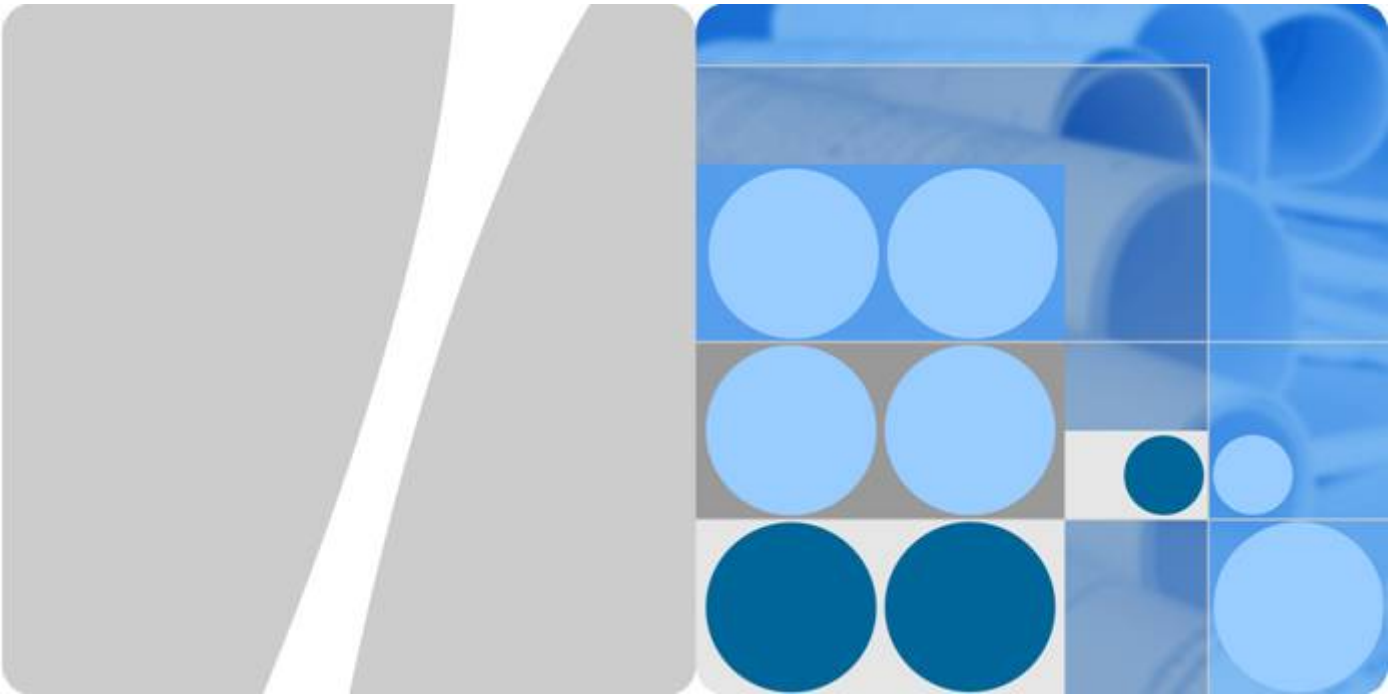


S1720, S2700, S3700, S5700, S6700, S7700, S7900, S9700 系列交换机

常用操作指南

文档版本　17

发布日期　2018-08-17

华为技术有限公司

HUAWEI

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://e.huawei.com

前 言

读者对象

本文档适用于负责配置和管理交换机的网络工程师。您应该熟悉以太网基础知识，且具有丰富的网络部署与管理经验。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
注意	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “注意”不涉及人身伤害。
说明	用于突出重要/关键信息、最佳实践和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

命令行格式约定

在本文中可能出现下列命令行格式，它们所代表的含义如下。

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。

格式	意义
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&的参数可以重复1～n次。
#	由“#”开始的行表示为注释行。

接口编号约定

本手册中出现的接口编号仅作示例，并不代表设备上实际具有此编号的接口，实际使用中请以设备上存在的接口编号为准。

安全约定

- 密码配置约定
  - 配置密码时请尽量选择密文模式(cipher)。为充分保证设备安全，请用户不要关闭密码复杂度检查功能，并定期修改密码。
  - 配置明文模式的密码时，请不要以“%^%#.....%^%#”、“%#%#.....%#%#”、“%@%@.....%@%@”或者“@%@%.....@%@%”作为起始和结束符。因为用这些字符为起始和结束符的是合法密文（本设备可以解密的密文），配置文件会显示与用户配置相同的明文密码。
  - 配置密文密码时，不同特性的密文密码不能互相使用。例如AAA特性生成的密文密码不能用于配置其他特性的密文密码。
- 加密算法约定

  目前设备采用的加密算法包括3DES、AES、RSA、SHA1、SHA2和MD5。3DES、RSA和AES加密算法是可逆的，SHA1、SHA2和MD5加密算法是不可逆的。DES/3DES/RSA(1024位以下)/MD5(数字签名场景和口令加密)/SHA1(数字签名场景)加密算法安全性低，存在安全风险。在协议支持的加密算法选择范围内，建议使用更安全的加密算法，比如AES/RSA(2048位以上)/SHA2/HMAC-SHA2。具体采用哪种加密算法请根据场景而定：对于管理员类型的密码，必须采用不可逆加密算法，推荐使用安全性更高的SHA2。
- 个人数据约定

  您购买的产品、服务或特性在业务运营或故障定位的过程中将可能获取或使用用户的某些个人数据（如终端用户的MAC地址或IP地址），因此您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。
- 本文档中出现的“镜像端口、端口镜像、流镜像、镜像”等相关词汇仅限于为了描述该产品进行检测通信传输中的故障和错误的目的而使用，不涉及采集、处理任何个人数据或任何用户通信内容。

特别声明

本手册仅作为使用指导，其内容（如Web界面、CLI命令格式、命令输出）依据实验室设备信息编写。手册提供的内容具有一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号不同、配置文件不同等原因，可能造成手册中提供的内容与用户使用的设备界面不一致。请以用户设备界面的信息为准，本手册不再针对前述情况造成的差异一一说明。

本手册中提供的最大值是设备在实验室特定场景（例如，被测试设备上只有某种类型的单板，或者只配置了某一种协议）达到的最大值。在现实网络中，由于设备硬件配置不同、承载的业务不同等原因会使设备测试出的最大值与手册中提供的数据不一致。

目 录

1 常见系统操作

关于本章

介绍设备登录和文件管理中的常见操作，例如密码丢失如何操作、配置本地用户、设置屏显等。

1.1 Console 口登录密码丢失后如何恢复

如果忘记了Console口登录密码，用户可以通过以下两种方式来设置新的Console口登录密码。

通过 STelnet/Telnet 登录交换机设置新的 Console 口登录密码

注意

使用Telnet协议存在安全风险，建议用户使用STelnet V2登录设备。

这种方法的前提是：用户拥有STelnet/Telnet账号并且具有管理员的权限。以下涉及的命令行及回显信息以STelnet登录设备修改Console口密码为例。用户通过STelnet账号登录交换机后，请按照如下步骤进行配置。

以登录用户界面的认证方式为密码认证，密码为**Huawei@123**为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] authentication-mode password
[HUAWEI-ui-console0] set authentication password cipher Huawei@123
[HUAWEI-ui-console0] return
<HUAWEI> save
```

以登录用户界面的认证方式为AAA认证，用户名为**admin123**，密码为**Huawei@123**为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] authentication-mode aaa
[HUAWEI-ui-console0] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin123 password irreversible-cipher Huawei@123
[HUAWEI-aaa] local-user admin123 service-type terminal
[HUAWEI-aaa] return
<HUAWEI> save
```

通过 BootROM/BootLoad 清除 Console 口登录密码

交换机的BootROM/BootLoad提供了清除Console口登录密码的功能，用户可以在交换机启动后修改Console口登录密码，然后保存配置。

说明

如果交换机是双主控，则需要在执行以下操作前将备用主控板拔下，待执行完以下操作后，再插上备用主控板，执行save命令以保证主用主控板和备用主控板配置一致。

交换机的BootROM/BootLoad提供了清除Console口登录密码的功能，用户可以在交换机启动后修改Console口登录密码，然后保存配置。请按照如下步骤进行配置。

以BootROM菜单为例，请按照如下步骤进行配置。

1. 通过Console口连接交换机，并重启交换机。当界面出现以下打印信息时，及时按下快捷键“Ctrl+B”并输入BootROM密码，进入BootROM主菜单。

   框式交换机打印信息：

   ```
   Press Ctrl+B to enter boot menu ...  1

   Password:       //输入BootROM密码
   ```

   盒式交换机打印信息：

   ```

   Press Ctrl+B or Ctrl+E to enter BootROM menu ... 2
   password:      //输入BootROM密码
   ```


说明

- 盒式交换机的某些款型支持使用快捷键“Ctrl+E”进入BootROM主菜单，请根据设备的界面提示操作。
- 盒式交换机在V100R006C03之前的版本，BootROM默认密码为**huawei**；在V100R006C03及之后的版本，默认密码为**Admin@huawei.com**。
- 框式交换机在V100R006及之前的版本，BootROM默认密码为**9300**；在V100R006之后的版本，默认密码为**Admin@huawei.com**。
- 不同版本和不同形态的设备回显有差异，请以实际设备显示为准。

2. 在BootROM主菜单下选择“Clear password for console user”清除Console口登录密码。
3. 根据交换机的提示，在BootROM主菜单下选择“Boot with default mode”启动设备。

   说明

   请注意，此处不要选择“Reboot”选项，否则此次清除密码将失效。
4. 完成系统启动后，通过Console口登录时不需要认证，登录后按照系统提示配置验证密码。（V200R009及之后版本，完成系统启动后，通过Console口登录时认证方式为None，系统启动后不会提示配置验证密码。）
5. 登录交换机后，用户可以根据需要配置Console用户界面的认证方式及密码。具体配置与**通过STelnet/Telnet登录交换机设置新的Console口登录密码**类似，不再赘述。

相关信息

视频

如何恢复Console口密码

1.2 Telnet 登录密码丢失后如何恢复

如果忘记了Telnet登录密码，用户可以通过Console口登录交换机后设置新的Telnet登录密码。

说明

以下涉及的命令行以V200R008C00版本的S7700交换机为例。

通过Console口登录设备。

1. 将Console通信电缆的DB9（孔）插头插入PC机的串口（COM）中，再将RJ-45插头端插入设备的Console口中。
2. 在PC上打开终端仿真软件，新建连接，设置连接的接口，配置通信参数如下：
   - 波特率：9600
   - 数据位：8
   - 停止位：1
   - 奇偶校验位：无
   - 流控：无
3. 单击“Connect”，根据提示输入或配置登录密码，完成登录。

以登录VTY0的验证方式为密码验证，密码为**Huawei@123**为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
```



```
[HUAWEI-ui-vty0] protocol inbound telnet   //V200R006及之前版本缺省使用的协议为Telnet协议，可以不配置该项；V200R007及之后版本缺省使用的协议为SSH协议，必须配置。
[HUAWEI-ui-vty0] authentication-mode password
[HUAWEI-ui-vty0] set authentication password cipher Huawei@123
[HUAWEI-ui-vty0] user privilege level 15
[HUAWEI-ui-vty0] return
<HUAWEI> save
```

以登录VTY0的验证方式为AAA授权验证，用户名为**admin123**，密码为**Huawei@123**为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] protocol inbound telnet   //V200R006及之前版本缺省使用的协议为Telnet协议，可以不配置该项；V200R007及之后版本缺省使用的协议为SSH协议，必须配置。
[HUAWEI-ui-vty0] authentication-mode aaa
[HUAWEI-ui-vty0] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin123 password irreversible-cipher Huawei@123
[HUAWEI-aaa] local-user admin123 service-type telnet
[HUAWEI-aaa] local-user admin123 privilege level 15
[HUAWEI-aaa] return
<HUAWEI> save
```

1.3 Web 登录密码丢失后如何恢复

如果忘记了Web登录密码，用户可以通过Console口、Telnet或STelnet方式登录交换机后设置新的Web登录密码。

注意

Telnet协议存在安全风险，建议用户通过Console口或STelnet方式登录设备。

以用户名为**admin123**，密码为**Huawei@123**为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin123 password irreversible-cipher Huawei@123
[HUAWEI-aaa] local-user admin123 service-type http
[HUAWEI-aaa] local-user admin123 privilege level 15
[HUAWEI-aaa] return
<HUAWEI> save
```

1.4 BootROM 密码丢失后如何恢复

如果忘记了BootROM密码，用户可以在登录交换机后在用户视图执行命令**reset boot password**重置BootROM菜单的密码为缺省值。

缺省情况下:

- 盒式交换机在V100R006C03之前的版本，BootROM默认密码为**huawei**；在V100R006C03及之后的版本，默认密码为**Admin@huawei.com**。
- 框式交换机在V100R006及之前的版本，BootROM默认密码为**9300**；在V100R006之后的版本，默认密码为**Admin@huawei.com**。

1.5 清空配置

如果需要清除配置，恢复成出厂配置，请执行命令**reset saved-configuration**，清除设备下次启动时使用的配置文件信息，然后重启设备，重启时如果提示保存配置，请选择“N”不保存。

注意

请慎重执行此命令，建议在技术支持人员指导下使用。

```
<HUAWEI> reset saved-configuration
Warning: The action will delete the saved configuration in the device.
The configuration will be erased to reconfigure. Continue? [Y/N]:y
Warning: Now clearing the configuration in the device.
Info: Succeeded in clearing the configuration in the device.
<HUAWEI> reboot
Info: The system is now comparing the configuration, please wait.
Warning: The configuration has been modified, and it will be saved to the next startup saved-
configuration file flash:/vrpcfg.zip. Continue? [Y/N]:n    //此处请选择“N”
Info: If want to reboot with saving diagnostic information, input 'N' and then execute 'reboot
save diagnostic-information'.
System will reboot! Continue?[Y/N]:y
```

以上显示信息请以设备实际显示为准。

相关信息

视频

如何恢复设备出厂配置

1.6 配置 Telnet 类型的本地用户

以登录用户界面的验证方式为AAA授权验证，用户名为**admin123**，密码为**Huawei@123**为例，配置如下。

本操作的前置条件是设备已经使能了Telnet服务器功能。

说明

以下涉及的命令行以V200R008C00版本的S7700交换机为例。

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] protocol inbound telnet   //V200R006及之前版本缺省使用的协议为Telnet协议，可以不配置该项；V200R007及之后版本缺省使用的协议为SSH协议，必须配置。
[HUAWEI-ui-vty0] authentication-mode aaa
[HUAWEI-ui-vty0] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin123 password irreversible-cipher Huawei@123
[HUAWEI-aaa] local-user admin123 service-type telnet
[HUAWEI-aaa] local-user admin123 privilege level 15
[HUAWEI-aaa] return
<HUAWEI> save
```


1.7 配置用户级别

当用户的认证方式为密码认证（password）或不验证（none）时，可以采用以下方式配置用户级别（以VTY用户界面为例）：

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] user privilege level 15  //配置VTY 0用户界面下用户级别为15
```

当用户的认证方式为AAA本地认证时，可以采用以下方式配置用户级别（以VTY用户界面为例），优先级由上到下依次降低：

- 配置某个用户的用户级别。

  ```
  <HUAWEI> system-view
  [HUAWEI] aaa
  [HUAWEI-aaa] local-user user1 privilege level 15  //配置用户user1的用户级别为15
  ```

- 配置某个域下所有用户的用户级别。

  ```
  <HUAWEI> system-view
  [HUAWEI] aaa
  [HUAWEI-aaa] service-scheme sch1
  [HUAWEI-aaa-service-sch1] admin-user privilege level 15  //配置用户级别为15
  [HUAWEI-aaa-service-sch1] quit
  [HUAWEI-aaa] domain domain1
  [HUAWEI-aaa-domain-domain1] service-scheme sch1  //在域domain1下绑定业务方案sch1
  ```

- 配置从某个用户界面登录的所有用户的用户级别。

  ```
  <HUAWEI> system-view
  [HUAWEI] user-interface maximum-vty 15  //配置VTY用户界面最大数目为15
  [HUAWEI] user-interface vty 0 14  //进入0～14的VTY用户界面视图
  [HUAWEI-ui-vty0-14] user privilege level 15  //配置VTY 0～VTY 14用户界面下用户级别为15
  ```

1.8 设置屏显

在用户视图或用户界面视图下，执行命令**screen-length** *screen-length* [**temporary**]，设置终端屏幕每屏显示的行数。在用户视图下执行该命令时，**temporary**关键字为必选，用于指定终端屏幕的临时显示行数。缺省情况下，终端屏幕每屏显示的行数为24行。

对于V200R005及之前版本，在任意视图下，执行命令**screen-width** *screen-length*，设置终端屏幕每屏显示的列数。缺省情况下，终端屏幕每屏显示的列数为80列，每个字符为一列。对于V200R005之后版本，不支持通过该命令调整屏幕显示列数，显示列数更改为自适应调整。

1.9 使用基本 ACL 规则限制用户登录

通过STelnet/Telnet登录设备后，用户可以配置ACL规则限制用户登录的源地址，只允许特定IP的用户或者网段登录设备。

说明

使用Telnet协议存在安全风险，建议用户使用STelnet V2登录设备。

本操作中假设用户已经使用STelnet/Telnet登录设备。

配置ACL 2005规则，限制VTY 0～VTY 4界面只允许IP地址为192.168.1.5的用户和10.10.5.0/24网段的用户登录设备，配置如下。

```
<HUAWEI> system-view
[HUAWEI] acl 2005
```



```
[HUAWEI-acl-basic-2005] rule permit source 192.168.1.5 0   //允许IP地址为192.168.1.5的用户登录设备。
[HUAWEI-acl-basic-2005] rule permit source 10.10.5.0 0.0.0.255   //允许10.10.5.0/24网段的用户登录设备。
[HUAWEI-acl-basic-2005] quit
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] acl 2005 inbound
[HUAWEI-ui-vty0-4] quit
```

1.10 备份配置文件

为防止设备意外损坏，导致配置文件无法恢复，用户可以通过FTP方式将配置文件备份至服务器。假设用户PC的IP地址为10.110.24.254/24，设备的IP地址为10.136.23.5/24，配置如下。

- 设备作为FTP服务器，用户PC作为FTP客户端

  # 配置设备的FTP功能及FTP用户信息。

  ```
  <HUAWEI> system-view
  [HUAWEI] ftp server enable
  [HUAWEI] aaa
  [HUAWEI-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
  [HUAWEI-aaa] local-user admin1234 privilege level 15
  [HUAWEI-aaa] local-user admin1234 service-type ftp
  [HUAWEI-aaa] local-user admin1234 ftp-directory cfcard:/
  [HUAWEI-aaa] quit
  [HUAWEI] quit
  ```

  # 保存设备当前配置。

  ```
  <HUAWEI> save
  ```

  # 从终端PC通过FTP连接设备，输入用户名**admin1234**和密码**Helloworld@6789**，并采用**binary**模式进行文件传输。

  终端以Windows XP操作系统为例说明。

  ```
  C:\Documents and Settings\Administrator> ftp 10.136.23.5
  连接到 10.136.23.5。
  220 FTP service ready.
  用户 (10.136.23.5:(none)): admin1234
  331 Password required for admin1234.
  密码:
  230 User logged in.
  ftp> binary
  200 Type set to I.
  ftp>
  ```

  # 备份配置文件。

  ```
  ftp> get vrpcfg.zip
  200 Port command okay.
  150 Opening BINARY mode data connection for vrpcfg.zip.
  226 Transfer complete.
  ftp: 收到 1257 字节，用时 0.03秒 40.55千字节/秒。
  ```

- 用户PC作为FTP服务器，设备作为FTP客户端

  # 启动FTP服务器程序。

  在用户PC上启动FTP服务器应用程序，设置好配置文件的传输路径、FTP服务器IP地址、端口号、用户名和密码。

  # 保存设备当前配置。

  ```
  <HUAWEI> save
  ```

  # 登录FTP服务器。

  ```
  <HUAWEI> ftp 10.110.24.254
  Trying 10.110.24.254 ...
  ```



```
Press CTRL+K to abort
Connected to 10.110.24.254.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user    //WFTPD为本地FTP服务器程序。
User(10.135.86.164:(none)):admin123    //输入用户名。
331 Give me your password, please
Enter password:    //输入用户密码。
230 Logged in successfully

[ftp]
```

备份配置文件。

```
[ftp] put config.cfg
200 Port command successful.
150 Opening data connection for config.cfg.
226 File received ok
FTP: 1257 byte(s) sent in 0.03 second(s) 40.55Kbyte(s)/sec.
```

说明

- 将配置文件备份到用户PC后，请对比用户PC上配置文件大小是否与设备上一致。如果不一致，可能是在文件备份过程中出现异常，请重新备份。
- 如果用户需要使用更简单的配置过程，可以使用TFTP方式备份配置文件，配置用户PC作为TFTP服务器，设备作为TFTP客户端。此配置过程与配置用户PC作为FTP服务器，设备作为FTP客户端的过程相似，只是在配置本地服务器程序的时候不需要用户名和密码，直接在设备上执行命令**tftp 10.110.24.254 put config.cfg**即可。
- TFTP方式没有授权和认证，并且为明文传输数据；FTP方式具有授权和认证功能，也采用明文传输数据。这两种方式均存在安全隐患，适合在网络条件良好的环境下使用。如果用户对网络安全性能要求较高，建议使用SFTP V2、SCP或FTPS方式备份配置文件。

1.11 恢复配置文件

当用户进行了错误的配置，导致功能异常的时候，可以将备份的配置文件传输到设备上并设置为下次启动配置文件。以用户PC的IP地址为10.110.24.254/24，设备的IP地址为10.136.23.5/24为例，配置如下。

1. 通过FTP方式将备份的配置文件传输到设备中
   - 设备作为FTP服务器，本地PC作为FTP客户端，将备份的配置文件上传到设备中

     # 配置设备的FTP服务器功能及FTP用户信息。

     ```
     <HUAWEI> system-view
     [HUAWEI] ftp server enable
     [HUAWEI] aaa
     [HUAWEI-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
     [HUAWEI-aaa] local-user admin1234 privilege level 15
     [HUAWEI-aaa] local-user admin1234 service-type ftp
     [HUAWEI-aaa] local-user admin1234 ftp-directory cfcard:/
     [HUAWEI-aaa] quit
     [HUAWEI] quit
     ```

     # 从终端PC通过FTP连接设备，输入用户名**admin1234**和密码**Helloworld@6789**，并采用**binary**模式进行文件传输。

     终端以Windows XP操作系统为例说明。

     ```
     C:\Documents and Settings\Administrator> ftp 10.136.23.5
     连接到 10.136.23.5。
     220 FTP service ready.
     用户 (10.136.23.5:(none)): admin1234
     331 Password required for admin1234.
     密码:
     230 User logged in.
     ftp> binary
     ```

```
200 Type set to I.
ftp>
```

上传备份的配置文件到设备中。

```
ftp> put vrpcfg.zip
200 Port command okay.
150 Opening BINARY mode data connection for vrpcfg.zip.
226 Transfer complete.
ftp: 发送 1257 字节，用时 0.03秒 40.55千字节/秒。
```

- 用户PC作为FTP服务器，设备作为FTP客户端

  # 启动FTP服务器程序。

  在PC上启动FTP服务器应用程序，设置好配置文件的传输路径、FTP服务器IP地址、端口号、用户名和密码。

  # 登录FTP服务器。

```
<HUAWEI> ftp 10.110.24.254
Trying 10.110.24.254 ...
Press CTRL+K to abort
Connected to 10.110.24.254.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user    //WFTPD为本地FTP服务器程序。
User(10.135.86.164:(none)):admin123    //输入用户名。
331 Give me your password, please
Enter password:    //输入用户密码。
230 Logged in successfully

[ftp]
```

  # 下载备份的配置文件到设备中。

```
[ftp] get config.cfg
Warning: The file config.cfg already exists. Overwrite it? [Y/N]:Y
//覆盖设备当前保存的配置文件。如果用户需要保留当前设备的配置文件，可以选择N后停止本次文件上传，重命名服务器中配置文件名，确保其与设备当前配置文件名不一致后再下载服务器中的配置文件。
200 Port command successful.
150 Opening data connection for config.cfg.
226 File sent ok
FTP: 1257 byte(s) received in 0.03 second(s) 40.55byte(s)/sec.
[ftp] bye
```

  说明

  - 将配置文件备份上传或者下载到设备后，请对比用户PC上配置文件大小是否与设备上一致。如果不一致，可能是在文件传输过程中出现异常，请重新传输。
  - 如果用户需要使用更简单的配置过程，可以使用TFTP方式下载服务器中的备份配置文件，配置用户PC作为TFTP服务器，设备作为TFTP客户端。此配置过程与配置用户PC作为FTP服务器，设备作为FTP客户端的过程相似，只是在配置本地服务器程序的时候不需要用户名和密码，直接在设备上执行命令**tftp 10.110.24.254 get config.cfg**即可。
  - TFTP方式没有授权和认证，并且为明文传输数据；FTP方式具有授权和认证功能，也采用明文传输数据。这两种方式均存在安全隐患，适合在网络条件良好的环境下使用。如果用户对网络安全性能要求较高，可以选择使用SFTP V2、SCP或FTPS方式上传或下载配置文件。

2. 设置恢复的配置文件为下次启动配置文件并重启设备

```
<HUAWEI> startup saved-configuration config.cfg
<HUAWEI> display startup
MainBoard:
  Configured startup system software:        cfcard:/device_software.cc
  Startup system software:                   cfcard:/device_software.cc
  Next startup system software:              cfcard:/device_software.cc
  Startup saved-configuration file:          cfcard:/config_old.cfg    //设备当前的配置文件名。
  Next startup saved-configuration file:     cfcard:/config.cfg    //下次启动的配置文件名。
  Startup paf file:                          default
```

```
  Next startup paf file:                    default
  Startup license file:                     default
  Next startup license file:                default
  Startup patch package:                    NULL
  Next startup patch package:               NULL

<HUAWEI> reboot    //重启设备。
Info: The system is now comparing the configuration, please wait.
Warning: The configuration has been modified, and it will be saved to the next startup saved-
configuration file cfcard:/config.cfg. Continue? [Y/N]:N    //输入N防止设备当前的配置保存到备
份的配置文件中。
Now saving the current configuration to the slot 13.
Save the configuration successfully.
Info: If want to reboot with saving diagnostic information, input 'N' and then execute
'reboot save diagnostic-information'.
System will reboot! Continue?[Y/N]:Y    //输入Y重启设备。
```

1.12 配置通过 STelnet 登录设备

以登录用户界面的验证方式为AAA授权验证，用户名为**admin123**，密码为**Huawei@123**为例，配置如下。

在服务器端生成本地密钥对。

```
<HUAWEI> system-view
[HUAWEI] dsa local-key-pair create
Info: The key name will be: HUAWEI_Host_DSA.
Info: The key modulus can be any one of the following : 1024, 2048.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
```

配置VTY用户界面。

```
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] protocol inbound ssh
[HUAWEI-ui-vty0-4] quit
```

注意

如果设备中已经配置了VTY 0 ~ VTY 4界面支持的协议为Telnet方式，如果将其修改为SSH方式，退出当前登录界面后，不能再使用Telnet方式登录设备。此时建议用户先配置VTY 0 ~ VTY 4界面支持的协议为all，即支持所有的协议。在成功配置STelnet后可以再执行protocol inbound ssh命令配置VTY 0 ~ VTY 4界面支持的协议为SSH。

新建用户名为**admin123**的SSH用户，且认证方式为**Password**。

```
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin123 password irreversible-cipher Huawei@123
[HUAWEI-aaa] local-user admin123 service-type ssh
[HUAWEI-aaa] local-user admin123 privilege level 15
[HUAWEI-aaa] quit
[HUAWEI] ssh user admin123 authentication-type password
```

设备开启STelnet服务功能。

```
[HUAWEI] stelnet server enable
```

配置SSH用户admin123的服务方式为STelnet。


```
[HUAWEI] ssh user admin123 service-type stelnet
```

通过第三方软件（例如PuTTY）登录设备，输入设备的IP地址，选择协议类型为SSH，输入用户名和密码STelnet登录设备。

配置STelnet是否成功的测试方法：配置完成后在系统视图下执行**ssh client first-time enable**和**stelnet 127.0.0.1**命令登录设备本身。如果出现登录界面，则代表配置成功，否则配置失败。

2 常见堆叠操作

关于本章

介绍堆叠的常见操作。

2.1 配置堆叠口

配置堆叠口就是在使用业务口组建堆叠时将业务口配置为堆叠成员口。

例如：将业务口XGE0/0/1配置为堆叠成员口。

V200R002之后的版本

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] port interface xgigabitethernet 0/0/1 enable  //将接口XGE0/0/1接口加入堆叠口，使业务口变为堆叠成员口，一次可以加入多个
Warning: Enabling stack function may cause configuration loss on the interface. Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait.......
```

V200R002及之前的版本

```
<HUAWEI> system-view
[HUAWEI] stack port interface xgigabitethernet 0/0/1 enable  //配置接口XGE0/0/1为堆叠口
Warning: This operation will clear all configurations on these interfaces, continue? [Y/
N]:y
Info: This operation may take a few seconds. Please wait for a moment...
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] port member-group interface xgigabitethernet 0/0/1  //将接口XGE0/0/1加入堆叠口
```


说明

- 交换机一共支持两个堆叠口，分别是Stack-Port*n*/1和Stack-Port*n*/2，*n*表示交换机的堆叠ID。
- 业务口配置为堆叠成员口后，仅支持堆叠相关业务功能，其他业务功能不可用。接口下与堆叠不相关的命令会被屏蔽，仅保留**description（接口视图）**等接口基本命令。

2.2 修改堆叠口

将逻辑堆叠口stack-port0/1中的成员端口XGE0/0/1修改为XGE0/0/3。

V200R002之后的版本

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] shutdown interface xgigabitethernet0/0/1  //为避免环路，先将成员口设置为down
[HUAWEI-stack-port0/1] undo port interface xgigabitethernet0/0/1 enable   //将原来成员端口XGE0/0/1退出堆叠口，恢复为业务口
[HUAWEI-stack-port0/1] port interface xgigabitethernet0/0/3 enable   //将接口XGE0/0/3设置为堆叠口
```

V200R002及之前的版本

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] undo port member-group interface xgigabitethernet 0/0/1  //将原来的堆叠口删除
[HUAWEI-stack-port0/1] quit
[HUAWEI] undo stack port interface xgigabitethernet 0/0/1 enable  //将接口恢复为业务口
[HUAWEI] stack port interface xgigabitethernet 0/0/3 enable  //将接口XGE0/0/3使能为堆叠口
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] port member-group interface xgigabitethernet 0/0/3  //将接口加入堆叠口
```

2.3 删除堆叠口

删除堆叠口就是将业务口从堆叠口中退出，恢复为正常的业务口。

例如：将堆叠成员口XGE0/0/1从堆叠口中删除。

V200R002之后的版本

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] shutdown interface xgigabitethernet0/0/1  //为避免环路，先将成员口设置为down
[HUAWEI-stack-port0/1] undo port interface xgigabitethernet0/0/1 enable   //将成员端口XGE0/0/1退出堆叠口，恢复为业务口
```

V200R002及之前的版本

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] undo port member-group interface xgigabitethernet 0/0/1  //将接口XGE0/0/1从堆叠口中退出
[HUAWEI-stack-port0/1] quit
[HUAWEI] undo stack port interface xgigabitethernet 0/0/1 enable  //将接口XGE0/0/1恢复为业务口
```

2.4 查看堆叠配置

说明

如果设备不支持堆叠功能，则下面命令将无法执行。

堆叠的配置不会记录在配置文件中，所以无法通过**display current-configuration**查看配置。

执行命令**display stack**可以查看堆叠系统的信息。

```
<HUAWEI> display stack
Stack mode: Service-port
Stack topology type: Link
Stack system MAC: 0000-1382-4569
MAC switch delay time: 10 min
Stack reserved VLAN: 4093
Slot of the active management port: 0
Slot    Role        MAC address       Priority   Device type
--------------------------------------------------------------
    0   Master      0018-82b1-6eb4   200
    1   Standby     0018-82b1-6eba   150
```

执行命令**display stack configuration**或**display stack current-configuration**可以查看堆叠的相关配置，以V200R012C00版本为例。

```
<HUAWEI> display stack configuration
*    : Invalid-
configuration

#    : Unsaved
configuration

---------------Configuration on slot 1
Begin---------------

stack
enable

stack slot 0 renumber
2

stack slot 2 priority
150

stack reserved-vlan
4093

stack timer mac-address switch-delay
10


interface stack-port
1/1

 *port interface XGigabitEthernet1/0/1 enable


interface stack-port
1/2

 #port interface XGigabitEthernet1/0/4
enable
---------------Configuration on slot 1 End-----------------
```

- 如果堆叠成员端口带有*号，表示当前配置不生效，不生效的可能原因为：
  - 当前配置为没有生效的配置。
  - 堆叠成员端口为子卡上的接口，当前子卡不在位。
- 如果堆叠成员端口带有#号，表示当前配置是专用堆叠线缆自动生成但未执行**save stack configuration**或**save**命令把配置写入Flash。

执行命令**display stack port**可以查看堆叠口的配置，以V200R012C00业务口堆叠为例。

```
<HUAWEI> display stack port
*down : administratively
down

(r)   : Runts trigger error
```



```
down

(c)   : CRC trigger error
down

(l)   : Link-flapping trigger error
down
(m)   : Media mismatch trigger error
down
Logic Port         Phy Port                    Online
Status
--------------------------------------------------------------------------------

stack-port0/1      XGigabitEthernet0/0/1       present      down
```

2.5 使能和去使能堆叠

对于**S5700EI和S5700SI**设备，可以在系统视图下执行命令**stack enable**和**undo stack enable**使能和去使能堆叠。使能和去使能堆叠都需要重启设备才生效。

```
<HUAWEI> system-view
[HUAWEI] stack enable  //使能堆叠
Warning: All the configurations related to the slot ID will be lost after the stack function is
enabled. Continue?[Y/N]: y
Info: Stack configuration has been changed, and the device needs to restart to make the
configuration effective.
<HUAWEI> system-view
[HUAWEI] undo stack enable  //去使能堆叠
Warning: All the configurations related to the slot ID will be lost after the stack function is
enabled. Continue?[Y/N]: y
Info: Stack configuration has been changed, and the device needs to restart to make the
configuration effective.
```

对于除**S5700EI和S5700SI**之外支持堆叠的设备，堆叠功能默认使能，无法通过命令去使能。

可以通过删除堆叠口或拔掉堆叠线缆的方式取消堆叠。删除堆叠口的方法如下：

V200R002之后的版本

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] shutdown interface xgigabitethernet0/0/1  //为避免环路，先将成员口设置为down
[HUAWEI-stack-port0/1] undo port interface xgigabitethernet0/0/1 enable   //将成员端口XGE0/0/1退出
堆叠口，恢复为业务口
```

V200R002及之前的版本

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] undo port member-group interface xgigabitethernet 0/0/1  //将接口XGE0/0/1从
堆叠口中退出
[HUAWEI-stack-port0/1] quit
[HUAWEI] undo stack port interface xgigabitethernet 0/0/1 enable  //将接口XGE0/0/1恢复为业务口
```

2.6 清除堆叠配置

对于V200R011C10及之后版本的设备，执行命令**reset stack configuration**可以清除堆叠相关配置。包括：交换机槽位号、堆叠优先级、堆叠保留VLAN、系统MAC切换时间、堆叠口配置、堆叠口速率配置。

```
<HUAWEI> system-view
[HUAWEI] reset stack configuration
Warning: This operation will clear all stack configurations and may lead to the loss of the slot
ID configuration and cause the device to reset immediately. Are you sure you want to continue? [Y/
N]: y
```


说明

执行该命令后会导致原有堆叠系统分裂，设备重启。

不支持该命令。

对于V200R011C10之前版本的设备及，需要根据配置分别删除，配置删除后需要重启设备才生效。

- 恢复堆叠优先级：

```
<HUAWEI> system-view
[HUAWEI] stack slot 2 priority 100  //将2槽位号的优先级恢复为缺省值100
```

- 恢复槽位号：

```
<HUAWEI> system-view
[HUAWEI] stack slot 2 renumber 0  //将设备槽位号修改为0
```

- 恢复堆叠保留VLAN：

```
<HUAWEI> system-view
[HUAWEI] stack reserved-vlan 4093  //将堆叠保留VLAN恢复到缺省值4093
```

- 恢复系统MAC切换时间：

```
<HUAWEI> system-view
[HUAWEI] undo stack timer mac-address switch-delay
```

- 删除堆叠口

V200R002之后的版本

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] shutdown interface xgigabitethernet0/0/1  //为避免环路，先将成员口设置为down
[HUAWEI-stack-port0/1] undo port interface xgigabitethernet0/0/1 enable   //将成员端口XGE0/0/1退出堆叠口，恢复为业务口
```

V200R002及之前的版本

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] undo port member-group interface xgigabitethernet 0/0/1  //将接口XGE0/0/1从堆叠口中退出
[HUAWEI-stack-port0/1] quit
[HUAWEI] undo stack port interface xgigabitethernet 0/0/1 enable  //将接口XGE0/0/1恢复为业务口
```


3 常见查看设备状态操作

关于本章

介绍查看设备状态的常见操作。

3.1 查看设备的序列号

每台设备的序列号ESN（Equipment Serial Number）是唯一的。当用户需要设备售后服务或者申请License时，都需要提供设备的序列号。

执行命令**display esn**查看设备的序列号。下面显示以框式为例，盒式显示请以设备为准。

```
<HUAWEI> display esn
ESN of master:77000601xxxxxxxx
ESN of slave:77000601xxxxxxxx
```

说明

- 框式所有款型都支持此命令。
- 盒式S2750EI、S5700LI、S5700S-LI和S5720EI不支持此命令。

3.2 查看设备的补丁信息

执行命令**display patch-information**查看当前设备的补丁信息。下面显示以框式为例，盒式显示请以设备为准。

```
<HUAWEI> display patch-information
Patch Package Name   :cfcard:/patch.pat
Patch Package Version:V200R008C00SPH001
The state of the patch state file is: Running
The current state is: Running
```



```
*************************************************************************
*           Information about hot patch errors is as follows:           *
*************************************************************************

     Slot            CurrentVersion
-------------------------------------------------------

No hot patch error occurs on any board.


*************************************************************************
*                The hot patch information, as follows:                 *
*************************************************************************

 Slot       Type           State     Count Time(YYYY-MM-DD HH:MM:SS)
-------------------------------------------------------------------------
 14         C              Running   1     2012-08-15 09:20:48+00:00
```

3.3 查看设备的版本信息和运行时间

执行命令**display version**查看当前设备的版本信息和运行时间。下面显示以框式为例，盒式显示请以设备为准。

```
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.160 (S7700 V200R007C00)
Copyright (C) 2000-2013 HUAWEI TECH CO., LTD
Quidway S7703 Terabit Routing Switch uptime is 0 week, 0 day, 1 hour, 3 minutes
BKP 0 version information:
1. PCB      Version  : LE02BAKB VER.A
2. Supporting PoE    : No
3. Board    Type     : ES0B017712P0
4. MPU Slot Quantity : 2
5. LPU Slot Quantity : 3

MPU 5(Master) : uptime is 0 week, 0 day, 1 hour, 1 minute
SDRAM Memory Size    : 512     M bytes
Flash Memory Size    : 128     M bytes
NVRAM Memory Size    : 512     K bytes
CF Card1 Memory Size : 977     M bytes
MPU version information :
1. PCB      Version  : LE02SRUA VER.D
2. MAB      Version  : 0
3. Board    Type     : ES0D00SRUA00
4. CPLD0    Version  : 1301.1014
5. BootROM  Version  : 0207.00ab
6. BootLoad Version  : 0207.0097

LPU 1 : uptime is 0 week, 0 day, 0 hour, 54 minutes
SDRAM Memory Size    : 256     M bytes
Flash Memory Size    : 8       M bytes
LPU version information :
1. PCB      Version  : LE02X4UX VER.B
2. MAB      Version  : 0
3. Board    Type     : ES0D0X2UXC00
4. CPLD0    Version  : 1310.1716
5. BootROM  Version  : 0207.00ab
6. BootLoad Version  : 0207.00bf

LPU 2 : uptime is 0 week, 0 day, 0 hour, 54 minutes
SDRAM Memory Size    : 128     M bytes
Flash Memory Size    : 8       M bytes
LPU version information :
1. PCB      Version  : LE02G48V VER.B
2. MAB      Version  : 0
3. Board    Type     : ES0D0G48TA00
```



```
4. CPLD0    Version  : 1102.1516
5. BootROM  Version  : 0207.00ab
6. BootLoad Version  : 0207.00bf

LPU 3 : uptime is 0 week, 0 day, 0 hour, 49 minutes
SDRAM Memory Size    : 256     M bytes
Flash Memory Size    : 8       M bytes
LPU version information :
1. PCB      Version  : LE02X4UX VER.B
2. MAB      Version  : 0
3. Board    Type     : ES0D0X4UXC00
4. CPLD0    Version  : 1310.1716
5. BootROM  Version  : 0207.00ab
6. BootLoad Version  : 0207.00bf
TCAM version information :
1. TCAM size         : 36      M bits
```

3.4 查看设备的机框类型

可以用户视图下使用**display version**查看当前设备的机框类型。

以下以S7700举例说明。**S7706**即为当前设备的机框类型。

```
[HUAWEI] display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.160 (S7700 V200R007C00)
Copyright (C) 2000-2014 HUAWEI TECH CO., LTD
Quidway S7706 Terabit Routing Switch uptime is 0 week, 0 day, 19 hours, 40 minutes
BKP 0 version information:
1. PCB      Version  : LE02BAKI VER.A
2. Support  PoE      : No
3. Board    Type     : ES0B00770600
4. MPU Slot Quantity : 2
5. LPU Slot Quantity : 6

MPU 7(Master) : uptime is 0 week, 0 day, 19 hours, 39 minutes
SDRAM Memory Size    : 1024    M bytes
Flash Memory Size    : 64      M bytes
NVRAM Memory Size    : 512     K bytes
CF Card1 Memory Size : 497     M bytes
MPU version information :
1. PCB      Version  : LE02SRUB VER.B
2. MAB      Version  : 3
3. Board    Type     : ES0D00SRUB00
4. CPLD0    Version  : 1411.2117
5. BootROM  Version  : 0207.00d3
6. BootLoad Version  : 0207.00d3

LPU 6 : uptime is 0 week, 0 day, 19 hours, 39 minutes
SDRAM Memory Size    : 256     M bytes
Flash Memory Size    : 16      M bytes
LPU version information :
1. PCB      Version  : LE02G48CE VER.A
2. MAB      Version  : 0
3. Board    Type     : ES0DG48CEA00
4. CPLD0    Version  : 1102.1515
5. BootROM  Version  : 0207.00d3
6. BootLoad Version  : 0207.00fb
```


4 常见硬件管理操作

关于本章

介绍硬件管理的常见操作。

4.1 主备倒换

对于盒式设备，在多台设备堆叠的情况下，当用户进行软件升级或者系统维护时，可以手动进行主交换机和备交换机的倒换。执行主备倒换后，主交换机将重新启动后加入堆叠系统；备交换机升级为主交换机。

对于框式设备，在软件升级或者系统维护时，用户可以手动进行主用主控板和备用主控板的倒换。执行主备倒换后，设备正在运行的主用主控板将重新启动；设备正在运行的备用主控板将成为主用主控板。

对系统进行主备倒换。

```
<HUAWEI> system-view
[HUAWEI] slave switchover enable
[HUAWEI] slave switchover
Warning: This operation will switch the slave board to the master board. Continue? [Y/N]:y
```

4.2 修改温度告警阈值

环境温度和设备运行时间会影响设备的温度。环境温度越高，设备运行时间越长，设备的温度就会越高。当设备温度超出一定范围时，会对设备的寿命以及性能产生影响。配置设备温度告警阈值，当设备温度超过设置范围时，产生告警，上报网管，提醒管理员采取降温措施。

说明

仅盒式交换机支持，框式交换机不支持。

将Slot ID为0的设备的温度告警阈值设置为下限20°C，上限45°C。

```
<HUAWEI> system-view
[HUAWEI] temperature threshold slot 0 lower-limit 20 upper-limit 45
```

4.3 修改风扇调速温度阈值

缺省情况下，风扇转速有固定的加速和降速温度阈值。只有当高于或低于缺省的温度阈值，风扇转速才会加快或降低。但如果需要设备温度较低，则可以使用此命令来调节风扇的转速的温度阈值，调速后的温度阈值低于缺省温度阈值，这样风扇将在低于缺省的加速温度阈值时就加快风扇转速以及在低于缺省的降速温度阈值时才会降低风扇转速。

缺省的风扇调速温度阈值和配置后的调速温度阈值可通过**display fan speed-adjust threshold minus**命令查看。

将调整风扇转速的温度阈值降低10°C。

```
<HUAWEI> system-view
[HUAWEI] set fan speed-adjust threshold minus 10
Info: Succeeded in setting the fan speed-adjust threshold.
```

说明

- 执行此命令，调速后的风扇温度阈值为缺省温度阈值减去*threshold-value*的值，且风扇的加速和降速温度阈值都同时降低。
- 对于准自然散热方式的风扇，执行此命令后将降低风扇起转和停转的温度阈值。准自然散热方式的风扇只有起转和停转两种方式，风扇转速固定，无加速或降速的状态。
- 例如，对于使用准自然散热方式的风扇的设备执行命令**display fan speed-adjust threshold minus**，查看到风扇转速当前阈值为40–50，其中40℃是停转温度，50℃是起转温度。当前设备温度是45℃时，需要根据风扇温度变化过程来判断当前风扇是否运转。
  - 当设备温度是从较低温度（例如30℃）上升到45℃时，由于还没有到达起转温度50℃，所以此时设备处于45℃，但是风扇不转。
  - 当设备温度是从较高温度（例如65℃）下降到45℃时，由于设备温度较高，风扇始终在运转，温度降至45℃，还是没有降至停转温度40℃，所以此时设备处于45℃，但是风扇仍然在转。

5 常见镜像操作

关于本章

介绍镜像的常见操作。

5.1 配置观察端口

配置任何一种镜像功能，都需要先将物理端口配置成观察端口。配置观察端口分单个配置和批量配置两种方式。批量配置的观察端口相当于加入了一个观察端口组，在配置镜像端口时，镜像端口会绑定整个观察端口组。因此批量配置一般在1：N镜像时使用，主要是为了配置方便。

配置单个观察端口

- 本地观察端口，即观察端口与监控设备直连

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 1/0/1
```

- 二层远程观察端口，即观察端口通过二层网络向监控设备转发镜像报文

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 1/0/1 vlan 10
```

配置批量观察端口（V200R005 及后续版本支持）

- 本地观察端口，即观察端口与监控设备直连

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface-range gigabitethernet 1/0/1 to gigabitEthernet 1/0/3
```

- 二层远程观察端口，即观察端口通过二层网络向监控设备转发镜像报文

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface-range gigabitethernet 1/0/1 to gigabitEthernet 1/0/3 vlan
10
```


5.2 配置端口镜像

端口镜像是指设备复制从镜像端口流经的报文，并将此报文传送到指定的观察端口进行分析和监控。根据观察端口的不同，端口镜像分为本地端口镜像和二层远程端口镜像。如何配置本地观察端口和二层远程观察端口，请参见**5.1 配置观察端口**，此处以配置本地端口镜像为例。详细的配置举例请参见《典型配置案例》 网络管理与监控典型配置 中的“镜像典型配置”。

配置 1：1 端口镜像

将一个镜像端口的报文复制到一个观察端口上。例如：将镜像端口GE2/0/1入方向的报文（即接收到的报文）复制到观察端口GE1/0/1上，GE1/0/1与监控设备直连。

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 1/0/1
[HUAWEI] interface gigabitethernet 2/0/1
[HUAWEI-GigabitEthernet2/0/1] port-mirroring to observe-port 1 inbound
```

配置 1：N 端口镜像

将一个镜像端口的报文复制到N个不同的观察端口上。例如：将镜像端口GE2/0/1入方向的报文（即接收到的报文）复制到观察端口GE1/0/1～GE1/0/3上，GE1/0/1～GE1/0/3与监控设备直连。

- 观察端口逐个进行配置

  ```
  <HUAWEI> system-view
  [HUAWEI] observe-port 1 interface gigabitethernet 1/0/1
  [HUAWEI] observe-port 2 interface gigabitethernet 1/0/2
  [HUAWEI] observe-port 3 interface gigabitethernet 1/0/3
  [HUAWEI] interface gigabitethernet 2/0/1
  [HUAWEI-GigabitEthernet2/0/1] port-mirroring to observe-port 1 inbound
  [HUAWEI-GigabitEthernet2/0/1] port-mirroring to observe-port 2 inbound
  [HUAWEI-GigabitEthernet2/0/1] port-mirroring to observe-port 3 inbound
  ```

- 观察端口批量进行配置（V200R005及后续版本支持）

  ```
  <HUAWEI> system-view
  [HUAWEI] observe-port 1 interface-range gigabitethernet 1/0/1 to gigabitEthernet 1/0/3
  [HUAWEI] interface gigabitethernet 2/0/1
  [HUAWEI-GigabitEthernet2/0/1] port-mirroring to observe-port 1 inbound
  ```

配置 N：1 端口镜像

将N个镜像端口的报文复制到一个观察端口上。例如：将镜像端口GE2/0/1～GE2/0/3入方向的报文（即接收到的报文）复制到观察端口GE1/0/1上，GE1/0/1与监控设备直连。

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 1/0/1
[HUAWEI] interface gigabitethernet 2/0/1
[HUAWEI-GigabitEthernet2/0/1] port-mirroring to observe-port 1 inbound
[HUAWEI-GigabitEthernet2/0/1] quit
[HUAWEI] interface gigabitethernet 2/0/2
[HUAWEI-GigabitEthernet2/0/2] port-mirroring to observe-port 1 inbound
[HUAWEI-GigabitEthernet2/0/2] quit
[HUAWEI] interface gigabitethernet 2/0/3
[HUAWEI-GigabitEthernet2/0/3] port-mirroring to observe-port 1 inbound
[HUAWEI-GigabitEthernet2/0/3] quit
```


相关信息

技术论坛

镜像原理配置篇

视频

如何配置端口镜像

5.3 配置流镜像

流镜像是指将设备、端口或者VLAN内收、发的指定类型报文复制到观察端口上，监控设备只对指定类型报文进行监测。流镜像有基于ACL和基于MQC（即复杂流分类）两种配置方式。前者配置简便，但是没有后者支持匹配的报文类型多，而且只支持入方向（即接收报文方向）的流镜像；后者配置复杂，但是支持匹配的报文类型比前者多，而且入方向、出方向（即发送报文方向）的流镜像都支持。

根据观察端口的不同，流镜像分为本地流镜像和二层远程流镜像。如何配置本地观察端口和二层远程观察端口，请参见**5.1 配置观察端口**，此处以配置本地流镜像为例。详细的配置举例请参见《典型配置案例》 网络管理与监控典型配置 中的“镜像典型配置”。

配置基于 ACL 的流镜像

1. **5.1 配置观察端口**。例如：配置与监控设备直连的本地观察端口GE1/0/1。

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 1/0/1
```

2. 创建ACL。例如：创建二层ACL，配置的规则是匹配802.1p优先级为6的报文。

```
[HUAWEI] acl 4001
[HUAWEI-acl-L2-4001] rule permit 8021p 6
[HUAWEI-acl-L2-4001] quit
```

3. 配置流镜像。例如：
   - 将整个设备所有端口入方向（即接收报文方向）802.1p优先级为6的报文复制到观察端口GE1/0/1。

     ```
     [HUAWEI] traffic-mirror inbound acl 4001 to observe-port 1
     ```

   - 将VLAN 10下所有端口入方向802.1p优先级为6的报文复制到观察端口GE1/0/1。

     ```
     [HUAWEI] traffic-mirror vlan 10 inbound acl 4001 to observe-port 1
     ```

   - 将端口GE2/0/1入方向802.1p优先级为6的报文复制到观察端口GE1/0/1。

     ```
     [HUAWEI] interface gigabitethernet 2/0/1
     [HUAWEI-GigabitEthernet2/0/1] traffic-mirror inbound acl 4001 to observe-port 1
     ```

配置基于 MQC 的流镜像

1. **5.1 配置观察端口**。例如：配置与监控设备直连的本地观察端口GE1/0/1。

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 1/0/1
```

2. 创建流分类。例如：创建流分类c1，并配置流分类规则是匹配802.1p优先级为6的报文。

```
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match 8021p 6
[HUAWEI-classifier-c1] quit
```


3. 创建动作是镜像的流行为。例如：创建流行为b1，并配置动作为流镜像。

```
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] mirroring to observe-port 1
[HUAWEI-behavior-b1] quit
```

4. 创建流策略，并将流分类和流行为绑定到流策略上。例如：创建流策略p1，并将上面配置的流分类和流行为绑定到流策略p1上。

```
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
```

5. 应用流策略。例如：
   - 将整个设备所有端口入方向（即接收报文方向）802.1p优先级为6的报文复制到观察端口GE1/0/1。

     ```
     [HUAWEI] traffic-policy p1 global inbound
     ```

   - 将VLAN 10下所有端口入方向802.1p优先级为6的报文复制到观察端口GE1/0/1。

     ```
     [HUAWEI] vlan 10
     [HUAWEI-vlan10] traffic-policy p1 inbound
     ```

   - 将端口GE2/0/1入方向802.1p优先级为6的报文复制到观察端口GE2/0/1。

     ```
     [HUAWEI] interface gigabitethernet 2/0/1
     [HUAWEI-GigabitEthernet2/0/1] traffic-policy p1 inbound
     ```

5.4 删除镜像配置

在使用完镜像功能后，如果希望将设备上的镜像配置删除，可按如下思路进行操作。

1. 执行命令**display current-configuration**，查看设备当前镜像的配置。例如：在设备上查看到的当前配置如下。

```
<HUAWEI> display current-configuration
#
vlan batch 10 20 30
#
observe-port 2 interface GigabitEthernet1/0/1
             ...
             ...
#
interface GigabitEthernet1/0/1
#
interface GigabitEthernet1/0/2
             ...
             ...
#
interface GigabitEthernet2/0/1
  port-mirroring to observe-port 2 inbound
#
             ...
             ...
```

2. 在镜像端口下执行命令**undo port-mirroring**，删除观察端口与镜像端口的绑定关系，恢复镜像端口为普通端口。例如：将第1步示例中的GE2/0/1恢复为普通端口。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 2/0/1
[HUAWEI-GigabitEthernet2/0/1] undo port-mirroring to observe-port 2 inbound
[HUAWEI-GigabitEthernet2/0/1] quit
```

3. 在系统视图下执行命令**undo observe-port**，删除观察端口。例如：将第1步示例中的观察端口删除，将GE1/0/1恢复为普通端口。

```
[HUAWEI] undo observe-port 2
```


只有先执行第2步，即先删除观察端口与镜像端口的绑定关系，才能删除观察端口。

6 常见 MAC 操作

关于本章

介绍MAC地址的常见操作。

6.1 查看所有 MAC 地址

执行命令**display mac-address**，查看所有的MAC地址表项。

```
<HUAWEI> display mac-address
------------------------------------------------------------------------------
MAC Address    VLAN/VSI                                Learned-From        Type
------------------------------------------------------------------------------
0000-0000-0002 10/-                                    -                   blackhole
0000-0000-0003 300/-                                   GE1/0/3             static
0026-6e5c-feac 3000/-                                  Eth-Trunk2          dynamic
0000-c116-0201 -/test                                  Eth-Trunk3          dynamic

------------------------------------------------------------------------------
Total items displayed = 4
```

相关信息

视频

如何查询MAC和ARP表项

6.2 查看某个接口学习到的 MAC 地址

执行命令**display mac-address dynamic gigabitethernet1/0/1**，查看接口GE1/0/1学习到的MAC地址表项。

```
<HUAWEI> display mac-address dynamic gigabitethernet1/0/1
--------------------------------------------------------------------------------
MAC Address    VLAN/VSI                                Learned-From        Type
--------------------------------------------------------------------------------
0000-0000-0003 300/-                                   GE1/0/1             dynamic
0026-6e5c-feac 3000/-                                  GE1/0/1             dynamic

--------------------------------------------------------------------------------
Total items displayed = 2
```

6.3 查看某个 VLAN 学习到的 MAC 地址

执行命令**display mac-address dynamic vlan 10**，查看VLAN 10学习到的MAC地址表项。

```
<HUAWEI> display mac-address dynamic vlan 10
--------------------------------------------------------------------------------
MAC Address    VLAN/VSI                                Learned-From        Type
--------------------------------------------------------------------------------
0000-0000-0003 10/-                                    GE1/0/1             dynamic
0026-6e5c-feac 10/-                                    GE1/0/2             dynamic

--------------------------------------------------------------------------------
Total items displayed = 2
```

6.4 查看系统的 MAC 地址

可以通过下面两种方式，查看设备的MAC地址。

- 二层接口的MAC地址就是设备的MAC地址，执行命令**display interface gigabitethernet1/0/1**，显示信息中的**00e0-f74b-6d00**，即为设备的MAC地址。

  ```
  <HUAWEI> display interface gigabitethernet1/0/1
  GigabitEthernet1/0/1  current state : UP
  Line protocol current state : UP
  Description:
  Switch Port, Link-type : access(configured),
  PVID :  103, TPID : 8100(Hex), The Maximum Frame Length is 9216
  IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-f74b-6d00
  ......
  ```

- 在V200R002版本及之后版本，执行命令**display bridge mac-address**，查看设备的MAC地址。

  ```
  <HUAWEI> display bridge mac-address
  System bridge MAC address: 00e0-f74b-6d00
  ```


6.5 查看接口的 MAC 地址

执行命令**display interface gigabitethernet1/0/1**，显示信息中的**00e0-f74b-6d00**，即为接口的MAC地址。

```
<HUAWEI> display interface gigabitethernet1/0/1
GigabitEthernet1/0/1  current state : UP
Line protocol current state : UP
Description:
Switch Port, Link-type : access(configured),
PVID :  103, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-f74b-6d00
......
```

6.6 查看 VLANIF 接口的 MAC 地址

执行命令**display interface vlanif10**，显示信息中的**00e0-0987-7891**，即为VLANIF接口的MAC地址。

```
<HUAWEI> display interface vlanif10
Vlanif10 current state : DOWN
Line protocol current state : DOWN
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 172.10.1.2/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-0987-7891
Current system time: 2014-08-14 16:40:09+08:00
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

6.7 根据 IP 获取对应设备的 MAC 地址

执行命令**display arp | include** *ip-address*，即可获取指定IP对应设备的MAC地址。

例如：根据IP地址192.168.150.20获取对应设备的MAC地址。

```
<HUAWEI> display arp | include 192.168.150.20
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-
INSTANCE
                                          VLAN/
CEVLAN
--------------------------------------------------------------------------------

192.168.150.20  000b-0935-766f  10        D-1
GE1/0/24
--------------------------------------------------------------------------------

Total:27        Dynamic:26      Static:0     Interface:1
```

说明

- 如果显示的表项为空，则说明无法根据IP获取对应设备的MAC地址。
- include后的参数指定为MAC时，可以根据MAC获取对应的IP地址。
- 回显内容，请以设备显示为准。

6.8 配置静态 MAC 地址

将与设备相连的固定上行设备或信任用户的MAC地址配置为静态MAC表项，可以保证其安全通信。

```
<HUAWEI> system-view
[HUAWEI] vlan 10  //创建VLAN 10
[HUAWEI-vlan10] quit
[HUAWEI] interface GigabitEthernet1/0/1
[HUAWEI-GigabitEthernet1/0/1] port link-type access
[HUAWEI-GigabitEthernet1/0/1] port default vlan 10  //接口加入vlan10
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] mac-address static 0000-0012-0034 GigabitEthernet1/0/1 vlan 10  //配置静态MAC地址，把mac地址0000-0012-0034和接口GigabitEthernet1/0/1静态绑定
```

说明

MAC地址绑定的接口必须属于vlan参数指定的VLAN，而且该VLAN必须事先已创建。

6.9 配置黑洞 MAC 地址

为了防止黑客通过MAC地址攻击用户设备或网络，可将非信任用户的MAC地址配置为黑洞MAC地址。当设备收到目的MAC或源MAC地址为黑洞MAC地址的报文，直接丢弃。

交换机提供两种配置黑洞MAC地址的方式：全局黑洞MAC地址和基于VLAN的黑洞MAC地址。

- 在系统视图下，配置MAC地址0000-0012-0034为全局黑洞MAC。
  ```
  <HUAWEI> system-view
  [HUAWEI] mac-address blackhole 0000-0012-0034
  ```
- 在系统视图下，配置MAC地址0000-0012-0035在VLAN10的广播域内为黑洞MAC地址。
  ```
  <HUAWEI> system-view
  [HUAWEI] mac-address blackhole 0000-0012-0035 vlan 10
  ```

6.10 查看和配置 MAC 地址的老化时间

在系统视图下，执行命令**mac-address aging-time 600**，配置动态MAC地址的老化时间为600秒，缺省老化时间是300秒。

```
<HUAWEI> system-view
[HUAWEI] mac-address aging-time 600
```

在任意视图下，执行命令**display mac-address aging-time**，查看当前动态MAC地址老化的时间。

```
<HUAWEI> display mac-address aging-time
  Aging time: 300 second(s)
```

6.11 配置 MAC 刷新 ARP 功能

在以太网中，MAC地址表项用于指导设备进行二层数据转发，ARP表项通过IP地址和MAC地址的映射指导设备进行不同网段间的通信。

MAC地址表项的出接口通过报文触发刷新的，ARP表项的出接口是在老化时间到后通过老化探测进行刷新的。这样就可能会出现MAC表项和ARP表项出接口不一致的情

况，即MAC地址表项的出接口已刷新，而ARP表项的出接口没有及时刷新的情况。此时可以使能MAC刷新ARP的功能，在MAC地址表项出接口刷新时，直接刷新ARP表项的出接口。

配置MAC刷新ARP功能。

```
<HUAWEI> system-view
[HUAWEI] mac-address update arp
```

6.12 配置端口安全

配置端口安全功能，可以实现用户的动态绑定。通过配置接口MAC地址学习限制数的功能可以阻止其他非信任的MAC主机通过本接口和交换机通信，提高设备与网络的安全性。

配置GE1/0/1接口的端口安全功能。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] port-security enable
```

配置GE1/0/1接口的MAC地址学习限制数为5，即最多可以学习到5个MAC地址表项。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] port-security enable
[HUAWEI-GigabitEthernet1/0/1] port-security max-mac-num 5
```

说明

在配置接口的MAC地址学习限制数之前，接口必须已经使能端口安全功能。

7 常见以太网接口操作

关于本章

介绍以太网接口的常见操作，如端口组等。

7.1 配置端口组

配置临时端口组

配置接口GE1/0/9至GE1/0/15加入到临时端口组（使用**port-group group-member**命令）。

```
<HUAWEI> system-view
[HUAWEI] port-group group-member gigabitethernet 1/0/9 to gigabitethernet 1/0/15
[HUAWEI-port-group]
```

配置接口GE1/0/16至GE1/0/20加入到临时端口组（使用**interface range**命令，此命令仅V200R003C00及后续版本支持）。

```
<HUAWEI> system-view
[HUAWEI] interface range gigabitethernet 1/0/16 to gigabitethernet 1/0/20
[HUAWEI-port-group]
```

配置永久端口组

配置接口GE1/0/1至GE1/0/8加入到永久端口组portgroup1（使用**port-group**命令）。

```
<HUAWEI> system-view
[HUAWEI] port-group portgroup1
[HUAWEI-port-group-portgroup1] group-member gigabitethernet 1/0/1 to gigabitethernet 1/0/8
```


相关信息

技术论坛

接口配置锦囊妙计—批量配置

视频

如何批量配置交换机端口

7.2 配置端口隔离

配置端口隔离组

配置接口GE1/0/1和GE1/0/2的端口隔离功能，实现两个接口之间的二层数据隔离，三层数据互通。

```
<HUAWEI> system-view
[HUAWEI] port-isolate mode l2
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] port-isolate enable group 1
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] interface gigabitethernet 1/0/2
[HUAWEI-GigabitEthernet1/0/2] port-isolate enable group 1
[HUAWEI-GigabitEthernet1/0/2] quit
```

配置接口GE1/0/10至GE1/0/20的端口隔离功能，实现多个接口之间的二三层数据均隔离。

```
<HUAWEI> system-view
[HUAWEI] port-isolate mode all
[HUAWEI] port-group portgroup1
[HUAWEI-port-group-portgroup1] group-member gigabitethernet 1/0/10 to gigabitethernet 1/0/20
[HUAWEI-port-group-portgroup1] port-isolate enable group 2
```

说明

S系列框式交换机均支持二层三层都隔离模式，S系列盒式交换机V100R006C05版本仅S2700SI、S2700EI不支持二层三层都隔离模式，V200R001及后续版本S1720GFR、S1720GW-E、S1720GWR-E、S1720X-E、S2720EI、S2750EI、S5710-C-LI、S5710-X-LI、S5700S-LI、S5700LI、S5720S-LI、S5720LI、S6720LI、S6720S-LI不支持二层三层都隔离模式。

配置单向隔离

配置接口GE1/0/5与GE1/0/6、GE1/0/7、GE1/0/8的单向隔离功能，实现GE1/0/5接口发送的二层数据报文无法到达接口GE1/0/6、GE1/0/7、GE1/0/8。

```
<HUAWEI> system-view
[HUAWEI] port-isolate mode l2
[HUAWEI] interface gigabitethernet 1/0/5
[HUAWEI-GigabitEthernet1/0/5] am isolate gigabitethernet 1/0/6 to 1/0/8
```

相关信息

技术论坛

接口配置锦囊妙计—端口隔离

视频

如何配置端口隔离

7.3 配置 Combo 接口工作模式

Combo接口视图下执行命令**combo-port** { **auto** | **copper** | **fiber** }，配置Combo接口工作模式。

配置接口GE1/0/1工作模式为电口模式。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] combo-port copper
```

- 指定Combo接口工作模式为**auto**，即自动选择模式时，系统将检测Combo光口是否有光模块插入，并根据如下情况进行模式选择：
  - Combo电口没有连接网线，当Combo光口插上光模块时，则Combo接口选择光口模式。
  - Combo电口已经连接网线，且Combo接口处于Up状态，此时即使Combo光口插上光模块，Combo接口仍选择为电口模式。但是设备重启后，Combo接口工作模式将变为光口模式。
  - Combo电口已经连接网线，且Combo接口处于Down状态，此时Combo光口插上光模块时，Combo接口将选择光口模式。

  综上所述，Combo接口工作模式为自动选择模式时，只要Combo光口已插上光模块，则设备重启后，Combo接口都将选择光口模式。
- 强制指定Combo接口的工作模式时，需要根据本端与对端设备连接的接口类型进行配置。如果本端Combo电口与对端电口相连，则需要强制指定Combo接口的工作模式为**copper**；如果本端Combo光口与对端光口相连，则需要强制指定Combo接口的工作模式为**fiber**。

7.4 配置接口速率

自协商模式下，手动配置接口速率

配置以太网接口GE1/0/1在自协商模式下协商速率为100Mbit/s。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] negotiation auto
[HUAWEI-GigabitEthernet1/0/1] auto speed 100
```

说明

GE光接口不支持在自协商模式下手动配置接口速率，插入GE光电模块的GE光接口除外。

非自协商模式下，配置接口速率

配置以太网接口GE1/0/1在非自协商模式下协商速率为100Mbit/s。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] undo negotiation auto
[HUAWEI-GigabitEthernet1/0/1] speed 100
```

相关信息

技术论坛

接口配置锦囊妙计—端口自协商

7.5 配置双工模式

自协商模式下，手动配置双工模式

配置以太网电接口GE1/0/1在自协商模式下双工模式为全双工模式。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] negotiation auto
[HUAWEI-GigabitEthernet1/0/1] auto duplex full
```

非自协商模式下，配置双工模式

配置以太网电接口GE1/0/1在非自协商模式下的双工模式为半双工模式。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] undo negotiation auto
[HUAWEI-GigabitEthernet1/0/1] duplex half
```

说明

- 盒式设备S6720EI、S6720HI和S6720S-EI的物理接口均不支持半双工模式。
- 框式设备的X系列单板的物理接口不支持半双工模式。其他单板上仅GE电口和FE电口支持半双工模式。
- GE电接口工作速率为1000Mbit/s时，不支持半双工模式。

相关信息

技术论坛

接口配置锦囊妙计—端口自协商

7.6 配置接口切换到三层模式

接口视图下执行命令**undo portswitch**，配置接口切换到三层模式。

将接口GE1/0/1切换为三层模式。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] undo portswitch
[HUAWEI-GigabitEthernet1/0/1] ip address 10.10.10.10 255.255.255.0
```

缺省情况下，以太网接口处于二层模式。

使用该命令进行接口的二三层模式切换时，接口下只能存在属性配置信息（例如**shutdown**、**description**配置），模式切换功能才可以生效。如果已经有业务配置存在时（例如**port link-type trunk**配置），需要先将该接口下的业务配置全部清除再执行该命令。

支持二层模式与三层模式切换的款型及版本如下：

- S5700EI：V200R005C00&C01
- S5700HI：V100R005C01、V100R006C01、V200R001C00、V200R002C00、V200R003C00、V200R005C00&C01
- S5710EI：V200R002C00、V200R003C00、V200R005C00

- S5720EI：V200R007C00、V200R008C00、V200R009C00、V200R010C00、V200R011C00、V200R011C10、V200R012C00
- S5710HI：V200R003C00、V200R005C00
- S5720HI：V200R006C00、V200R007C00、V200R008C00、V200R009C00、V200R010C00、V200R011C00、V200R011C10、V200R012C00
- S5730HI：V200R012C00
- S6700EI：V200R005C00&C01
- S6720EI：V200R008C00、V200R009C00、V200R010C00、V200R011C00、V200R011C10、V200R012C00
- S6720HI：V200R012C00
- S6720S-EI：V200R008C00、V200R009C00、V200R010C00、V200R011C00、V200R011C10、V200R012C00
- S7700&S9700：V200R001C00&C01、V200R002C00、V200R003C00、V200R005C00、V200R006C00、V200R007C00、V200R008C00、V200R009C00、V200R010C00、V200R011C10、V200R012C00
- S7900：V200R011C10、V200R012C00、V200R012C10

对于V200R005C00及后续版本，在接口使用命令**undo portswitch**，将以太网接口从二层模式切换到三层模式后，支持配置IP地址。

7.7 一键清除接口下的配置

在系统视图下执行命令**clear configuration interface**清除GE1/0/1接口下的配置。

```
<HUAWEI> system-view
[HUAWEI] clear configuration interface gigabitethernet 1/0/1
Warning: All configurations of the interface will be cleared, and its state will be shutdown.
Continue? [Y/N] :y
Info: Total 5 command(s) executed, 5 successful, 0 failed.
```

在接口视图下执行命令**clear configuration this**清除GE1/0/1接口下的配置。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] clear configuration this
Warning: All configurations of the interface will be cleared, and its state will be shutdown.
Continue? [Y/N] :y
Info: Total 3 command(s) executed, 3 successful, 0 failed.
```

说明

执行命令一键式清除接口下配置后，接口的状态将被置为shutdown状态。

8 常见链路聚合操作

关于本章

介绍以太链路聚合功能的常见操作。

8.1 将成员接口批量加入聚合组

在Eth-Trunk1中批量加入五个成员接口GigabitEthernet1/0/1到GigabitEthernet1/0/5。

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] trunkport gigabitethernet 1/0/1 to 1/0/5
```

8.2 将指定成员接口从聚合组中删除

删除成员接口有如下两种方式，请根据需要选择其一即可。

- 在Eth-Trunk接口视图下执行命令**undo trunkport** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-8>。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface eth-trunk 1
  [HUAWEI-Eth-Trunk1] undo trunkport gigabitethernet 1/0/1
  ```

- 在成员接口视图下执行命令**undo eth-trunk**。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] undo eth-trunk
  ```

8.3 删除聚合组

前提条件

将所有的成员接口从聚合组中删除，具体请参见**8.2 将指定成员接口从聚合组中删除**。

操作步骤

在系统视图下执行命令**undo interface eth-trunk** *trunk-id*。

```
<HUAWEI> system-view
[HUAWEI] undo interface eth-trunk 10
```

8.4 查看 Eth-Trunk 接口的配置信息

查看所有Eth-Trunk接口配置信息。

```
<HUAWEI> display eth-trunk
Eth-Trunk10's state information is:
Local:
LAG ID: 10                  WorkingMode: LACP
Preempt Delay Time: 10      Hash arithmetic: According to SIP-XOR-DIP
System Priority: 120        System ID: 0018-82d4-04c3
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName                   Status   PortType     PortPri PortNo PortKey PortState Weight
GigabitEthernet1/0/2            Selected 1GE          10      262    2609    10111100  1
GigabitEthernet1/0/3            Selected 1GE          10      263    2609    10111100  1
GigabitEthernet1/0/4            Unselect 1GE          32768   264    2609    10100000  1

Partner:
--------------------------------------------------------------------------------
ActorPortName                   SysPri  SystemID    PortPri PortNo  PortKey   PortState
GigabitEthernet1/0/2            32768   00e0-fc6e-bb11  32768  262   2609      10111100
GigabitEthernet1/0/3            32768   00e0-fc6e-bb11  32768  263   2609      10111100
GigabitEthernet1/0/4            32768   00e0-fc6e-bb11  32768  264   2609      10110000

Eth-Trunk11's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
PortName                                Status      Weight
GigabitEthernet1/0/1                    Up          1
```

查看ID为10的Eth-Trunk接口（LACP模式）的配置信息。

```
<HUAWEI> display eth-trunk 10
Eth-Trunk10's state information is:
Local:
LAG ID: 10                  WorkingMode: LACP
Preempt Delay Time: 10      Hash arithmetic: According to SIP-XOR-DIP
System Priority: 120        System ID: 0018-82d4-04c3
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName                   Status   PortType     PortPri PortNo PortKey PortState Weight
GigabitEthernet1/0/2            Selected 1GE          10      262    2609    10111100  1
GigabitEthernet1/0/3            Selected 1GE          10      263    2609    10111100  1
GigabitEthernet1/0/4            Unselect 1GE          32768   264    2609    10100000  1
```



```
Partner:
--------------------------------------------------------------------------------
ActorPortName                SysPri    SystemID  PortPri PortNo  PortKey   PortState
GigabitEthernet1/0/2         32768  00e0-fc6e-bb11  32768  262   2609      10111100
GigabitEthernet1/0/3         32768  00e0-fc6e-bb11  32768  263   2609      10111100
GigabitEthernet1/0/4         32768  00e0-fc6e-bb11  32768  264   2609      10110000
```

查看ID为11的Eth-Trunk接口（手工负载分担模式）的配置信息。

```
<HUAWEI> display eth-trunk 11
Eth-Trunk11's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
PortName                                  Status      Weight
GigabitEthernet1/0/1                      Up          1
```

8.5 查看 Eth-Trunk 的成员接口信息

查看ID为2的Eth-Trunk的成员接口信息。

```
<HUAWEI> display trunkmembership eth-trunk 2
Trunk ID: 2
Used status: VALID
TYPE: ethernet
Working Mode : Normal
Number Of Ports in Trunk = 2
Number Of Up Ports in Trunk = 2
Operate status: up
Interface GigabitEthernet1/0/1, valid, operate up, weight=1
Interface GigabitEthernet1/0/2, valid, operate up, weight=1
```

8.6 查看设备支持的链路聚合组数目和成员接口数目

说明

V200R005及以后版本支持此命令。

查看设备支持的链路聚合组数目和成员接口数目。

```
<HUAWEI> display trunk configuration
------------------------------------------------
Item            Default    Current    Configured
------------------------------------------------
trunk-group     128        64         64
trunk-member    8          16         16
------------------------------------------------
```

表 8-1 display trunk configuration 命令输出信息描述

项目	描述
Item	项目名称。
Default	设备缺省情况下支持的Eth-Trunk的规格。
Current	设备当前支持的Eth-Trunk的规格。
Configured	设备当前配置的Eth-Trunk的规格，若与**Current**列不同，则在重启设备后**Configured**列配置生效。

项目	描述
trunk-group	设备支持的Eth-Trunk组的数目。
trunk-member	每个Eth-Trunk组支持的成员接口数。

9 常见 VLAN 操作

关于本章

9.1 接口加入 VLAN

接口加入VLAN之前，需要在接口上设置对应的链路类型。具体请参见“**修改接口的链路类型**”。

- Access接口加入VLAN

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type access  //设置接口的链路类型为Access
[HUAWEI-GigabitEthernet0/0/1] port default vlan 10  //把接口GigabitEthernet0/0/1加入VLAN 10
```

- Trunk接口加入VLAN

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk  //设置接口的链路类型为Trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10  //把接口GigabitEthernet0/0/1加入VLAN 10
```

- Hybrid接口加入VLAN

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid  //设置接口的链路类型为Hybrid
[HUAWEI-GigabitEthernet0/0/1] port hybrid tagged vlan 10  //接口GigabitEthernet0/0/1以Tagged方式加入VLAN 10
```

```
[HUAWEI-GigabitEthernet0/0/1] port hybrid untagged vlan 20  //接口GigabitEthernet0/0/1以Untagged方式加入VLAN 20
```

- QinQ接口加入VLAN

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type dot1q-tunnel  //设置接口的链路类型为QinQ
[HUAWEI-GigabitEthernet0/0/1] port default vlan 10  //接口GigabitEthernet0/0/1加入VLAN 10
```

9.2 批量创建 VLAN

系统视图下执行命令**vlan batch**，批量创建VLAN。

- 批量创建10个连续的VLAN：VLAN11到VLAN20。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 11 to 20
```

- 批量创建10不连续的VLAN：VLAN10、VLAN15到VLAN19、VLAN25、VLAN28到VLAN30。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10 15 to 19 25 28 to 30
```

说明

批量创建不连续的VLAN时，一次最多可以输入10个不连续的VLAN或VLAN段，超过10个可以多次使用该命令进行配置。例如：**vlan batch 10 15 to 19 25 28 to 30** 一共是4个不连续的VLAN段。

9.3 接口批量加入 VLAN

通过端口组可以把接口批量加入VLAN；对于Access接口，还可以在VLAN视图下直接批量将接口加入VLAN。

- access接口类型。
  - 通过端口组批量将接口加入VLAN

```
<HUAWEI> system-view
[HUAWEI] port-group pg1  //创建端口组pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet1/0/1 to gigabitethernet1/0/5  //把接口gigabitethernet1/0/1到gigabitethernet1/0/5加入端口组
[HUAWEI-port-group-pg1] port link-type access  //批量修改端口gigabitethernet1/0/1 to gigabitethernet1/0/5的链路类型为access
[HUAWEI-port-group-pg1] port default vlan 10  //批量把端口gigabitethernet1/0/1 to gigabitethernet1/0/5加入VLAN10
```

  - 在VLAN视图下批量将接口加入VLAN

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] port gigabitethernet 1/0/1 to 1/0/5  //批量把端口gigabitethernet1/0/1 to gigabitethernet1/0/5加入VLAN10
```

说明

执行此操作前，须先将所有要批量加入VLAN的接口的接口类型配置为access。

- trunk接口类型。

```
<HUAWEI> system-view
[HUAWEI] port-group pg1  //创建端口组pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet1/0/1 to gigabitethernet1/0/5  //把接口gigabitethernet1/0/1到gigabitethernet1/0/5加入端口组
[HUAWEI-port-group-pg1] port link-type trunk  //批量修改端口gigabitethernet1/0/1 to gigabitethernet1/0/5的链路类型为trunk
[HUAWEI-port-group-pg1] port trunk allow-pass vlan 10 20  //批量把端口gigabitethernet1/0/1 to gigabitethernet1/0/5加入VLAN10和VLAN20
```


- hybrid接口类型。

```
<HUAWEI> system-view
[HUAWEI] port-group pg1  //创建端口组pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet1/0/1 to gigabitethernet1/0/5  //把接口gigabitethernet1/0/1到gigabitethernet1/0/5加入端口组
[HUAWEI-port-group-pg1] port link-type hybrid  //批量修改端口gigabitethernet1/0/1 to gigabitethernet1/0/5的链路类型为hybrid
[HUAWEI-port-group-pg1] port hybrid tagged vlan 10  //批量把端口gigabitethernet1/0/1 to gigabitethernet1/0/5以tagged方式加入VLAN10
[HUAWEI-port-group-pg1] port hybrid untagged vlan 20  //批量把端口gigabitethernet1/0/1 to gigabitethernet1/0/5 以untagged方式加入VLAN20
```

9.4 恢复接口下 VLAN 的缺省配置

接口下VLAN的缺省配置包括接口的PVID和接口缺省加入VLAN1。

- 恢复access接口的缺省配置。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] undo port default vlan
```

- 恢复trunk接口的缺省配置。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] undo port trunk pvid vlan
[HUAWEI-GigabitEthernet1/0/1] undo port trunk allow-pass vlan all
[HUAWEI-GigabitEthernet1/0/1] port trunk pvid vlan 1
```

- 恢复hybrid接口的缺省配置。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] undo port hybrid pvid vlan
[HUAWEI-GigabitEthernet1/0/1] undo port hybrid vlan all
[HUAWEI-GigabitEthernet1/0/1] port hybrid untagged vlan 1
```

9.5 删除 VLAN

设备支持删除批量VLAN和删除单个VLAN两种方式。

- 删除单个VLAN10。

```
<HUAWEI> system-view
[HUAWEI] undo vlan 10
```

- 删除批量VLAN10到VLAN20。

```
<HUAWEI> system-view
[HUAWEI] undo vlan batch 10 to 20
```

说明

V200R005之前版本，如果VLAN已经绑定VLANIF接口，删除VLAN之前必须使用**undo interface vlanif**命令删除对应的VLANIF接口。

9.6 修改接口的链路类型

接口的链路类型总共有4种，分别为：Access、Trunk、Hybrid、Dot1q-tunnel。不同版本，接口类型的修改方法不同。

- V200R005及后续版本：直接执行命令**port link-type** { **access** | **trunk** | **hybrid** | **dot1q-tunnel** }，然后根据提示输入“y”或“n”。当接口上VLAN的配置为缺省配置时，不会出现提示信息，会直接修改链路类型。
  - 若输入“y”后回车，设备会自动删除接口上VLAN的非默认配置，然后设置接口的链路类型为指定的类型。

- 若输入“n”后回车，设备不做任何处理，保持当前的链路类型和接口上的VLAN配置不变。

例如：将接口类型修改为Hybrid。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
Warning: This command will delete VLANs on this port. Continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment...done.
```

- V200R005以前版本：当接口上VLAN的缺省配置为默认加入VLAN 1，并且PVID为VLAN 1，可以执行命令**port link-type { access | trunk | hybrid | dot1q-tunnel }**，修改接口类型。

  - 将接口类型修改为Access

    ```
    <HUAWEI> system-view
    [HUAWEI] interface gigabitethernet0/0/1
    [HUAWEI-GigabitEthernet0/0/1] port link-type access
    [HUAWEI-GigabitEthernet0/0/1] port default vlan 10   //设置接口的PVID为VLAN 10，并同时将VLAN 10加入接口
    ```

  - 将接口类型修改为Trunk

    ```
    <HUAWEI> system-view
    [HUAWEI] interface gigabitethernet0/0/1
    [HUAWEI-GigabitEthernet0/0/1] port link-type trunk
    [HUAWEI-GigabitEthernet0/0/1] port trunk pvid vlan 10   //设置接口的PVID为VLAN 10
    [HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 2 10 20   //将VLAN 2、VLAN 10和VLAN 20加入接口
    ```

  - 将接口类型修改为Hybrid

    ```
    <HUAWEI> system-view
    [HUAWEI] interface gigabitethernet0/0/1
    [HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
    [HUAWEI-GigabitEthernet0/0/1] port hybrid pvid vlan 10   //设置接口的PVID为VLAN 10
    [HUAWEI-GigabitEthernet0/0/1] port hybrid untagged vlan 2 10   //将接口以Untagged方式加入VLAN 2和VLAN 10
    [HUAWEI-GigabitEthernet0/0/1] port hybrid tagged vlan 20   //将接口以Tag方式加入VLAN 20
    ```

  - 将接口类型修改为Dot1q-tunnel

    ```
    <HUAWEI> system-view
    [HUAWEI] interface gigabitethernet0/0/1
    [HUAWEI-GigabitEthernet0/0/1] port link-type dot1q-tunnel
    [HUAWEI-GigabitEthernet0/0/1] port default vlan 10   //设置接口的PVID为VLAN 10，对该接口收到的所有数据报文统一封装一层VLAN为10的Tag
    ```

  在修改链路类型时，如果接口上VLAN的配置不是缺省值，会出现以下提示信息：**Error: Please renew the default configurations.**

  此时需要先把接口上VLAN的配置恢复为缺省值，然后再修改链路类型。

  - 恢复Access或Dot1q-tunnel接口上VLAN的缺省配置

    ```
    <HUAWEI> system-view
    [HUAWEI] interface gigabitethernet0/0/1
    [HUAWEI-GigabitEthernet0/0/1] undo port default vlan
    ```

  - 恢复Trunk接口上VLAN的缺省配置

    ```
    <HUAWEI> system-view
    [HUAWEI] interface gigabitethernet0/0/1
    [HUAWEI-GigabitEthernet0/0/1] undo port trunk pvid vlan
    [HUAWEI-GigabitEthernet0/0/1] undo port trunk allow-pass vlan all
    [HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 1
    ```

  - 恢复Hybrid接口上VLAN的缺省配置

    ```
    <HUAWEI> system-view
    [HUAWEI] interface gigabitethernet0/0/1
    [HUAWEI-GigabitEthernet0/0/1] undo port hybrid pvid vlan
    [HUAWEI-GigabitEthernet0/0/1] undo port hybrid vlan all
    [HUAWEI-GigabitEthernet0/0/1] port hybrid untagged vlan 1
    ```


9.7 使用 Access 和 Trunk 接口连接用户主机

如图9-1所示，PC划分在VLAN 10中，通过接入交换机SwitchA上行接入汇聚交换机SwitchB。

图 9-1 PC 连接交换机组网图

- # 配置接入交换机SwitchA。

```
<SwitchA> system-view
[SwitchA] vlan batch 10  //如果不适用batch，会进入VLAN视图，需要执行quit命令退出该视图
[SwitchA] interface gigabitethernet0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk  //设置接口的链路类型为Trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 10  //把接口GigabitEthernet0/0/1加入VLAN 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access  //设置接口的链路类型为Access
[SwitchA-GigabitEthernet0/0/2] port default vlan 10  //把接口GigabitEthernet0/0/2加入VLAN 10
[SwitchA-GigabitEthernet0/0/2] quit
```

- # 配置汇聚交换机SwitchB。

```
<SwitchB> system-view
[SwitchB] vlan batch vlan 10  //如果不适用batch，会进入VLAN视图，需要执行quit命令退出该视图
[SwitchB] interface gigabitethernet0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type trunk  //设置接口的链路类型为Trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 10  //把接口GigabitEthernet0/0/1加入VLAN 10
[SwitchB-GigabitEthernet0/0/1] quit
```

9.8 使用 Hybrid 接口连接用户主机

如图9-2所示，PC划分在VLAN 10中，通过接入交换机SwitchA上行接入汇聚交换机SwitchB。

图 9-2 PC 连接交换机组网图

- # 配置接入交换机SwitchA。

```
<SwitchA> system-view
[SwitchA] vlan batch 10  //如果不适用batch，会进入VLAN视图，需要执行quit命令退出该视图
[SwitchA] interface gigabitethernet0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type hybrid  //设置接口的链路类型为Hybrid
[SwitchA-GigabitEthernet0/0/1] port hybrid tagged vlan 10  //把接口GigabitEthernet0/0/1以Tagged方式加入VLAN 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type hybrid  //设置接口的链路类型为Hybrid
[SwitchA-GigabitEthernet0/0/2] port hybrid pvid vlan 10  //设置接口的PVID为VLAN 10
```

```
[SwitchA-GigabitEthernet0/0/2] port hybrid untagged vlan 10  //把接口GigabitEthernet0/0/2以
Untagged方式加入VLAN 10
[SwitchA-GigabitEthernet0/0/2] quit
```

- # 配置汇聚交换机SwitchB。

```
<SwitchB> system-view
[SwitchB] vlan batch 10  //如果不适用batch，会进入VLAN视图，需要执行quit命令退出该视图
[SwitchB] interface gigabitethernet0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type hybrid  //设置接口的链路类型为Hybrid
[SwitchB-GigabitEthernet0/0/1] port hybrid tagged vlan 10  //把接口GigabitEthernet0/0/1以
Tagged方式加入VLAN 10
[SwitchB-GigabitEthernet0/0/1] quit
```


10 常见 VLAN Mapping 操作

关于本章

10.1 配置 1 to 1 VLAN Mapping

1 to 1 VLAN Mapping指的是把报文中的VLAN ID映射为公网的VLAN ID。

例如：将进入GE1/0/1接口的VLAN ID为2的报文映射为VLAN ID为200的报文。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet1/0/1
[HUAWEI-GigabitEthernet1/0/1] port link-type trunk  //设置接口的链路类型为trunk，仅接口的链路类型为trunk或hybrid，才能够配置VLAN Mapping
[HUAWEI-GigabitEthernet1/0/1] qinq vlan-translation enable  //盒式设备，必须先使能VLAN转换功能，框式设备不需要
[HUAWEI-GigabitEthernet1/0/1] port vlan-mapping vlan 2 map-vlan 200
```

10.2 配置 N to 1 VLAN Mapping

N to 1 VLAN Mapping可以同时把一段VLAN ID映射为同一个公网的VLAN ID。

例如：将进入GE1/0/1接口的VLAN ID为3、4、5或6的报文映射为VLAN ID为200的报文。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet1/0/1
[HUAWEI-GigabitEthernet1/0/1] port link-type trunk  //设置接口的链路类型为trunk，仅接口的链路类型为trunk或hybrid，才能够配置VLAN Mapping
[HUAWEI-GigabitEthernet1/0/1] qinq vlan-translation enable  //盒式设备，必须先使能VLAN转换功能，框式设备不需要
[HUAWEI-GigabitEthernet1/0/1] port vlan-mapping vlan 3 to 6 map-vlan 200
```

说明

S5720HI、S5730HI和S6720HI不支持该配置。

10.3 配置 2 to 1 VLAN Mapping

2 to 1 VLAN Mapping指的是当接口收到带有双层VLAN Tag的报文时，将报文中携带的外层Tag的VLAN ID映射为公网的VLAN ID，内层Tag作为数据透传。

例如：将进入GE1/0/1接口的外层VLAN ID为8，内层VLAN ID为7的报文映射为外层VLAN ID为200的报文，内层VLAN ID保持不变。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet1/0/1
[HUAWEI-GigabitEthernet1/0/1] port link-type trunk  //设置接口的链路类型为trunk，仅接口的链路类型为trunk或hybrid，才能够配置VLAN Mapping
[HUAWEI-GigabitEthernet1/0/1] qinq vlan-translation enable  //盒式设备，必须先使能VLAN转换功能，框式设备不需要
[HUAWEI-GigabitEthernet1/0/1] port vlan-mapping vlan 8 inner-vlan 7 map-vlan 200
```

说明

盒式设备仅S1720X-E、S3700HI、S5700EI、S5700HI、S5710EI、S5710HI、S5720EI、S5720HI、S5730HI、S5730S-EI、S5730SI、S6700EI、S6720EI、S6720HI、S6720LI、S6720S-EI、S6720S-LI、S6720S-SI和S6720SI支持该配置。框式设备均支持该配置。

10.4 配置 2 to 2 VLAN Mapping

2 to 2 VLAN Mapping指的是当接口收到带有双层VLAN Tag的报文时，将报文中携带的双层VLAN Tag的VLAN ID都映射为公网对应的VLAN ID。

例如：将进入GE1/0/1接口的外层VLAN ID为11，内层VLAN ID为10的报文映射为外层VLAN ID为200，内层VLAN ID为201的报文。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet1/0/1
[HUAWEI-GigabitEthernet1/0/1] port link-type trunk  //设置接口的链路类型为trunk，仅接口的链路类型为trunk或hybrid，才能够配置VLAN Mapping
[HUAWEI-GigabitEthernet1/0/1] qinq vlan-translation enable  //盒式设备，必须先使能VLAN转换功能，框式设备不需要
[HUAWEI-GigabitEthernet1/0/1] port vlan-mapping vlan 11 inner-vlan 10 map-vlan 200 map-inner-vlan 201
```

说明

盒式设备仅S1720X-E、S5720EI、S5720HI、S5730HI、S5730S-EI、S5730SI、S6720EI、S6720HI、S6720LI、S6720S-EI、S6720S-LI、S6720S-SI和S6720SI支持此配置。

11 常见 QinQ 操作

关于本章

介绍QinQ的常见操作。

11.1 配置基本 QinQ

基本QinQ又称为普通QinQ，是基于接口方式实现的。接口开启基本QinQ功能后，设备会为该接口接收到的报文添加上本接口缺省VLAN的Tag。

- 如果接收到的是已经带有VLAN Tag的报文，该报文就成为双Tag的报文。
- 如果接收到的是不带VLAN Tag的报文，该报文就成为带有接口缺省VLAN Tag的报文。

创建外层VLAN 10。

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
```

配置下行接口GE1/0/1。

```
[HUAWEI] interface gigabitethernet1/0/1
[HUAWEI-GigabitEthernet1/0/1] port link-type dot1q-tunnel   //设置链路类型为dot1q-tunnel
[HUAWEI-GigabitEthernet1/0/1] port default vlan 10   //对接口GE1/0/1收到的所有数据报文统一封装一层VLAN为10的Tag
```

配置上行接口GE1/0/2透传外层VLAN 10。

```
[HUAWEI] interface gigabitethernet1/0/2
[HUAWEI-GigabitEthernet1/0/2] port link-type trunk
[HUAWEI-GigabitEthernet1/0/2] port trunk allow-pass vlan 10
```

相关信息

技术论坛

玩转高大上的QinQ技术

11.2 配置灵活 QinQ

灵活QinQ又称为VLAN Stacking或QinQ Stacking，它是基于接口与VLAN相结合的方式实现的。

配置需求：对内层VLAN 100～200的报文添加上VLAN ID为2的外层Tag，对内层VLAN 300～400的报文添加上VLAN ID为3的外层Tag，对VLAN 1000的报文做单层透传。

- **盒式交换机配置灵活QinQ**

  # 创建外层VLAN 2、VLAN 3和需要单层透传的VLAN 1000。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 2 3 1000
```

  # 配置下行接口GE0/0/1。

```
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable   //盒式设备，必须先使能VLAN转换功能
[HUAWEI-GigabitEthernet0/0/1] port hybrid untagged vlan 2 3   //接口以Untagged方式加入叠加后的VLAN 2和VLAN 3
[HUAWEI-GigabitEthernet0/0/1] port hybrid tagged vlan 1000   //接口透传单层VLAN 1000
[HUAWEI-GigabitEthernet0/0/1] port vlan-stacking vlan 100 to 200 stack-vlan 2   //对内层VLAN 100～200的报文添加上VLAN ID为2的外层Tag
[HUAWEI-GigabitEthernet0/0/1] port vlan-stacking vlan 300 to 400 stack-vlan 3   //对内层VLAN 300～400的报文添加上VLAN ID为3的外层Tag
[HUAWEI-GigabitEthernet0/0/1] port vlan-mapping vlan 1000 map-vlan 1000   //盒式S5700EI、S3700EI和S3700SI对单层透传的VLAN，需要配置自身映射到自身的VLAN Mapping，其他形态不需要配置
[HUAWEI-GigabitEthernet0/0/1] quit
```

  # 配置上行接口GE0/0/5透传叠加后的外层VLAN和需要单层透传的VLAN。

```
[HUAWEI] interface gigabitethernet0/0/5
[HUAWEI-GigabitEthernet0/0/5] port link-type trunk
[HUAWEI-GigabitEthernet0/0/5] port trunk allow-pass vlan 2 3 1000
```

- **框式交换机配置灵活QinQ**

  # 创建外层VLAN 2、VLAN 3和需要单层透传的VLAN 1000。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 2 3 1000
```

  # 配置下行接口GE1/0/1。

```
[HUAWEI] interface gigabitethernet1/0/1
[HUAWEI-GigabitEthernet1/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet1/0/1] port hybrid untagged vlan 2 3   //接口以Untagged方式加入叠加后的VLAN 2和VLAN 3
[HUAWEI-GigabitEthernet1/0/1] port hybrid tagged vlan 1000   //接口透传单层VLAN 1000
[HUAWEI-GigabitEthernet1/0/1] port vlan-stacking vlan 100 to 200 stack-vlan 2   //对内层VLAN 100～200的报文添加上VLAN ID为2的外层Tag
[HUAWEI-GigabitEthernet1/0/1] port vlan-stacking vlan 300 to 400 stack-vlan 3   //对内层VLAN 300～400的报文添加上VLAN ID为3的外层Tag
[HUAWEI-GigabitEthernet1/0/1] port vlan-mapping vlan 1000 map-vlan 1000   //EF1D2G24SE3L、ES0D0G24SA00、ES0D0G24CA00、EH1D2G24SSA0和EH1D2S24CSA0单板对单层透传的VLAN，需要配置自身映射到自身的VLAN Mapping，其他单板不需要配置
[HUAWEI-GigabitEthernet1/0/1] quit
```

  # 配置上行接口GE2/0/1透传叠加后的外层VLAN和需要单层透传的VLAN。

```
[HUAWEI] interface gigabitethernet2/0/1
[HUAWEI-GigabitEthernet2/0/1] port link-type trunk
[HUAWEI-GigabitEthernet2/0/1] port trunk allow-pass vlan 2 3 1000
```

相关信息

技术论坛

玩转高大上的QinQ技术

11.3 配置对 Untagged 报文添加双层 Tag 功能

配置接口GE0/0/1对收到的Untagged报文，直接添加双层Tag的功能。

```
<HUAWEI> system-view
[HUAWEI] vlan 10   //创建双层Tag中外层Tag对应的VLAN
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable   //盒式设备，必须先使能VLAN转换功能，框式设备不需要配置
[HUAWEI-GigabitEthernet0/0/1] port hybrid untagged vlan 10   //接口以Untagged方式加入叠加后的外层VLAN 10
[HUAWEI-GigabitEthernet0/0/1] port vlan-stacking untagged stack-vlan 10 stack-inner-vlan 5   //该接口收到的Untagged报文，叠加两层VLAN Tag，内层VLAN为5，外层VLAN为10
```

说明

- 盒式S5700SI和S5700EI，EF1D2G24SE3L、ES0D0G24SA00、ES0D0G24CA00、EH1D2G24SSA0和EH1D2S24CSA0单板不支持此配置。
- 在配置对Untagged报文添加双层Tag的命令时，若出现如下提示信息，请先通过命令**port link-type hybrid**设置接口的链路类型为Hybrid。

  ```
  [HUAWEI-GigabitEthernet0/0/1] port vlan-stacking untagged stack-vlan 10 stack-inner-vlan 5
  Error: The port is not a Trunk or Hybrid port.
  ```

- 盒式设备，在配置对Untagged报文添加双层Tag的命令时，若出现如下提示信息，请先通过命令**qinq vlan-translation enable**使能VLAN转换功能。

  ```
  [HUAWEI-GigabitEthernet0/0/1] port vlan-stacking untagged stack-vlan 10 stack-inner-vlan 5
  Error: Please configure qinq vlan-translation enable on this port first.
  ```

- 在配置对Untagged报文添加双层Tag的命令时，若出现如下提示信息时，请先通过命令**undo port hybrid pvid vlan**恢复接口的PVID为缺省值1。

  ```
  [HUAWEI-GigabitEthernet0/0/1] port vlan-stacking untagged stack-vlan 10 stack-inner-vlan 5
  Error: This port has been configured with default VLAN or PVID, please undo it first.
  ```

相关信息

技术论坛

玩转高大上的QinQ技术

11.4 删除灵活 QinQ 配置

删除某一接口下所有灵活QinQ的配置。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] undo port vlan-stacking all
```

删除灵活QinQ中某一个内层VLAN的配置。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] undo port vlan-stacking vlan 3 stack-vlan 10   //删除内层VLAN为3的灵活QinQ配置
```


12 常见 STP/RSTP 操作

关于本章

介绍STP/RSTP功能的常见操作。

12.1 开启 STP/RSTP

开启全局 STP/RSTP

在系统视图下执行命令**stp enable**。

```
<HUAWEI> system-view
[HUAWEI] stp enable
```

开启接口 STP/RSTP

在接口视图下执行命令**stp enable**。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] stp enable
```

12.2 关闭 STP/RSTP

关闭全局 STP/RSTP

在系统视图下执行命令**undo stp enable**。

```
<HUAWEI> system-view
[HUAWEI] undo stp enable
```

关闭接口 STP/RSTP

在接口视图下执行命令**undo stp enable**。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] undo stp enable
```

12.3 配置根桥和备份根桥

可以通过计算来自动确定生成树的根桥，用户也可以手动配置设备为指定生成树的根桥或备份根桥。

配置根桥。

```
<HUAWEI> system-view
[HUAWEI] stp root primary
```

配置备份根桥。

```
<HUAWEI> system-view
[HUAWEI] stp root secondary
```

12.4 配置根保护

在接口视图下执行命令**stp root-protection**。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] stp root-protection
```

12.5 配置边缘端口

在接口视图下执行命令**stp edged-port enable**。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] stp edged-port enable
```

12.6 修改 STP/RSTP 的 cost 值

在接口视图下执行命令**stp cost** *cost*。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] stp cost 20000
```


12.7 查看 STP/RSTP 状态

查看生成树的状态和统计信息摘要。

```
<HUAWEI> display stp brief
MSTID    Port                        Role  STP State     Protection
    0    GigabitEthernet1/0/22       DESI  FORWARDING      NONE
    0    GigabitEthernet1/0/27       DESI  FORWARDING      NONE
    0    GigabitEthernet1/0/28       DESI  FORWARDING      NONE
    0    GigabitEthernet1/0/35       DESI  FORWARDING      NONE
    0    GigabitEthernet1/0/40       DESI  FORWARDING      NONE
```

12.8 查看根桥信息

查看根桥的生成树状态信息。

```
<HUAWEI> display stp bridge root
MSTID             Root ID  Root Cost Hello Max Forward Root Port
                                     Time Age   Delay
----- -------------------- ---------- ----- --- ------- -----------------
    0 61440.781d-ba56-f06c          0     2  20      15
```


13 常见 DHCP 操作

关于本章

介绍DHCP的常见操作。

13.1 排除不参与自动分配的 IP 地址

以下场景中可以配置某些IP地址不参与自动分配：

- 某企业希望为员工办公电脑分配的IP地址范围是10.1.1.2～10.1.1.254（网关地址为10.1.1.1）。但是企业中部署的DNS服务器，为了保证稳定性，希望通过手工配置IP地址为10.1.1.10。这时，可以把10.1.1.10配置为不参与自动分配的IP地址。
- 基于全局方式下，假设某企业希望给部门A的客户端分配的IP地址范围是：10.1.1.2～10.1.1.100（网关地址为10.1.1.1）；给部门B的客户端分配的IP地址范围是：10.1.1.101～10.1.1.254。设备做DHCP服务器，可以创建两个地址池pool1（为部门A的主机分配地址）和pool2（为部门B的主机分配地址），地址池网络掩码均为24；并且在pool1中排除10.1.1.101～10.1.1.254，在pool2中排除10.1.1.1～10.1.1.100。

在作为DHCP服务器的设备上，排除不参与自动分配的IP地址。例如：在网段地址为10.1.1.0、掩码长度为24的地址池中，配置IP地址10.1.1.100～10.1.1.200不参与自动分配。

- 采用全局地址池时的配置：

```
<HUAWEI> system-view
[HUAWEI] ip pool pool1
[HUAWEI-ip-pool-pool1] network 10.1.1.0 mask 24
[HUAWEI-ip-pool-pool1] gateway-list 10.1.1.1
[HUAWEI-ip-pool-pool1] excluded-ip-address 10.1.1.100 10.1.1.200
```

- 采用接口地址池时的配置：

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server excluded-ip-address 10.1.1.100 10.1.1.200
```

13.2 修改租期

作为DHCP服务器和DHCP客户端的设备都可以修改租期。DHCP服务器在分配租期时，比较DHCP客户端期望的租期和DHCP服务器地址池中的租期，把较短的租期分配给DHCP客户端。

缺省情况下，设备作为DHCP服务器的缺省租期是1天；设备作为DHCP客户端时未配置缺省租期。

在作为DHCP服务器的设备上，将全局地址池pool1或接口地址池VLANIF100内的IP地址的租期修改为10天。

- 采用全局地址池时的配置：

```
<HUAWEI> system-view
[HUAWEI] ip pool pool1
[HUAWEI-ip-pool-pool1] lease day 10
```

- 采用接口地址池时的配置：

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp server lease day 10
```

在作为DHCP客户端的设备上，修改租期为10天（即864000秒）。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client expected-lease 864000
```

13.3 为客户端分配固定的 IP 地址

网络规划时，有些重要设备为了保证稳定性，需要使用固定的IP地址。例如，企业内的DNS服务器、办公楼内的打印机等。该IP地址可以静态配置（通过命令**ip address**）也可以通过DHCP方式获取。下面介绍通过DHCP方式为客户端分配固定IP地址的方法。

在作为DHCP服务器的设备上，为客户端分配固定的IP地址。例如：在网段地址为10.1.1.0、掩码长度为24的地址池中，配置IP地址10.1.1.100只能分配给MAC地址为dcd2-fc96-e4c0的客户端。

- 采用全局地址池时的配置：

```
<HUAWEI> system-view
[HUAWEI] ip pool pool1
[HUAWEI-ip-pool-pool1] static-bind ip-address 10.1.1.100 mac-address dcd2-fc96-e4c0
```

- 采用接口地址池时的配置：

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp server static-bind ip-address 10.1.1.100 mac-address dcd2-fc96-e4c0
```

13.4 取消为客户端分配固定的 IP 地址

在作为DHCP服务器的设备上，取消将指定的IP地址分配给固定的客户端。例如：在网段地址为10.1.1.0、掩码长度为24的地址池中，取消将IP地址10.1.1.5固定分配给某个客户端。客户端与IP地址的静态绑定关系可以通过命令**display ip pool** { **interface** *interface-pool-name* | **name** *ip-pool-name* } **used**查看，具体显示可参见**13.5 查看已使用的IP地址**。

- 采用全局地址池时的配置：
  a. 回收IP地址10.1.1.5

```
<HUAWEI> reset ip pool name pool1 10.1.1.5
```

  b. 解除静态绑定关系

```
<HUAWEI> system-view
[HUAWEI] ip pool pool1
[HUAWEI-ip-pool-pool1] undo static-bind ip-address 10.1.1.5
```

- 采用接口地址池时的配置：
  a. 回收IP地址10.1.1.5

```
<HUAWEI> reset ip pool interface vlanif100 10.1.1.5
```

  b. 解除静态绑定关系

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] undo dhcp server static-bind ip-address 10.1.1.5
```

13.5 查看已使用的 IP 地址

在作为DHCP服务器的设备上，执行命令**display ip pool** { **interface** *interface-pool-name* | **name** *ip-pool-name* } **used**，查看已使用的IP地址。

例如，以下回显信息表示全局地址池pool1中，可用的IP地址一共有253个（10.1.1.1～10.1.1.254，除去网关地址10.1.1.2），其中IP地址10.1.1.254被MAC地址为0235-2036-adcc的DHCP客户端被使用；IP地址10.1.1.5与MAC地址为00e0-0987-7895的DHCP客户端绑定。

```
<HUAWEI> display ip pool name pool1 used
  Pool-name      : pool1
  Pool-No        : 0
  Lease          : 1 Days 0 Hours 0 Minutes
  Domain-name    : -
  DNS-server0    : -
  NBNS-server0   : -
  Netbios-type   : -
  Position       : Local           Status          : Unlocked
  Gateway-0      : 10.1.1.2
  Network        : 10.1.1.0
  Mask           : 255.255.255.0
  VPN instance   : --

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



```
        Start           End      Total  Used  Idle(Expired)  Conflict  Disable
-------------------------------------------------------------------------------
      10.1.1.1      10.1.1.254   253     2        252(0)         0         0
-------------------------------------------------------------------------------
Network section :
-------------------------------------------------------------------------------
Index              IP              MAC        Lease   Status
-------------------------------------------------------------------------------
  253       10.1.1.254    0235-2036-adcc        178   Used
  4         10.1.1.5      00e0-0987-7895        60    Static-bind
-------------------------------------------------------------------------------
```

13.6 清除冲突地址

在作为DHCP服务器的设备上，清除地址池中冲突的地址，使冲突的地址成为可以正常使用的地址。例如：清除全局地址池pool1或接口地址池VLANIF100内冲突的IP地址。

说明

地址冲突的客户端需要重新上线来获取新的IP地址。

- 采用全局地址池时的配置：

```
<HUAWEI> reset ip pool name pool1 conflict
```

- 采用接口地址池时的配置：

```
<HUAWEI> reset ip pool interface vlanif100 conflict
```

13.7 扩大地址池范围

缩小地址池的掩码长度，可以扩大地址池范围。例如：DHCP服务器可以为126个用户分配IP地址（地址池掩码长度为25），现在网络中新增120个用户，同样使用DHCP方式获取IP地址；此时需要将地址池掩码长度缩小到24。在扩大地址池范围之前，需要确认IP地址是否已经分配给客户端，请参见**13.5 查看已使用的IP地址**。

说明

- 掩码由25调整到24后，可以多为128个用户分配IP地址。
- 扩大的地址范围不能与网络中其他地址范围冲突。
- 根据客户端在线的情况适当规划客户端数量和地址池范围的比例。如果所有客户端都要同时在线，例如企业员工的PC，需要确保地址池中可供分配的地址数不能少于客户端的数量；如果客户端不同时在线，例如针对酒店、网吧等公共场所的PC，PC不是在同一时间在线，地址池中可供分配的地址数可以少于客户端的数量。

- **如果没有分配出去**

  在作为DHCP服务器的设备上，缩小地址池的掩码长度，可以扩大地址池范围。

  - 采用全局地址池时的配置：

```
<HUAWEI> system-view
[HUAWEI] ip pool pool1
[HUAWEI-ip-pool-pool1] undo network
[HUAWEI-ip-pool-pool1] network 10.1.1.0 mask 24  //调整掩码长度
```

  - 采用接口地址池时的配置：

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24  //调整掩码长度
[HUAWEI-Vlanif100] dhcp select interface  //重新使能接口地址池功能
```

- **如果已经分配出去**

  在作为DHCP服务器的设备上，按“回收IP地址（仅全局地址池时需要配置）->配置防止IP地址重复分配功能->调整地址池掩码长度”的步骤，扩大地址池范围。

- 采用全局地址池时的配置：

```
<HUAWEI> reset ip pool name pool1 all  //回收所有的IP地址
<HUAWEI> system-view
[HUAWEI] dhcp server ping packet 3  //配置防止IP地址重复分配功能
[HUAWEI] dhcp server ping timeout 100  //配置防止IP地址重复分配功能
[HUAWEI] ip pool pool1
[HUAWEI-ip-pool-pool1] undo network
[HUAWEI-ip-pool-pool1] network 10.1.1.0 mask 24  //调整掩码长度
```

- 采用接口地址池时的配置：

```
<HUAWEI> system-view
[HUAWEI] dhcp server ping packet 3  //配置防止IP地址重复分配功能
[HUAWEI] dhcp server ping timeout 100  //配置防止IP地址重复分配功能
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24  //调整掩码长度
[HUAWEI-Vlanif100] dhcp select interface  //重新使能接口地址池功能
```

13.8 缩小地址池范围

扩大地址池的掩码长度可以缩小地址池范围。例如：DHCP服务器可以为254个用户分配IP地址（地址池掩码长度为24），现在网络中减少140个用户，为避免地址浪费，此时可以将地址池掩码长度扩大到25，以缩小地址池的范围。在缩小地址池范围之前，需要IP地址是否已经分配给客户端，请参见13.5 查看已使用的IP地址。

说明

掩码由24调整到25后，可以节约128个IP地址。

- **如果没有分配出去**

  在作为DHCP服务器的设备上，扩大地址池的掩码长度，可以缩小地址池范围。

  - 采用全局地址池时的配置：

```
<HUAWEI> system-view
[HUAWEI] ip pool pool1
[HUAWEI-ip-pool-pool1] undo network
[HUAWEI-ip-pool-pool1] network 10.1.1.0 mask 25  //调整掩码长度
```

  - 采用接口地址池时的配置：

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 25  //调整掩码长度
[HUAWEI-Vlanif100] dhcp select interface  //重新使能接口地址池功能
```

- **如果已经分配出去**

  在作为DHCP服务器的设备上，按“回收IP地址（仅全局地址池时需要配置）->配置防止IP地址重复分配功能->调整地址池掩码长度”的步骤，缩小地址池范围。

  说明

  缩小地址池范围之后，拥有地址池范围之外IP地址的客户端，在租期到期后会重新申请IP地址。

  - 采用全局地址池时的配置：

```
<HUAWEI> reset ip pool name pool1 all  //回收所有的IP地址
<HUAWEI> system-view
[HUAWEI] dhcp server ping packet 3  //配置防止IP地址重复分配功能
[HUAWEI] dhcp server ping timeout 100  //配置防止IP地址重复分配功能
[HUAWEI] ip pool pool1
[HUAWEI-ip-pool-pool1] undo network
[HUAWEI-ip-pool-pool1] network 10.1.1.0 mask 25  //调整掩码长度
```

  - 采用接口地址池时的配置：

```
<HUAWEI> system-view
[HUAWEI] dhcp server ping packet 3  //配置防止IP地址重复分配功能
```

```
[HUAWEI] dhcp server ping timeout 100  //配置防止IP地址重复分配功能
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 25  //调整掩码长度
[HUAWEI-Vlanif100] dhcp select interface  //重新使能接口地址池功能
```

13.9 防止从仿冒的 DHCP 服务器获取 IP 地址

在二层网络的接入设备或第一个DHCP中继上，配置DHCP Snooping功能防止从仿冒的DHCP服务器获取IP地址。

说明

- 对于二层接入设备来说，1、2和3都是必选步骤，请按照以下顺序配置。
- 对于DHCP中继设备来说，仅需配置步骤1和2。

1. 全局下的配置。

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
```

2. 连接DHCP客户端侧接口的配置。所有连接DHCP客户端的接口都需要配置，以接口GE 1/0/1为例。

```
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet1/0/1] quit
```

3. 连接DHCP服务器侧接口的配置。

```
[HUAWEI] interface gigabitethernet 1/0/2
[HUAWEI-GigabitEthernet1/0/2] dhcp snooping trusted
[HUAWEI-GigabitEthernet1/0/2] quit
```

13.10 关闭 DHCP 服务

在作为DHCP服务器、DHCP中继或DHCP Snooping的设备上，关闭DHCP服务。缺省情况下，DHCP服务处于关闭状态。

```
<HUAWEI> system-view
[HUAWEI] undo dhcp enable
```


14 常见 ARP 操作

关于本章

介绍ARP的常见操作。

14.1 查看 ARP 表项

在日常维护工作中，用户可以在任意视图下执行**display arp**相关命令，查看设备上的ARP表项信息。

通过在网关设备上查看ARP表项，网络管理员可以查看下挂用户的IP地址、MAC地址和接口等信息。例如，当网络管理员知道某个用户的IP地址，想查询该用户的MAC地址时，可以通过查看ARP表项信息获取。

当网关设备上没有学习到下挂用户的IP地址时，可以在网关设备上ping该网段的广播地址。例如网关的IP地址为10.10.10.1/24，在网关设备上ping 10.10.10.255，同一网段的用户会发送ARP应答报文，网关设备收到ARP应答报文后即能学习到用户的IP地址。

查看设备上172.16.0.0/16网段的ARP表项。

```
<HUAWEI> display arp network 172.16.0.0 16
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-
INSTANCE
                                          VLAN/
CEVLAN
```



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

172.16.10.3     0025-9efb-be55            S--         GE1/0/6

100/-
172.16.20.3     0200-0000-00e8            S--         GE1/0/19
172.16.10.1     0025-9ef4-abcd            I -
Vlanif100
172.16.10.2     0025-9efb-be55  20        D-0         GE1/0/6

100/-
172.16.20.1     0025-9ef4-abcd            I -         GE1/0/19
172.16.20.2     0200-0000-00e8  18        D-0         GE1/0/19
--------------------------------------------------------------------------------

Total:6         Dynamic:2       Static:2     Interface:2
```

上述回显中，每行ARP表项的具体含义如下：

- IP地址为172.16.10.3，MAC地址为0025-9efb-be55，TYPE字段为S（代表该ARP表项为静态ARP表项）。这条静态ARP表项出接口为GE1/0/6，VLAN编号为100。
- IP地址为172.16.20.3，MAC地址为0200-0000-00e8，TYPE字段为S（代表该ARP表项为静态ARP表项）。这条静态ARP表项出接口为GE1/0/19。
- IP地址为172.16.10.1，MAC地址为0025-9ef4-abcd，TYPE字段为I（代表该ARP表项为接口本身的ARP表项）。这条ARP表项代表IP地址172.16.10.1是接口Vlanif100的IP地址。
- IP地址为172.16.10.2，MAC地址为0025-9efb-be55，TYPE字段为D（代表该ARP表项为动态ARP表项）。这条动态ARP表项是从接口GE1/0/6动态学习到的，VLAN编号为100，剩余存活时间为20分钟。
- IP地址为172.16.20.1，MAC地址为0025-9ef4-abcd，TYPE字段为I（代表该ARP表项为接口本身的ARP表项）。这条ARP表项代表IP地址172.16.20.1是接口GE1/0/19的IP地址。
- IP地址为172.16.20.2，MAC地址为0200-0000-00e8，TYPE字段为D（代表该ARP表项为动态ARP表项）。这条动态ARP表项是从接口GE1/0/19动态学习到的，剩余存活时间为18分钟。

说明

如果MAC ADDRESS字段显示为“Incomplete”，表示当前ARP表项为临时ARP表项。当IP报文触发ARP Miss消息时，设备会根据ARP Miss消息生成临时ARP表项，并且向目的网段发送ARP请求报文。

- 在临时ARP表项老化时间范围内：
  - 设备收到ARP应答报文前，匹配临时ARP表项的IP报文将被丢弃并且不会触发ARP Miss消息。
  - 设备收到ARP应答报文后，则生成正确的ARP表项来替换临时ARP表项。
- 在临时ARP表项老化超时后，设备会清除临时ARP表项。

相关信息

技术论坛

IP与MAC一线牵之ARP

视频

如何查询MAC和ARP表项

14.2 刷新 ARP 表项

当需要刷新设备上的ARP表项时，可以先清除设备上的ARP表项，这样设备会重新学习ARP表项。

注意

清除ARP表项后，将取消IP地址和MAC地址的映射关系，可能导致无法访问某些节点。清除前请务必仔细确认。

清除设备上所有的ARP表项。

说明

V200R009C00及后续版本设备不支持该功能。

```
<HUAWEI> reset arp all
```

清除设备上IP地址为172.16.10.1的动态ARP表项。

```
<HUAWEI> reset arp dynamic ip 172.16.10.1 //如果不指定IP地址，则删除设备上所有的动态ARP表项。
```

清除设备上所有的静态ARP表项。

```
<HUAWEI> reset arp static
Warning: This operation will reset all static ARP entries, and clear the configurations of all
static ARP, continue?[Y/N]:y
```

清除设备上IP地址为172.16.20.1，MAC地址为0023-0045-0067，出接口为GE1/0/1的静态ARP表项。

```
<HUAWEI> system-view
[HUAWEI] undo arp static 172.16.20.1 0023-0045-0067 interface gigabitethernet 1/0/1
```

清除设备上IP地址为172.16.20.1，从VLANIF100接口学习到的ARP表项。

```
<HUAWEI> reset arp interface vlanif 100 ip 172.16.20.1 //如果不指定IP地址，则删除设备上所有
VLANIF100接口学习到的ARP表项。
```

14.3 配置 ARP 老化时间

ARP老化时间仅对动态ARP表项生效，缺省值是20分钟。用户可以在系统视图或接口视图下执行命令**arp expire-time** *expire-time*，配置动态ARP表项的老化时间。ARP老化时间*expire-time*取值范围：框式交换机是60～62640，盒式交换机是30～62640，单位是秒。

如果只在系统视图下进行了配置，则对设备上所有接口学习到的动态ARP表项生效。如果在某接口视图和系统视图下同时进行了配置，则该接口学习到的动态ARP表项的老化时间与接口视图下的配置保持一致。

配置动态ARP表项的老化时间为1800秒。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp expire-time 1800
```


配置完成后可以在任意视图下执行命令**display current configuration | include arp**，查看设备上已配置的动态ARP表项的老化时间。

```
<HUAWEI> display current-configuration | include arp
arp expire-time 1800
```

14.4 配置静态 ARP 表项

静态ARP表项不会被老化，不会被动态ARP表项覆盖。用户可以通过手工方式配置静态ARP表项，也可以通过自动扫描与固化方式批量配置静态ARP表项。

通过手工方式配置静态 ARP 表项

说明

对于出接口是以太网接口，并且以太网接口处于二层模式的情况，建议用户尽量配置长静态ARP表项，即配置ARP表项时同时指定VLAN和出接口。

配置一条静态ARP表项，IP地址为172.16.10.2，MAC地址为0023-0045-0067，出接口GE1/0/1处于二层模式，此条ARP表项属于VLAN100。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 172.16.10.1 24 //VLANIF接口的IP地址需要与静态ARP表项中的IP地址（172.16.10.2）同网段。
[HUAWEI-Vlanif100] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] port link-type trunk
[HUAWEI-GigabitEthernet1/0/1] port trunk allow-pass vlan 100 //接口GigabitEthernet1/0/1处于二层模式，需要加入VLAN100。
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] arp static 172.16.10.2 0023-0045-0067 vid 100 interface gigabitethernet 1/0/1
```

配置一条静态ARP表项，IP地址为172.16.20.2，MAC地址为0023-0045-0068，出接口GE1/0/2处于三层模式。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/2
[HUAWEI-GigabitEthernet1/0/2] undo portswitch
[HUAWEI-GigabitEthernet1/0/2] ip address 172.16.20.1 24 //GigabitEthernet1/0/2的IP地址需要与静态ARP表项中的IP地址（172.16.20.2）同网段。
[HUAWEI-GigabitEthernet1/0/2] quit
[HUAWEI] arp static 172.16.20.2 0023-0045-0068 interface gigabitethernet 1/0/2
```

配置一条静态ARP表项，IP地址为172.16.30.2，MAC地址为0023-0045-0069，此静态ARP表项属于VPN实例vpn1。

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
[HUAWEI-vpn-instance-vpn1] quit
[HUAWEI] arp static 172.16.30.2 0023-0045-0069 vpn-instance vpn1
```

配置一条静态ARP表项，IP地址为172.16.40.2，MAC地址为02bf-0045-0070。（例如设备采用多端口ARP方式与NLB服务器群集连接时，可以配置这种短静态的ARP表项。）

```
<HUAWEI> system-view
[HUAWEI] arp static 172.16.40.2 02bf-0045-0070
```


通过自动扫描与固化方式批量配置静态 ARP 表项

接口VLANIF103的IP地址为172.16.50.1/24，自动扫描该网段IP地址为172.16.50.2～172.16.50.4的ARP表项，并将学习到的ARP表项固化为静态ARP表项。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 103
[HUAWEI] interface vlanif 103
[HUAWEI-Vlanif103] ip address 172.16.50.1 24
[HUAWEI-Vlanif103] quit
[HUAWEI] interface gigabitethernet 1/0/3
[HUAWEI-GigabitEthernet1/0/3] port link-type trunk
[HUAWEI-GigabitEthernet1/0/3] port trunk allow-pass vlan 103
[HUAWEI-GigabitEthernet1/0/3] quit
[HUAWEI] display arp network 172.16.50.0 24
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-
INSTANCE
                                          VLAN/
CEVLAN
--------------------------------------------------------------------------------

172.16.50.1     00e0-0987-7895            I -
Vlanif103
--------------------------------------------------------------------------------

Total:1         Dynamic:0       Static:0     Interface:1
[HUAWEI] interface vlanif 103
[HUAWEI-Vlanif103] arp scan 172.16.50.2 to 172.16.50.4 //在接口VLANIF103上进行自动扫描，172.16.50.2～172.16.50.4与VLANIF103接口的IP地址172.16.50.1在同一网段，即ARP自动扫描区间的起始IP地址和结束IP地址必须与VLANIF接口的IP地址（主IP地址或者从IP地址）在同一网段。
Warning: This operation may take a long time, press CTRL+C to break. Continue?[Y/
N]:y
Processing...

Info: ARP scanning is completed.
[HUAWEI-Vlanif103] display arp network 172.16.50.0 24 //自动扫描后，查看ARP表项，设备新学习到3条动态ARP表项。
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-
INSTANCE
                                          VLAN/
CEVLAN
--------------------------------------------------------------------------------

172.16.50.1     00e0-0987-7895            I -
Vlanif103
172.16.50.2     0200-0000-0212  20        D-0
GE1/0/3

103/-
172.16.50.3     0200-0000-0212  20        D-0
GE1/0/3

103/-
172.16.50.4     0200-0000-0212  20        D-0
GE1/0/3

103/-
--------------------------------------------------------------------------------

Total:4         Dynamic:3       Static:0     Interface:1
[HUAWEI-Vlanif103] arp fixup //在接口VLANIF103上进行固化，将学习的动态ARP表项固化为静态ARP表项。
Warning: This operation may generate configuration of static ARP, and take a long time, press CTRL
+C to break. Continue?[Y/N]:y
Processing...

Info: ARP fixup is completed.
[HUAWEI-Vlanif103] display arp network 172.16.50.0 24 //固化后，查看ARP表项，设备新学习到的3条动态ARP表项已经被固化为静态ARP表项。
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-
```



```
INSTANCE
                                        VLAN/
CEVLAN
--------------------------------------------------------------------------------

172.16.50.2     0200-0000-0212          S--         GE1/0/3

103/-
172.16.50.3     0200-0000-0212          S--         GE1/0/3

103/-
172.16.50.4     0200-0000-0212          S--         GE1/0/3

103/-
172.16.50.1     00e0-0987-7895          I -
Vlanif103
--------------------------------------------------------------------------------

Total:4         Dynamic:0       Static:3     Interface:1
```

14.5 配置 ARP 代理

Proxy ARP 分类

Proxy ARP分为路由式Proxy ARP、VLAN内Proxy ARP和VLAN间Proxy ARP，如表14-1所示。

表 14-1 Proxy ARP 方式

Proxy ARP方式	适用场景
路由式Proxy ARP	需要互通的主机（主机上没有配置缺省网关）处于相同的网段但不在同一物理网络（即不在同一广播域）的场景。
VLAN内Proxy ARP	需要互通的主机处于相同网段，并且属于相同VLAN，但是VLAN内配置了端口隔离的场景。
VLAN间Proxy ARP	需要互通的主机处于相同网段，但属于不同VLAN的场景。

路由式 Proxy ARP

接口VLANIF100上配置IP地址为172.16.1.1/24，并使能路由式Proxy ARP功能。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 172.16.1.1 24
[HUAWEI-Vlanif100] arp-proxy enable
```

VLAN 内 Proxy ARP

接口VLANIF100上配置IP地址为172.16.1.1/24，并使能VLAN内Proxy ARP功能。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 172.16.1.1 24
[HUAWEI-Vlanif100] arp-proxy inner-sub-vlan-proxy enable
```


VLAN 间 Proxy ARP

接口VLANIF100上配置IP地址为172.16.1.1/24，并使能VLAN间Proxy ARP功能。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 172.16.1.1 24
[HUAWEI-Vlanif100] arp-proxy inter-sub-vlan-proxy enable
```

相关信息

技术论坛

IP与MAC一线牵之ARP

14.6 屏蔽基于源 IP 地址的 ARP Miss 告警

当某个源IP地址触发了ARP Miss告警，用户希望屏蔽此源IP地址的ARP Miss告警时，可以对这个IP地址的ARP Miss消息不进行限速。

说明

S1720GFR、S1720GW-E、S1720GWR-E、S1720X-E、S2720EI、S2750EI、S5710-C-LI、S5710-X-LI、S5700LI、S5700S-LI、S5720LI和S5720S-LI不支持该功能。

配置对IP地址为10.0.0.1的ARP Miss消息不进行限速。

```
<HUAWEI> system-view
[HUAWEI] arp-miss speed-limit source-ip 10.0.0.1 maximum 0
```

配置对所有源IP地址的ARP Miss消息不进行限速。

```
<HUAWEI> system-view
[HUAWEI] arp-miss speed-limit source-ip maximum 0
```

14.7 配置动态 ARP 检测（DAI）

动态ARP检测DAI（Dynamic ARP Inspection）功能主要用于防御中间人攻击的场景，避免设备上合法用户的ARP表项被攻击者发送的伪造ARP报文错误更新。

DAI功能是基于绑定表（DHCP动态和静态绑定表）对ARP报文进行匹配检查。

设备收到ARP报文时，将ARP报文对应的源IP地址、源MAC地址、接口、VLAN信息和绑定表的信息进行比较（比较的内容用户可以根据需要进行配置，例如可以只将ARP报文中的源IP地址和VLAN信息与绑定表的信息进行比较）：

- 如果信息匹配，说明发送该ARP报文的用户是合法用户，允许此用户的ARP报文通过。
- 否则就认为是攻击，丢弃该ARP报文。

设备上配置DHCP Snooping功能，并在设备与用户侧相连的接口上使能DAI功能。

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable ipv4
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dhcp snooping enable //设备与用户侧相连的接口使能DHCP Snooping功能。
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] interface gigabitethernet 1/0/2
```



```
[HUAWEI-GigabitEthernet1/0/2] dhcp snooping trusted //设备与DHCP Server侧相连的接口配置为信任接口。如果DHCP Snooping功能部署在DHCP中继设备上，可以不配置信任接口。
[HUAWEI-GigabitEthernet1/0/2] quit
[HUAWEI] user-bind static ip-address 10.10.10.1 vlan 100 //对于静态配置IP地址的用户，在设备上配置静态绑定表。
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] arp anti-attack check user-bind enable //设备与用户侧相连的接口使能DAI功能。
[HUAWEI-GigabitEthernet1/0/1] quit
```

设备上配置DHCP Snooping功能，并在用户侧所属VLAN内使能DAI功能。

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable ipv4
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping enable //用户设备所属VLAN内使能DHCP Snooping功能。
[HUAWEI-vlan100] quit
[HUAWEI] vlan 200
[HUAWEI-vlan200] dhcp snooping enable
[HUAWEI-vlan200] dhcp snooping trusted interface gigabitethernet 1/0/2 //设备与DHCP Server侧相连的接口配置为信任接口。如果DHCP Snooping功能部署在DHCP中继设备上，可以不配置信任接口。
[HUAWEI-vlan200] quit
[HUAWEI] user-bind static ip-address 10.10.10.1 vlan 100 //对于静态配置IP地址的用户，在设备上配置静态绑定表。
[HUAWEI] vlan 100
[HUAWEI-vlan100] arp anti-attack check user-bind enable //用户侧所属VLAN内使能DAI功能。
[HUAWEI-vlan100] quit
```

14.8 配置 ARP 防网关冲突

如果有攻击者仿冒网关，在局域网内发送源IP地址是网关IP地址的ARP报文，会导致局域网内其他用户主机的ARP表记录错误的网关地址映射关系。这样其他用户主机就会把发往网关的流量均发送给了攻击者，攻击者可轻易窃听到他们发送的数据内容，并且最终会造成这些用户主机无法访问网络。

为了防范攻击者仿冒网关，当用户主机直接接入网关时，可以在网关设备上使能ARP防网关冲突攻击功能。当设备收到的ARP报文存在下列情况之一：

- ARP报文的源IP地址与报文入接口对应的VLANIF接口的IP地址相同
- ARP报文的源IP地址是入接口的虚拟IP地址，但ARP报文源MAC地址不是VRRP虚MAC

设备就认为该ARP报文是与网关地址冲突的ARP报文，设备将生成ARP防攻击表项，并在后续一段时间内丢弃该接口收到的同VLAN以及同源MAC地址的ARP报文，这样就可以防止与网关地址冲突的ARP报文在VLAN内广播。

在网关设备上使能ARP防网关冲突攻击功能。缺省情况下设备上防网关冲突攻击功能处于未使能状态。

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack gateway-duplicate enable
```


15 常见 ACL 操作

关于本章

介绍ACL的常见操作，如删除生效时间段、删除ACL和ACL6、配置基于时间的ACL规则等。

15.1 删除生效时间段

删除生效时间段前，需要先删除关联生效时间段的ACL规则或者整个ACL。

例如，在ACL 2001中配置了rule 5，该规则关联了时间段time1。

```
#
time-range time1 from 00:00 2014/1/1 to 23:59 2014/12/31
```

```
#
acl number 2001
 rule 5 permit time-range time1
#
```

如果需要删除时间段time1，则需先删除rule 5或者先删除ACL 2001：

- 先删除rule 5，再删除time1。

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] undo rule 5
[HUAWEI-acl-basic-2001] quit
[HUAWEI] undo time-range time1
```

- 先删除ACL 2001，再删除time1。

```
<HUAWEI> system-view
[HUAWEI] undo acl 2001
[HUAWEI] undo time-range time1
```

15.2 删除 ACL 和 ACL6

- 系统视图下执行命令**undo acl** { [**number**] *acl-number* | **all** }或**undo acl name** *acl-name*，可以直接删除ACL，不受引用ACL的业务模块影响，即无需先删除引用ACL的业务配置。
- 系统视图下执行命令**undo acl ipv6** { **all** | [**number**] *acl6-number* }或**undo acl ipv6 name** *acl6-name*，可以直接删除ACL6，不受引用ACL6的业务模块影响，即无需先删除引用ACL6的业务配置。

15.3 配置基于时间的 ACL 规则

创建时间段working-time（周一到周五每天8:00到18:00），并在名称为work-acl的ACL中配置规则，在working-time限定的时间范围内，拒绝源IP地址是192.168.1.0/24网段地址的报文通过。

```
<HUAWEI> system-view
[HUAWEI] time-range working-time 8:00 to 18:00 working-day
[HUAWEI] acl name work-acl basic
[HUAWEI-acl-basic-work-acl] rule deny source 192.168.1.0 0.0.0.255 time-range working-time
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.4 配置基于源 IP 地址（主机地址）过滤报文的规则

在ACL 2001中配置规则，允许源IP地址是192.168.1.3主机地址的报文通过。


```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule permit source 192.168.1.3 0
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.5 配置基于源 IP 地址（网段地址）过滤报文的规则

在ACL 2001中配置规则，仅允许源IP地址是192.168.1.3主机地址的报文通过，拒绝源IP地址是192.168.1.0/24网段其他地址的报文通过，并配置ACL描述信息为Permit only 192.168.1.3 through。

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule permit source 192.168.1.3 0
[HUAWEI-acl-basic-2001] rule deny source 192.168.1.0 0.0.0.255
[HUAWEI-acl-basic-2001] description Permit only 192.168.1.3 through
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.6 配置基于 IP 分片信息、源 IP 地址（网段地址）过滤报文的规则

在ACL 2001中配置规则，拒绝源IP地址是192.168.1.0/24网段地址的非首片分片报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule deny source 192.168.1.0 0.0.0.255 fragment
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.7 配置基于 ICMP 协议类型、源 IP 地址（主机地址）和目的 IP 地址（网段地址）过滤报文的规则

在ACL 3001中配置规则，允许源IP地址是192.168.1.3主机地址且目的IP地址是192.168.2.0/24网段地址的ICMP报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule permit icmp source 192.168.1.3 0 destination 192.168.2.0 0.0.0.255
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.8 配置基于 TCP 协议类型、TCP 目的端口号、源 IP 地址（主机地址）和目的 IP 地址（网段地址）过滤报文的规则

- 在名称为deny-telnet的高级ACL中配置规则，拒绝IP地址是192.168.1.3的主机与192.168.2.0/24网段的主机建立Telnet连接。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl name deny-telnet
  [HUAWEI-acl-adv-deny-telnet] rule deny tcp destination-port eq telnet source 192.168.1.3 0
  destination 192.168.2.0 0.0.0.255
  ```

- 在名称为no-web的高级ACL中配置规则，禁止192.168.1.3和192.168.1.4两台主机访问Web网页（HTTP协议用于网页浏览，对应TCP端口号是80），并配置ACL描述信息为Web access restrictions。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl name no-web
  [HUAWEI-acl-adv-no-web] description Web access restrictions
  [HUAWEI-acl-adv-no-web] rule deny tcp destination-port eq 80 source 192.168.1.3 0
  [HUAWEI-acl-adv-no-web] rule deny tcp destination-port eq 80 source 192.168.1.4 0
  ```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）

- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.9 配置基于 TCP 协议类型、源 IP 地址（网段地址）和 TCP 标志信息过滤报文的规则

在ACL 3002中配置规则，拒绝192.168.2.0/24网段的主机主动发起的TCP握手报文通过，允许该网段主机被动响应TCP握手的报文通过，实现192.168.2.0/24网段地址的单向访问控制。同时，配置ACL规则描述信息分别为Allow the ACK TCP packets through、Allow the RST TCP packets through和Do not Allow the other TCP packet through。

完成以上配置，必须先配置两条permit规则，允许192.168.2.0/24网段的ACK=1或RST=1的报文通过，再配置一条deny规则，拒绝该网段的其他TCP报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 3002
[HUAWEI-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack
[HUAWEI-acl-adv-3002] display this   //如果配置规则时未指定规则编号，则可以通过此步骤查看到系统为该规则分配的编号，然后根据该编号，为该规则配置描述信息。
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack           //系统分配的规则编号是5
#
return
[HUAWEI-acl-adv-3002] rule 5 description Allow the ACK TCP packets through
[HUAWEI-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst
[HUAWEI-acl-adv-3002] display this
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack
 rule 5 description Allow the ACK TCP packets through
 rule 10 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst       //系统分配的规则编号是10
#
return
[HUAWEI-acl-adv-3002] rule 10 description Allow the RST TCP packets through
[HUAWEI-acl-adv-3002] rule deny tcp source 192.168.2.0 0.0.0.255
[HUAWEI-acl-adv-3002] display this
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack
 rule 5 description Allow the ACK TCP packets through
 rule 10 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst
 rule 10 description Allow the RST TCP packets through
 rule 15 deny tcp source 192.168.2.0 0.0.0.255       //系统分配的规则编号是15
#
return
[HUAWEI-acl-adv-3002] rule 15 description Do not Allow the other TCP packet through
```

也可以通过配置established参数，允许192.168.2.0/24网段的ACK=1或RST=1的报文通过，再配置一条deny规则，拒绝该网段的其他TCP报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 3002
[HUAWEI-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag established
[HUAWEI-acl-adv-3002] rule 5 description Allow the Established TCP packets through
[HUAWEI-acl-adv-3002] rule deny tcp source 192.168.2.0 0.0.0.255
[HUAWEI-acl-adv-3002] rule 10 description Do not Allow the other TCP packet through
```



```
[HUAWEI-acl-adv-3002] display this
#

acl number
3002

 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag
established
 rule 5 description Allow the Established TCP packets
through
 rule 10 deny tcp source 192.168.2.0
0.0.0.255
 rule 10 description Do not Allow the other TCP packet
through
#

return
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.10 配置基于源 MAC 地址（单个 MAC 地址）、目的 MAC 地址（单个 MAC 地址）和二层协议类型过滤报文的规则

- 在ACL 4001中配置规则，允许目的MAC地址是0000-0000-0001、源MAC地址是0000-0000-0002的ARP报文（二层协议类型值为0x0806）通过。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl 4001
  [HUAWEI-acl-L2-4001] rule permit destination-mac 0000-0000-0001 source-mac 0000-0000-0002 l2-
  protocol 0x0806
  ```

- 在ACL 4001中配置规则，拒绝PPPoE报文（二层协议类型值为0x8863）通过。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl 4001
  [HUAWEI-acl-L2-4001] rule deny l2-protocol 0x8863
  ```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.11 配置基于源 MAC 地址（MAC 地址段）和内层 VLAN 过滤报文的规则

在名称为deny-vlan10-mac的二层ACL中配置规则，拒绝来自VLAN10且源MAC地址在00e0-fc01-0000～00e0-fc01-ffff范围内的报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl name deny-vlan10-mac link
[HUAWEI-acl-L2-deny-vlan10-mac] rule deny vlan-id 10 source-mac 00e0-fc01-0000 ffff-ffff-0000
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

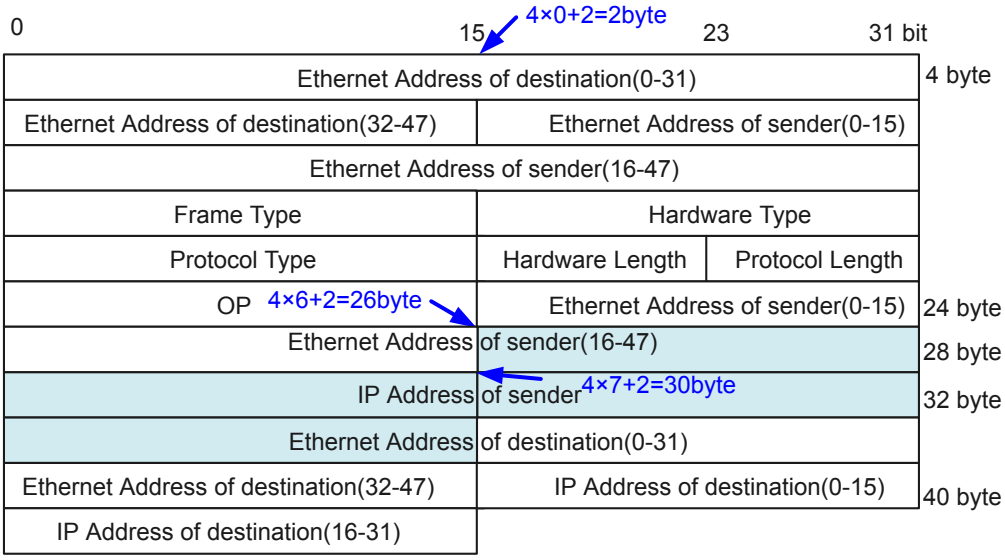
如何配置ACL

15.12 配置基于报文的二层头、偏移位置、字符串掩码和用户自定义字符串过滤报文的规则

- 在ACL 5001中配置规则，拒绝源IP地址为192.168.0.2的ARP报文通过。

  以下规则中的0x00000806是ARP帧类型，0x0000ffff是字符串掩码，10是设备内部处理不含VLAN信息的ARP报文中的协议类型字段的偏移量，c0a80002是192.168.0.2的十六进制形式，26和30分别是设备内部处理不含VLAN信息的ARP报文中源IP地址字段高两个字节和低两个字节的偏移量（ARP报文的源IP地址字段从二层头第28个字节开始占4个字节，受到用户自定义ACL规定二层头偏移位置只能是“4n+2”（n是整数）的限制，因此针对源IP地址，需要拆分成两段进行匹配，即偏移量为4×6+2=26的位置开始往后匹配4个字节的低两个字节以及偏移量为4×7+2=30的位置开始往后匹配4个字节的高两个字节）。如果要对携带VLAN信息的ARP报文进行过滤，则要将以下规则中的三个偏移量值再分别加上4。

图 15-1 ARP 报文源 IP 地址字段在二层头中的偏移量示意图




```
<HUAWEI> system-view
[HUAWEI] acl 5001
[HUAWEI-acl-user-5001] rule deny l2-head 0x00000806 0x0000ffff 10 0x0000c0a8 0x0000ffff 26
0x00020000 0xffff0000 30
```

说明

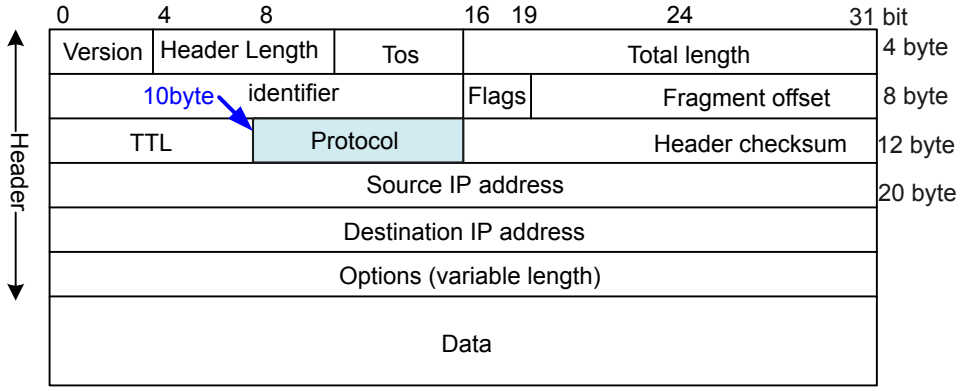
S1720GFR、S1720GW-E、S1720GWR-E、S1720X-E、S2720EI、S2750EI、S5700EI、S5700LI、S5700S-LI、S5700SI、S5710-C-LI、S5710-X-LI、S5720I-SI、S5720LI、S5720S-LI、S5720S-SI、S5720SI、S5730S-EI、S5730SI、S6720LI、S6720S-LI、S6720S-SI和S6720SI的用户自定义ACL不支持上述配置，仅支持指定一个匹配字符串。

- 在名称为deny-tcp的用户自定义ACL中配置规则，拒绝所有TCP报文通过。

  以下规则中的0x00060000是TCP协议号，8是设备内部处理IP报文中协议字段的偏移量（由于IP报文中的协议字段从IPv4头第10个字节开始占1个字节，并且受到用户自定义ACL规定IPv4头偏移位置只能是“4n”（n是整数）的限制，因此针对协议字段，需要从IPv4头偏移量为8的位置开始往后匹配4个字节的第二个高位字节）。

```
<HUAWEI> system-view
[HUAWEI] acl name deny-tcp user
[HUAWEI-acl-user-deny-tcp] rule 5 deny ipv4-head 0x00060000 0x00ff0000 8
```

图 15-2 TCP 协议字段在 IPv4 头中的偏移量示意图



相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

16 常见 QoS 操作

关于本章

介绍QoS和MQC功能的常见操作，如接口限速等。

16.1 配置接口限速（框式交换机）

配置入方向接口限速

配置名称为qoscar1的CAR模板指定限速带宽大小，并将该模板在接口GE1/0/1下应用。

```
<HUAWEI> system-view
[HUAWEI] qos car qoscar1 cir 10000 cbs 10240
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] qos car inbound qoscar1
```

配置出方向接口限速

在接口视图下执行命令**qos lr cir** *cir-value* [**cbs** *cbs-value*] [**outbound**]，对通过该接口的流量进行限速。

（可选）帧间隙和前导码配置

V200R005C00版本及后续版本开始，支持配置在计算接口限速速率时，是否包含报文的帧间隙和前导码。缺省情况下，计算接口限速的速率时包括帧间隙和前导码。用户

可以在系统视图下执行以下命令用来实现计算限速速率时不包括报文的帧间隙和前导码，从而提高限速的准确性。

- 入方向：**qos-car exclude-interframe**
- 出方向：**qos-shaping exclude-interframe**

相关信息

视频

QoS限速配置之“接口限速”

16.2 配置接口限速（盒式交换机）

配置入方向接口限速

在接口视图下执行命令**qos lr inbound cir** *cir-value* [**cbs** *cbs-value*]，对通过该接口的流量进行限速。

配置出方向接口限速

在接口视图下执行命令**qos lr outbound cir** *cir-value* [**cbs** *cbs-value*]，对通过该接口的流量进行限速。

（可选）帧间隙和前导码配置

V200R005C00版本及后续版本开始，设备支持配置在计算接口限速速率时，是否包含报文的帧间隙和前导码。缺省情况下，计算接口限速的速率时包括帧间隙和前导码。用户可以在系统视图下执行以下命令用来实现计算限速速率时不包括报文的帧间隙和前导码，从而提高限速的准确性。

- 入方向：**qos-car exclude-interframe**
- 出方向：**qos-shaping exclude-interframe**

相关信息

视频

QoS限速配置之“接口限速”

16.3 删除接口限速配置（框式交换机）

删除入方向接口限速配置

取消名称为qoscar1的CAR模板在接口GE1/0/1下的应用，并将该模板删除。

```
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] undo qos car inbound
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] undo qos car qoscar1
```


删除出方向接口限速配置

在接口视图下执行命令**undo qos lr [outbound]**，删除该接口的限速配置。

16.4 删除接口限速配置（盒式交换机）

删除入方向接口限速配置

在接口视图下执行命令**undo qos lr inbound**，删除该接口的限速配置。

删除出方向接口限速配置

在接口视图下执行命令**undo qos lr outbound**，删除该接口的限速配置。

16.5 使用流策略进行限速

根据 IP 地址进行限速

对IP地址为192.168.1.10的PC限速，带宽限制为4M。

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 192.168.1.10 0.0.0.0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match acl 2000
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] car cir 4096
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] traffic-policy p1 inbound
```

对某网段设备进行限速

对IP地址为192.168.1.0网段设备进行限速，带宽限制为50M。

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[HUAWEI-acl-basic-2000] quit
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match acl 2000
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] car cir 51200
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] traffic-policy p1 inbound
```

根据 IP 地址和协议进行限速

限制192.168.1.0网段设备访问Internet的HTTP（端口号为80）流量不超过10Mbps。


```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule permit tcp destination-port eq 80 source 192.168.1.0 0.0.0.255
[HUAWEI-acl-adv-3000] quit
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match acl 3000
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] car cir 10240
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] traffic-policy p1 inbound
```

16.6 使用流策略对报文进行过滤

禁止指定主机访问网络

禁止IP地址为192.168.1.10的PC访问网络。

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule deny source 192.168.1.10 0.0.0.0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match acl 2000
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] deny
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] traffic-policy p1 inbound
```

禁止指定网段所有设备访问网络

禁止192.168.1.0网段所有设备访问网络。

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule deny source 192.168.1.0 0.0.0.255
[HUAWEI-acl-basic-2000] quit
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match acl 2000
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] deny
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] traffic-policy p1 inbound
```

过滤指定应用协议报文

- 禁止TCP目的端口号为25的报文（SMTP）通过。
- 禁止TCP目的端口号为110的报文（POP3）通过。

- 禁止TCP目的端口号为80的报文（HTTP）通过。

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule deny tcp destination-port eq 25
[HUAWEI-acl-adv-3000] rule deny tcp destination-port eq 110
[HUAWEI-acl-adv-3000] rule deny tcp destination-port eq 80
[HUAWEI-acl-adv-3000] quit
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match acl 3000
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] deny
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] traffic-policy p1 inbound
```

16.7 使用流策略配置流量统计

配置指定主机的统计信息

配置对源MAC为0000-0000-0003的报文进行流量统计。

```
<HUAWEI> system-view
[HUAWEI] acl 4000
[HUAWEI-acl-L2-4000] rule permit source-mac 0000-0000-0003 ffff-ffff-ffff
[HUAWEI-acl-L2-4000] quit
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match acl 4000
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] statistic enable
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] traffic-policy p1 inbound
[HUAWEI-GigabitEthernet1/0/1] traffic-policy p1 outbound
```

配置对 ICMP 报文进行统计

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 0 permit icmp source 192.168.1.1 0 destination 192.168.2.1 0
[HUAWEI-acl-adv-3000] rule 5 permit icmp source 192.168.2.1 0 destination 192.168.1.1 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match acl 3000
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] statistic enable
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] traffic-policy p1 inbound
[HUAWEI-GigabitEthernet1/0/1] traffic-policy p1 outbound
```


配置对 ARP 报文进行统计

统计接口发送的ARP报文和回应的ARP报文。

```
<HUAWEI> system-view
[HUAWEI] traffic classifier arp-request
[HUAWEI-classifier-arp-request] if-match l2-protocol arp
[HUAWEI-classifier-arp-request] if-match source-mac 1111-1111-1111
[HUAWEI-classifier-arp-request] if-match destination-mac ffff-ffff-ffff
[HUAWEI-classifier-arp-request] quit
[HUAWEI] traffic classifier arp-reply
[HUAWEI-classifier-arp-reply] if-match l2-protocol arp
[HUAWEI-classifier-arp-reply] if-match source-mac 2222-2222-2222
[HUAWEI-classifier-arp-reply] if-match destination-mac 1111-1111-1111
[HUAWEI-classifier-arp-reply] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] statistic enable
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy arp-request
[HUAWEI-trafficpolicy-arp-request] classifier arp-request behavior b1
[HUAWEI-trafficpolicy-arp-request] quit
[HUAWEI] traffic policy arp-reply
[HUAWEI-trafficpolicy-arp-reply] classifier arp-reply behavior b1
[HUAWEI-trafficpolicy-arp-reply] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] traffic-policy arp-request inbound
[HUAWEI-GigabitEthernet1/0/1] traffic-policy arp-reply outbound
```

查看报文统计信息

配置通过流策略对报文进行统计之后，可以使用如下命令查看报文统计信息。

显示全局入方向应用流策略后基于匹配规则的报文统计信息。

```
<HUAWEI> display traffic policy statistics interface gigabitethernet 1/0/1 inbound verbose rule-
base

  Interface: GigabitEthernet1/0/1
  Traffic policy inbound: arp-request
  Rule number: 1
  Current status: success
  Statistics interval: 300
 -------------------------------------------------------------------------
  Classifier: arp-request operator and
  Behavior: b1
  if-match l2-protocol arp
  if-match source-mac 1111-1111-1111
  if-match destination-mac ffff-ffff-ffff
  Board : 0
 -------------------------------------------------------------------------
  Passed            |      Packets:                          0
                    |      Bytes:                            0
                    |      Rate(pps):                        0
                    |      Rate(bps):                        0
 -------------------------------------------------------------------------
  Dropped           |      Packets:                          0
                    |      Bytes:                            0
                    |      Rate(pps):                        0
                    |      Rate(bps):                        0
 -------------------------------------------------------------------------
```

说明

E3L系列单板和SA系列单板不支持基于字节的信息统计，**Bytes**和**Rate(bps)**统一显示为“-”。

17 常见 IPSG 操作

关于本章

介绍IPSG的常见操作。

17.1 配置 IP+VLAN 静态绑定

通过配置基于静态绑定表的IPSG，对非信任接口上接收的IP报文进行过滤，可以有效防止恶意主机盗用合法主机的IP地址仿冒合法主机非法访问网络。适用于局域网络中主机数较少，且主机使用静态配置IP地址的网络环境。

以添加源IP为192.168.2.1、VLAN ID为10的静态绑定表项，并在VLAN 10上使能IPSG功能为例，配置过程如下：

```
<HUAWEI> system-view
[HUAWEI] user-bind static ip-address 192.168.2.1 vlan 10
[HUAWEI] vlan 10
[HUAWEI-vlan10] ip source check user-bind enable
```

17.2 配置 IP+MAC 静态绑定

通过配置基于静态绑定表的IPSG，对非信任接口上接收的IP报文进行过滤，可以有效防止恶意主机盗用合法主机的IP地址仿冒合法主机非法访问网络。适用于局域网络中主机数较少，且主机使用静态配置IP地址的网络环境。

以添加源IP为192.168.2.1、源MAC为0002-0002-0002的静态绑定表项，并在VLAN 10上使能IPSG功能为例，配置过程如下：

```
<HUAWEI> system-view
[HUAWEI] user-bind static ip-address 192.168.2.1 mac-address 0002-0002-0002
[HUAWEI] vlan 10
[HUAWEI-vlan10] ip source check user-bind enable
```


17.3 配置 IP+MAC+接口静态绑定

通过配置基于静态绑定表的IPSG，对非信任接口上接收的IP报文进行过滤，可以有效防止恶意主机盗用合法主机的IP地址仿冒合法主机非法访问网络。适用于局域网络中主机数较少，且主机使用静态配置IP地址的网络环境。

以添加源IP为192.168.2.1、源MAC为0002-0002-0002、接口为GE0/0/1的静态绑定表项，并在VLAN 10上使能IPSG为例，配置过程如下：

```
<HUAWEI> system-view
[HUAWEI] user-bind static ip-address 192.168.2.1 mac-address 0002-0002-0002 interface
gigabitethernet 0/0/1
[HUAWEI] vlan 10
[HUAWEI-vlan10] ip source check user-bind enable
```

17.4 配置基于 DHCP Snooping 动态绑定表的 IPSG

通过配置基于DHCP Snooping动态绑定表的IPSG，对非信任接口上接收的IP报文进行过滤控制，可以有效防止恶意主机盗用合法主机的IP地址来仿冒合法主机后非法访问网络。适用于局域网络中主机较多，且主机使用DHCP动态获取IP地址的网络环境。配置过程如下：

1. 配置DHCP Snooping，生成DHCP Snooping动态绑定表。
   a. 系统视图下执行命令**dhcp enable**，全局使能DHCP功能。
   b. 系统视图下执行命令**dhcp snooping enable**，全局使能DHCP Snooping功能。
   c. 接口或VLAN视图下执行命令**dhcp snooping enable**，使能接口或者VLAN的DHCP Snooping功能。
   d. 接口视图下执行**dhcp snooping trusted**或者VLAN视图下执行**dhcp snooping trusted interface** *interface-type interface-number*，配置信任接口。

      对于从信任接口收到的IP报文，IPSG不做匹配检查且允许通过。
2. 接口或者VLAN视图下执行命令**ip source check user-bind enable**，使能IPSG功能。

以下通过示例介绍如何配置基于DHCP Snooping动态绑定表的IPSG。

配置DHCP Snooping功能，指定GE1/0/1为信任接口，并在GE0/0/2上使能IPSG。

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dhcp snooping trusted
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/2] ip source check user-bind enable
```

配置DHCP Snooping功能，指定GE1/0/1为信任接口，并在VLAN10上使能IPSG。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] port link-type trunk
[HUAWEI-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
```



```
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping enable
[HUAWEI-vlan10] dhcp snooping trusted interface gigabitethernet 1/0/1
[HUAWEI-vlan10] ip source check user-bind enable
```

17.5 删除静态绑定表项

当绑定表创建错误或者已绑定主机的网络权限变更时，需要执行命令**undo user-bind static** [{ { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **ipv6-prefix** *prefix/prefix-length* } | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]] *，删除静态绑定表项。

- 删除单条绑定表时，**undo**命令指定的参数必须和绑定表中表项完全匹配，才能删除成功。
- 支持批量删除绑定表项。例如：
  - 执行命令**undo user-bind static**，删除所有绑定表信息。
  - 执行命令**undo user-bind static interface gigabitethernet 1/0/1**，删除指定接口**GE1/0/1**的所有表项。
  - 执行命令**undo user-bind static vlan 10**，删除指定**VLAN10**的所有表项。

以下通过示例介绍如何删除静态绑定表项。

首先，通过命令**display dhcp static user-bind all**查看已存在的静态绑定表项。

```
<HUAWEI> display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                      MAC Address     VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
192.168.1.1                     0001-0001-0001  --  /--  /--    --
192.168.1.2                     0002-0002-0002  --  /--  /--    GE1/0/2
192.168.2.1                     --              --  /--  /--    GE1/0/1
192.168.2.2                     --              --  /--  /--    GE1/0/1
192.168.2.3                     --              --  /--  /--    GE1/0/1
192.168.3.1                     0004-0004-0004  10  /--  /--    --
192.168.3.2                     0005-0005-0005  10  /--  /--    --
--------------------------------------------------------------------------------
Print count:          7          Total count:          7
```

删除IP地址为192.168.1.1的静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] undo user-bind static ip-address 192.168.1.1 mac-address 0001-0001-0001
```

删除IP地址为192.168.1.2的静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] undo user-bind static ip-address 192.168.1.2 mac-address 0002-0002-0002 interface
gigabitethernet 1/0/2
```

删除GE1/0/1接口的所有静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] undo user-bind static interface gigabitethernet 1/0/1
```

删除VLAN10的所有静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] undo user-bind static vlan 10
```

以上步骤顺序执行完后，所有绑定表项均被删除。

18 常见 AAA 操作

关于本章

介绍AAA的常见操作。

18.1 配置用户通过 Telnet 登录设备的身份认证（AAA 本地认证）

背景信息

用户通过Telnet登录设备时，设备上必须配置验证方式，否则用户无法成功登录设备。设备支持不认证、密码认证和AAA认证三种用户界面的验证方式，其中AAA认证方式安全性最高。

采用AAA本地认证方式实现用户通过Telnet登录设备的身份认证，设备上需要开启Telnet服务，将用户界面（以VTY用户界面为例）的验证方式设为aaa，同时在AAA视图下创建本地用户，配置该用户的接入方式和用户级别。

```
<HUAWEI> system-view
[HUAWEI] telnet server enable  //开启Telnet服务
[HUAWEI] user-interface maximum-vty 15  //配置VTY用户界面的登录用户最大数目为15
[HUAWEI] user-interface vty 0 14  //进入0～14的VTY用户界面视图
[HUAWEI-ui-vty0-14] authentication-mode aaa  //配置VTY用户界面的验证方式为aaa
[HUAWEI-ui-vty0-14] protocol inbound telnet  //配置VTY用户界面支持的协议为Telnet，V200R006及之前版本缺省使用的协议为Telnet协议，可以不配置该项；V200R007及之后版本缺省使用的协议为SSH协议，必须配置。
[HUAWEI-ui-vty0-14] quit
[HUAWEI] aaa
```

```
[HUAWEI-aaa] local-user user1 password irreversible-cipher Huawei@1234  //创建本地用户user1并配置密码，由于配置文件中密码以密文显示，建议记住该密码，否则需要重新执行该命令覆盖配置
[HUAWEI-aaa] local-user user1 service-type telnet  //配置本地用户user1的接入类型为Telnet，该用户只能使用Telnet方式登录
[HUAWEI-aaa] local-user user1 privilege level 15  //配置本地用户user1的用户级别为15，该用户登录后可以执行0~15级的命令
[HUAWEI-aaa] quit
```

18.2 配置用户级别

用户级别与命令级别相对应，用户登录设备后只能执行命令级别等于或低于自己用户级别的命令，如用户级别为2的用户只能执行命令级别为0，1和2的命令。

用户采用AAA本地认证方式登录设备时，设备上必须配置该用户的用户级别，否则该用户的用户级别为0级（参观级），即用户登录设备后只能执行命令级别为0的命令：**ping**、**tracert**等网络诊断工具命令。如果希望该用户登录设备后可以执行命令级别更高的命令，如监控级、配置级或管理级的命令，用户必须具有更高的用户级别。

当用户的认证方式为AAA本地认证时，可以采用以下方式配置用户级别，**优先级由上到下依次降低**：

- 在AAA视图下配置单个用户的用户级别。

  ```
  <HUAWEI> system-view
  [HUAWEI] aaa
  [HUAWEI-aaa] local-user user1 privilege level 15   //配置用户user1的用户级别为15
  ```

- 在业务方案视图下配置某个域下所有用户的用户级别。

  ```
  <HUAWEI> system-view
  [HUAWEI] aaa
  [HUAWEI-aaa] service-scheme sch1
  [HUAWEI-aaa-service-sch1] admin-user privilege level 15   //配置某个域下所有用户的用户级别为15
  ```

- 在用户界面视图下配置从指定用户界面登录的用户的用户级别（以VTY用户界面为例）。缺省情况下，Console口用户界面下用户的级别是15，而VTY用户界面下用户的级别是0。

  ```
  <HUAWEI> system-view
  [HUAWEI] user-interface maximum-vty 15
  [HUAWEI] user-interface vty 0 14
  [HUAWEI-ui-vty0-14] user privilege level 15   //配置VTY 0～VTY 14用户界面下用户级别为15
  ```

说明

用户级别为1的用户仍然可以执行配置级命令，可能是因为该级别为用户界面视图下的级别，而设备在业务方案视图或AAA视图下为该用户配置了更大的级别。

18.3 配置全局默认域

对于某部门用户，管理员规划其在域“huawei”中进行认证。由于用户认证时提供的用户名经常为不带域名格式，譬如“zhangsan”，这样就导致接入设备无法将用户名上送到在“huawei”域中配置的AAA服务器上进行认证，用户无法通过认证。针对这种情况，可将全局默认域配置为“huawei”。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain huawei
[HUAWEI-aaa-domain-huawei] quit
[HUAWEI-aaa] quit
[HUAWEI] domain huawei
```


18.4 配置实时计费

实时计费功能有两种配置方法：

- 在设备上通过命令行进行配置：在用户使用的AAA计费方案视图下执行**accounting realtime** *interval*命令开启实时计费功能，并设置实时计费时间间隔。
- 通过RADIUS服务器对认证成功的用户下发RADIUS标准属性**Acct-Interim-Interval**开启实时计费功能，并设置实时计费时间间隔。

开启实时计费

上述两种方法选择任一即可开启实时计费功能。同时配置时，RADIUS标准属性**Acct-Interim-Interval**指定的实时计费时间间隔生效。

关闭实时计费

如果用户希望关闭实时计费功能，必须同时满足以下条件：

1. 设备上已执行**accounting realtime 0**命令或**undo accounting realtime**命令关闭实时计费功能。
2. RADIUS服务器未对认证成功的用户下发RADIUS标准属性**Acct-Interim-Interval**。
3. 如果RADIUS服务器已对认证成功的用户下发RADIUS标准属性**Acct-Interim-Interval**，则必须在相应的RADIUS服务器模板下执行**radius-attribute disable Acct-Interim-Interval receive send**命令禁用RADIUS标准属性**Acct-Interim-Interval**。

18.5 删除本地用户

在AAA视图下执行**undo local-user** *user-name*命令即可删除指定本地用户，包括管理员用户和普通接入用户。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] undo local-user mike
```

说明

本地用户在线时，无法删除。可以等用户不在线时，或在AAA视图下执行**cut access-user username** *user-name*命令切断该用户连接后，再删除该用户。

18.6 配置用户连接的超时时间

管理用户

对于管理用户，用户登录设备后如果长时间没有进行操作，会造成资源的浪费。此时，可以指定当用户登录设备的时间达到指定数值之后，断开该用户连接。有三种方法：

1. 在用户界面视图下执行**idle-timeout** *minutes* [*seconds*]命令配置管理用户连接的超时时间。


```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] idle-timeout 10
```

2. （仅适用于管理用户的认证方式为AAA本地认证）在AAA视图下执行**local-user** *user-name* **idle-timeout** *minutes* [*seconds*]命令配置管理用户连接的超时时间。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user1@vipdomain idle-timeout 10
```

3. （仅适用于管理用户的认证方式为RADIUS认证）通过RADIUS服务器为认证成功的用户授权RADIUS属性28（Idle-Timeout），指定管理用户连接的超时时间。

上述三种方法，方法2和方法3的优先级比方法1高。如果方法1和方法2同时配置，方法2生效；如果方法1和方法3同时配置，方法3生效。

普通接入用户

对于普通接入用户，用户接入网络后长时间没有访问网络，会造成资源的浪费。此时，可以通过以下两种方法断开普通接入用户的连接：

1. 在设备业务方案视图下执行**idle-cut** *idle-time flow-value*命令，将在超时时间内流量低于指定的流量阈值的用户连接自动断开。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme huawei
[HUAWEI-aaa-service-huawei] idle-cut 1 10
```

2. 通过RADIUS服务器为认证成功的用户授权RADIUS属性28（Idle-Timeout），指定普通接入用户连接的超时时间。

上述两种方法同时配置时，后者生效。

19 常见 NAC 操作

关于本章

介绍NAC的常见操作。

19.1 配置 MAC 旁路认证

在同时存在PC以及少量哑终端（如打印机）的网络环境中，可配置802.1X认证MAC旁路认证功能保证哑终端同样能够接入802.1X认证网络。例如接口GE1/0/1和GE1/0/5下均接有大量PC以及少量哑终端，为保证PC以及哑终端都能够接入网络，可在接口下使能802.1X认证MAC旁路认证功能。以接口GE1/0/1为例，GE1/0/5的配置与之类似。

NAC传统模式下配置MAC旁路认证功能：

- 在系统视图下对多个接口进行批量配置

```
<HUAWEI> system-view
[HUAWEI] dot1x enable
[HUAWEI] dot1x enable interface gigabitethernet 1/0/1 gigabitethernet 1/0/5
[HUAWEI] dot1x mac-bypass interface gigabitethernet 1/0/1 gigabitethernet 1/0/5
```

- 在接口视图下对每个接口进行单个配置

```
<HUAWEI> system-view
[HUAWEI] dot1x enable
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dot1x enable
[HUAWEI-GigabitEthernet1/0/1] dot1x mac-bypass
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] interface gigabitethernet 1/0/5
[HUAWEI-GigabitEthernet1/0/5] dot1x enable
[HUAWEI-GigabitEthernet1/0/5] dot1x mac-bypass
```

NAC统一模式下配置MAC旁路认证功能：

- 对于V200R009C00之前的版本

  需要在接口下同时配置802.1X和MAC认证，并且802.1X认证配置在前。


```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] authentication dot1x mac-authen
[HUAWEI-GigabitEthernet1/0/1] quit
```

- 对于V200R009C00及其之后的版本

  需要在认证模板下同时绑定802.1X接入模板和MAC接入模板，并且配置命令**authentication dot1x-mac-bypass**。之后将认证模板绑定到接口上。

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] quit
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] quit
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] mac-access-profile m1
[HUAWEI-authen-profile-p1] dot1x-access-profile d1
[HUAWEI-authen-profile-p1] authentication dot1x-mac-bypass
[HUAWEI-authen-profile-p1] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] authentication-profile p1
[HUAWEI-GigabitEthernet1/0/1] quit
```

相关信息

技术论坛

一个门卫的故事（一）

一个门卫的故事（二）

19.2 配置 Guest VLAN 功能

为了满足用户不进行认证即能访问某些网络资源需求，譬如下载客户端软件、升级客户端、更新病毒库等，可配置Guest VLAN功能。例如为保证接口GE1/0/1和GE1/0/5下的用户能够实时更新病毒库，可在接口下是配置Guest VLAN功能。假设病毒库服务器在VLAN10中。

说明

交换机V200R005C00及其之后版本，仅NAC传统模式支持Guest VLAN功能。

- 在系统视图下对多个接口进行批量配置

```
<HUAWEI> system-view
[HUAWEI] dot1x enable
[HUAWEI] dot1x enable interface gigabitethernet 1/0/1 gigabitethernet 1/0/5
[HUAWEI] authentication guest-vlan 10 interface gigabitethernet 1/0/1 gigabitethernet 1/0/5
```

- 在接口视图下对每个接口进行单个配置

```
<HUAWEI> system-view
[HUAWEI] dot1x enable
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dot1x enable
[HUAWEI-GigabitEthernet1/0/1] authentication guest-vlan 10
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] interface gigabitethernet 1/0/5
[HUAWEI-GigabitEthernet1/0/5] dot1x enable
[HUAWEI-GigabitEthernet1/0/5] authentication guest-vlan 10
```

相关信息

技术论坛

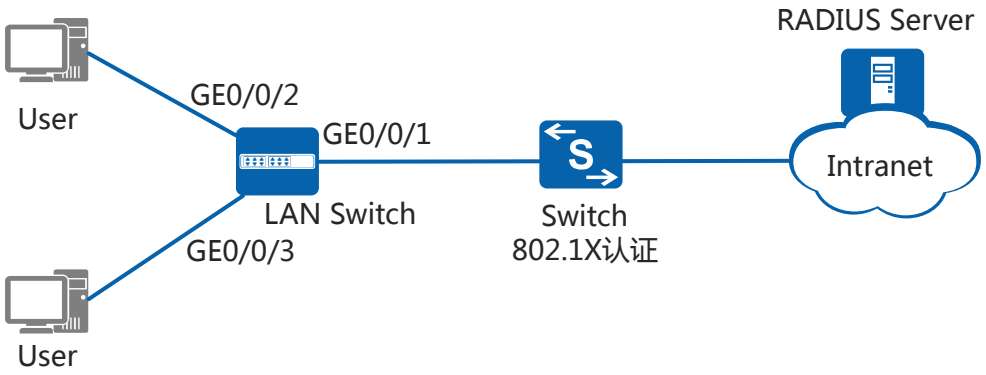
一个门卫的故事（一）

一个门卫的故事（二）

19.3 配置 802.1X 认证报文二层透明传输功能

802.1X认证过程中的EAP协议报文，是一种BPDU报文。对于BPDU报文，华为公司的交换机设备当前缺省是不做二层转发的。因此如果使能802.1X的设备和用户之间还存在二层交换机，就必须在其上配置二层透明传输，否则用户发送的EAP报文将无法到达认证设备，用户自然无法通过认证。

图 19-1 配置 802.1X 认证报文二层透明传输功能示意图



如图19-1所示，使能802.1X认证的接入设备Switch与用户之间存在二层交换机LAN Switch，为保证用户的802.1X认证报文能够通过LAN Switch到达Switch，需要在LAN Switch上进行如下配置（二层交换机以S5700LI为例进行说明）。

```
<HUAWEI> system-view
[HUAWEI] sysname LAN Switch
[LAN Switch] l2protocol-tunnel user-defined-protocol dot1x protocol-mac 0180-c200-0003 group-mac 0100-0000-0002   //group-mac不能设置为保留的组播MAC地址（0180-C200-0000～0180-C200-002F）以及其他几种特殊MAC地址，其余MAC地址均可。
[LAN Switch] interface gigabitethernet 0/0/1 //需要在二层交换机连接上行网络以及用户的所有接口上进行配置
[LAN Switch-GigabitEthernet0/0/1] l2protocol-tunnel user-defined-protocol dot1x enable
[LAN Switch-GigabitEthernet0/0/1] bpdu enable
[LAN Switch-GigabitEthernet0/0/1] quit
[LAN Switch] interface gigabitethernet 0/0/2
[LAN Switch-GigabitEthernet0/0/2] l2protocol-tunnel user-defined-protocol dot1x enable
[LAN Switch-GigabitEthernet0/0/2] bpdu enable
[LAN Switch-GigabitEthernet0/0/2] quit
[LAN Switch] interface gigabitethernet 0/0/3
[LAN Switch-GigabitEthernet0/0/3] l2protocol-tunnel user-defined-protocol dot1x enable
[LAN Switch-GigabitEthernet0/0/3] bpdu enable
[LAN Switch-GigabitEthernet0/0/3] quit
```

相关信息

技术论坛

一个门卫的故事（一）

一个门卫的故事（二）

19.4 限制 802.1X 认证接口可以学习的 MAC 地址数量

由于802.1X认证功能与**mac-limit**命令（配置接口能够学习的最大MAC地址数量）以及**mac-address learning disable**命令（关闭接口的MAC地址学习功能）冲突，因此当接口使能802.1X认证功能之后，无法再通过执行**mac-limit**命令和**mac-address learning disable**命令限制接口可以学习的MAC地址数量，下面是几种替代方法。

NAC 传统模式

- （适用于所有版本）通过限制接口下允许接入的802.1X认证用户数量，从而限制该接口可以学习的MAC地址数量。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x max-user 3
```

- （适用于V200R012及之后版本）在接口下配置端口安全功能，并限制该接口能够学习的MAC地址数量。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security max-mac-num 3
```

NAC 统一模式

- （适用于V200R005-V200R008版本）通过限制接口下允许接入的用户数量，从而限制该接口可以学习的MAC地址数量。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1]  authentication mode multi-authen max-user 3
```

- （适用于V200R009及之后版本）通过在认证模板下配置允许接入的802.1X认证用户数量并将该模板应用到指定接口，从而限制该接口可以学习的MAC地址数量。

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] quit   //缺省的802.1X认证方式为EAP中继认证
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] dot1x-access-profile d1
[HUAWEI-authen-profile-p1] authentication mode multi-authen max-user 3 dot1x
[HUAWEI-authen-profile-p1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication-profile p1
```

- （适用于V200R012及之后版本）在接口下配置端口安全功能，并限制该接口能够学习的MAC地址数量。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security max-mac-num 3
```


20 常见 VRRP 操作

关于本章

介绍VRRP的常见操作。

20.1 使能虚拟 IP 地址 ping 功能

使能虚拟IP地址ping功能。

```
<HUAWEI> system-view
[HUAWEI] vrrp virtual-ip ping enable
```

20.2 配置 VRRP 与接口状态联动

配置VRRP与接口状态联动实现VRRP主备切换。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 10.1.1.1 24
[HUAWEI-Vlanif10] vrrp vrid 1 virtual-ip 10.1.1.3
```

```
[HUAWEI-Vlanif10] vrrp vrid 1 track interface gigabitethernet 1/0/1 reduced 40
[HUAWEI-Vlanif10] quit
```

20.3 配置 VRRP 与 BFD 联动

配置VRRP与BFD联动实现VRRP快速切换。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 10.1.1.1 24
[HUAWEI-Vlanif10] vrrp vrid 1 virtual-ip 10.1.1.3
[HUAWEI-Vlanif10] quit
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atob bind peer-ip 10.1.1.2 interface vlanif 10
[HUAWEI-bfd-session-atob] discriminator local 1
[HUAWEI-bfd-session-atob] discriminator remote 2
[HUAWEI-bfd-session-atob] min-rx-interval 100
[HUAWEI-bfd-session-atob] min-tx-interval 100
[HUAWEI-bfd-session-atob] commit
[HUAWEI-bfd-session-atob] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] vrrp vrid 1 track bfd-session 1 increased 40
[HUAWEI-Vlanif10] quit
```

20.4 配置 VRRP 与 NQA 联动

配置VRRP与NQA联动实现VRRP主备切换。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 10.1.1.1 24
[HUAWEI-Vlanif10] vrrp vrid 1 virtual-ip 10.1.1.3
[HUAWEI-Vlanif10] quit
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] destination-address ipv4 10.20.1.2
[HUAWEI-nqa-user-test] frequency 15
[HUAWEI-nqa-user-test] start now
[HUAWEI-nqa-user-test] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] vrrp vrid 1 track nqa user test reduced 40
[HUAWEI-Vlanif10] quit
```

20.5 配置 VRRP 与路由联动

配置VRRP与路由联动实现VRRP主备切换。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 10.1.1.1 24
[HUAWEI-Vlanif10] vrrp vrid 1 virtual-ip 10.1.1.3
[HUAWEI-Vlanif10] vrrp vrid 1 track ip route 10.20.1.0 24 reduced 40
[HUAWEI-Vlanif10] quit
```

20.6 配置 VRRP 协议版本号

配置VRRP协议版本号。


```
<HUAWEI> system-view
[HUAWEI] vrrp version v3
```

20.7 配置 VRRP 抢占模式

配置 VRRP 抢占模式为非抢占方式

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] vrrp vrid 1 preempt-mode disable
```

配置 VRRP 抢占模式为抢占方式

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] vrrp vrid 1 preempt-mode timer delay 20
```

20.8 配置 VRRP 报文在 Super-VLAN 中的发送方式

配置VRRP报文在Super-VLAN中的发送方式。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp advertise send-mode 10
```

20.9 配置 MAC 刷新 ARP 功能

在以太网中，MAC地址表项用于指导设备进行二层数据转发，ARP表项通过IP地址和MAC地址的映射指导设备进行不同网段间的通信。

MAC地址表项的出接口通过报文触发刷新的，ARP表项的出接口是在老化时间到后通过老化探测进行刷新的。这样就可能会出现MAC表项和ARP表项出接口不一致的情况，即MAC地址表项的出接口已刷新，而ARP表项的出接口没有及时刷新的情况。此时可以使能MAC刷新ARP的功能，在MAC地址表项出接口刷新时，直接刷新ARP表项的出接口。

配置MAC刷新ARP功能。

```
<HUAWEI> system-view
[HUAWEI] mac-address update arp
```


21 常见 SNMP 操作

关于本章

介绍SNMP的常见操作。

21.1 限制网管对设备的管理

为了确保设备的安全性，可以通过ACL、MIB视图和ACL与MIB视图的组合三种方式限制网管对设备的管理。

ACL

通过配置ACL，可以限制能够管理设备的网管。ACL可以是基本ACL，对于V200R09C00或之后版本的设备，ACL还可以是高级ACL。

1. 创建ACL 2001。仅允许IP地址在192.168.1.0/24网段的报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule permit source 192.168.1.0 0.0.0.255
[HUAWEI-acl-basic-2001] rule deny source any
[HUAWEI-acl-basic-2001] quit
```

2. 将ACL 2001作为过滤规则，即设备仅允许IP地址在192.168.1.0/24网段的网管管理设备。

网管使用的SNMP协议版本	配置方法
SNMPv1或SNMPv2c	[HUAWEI] snmp-agent community write cipher market acl 2001
SNMPv3	● 基于单个SNMPv3用户： [HUAWEI] snmp-agent usm-user v3 acl 2001 ● 基于SNMPv3用户组： [HUAWEI] snmp-agent group admin privacy acl 2001
任一SNMP协议版本	[HUAWEI] snmp-agent acl 2001

MIB 视图

通过配置MIB视图，可以限制网管能够管理的设备上的MIB节点范围。

1. 创建MIB视图alliso，该MIB视图包含iso节点及其所有子节点。
   ```
   <HUAWEI> system-view
   [HUAWEI] snmp-agent mib-view included alliso iso
   ```
2. 将MIB视图alliso作为过滤规则，即设备仅允许网管管理iso节点及其所有子节点。

网管使用的SNMP协议版本	配置方法
SNMPv1或SNMPv2c	[HUAWEI] snmp-agent community write cipher market mib-view alliso
SNMPv3	仅支持基于用户组进行配置： [HUAWEI] snmp-agent group admin privacy write-view alliso

ACL 和 MIB 视图的组合

对于使用SNMPv1或SNMPv2c协议的网管，可以同时使用ACL和MIB视图限制网管对设备的管理。

- 第一种组合方式：先配置**ACL**，再配置**MIB视图**；或者先配置**MIB视图**，再配置**ACL**。
- 第二种组合方式：对于使用SNMPv1或SNMPv2c协议的网管，可以通过同时指定ACL和MIB视图对网管进行限制。
  ```
  [HUAWEI] snmp-agent community write cipher market mib-view alliso acl 2001
  ```

21.2 配置 SNMP 的版本和团体名

SNMP有三个版本分别是v1、v2c和v3。v1和v2c版本支持配置团体名，v3版本不支持。配置团体名的时候可以应用访问控制，限制网管对设备的访问。

- SNMPv1

  SNMP的版本号为v1，读写团体名为community001，并应用访问控制。

```
<HUAWEI> system-view
[HUAWEI] snmp-agent sys-info version v1
[HUAWEI] snmp-agent community write community001 mib-view alliso acl 2001
```

- SNMPv2c

  SNMP的版本号为v2c，读写团体名为community001，并应用访问控制。

```
<HUAWEI> system-view
[HUAWEI] snmp-agent sys-info version v2c
[HUAWEI] snmp-agent community write community001 mib-view alliso acl 2001
```

21.3 配置用户组和用户名

仅v3版本支持配置用户组和用户名，v1和v2c版本不支持，设备缺省情况下使能SNMPv3。

在配置安全级别时，用户的安全级别需要高于或等于用户组的安全级别。安全级别按照安全性从高到低为：

- privacy：认证并加密
- authentication：认证不加密
- none：不认证不加密

即如果用户组是privacy级别，用户和告警主机就必须是privacy级别；用户组是authentication级别，用户和告警主机可以是privacy或者authentication级别。

- V200R003C00之前版本

  # 配置用户组名为group001，安全级别为privacy，并应用访问控制，限制网管对设备的访问。

```
<HUAWEI> system-view
[HUAWEI] snmp-agent group v3 group001 privacy write-view alliso acl 2001
```

  # 配置用户名为user001，认证密码为Authe1234，加密密码为Priva1234。

```
<HUAWEI> system-view
[HUAWEI] snmp-agent usm-user v3 user001 group001 authentication-mode sha Authe1234 privacy-mode des56 Priva1234
```

- V200R003C00及后续版本

  # 配置用户组名为group001，安全级别为privacy，并应用访问控制，限制网管对设备的访问。

```
<HUAWEI> system-view
[HUAWEI] snmp-agent group v3 group001 privacy write-view alliso acl 2001
```

  # 配置用户名为user001，认证密码为Authe@1234，加密密码为Priva@1234。

```
<HUAWEI> system-view
[HUAWEI] snmp-agent usm-user v3 user001 group group001
[HUAWEI] snmp-agent usm-user v3 user001 authentication-mode sha
Please configure the authentication password (8-64)
Enter Password:                 //输入认证密码Authe@1234
Confirm Password:               //输入认证密码Authe@1234
[HUAWEI] snmp-agent usm-user v3 user001 privacy-mode aes256
Please configure the privacy password (8-64)
Enter Password:                 //输入加密密码
Priva@1234
Confirm Password:               //输入加密密码Priva@1234
```


21.4 配置 SNMP Trap 功能

配置逻辑

打开指定模块的告警开关，并指定SNMP Trap主机（即接收Trap报文的网管）后，当该模块产生告警时，设备会主动通过SNMP Trap报文将告警信息发送至网管。

配置示例

1. 打开ARP模块的告警开关。

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name arp
```

说明

如需了解更多信息，请参见**21.7 打开或关闭指定模块的告警开关**和**21.6 查看指定模块的告警开关状态**。

2. 执行**snmp-agent trap source**命令配置设备发送SNMP Trap报文的源地址。

```
[HUAWEI] interface loopback 0
[HUAWEI-LoopBack0] ip address 10.1.1.1 32
[HUAWEI-LoopBack0] quit
[HUAWEI] snmp-agent trap source loopback 0   //配置设备以Loopback 0接口的地址作为发送SNMP Trap报文的源IP地址
```

3. 执行**snmp-agent target-host trap**命令指定接收SNMP Trap报文的网管。

```
[HUAWEI] snmp-agent target-host trap address udp-domain 10.1.2.10 udp-port 50000 params securityname user001 v3 privacy
```

21.5 删除团体名

删除团体名时，和团体名一起配置的信息也会被删除。由于团体名以密文的形式保存在设备上，因此可以使用两种方式删除团体名。

- 明文形式删除

  需要牢记团体名，团体名输入错误会导致删除失败。

```
<HUAWEI> system-view
[HUAWEI] undo snmp-agent community community001
```

- 密文形式删除

  密文形式删除之前需要先查询加密后的团体名。

```
<HUAWEI> system-view
[HUAWEI] display snmp-agent community
   Community name:%^%#v_@eE"TW3Yw"7"Q2Vd!"/$XsX|}+GOBz8V.pEh>=x9)J,Tuy}3Mp#
+X4QV5CAI^:Z;NlA3*&ta4}a53-%^%#
       Group name:%^%#v_@eE"TW3Yw"7"Q2Vd!"/$XsX|}+GOBz8V.pEh>=x9)J,Tuy}3Mp#
+X4QV5CAI^:Z;NlA3*&ta4}a53-%^%#
       Acl:
2001


       Storage-type: nonVolatile
[HUAWEI] undo snmp-agent community %^%#v_@eE"TW3Yw"7"Q2Vd!"/$XsX|}+GOBz8V.pEh>=x9)J,Tuy}3Mp#
+X4QV5CAI^:Z;NlA3*&ta4}a53-%^%#
```

21.6 查看指定模块的告警开关状态

交换机已配置SNMP告警功能，而部分告警无法在网管上接收到，则有可能是因为交换机并未打开该告警开关，即交换机不会向网管发送该告警。在任意视图下执行**display**

snmp-agent trap feature-name *feature-name* **all**命令可以查看指定模块的告警开关状态。如需打开或关闭指定模块的告警开关，请参见**21.7 打开或关闭指定模块的告警开关**。

查看TRUNK模块的告警开关状态。

```
<HUAWEI> display snmp-agent trap feature-name trunk all
-------------------------------------------------------------------------------
Feature name: TRUNK
Trap number : 4
-------------------------------------------------------------------------------
Trap name                       Default switch status   Current switch status
hwExtLinkDown                   off                     on
hwExtLinkUp                     off                     on
hwExtAllMemberDownNotify        off                     on
hwExtAllMemberDownResume        off                     on
-------------------------------------------------------------------------------
```

表 21-1 display snmp-agent trap feature-name 命令输出信息描述

项目	描述
Feature name	产生告警的特性名称。
Trap number	该特性下包含的告警数量。
Trap name	告警名称。
Default switch status	缺省告警开关状态： ● on：打开，表示交换机会向网管发送该告警。 ● off：关闭，表示交换机不会向网管发送该告警。
Current switch status	当前告警开关状态： ● on：打开，表示交换机会向网管发送该告警。 ● off：关闭，表示交换机不会向网管发送该告警。 该状态可通过命令**snmp-agent trap enable feature-name**配置。

21.7 打开或关闭指定模块的告警开关

需求	命令
一次性打开所有模块的告警开关	**snmp-agent trap enable**
一次性关闭所有打开的告警开关	**snmp-agent trap disable**
打开指定模块下的所有告警开关	**snmp-agent trap enable feature-name**

需求	命令
关闭指定模块下的所有告警开关	**undo snmp-agent trap enable feature-name**
打开指定模块下的指定告警开关	**snmp-agent trap enable feature-name** *feature-name* **trap-name** *trap-name*
关闭指定模块下的指定告警开关	**undo snmp-agent trap enable feature-name** *feature-name* **trap-name** *trap-name*
一次性恢复所有模块的告警开关至缺省状态	**undo snmp-agent trap disable**或**undo snmp-agent trap enable**

说明

如需查看指定模块的告警开关状态，请参见**21.6 查看指定模块的告警开关状态**。

打开ARP模块下的所有告警开关。

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name arp
```

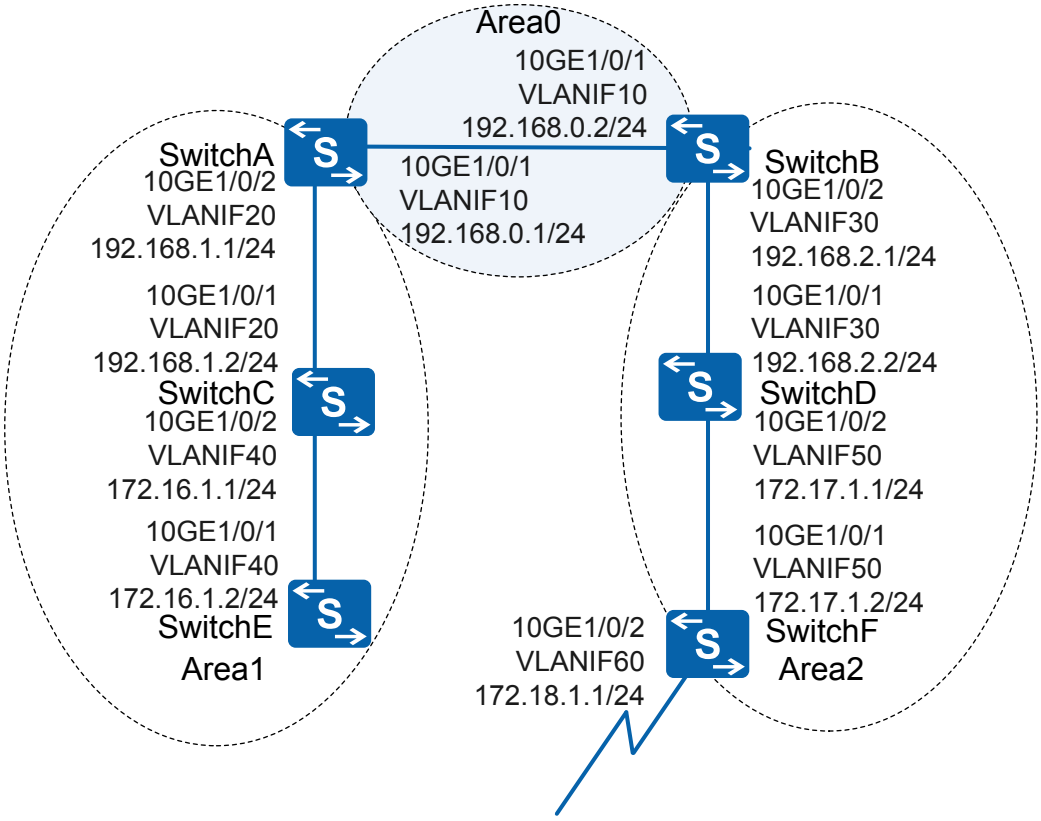
打开DHCP模块下的所有告警开关。

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name dhcp
```


22 常见 OSPF 操作

以如图22-1所示的OSPF网络，介绍OSPF功能的一些常见操作。

图 22-1 OSPF 基本网络示意图



配置 OSPF 基本功能

SwitchA为例，其他交换机都是相似的配置步骤。

```
<SwitchA> system-view
[SwitchA] ospf 1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255      //使能VLANIF10的OSPF功能
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] area 1
```

```
[SwitchA-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255     //使能VLANIF20的OSPF功能
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

配置 STUB 区域

STUB区域的ABR不传播它们接收到的自治系统外部路由，在这些区域中路由器的路由表规模以及路由信息传递的数量都会大大减少。一般将OSPF网络的边缘区域配置为STUB区域。例如：将Area1配置为STUB区域。

SwitchA为例，Area1内其他交换机都是相似的配置步骤。

```
[SwitchA] ospf 1
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] stub
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

配置 NSSA 区域

NSSA区域与STUB区域相同的是，ABR不会传播来源于其他区域的自治系统外部路由信息；不同的是，它本身能够引入自治系统外部路由并传播到整个OSPF自治域中。一般将OSPF网络中有与其他自治系统相连的边缘区域配置为NSSA区域。例如：将Area2配置为NSSA区域。

SwitchB为例，Area2内其他交换机都是相似的配置步骤。

```
[SwitchB] ospf 1
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] nssa
[SwitchB-ospf-1-area-0.0.0.2] quit
[SwitchB-ospf-1] quit
```

配置 OSPF 引入其他路由

当OSPF网络中的设备需要访问运行其他协议的网络中的设备时，需要将其他协议的路由引入到OSPF网络中。例如：将SwitchF的直连路由引入到OSPF网络中。

```
[SwitchF] ospf 1
[SwitchF-ospf-1] import-route direct
[SwitchF-ospf-1] quit
```

配置 OSPF 的接口开销

缺省情况下，OSPF会根据接口的带宽自动计算其开销值。也可以手动设置接口的开销值。例如：将SwitchA的接口VLANIF20开销值设置为5。

```
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ospf cost 5
[SwitchA-Vlanif20] quit
```

配置 OSPF 与 BFD 联动

如果需要提高链路状态变化时OSPF的收敛速度，可以在运行OSPF的链路上配置BFD特性。当BFD检测到链路故障时，能够将故障通告给路由协议，触发路由协议的快速收敛；当邻居关系为Down时，则动态删除BFD会话。

例如：在SwitchA与SwitchB之间的OSPF链路上建立BFD会话。

配置SwitchA


```
[SwitchA] bfd
[SwitchA-bfd] quit
[SwitchA] ospf 1
[SwitchA-ospf-1] bfd all-interfaces enable
[SwitchA-ospf-1] quit
```

配置SwitchB

```
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] ospf 1
[SwitchB-ospf-1] bfd all-interfaces enable
[SwitchB-ospf-1] quit
```

配置 OSPF 发布缺省路由

OSPF实际组网应用中，区域边界和自治系统边界通常都是由多个交换机组成的多出口冗余备份或者负载分担。此时，为了减少路由表的容量，可以配置缺省路由，保证网络的高可用性。

OSPF缺省路由的发布方式取决于引入缺省路由的区域类型。如表22-1所示。

表 22-1 缺省路由发布方式

区域类型	产生条件	发布方式	产生LSA的类型	泛洪范围
普通区域	通过**default-route-advertise**命令配置	ASBR发布	Type5 LSA	普通区域
STUB区域	自动产生	ABR发布	Type3 LSA	STUB区域
NSSA区域	通过**nssa** [**default-route-advertise**]	ASBR发布	Type7 LSA	NSSA区域
完全NSSA区域	自动产生	ABR发布	Type3 LSA	NSSA区域

相关信息

技术论坛

问鼎OSPF系列技术贴