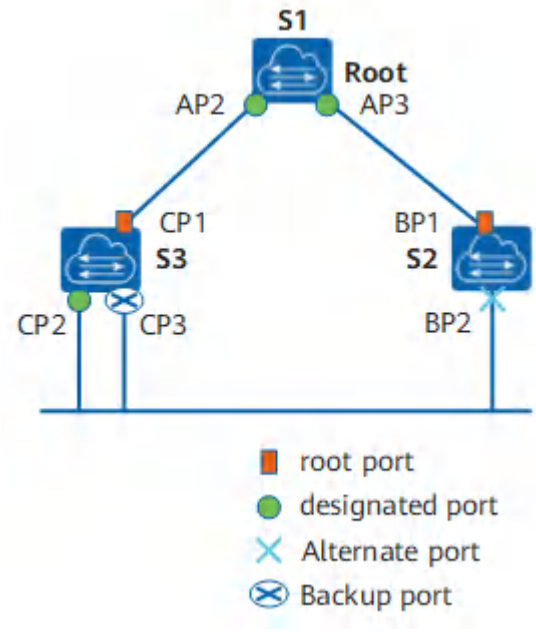
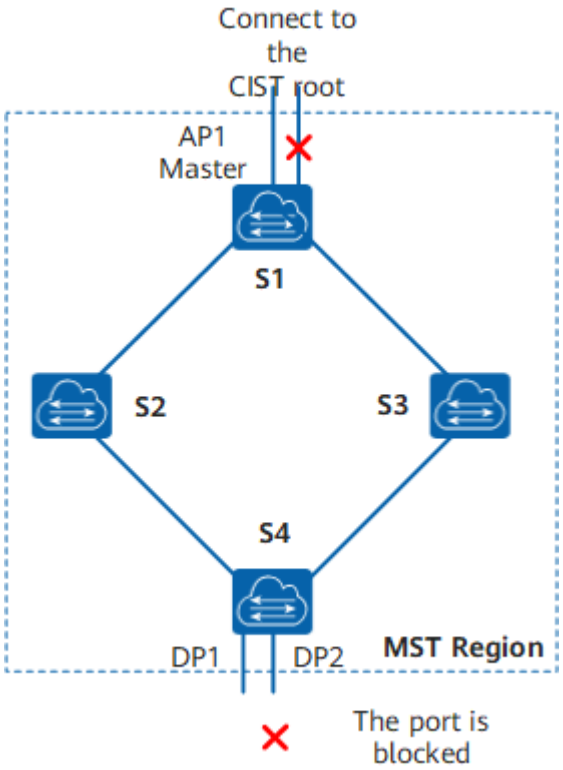


图 12-21 Master 端口和域边缘端口示意图



MSTP 的端口状态

MSTP 定义的端口状态与 RSTP 协议中定义相同，如下表所示。

表 12-12 端口状态

端口状态	说明
Forwarding	在这种状态下，端口既转发用户流量又接收/发送 BPDU 报文。
Learning	这是一种过渡状态。在 Learning 下，交换设备会根据收到的用户流量，构建 MAC 地址表，但不转发用户流量，所以叫做学习状态。Learning 状态的端口接收/发送 BPDU 报文，不转发用户流量。
Discarding	Discarding 状态的端口只接收 BPDU 报文。

端口状态和端口角色是没有必然联系的，下表显示了各种端口角色能够具有的端口状态。

表 12-13 端口状态和端口角色对应表

端口状态	根端口/Master 端口	指定端口	域边缘端口	Alternate 端口	Backup 端口
Forwarding	Yes	Yes	Yes	No	No
Learning	Yes	Yes	Yes	No	No
Discarding	Yes	Yes	Yes	Yes	Yes

Yes：表示端口支持的状态。No：表示端口不支持的状态。

12.1.3.3. 报文格式

MSTP 使用多生成树桥协议数据单元 MST BPDU（Multiple Spanning Tree Bridge Protocol Data Unit）作为生成树计算的依据。MST BPDU 报文用来计算生成树的拓扑、维护网络拓扑以及传达拓扑变化记录。

STP 中定义的配置 BPDU、RSTP 中定义的 RST BPDU、MSTP 中定义的 MST BPDU 及 TCN BPDU 差异对比如下表所示。

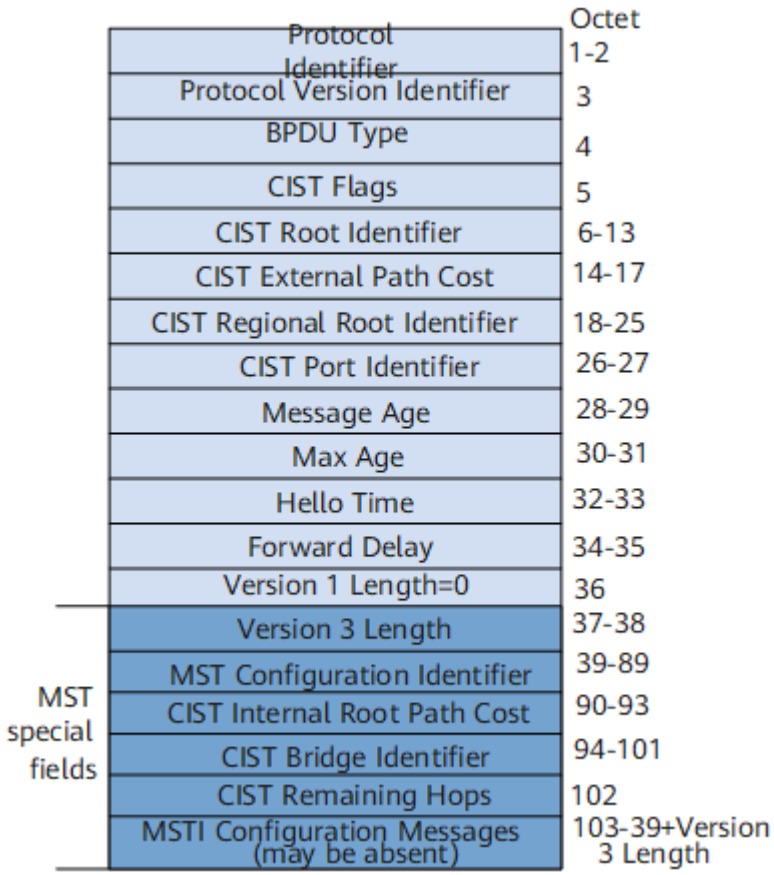
表 12-14 四种 BPDU 差异比较

版本	类型	名称
0	0x00	配置 BPDU
0	0x80	TCN BPDU
2	0x02	RST BPDU
3	0x02	MST BPDU

MSTP 报文格式

MST BPDU 报文结构如下图所示。

图 12-22 MST BPDU 报文结构



无论是域内的 MST BPDU 还是域间的，前 36 个字节和 RST BPDU 相同。

从第 37 个字节开始是 MSTP 专有字段。最后的 MSTI 配置信息字段由若干 MSTI 配置信息组连缀而成。

MST BPDU 中的主要信息如下表所示。

表 12-15 MST BPDU 中主要信息说明

字段内容	字节	说明
Protocol Identifier	2	协议标识符。
Protocol Version Identifier	1	协议版本标识符，STP 为 0，RSTP 为 2，MSTP 为 3。
BPDU Type	1	BPDU 类型： 0x00：STP 的 Configuration BPDU 0x80：STP 的 TCN BPDU（Topology Change Notification BPDU） 0x02：RST BPDU（Rapid Spanning-Tree BPDU）或者 MST BPDU（Multiple Spanning-Tree BPDU）
CIST Flags	1	CIST 标志字段。
CIST Root Identifier	8	CIST 的总根交换设备 ID。
CIST External	4	CIST 外部路径开销指从本交换设备所属的 MST

Path Cost		域到 CIST 根交换设备所属的 MST 域的累计路径开销。CIST 外部路径开销根据链路带宽计算。
CIST Regional Root Identifier	8	CIST 的域根交换设备 ID，即 IST Master 的 ID。如果总根在这个域内，那么域根交换设备 ID 就是总根交换设备 ID。
CIST Port Identifier	2	本端口在 IST 中的指定端口 ID。
Message Age	2	BPDU 报文的生存期。
Max Age	2	BPDU 报文的最大生存期，超时则认为到根交换设备的链路故障。
Hello Time	2	Hello 定时器，缺省为 2 秒。
Forward Delay	2	Forward Delay 定时器，缺省为 15 秒。
Version 1 Length	1	Version1 BPDU 的长度，值固定为 0。
Version 3 Length	2	Version3 BPDU 的长度。
MST Configuration Identifier	51	MST 配置标识，表示 MST 域的标签信息，包含 4 个字段。
CIST Internal Root Path Cost	4	CIST 内部路径开销指从本端口到 IST Master 交换设备的累计路径开销。CIST 内部路径开销根据链路带宽计算。
CIST Bridge Identifier	8	CIST 的指定交换设备 ID。
CIST Remaining Hops	1	BPDU 报文在 CIST 中的剩余跳数。
MSTI Configuration Messages(may be absent)	16	MSTI 配置信息。每个 MSTI 的配置信息占 16 bytes，如果有 n 个 MSTI 就占用 n×16bytes。

每个 Hello Time 时间内端口最多能发送 BPDU 的报文数可配置

Hello Time 用于生成树协议定时发送配置消息维护生成树的稳定。如果交换设备在一段时间内没有收到 BPDU 报文，则会由于消息超时而对生成树进行重新计算。

当交换设备成为根交换设备时，该交换设备会按照该设置值为时间间隔发送 BPDU 报文。非根交换设备采用根交换设备所设置的 Hello Time 时间值。

12.1.3.4. 拓扑计算

MSTP 的基本原理

MSTP 可以将整个二层网络划分为多个 MST 域，各个域之间通过计算生成 CST。域内则通过计算生成多棵生成树，每棵生成树都被称为是一个多生成树实例。其中实例 0 被称为 IST，其他的多生成树实例为 MSTI。MSTP 同 STP 一样，使用配置消息进行生成树的计算，只是配置消息中携带的是设备上 MSTP 的配置信息。

优先级向量

MSTI 和 CIST 都是根据优先级向量来计算的，这些优先级向量信息都包含在 MST BPDU 中。各交换设备互相交换 MST BPDU 来生成 MSTI 和 CIST。

- 优先级向量简介

参与 CIST 计算的优先级向量为：
< 根交换设备 ID，外部路径开销，域根 ID，内部路径开销，指定交换设备 ID，指定端口 ID，接收端口 ID >
参与 MSTI 计算的优先级向量为：
< 域根 ID，内部路径开销，指定交换设备 ID，指定端口 ID，接收端口 ID >
括号中的向量的优先级从左到右依次递减。
下表对每个优先级向量进行解释。

表 12-16 向量说明

向量名	说明
根交换设备 ID	根交换设备 ID 用于选择 CIST 中的根交换设备。根交换设备 ID = Priority(16bits) + MAC(48bits)。 其中 Priority 为 MSTI0 的优先级。
外部路径开销（ERPC）	从 CIST 的域根到达总根的路径开销。MST 域内所有交换设备上保存的外部路径开销相同。若 CIST 根交换设备在域中，则域内所有交换设备上保存的外部路径开销为 0。
域根 ID	域根 ID 用于选择 MSTI 中的域根。域根 ID = Priority(16bits) + MAC(48bits)。 其中 Priority 为 MSTI0 的优先级。
内部路径开销（IRPC）	本桥到达域根的路径开销。域边缘端口保存的内部路径开销大于非域边缘端口保存的内部路径开销。
指定交换设备 ID	CIST 或 MSTI 实例的指定交换设备是本桥通往域根的最邻近的上游桥。如果本桥就是总根或域根，则指定交换设备为自己。
指定端口 ID	指定交换设备上同本设备上根端口相连的端口。Port ID = Priority(4 位) + 端口号（12 位）。端口优先级必须是 16 的整数倍。
接收端口 ID	接收到 BPDU 报文的端口。Port ID = Priority(4 位) + 端口号（12 位）。端口优先级必须是 16 的整数倍。

- 比较原则

同一向量比较，值最小的向量具有最高优先级。
优先级向量比较原则如下。
首先，比较根交换设备 ID。
如果根交换设备 ID 相同，再比较外部路径开销。
如果外部路径开销相同，再比较域根 ID。
如果域根 ID 仍然相同，再比较内部路径开销。
如果内部路径仍然相同，再比较指定交换设备 ID。
如果指定交换设备 ID 仍然相同，再比较指定端口 ID。
如果指定端口 ID 还相同，再比较接收端口 ID。
如果端口接收到的 BPDU 内包含的配置消息优于端口上保存的配置消息，则端口上原来保存的配置消息被新收到的配置消息替代。端口同时更新交换设备保存的全局配置消息。反之，新收到的 BPDU 被丢弃。

- CIST 的计算

经过比较配置消息后，在整个网络中选择一个优先级最高的交换设备作为 CIST 的树根。在每个 MST 域内 MSTP 通过计算生成 IST；同时 MSTP 将每个 MST 域作为单台交换设备对待，

通过计算在 MST 域间生成 CST。CST 和 IST 构成了整个交换设备网络的 CIST。

- MSTI 的计算

在 MST 域内，MSTP 根据 VLAN 和生成树实例的映射关系，针对不同的 VLAN 生成不同的生成树实例。每棵生成树独立进行计算，计算过程与 STP 计算生成树的过程类似。

MSTI 的特点：

每个 MSTI 独立计算自己的生成树，互不干扰。

每个 MSTI 的生成树计算方法与 STP 基本相同。

每个 MSTI 的生成树可以有不同的根，不同的拓扑。

每个 MSTI 在自己的生成树内发送 BPDU。

每个 MSTI 的拓扑通过命令配置决定。

每个端口在不同 MSTI 上的生成树参数可以不同。

每个端口在不同 MSTI 上的角色、状态可以不同。

在运行 MSTP 协议的网络中，一个 VLAN 报文将沿着如下路径进行转发：

在 MST 域内，沿着其对应的 MSTI 转发。

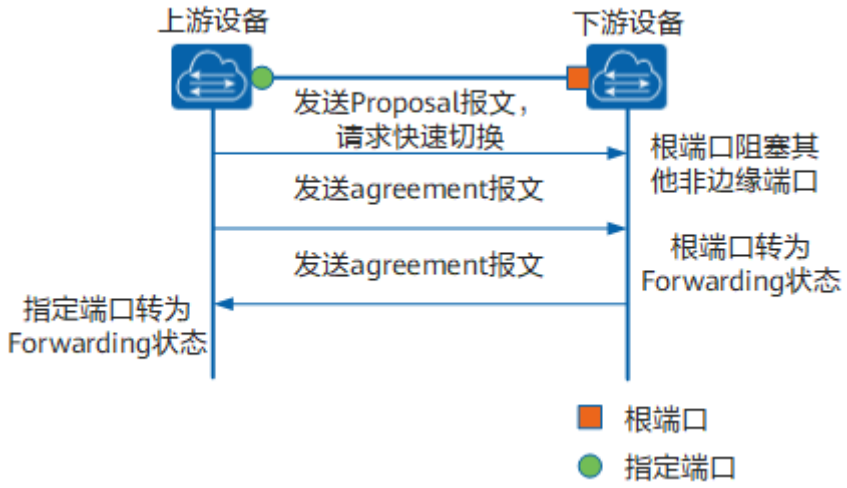
在 MST 域间，沿着 CST 转发。

- MSTP 对拓扑变化的处理

MSTP 拓扑变化处理与 RSTP 拓扑变化处理过程类似，请参见 RSTP 拓扑变化处理。

12.1.3.5. 快速收敛

图 12-23 MSTP 的 P/A 机制



如上图所示，在 MSTP 中，P/A 机制工作过程如下：

上游设备发送 Proposal 报文，请求进行快速迁移。下游设备接收到后，把与上游设备相连的端口设置为根端口，并阻塞所有非边缘端口。

上游设备继续发送 Agreement 报文。下游设备接收到后，根端口转为 Forwarding 状态。

下游设备回应 Agreement 报文。上游设备接收到后，把与下游设备相连的端口设置为指定端口，指定端口进入 Forwarding 状态。

12.1.3.6. 标准规范

与生成树相关的协议规范有：

- IEEE 802.1D：Media Access Control (MAC) Bridges
- IEEE 802.1w：Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration

- IEEE 802.1s：Virtual Bridged Local Area Networks—Amendment 3: Multiple Spanning Trees

12.2. 配置命令

12.2.1. 缺省配置

参数	缺省值
STP 工作模式	RSTP 模式
功能开关	全局功能关闭，端口功能使能
交换设备的优先级	32768
端口的优先级	128
路径开销的计算方法	Dot1t，即 IEEE 802.1t 标准
Forward Delay Time	1500 厘秒（15 秒）
Hello Time	200 厘秒（2 秒）
Max Age Time	2000 厘秒（20 秒）

12.2.2. 配置 STP 模式和开关

- 配置 STP 模式

命令	SWITCH(config)#**spanning-tree mode** <**stp	rstp	mstp**>
描述	stp：Spanning tree protocol(IEEE 802.1d) rstp：Rapid spanning tree protocol(IEEE 802.1w) mstp：Multiple spanning tree protocol(IEEE 802.1s) 默认为 rstp 模式，模式切换后生成树协议默认关闭，需要重新启用。 全局模式。

- 启用生成树协议

命令	SWITCH(config)#**spanning-tree enable** SWITCH(config)#**no spanning-tree enable**
描述	启用/关闭 STP 功能；默认关闭。 全局模式。

12.2.3. 配置 STP 选举参数

- 配置设备优先级

命令	SWITCH(config)#**spanning-tree priority** <0-61440> SWITCH(config)#**no spanning-tree priority** SWITCH(config)#**spanning-tree instance** <1-63> **priority** <0-61440> SWITCH(config)#**no spanning-tree instance** <1-63> **priority**
描述	配置/删除 STP 系统优先级；默认 32768。可选配置。 全局模式。

- 配置端口优先级

命令	SWITCH(config-if)#**spanning-tree priority** <0-240> SWITCH(config-if)#**spanning-tree instance** <1-63> **priority** <0-240>
描述	配置端口 STP 优先级；默认 128。可选配置。

	接口配置模式。

- 配置端口路径花费

命令	SWITCH(config-if)#**spanning-tree path-cost** <1-200000000> SWITCH(config-if)#**no spanning-tree path-cost**
描述	配置/重置端口的路径花费；可选配置。 接口配置模式。

12.2.4. 配置拓扑收敛参数

- 配置 Hello Time

命令	SWITCH(config)#**spanning-tree hello-time** <1-10> SWITCH(config)#**no spanning-tree hello-time**
描述	配置/重置 BPDU 报文周期，单位为秒；默认为 2s。可选配置。 全局模式。

- 配置 Forward-Delay Time

命令	SWITCH(config)#**spanning-tree forward-time** <4-30> SWITCH(config)#**no spanning-tree forward-time**
描述	配置/重置 STP 端口转发状态延迟时间，单位为秒；默认为 15s。可选配置。 全局模式。

- 配置 Max-Age Time

命令	SWITCH(config)#**spanning-tree max-age** <6-40> SWITCH(config)#**no spanning-tree max-age**
描述	配置/重置 BPDU 报文的生命周期，单位为秒；默认为 20s。可选配置。 Hello Time、Forward-Delay Time、Max-Age Time 需要遵循条件：2*(Hello Time + 1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay – 1.0seconds)，否则有可能导致拓扑不稳定。 STP/RSTP 网络最长路径受本参数影响，默认最长路径为 20 台，当超出 20 台设备时，需要修改配置(可以配置 forward-delay 21s，max-age 40s)，最大支持最长路径 40 台。 全局模式。

- 配置 Max-Hops

命令	SWITCH(config)#**spanning-tree max-hops** <1-40> SWITCH(config)#**no spanning-tree max-hops**
描述	配置/重置 BPDU 报文的最大跳数；默认为 20。可选配置。 MSTP 网络最长路径受本参数影响，当超过 20 台设备时需要修改配置，最大 40。 MSTP 兼容 max-age 功能，需要同时调整 max-age 参数，参考对应命令。 全局模式。

12.2.5. 配置边缘端口

- 配置 Edge Port

命令	SWITCH(config-if)#**spanning-tree <edgeport | autoedge>**

	SWITCH(config-if)#**no spanning-tree <edgeport | autoedge>**
描述	配置/删除端口 Edge Port；配置为 edgeport 表示该端口直连设备不是网桥设备，可以快速 forward；配置为 autoedge 表示该端口依据 BPDU 自动识别是否边缘端口；默认关闭；可选配置。 接口配置模式。

- 打开 Portfast

命令	SWITCH(config-if)#**spanning-tree portfast** SWITCH(config-if)#**no spanning-tree portfast**
描述	配置/删除端口 portfast；打开 portfast 后该端口会直接 Forwarding。但会因为收到 BPDU 而使 Port Fast Operational State 为 disabled，从而正常的参与 STP 算法而 Forwarding；默认关闭；可选配置。 接口配置模式。

12.2.6. 配置 MST 参数

- 进入 MST 模式

命令	SWITCH(config)#**spanning-tree mst configuration**
描述	进入 MST 模式。 全局模式。

- 配置 MST VLAN 和 instance 的对应关系

命令	SWITCH(config-mst)# **instance** <1-63> **vlan** VLANID SWITCH(config-mst)# **no instance** <1-63> **vlan** VLANID
描述	配置/删除 MST 实例和 VLAN 的关联；可选配置。 MST 模式。

- 配置 MST 区域名

命令	SWITCH(config-mst)#**region** NAME SWITCH(config-mst)#**no region** NAME
描述	配置/删除 MST 区域名；可选配置。 MST 模式。

- 配置 MST 版本号

命令	SWITCH(config-mst)#**revision** <0-65535>
描述	配置/删除 MST 版本号，默认为 0；可选配置。 MST 模式。

- 配置端口和 MST 实例的关联

命令	SWITCH(config-if)# **spanning-tree instance** <1-63> SWITCH(config-if)# **no spanning-tree instance** <1-63>
描述	配置/删除端口和实例的关联；可选配置。 默认情况下，配置实例和 VLAN 关系时系统会依据 VLAN 和端口关系自动生成端口和实例

	的关系数据，无需手动配置。 在实例配置就绪后，如果出现手动修改端口和 VLAN 关系时，比如某个实例的 VLAN 全部加入/退出端口，需要通过本命令手动维护端口和实例的关系。 出现较大配置变化时，建议通过重新配置实例-VLAN 关系，或重启设备来自动生成端口和实例的数据。 MST 模式。

12.2.7. 配置保护功能

- 配置 Root Guard

命令	SWITCH(config-if)# **spanning-tree guard root** SWITCH(config-if)#**no spanning-tree guard root**
描述	配置/删除端口 Root Guard；接口打开 Root Guard 功能时，强制其在所有实例上的端口角色为指定端口，一旦该端口收到优先级更高的配置信息时，Root Guard 功能会将该接口置为 blocked 状态；默认关闭；可选配置。 接口配置模式。

- 配置 BPDU Guard

命令	SWITCH(config)#**spanning-tree portfast bpdu-guard** SWITCH(config)#**no spanning-tree portfast bpdu-guard** SWITCH(config-if)#**spanning-tree portfast** SWITCH(config-if)#**no spanning-tree portfast** 或: SWITCH(config-if)#**spanning-tree bpdu-guard enable** SWITCH(config-if)#**spanning-tree bpdu-guard disable**
描述	配置/删除 BPDU Guard；端口打开 BPDU Guard 后，如果在该端口上收到 BPDU，则会进入 Error-disabled (blocked) 状态；可选配置。 接口配置模式。

- 配置 BPDU Filter

命令	SWITCH(config)#**spanning-tree portfast bpdu-filter** SWITCH(config)#**no spanning-tree portfast bpdu-filter** SWITCH(config-if)#**spanning-tree portfast** SWITCH(config-if)#**no spanning-tree portfast** 或: SWITCH(config-if)#**spanning-tree bpdu-filter enable** SWITCH(config-if)#**spanning-tree bpdu-filter disable**
描述	配置/删除 BPDU Filter；端口打开 BPDU Filter 后，既不发送 BPDU，也不接收 BPDU 报文；可选配置。 接口配置模式。

- 配置 TC 拓扑改变通告

命令	SWITCH(config-if)#**spanning-tree restricted-tcn** SWITCH(config-if)#**no spanning-tree restricted-tcn** SWITCH(config-if)#**spanning-tree instance** <1-63> **restricted-tcn** SWITCH(config-if)#**no spanning-tree instance** <1-63> **restricted-tcn**
描述	配置/重置拓扑变化通告限制，配置后，端口不转发 TC BPDU，也不刷新地址表；可选配置。

	接口配置模式。

- 配置错误端口超时功能

命令	SWITCH(config)#**spanning-tree errdisable-timeout enable** SWITCH(config)#**no spanning-tree errdisable-timeout enable** SWITCH(config)#**spanning-tree errdisable-timeout interval** <10-1000000> SWITCH(config)#**no spanning-tree errdisable-timeout interval**
描述	配置/重置错误端口超时功能。 默认不开启错误端口超时功能，即错误端口永不超时自动恢复，必须手动恢复。 超时时间单位为秒，默认 300 秒； 可选配置。 全局配置模式。

12.2.8. 其他可选配置

- 配置 Transmit-Holdcount

命令	SWITCH(config)#**spanning-tree transmit-holdcount** <1-10> SWITCH(config)#**no spanning-tree transmit-holdcount**
描述	配置/重置每秒最多发送的 BPDU 数；默认为 6 个。可选配置。 全局配置模式。

- 配置 Link-Type

命令	SWITCH(config-if)#**spanning-tree link-type <auto | point-to-point | shared>** SWITCH(config-if)#**no spanning-tree link-type**
描述	配置/重置链路类型，默认为 auto。可选配置。 auto：基于链路协商的双工能力自动设置模式，全双工为点对点连接。 point-to-point：使能快速 Forwarding。 shared：禁止快速 Forwarding。 接口配置模式。

- 配置 Protocol Migration 处理

命令	SWITCH#**clear spanning-tree detected protocols**
描述	对所有端口强制进行版本检查。 特权模式。

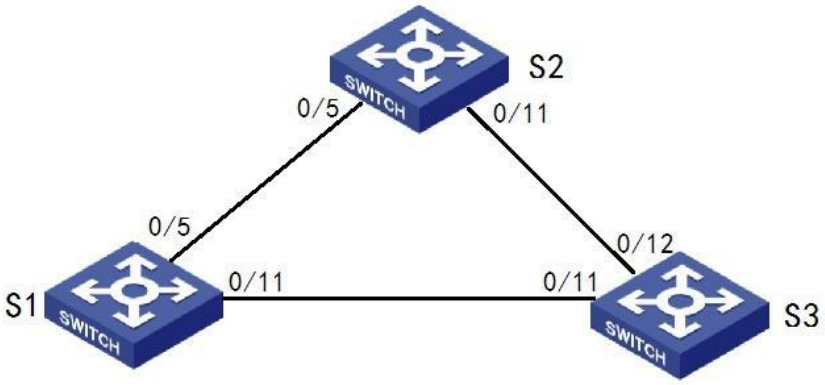
- 开启日志

命令	SWITCH(config)#**spanning-tree logging** SWITCH(config)#**no spanning-tree logging**
描述	开启/关闭生成树日志。 全局模式。

12.3. 配置案例

12.3.1. RSTP 防环实现链路冗余方案

简化拓扑:



用户 P1 接在 S1 下，P2 接在 S2 下，P3 接在 S3 下；

需求描述：

网络无故障时，用户间通信(ping)正常

网络出现单链故障时，用户间依然通信正常

典型配置：

S1/S2/S3：

- 进入全局配置模式，配置使用 rstp 模式，使能 stp 开关：

使用 rstp 模式

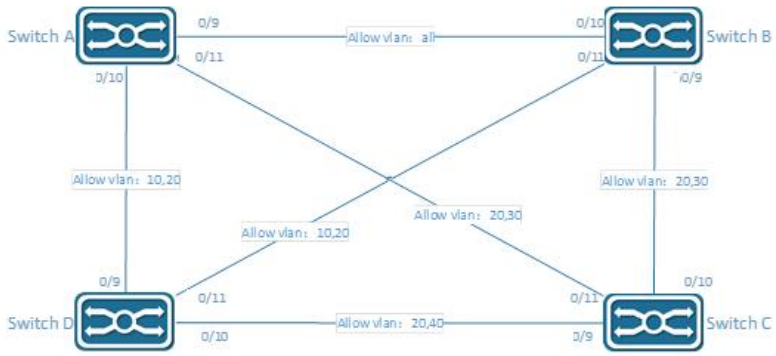
```
spanning-tree mode rstp
```

使能 stp 开关

```
spanning-tree enable
```

12.3.2. MSTP 实现基于域和实例的防环和链路冗余

简化拓扑：



需求描述：

网络正常时同一个 VLAN 内用户通信正常

通过冗余链路提高网络可靠性；比如对 VLAN 10 20 而言，Switch A B D 间单一链路故障不影响其下用户通信

配置规划：

设备同属于一个域，此处使用默认 Default 域，无需额外配置

VLAN 20 为共有 vlan，直接划入 CST 中

实例	VLAN
0	20
1	10

3	30
4	40

典型配置:

Switch A:

配置 VLAN 和端口

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface gigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
SWITCH(config)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
```

配置 MSTP 实例

```
SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
```

启用 MSTP

```
SWITCH(config)#spanning-tree enable
```

Switch B:

配置 VLAN 和端口

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface gigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
```

配置 MSTP 实例

```
SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
```

启用 MSTP

```
SWITCH(config)#spanning-tree enable
```

Switch C:

配置 VLAN 和端口

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface gigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,40
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
SWITCH(config)#interface gigabitEthernet0/11
```

```
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
```

配置 MSTP 实例

```
SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
```

启用 MSTP

```
SWITCH(config)#spanning-tree enable
```

Switch D:

配置 VLAN 和端口

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface gigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,40
SWITCH(config)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
```

配置 MSTP 实例

```
SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
```

启用 MSTP

```
SWITCH(config)#spanning-tree enable
```

12.4. 显示命令

- 查看 STP 状态

```
SWITCH#show spanning-tree
```

- 查看 MSTP 实例状态

```
SWITCH#show spanning-tree mst instance <1-63>
```

注意：MSTP 配置后请确保接口上有生成 **spanning-tree instance** <1-63>命令，如果没有自动生成，需要手动配置，或者通过设备重启来完成自动生成；更多细节请参考该命令的配置说明!

13. MAC 地址管理

13.1. MAC 地址概述

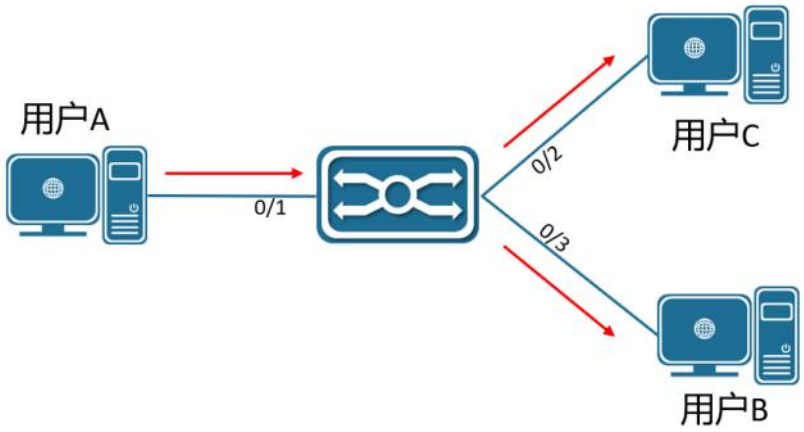
以太网交换机通过解析报文所携带的目的 MAC 地址，查询 MAC 地址表，将报文发送到相应的端口。MAC 地址表记录了与该设备相连的设备的 MAC 地址、接口以及所属的 VLAN ID 信息。以太网交换机根据 MAC 地址表查找的结果决定采用知名单播或未知名广播的转发方式。

知名单播：以太网交换机在 MAC 地址表中查到与报文的目的 MAC 地址和 VLAN ID 相对应的表项并且表项中的输出端口是唯一的，报文直接从表项对应的端口输出。

未知名广播：以太网交换机在地址表中没有找到目标 MAC 地址对应的表项，报文被送到所属的 VLAN 中除报文输入端口外的其他所有端口输出。

以太网交换机的 MAC 地址可通过动态获取或静态配置，一般情况下通过动态获取得到。下面通过分析用户 A 与用户 C 交互过程，给出 MAC 地址动态学习的工作原理。

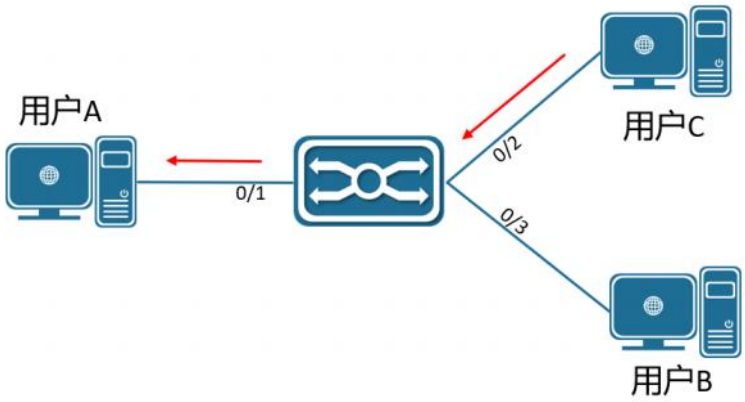
用户 A 发送报文到交换机的端口 gigabitEthernet0/1，此时以太网交换机将用户 A 的 MAC 地址学习到 MAC 地址表中。由于地址表中没有用户 C 的源 MAC 地址，因此以太网交换机以广播的方式将报文发送到除连接用户 A 的 gigabitEthernet0/1 以外的同属 VLAN1 的所有端口，包括用户 B 与用户 C 的端口，此时用户 B 能够收到用户 A 所发出的不属于它的报文。



当前动态 MAC 地址表信息：

用户	VLAN	MAC 地址	端口
用户 A	1	000E.C6C1.C8AB	gigabitEthernet0/1

用户 B 收到报文后将回应报文通过以太网交换机的端口 gigabitEthernet0/2，发送给用户 A，此时以太网交换机的 MAC 地址表中已存在用户 A 的 MAC 地址，报文被以单播的方式转发到 gigabitEthernet0/1 端口，同时以太网交换机将学习用户 C 的 MAC 地址，与前面所不同的是用户 B 此时接收不到用户 C 发送给用户 A 的报文。



当前动态 MAC 地址表信息：

用户	VLAN	MAC 地址	端口
用户 A	1	000E.C6C1.C8AB	gigabitEthernet0/1
用户 C	1	000E.C6C1.C8AD	gigabitEthernet0/2

通过用户 A 与用户 C 的一次交互过程后，设备学习到了用户 A 与用户 C 的源 MAC 地址，之后用户 A 与用户 C 之间的报文交互则采用单播的方式进行转发，此后用户 B 将不再接收到用户 A 与用户 C 之间的交互报文。

13.2. 配置命令

- 配置动态 MAC 地址老化时间

命令	SWITCH(config)#**mac-address-table aging-time** <0-600> SWITCH(config)#**no mac-address-table aging-time**
描述	配置 MAC 地址老化时间，范围 0-600 秒； 默认 MAC 地址老化时间 300 秒； 当配置为 0，表示关闭 MAC 地址老化功能；

- 配置静态 MAC 地址

命令	SWITCH(config)#**mac-address-table static** MAC_ADDR **vlan** VLANID **interface** IFNAME SWITCH(config)#**no mac-address-table static** MAC_ADDR **vlan** VLANID **interface** IFNAME
描述	配置静态 MAC 地址； 当设备在 VLANID 指定的 VLAN 上接收到以 MAC_ADDR 为目的地址的报文时，这个报文将被转发到 IFNAME 所指定的接口上； IFNAME 支持物理口与聚合口

- 配置 MAC 地址过滤

命令	SWITCH(config)#**mac-address-table filter** MAC_ADDR **vlan** VLANID SWITCH(config)#**no mac-address-table filter** MAC_ADDR **vlan** VLANID
描述	配置 MAC 地址过滤； 当设备在 VLANID 指定的 VLAN 上接收到以 MAC_ADDR 指定的地址为源地址或目的 地

	址的报文将被丢弃

- 清除动态 MAC 地址

命令	SWITCH#**clear mac-address-table dynamic** SWITCH#**clear mac-address-table dynamic vlan** VLANID SWITCH#**clear mac-address-table dynamic interface** IFNAME
描述	动态 MAC 地址清除操作； 支持全部、基于 VLAN、基于端口的 MAC 地址清除操作

- 开启/关闭端口 MAC 地址学习

主要应用在以下场景：

- 在网络比较稳定、报文的 MAC 地址相对固定的情况下，设备没有必要继续学习其他所有报文的 MAC 地址。此时通过应用流策略，对策略下所有流分类禁止 MAC 地址学习功能，既可以节省 MAC 地址表项开支，也可以提高设备的运行效率。
- 某些非法用户有时会采用频繁变换 MAC 地址的方式对网络进行攻击，此时通过应用流策略，对策略下所有流分类禁止 MAC 地址学习功能，可以避免此类攻击所造成的设备 MAC 地址表项溢出的问题，保护设备性能不受影响。

命令	SWITCH(config-if)#**mac-address-table learning disable action** (**forward** | **drop**) SWITCH(config-if)#**no mac-address-table learning disable**
描述	该命令支持物理口、AP 口，不支持 AP 成员口 配置关闭端口 MAC 地址学习功能 **forward**: 若 MAC 地址表中有匹配表项，即按照 MAC 表进行转发；若无匹配表项，即广播报文 **discard** 时，若 MAC 地址表中有匹配表项，即按照 MAC 表进行转发；若无匹配表项，则丢弃该报文 缺省端口 MAC 地址学习处于使能状态

- 端口 MAC 地址学习个数限制

为了控制接入用户数量或防止 MAC 地址表受攻击，可以限制交换模块允许学习的 MAC 地址数量，从而控制接入用户数量，以提高网络安全性。

命令	SWITCH(config-if)#**mac-address-table limit maximum** MAXINUM **action** (**forward** | **drop**) SWITCH(config-if)#**no mac-address-table limit**
描述	该命令支持物理口、AP 口，不支持 AP 成员口 配置端口 MAC 地址学习个数限制功能 MAXINUM: 限制值，<1-32767> forward: MAC 地址表项数目达到限制值后，源 MAC 为新 MAC 地址的报文继续被转发，但是 MAC 地址表项不记录 discard: MAC 地址表项数目达到限制值后，源 MAC 为新 MAC 地址的报文将被丢弃

- 开启/关闭 VLAN MAC 地址学习

网络管理人员为提高设备的安全性，可以指定某些 VLAN 只允许某些 MAC 地址的报文通过。关闭 MAC 地址学习功能后，设备将不会再从该 VLAN 学习新的 MAC 地址，这样将无法通过该 VLAN 通信，增强了

网络的稳定性和安全性。

当 MAC 地址学习功能处于打开状态时，收到来自周边设备的以太网帧，解析出源 MAC 地址，在 MAC 地址表项中添加新表项。以后，交换模块接收到去往该目的 MAC 地址的以太网帧时，则直接查询 MAC 地址表项就可以得到正确的发送接口，避免了广播。

命令	SWITCH(config)#**mac-address-table learning disable vlan** VLAN-LIST **action** (**forward** | **drop**) SWITCH(config)#**no mac-address-table learning disable vlan** VLAN-LIST
描述	配置关闭 VLAN MAC 地址学习功能 VLAN-LIST: 支持单个 vlan 或 range 模式，例如：10 或 10-20 **forward**: 若 MAC 地址表中有匹配表项，即按照 MAC 表进行转发；若无匹配表项，即广播报文 **discard** 时，若 MAC 地址表中有匹配表项，即按照 MAC 表进行转发；若无匹配表项，则丢弃该报文 缺省端口 MAC 地址学习处于使能状态

- 端口 VLAN 地址学习个数限制

为了控制接入用户数量或防止 MAC 地址表受攻击，可以限制交换模块允许 VLAN 内学习的 MAC 地址数量，从而控制接入用户数量，以提高网络安全性。

命令	SWITCH(config-if)#**mac-address-table limit vlan** VLAN-LIST **maximum** MAXINUM **action** (**forward** | **drop**) SWITCH(config-if)#**no mac-address-table limit vlan** VLAN-LIST
描述	配置 VLANMAC 地址学习个数限制功能 VLAN-LIST: 支持单个 vlan 或 range 模式，例如：10 或 10-20 MAXINUM: 限制值，<1-32767> forward: MAC 地址表项数目达到限制值后，源 MAC 为新 MAC 地址的报文继续被转发，但是 MAC 地址表项不记录 discard: MAC 地址表项数目达到限制值后，源 MAC 为新 MAC 地址的报文将被丢弃

- 开启/关闭 flapping 功能

MAC 地址漂移即设备上一个接口学习到的 MAC 地址在同一 VLAN 中另一个接口上也被学习到，后学习到的 MAC 地址表项覆盖原来的表项。

MAC 地址漂移可由以下原因引起：

- 网络中交换模块网线误接或配置错误形成了环网，导致 MAC 地址漂移。
- 网络中某些非法用户进行 MAC 地址攻击。

配置 MAC 地址漂移检测功能可以检测到设备上所有的 MAC 地址是否发生了漂移。若发生漂移，将记录漂移事件，维护人员可根据告警信息定位故障。

命令	SWITCH(config)#**mac-address-table flapping detect** SWITCH(config)#**no mac-address-table flapping detect**
描述	配置使能 MAC 地址 flapping 功能，默认关闭

- 检测到 flapping 触发 shutdown

接口配置了 MAC 地址漂移处理动作后，如果系统检测到是该接口学习的 MAC 发生漂移，会将该接口关闭。

端口 shutdown 动作是否执行，还需看 errdisable 模块 Mac-address-table-flapping 选项是否选择，默认使能。

命令	SWITCH(config)#**mac-address-table flapping detect action shutdown** SWITCH(config)#**no mac-address-table flapping detect action**
描述	配置使能 MAC 地址 flapping 功能，默认关闭

- 配置 flapping 触发的迁移发生次数

MAC 地址迁移可能是正常拔插导致，也可能因环路等其他非正常原因导致，若 MAC 地址迁移次数超出配置值，则认为发生漂移事件。

命令	SWITCH(config)#**mac-address-table flapping detect times** VALUE SWITCH(config)#**no mac-address-table flapping detect times**
描述	配置 flapping 触发的迁移发生次数 VALUE：<1 50>，默认值 5

- 清除 flapping 记录信息

命令	SWITCH#**clear mac-address-table flapping**
描述	清除 flapping 记录信息

13.3. 配置案例

案例一：配置动态 MAC 地址老化时间为 60 秒。

- 进入全局模式：

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

- 配置动态地址老化时间

```
SWITCH(config)#mac-address-table aging-time 60
```

案例二：配置静态 MAC 地址，所有目的 MAC 地址 000E.C6C1.C8AB，VLAN 1 的报文从端口 gigabitEthernet0/1 转发。

- 进入全局模式：

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

- 配置静态 MAC 地址

```
SWITCH(config)#mac-address-table static 000E.C6C1.C8AB vlan 1 interface gigabitEthernet0/1
```

案例三：配置 MAC 地址过滤，丢弃 VLAN 1 源或目的 MAC 地址为 000E.C6C1.C8AB 的报文。

- 进入全局模式：

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

- 配置过滤 MAC 地址

```
SWITCH(config)#mac-address-table filter 000E.C6C1.C8AB vlan 1
```

案例四：清除端口 gigabitEthernet0/1 下的动态 MAC 地址。

- 清除动态 MAC 地址

```
SWITCH#clear mac-address-table dynamic interface gigabitEthernet0/1
```

13.4. 显示命令

- 显示 MAC 地址

```
SWITCH#show  mac-address-table
 VLAN     MAC Address     Type      Ports
  -----+----------------+---------+----------------------+
  20     0000.0000.0009   filter    drop
  20     0000.0000.000a   filter    drop
```

- 显示 MAC 地址个数统计

```
SWITCH#show  mac-address-table count
Static Address Count: 0
Filter Address Count: 2
Dynamic Address Count: 0
```

- 显示 MAC 地址 learning 配置信息

```
SWITCH#show mac-address-table learning

Interface               Status          Action
--------------------------------------------------
GiE0/4                  Disabled        Forward
Vlan 3-6                Disabled        Drop
Vlan 9-10               Disabled        Drop
```

- 显示 MAC 地址 limit 配置信息

```
SWITCH#show mac-address-table limit

Interface               Limit           Action
--------------------------------------------------
GiE0/5                  1000            Drop
Vlan 20-25              100             forward
```

- 显示 MAC 地址 flapping 信息

```
SWITCH#show mac-address-table flapping

Mac-address-table Flapping Configurations:
------------------------------------------------------------
Mac-address-table flapping detect   :  Disabled
Mac-address-table flapping times    :  5
Mac-address-table flapping action   :  none
------------------------------------------------------------

Mac-address-table Flapping entries  :  0
```

14. 配置 LLDP

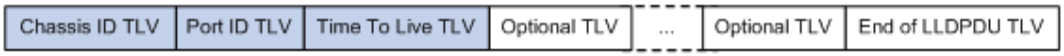
14.1. 协议概述

LLDP（Link Layer Discovery Protocol，链路层发现协议）提供了一种标准的链路层发现方式，使不同厂商的设备能够在网络中相互发现并交互各自的系统及配置信息。LLDP 将本端设备的信息（包括主要能力、管理地址、设备标识、接口标识等）封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB 的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

LLDPDU

LLDPDU 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。

图 14-1 LLDPDU 的封装格式



如图 14-1 所示，蓝色的 Chassis ID TLV、Port ID TLV、Time To Live TLV 是每个 LLDPDU 都必须携带的，其余的 TLV 则为可选携带。每个 LLDPDU 最多可携带 32 种 TLV。

TLV

TLV 是组成 LLDPDU 的单元，每个 TLV 都代表一个信息。LLDP 可以封装的 TLV 包括基本 TLV、802.1 组织定义 TLV、802.3 组织定义 TLV 和 LLDP-MED（Link Layer Discovery Protocol Media Endpoint Discovery，链路层发现协议媒体终端发现）TLV。

基本 TLV

基本 TLV 是网络设备管理基础的一组 TLV，802.1 组织定义 TLV、802.3 组织定义 TLV 和 LLDP-MED TLV 则是由标准组织或其他机构定义的 TLV，用于增强对网络设备的管理，可根据实际需要选择是否在 LLDPDU 中发送。

在基本 TLV 中，有几种 TLV 对于实现 LLDP 功能来说是必选的，即必须在 LLDPDU 中发布，如表 14-1 所示。

表 14-1 基本 TLV

TLV 名称	说明	是否必须发布
Chassis ID	发送设备的桥 MAC 地址	是
Port ID	标识 LLDPDU 发送端的端口。如果 LLDPDU 中携带有 LLDP-MED TLV，其内容为端口的 MAC 地址；否则，其内容为端口的名称	是
Time To Live	本设备信息在邻居设备上的存活时间	是
End of LLDPDU	LLDPDU 的结束标识，是 LLDPDU 的最后一个 TLV	否
Port Description	端口的描述	否

TLV 名称	说明	是否必须发布
System Name	设备的名称	否
System Description	系统的描述	否
System Capabilities	系统的主要功能以及已开启的功能项	否
Management Address	管理地址，以及该地址所对应的接口号和 OID（Object Identifier，对象标识符）	否

802.1 组织定义 TLV

IEEE 802.1 组织定义 TLV 的内容如表 14-2 所示。

表 14-2 IEEE 802.1 组织定义的 TLV

TLV 名称	说明
Port VLAN ID(PVID)	端口 VLAN ID
Port and protocol VLAN ID(PPVID)	端口协议 VLAN ID
VLAN Name	端口所属 VLAN 的名称
Protocol Identity	端口所支持的协议类型
DCBX	数据中心桥能力交换协议（Data Center Bridging Exchange Protocol）
EVB 模块	（暂不支持）边缘虚拟桥接（Edge Virtual Bridging）模块，具体包括 EVB TLV 和 CDCP（S-Channel Discovery and Configuration Protocol，S 通道发现和配置协议） TLV 这两种 TLV。有关这两种 TLV 的详细介绍，请参见“EVB 配置指导”
Link Aggregation	端口是否支持链路聚合以及是否已开启链路聚合
Management VID	管理 VLAN
VID Usage Digest	包含 VLAN ID 使用摘要的数据
ETS Configuration	增强传输选择（Enhanced Transmission Selection）配置
ETS Recommendation	增强传输选择推荐
PFC	基于优先级的流量控制（Priority-based Flow Control）
APP	应用协议（Application Protocol）
QCN	（暂不支持）量化拥塞通知（Quantized Congestion Notification）

802.3 组织定义 TLV

IEEE 802.3 组织定义 TLV 的内容如表 14-3 所示。

Power Stateful Control TLV 是在 IEEE P802.3at D1.0 版本中被定义的，之后的版本不再支持该 TLV。

表 14-3 IEEE 802.3 组织定义的 TLV

TLV 名称	说明
MAC/PHY Configuration/Status	端口支持的速率和双工状态、是否支持端口速率自动协商、是否已开启自动协商功能以及当前的速率和双工状态
Link Aggregation	端口是否支持链路聚合以及是否已开启链路聚合
Power Via MDI	端口的供电能力，包括 PoE（Power over Ethernet，以太网供电）的类型（包括 PSE（Power Sourcing Equipment，供电设备）和 PD（Powered Device，受电设备）两种）、PoE 端口的远程供电模式、是否支持 PSE 供电、是否已开启 PSE 供电、供电方式是否可控、供电类型、功率来源、功率优先级、PD 请求功率值、PSE 分配功率值
Maximum Frame Size	端口支持的最大帧长度
Power Stateful Control	端口的电源状态控制，包括 PSE/PD 所采用的电源类型、供/受电的优先级以及供/受电的功率
Energy-Efficient Ethernet	节能以太网

管理地址

管理地址是供网络管理系统标识网络设备并进行管理的地址。管理地址可以明确地标识一台设备，从而有利于网络拓扑的绘制，便于网络管理。管理地址被封装在 LLDP 报文的 Management Address TLV 中向外发布。

LLDP 的工作模式

在指定类型的 LLDP 代理下，LLDP 有以下四种工作模式：

- TxRx：既发送也接收 LLDP 报文。
- Tx：只发送不接收 LLDP 报文。
- Rx：只接收不发送 LLDP 报文。
- Disable：既不发送也不接收 LLDP 报文。

当端口的 LLDP 工作模式发生变化时，端口将对协议状态机进行初始化操作。为了避免端口工作模式频繁改变而导致端口不断执行初始化操作，可配置端口初始化延迟时间，当端口工作模式改变时延迟一段时间再执行初始化操作。

协议规范

与 LLDP 相关的协议规范有：

- IEEE 802.1AB-2005：Station and Media Access Control Connectivity Discovery
- IEEE 802.1AB 2009：Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057：Link Layer Discovery Protocol for Media Endpoint Devices

IEEE Std 802.1Qaz-2011：Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes

14.2. 配置命令

14.2.1. 开关和工作模式配置

- 全局开启/关闭 LLDP 功能

命令	SWITCH(config)# **lldp run** SWITCH(config)#**no lldp run**
描述	全局配置模式。 开启/关闭 LLDP 功能。 必选。

- 进入 LLDP 接口代理配置模式

命令	SWITCH(config-if)# **lldp-agent** SWITCH(lldp-agent)# **exit**
描述	接口配置模式。 进入 LLDP 接口代理配置模式。 可选。

- 配置 LLDP 接口的工作模式

命令	SWITCH(lldp-agent)# **lldp enable** { rxonly | txonly | txrx } SWITCH(lldp-agent)# **lldp disable**
描述	LLDP 接口代理配置模式。 配置 LLDP 接口的工作模式。 可选。

14.2.2. 可选基本参数配置

- 配置系统名称

命令	SWITCH(config)# **lldp system-name** NAME SWITCH(config)# **no lldp system-name**
描述	全局配置模式。 配置/重置系统名称。 可选。

- 配置系统描述符

命令	SWITCH(config)# **lldp system-description** LINE SWITCH(config)# **no lldp system-description**
描述	全局配置模式。 配置/重置系统描述符。 可选。

- 配置设备 locally-assigned

命令	SWITCH(config)# **lldp chassis locally-assigned** NAME SWITCH(config)# **no lldp chassis locally-assigned**
描述	全局配置模式。 配置/重置设备 locally-assigned。 可选。

- 配置接口 locally-assigned

命令	SWITCH(config-if)# **lldp locally-assigned** NAME SWITCH(config-if)# **no lldp locally-assigned**
描述	接口配置模式。 配置/重置接口 locally-assigned。 可选。

- 配置接口代理线缆标识

命令	SWITCH(config-if)# **lldp agt-circuit-id** VALUE SWITCH(config-if)# **no lldp agt-circuit-id**
描述	接口配置模式。 配置/重置接口 agt-circuit-id。 可选。

- 配置接口端口描述符

命令	SWITCH(config-if)# **lldp port-description** LINE SWITCH(config-if)# **no lldp port-description**
描述	接口配置模式。 配置/重置接口端口描述符。 可选。

- 配置 LLDP 接口的设备标识类型

命令	SWITCH(lldp-agent)# **lldp chassis-id-tlv** { if-alias | if-name | ip-address | locally-assigned | mac-address } SWITCH(lldp-agent)# **no lldp chassis-id-tlv**
描述	LLDP 接口代理配置模式。 配置 LLDP 接口的设备标识类型。 可选。

- 配置 LLDP 接口的管理地址类型

命令	SWITCH(lldp-agent)# **lldp management-address-tlv** { ip-address | mac-address } SWITCH(lldp-agent)# **no lldp management-address-tlv**
描述	LLDP 接口代理配置模式。 配置 LLDP 接口的管理地址类型。 可选。

- 配置 LLDP 接口的端口标识类型

命令	SWITCH(lldp-agent)# **lldp port-id-tlv** { agt-circuit-id | if-alias | if-name | ip-address | locally-assigned | mac-address }

	SWITCH(lldp-agent)# **no lldp port-id-tlv**
描述	LLDP 接口代理配置模式。 配置 LLDP 接口的端口标识类型。 可选。

14.2.3. 可选状态机参数配置

- 配置 LLDP 接口的 msgTxHold 参数

命令	SWITCH(lldp-agent)# **lldp msg-tx-hold** <1-100> SWITCH(lldp-agent)# **no lldp msg-tx-hold**
描述	LLDP 接口代理配置模式。 此变量用作 msgTxInterval 的乘数，以确定由 LLDP 代理传输的 LLDP 帧中携带的 txTTL 的值。默认值 msgTxHold 为 4。 管理员可以将此值更改为 1 到 100 范围内的任何值。TTL=msgTxInterval * msgTxHold + 1。 可选。

- 配置 LLDP 接口的 txFastInit 参数

命令	SWITCH(lldp-agent)# **lldp tx-fast-init** <1-8> SWITCH(lldp-agent)# **no lldp tx-fast-init**
描述	LLDP 接口代理配置模式。 该变量用作 txFast 变量的初始值。 该值确定在快速传输周期内传输的 LLDPDU 的数量。默认值 txFastInit 为 4。 管理员可以将此值更改为 1 到 8 之间的任何值。 可选。

- 配置 LLDP 接口的 txCredit 参数

命令	SWITCH(lldp-agent)# **lldp tx-max-credit** <1-8> SWITCH(lldp-agent)# **no lldp tx-max-credit**
描述	LLDP 接口代理配置模式。 配置 txCredit 的最大值。默认值为 5。 管理员可以将此值更改为 1 到 10 范围内的任何值。 可选。

- 配置 LLDP 接口的 msgFastTx 参数

命令	SWITCH(lldp-agent)# **lldp timer msg-fast-tx** <1-3600> SWITCH(lldp-agent)# **no lldp timer msg-fast-tx**
描述	LLDP 接口代理配置模式。 此变量定义了在快速传输周期内两次传输之间的计时器间隔的时间间隔（即 txFast 不为零）。 msgFastTx 的默认值是 1; 管理员可以将此值更改为 1 到 3600 之间的任何值。 可选。

- 配置 LLDP 接口的 msgTxInterval 参数

命令	SWITCH(lldp-agent)# **lldp timer msg-tx-interval** <5-3600> SWITCH(lldp-agent)# **no lldp timer msg-tx-interval**

描述	LLDP 接口代理配置模式。 此变量定义了在正常传输（即 txFast 为零）之间的计时器间隔。 msgTxInterval 的默认值为 30 s； 管理员可以将此值更改为 5 到 3600 之间的任何值。 可选。

- 配置 LLDP 接口的 reinitDelay 参数

命令	SWITCH(lldp-agent)# **lldp timer reinit-delay** <1-10> SWITCH(lldp-agent)# **no lldp timer reinit-delay**
描述	LLDP 接口代理配置模式。 此参数表示从 adminStatus 变为“禁用”到尝试重新初始化之间的延迟量。 reinitDelay 的默认值为 2 s。 可选。

14.2.4. 发送 tlv 列表配置

- 配置 LLDP 接口的 tlv 选择

命令	SWITCH(lldp-agent)# [**no**] **lldp tlv-select basic-mgmt** { management-address | port-description | system-capabilities | system-description | system-name} SWITCH(lldp-agent)# [**no**] **lldp tlv-select ieee-8021-org-specific** {link-agg | mgmt-vid | port-ptcl-vlanid | port-vlanid | ptcl-identity | vid-digest | vlan-name} SWITCH(lldp-agent)# [**no**] **lldp tlv-select ieee-8023-org-specific** { mac-phy | max-mtu-size}
描述	LLDP 接口代理配置模式。 可以通过多条命令来选择多个 tlv。 可选。 注意：设备 VLAN 配置较多时，VLAN 相关 tlv 可能导致报文长度超过 MTU，造成发包错误，需要通过配置不发送该类 tlv。

14.3. 配置案例

14.3.1. LLDP 基本功能配置举例

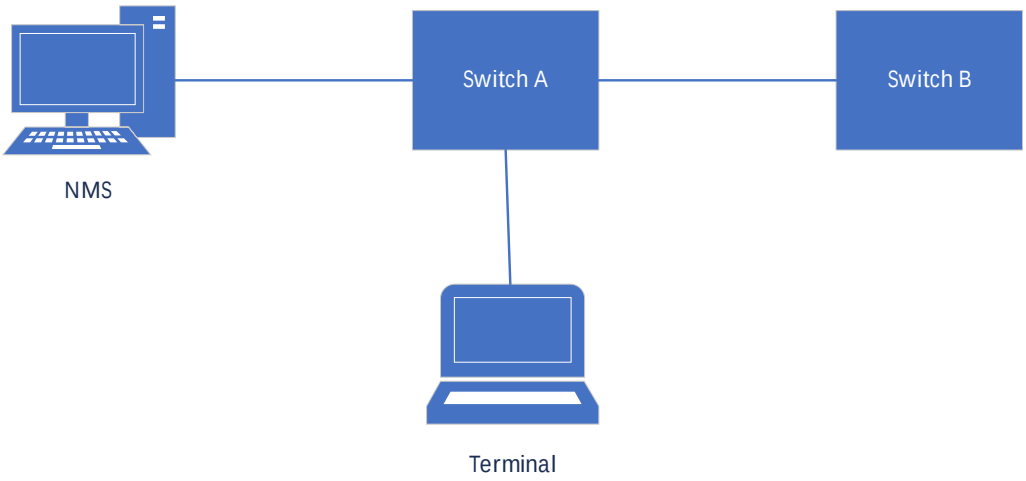
组网需求

NMS（Network Management System，网络管理系统）与 Switch A 相连，Switch A 分别与 Terminal 设备和 Switch B 相连。

通过在 Switch A 和 Switch B 上配置 LLDP 功能，使 NMS 可以对 Switch A 与 Terminal 设备之间、以及 Switch A 与 Switch B 之间链路的通信情况进行判断。

组网图

图 14-2 LLDP 基本功能配置组网图



典型配置举例

Switch A/B:

```
Lldp run
```

14.4. 显示命令

- 显示 LLDP 接口的状态

```
#show lldp interface gigabitEthernet0/2

Agent Mode : Nearest bridge
Enable (tx/rx): Y/Y
Message fast transmit time:1
Message transmission interval:30
Reinitialisation delay:2
MED Enabled :Y
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 4608
Total entries aged: 0
Total frames received: 150
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0
```

- 显示 LLDP 接口邻居

说明：LLDP 邻居默认老化时间 2min.端口 down 时邻居会被清除

```
#show lldp interface gigabitEthernet0/2 neighbor
 Nearest bridge Neighbors
Interface Name      : gigabitEthernet0/2
System Name         :
System Description  :
Port Description    :
TTL                 : 3601
System Capabilities : Routing
 Mandatory TLVs :
  CHASSIS ID TYPE :
```

```
    Chassis MAC Address: 000e.c6c1.3841
   PORT ID TYPE :
    Port MAC Address: 000e.c6c1.3841
  8021 ORIGIN SPECIFIC TLV
   Port Vlan id  :0
   PP Vlan id    :0
   Remote Protocols Advertised  :
   Remote VID Usage Digest  : 0
   Remote Management Vlan   : 0
   Link Aggregation Status  : Disabled
   Link Aggregation Port ID : 0
  8023 ORIGIN SPECIFIC TLV
   AutoNego Support     :  Supported Enabled
   AutoNego Capability  : 1
   Operational MAU Type : 0
   Max Frame Size       : 0
   MED Capabilities  :  Capabilities
   MED Capabilities Dev Type : End Point Class-1
   MED Application Type : Reserved
   MED Vlan id : 0
   MED Tag/Untag: Untagged
   MED L2 Priority : 0
   MED DSCP Val : 0
```

15. LOOP-DETECT

15.1. LOOP-DETECT 概述

LOOP-DETECT 是一种以太网环路检测协议，用于快速检测下联接口环路故障。如果发现故障存在，LOOP-DETECT 会根据用户配置的故障处理方式，通知用户手工关闭或自动关闭相关端口，以避免因环路影响正常数据交互。

使能控制：使能控制分全局使能控制与接口使能控制，当全局使能，且接口上开启环路检测时，该接口支持环路检测功能。

违例处理：当接口上检测到环路故障，默认通过 log 通告用户手工处理环路故障，也可配置自动关闭端口方式。当采用自动关闭端口方式，且端口触发违例事件时，可通过等待违例超时、 shutdown/no shutdown 端口、违例恢复命令或重启设备等方式实现端口从违例中恢复。

指定 vlan：默认情况下，当链路存在环路数据通路，忽略端口 vlan 属性，则认为单口环路；若需检测具体某 vlan 域内是否发生环路故障，可在端口上配置指定 vlan，仅检测该 vlan 域内是否存在环路数据通路。

设备支持环路故障告警与环路故障恢复消息 trap 到 snmp 服务器，默认关闭，支持全局开启。

15.2. 配置命令

15.2.1. 配置全局使能

命令	SWITCH(config)#**loop-detect enable** SWITCH(config)#**no loop-detect enable**
描述	全局使能 LOOP-DETECT 功能 默认全局关闭

15.2.2. 配置端口使能

命令	SWITCH(config-if)#**loop-detect enable** SWITCH(config-if)#**no loop-detect enable**
描述	基于端口使能 LOOP-DETECT 功能 默认关闭 支持物理口、AP 口，不支持 AP 成员口

说明

✦ 对于 block 状态的端口，协议认为不存在环路可能性，即使端口开启环路检测，实际功能无法正常运行，在开启 stp、erps 的环境中，可能存在类似情况，建议在配置上做功能互斥。

15.2.3. 配置端口违例处理

命令	SWITCH(config-if)#**loop-detect action (alarm | error-down)** SWITCH(config-if)#**no loop-detect action**
描述	配置端口违例处理 Alarm：打印告警信息 Error-down：打印告警信息，同时 shutdown 端口

	默认为 alarm 方式

15.2.4. 配置端口指定 VLAN

命令	SWITCH(config-if)#**loop-detect vlan** VID SWITCH(config-if)#**no loop-detect vlan** VID SWITCH(config-if)#**no loop-detect vlan**
描述	在指定 vlan 域内检测是否发生数据通路环路 VID 支持单 vlan 方式，也支持范围方式，如 10-12，中间用”，”分开 单端口最多指定 8 个 vlan 默认无指定 vlan，则忽略端口 vlan 属性，当存在环路数据通路，则认为端口环路。若端口为 block 状态，则认为该数据通路为阻断状态

15.2.5. 配置报文发送时间间隔

命令	SWITCH(config)#**loop-detect interval** SECONDS SWITCH(config)#**no loop-detect interval**
描述	全局配置环路检测报文发送间隔时间 SECONDS：范围 5-300， 默认 5，单位秒

15.2.6. 配置违例恢复时间

命令	SWITCH(config)#**errdisable timeout (interval** SECONDS | enable | disable) SWITCH(config)#**no errdisable timeout interval**
描述	配置使能违例恢复 配置违例恢复时间 SECONDS：范围 10-1000000，单位秒 默认时间为 300 秒 违例时间为所有违例处理共用，配置该参数会对其他功能违例处理造成影响

15.2.7. 违例恢复

如果在 errdisable 模块中设置为违例不恢复，则无法通过该命令实现端口违例恢复，建议使用 shutdown+no shutdown 命令实现恢复操作。

命令	SWITCH#**errdisable recovery interface** IFNAME
描述	违例恢复接口

15.2.8. 配置 Trap 使能

命令	SWITCH(config)#**loop-detect trap enable** SWITCH(config)#no **loop-detect trap enable**
描述	使能 trap 环路故障发生与环路故障恢复消息到 snmp 服务器 默认关闭

环路告警 trap 节点定义：

Node	Data
Mib files	DK-LDET-MIB.my
oid	1, 3, 6, 1, 4, 1, 57430, 1, 6, 2,1
Ifindex	端口号

环路告警恢复 trap 节点定义：

Node	Data
Mib files	DK-LDET-MIB.my
oid	1, 3, 6, 1, 4, 1, 57430, 1, 6, 2,2
Ifindex	端口号

15.3. 配置案例

案例一：配置端口 gi0/1 开启环路检测功能，配置违例模式为 err-down。

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#loop-detect enable
SWITCH(config)#interface gigabitEthernet 0/1
SWITCH(config-if)# loop-detect enable
SWITCH(config-if)# loop-detect action error-down
```

当 gi0/1 检测到下联环路时，提示下面信息，并 shutdown 端口。

```
LOOPDETECT-4:   %Loop error detected on interface GigabitEthernet 0/1, set
interface err-down.
```

案例二：配置端口 gi0/1 在 vlan10 域内做环路检测。

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#vlan 10
SWITCH(config)#loop-detect enable
SWITCH(config)#interface gigabitEthernet 0/1
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)# loop-detect enable
SWITCH(config-if)# loop-detect vlan 10
```

Gi0/1 口对外发送带 tag，vid=10 的环路检测报文，若检测到 vlan10 域内存在环路，输出 log 提示信息。

```
LOOPDETECT-4:   %Loop error detected on interface GigabitEthernet 0/1.
```

案例三：配置端口 gi0/1 口开启环路检测，配置环路告警信息 trap 服务器 192.168.64.1。

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#snmp-server group public v2c read all write all
SWITCH(config)#snmp-server community public
SWITCH(config)#snmp-server host 192.168.64.1 traps v2c  community public
SWITCH(config)#loop-detect enable
SWITCH(config)# loop-detect trap enable
SWITCH(config)#interface gigabitEthernet 0/1
SWITCH(config-if)# loop-detect enable
```

当 gi0/1 口检测到下联环路，snmp 服务器接收到环路告警 trap 信息。

15.4. 显示命令

15.4.1. 显示 LOOP-DETECT 信息

```
SWITCH#show loop-detect
Global configuration:
    Loop-detect State            : Enabled
    Loop-detect Interval         : 5
    Loop-detect trap             : Enabled

Interface gigabitEthernet 0/1:
    Loop-detect State            : Enabled
    Loop-detect Action           : Alarm
    Loop-detect Action Last      : Normal
    Loop-detect Action Last Time : --
    Loop-detect Action Count     : 0
    Loop-detect Vlans            : 10, 20, 30-32
```

显示的信息含义：

全局信息	
Loop-detect State	全局使能状态，Enabled 或 Disabled
Loop-detect Interval	环路检测报文发送间隔，单位秒
Loop-detect trap	是否使能告警消息 trap 到服务器，Enabled 或 Disabled
接口信息	
Loop-detect State	接口使能状态，Enabled 或 Disabled
Loop-detect Action	检测到环路后动作，支持 alarm、error-down 两种
Loop-detect Action Last	最后一次发生故障： Normal：正常 Alarm：输出告警 Error-down：端口 down 掉
Loop-detect Action Last Time	最后一次故障发生时间： 未发生过故障：-- 发生过，例如：2022-01-10 22:45:23
Loop-detect Action Count	故障发生次数
Loop-detect Vlans	环路报文指定 vlan 链表

16. 配置 GVRP

16.1. GVRP 概述

16.1.1. GVRP 简介

GVRP（GARP VLAN Registration Protocol，GARP VLAN 注册协议）是一种动态配置 VLAN 属性的协议，是 GARP（Generic Attribute Registration Protocol，通用属性注册协议）的一种应用。它通过 GARP 协议注册传播 VLAN 属性，在 802.1Q Trunk 口上，实现 VLAN 动态创建删除。

16.1.2. GARP 简介

GARP 提供了一种机制，协助同一交换网内的成员相互分发、传播和注册 VLAN、组播地址等信息。 遵循 GARP 协议的应用实体称为 GARP 应用。目前主要的 GARP 应用为 GVRP 和 GMRP。
GVRP 是一种 GARP 应用。它可以动态配置和扩散 VLAN 属性，在 802.1Q Trunk 口上，实现 VLAN 动态自动注册/注销功能。
GMRP（GARP Multicast Registration Protocol，GARP 组播注册协议）是另一种 GARP 应用。主要提供一种类似于 IGMP 探查技术的受限组播扩散功能。
GARP 协议在 802.1D 中定义。

16.1.3. 端口注册模式

GVRP 的端口注册模式有三种：Normal、Fixed 和 Forbidden：
Normal 模式：允许该端口动态注册、注销 VLAN，传播动态 VLAN 以及静态 VLAN 信息。
Fixed 模式：禁止该端口动态注册、注销 VLAN，只传播静态 VLAN 信息，不传播动态 VLAN 信息。也就是说被设置为 Fixed 模式的 Trunk 口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是手动配置的那部分。
Forbidden 模式：禁止该端口动态注册、注销 VLAN，不传播除 VLAN1 以外的任何 VLAN 信息。也就是说被配置为 Forbidden 模式的 Trunk 端口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是 VLAN 1。

16.1.4. 消息与定时器

GARP 消息
GARP 成员之间的信息交换借助于消息的传递来完成，主要有三类消息起作用，分别为 Join 消息、Leave 消息和 LeaveAll 消息。
当一个 GARP 应用实体希望其它设备注册自己的属性信息时，它将对外发送 Join 消息；当收到其它实体的 Join 消息或本设备静态配置了某些属性，需要其它 GARP 应用实体进行注册时，它也会向外发送 Join 消息。
当一个 GARP 应用实体希望其它设备注销自己的属性信息时，它将对外发送 Leave 消息；当收到其它实体的 Leave 消息注销某些属性或静态注销了某些属性后，它也会向外发送 Leave 消息。
每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后 GARP 应用实体将对外发送 LeaveAll 消息，LeaveAll 消息用来注销所有的属性，以使其它 GARP 应用实体重新注册本实体上所有的属性信息。
Join 消息、Leave 消息与 LeaveAll 消息配合确保信息的重新注册或注销。
通过消息交互，所有待注册的属性信息可以传播到同一局域网配置了 GARP 的所有设备上。
GARP 定时器

GARP 消息发送的时间间隔是通过定时器来实现的，GARP 定义了四种定时器，用于控制 GARP 消息的发送周期。

Hold 定时器：当 GARP 应用实体接收到其它设备发送的注册信息时，不会立即将该注册信息作为一条 Join 消息对外发送，而是启动 Hold 定时器，当该定时器超时后，GARP 应用实体将此时段内收到的所有注册信息放在同一个 Join 消息中向外发送，从而节省带宽资源。

Join 定时器：GARP 应用实体可以通过将每个 Join 消息向外发送两次来保证消息的可靠传输，在第一次发送的 Join 消息没有得到回复的时候，GARP 应用实体会第二次发送 Join 消息。两次 Join 消息发送之间的时间间隔用 Join 定时器来控制。

Leave 定时器：当一个 GARP 应用实体希望注销某属性信息时，将对外发送 Leave 消息，接收到该消息的 GARP 应用实体启动 Leave 定时器，如果在该定时器超时之前没有收到 Join 消息，则注销该属性信息。

LeaveAll 定时器：每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后，GARP 应用实体将对外发送 LeaveAll 消息，以使其它 GARP 应用实体重新注册本实体上所有的属性信息。随后再启动 LeaveAll 定时器，开始新的一轮循环。

16.1.5. 报文格式

GVRP 的协议报文封装在以太网帧中，报文格式下图所示。

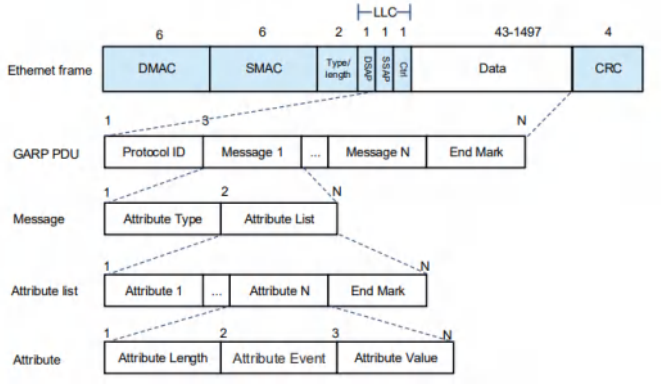


表 GVRP 以太网报文字段含义

报文字段	字节	字段含义
Protocol ID	2	协议 ID，固定 0x0001
Message	N	消息内容，支持 N 条消息
Attribute type	1	属性类型，GVRP 固定位 0x01
Attribute list	N	属性列表，由多个属性与 end mask 组成
Attribute	N	属性内容
Attribute length	1	属性内容长度
Attribute event	1	事件，包括： 0x0:LeaveAll Event 0x1:JoinEmpty Event 0x2:JoinIn Event 0x3:LeaveEmpty Event 0x4:LeaveIn Event 0x5:Empty Event
Attribute value	N	属性值
End mask	1	结束标志，固定为 0x00

16.2. 配置命令

16.2.1. GVRP 使能控制

- 全局使能 GVRP

命令	SWITCH(config)#**gvrp enable** SWITCH(config)#**no gvrp enable**
描述	全局使能 GVRP 功能 缺省情况下，全局的 GVRP 功能处于未使能状态

- 接口上使能 GVRP 功能

命令	SWITCH(config-if)#**gvrp enable** SWITCH(config-if)#**no gvrp enable**
描述	接口使能 GVRP 功能 缺省情况下，接口的 GVRP 功能处于未使能状态 开启接口 GVRP 功能必须在 Trunk 类型接口操作 在全局 GVRP 使能情况下，接口使能 GVRP，接口上 GVRP 功能才生效

16.2.2. 配置接口模式

命令	SWITCH(config-if)#**gvrp registration (fixed | forbidden | normal)** SWITCH(config-if)#**no gvrp registration**
描述	Normal 模式：允许该接口动态注册、注销 VLAN，传播动态 VLAN 以及静态 VLAN 信息。 Fixed 模式：禁止该接口动态注册、注销 VLAN，只传播静态 VLAN 信息，不传播动态 VLAN 信息。也就是说被设置为 Fixed 模式的 Trunk 接口，即使允许所有 VLAN 通过，实际通过的 VLAN 也只能是手动配置的那部分。 Forbidden 模式：禁止该接口动态注册、注销 VLAN，不对外传播任何的 VLAN 信息。

16.2.3. 配置定时器

命令	SWITCH(config)#**gvrp timer (join | leave | leaveall)** CENTISEC SWITCH(config)#**no gvrp timer**
描述	设置 GARP 定时器的值 Join：范围<20 32765>，默认 20，单位厘秒，要求小于等于 1/3 Leave 定时器值 Leave：范围<20 32765>，默认 60，单位厘秒，要求大于等于 3 倍 join 定时器值，小于 Leaveall 定时器值 Leaveall：范围<20 32765>，默认 1000，单位厘秒，要求大于 Leave 定时器值

说明

✦ 在全网有多台设备的情况下，各个设备的 LeaveAll 定时器的取值可能不相同，但每台设备都将以全网最小的 LeaveAll 定时器为准发送 LeaveAll 消息。因为每次 LeaveAll 定时器超时后发送 LeaveAll 消息，其它的设备接收到之后都会清零 LeaveAll 定时器，因此即使全网存在很多不同的 LeaveAll 定时器，也只

有最小的那个 LeaveAll 定时器起作用。

16.2.4. 清除统计信息

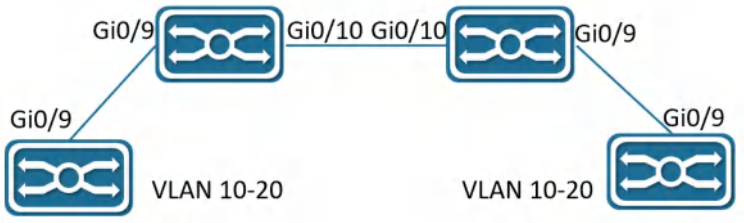
命令	SWITCH#**clear gvrp statistics** (| **interface** IFNAME)
描述	清除端口事件统计信息 不带 interface 参数，清除所有端口 带 interface 参数，清除具体某端口

16.3. 配置案例

16.3.1. 典型配置案例

案例需求：

SW1、SW2、SW3、SW4 通过 trunk 口相连，SW1 和 SW4 上存在静态 VLAN 10～20，要求 SW2、SW3 自动学习到这些 VLAN，而无需手工配置。在各台 SW 全局和接口上启用 GVRP，即可实现设备之间 VLAN 信息的动态注册和更新。



操作步骤

SW1 配置：

```
SWITCH(config)#Vlan  10-20
SWITCH(config)#gvrp enable
SWITCH(config)#interface gigabitEthernet 0/9
SWITCH(config-if)switchport mode trunk
SWITCH(config-if)gvrp enable
```

SW2 配置：

```
SWITCH(config)#gvrp enable
SWITCH(config)#interface gigabitEthernet 0/9-10
SWITCH(config-if)switchport mode trunk
SWITCH(config-if)gvrp enable
```

SW3 配置：

```
SWITCH(config)#gvrp enable
SWITCH(config)#interface gigabitEthernet 0/9-10
SWITCH(config-if)switchport mode trunk
SWITCH(config-if)gvrp enable
```

SW4 配置：

```
SWITCH(config)#Vlan  10-20
SWITCH(config)#gvrp enable
SWITCH(config)#interface gigabitEthernet 0/9
SWITCH(config-if)switchport mode trunk
```

```
SWITCH(config-if)gvrp enable
```

验证配置结果：

在 SW2、SW3 上执行 show gvrp vlan，显示 gi0/9、gi0/10 动态学习到 vlan 10-20。

在 SW2、SW3 上执行 show vlan all，显示 gi0/9、gi0/10 属于 vlan 10-20。

16.4. 显示命令

16.4.1. 查看配置状态

```
SWITCH#show gvrp status
GVRP Global Information:
    Global State        :  Enabled
    Join Timer          :  20 centisec
    Leave Timer         :  60 centisec
    LeaveAll Timer      :  1000 centisec

GVRP Port Based Information:
Interface               State        Registration Mode
--------------------    --------     --------------------
gigabitEthernet0/3      Enabled      normal
 po1                     Enabled      normal
```

显示的信息定义：

GVRP Global Information:	全局配置状态信息
Global State	全局状态，Enabled 或 Disabled
Join Timer	Join 定时器时间
Leave Timer	Leave 定时器时间
LeaveAll Timer	Leaveall 定时器时间
GVRP Port Based Information:	端口配置状态信息，默认状态端口忽略不显示
Interface	端口名称
State	端口状态，Enabled 或 Disabled
Registration Mode	端口注册模式，Normal、Fixed、Forbidden

16.4.2. 查看 GVRP VLAN 信息

```
SWITCH#show gvrp vlan
Interface gigabitEthernet0/3:
    Static Vlan List    : 1
    Dynamic Vlan List   : 15-21
    Allow Vlan List     : all
Interface po1:
    Static Vlan List    : 1
    Dynamic Vlan List   : 1000-2000
    Allow Vlan List     : all
SWITCH#show gvrp vlan interface gigabitEthernet 0/3
Interface gigabitEthernet0/3:
    Static Vlan List    : 1
    Dynamic Vlan List   : 15-21
    Allow Vlan List     : all
```

显示的信息定义：

Static Vlan List	端口支持的静态 vlan 列表
Dynamic Vlan List	端口支持的动态 vlan 列表
Allow Vlan List	端口 allow vlan 列表

16.4.3. 查看报文统计

```
SWITCH#show gvrp statistics
Interface               Received        Transmitted     Drop
--------------------    ------------    ------------    --------
gigabitEthernet0/3      1462120         7202490         0
po1                     7181418         1790511         0
```

显示的信息定义：

Interface	端口名称
Received	接收 GVRP attribute 数
Transmitted	发送 GVRP attribute 数
Drop	丢弃 GVRP attribute 数

```
SWITCH#show gvrp statistics interface gigabitEthernet 0/3
Interface gigabitEthernet0/3:
    Received Valid Attributes           :  1017
    Transmitted Attributes              :  1
    Drop Invalid Attributes             :  0
    Received JoinEmpty Attributes       :  14
    Received JoinIn Attributes          :  2
    Received Empty Attributes           :  1001
    Received LeaveEmpty Attributes      :  0
    Received LeaveIn Attributes         :  0
    Received LeaveAll Attributes        :  0
    Transmitted JoinEmpty Attributes    :  1
    Transmitted JoinIn Attributes       :  0
    Transmitted Empty Attributes        :  0
    Transmitted LeaveEmpty Attributes   :  0
    Transmitted LeaveIn Attributes      :  0
    Transmitted LeaveAll Attributes     :  0
```

显示的信息定义：

Received Valid Attributes	接收到的有效 Attributes 总数
Transmitted Attributes	发送 Attributes 总数
Drop Invalid Attributes	丢弃的无效 Attributes 总数
Received JoinEmpty Attributes	接收到的 JoinEmpty Attributes 数
Received JoinIn Attributes	接收到的 JoinIn Attributes 数
Received Empty Attributes	接收到的 Empty Attributes 数
Received LeaveEmpty Attributes	接收到的 LeaveEmpty Attributes 数
Received LeaveIn Attributes	接收到的 LeaveIn Attributes 数
Received LeaveAll Attributes	接收到的 LeaveAll Attributes 数
Transmitted JoinEmpty Attributes	发送的 JoinEmpty Attributes 数
Transmitted JoinIn Attributes	发送的 JoinIn Attributes 数
Transmitted Empty Attributes	发送的 Empty Attributes 数
Transmitted LeaveEmpty Attributes	发送的 LeaveEmpty Attributes 数
Transmitted LeaveIn Attributes	发送的 LeaveIn Attributes 数
Transmitted LeaveAll Attributes	发送的 LeaveAll Attributes 数

17. 配置 L3

17.1. L3 概述

L3 功能包括三层口管理，ARP 管理以及路由管理。路由管理不包含动态路由管理。

- 三层口管理：

三层口是针对二层（交换）口而言的，一般分为路由口（普通物理端口或者聚合口切换为三层口）或者 SVI 口（Switch Virtual Interface，与一个 VLAN 相对应）。SVI 口是一个逻辑接口，架构在对应 VLAN 所包含的所有成员端口之上，与路由口不同，经过 SVI 进行三层转发的报文，在输入时会先经过二层（比如 VLAN 过滤，地址学习）再经过三层，在输出时先经过三层再经过二层（比如 VLAN 输出规则）。

因特网协议（Internet Protocol，IP）使用逻辑虚拟的地址将数据包从源方发送到目的方，即 IP 地址。在网络层，路由设备使用 IP 地址完成数据包转发。(协议规范：RFC 1918：Address Allocation for Private Internets， RFC 1166：Internet Numbers)

三层口管理也包含三层口的 IP 地址维护。IP 地址由 32 位二进制组成，为了书写和描述方便，一般用点分十进制表示。点分十进制表示时，分为四组，每组 8 位，范围从 0~255，组之间用“.”号隔开，比如“192.168.1.1”就是用十进制表示的 IP 地址。IP 地址顾名思义，自然是 IP 层协议的互连地址。32 位的 IP 地址由两个部分组成：1）网络地址部分，表明是哪个网络；2）主机地址部分，表明是网络中的哪个主机。IP 地址的网络地址部分和主机地址地址部分由网络掩码来划分，网络掩码也是一个 32 比特的数值，由前面若干个比特“1”和后面若干个比特“0”组成，IP 地址与网络掩码相与得到的就是对应网络地址部分。同样，网络掩码也可以直接通过掩码长度来表示。比如“192.168.1.1 255.255.255.0”和“192.168.1.1/24”表示相同的 IP 地址。

本设备三层口不支持配置 second IP 地址，即一个三层口最多配置一个 IP 地址。当一个三层口配置了 IP 地址，就确定了一个网段，同台设备的不同三层口必须属于不同的网段，不同三层口配置的 IP 地址必须属于不同网段。SVI 表示的三层口，对应的 VLAN 作为该三层口的唯一标识。

设备的不同三层口划分了不同网段后，这些不同网段（比如 VLAN1 和 VLAN2）间的转发就称为“三层转发”（跨越网段，或者说跨越了不同 VLAN)。

- ARP 管理：

在局域网中，每个 IP 网络设备都有两个地址：1）本地地址，由于它包含在数据链路层的帧头中，更准确地说应该是数据链路层地址，但实际上对本地地址进行处理的是数据链路层中的 MAC 子层，因此习惯上称为 MAC 地址，MAC 地址在局域网上代表着 IP 网络设备；2）网络地址，在互联网上代表着 IP 网络设备，同时它也说明了该设备所属的网络。

局域网上两台 IP 设备之间需要通信，必须要知道对方的 48 比特的 MAC 地址。根据 IP 地址来获知 MAC 地址的过程称为地址解析。地址解析的方式有两类：1）地址解析协议（ARP）；2）代理地址解析协议（Proxy ARP)。关于 ARP 、Proxy ARP，分别在 RFC 826，RFC 1027 文档中描述。

ARP(Address Resolution Protocol，地址解析协议)是用来绑定 MAC 地址和 IP 地址的，以 IP 地址作为输入，ARP 能够知道其关联的 MAC 地址。一旦知道了 MAC 地址，IP 地址与 MAC 地址对应关系就会保存在设备的 ARP 缓存中。有了 MAC 地址，IP 设备就可以封装链路层的帧，然后将数据帧发送到局域网上去。以太网上 IP 和 ARP 的封装为 Ethernet II 类型。

ARP 表项分为两类：来源于 ARP 协议生成的动态表项，来源于静态配置的静态表项。动态 ARP 表项靠 IP 报文触发打通形成，打通过程是一个 ARP 请求/应答的过程，打通后形成的 ARP 表项，若后续不可达，会自动老化。静态 ARP 表项不需要打通，也不会老化。

- 路由管理：

路由管理负责管理路由表，整合各种路由协议下发的路由，进行优选。路由表中根据来源不同，通常分为

以下三类：

- 直连路由：链路层协议发现的路由，也称为接口路由。直连路由由三层口配置 IP 地址时自动生成，路由前缀为该三层口直连的网络。
- 静态路由：网络管理员手工配置的。
- 动态路由：动态路由协议（比如 RIP， OSPF）发现的路由。

本设备不支持动态路由协议，因此，也不支持动态路由。
路由表项由两个部分组成：

- 前缀：由一个 IP 地址及网络掩码(或者掩码长度)来表示，指路由表项所确定的目的网络或者主机（当掩码长度为 32 表示主机）。
- 直连或者下一跳：直连表示目的网络或者主机属于直连网络，直连路由即属于此情况，在配置静态路由时，指定三层口而非 IP 地址，也会生成此类路由表项；下一跳由一个 IP 主机地址来表示，表示了要到达目的网络或主机，需要先转发到该 IP 地址表明的 IP 网络设备。

根据路由表项进行 IP 报文转发时，若该路由表项指定的是下一跳，链路层封装查询 ARP 时，使用下一跳的 IP，即链路层封装的目的 MAC 地址为下一跳的目的 MAC 地址。若该路由表项为直连的，则直接使用报文的目的 IP 进行 ARP 查询，即链路层封装的目的 MAC 地址为报文最终目的的 MAC 地址。不管哪种方式，若 ARP 查询不到，则会触发路由打通（生成动态 ARP 表项），若无法打通，IP 报文无法完成转发，将被丢弃。
路由表项间可能存在包含关系（根据掩码长度不同），所以，路由查找过程满足 LPM（Longest Prefix Match，最长前缀匹配）。即 IP 报文转发进行路由查找时，若同时命中多个路由表项，则选择前缀的掩码长度最长的那个路由表项。

17.2. 配置命令

17.2.1. 配置/删除 SVI 口 IP 地址

命令	**配置三层口 IP 地址：** SWITCH(config)#int vlan10 SWITCH(config-if)#**ip address** IPADDR/MASKLEN 或者 SWITCH(config-if)#**ip address** IPADDR MASK **删除三层口 IP 地址：** SWITCH(config)#int vlan10 SWITCH(config-if)#**no ip address** IPADDR/MASKLEN 或者 SWITCH(config-if)#**no ip address** IPADDR MASK **查看三层口 IP 地址：** SWITCH#**show ip interface brief**
描述	在 SVI 的接口模式下进行配置。 当 VLAN 创建时，SVI 自动创建，VLAN 删除时，SVI 自动删除。int vlanXX 是进入该 SVI 的接口模式，而非创建 SVI 口，因此，当 SVI 不存在（对应 VLAN 不存在）时，进入该 SVI 的接口模式将会失败。同时，当 SVI 删除时，其上配置的 IP 地址会自动清除。 三层口支持进行 IP 地址配置更新，与删除再配置效果一样。不同三层口配置的 IP 地址必须属于不同网段。

	三层口不支持配置 second ip。 注意：配置本命令后，系统会将管理 IP 配置清除(参考:配置管理 IP)，转而使用三层口 IP 地址作为设备管理 IP。

17.2.2. 配置/删除路由口 IP 地址

命令	**配置路由口 IP 地址：**
	SWITCH(config)#**interface** gigabitEthernet0/1
	SWITCH(config-if)#**no switchport**
	SWITCH(config-if)#**ip address** IP(A.B.C.D/M)
	或者
	SWITCH(config-if)#ip address IP(A.B.C.D) MASK(A.B.C.D)
	
	删除三层口 IP 地址：
	SWITCH(config)# interface gigabitEthernet0/1
	SWITCH(config-if)#no ip address IP(A.B.C.D/M)
	或者
	SWITCH(config-if)#no ip address IP(A.B.C.D) MASK(A.B.C.D)
	SWITCH(config-if)#switchport

描述	在接口模式下进行配置。 在配置路由口 IP 前，由于接口的默认属性是二层端口属性，因此需要使用 no switchport 命令将端口从二层端口属性切换成三层的路由口属性，然后再使用 ip address 命令进行路由口的 IP 配置，反之，将路由口切换会二层端口属性，使用 switchport 命令。 三层口支持进行 IP 地址配置更新，与删除再配置效果一样。不同三层口配置的 IP 地址必须属于不同网段。 三层口不支持配置 second ip。

17.2.3. 配置/删除静态 ARP 表项

命令	SWITCH(config)#**arp** IPADDR MACADD SWITCH(config)#**no arp** IPADDR
描述	在全局配置模式下进行配置。 静态 ARP 配置的 IP 地址必须属于直连网段，否则配置失败。 静态 ARP 优先级高于动态 ARP，当两者冲突，以静态 ARP 生效。 当三层口的 IP 地址删除或者三层口删除，若静态 ARP 的 IP 地址属于该三层口的直连网段，则该静态 ARP 失效（通过 show arp 可以看到不存在该表项，但 show run 可以看到配置还在）；同样，当某个三层口配置 IP 地址，其 IP 地址属于该三层口的直连网段的 ARP 表项将会从无效状态变为有效状态。(通过 show arp 可以看到 ARP 表项存在)。

17.2.4. 清除 ARP 缓存

命令	SWITCH#**clear arp-cache**
描述	在特权模式下进行 ARP 缓存的清除。 该命令只是清除动态 ARP 表项，静态 ARP 表项不会被清除。

17.2.5. 配置/删除静态路由

命令	SWITCH(config)#**ip route** {IPADDR/MASKLEN) | IPADDR MASK} {NH_IPADDR | IFNAME} SWITCH(config)#**no ip route** {IPADDR/MASKLEN | IPADDR MASK} {NH_IPADDR | IFNAME}
描述	在全局配置模式下进行配置。 不支持递归路由（配置的下一跳 IP 必须属于直连网段）； 路由前缀不能属于直连网段（即直连路由自动生成，不能静态配置）。 当三层口配置 IP 地址时，若某条静态路由表项的前缀属于该三层口的直连网段，则该静态路由自动删除，以 LOG 方式提示； 当三层口删除 IP 地址或者三层口删除时，若某条静态路由表项的下一跳 IP 属于该三层口的直连网段，则该静态路由自动删除，以 LOG 方式提示。

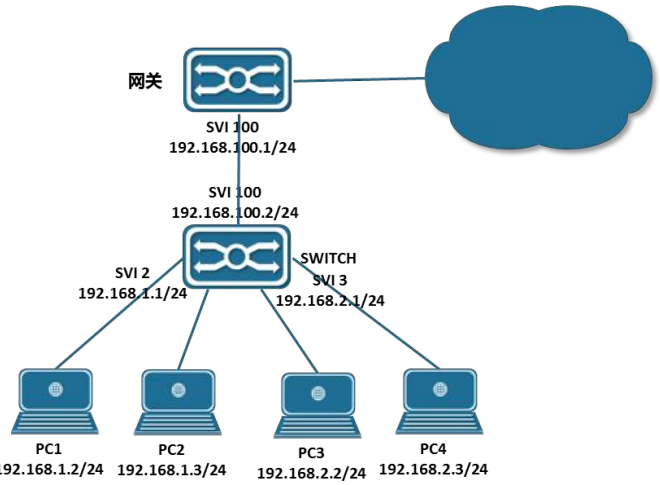
17.2.6. 配置 ECMP 策略

如果网络环境中存在冗余的链路，即到达同一个目的地址的路由存在多个下一跳。在支持 ECMP 技术的设备上，多个下一跳可以同时工作，使得冗余链路得到充分利用，并且支持在冗余链路发生链路故障时将流量切换到其它的冗余链路上提升网络的可靠性和稳定性。

ECMP(Equal-Cost Multipath Routing，等价路由)，该技术使得设备可以并发使用对应路由的多个下一跳链路，根据所设置的均衡因子在多个下一跳链路中将流量进行均衡分配；且支持故障链路的快速切换。

17.3. 配置案例

案例一：弱三层网关



Switch 作为弱三层网关，为真正的网关减少 ARP 负担。

- 配置 PC：

  PC1，PC2 和 PC3 按照如图所示配置 IP 地址，同时指定网关，比如 PC1 和 P2 的网关为 192.168.1.1。

- 配置 SWITCH：

  - 配置三层口和 IP 地址：（假设连接 PC1-PC4 的接口为 gigabitEthernet0/1-4，上链接口为 gigabitEthernet0/17）

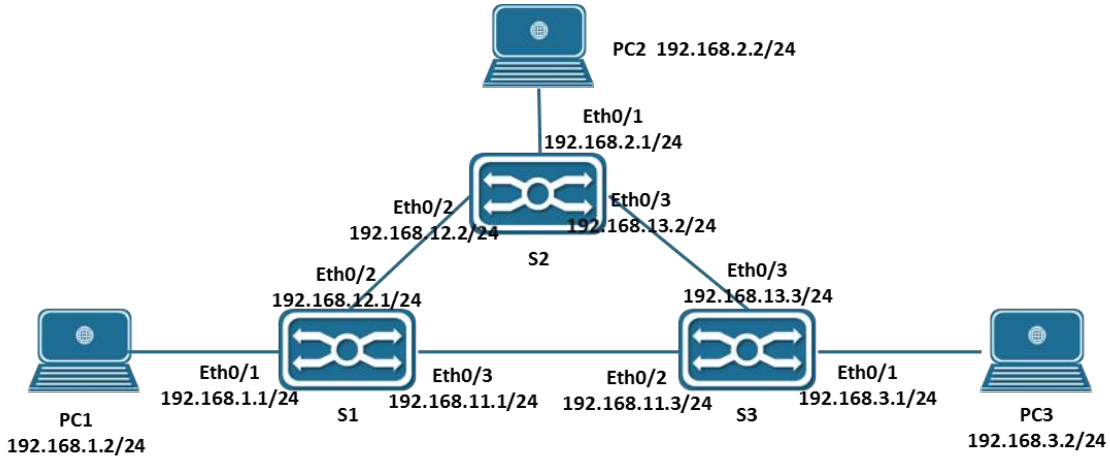
```
SWITCH(config)#vlan 2-3,100
```

```
SWITCH(config)#interface gigabitEthernet0/1-2
SWITCH(config-if)#switch access vlan 2
SWITCH(config)#interface gigabitEthernet0/3-4
SWITCH(config-if)#switch access vlan 3
SWITCH(config)#interface gigabitEthernet0/17
SWITCH(config-if)#switch access vlan 100
SWITCH(config)#int vlan2
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config)#int vlan3
SWITCH(config-if)#ip address 192.168.2.1/24
SWITCH(config)#int vlan100
SWITCH(config-if)#ip address 192.168.100.2/24
```

- 配置静态路由（默认路由）：

```
SWITCH(config-if)ip route 0.0.0.0/0 192.168.100.1
```

案例二：内网三层互联



如上图的网络环境，PC1，PC2 和 PC3 分别通过 S1，S2 和 S3 进行互联。

- 配置 PC

  PC1，PC2 和 PC3 按照如图所示配置 IP 地址，同时指定网关，比如 PC1 的网关为 192.168.1.1。

- 配置 S1

  - 配置三层口和 IP 地址：

```
SWITCH(config)#vlan 2-4
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#switch access vlan 2
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#switch access vlan 3
SWITCH(config)#interface gigabitEthernet0/3
SWITCH(config-if)#switch access vlan 4
SWITCH(config)#int vlan2
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config)#int vlan3
SWITCH(config-if)#ip address 192.168.12.1/24
SWITCH(config)#int vlan4
SWITCH(config-if)#ip address 192.168.13.1/24
```

  - 配置静态路由

```
SWITCH(config)#ip route 192.168.2.0/24 192.168.12.2
```

```
SWITCH(config)#ip route 192.168.3.0/24 192.168.11.3
```

- S2 和 S3 类似 S1 的配置。

17.4. 显示命令

- 显示 ARP 表项

```
SWITCH#show arp
Address                  HWaddress             Interface      Type
192.168.1.238         00:00:00:00:04:86       vlan2         Static
192.168.2.46           00:00:00:00:05:45       vlan3         Static
192.168.3.110         00:00:00:00:08:59       vlan4         Static
192.168.0.12           00:00:00:00:00:09       vlan1         Static
192.168.0.1             00:0e:c6:d8:c7:f7         vlan1          Dynamic
10.100.2.2              00:01:a0:00:10:11       GiE0/2         Dynamic
```

- 显示路由表项

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default
IP Route Table for VRF "default"
Gateway of last resort is 192.168.1.3 to network 0.0.0.0
S*      0.0.0.0/0 [1/0] via 192.168.1.3, vlan2
S       192.168.0.0/16 [1/0] via 192.168.0.10, vlan1
C       192.168.0.0/24 is directly connected, vlan1
C       192.168.1.0/24 is directly connected, vlan2
C       192.168.2.0/24 is directly connected, vlan3
C       192.168.3.0/24 is directly connected, vlan4
C       10.100.2.0/30 is directly connected, gigabitEthernet0/2
```

18. 配置 ACL

18.1. ACL 概述

ACL（Access Control List，访问控制列表）通过配置对报文的匹配规则和处理操作来实现包过滤的功能。可以有效防止非法用户对网络的访问，同时也可以控制流量，节约网络资源。

由 ACL 定义的数据包匹配规则，也可以被其它需要对流量进行区分的功能引用，如 QoS 中流分类规则的定义。

ACL 通过一系列匹配条件对数据包进行分类，这些条件可以是数据包的 SMAC、DMAC、SIP、DIP 等。

根据匹配条件，可将 ACL 分为以下几种：

基于 IP 的标准 ACL：只根据数据包的源 IP 地址制定规则。

基于 IP 的扩展 ACL：根据数据包的源 IP 地址、目的 IP 地址、ETYPE、protocol 制订规则。

基于 MAC 的 ACL：根据数据包的源 MAC 地址、目的 MAC 地址制订规则。

基于 IPV6 的 ACL：根据数据包的源 IPV6 地址、目的 IPV6 地址、protocol 等制订规则。

18.2. 配置命令

18.2.1. 配置 IP 标准 ACL

- 配置基于 IP 的标准 ACL 规则

命令	SWITCH(config)# **ip-access-list** {<1-99> | <1300-1999>} {**permit** | **deny**} {**host** SIPADDR | SIPADDR SIPADDRMASK | **any**} SWITCH(config)#**no ip-access-list** {<1-99> | <1300-1999>}
描述	创建/删除基于 IP 的标准 ACL 规则

- 创建标准 IP ACL

命令	SWITCH(config)#**ip-access-list standard** {<1-99> | <1300-1999> | NAME} SWITCH(config)#**no ip-access-list standard** {<1-99> | <1300-1999> | NAME}
描述	创建/删除标准 IP ACL，并切换为 IP 标准 ACL 模式

- 配置标准 IP ACL 规则

命令	SWITCH(config-std-acl)# [SN] {**permit** | **deny**} {**host** SIPADDR | SIPADDR SIPADDRMASK | **any**} SWITCH(config-std-acl)# no {**permit** | **deny**} {**host** SIPADDR | SIPADDR SIPADDRMASK | **any**} SWITCH(config-std-acl)# **no** SN
描述	创建/删除一条标准 IP ACL 规则 SN：每条规则的序列号(1-2147483647)

18.2.2. 配置 IP 扩展 ACL

- 配置基于 IP 的扩展 ACL 规则

命令	SWITCH(config)# **ip-access-list** {<100-199> | <2000-2699>} {**permit** | **deny**} PROTOCOL {**host** SIPADDR | SIPADDR SIPADDRMASK | **any**} [**eq** SPORT] { **host** | DIPADDR DIPADDRMASK | **any**} [**eq** DPORT] SWITCH(config)#**no ip-access-list** {<100-199> | <2000-2699>}

描述	创建/删除基于 IP 的扩展 ACL 规则 PROTOCOL 列表： <0-255>：指定 protocol 的 ID any：任意 protocol 报文 gre：GRE 报文 icmp: ICMP 报文 igmp: IGMP 报文 ip：IPv4 报文(0x4) ipcomp：IPCOMP 报文 ospf：OSPF 报文 pim： PIM 报文 rsvp：RSVP 报文 tcp：TCP 报文 udp：UDP 报文 vrrp：VRRP 报文 eq 选项仅 TCP 与 UDP 协议可选 下面端口号名称，可以使用端口号名称或者端口号来指定具体的端口： TCP 端口号列表： <0-65535> 指定端口号 bgp(179) ftp(21) ftp-data (20) login(513) pop2(109) pop3(110) smtp(25) telnet(23) www(80) UDP 端口号列表： <0-65535> 指定端口号 bootpc (68) bootps (67) domain (53) echo (7) rip (520) snmp (161) syslog (514) tftp (69)

- 创建扩展 IP ACL

命令	SWITCH(config)# **ip-access-list extended** {<100-199> | <2000-2699> | NAME} SWITCH(config)# **no ip-access-list extended** {<100-199> | <2000-2699> | NAME}
描述	创建/删除扩展 IP ACL，并切换为 IP 扩展 ACL 模式

- 配置扩展 IP ACL 规则

命令	SWITCH(config-ext-acl)# [SN] {**permit** | **deny**} PROTOCOL {**host** SIPADDR | SIPADDR SIPADDRMASK | **any**} [**eq** SPORT] { **host** DIPADDR | DIPADDR DIPADDRMASK | **any**} [**eq** DPORT] SWITCH(config-ext-acl)# **no** {**permit** | **deny**} PROTOCOL {**host** SIPADDR | SIPADDR SIPADDRMASK | **any**} [**eq** SPORT] { **host** DIPADDR | DIPADDR DIPADDRMASK | any} [**eq** DPORT]

	SWITCH(config-ext-acl)# **no** SN
描述	创建/删除一条扩展 IP ACL 规则 SN：每条规则的序列号(1-2147483647) PROTOCOL 列表： <0-255>：指定 protocol 的 ID any：任意 protocol 报文 gre：GRE 报文 icmp: ICMP 报文 igmp: IGMP 报文 ip：IPv4 报文(0x4) ipcomp：IPComp 报文 ospf：OSPF 报文 pim： PIM 报文 rsvp：RSVP 报文 tcp：TCP 报文 udp：UDP 报文 vrrp：VRRP 报文 下面端口号名称，可以使用端口号名称或者端口号来指定具体的端口： eq(仅 TCP 与 UDP) TCP 端口号列表： <0-65535> 指定端口号 bgp(179) ftp(21) ftp-data (20) login(513) pop2(109) pop3(110) smtp(25) telnet(23) www(80) UDP 端口号列表： <0-65535> 指定端口号 bootpc (68) bootps (67) domain (53) echo (7) rip (520) snmp (161) syslog (514) tftp (69)

18.2.3. 配置 MAC ACL

- 配置基于 MAC 的 ACL 规则

命令	SWITCH(config)# **mac-access-list** <200-699> {**permit** | **deny**} {**host** SMAC | SMAC SMACMASK | **any**} {**host** DMAC | DMAC DMACMASK | **any**} [**ethertype** ETYPE] [**cos** VALUE] SWITCH(config)# **no mac-access-list** <200-699>
描述	创建/删除基于 MAC 的 ACL 规则 ethertype: 以太网协议类型 (0x05DD-0xFFFF)

	cos: 报文的优先级值（0-7）

- 创建 MAC ACL

命令	SWITCH(config)# **mac-access-list** { <200-699> | NAME} SWITCH(config)# **no mac-access-list** { <200-699> | NAME}
描述	创建/删除标准 MAC ACL，并切换为 MAC ACL 模式

- 配置 MAC ACL 规则

命令	SWITCH(config-mac-acl)# [SN] {**permit** | **deny**} {**host** SMAC | SMAC SMACMASK | **any**} {**host** DMAC | DMAC DMACMASK | **any**} [**ethertype** ETYPE] [cos VALUE] SWITCH(config-mac-acl)# **no** {**permit** | **deny**} {**host** SMAC | SMAC SMACMASK | **any**} {**host** DMAC | DMAC DMACMASK | **any**} [**ethertype** ETYPE] [**cos** VALUE] SWITCH(config-mac-acl)# **no** SN
描述	创建/删除一条基于 MAC ACL 规则 SN：每条规则的序列号(1-2147483647) ethertype: 以太网协议类型 (0x05DD-0xFFFF) cos: 报文的优先级别值（0-7）

18.2.4. 配置 IPV6 ACL

- 创建 IPV6 ACL

命令	SWITCH(config)# **ipv6-access-list** { NAME } SWITCH(config)# **no ipv6-access-list** { NAME }
描述	创建/删除 IPV6 ACL，并切换为 IPV6 ACL 模式

- 配置 IPV6 ACL 规则

命令	SWITCH(config-ipv6-acl)# [SN] {**permit** | **deny**} [PROTOCOL] {SOURCE-IPV6-PREFIX/PREFIX-LENGTH | **any** | **host** SOURCE-IPV6-ADDRESS} [**eq** SPORT] {DESTINATION- IPV6-PREFIX / PREFIX-LENGTH | **any**| **host** DESTINATION-IPV6-ADDRESS} [**eq** DPORT] SWITCH(config-ipv6-acl)# **no** {**permit** | **deny**} [PROTOCOL] {SOURCE-IPV6-PREFIX/PREFIX-LENGTH | **any** | **host** SOURCE-IPV6-ADDRESS} [**eq** SPORT] {DESTINATION- IPV6-PREFIX / PREFIX-LENGTH | **any**| **host** DESTINATION-IPV6-ADDRESS} [**eq** DPORT] SWITCH(config-ipv6-acl)# **no** SN
描述	创建/删除一条 IPV6 ACL 规则 SN：每条规则的序列号(1-2147483647) PROTOCOL 列表： 　<0-255>：指定 protocol 的 ID 　any：任意 protocol 报文 　icmp：ICMP 报文 　tcp：TCP 报文 　udp：UDP 报文 下面端口号名称，可以使用端口号名称或者端口号来指定具体的端口： eq(仅 TCP 与 UDP) TCP 端口号列表：

	<0-65535> 指定端口号 bgp (179) ftp (21) ftp-data (20) login (513) pop2 (109) pop3 (110) smtp (25) telnet (23) www (80) UDP 端口号列表: <0-65535> 指定端口号 biff (512) bootpc (68) bootps (67) discard (9) dnsix (195) domain 53) echo (7) Isakmp (500) ntp (123) pim-auto-rp (496) rip (520) snmp (161) snmptrap (162) tftp (69)

说明

- ✦ 单个 ACL-ID 下最多可以配置 128 条规则;
- ✦ 掩码取反，如匹配 192.168.1.0/24 范围的 IP 地址，应配置 192.168.1.0 0.0.0.255;
- ✦ 可命名 ACL 的 name，首字符不能是数字;
- ✦ 基于 MAC 的 ACL，对 IPV6 报文不生效;
- ✦ 每个 ACL 的最后默认配置一条 deny any;

18.2.5. 其他配置项

- 配置 ACL 计数器

如果用户想在访问列表上开始报文匹配计数功能，请在该访问列表中的开启。

命令	SWITCH(config-std-acl)#**counter enable** SWITCH(config-std-acl)#**no counter enable**
描述	开启/关闭 ACL 的计数器 可在所有 ACL 模式下配置

- 清除 ACL 计数器

命令	SWITCH#**clear access-list counter** NAME
描述	清除 ACL 的计数值

- 配置 ACL 描述符

命令	SWITCH(config-std-acl)#**description** TEXT SWITCH(config-std-acl)#**no description**
描述	配置/删除 ACL 的描述符 TEXT：描述符（最多 64 字符） 可在所有 ACL 模式下配置

- 触发 ACL 序列号重新排序

SN 为规则表项的序号，取值范围为[1,2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文，如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号起始值为 10，递增值为 10。

命令	SWITCH(config-std-acl)#**resequence** START STEP SWITCH(config-std-acl)#**no resequence**
描述	对序列号重新排序 START：起始位置（缺省值:10, 范围<1-2147483647>） STEP：步长（缺省值:10, 范围<1-2147483647>） 可在所有 ACL 模式下配置

说明

✦ 序列号唯一；

✦ 配置 ACL 表项时，若未指定序列号，则会在当前最大的序列号后按步长进行指定（超出设定范围则无法添加规则）；

- 配置 ACL 应用在端口上

命令	SWITCH(config-if)#**access-group** ACLNAME { **in** | **out** } SWITCH(config-if)#**no access-group** ACLNAME { **in** | **out** }
描述	配置/删除 ACL 应用在端口上

说明

✦ 当 ACL 已经应用在端口上或已经配置为 QOS 的流匹配规则时，若需要添加删除规则，需先从端口或 QOS 的流匹配规则中解应用；

✦ 聚合口不支持 out 方向的 ACL 应用，聚合口的成员口不支持 ACL 应用；

✦ VLAN 端口不支持的 ACL 应用；

18.3. 配置案例

案例一：对端口 gigabitEthernet0/1 入口报文进行过滤，放行 SIP 为 192.168.1.0/24 的报文，其他报文丢弃。

- 配置 ACL 规则：

```
SWITCH(config)#ip-access-list 1 permit 192.168.1.0 0.0.0.255
```

或

```
SWITCH(config)#ip-access-list standard 1
SWITCH(config-std-acl)#permit 192.168.1.0 0.0.0.255
```

- 将 ACL 应用在端口 gigabitEthernet0/1 上

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#access-group 1 in
```

案例二：对端口 gigabitEthernet0/1 入口报文进行过滤，拒绝主机 IP 为 192.168.1.2 发送的报文类型为 TCP 且源端口号为 40 的报文，其他报文通过

- 配置 ACL 规则：

```
SWITCH(config)#ip-access-list 100 deny tcp host 192.168.1.2 eq 40 any
SWITCH(config)#ip-access-list 100 permit any any any
```

或

```
SWITCH(config)#ip-access-list extended 100
SWITCH(config-ext-acl)#deny tcp host 192.168.1.2  eq 40 any
SWITCH(config-ext-acl)#permit any any any
```

- 将 ACL 应用在端口 gigabitEthernet0/1 上

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#access-group 100 in
```

案例三：对端口 gigabitEthernet0/1 出口报文进行过滤，拒绝 MAC 为 0000.0047.5124 的主机发送的以太网类型为 0x804 报文，其他报文通过

- 配置 ACL 规则：

```
SWITCH(config)#mac-access-list 200 deny host 0000.0047.5124 any ethertype
0x804
SWITCH(config)#mac-access-list 200 permit any any
```

或

```
SWITCH(config)#mac-access-list 200
SWITCH(config-mac-acl)#deny host 0000.0047.5124 any ethertype 0x804
SWITCH(config-mac-acl)#permit any any
```

- 将 ACL 应用在端口 gigabitEthernet0/1 上

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#access-group 200 out
```

案例四：对端口 gigabitEthernet0/1 入口报文进行过滤，放行目的主机的 IPv6 地址为::D0F8:1900:9F51:0000 的报文，其他报文丢弃。

- 配置 ACL 规则：

```
SWITCH(config)#ipv6-access-list ip6-acl
SWITCH(config-ipv6-acl)#permit any any host ::D0F8:1900:9F51:0000
```

- 将 ACL 应用在端口 gigabitEthernet0/1 上

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#access-group ip6-acl in
```

案例五：对端口 gigabitEthernet0/1 入口报文进行过滤，放行 SIP 为 192.168.2.1 的报文，其他报文丢弃，开启计数器查看报文统计。

- 配置 ACL 规则：

```
SWITCH(config)#ip-access-list standard 1
SWITCH(config-std-acl)#permit host 192.168.2.1
SWITCH(config-std-acl)#counter enable
```

- 将 ACL 应用在端口 gigabitEthernet0/1 上

```
SWITCH(config)#interface gigabitEthernet0/1
```

```
SWITCH(config-if)#access-group 1 in
```

- 端口 gigabitEthernet0/1 的入口处，发送 10 条 SIP 为 192.168.2.1 与 SIP 为 192.168.2.2 的报文，

查看报文统计

```
SWITCH#show access-list 1
ip-access-list standard 1
 10 permit host 192.168.2.1(10 match)
 deng any (10 match)
```

18.4. 显示命令

- 显示 ACL

```
SWITCH#show access-list 1
  ip-access-list standard 1
   10 permit host 1.1.1.1
   deny   any

SWITCH#show access-list 200
  mac-access-list 200
   10 permit host  0001.0002.0003 any
   deny any

SWITCH#show access-list ip6-acl
ipv6-access-list ip6-acl
 10 permit tcp host a::1 eq bgp any
 deny any
```

19. 配置 QOS

19.1. QOS 概述

QoS（Quality of Service，服务质量）指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力。

传统网络采用“尽力而为”的转发机制，当网络带宽充裕的时候，所有的数据流都得到了较好的处理，当网络发生拥塞的时候，所有的数据流都有可能被丢弃。为满足不同应用不同服务质量的要求，需要网络能根据用户的要求分配和调度资源，对不同的数据流提供不同的服务质量。

支持 QoS 功能的设备，能够提供传输品质服务，针对某种类别的数据流，可以为它赋予某个级别的传输优先级，来标识它的相对重要性，并使用设备所提供的各种优先级转发策略、拥塞避免等机制为这些数据流提供特殊的传输服务。

配置了 QoS 的网络环境，增加了网络性能的可预知性，并能够有效地分配网络带宽，更加合理地利用网络资源。

19.2. 配置命令

- 全局开启/关闭 QOS

命令	SWITCH(config)#**mls qos enable** SWITCH(config)#**no mls qos**
描述	全局开启、关闭 QOS 功能 默认关闭

- 配置队列调度算法

命令	SWITCH(config)#**mls qos algorithm** {**sp	wrr**}
描述	配置队列调度算法，支持 2 种模式：wrr（均衡调度）、sp（绝对调度） 默认为 wrr 模式

- 配置队列权重

命令	SWITCH(config)#**mls qos weight** <0-7> <0-32>
描述	配置队列权重，队列权重仅对 wrr 模式有效 默认所有队列权重为 1 当在 wrr 模式下，配置队列权重为 0，该队列调度权重为无穷大

- 配置端口信任模式

命令	SWITCH(config-if)#**mls qos trust** {**cos	dscp**} SWITCH(config-if)#**no mls qos trust**
描述	配置端口信任模式，默认 not trust 当处于 no trust 模式时，入口阶段根据端口默认 cos 修改报文 cos 字段以及 dscp 字段；当配置 trust cos 时，对于 untagged 报文同 no trust 模式，对于带 tag 报文，选择报文自带 cos；当配置 trust dscp 时，对于 ip 报文，选择报文自带 dscp，对于非 ip 报文，同 trust cos 模式。

- 配置端口默认 cos

命令	SWITCH(config-if)#**mls qos cos** <0-7> SWITCH(config-if)#**no mls qos cos**
描述	配置端口默认 cos，默认 cos 对入口端口不带 tag 报文生效 默认端口 cos 为 0

- 配置 cos-dscp 映射关系

命令	SWITCH(config)#**mls qos cos-dscp** <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> SWITCH(config)#**no mls qos cos-dscp**
描述	配置/删除 cos-dscp 映射关系 默认映射关系：0-0，1-8，2-16，3-24，4-32，5-40，6-48，7-56

- 配置 cos-queue 映射关系

命令	SWITCH(config)#**mls qos cos-queue** <0-7> <0-7> SWITCH(config)#**no mls qos cos-queue** <0-7>
描述	配置/删除 cos-queue 映射关系 默认映射关系：0-0，1-1，2-2，3-3，4-4，5-5，6-6，7-7

说明

✦ 在配置端口为 no trust、trust cos 或 trust dscp 且非 ip 报文时：cos-dscp 配置生效，根据映射关系修改报文 dscp，cos-queue 配置生效，根据映射关系修改报文出口队列；

- 配置 dscp-cos 映射关系

命令	SWITCH(config)#**mls qos dscp-cos** <0-63> to <0-7> SWITCH(config)#**no mls qos dscp-cos**
描述	配置 dscp-cos 映射关系 默认映射关系：<0-7>-0，<8-15>-1，<16-23>-2，<24-31>-3，<32-39>-4，<40-47>-5，<48-55>-6，<56-63>-7

- 配置 dscp-dscp 映射关系

命令	SWITCH(config)#**mls qos dscp-mutation** <0-63> to <0-63> SWITCH(config)#**no mls qos dscp-mutation**
描述	配置 dscp-dscp 映射关系

- 配置 dscp-queue 映射关系

命令	SWITCH(config)#**mls qos dscp-queue** <0-63> <0-7> SWITCH(config)#**no mls qos dscp-queue** <0-63>
描述	配置 dscp-queue 映射关系 默认映射关系：<0-7>-0，<8-15>-1，<16-23>-2，<24-31>-3，<32-39>-4，<40-47>-5，<48-55>-6，<56-63>-7

说明

✦ 在配置端口为 trust dscp 且 ip 报文时：dscp-cos 配置生效，根据映射关系修改报文 dscp，dscp-queue 配置生效，根据映射关系修改报文出口队列。当同时同事配置了 dscp-dscp 时，先进行 dscp-dscp 转换，结果再进行 dscp-cos 映射；

- 配置 class-map

命令	SWITCH(config)#**class-map** CNAME SWITCH(config-cmap)# SWITCH(config)#**no class-map** CNAME
描述	创建/删除 class-map 创建 class-map 后，自动进入 class-map 模式

- 配置流匹配规则

命令	SWITCH(config-cmap)# **match access-group** ACLNAME SWITCH(config-cmap)#**no match access-group** ACLNAME
描述	配置基于 ACL 的 chass-map，支持标准 IP、扩展 IP，MAC 的 ACL

命令	SWITCH(config-cmap)#**match ip-dscp** <0-63> SWITCH(config-cmap)#**no match ip-dscp**
描述	配置匹配 IP 报文中的 dhcp 字段，最多可配置 8 个不同的 dhcp 数值

命令	SWITCH(config-cmap)#**match cos** <0-7> SWITCH(config-cmap)#**no match cos**
描述	配置匹配报文中的 cos 字段，最多可配置 8 个不同的 cos 数值

命令	SWITCH(config-cmap)#**match ethertype** ETYPE SWITCH(config-cmap)#**no match ethertype**
描述	匹配报文以太网协议类型字段

命令	SWITCH(config-cmap)#**match** {**vlan** <1-4094> | **vlan-range** <1-4094> **to** <1-4094>} SWITCH(config-cmap)#**no match** {**vlan | vlan-range**}
描述	匹配报文 vlan，支持 range 的配置

命令	SWITCH(config-cmap)#**match layer4** {**tcp | udp**} {**source-port | destination-port**} VALUE SWITCH(config-cmap)#**no match layer4** {**tcp | udp**} {**source-port | destination-port**} VALUE
描述	支持 IPv4 协议报文 4 层端口号配置

命令	SWITCH(config-cmap)#**match vlan-range** <1-4094> to <1-4094> **ethertype** ETYPE SWITCH(config-cmap)#**no match vlan-range**
描述	匹配报文 vlan，支持 range 的配置，同时匹配报文 etype

- 配置 policy-map

命令	SWITCH(config)#**policy-map** PNAME SWITCH(config-pmap)# SWITCH(config)#**no policy-map** PNAME
描述	配置/删除 policy-map

- 配置 policy-map 关联 class-map

命令	SWITCH(config-pmap)# **class** CNAME SWITCH(config-pmap-c)# SWITCH(config-pmap)#**no class** CNAME
描述	policy-map 关联/解关联 class-map 一个 policy-map 最多 attach8 个 class-map

- 配置策略

命令	SWITCH(config-pmap-c)#**set cos** <0-7> SWITCH(config-pmap-c)#**no set cos**
描述	配置/删除策略，修改报文 cos 字段

命令	SWITCH(config-pmap-c)#**set ip-dscp** <0-63> SWITCH(config-pmap-c)#**no set ip-dscp**
描述	配置/删除策略，修改报文 ip-dscp 字段

命令	SWITCH(config-pmap-c)#**set vlan** <1-4094> SWITCH(config-pmap-c)#**no set vlan**
描述	配置/删除策略，修改报文 vlan

命令	SWITCH(config-pmap-c)#**nest vlan** <1-4094> SWITCH(config-pmap-c)#**no nest vlan**
描述	配置/删除策略，为匹配报文添加外 tag

命令	SWITCH(config-pmap-c)#**police cir** <32-1000000> **cbs** <4-31250> **exceed-action drop** SWITCH(config-pmap-c)#**no police**
描述	配置/删除策略 Cir 是限速水线，单位 kbps Cbs 是 burst 能力，单位 Kbyte

说明

✦ cir 数值是可确定的，比如限速 1M，那么 cir 数值为 1024，但是 cbs 的数值却取自经验数值。当 cbs 数值配大，流量尖峰更高，限速较稳定，但平均速率可能高于限速值；当 cbs 数值配小，流量尖峰较低，限速波动较大，平均速率可能小于限速值。建议 cbs 配置取 cir 的 4 倍值与 31250 的小值。

- 配置 policy-map 在接口上应用

命令	SWITCH(config-if)#**service-policy input** PNAME SWITCH(config-if)#**no service-policy input** PNAME
描述	配置/删除策略在接口上的应用 一个接口上只能应用一条 policy-map

- 配置端口入口限速

命令	SWITCH(config-if)#**rate-limit input** <64-1000000> <32-16384> SWITCH(config-if)#**no rate-limit input**
描述	配置/删除端口入口限速 第一个参数为 limit，单位 kbps 第二个参数为 burst，单位 Kbyte

- 配置端口出入口限速

命令	SWITCH(config-if)#**rate-limit output** <64-1000000> <32-16384> SWITCH(config-if)#**no rate-limit output**
描述	配置/删除端口出口限速 第一个参数为 limit，单位 kbps 第二个参数为 burst，单位 Kbyte

说明

✦ limit 数值是可确定的，比如限速 1M，那么 limit 数值为 1024，但是 burst 的数值却取自经验数值。当 burst 数值配大，流量尖峰更高，限速较稳定，但平均速率可能高于限速值；当 burst 数值配小，流量尖峰较低，限速波动较大，平均速率可能小于限速值。建议 burst 配置取 limit 的 4 倍值与 16384 的小值。

19.3. 配置案例

案例一：对端口 gigabitEthernet0/1 进行入口限速 1024kbps，出口限速 1024kbps。

- 配置 gigabitEthernet0/1 入口限速：

```
SWITCH(config-if)#rate-limit input 1024 4096
```

- 配置 gigabitEthernet0/1 出口限速：

```
SWITCH(config-if)#rate-limit output 1024 4096
```

案例二：对端口 gigabitEthernet0/1，满足 SIP 为 192.168.64.1 的流进行入口限速，限速 1024kbps。

- 配置全局打开 QOS 功能：

```
SWITCH(config)#mls qos enable
```

- 创建 ACL 流：

```
SWITCH(config)#ip-access-list 1 permit 192.168.64.1
```

- 配置 class-map、policy-map：

```
SWITCH(config)#class-map c1
SWITCH(config-cmap)#match access-group 1
SWITCH(config-cmap)#exit
SWITCH(config)#policy-map p1
SWITCH(config-pmap)#class c1
SWITCH(config-pmap-c)#police cir 1024 cbs 4096 exceed-action drop
```

- 配置端口应用 policy-map：

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#service-policy input p1
```

案例三：在网络拥堵情况下，要求 gigabitEthernet0/2 的入口不带 tag 报文优先转发

- 配置全局打开 QOS 功能：

```
SWITCH(config)#mls qos enable
```

- 配置 gigabitEthernet0/2 的端口默认 cos 为 2，端口信任 cos，配置 gigabitEthernet0/1 的端口默认 cos 为 0，信任 cos：

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#mls qos trust cos
SWITCH(config-if)#mls qos cos 0
SWITCH(config-if)#exit
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#mls qos trust cos
SWITCH(config-if)#mls qos cos 2
```

- 配置 cos-queue 队列映射关系：

```
SWITCH(config)#mls qos cos-queue 0 0
SWITCH(config)#mls qos cos-queue 2 2
```

- 配置调度模式为 wrr：

```
SWITCH(config)#mls qos algorithm wrr
```

- 配置队列 2 权重为 0：

```
SWITCH(config)#mls qos weight 2 0
```

19.4. 显示命令

- 显示调度模式、权重配置信息

```
SWITCH#show mls qos algorithm
Mls qos algorithm is WRR.

Queue-id    0     1     2     3     4     5     6     7
Weight       1     1     1     1     1     1     1     1
```

- 显示 cos-map 配置信息

```
SWITCH#show mls qos cos-maps
----------------------------
Cos      Dscp      Queue
----------------------------
0        0         0
1        8         1
2        16        2
3        24        3
4        32        4
```

```
5        40        5
6        48        6
7        56        7
```

- 显示 dscp-map 配置信息

```
SWITCH#show mls qos dscp-maps
----------------------------------------
Dscp      Cos      Mutation      Queue
----------------------------------------
0         0        0                0
1         0        1                0
2         0        2                0
3         0        3                0
4         0        4                0
5         0        5                0
6         0        6                0
7         0        7                0
8         1        8                1
9         1        9                1
10        1        10               1
11        1        11               1
12        1        12               1
13        1        13               1
14        1        14               1
15        1        15               1
```

- 显示端口配置信息

```
SWITCH#show mls qos interfaces
-------------------------------
Interface     Trust mode  Cos
-------------------------------
GiEO/1        Not         0
GiEO/2        Not         0
GiEO/3        Not         0
GiEO/4        Not         0
GiEO/5        Not         0
GiEO/6        Not         0
GiEO/7        Not         0
GiEO/8        Not         0
GiEO/9        Not         0
GiEO/10       Not         0
```

- 显示 class-map 配置信息

```
SWITCH#show class-map

    CLASS-MAP-NAME: c1
      Match Cos: 3
```

- 显示 policy-map 配置信息

```
SWITCH#show policy-map

  POLICY-MAP-NAME: p1
    State: detached

    CLASS-MAP-NAME: c1
```

```
        Match Cos: 3
        Police: Mode: SrTCM
                cir (1024 Kbps)
                cbs (4096 KBytes)
                exceed-action (drop)
```

- 显示端口限速配置信息

```
SWITCH#show rate-limit
-------------------------------------------------------
Interface     In limit  In burst  Out limit  Out burst
-------------------------------------------------------
GiE0/1        --        --        --         --
GiE0/2        --        --        --         --
GiE0/3        1024      4096      --         --
GiE0/4        --        --        --         --
GiE0/5        --        --        --         --
GiE0/6        --        --        --         --
GiE0/7        --        --        --         --
GiE0/8        --        --        --         --
GiE0/9        --        --        --         --
GiE0/10       --        --        1024       4096
```

20. 配置 DHCP Snooping

20.1. DHCP Snooping 概述

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一个局域网的网络协议， 被广泛用来动态分配可重用的网络资源，是一种用户或者内部网络管理员对所有计算机作中央管理的手段。

DHCP Snooping 是 DHCP 安全技术，通过侦测管理 DHCP 交互报文，实现对非法 DHCP Server 的隔离功能，DHCP 隔离功能可基于 VLAN 生效。

DHCP TRUST 端口

对于连接合法 DHCP Server 的端口，认定为 TRUST 端口，其他端口为 UNTRUST 端口。当开启 DHCP Snooping 功能时，设备将阻止客户端的 DHCP 广播报文发送往 UNTRUST 端口。

DHCP 报文端口限速

针对端口部分用户的 DHCP 报文流量攻击，支持 DHCP 报文端口限速，降低或消除该端口下用户攻击对网络环境影响。

MAC Address 检验

UNTRUST 端口送上来的 DHCP 报文，检测报文中二层头部源 MAC 地址与数据段中 CLIENT HARDWARE ADDRESS 字段，不一样则为非法报文。

Option-82 选项

DHCP Option82 选项又称为 DHCP 中继代理信息选项（Relay Agent Information Option），是 DHCP 报文中的一个选项。Option82 选项是为了增强 DHCP 服务器的安全性，改善 IP 地址的分配策略而提出的一种 DHCP 选项，由中继组件实现选项的添加与剥离。

DHCP 合法用户

DHCP Snooping 通过监控 DHCP 报文，统计合法服务器分配的用户信息。当端口开启 ip verify source 功能时，作为端口上的合法用户。

20.2. 配置命令

- 全局开启/关闭 DHCP Snooping

命令	SWITCH(config)#**ip dhcp snooping** SWITCH(config)#**no ip dhcp snooping**
描述	全局开启、关闭 DHCP Snooping 功能 默认关闭

- 配置 dhcp vlan

命令	SWITCH(config)#**ip dhcp snooping vlan** VID SWITCH(config)#**no ip dhcp snooping vlan** VIID
描述	默认 DHCP Snooping 功能在所有 vlan 上生效 VID 可以是单个 VLAN ID，也可以是 range 模式，如 3-10

- 配置信任口

命令	SWITCH (config-if)#**ip dhcp snooping trust** SWITCH (config-if)#**no ip dhcp snooping trust**
描述	设置端口为 TRUST/UNTRUST 口 默认所有端口为非信任口

- 配置 MAC ADDRESS 检验

命令	SWITCH (config)#**ip dhcp snooping verify mac-address** SWITCH (config)#**no ip dhcp snooping verify mac-address**
描述	设置支持 MAC 地址检测 默认不支持

- 配置端口 DHCP 限速

命令	SWITCH (config-if)#**ip dhcp snooping rate-limit** PPS SWITCH (config-if)#**no ip dhcp snooping rate-limit**
描述	设置端口 DHCP 限速 PPS 为每秒报文数，范围 0 – 128，当设置为 0 时，硬件丢弃 默认不限速

说明

✦ 由于硬件限制，对于端口 DHCP 限速配置，当限速值为非 0 时，采用软件限速，当限速值为 0 时，为硬件限速。若单端口 DHCP 攻击流对环境造成影响，请将端口 DHCP 限速值配置为 0。

- 配置插入 option-82

命令	SWITCH (config)#**ip dhcp snooping information option-82** SWITCH (config)#**no ip dhcp snooping information option-82**
描述	配置在 dhcp 请求报文中添加 option-82 信息，在应答报文中剔除 option-82 信息 默认不支持

- 配置接口 option-82 的 circuit-id

命令	SWITCH (config-if)#**ip dhcp snooping information option-82 circuit-id** WORD SWITCH (config-if)#**no ip dhcp snooping information option-82 circuit-id**
描述	配置 circuit-id 定制内容 默认带 vlan+端口信息 WORD：字符串信息，有效长度 3-63 字符

- 配置接口 option-82 的 remote-id

命令	SWITCH (config-if)#**ip dhcp snooping information option-82 remote-id** WORD SWITCH (config-if)#**no ip dhcp snooping information option-82 remote-id**
描述	配置 remote-id 定制内容 默认带设备 MAC 地址信息 WORD：字符串信息，有效长度 1-63 字符

- 配置 DHCP Snooping database 数据定时写入 flash

命令	SWITCH (config)#**ip dhcp snooping database write-delay** SECONDS SWITCH (config-if)#**no ip dhcp snooping database write-delay**
描述	配置 DHCP Snooping 数据定时写入 flash，单位秒 SECONDS：<600 86400>

	默认不支持

- 配置 DHCP Snooping database 数据实时写入 flash

命令	SWITCH (config)#**ip dhcp snooping database write-flash**
描述	触发 DHCP Snooping 数据实时写入 flash

- 配置 DHCP Snooping database 数据从 flash 更新

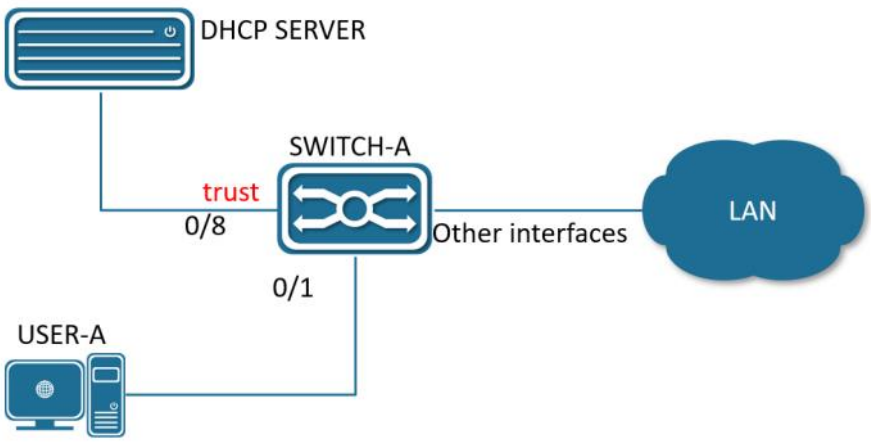
命令	SWITCH(config)#**ip dhcp snooping database renew**
描述	触发 DHCP Snooping 数据从 flash 更新

- 清除 DHCP Snooping database 数据

命令	SWITCH#**clear ip dhcp snooping database (vlan** VLANID **| interface** IFNAME **| mac-address** XXXX.XXXX.XXXX **| ip-address** A.B.C.D **| flash)**
描述	支持基于端口、vlan、MAC 地址、IP 地址清除 database 支持 flash 中 database 数据清除

20.3. 配置案例

案例一：对于 SWITCH-A，gigabitEthernet0/8 口接 DHCP 服务器，USER-A 通过动态获取 IP 地址。LAN 中存在其他 DHCP 服务器，会影响 USER-A 的 IP 地址分配。



- 进入全局模式，全局开启 DHCP Snooping 功能：

```
SWITCH#configure terminal
SWITCH(config)#ip dhcp snooping
```

- 配置与服务器连接的上联口 gigabitEthernet0/8 为信任口

```
SWITCH(config)#interface gigabitEthernet0/8
SWITCH(config-if)#ip dhcp snooping trust
```

20.4. 显示命令

- 显示 DHCP Snooping 配置信息

```
SWITCH#show ip dhcp snooping
Ip dhcp snooping                      : Enabled
No ip dhcp snooping vlan              : 2-5
Verify mac-address                    : Disabled
Information option-82                 : No
database write-delay                  : 0 seconds

Interface               Trusted         Rate limit (pps)
-----------------------------------------------------------
gigabitEthernet0/16     yes             unlimited
```

21. 配置 802.1X 认证

21.1. 协议概述

IEEE802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1X 协议。后来，802.1X 协议作为局域网端口的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。802.1X 协议是一种基于端口的网络接入控制协议（port based network access control protocol）。“基于端口的网络接入控制”是指，在局域网接入设备的端口这一级，对所接入的用户设备通过认证来控制对网络资源的访问。

21.1.1. 802.1X 的体系结构

802.1X 系统为典型的 Client/Server 结构，如图 21-1 所示，包括三个实体：客户端（Client）、设备端（Device）和认证服务器（Server）。

图 21-1 802.1X 认证系统的体系结构

- 客户端是位于局域网段一端的一个实体，由该链路另一端的设备端对其进行认证。客户端一般为一个用户终端设备，用户可以通过启动客户端软件发起 802.1X 认证。客户端必须支持 EAPOL（Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议）。
- 设备端是位于局域网段一端的另一个实体，对所连接的客户端进行认证。设备端通常为支持 802.1X 协议的网络设备，它为客户端提供接入局域网的端口，该端口可以是物理端口，也可以是逻辑端口。
- 认证服务器是为设备端提供认证服务的实体。认证服务器用于实现对用户进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。

21.1.2. 802.1X 的认证方式

802.1X 认证系统使用 EAP（Extensible Authentication Protocol，可扩展认证协议），来实现客户端、设备端和认证服务器之间认证信息的交换。

- 在客户端与设备端之间，EAP 协议报文使用 EAPOL 封装格式，直接承载于 LAN 环境中。
- 在设备端与 RADIUS 服务器之间，可以使用两种方式来交换信息。一种是 EAP 协议报文由设备端进行中继，使用 EAPOR（EAP over RADIUS）封装格式承载于 RADIUS 协议中；另一种是 EAP 协议报文由设备端进行终结，采用包含 PAP（Password Authentication Protocol，密码验证协议）或 CHAP（Challenge Handshake Authentication Protocal，质询握手验证协议）属性的报文与 RADIUS 服务器进行认证交互。

21.1.3. 802.1X 的基本概念

21.1.3.1. 受控/非受控端口

设备端为客户端提供接入局域网的端口，这个端口被划分为两个逻辑端口：受控端口和非受控端口。任何到达该端口的帧，在受控端口与非受控端口上均可见。

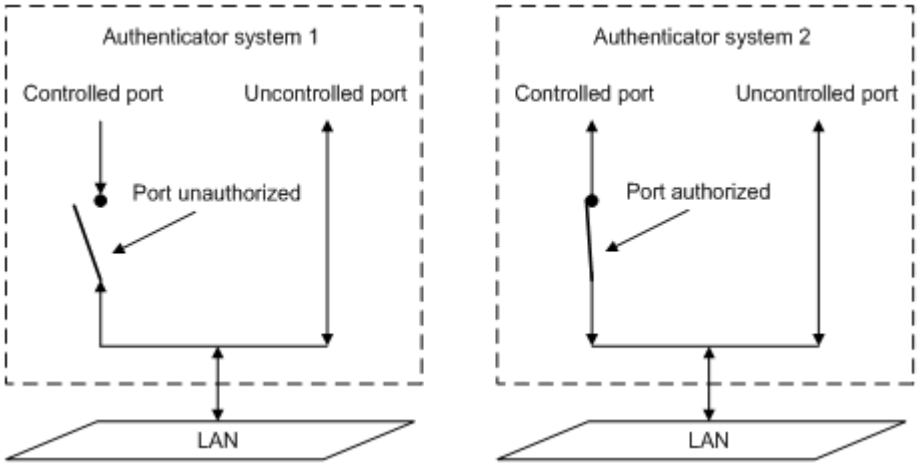
- 非受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，保证客户端始终能够发出或接收认证报文。
- 受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。

21.1.3.2. 授权/非授权状态

设备端利用认证服务器对需要接入局域网的客户端执行认证，并根据认证结果（Accept 或 Reject）对受控端口的授权/非授权状态进行相应地控制。

图 21-2 显示了受控端口上不同的授权状态对通过该端口报文的影响。图中对比了两个 802.1X 认证系统的端口状态。系统 1 的受控端口处于非授权状态（相当于端口开关打开），系统 2 的受控端口处于授权状态（相当于端口开关关闭）。

图 21-2 受控端口上授权状态的影响



用户可以通过在端口下配置的接入控制的模式来控制端口的授权状态。端口支持以下三种接入控制模式：

- 强制授权模式（**authorized-force**）：表示端口始终处于授权状态，允许用户不经认证授权即可访问网络资源。
- 强制非授权模式（**unauthorized-force**）：表示端口始终处于非授权状态，不允许用户进行认证。设备端不对通过该端口接入的客户端提供认证服务。
- 自动识别模式（**auto**）：表示端口初始状态为非授权状态，仅允许 EAPOL 报文收发，不允许用户访问网络资源；如果认证通过，则端口切换到授权状态，允许用户访问网络资源。这也是最常见的情况。

21.1.3.3. 受控方向

在非授权状态下，受控端口可以被设置成单向受控和双向受控。

- 实行双向受控时，禁止帧的发送和接收；
- 实行单向受控时，禁止从客户端接收帧，但允许向客户端发送帧。

21.1.4. 802.1X 的认证过程

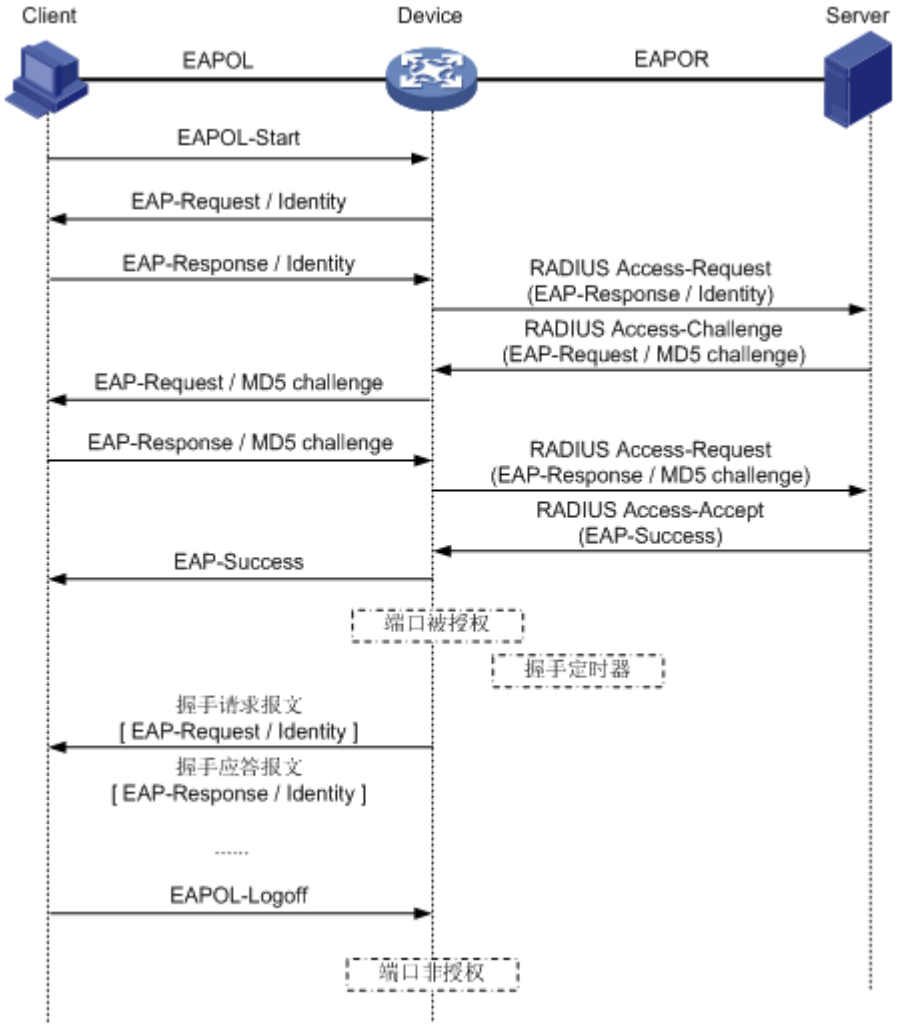
802.1X 系统支持 EAP 中继方式和 EAP 终结方式与远端 RADIUS 服务器交互完成认证。以下关于两种认证方式的过程描述，都以客户端主动发起认证为例。

21.1.4.1. EAP 中继方式

这种方式是 IEEE 802.1X 标准规定的，将 EAP（可扩展认证协议）承载在其它高层协议中，如 EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP 中继方式需要 RADIUS 服务器支持 EAP 属性：EAP-Message 和 Message-Authenticator，分别用来封装 EAP 报文及对携带 EAP-Message 的 RADIUS 报文进行保护。

下面以 EAP-MD5 方式为例介绍基本业务流程，如图 21-3 所示。

图 21-3 IEEE 802.1X 认证系统的 EAP 中继方式业务流程



认证过程如下：

1) 当用户有访问网络需求时打开 802.1X 客户端程序，输入已经申请、登记过的用户名和密码，发起连接请求（EAPOL-Start 报文）。此时，客户端程序将发出请求认证的报文给设备端，开始启动一次认证过程。
2) 设备端收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity 报文）要求用户的客户端程序发送输入的用户名。
3) 客户端程序响应设备端发出的请求，将用户名信息通过数据帧（EAP-Response/Identity 报文）发送给设备端。设备端将客户端发送的数据帧经过封包处理后（RADIUS Access-Request 报文）送给认证服务器进行处理。
4) RADIUS 服务器收到设备端转发的用户名信息后，将该信息与数据库中的用户名表对比，找到该用户名对应的密码信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过 RADIUS Access-Challenge 报文发送给设备端，由设备端转发给客户端程序。
5) 客户端程序收到由设备端传来的加密字（EAP-Request/MD5 Challenge 报文）后，用该加密字对密码部分进行加密处理（此种加密算法通常是不可逆的），生成 EAP-Response/MD5 Challenge 报文，并通过设备端传给认证服务器。
6) RADIUS 服务器将收到的已加密的密码信息（RADIUS Access-Request 报文）和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息（RADIUS Access-Accept 报文和 EAP-Success 报文）。
7) 设备收到认证通过消息后将端口改为授权状态，允许用户通过端口访问网络。在此期间，设备端会通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。缺省情况下，两次握手请求报文都得不到客户端应答，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。
8) 客户端也可以发送 EAPOL-Logoff 报文给设备端，主动要求下线。设备端把端口状态从授权状态改变成未授权状态，并向客户端发送 EAP-Failure 报文。

21.2. 配置命令

- 全局开启/关闭 802.1X 认证

命令	SWITCH(config)# **dot1x enable** SWITCH(config)#**no dot1x enable**
描述	全局开启、关闭 802.1X 功能。

- 端口开启/关闭 802.1X 认证

命令	SWITCH(config-if)# **dot1x port-control auto** SWITCH(config-if)#**no dot1x port-control auto**
描述	端口开启、关闭 802.1X 功能。

- 配置 RADIUS 服务器

命令	SWITCH(config)# **radius-server host** A.B.C.D **auth-port** <0-65535> **acct-port** <0-65535> **key** WORD SWITCH(config)#**no radius-server host** A.B.C.D

描述	配置认证服务器信息。 默认认证端口为 1812，记账端口为 1813。 请确保 RADIUS 服务器和设备管理地址互通。

- 配置 EAPOL 协议版本号

命令	SWITCH(config-if)# **dot1x protocol-version** <1-2> SWITCH(config-if)#**no dot1x protocol-version**
描述	配置指定端口 EAPOL 协议版本号。 可选配置，默认为 2。

- 配置认证静默时间

命令	SWITCH(config-if)# **dot1x quiet-period** <1-65535> SWITCH(config-if)#**no dot1x quiet-period**
描述	配置 HELD 状态的保持时间。 可选配置，单位为秒，默认为 60.

- 配置重认证功能

命令	SWITCH(config-if)# **dot1x reauthentication** SWITCH(config-if)#**no dot1x reauthentication**
描述	配置端口开启重认证功能。 可选配置，默认关闭.

- 配置重认证最大次数

命令	SWITCH(config-if)# **dot1x reauthMax** <1-10> SWITCH(config-if)#**no dot1x reauthMax**
描述	配置端口重认证最大次数，重认证请求超过次数限制且未有响应，端口变为未授权状态。 可选配置，默认 2 次.

- 配置使能密钥传输能力

命令	SWITCH(config-if)# **dot1x keytxenabled { disable | enable}**
描述	配置端口密钥传输功能。 可选配置，默认关闭.

- 配置定时器超时时间

命令	SWITCH(config-if)# **dot1x timeout {re-authperiod** <1-4294967295> **| server-timeout** <1-65535> **| supp-timeout** <1-65535> **| tx-period** <1-65535>**}** SWITCH(config-if)#**no dot1x timeout {re-authperiod | server-timeout | supp-timeout | tx-period}**
描述	配置端口定时器时间。 可选配置，默认重认证周期为 3600 秒，服务器超时 30 秒，客户端认证超时 30 秒，客户端请求超时 30 秒.

- 全局开启/关闭 MAC 认证

命令	SWITCH(config)# **mac-auth enable**

	SWITCH(config)#**no mac-auth enable**
描述	全局开启、关闭 MAC 认证功能。

- 端口开启/关闭 MAC 认证

命令	SWITCH(config-if)# **mac-auth {enable | disable}**
描述	端口开启、关闭 MAC 认证功能。

- 端口开启/关闭 MAC 认证动态 VLAN 下发

命令	SWITCH(config-if)# **mac-auth dynamic-vlan-creation {enable | disable}**
描述	端口开启、关闭 MAC 认证动态 VLAN 下发。 当前版本不支持。

- 配置 MAC 认证失败处理

命令	SWITCH(config-if)# **mac-auth auth-fail-action {drop-traffic | restrict-vlan** <2-4094>**}**
描述	配置 MAC 认证失败的行为。 可选配置，默认为 drop-traffic：丢弃流量。 当前版本不支持。

- 配置 RADIUS 服务器死亡时间

命令	SWITCH(config)# **radius-server deadtime** <0-1440> SWITCH(config)# **no radius-server deadtime**
描述	配置 RADIUS 服务器死亡时间。在认证过程中会自动跳过死亡的服务器，选择未死亡的服务器进行认证。 可选配置，默认为 0 分钟。

- 配置 RADIUS 服务器默认密钥

命令	SWITCH(config)# **radius-server key** STRING SWITCH(config)# **no radius-server key**
描述	配置 RADIUS 服务器默认密钥。 可选配置。

- 配置 RADIUS 服务器重传次数

命令	SWITCH(config)# **radius-server retransmit** <1-100> SWITCH(config)# **no radius-server retransmit**
描述	配置 RADIUS 服务器重传次数。 可选配置，默认为 3 次。

- 配置 RADIUS 服务器超时时间

命令	SWITCH(config)# **radius-server timeout** <1- 60> SWITCH(config)# **no radius-server timeout**

描述	配置 RADIUS 服务器超时时间。 可选配置，默认为 5 秒。

21.3. 配置案例

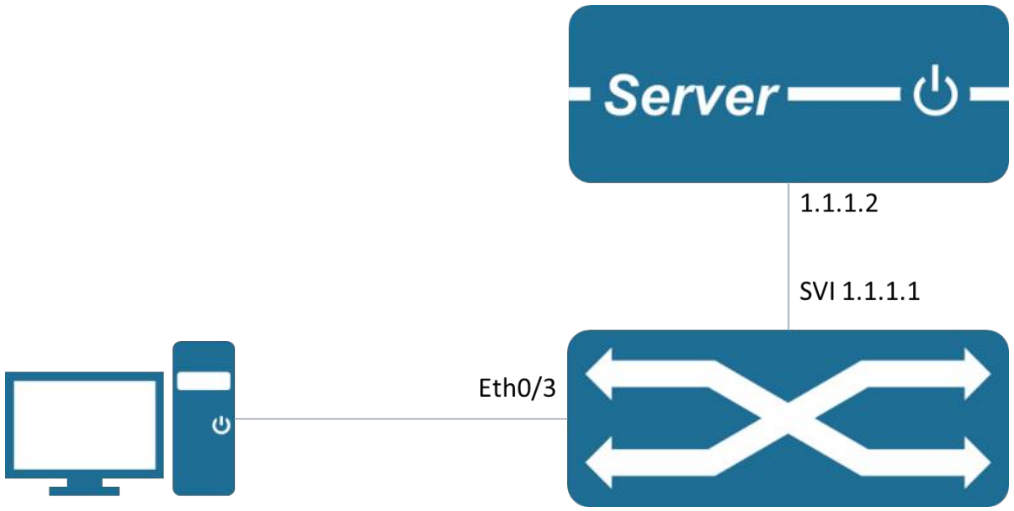
21.3.1. 802.1X 端口认证场景

1) 需求

- 要求在端口 GigabitEthernet0/3 上对接入用户进行认证，以控制其访问 Internet。
- RADIUS 服务器组 IP 地址 1.1.1.2。
- 设置系统与 RADIUS 服务器交互报文时的共享密钥为 name。

2) 组网图

图 21-4 802.1X 认证典型组网图



3) 典型配置举例

设备端：

```
SWITCH(config)#dot1x enable
SWITCH(config)#interface gigabitEthernet0/3
SWITCH(config-if)#dot1x port-control auto
SWITCH(config-if)#exit
SWITCH(config)#radius-server host 1.1.1.2 key name
```

服务器端：

配置 NAS 认证设备 1.1.1.1 及通信密钥 name。

添加用户账户 test 密码 test。

需要支持对应的认证方法，比如 EAP-MSCHAPv2

客户端：

开启 802.1X 认证客户端，使用账户 test 登录。

需要支持对应的认证方法，比如 EAP-MSCHAPv2 方法。

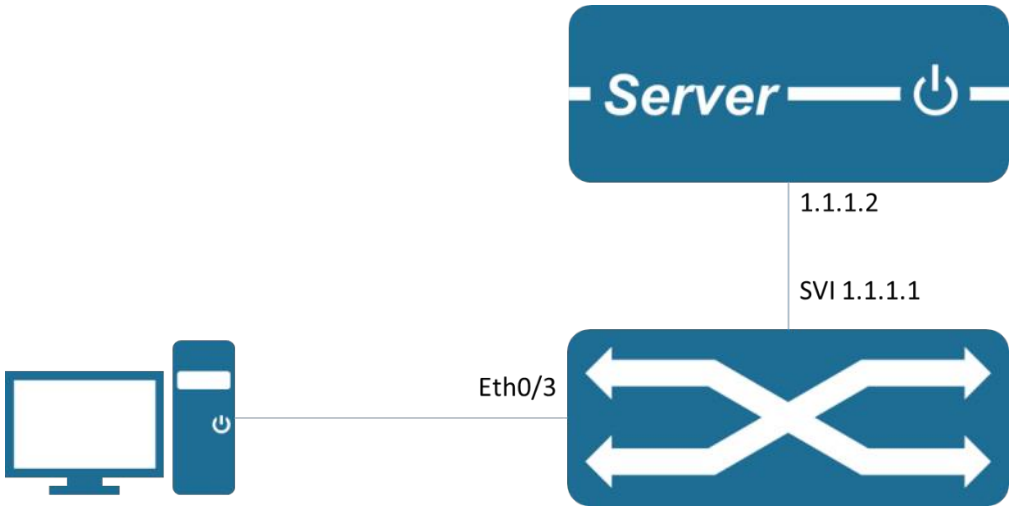
21.3.2. MAC 认证场景

1) 需求

- 要求在端口 GigabitEthernet0/3 上对接入用户进行认证，以控制其访问 Internet。
- RADIUS 服务器组 IP 地址 1.1.1.2。
- 设置系统与 RADIUS 服务器交互报文时的共享密钥为 name。

2) 组网图

图 21-5 MAC 认证典型组网图



3) 典型配置举例

设备端：

```
SWITCH(config)# mac-auth enable
SWITCH(config)#interface gigabitEthernet0/3
SWITCH(config-if)#mac-auth enable
SWITCH(config-if)#exit
SWITCH(config)#radius-server host 1.1.1.2 key name
```

服务器端：

配置 NAS 认证设备 1.1.1.1 及通信密钥 name。

将客户端 MAC 地址作为用户账号和密码添加到用户数据库。

客户端：

开启 802.1X 认证客户端，使用任意账号登录。

21.4. 显示命令

- 显示 802.1X 端口认证信息

```
SWITCH#show dot1x all
802.1X Port-Based Authentication Enabled
  RADIUS server address: 1.1.1.2:1812
  Next radius message id: 0
  RADIUS client address: not configured

802.1X info for interface gigabitEthernet0/6
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 1
  protocol version: 2
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:F
```

```
          PAE: state: Connecting - portMode: Auto
          PAE: reAuthCount: 1 - rxRespId: 0
          PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
          BE: state: Idle - reqCount: 0 - idFromServer: 0
          BE: suppTimeout: 30 - serverTimeout: 30
          CD: adminControlledDirections: in - operControlledDirections: in
          CD: bridgeDetected: false
          KR: rxKey: false
          KT: keyAvailable: false - keyTxEnabled: false
```

- 显示 MAC 认证信息

```
        SWITCH#show bridge
         Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-
out
         ---------+------+------+------+-----------+-----------------+-----+-------
--+
```

22. 配置 Port Security

22.1. Port Security 功能概述

Port Security 功能通过对端口合法 MAC 地址个数限制，达到限制非法用户对该端口访问的目的，对于非合法 MAC 的报文，将直接丢弃。

合法 MAC 可通过静态或动态的方式生成。静态合法 MAC 通过用户命令行配置生成；动态合法 MAC 则通过 MAC 地址学习功能动态生成。

当端口上安全地址个数已经达到最大安全地址个数配置值后，新 MAC 访问端口将认定为非法 MAC，产生违例事件，用户可配置违例事件产生时的应对操作，分别为 restrict 或 shutdown 端口。

Restrict：禁止非法 MAC 数据通过，并产生告警 log 提示信息。非法 MAC 将在 MAC 地址老化时间内禁止访问端口。通过 shutdown、no shutdown 端口可恢复。

Shutdown：强制端口 down 掉，并可配置端口恢复时间，时间到了端口自动恢复；也可通过 shutdown，no shutdown 命令恢复。

若希望将动态安全用户转换为静态安全用户，可开启端口上 sticky 功能。端口开启 sticky 功能，端口上学习到的动态用户将以静态用户的方式存在，若保存配置，设备重启后依然存在。

限制说明

- 仅支持 L2 端口配置端口安全，如普通物理口，AP 口。
- 仅支持在 access 模式下配置端口安全功能。
- 不支持 AP 成员口配置端口安全功能。
- 不支持 SPAN 的目的端口配置端口安全功能。
- 不支持在已配置静态 MAC 地址端口欲之端口安全功能。

22.2. 配置命令

- 使能端口安全功能

命令	SWITCH(config-if)#**switchport port-security** SWITCH(config-if)#**no switchport port-security**
描述	使能/关闭接口上端口安全功能

- 配置端口最大安全地址个数

命令	SWITCH(config-if)#**switchport port-security maximum** VALUE SWITCH(config-if)#**no switchport port-security maximum**
描述	默认最大安全地址个数为 1 范围<1 1024>

- 配置静态安全地址

命令	SWITCH(config-if)#**switchport port-security mac-address** MAC_ADDR SWITCH(config-if)#**no switchport port-security mac-address** MAC_ADDR
描述	安全地址格式：XXXX.XXXX.XXXX 安全地址不能是广播或组播地址

- 配置端口安全 sticky 功能

命令	SWITCH(config-if)# **switchport port-security mac-address sticky** SWITCH(config-if)#**no switchport port-security mac-address sticky**
描述	打开/关闭 sticky 功能

- 配置安全地址老化时间

命令	SWITCH(config-if)#**switchport port-security aging time** MINUTES SWITCH(config-if)#**no switchport port-security aging time**
描述	默认老化时间为 0，表示关闭老化功能 老化时间范围<0 1440> 默认老化功能仅对动态、sticky 安全地址生效

- 配置使能静态安全地址老化功能

命令	SWITCH(config-if)# **switchport port-security aging static** SWITCH(config-if)#**no switchport port-security aging static**
描述	使能老化静态安全地址

- 配置端口安全违例处理

命令	SWITCH(config-if)# **switchport port-security violation** { **strict** | **shutdown** } SWITCH(config-if)#**no switchport port-security violation**
描述	默认违例处理模式 restrict Restrict：禁止非法用户数据通过，并 log 提示 Shutdown：shutdown 端口，并在 errdisable 恢复时间后恢复 通过 shutdown/no shutdown 命令，同样可恢复

22.3. 显示命令

在特权模式下，可以查看端口安全配置信息、安全地址信息等。

- 显示所有端口端口安全概要信息

```
SWITCH#show port-security brief
interface   mac-address     mac-address     violation    violation
                maxinum         count         count     action
-----------------------------------------------------------------------------------------------------
GiE0/1      10              3               0          shutdown
GiE0/2      1               0               0          restrict
GiE0/3      1               0               0          restrict
GiE0/4      1               0               0          restrict
GiE0/5      1               0               0          restrict
GiE0/6      1               0               0          restrict
GiE0/7      1               0               0          restrict
GiE0/8      1               0               0          restrict
```

- 显示接口端口安全信息

```
SWITCH#show port-security interface gigabitEthernet0/1
Port Security               : Enabled
Maimum MAC Addresses     : 10
Violation Mode              : Shutdown
Aging Time(mins)            : 10
```

```
Aging static                : Enabled
Total MAC Addresses         : 3
Configured MAC Addresses    : 2
Security Violation Count    : 0
Last Violate Address        : --
```

- 显示安全地址信息

```
SWITCH#show port-security mac-address
interface   vlan    mac-address         type        left-time(min)
-------------------------------------------------------------------------------
GiE0/1      1       0001.0002.0004      static      10
GiE0/1      1       0001.0002.0003      static      10
GiE0/1      1       000e.c6c1.3a03      dynamic     10
```

- 显示接口安全地址信息

```
SWITCH#show port-security mac-address interface gigabitEthernet0/1
interface   vlan    mac-address         type        left-time(min)
-------------------------------------------------------------------------------
GiE0/1      1       0001.0002.0004      static      10
GiE0/1      1       0001.0002.0003      static      10
GiE0/1      1       000e.c6c1.3a03      dynamic     10
```

22.4. 典型案例

- 限制接口 gigabitEthernet0/1 合法用户数 3 个，非法用户不能访问设备

```
SWITCH(config-if)#switchport port-security
SWITCH(config-if)#switchport port-security maximum 3
SWITCH(config-if)#switchport port-security mac-address 0001.0001.0001
SWITCH(config-if)#switchport port-security mac-address 0001.0001.0002
SWITCH(config-if)#switchport port-security mac-address 0001.0001.0003
```

23. 配置 Ip Source Guard

23.1. Ip Source Guard 功能概述

Ip Source Guard 绑定功能，允许符合 IP+MAC 绑定的 IP 报文通过端口，不符合的报文则直接丢弃，从而达到防止 IP/MAC 欺骗攻击的目的。

Ip Source Guard 的绑定条目，主要有两个来源：用户静态配置与 ip dhcp snooping 环境中动态获取。

用户静态配置：主要应对局域网络中 IP 地址静态配置的主机用户。

Ip dhcp snooping 动态获取：主要应对局域网络中通过 dhcp 动态获取到 IP 地址的主机用户。

IP/MAC 欺骗攻击：非法 MAC 用户，发送带合法源 IP 的 IP 报文，实现访问身份的合法化。

限制说明

- 当前软件版本仅支持绑定条目用户静态配置方式。
- 不支持 AP 成员口配置 Ip Source Guard 功能。

23.2. 配置命令

- 使能 Ip Source Guard 功能

命令	SWITCH(config-if)#**ip verify source** SWITCH(config-if)#**no ip verify source**
描述	使能/关闭接口上 Ip Source Guard 功能

- 配置绑定表项

命令	SWITCH(config)# **ip source binding** XXXX.XXXX.XXXX **vlan** VALUE A.B.C.D **interface** IFNAME SWITCH(config)#**no ip source binding** XXXX.XXXX.XXXX **vlan** VALUE A.B.C.D **interface** IFNAME
描述	安全地址格式：XXXX.XXXX.XXXX IP 地址格式：A.B.C.D 单端口最多配置 128 条表项

23.3. 显示命令

在特权模式下，可以查看 ip verify source 生效规则与 ip source binding 绑定项。

- 查看 ip verify source 生效规则

```
SWITCH#show ip verify source
interface  Filter-type  Filter     IP-address      Mac-address  vlan
------------------------------------------------------------------------
GiE0/1     Ip        Permit    1.1.1.1        0001.0001.0001 1
GiE0/1     Ip        Deny      All            All            All
GiE0/2     Ip        Deny      All            All            All
```

- 查看端口 ip verify source 生效规则

```
SWITCH#show ip verify source interface gigabitEthernet0/1
interface  Filter-type  Filter     IP-address      Mac-address  vlan
-----------------------------------------------------------------------------------------------
GiE0/1     Ip        Permit     1.1.1.1        0001.0001.0001 1
GiE0/1     Ip        Deny      All            All            All
```

- 显示 ip source binding 表项

```
SWITCH#show ip source binding
interface  vlan  IP-address      Mac-address    Lease    Type
-------------------------------------------------------------------------------------------
GiE0/1     1     1.1.1.1         0001.0001.0001 infinite    static
GiE0/2     1     1.1.2.1         0001.0002.0001 infinite    static
```

- 显示接口 ip source binding 表项

```
SWITCH#show ip source binding
interface  vlan  IP-address      Mac-address    Lease    Type
-------------------------------------------------------------------------------------------
GiE0/1     1     1.1.1.1         0001.0001.0001 infinite    static
```

23.4. 典型案例

- Dhcp 服务器有三个用户连接 gigabitEthernet0/1 口，要求防止局域网内非法用户 IP/MAC 攻击

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#ip verify source
SWITCH(config)#ip source binding 0001.0001.0001 vlan 1 1.1.1.10 interface gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0002 vlan 1 1.1.1.11 interface gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0003 vlan 1 1.1.1.12 interface gigabitEthernet0/1
```

24. 配置 Arp-check

24.1. Arp-check 功能概述

Arp-check(ARP 报文检查)功能，对端口下所有的 ARP 报文进行过滤，对所有非法的 ARP 报文进行丢弃，能够有效的防止网络中 ARP 欺骗，提高网络的稳定性。

在支持 Arp-check 功能的设备中，Arp-check 功能能够根据 IP Source Guard 等安全应用模块所生成的合法用户信息(IP+MAC)产生相应的 ARP 过滤信息，从而实现对网络中的非法 ARP 报文的过滤。

限制说明

- 不支持 AP 成员口配置 Arp-check 功能。

24.2. 配置命令

- 使能 Arp-check 功能

命令	SWITCH(config-if)#**arp-check** SWITCH(config-if)#**no arp-check**
描述	使能/关闭接口上 Arp-check 功能

24.3. 典型案例

- Dhcp 服务器有三个用户连接 gigabitEthernet0/1 口，要求防止局域网内非法用户 IP/MAC 攻击，并开启非法 ARP 攻击检测

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#ip verify source
SWITCH(config-if)#arp-check
SWITCH(config)#ip source binding 0001.0001.0001 vlan 1 1.1.1.10 interface gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0002 vlan 1 1.1.1.11 interface gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0003 vlan 1 1.1.1.12 interface gigabitEthernet0/1
```

25. 配置 SNMP 网管

25.1. 概述

SNMP 是 Simple Network Management Protocol（简单网络管理协议）的缩写，在 1988 年 8 月就成为一个网络管理标准 RFC1157。到目前，因众多厂家对该协议的支持，SNMP 已成为事实上的网管标准，适合于在多厂家系统的互连环境中使用。

利用 SNMP 协议，网络管理员可以对网络上的节点进行信息查询、网络配置、故障定位、容量规划，网络监控和管理是 SNMP 的基本功能。

目前 SNMP 存在以下版本：

SNMPv1： 简单网络管理协议的第一个正式版本，在 RFC1157 中定义。

SNMPv2C：基于共同体（Community-Based）的 SNMPv2 管理架构, 在 RFC1901 中定义。

SNMPv3： 通过对数据进行鉴别和加密，提供了以下的安全特性：

1)确保数据在传输过程中不被篡改。

2)确保数据从合法的数据源发出。

3)加密报文，确保数据的机密性。

25.2. 配置命令

- 配置通信团体字

命令	SWITCH(config)#**snmp-server community** COMMUNITY **{ro | }** SWITCH(config)#**no snmp-server community** COMMUNITY
描述	配置/删除 SNMP 通信团体字； **ro**: 只读标识，将团体字配置为只有读权限的团体字；默认配置为同时具备读写权限的团体字； 支持同时配置多个团体字

- 配置 SNMPv3 视图

命令	SWITCH(config)# **snmp-server view** NAME **{include | exclude}** OID SWITCH(config)# **no snmp-server view** NAME
描述	配置/删除 SNMPv3 视图； 支持同时配置多个视图，支持单个视图配置多个规则； 系统默认存在 all 和 none 视图，不可修改

- 配置 SNMP 组

命令	SWITCH(config)# **snmp-server group** NAME **{v3 | } {noAuthNoPriv | authNoPriv | authPriv} read** RVIEW **write** WVIEW SWITCH(config)# **snmp-server group** NAME **{v1 | v2c} read** RVIEW **write** WVIEW SWITCH(config)# **no snmp-server group** NAME
描述	配置/删除 SNMP 组； 支持同时配置多个组； SNMPv1 SNMPv2c 在配置 community 时为了兼容旧的配置，会自动创建组信息，通常无需额外关注

- 配置 SNMPv3 用户

命令	SWITCH(config)# **snmp-server user** NAME **group** GROUPNAME **auth {md5 | sha}** {AUTHPASS} **priv {aes | des}** PRIVPASS SWITCH(config)# **no snmp-server user** NAME
描述	配置/删除 SNMP 用户； 支持同时配置多个用户；

- 配置 SNMP Host 通告服务器

命令	SWITCH(config)# **snmp-server host** IPADDR **{informs | traps} {v3 |} {noAuthNoPriv | authNoPriv | authPriv} user** NAME SWITCH(config)# **snmp-server host** IPADDR **{informs | traps} {v1 | v2c} community** NAME SWITCH(config)# **no snmp-server host** NAME
描述	配置/删除 SNMP 服务器； 支持同时配置多个服务器；

25.3. 配置案例

案例需求：SNMP 网管服务器 IP 地址为 2.2.2.2，读写通信团体字统一为 public。

- 进入全局配置模式配置：

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#snmp-server community public
SWITCH(config)#snmp-server 2.2.2.2 community public
SWITCH(config)#
```

案例需求：SNMP 网管服务器 IP 地址为 2.2.2.2，使用 SNMPv3，用户 test 密码 12345678，加密密钥 87654321；认证算法 MD5，加密算法 DES

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)# snmp-server group test v3 authPriv read all write all
SWITCH(config)# snmp-server user test group test auth MD5 12345678 priv DES
87654321
SWITCH(config)# snmp-server host 2.2.2.2 informs v3 authPriv user test
```

26. 配置 RMON

26.1. 概述

SNMP 是互联网络中使用最广泛的网管协议，通过嵌入到设备中的代理软件来实现对网络通信信息的收集和统计。管理软件通过轮询方式向代理的 MIB 发出查询信号得到这些信息，通过得到的信息实现对网络的管理。虽然 MIB 计数器把统计数据的总和记录下来了，但它无法对日常的通信情况进行历史分析。为了能全面的查看一天中的流量和流量的变化情况，网管软件需要不断的轮询，才能通过得到的信息分析出网络的状况。

采用 SNMP 进行轮询有两个明显的缺点：

- 占用了大量的网络资源，在大型的网络中，通过轮询的方式会产生大量的网络通信报文，这样将会导致网络的拥塞甚至于会引起网络的阻塞，故 SNMP 不适合管理大型的网络，不适合回收大量的数据，如路由表信息。
- 加重了管理者的负担，在 SNMP 轮询中收集数据的任务是由网络管理者通过网管软件完成的，如果网络管理者监控了 3 个以上的网段，就有可能出现由于负担过重，网络管理者无法完成任务的情况。

为了提高管理信息的可用性、减少管理站的负担、满足网络管理员监控多个网段性能的需求，IETF 开发了 RMON 用以解决 SNMP 在日益扩大的分布式互联中的局限性，主要实现对一个网段乃至整个网络的数据流量的监视功能。以下是 RMON 的特点：

- SNMP 是 RMON 实现的基础，RMON 是 SNMP 功能的增强。

  RMON 基于 SNMP 体系结构实现，与现存 SNMP 框架兼容，仍然是网管工作站 NMS 和运行在各网络设备上的代理 Agent 两部分组成。由于 RMON 没有使用另外一套机制，网管工作站 NMS 和 SNMP 共用，网络管理人员无需进行额外的学习，因此实现比较简单。
- RMON 使 SNMP 能更有效、更积极主动地监测远程网络设备，为监控网络的运行提供了一种高效的手段。

  RMON 协议规定达到告警阈值时被管理设备能自动发送 Trap 信息，所以管理设备不需要多次通过轮询获取 MIB 变量的值进行比较，从而能够减少管理设备同被管理设备的通信流量，达到简便而有效地管理大型互连网络的目的。

RMON 允许有多个监控者，监控者可用如下两种方法收集数据：

- 通过专用的 RMON Probe（探测仪），NMS 直接从 RMON Probe 获取管理信息并控制网络资源，这种方式可以获取 RMON MIB 的全部信息。
- 将 RMON Agent 直接嵌入网络设备中，使它们成为带 RMON Probe 功能的网络设备。NMS 使用 SNMP 与其交换数据信息，收集网络管理信息。这种方式受设备资源限制，一般无法获取 RMON MIB 的所有数据，基本上只收集四个组（告警、事件、历史和统计）的信息。

我司设备采用第二种方法，在设备上实现了 RMON Agent 功能。通过该功能，管理设备可以获得与被管网络设备接口相连的网段上的整体流量、错误统计和性能统计等信息，进而实现对网络的监控。

26.2. 原理

在配置 RMON 之前，需要了解 RMON 规范定义的统计、历史、告警和事件四个组的基本概念。

RMON 特性

RMON 主要实现了统计和告警功能，用于网络中管理设备对被管理设备的远程监控和管理。

RMON 的统计功能可以通过 RMON 统计组或者 RMON 历史组来实现，分为以太网统计功能和历史统计

功能。

- 以太网统计功能（对应 RMON MIB 中的统计组）：系统统计被监控的每个网络的基本统计信息。系统将持续的统计某一网段的流量和各种类型包的分布，或者各种类型的错误帧数、碰撞次数等，统计对象包括网络冲突数、CRC 校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。
- 历史统计功能（对应 RMON MIB 中的历史组）：系统定期采样收集网络状态统计信息并存储，以便后续的处理。系统将按周期定时对各种流量信息进行统计，统计数据包括带宽利用率、错误包数和总包数等。

RMON 告警功能包含事件定义功能和设置告警阈值功能，由这两个子功能的组合使用来实现了 RMON 告警功能。

- 事件定义功能（对应 RMON MIB 中的事件组）：事件组控制从设备来的事件和提示，提供关于 RMON Agent 所产生的所有事件。当某事件发生时，可以记录日志或发送 Trap 到网管站。
- 设置告警阈值功能（对应 RMON MIB 中的告警组）：系统针对指定的告警变量（任意告警对象对应的 OID）进行监控。在用户预先定义指定告警的一组阈值和采样时间后，系统会按照定义的时间周期去获取指定告警变量的值，当告警变量的值大于或等于上限阈值时，触发一次上限告警事件；当告警变量的值小于或等于下限阈值，触发一次下限告警事件。RMON Agent 会将上述监控到的状态记录为日志或者把 Trap 发往网管站。

RMON 规范（RFC2819）中定义了多个 RMON 组，设备实现了公有 MIB 中支持的统计、历史、告警和事件四个组。下面对这几个组分别进行介绍。

- 统计组

统计组规定系统将持续地对以太网接口的各种流量信息进行统计，并将统计结果存储在以太网统计表（etherStatsTable）中以便管理设备随时查看。统计信息包括网络冲突数、CRC 校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。

在指定接口下创建统计表项成功后，统计组就对当前接口的报文数进行统计，它统计的结果是一个连续的累加值。

- 历史组

历史组定期收集网络状态统计信息并存储，以便后续的处理。

历史组包含两个表：

  - 历史控制表（historyControlTable）：主要用来设置采样间隔时间等控制信息。
  - 以太网历史表（etherHistoryTable）：主要用来存储历史组定期收集网络状态统计信息，为网络管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

- 事件组

事件组定义的事件用于告警组配置项和扩展告警组配置项中，当监控对象达到告警条件时，就会触发事件。

RMON 事件管理即是在事件表的指定行添加事件，并定义事件的处理方式：

  - log：只发送日志
  - trap：只向 NMS 发送 Trap 消息
  - log-trap：既发送日志同时也向 NMS 发送 Trap 消息

- none：不做任何处理

- 告警组

告警组允许针对告警变量（可以是本地 MIB 的任意对象）预先定义一组阈值进行监视。用户定义了告警表项（alarmTable）后，系统会按照定义的时间周期去获取被监视的告警变量的值，当告警变量的值大于或等于上限阈值时，触发一次上限告警事件；当告警变量的值小于或等于下限阈值，触发一次下限告警事件，告警管理将按照事件的定义进行相应的处理。

26.3. 配置命令

- 配置统计组

命令	SWITCH(config)# **rmon statistics** <1-65535> **interface** IFNAME **{owner** OWNERNAME **|}** SWITCH(config)#**no rmon statistics** <1-65535>
描述	配置/删除统计组； <1-65535>: 组索引 IFNAME：接口名称 OWNERNAME：所有者信息

- 配置历史组

命令	SWITCH(config)# **rmon history** <1-65535> **interface** IFNAME **buckets** <1-65535> **interval** <1-3600> **{owner** OWNERNAME **|}** SWITCH(config)#**no rmon history** <1-65535>
描述	配置/删除历史组； <1-65535>: 组索引 IFNAME：接口名称 <1-65535>：历史桶大小 <1-3600>：记录周期；单位为秒 OWNERNAME：所有者信息

- 配置事件组

命令	SWITCH(config)# **rmon event** <1-65535> **{description** DESCRIPTION **|} {log | trap** COMMUNITY **| log-trap** COMMUNITY **| none} {owner** OWNERNAME **|}** SWITCH(config)#**no rmon event** <1-65535>
描述	配置/删除事件组； <1-65535>: 组索引 DESCRIPTION：事件描述 COMMUNITY：Trap 通信团体字 OWNERNAME：所有者信息

- 配置告警组

命令	SWITCH(config)# **rmon alarm** <1-65535> **object** STRING <1-65535> **{absolute | delta} rising-threshold** <1-2147483645> <1-65535> **falling-threshold** <1-2147483645> <1-65535> **{owner** OWNERNAME **|}** SWITCH(config)#**no rmon alarm** <1-65535>
描述	配置/删除告警组；

	<1-65535>: 组索引 STRING：告警监控的 OID；比如 1.3.6.1.2.1.2.2.1.10.1 表示监控接口 1 收到的字节数 <1-65535>：监控周期；单位为秒 <1-2147483645>：上升阈值 <1-65535>：上升事件索引；对应事件组中的索引 <1-2147483645>：下降阈值 <1-65535>：下降事件索引；对应事件组中的索引 OWNERNAME：所有者信息

- 配置 log 条目上限

命令	SWITCH(config)# **rmon max-log** <1-65535> SWITCH(config)#**no rmon max-log**
描述	配置/重置 log 条目上限； <1-65535>: 条目数 此处的 log 指由事件组产生的 log，不是系统 log 默认上限为 100 条；当产生的 log 数超过限定条目数时，会按照产生时间将旧的 log 删除，维持上限的限制

26.4. 配置案例

案例需求

SNMP 网管服务器 IP 地址为 2.2.2.2，读写通信团体字统一为 public。

网管服务器需要通过 rmon 查询设备端口 1 的流量

网管服务器需要通过 rmon 监控设备端口 1 的输入流量，10 秒为周期，一旦输入字节数变化超过 1MB(1000000B)，触发告警并记录 log

配置步骤

初始化网管配置

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#snmp-server community public
SWITCH(config)#snmp-server 2.2.2.2 community public
SWITCH(config)#
```

配置 rmon 统计组（以下 rmon 配置均可在网管端通过 MIB 来配置）

```
SWITCH(config)# rmon statistics 1 interface gigabitEthernet0/1 owner abc
SWITCH(config)#
```

配置 rmon 事件和告警组（以下 rmon 配置均可在网管端通过 MIB 来配置）

```
SWITCH(config)# rmon event 1 log-trap public owner abc
SWITCH(config)# rmon alarm 1 object 1.3.6.1.2.1.2.2.1.10.1 10 delta rising-threshold 1000000 1 falling-threshold 1000000 1
```

26.5. 显示命令

- 显示事件组日志

```
SWITCH#show rmon log
event 1 log 226 time 2304 desc
event 1 log 227 time 2314 desc
```

```
event 1 log 228 time 2324 desc
event 1 log 229 time 2334 desc
event 1 log 230 time 2344 desc
event 1 log 231 time 2354 desc
event 1 log 232 time 2364 desc
event 1 log 233 time 2374 desc
……
```

27. 配置 sFlow

27.1. 概述

sFlow 是由 InMon、HP 和 Foundry Networks 于 2001 年联合开发的一种网络监测技术,目前已经完成标准化，可提供完整的第二层到第四层信息，可以适应超大网络流量环境下的流量分析，让用户详细、实时地分析网络传输流的性能、趋势和存在的问题。

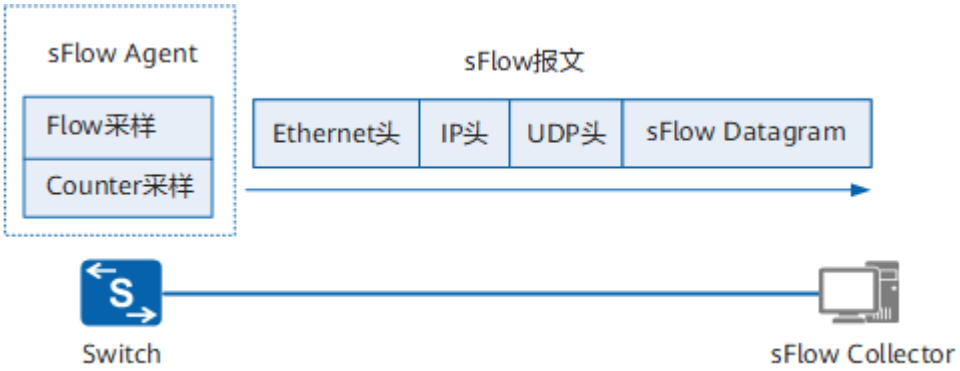
sFlow 具有如下优势：

- 支持在千兆或更高速的网络上精确地监控网络流量。
- 一个 sFlow Collector 能够监控成千上百个 sFlow Agent，具有良好的扩展性。
- sFlow Agent 内嵌在网络设备中，成本较低。

27.2. 原理

27.2.1. sFlow 系统组成

如图所示，sFlow 系统包含一个嵌入在设备中的 sFlow Agent 和远端的 sFlow Collector。其中，sFlow Agent 通过 sFlow 采样获取接口统计信息和数据信息，将信息封装成 sFlow 报文，当 sFlow 报文缓冲区满或是在 sFlow 报文缓存时间（缓存时间为 1 秒）超时后，sFlow Agent 会将 sFlow 报文发送到指定的 sFlow Collector。sFlow Collector 对 sFlow 报文进行分析，并显示分析结果。



27.2.2. sFlow 采样

sFlow Agent 提供了两种采样方式供用户从不同的角度分析网络流量状况，分别为 Flow 采样以及 Counter 采样。

Flow 采样

Flow 采样是 sFlow Agent 设备在指定接口上按照特定的采样方向和采样比对报文进行采样分析，用于获取报文数据内容的相关信息。该采样方式主要是关注流量的细节，这样就可以监控和分析网络上的流行为。

字段内容	说明
Raw packet	截取原始报文全部或者一部分报文头（具体截取多长的长度由配置决定），将这部分原始报文封装到 sFlow 报文中发送给 Collector。
Ethernet Frame Data	针对 Ethernet 报文，解析报文的 Ethernet 头信息，将解析数据封装到 sFlow 报文中发送给 Collector。

字段内容	说明
Extende Switch Data	针对转发的 Ethernet 报文，记录报文的 VLAN 转换以及 VLAN 优先级的转换，将转发信息封装到 sFlow 报文中发送给 Collector。VLAN ID 为 0 时表示无效 VLAN。

Counter 采样

Counter 采样是 sFlow Agent 设备周期性的获取接口上的流量统计信息，Counter 采样支持获取的采样信息如下表所示。与 Flow 采样相比，Counter 采样只关注接口上流量的数量，而不关注流量的详细信息。

字段内容	说明
Generic Interface Counters	通用接口统计信息，包括接口的基本信息，通用的接口流量统计。
Ethernet Interface Counters	针对于 Ethernet 接口，用于统计 Ethernet 相关的流量统计信息。
Processor Information	用于统计设备 CPU 占用率，内存使用情况。

27.2.3. sFlow 报文

sFlow 报文采用 UDP 封装，缺省目的端口号为知名端口 6343。sFlow 报文共有 4 种报文头格式，分别为 Flow sample、Expanded Flow sample、Counter sample、Expanded Counter sample。其中 Expanded Flow sample 和 Expanded Counter sample 是 sFlow version 5 新增内容，是 Flow sample 和 Counter sample 的扩展，但不前向兼容。所有的 Extended 的采样内容必须使用 Expanded 采样报文头封装。

27.3. 配置命令

- 配置 agent 地址

命令	SWITCH(config)# **sflow agent {ip** IPV4ADDR **| ipv6** IPV6ADDR**}** SWITCH(config)#**no sflow agent {ip | ipv6}**
描述	配置/删除 agent 地址； IPV4ADDR: agent/设备 IPv4 地址 IPV6ADDR：agent/设备 IPv6 地址 支持同时配置 ipv4 和 ipv6 地址，分别用于 ipv4 和 ipv6 的 collector 缺省无配置，不配置时可能导致协议不发包。

- 配置 collector

命令	SWITCH(config)# **sflow collector** <1-2> **{ ip** IPV4ADDR **| ipv6** IPV6ADDR **} [datagram-size** <200-9000> **| port** <1024-65535> **| description** STRING**]** SWITCH(config)#**no sflow collector** <1-2>
描述	配置/删除 collector； <1-2>: collector 索引 IPV4ADDR: collector/服务器 IPv4 地址 IPV6ADDR：collector/服务器 IPv6 地址 <200-9000>：数据包最大长度，可选，默认 1400 <1024-65535>：服务器端口号，可选，默认 6343

	STRING：collector 描述信息，可选，默认无

- 配置接口 flow 采样

命令	SWITCH(config-if)# **sflow flow-sampling collector** <1-2> SWITCH(config-if)#**no flow-sampling collector**
描述	配置/删除接口 flow 采样； <1-2>: collector 索引 ss

- 配置接口 counter 采样

命令	SWITCH(config-if)# **sflow counter-sampling collector** <1-2> SWITCH(config-if)#**no counter-sampling collector**
描述	配置/删除接口 counter 采样； <1-2>: collector 索引 ss

- 配置接口 flow 采样参数

命令	SWITCH(config-if)# **sflow flow-sampling direction { inbound | outbound }** SWITCH(config-if)# **sflow flow-sampling rate** <1024-65536> SWITCH(config-if)# **sflow flow-sampling max-header** <18-256> SWITCH(config-if)#**no flow-sampling direction** SWITCH(config-if)#**no flow-sampling rate** SWITCH(config-if)#**no flow-sampling max-header**
描述	配置/重置接口 flow 采样参数； { inbound | outbound }：flow 采样方向，可选，默认为同时采样 inbound+outbound <1024-65536>: flow 采样率，可选，默认为 2048，每 2048 条流采样一条 <18-256>：flow 采样报文长度，单位字节，可选，默认 64

- 配置接口 counter 采样参数

命令	SWITCH(config-if)# **sflow counter-sampling interval** <3-65535> SWITCH(config-if)#**no sflow counter-sampling interval**
描述	配置/重置接口 counter 采样参数； <3-65535>: counter 采样周期，单位秒，可选，默认 10

27.4. 配置案例

案例需求

sFlow 网管服务器 IP 地址为 2.2.2.2，设备 IP 地址为 2.2.2.95。

网管服务器需要通过 sFlow 监控设备端口 3 的状态，要求同时进行 flow 采样和 counter 采样，参数默认即可。

配置步骤

初始化网管配置

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#  sflow agent ip 2.2.2.95
SWITCH(config)#  sflow collector 1 ip 2.2.2.2
SWITCH(config)#
```

配置端口 3 的采样

```
SWITCH(config)#int gi 0/3
SWITCH(config-if)#sflow flow-sampling collector 1
SWITCH(config-if)#sflow counter-sampling collector 1
```

27.5. 显示命令

- 显示 sFlow

```
SWITCH#show sflow
Collector 1:
        Address: 2.2.2.2              Agent: 2.2.2.95
        Port: 6343              Datagram-Size: 1400             Description:
        Fd: 11                  Seq: 45                 Tx Timer: (nil)
        Buf: 0xab0d8            Alloc: 1400             Used: 0
-------------------------------------------------------------------------------
          |                   Flow                    |          Counter        |
Interface | ID Rate   Direction Max-header Sequence   | ID Interval Sequence    |
-------------------------------------------------------------------------------
GiE0/3      1  2048   both      64         2           1  10       7462
SWITCH#
```

28. 配置 DHCP 服务器

28.1. 协议概述

DHCP（Dynamic Host Configuration Protocol，动态主机设置协议）是一个局域网的网络协议，使用 UDP 协议工作，被广泛用来动态分配可重用的网络资源，如 IP 地址。

DHCP 是基于 Client/Server 工作模式，DHCP 客户端通过发送请求消息向 DHCP 服务器获取 IP 地址，等其他配置信息。当 DHCP 客户端与服务器不在同一个子网上，必须有 DHCP 中继代理（DHCP Relay）来转发 DHCP 请求和应答消息。

28.1.1. 协议标准

RFC2132 DHCP Options and BOOTP Vendor Extensions. S. Alexander, R. Droms. March 1997. (Format: TXT, HTML) (Obsoletes RFC1533) (Updated by RFC3442, RFC3942, RFC4361, RFC4833, RFC5494) (Status: DRAFT STANDARD) (DOI: 10.17487/RFC2132)

28.2. 配置命令

28.2.1. 全局配置命令

- 全局开启/关闭 DHCP 服务器

命令	SWITCH(config)# **ip dhcp-server enable** SWITCH(config)#**no ip dhcp-server enable**
描述	全局开启、关闭 DHCP 服务器。

- 配置全局参数

命令	SWITCH(config)# **ip dhcp-server parameter** NAME VALUE SWITCH(config)# **ip dhcp-server parameter (authoritative (on|off) | server-name** NAME **| server-identifier** IDENTIFY **| default-lease-time** <1-2147483648> **| max-lease-time** <1-2147483648> **| ping-timeout-ms** <1-65535> **| ping-timeout** <1-65535>**)** SWITCH(config)# **no ip dhcp-server parameter** NAME SWITCH(config)# **no ip dhcp-server parameter (authoritative | server-name | server-identifier | default-lease-time | max-lease-time | ping-timeout-ms | ping-timeout)**
描述	全局参数配置。参数值冲突时，全局参数优先级低于范围更精确的子网和地址池的参数。 默认的租约时间：43200s/12h 可选配置。

- 配置全局选项

命令	SWITCH(config)# **ip dhcp-server option** NAME VALUE SWITCH(config)# **ip dhcp-server option (routers** A.B.C.D **| domain-name** NAME **| domain-name-servers** A.B.C.D **| capwap-ac-v4** A.B.C.D**)** SWITCH(config)# **no ip dhcp-server option** NAME SWITCH(config)# **no ip dhcp-server option (routers | domain-name | domain-name-servers | capwap-ac-v4)**
描述	全局选项配置。选项值冲突时，全局选项优先级低于范围更精确的子网和地址池的选项。 可选配置。

- 配置定制域字段

命令	SWITCH(config)# **ip dhcp-server custom-space** NAME **[code width** <1-4>**] [length width** <1-4>**] [hash size** <1-65535>**]** SWITCH(config)#**no ip dhcp-server custom-space** NAME
描述	配置自定义域信息字段。 可选配置。

- 配置定制选项

命令	SWITCH(config)# **ip dhcp-server custom-option** NAME **code** <1-255> **(boolean|integer|ip-address|text|string|encapsulate)** SWITCH(config)#**no ip dhcp-server custom-option** NAME
描述	配置定制选项字段。配置的定制选项 code 值不能和已经配置的普通选项冲突。 可选配置。

- 配置强制发送选项

命令	SWITCH(config)# **ip dhcp-server force-option** <1-255> SWITCH(config)#**no ip dhcp-server force-option** <1-255>
描述	配置强制携带的选项字段。 可选配置。

- 配置静态地址

命令	SWITCH(config)# **ip dhcp-server static-lease** NAME XX:XX:XX:XX:XX:XX A.B.C.D SWITCH(config)#**no ip dhcp-server static-lease** NAME
描述	配置静态地址绑定。 可选配置。

- 配置白名单

命令	SWITCH(config)# **ip dhcp-server whitelist** NAME XX:XX:XX:XX:XX:XX SWITCH(config)#**no ip dhcp-server whitelist** NAME
描述	配置白名单。 可选配置。

- 配置黑名单

命令	SWITCH(config)# **ip dhcp-server blacklist** NAME XX:XX:XX:XX:XX:XX SWITCH(config)#**no ip dhcp-server blacklist** NAME
描述	配置黑名单。 可选配置。

- 配置自定义分类

命令	SWITCH(config)# **ip dhcp-server class** NAME **match** EXP SWITCH(config)#**no ip dhcp-server class** NAME
描述	配置自定义分类。专业类用法，请在技术人员指导下配置。 举例：ip dhcp-server class win_pc match "substring (option vendor-class-identifier,0,4)=MSFT" 可选配置。

28.2.2. 子网配置命令

- 配置子网信息

命令	SWITCH(config)# **ip dhcp-server subnet** A.B.C.D/M SWITCH(config)#**no ip dhcp-server subnet** A.B.C.D/M
描述	配置子网信息，并进入子网配置模式。 服务器正常启动至少需要一个正确的子网配置。

- 配置子网地址范围

命令	SWITCH(config-dhcp-subnet)# **range** A.B.C.D A.B.C.D SWITCH(config-dhcp-subnet)#**no range** A.B.C.D
描述	配置子网的地址范围。 服务器正常启动至少需要一个可分配地址范围，可以配置在下面的地址池中。 可以多次配置，配置不同范围。

- 配置子网参数

命令	SWITCH(config-dhcp-subnet)# **parameter** NAME VALUE SWITCH(config-dhcp-subnet)# **parameter (authoritative (on|off) | server-name** NAME **| server-identifier** IDENTIFY **| default-lease-time** <1-2147483648> **| max-lease-time** <1-2147483648> **| ping-timeout-ms** <1-65535> **| ping-timeout** <1-65535>**)** SWITCH(config-dhcp-subnet)#**no parameter** NAME SWITCH(config-dhcp-subnet)#**no parameter (authoritative | server-name | server-identifier | default-lease-time | max-lease-time | ping-timeout-ms | ping-timeout)**
描述	配置参数信息。 可选配置。

- 配置子网选项

命令	SWITCH(config-dhcp-subnet)# **option** NAME VALUE SWITCH(config-dhcp-subnet)# **option (routers** A.B.C.D **| domain-name** NAME **| domain-name-servers** A.B.C.D **| capwap-ac-v4** A.B.C.D**)** SWITCH(config-dhcp-subnet)#**no option** NAME SWITCH(config-dhcp-subnet)#**no option (routers | domain-name | domain-name-servers | capwap-ac-v4)**
描述	配置选项信息。通常需要配置子网的网关路由地址和 DNS 服务器地址。 可选配置。

28.2.3. 地址池配置命令

- 配置地址池信息

命令	SWITCH(config-dhcp-subnet)# **pool** NAME SWITCH(config-dhcp-subnet)#**no pool** NAME
描述	在子网模式中配置地址池。通过地址池可以进一步划分子网，按需使用。 可选配置。

- 配置地址池地址范围

命令	SWITCH(config-dhcp-pool)# **range** A.B.C.D A.B.C.D SWITCH(config-dhcp-pool)#**no range** A.B.C.D

描述	配置地址池的地址范围。 服务器正常启动至少需要一个可分配地址范围，可以配置在上面的子网中。 可以多次配置，配置不同范围。

- 配置地址池参数

命令	SWITCH(config-dhcp-pool)# **parameter** NAME VALUE SWITCH(config-dhcp-pool)# **parameter (authoritative (on|off) | server-name** NAME **| server-identifier** IDENTIFY **| default-lease-time** <1-2147483648> **| max-lease-time** <1-2147483648> **| ping-timeout-ms** <1-65535> **| ping-timeout** <1-65535>**)** SWITCH(config-dhcp-pool)#**no parameter** NAME SWITCH(config-dhcp-pool)#**no parameter (authoritative | server-name | server-identifier | default-lease-time | max-lease-time | ping-timeout-ms | ping-timeout)**
描述	配置参数信息。 可选配置。

- 配置地址池选项

命令	SWITCH(config-dhcp-pool)# **option** NAME VALUE SWITCH(config-dhcp-pool)# **option (routers** A.B.C.D **| domain-name** NAME **| domain-name-servers** A.B.C.D **| capwap-ac-v4** A.B.C.D**)** SWITCH(config-dhcp-pool)#**no option** NAME SWITCH(config-dhcp-pool)#**no option (routers | domain-name | domain-name-servers | capwap-ac-v4)**
描述	配置选项信息。通常需要配置地址池的网关路由地址和 DNS 服务器地址。 可选配置。

- 配置条件过滤指令

命令	SWITCH(config-dhcp-pool)# **(allow|deny|ignore)** CLASSNAME SWITCH(config-dhcp-pool)# **(allow|deny|ignore) (known-clients|unknown-clients|bootp|duplicates|declines)** SWITCH(config-dhcp-pool)# **no (allow|deny|ignore) (**CLASSNAME**|known-clients|unknown-clients|bootp|duplicates|declines)**
描述	配置地址池过滤条件。自定义 CLASSNAME 参考全局配置中配置自定义分类部分。 可选配置。

28.3. 配置案例

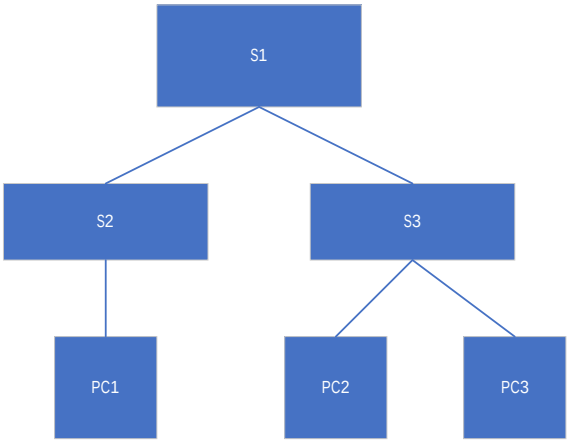
28.3.1. 常规 DHCP 服务器地址分配场景

4) 需求

- 见组网图描述

5) 组网图

图 28-1 DHCP 服务器典型组网图



S1: 三层交换机
　　VLAN 100: 192.168.100.1/24 直连S2
　　VLAN 200: 192.168.200.1/24 直连S3
S2、S3: 二层交换机
PC1、PC2、PC3均自动分配IP
期望：
　　PC1、PC2能够分别获取到各自网段的IP，且互Ping能通
　　PC3能够分配到192.168.200.2的地址

说明：测试时 PC3 的 MAC 地址为 00:0E:C6:C1:38:41

6)　典型配置举例

S1：

```
SWITCH(config)# ip dhcp-server subnet 192.168.100.0/24
SWITCH(config-dhcp-subnet)#range 192.168.100.2 192.168.100.254
SWITCH(config-dhcp-subnet)#option routers 192.168.100.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)# ip dhcp-server subnet 192.168.200.0/24
SWITCH(config-dhcp-subnet)#range 192.168.200.2 192.168.200.254
SWITCH(config-dhcp-subnet)#option routers 192.168.200.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)# ip dhcp-server static-lease pc3 00:0E:C6:C1:38:41
192.168.200.2
SWITCH(config)#ip dhcp-server option domain-name-servers 114.114.114.114
SWITCH(config)#ip dhcp-server enable
```

S2/S3：空配置透传

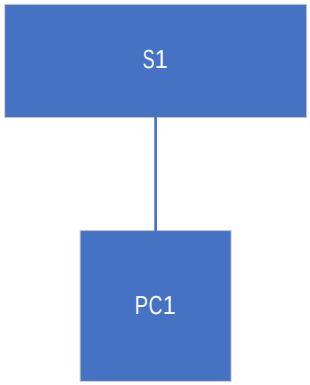
28.3.2. 支持私有属性下发的 DHCP 服务器地址分配场景

1)　需求

- 见组网图描述

2)　组网图

图 28-2 DHCP 服务器典型组网图



S1: 三层交换机

VLAN 100: 192.168.100.1/24 直连PC1

PC1自动分配IP

期望：

PC1能够获取到正确的IP，及私有选项信息

3) 典型配置举例

S1：

```
SWITCH(config)# ip dhcp-server custom-space dkwl code width 1 length width
1
SWITCH(config)# ip dhcp-server custom-option dkwl.name code 1 string
SWITCH(config)# ip dhcp-server custom-option dkwl.ip code 2 ip-address
SWITCH(config)# ip dhcp-server custom-option vendor_dkwl code 43
encapsulate dkwl
SWITCH(config)# ip dhcp-server option dkwl.ip 1.1.1.1
SWITCH(config)# ip dhcp-server option dkwl.name "dockeer"
SWITCH(config)# ip dhcp-server subnet 192.168.100.0/24
SWITCH(config-dhcp-subnet)#range 192.168.100.2 192.168.100.254
SWITCH(config-dhcp-subnet)#option routers 192.168.100.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)#ip dhcp-server option domain-name-servers 114.114.114.114
SWITCH(config)#ip dhcp-server enable
```

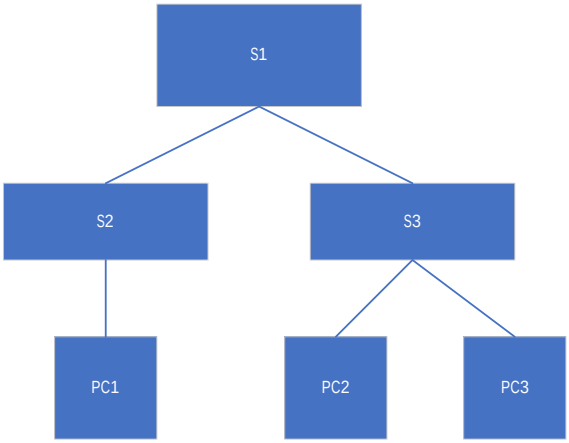
28.3.3. 支持访客分离的 DHCP 服务器地址分配场景

1) 需求

- 见组网图描述
- 正常用户分配地址 192.168.100.2-192.168.100.100 和 192.168.200.2-192.168.200.100
- 访客分配地址 192.168.100.200-192.168.100.254

2) 组网图

图 28-3 DHCP 服务器典型组网图



S1: 三层交换机
VLAN 100: 192.168.100.1/24 直连S2
VLAN 200: 192.168.200.1/24 直连S3
S2、S3: 二层交换机
PC1、PC2、PC3均自动分配IP
期望：
PC1、PC2能够分别获取到正常用户IP
PC3能够分配到访客段地址

3) 典型配置举例

S1:

```
SWITCH(config)# ip dhcp-server subnet 192.168.100.0/24
SWITCH(config-dhcp-subnet)#range 192.168.100.2 192.168.100.100
SWITCH(config-dhcp-subnet)#option routers 192.168.100.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)# ip dhcp-server subnet 192.168.200.0/24
SWITCH(config-dhcp-subnet)#pool employee
SWITCH(config-dhcp-pool)#range 192.168.200.2 192.168.200.100
SWITCH(config-dhcp-pool)#deny unknown-clients
SWITCH(config-dhcp-pool)#pool guest
SWITCH(config-dhcp-pool)#range 192.168.200.200 192.168.200.254
SWITCH(config-dhcp-pool)#allow unknown-clients
SWITCH(config-dhcp-pool)#exit
SWITCH(config-dhcp-subnet)#option routers 192.168.200.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)#ip dhcp-server option domain-name-servers 114.114.114.114
SWITCH(config)#ip dhcp-server enable
```

S2/S3：空配置透传

28.4. 显示命令

- 显示 DHCP 服务器状态信息

```
SWITCH#show ip dhcp-server status
DHCP Server: Enable (conf.Enable)
```

- 显示地址分配信息

```
SWITCH#show ip dhcp-server leases
Name                MAC                IP              Begin               End                 Manufacturer
------------------- ------------------ --------------- ------------------- ------------------- --------------------
liulang-work        00:0e:c6:c1:38:4a  3.3.3.254       1970-01-01 00:00:36 1970-01-01 00:10:36 ASIX ELECTRONICS CORP.
```

29. 配置 AAA

29.1. 协议概述

AAA 是 Authentication Authorization and Accounting（认证、授权和记账）的简称，它提供了对认证、授权和记账功能进配置的一致性框架。

AAA 以模块方式提供以下服务：

- 认证：验证用户是否可获得访问权，可选使用 RADIUS 协议、TACACS+协议或 Local（本地）等。身份认证是在允许用户访问网络和网络服务前对其身份进行识别的一种方法。
- 授权：授权用户可使用哪些服务。AAA 授权通过定义一系列的属性对来实现，这些属性对描述了用户被授权执行的操作。这些属性对可以存放在网络设备上，也可以远程存放在安全服务器上。
- 记账：记录用户使用网络资源的情况。当 AAA 记账被启用时，网络设备便开始以统计记录的方式向安全服务器发送用户使用网络资源的情况。每个记账记录都是以属性对的方式组成，并存放在安全服务器上，这些记录可以通过专门软件进行读取分析，从而实现对用户使用网络资源的情况进行记账、统计、跟踪。

使用 AAA 有以下优点：

- 灵活性和可控制性强
- 可扩充性
- 标准化认证
- 多个备用系统。

29.1.1. 协议标准

AAA 本身无明确标准

RFC2865 Remote Authentication Dial In User Service (RADIUS). C. Rigney, S. Willens, A. Rubens, W. Simpson. June 2000. (Format: TXT, HTML)

RFC2866 RADIUS Accounting. C. Rigney. June 2000. (Format: TXT, HTML)

RFC8907 The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol. T. Dahm, A. Ota, D.C. Medway Gash, D. Carrel, L. Grant. September 2020.

29.2. 配置命令

29.2.1. 全局配置命令

- 全局开启/关闭 AAA 功能

命令	SWITCH(config)# **aaa new-model** SWITCH(config)#**no aaa new-model**
描述	全局开启、关闭 AAA 功能。

- 配置 AAA 服务器组

命令	SWITCH(config)# **aaa group server (radius) (default|**NAME**)** SWITCH(config)# **aaa group server (tacacs+) (default|**NAME**)**

	SWITCH(config)# **no aaa group server (radius|tacacs+) (default|**NAME**)**
描述	服务器组配置。 可选配置。默认不存在服务器组配置，也不使用服务器方法。

- 配置 AAA 服务器

命令	SWITCH(config-gs-rad)# **server** A.B.C.D **(auth-port** <1-65535>**|) (acct-port** <1-65535>**|) (key** STRING**)** SWITCH(config-gs-tac)# **server** A.B.C.D **(port** <1-65535>**|) (key** STRING**)** SWITCH(config-gs-rad)# **no server** A.B.C.D SWITCH(config-gs-tac)# **no server** A.B.C.D
描述	服务器组模式下配置。 配置 RADIUS、TACACS+服务器信息，包含基本 IP 地址，端口信息，共享密钥 可选配置。 **注意：受实现限制，当前 radius 记账端口号始终为认证端口号+1，配置无效**

- 配置服务器组超时时间

命令	SWITCH(config-gs-rad)# **timeout** <1-120> SWITCH(config-gs-tac)# **timeout** <1-120> SWITCH(config-gs-rad)# **no timeout** SWITCH(config-gs-tac)# **no timeout**
描述	服务器组模式下配置。 配置组内服务器超时时间。 可选配置。

- 配置组服务信息字段

命令	SWITCH(config-gs-tac)# **service** NAME SWITCH(config-gs-tac)# **no service**
描述	TACACS+服务器组模式下配置。 配置组内服务信息。 可选配置。

- 配置 AAA 方法信息

命令	SWITCH(config)# **aaa (authentication|authorization|accounting) (login|ssh|web|dot1x|command) default {group (radius|tacacs+|**NAME**)|local|none}** SWITCH(config)#**no aaa (authentication|authorization|accounting) (login|ssh|web|dot1x|command) default**
描述	全局配置模式。 配置 AAA 方法信息。 可选配置。默认使用本地认证。 **注意 1：none 认证时也需要提供本机存在的用户名(比如 admin)，否则可能出错** **注意 2: web 服务不支持授权/记账**

29.3. 配置案例

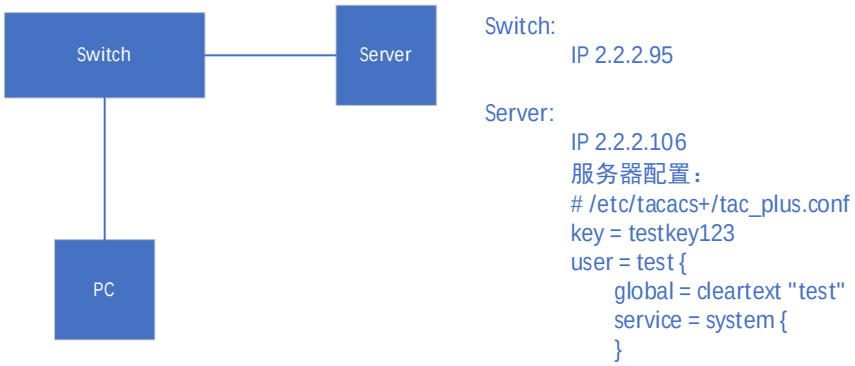
29.3.1. 使用 tacacs+方法进行 ssh 登录认证

7) 需求

- 见组网图描述

8) 组网图

图 29-1SSH 通过 tacacs+服务器认证记账典型组网图



说明：无

9) 典型配置举例

Switch：

```
SWITCH(config)# aaa new-model
SWITCH(config)# aaa group server tacacs+ default
SWITCH(config-gs-tac)# server 2.2.2.106 key testkey123
SWITCH(config-gs-tac)# exit
SWITCH(config)# aaa authentication ssh default group tacacs+
SWITCH(config)# aaa accounting ssh default group tacacs+
SWITCH(config)# username test remote
```

设备 IP 配置和 ssh 配置参考配置文档对应章节，此处省略

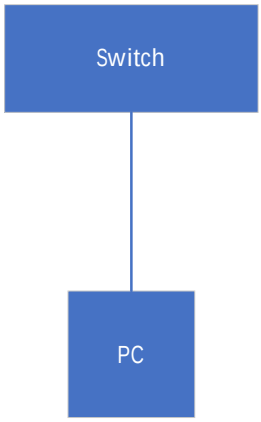
29.3.2. 使用 none 方法执行串口登录

4) 需求

- 见组网图描述

5) 组网图

图 29-2 串口使用 none 认证记账典型组网图




```
Switch:
        aaa new-model
        aaa authentication login default none
        aaa accounting login default none
```

6) 典型配置举例

参考组网图

29.4. 显示命令

- 无

30. 故障诊断

30.1. Ping/tracerout

- 执行 ping 功能

命令	SWITCH#**ping {ip** IPADDR **| ipv6** IPV6ADDR**}**
描述	执行 ping 命令

- 执行 traceroute 功能

命令	SWITCH# **traceroute {ip** IPADDR **| ipv6** IPV6ADDR **}**
描述	执行 traceroute 命令

30.2. 光模块信息检测

30.2.1. 光模块配置命令

- 配置端口监控使能

Command	SWITCH(config-if)# **optical-transceiver monitor enable** SWITCH(config-if)# **no optical-transceiver monitor enable**
Description	使能监控端口光模块状态 默认关闭

- 配置端口监控时间间隔

Command	SWITCH(config)# **optical-transceiver monitor interval** MINUTES SWITCH(config-if)# **no optical-transceiver monitor interval**
Description	设置端口监控光模块时间间隔 默认 15 分钟 范围 1 ~ 1440，单位分钟

- 配置端口光模块温度告警阈值

Command	SWITCH(config-if)# **optical-transceiver threshold temperature** HALARM HWARN LWARN LALARM SWITCH(config-if)# **no optical-transceiver threshold temperature**
Description	默认情况下，光模块自身已带有默认温度阈值信息，因此不建议用户做此配置 HALARM: 高温告警阈值, 范围 -255 to 255 C HWARN: 高温警告阈值，范围 -255 to 255 C LWARN: 低温警告阈值，范围 -255 to 255 C LALARM: 低温告警阈值，范围 -255 to 255 C 高温告警阈值不能小于高温警告阈值 低温警告阈值不能小于低温告警阈值

- 配置端口光模块电压告警阈值

Command	SWITCH(config-if)# **optical-transceiver threshold voltage** HALARM HWARN LWARN

	LALARM SWITCH(config-if)# **no optical-transceiver threshold voltage**
Description	默认情况下，光模块自身已带有默认电压阈值信息，因此不建议用户做此配置 HALARM: 过压告警阈值, 范围 0.00 to 5.00 V HWARN: 过压警告阈值，范围 0.00 to 5.00 V LWARN: 欠压警告阈值，范围 0.00 to 5.00 V LALARM: 欠压告警阈值，范围 0.00 to 5.00 V 过压告警阈值不能小于过压警告阈值 欠压警告阈值不能小于欠压告警阈值

- 配置端口光模块电流告警阈值

Command	SWITCH(config-if)# **optical-transceiver threshold bias** HALARM HWARN LWARN LALARM SWITCH(config-if)# **no optical-transceiver threshold bias**
Description	默认情况下，光模块自身已带有默认电流阈值信息，因此不建议用户做此配置 HALARM: 过流告警阈值, 范围 0.00 to 500.00 mA HWARN: 过流警告阈值，范围 0.00 to 500.00 mA LWARN: 欠流警告阈值，范围 0.00 to 500.00 mA LALARM: 欠流告警阈值，范围 0.00 to 500.00 mA 过流告警阈值不能小于过流警告阈值 欠流警告阈值不能小于欠流告警阈值

- 配置端口光模块接收功率告警阈值

Command	SWITCH(config-if)# **optical-transceiver threshold rx-power** HALARM HWARN LWARN LALARM SWITCH(config-if)# **no optical-transceiver threshold rx-power**
Description	默认情况下，光模块自身已带有默认接收功率阈值信息，因此不建议用户做此配置 HALARM: 过高告警阈值, 范围-40.00 to 10.00 dBm HWARN: 过高警告阈值，范围-40.00 to 10.00 dBm LWARN: 过低警告阈值，范围-40.00 to 10.00 dBm LALARM: 过低告警阈值，范围-40.00 to 10.00 dBm 过高告警阈值不能小于过高警告阈值 过低警告阈值不能小于过低告警阈值

- 配置端口光模块发送功率告警阈值

Command	SWITCH(config-if)# **optical-transceiver threshold tx-power** HALARM HWARN LWARN LALARM SWITCH(config-if)# **no optical-transceiver threshold tx-power**
Description	默认情况下，光模块自身已带有默认发送功率阈值信息，因此不建议用户做此配置 HALARM: 过高告警阈值, 范围-40.00 to 10.00 dBm HWARN: 过高警告阈值，范围-40.00 to 10.00 dBm LWARN: 过低警告阈值，范围-40.00 to 10.00 dBm LALARM: 过低告警阈值，范围-40.00 to 10.00 dBm 过高告警阈值不能小于过高警告阈值 过低警告阈值不能小于过低告警阈值

30.2.2. 光模块告警 trap 节点

除发出告警或警告信息，光模块监控单元还将 tarp 消息到 snmp 服务器

Node	data
Mib files	TNPL_private_2.1.89(interface_ddm).mib
Alarm oid	1, 3, 6, 1, 4, 1, 37831, 101, 110, 1
Warning oid	1, 3, 6, 1, 4, 1, 37831, 101, 110, 2
Ifindex oid	1, 3, 6, 1, 4, 1, 37831, 100, 30, 2, 1, 1
Information oid	1, 3, 6, 1, 4, 1, 37831, 100, 30, 2, 1, 2

30.2.3. 光模块信息显示

- 显示端口光/铜缆模块信息

该命令用于显示光口上插入的的光/铜缆模块的信息。

命令	SWITCH#**show interface {**IFNAME **|} optical-transceiver {info |}**
描述	不指定 **interface-id** 则显示所有端口的模块信息 不指定 **info** 则显示端口模块的 DDM 信息,z 指定则显示完整模块信息（基本信息，告警信息，厂商信息）

显示所有端口模块 DDM 信息

DDM 信息显示要素如下:

字段	说明
Temp	模块当前的工作温度, 单位为℃，精确到 1°C。
Voltage	模块当前的工作电压，单位为 V，精确到 0.01V。
Bias	模块当前的工作电流，单位为 mA，精确到 0.01mA。
RX power	模块当前的接收光功率，单位为 dBm，精确到 0.01dBM。
TX power	模块当前的发送光功率，单位为 dBm，精确到 0.01dBM。
OK	正常，无需干预
WARN	告警，表示超过设备允许范围，需要注意。
ALARM	异常，表示严重超过设备允许状态，需要立即干预。
ABSENT	不在位
NA	端口不支持/模块不支持
TIMEOUT	超时
ERR	错误

```
SWITCH#show interface optical-transceiver
  Port      Temp       Voltage       Bias         RX power      TX power
            [C]          [V]         [mA]          [dBm]         [dBm]
------- ---------- ------------ ------------ ------------- -------------
GiE0/9    42(OK)       3.20(OK)     32.34(OK)     -3.98(OK)      1.64(OK)
GiE0/10   ABSENT       ABSENT        ABSENT        ABSENT         ABSENT
GiE0/11   ABSENT       ABSENT        ABSENT        ABSENT         ABSENT
GiE0/12   ABSENT       ABSENT        ABSENT        ABSENT         ABSENT
```

显示端口光模块/铜缆模块总体信息:

模块总体信息显示要素如下:

操作错误信息

字段	说明
Transceiver absent!	获取信息失败，可能模块不在位
Get transceiver info timeout!	获取信息超时，需要重新获取
Port doesn't support get module info!	端口不支持获取模块信息

基本信息

字段	说明
Transceiver Type	模块类型
Connector Type	接口类型
Wavelength(nm)	波长
Link Length	支持的链路长度
Digital Diagnostic Monitoring	是否支持 DDM 功能
Vendor Serial Number	模块序列号

告警信息

字段	说明
RX Channel loss of signal	接收信号丢失
RX Channel power high	接收光功率高告警
RX Channel power low	接收光功率低告警
TX Channel fault	发送错误
TX Channel bias high	偏置电流高告警
TX Channel bias low	偏置电流低告警
TX Channel power high	发送光功率高告警
TX Channel power low	发送光功率低告警
Temperature high	温度高告警
Temperature low	温度低告警
Voltage high	电压高告警
Voltage low	电压低告警
None	无告警
This module doesn't support getting alarm!	模块不支持获取告警信息

厂商信息

字段	说明
Vendor Name	厂商名称
Vendor OUI	厂商 OUI
Vendor Part Number	厂商部件号
Vendor Revision	厂商版本号
Manufacturing Date	生产日期
Encoding	编码类型

```
SWITCH#show interface gigabitEthernet0/9 optical-transceiver info
#####################################################
                  gigabitEthernet0/9
+-------------------------------------------------+
|Transceiver base information:                    |
+-------------------------------------------------+
|Transceiver Type    :  1000BASE-ZX-SFP           |
|Connector Type      :  LC                        |
```

```
|Wavelength(nm)      :  1550                      |
|Link Length     :                               |
|    SMF fiber                                   |
|        -- 80km                                 |
|Digital Diagnostic Monitoring  : YES            |
|Vendor Serial Number           : WT1703230031   |
+------------------------------------------------+
|Transceiver current alarm information:          |
+------------------------------------------------+
|None                                            |
+------------------------------------------------+
|Transceiver vendor information:                 |
+------------------------------------------------+
|Vendor Name         : OEM                       |
|Vendor OUI          : 000000                    |
|Vendor Part Number  : SFP-GE-ZX-SM1550          |
|Vendor Revision     : V2                        |
|Manufacturing Date  : 2017-03-25                |
|Encoding            : 8B10B                     |
+------------------------------------------------+
```

- 显示端口光模块阈值信息

显示接入到设备端口的光模块阈值信息

Command	SWITCH#**show interface {**IFNAME **|} optical-transceiver threshold**
Description	不指定 **interface-id** 则显示所有端口的模块信息 如果没有配置该端口的光模块阈值信息，将采用光模块默认阈值参数

```
SWITCH#show interface optical-transceiver threshold

Interface tengigabitEthernet0/25:
Item            High-alarm      High-warn       Low-warn        Low-alarm
Temp(Celsius)   100             90              -40             -50
Voltage(V)      3.50            3.47            3.15            3.04
Bias(mA)        15.00           12.00           4.00            5.58
RX power(dBm)   10.25           5.30            -10.22          -12.40
TX power(dBm)   2.100           1.100           -9.100          -11.00
```

30.3. Dying-gasp

Dying-gasp 功能为断掉设备供电瞬间，依靠设备内部电容等储能器件供电 10-20ms 时间，支持设备发出掉电告警信息。

根据 802.3ah 中定义，当发生设备掉电事件后，设备向其连接设备发出 OAM 事件报文，由于 OAM 为点到点协议，掉电事件报文在送达到下一个支持 OAM 的设备后，不再继续转发。接收到掉电事件的设备将输出掉电 LOG 提示信息。

除 OAM 告警信息，掉电设备还将发出一条 trap 信息到 smmp 服务器。

节点信息	数据
Mib files	DOT3-OAM-MIB.mib
oid	1, 3, 6, 1, 2, 1, 158, 1, 6, 1, 4

value	dyingGaspEvent(257)

- 使能 dying-gasp 功能

命令	SWITCH(config)#**dying-gasp enable** SWITCH(config)#**no dying-gasp**
描述	打开/关闭 dying-gasp 功能

LOG 信息

掉电告警 log：”Device 00:d0:f8:c8:23:12 power down.”

30.4. 线缆检测

电缆故障可能会导致接口处于 Down 状态或者接口即使处于 Up 状态但是接口速率发生异常。用户可以执行此命令检测电缆是否出现故障，并定位故障点，从而帮助解决电缆故障。使用线缆检测功能需注意下面几点：

- 仅电接口支持此命令。
- 执行本命令时，可能会在短时间内影响该接口的业务正常使用。
- 当线长小于 6 米时，测试结果与实际值存在偏差，线越短偏差越大。

- 端口执行线缆检测功能

命令	SWITCH(config-if))#**cable-detect**
描述	在端口上执行一次线缆检测，2 秒钟后，通过 show 命令查看检测结果

在端口 gi0/1 上执行线缆检测：

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet 0/1
SWITCH(config-if)#cable-detect

%Please wait for about 2 seconds and execute the show cable-detect command to view
the execution results.
```

查看线缆检测结果：

```
SWITCH#show cable-detect interface gigabitEthernet 0/1
 Pair A length(meters): 0
 Pair B length(meters): 0
 Pair C length(meters): 0
 Pair D length(meters): 0
 Pair A state: OK
 Pair B state: OK
 Pair C state: OK
 Pair D state: OK
```

字段	说明
Pair X length(meters)	电缆长度。 有故障时为接口到故障位置的长度。 单位米。
Pair X state	网线状态： OK（正常）：表示线对（PAIR）正常终结。

	Open（开路）：表示线对开路。 Short（短路）：表示线对短路。 Unknown（未知）：其他未知故障原因。