# 目录

# 第 1 章 基本管理命令

## 1.1 交换机基本配置

### 1.1.1 基本配置

#### 1.1.1.1 authentication line login

**命令：authentication line {console | vty | web} login {local | radius | tacacs}**

**no authentication line {console | vty | web} login**

**功能：** 配置 VTY（即指 Telnet 和 ssh 登录方式）、Web 和 Console 方式对登录用户的验证方式和验证选择优先级；该命令的 no 命令恢复缺省验证方式。

**缺省情况：** 缺省 Console 登陆方式为没有任何登录验证，缺省 VTY 与 Web 登录方式默认为本地验证。

**命令模式：** 全局配置模式。

**使用指南：** Console、VTY 与 Web 登录可以分别设置相应的登录验证方法，其验证方式可以选择 Local、RADIUS 和 TACACS 的任意组合。当采用组合验证方式时，在最前面的验证方式优先级最高，并依次递减；如果高优先级方式验证通过，则直接允许用户登陆，并忽略后面的验证方式。需要注意的是：只要有一种验证方式收到相应协议的明确回应，无论是拒绝还是接收，都不再尝试下一种验证方式（例外的是，local 验证方式失败时，必然会尝试下一种验证方式）；若未收到相应协议的明确回应，则尝试下一种验证方式。当使用 RADIUS 验证时，必须使能 AAA 功能并配置 RADIUS 服务器。当使用 TACACS 验证时，必须配置 TACACS 服务器。

authentication line console login 命令与 login 命令互斥。authentication line console login 命令配置 Console 的登录验证方法，而 login 命令使能 password 命令配置的 Console 登录验证。

即使配置了本地选项，如果没有配置任何本地用户，Console 方式可以直接登录交换机。

举例： 配置 Telnet 和 ssh 登录的验证方式为 RADIUS。

Switch(config)#authentication line vty login **radius**

相关命令：aaa **enable，radius-server authentication host，tacacs-server authentication host， tacacs-server key**

#### 1.1.1.2 banner

**命令：banner motd *<LINE>***

**no banner motd**

**功能：**该命令用来配置使用 telnet 或通过 console 等方式登陆交换机认证成功时显示的欢迎信息，本命令的 no 操作设置认证成功时不显示信息。

**参数：** <LINE>：用户认证成功时显示的欢迎信息，长度限制为 1-256 个字符。

**命令模式：** 全局配置模式。

**缺省情况：** 缺省认证成功时不显示欢迎信息。

**举例：** Switch(config)#banner motd Welcome

## 1.1.1.3 boot img

**命令：boot img <img-file-url> {primary | backup}**

**功能：** 配置主控卡下次启动时的第一、第二 img 文件。

**参数：** primary 表示配置第一启动 IMG 文件，backup 表示配置第二启动 IMG 文件，**<img-file-url>** 为启动 IMG 文件全路径。IMG 文件全路径的格式要求如下：

1.文件路径由相当于根目录的设备前缀（flash:/）和文件名两部分组成。每一部分内不允许有空格存在，每两部分之间也不允许有空格存在。

2.文件名必须以.img 为后缀。

3. 文件全路径不能超过 128 个字符，文件名部分不能超过 80 个字符。

命令模式： 特权用户配置模式。

缺省情况： 出厂配置时只有第一启动 IMG 文件，即 FLASH 中的 nos.img 文件。第二启动 IMG 文件为空。

举例：

1.设置系统下次启动的第二启动 IMG 文件为 flash:/nos.img。

Switch#boot img flash:/nos.img backup

2.设置系统下次启动的第一启动 IMG 文件为 flash:/5.4.128.0_nos.img。

Switch#boot img flash:/5.4.128.0_nos.img primary

## 1.1.1.4 boot startup-config

**命令：boot startup-config {NULL | <file-url>}**

**功能：** 配置主控板卡下次启动的 CFG 文件。

**参数说明：** NULL 关键字表示下次启动时以出厂缺省配置来启动。当配置下次启动的 CFG 文件为 NULL 时相当于执行 set default 和 write 两条命令。<file-url>为下次启动的 CFG 文件全路径。CFG 文件全路径的格式要求如下：

1. 路径由相当于根目录的设备前缀（flash:/）和文件名两部分组成，每一部分内及每两部分之间不允许有空格存在。

2. 配置文件必须以.cfg 为后缀。

3. 文件全路径不能超过 128 个字符，文件名部分不能超过 80 个字符。

命令模式： 特权用户配置模式。

缺省情况： 无。

**举例：**

1.设置系统下次启动的 CFG 文件为 flash:/ startup.cfg。

Switch# boot startup-config flash:/ startup.cfg

2.设置系统下次启动的 CFG 文件为 flash:/ test-trunk.cfg。

Switch#boot startup-config flash:/ test-trunk.cfg

## 1.1.1.5 clock set

**命令：clock set *<HH:MM:SS> <YYYY.MM.DD>***

**功能：**设置系统日期和时钟。

**参数：*<HH:MM:SS>***为当前时钟，***HH*** 取值范围为 0~23，***MM*** 和 ***SS*** 取值范围为 0~59；***<YYYY.MM.DD>***为当前年、月和日，***YYYY*** 取值范围为 2001~2037，***MM*** 取值范围为 1~12，***DD*** 取值范围为 1~31。

**命令模式：**特权用户配置模式。

**缺省情况：**系统启动时缺省为 2006 年 1 月 1 日 0：0：0。

**使用指南：**交换机在断电后不能继续计时，因此在要求使用确切时间的应用环境中，必须先设定交换机当前的日期和时间。

**举例：**设置交换机当前日期为 2002 年 8 月 1 日 23 时 0 分 0 秒。

Switch#clock set 23:0:0 2002.8.1

**相关命令：show clock**

## 1.1.1.6 config

**命令：config [terminal]**

**功能：**从特权用户配置模式进入到全局配置模式。

**参数：[terminal]**表示进行终端配置。

**命令模式：**特权用户配置模式。

**举例：**

Switch#config

## 1.1.1.7 debug ssh-server

**命令：debug ssh-server**

**no debug ssh-server**

**功能：**打开 SSH 服务器的调试信息；本命令的 no 操作为关闭 SSH 服务器的调试信息。

**缺省情况：**缺省调试开关是关闭的。

**命令模式：**特权用户配置模式。

### 1.1.1.8 disable

**命令：disable**

**功能：**关闭特权模式。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权用户配置模式。

**使用指南：**

**举例：**

Switch#disable

Switch>

### 1.1.1.9 enable

**命令：enable [<*1-15*>]**

**功能：**用户使用 **enable** 命令，从普通用户配置模式进入特权用户配置模式，或者切换用户权限级别。

**命令模式：**一般用户配置模式/特权用户配置模式。

**缺省情况：**无。

**使用指南：**为了防止非特权用户的非法访问，在从普通用户配置模式进入到特权用户配置模式时，要进行用户身份验证，即需要输入特权用户口令，输入正确的口令，则进入特权用户配置模式，否则保持普通用户配置模式不变；或者，当从权限较高的级别切换至权限较低的级别时，不进行相应级别口令验证；从权限较低的级别切换至权限较高的级别时，需要验证相应级别的口令。特权用户口令的设置为全局配置模式下的命令 **enable password**。

**举例：**

Switch>enable

Switch#

### 1.1.1.10 enable password

**命令：enable password [level <*1-15*>] [0 | 7] <*password*>**

**no enable password [level <*1-15*>]**

**功能：**修改从普通用户配置模式进入特权用户配置模式的口令。

**参数：level <*1-15*>**用于指定权限级别，默认为 15 级。**<*password*>**为用户设置的密码，在设置密码时，若输入选项为 0，则应输入明文密码，且不对输入的明文密码进行加密处理；若输入选项为 7，则应输入明文密码加密后的密文字符串。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省的特权用户口令为空。

**使用指南：**配置特权用户口令，可以防止非特权用户的非法侵入，建议网络管理员在首次配置交换机时就设定特权用户口令。另外当管理员需要长时间离开终端屏幕时，最好执行 exit 命令退出特权用户配置模式。

### 1.1.1.11 end

**命令：end**

**功能：**当前处于非一般用户配置模式或特权用户配置模式时，使用该命令可以直接退回到特权用户配置模式。

**命令模式：**一般用户配置模式和特权用户配置模式之外的其它模式。

**举例：**从 VLAN 配置模式退回到特权模式。

Switch(config-vlan1)#end

Switch#

### 1.1.1.12 exec-timeout

**命令：exec-timeout *<minutes>* [*<seconds>*]**

**no exec-timeout**

**功能：**设置退出特权用户配置模式超时时间，本命令的 no 操作为恢复缺省值。

**参数：*<minute>***为时间值，单位为分钟，取值范围为 0~35791。

***<seconds>***为时间值，单位为秒，取值范围为 0~59。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省为 10 分钟。

**使用指南：**为确保交换机使用的安全性，防止非法用户的恶意操作，当特权用户在做完最后一项配置后，开始计时，到达设置时间值时，系统就自动退出特权用户配置模式。用户如果想再次进入特权用户配置模式，需要再次输入特权用户密码和口令。当设置超时时间为 0 时，停止超时计时器。

**举例：**设置交换机退出特权用户配置模式的超时时间为 6 分钟。

Switch(config)#exec-timeout 6

设置交换机退出特权用户配置模式的超时时间为 5 分 30 秒：

Switch(config)#exec-timeout 5 30

### 1.1.1.13 exit

**命令：exit**

**功能：**从当前模式退出，进入上一个模式，如在全局配置模式使用本命令退回到特权用户配置模式，在特权用户配置模式使用本命令退回到一般用户配置模式等。

**命令模式：**各种配置模式。

**举例：**

Switch#exit

Switch>

## 1.1.1.14 help

**命令：help**

**功能：**输出有关命令解释器帮助系统的简单描述。

**命令模式：**各种配置模式。

**使用指南：**交换机提供随时随地的在线帮助，help 命令则显示关于整个帮助体系的信息，包括完全帮助和部分帮助，用户可以随时随地键入’?’获取在线帮助。

**举例：**

switch(config)#help

CLI provides advanced help feature. When you need help,

anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup

until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a

command argument (e.g. 'show ?') and describes each possible

argument.

2. Partial help is provided when an abbreviated argument is entered

and you want to know what arguments match the input

(e.g. 'show ve?'.)

## 1.1.1.15 hostname

**命令：hostname *<hostname>***

**no hostname**

**功能：**设置交换机命令行界面的提示符，本命令的 no 操作为删除该设置。

**参数：*<hostname>***为提示符的字符串，最长不超过 64 个字符。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省提示符和交换机型号有关。

**使用指南：**通过本命令用户可以根据实际情况设置交换机命令行的提示符。

**举例：**设置提示符为 Test。

Switch(config)#hostname Test

Test(config)#

## 1.1.1.16 ip host

**命令：ip host *<hostname> <ip_addr>***

**no ip host {*<hostname>* | all}**

**功能：**设置主机与 IP 地址映射关系；本命令的 no 操作为删除该项映射关系。

**参数：*<hostname>***为主机名称，最长不超过 64 个字符；***<ip_addr>***为主机名相应 IP 地址，点分十进制格式；**all** 为所有主机地址。

**命令模式：**全局配置模式。

**使用指南：**设置一个确定的主机和 IP 地址的对应关系，可用于如“**ping host *<hostname>***”等命令中。

**举例：**设置主机名为 beijing 的主机的 IP 地址为 200.121.1.1。

Switch(config)#ip host beijing 200.121.1.1

**相关命令：telnet、ping、traceroute**

## 1.1.1.17 ipv6 host

**命令：ipv6 host *<hostname> <ipv6_addr>***

**no ipv6 host { *<hostname>* | all}**

**功能：** 设置主机与 IPv6 地址映射关系；本命令的 no 操作为删除该项映射关系。

**参数：** ***<hostname>*** 为主机名称，最长不超过 64 个字符； ***<ipv6_addr>*** 为主机名相应 IPv6 地址； **all** 为所有主机地址。

**命令模式：** 全局配置模式。

**使用指南：** 设置一个确定的主机和 IPv6 地址的对应关系，可用于如 **traceroute6 <host>** 等命令中。

**举例：** 设置主机名为 beijing 的主机的 IPv6 地址为 2001:1:2:3::1。

Switch(config)#ipv6 host beijing 2001:1:2:3::1

**相关命令： ping6、traceroute6**

## 1.1.1.18 ip http server

**命令：ip http server**

**no ip http server**

**功能：**使能 Web 配置；本命令的 no 操作为关闭 Web 配置。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省为 web server 是开启的。

**使用指南：**Web 配置是给用户提供一个以 HTTP 方式配置的界面。Web 配置的优点是配置直观、形象，容易理解。本命令的作用相当于在 Setup 配置模式的主菜单中选择[3]，进行 Web Server 的配置。

**举例：**打开 Web Server 功能，使能 Web 配置。

Switch(config)#ip http server

## 1.1.1.19 language

**命令：language {chinese | english}**

**功能：**设置显示的帮助信息的语言类型。

**参数：chinese** 为中文显示；**english** 为英文显示。

**命令模式：**特权和配置模式。

**缺省情况：**系统缺省英文显示。

**使用指南：**用户可根据自己的喜好选择语言类型。系统若重启后，帮助显示信息恢复为英文显示。

## 1.1.1.20 login

**命令：login**

**no login**

**功能：login** 使能密码验证，**no login** 取消 login 的设置。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省为 no login。

**使用指南：**该命令使 console 进入一般用户配置模式时，必须键入 password 命令设置的密码，否则不能进入该模式，no login 取消该限制。

**举例：**使能密码验证：

Switch(config)#login

## 1.1.1.21 login-fail retry-times<0-10> lock-time <1-120>

**命令:**login-fail retry-time<0-10>

**功能:** 设置允许输入错误密码的次数

**参数:**<0-10>次, <1-120>f 分钟

**命令模式：**全局配置模式

**缺省情况:**缺省值为 0

**举例:**

Switch(config)#login-fail retry-times 9 lock-time 2

## 1.1.1.22 password

**命令：password [0 | 7] *<password>***

**no password**

**功能：**设置用户在 console 上进入一般用户配置模式时的口令，该命令的 no 形式删除配置的口令。

**参数：**password 为用户设置的密码，在设置密码时，若输入选项为 0，则应输入明文密码，且不对输入的明文密码进行加密处理；若输入选项为 7，则应输入明文密码加密后的密文字符串。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省该口令为空。

**使用指南：**如果配置了该口令，并且设置了 login 命令后，在 console 上进入一般用户配置模式时，需要验证该口令，才能进入一般用户配置模式。

**举例：**

Switch(config)#password 0 test

Switch(config)#login

## 1.1.1.23 privilege

**命令：privilege mode level <*1-15*> LINE**

**no privilege mode level <*1-15*> LINE**

**功能：**为选定的命令配置指定的优先级；本命令的 no 操作为恢复命令的初始优先级。

**参数：**mode 为要配置的命令的注册模式，“Tab”或者“？”可以显示所有注册模式

<*1-15*>为要设置的优先级，有效范围为 1-15

LINE 为要设置的命令，支持命令的缩写格式

**命令模式：**全局配置模式

**使用指南：**该命令不能修改命令本身；LINE 必须为完整的命令格式，命令的缩写格式必须是能够解析成功的命令，对于不完整的命令、书写错误的命令、缩写不能正确解析的命令，配置失败；对于修改带参数的命令行，要按照命令行要求的格式填好参数，参数可以任意选择。no 命令中的 level 级别可以随便设置，不对结果产生影响。使用 no 命令时，LINE 必须是配置过的命令行，如果是带参数的命令行，参数要完全匹配。（配置了 enable 命令的分级后，请再添加“authentication line console login local”并配置对应权限的用户名密码，以保证其可以再次进入特权模式。如果通过其他登陆方式配置完成后，console 的连接已经在一般用户模式了请再次输入“exit”或“quit”，其就能提示用户输入用户名密码重新进入特权模式。）

**举例：**修改命令 show ip route 至 5 级。

Switch(config)#privilege exec level 5 show ip route

修改命令 peer A.B.C.D 至 6 级。

Switch(config)#privilege router-msdp level 6 peer 1.2.3.4

恢复 show ip route 的优先级至初始状态。

Switch(config)#no privilege exec level 5 show ip route

恢复 peer A.B.C.D 的优先级至初始状态。

Switch(config)#no privilege router-msdp level 6 peer 1.2.3.4

## 1.1.1.24 privilege mode level <1-15> all

**命令：privilege mode level <1-15> all**

**no privilege mode level all**

**功能：** 为选定模式下的所有命令配置指定的优先级；本命令的 no 操作为恢复命令的初始优先级。

**参数：** mode 为要配置的命令的注册模式，'Tab'或者'？'可以显示所有注册模式

<1-15>为要设置的优先级，有效范围为 1-15

**命令模式：** 全局配置模式

**使用指南：** 该命令不修改 enable、end、exit、help 命令的优先级，如有需要，可使用 privilege mode level <1-15> LINE 命令单独做修改。

**举例：** 修改全局配置模式下的命令至 15 级。

Switch(config)#privilege config level 15 all

恢复全局配置模式下的命令优先级至初始状态。

Switch(config)#no privilege config level al

## 1.1.1.25 reload

**命令：reload**

**功能：**热启动交换机。

**命令模式：**特权用户配置模式。

**使用指南：**用户可以通过本命令，在不关闭电源的情况下，重新启动交换机。

## 1.1.1.26 service password-encryption

**命令：service password-encryption**

**no service password-encryption**

**功能：**加密系统密码，no 命令取消加密。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省为 no service password-encryption。

**使用指南：**执行该命令后，对当前配置的 password，enable password，ip ftp 命令，以及 username 的未加密的密码进行加密，同时，对以后配置的该命令的密码进行加密处理。no service password-encryption，则取消该功能，但已经加密后的密码仍然保持加密。

**举例：**加密系统密码：

Switch(config)#service password-encryption

## 1.1.1.27 service terminal-length

**命令：service terminal-length <0-512>**

**no service terminal-length**

**功能：**设置终端（vty）的每屏显示字符行数，no 命令取消换屏操作。

**参数：**vty 的每屏显示字符行数，取值范围为 0-512。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省的行数为 25。

**使用指南：**设置终端每屏的显示行数，设置该命令后，新连接的 telnet,ssh 客户端，以及 Console，其每屏显示行数为该设置。

**举例：**设置 vty 线程数为 20：

Switch(config)#service terminal-length 20

## 1.1.1.28 service user password valid-time <0-90>

**命令：**service user password valid-time <0-90>

**功能:** 设置口令生存周期

**参数: <0-90>**天

**命令模式：**全局配置模式

**缺省情况:**缺省值为 0

**举例:**

Switch(config)#service user password valid-time 10

## 1.1.1.29 sysContact

**命令：sysContact <LINE>**

**no sysContact**

**功能：**设置厂商联系方式，本命令的 no 操作为恢复初始配置。

**参数：**<LINE>为提示符的字符串，范围 0-255 个字符。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省为出厂模式。

**使用指南：**通过本命令用户可以根据实际情况设置交换机厂商的联系方式。

**举例：**设置厂商联系方式为 test。

Switch(config)#sysContact test

## 1.1.1.30 sysLocation

**命令：sysLocation <LINE>**

**no sysLocation**

**功能：**设置厂商地址，本命令的 no 操作为恢复初始配置。

**参数：**<LINE>为提示符的字符串，范围 0-255 个字符。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省为出厂模式。

**使用指南：**通过本命令用户可以根据实际情况设置交换机厂商的地址。

**举例：**设置厂商地址为 test。

Switch(config)#sysLocation test

## 1.1.1.31 set default

**命令：set default**

**功能：**恢复交换机的出厂设置。

**命令模式：**特权用户配置模式。

**使用指南：**恢复交换机的出厂设置，即用户对交换机做的所有配置都消失，用户重新启动交换机后，出现的提示与交换机首次上电一样。

**注意：**配置本命令后，必须执行 **write** 命令，进行配置保留后重启交换机即可使交换机恢复到出厂设置。

**举例：**

Switch#set default

Are you sure? [Y/N] = y

Switch#write

Switch#reload

## 1.1.1.32 set boot password

**命令：set boot password**

**功能：**设置进入 boot 命令行的密码

**命令模式：**全局配置模式

**使用指南：**如果之前没有设置过密码，可以直接设置新密码，如果之前设置过密码，需要先输入旧密码，然后才能输入新密码

**注意：**配置本命令后，重启按住 crtl+b 进入 boot 的时候，需要输入密码，密码请妥善保管。

**举例：**

Switch(config)#set boot password

Old password :***

Wrong password, please enter again!

Old password :*****

New password :*****

Confirm password :*****

Set password success!

## 1.1.1.33 setup

**命令：setup**

**功能：**进入交换机的 Setup 配置模式。

**命令模式：**特权用户配置模式。

**使用指南：**在 Setup 配置模式下用户可进行 IP 地址、Web 服务等的配置。

## 1.1.1.34 show clock

**命令：show clock**

**功能：**显示系统当前的时钟。

**命令模式：**特权和配置模式。

**使用指南：**用户可以通过查看系统日期和时钟，发现如果系统时间有误，可及时调整。

**举例：**

switch(config)#show clock

Current time is Sun Feb 07 14:24:38 2021 [UTC]

**相关命令：clock set**

## 1.1.1.35 show cpu usage

**命令：show cpu usage [<slotno>]**

**功能：**显示CPU使用率。

**命令模式：**特权和配置模式。

**使用指南：**通过 show cpu usage 命令可以查看当前 CPU 资源的使用情况。参数 slotno 只在机架式交换机上使用，用于显示指定槽位号上的板卡 CPU 使用率，不带参数时默认为本卡。

**举例：**显示本卡当前CPU使用率。

Switch#show cpu usage

Last 5 second CPU IDLE: 87%

Last 30 second CPU IDLE: 89%

Last 5 minute CPU IDLE: 89%

From running CPU IDLE: 89%

## 1.1.1.36 show cpu utilization

**命令：show cpu utilization**

**功能：**显示当前 CPU 的使用率。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**该命令显示 CPU 在过去 5 秒，30 秒，5 分钟的使用率。

**举例：**

在交换机上显示 CPU 使用率

Switch#show cpu utilization

Last 5 second CPU USAGE: 9%
Last 30 second CPU USAGE: 11%
Last 5 minute CPU USAGE: 11%
From running CPU USAGE: 11%

## 1.1.1.37 show memory usage

**命令：show memory usage [<slotno>]**
**功能：**显示内存使用率。
**命令模式：**特权和配置模式。
**使用指南：**通过show memory usage命令可以查看当前内存资源的使用情况。参数slotno只在机架式交换机上使用，用于显示指定槽位号上的板卡内存使用率，不带参数时默认为本卡。
**举例：**显示本卡当前内存使用率。
switch(config)#show memory usage

The memory total 1024 MB , free 504987648 bytes , usage is 52.97%

## 1.1.1.38 show privilege

**命令：show privilege**
**功能：**显示当前用户权限。
**参数：**无。
**命令模式：**各种配置模式。
**举例：**显示当前用户权限。
Switch(Config)#show privilege
Current privilege level is 15

## 1.1.1.39 show privilege mode LINE

**命令：show privilege mode LINE**
**功能：**显示指定命令的优先级。
**参数：**mode 为要配置的命令的注册模式，“Tab”或者“？”可以显示所有注册模式
LINE 为要设置的命令，支持命令的缩写格式
**命令模式：**特权和配置模式
**使用指南：**LINE 必须为完整的命令格式，命令的缩写格式必须是能够解析成功的命令，对于不完整的命令、书写错误的命令、缩写不能正确解析的命令，不能显示级别。
**举例：**显示命令 **privilege** 的优先级。

Switch(config)#show privilege exec show ip route

The command : show ip route

Privilege is : 15

## 1.1.1.40 show tcam usage

**命令：show tcam usage**

**功能：**显示系统 acl 资源信息

**参数：**无

**命令模式：**各种配置模式

**使用指南：**该命令用于查看当前系统里面的 ACL 资源信息

**举例：**查看当前系统的 ACL 资源使用情况，unit 表示芯片单元，一般为 0；block id 表示 acl 资源使用的 block 号，一般为 0-31；phase 表示 acl 应用的位置，eacl 表示出口方向、vlan 表示与 vlan 相关的 acl，ingress 表示入口方向；used entry 表示使用的 acl 资源数；free entry 表示未使用的 acl 资源数；status 表示当前的状态，free 表示没有使用，L4 Protocol 表示给相关协议使用了。

Switch(config)#show tcam usage

----------Member:1----------

| unit | block id | phase | used entry | free entry | status |
|---|---|---|---|---|---|
| 0 | 0 | eacl | 0 | 128 | Free |
| 0 | 1 | eacl | 0 | 128 | Free |
| 0 | 2 | eacl | 0 | 128 | Free |
| 0 | 3 | eacl | 0 | 128 | Free |
| 0 | 4 | eacl | 0 | 128 | Free |
| 0 | 5 | eacl | 0 | 128 | Free |
| 0 | 6 | eacl | 0 | 128 | Free |
| 0 | 7 | eacl | 0 | 128 | Free |
| 0 | 8 | eacl | 0 | 128 | Free |
| 0 | 9 | eacl | 0 | 128 | Free |
| 0 | 10 | eacl | 0 | 128 | Free |
| 0 | 11 | eacl | 0 | 128 | Free |
| 0 | 12 | eacl | 0 | 128 | Free |
| 0 | 13 | eacl | 0 | 128 | Free |
| 0 | 14 | eacl | 0 | 128 | Free |
| 0 | 15 | eacl | 0 | 128 | Free |
| 0 | 16 | eacl | 0 | 128 | Free |
| 0 | 17 | eacl | 0 | 128 | Free |
| 0 | 18 | eacl | 0 | 128 | Free |
| 0 | 19 | eacl | 0 | 128 | Free |

| | | | | | |
|---|---|---|---|---|---|
| 0 | 20 | eacl | 0 | 128 | Free |
| 0 | 21 | eacl | 0 | 128 | Free |
| 0 | 22 | eacl | 0 | 128 | Free |
| 0 | 23 | eacl | 0 | 128 | Free |
| 0 | 24 | eacl | 0 | 128 | Free |
| 0 | 25 | eacl | 0 | 128 | Free |
| 0 | 26 | vlan | 0 | 128 | Free |
| 0 | 27 | vlan | 0 | 128 | Free |
| 0 | 28 | vlan | 0 | 128 | Free |
| 0 | 29 | vlan | 0 | 128 | Free |
| 0 | 30 | ingress | 40 | 88 | L4 Protocol |
| 0 | 31 | ingress | 48 | 80 | L4 Protocol |

Free Block :30

Used entry total :88

Free entry total :4008

## 1.1.1.41 show temperature

命令：show **temperature**

**功能：** 显示交换机 CPU 当前温度。

**参数：** 无。

**命令模式：** 各种配置模式

**使用指南：** 该命令用于监测交换机 CPU 的温度。

**举例：** 显示交换机 CPU 当前温度。

switch(config)#show temperature

Temperature: 30C/86F

## 1.1.1.42 show tech-support

**命令：show tech-support [no-more]**

**功能：**显示交换机运行的信息和各任务的状态，技术支持人员利用该命令，诊断交换机的运行是否正常。

**参数：no-more:** 直接全部显示交换机运行的信息和各任务的状态，不通过 more 进行用户交互。

**命令模式：**特权和配置模式。

**使用指南：**在交换机出现运行故障时，可以利用该命令获取相关信息，诊断故障原因。

**举例：**

Switch#show tech-support

## 1.1.1.43 show version

**命令：show version**

**功能：**显示交换机版本信息。

**命令模式：**特权和配置模式。

**参数：**无。

**使用指南：** 通过使用此命令来查看交换机的版本信息，包括硬件版本和软件版本信息。

**举例：**

Switch#show version

## 1.1.1.44 username

**命令：username *<username>* [privilege *<privilege>*] [password [0 | 7] *<password>*]**

**no username *<username>***

**功能：**在本地设置利用用户名和密码验证方式登录的用户及其优先级。

**参数：*<username>***为用户名，取值范围不超过 32 字符；***<privilege>***为该用户可执行的命令的最大等级，级别为 1-15，缺省级别为 1；***<password>***为用户密码，如果在设定密码时，输入选项为 0，则应输入明文密码，且不对输入的明文密码进行加密处理；若输入选项 7，则应输入明文密码加密后的密文字符串（使用 MD5 加密的 32 位密码）。

**命令模式：**全局配置模式。

**使用指南：**目前系统中注册的命令有两个优先级 1 和 15。优先级为 1 的命令注册在一般用户配置模式。优先级为 15 的命令注册在除一般用户配置模式以外的其它模式。本命令最多允许配置 16 个本地认证用户，密码最大长度为 32。

**注意：**用户利用该命令配置完毕可登录的用户和优先级，在执行 authentication line console login local 命令（使能 Console 登录方式的本地用户验证）以前，必须确保有一个用户的优先级为 15，以便能够利用该用户进行登录，并进入特权模式和全局配置模式，修改系统的配置。当配置的本地用户没有一个权限达到 15，并且 Console 登录验证方式仅仅配置了 Local 方式时，通过 Console 可以直接登录交换机而不需要验证。在以 HTTP 方式访问交换机时，必须使用执行命令等级为 15 的用户登录交换机，优先级低于 15 的用户登录必会被拒绝。

**举例：**配置一个管理员用户 admin，优先级为 15，配置两个普通用户，优先级为 1，并启用本地用户名和密码登录认证方式。

其中只有用户 admin 可以通过 Telnet 或 Console 登录至特权模式下，user1 与 user2 的只能通过 Telnet 或 Console 登录至一般用户配置模式。HTTP 登录方式下，只有 admin 才能登录成功，user1 与 user2 的登录权限均不足。

Switch(config)#username admin privilege 15 password 0 admin

Switch(config)#username user1 privilege 1 password 7 4a7d1ed414474e4033ac29ccb8653d9b(该密码为 0000 使用 MD5 加密的 32 位暗文密码)

Switch(config)#username user2 password 0 user2

Switch(config)#authentication line console login local

## 1.1.1.45 web-auth privilege <1-15>

**命令：web-auth privilege <1-15>**

**no web-auth privilege**

**功能：**设置 web 登录交换机的级别。

**参数：<1-15>：**指定通过 web 登录交换机的级别，范围是 1-15。

**命令模式：**全局配置模式。

**缺省情况：**缺省级别是 15。

**使用指南：**设置 web 登录交换机的级别后，只有高于或等于该级别的用户才能通过 web 登录上交换机。

**举例：**设置通过 web 登录交换机的级别为 10。

Switch(config)# web-auth privilege 10

## 1.1.1.46 write

**命令：write**

**功能：**将当前运行时配置参数保存到 Flash Memory。

**命令模式：**特权用户配置模式。

**使用指南：**当完成一组配置，并且已经达到预定功能，应将当前配置保存到用户指定的配置恢复文件中，以便因不慎关机或断电时，系统可以自动恢复到原先保存的配置。相当于 **copy running-config startup-config** 命令。

## 1.1.1.47 write running-config

**命令：write running-config [<*startup-config-file-name*>]**

**功能：**将交换机当前运行参数保存名称为任意名称的.cfg 文件，保存到 Flash Memory。

**参数：**<*startup-config-file-name*>为 cfg 文件全路径。cfg 文件全路径的格式要求如下：

1. 路径由相当于根目录的设备前缀（flash:/）和文件名两部分组成，每一部分内及每两部分之间不允许有空格存在。

2. 配置文件必须以.cfg 为后缀。

3. 文件全路径不能超过 128 个字符，文件名部分不能超过 76 个字符。

**命令模式：**特权用户配置模式。

**使用指南：**保存到 Flash Memory 的配置文件可以被选择作为启动配置文件。

**举例：**将交换机当前运行参数保存为文件名为 123 的.cfg 文件。

Switch#write running-config 123.cfg

## 1.1.2 远程管理

### 1.1.2.1 aaa authorization config-commands

**命令：aaa authorization config-commands**

**no aaa authorization config-commands**

**功能：**对 VTY（即指 Telnet 和 ssh 登录方式）登录用户开启命令授权功能，相应 no 命令关闭命令授权功能。只有开启了此功能并且配置了命令授权方法，执行某个命令时才会要求进行授权。

**缺省情况：**缺省对 VTY 登录用户没有开启命令授权功能。

**命令模式：**全局配置模式。

**使用指南：**只有配置了该命令并配置了 VTY 登录用户的命令授权方式和授权选择优先级之后，对于 VTY 登陆用户配置相应命令级别的命令时才进行授权。

**举例：**开启 VTY 命令授权功能。

Switch(config)# aaa authorization config-commands

### 1.1.2.2 accounting command

**命令：accounting line {console | vty} command *<1-15>* none method1 [method2…]**

**no accounting line {console | vty} command *<1-15>***

**功能：**配置 VTY（即指 Telnet 和 ssh 登录方式）和 Console 方式命令活动记账方法列表；该命令的 no 命令恢复缺省记账方式。

**参数：line** 参数为记账线路选择，包括 **console** 和 **vty**（包括 telnet 和 ssh）；**command *<1-15>*** 参数表示记账命令的级别；**none** 表示不发送记账开始和记账停止；**method** 参数为记账方法列表，目前仅支持 **tacacs** 关键字，**tacacs** 表示使用 TACACS+远程服务器进行记账。

**缺省情况：**缺省没有记账方式。

**命令模式：**全局配置模式。

**使用指南：console** 和 **vty** 登录可以分别设置相应的命令活动记账方法，其记账方式目前仅支持 TACACS+方式。

**举例：**配置 telnet 远程登录后命令活动记账。

Switch(config)#authorization line vty command 15 tacacs

### 1.1.2.3 accounting exec

**命令：accounting line {console | vty} exec {start-stop | stop-only | none} method1 [method2…]**

**no accounting line {console | vty} exec**

**功能：**配置 VTY（即指 Telnet 和 ssh 登录方式）和 Console 方式用户登录的记账方法列表；该命令的 no 命令恢复缺省记账方式。

**参数：line** 参数为记账线路选择，包括 **console** 和 **vty**（包括 telnet 和 ssh）；**start-stop** 表示在用户登录时发送记账开始，在用户退出登录时发送记账停止，**stop-only** 表示仅仅在用户退出登录时发送记账停止，**none** 表示不发送记账开始和记账停止；**method** 参数为记账方法列表，目前仅支持 **tacacs** 关键字，**tacacs** 表示使用 TACACS+远程服务器进行记账。

**缺省情况：**缺省无需记账。

**命令模式：**全局配置模式。

**使用指南：console** 和 **vty** 登录可以分别设置相应的登录记账方法，其记账方式目前仅支持 TACACS+方式。

**举例：**配置 telnet 远程登录记账。

Switch(config)#accounting line vty exec start-stop tacacs

### 1.1.2.4 authentication enable

**命令：authentication enable method1 [method2…]**

**no authentication enable**

**功能：**配置用户 enable 认证方法列表；该命令的 no 命令恢复缺省验证方式。

**参数：method** 参数为认证方法列表，必须为 **local**、**tacacs** 和 **radius** 关键字其中之一。**local** 表示使用本地数据库进行认证，**tacacs** 表示使用 TACACS+远程认证服务器进行认证，**radius** 表示使用 RADIUS 远程认证服务器进行认证。

**缺省情况：**缺省 enable 命令默认为本地验证。

**命令模式：**全局配置模式。

**使用指南：**enable 认证方式可以选择 **local**、**radius**、**tacacs** 的任意组合。当采用组合验证方式时，在最前面的验证方式优先级最高，并依次递减；如果高优先级方式验证通过，则直接允许用户登陆，并忽略后面的验证方式。需要注意的是：只要有一种验证方式收到相应协议的明确回应，无论是拒绝还是接受，都不再尝试下一种验证方式（例外的是，local 验证方式失败时，必然会尝试下一种验证方式）；若未收到相应协议的明确回应，则尝试下一种验证方式。当使用 RADIUS 验证时，必须使能 AAA 功能并配置 RADIUS 服务器。当 使用 TACACS 验证时，必须配置 TACACS 服务器。

**举例：**配置 enable 认证方式为 tacacs 和 local。

Switch(config)#authentication enable tacacs local

### 1.1.2.5 authentication ip access-class

**命令：authentication ip access-class {<num-std>|<name>}**

**no authentication ip access-class**

**功能：**为 Telnet/SSH/Web 登录方式绑定标准的 IP ACL 规则；本命令的 no 操作为取消绑定 ACL。

**参数：**<num-std>为标准数字 ACL 的访问表标号，取值范围为<1-99>；<name>为标准命名 ACL 的访问表标名，字符串长度为 1-32。

**缺省情况：**系统默认关闭 Telnet/SSH/Web 绑定 ACL 功能。

**命令模式：**全局配置模式

**举例：**绑定标号为 1 的数字标准 ACL 规则。

Switch(config)#authentication ip access-class 1 in

## 1.1.2.6 authentication ipv6 access-class

**命令：authentication ipv6 access-class {<num-std>|<name>} in**

**no authentication ipv6 access-class**

**功能：**为 Telnet/SSH/Web 登录方式绑定标准的 IPv6 ACL 规则；本命令的 no 操作为取消绑定 ACL。

**参数：**<num-std>为标准数字 ACL 的访问表标号，取值范围为<500-599>；<name>为标准命令 ACL 的访问表标名，字符串长度为 1-64。

**缺省情况：**系统默认关闭 Telnet/SSH/Web 绑定 ACL 功能。

**命令模式：**全局配置模式

**举例：**绑定标号为 500 的数字标准 ACL 规则。

Switch(config)#authentication ipv6 access-class 500 in

## 1.1.2.7 authentication line login

**命令：authentication line {console | vty | web} login method1 [method2…]**

**no authentication line {console | vty | web} login**

**功能：**配置 VTY（即指 Telnet 和 ssh 登录方式）、Web 和 Console 方式对登录用户的认证方法列表；该命令的 no 命令恢复缺省认证方式。

**参数：line** 参数为登录线路选择，包括 **console**、**vty**（包括 telnet 和 ssh）和 **web**；**method** 参数为认证方法列表，必须为 **local**、**tacacs** 和 **radius** 关键字其中之一。**local** 表示使用本地数据库进行认证，**tacacs** 表示使用 TACACS+远程认证服务器进行认证，**radius** 表示使用 RADIUS 远程认证服务器进行认证。

**缺省情况：**缺省 **console** 登陆方式无需登录验证，缺省 **vty** 与 **web** 登录方式默认为本地验证。

**命令模式：**全局配置模式。

**使用指南：**Console、VTY 与 Web 登录可以分别设置相应的登录验证方法，其验证方式可以选择 Local、RADIUS 和 TACACS 的任意组合。当采用组合验证方式时，在最前面的验证方式优先级最高，并依次递减；如果高优先级方式验证通过，则直接允许用户登陆，并忽略后面的验证方式。需要注意的是：只要有一种验证方式收到相应协议的明确回应，无论是拒绝还

是接收，都不再尝试下一种验证方式（例外的是，local 验证方式失败时，必然会尝试下一种验证方式）；若未收到相应协议的明确回应，则尝试下一种验证方式。当使用 RADIUS 验证时，必须使能 AAA 功能并配置 RADIUS 服务器。当使用 TACACS 验证时，必须配置 TACACS 服务器。

authentication line console login 命令与 login 命令互斥。authentication line console login 命令配置 Console 的登录验证方法，而 login 命令使能 password 命令配置的 Console 登录验证。

即使配置了本地选项，如果没有配置任何本地用户，Console 方式可以直接登录交换机。

**举例：**配置通过 RADIUS 远程验证 telnet 和 ssh 登录用户。

Switch(config)#authentication line vty login radius

**相关命令：aaa enable，radius-server authentication host，tacacs-server authentication host，tacacs-server key**

## 1.1.2.8 authentication securityip

**命令：authentication securityip <*ip-addr*>**

**no authentication securityip <*ip-addr*>**

**功能：**配置允许使用 Telnet 和 HTTP 方式登录交换机的安全 IP 地址；本命令的 no 操作为删除指定的安全 IP 地址。

**参数：<*ip-addr*>** 可以访问本交换机的安全 IP 地址，点分十进制格式。

**缺省情况：**系统缺省不配置任何安全 IP 地址。

**命令模式：**全局配置模式。

**使用指南：**没有配置安全 IP 地址前，不限制登录交换机的 IP 地址；配置安全 IP 地址后，只有安全 IP 地址的主机才能够登录到交换机进行配置。交换机允许配置最多 32 个安全 IP 地址。

**举例：**设置 192.168.1.21 为安全 IP 地址。

Switch(config)#authentication securityip 192.168.1.21

## 1.1.2.9 authentication securityipv6

**命令：authentication securityipv6 <*ipv6-addr*>**

**no authentication securityipv6 <*ipv6-addr*>**

**功能：** 配置允许使用 Telnet 和 HTTP 方式登录交换机的用户安全 IPv6 地址；本命令的 no 操作为删除指定的安全 IPv6 地址。

**参数：** **<*ipv6-addr*>** 可以访问本交换机的安全 IPv6 地址。

**缺省情况：** 系统缺省不配置任何安全 IPv6 地址。

**命令模式：** 全局配置模式。

**使用指南：** 没有配置安全 IPv6 地址前，不限制登录交换机的 IPv6 地址；配置安全 IPv6 地址后，只有安全 IPv6 地址的主机才能够登录到交换机进行配置。交换机允许配置最多 32 个安全 IPv6 地址。

**举例：** 设置 2001:da8:123:1::1 为安全 IPv6 地址。

Switch(config)#authentication securityipv6 2001:da8:123:1::1

## 1.1.2.10 authorization

**命令：authorization line {console | vty | web} exec method1[method2…]**

**no authorization line {console | vty | web} exec**

**功能：**配置 VTY（即指 Telnet 和 ssh 登录方式）、Web 和 Console 方式登录用户的授权方法列表；该命令的 no 命令恢复缺省授权方式。

**参数：line** 参数为授权线路选择，包括 **console**、**vty**（包括 telnet 和 ssh）和 **web**；**method** 参数为授权方法列表，必须为 **local**、**tacacs** 和 **radius** 关键字其中之一。**local** 表示使用本地数据库进行授权，**tacacs** 表示使用 TACACS+远程服务器进行授权，**radius** 表示使用 RADIUS 远程服务器进行授权。

**缺省情况：**缺省无需授权。

**命令模式：**全局配置模式。

**使用指南：console**、**vty** 与 **web** 登录可以分别设置相应的登录授权方法，其授权方式可以选择 **local**、**radius** 和 **tacacs** 的任意组合。当采用组合授权方式时，在最前面的授权方式优先级最高，并依次递减；如果高优先级方式授权通过，则直接允许用户登陆，并忽略后面的授权方式。需要注意的是：只要有一种授权方式收到相应协议的明确回应，无论是拒绝还是接收，都不再尝试下一种授权方式；若未收到相应协议的明确回应，则尝试下一种授权方式。当使用 RADIUS 授权时，必须使能 AAA 功能并配置 RADIUS 服务器。当使用 TACACS 授权时，必须配置 TACACS 服务器。若没有配置了授权 命令 authorization，本地方式授权登录的用户直接采用 username 命令配置的权限，而 RADIUS/TACACS 验证登录的用户只能在最小权限下工作。

**举例：**配置 telnet 远程登录的验证方式为 RADIUS。

Switch(config)#authorization line vty exec radius

## 1.1.2.11 authorization line vty command

**命令：authorization line vty command <1-15> {local | radius | tacacs} (none|)**

**no authorization line vty command <1-15>**

**功能：**配置 VTY（即指 Telnet 和 ssh 登录方式）登录用户的命令授权方式和授权选择优先级；该命令的 no 命令恢复缺省授权方式。

**缺省情况：**缺省没有配置授权方式。

**命令模式：**全局配置模式。

**使用指南：**设置 VTY 登录的用户在配置命令时的授权方法，其授权方式可以选择 Local、RADIUS 和 TACACS 的任意组合，none 方法仅作为最后一种方法。当采用组合授权方式时，在最前面的授权方式优先级最高，并依次递减；如果高优先级方式授权通过，则配置命令成功，并忽略后面的授权方式。需要注意的是：只要有一种授权方式收到相应协议的明确回应，无论是拒绝还是接收，都不再尝试下一种授权方式；若未收到相应协议的明确回应，则尝试下一种授权方式。当使用 RADIUS 授权时，必须使能 AAA 功能并配置 RADIUS 服务器。当使用 TACACS 授权时，必须配置 TACACS 服务器。none 方法为逃生功能只能作为最后一种授权方法，该方法直接返回授权通过，配置命令成功。

**举例：**配置 telnet 远程登录用户的 1 级命令授权方式为 TACACS。

Switch(config)#authorization line vty command 1 tacacs

## 1.1.2.12 clear line vty <0-31>

**命令：clear line vty <0-31>**

**功能：**删除指定线路上登陆的用户，强制 telnet 或 ssh 登陆的用户下线。

**命令模式：**特权模式。

**使用指南：**当输信该命令后，需要对该命令进行确认判断，“Confirm[Y/N]:”，当输入“Y”或“y”时，执行删除操作；输入“N”，不执行删除操作，只打印提示信息;输入其它任何字符均不执行删除操作。

## 1.1.2.13 crypto key clear rsa

**命令：crypto key clear rsa**

**功能：**清除 ssh 加密密钥。

**命令模式：**特权模式

## 1.1.2.14 terminal length

**命令：terminal length <0-512>**

**terminal no length**

**功能：**设置当前终端每屏显示字符的行数，no 命令取消换屏操作，一次显示所有内容。

**参数：**每屏显示字符的行数，取值范围为 0-512(0 为不停顿，一次显示所有字符)。

**命令模式：**特权用户配置模式。

**缺省情况：**系统缺省的行数为 25。

**使用指南：**设置当前的 console 或者 telnet，ssh 客户端每屏的显示行数，当显示信息超过一屏时，会出现—More—提示，按任意键则显示下一屏信息，默认设置是 25 行。

**举例：**设置每次显示字符的行数为 20：

Switch#terminal length 20

## 1.1.2.15 terminal monitor

**命令：terminal monitor**

**terminal no monitor**

**功能：**复制调试信息到当前显示终端，no 命令恢复缺省值。

**命令模式：**特权用户配置模式。

**使用指南：**控制当前的调试信息是否显示在该终端，如果在 telnet 或者是 ssh 客户端设置该命令，则 debug 信息将会送到该客户端，默认为调试信息显示在 console。

**举例：**

Switch#terminal monitor

## 1.1.2.16 telnet

**命令：telnet [vrf <*vrf-name*>] {<*ip-addr*> | <*ipv6-addr*> | host <*hostname*>} [<*port*>]**

**功能：**以 Telnet 方式登录到 IP 地址为***<ip-addr>***的远程主机。

**参数：*<vrf-name>***为指定的 VRF 名称；***<ip-addr>***为远端主机的 IP 地址，点分十进制格式；***<ipv6-addr>*** 为远端主机的 IPv6 地址；***<hostname>***是为远端主机的主机名，最长不超过 64 个字符；***<port>***为端口号，取值范围 0~65535。

**命令模式：**特权用户配置模式。

**使用指南：**本命令是交换机作为 Telnet 客户端时使用的，用户通过本命令登录远程主机进行配置。当交换机作为 Telnet 客户端时，只能与一个远程主机建立 TCP 连接，如果想与另一个远程主机建立连接，则必须先断开与上一个远程主机的 TCP 连接。断开与远程主机的连接可以使用快捷键“CTRL+\ ”。当 telnet 主机名时，应预先配置主机名与 IP/IPv6 地址的映射关系，命令可参考 ip host 和 ipv6 host。如果同一个主机名对应一个 IPv4 且对应一个 IPv6 地址，则 telnet 该主机名时优先使用该主机名对应的 IPv6 地址。

**举例：**交换机 Telnet 到 IP 地址为 20.1.1.1 的远程路由器 router。

Switch#telnet 20.1.1.1 23

Connecting Host 20.1.1.1 Port 23...

Service port is 23

Connected to 20.1.1.1

login:123

password:***

router>

## 1.1.2.17 telnet-server enable

**命令：telnet-server enable**

**no telnet-server enable**

**功能：**打开交换机的 Telnet 服务器功能；本命令的 no 操作为关闭交换机的 Telnet 服务器功能。

**缺省情况：**系统缺省打开 Telnet 服务器功能。

**命令模式：**全局配置模式。

**使用指南：**该命令只能在 Console 下使用，管理员使用本命令允许或拒绝 Telnet 客户端登录到交换机。

**举例：**关闭交换机的 Telnet 服务器功能。

Switch(config)#no telnet-server enable

## 1.1.2.18 telnet-server max-connection

**命令：telnet-server max-connection {<max-connection-number>|default}**

**功能：**配置交换机 Telnet 服务器支持的最大连接数。

**参数：**<max-connection-number>为 Telnet 服务器支持的最大连接数，范围为 1-16。default 选项恢复本命令的缺省配置。

**缺省情况：**系统设置的缺省最大连接数为 5。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**设置 Telnet 服务器支持的最大连接数为 10。

Switch(config)#telnet-server max-connection 10

## 1.1.2.19 ssh-server authentication-retries

**命令：ssh-server authentication-retries <authentication-retries>**

**no ssh-server authentication-retries**

**功能：**设置 SSH 客户端的验证重试次数；本命令的 no 操作为恢复缺省的重试次数。

**参数：<authentication-retries>**为验证重试次数，范围为 1-10 次。

**缺省情况：**系统设置的 SSH 验证重试次数为 3 次。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**设置 SSH 客户端的验证重试次数为 5 次。

Switch(config)#ssh-server authentication-retries 5

## 1.1.2.20 ssh-server enable

**命令：ssh-server enable**

**no ssh-server enable**

**功能：**打开交换机的 SSH 服务器功能；本命令的 no 操作为关闭交换机的 SSH 服务器功能。

**缺省情况：**系统缺省关闭 SSH 服务器功能。

**命令模式：**全局配置模式。

**使用指南：**如果需要 SSH 客户端登录到该交换机，需要交换机配置 SSH 用户，且打开 SSH 服务，然后 SSH 客户端才能正确登录 SSH 服务器，对交换机进行配置管理。

**举例：**打开交换机的 SSH 服务器功能。

Switch(config)#ssh-server enable

## 1.1.2.21 ssh-server host-key create rsa

**命令：ssh-server host-key create rsa [modulus <modulus>]**

**功能：**为 SSH 服务器创建新的 RSA 主机密钥。

**参数：modulus** 为计算主机密钥所使用的模，范围为 768-2048，缺省为 1024。

**缺省情况：**系统缺省使用 ssh-server 服务第一次启动时自动生成的密钥。

**命令模式：**全局配置模式。

**使用指南：**使用该命令可以创建新的主机密钥，然后 SSH 客户端登录该服务时，使用新生成的密钥进行主机认证。在生成新的密钥，并用 write 命令配置保留后，系统以后都使用该密钥进行主机认证。由于密钥计算需要较长时间，而且有个别客户端软件不兼容利用模 2048 计算出来的密钥，所以从安全效率和兼容性上考虑，建议采用缺省的模 1024 生成主机密钥。

**举例：**生成新的主机密钥。

Switch(config)#ssh-server host-key create rsa

## 1.1.2.22 ssh-server max-connection

**命令：ssh-server max-connection {<max-connection-number>|default}**

**功能：**配置交换机 SSH 服务器支持的最大连接数。

**参数：<max-connection-number>**为 SSH 服务器支持的最大连接数，范围为 1-16。**default** 选项恢复本命令的缺省配置。

**缺省情况：**系统设置的缺省最大连接数为 5。

**命令模式：**全局配置模式。

**举例：**设置 SSH 服务器支持的最大连接数为 10。

Switch(config)#ssh-server max-connection 10

## 1.1.2.23 ssh-server timeout

**命令：ssh-server timeout *<timeout>***

**no ssh-server timeout**

**功能：**设置 SSH 客户端的验证超时时间；本命令的 no 操作为恢复缺省的超时时间。

**参数：*<timeout>***为超时时间，范围为 10-600 秒。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省设置 SSH 客户端验证超时时间为 180 秒。

**使用指南：**本命令设置 SSH 客户端验证超时时间，系统缺省的超时时间为 180 秒。

**举例：**设置 SSH 客户端验证超时时间为 240 秒。

Switch(config)#ssh-server timeout 240

## 1.1.2.24 show crypto key

**命令：show crypto key**

**功能：**显示 ssh 加密密钥。

**命令模式：**特权模式

## 1.1.2.25 show ssh-server

**命令：show ssh-server**

**功能：**显示 SSH 服务器的状态是打开还是关闭，以及已经登录的 SSH 用户信息。

**命令模式：**特权和配置模式。

**举例：**

Switch#show ssh-server

ssh server is enabled

ssh-server timeout 180s

ssh-server authentication-retries 3

ssh-server max-connection number 6

ssh-server login user number 2

## 1.1.2.26 show telnet login

**命令：show telnet login**

**功能：**显示当前与交换机建立起 Telnet 连接的 Telnet 客户端的信息。

**命令模式：**特权和配置模式。

**使用指南：**本命令用以查看当前登录到系统的远程用户的信息。

**举例：**

Switch#show telnet login

Authenticate login by local.

Login user:

aa

## 1.1.2.27 show users

**命令：show users**

**功能：**显示通过 telnet 和 ssh 登陆的用户信息，包括线路号，登陆的用户名及用户的 IP。

**命令模式：**特权模式。

**使用指南：**当输入该命令时，显示通过 telnet 和 ssh 登陆的用户信息，包括线路号、登陆的用户名及用户的 IP。因为目前交换机最多支持 16 个 telnet 和 16 个 ssh 用户同时上线，所以将 vty 0-15 给 telnet 使用，16-31 供 ssh 使用;

**举例：**

Switch#show users

| Line | User | Location |
|---|---|---|
| vty 16 | a | 192.168.1.1 |
| vty 0 | admin | 192.168.1.2 |
| vty 17 | mab | 192.168.1.13 |
| vty 1 | test | 192.168.1.40 |

### 1.1.2.28 who

**命令：who**

**功能：**显示当前 vty 登录用户。

**参数：**无。

**命令模式：**各种配置模式

**举例：**显示当前 vty 登录用户。

Switch#who

Telnet user a login from 192.168.1.20

## 1.1.3 配置交换机的 IP 地址

### 1.1.3.1 interface vlan

**命令：interface vlan *<vlan-id>***

**no interface vlan *<vlan-id>***

**功能：**进入 VLAN 接口配置模式；本命令的 no 操作为删除已存在的 VLAN 接口。

**参数：*<vlan-id>*** 是已建立的 VLAN 的 VLAN ID，取值范围：1~4094。

**命令模式：**全局配置模式。

**使用指南：**要配置一个 VLAN 接口前，应确认此 VLAN 存在。使用命令 **exit** 可以从 VLAN 接口配置模式退回到全局配置模式。

**举例：**进入 VLAN 1 接口配置模式。

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#

### 1.1.3.2 interface ethernet 0

**命令：interface ethernet *<interface-name>***

**功能：** 从全局配置模式进入到网管端口配置模式。

**参数：** ***<interface-name>***为端口号，取 0。

**命令模式：** 全局配置模式。

**使用指南：** 使用命令 exit 可从以网管端口配置模式退回到全局配置模式。

**举例：** 进入网管端口。

Switch(config)#interface ethernet 0

Switch(Config-If-Ethernet0)#

### 1.1.3.3 ip address

**命令：ip address *<ip-address>* *<mask>* [secondary]**

**no ip address [*<ip-address>* *<mask>*] [secondary]**

**功能：**设置交换机的指定 VLAN 接口的 IP 地址及掩码；本命令的 no 操作为删除该 IP 地址配置。

**参数：*<ip-address>***为 IP 地址，点分十进制格式；***<mask>***为子网掩码，点分十进制格式；**[secondary]**为表示配置的 IP 地址为从 IP 地址。

**缺省情况：**出厂时交换机无 IP 地址。

**命令模式：**VLAN 接口配置模式。

**使用指南：**用户若要为交换机配置 IP 地址，必须首先创建一个 VLAN 接口。

**举例：**设置 VLAN1 接口的 IP 地址为 10.1.128.1/24。

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip address 10.1.128.1 255.255.255.0

Switch(Config-if-Vlan1)#exit

Switch(config)#

**相关命令：ip bootp-client enable、ip dhcp-client enable**

### 1.1.3.4 ipv6 address

**命令：ipv6 address *<ipv6address* | *prefix-length>* [eui-64]**

**no ipv6 address *<ipv6address* | *prefix-length>* [eui-64]**

**功能：** 为接口配置可聚合全球单播地址、本地站点地址、本地链路地址。

**参数：** ***<ipv6address>*** 参数为 IPv6 地址的前缀， ***<prefix-length>*** 参数为 IPv6 地址的前缀长度，前缀长度为 3-128 之间， **eui-64** 表明根据接口的 eui64 接口标识符自动生成 IPv6 地址。

**命令模式：** 接口配置模式。

**缺省情况：** 无。

**使用指南：** IPv6 地址前缀不能是多播地址，及其它有特定用途的 IPv6 地址，不同的 vlan 三层接口不能配置相同的地址前缀。对于全球单播地址，前缀必须在 2001::至 3fff::范围之内，前缀长度必须大于或等于 3。对于本地站点地址和本地链路地址，前缀长度必须大于或等于 10。

**举例：** 在 Vlan1 三层接口上配置一个 IPv6 地址：前缀为 2001:3f:ed8::99，前缀长度为 64。

Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64

## 1.1.3.5 ip bootp-client enable

**命令：ip bootp-client enable**

**no ip bootp-client enable**

**功能：**使能交换机为 BootP Client，通过 BootP 协商方式获取 IP 地址及网关地址；本命令的 no 操作为关闭 BootP Client 功能，并且释放以 BootP 方式获取的地址和网关地址。

**缺省情况：**缺省关闭 BootP Client 功能。

**命令模式：**VLAN 接口配置模式。

**使用指南：**通过 BootP 方式获取 IP 地址和手工配置、DHCP 方式获取 IP 地址是互斥的，不允许同时打开两种获取 IP 地址的方式。注意：要获得 IP 地址，网络上需要有 DHCP Server，或者 BootP Server。

**举例：**通过 BootP 方式获取 IP 地址。

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip bootp-client enable

Switch (Config-if-Vlan1)#exit

Switch (config)#

**相关命令：ip address、ip dhcp-client enable**

## 1.1.3.6 ip dhcp-client enable

**命令：ip dhcp-client enable**

**no ip dhcp-client enable**

**功能：**使能交换机为 DHCP Client，通过 DHCP 协商方式获取 IP 地址及网关地址；本命令的 no 操作为关闭 DHCP Client 功能，并且释放以 DHCP 方式获取的地址和网关地址。注意：要获得 IP 地址，网络上需要有 DHCP Server。

**缺省情况：**缺省关闭 DHCP Client 功能。

**命令模式：**VLAN 接口配置模式。

**使用指南：**通过 DHCP 方式获取 IP 地址和手工配置、BootP 方式获取 IP 地址是互斥的，不允许同时打开两种获取 IP 地址的方式。

**举例：**通过 DHCP 方式获取 IP 地址。

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip dhcp-client enable

Switch(Config-if-Vlan1)#exit

Switch(config)#

# 1.1.4 SNMP

## 1.1.4.1 debug snmp mib

**命令：debug snmp mib**

**no debug snmp mib**

**功能：**打开 SNMP mib 的调试开关；本命令的 no 操作为关闭该调试开关。

**命令模式：**特权用户配置模式。

**使用指南：** 当用户在使用 SNMP 时遇到问题，可以打开 SNMP 的调试开关，查找问题的原因。

**举例：**

Switch#debug snmp mib

## 1.1.4.2 debug snmp kernel

**命令：debug snmp kernel**

**no debug snmp kernel**

**功能：**打开 SNMP kernel 的调试开关；本命令的 no 操作为关闭该调试开关。

**命令模式：**特权用户配置模式。

**使用指南：**当用户在使用 SNMP 时遇到问题，可以打开 SNMP 的调试开关，查找问题的原因。

**举例：**

Switch#debug snmp kernel

## 1.1.4.3 rmon enable

**命令：rmon enable**

**no rmon enable**

**功能：**打开 RMON；本命令的 no 操作为关闭 RMON。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省开启 RMON。

**举例：**

启动 RMON。

Switch(config)#rmon enable

关闭 RMON。

Switch(config)#no rmon enable

## 1.1.4.4 show private-mib oid

**命令：show private-mib oid**

**功能：**显示设备私有Mib的起始oid。

**命令模式：**特权和配置模式。

**使用指南：**通过show private-mib oid命令可以查看到私有mib的起始oid。

**举例：**显示私有Mib的起始oid。

Switch# show private-mib oid

Private MIB OID:1.3.6.1.4.1.6339

## 1.1.4.5 show snmp

**命令：show snmp**

**功能：**显示 SNMP 各种计数器信息。

**命令模式：**特权和配置模式。

**举例：**

Switch#show snmp

0 SNMP packets input

0 Bad SNMP version errors

0 Unknown community name

0 Illegal operation for community name supplied

0 Encoding errors

0 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

0 SNMP packets output

0 Too big errors (Max packet size 1500)

0 No such name errors

0 Bad values errors

0 General errors

0 Get-response PDUs

0 SNMP trap PDUs

| 显示内容 | 解释 |
|---|---|
| snmp packets input | 输入的 snmp 报文的总数 |
| bad snmp version errors | 版本信息错误的报文数目 |
| unknown community name | 团体名错误的报文数目 |
| illegal operation for community name supplied | 团体名对应的权限错误的报文数目 |
| encoding errors | 编码错误的 snmp 报文数目 |
| Number of requested variables | nms 请求的变量的数目 |
| number of altered variables | nms 设置的变量的数目 |
| get-request PDUs | 收到的 get 请求的报文数目 |
| get-next PDUs | 收到的 getnext 请求的报文数目 |
| set-request PDUs | 收到的 set 请求的报文数目 |

| | |
|---|---|
| snmp packets output | 输出的 snmp 报文的总数 |
| too big errors | too_big 错误的 snmp 报文数目 |
| maximum packet size | snmp 报文的最大长度 |
| No such name errors | 对不存在的 MIB 对象进行请求的报文的数目 |
| bad values errors | bad_values 错误的 snmp 报文的数目 |
| general errors | general_errors 错误的 snmp 报文的数目 |
| response PDUs | 发送的响应报文的数目 |
| trap PDUs | 发送的 trap 报文的数目 |

## 1.1.4.6 show snmp engineid

**命令：show snmp engineid**

**功能：**显示引擎号的命令。

**命令模式：**特权和配置模式。

**举例：**

Switch#show snmp engineid

SNMP engineID:3138633303f1276c Engine Boots is:1

| 显示内容 | 解释 |
|---|---|
| SNMP engineID | 引擎号 |
| Engine Boots | 引擎启动次数 |

## 1.1.4.7 show snmp group

**命令：show snmp group**

**功能：**显示组信息的命令。

**命令模式：**特权和配置模式。

**举例：**

Switch#show snmp group

Group Name:initial Security Level:noAuthnoPriv

Read View:one

Write View:<no writeview specified>

Notify View:one

| 显示内容 | 解释 |
|---|---|
| Group Name | 组名 |
| Security level | 安全级别 |
| Read View | 读视图名 |
| Write View | 写视图名 |
| Notify View | 通告视图名 |
| <no writeview specified> | 用户没有指定适用的视图名 |

## 1.1.4.8 show snmp mib

**命令：show snmp mib**
**功能：**显示本机支持的所有 MIB。
**命令模式：**特权和配置模式。

## 1.1.4.9 show snmp status

**命令：show snmp status**
**功能：**显示 SNMP 配置信息。
**命令模式：**特权和配置模式。
**举例：**
Switch#show snmp status
Trap enable
RMON enable
Community Information:
V1/V2c Trap Host Information:
V3 Trap Host Information:
Security IP Information:

| 显示内容 | 解释 |
|---|---|
| Community string | 团体字符串 |
| Community access | 团体字符串的读写方式 |
| Trap-rec-address | 接收 Trap 的 IP 地址 |
| Trap enable | 是否允许发送 trap 消息 |
| SecurityIP | 允许访问 Agent 的管理站 IP 地址 |

## 1.1.4.10 show snmp user

**命令：show snmp user**
**功能：**显示用户信息的命令。
**命令模式：**特权和配置模式。
**举例：**
Switch#show snmp user
User name: initialsha
Engine ID: 1234567890
Auth Protocol:MD5 Priv Protocol:DES-CBC
Row status:active

| 显示内容 | 解释 |
|---|---|
| User name | 用户名 |
| Engine ID | 引擎号 |
| Priv Protocol | 使用的加密算法 |
| Auth Protocol | 使用的鉴别算法 |
| Row status | 用户状态 |

## 1.1.4.11 show snmp view

**命令：show snmp view**

**功能：**显示视图信息的命令。

**命令模式：**特权和配置模式。

**举例：**

Switch#show snmp view

View Name:readview 1. -Included active

1.3. - Excluded active

| 显示内容 | 解释 |
|---|---|
| View Name | 视图名 |
| 1.和 1.3. | OID 号 |
| Included | 视图包含以此 OID 为根的子树 |
| Excluded | 视图不包含以此 OID 为根的子树 |
| active | 状态 |

## 1.1.4.12 snmp-server community

**命令：snmp-server community {ro | rw} {0 | 7} *<string>* [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}] [read *<read-view-name>*] [write *<write-view-name>*]**

**no snmp-server community *<string>* [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]**

**功能：**设置交换机的团体字符串；本命令 no 操作为删除配置的团体字符串。

**参数：*<string>***为设置的团体字符串，如果密钥选项为 0，则后续指定明文团体字符串，如果选项为 7，则后续指定为明文团体字符串加密后的密文字符串；

**ro | rw** 为指定对 MIB 库的访问方式，**ro** 只读方式还是 **rw** 读写方式；

***<num-std>***为 IP 标准数字 ACL 的访问表标号，取值范围为<1-99>；

***<name>***为 IP 标准命名 ACL 的访问表标名，字符串长度为 1-64；

***<ipv6-num-std>***为 IPv6 标准数字 ACL 的访问表标号，取值范围为<500-599>；

***<name>***为 IPv6 标准命名 ACL 的访问表标名，字符串长度为 1-64；

***<read-view-name>***为读访问控制的视图名，字符串长度为 1-32；

***<write-view-name>***为写访问控制的视图名，字符串长度为 1-32。

**命令模式：**全局配置模式。

**使用指南：**交换机支持最多 4 个团体字符串。可以通过将团体名绑定到特定的读视图或者写视图，来实现对特定团体视图的访问控制。

**举例：**

添加读写权限的团体字符串 private。

Switch(config)#snmp-server community rw 0 private

添加只读权限的团体字符串 public。

Switch(config)#snmp-server community ro 0 public

修改原读写权限的团体字符串 private 为只读权限。

Switch(config)# snmp-server community ro 0 private

删除团体字符串 private。
Switch(config)#no snmp-server community 0 private
将只读权限团体字符串 public 绑定到读视图 pviewr
Switch(config)#snmp-server community ro 0 public read pviewr
将读写权限团体字符串 private 绑定到读视图 pviewr 和写视图 pvieww
Switch(config)#snmp-server community rw 0 private read pviewr write pvieww

## 1.1.4.13 snmp-server ddm-electronic-hidden

**命令：snmp-server ddm-electronic-hidden { enable | disable }**
**功能：**打开交换机作为 SNMP 代理服务器获取光模块 DDM 信息的功能；本命令的 no 操作为关闭此功能。
**参数：**enable 为开启这项功能；disable 为关闭这项功能。
**命令模式：**全局配置模式。
**缺省情况：**系统缺省关闭此功能。
**使用指南：**交换机若要通过网管软件进行配置管理，必须首先使用本命令打开交换机的 SNMP 代理服务器功能。
**举例：**打开交换机作为 SNMP 代理服务器获取光模块 DDM 信息的功能。
Switch(config)# snmp ddm-electronic-hidden enable

## 1.1.4.14 snmp-server ddm-mib

**命令：snmp-server ddm-mib { enable | disable }**
**功能：**打开交换机作为 SNMP 代理服务器获取光模块 DDM MIB 节点信息的功能。
**参数：**enable 为开启这项功能；disable 为关闭这项功能。
**命令模式：**全局配置模式。
**缺省情况：**系统缺省关闭此功能。
**使用指南：**交换机若要通过网管软件进行配置管理，必须首先使用本命令打开交换机的 SNMP 代理服务器功能。
**举例：**打开交换机作为 SNMP 代理服务器获取光模块 DDM MIB 节点信息的功能。
Switch(config)# snmp ddm-mib enable

## 1.1.4.15 snmp-server enable

**命令：snmp-server enable**
**no snmp-server enable**
**功能：**打开交换机作为 SNMP 代理服务器功能；本命令的 no 操作为关闭 SNMP 代理服务器功能。

**命令模式：**全局配置模式。
**缺省情况：**系统缺省关闭 SNMP 代理服务器功能。
**使用指南：**交换机若要通过网管软件进行配置管理，必须首先使用本命令打开交换机的 SNMP 代理服务器功能。
**举例：**打开交换机的 SNMP 代理服务器功能。
Switch(config)#snmp-server enable

## 1.1.4.16 snmp-server enable traps

**命令：snmp-server enable traps**
**no snmp-server enable traps**
**功能：**设置允许设备发送 Trap 消息；本命令的 no 操作为禁止发送 Trap 消息。
**命令模式：**全局配置模式。
**缺省情况：**系统缺省禁止发送 trap 消息。
**使用指南：**当设备允许发送 Trap 消息时，如果设备的端口发生 down/up 或者系统发生 down/up 等现象时，设备都会向接收 Trap 消息的管理站发送 Trap 消息。
**举例：**
允许发送 trap 消息
Switch(config)#snmp-server enable traps
禁止发送 trap 消息
Switch(config)#no snmp-server enable traps

## 1.1.4.17 snmp-server engineid

**命令：snmp-server engineid *<engine-string>***
**no snmp-server engineid**
**功能：**配置引擎号；本命令的 no 操作为恢复默认引擎号。
**命令模式：**全局配置模式。
**参数：<engine-string>**为引擎号，为 1-32 位十六进制字符
**缺省情况：**缺省值为企业号+本机 MAC 地址。
**使用指南：**
**举例：**配置当前引擎号为 A66688999F
Switch(config)#snmp-server engineid A66688999F
恢复默认引擎号
Switch(config)#no snmp-server engineid

## 1.1.4.18 snmp-server fdbMacInfoTable-mib

**命令：snmp-server fdbMacInfoTable-mib { enable | disable }**
**功能：**打开交换机作为 SNMP 代理服务器通过 mib 去获取 FDB 统计信息的功能。
**参数：**enable 为开启这项功能；disable 为关闭这项功能。
**命令模式：**全局配置模式。
**缺省情况：**系统缺省关闭此功能。

**使用指南：**交换机若要通过网管软件进行配置管理，必须首先使用本命令打开交换机的 SNMP 代理服务器功能。

**举例：**打开交换机作为 SNMP 代理服务器通过 mib 去获取 FDB 统计信息的功能。

Switch(config)# snmp-server fdbMacInfoTable-mib enable

## 1.1.4.19 snmp-server group

**命令：snmp-server group *<group-string>* {NoauthNopriv | AuthNopriv | AuthPriv} [[read *<read-string>*] [write *<write-string>*] [notify *<notify-string>*]] [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]**

**no snmp-server group *<group-string>* {NoauthNopriv | AuthNopriv | AuthPriv} [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]**

**功能：**该命令用来配置一个新的组；本命令的 no 操作为删除这个组。

**命令模式：**全局配置模式。

**参数：<group-string >** 组名，为 1-32 个字符；

**NoauthNopriv** 采用不鉴别不加密的安全级别；

**AuthNopriv** 采用鉴别不加密的安全级别；

**AuthPriv** 采用鉴别且加密的安全级别；

**read-string** 可用于读的视图名，为 1-32 个字符；

**write-string** 可用于写的视图名，为 1-32 个字符；

**notify-string** 可用于通告（trap）的视图名，为 1-32 个字符；

***<num-std>***为 IP 标准数字 ACL 的访问表标号，取值范围为<1-99>；

***<name>***为 IP 标准命名 ACL 的访问表标名，字符串长度为 1-64；

***<ipv6-num-std>***为 IPv6 标准数字 ACL 的访问表标号，取值范围为<500-599>；

***<name>***为 IPv6 标准命名 ACL 的访问表标名，字符串长度为 1-64。

**使用指南：**系统含一个默认视图为 v1defaultviewname，建议采用这个视图作为通告的视图名。如果读或写视图为空，则禁止相应操作。

**举例：**

创建一个组 CompanyGroup，安全级别为鉴别且加密，用于读的视图名为 readview,禁止写操作

Switch (config)#snmp-server group CompanyGroup AuthPriv read readview

删除组

Switch (config)#no snmp-server group CompanyGroup AuthPriv

## 1.1.4.20 snmp-server host

**命令：snmp-server host *{<host-ipv4-address> / <host-ipv6-address>}* {v1 | v2c | | [0|7] {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} *<user-string>***

**no snmp-server host *{<host-ipv4-address> / <host-ipv6-address>}* {v1 | v2c | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} *<user-string>***

**功能：**对 v1/v2c 版本来说，设置接收 SNMP 的 Trap 消息的网络管理站的 IPv4 或 IPv6 地址及 Trap 团体字符串，对 v3 版本来说，设置接收 SNMP 的 Trap 消息的网络管理站的 IPv4 或 IPv6

地址及 Trap 用户名和安全级别；本命令的 no 操作为取消这个网络管理站的 IPv4 或 IPv6 地址。

**命令模式：**全局配置模式。

**参数：*<host-ipv4-addr>***为接收Trap消息的NMS管理站IP地址；

***<host-ipv6-addr>***为接收Trap消息的NMS管理站IPv6地址；

**v1 | v2c | v3**发送trap使用的版本号；

**0 | 7**表示community字符串是明文还是密文；

**NoauthNopriv | AuthNopriv | AuthPriv**发送v3 trap使用的安全级别，不鉴别不加密|鉴别不加密|鉴别且加密；

***<user-string>***v1/v2c时为发送Trap消息时使用的community字符串，v3时为用户名。

**使用指南：**本命令设置发送 Trap 的团体字符串是 RMON 事件组团体字符串的缺省值。如果 RMON 事件组没有设置团体字符串，则发送 RMON 的 Trap 时使用本命令设置的团体字符串；如果 RMON 事件组设置团体字符串，则发送 RMON 的 trap 时按照 RMON 设置的团体字符串发送。本命令允许同时设置接收 Trap 消息的 SNMP 网管工作站的 IPv4 或 IPv6 地址，但配置版本号为 v1 和 v2c 的 IPv4 和 IPv6 地址总共不可以超过 8 个。

**举例：**

设置一个接受Trap的IP地址。

Switch(config)#snmp-server host 1.1.1.5 v1 usertrap

删除一个接受Trap的IPv6地址。

Switch(config)#no snmp-server host 2001::1 v1 usertrap

## 1.1.4.21 snmp-server packet delay

**命令：snmp-server packet delay (0|10|20)**

**no snmp-server packet delay**

**功能：**snmp收报文延迟时间。

**参数：**(0|10|20)为延迟时间，单位毫秒。

**命令模式：**全局配置模式。

**缺省情况：**缺省为10毫秒。

使用指南：使用前开启snmp功能，才可以使用本功能。

举例：配置snmp收包延迟时间为20毫秒。

Switch(config)#snmp-server packet delay 20

## 1.1.4.22 snmp-server securityip

**命令：snmp-server securityip *{<ipv4-address> | <ipv6-address>}***

**no snmp-server securityip *{<ipv4-address> | <ipv6-address>}***

**功能：** 设置允许访问本交换机的NMS管理站的安全IPv4或IPv6地址；本命令的no操作为删除配置的安全IPv4或IPv6地址。

**命令模式：** 全局配置模式。

**参数: *<ipv4-address>*** 为NMS的安全IPv4地址，点分十进制格式。

**<ipv6-address>** 为NMS的安全IPv6地址，冒号分十六进制格式。

**使用指南：** 只有NMS管理站的IPv4或IPv6地址与本命令设置的安全IPv4或IPv6地址相一致，它发出的SNMP包才会被交换机处理，该命令只适用于SNMP v1和SNMP v2c。允许同时设置交换机的NMS管理站的安全IPv4或IPv6地址，但二者总共不能超过20个。

**举例：**

设置NMS管理站的安全IP地址

Switch(config)#snmp-server securityip 1.1.1.5

删除安全IPv6地址

Switch(config)#no snmp-server securityip 2001::1

## 1.1.4.23 snmp-server securityip

**命令：snmp-server securityip {enable | disable}**

**功能：**打开/关闭 NMS 管理站的安全 IP 地址检查功能。

**命令模式：**全局配置模式。

**缺省情况：**打开安全 IP 地址检查功能。

**举例：**

关闭安全 IP 地址检查功能

Switch(config)#snmp-server securityip disable

## 1.1.4.24 snmp-server trap-resend-interval

**命令：snmp-server trap-resend-interval <6-65535>**

**no snmp-server trap-resend-interval**

**功能：**设置本交换机发送trap告警的重发等待时间；本命令的no操作为恢复默认的重发等待时间。

**参数: *<6-65535>*** 为发送trap告警的重发等待时间范围，单位为秒。

**命令模式：**全局配置模式。

**使用指南：**发送trap告警的重发等待时间默认为300s。

**举例：**设置交换机发送trap告警的重发等待时间为500s。

Switch(config)# snmp-server trap-resend-interval 500

## 1.1.4.25 snmp-server trap-source

**命令：snmp-server trap-source {<ipv4-address> | <ipv6-address>}**

**no snmp-server trap-source {<ipv4-address> | <ipv6-address>}**

**功能：**设置本交换机发送trap时所使用源IPv4或IPv6地址；本命令的no操作为删除配置的发送trap使用的源IPv4或IPv6地址。

**参数:** ***<ipv4-address>*** 为本交换机发送trap时所使用的IPv4地址，点分十进制格式。

**<ipv6-address>** 为本交换机发送trap时所使用的IPv6地址，冒号分十六进制格式。

**命令模式：**全局配置模式。

**使用指南：**默认没有本配置，根据实际trap报文发送的接口地址选择源地址，当配置时则采用配置的源地址作为trap报文的源地址。

**举例：**

设置交换机发送trap报文所使用的IP地址

Switch(config)#snmp-server trap-source 1.1.1.5

删除配置的发送ipv6 trap报文的源地址

Switch(config)#no snmp-server trap-source 2001::1

## 1.1.4.26 snmp-server trap-threshold

**命令：snmp-server trap-threshold {cpu-usage|memory-usage}{<0-100>}**

**no snmp-server trap-threshold {cpu-usage|memory-usage}**

**功能：**设置本交换机发送CPU或者内存利用率过高告警的阈值；本命令的no操作为恢复默认的阈值。

**参数: cpu-usage**代表交换机CPU利用率；**memory-usage**代表交换机内存利用率；**<0-100>**则表示以百分比的形式设置的告警阈值。

**命令模式：**全局配置模式。

**使用指南：**默认不开启此功能。

**举例：**设置本交换机发送CPU利用率过高告警的阈值为70%。

Switch(config)# snmp-server trap-threshold cpu-usage 70

## 1.1.4.27 snmp-server user

**命令：snmp-server user *<use-string>* *<group-string>* [{authPriv (aes|des|3des) [0|7] | authNoPriv} auth {md5 | sha} <word>] [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]**

**no snmp-server user *<user-string>* [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]**

**功能：**为一个 SNMP 的组添加一个新用户；本命令的 no 操作为删除这个用户。

**命令模式：**全局配置模式。

**参数：<user-string>**为用户名称，1-32 个字符；

**<group-string>**为用户所属的组名，1-32 个字符；

**authPriv** 对报文使用 DES 进行加密；

**aes** 使用 AES 进行加密；

**des** 使用 DES 进行加密；

**3des** 使用 3DES 进行加密；

**0|7** 表示用户字符串以及组字符串是明文还是密文；

**authNoPriv** 不对报文使用 DES 进行加密；

**auth** 对报文进行鉴别；

**md5** 使用 HMAC MD5 算法鉴别；

**sha** 使用 HMAC SHA 算法鉴别；

**<word>**，用户密码 长度 8-32 个字符；

***<num-std>***为 IP 标准数字 ACL 的访问表标号，取值范围为<1-99>；

***<name>***为 IP 标准命名 ACL 的访问表标名，字符串长度为 1-32；

***<ipv6-num-std>***为 IPv6 标准数字 ACL 的访问表标号，取值范围为<500-599>；

***<name>***为 IPv6 标准命名 ACL 的访问表标名，字符串长度为 1-64。

**使用指南：**如果不选择是否加密鉴别，默认为不加密不鉴别。如果选择进行加密，则必须选择进行鉴别。删除一个用户时，如果输入正确的用户名和错误的组名，同样可以删除用户。

**举例：**

为组 UserGroup 加入一个用户 tester，安全级别为需要加密、使用 HMAC md5 鉴别，密码 hellohello

Switch(config)#snmp-server user tester UserGroup authPriv auth md5 hellohello

删除一个用户

Switch(config)#no snmp-server user tester

## 1.1.4.28 snmp-server view

**命令：snmp-server view *<view-string>* *<oid-string>* {include | exclude}**

**no snmp-server view *<view-string>* [ *<oid-string>* ]**

**功能：**该命令用来创建或者更新视图的信息；本命令的 **no** 形式用来删除视图信息。

**命令模式：**全局配置模式。

**参数：<view-string>** 视图名，为 1-32 个字符；

**<oid-string>** OID 号或者对应的节点名，为 1-255 个字符；

**include | exclude** 包含/不包含此 OID。

**使用指南：**该命令不仅支持以变量 OID 的字符串作为参数输入，同时还支持以节点名作为参数输入。

**举例：**

创建一个视图名为 readview，包含 iso 节点，但不包含 iso.3 节点

Switch (config)#snmp-server view readview iso include

Switch (config)#snmp-server view readview iso.3 exclude

删除视图

Switch (config)#no snmp-server view readview

## 1.1.4.29 switchport updown notification enable

**命令：[no] switchport updown notification enable**

**功能：**开启或者关闭端口 UP/DOWN 事件发送 trap 信息的功能。

**缺省情况：**默认是对端口 IP/DOWN 事件发送 trap 信息。

**命令模式：**端口配置模式。

**使用指南：**该命令可以灵活的控制端口发生 UP/DOWN 事件时是否发送 trap 信息。缺省状态下，全局使能 snmp trap 之后，默认是对全部端口的 UP/DOWN 事件都发 trap。

**举例：**关闭 1/1/1 端口 UP/DOWN 事件发送 trap 信息的功能。

Switch(config)#interface ethernet1/1/1

Switch(config-if-ethernet1/1/1)#no switchport updown notification enable

Switch(config-if-ethernet1/1/1)#show running-config current-mode

!

Interface Ethernet1/1/1

no switchport updown notification enable

## 1.1.5 交换机升级

### 1.1.5.1 copy（FTP）

**命令：copy *<source-url>* *<destination-url>* [ascii | binary]**

**功能：**FTP 客户机上下载文件。

**参数：*<source-url>***为被拷贝的源文件或目录的位置；***<destination-url>***为文件或目录所要拷贝到的目的地址；***<source-url>***和***<destination-url>***的具体形式是随着文件或目录位置的不同而变化的。**ascii** 表示文件传输使用 ASCII 标准；**binary** 表示文件传输使用二进制标准（缺省传输方式）。当 URL 是 FTP 地址时的格式为：ftp://<username>:<password>@{<ipaddress>|<ipv6address>|<hostname> }/<filename>，其中<username>为 FTP 用户名，<password>为 FTP 用户口令，<ipaddress>|<ipv6address>为 FTP 服务器/客户机的 IPv4 或者 IPv6 地址，*<hostname>*是与 IPv6 地址映射的主机名，不支持与 IPv4 地址映射的主机名进行文件的下载和上传，*<filename>*为 FTP 上下载文件名。

filename 的特殊关键字：

| **关键字** | **源地址或目的地址** |
|---|---|
| **running-config** | 运行配置文件 |
| **startup-config** | 在使用 copy running-config startup-config 命令时，代表下次启动的配置文件。 |
| **nos.img** | 系统文件 |
| **boot.rom** | 系统启动文件 |
| **stacking/nos.img** | 作为目的地址在堆叠模式下对 Slave 进行系统文件升级 |
| **stacking/nos.rom** | 作为目的地址在堆叠下对 Slave 进行系统启动文件升级 |

**命令模式：** 特权用户配置模式。

**使用指南：** 本命令支持命令行提示，即如果用户可以输入如下形式的命令 **copy *<filename>* ftp://**或者 **copy ftp:// *<filename>***后直接回车，系统会出现如下的提示：

ftp server ip/ipv6 address [x.x.x.x]/[x:x::x:x] >

ftp username>

ftp password>

ftp filename>

要求输入 FTP 服务器的地址、用户名、密码及文件名。

**举例：**

（1）储存 FLASH 内的映像到 FTP 服务器 10.1.1.1，FTP 服务器的登录用户名为 Switch，密码为 superuser：

Switch#copy nos.img ftp://Switch:superuser@10.1.1.1/nos.img

（2）从 FTP 服务器 10.1.1.1 上得到系统文件 nos.img，用户名为 Switch，密码为 superuser：

Switch#copy ftp://Switch:superuser@10.1.1.1/nos.img nos.img

（3）储存 FLASH 内的映像到 FTP 服务器 2004:1:2:3::6

Switch#copy nos.img ftp://username:password@2004:1:2:3::6/ nos.img

（4）从 FTP 服务器 2004:1:2:3::6 上得到系统文件 nos.img：

Switch#copy ftp:// username:password@2004:1:2:3::6/nos.img nos.img

（5）保存运行配置文件：

Switch#copy running-config startup-config

**相关命令：write**

## 1.1.5.2 copy（TFTP）

**命令：copy *<source-url>* *<destination-url>* [ascii | binary]**

**功能：**TFTP 客户机上下载文件。

**参数：*<source-url>***为被拷贝的源文件或目录的位置；***<destination-url>***为文件或目录所要拷贝到的目的地址；***<source-url>***和***<destination-url>***的具体形式是随着文件或目录位置的不同而变化的。**ascii** 表示文件传输使用 ASCII 标准；**binary** 表示文件传输使用二进制标准（缺省传输方式）。当 URL 是 TFTP 地址时的格式为：tftp://{<ipaddress>|<ipv6address>|<hostname> }/<filename>，其中<ipaddress>|<ipv6address>为 TFTP 服务器/客户机的 IPv4 或者 IPv6 地址,*<hostname>*为与 IPv6 地址映射的主机名，不支持与 IPv4 地址映射的主机名进行文件的下载和上传，*<filename>*为 TFTP 上下载文件名。

filename 的特殊关键字：

| 关键字 | 源地址或目的地址 |
|---|---|
| **running-config** | 运行配置文件 |
| **startup-config** | 在使用 copy running-config startup-config 命令时，代表下次启动的配置文件。 |
| **nos.img** | 系统文件 |
| **boot.rom** | 系统启动文件 |

**命令模式：**特权用户配置模式。

**使用指南：** 本命令支持命令行提示，即如果用户可以输入如下形式的命令 **copy *<filename>* tftp://** 或者 **copy tftp:// *<filename>*** 后直接回车，系统会出现如下的提示：

tftp server ip/ipv6 address[x.x.x.x]/[x:x::x:x]>

tftp filename>

要求输入 TFTP 服务器的地址和文件名。

**举例：**

（1）储存 FLASH 内的系统映像文件到 TFTP 服务器 10.1.1.1

Switch#copy nos.img tftp://10.1.1.1/nos.img

（2）从 TFTP 服务器 10.1.1.1 上得到系统映像文件 nos.img：

Switch#copy tftp://10.1.1.1/nos.img nos.img

（3）储存 FLASH 内的映像到 TFTP 服务器 2004:1:2:3::6

Switch#copy nos.img tftp:// 2004:1:2:3::6/ nos.img

（4）从 TFTP 服务器 2004:1:2:3::6 上得到系统文件 nos.img：

Switch#copy tftp:// 2004:1:2:3::6/nos.img nos.img

（5）保存运行配置文件：

Switch#copy running-config startup-config

**相关命令：write**

## 1.1.5.3 copy（SFTP）

**命令：copy *<source-url>* *<destination-url>* [ascii | binary]**

**功能：**SFTP 客户机上下载文件。

**参数：*<source-url>***为被拷贝的源文件或目录的位置；***<destination-url>***为文件或目录所要拷贝到的目的地址；***<source-url>***和***<destination-url>***的具体形式是随着文件或目录位置的不同而变化的。**ascii** 表示文件传输使用 ASCII 标准；**binary** 表示文件传输使用二进制标准（缺省传输方式）。当 URL 是 SFTP 地址时的格式为：

ftp://<username>:<password>@{<ipaddress>|<ipv6address>|<hostname> }/<filename>，其中<username>为 SFTP 用户名，<password>为 SFTP 用户口令，<ipaddress>|<ipv6address>为 SFTP 服务器/客户机的 IPv4 或者 IPv6 地址，*<hostname>*是与 IPv6 地址映射的主机名，不支持与 IPv4 地址映射的主机名进行文件的下载和上传，*<filename>*为 SFTP 上下载文件名。

filename 的特殊关键字：

| 关键字 | 源地址或目的地址 |
|---|---|
| **running-config** | 运行配置文件 |
| **startup-config** | 在使用 copy running-config startup-config 命令时，代表下次启动的配置文件。 |
| **nos.img** | 系统文件 |
| **boot.rom** | 系统启动文件 |
| **stacking/nos.img** | 作为目的地址在堆叠模式下对 Slave 进行系统文件升级 |
| **stacking/nos.rom** | 作为目的地址在堆叠下对 Slave 进行系统启动文件升级 |

**命令模式：** 特权用户配置模式。

**使用指南：** 本命令支持命令行提示，即如果用户可以输入如下形式的命令 **copy *<filename>* *s*ftp://**或者 **copy sftp:// *<filename>***后直接回车，系统会出现如下的提示：

sftp server ip/ipv6 address [x.x.x.x]/[x:x::x:x] >

sftp username>

sftp password>

sftp filename>

要求输入 SFTP 服务器的地址、用户名、密码及文件名。

**举例：**

（1）储存 FLASH 内的映像到 SFTP 服务器 10.1.1.1，SFTP 服务器的登录用户名为 Switch，密码为 superuser：

Switch#copy nos.img sftp://Switch:superuser@10.1.1.1/nos.img

（2）从 SFTP 服务器 10.1.1.1 上得到系统文件 nos.img，用户名为 Switch，密码为 superuser：

Switch#copy sftp://Switch:superuser@10.1.1.1/nos.img nos.img

（3）储存 FLASH 内的映像到 SFTP 服务器 2004:1:2:3::6

Switch#copy nos.img sftp://username:password@2004:1:2:3::6/ nos.img

（4）从 SFTP 服务器 2004:1:2:3::6 上得到系统文件 nos.img：

Switch#copy sftp:// username:password@2004:1:2:3::6/nos.img nos.img

（5）保存运行配置文件：

Switch#copy running-config startup-config

**相关命令：write**

## 1.1.5.4 ftp-dir

**命令：ftp-dir *<ftp-server-url>***

**功能：**查看 FTP 服务器上的文件列表。

**参数：<ftp-server-url>** 格式为：ftp://<username>:<password>@{<ipv4address>|<ipv6address>}，其中<username>为 FTP 用户名，<password>为 FTP 用户口令，{<ipv4address>|*<ipv6address>*} 为 FTP 服务器 IPv4 或者 IPv6 地址。

**命令模式：**特权用户配置模式。

**举例：**查看地址为10.1.1.1的FTP服务器的文件列表，用户名和口令分别为Switch、superuser。

Switch#ftp-dir ftp:// Switch:superuser@10.1.1.1

## 1.1.5.5 ftp-server enable

**命令：ftp-server enable**

**no ftp-server enable**

**功能：**启动 FTP Server；本命令的 no 操作为关闭 FTP Server 服务，禁止 FTP 用户登录。

**缺省情况：**缺省不启动 FTP Server。

**命令模式：**全局配置模式。

**使用指南：**当启动 FTP 服务器功能后，交换机仍保留 FTP 客户机的功能。系统缺省情况下不启动 FTP Server。

**举例：**打开 FTP Server 服务。

Switch#config

Switch(config)# ftp-server enable

**相关命令：ip ftp**

## 1.1.5.6 ftp-server timeout

**命令：ftp-server timeout *<seconds>***

**功能：**设置数据连接空闲时限。

**参数：*<seconds>***为 FTP 连接空闲时限，单位秒，取值范围为 5~3600。

**缺省情况：**系统缺省空闲时限为 600 秒。

**命令模式：**全局配置模式。

**使用指南：**当 FTP 数据连接空闲实现超过此值时，切断 FTP 控制连接。

**举例：**修改空闲时限为 100 秒。

Switch#config

Switch(config)#ftp-server timeout 100

## 1.1.5.7 ip ftp

**命令：ip ftp username <*username*> password [0 | 7] <*password*>**

**no ip ftp username <*username*>**

**功能：**配置 FTP 登录用户名和登陆口令；本命令的 no 操作为删除配置的用户名，同时也删除密码。

**参数：<*username*>**为 FTP 连接的用户名，取值范围不超过 32 字符； **<*password*>**为 FTP 连接时使用的密码，在设置密码时，若输入选项为 0，则应输入明文密码，且不对输入的明文密码进行加密处理；若输入选项为 7，则应输入明文密码加密后的密文字符串。

**缺省情况：**系统缺省为匿名 FTP 连接。

**命令模式：**全局配置模式。

**举例：**配置用户名为 Switch，密码为 superuser。

```
Switch#
Switch#config
Switch(config)#ip ftp username Switch password 0 superuser
Switch(config)#
```

## 1.1.5.8 show ftp

**命令：show ftp**

**功能：**显示 FTP 服务器参数的设置情况。

**命令模式：**特权和配置模式。

**缺省情况：**缺省不显示。

**举例：**

```
Switch#show ftp
Timeout :600
```

| 显示信息 | 描述 |
| --- | --- |
| Timeout | 超时时间 |

## 1.1.5.9 show tftp

**命令：show tftp**

**功能：**显示 TFTP 服务器参数的设置情况。

**缺省情况：**缺省不显示。

**命令模式：**特权和配置模式。

**举例：**

```
Switch#show tftp
timeout         :60
Retry Times     :10
```

| 显示信息 | 解释 |
| --- | --- |
| Timeout | 超时时间 |
| Retry Times | 重传次数 |

## 1.1.5.10 tftp-server enable

**命令：tftp-server enable**

**no tftp-server enable**

**功能：**启动 TFTP Server；本命令的 no 操作为关闭 TFTP Server 服务，禁止 TFTP 用户登录。

**缺省情况：**缺省不启动 TFTP Server。

**命令模式：**全局配置模式。

**使用指南：**当启动 TFTP 服务器功能后，交换机仍保留 TFTP 客户机的功能。系统缺省情况下不启动 TFTP Server。

**举例：**打开 TFTP Server 服务。

Switch#config

Switch(config)#tftp-server enable

**相关命令：tftp-server timeout**

## 1.1.5.11 tftp-server retransmission-number

**命令：tftp-server retransmission-number <*number*>**

**功能：**设置 tftp 服务器重新传输数据的次数。

**参数：<*number*>**为重传次数，取值范围为 1~20。

**缺省情况：**系统缺省重传 5 次。

**命令模式：**全局配置模式。

**举例：**修改重传次数为 10 次。

Switch#config

Switch(config)#tftp-server retransmission-number 10

## 1.1.5.12 tftp-server transmission-timeout

**命令：tftp-server transmission-timeout <*seconds*>**

**功能：**设置 tftp 服务器传输超时时间。

**参数：<*seconds*>**为超时时间，取值范围为 5~3600s。

**缺省情况：**系统缺省超时时间为 600s。

**命令模式：**全局配置模式。

**举例：**修改超时时间为 60s。

Switch#config

Switch(config)#tftp-server transmission-timeout 60

# 1.1.6 Boot

## 1.1.6.1 boot img

**命令：boot img*<img-file-url>* {primary | backup}**

**功能：**设置交换机下次启动的 IMG 文件。

**参数： primary** 表示配置第一启动 IMG 文件，**backup** 表示配置第二启动 IMG 文件，**<img-file-url >**为启动 IMG 文件路径。

**命令模式：** boot 配置模式。

**缺省情况：**缺省情况下只有第一启动 IMG 文件名，即 nandFLASH 中的 nos.img 文件，第二启动 IMG 文件为空。

**使用指南：**通过该命令可以配置系统下次启动时的第一启动 img 文件和第二启动 img 文件，如果第一启动 img 文件启动失败则系统会自动启动第二启动 img 文件。IMG 文件全路径的格式要求如下：

1.文件路径由相当于根目录的设备前缀（nandflash:/）和文件名两部分组成。每一部分内不允许有空格存在，每两部分之间也不允许有空格存在。

2.文件名必须以.img 为后缀。

3. 文件全路径不能超过 128 个字符，文件名部分不能超过 80 个字符。

**举例：**设置当前交换机下次启动的第一启动 IMG 文件为 nandflash:/nos.img。

[Boot]: boot img nandflash:/nos.img primary

## 1.1.6.2 boot startup-config

**命令：boot startup-config *<file-url>***

**功能：**设置交换机下次启动的 CFG 文件

**参数：*<file-url >***为下次启动的 CFG 文件路径。

**命令模式：** boot 配置模式。

**缺省情况：** 出厂配置时默认 CFG 文件为 null，即空配置。

**使用指南：**通过该命令可以配置系统下次启动时的配置文件，配置文件名都必须带后缀.cfg。CFG 文件全路径的格式要求如下：

1. 路径由相当于根目录的设备前缀（flash:/）和文件名两部分组成，每一部分内及每两部分之间不允许有空格存在。

2. 配置文件必须以.cfg 为后缀。

3. 文件全路径不能超过 128 个字符，文件名部分不能超过 76 个字符。

**举例：**设置交换机下次启动的 CFG 文件为 flash:/ startup.cfg。

[Boot]: boot startup-config flash:/startup-config

## 1.1.6.3 dir

**命令：dir**

**功能：**显示当前交换机中存在的文件列表及其属性。

**参数：**无。

**命令模式：**boot 配置模式。

**缺省情况：**无。

**使用指南：**直接输入 dir 命令，可将当前交换机中的文件名及文件大小。注意，rom 文件不显示。

**举例说明：**查看当前交换机中存在的文件列表。

```
[boot]:dir
          37650852        Thu Jan 1 0:6:55 1970    backup.img
          37692336       Thu Jan 1 0:49:53 1970    74.img
          37713857        Thu Jan 1 1:41:2 1970    nos.img
```

## 1.1.6.4 help

**命令：h**

**功能：**显示当前 bootRom 支持的命令及其功能解释。

**参数：**无。

**缺省情况：**无。

**命令模式：**boot 配置模式。

**使用指南：**查看常用命令的解释。

**举例：**打印出常用命令的解释。

```
[boot]:h
                                        dcncmd
              h    on-line help
           load    load file from server
          write    write file to flash; file gotten by 'load'
            run    run dcn img
            dir    display the contents of the current directory
             cd    enter directory
     setconfig    set bootrom configurations
    saveconfig    save bootrom configurations
    showconfig    save bootrom configurations
       settype    set typid
        setmac    set mac address
         setsn    set sn
         setpn    set pn
         setan    set an
        setver    set hardware version
```

```
          setdate    set Manufacture date
setatemlicense    set atem license
    showlicense    show license
     showatemsn    show atem sn
           show    show board info
           boot    set boot img or starup-cfg
           ping    ping remote host
         reboot    reboot board
          shell    Enter pmon
```

## 1.1.6.5 load

**命令：load*<filename>***

**功能：**通过 tftp 方式加载文件。

**参数：*<filename>***为需要加载的文件名称。

**缺省情况：**无。

**命令模式：**boot 配置模式。

**使用指南：**输入 load + filename 命令，可通过 TFTP 加载文件。

**举例：加载 boot**.rom 文件。

[Boot]:load boot.rom

本型号交换机不支持此命令。

## 1.1.6.6 ping

**命令：ping *<x.x.x.x>***

**功能：**检验网络连接是否成功。

**参数：*<x.x.x.x>***为需要 ping 的 ip 地址，一般为 pc 的 ip 地址。

**缺省情况：**无

**命令模式：**boot 配置模式

**使用指南：**检验网络连接是否成功，类似 PC 中的 ping 命令，只是没有可选参数，并且只能从交换机往外 ping PC。

举例：检查到 192.168.0.1 的网络连接是否通。

[Boot]:ping 192.168.0.1

## 1.1.6.7 reboot

**命令：reboot**

**功能：**重启交换机。

**参数：**无。

**缺省情况：**无。

**命令模式：**boot 配置模式。

**使用指南：**直接输入 reboot 命令，可以热启交换机。

**举例：**重启交换机。

[Boot]:reboot

## 1.1.6.8 saveconfig

**命令：saveconfig**

**功能：**保存 bootrom 的配置参数。

**参数：**无.

**缺省情况：**无.

**命令模式：**boot 配置模式。

**使用指南：**直接输入 saveconfig 命令，可以保存用户配置。

**举例：**保存 bootrom 的配置参数.

[Boot]: saveconfig

change boot params is OK

本型号交换机不支持此命令。

## 1.1.6.9 setconfig

**命令：setconfig**

**功能：**设置 bootrom 的配置参数。

**参数：**无。

**缺省情况：**缺省情况下 Host IP 为 10.1.1.1，Server IP 为 10.1.1.2。

**命令模式：**boot 配置模式。

**使用指南：**直接输入 setconfig 命令，可以设置用户配置。目前能设置 Host IP 和 Server IP 两个参数，只支持 TFTP 协议。

**举例：**设置 bootrom 的配置参数。

[Boot]: setconfig

Host IP Address: [10.1.1.1] 192.168.1.1

Server IP Address: [10.1.1.2] 192.168.1.2

## 1.1.6.10 show

**命令：show [board|config]**

**功能：**显示相应交换机的信息。

**参数：board** 为交换机相应参数信息，比如 type、mac、sn 值。**config** 为当前 bootrom 的配置参数。**缺省情况：**无。

**命令模式：**boot 配置模式。

**使用指南：show board** 可以显示交换机相应参数信息，比如 type、mac、sn 值。**Show config** 显示 bootrom 的配置参数。**举例：**查看交换机的启动 img。

[boot]:show board

Board Type is:418

Vlan MAC:00-03-0f-d3-07-ee

CPU MAC:00-03-0f-d3-07-ef

S/N:SW082610L112000015

P/N:SW082610L112000015

A/N:

Manufacture Date:3921/2/16

H/W:1.0.1

## 1.1.6.11 showconfig

**命令：showconfig**

**功能：**显示 bootrom 的配置参数。该命令效果同 show confnig。

**参数：**无。

**缺省情况：**无。

**命令模式：**boot 配置模式。

**使用指南：**直接输入 showconfig 命令，可以显示用户配置。

**举例：**显示 bootrom 的配置参数。

[Boot]: showconfig

Host IP Address: 192.168.1.1

Server IP Address: 192.168.1.2

## 1.1.6.12 write

**命令：write *<filename>***

**功能：**将刚通过 load 下载的文件写入存储器（如 FLASH）中。

**参数：**<filename>为写入存储器中的文件名称。

**命令模式：**boot 配置模式。

**使用指南：**输入 write + filename 命令，可将文件写入 Bootrom 或 Flash 中。

将 load 的 boot 文件写入 flash 中，命名为 boot.rom 文件。

[Boot]:write boot.rom

# 1.2 文件系统

## 1.2.1 cd

**命令：cd <*directory*>**

**功能：**修改当前存储设备的工作路径。

**参数说明：*<directory>***为子目录名称，取值范围为 **1~80** 个连续字符。

**命令模式：**特权模式。

**缺省情况：**默认的工作路径为 Flash。

**使用指南：**执行该命令后，当前存储设备会切换到新的工作路径。修改后可以通过 pwd 命令进行查看。

**举例：**修改当前存储设备的工作路径为 flash。

Switch#cd flash：

Switch#pwd

flash:/

Switch#

## 1.2.2 copy

**命令：copy <*source-file-url*> <*dest-file-url*>**

**功能：**把交换机上的某个指定文件复制为新的文件。

**参数说明：*<source-file-url>***为源文件；***<dest-file-url>***为目标文件。用户在 IMG 下对备用主控板卡和线卡上的文件进行操作时，源文件和目标文件的 URL 格式必须满足以下要求：

1.源文件的 URL 格式中前缀必须为以下几种形式：

- “flash:/”开头
- “ftp://username:pass@server-ip/file-name”
- “tftp://server-ip/file-name”

2.目标文件的 URL 格式中前缀必须为以下几种形式：

- “flash:/”开头
- “ftp://username:pass@server-ip/file-name”
- “tftp://server-ip/file-name”

**命令模式：**特权模式。

**缺省情况：**无

**使用指南：**

1．在使用此命令时，当源文件的 URL 格式中前缀为 ftp://或 tftp://时，目标文件的 URL 格式中前缀不能为 ftp://或 tftp://。

2．在使用此命令时，应保证源文件存在，并且目标文件名不能和已有的目录名或已有的文件名重名，否则会提示 copy 操作执行失败或将已有文件覆盖等信息。

3. 如果目标文件与源文件在不同路径目录下，执行此命令后，也可以将不同路径目录下的文件复制到当前目录下。

URL 书写举例：Flash 设备上根路径下的 nos.img 文件的 URL 必须是 flash:/nos.img。

**举例：**将当前 flash:/nos.img 文件复制到 flash:/ 6.1.11.0.img。

Switch#copy flash:/nos.img flash:/nos-6.1.11.0.img

Copy flash:/nos.img to flash:/nos-6.1.11.0.img? [Y:N] y

Copyed file flash:/nos.img to flash:/nos-6.1.11.0.img.

## 1.2.3 delete

**命令：delete <*file-url*>**

**功能：**删除存储设备上的指定文件。

**参数说明：*<file-url>***为要删除的文件全路径。

**命令模式：**特权模式。

**缺省情况：**无

**使用指南：**执行该命令后会将指定的文件删除。

**举例：**删除文件 flash:/nos.img。

Switch#delete flash:/nos5.img

Delete file flash:/nos5.img?[Y:N]y

Deleted file flash:/nos.img.

## 1.2.4 dir

**命令：dir [WORD|all]**

**功能说明：**显示存储设备中的指定目录的信息。

**参数说明：<WORD>**为显示的目录名称。可能有如下形式：目录名，slot-xx#目录名，flash:/目录名，cf:/目录名。all 为同时显示目录 flash:/和 nandflash:/下的信息。

**命令模式：**特权用户配置模式。

**缺省情况：**如果不输入**<WORD>**则显示当前工作目录的信息。

**使用指南：**执行此命令后会显示出指定目录下的文件与子目录信息。

**注意：**该命令不支持递归显示所有子目录信息。

**举例：**显示目录 flash:/的信息：

switch#dir flash:/

| | | |
|---|---|---|
| -rw- | 512 | ic.log |
| -rw- | 2.2K | inntial.cfg |
| -rw- | 2.3K | startup.cfg |

-rw- 71 vsf.cfg

-rw- 3.5K vsf_startup.cfg

Drive : flash:

Size:30.5M Used:480.0K Available:30.0M Use:2%

## 1.2.5 format

本型号交换机不支持此命令。

## 1.2.6 mkdir

**命令：** **mkdir <directory>**

**功能：** 在指定存储设备的指定目录下创建子目录。

**参数说明：** ***<directory>***为子目录名称，取值范围为 1~80 个连续字符。

**命令模式：** 特权用户配置模式。

**缺省情况：** 无。

**使用指南：** 创建的目录名不能与指定目录下的其它目录或文件名重名，且不能在 flash 设备中创建子目录。如果创建过程中出错则提示错误信息。

## 1.2.7 pwd

**命令：pwd**

**功能：**显示当前工作路径。

**参数说明：**无

**命令模式：**特权用户配置模式。

**缺省情况：**默认的工作路径为 flash。

**举例：**显示当前工作路径。

Switch#pwd

flash:/

Switch#

## 1.2.8 rename

**命令：rename *<source-file-url>* *<new-filename>***

**功能：**把交换机上的某个指定的文件重命名为新的文件名。

**参数说明：*<source-file-url>***为源文件，可以带有文件路径；***<new-filename>***为不含路径的新文件名。

**命令模式：**特权用户配置模式。

**缺省情况：**无。

**使用指南：**在使用此命令的时候，当新的文件名与已经存在的目录或文件均不重名且文件未被使用时，可以将文件重命名，否则提示重命名操作失败。

**举例：**将当前工作路径下的文件 nos.img 重命名为 nos-6.1.11.0.img。

Switch#rename nos5.img nos-6.1.11.0.img

Rename flash:/nos5.img to flash:/nos-6.1.11.0.img ok！

### 1.2.9 rmdir

**命令：rmdir** <directory>

**功能：** 在指定存储设备的指定目录下删除子目录。

**参数说明：** <directory>为子目录名称，取值范围为 1~80 个连续字符。

**命令模式：** 特权用户配置模式。

**缺省情况：** 无。

**使用指南：** 被删除的目录必须存在且为空目录，即删除目录前必须先删除该目录下的所有文件，否则会给出错误提示。如果子目录删除成功，提示成功信息；如果子目录删除过程中出错，则提示错误信息

## 1.3 集群网管

### 1.3.1 clear cluster nodes

**命令：clear cluster nodes [nodes-sn *<candidate-sn-list>* | mac-address *<mac-addr>*]**

**功能：**清除命令交换机发现的候选交换机列表中的节点。

**参数说明:** candidate-sn-list：candidate 交换机编号，支持同时选择多个 candidate。范围为 1～256。不输入参数表示清除所有交换机信息。

mac-address：交换机的 mac 地址（交换机包括所有的 candidate，member 和 other 交换机）。

**缺省情况：**不输入参数表示清除所有交换机信息。

**命令模式：**特权模式。

**使用指南：**执行该命令后，该节点的信息将从 commander 保存的链表中删除。在 30 秒之内 commander 会重建 cluster 拓扑，然后重新加入此节点。但重新加入后，其 candidate 编号可能发生变化。此命令只能在 commander 上执行。

**举例:** 清除命令交换机发现的所有候选交换机列表。

Switch#clear cluster nodes

### 1.3.2 cluster auto-add

**命令：cluster auto-add**

**no cluster auto-add**

**功能：**在命令交换机上使能该命令以后，可以把新发现的候选交换机自动加入集群，成为集群的成员交换机；该命令的 no 操作禁止该操作。

**参数说明：**无。

**缺省情况：**系统默认禁止该功能，即不自动把候选交换机加入集群。

**命令模式：**全局配置模式。

**使用指南：**在命令交换机上使能该命令以后，把候选交换机自动加为 member。

**举例：**在命令交换机上打开集群自动加入功能。

Switch(config)#cluster auto-add

## 1.3.3 cluster commander

**命令：cluster commander [*<cluster-name>*]**

**no cluster commander**

**功能：**设置交换机为命令交换机，并创建一个集群。

**参数：*<cluster-name>***是创建的集群的名字，不超过 32 个字符。

**缺省情况：**默认为非 commander 交换机。cluster_name 默认为 null。

**命令模式：**全局配置模式。

**使用指南：**本命令指定该交换机的角色为命令交换机，创建一个集群。此命令只能在非 commander 上执行。在成为 commander 之后 cluster_name 不可更改。若需要更改，必须先执行 no cluster commander。该命令的 no 操作，取消交换机的 commander 配置。

**举例：**在本交换机上指定为命令交换机,集群的名字为 switch。

Switch(config)#cluster commander switch

## 1.3.4 cluster ip-pool

**命令：cluster ip-pool *<commander-ip>***

**no cluster ip-pool**

**功能：**配置集群中成员设备使用的私有 IP 地址池。

**参数：*commander-ip*：**cluster IP 地址池，用于分配 cluster 的内部 IP 地址。commander-ip 为地址池的首地址。有效地址的形式为 10.x.x.x，点分十进制格式；地址池必须足够大，使得能够容纳 128 个 member，即地址最后的一个字节必须小于 126（254 – 128 = 126）。

在配置 commander 后 IP 地址池不能改变。若需要改变，必须先执行 no cluster commander 命令。

**缺省情况：**默认地址池为 10.254.254.1。

**命令模式：**全局配置模式。

**使用指南：**当候选交换机加入集群时，命令交换机为每个成员分配一个可以在集群范围内使用的私有 IP 地址，并分发给成员交换机，用于集群内部的通讯，以实现命令交换机对成员

交换机的管理和维护。该命令只能在非 commander 上使用。若集群已经建立，则用户不能修改 IP 地址池。此命令的 NO 命令恢复地址池为默认值，默认地址池为 10.254.254.1。

**举例：**配置集群中成员设备使用的私有 IP 地址池 ip-pool 为 10.254.254.10。

Switch(config)#cluster ip-pool 10.254.254.10

## 1.3.5 cluster keepalive interval

**命令：cluster keepalive interval *<second>***

**no cluster keepalive interval**

**功能：**配置 cluster 内部的 keepalive 报文时间间隔。

**参数说明：**<second>：keepalive 时间间隔，以秒为单位。范围 3～30 秒。

**缺省情况：**默认为 30 秒。

**命令模式：**全局配置模式。

**使用指南：**在 commander 上配置此命令后，会将此参数通过 commander 和 member 之间的 TCP 连接分发给各 member 交换机。

在非 commander 上配置此命令后，配置值会被保存，等自己成为 commander 后使用。而在此之前，使用的 keepalive interval 为自己所属的 commander 下发的值。

commander 在每一个 keepalive interval 内在 cluster 内发送一次 DP 报文。member 收到 DP 报文后回复 DR 报文。

该命令的 no 操作恢复 cluster 内部的 keepalive 报文时间间隔为默认值。

**举例**:设置集群内部的 keepalive 报文间隔为 10。

Switch(config)#cluster keepalive interval 10

## 1.3.6 cluster keepalive loss-count

**命令：cluster keepalive loss-count *<loss-count>***

**no cluster keepalive loss-count**

**功能：**配置 cluster 内部的 keepalive 报文的允许的最大丢失报文个数。

**参数说明：**loss-count：允许的最大丢失报文个数。范围 1～10 个。

**缺省情况：**默认值为 3 个。

**命令模式：**全局配置模式。

**使用指南：**在 commander 上配置此命令后，会将此参数通过 commander 和 member 之间的 TCP 连接分发给各 member 交换机。

在非 commander 上配置此命令后，配置值会被保存，等自己成为 commander 后使用。而在此之前，使用的 loss-count 为自己所属的 commander 下发的值。

commander 发送 DP 报文后，启动 loss-count 计数。每发送一个报文，将所有交换机的 loss-count 计数加 1；但当收到交换机发送的 DR 报文后，将此交换机对应的 loss-count 清 0。当 loss-count 到达配置的值后（默认 3 个）还没有收到 DR 报文，将此交换机从 candidate 链表中删除。

如果 member 连续 loss-count 次没有收到 commander 发送的 DP 报文，则将自己的状态置为 candidate。

该命令的 no 操作将 cluster 内部的 keepalive 报文允许的最大丢失报文个数恢复为默认值 3 个。

**举例:** 设置 cluster 内部的 keepalive 报文的允许的最大丢失报文个数为 5。

Switch(config)#cluster keepalive loss-count 5

## 1.3.7 cluster member

**命 令：cluster member {nodes-sn *<candidate-sn-list>* | mac-address *<mac-addr>* [id *<member-id>*]}**

**no cluster member {id *<member-id>* | mac-address *<mac-addr>*}**

**功能**：在命令交换机上，手动把候选交换机加入命令交换机创建的集群；该命令的 no 操作删除指定的 member 交换机，使其转变为 candidate。

**参数说明**：nodes-sn：集群内所有交换机都保存在一个链表上，每个交换机都有一个 nodes 编号可以通过命令 show cluster candidates 查看。可以同时将一个或多个 candidate 加为 member。candidate-sn-list 的有效范围为 1~256。

mac-address：candidate 交换机的 CPU Mac。

member-id：可以将 candidate 加入为 member 时对其指定一个 member 编号，范围为 1～128，默认为从 1 开始递增。

nodes-sn 为自动生成的编号，candidate 状态变为 member 之后，此值可能会发生变化。以此方式加为 member 实际上也会转化为以 mac-addr 的方式加为 member。配置文件也都是以 mac-addr 的方式保存的。

若同时指定多个交换机加为 member，则不能指定 member-id；以 nodes-sn 的方式加入 member，不能指定 member-id。

**缺省情况**：无。

**命令模式**：全局配置模式。

**使用指南**：命令交换机执行该命令后，把***<nodes-sn>***或***<mac-address>***标示的交换机加入命令交换机所在的集群。可以同时将一个或多个 candidate 加为 member，以‘-’或者‘；’连接。已经成为 member 或者 commander 的不能再成为其他 cluster 的 member。如果在非命令交换机上运行该命令时，返回错误。

**举例:** 在命令交换机上把编号为 1 的候选交换机加入到集群中；在命令交换机上把 mac 地址为 11-22-33-44-55-66 的交换机加为 member，并且指定加入后的 member-id 为 5。

Switch(config)#cluster member nodes-sn 1

Switch(config)#cluster member mac-address 11-22-33-44-55-66 id 5

## 1.3.8 cluster member auto-to-user

**命令：cluster member auto-to-user**

**功能**：在配置 no cluster auto-add 时会将所有自动加为 member 的交换机删除。若需要保留这些 member，可将自动加为 member 的交换机转化为手动加为 member 的交换机。

**参数说明**：无。

**缺省情况**：无。

**命令模式**：全局配置模式。

**使用指南**：在命令交换机上运行该命令，使自动加为 member 的交换机变成手动加为 member 的交换机。

**举例**：使自动加为 member 的交换机变成手动加为 member 的交换机。

Switch(config)#cluster member auto-to-user

## 1.3.9 cluster reset member

**命令**：**cluster reset member [id *<member-id>* | *mac-address <mac-addr>*]**

**功能**：在命令交换机上使用该命令重启成员交换机。

**参数说明**：member-id：取值范围：1-128，可以使用连接号“-”和分号“；”同时选择多个 member。若不输此参数，表示重启所有 member 交换机。

**缺省情况**：启动所有成员交换机。

**命令模式**：特权模式。

**使用指南**：本命令使命令交换机分发重启命令到成员交换机，成员交换机重启。如果在非命令交换机上运行该命令，返回错误。

**举例**：在命令交换机上重启成员交换机 1。

Switch#cluster reset member id 1

## 1.3.10 cluster run

**命令**：**cluster run [key <*WORD*>] [ vid <*VID*>]**

**no cluster run**

**功能**：启动集群功能，该命令的 no 操作停止集群功能。

**参数**：key：一个 cluster 内的 key 必须一致，不超过 16 个字符。

vid：cluster 的 vlan id，值的范围是 1-4094。

**缺省情况**：默认关闭集群功能，key：NULL（\0） vid：1。

**命令模式**：全局配置模式。

**使用指南**：本命令启动集群任务，只有集群功能开启，才能执行一切集群相关命令。执行 no 命令，将关闭本设备集群功能。建议用户划分一个专门的 vlan（比如 vlan100）来给 cluster 使用。

注意：在 cluster vlan 所在的三层接口不要起路由协议，以避免将 cluster 的私有路由广播出去。

**举例**：本地交换机上关闭集群任务。

Switch(config)#no cluster run

## 1.3.11 cluster update member

**命令：cluster update member *<member-id> <src-url>* [ascii | binary]**

**功能：**命令交换机上对成员交换机进行远程升级。

**参数说明：member-id：**取值范围：1-128，可以使用连接号“-”和分号“;”同时选择多个 member；

**src-url：**被拷贝的源文件的位置；

**dst-filename：**文件存放在交换机 flash 中的文件名；

**ascii** 表示文件传输使用 ASCII 标准；**binary** 表示文件传输使用二进制标准，缺省为 **binary** 方式。

当 src-url 是 FTP 地址时的格式为：ftp://<username>:<password>@<ipadress>/<filename>，其中<username>为 FTP 用户名，<password>为 FTP 用户口令，<ipadress>为 FTP 服务器的 IP 地址，<filename>为 FTP 下载文件名。

当 src-url 是 TFTP 地址时的格式为：tftp://<ipadress>/<filename>，其中<ipadress>为 TFTP 服务器的 IP 地址，<filename>为 TFTP 下载文件名。

filename 的特殊关键字：

| **关键字** | **源地址或目的地址** |
|---|---|
| **startup-config** | 启动配置文件 |
| **nos.img** | 系统文件 |

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**通过 commander 和 member 之间的 TCP 连接，commander 分发远程升级命令到 member，member 执行远程升级并重启。如果在非 commander 上运行该命令则返回错误。用户在一次升级多个成员时，应该确保这些成员为同一型号的交换机，避免给成员升级不匹配的 IMG 文件，导致交换机无法正常启动。

**举例:**在命令交换机上对成员交换机进行远程升级，成员交换机 member-id 为 1，src-url 为 ftp:// switch: switch @192.168.1.1/nos.img

Switch#cluster update member 1 ftp:// switch:switch@192.168.1.1/nos.img

## 1.3.12 debug cluster

**命令：debug cluster {statemachine | application | tcp}**

**no debug cluster {statemachine | application | tcp}**

**功能：**打开 cluster 应用调试开关；本命令的 no 操作为关闭打开的相应的调试开关。

**参数：**statemachine：交换机状态发生变化时打印 debug 信息。

application：有用户通过 SNMP，WEB 登陆交换机进行配置管理时打印 debug 信息。

Tcp：commander 和 member 之间的 TCP 连接信息。

**缺省情况：**无。

**命令模式：**特权用户配置模式。

**实用指南：**无。

**举例：**打开交换机状态发生变化时的 debug 开关。

Switch#debug cluster statemachine

## 1.3.13 debug cluster packets

**命令：debug cluster packets {DP | DR | CP} {receive | send}**

**no debug cluster packets {DP | DR | CP} {receive | send}**

**功能：**打开 cluster 应用调试开关；本命令的 no 操作为关闭打开的相应的调试开关。

**参数：**DP：发现报文。

DR：回应报文。

CP：命令报文。

receive：接收报文。

send：发送报文。

**缺省情况：**无。

**命令模式：**特权用户配置模式。

**实用指南：**打开集群报文调试开关，分组开关打开后，cluster 内发送或接收 DP、DP、CP 报文都会打印出来。

**举例：**打开接收 DP 报文的 debug 开关。

Switch#debug cluster packets DP receive

## 1.3.14 show cluster

**命令：show cluster**

**功能：**显示交换机中 cluster 信息。

**参数：**无。

**命令模式：**特权和配置模式。

**使用指南：**无。

**举例：**在不同角色类型的交换机上运行该命令：

----in a commander----------

Switch#show cluster

Status: Enabled

Cluster VLAN: 1

Role: commander

IP pool: 10.254.254.1

Cluster name: MIS_zebra

Keepalive interval: 30

Keepalive loss-count: 3

Auto add: Disabled

Number of Members: 0
Number of Candidates: 3
----in a member ----------
Switch#show cluster
Status: Enabled
Cluster VLAN: 1
Role: Member
Commander Ip Address: 10.254.254.1
Internal Ip Address: 10.254.254.2
Commamder Mac Address: 00-12-cf-39-1d-90
---- a candidate ----------
Switch#show cluster
Status: Enabled
Cluster VLAN: 1
Role: Candidate
---- disabled ----------
Switch#show cluster
Status: Disabled

## 1.3.15 show cluster members

**命令：show cluster members [id *<member-id>* | mac-address *<mac-addr>*]**
**功能：**显示 cluster 中 member 信息，此命令只能在 commander 上执行。
**参数：**member-id：member 交换机的编号。
mac-addr：member 交换机的 CPU Mac。
**默认配置：**不输入参数表示显示所有成员交换机。
**命令模式：**特权和配置模式。
**使用指南：**在命令交换机上执行该命令，可以显示加入集群的成员交换机的配置信息。
**举例：**在命令交换机运行该命令显示所有成员交换机和显示指定成员交换机的配置信息。
Switch#show cluster members
Member From : User config(U); Auto member (A)
ID From Status Mac Hostname Description Internal IP
--- - ---------- ---------- ---------- ---------- ----------
xxx x xxxxxxxxxx12 xx-xx-xx-xx-xx-xx xxxxxxxxxx12 xxxxxxxxxx12 xxx.xxx.xxx.xxx
1 U Inactive 00-01-02-03-04-05 MIS_zebra DCRS-6804 10.254.254.2
2 A Active 00-01-02-03-04-05 MIS_bison DCRS-6804 10.254.254.3
3 U Active 00-01-02-03-04-05 SRD_jaguar DCRS-9808 10.254.254.4
4 A Inactive 00-01-02-03-04-05 HRD_puma DCRS-5950-28T 10.254.254.5
---

Switch#show cluster members id 1
Cluster Members:
ID: 1
Member status: Inactive member (user_config)
IP Address: 10.254.254.2
MAC Address: 00-01-02-03-04-06
Description: DCRS-9808
Hostname: DSW102

## 1.3.16 show cluster candidates

**命令：show cluster candidates [nodes-sn *<candidate-sn-list>* | mac-address *<mac-addr>*]**
**功能：**显示在命令交换机上的候选成员交换机的配置信息。
**参数：**candidate-sn-list：candidate 交换机编号，支持选择多个 candidate。范围为 1～256。不输入参数表示显示所有交换机信息。
mac-address：candidate 交换机的 mac 地址。
**默认配置：**不输入参数表示显示所有交换机信息。
**命令模式：**特权和配置模式。
**使用指南：**在命令交换机上执行该命令，可以显示尚未加入集群的候选成员交换机的配置信息。
**举例：**显示集群的所有候选交换机的配置信息。
Switch#show cluster candidates
Cluster Candidates:
SN Mac Description Hostname
--- ----------------- ---------------------- ----------------------
xxx xx-xx-xx-xx-xx-xx xxxxxxxxxxxxxxxxxxxxx24 xxxxxxxxxxxxxxxxxxxxx24
1 00-01-02-03-04-06 ES3528M
2 01-01-02-03-04-05 ES3528M MIS_zebra

## 1.3.17 show cluster topology

**命令：show cluster topology [root-sn *<starting-node-sn>* | nodes-sn *<node-sn-list>* | mac-address *<mac-addr>*]**
**功能：**显示 cluster topology 信息，此命令只能在 commander 上执行。
**参数：**starting-node-sn：拓扑图的起始节点。
node-sn-list：交换机编号。
mac-addr：交换机 CPU Mac。

若不输入参数，表示显示全部拓扑信息。

**命令模式：**特权和配置模式。

**使用指南：**在命令交换机上执行该命令，可以显示指定开始节点的拓扑信息。

**举例：**在命令交换机上运行该命令，显示各种情况的拓扑信息。

```
Switch#show cluster topology
Role: commander(CM);Member(M);Candidate(CA);Other commander(OC);Other member(OM)
LV SN Description Hostname Role MAC_ADDRESS Upstream Upstream leaf
                                                local-port remote-port node
  == ============ ============ == ================= ============ ============ =
x xxx xxxxxxxxxx12 xxxxxxxxxx12 xx xx-xx-xx-xx-xx-xx xxxxxxxxxx12 xxxxxxxxxx12 x
1  1 ES4626H  LAB_SWITCH_1 CM 01-02-03-04-05-01 -root-  -root-  -
   2 ES4626H  LAB_SWITCH_2 M  01-02-03-04-05-02 eth 1/1/1  eth 1/1/2  N
   3 ES4626H  LAB_SWITCH_3 CA 01-02-03-04-05-03 eth 1/1/1  eth 1/1/3  Y
   4 ES4626H  LAB_SWITCH_4 CA 01-02-03-04-05-04 eth 1/1/1  eth 1/1/4  Y
.....................................................................................
2  2 ES4626H  LAB_SWITCH_2 M  01-02-03-04-05-02 eth 1/1/1  eth 1/1/2  -
   5 ES3528M  LAB_SWITCH_1 OC 01-02-03-04-05-13 eth 1/1/1  eth 1/1/2  Y
   6 ES3528M  LAB_SWITCH_1 OM 01-02-03-04-05-14 eth 1/1/1  eth 1/1/3  Y
-------------------------------------------------------------
Switch#show cluster topology root-sn 2
Role: commander(CM);Member(M);Candidate(CA);Other commander(OC);Other member(OM)
SN Description Hostname Role MAC_ADDRESS Upstream Upstream leaf
                                          local-port remote-port node
  == ============ ============ == ================= ============ ============ =
*  2 ES4626H  LAB_SWITCH_2 M  01-02-03-04-05-02 eth 1/1/1  eth 1/1/2  -
   5 ES3528M  LAB_SWITCH_1 OC 01-02-03-04-05-13 eth 1/1/1  eth 1/1/2  Y
   6 ES3528M  LAB_SWITCH_1 OM 01-02-03-04-05-14 eth 1/1/1  eth 1/1/3  Y
---------------------------------------------
Switch#show cluster topology nodes-sn 2
Toplogy role:  Member
Member status: Active member (user-config)
SN:            2
```

MAC Address: 01-02-03-04-05-02
Description: ES4626H
Hostname : LAB_SWITCH_2
Upstream local-port: eth 1/1/1
Upstream node: 01-02-03-04-05-01
Upstream remote-port:eth 1/1/2
Upstream speed: 100full
Console#
---
Switch#show cluster topology mac-address 01-02-03-04-05-02
Toplogy role: Member
Member status: Active member (user-config)
SN: 2
MAC Address: 01-02-03-04-05-02
Description: ES4626H
Hostname : LAB_SWITCH_2
Upstream local-port: eth 1/1/1
Upstream node: 01-02-03-04-05-01
Upstream remote-port:eth 1/1/2
Upstream speed: 100full

## 1.3.18 rcommand commander

**命令：rcommand commander**
**功能：**在成员交换机上使用该命令远程管理和配置命令交换机。
**参数说明：**无。
**缺省情况：**无。
**命令模式：**特权模式。
**使用指南：**执行该命令后可以对命令交换机进行远程管理和配置，但要通过命令交换机上的 telnet 用户名密码验证。使用 exit 退出命令交换机的配置界面。该命令只能在成员交换机上运行。
**举例:** 在成员交换机上使用该命令进入命令交换机的配置界面。
Switch#rcommand commander

## 1.3.19 rcommand member

**命令：rcommand member *<member-id>***
**功能：**在命令交换机上使用该命令对集群的成员交换机进行远程配置管理。
**参数说明：**member-id：commander 分配给每个 commander 的 member 编号。范围 1～128。

**缺省情况**：无。

**命令模式**：特权模式。

**使用指南**：执行该命令后，远程登录到 member 上，进入 member 的特权模式。使用 exit 退出 member 的配置界面。由于使用的是内部私有 IP，所以 member 交换机将跳过 telnet 认证。此命令只能在 commander 上执行。

**举例**: 在命令交换机上进入 member-id 为 1 的成员交换机的配置界面。

Switch#rcommand member 1

# 1.4 USB

## 1.4.1 cd usb:

**命令：cd usb:**

**功能**：进入 USB 盘符。

**命令模式**：特权配置模式。

**缺省情况**：无。

**使用指南**：当有 U 盘存在时，进入 U 盘目录，并打印“Change the current directory to “usb:/”!”，若无此设备，需打印“Device “usb:” has not inserted！”。

**举例**：

Switch#cd usb：

Change the current directory to “usb:/”!

## 1.4.2 dir

**命令：dir**

**功能**：进入 U 盘目录，显示 U 盘信息。

**命令模式**：特权配置模式。

**缺省情况**：无。

**使用指南**：进入 U 盘目录，打印 U 盘下文件内容，无 U 盘插入，打印错误信息。

**举例**：

Switch#dir

drwx 4.0K 7.0tset

-rwx 1.2K bootex.log

drwx 4.0K crt

dr-x 4.0K recycler

drwx 8.0K reliability

drwx 4.0K test

-rwx 141.3K 186.pdf

drwx 4.0K new

Drive : usb:

Size:7.4G Used:227.6M Avaliable:7.2G Use:3%

## 1.4.3 delete

**命令：delete <filename>**

**功能：**删除文件内容

**命令模式：**特权配置模式。

**缺省情况：**无。

**举例：**将 usb 盘符下的 log.txt 删除。

Switch#delete log.txt

Delete file, Are you sure? (Y/N)?[N]y

Delete file ok.

## 1.4.4 rename

**命令：rename <source> <destination>**

**功能：**重命名文件名。

**命令模式：**特权配置模式。

**缺省情况：**无。

**使用指南：**source-源文件名；destination-目的文件名。若 U 盘未插入，会先判断目的文件名有效性，再判断源文件名有效性，若输入目的文件名无效，则打印错误信息。

**举例：**将 log1.txt 重命名为 log2.txt。

Switch#rename log1.txt log2.txt

Rename log1.txt to log2.txt ok!

## 1.4.5 copy

**命令：copy <source> <destination>**

**功能：**将源文件拷贝成目的文件。

**命令模式：**特权配置模式。

**缺省情况：**无。

**使用指南：**1）可以进行 U 盘的拷贝：copy source.txt destination.txt 将 usb 盘符下的 source.txt 拷贝成 destination.txt；

2）copy usb:/startup.cfg startup.cfg 将 usb 盘符下的 startup.cfg 升级到交换机中

同时支持反向传输：copy startup.cfg usb:/startup.cfg

3）copy usb:/boot.rom boot.rom 支持 usb 盘符下的 boot.rom 升级

同时支持反向传输：copy boot.rom usb:/boot.rom

4）copy usb:/nos.img nos.img 支持 usb 盘符下的 nos.img 升级

同时支持反向传输：copy nos.img usb:/nos.img

5）以上命令支持绝对路径和相对路径。

**举例：**当有 U 盘存在时，执行相应的 copy 操作；若无 U 盘，将打印下述不同的错误信息：

Switch#copy usb:/tt.txt usb:/tttt.txt

Device "usb:" has not inserted!

Read local file usb:/tt.txt error.

Switch #copy startup.cfg usb:/startup.cfg

Can't write in non-existent directory "usb:/"!

Write config usb:/startup.cfg error!

Write error.

Switch #

Switch #copy usb:/startup.cfg startup.cfg

Confirm to overwrite the existed destination file? [Y/N]:y

Get file "startup.cfg" length error!

Read local file usb:/startup.cfg error.

## 1.4.6 mkdir

**命令：mkdir <目录名>**

**功能：**创建目录。

**命令模式：**特权配置模式。

**缺省情况：**无。

**使用指南：**1）若创建的目录名与已经存在的目录和文件同名，创建不成功，同时打印“Target path is exist now!”；

2）若创建的目录名不存在，创建成功，并打印“Make directory ok.”信息。

**举例:**创建目录名为 sw1 的目录：

Switch#mkdir sw1

Make directory ok.

## 1.4.7 rmdir

**命令：rmdir <目录名>**

**功能：**删除已存在目录。

**命令模式：**特权配置模式。

**缺省情况：**无。

**使用指南：**如果目录存在，且已为空目录，则可以正确的删除。若目录存在，但不为空，则不能删除，打印错误提示信息。

**举例：**删除目录 sw1。

Switch#rmdir sw1

Remove directory, Are you sure? (Y/N)?[N]y

Remove directory ok.

# 1.5 设备管理

## 1.5.1 debug devsm

**功能：**显示设备管理收发报文的情况和板卡状态转换情况，该命令的 no 形式关闭 DEBUG 显示。

**参数：send** 显示发送出去的设备管理报文。

**receive** 显示接收的设备管理报文。

**state** 显示板卡的板卡状态转变信息。

**缺省情况：**缺省调试开关是关闭的。

**命令模式：**特权用户配置模式。

## 1.5.2 force runcfg-sync

**命令：force runcfg-sync**

**功能：**强制将 running-config 从 active master 同步到 standby master。

**命令模式：**特权用户配置模式。

**使用指南：**running-config 与 startup-config 不同时，通过此命令可以将 running-config 从 active master 同步到 standby master。这样主备切换时会采用新的 running-config 作为配置恢复信息。

## 1.5.3 force sync software-version

**命令：force {sm|} sync software-version {enable|disable}**

**功能：**堆叠形成过程中，强制同步 nos 版本到 sm 或者 slave 上面。

**命令模式：**特权用户配置模式。

**使用指南：**堆叠形成过程中，am 会检查新加入线卡与自身版本是否相同，不同则将自身的 img 同步到新加入线卡上

## 1.5.4 force switchover

**命令：force switchover**

**功能：**强行要求 active master 切换到 standby master 上。

**命令模式：**特权用户配置模式。

**使用指南：**存在 standby master 时，在 active master 上执行此命令会触发主备切换，原来的 standby master 会成为新的 active master。

## 1.5.5 reset slot

**命令：reset [<*memID*>] slot <*slotno*>**

**功能：**复位指定板卡。

**参数：*<memID>*** 为 VSF 模式下，成员设备的编号,取值范围为 1～8

**命令模式：**特权用户配置模式。

**使用指南：**reset 重启板卡的命令可以复位线卡和 Standby Master 主控板，但是不能复位 Active Master 主控板。

## 1.5.6 runcfg-sync

**命令：runcfg-sync [<*interval*>]**

**功能：**配置 running-config 同步间隔时间。

**参数：*<interval>***为同步时间间隔，单位为分钟，取值范围为 5～1440 或 0；0 表示关闭自动同步功能；如果不加任何参数表示打开 running-config 同步功能，当配置文件有变化时缺省同步时间间隔为 5 分钟。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省开启自动同步功能，默认每 5 分钟检查一次配置进行同步。

**使用指南：**此命令配置 active master 向 standby master 定时同步 running-config 的时间间隔。同步时间设置的过小会给交换机增加不必要的负担。如果配置不经常变化或变更后通过 write 命令保存了配置，建议关闭自动同步功能。

**举例：**设置 running-config 同步间隔时间为 1440 分钟。

Switch(config)#runcfg-sync 1440

## 1.5.7 show fan

**命令：show fan**

**功能：**显示风扇是否在位，工作状态是否正常以及风扇的速率。

**参数：**无。

**缺省情况：**不显示。

**命令模式：**特权用户配置模式。

**使用指南：**该命令显示风扇的运行情况，Fan board inserted 指风扇板是否在位；fan status 指运行状态是否正常；fan speed 指风扇运行速率。

**举例：**

switch#show fan

Fan board information:

| Fan No | Inserted | Status | Speed |
|---|---|---|---|
| 1 | YES | Normal | Low |
| 2 | YES | Normal | Low |
| 3 | YES | Normal | Low |

## 1.5.8 show power

**命令：show power**

**命令：show** power

功能： 显示各电源是否在位，工作状态是否正常。

参数： 无。

**缺省情况：** 不显示。

命令模式： 特权用户配置模式。

**使用指南：** power Inserted 指电源是否在位，power Status 指电源运行状态是否正常。

**举例：**

switch#show power

System power information:

| Power No | Inserted | Status |
|---|---|---|
| 1 | YES | Normal |
| 2 | NO | NA |

## 1.5.9 show slot

命令：show **[member <member-id>] slot <slot-id>**

**功能：**显示各板卡基本信息。

**参数：*<member-id>*** 为 VSF 模式下，成员设备的编号,取值范围为 1～8；***<slot-id>***为板卡所在槽号，盒式机槽位都是 1。

**缺省情况：**member-id 和 slot-id 如都不指定，缺省为列出 vsf 中所有板卡信息。

**命令模式：** 特权用户配置模式。

**使用指南：**执行此命令后，会显示各板卡的基本信息。其中，MCU state 指主控板卡上上电控制器的状态（上电控制器主机或从机）；MCU version 指上电控制器文件的版本；Uptime 指系统启动后的运行时间。

**举例：**

switch#show member 8 slot 1

----------member :8----------

Inserted : YES

Module type : Switch

Work mode : ACTIVE MASTER

Work state : RUNNING
Software package version : 7.6.3.1(R0001.0095)
Bootrom version : 7.6.9
CPLD version : 3.03
Hardware version : 1.0.1
Serial number : SW082610L112000015
Manufacture date : 3921/12/16
Temperature : 29C/84F
Uptime : 0 weeks, 0 days, 0 hours, 2 minutes, 11 seconds

## 1.5.10 show chip info

**功能：**查看 cpu 芯片信息和交换芯片信息
**参数：**无
**命令模式：**特权用户模式。
**缺省情况：**无
**使用指南：**无
**举例：**无

# 第 2 章 网络安全

## 2.1 网络安全

### 2.1.1 default user password macbased

**命令：service default user password macbased**

**no service default user password macbased**

**功能：**配置设备出厂缺省密码由设备 VLAN MAC 地址计算 MD5 后，通过特定组合生成，本命令的 no 操作为恢复出厂缺省密码。

**参数：**无。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**该命令行由vendor控制，当需要使用该功能时，添加该条配置到vendor缺省配置中，通过升级新vendor产生的img文件来开启该功能。

**举例：**无。

### 2.1.2 first-login change password

**命令：first-login change password**

**no first-login change password**

**功能：**配置用户初次登录时，强制修改缺省密码，本命令的 no 操作为无需强制修改缺省密码。

**参数：**无。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**该命令行由vendor控制，当需要使用该功能时，添加该条配置到vendor缺省配置中，通过升级新vendor产生的img文件来开启该功能。

**举例：**无。

### 2.1.3 userpassword restriction

**命令：userpassword restriction {min-length <1-32> | format-mix (<2-4>|)**

**| max-consecutive-char <2-32> | max-consecutive-identical-char <2-32>}**

**no userpassword restriction {min-length <1-32> | format-mix (<2-4>|)**

**| max-consecutive-char <2-32> | max-consecutive-identical-char <2-32> | }**

**功能：**配置密码强度检查，本命令的 no 操作为删除密码强度检查。

**参数：min-length <1-32>：**密码最小长度<1-32>；

**format-mix (<2-4>|)**：密码格式为混合模式，格式个数为<2-4>，不带参数默认为2种格式；

**max-consecutive-char <2-32>**：密码允许的相邻字符最大个数，<2-32>；

**max-consecutive-identical-char <2-32>**：密码允许的连续相同字符最大个数，<2-32>。

**缺省情况**：无。

**命令模式**：全局配置模式。

**使用指南**：若是需要对用户密码强度进行检查，即可配置该命令行。

**举例**：配置密码强度最小长度为 8，最少三种格式，连续相同字符最大个数为 3，相邻字符最大个数为 3

```
Switch#config terminal
Switch(config)#userpassword restriction min-length 8 format-mix 3
                max-consecutive-identical-char 3 max-consecutive-char 3
```

## 2.1.4 password valid-time

**命令**：**service user password valid-time <0-90>**

**no service user password valid-time**

**功能**：配置用户密码有效期，本命令的 no 操作为取消用户有效期配置。

**参数**：**<0-90>**：有效期天数<0-90>，0表示永久有效。

**缺省情况**：无。

**命令模式**：全局配置模式。

**使用指南**：若是需要密码有效期控制，即可配置该命令行。

**举例**：配置用户有效期为 30 天

```
Switch#config terminal
Switch(config)#service user password valid-time 30
```

## 2.1.5 user-login failed msg

**命令**：**user-login failed msg neutral**

**no user-login failed msg neutral**

**功能**：用户登录失败时，提示信息不包含认证失败具体原因的内容：密码错误、用户不存在等，仅提示登录失败的中性信息，本命令的 no 操作恢复默认提示信息。

**参数**：无。

**缺省情况**：提示登录失败的中性信息。

**命令模式**：全局配置模式。

**使用指南**：若是需要登录失败后提示中性信息，即可配置该命令行。

**举例**：配置用户登录失败后提示中性信息

```
Switch#config terminal
Switch(config)#user-login failed msg neutral
```

## 2.1.6 password feedback

**命令：password feedback (none|star)**

**no password feedback**

**功能：**配置用户登录时，密码不回显或者回显为*号，本命令的 no 操作为删除该规则。

**参数：none：**密码不回显；

**star：**密码显示*号。

**缺省情况：**默认显示*号。

**命令模式：**全局配置模式。

**使用指南：**若是需要配置密码显示规则，即可配置该命令行。

**举例：**配置密码显示为空

Switch#config terminal

Switch(config)#password feedback none

## 2.1.7 password security-config

**命令：userpassword security-config**

**no userpassword security-config**

**功能：**配置用户密码强制安全输入，本命令的 no 操作为取消强制用户密码安全输入。

**参数：无。**

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**若是需要用户密码强制安全输入，即可配置该命令行。

**举例：**配置用户密码强制安全输入

Switch#config terminal

Switch(config)#userpassword security-config

配置命令后，输入密码（所有密码）的时候需要按照以下操作进行

Switch(config)#username user privilege 15 password

Password:*******

## 2.1.8 boot-file security check

**命令：boot (img | startup-config) check enable**

**no boot (img | startup-config) check enable**

**功能：**配置 img、cfg 文件进行安全校验，本命令的 no 操作为取消 img、cfg 文件安全校验。

**参数：img：**img文件；

**startup-config：**cfg文件。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**若是需要对img、cfg文件进行安全检查，即可配置该命令行，该命令行生效为环境变量的方式，通过show boot-files可查看。

**举例：**配置 img 文件进行安全校验

Switch#config terminal

Switch(config)#boot img check enable

## 2.1.9 ssh-server dst-port

**命令：ssh-server dst-port *<port-number>***

**no ssh-server dst-port**

**功能：**配置/删除 SSH 服务器的端口号。no 命令为恢复默认配置。

**参数：***<port-number>*为设置的 SSH 服务端的端口号，范围 1025～65535。

**命令模式：**全局配置模式。

**缺省情况：**缺省端口号为 22。

**使用指南：**只有在 SSH 功能关闭时才可修改端口号，若已开启会提示先关闭功能再配置。设置了 SSH 服务器的端口号以后，只有当服务器正在尝试连接的端口号是 22 时，SSH 客户端登录时可以不指定端口号；否则如果是其他端口号，SSH 客户端登录时必须指定端口号。

**举例：**配置 SSH 服务端使用的端口号 1200。

Switch(config)# ssh-server dst-port 1200

## 2.1.10 telnet-server dst-port

**命令：telnet-server dst-port *<port-number>***

**no telnet-server dst-port**

**功能：**配置/删除 Telnet 服务器的端口号。no 命令为恢复默认配置。

**参数：***<port-number>*为设置的 Telnet 服务端的端口号，范围 1025～65535。

**命令模式：**全局配置模式。

**缺省情况：**缺省端口号为 23。

**使用指南：**只有在 Telnet 功能关闭时才可修改端口号，若已开启会提示先关闭功能再配置。设置了 Telnet 服务器的端口号以后，只有当服务器正在尝试连接的端口号是 23 时，Telnet 客户端登录时可以不指定端口号；否则如果是其他端口号，Telnet 客户端登录时必须指定端口号。

**举例：**配置 Telnet 服务端使用的端口号 1300。

Switch(config)# telnet-server dst-port 1300

## 2.1.11 snmp-server dst-port

**命令：snmp-server dst-port <port-number>**

**no snmp-server dst-port**

**功能：**配置/删除 snmp 服务与网管连接使用的端口号。no 命令为恢复默认配置。

**参数：***<port-number>*为设置的 snmp 服务与网管连接使用的端口号，范围 1025～65535。

**命令模式：**全局配置模式。

**缺省情况：**缺省端口号为 161。

**使用指南：**只有在 snmp 功能关闭时才可修改端口号，若已开启会提示先关闭功能再配置。在配置了 snmp 与网管连接所使用的端口号以后，通过网管管理设备时，网管端指定的端口号必须与 snmp-server dst-port 命令配置的端口号保持一致，否则无法连接设备。

**举例：**配置 snmp 服务与网管连接使用的端口号 1400。

Switch(config)# snmp-server dst-port 1400

## 2.1.12 ip http secure- ciphersuite

**命令：ip http secure-ciphersuite {aes128-gcm-sha256 | aes128-sha | aes128-sha256 | aes256-sha | aes256-sha256 | ecdhe-rsa-aes128-gcm-sha256 | ecdhe-rsa-aes128-sha | ecdhe-rsa-aes256-sha}**

**no ip http secure-ciphersuite**

**功能：**配置/删除 SSL 使用的加密套件。no 命令为恢复默认配置。

**参数：aes128-gcm-sha256** 加密算法 AES128_GCM_SHA256。

**aes128-sha** 加密算法 AES128_SHA。

**aes128-sha256** 加密算法 AES128_SHA256。

**aes256-sha** 加密算法 AES256_SHA。

**aes256-sha256** 加密算法 AES256_SHA256。

**ecdhe-rsa-aes128-gcm-sha256** 加密算法 ECDHE_RSA_AES128_GCM_SHA256。

**ecdhe-rsa-aes128-sha** 加密算法 ECDHE_RSA_AES128_SHA。

**ecdhe-rsa-aes256-sha** 加密算法 ECDHE_RSA_AES256_SHA。

**命令模式：**全局配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**如果使用了本命令配置了加密套件，则使用配置的加密套件进行加密的协商。加密套件的修改每次都需要重启 SSL 功能。

**举例：**配置 SSL 使用的加密套件 aes128-gcm-sha256。

Switch(config)# ip http secure- ciphersuite aes128-gcm-sha256

## 2.1.13 ssh-server encryption-algorithm

**命令：ssh-server encryption-algorithm (add | remove) {aes128-cbc | 3des-cbc | aes128-ctr | aes256-ctr | aes256-cbc | 3des-ctr | all}**

**no ssh-server encryption-algorithm**

**功能：**配置/删除 SSH 服务器端的加密算法。no 命令为恢复默认配置。

**参数：add | remove** 添加或者移除算法。

**aes128-cbc** 加密算法 AES128_CBC。

**3des-cbc** 加密算法 3DES_CBC。

**aes128-ctr** 加密算法 AES128_CTR。

**aes256-ctr** 加密算法 AES256_CTR。

**aes256-cbc** 加密算法 AES256_CBC。

**3des-ctr** 加密算法 3DES_CTR。

**all** 表示所有的加密算法。

**命令模式：**全局配置模式。

**缺省情况：**默认开启三种算法：aes128-ctr，aes256-ctr，3des-ctr。

**使用指南：**SSH 服务器端的加密算法必须包含 SSH 客户端的算法，不然会协商失败导致无法连接成功。

**举例：**配置 SSH 服务器端使用所有的加密算法。

Switch(config)# ssh-server encryption-algorithm add all

## 2.1.14 service password-encryption type user

**命令：service password-encryption type user algo (md5|sha256|aes (salt|)|sm4 (salt|))**

**no service password-encryption type user**

**功能：**配置密码使用 sm4/AES 算法加密输出在配置文件中，保证设备的安全性，搭配盐值配置，确保密码的多样性。

**参数：md5** md5加密算法

**sha256** sha256加密算法

**sm4** sm4国密加密算法

**aes** aes加密算法

**salt** 盐值，使用盐值双重加密。

**命令模式：**全局配置模式。

**缺省情况：**缺省不启用

**使用指南：**必须要先配置 service password-encryption，才能配置当前命令，保证命令生效。

**举例：**配置使用 sm4 加密配置中的密码，且携带盐值。

Switch(config)# service password-encryption type user algo sm4 salt

## 2.1.15 bfd authentication key md5

**命令：*bfd authentication key <1-255> md5 (0 WORD |7 WORD|WORD|)***

**no bfd authentication key *<1-255>***

**功能：**配置 BFD 使用的 key 和 md5 方式加密的认证字符串。no 命令为删除配置的 key。

**参数：**<*1-255*>密钥号，<*WORD*>认证密钥串，长度为 1-16 个字节。设置密码时，若输入选项为 0，则应输入明文密码，且不对输入的明文密码进行加密处理； 若输入选项为 7，则应输入明文密码加密后的密文字符串；直接回车则进入安全模式输入密码。

**缺省情况：**缺省没有配置认证的 key 和认证字符串。

**命令模式：**全局配置模式。

**使用指南：**配置 BFD 认证使用的 md5 模式和认证密钥串，配置该命令后 BFD 会使用报文

中的可选字段进行认证，只有 BFD 两端的密钥配置一致时 BFD 才会建立邻居。

**举例：**采用 MD5 方式加密，密钥号为 1，认证字符串为 123456。

s5(config)#in vlan 50

s5(config)#bfd authentication key 1 md5 123456

## 2.1.16 enable password

**命令：enable password (level <1-15> |) (0 LINE|7 WORD|LINE|)**

**no enable password [level <*1-15*>]**

**功能：**修改从普通用户配置模式进入特权用户配置模式的口令。

**参数：level <*1-15*>**用于指定权限级别，默认为 15 级。**<*WORD*> <*LINE*>**为用户设置的密码，在 设置密码时，若输入选项为 0，则应输入明文密码，且不对输入的明文密码进行加密处理； 若输入选项为 7，则应输入明文密码加密后的密文字符串；直接回车则进入安全模式输入密码。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省的特权用户口令为空。

**使用指南：**配置特权用户口令，可以防止非特权用户的非法侵入，建议网络管理员在首次配置交换机时就设定特权用户口令。另外当管理员需要长时间离开终端屏幕时，最好执行 exit 命令退出特权用户配置模式。

## 2.1.17 enable trustview key

**命令：enable trustview key (0 WORD|7 WORD|)**

**no enable trustview key**

**功能：**配置私有报文的 DES 加密密钥，本命令同时也是交换机启用私有报文加密/散列功能的开关。

**参数：<*WORD*>**是长度小于 16 的字符串，用作 DES 加密密钥。0 表示以明文方式显示密钥，7 表示以密文方式显示密钥，直接回车则进入安全模式输入密码。

**命令模式：**全局配置模式。

**缺省情况：**交换机默认没有配置 DES 加密密钥，即交换机默认不启用私有报文加密/散列功

能。

**使用指南：**交换机与 DCN 内网安全管理后台系统通过私有报文进行私有信息的传输，在默

认情况下，私有报文是以明文传递的，为了防止私有报文被窃听破解，可选择对私有报文的内容进行加密，同时，管理员也需要在 DCN 内网安全管理后台配置相同的密钥。

**举例：**使能私有报文的加密/散列功能。

Switch(config)#enable trustview key 0 digitalchina

## 2.1.18 ip ftp

**命令：*ip ftp username <username>password (0 LINE|7 WORD|LINE|)***

**no ip ftp username <*username*>**

**功能：**配置 FTP 登录用户名和登陆口令；本命令的 no 操作为删除配置的用户名，同时也删除密码。

**参数：*<username>***为 FTP 连接的用户名，取值范围不超过 32 字符； ***<LINE> <WORD>*** 为 FTP 连接时使用的密码，在设置密码时，若输入选项为 0，则应输入明文密码，且不对输入的明 文密码进行加密处理；若输入选项为 7，则应输入明文密码加密后的密文字符串；直接回车则进入安全模式输入密码。

**缺省情况：**系统缺省为匿名 FTP 连接。

**命令模式：**全局配置模式。

**举例：**配置用户名为 Switch，密码为 superuser。

Switch#

Switch#config

Switch(config)#ip ftp username Switch password 0 superuser

Switch(config)#

## 2.1.19 ntp authentication-key

**命令：ntp authentication-key <key-id> md5 (0 WORD | 7 WORD |)**

**no ntp authentication-key *<key-id>***

**功能：**启动/取消 NTP 身份验证功能，定义 NTP 身份验证的验证密钥。

**参数：*key-id***：密钥编号，范围为 1-4294967295。 ***WORD***：密钥值，1-16 个 ascii 码字符。直接回车则进入安全模式输入密码。

**缺省情况：**不配置 NTP 身份验证的验证密钥。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**定义 NTP 身份验证的验证密钥，key-id 为 20，md5 为 abc。

Switch(config)#ntp authentication-key 20 md5 abc

## 2.1.20 password

**命令：password (0 LINE|7 WORD|LINE|)**

**no password**

**功能：**设置用户在 console 上进入一般用户配置模式时的口令，该命令的 no 形式删除配置的口令。

**参数：*<LINE> <WORD>***为用户设置的密码，在设置密码时，若输入选项为 0，则应输入明文密码，且不对输入的明文密码进行加密处理；若输入选项为 7，则应输入明文密码加密后的密文字符串；直接回车则进入安全模式输入密码。

**命令模式：**全局配置模式。

**缺省情况：**系统缺省该口令为空。

**使用指南：**如果配置了该口令，并且设置了 login 命令后，在 console 上进入一般用户配置

模式时，需要验证该口令，才能进入一般用户配置模式。

**举例：**

Switch(config)#password 0 test

Switch(config)#login

## 2.1.21 radius-server accounting host

**命令：radius-server accounting host {{vrf <vrf-name>| }<ipv4-address> |**

**<ipv6-address>} ((port <port**

**number>|) (key (0 WORD|7 WORD| WORD)|) (primary|)|)**

**no radius-server accounting host {*<ipv4-address>* | *<ipv6-address>*}**

**功能：** 设置 RADIUS 计费服务器 IPv4 或者 IPv6 地址和监听端口号、是否为主用服务器；本命令的 no 操作为删除 RADIUS 计费服务器。

**参数： <vrf-name>为指定的 VRF 名称**

**{*<ipv4-address>* | *<ipv6-address>*}** 服务器的 IPv4 地址或者 IPv6 地址。

***<port-number>*** 为服务器的监听端口号，取值范围为 0~65535。

***<WORD>*** 为密钥字符串。如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符；如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符；直接回车则进入安全模式输入密码。

**[primary]** 是否设为主用服务器，在配置 radius server 时，可以配置多个，使用顺序如果不配置 primary 时，按配置顺序查找可以使用的 radius server。如果配置的 primary，则首先使用这个 radius server。

**命令模式：**全局配置模式。

**缺省情况：**系统没有设置 RADIUS 计费服务器。

**使用指南：**本命令用于指定与交换机进行计费的 RADIUS 服务器的 IPv4 地址或者 IPv6 地址和端口号，可以配置多条该命令。其中参数***<port-number>***用于指定计费端口号，该端口号必须与指定的 RADIUS 服务器上的计费端口号相同，缺省为 1813，若将该端口号配置为 0，端口随机产生，可能导致无效。本命令可以反复配置多条以指定多台与交换机建立通讯关系的 RADIUS 服务器，交换机将向所有配置好的计费服务器发送计费报文，所配置的这些 RADIUS 计费服务器可以相互作为备份服务器。如果配置 primary，则将此 RADIUS 服务器作为主用服务器。只能配置一个 RADIUS 主服务器，不管该服务器使用 IPv4 还是 IPv6 地址。

**举例：**设置 RADIUS 计费服务器的 IPv6 地址为 2004:1:2:3::2，端口号为 3000，并作为主用服务器。

Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary

## 2.1.22 radius-server authentication host

**命令：radius-server authentication host {*<ipv4-address>* | *<ipv6-address>*} (port <0-65535>|)(primary|escape-server|) (access-mode (telnet|dot1x)|)(key (0 WORD |7 WORD| WORD|)|)**

**no radius-server authentication host {*<ipv4-address>* | *<ipv6-address>*}**

**功能：** 设置 RADIUS 认证服务器 IPv4 地址或者 IPv6 地址和监听端口号、加密密钥、是否为主用服务器以及使用模式；本命令的 no 操作为删除 RADIUS 服务器。

**参数：{*<ipv4-address>* | *<ipv6-address>*}** 服务器的 IPv4 地址或者 IPv6 地址。

***<port-number>*** 为服务器的监听端口号，取值范围为：0～65535。

***<WORD>*** 为密钥字符串。如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符；如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符；直接回车则进入安全模式输入密码。

**[primary]**是否设为主用服务器，在配置 radius server 时，可以配置多个，使用顺序如果不配置 primary 时，按配置顺序查找可以使用的 radius server。如果配置的 primary，则首先使用最后配置的这个 radius server。

**[access-mode {dot1x | telnet}]** 指明当前 RADIUS 服务器只为 802.1x 认证或 telnet 远程认证使用，默认所有服务均可使用当前 RADIUS 服务器。

**命令模式：**全局配置模式。

**缺省情况：**系统没有设置 RADIUS 认证服务器。

**使用指南：**本命令用于指定与交换机进行认证的 RADIUS 服务器的 IPv4 地址或者 IPv6 地址和端口号以及密钥字符串和访问模式，可以配置多条该命令。其中参数***<port-number>*** 用于指定认证端口号，该端口号必须与指定的 RADIUS 服务器上的认证端口号相同，缺省为 1812，若将该端口号配置为 0 端口随机产生，可能导致无效。本命令可以反复配置多条以指定多台与交换机建立通讯关系的 RADIUS 服务器，其中以配置的顺序作为交换机认证

服务器的顺序，当第一服务器有响应（无论是认证成功或失败）时，交换机不向下一个服务器发送认证请求。如果配置 primary，则将此 RADIUS 服务器作为主用服务器。当前 RADIUS 服务器若没有配置 key <string>，则使用命令 **radius-server key <string>全**局配置的密钥。另外，还可以通过 access-mode 选项指定当前 RADIUS 服务器只为 802.1x 认证或 telnet 远程认证使用。默认不配置 access-mode 选项，所有远程认证服务均可使用该 RADIUS 服务器。

**举例：**配置 RADIUS 认证服务器的 IPv6 地址为 2004:1:2:3::2。

Switch(config)#radius-server authentication host 2004:1:2:3::2

## 2.1.23 radius-server key

**命令：radius-server key (0 WORD|7 WORD|)**

**no radius-server key**

**功能：** 设置 RADIUS 服务器（包括认证和计费）的密钥；本命令的 no 操作为删除 RADIUS 服务器的密钥。

**参数：<*WORD*>** 为 RADIUS 服务器的密钥字符串。如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符；如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符；直接回车则进入安全模式输入密码。

**命令模式：** 全局配置模式。

**使用指南：** 该密钥为交换机与设置的 RADIUS 服务器进行加密的报文通信使用。该设置的密钥必须与交换机设置的 RADIUS 服务器上的密钥相同，否则将不能进行正确的 RADIUS 认证和计费。

**举例：** 配置 RADIUS 认证密钥为 test。

Switch(config)#radius-server key 0 test

## 2.1.24 tacacs-server authentication host

**命令：tacacs-server authentication host {{vrf <vrf-name>| } <ip-address>} [port <port-number>][timeout <seconds>][key (0 WORD|7 WORD|WORD|)][primary]**

**no tacacs-server authentication host <ip-address>**

**功能：** 设置 TACACS+服务器 IP 地址、监听端口号、认证服务器超时时间、密钥字符串；本命令的 no 操作为删除 TACACS+认证服务器。

**参数：<vrf-name>为指定的 VRF 名称**

***<ip-address>*** 服务器的 IP 地址；***<port-number>*** 为服务器的监听端口号，取值范围为 0~65535，其中 0 表示不作认证服务器使用；***<seconds>*** 为 TACACS+认证超时定时器值，单位为秒，取值范围为 1~60； ***<WORD>*** 为密钥字符串，如果密钥类型选项为 0，

则后续指定明文密钥，取值范围不超过 64 个字符，如果选项为 7，则后续指定为明文密钥加密后的密文字串，直接回车则进入安全模式输入密码；该密文字串解密后对应的明文长度不超过 64 个字符；primary 为主用服务器。

**命令模式：**全局配置模式。

**缺省情况：**系统没有设置 TACACS+认证服务器。

**使用指南：** 本命令用于指定与交换机进行认证的 TACACS+服务器的 IP 地址、端口号、认证服务器超时时间和密钥字符串，可以配置多条该命令。其中参数 port 用于指定认证端口号，该端口号必须与指定的 TACACS+服务器上的认证端口号相同，缺省为 49，参数 key 和 timeout，用于设置该服务器自身单独的 key 和 timeout，如果不配置这两个参数，缺省使用 **tacacs-server key <*string*>**，**tacacs-server timeout <*seconds*>** 全局配置命令；本命令可以反复配置多条以指定多台与交换机建立通讯关系的 TACACS+服务器，其中以配置的顺序作为交换机认证服务器的顺序。如果配置 **primary**，则将此 TACACS+服务器作为主用服务器。

**举例：**配置 TACACS+认证服务器地址为 192.168.1.2，且使用全局配置的 key。

Switch(config)#tacacs-server authentication host 192.168.1.2

## 2.1.25 tacacs-server key

**命令：tacacs-server key (0 WORD|7 WORD|)**

**no tacacs-server key**

**功能：** 设置 TACACS+认证服务器的密钥；本命令的 no 操作为删除 TACACS+服务器的密钥。

**参数：** ***<WORD>*** 为 TACACS+服务器的密钥字符串，如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符，如果选项为 7，则后续指定为明文密钥加密后的密文字串，直接回车则进入安全模式输入密码，该密文字串解密后对应的明文长度不超过 64 个字符。

**命令模式：** 全局配置模式。

**使用指南：** 该密钥为交换机与 TACACS+服务器进行加密的报文通信使用。该设置的密钥必须与 TACACS+服务器上的密钥相同，否则将不能进行正确的 TACACS+认证。为保证 TACACS+认证数据的安全，建议配置认证服务器密钥。

**举例：** 配置 TACACS+服务器认证密钥为 test。

Switch(config)# tacacs-server key 0 test

## 2.1.26 username

**命令：username <*username*> [privilege <*privil*ege>] [password (0 LINE|7 WORD|LINE|)]**

**no username *<username>***

**功能：**在本地设置利用用户名和密码验证方式登录的用户及其优先级。

**参数：*<username>***为用户名，取值范围不超过 32 字符；***<privilege>***为该用户可执行的命令的最大等级，级别为 1-15，缺省级别为 1；***<LINE> <WORD>***为用户密码，如果在设定密码时，输入选项为 0，则应输入明文密码，且不对输入的明文密码进行加密处理；若输入选项 7，则应输入明文密码加密后的密文字符串（使用 MD5 加密的 32 位密码）；直接回车则进入安全模式输入密码。

**命令模式：**全局配置模式。

**使用指南：**目前系统中注册的命令有两个优先级 1 和 15。优先级为 1 的命令注册在一般用户配置模式。优先级为 15 的命令注册在除一般用户配置模式以外的其它模式。本命令最多允许配置 16 个本地认证用户，密码最大长度为 32。

**注意：**用户利用该命令配置完毕可登录的用户和优先级，在执行 authentication line console login local 命令（使能 Console 登录方式的本地用户验证）以前，必须确保有一个用户的优先级为 15，以便能够利用该用户进行登录，并进入特权模式和全局配置模式，修改系统的配置。当配置的本地用户没有一个权限达到 15，并且 Console 登录验证方式仅仅配置了 Local 方式时，通过 Console 可以直接登录交换机而不需要验证。在以 HTTP 方式访问交换机时，必须使用执行命令等级为 15 的用户登录交换机，优先级低于 15 的用户登录必会被拒绝。

**举例：**配置一个管理员用户 admin，优先级为 15，配置两个普通用户，优先级为 1，并启用 本地用户名和密码登录认证方式。其中只有用户 admin 可以通过 Telnet 或 Console 登录至特权模式下，user1 与 user2 的只能通过 Telnet 或 Console 登录至一般用户配置模式。HTTP 登录方式下，只有 admin 才能登录成功，user1 与 user2 的登录权限均不足。

Switch(config)#username admin privilege 15 password 0 admin

Switch(config)#username user1 privilege 1 password 7

4a7d1ed414474e4033ac29ccb8653d9b(该密码为 0000 使用 MD5 加密的 32 位暗文密码)

Switch(config)#username user2 password 0 user2

Switch(config)#authentication line console login local

# 第 3 章 二层业务命令

## 3.1 端口配置

### 3.1.1 以太网端口配置命令

#### 3.1.1.1 Bandwidth

**命令：bandwidth control <*bandwidth*> [both | receive | transmit]**

**no bandwidth control**

**功能：**打开端口的带宽限制功能；本命令的 no 操作为关闭端口的带宽限制功能。

**参数：<*bandwidth*>**为限制带宽，单位为 Kbps，若为千兆带宽，取值范围为 1-1000000K，若为百兆带宽，取值范围为 1-100000K；**both** 为端口收发时均进行带宽控制；**receive** 为仅在端口从交换机外接收数据时进行带宽控制；**transmit** 为仅在端口向交换机外发送数据时进行带宽控制。

**命令模式：**端口配置模式。

**缺省情况：**端口缺省关闭带宽限制功能。

**使用指南：**当端口设置了带宽限制功能，并且指定了限制带宽的大小，那么端口的最大带宽就被确定，而不以 10/100/1000M 为最大带宽。如果不指定[both | receive | transmit]关键字，缺省为 both。汇聚端口配置模式下，当配置不同带宽限制值时，由于存在一定的精度，输入的值可能跟实际值有些许偏差，

注意：设置端口带宽限制值不能超过端口可能的物理连接最大速度。例如一个 10/100M 以太网端口不能设置为限制 101000K（或 101000K 以上）的带宽。但是当一个 10/100/1000M 端口工作在 100M 速度时，可以设置 101000K（或 101000K 以上）流量限制。实际设置的带宽为芯片带宽粒度的整数倍，若用户输入不满足该条件，将会被自动修改。例如芯片带宽粒度为 10K，而用户输入为 1，那么软件会提示用户，带宽将被转换为 10K。

**举例：**设置以太网端口 1/1/1-8 的收发带宽限制为 40000K。

Switch(config)#interface ethernet 1/1/1-8

Switch(Config-If-Port-Range)#bandwidth control 40000 both

#### 3.1.1.2 clear counters interface

**命令：clear counters [interface {ethernet <*interface-list*> | vlan <*vlan-id*> | port-channel <*port-channel-number*> | <*interface-name*>}]**

**功能：**清除指定端口的统计信息。

**参数：<*interface-list*>**是以太网端口号，**<*vlan-id*>**是 VLAN 接口号，**<*port-channel-number*>**是汇聚接口号，**<*interface-name*>**为接口名称如 port-channel1。

**命令模式：**特权用户配置模式。

**缺省情况**：缺省不会删除端口的统计信息。

**使用指南**：如果不指定端口，则删除所有端口的统计信息。

**举例**：清除以太网端口 1/1/1 的统计信息。

Switch#clear counters interface ethernet 1/1/1

### 3.1.1.3 description

**命令**：**description <*string*>**

**no description**

**功能**：为指定的端口设置名字；本命令的 no 操作为取消该项配置。

**参数**：**<*string*>**为字符串，最长不超过 200 个字符。

**命令模式**：端口配置模式。

**缺省情况**：端口缺省没有名字。

**使用指南**：本命令有助于用户管理交换机，如用户可以根据端口的使用情况设置名字，如 1/1/1-2 号端口归财务部门使用，则定义为 financial，1/1/9 号端口归工程部门使用，则定义了 engineering，1/1/12 号端口连接服务器，则定义 Servers。这样端口的使用情况就一目了然了。

**举例**：指定 1/1/1-2 端口 description 为 financial。

Switch(config)#interface ethernet 1/1/1-2

Switch(Config-If-Port-Range)#description financial

### 3.1.1.4 flow control

**命令**：**flow control**

**no flow control**

**功能**：打开指定端口的流控功能；本命令的 no 操作为关闭端口的流控功能。

**命令模式**：端口配置模式。

**缺省情况**：端口的流控功能缺省为关闭。

**使用指南**：打开端口的流控功能后，当端口接收到的流量大于端口缓存所能容纳的大小时，端口将通过算法或者协议通知向其发送流量的设备减慢发送速度，以防止丢包。交换机的端口支持基于背压的 802.3X 流量控制；端口工作在半双工模式下，支持背压流控。当背压控制达到可能出现严重的头阻塞（HOL）时，交换机将自动进行头阻塞控制（丢弃可能产生头阻塞的 COS 队列中的一些包），以避免网络性能大幅下降。

**注意**：除非用户需要一种速度慢，性能低，但包损失较小的网络，否则不建议用户打开端口流控功能。在打开端口的流控功能时，请务必确认两端的速率和双工模式相同。

**举例**：打开以太网端口 1/1/1-8 的流控功能。

Switch(config)#interface ethernet 1/1/1-8

Switch(Config-If-Port-Range)#flow control

### 3.1.1.5 hardware profile module <1-4> 4×10G

本型号交换机不支持此命令。

### 3.1.1.6 interface ethernet

**命令：interface ethernet *<interface-list>***

**功能：**从全局配置模式进入到以太网端口配置模式。

**参数：*<interface-list>***为端口号。

**命令模式：**全局配置模式。

**使用指南：**使用命令 **exit** 可从以太网端口配置模式退回到全局配置模式。

**举例：**进入以太网端口 1/1/1，1/1/4-5，1/1/8。

Switch(config)#interface ethernet 1/1/1;1/1/4-5;1/1/8

Switch(Config-If-Port-Range)#

### 3.1.1.7 interface mode

本型号交换机不支持此命令。

### 3.1.1.8 loopback

**命令：loopback**

**no loopback**

**功能：**设置以太网端口进行环回测试功能；本命令的 no 操作用来取消以太网端口的环回测试。

**命令模式：**端口配置模式。

**缺省情况：**以太网端口不进行环回测试。

**使用指南：**使用环回测试可以检验以太网端口是否正常工作。设置回环后，端口会假设已经和自己建立一个连接，所有从该端口发出的流量都会又从该端口收到。

**举例：**设置以太网端口 1/1/1-8 进行环回测试。

Switch(config)#interface ethernet 1/1/1-8

Switch(Config-If-Port-Range)#loopback

### 3.1.1.9 media-type

本型号交换机不支持此命令。

### 3.1.1.10 Negotiation

**命令：negotiation {on | off}**

**功能：**打开或关闭 10G 端口的自动协商功能。

**参数：**on 表示打开自动协商；off 表示关闭自动协商。

**命令模式：**端口配置模式。

**缺省情况：**缺省为协商打开。

**使用指南：**本命令只针对10G接口生效。对于1000M接口，negotiation命令不可用。

**举例：**交换机 Switch1 端口 1 同交换机 Switch2 端口 1 用线相连，将该两个端口设置为关闭协商。

Switch1(config)#interface ethernet1/1/49

Switch1(Config-If-Ethernet1/1/1)#negotiation off

Switch2(config)#interface ethernet1/1/49

Switch2(Config-If-Ethernet1/1/1)#negotiation off

### 3.1.1.11 port-rate-statistics interval

**命令：port-rate-statistics interval <interval-value>**

**功能：**设置端口速率统计的间隔时间。间隔时间范围 5—600。

**参数：**interval-value，端口速率统计的间隔时间，以秒为单位，取值为<5-600>，以 5 秒为步长。

**缺省情况：**缺省只能看到 5 秒和 5 分钟的端口速率统计值。

**命令模式：**全局模式。

**使用指南：**无。

**举例：**统计端口速率统计时间为 20 秒。

Switch(config)#port-rate-statistics interval 20

### 3.1.1.12 port-scan-mode

**命令：port-scan-mode {interrupt | poll}**

**no port-scan-mode**

**功能：** 配置扫描端口方式为中断或查询方式。本命令的 no 操作恢复默认的端口扫描方式。

**参数：** interrupt：中断方式；poll：查询方式。

**命令模式：** 全局配置方式。

**缺省情况：** 缺省为查询方式。

**使用指南：** 交换机有两种方式响应端口 up/down 事件。中断方式是指，由硬件中断通知端口 up/down 事件变化。查询方式是指，由软件查询来 获得端口事件。中断方式速度快于查

询方式。此功能会影响 mrpp 环网的收敛时间。若使用查询方式，在简单环网内，mrpp 收敛时间为几百毫秒；若使用中断方式，收敛时间在 50 毫秒以内。

注意：一般情况下，端口扫描配置为查询方式即可。中断方式仅适用于对性能要求较高的环境。相比于中断，查询方式的安全性更高。

**举例：** 设置端口扫描为中断方式

Switch(config)#port-scan-mode interrupt

### 3.1.1.13 port-status-check interval

本型号交换机不支持此命令。

### 3.1.1.14 rate-violation

**命令：rate-violation {unicast | broadcast | multicast |all} <200-148809523>**

**no rate-violation**

**功能： 设置交换机端口的报文最大收包速率，如果端口的接收报文速率违背了收包速率则 shutdown 端口或者 block 端口，本命令的 no 操作为关闭端口的速率违背功能。**

**本命令的违背速率是指该端口接收所有报文的速率，即每秒钟接收的报文数量，可区分具体的报文类型。**

**参数： <200-148809523>：** 端口最大收包速率，单位 packets/s

**命令模式： 端口配置模式**

**缺省情况：** 缺省端口速率违背无控制操作。

使用指南： 该命令主要应用于端口流量异常的情况，比如端口出现环路，导致出现大量的广播报文影响交换机对其他业务的处理，此时通过 shutdown 出问题的端口，来保证交换机对其他业务的正常处理。

举例：设置交换机 1/0/8-10 号端口（千兆）的单播报文违背速率为 10000pps。

**Switch(Config)**#interface ethernet 1/0/8-10

Switch(Config-Port-Range)#rate-violation unicast 10000

### 3.1.1.15 rate-violation all-bits

**命令：rate-violation all-bits <1- 100000>**

**no rate-violation all-bits**

**功能： 设置交换机端口的报文最大收包速率，如果端口的接收报文速率违背了收包速率则 shutdown 端口或者 block 端口，本命令的 no 操作为关闭端口的速率违背功能。**

**本命令的违背速率是指该端口接收报文的速率。**

**参数： <1- 100000>：** 端口最大收包速率，单位 Mbps/s

**命令模式： 端口配置模式**

**缺省情况：** 缺省端口速率违背无控制操作。

使用指南： 该命令主要应用于端口流量异常的情况，比如端口出现环路，导致出现大量的广播报文影响交换机对其他业务的处理，此时通过 shutdown 出问题的端口，来保证交换机对其他业务的正常处理。

举例：设置交换机 1/0/8-10 号端口的报文违背速率为 1000Mbps。

**Switch(Config)**#interface ethernet 1/0/8-10

Switch(Config-Port-Range)#rate-violation all-bits 1000

## 3.1.1.16 rate-violation control

**命令：rate-violation control {shutdown | block }** recovery **<0-86400>**

**no rate-violation**

**功能： 设置交换机端口违背了收包速率则 shutdown 端口或者 block 端口，并且端口被 shutdown 或者 block 后自动恢复端口的时间。本命令的 no 操作为关闭端口的速率违背控制功能。**

**参数： <0-86400>：端口恢复时间，单位为秒。**

**命令模式： 端口配置模式**

**缺省情况：** 缺省端口速率违背无控制操作。

使用指南： 该命令主要应用于端口流量异常的情况，比如端口出现环路，导致出现大量的广播报文影响交换机对其他业务的处理，此时通过 shutdown 出问题的端口，来保证交换机对其他业务的正常处理。

举例：设置交换机 1/0/8-10 号端口（千兆）的单播报文违背速率动作为 shutdown，恢复时间为 20s。

**Switch(Config)**#interface ethernet 1/0/8-10

Switch(Config-Port-Range)#rate-violation control shutdown recovery 20

## 3.1.1.17 remote-statistics interval

本型号交换机不支持此命令。**命令：remote-statistics interval <*seconds*>**

**功能：** 设置机架式交换机线卡端口流量统计间隔时间。

**参数：** ***<seconds>*** 为线卡端口流量统计间隔时间，单位为秒，取值范围为 5～300，且应当是 5 的倍数。

**命令模式：** 全局配置模式。

**缺省情况：** 缺省的线卡端口流量统计间隔时间为 60 秒。

**使用指南：** 在机架式交换机上，各个线卡每间隔一定时间自动向主控卡通报其各个端口的流量信息，主卡上保存所有线卡各个端口的流量信息。当网管软件向主控卡发起请求操作时，

主控卡将本地保存的各个线卡的端口的流量信息直接发送给网管软件，这样可以使各种网管软件在正常监控流量时不会影响其它业务。

应当注意的是：线卡向主控卡通报流量的间隔时间减小，则流量统计越精确，但占用系统资源也就越大；间隔时间加长，则流量统计误差加大，但占用系统资源越小。因而在实际运营中，该间隔时间应当根据实际情况合理地选择。否则由于网管软件监控机架式交换机时读取流量信息需要花费一定的时间，以及网管软件监控交换机流量的间隔时间与线卡向主控卡通报流量间隔时间之间存在不匹配，流量监控中可能出现各种毛刺现象。

在实际运营中，为了使网管软件对交换机业务不造成大的影响，而又能够获取到比较精确的流量统计信息，推荐网管软件监控交换机流量的间隔时间是线卡向主控卡通报流量间隔时间的 10 倍。由于线卡向主控卡通报流量间隔时间缺省为 60 秒钟，因而推荐网管软件监控交换机流量的间隔时间为 600 秒钟，即 10 分钟。

**举例：** 网管软件监控机架式交换机流量的间隔时间为 900 秒钟，则在交换机上设置线卡端口流量统计间隔时间为 90 秒。

```
Switch(config)#remote-statistics interval 90
```

## 3.1.1.18 show interface

**命令：show interface [ethernet <interface-number> | port-channel <port-channel-number> | loopback <loopback-id> | vlan <vlan-id> | tunnel <tunnel-id> | <interface-name>] [detail]**

**show interface ethernet statu s**

**show interface ethernet counter {packet | rate}**

**功能：** 显示交换机三层接口或二层端口的相关信息。

**参数：** ***<vlan-id>*** 是 VLAN 接口，取值范围 1-4094， **<tunnel-number>** 是隧道号，取值范围 1-50， **<loopback-id>** 是环回接口序号，取值范围为 1-1023， ***<interface-number>*** 是以太网端口号，status 用于显示所有二层端口的重要状态信息，**counter {*packet* | rate}** 用于显示所有二层端口的包数量/速率统计信息，***<port-channel-number>*** 是汇聚接口号，***<interface-name>*** 为接口名称，如 port-channel1。 **[detail]** 用于显示端口的详细信息。

**命令模式：** 特权和配置模式。

**使用指南：** 对于 vlan 接口，本命令显示接口的 MAC 地址，IP 地址以及收发数据包的统计情况；对于 tunnel 接口，本命令显示隧道接口状态以及控制层收发隧道数据包的统计情况，关于物理接口收发隧道数据包的统计数据请参见 show interface ethernet 命令；对于 loopback 接口，本命令显示接口的 IP 地址以及收发数据包的统计情况；对于 ethernet 端口，本命令显示端口的端口速率、双工模式、流控开关情况、广播风暴抑制以及收发数据包的统计情况等；对于汇聚端口，本命令显示汇聚接口的端口速率、双工模式、流控开关情况、广播风暴抑制以及收发数据包的统计情况。如果不指定端口，则会显示交换机所有端口的信息。

对于 ethernet 和 port-channel 端口，可以用 **[detail]** 来显示端口的详细信息，具体的信息和机器、板卡的类型有关。

对于 ethernet 端口，使用 **status 以列表的形式显示所有二层端口的重要状态信息，每个端口一行，显示的信息包括端口号、Link 和 Protocol 状态、Speed、Duplex、Vlan、端口类型、端口名； counter packets** 显示所有 ethernet 端口的包数量统计信息，包括输入和输出方向的二层单播、广播、组播、错误的包数量； **counter rate** 显示所有 ethernet 端口的速率统计信息，为 5 分钟和 5 秒钟的输入和输出的包的数量及字节数。

**举例：**

显示端口 1/1/1 的信息。

```
switch(config)#show interface ethernet 1/1/1
Interface brief:
  Ethernet1/1/1 is up, line protocol is up
  Ethernet1/1/1 is layer 2 port, alias name is (null), index is 1
  Hardware is Gigabit-TX, address is 00-03-0f-d3-07-ef
  PVID is 1
  MTU 1500 bytes, BW 1000000 Kbit
  Time since last status change:0w-0d-1h-38m-25s  (5905 seconds)
  Encapsulation ARPA, Loopback not set
  Auto-duplex: Negotiation full-duplex, Auto-speed: Negotiation 1G bits
  FlowControl is off, MDI type is auto
Statistics:
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  The last 5 second input rate 0 bits/sec, 0 packets/sec
  The last 5 second output rate 0 bits/sec, 0 packets/sec
  The last 555 second input rate 0 bits/sec, 0 packets/sec
  The last 555 second output rate 0 bits/sec, 0 packets/sec
  Input packets statistics:
    2 input packets, 188 bytes, 0 no buffer
    0 unicast packets, 2 multicast packets, 0 broadcast packets
    0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored,
    0 abort, 0 length error, 0 undersize 0 jabber, 0 fragments, 0 pause frame
  Output packets statistics:
    2 output packets, 188 bytes, 0 underruns
    0 unicast packets, 2 multicast packets, 0 broadcast packets
    0 output errors, 0 collisions, 0 late collisions, 0 pause frame
```

显示所有二层端口的重要状态信息。

```
Switch#show interface ethernet status
Codes: A-Down - administratively down, a - auto, f - force, G - Gigabit
```

| Interface | Link/Protocol | Speed | Duplex | Vlan | Type | Alias Name |
|---|---|---|---|---|---|---|
| 1/1/1 | UP/UP | f-100M | f-full | 1 | G-TX | |
| 1/1/2 | UP/UP | a-100M | a-full | trunk | G-TX | |
| 1/1/3 | UP/DOWN | auto | auto | 1 | G-TX | |
| 1/1/4 | A-Down/DOWN | auto | auto | 1 | G-TX | |

…

显示所有二层端口的包数量统计信息

Switch#show interface ethernet counter packet

| Interface | | Unicast(pkts) | BroadCast(pkts) | MultiCast(pkts) | Err(pkts) |
|---|---|---|---|---|---|
| 1/1/1 | IN | 12,345,678 | 12,345,678,9 | 12,345,678,9 | 4,567 |
| | OUT | 23,456,789 | 34,567,890 | 5,678 | 0 |
| 1/1/2 | IN | 0 | 0 | 0 | 0 |
| | OUT | 0 | 0 | 0 | 0 |
| 1/1/3 | IN | 0 | 0 | 0 | 0 |
| | OUT | 0 | 0 | 0 | 0 |
| 1/1/4 | IN | 0 | 0 | 0 | 0 |
| | OUT | 0 | 0 | 0 | 0 |

…

显示所有二层端口的速率统计信息

Switch#show interface ethernet counter rate

| Interface | | IN(pkts/s) | IN(bytes/s) | OUT(pkts/s) | OUT(bytes/s) |
|---|---|---|---|---|---|
| 1/1/1 | 5m | 13,473 | 12,345,678 | 12,345 | 1,234,567 |
| | 5s | 135 | 65,800 | 245 | 92,600 |
| 1/1/2 | 5m | 0 | 0 | 0 | 0 |
| | 5s | 0 | 0 | 0 | 0 |
| 1/1/3 | 5m | 0 | 0 | 0 | 0 |
| | 5s | 0 | 0 | 0 | 0 |
| 1/1/4 | 5m | 0 | 0 | 0 | 0 |
| | 5s | 0 | 0 | 0 | 0 |

…

## 3.1.1.19 shutdown

**命令：shutdown**

**no shutdown**

**功能：**关闭指定的以太网端口；本命令的 no 操作为打开端口。

**命令模式：**端口配置模式。

**缺省情况：**以太网端口缺省为打开。

**使用指南：**当关闭以太网端口时，以太网端口将不发送数据帧，并且在用户输入 **show interface** 命令时显示端口状态为 down。

**举例：**打开 1/1/1-8 号端口。

Switch(config)#interface ethernet1/1/1-8

Switch(Config-If-Port-Range)#no shutdown

## 3.1.1.20 speed-duplex

**命令：speed-duplex {auto [10 [100 [1000]] [auto | full | half |]] | force10-half | force10-full | force100-half | force100-full | force100-fx [module-type {auto-detected | no-phy-integrated | phy-integrated}] | {{force1g-half | force1g-full} }| force10g-full}**

**no speed-duplex**

**功能：**设置 1000Base-TX、100Base-TX 或 100Base-FX 端口的速率和双工模式；本命令的 no 操作恢复速度双工的默认值，即自动协商速度和双工（auto）。

**参数：**auto 为自动协商速率双工，10 为 10Mbit/s 速率能力，100 为 100Mbit/s 速率能力，1000 为 1000Mbit/s 速率能力，auto 为双工能力协商，full 为全双工能力，half 为半双工能力；force10-half 为强制 10Mbit/s 速率，半双工模式；force10-full 为强制 10Mbit/s 速率，全双工模式；force100-half 为强制 100Mbit/s 速率，半双工模式；force100-full 为强制 100Mbit/s 速率，全双工模式；force100-fx 为强制 100Mbit/s 速率，全双工模式，光接口；module-type：百兆光模块类型；auto-detected：自动检测识别；no-phy-integrated：没有集成 PHY 百兆光模块；phy-integrated：集成 PHY 百兆光模块；force1g-half 为强制 1000Mbit/s 速率，半双工模式；force1g-full 为强制 1000Mbit/s 速率，全双工模式；nonegotiate 为强制关闭千兆端口自动协商；master 为强制千兆端口为 master 模式；slave 为强制千兆端口为 slave 模式；force10g-full 为强制 10000Mbit/s 速率，全双工模式。

**命令模式：**端口配置模式。

**缺省情况：**端口缺省为自动协商速率和双工模式（auto）。

**使用指南：**本命令用来配置端口的速率双工。在配置端口的速率和双工模式时，端口的速率和双工模式必须和对端设备速率和双工模式保持一致，即如果对端设备自动协商方式则本端也设置成自动协商方式；如果对端是强制方式，则本端也应设置成相应的强制方式。

目前不支持force1g-half的配置。

**举例：**交换机 Switch1 端口 1 同交换机 Switch2 端口 1 用线相连，将该两个端口设置为强制 100Mbit/s 速率，半双工模式。

Switch1(config)#interface ethernet1/1/1

Switch1(Config-If-Ethernet1/1/1)#speed-duplex force100-half

Switch2(config)#interface ethernet1/1/1

Switch2(Config-If-Ethernet1/1/1)#speed-duplex force100-half

## 3.1.1.21 storm-control

**命令：storm control {unicast | broadcast | multicast} {kbps <Kbits> | pps <PPS>}**

**no strom control {unicast | broadcast | multicast}**

**功能：** 设置交换机所有端口允许通过的广播、组播或未知地址的单播流量；本命令的 no 操作为关闭端口对广播、组播或未知地址的单播流量的抑制功能，即允许线速通过广播、组播或未知地址的单播流量。

**参数：** **unicast** 表示限制未知地址单播流量， **multicast** 表示限制组播流量， **broadcast** 表示限制广播流量。 ***<Kbits>*** 代表每秒钟允许通过的 Kbit 数，取值范围为 1-1000000。<PPS>代表每秒钟允许通过的 packet 个数，取值范围为 1-14880952。

**命令模式：** 端口配置模式。

**缺省情况：** 缺省不限制，允许线速通过广播、组播和未知地址的单播流量。

**使用指南：** 在没有任何 VLAN 设置的情况下，交换机的所有端口都处在同一个广播域。对于上述三种流量，交换机都会向广播域中的所有端口发送，可能形成广播风暴。广播风暴极其影响交换机的性能，打开交换机的广播风暴抑制功能，可以保护交换机尽量少地受广播风暴的影响。注意本命令对于万兆端口和其他端口的意义有区别。当设置端口允许通过的广播流量为 1000kbps 时，表示当端口每秒钟接收的 kbit 数大于 1000 时，多于 1000 的部分将被抑制。本交换机支持两种方式的限速，分别是按带宽限速(kbps)和按包的个数限速（pps），两种方式二选一，不能同时设置这两种方式。

广播抑制和带宽控制（bandwidth control）类似，芯片是有粒度限制的，以 kbps 限速时，本交换机的粒度为 8kbps。如果用户输入的<Kbits>不是 8 的整数倍，系统将自动调整为 8 的整数倍并将真实的限速值打印给用户显示。

对于广播抑制，broadcast、multicast、unicast 必须设置相同的阈值。

**举例：设置 1-8 号端口最多允许每秒钟通过 1000kbit 的广播数据包。**

Switch(config-if-port-range)#storm-control broadcast kbps 1000

## 3.1.1.22 storm-control bypass

**命令：storm-control bypass {arp | bpdu | igmp | rma | rtk} (enable |disable)**

**功能：** 指定 arp、bpdu、igmp、rma、rtk-packet 协议报文不受风暴控制影响。

**参数：** **arp** 表示 arp 协议报文， **bpdu** 表示 bpdu 协议报文， **igmp** 表示 igmp 协议报文，**rma** 表示 rma 协议报文，**rtk** 表示 rtk 协议报文。 **< enable >** 代表使能协议不受风暴控制影响，<disable>代表去使能。

**命令模式：** 全局配置模式。

**缺省情况：** 缺省去使能，这些协议受风暴控制的限速。

**使用指南：** 如果想让 arp 协议不被风暴控制限速，可以使能 arp 协议。

**举例：**如果想让 arp 协议不被风暴控制限速，可以使能 arp 协议。

Switch(config-if-port-range)#storm-control bypass arp enable

## 3.1.1.23 virtual-cable-test

**命令：virtual-cable-test interface (ethernet |)IFNAME**

**功能：** 对连接到以太网端口上的双绞线进行线路检测。返回的信息可能包括：线路正常（well）、线路短路（short）、线路断路（open）、检测失败（fail）。如果检测信息为非正常，则同时显示相应故障的位置（自端口起始以米为单位的长度）。

**参数：*<interface-list>*：**端口号

**命令模式：** 特权模式。

**缺省情况：** 没有进行线路检测。

**使用指南：** 待测双绞线所连的 RJ-45 接头必须符合 IEEE 802.3 对线序的规定，否则检测结果中的线对会与实际线对不相符。在百兆端口上，只使用到（1，2）与（3，6）两个线对，在检测结果中只有这两个线对的结果有效。若千兆端口另一端接百兆时，（4，5）线对与（7，8）线对的检测结果无效。检测结果会因双绞线的类型、当时的温度、工作电压等而产生误差，在温度为 20 摄氏度、电压恒定无干扰的环境下，待检测的双绞线长度不超过 100 米，这时允许存在+/-2 米的误差，如果端口是 Link UP 状态，此时允许+/-10 米的误差。注意，检测过程会中断待测线路上的所有数据流量，该状态在持续 5~10 秒后，自动恢复初始状态。

**注意：**combo 端口只在电口模式下支持 VCT 功能检测，百兆端口在 Link UP 的情况下无法诊断出线路长度。

568A 线序标准：（1 绿白，2 绿）、（3 橙白，6 橙）、（4 蓝，5 蓝白）、（7 棕白，8 棕）。

568B 线序标准：（1 橙白，2 橙）、（3 绿白，6 绿）、（4 蓝，5 蓝白）、（7 棕白，8 棕）。

**举例：** 检测千兆端口 1/1/25 所连双绞线的线路状态。

```
Switch#virtual-cable-test interface ethernet 1/1/25
Interface Ethernet1/1/25:
------------------------------------------------------------------------
Cable pairs      Cable status      Error length (meters)
---------------  ----------------  -------------------------
(1, 2)             open            5
(3, 6)             open            5
(4, 5)             open            5
(7, 8)             short           5
```

## 3.1.1.24 switchport discard packet

**命令：switchport discard packet { tag | untag }**

**no switchport discard packet { tag | untag }**

**功能：**设置端口不接收 tag 报文或 untag 的报文；本命令的 no 操作取消端口的 discard 限制，即允许端口接收 tag 报文或 untag 的报文。

**参数：all** 表示不接收 tag 报文。**untag** 表示不接收 untag 报文。

**命令模式：**端口配置模式。

**缺省情况：**缺省不限制。

**使用指南：**无

**举例：** 设置交换机 1/1/8 端口不接收 tag 报文。

Switch(config)#interface ethernet 1/1/8

Switch(config-if-ethernet1/1/8)#switchport discard packet tag

## 3.1.1.25 switchport flood-control

**命令：switchport flood-control { bcast|mcast|ucast }**

**no switchport flood-control { bcast|mcast|ucast }**

**功能：**设置交换机不再往指定的端口转发广播、未知组播或未知单播报文；本命令的 no 操作为允许往端口转发广播、未知组播或未知单播报文，即恢复缺省状态。

**参数：**bcast 表示阻止广播报文往该端口转发，mcast 表示阻止未知组播报文往该端口转发，ucast 表示阻止未知单播报文往该端口转发。

**命令模式：**端口配置模式。

**缺省情况：**默认情况下，交换机在广播域内其他端口转发广播、未知组播和未知单播的报文。

**使用指南：**该命令对百兆口和千兆口均有效，对 Access、Trunk 与 Hybrid 口均有效。当命令生效后，若端口学习到对应的单播 mac 或组播 mac 后，放行相应的单播或组播流量。

该命令只控制从其他端口过来的广播、组播、未知单播报文不能被转发到特定的端口。但不能控制从特定端口上进入的广播、组播、未知单播报文。如在 1/1 端口上设置了 switchport flood-control bcast 命令，则从其他端口收到的广播报文不能转发到 1/1 端口，但 1/1 端口仍然可接收广播报文并正常转发。

**举例：**分别设置交换机 1/1/1 或 1/1/8-10 号端口对广播和多播进行 flood-control。

Switch(config)#interface ethernet 1/1/1

Switch(config-if-ethernet1/1)#switchport flood-control bcast

Switch(config)#interface ethernet 1/1/8-10

Switch(config-if-port-range)#switchport flood-control mcast

## 3.1.1.26 switchport flood-forwarding

**命令：switchport flood-forwarding mcast**

**no switchport flood-forwarding mcast**

**功能：**设置交换机往指定的端口转发未知组播或未知单播报文；本命令的 no 操作恢复缺省状态。

**参数：** mcast表示允许未知组播报文往该端口转发。

**命令模式：** 端口模式。

**缺省情况：** 默认情况下，交换机在广播域内可以往其他端口转发未知组播报文。

**使用指南：** 该命令对百兆口和千兆口均有效，对 Access、Trunk 与 Hybrid 口均有效。该命令一般与 ip igmp snooping 结合使用，ip igmp snooping 不允许未知组播广播，配置 switchport flood-forwarding mcast 命令之后可以转发未知组播流量。

**举例：**设置交换机 1/1/1 口对广播行 flood-forwarding

```
switch#
switch#confi
switch(config)#interface ethernet 1/1/1
switch(config-if-ethernet1/1/1)# switchport flood-forwarding mcast
switch(config-if-ethernet1/1/1)#exit
```

# 3.2 端口隔离

## 3.2.1 isolate-port group

**命令：isolate-port group <*WORD*>**

**no isolate-port group <*WORD*>**

**功能：**设置隔离组，该隔离组将作为端口隔离的作用域；本命令的 no 操作将删除隔离组，删除隔离组的同时移出该隔离组内的所有端口。

**参数：<*WORD*>**为隔离组的名称标识，长度不超过 32 个字符。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**用户可以根据需求创建不同的隔离组，例如若要将交换机某个 vlan 内的所有下联端口进行隔离，就可以通过创建一个隔离组并把该 vlan 内所有下联端口加入隔离组来实现。一台交换机上最多能够配置 30 个隔离组。当用户需要改变端口隔离的配置或者需要重新配置隔离组时，可以使用该命令的 no 操作删除已经存在的隔离组。

**举例：**配置名称为 test 的隔离组。

Switch>enable

Switch#config

Switch(config)#isolate-port group test

## 3.2.2 isolate-port group switchport interface

**命令：isolate-port group <*WORD*> switchport interface [ethernet | port-channel] <*IFNAME*>**

**no isolate-port group <*WORD*> switchport interface [ethernet | port-channel] <*IFNAME*>**

**功能：** 将一个或一组以太网端口加入某个隔离组成为该隔离组的隔离端口，加入隔离组后该隔离组内的所有端口相互隔离。本命令的 no 操作是将一个或一组以太网端口从某个隔离组中移出，被移出的以太网端口将不再与该隔离组内的所有端口相互隔离；如果被移出的以太网端口同时还属于其他的隔离组，则该以太网端口与它所属的隔离组中的端口仍然相互隔离。如果一个以太网端口属于某个汇聚组，则禁止将该端口加入某个隔离组，同时禁止将属于某个隔离组的以太网端口配置为汇聚组的成员端口。一个端口可以加入一个隔离组或者多个隔离组。

**参数：** **< *WORD* >** 为隔离组的名称标识，长度不超过32个字符，如果指定名称的隔离组不存在，则创建该隔离组； ethernet 表示要加入的隔离端口为以太网端口，后面跟以太网端口列表，支持';' '-'，如：'ethernet 1/1/1;3;4-7;8'； port-channel 表示要加入的隔离端口为汇聚端口； <IFNAME> 为端口名称，如e1/1/1，若选择端口名称则不用选ethernet。

**命令模式：** 全局配置模式。

**缺省情况：** 无。

**使用指南：** 用户可以根据需要将相应的以太网端口加入到某个隔离组中，或者将以太网端口从某个隔离组中删除。当一个以太网端口属于多个隔离组时，这个端口将与每个它所在的隔离组内的所有端口相互隔离。

**举例：** 将以太网端口 1/1/1-2 和 1/1/5 加入到名称为 test 的隔离组中

Switch(config)#isolate-port group test switchport interface ethernet 1/1/1-2;1/1/5

## 3.2.3 isolate-port apply

**命令：isolate-port apply [ <*l2* |*all*> ]**

**功能：** 该命令使端口隔离的配置应用于 2 层流量或者所有的流量。

**参数：** ***<l2| all>*** 为需要隔离的流量，l2表示隔离2层流量， all表示隔离所有的流量。

**命令模式：** 全局配置模式。

**缺省情况：** 隔离所有的流量。

**使用指南：** 用户可以根据需要将端口隔离应用于隔离 2 层流量或者所有的流量。

**举例：** 在交换机上，将端口隔离只应用于隔离 2 层流量。

Switch(config)#isolate-port apply l2

### 3.2.4 show isolate-port group

**命令：show isolate-port group [<*WORD*>]**

**功能：**显示端口隔离的相关配置，包括已经配置的隔离组和隔离组内的所有以太网端口。

**参数：<*WORD*>**为已经创建的隔离组的名称标识，长度不超过32个字符；不输入参数将显示所有隔离组的配置情况。

**命令模式：**特权配置模式和全局配置模式。

**缺省情况：**显示所有隔离组的配置情况。

**使用指南：**用户通过该命令查看端口隔离的配置情况。

**举例：**显示名称为 test 的隔离组配置信息。

Switch(config)#show isolate-port group test

Isolate-port group test

The isolate-port Ethernet1/1/5

The isolate-port Ethernet1/1/2

## 3.3 端口环路检测

### 3.3.1 debug loopback-detection

**命令：debug loopback-detection**

**功能：**当打开端口环回检测 debug 后，报文的发送和接收以及状态变化应有 DEBUG 信息。

**参数：**无。

**命令模式：**特权模式。

**缺省情况：**缺省没有配置。

**使用指南：**通过该命令显示报文的发送和接收以及状态变化。

**举例：**

Switch#debug loopback-detection

%Jan 01 00:07:45:106 2006 Send loopback detection probe packet:dev Ethernet1/1/5, vlan id 1

%Jan 01 00:07:45:107 2006 Send loopback detection probe packet:dev Ethernet1/1/5, vlan id 1

%Jan 01 00:07:45:110 2006 Loopback detected on port Ethernet1/1/5, VLAN 1

## 3.3.2 loopback-detection control

**命令：loopback-detection control {shutdown | block }**

**no loopback-detection control**

**功能：**打开端口的环路检测受控功能；本命令的 no 操作为关闭端口的环路检测受控功能。

**参数：shutdown** 采用 shutdown 的受控方式，即发现端口环路后将该端口 down 掉。

**block** 采用 block 的受控方式，即发现环路以后 block 该端口，只允许 bpdu 和环路检测报文通过。

**缺省情况：**关闭环路检测受控功能。

**命令模式：**端口配置模式。

**使用指南：**如果存在环路时，端口采用受控操作以后默认是不恢复受控状态的。如果配置了端口受控的超时时间，当这个时间超时后，端口恢复到正常的状态。当使用 block 的受控方式时需要手动配置 instance 和 vlan id 的对应关系，这个使用时需要注意。

**举例：**端口 1/1/2 模式上打开环路检测受控功能。

Switch(config)#interface ethernet 1/1/2

Switch(Config-If-Ethernet1/1/2)#loopback-detection control shutdown

Switch(Config-If-Ethernet1/1/2)#no loopback-detection control

## 3.3.3 loopback-detection control-recovery timeout

**命令：loopback-detection control-recovery timeout <0-3600>**

**功能：** 该命令是使端口检测到环路进入受控状态后，经过一定的时间恢复到不受控的状态。

**参数：**<0-3600>秒是受控状态恢复的时间，0 是不恢复状态。

**缺省情况：**默认是不自动恢复的。

**命令模式：**全局配置模式

**使用指南：**当某端口检测到环路并且端口进入受控状态后，端口一直处于受控状态，不进行恢复，如果端口 shutdown 状态则无法进行发包探测了，如果是 block 控制方式，在这种状态下仍然发送环路检测探测包检测下面是否有环路。如果配置了状态恢复时间，到这个时间超时后端口恢复到正常状态。这个恢复时间对于 shutdown 受控方式比较有意义，因为其它受控状态下仍然可以检测环路，不建议使用该命令。

**举例：**配置环路检测的受控方式为 30s 后自动恢复

Switch(Config)# loopback-detection control-recovery timeout 30

## 3.3.4 loopback-detection interval-time

**命令：loopback-detection interval-time <*loopback*> <*no-loopback*>**

**no loopback-detection interval-time**

**功能：**设置环路检测的时间间隔。本命令的 no 操作为关闭环路检测的时间间隔功能。

**参数：<*loopback* >**为存在环路时的检测时间间隔，单位秒，取值范围 5~300。

**<*no-loopback* >**为不存在环路时的检测时间间隔，单位秒，取值范围 1~30。

**缺省情况：**默认 5s 有环路检测，3s 无环路检测。

**命令模式：**全局配置模式。

**使用指南：**在配置检测时间间隔时，如果不存在环路检测可以时间间隔短一些，如果存在环路，时间太短对整个网络将会是灾难性的，因此建议配置长一点时间。

**举例：**设置环路检测的时间间隔为 35、15。

Switch(config)#loopback-detection interval-time 35 15

## 3.3.5 loopback-detection trap enable

**命令：loopback-detection trap enable**

**no loopback-detection trap enable**

**功能：**打开环路检测向 SNMP 服务器发送 TRAP 消息功能；本命令的 no 操作为关闭环路检测向 SNMP 服务器发送 TRAP 消息功能。

**参数：无。**

**缺省情况：**关闭通过该端口的环路检测功能。

**命令模式：**全局配置模式。

**使用指南：**开启环路检测发送 TRAP 消息功能后，当端口下检测到。

**举例：**打开环路检测向 SNMP 服务器发送 TRAP 消息功能。

Switch(config)# loopback-detection trap enable

## 3.3.6 loopback-detection specified-vlan

**命令：loopback-detection specified-vlan <*vlan-list*>**

**no loopback-detection specified-vlan [<*vlan-list*>]**

**功能：**打开该端口的环路检测功能并指定检测的 VLAN；本命令的 no 操作为关闭通过该端口的环路检测功能或者指定的 VLAN 中的环路检测功能。

**参数：<*vlan-list*>**为允许在该端口上通过的 VLAN 列表，因为 trunk 口的情况，可以检测指定的 vlan，所以用该命令配置检测的 vlan 列表。

**缺省情况：**关闭通过该端口的环路检测功能。

**命令模式：**端口配置模式。

**使用指南：**当一个端口是可以通过多个 Vlan 的 TRUNK 口时，环路检测可以基于端口＋Vlan 来进行，可以对端口上指定的 Vlan 中存在的环路情况进行检测。如果是 ACCESS 口，虽然可以配置多个 Vlan，但是也只对该端口所属的一个 Vlan 中进行检测。Port-channel 下不支持该功能。

**举例：**端口 1/1/2 模式上打开环路检测功能。

Switch(config)#interface ethernet 1/1/2

Switch(Config-If-Ethernet1/1/2)#switchport mode trunk

Switch(Config-If-Ethernet1/1/2)#switchport trunk allowed vlan all

Switch(Config-If-Ethernet1/1/2)#loopback-detection specified-vlan 1;3;5-20

Switch(Config-If-Ethernet1/1/2)#no loopback-detection specified-vlan 1;3;5-20

## 3.3.7 loopback-detection send packet number

**命令：loopback-detection send packet number *<1-10>***

**no loopback-detection send packet number**

**功能：**配置端口在每个探测周期发送的报文个数；本命令的 no 操作为恢复端口在每个探测周期发送的报文个数。

**参数：*<1-10>***为允许在该端口在每个探测周期允许发送的报文个数。

**缺省情况：**默认端口在每个探测周期允许发送的报文个数为 1 个。

**命令模式：**端口配置模式。

**使用指南：**开启环路检测后，端口在每个探测周期发送的报文个数为 1 个。如果产生环路，由于广播风暴等可能会将端口的带宽占满，导致环路检测报文被丢弃，此时可以调整探测报文个数，避免因为报文丢失导致端口上无法及时检测到环路。

**举例：**端口 1/0/2 模式上打开环路检测功能。

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)# loopback-detection send packet number 2

## 3.3.8 show loopback-detection

**命令：show loopback-detection [interface *<interface-list>*]**

**功能：**不输入参数则显示所有端口的环路检测状态和检测结果，输入参数则显示相应端口的状态和结果

**参数：*<interface-list>*** 要显示的端口的列表，如：ethernet 1/1/1。

**命令模式：**特权和配置模式。

**使用指南：**通过该命令显示出端口的环路检测状态和检测结果。

**举例：**显示端口 4 的环路检测状态。

Switch#show loopback-detection interface Ethernet 1/1/4

loopback detection config and state information in the switch!

| PortName | Loopback Detection | Control Mode | Is Controlled |
|---|---|---|---|
| Ethernet1/1/4 | Enable | Shutdown | No |

# 3.4 ULDP

## 3.4.1 debug uldp

**命令：debug uldp (hello | probe | echo | unidir | all) [receive | send] interface [ethernet] IFNAME**

**no debug uldp (hello | probe | echo | unidir | all) [receive | send] interface [ethernet] IFNAME**

**功能：**打开指定端口收发某种类型或者所有 ULDP 报文的调试开关。该调试项打开后，在终端显示收发的报文的信息；no 命令关闭调试项。

**参数：**

hello ：报文类型为 hello，通告报文，包括普通通告报文，RSY 和 Flush 报文

probe：报文类型为 probe，即探测报文

echo：报文类型为 echo，探测报文的回复

unidir：报文类型为 unidir，即发现单通链路的通知报文

all：所有 ULDP 报文

**命令模式：**特权配置模式。

**缺省情况：**默认关闭。

**使用指南：**使用该命令查看指定端口 1/1/2 上接收到 probe 类型的报文。

Switch#debug uldp probe receive interface ethernet 1/1/2

## 3.4.2 debug uldp error

**命令：debug uldp error**

**no debug uldp error**

**功能：**打开错误信息调试项，no 命令关闭调试项。

**参数：**无。

**命令模式：**特权配置模式。

**缺省情况：**默认关闭。

**使用指南：**使用该命令查看错误信息。

**举例：**查看错误信息。

Switch#debug uldp error

## 3.4.3 debug uldp event

**命令：debug uldp event**

**no debug uldp event**

**功能：**打开显示事件信息调试项；no 命令关闭调试项。

**参数：**无。

**命令模式：**特权配置模式。

**缺省情况：**默认关闭。

**使用指南：**使用该命令查看各种事件信息。

**举例：**查看事件信息。

Switch#debug uldp event

## 3.4.4 debug uldp fsm interface ethernet

**命令：debug uldp fsm interface ethernet *<IFname>***

**no debug uldp fsm interface ethernet *<IFname>***

**功能：**本命令打开端口的状态机迁移信息调试项，no 命令关闭调试项。

**参数：*<IFname>*：**端口名。

**命令模式：**特权配置模式。

**缺省情况：**默认关闭。

**使用指南：**使用该命令查看某端口的状态迁移信息。

**举例：**打印 1/1/1 的状态迁移信息。

Switch#debug uldp fsm interface ethernet 1/1/1

## 3.4.5 debug uldp interface ethernet

**命令：debug uldp {hello|probe|echo|unidir|all} [receive|send] interface ethernet *<IFname>***

**no debug uldp {hello|probe|echo|unidir|all} [receive|send] interface ethernet *<IFname>***

**功能：**打开显示报文详情调试项，该调试项打开后，在终端显示端口收发的某种类型报文的详细内容，no 命令关闭调试项。

**参数：*<IFname>*：**端口名。

**命令模式：**特权配置模式。

**缺省情况：**默认关闭。

**使用指南：**使用该命令查看端口 interface Ethernet 1/1/1 上接收到的 Hello 报文详细内容。

Switch#debug uldp hello receive interface Ethernet 1/1/1

## 3.4.6 debug uldp packet

**命令：debug uldp packet [receive|send]**

**no debug uldp packet [receive|send]**

**功能：**打开收发报文调试项。该调试项打开后，在终端显示收发的报文的类型和端口；no 命令关闭调试项。

**参数：**无。

**命令模式：**特权配置模式。

**缺省情况：**默认关闭。

**使用指南：**使用该命令查看各个端口上接收到的报文。

Switch#debug uldp packet receive

## 3.4.7 uldp aggressive-mode

**命令：uldp aggressive-mode**

**no uldp aggressive-mode**

**功能：**本命令设置 ULDP 的工作模式为积极模式。no 命令恢复普通模式。

**参数：**无。

**命令模式：**全局配置模式和端口配置模式。

**缺省情况：**默认普通模式。

**使用指南：**全局启动 ULDP 功能后，才能设置工作模式。在全局启用积极模式后，所有光口都工作在积极模式下，对于电口和新加入的光口，需要进入到端口配置模式下启用。

**举例：**全局启用积极模式。

Switch(config)#uldp aggressive-mode

## 3.4.8 uldp enable

**命令：uldp enable**

**功能：**命令启用 ULDP 功能，在全局模式下启用全局 ULDP 功能，端口模式下启用本端口的 ULDP 功能。

**参数：**无。

**命令模式：**全局配置模式和端口配置模式。

**缺省情况：**默认不启动 ULDP 功能。

**使用指南：**必须全局启动 ULDP 功能后，在端口上的 ULDP 才能启用。全局启用 ULDP 后，所有已存在光口上启用 ULDP，对电口和新加入光口，需要进入到端口模式下启用。

**举例：**全局启动 ULDP。

Switch(config)#uldp enable

## 3.4.9 uldp disable

**命令：uldp disable**

**功能：**命令禁用 ULDP 功能。

**参数：**无。

**命令模式：**全局配置模式和端口配置模式。

**缺省情况：**默认不启动 ULDP 功能。

**使用指南：**全局禁用 ULDP 后，则所有端口禁用 ULDP。

**举例：**全局禁用 ULDP。

Switch(config)#uldp disable

## 3.4.10 uldp hello-interval

**命令：uldp hello-interval <*integer*>**

**no uldp hello-interval**

**功能：**本命令设置 Hello 报文发送的时间间隔。no 命令将 Hello 报文的时间间隔恢复默认值。

**参数：<*integer*>：**Hello 报文的时间间隔，范围为 5－100 秒，默认值为 10 秒。

**命令模式：**全局配置模式。

**缺省情况：**默认值为 10 秒。

**使用指南：**全局启动 ULDP 功能后，才能配置 Hello 报文时间间隔。范围为 5－100 秒。

**举例：**将 Hello 报文的时间间隔设置为 12 秒。

Switch(config)#uldp hello-interval 12

## 3.4.11 uldp manual-shutdown

**命令：uldp manual-shutdown**

**no uldp manual-shutdown**

**功能：**本命令启用关闭单通端口模式为手动模式。no 命令恢复为自动关闭模式。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**默认为自动模式。

**使用指南：**全局启动 ULDP 功能后，才能进行设置。

**举例：**全局启用手动模式。

Switch(config)#uldp manual-shutdown

## 3.4.12 uldp recovery-time

**命令：uldp recovery-time<*integer*>**

**no uldp recovery-time**

**功能：**本命令设置 recovery 定时器时间，no 命令恢复为默认值。

**参数：<*integer*>：**recovery 定时器的超时时间，范围为 30-86400 秒。

**命令模式：**全局配置模式。

**缺省情况：**默认值为 0 秒，不开启重启机制。

**使用指南：**端口被 ULDP 关闭，且 recovery 定时器超时，该端口自动重启。若该定时器为默认值 0 秒，则端口不会重启。

**举例：**将 recovery 定时器设置为 600 秒。

Switch(config)#uldp recovery-time 600

## 3.4.13 uldp reset

**命令：uldp reset**

**功能：**重启被 ULDP 关闭的端口。

**参数：**无。

**命令模式：**全局配置模式和端口配置模式。

**缺省情况：**无。

**使用指南：**只有该端口是被 ULDP 关闭的，才能用该命令重新启用。全局模式下启用所有被 ULDP 关闭的端口，端口模式下重启指定端口。

**举例：**重启被 ULDP 关闭的所有端口。

Switch(config)#uldp reset

## 3.4.14 show uldp

**命令：show uldp [interface ethernet<*interface-name*>]**

**功能：**显示全局 ULDP 配置及端口状态信息，如果有端口显示端口的 ULDP 配置及状态信息，包括端口的邻居及其状态信息。

**参数：<*interface-name*>：**端口名。

**命令模式：**特权和配置模式。

**缺省情况：**无。

**使用指南：**若不带参数，则显示全局 ULDP 信息。若带参数，则除显示全局信息外，还显示该端口邻居信息。

**举例：**显示全局 ULDP 信息。

```
switch(config)#show uldp
uldp enable
uldp hello interval is                10
uldp recovery time is                 86400
uldp shut down mode is                MANUAL
uldp global work mode is              AGGRESSIVE
the total number of the port is       6

-------------------------------------------------------------------------
   PortName       PhyLink    LineProto    WorkMode        PortState   NeighborNum
-------------------------------------------------------------------------
 Ethernet1/1/49     UP          DOWN       AGGRESSIVE      INACTIVE       0
 Ethernet1/1/50     UP          DOWN       AGGRESSIVE      INACTIVE       0
 Ethernet1/1/51     UP          DOWN       AGGRESSIVE      INACTIVE       0
 Ethernet1/1/52     UP          DOWN       AGGRESSIVE      INACTIVE       0
 Ethernet1/1/53     UP          DOWN       AGGRESSIVE      INACTIVE       0
```

Ethernet1/1/54 UP DOWN AGGRESSIVE INACTIVE 0

---

# 3.5 LLDP

## 3.5.1 clear lldp remote-table

**命令：clear lldp remote-table**

**功能：**清空端口的 Remote-table。

**参数：**无。

**缺省情况：**不做清空表项操作。

**命令模式：**端口配置模式。

**使用指南：**清空本端口的 Remote 表项。

Switch(Config-If-Ethernet1/1/1)#clear lldp remote-table

## 3.5.2 debug lldp

**命令：debug lldp**

**no debug lldp**

**功能：**打开 LLDP 功能的调试信息；no 命令关闭 LLDP 功能的调试信息。

**参数：**无。

**缺省情况：**关闭 LLDP 功能的调试信息。

**命令模式：**特权模式。

**使用指南：**打开 debug 调试开关时，可看到包发送接收的情况和其他信息。

**举例：**在交换机上启动 LLDP 功能的 debug 开关。

Switch#debug lldp

## 3.5.3 debug lldp packets

**命令：debug lldp packets interface ethernet *<IFNAME>***

**no debug lldp packets interface ethernet *<IFNAME>***

**功能：**显示端口 LLDP 收发数据报文信息；no 命令关闭端口 Debug 信息开关。

**参数：**无。

**缺省情况：**关闭端口 Debug 信息开关。

**命令模式：**特权模式。

**使用指南：**打开 debug 调试开关时，可看到端口包发送接收的情况和其他信息。

**举例：**在交换机上启动 LLDP 功能的 debug 开关。

Switch#debug lldp packets interface ethernet 1/1/1

%Jan 01 00:02:40 2006 LLDP-PDU-TX PORT= ethernet 1/1/1

## 3.5.4 lldp enable

**命令：lldp enable**

**lldp disable**

**功能：**全局启动 LLDP 功能；disable 命令全局关闭 LLDP 功能。

**参数：**无。

**缺省情况：**关闭 LLDP 功能。

**命令模式：**全局配置模式。

**使用指南：**全局 LLDP 功能打开时，所有端口使能 LLDP 功能。

**举例：**在交换机上启动 LLDP 功能。

Switch(config)#lldp enable

## 3.5.5 lldp enable（端口）

**命令：lldp enable**

**lldp disable**

**功能：**配置端口模式下使能端口 LLDP 功能模块；disable 命令端口模式下不使能端口 LLDP 功能模块。

**参数：**无。

**缺省情况：**缺省端口模式下使能端口 LLDP 功能模块。

**命令模式：**端口配置模式。

**使用指南：**全局 LLDP 功能打开时，所有端口使能 LLDP 功能，通过端口开关关闭不需要开启 LLDP 功能的端口。

**举例：**将交换机的端口 ethernet 1/1/5 配置为不使能端口 LLDP 功能。

Switch(config)#in ethernet 1/1/5

Switch(Config-If-Ethernet1/1/5)#lldp disable

## 3.5.6 lldp management-address tlv

**命令：lldp management-address tlv [A.B.C.D]**

**no lldp management-address tlv**

**功能：**配置端口 lldp 管理地址 tlv 使能功能。

**参数：**A.B.C.D：可选参数，用户为端口指定的管理地址，必须是单播 IPV4 地址。

**缺省情况：**缺省不开启，LLDP 报文不携带端口的管理地址信息。

**命令模式：**端口配置模式。

**使用指南：**用户可以根据配置选择合适管理地址 IPV4 地址作为管理地址。如果用户开启功能时指定了管理地址，则以用户指定的管理地址为准发送管理地址 TLV；如果用户没有指定

管理地址，则从端口的 VLAN 三层口中选择合适的 IPV4 地址作为管理地址发送管理地址 TLV；在没指定的情况下，如果端口没有合适的管理地址，则不发送管理地址 TLV 信息。

**举例：**交换机的端口 ethernet1/1/1 开启管理地址 TLV 功能，并指定端口发送的管理地址。

switch(config-if-ethernet1/1/1)#lldp management-address tlv 192.168.24.32

## 3.5.7 lldp mode

**命令：lldp mode <*send* | *receive* | *both* | *disable*>**

**功能：**配置端口 lldp 功能的运行状态。

**参数：**send: 配置 LLDP 功能为只发送报文类型。

receive: 配置 LLDP 功能为只接收报文类型。

both: 配置 LLDP 功能为可接收发送报文类型。

disable: 配置 LLDP 功能为不可接收发送报文类型。

**缺省情况：**缺省端口运行状态为 both。

**命令模式：**端口配置模式。

**使用指南：**选择端口上 lldp Agent 的运行状态功能。

**举例：**将交换机的端口 ethernet 1/1/5 配置为只接受状态。

Switch(config)#in ethernet 1/1/5

Switch(Config-If-Ethernet1/1/5)#lldp mode receive

## 3.5.8 lldp msgTxHold

**命令：lldp msgTxHold <*value*>**

**no lldp msgTxHold**

**功能：**设置所有使能 LLDP 的端口发送更新报文所携带的老化时间的乘法器值，范围为 2 至 10。

**参数：<*value*>**为发送报文的老化时间乘法器。范围为 2 至 10。

**缺省情况：**乘法器值为 4。

**命令模式：**全局配置模式。

**使用指南：**配置乘法器值后，报文老化时间在定义上等于乘法器和报文发送间隔的乘积，老化时间最大为 65535 秒。

**举例：**在交换机上配置老化时间乘法器值为 6。

Switch(config)#lldp msgTxHold 6

## 3.5.9 lldp neighbors max-num

**命令：lldp neighbors max-num <*value*>**

**no lldp neighbors max-num**

**功能：**设置 Remote MIB 中所能存储的最大数据条数。

**参数：<*value*>**为设置的数据条数，有效范围为 5-500。

**缺省情况：**Remote MIB 中数据存储最大为 100。

**命令模式：**端口配置模式。

**使用指南：**Remote MIB 可以存储的数据最大条数。

**举例：**将交换机的端口 ethernet 1/1/5 配置为 Remote 为 200。

Switch(config)#interface ethernet 1/1/5

Switch(Config-If-Ethernet1/1/5)#lldp neighbors max-num 200

## 3.5.10 lldp notification interval

**命令: lldp notification interval <*seconds*>**

**no lldp notification interval**

**功能：**设定当此时间终止时，系统检查 Remote Table 是否被改变，如果改变则发送 Trap 给 SNMP 管理端。

**参数：<*seconds*>**为时间间隔。有效范围为 5-3600 秒。

**缺省情况：**时间间隔为 5 秒。

**命令模式：**全局配置模式。

**使用指南：**配置通知时间间隔后，Remote Table 发生改变时，在该时间间隔后发送 trap 报文。

**举例：**在交换机上配置 Trap 报文发送间隔为 20 秒。

Switch(config)#lldp notification interval 20

## 3.5.11 lldp tooManyNeighbors

**命令：lldp tooManyNeighbors {discard | delete}**

**功能：**设置当 Remote Table 满时，执行何种操作。

**参数：**discard：丢弃当前报文。

delete：删除Remoter Table中TTL最小的。

**缺省情况：**discard。

**命令模式：**端口配置模式。

**使用指南：**在 Remote MIB 满时，Discard 对收到的报文进行丢弃处理；Delete 删除 Remote 中 TTL 最小的表项。

**举例：**将交换机的端口 ethernet 1/1/5 配置为 delete。

Switch(config)#interface ethernet 1/1/5

Switch(Config-If-Ethernet1/1/5)# lldp tooManyNeighbors delete

## 3.5.12 lldp transmit delay

**命令: lldp transmit delay <*seconds*>**

**no lldp transmit delay**

**功能：**由于网络环境的多变性导致本地信息可能频繁变化，可能会导致在短时间内发送大量连续的更新报文，所以需要一定的延迟时间来统计本地信息，保证其准确性。

当 transmit delay 为默认值，且 tx-interval 通过命令进行了配置，那么 transmit delay 的默认值由 2 变为 1/4 倍的 transmit delay。

**参数：*<seconds>***为时间间隔。有效范围为 1-8192 秒。

**缺省情况：**时间间隔为 2 秒。

**命令模式：**全局配置模式。

**使用指南：**连续报文发送时，避免同时发送报文导致远端 Remote 信息被不断更新，设置报文发送延迟时间。

**举例：**在交换机上配置报文发送延迟时间间隔为 3。

Switch(config)#lldp transmit delay 3

## 3.5.13 lldp transmit optional tlv

**命令：lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap]**

**no lldp transmit optional tlv**

**功能：**配置指定端口可选 TLV 的类型。

**参数：portDesc** 为端口描述信息；**sysName** 为统名称；**sysDesc** 为统描述信息；**sysCap** 为统能力信息。

**缺省情况：**缺省报文不携带任何可选 TLV。

**命令模式：**端口配置模式。

**使用指南：**在配置可选 TLV 时，遵循每个 TLV 只能在报文中出现一次的原则，**portDesc** 可选 TLV 在这里为本地端口名称；**sysName** 可选 TLV 在这里为本地系统名称；**sysDesc** 可选 TLV 在这里为本地系统描述；**sysCap** 可选 TLV 在这里为本地系统能力信息。

**举例：**将交换机的端口 ethernet 1/1/5 配置为携带 portDesc 和 sysCap TLV。

Switch(config)#in ethernet 1/1/5

Switch(Config-If-Ethernet1/1/5)#lldp transmit optional tlv portDesc sysCap

## 3.5.14 lldp trap

**命令：lldp trap *<enable* | *disable>***

**功能：**enable 配置指定端口使能 Trap 功能；disable 配置指定端口不使能 Trap 功能。

**参数：**无。

**缺省情况：**缺省指定端口不使能 Trap 功能。

**命令模式：**端口配置模式。

**使用指南：**端口向外发送 Trap 报文功能。

**举例：**将交换机的端口 ethernet 1/1/5 配置为使能 Trap 功能。

Switch(config)#in ethernet 1/1/5

Switch(Config-If-Ethernet1/1/5)#lldp trap enable

## 3.5.15 lldp tx-interval

**命令：lldp tx-interval *<integer>***

**no lldp tx-interval**

**功能：**设置所有使能 LLDP 功能的端口发送更新报文的时间间隔,范围为 5 至 32768 秒，默认情况下为 30 秒。

**参数：*<integer>***为发送更新报文的时间间隔。范围为 5 至 32768 秒。

**缺省情况：**30 秒。

**命令模式：**全局配置模式。

**使用指南：**配置了报文发送时间间隔值后，在该时间后才能收到 LLDP 报文，此时间间隔最大只能等于老化时间的二分之一, 如果设定的时间太长，会导致经常性的老化与重建；如果设定的时间太短，会增加网络的流量，减少端口的带宽。报文老化时间在定义上等于乘法器和报文发送间隔的乘积，老化时间最大为 65535 秒。

当 tx-interval 为默认值，且 transmit delay 通过命令进行了配置，那么 tx-interval 的默认值由 40 变为 4 倍的 transmit delay。

**举例：**在交换机上配置报文发送时间间隔为 40 秒。

Switch(config)#lldp tx-interval 40

## 3.5.16 show debugging lldp

**命令：show debugging lldp**

**功能：**显示所有开启 lldp debug 开关的端口。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**配置 show debugging lldp 时，可以看到所有开启 debug 开关的端口。

**举例：**在交换机上显示所有开启 lldp debug 开关的端口。

Switch(config)# show debugging lldp

====BEGINNING OF LLDP DEBUG SETTINGS====

debug lldp

debug lldp packets interface Ethernet1/1/1

debug lldp packets interface Ethernet1/1/2

debug lldp packets interface Ethernet1/1/3

debug lldp packets interface Ethernet1/1/4

debug lldp packets interface Ethernet1/1/5

==========END OF DEBUG SETTINGS==========

## 3.5.17 show lldp

**命令：show lldp**

**功能：**显示全局 LLDP 的配置信息。如：LLDP 的启用端口列表，更新报文的发送时间间隔，报文老化时间配置，发送模块等待重新初始化时间间隔，TRAP 发送时间间隔，Remote 表项数量限制等。

**参数：**无。

**缺省情况：**不显示全局 LLDP 的配置信息。

**命令模式：**特权模式、全局配置模式。

**使用指南：**配置 show lldp 时可以看到全局 LLDP 的所有配置信息。

**举例：**在交换机上启动 LLDP 功能后查看全局配置的情况。

```
Switch(config)#show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP enabled port : Ethernet 1/1/1
LLDP interval :30
LLDP txTTL :120
LLDP txShutdownWhile :2
LLDP NotificationInterval :5
LLDP txDelay :20
------------END-----------------
```

## 3.5.18 show lldp interface ethernet

**命令：show lldp interface ethernet *<IFNAME>***

**功能：**显示端口 LLDP 的配置信息。如：LLDP Agent 的工作状态等。

**参数：*<IFNAME>*:**端口名称。

**缺省情况：**不显示 LLDP 端口配置信息。

**命令模式：**特权模式、全局配置模式。

**使用指南：**配置 show lldp interface ethernet XXX 时可以看到端口配置的信息。

**举例：**在交换机上启动 LLDP 功能后查看端口配置信息。

```
Switch(config)#show lldp interface ethernet 1/1/1
Port name :     ethernet 1/1/1
LLDP Agent Adminstatus : Both
LLDP Optional TLV : portDecs   sysName   sysDesc   sysCap
LLDP Trap Status : disable
LLDP maxRemote :100
LLDP Overflow handle : discard
LLDP interface remote status : Full
```

## 3.5.19 show lldp neighbors interface ethernet

**命令：show lldp neighbors interface ethernet < *IFNAME* >**

**功能：**显示端口 LLDP 的邻居信息。

**参数：**无。

**缺省情况：**不显示 LLDP 端口邻居信息。

**命令模式：**特权模式、全局配置模式。

**使用指南：**配置 show lldp neighbors interface ethernet XXX 时可以看到端口邻居的信息。

**举例：**在交换机上启动 LLDP 功能后查看端口邻居信息。

Switch(config)#show lldp neighbors interface ethernet 1/1/1

## 3.5.20 show lldp traffic

**命令：show lldp traffic**

**功能：**显示 LLDP 数据包统计信息。

**参数：**无。

**缺省情况：**不显示 LLDP 数据包统计信息。

**命令模式：**特权模式、全局配置模式。

**使用指南：**配置 show lldp traffic 时可以看到数据包的统计信息。

**举例：**在交换机上启动 LLDP 功能后查看数据包统计信息。

Switch(config)#show lldp traffic

| PortName | Ageouts | FramesDiscarded | FramesInErrors | FramesIn | FramesOut | TLVsDiscarded | TLVsUnrecognized |
|---|---|---|---|---|---|---|---|
| Ethernet1/1/1 | 0 | 0 | 0 | 0 | 7 | 0 | 0 |

# 3.6 LLDP-MED

## 3.6.1 civic location

**命令：civic location {dhcp server | switch | endpointDev} <*country-code*>**

**no civic location**

**功能：**配置 Civic Address LCI 格式地址的设备类型和国家编号，同时进入端口的 Civic Address LCI 格式地址配置模式，no 命令操作为取消端口 Civic Address LCI 格式地址的所有配置。

**参数：**dhcp server：设置设备类型为 DHCP server；

switch：设置设备类型为 Switch；

endpointDev：设置设备类型为 LLDP-MED Endpoint；

country-code：设置国家编号的值，由两个字母组成，比如 DE 或者 US，要符合 ISO 3166 标准的国家编号。

**缺省情况**：缺省没有在端口配置 Civic Address LCI 格式地址。

**命令模式**：端口配置模式

**使用指南**：在端口上配置 Civic Address LCI 格式地址的设备类型和国家编号，配置后进入 Civic Address LCI 格式地址配置模式，可以进行更加详细的地址配置。

**举例**：端口 19 上配置 Civic Address LCI 格式地址的设备类型为 switch，国家编号为 US。

Switch(Config-If-Ethernet1/1/19)# civic location switch US

Switch(Med-Civic)#

## 3.6.2 {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}

**命令：{description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo} *<address>***

**no {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}**

**功能**：进入端口的 Civic Address LCI 格式地址配置模式后，配置详细的地址信息。

**参数**：description-language：描述 location 的语言（language），比如“English”；

province-state：州，省等（state, canton, region, province prefecture)，比如“clara”；

city：城市（city），比如“New York”；

county：县等（county, parish），比如“santa clara”；

street：街道（street），比如“1301 Shoreway Road”；

locationNum：房子号（house number），比如“9”；

location：location 的名字（name and occupant of a location），比如“Carrillo's Holiday Market”；

floor：楼层（floor number），比如“13”；

room：房间号（room number），比如“1308”；

postal：邮编（postal/zip code），比如“10027-1234”；

otherInfo：附加地址信息（Additional location information），比如“South Wing”；

address：地址详细信息，不能超过 250 个字符。

**缺省情况**：缺省没有在端口配置 Civic Address LCI 格式地址的详细信息。

**命令模式**：Civic Address LCI 格式地址配置模式

**使用指南**：通过该命令对端口 Civic Address LCI 格式地址的详细信息进行配置，通过该命令最多进行 10 种地址类型信息的配置。

**举例**：Civic Address LCI 格式地址配置模式下配置详细的地址信息。

Switch(Med-Civic)# city Beijing

Switch(Med-Civic)# street shangdi

## 3.6.3 ecs location

**命令**：**ecs location *<tel-number>***

**no ecs location**

**功能**：在端口上配置 ECS ELIN 格式的地址，no 命令操作取消在端口上已经配置的 ECS ELIN 格式的地址。

**参数**：***<tel-number>***：端口 ECS ELIN 格式的地址字符串，比如紧急电话号码，值为 10-25 个字符组成的字符串。

**缺省情况**：缺省没有在端口配置 ECS ELIN 格式的地址。

**命令模式**：端口配置模式

**使用指南**：ECS ELIN 格式的地址字符串的长度范围为 10 到 25。

**举例**：端口 19 上配置 ECS ELIN 格式的地址。

Switch(Config-If-Ethernet1/1/19)#ecs location 880-445-3381

## 3.6.4 lldp med fast count

**命令**：**lldp med fast count *<value>***

**no lldp med fast count**

**功能**：LLDP-MED 快速启动机制激活的情况下，需要快速发送含有 LLDP-MED TLV 的 LLDP 报文，该命令对快速发送报文的个数进行设置。no 命令恢复快速发送报文的个数为默认值。

**参数**：value：快速发送报文的数目，取值范围为 1～10，单位为个。

**缺省情况**：缺省情况快速发送报文的个数为 4。

**命令模式**：全局配置模式

**使用指南**：该命令对快速发送报文的个数进行设置。

**举例**：

Switch(config)#lldp med fast count 5

## 3.6.5 lldp med trap

**命令**：**lldp med trap {enable | disable}**

**功能**：配置指定端口使能或者禁止 LLDP-MED 网络拓扑发生变化发送 TRAP 消息功能。

**参数**：enable：使能端口的 LLDP-MED TRAP 功能

disable：禁止端口的 LLDP-MED TRAP 功能

**缺省情况**：端口的 LLDP-MED TRAP 功能被禁用。

**命令模式**：端口配置模式

**使用指南**：打开或者关闭端口的 LLDP-MED TRAP 功能。

**举例：**使能端口 19 上的 LLDP-MED TRAP 功能

Switch(Config-If-Ethernet1/1/19)#lldp med trap enable

## 3.6.6 lldp transmit med tlv all

**命令：lldp transmit med tlv all**

**no lldp transmit med tlv all**

**功能：**配置指定端口发送所有 LLDP-MED TLV 的功能。no 命令为关闭端口发送 LLDP-MED TLV 的功能。

**参数：**无。

**缺省情况：**端口没有开启发送任何 LLDP-MED TLV 的功能。

**命令模式：**端口配置模式

**使用指南：**配置端口发送所有 LLDP-MEDTLV，配置该命令后，如果端口具备发送 LLDP-MED TLV 的能力,则在端口发送的 LLDP 报文中,包含所有交换机支持的 LLDP-MED TLV。否则，如果交换机上配置了对应的 no 命令，即使端口具备发送 LLDP-MED TLV 的能力，端口发送的 LLDP 报文中也不能包含任何 LLDP-MED TLV。

**举例：**端口 19 开启发送所有 LLDP-MED TLV 的功能。

Switch(Config-If-Ethernet1/1/19)#lldp transmit med tlv all

## 3.6.7 lldp transmit med tlv capability

**命令：lldp transmit med tlv capability**

**no lldp transmit med tlv capability**

**功能：**配置指定端口发送 LLDP-MED Capability TLV。no 命令为关闭端口发送 LLDP-MED Capability TLV 的能力。

**参数：**无。

**缺省情况：**端口没有开启发送 LLDP-MED Capability TLV 的功能。

**命令模式：**端口配置模式

**使用指南：**配置端口发送 LLDP-MED Capability TLV，配置该命令后，如果端口具备发送 LLDP-MED TLV 的能力，则在端口发送的 LLDP 报文中，包含 LLDP-MED Capability TLV。否则，如果交换机上配置了对应的 no 命令，即使端口具备发送 LLDP-MED TLV 的能力，端口发送的 LLDP 报文中也不能包含 LLDP-MED Capability TLV。注意，LLDP-MED Capability TLV 是最重要的 LLDP-MED TLV，如果不先配置发送该 TLV，则不能配置发送任何其他的 LLDP-MED TLV。

**举例：**端口 19 开启发送 LLDP-MED capability TLV 的功能。

Switch(Config-If-Ethernet1/1/19)#lldp transmit med tlv capability

## 3.6.8 lldp transmit med tlv extendPoe

**命令：lldp transmit med tlv extendPoe**

**no lldp transmit med tlv extendPoe**

**功能**：配置指定端口发送 LLDP-MED Extended Power-Via-MDI TLV。no 命令为关闭端口发送 LLDP-MED Extended Power-Via-MDI TLV 的能力。

**参数**：无。

**缺省情况**：端口没有开启发送 LLDP-MED Extended Power-Via-MDI TLV 的功能。

**命令模式**：端口配置模式

**使用指南**：配置端口发送 LLDP-MED Extended Power-Via-MDI TLV，配置该命令后，如果端口具备发送 LLDP-MED TLV 的能力，则在端口发送的 LLDP 报文中，包含 LLDP-MED Extended Power-Via-MDI TLV。否则，如果交换机上配置了对应的 no 命令，即使端口具备发送 LLDP-MED TLV 的能力，端口发送的 LLDP 报文中也不能包含 LLDP-MED Extended Power-Via-MDI TLV。注意，配置端口发送 LLDP-MED Extended Power-Via-MDI TLV 前，必须配置端口发送 LLDP-MED Capability TLV，否则无法配置成功。另外，如果设备不支持 POE 或者端口的 POE 功能通过命令被关闭，则不发送该 TLV。

**举例**：端口 19 开启发送 LLDP-MED Extended Power-Via-MDI TLV 的功能。

Switch(Config-If-Ethernet1/1/19)#lldp transmit med tlv extendPoe

## 3.6.9 lldp transmit med tlv location

**命令：lldp transmit med tlv location**

**no lldp transmit med tlv location**

**功能**：配置指定端口发送 LLDP-MED Location Identification TLV。no 命令为关闭端口发送 LLDP-MED Location Identification TLV 的能力。

**参数**：无。

**缺省情况**：端口没有开启发送 LLDP-MED Location Identification TLV 的功能。

**命令模式**：端口配置模式

**使用指南**：配置端口发送 LLDP-MED Location Identification TLV，配置该命令后，如果端口具备发送 LLDP-MED TLV 的能力，则在端口发送的 LLDP 报文中，包含 LLDP-MED Location Identification TLV。否则，如果交换机上配置了对应的 no 命令，即使端口具备发送 LLDP-MED TLV 的能力，端口发送的 LLDP 报文中也不能包含 LLDP-MED Location Identification TLV。注意，配置端口发送 LLDP-MED Location Identification TLV 前，必须配置端口发送 LLDP-MED Capability TLV，否则无法配置成功。另外，如果设备不支持 POE 或者端口的 POE 功能通过命令被关闭，则不发送该 TLV。

**举例**：端口 19 开启发送 LLDP-MED Location Identification TLV 的功能。

Switch(Config-If-Ethernet1/1/19)#lldp transmit med tlv location

## 3.6.10 lldp transmit med tlv inventory

**命令：lldp transmit med tlv inventory**

**no lldp transmit med tlv inventory**

**功能**：配置指定端口发送 LLDP-MED Inventory Management TLVs 集合，该 TLVs 集合共包括 7 个 TLV，分别是：Hardware Revision TLV，Firmware Revision TLV，Software Revision TLV，Serial Number TLV，Manufacturer Name TLV，Model Name TLV，Asset ID TLV。no 命令为关闭端口发送 LLDP-MED Inventory Management TLVs 的能力。

**参数**：无。

**缺省情况**：端口没有开启发送 LLDP-MED Inventory Management TLVs 的功能。

**命令模式**：端口配置模式

**使用指南**：配置端口发送 LLDP-MED Inventory Management TLVs，配置该命令后，如果端口具备发送 LLDP-MED TLV 的能力，则在端口发送的 LLDP 报文中，包含 LLDP-MED Inventory Management TLVs。否则，如果交换机上配置了对应的 no 命令，即使端口具备发送 LLDP-MED TLV 的能力，端口发送的 LLDP 报文中也不能包含 LLDP-MED Inventory Management TLVs。注意，配置端口发送 LLDP-MED Inventory Management TLVs 前，必须配置端口发送 LLDP-MED Capability TLV，否则无法配置成功。

**举例**：端口 19 开启发送 LLDP-MED Inventory Management TLVs 的功能。

Switch(Config-If-Ethernet1/1/19)#lldp transmit med tlv inventory

## 3.6.11 lldp transmit med tlv networkPolicy

**命令**：**lldp transmit med tlv networkPolicy**

**no lldp transmit med tlv networkPolicy**

**功能**：配置指定端口发送 LLDP-MED Network Policy TLV。no 命令为关闭端口发送 LLDP-MED Network Policy TLV 的能力。

**参数**：无。

**缺省情况**：端口没有开启发送 LLDP-MED Network Policy TLV 的功能。

**命令模式**：端口配置模式

**使用指南**：配置端口发送 LLDP-MED Network Policy TLV，配置该命令后，如果端口具备发送 LLDP-MED TLV 的能力，则在端口发送的 LLDP 报文中，包含 LLDP-MED Network Policy TLV。否则，如果交换机上配置了对应的 no 命令，即使端口具备发送 LLDP-MED TLV 的能力，端口发送的 LLDP 报文中也不能包含 LLDP-MED Network Policy TLV。注意，配置端口发送 LLDP-MED Network Policy TLV 前，必须配置端口发送 LLDP-MED Capability TLV，否则无法配置成功。

**举例**：端口 19 开启发送 LLDP-MED Network Policy TLV 的功能。

Switch(Config-If-Ethernet1/1/19)#lldp transmit med tlv networkPolicy

## 3.6.12 network policy

**命令**：**network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} [status**

**{enable | disable}] [tag {tagged | untagged}] [vid {<*vlan-id*> | dot1p}] [cos <*cos-value*>] [dscp <*dscp-value*> ]**

**no network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming- video | video-signaling}**

**功能**：配置端口的网络策略，包括端口的 VLAN ID、支持的应用（如语音和视频）、应用优先级以及使用策略等。

**参数**：voice，voice-signaling，guest-voice，guest-voice-signaling，softphone-voice，video-conferencing，streaming-video 和 video-signaling：表示端口支持的媒体应用类型；

status：网络策略是否可用；

enable：表示特定应用类型的 Network Policy 已定义，enable 为网络策略的默认值；

disable：表示特定应用类型的 Network Policy 是未知的，在这种情况下，忽略 VLAN ID，L2 priority 和 DSCP 等字段，网络连接设备不发送该类型的 TLV；

tag：配置特定应用使用 tagged 或者 untagged 的 VLAN 方式；

tagged：配置特定应用的流量使用 tagged vlan 的方式，在这种情况下，VLAN ID，Layer2 priority 和 DSCP value 字段都有效；

untagged：配置特定应用的流量不要打任何标记，在这种情况下，VLAN ID 和 Layer2 priority 字段被忽略，只有 DSCP value 字段有效。Untagged 为 VLAN 方式的默认值；

vid：对 VLAN ID 进行配置，告诉对端，特定应用应属的 VLAN 号，那么对端发送特定应用流量的时候，就打上该 VLAN ID。如果不对 vid 配置，vlan-id 的默认值为 1；

vlan-id：配置 VLAN ID 的值，取值范围 1-4094；

dot1p：配置特定应用使用 802.1p 优先级对流量打标，同时使用 vlan 0 承载流量；

cos：对 VLAN 的以太帧优先级配置；

cos-value：配置 VLAN 的以太帧优先级的值，取值范围为 0-7，默认值为 5；

dscp：对 VLAN 的 DSCP 进行配置；

dscp-value：用户输入的 DSCP 的值，取值范围 0-63，默认值为 46。

**缺省情况**：缺省没有在端口配置任何网络策略。

**命令模式**：端口模式

**使用指南**：用户可以在一个端口配置多种网络策略，但策略的媒体应用类型不能重复。一种网络策略对应一个 LLDP-MED network policy TLV。如果用户在一个端口上配置了多条策略，会在一个 LLDP 报文中发送多个 LLDP-MED network policy TLV；如果用户没有配置任何网络策略，则 LLDP 报文中不发送 LLDP-MED network policy TLV。

**举例**：端口 19 上配置一条媒体应用类型为 voice 的网络应用策略。

Switch(Config-If-Ethernet1/1/19)#network policy voice tag tagged vid 2 cos 6 dscp 23

# 3.7 Port Channel

## 3.7.1 debug port-channel

**命令：debug port-channel <*port-group-number*> {all | event | fsm | packet | timer}**

**no debug port-channel [<*port-group-number*>]**

**功能：**打开 port-channel 的调试开关。

**参数：port-group-number**：Port Channel 的组号，范围为 1～128。

**all**：所有调试信息开关。

**event**：事件信息调试开关。

**fsm**：状态机信息调试开关。

**packet**：LACP 数据包信息调试开关。

**timer**：定时器信息调试开关。

**命令模式：**特权配置模式。

**缺省情况：**关闭 port-channel 的调试开关。

**使用指南：**打开调试开关，可以看到 port-channel 的各种调试信息。

**举例：**

(1)打开组号为 1 的 port channel 的状态机调试开关。

Switch#debug port-channel 1 fsm

(2)打开组号为 2 的 port channel 的 LACP 数据包信息调试开关。

Switch#debug port-channel 2 packet

(3)打开组号为 1 的 port-channel 的所有调试开关。

Switch#debug port-channel 1 all

## 3.7.2 interface port-channel

**命令：interface port-channel <*port-channel-number*>**

**功能：**进入汇聚接口配置模式。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**进入汇聚端口模式下配置时，如果是对 gvrp，spanning tree 模块做配置则对汇聚端口生效，如果汇聚端口不存在，也就是说在端口没有汇聚起来时先提示错误信息，记录该用户配置操作，当端口真正汇聚起来以后恢复用户刚才对未形成汇聚端口的配置动作，注意只能恢复一次，如果因为某种原因汇聚组被拆散然后又汇聚起来，用户一开始的配置不能被恢复。如果是对其他模块做配置，比如做 shutdown 配置，则是对该 port-channel 对应的 port-group 中的所有成员端口生效，起到一个群配的作用。

**举例：**进入 port-channel1 配置模式。

Switch(config)#interface port-channel 1

Switch(Config-If-Port-Channel1)#

## 3.7.3 lacp port-priority

**命令：lacp port-priority <*port-priority*>**

**no lacp port-priority**

**功能：**设置 LACP 协议的端口优先级。

**参数：<*port-priority*>**：LACP 协议中的端口优先级，范围为 0～65535。

**命令模式：**端口配置模式。

**缺省情况：**系统默认的优先级为 32768。

**使用指南：**使用此命令可以修改 LACP 协议的端口优先级，no 命令为恢复为默认值。

**举例：**设置 LACP 协议的端口优先级。

Switch(Config-If-Ethernet1/1/1)# lacp port-priority 30000

## 3.7.4 lacp system-priority

**命令：lacp system-priority <*system-priority*>**

**no lacp system-priority**

**功能：**设置 LACP 协议的系统优先级。

**参数：<*system-priority*>**：LACP 协议中的系统优先级，范围为 0～65535。

**命令模式：**全局配置模式。

**缺省情况：**系统默认的优先级为 32768。

**使用指南：**使用此命令可以修改 LACP 协议的系统优先级，no 命令为恢复为默认值。

**举例：**设置 LACP 协议的系统优先级。

Switch(config)# lacp system-priority 30000

## 3.7.5 lacp timeout

**命令：lacp timeout {short | long}**

**no lacp timeout**

**功能：**设置当前端口 LACP 协议中的端口 Timeout 模式。

**参数：**LACP 协议中的端口 Timeout 模式有 long 和 short 两种。

**命令模式：**端口配置模式。

**缺省情况：**端口默认的 Timeout 模式为 long。

**使用指南：**设置当前端口 LACP 协议中的端口 Timeout 模式。

**举例：**将 LACP 协议中当前端口的端口 Timeout 模式设置为 short。

Switch(Config-If-Ethernet1/1/1)#lacp timeout short

## 3.7.6 load-balance enhanced profile

**命令：load-balance enhanced profile**

**功能：**该命令是进入汇聚口增强型负载分担模式。

**参数：**无。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**全局模式下输入 load-balance enhanced profile 即可以配置增强型负载分担模板

Switch(config)#load-balance enhanced profile

**相关命令：**show load-balance enhanced-profile

## 3.7.7 l2 field

**命令：l2 field [dst-mac] [ingress-port] [l2-protocol] [src-mac] [vlan]**

**no l2 field**

**功能：该命令用来配置汇聚口增强型 l2** packets 协议字段负载分担方式，本命令的 no 操作恢复默认配置，即所有的字段均配置。

**参数：dst-mac：**根据目的 mac 地址进行流量分担；

**ingress-port：**根据上行物理端口进行流量分担；

**l2-protocol：**根据 l2 层 ethernet type 进行流量分担；

**src-mac：**根据源 mac 地址进行流量分担；

**vlan：**根据 vlan 进行流量分担。

**缺省情况：**缺省所有字段均配置。

**命令模式：**汇聚端口增强型负载分担模式。

**使用指南：**全局模式下输入 load-balance enhanced profile，进入增强型负载分担模式，然后就可以配置 l2 field 模板。

**举例：**配置汇聚口增强型负载分担 l2 field 模板。

Switch(config-load-balance-enhanced-profile)#l2 field dst-mac ingress-port l2-protocol src-mac vlan

**相关命令：**show load-balance enhanced-profile

## 3.7.8 l2 mpls field l2payload

本型号交换机不支持此命令

## 3.7.9 l2 mpls field l3payload

本型号交换机不支持此命令

## 3.7.10 ipv4 field

**命令：ipv4 field [dst-ip] [ingress-port] [l4-dst-port] [l4-src-port] [protocol] [src-ip] [vlan]**

**no ipv4 field**

**功能：**该命令用来配置汇聚口增强型 ipv4 packets 协议字段负载分担方式，本命令的 no 操作恢复默认配置，即所有的字段均配置。

**参数：dst-ip：** 根据目的 IP 地址进行流量分担；

**ingress-port：**根据上行物理端口进行流量分担；

**l4-dst-port：**根据 TCP/UDP 目的端口进行流量分担；

**l4-src-port：**根据 TCP/UDP 源端口进行流量分担；

**protocol：**根据 ip 协议进行流量分担；

**src-ip：** 根据源 IP 地址进行流量分担；

**vlan：**根据 vlan 进行流量分担。

**缺省情况：**缺省所有字段均配置。

**命令模式：**汇聚端口增强型负载分担模式。

**使用指南：**全局模式下输入 load-balance enhanced profile，进入增强型负载分担模式，然后就可以配置 ipv4 field 模板。

**举例：**配置汇聚口增强型负载分担 ipv4 field 模板。

Switch(config-load-balance-enhanced-profile)#ipv4 field dst-ip ingress-port l4-dst-port l4-src-port protocol src-ip vlan

**相关命令：**show load-balance enhanced-profile

## 3.7.11 ipv6 field

**命令：ipv6 field [dst-ip] [ingress-port] [l4-dst-port] [l4-src-port] [protocol] [src-ip] [vlan]**

**no ipv6 field**

**功能：**该命令用来配置汇聚口增强型 ipv6 packets 协议字段负载分担方式，本命令的 no 操作恢复默认配置，即所有的字段均配置。

**参数：dst-ip：** 根据目的 IP 地址进行流量分担；

**ingress-port：**根据上行物理端口进行流量分担；

**l4-dst-port：**根据 TCP/UDP 目的端口进行流量分担；

**l4-src-port**：根据 TCP/UDP 源端口进行流量分担；

**protocol**：根据 IP 协议进行流量分担；

**src-ip**： 根据源 IP 地址进行流量分担；

**vlan**：根据 vlan 进行流量分担。

**缺省情况**：缺省所有字段均配置。

**命令模式**：汇聚端口增强型负载分担模式。

**使用指南**：全局模式下输入 load-balance enhanced profile，进入增强型负载分担模式，然后就可以配置 ipv6 field 模板。

**举例**：配置汇聚口增强型负载分担 ipv6 field 模板。

Switch(config-load-balance-enhanced-profile)#ipv6 field dst-ip ingress-port l4-dst-port l4-src-port protocol src-ip vlan

**相关命令**：show load-balance enhanced-profile

## 3.7.12 l2-only

**命令**：l2-only {enable | disable}

**功能**：开启/关闭 l2-only 分担开关

**参数**：enable/ disable:开启或关闭。

enable 以后，所有报文只根据 L2 field 分担

disable 以后,根据报文类型选择分担方式：二层报文根据 l2 field 分担，IP 报文根据 ip field 分担

**缺省情况**：缺省关闭。

**使用指南**：无。

**举例**：只根据 l2 字段分担

switch(config-load-balance-enhanced-profile)#l2-only enable

## 3.7.13 l3 mpls field

本型号交换机不支持此命令

## 3.7.14 mpls tunnel field

本型号交换机不支持此命令

## 3.7.15 mim field l2payload

本型号交换机不支持此命令

## 3.7.16 mim field l3payload

本型号交换机不支持此命令

## 3.7.17 mim tunnel field

本型号交换机不支持此命令

## 3.7.18 trill field l2payload

本型号交换机不支持此命令

## 3.7.19 trill field l3payload

本型号交换机不支持此命令

## 3.7.20 trill tunnel field l2payload

本型号交换机不支持此命令

## 3.7.21 trill tunnel field l3payload

本型号交换机不支持此命令

## 3.7.22 trill tunnel field outerl2

本型号交换机不支持此命令

## 3.7.23 port-group

**命令：port-group *<port-group-number>***

**no port-group *<port-group-number >***

**功能：**新建一个 port group，该命令的 no 操作为删除该 group。

**参数：***<port-group-number>* 为 Port Channel 的组号，范围为 1～128

**缺省情况：**缺省交换机没有 port-group。

**命令模式：**全局配置模式。

**举例：**新建一个 port group。

Switch (config)#port-group 1

删除一个 port group

Switch (config)#no port-group 1

## 3.7.24 port-group mode

**命令：port-group *<port-group-number>* mode {active | passive | on}**

**no port-group**

**功能：**将物理端口加入 Port Channel，该命令的 no 操作为将端口从 Port Channel 中去除，一个 Port Channel 最多支持 16 个成员端口。

**参数：*<port-group-number>*** 为 Port Channel 的组号，范围为 1～128；**active** 启动端口的 LACP 协议，并设置为 Active 模式；**passive** 启动端口的 LACP 协议，并且设置为 Passive 模式；**on** 强制端口加入 Port Channel，不启动 LACP 协议。

**命令模式：**端口配置模式。

**缺省情况：**缺省交换机端口不属于 Port Channel，不启动 LACP 协议。

**使用指南：**加入 port-group 的各个端口在速率、配置、物理属性等方面必须保持一致。如果指定组号的 port group 不存在，那么打印错误提示信息。在一个 port-group 中所有的端口加入的模式必须一样，以第一个加入该组的端口模式为准。端口以 on 模式加入一个组是强制性的，所谓强制性的表示本端交换机端口汇聚不依赖对端的信息，只要这些端口的 VLAN 信息都一致则组中的端口就能汇聚成功。端口以 active 和 passive 方式加入一个组是运行 LACP 协议的，但两端必须有一个组中的端口是以 active 方式加入的，如果两端都是 passive，端口永远都无法汇聚起来。

**举例：**在 Ethernet1/1/1 端口模式下，将本端口以 active 模式加入 port-group 1。

Switch (Config-If-Ethernet1/1/1)#port-group 1 mode active

## 3.7.25 show port-group

**命令：show port-group [*<port-group-number>*] {brief | detail |}**

**功能：**显示指定组号或所有已配置的 port channel 的配置信息。

**参数：*<port-group-number>*** 要显示的 Port Channel 的组号，范围为 1～128；**brief** 显示摘要信息；**detail** 显示详细信息。

**命令模式：**所有配置模式。

**缺省情况：**无。

**使用指南：**如果用户没有输入 port-group-number 则表示显示所有已存在的 port-group 的信息；如果输入参数 port-group-number 对应组号的 port channel 不存在，打印错误提示信息；否则打印指定组号的 port-channel 当前相应信息。

**举例：**

(1)显示组号为 1 的 port-channel 的概要信息。

```
 switch(config)#show port-group 1 brief
ID: port group number;    Mode: port group mode such as on active or passive;
Ports: different types of port number of a port group,
          the first is selected ports number, the second is standby ports number, and
          the third is unselected ports number.

ID     Mode        Partner ID                        Ports          Load-balance
--------------------------------------------------------------------
1      active      0x8000,00-03-0f-08-08-10      2,0,0          enhance-profile
```

(2) 显示组号为 1 的 port-channel 的详细信息。

```
switch(config)#show port-group 1 detail
Flags:   A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
           D -- Synchronization, E -- Collecting, F -- Distributing,
           G -- Defaulted, H -- Expired

Port-group number: 1,   Mode: active,     Load-balance: enhance-profile
 Port-group detail information:
 System ID: 0x8000,00-03-0f-d3-07-ef
 Local:
  Port                    Status        Priority   Oper-Key Flag
  ---------------------------------------------------------
  Ethernet1/1/1           Selected      32768      1        {ACDEF}
  Ethernet1/1/2           Selected      32768      1        {ACDEF}

 Remote:
  Actor                                 Partner      Priority     Oper-Key   SystemID
Flag
  ---------------------------------------------------------------------------
  Ethernet1/1/1           1             32768        1            0x8000,00-03-0f-08-08-10
{ACDEF}
```

Ethernet1/1/2 2 32768 1 0x8000,00-03-0f-08-08-10 {ACDEF}

## 3.7.26 show load-balance enhanced-profile

**命令：show load-balance enhanced-profile**

**功能：显示当前配置的增强型负载分担配置模板。**

**参数：无。**

**命令模式：特权和配置模式。**

**缺省情况：无。**

**使用指南：显示当前所有增强型 load-balance 配置模板 。**

**举例：查看汇聚口增强型负载分担配置模板**

Switch#show load-balance enhanced-profile

l2 field src-mac dst-mac l2-protocol vlan ingress-port

ipv4 field src-ip dst-ip protocol l4-src-port l4-dst-port vlan ingress-port

ipv6 field src-ip dst-ip protocol l4-src-port l4-dst-port vlan ingress-port

l2 mpls field l2payload src-mac dst-mac vlan l2-protocol

l3 mpls field src-ip dst-ip protocol l4-src-port l4-dst-port vlan

mpls tunnel field src-ip dst-ip top-label 2nd-label label-4msb 3nd-label

trill field l2payload src-mac dst-mac vlan l2-protocol

trill tunnel field l2payload src-mac dst-mac vlan l2-protocol ing-rbridge-name egr-rbridge-name

mim field l2payload src-mac dst-mac vlan l2-protocol

mim tunnel field src-mac dst-mac lookup-id

## 3.7.27 port-group <port-group-number> local-first

**命令：**port-group <port-group-number> local-first

no port-group <port-group-number >

**功能：**新建一个 port group，并开启本地优先功能，该命令的 no 操作为删除该 group。

**参数：**<port-group-number> 为Port Channel 的组号，范围为 1～64。

**命令模式：**全局配置模式。

**缺省情况：**缺省交换机没有port-group。

**使用指南：**开启本地优先时，堆叠的情况下，进来报文会优先负载到本member的聚合后进行转发，该命令只对已知单播报文有效。

**举例：**新建一个port group, 并开启本地优先

Switch (config)#port-group 1 local-first

删除一个port group

Switch (config)#no port-group 1

# 3.8 MTU

## 3.8.1 mtu

**命令：mtu [<mtu-value>]**

**no mtu**

**功能：**打开超大帧的接收功能。no 操作恢复为正常帧的接收范围 64—1518。

**参数：<mtu-value>**可以接收的超大帧的 MTU 值，以字节为单位，取值为<1500-12270>，对应的帧长度则为<1518/1522-12288/12292>。如果不设置该参数，允许的最大帧长度为最大值 12288/12292。

**缺省情况：**缺省没有打开 MTU 功能。

**命令模式：**全局模式。

**使用指南：**以太网连接的两端交换机必须都设置为 mtu，否则 mtu 帧会在未设置的一端被丢弃。

**举例：**打开交换机的 MTU 功能。

Switch(config)#mtu

# 3.9 bpdu-tunnel

## 3.9.1 bpdu-tunnel-protocol

**命令：bpdu-tunnel-protocol { stp | dot1x | gvrp } { default-group-mac | group-mac < *mac-address*> }**

**no bpdu-tunnel-protocol { stp | dot1x | gvrp }**

**功能：**配置协议报文对应的组 mac 地址；no 命令取消协议报文对应的组 mac 地址。

**参数：< *mac-address*>：**组 mac 地址。

**缺省情况：**缺省不对任何协议报文进行隧道转发。

**命令模式：**全局配置模式。

**使用指南：**在全局配置模式下配置协议报文对应的组 mac 地址。

**举例：**配置 stp 协议报文对应的组 mac 地址。

Switch(config)#bpdu-tunnel-protocol stp group-mac 01-02-03-04-05-06

## 3.9.2 bpdu-tunnel-protocol user-defined-protocol

**命 令 ： bpdu-tunnel-protocol user-defined-protocol <*strings*> protocol-mac <*mac-address*> { default-group-mac | encape-type | group-mac }**

**no bpdu-tunnel-protocol user-defined-protocol <*strings*>**

**功能：**配置自定义协议报文的组 mac 地址或封装类型地址；no 命令取消自定义协议报文的组 mac 地址或封装类型地址。

**参数：<*strings*>：**自定义协议类型，范围为 1-31 个字符；

**<*mac-address*>：**mac 地址。

**缺省情况：**缺省没有配置自定义协议报文的组 mac 地址或封装类型地址。

**命令模式：**全局配置模式。

**使用指南：**全局模式下配置自定义 uldp 协议对应的协议 mac 地址以及组 mac 地址。

**举例：**将交换机的端口 ethernet 4/5 配置为对 dot1x 报文进行隧道转发。

Switch(config)#bpdu-tunnel-protocol user-defined-protocol uldp protocol-mac 01-02-03-04-05-06 default-group-mac

## 3.9.3 bpdu-tunnel-protocol dmac

本型号交换机不支持此命令。

## 3.9.4 bpdu-tunnel-protocol stp

**命令：bpdu-tunnel-protocol stp**

**no bpdu-tunnel-protocol stp**

**功能：**配置指定端口对 stp 报文进行隧道转发；no 命令取消对端口的 stp 报文进行隧道转发。

**参数：**无。

**缺省情况：**缺省端口不对任何协议报文进行隧道转发。

**命令模式：**端口配置模式。

**使用指南：**在配置该命令时需要在端口上先关闭 stp 功能。

**举例：**将交换机的端口 ethernet 4/0/5 配置为对 stp 报文进行隧道转发。

Switch(Config)#interface ethernet 4/0/5

Switch(Config-if-ethernet 4/0/5)#bpdu-tunnel-protocol stp

## 3.9.5 bpdu-tunnel-protocol gvrp

**命令：bpdu-tunnel-protocol gvrp**

**no bpdu-tunnel-protocol gvrp**

**功能：**配置指定端口对 gvrp 报文进行隧道转发；no 命令取消对端口的 gvrp 报文进行隧道转发。

**参数：**无。

**缺省情况：**缺省端口不对任何协议报文进行隧道转发。

**命令模式：**端口配置模式。

**使用指南：**在配置该命令时需要在端口上先关闭 gvrp 功能。

**举例：**将交换机的端口 ethernet 4/0/5 配置为对 gvrp 报文进行隧道转发。

Switch(Config)#in ethernet 4/0/5

Switch(Config-if-ethernet 4/0/5)#bpdu-tunnel-protocol gvrp

### 3.9.6 bpdu-tunnel-protocol uldp

本型号交换机不支持此命令。

### 3.9.7 bpdu-tunnel-protocol lacp

本型号交换机不支持此命令。

### 3.9.8 bpdu-tunnel-protocol dot1x

**命令：bpdu-tunnel-protocol dot1x**

**no bpdu-tunnel-protocol dot1x**

**功能：**配置指定端口对 dot1x 报文进行隧道转发；no 命令取消对端口的 dot1x 报文进行隧道转发。

**参数：**无。

**缺省情况：**缺省端口不对任何协议报文进行隧道转发。

**命令模式：**端口配置模式。

**使用指南：**在配置该命令时需要在端口上先关闭 dot1x 功能。

**举例：**将交换机的端口 ethernet 4/0/5 配置为对 dot1x 报文进行隧道转发。

Switch(Config)#in ethernet 4/0/5

Switch(Config-if-ethernet 4/0/5)#bpdu-tunnel-protocol dot1x

## 3.10 DDM

### 3.10.1 clear transceiver threshold-violation

**命令：clear transceiver threshold-violation [interface ethernet <interface-list>]**

**功能：**清空软件监控的阈值异常信息。

**参数：interface ethernet <interface-list>:**要清空软件监控的阈值异常信息的端口列表。

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**清除端口 49-54 上的软件监控阈值异常信息。

Switch#clear transceiver threshold-violation interface ethernet1/1/49-54

## 3.10.2 debug transceiver

**命令：debug transceiver {on | off}**

**功能：**开启/关闭 DDM 的调试开关。

**参数：on/off:**开启或关闭。

**命令模式：**特权模式。

**缺省情况：**缺省关闭。

**使用指南：**可以使用 ctrl+o 进行关闭操作。

**举例：**打开 DDM 的调试开关。

Switch#debug transceiver on

## 3.10.3 show transceiver

**命令：show transceiver [interface ethernet <interface-list>] [detail]**

**功能：**显示收发器的监测信息。

**参数：interface ethernet <interface-list>:**要显示收发器的监测信息的端口列表。

**detail：**显示收发器的监测信息的详细信息。

**命令模式：**用户模式、特权模式、全局配置模式。

**缺省情况：**无。

**使用指南：**温度的显示精确到整数部分，其余值的显示精确到小数点后第 2 位。当某个参数值超过 Warning 阈值，显示为超过上限（W+）或超过下限（W-）；同样，当某个参数值超过 Alarm 阈值，显示为超过上限（A+）或超过下限（A-），无任何标记的参数值为正常。

**举例：**显示所有端口的 DDM 简要信息。

Switch#show transceiver

Interface Temp（℃） Voltage（V） Bias（mA） RX Power（dBM） TX Power（dBM）

## 3.10.4 show transceiver threshold-violation

**命令：show transceiver threshold-violation [interface ethernet <interface-list>]**

**功能：**显示软件监控信息。

**参数：interface ethernet <interface-list>:**要显示收发器的软件监控信息的端口列表。

**命令模式：**特权模式、全局配置模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**显示收发器的软件监控信息。

Switch(config)#show transceiver threshold-violation interface ethernet 1/1/49

## 3.10.5 transceiver-monitoring

**命令：transceiver-monitoring {enable | disable}**

**功能：**开启/关闭软件监控功能。

**参数：enable/ disable:**开启或关闭。

**命令模式：**端口配置模式。

**缺省情况：**缺省关闭。

**使用指南：**无。

**举例：**打开端口 ethernet1/1/1 软件监控功能。

Switch(config-if-ethernet1/1/1)#transceiver-monitoring enable

## 3.10.6 transceiver-monitoring interval

**命令：transceiver-monitoring interval <minutes>**

**no transceiver-monitoring interval**

**功能：**设置软件监控的时间间隔。本命令的 no 命令为设置时间间隔为默认时间间隔 15 分钟。

**参数：<minutes>**:要设置的软件监控时间间隔。

**命令模式：**全局配置模式。

**缺省情况：**缺省时间间隔为 15 分钟。

**使用指南：**无。

**举例：**设置软件监控时间间隔为 1 分钟。

Switch(config)#transceiver-monitoring interval 1

## 3.10.7 transceiver threshold

**命令：transceiver threshold {default | {temperature | voltage | bias | rx-power | tx-power} {high-alarm | low-alarm | high-warn | low-warn} {<value> | default}}**

**功能：**设置用户自定义的阈值。

**参数：default:**阈值恢复为厂商预先设置的阈值，若没指明具体的监测指标，则将所有阈值全部恢复，若指明具体的监测指标，则将此监测指标的阈值单独恢复。

**temperature：**监测指标——温度。

**voltage：**监测指标——电压。

**bias：**监测指标——偏置电流。

**rx-power：**监测指标——接收功率。

**tx-power：**监测指标——发射功率。

**high-alarm：**监测指标的报警上限，即超过此阈值，会有A+的报警。

**low-alarm：**监测指标的报警下限，即超过此阈值，会有A-的报警。

**high-warn：**监测指标的警告上限，即超过此阈值，会有W+的警告。

**low-warn**：监测指标的警告下限，即超过此阈值，会有W-的警告。

**命令模式**：端口配置模式。

**缺省情况**：缺省采用厂商预先设置的阈值。

**使用指南**：各监测指标的阈值的参数设置范围如下：

温度temperature：-128.00~128.00摄氏度（℃）

电压voltage：0.00~7.00伏（V）

偏置电流bias：0.00~140.00毫安（mA）

接收功率rx-power：-50.00~9.00分贝（dBM）

发射功率tx-power：-50.00~9.00分贝（dBM）

用户配置的各阈值参数长度最大为 20 位。当用户配置了某一实时参数的阈值后，阈值的显示时，厂商预先设置的阈值将用括号标注起来，同时也会根据用户的设置进行判断是否需要报警。

**举例**：配置端口 ethernet1/1/1 上的光模块的发送功率阈值，警告下限阈值为-12。

Switch(config-if-ethernet1/1/1)#transceiver threshold tx-power low-warning -12

## 3.10.8 optician monitor enable|disable

**命令**：**optician monitor enable|disable**

**功能**：设置 tsfpmonitor 线程的开启和关闭

**参数**：无

**命令模式**：全局配置模式。

**缺省情况**：线程默认开启。

**使用指南**：无。

**举例**：设置开启 tsfpmonitor 线程监控

Switch(config)#optician monitor enable

插入光模块：

%MODULE-1-INSERT: connector of Ethernet1/1/49 is inserted!

拔出光模块：

%MODULE-1-REMOVE: connector of Ethernet1/1/49 is removed!

Switch(config)#optician monitor disable

插入光模块 不会有任何输出提示

# 3.11 EFM OAM

## 3.11.1 clear ethernet-oam

**命令：clear ethernet-oam [interface {ethernet | } <IFNAME>]**

**功能：**清除在 OAM 特定或全部端口上报文统计信息和链路事件的统计信息。

**参数：<IFNAME>:**要清除 OAM 统计信息的端口名。

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**清除所有端口的 OAM 报文统计信息和链路事件的统计信息。

Switch#clear ethernet-oam

## 3.11.2 debug ethernet-oam error

**命令：debug ethernet-oam error**

**no debug ethernet-oam error**

**功能：**开启 OAM 错误信息的调试开关；本命令的 no 操作为关闭 OAM 错误信息的调试开关。

**参数：<*IFNAME*>**:要开启或关闭调试的端口名。

**命令模式：**特权模式。

**缺省情况：**缺省关闭。

**使用指南：**无。

**举例：**开启 OAM 错误信息调试。

Switch#debug ethernet-oam error

## 3.11.3 debug ethernet-oam event

**命令：debug Ethernet-oam event**

**功能：**全局开启 OAM 事件信息的调试开关；本命令的 no 操作为关闭 OAM 错误信息的调试开关。

**参数：**无。

**命令模式：**特权模式。

**缺省情况：**缺省关闭。

**举例：**全局开启 OAM 的事件信息调试开关。

Switch#debug ethernet-oam event

## 3.11.4 debug ethernet-oam fsm

**命令： debug ethernet-oam fsm {all | Discovery | Transmit} [interface {ethernet | } <*IFNAME*>]**

**no debug ethernet-oam fsm {all | Discovery | Transmit}[interface {ethernet | } <*IFNAME*>]**

**功能：**开启 OAM 状态机的调试开关；本命令的 no 操作为关闭 OAM 状态机的调试开关。

**参数：*<IFNAME>***:要开启或关闭调试的端口名。

**命令模式：**特权模式。

**缺省情况：**缺省关闭。

**使用指南：**无。

**举例：**打开端口 ethernet1/1/1 上的 Discovery 状态机的调试开关。

Switch# debug ethernet-oam fsm Discovery interface ethernet1/1/1

## 3.11.5 debug ethernet-oam packet

**命令：debug ethernet-oam packet [detail] {all | send | receive} [interface {ethernet | } *<IFNAME>*]**

**no debug ethernet-oam packet [detail] {all | send | receive} interface {ethernet | } *<IFNAME>***

**功能：**开启 OAM 收发数据报文信息的调试开关；本命令的 no 操作为关闭 OAM 收发数据报文信息的调试开关。

**参数：*<IFNAME>***:要开启或关闭调试的端口名。

**命令模式：**特权模式。

**缺省情况：**缺省关闭。

**使用指南：**无。

**举例：**打开端口 ethernet1/1/1 的收发报文信息调试开关。

Switch#debug ethernet-oam packet detail all interface ethernet1/1/1

## 3.11.6 debug ethernet-oam timer

**命令：debug ethernet-oam timer {all | pdu_timer | local_lost_link_timer} [interface {ethernet | } <IFNAME>]**

**no debug ethernet-oam timer {all | pdu_timer | local_lost_link_timer} [interface {ethernet | } <IFNAME>]**

**功能：**开启 OAM 指定或全部定时器刷新信息的调试开关；本命令的 no 操作为关闭 OAM 指定或全部定时器刷新信息的调试开关。

**参数：*<IFNAME>***:要开启或关闭调试的端口名。

**命令模式：**特权模式。

**缺省情况：**缺省关闭。

**使用指南：**无。

**举例：**打开端口 ethernet1/1/1 的所有定时器刷新信息的调试开关。

Switch#debug ethernet-oam timer all interface ethernet1/1/1

## 3.11.7 ethernet-oam

**命令：ethernet-oam**

**no ethernet-oam**

**功能：**使能端口 ethernet-oam 功能，本命令的 no 操作为关闭端口的 ethernet-oam 功能。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**缺省关闭 ethernet-oam 功能。

**使用指南：**无。

**举例：**使能端口 Ethernet 1/1/4 的 ethernet-oam 功能。

Switch(config)#interface ethernet 1/1/4

Switch(Config-If-Ethernet1/1/4)#ethernet-oam

## 3.11.8 ethernet-oam errored-frame threshold high

**命令：ethernet-oam errored-frame threshold high {<*high-frames*> | none}**

**no ethernet-oam errored-frame threshold high**

**功能：**配置错误帧事件的高阈值，本命令的 no 操作为恢复配置为默认值。

**参数：<*high-frames*>:**错误帧事件的检测高阈值，取值范围是 2-4294967295(frames)。

**none:** 取消高阈值的配置。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 **none**。

**使用指南：**在指定的检测周期内，如果错误帧数量大于或等于高阈值，则产生严重链路事件，设备通过发送 Flags 域中 Link Fault 标志位置为 1 的 Information OAMPDU 通知对端；高阈值配置不能小于低阈值。

**举例：**配置端口 1/1/4 的错误帧事件的高阈值为 3000。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam errored-frame threshold high 3000

## 3.11.9 ethernet-oam errored-frame threshold low

**命令：ethernet-oam errored-frame threshold low <*low-frames*>**

**no ethernet-oam errored-frame threshold low**

**功能：**配置错误帧事件的低阈值，本命令的 no 操作为恢复配置为默认值。

**参数：<*low-frames*>:**错误帧事件的检测低阈值，范围是 1-4294967295 (frames)。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 1。

**使用指南：**在指定的检测周期内，如果错误帧数量大于或等于低阈值，则产生错误帧事件，设备通过发送 event notification OAMPDU 来通知对端；低阈值配置不能大于高阈值。

**举例：**配置端口 1/1/4 的错误帧事件的低阈值为 100。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam errored-frame threshold low 100

## 3.11.10 ethernet-oam errored-frame window

**命令：ethernet-oam errored-frame window <*seconds*>**

**no ethernet-oam errored-frame window**

**功能：**配置错误帧事件的检测周期值，本命令的 no 操作为恢复配置为默认值。

**参数：<*seconds*>**为统计指定的帧数量的时间，范围是 5 到 300，单位是 200ms。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 5。

**使用指南：**经过指定的检测周期时间后，检测端口错误帧数量，如果错误帧数量大于或等于阈值，则产生相应事件并通过 OAMPDU 来通知对端。

**举例：**配置端口 1/1/4 的错误帧事件的检测周期为 20s。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam errored-frame window 100

## 3.11.11 ethernet-oam errored-frame-period threshold high

**命令：ethernet-oam errored-frame-period threshold high {<*high-frames*> | none}**

**no ethernet-oam errored-frame-period threshold high**

**功能：**配置错误帧周期事件的高阈值，本命令的 no 操作为恢复配置为默认值。

**参数：<*high-frames*>:**错误帧周期事件的检测高阈值，取值范围是 2-4294967295(frames)。

**none:** 取消高阈值的配置。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 **none**。

**使用指南：**在指定的检测周期内，如果错误帧数量大于或等于高阈值，则产生严重链路事件，设备通过发送 Flags 域中 Link Fault 标志位置为 1 的 Information OAMPDU 通知对端；高阈值配置不能小于低阈值。

**举例：**配置端口 1/1/4 的错误帧周期事件的高阈值为 3000。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam errored-frame-period threshold high 3000

## 3.11.12 ethernet-oam errored-frame-period threshold low

**命令：ethernet-oam errored-frame-period threshold low <*low-frames*>**

**no ethernet-oam errored-frame-period threshold low**

**功能：**配置错误帧周期事件的低阈值，本命令的 no 操作为恢复配置为默认值。

**参数：<*low-frames*>:**错误帧周期事件的检测低阈值，范围是 1-4294967295 (frames)。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 1。

**使用指南：**在指定的检测周期内，如果错误帧数量大于或等于低阈值，则产生错误帧周期事件，设备通过 event notification OAMPDU 来通知对端；低阈值配置不能大于高阈值。

**举例：**配置端口 1/1/4 的错误帧周期事件的低阈值为 100。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam errored-frame-period threshold low 100

## 3.11.13 ethernet-oam errored-frame-period window

**命令：ethernet-oam errored-frame-period window <*seconds*>**

**no ethernet-oam errored-frame-period window**

**功能：**配置错误帧周期事件的检测周期值，本命令的 no 操作为恢复配置为默认值。

**参数：<*seconds*>**为统计指定的帧数量的时间，范围是 1 到 300，单位是 200ms。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 5。

**使用指南：**经过指定的检测周期后，检测端口错误帧数量，如果错误帧数量大于或等于阈值，则产生相应事件并通过 OAMPDU 来通知对端。在发送报文时，错误帧周期事件中的 window 值填的是最大帧数，转换规则是：最大帧数＝接口带宽×错误帧周期事件的检测周期（s）÷（64×8）。检测周期即配置的 window 中的秒数。

**举例：**配置端口 1/1/4 的错误帧周期事件的检测周期为 10s。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam errored-frame-period window 50

## 3.11.14 ethernet-oam errored-frame-seconds threshold high

**命令：ethernet-oam errored-frame-seconds threshold high {<*high-seconds*> | none}**

**no ethernet-oam errored-frame-seconds threshold high**

**功能：**配置错误帧秒总数事件的高阈值，本命令的 no 操作为恢复配置为默认值。

**参数：<*high-seconds*>:**错误帧秒总数事件的检测高阈值，取值范围是 2-65535 (seconds)。

**none:** 取消高阈值的配置。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 **none**。

**使用指南：**在指定的检测周期内，如果错误帧秒数量大于或等于高阈值，则产生严重链路事件，设备通过发送 Flags 域中 Link Fault 标志位置为 1 的 Information OAMPDU 通知对端；高阈值配置不能小于低阈值。错误帧秒的定义：在某一秒内接收到了错误帧，则该秒称为错误帧秒。

**举例：**配置端口 1/1/4 的错误帧秒总数事件的高阈值为 3000。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam errored-frame-seconds threshold high 3000

## 3.11.15 ethernet-oam errored-frame-seconds threshold low

**命令：ethernet-oam errored-frame-seconds threshold low <*low-seconds*>**

**no ethernet-oam errored-frame-seconds threshold low**

**功能：**配置错误帧秒总数事件的低阈值，本命令的 no 操作为恢复配置为默认值。

**参数：<*low-seconds*>:**错误帧秒总数事件的检测低阈值，范围是 1-65535(seconds)。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 1。

**使用指南：**在指定的检测周期内，如果错误帧秒数量大于或等于低阈值，则产生错误帧秒总数事件，设备通过 event notification OAMPDU 来通知对端；低阈值配置不能大于高阈值。错误帧秒的定义：在某一秒内接收到了错误帧，则该秒称为错误帧秒。

**举例：**配置端口 1/1/4 的错误帧秒总数事件的低阈值为 100。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam errored-frame-seconds threshold low 100

## 3.11.16 ethernet-oam errored-frame-seconds window

**命令：ethernet-oam errored-frame-seconds window <*seconds*>**

**no ethernet-oam errored-frame-seconds window**

**功能：**配置错误帧秒总数事件的检测周期值，本命令的 no 操作为恢复配置为默认值。

**参数：<*seconds*>**为统计指定的帧数量的时间，范围是 50 到 4500，单位是 200ms。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 300。

**使用指南：**经过指定的检测周期时间后，检测端口错误帧秒数量，如果错误帧秒数量大于或等于阈值，则产生相应事件并通过 OAMPDU 来通知对端。

**举例：**配置端口 1/1/4 的错误帧秒总数事件的检测周期为 120s。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam errored-frame-seconds window 600

## 3.11.17 ethernet-oam errored-symbol-period threshold high

**命令：ethernet-oam errored-symbol-period threshold high {<*high-symbols*> | none}**

**no ethernet-oam errored-symbol-period threshold high**

**功能：**配置错误符号事件的高阈值，本命令的 no 操作为恢复配置为默认值。

**参数：<*high-symbols*>:** 错误符号事件的检测高阈值，取值范围是 2-18446744073709551615 (symbols)。

**none:** 取消高阈值的配置。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 **none**。

**使用指南：**在指定的检测周期内，如果错误符号数量大于或等于高阈值，则产生严重链路事件，设备通过发送 Flags 域中 Link Fault 标志位置为 1 的 Information OAMPDU 通知对端；高阈值配置不能小于低阈值。

**举例：**配置端口 1/1/4 的错误符号事件的高阈值为 none。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam errored-symbol-period threshold high none

## 3.11.18 ethernet-oam errored-symbol-period threshold low

**命令：ethernet-oam errored-symbol-period threshold low <*low-symbols*>**

**no ethernet-oam errored-symbol-period threshold low**

**功能：**配置错误符号事件的低阈值，本命令的 no 操作为恢复配置为默认值。

**参数：<*low-symbols*>:**错误符号事件的检测低阈值，范围是 1-18446744073709551615 (symbols)。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 1。

**使用指南：**在指定的检测周期内，如果错误符号数量大于或等于低阈值，则产生错误符号事件，设备通过 event notification OAMPDU 来通知对端；低阈值配置不能大于高阈值。

**举例：**配置端口 1/1/4 的错误符号事件的低阈值为 5。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam errored-symbol-period threshold low 5

## 3.11.19 ethernet-oam errored-symbol-period window

**命令：ethernet-oam errored-symbol-period window <*seconds*>**

**no ethernet-oam errored-symbol-period window**

**功能：**配置错误符号事件的检测周期值，本命令的 no 操作为恢复配置为默认值。

**参数：<*seconds*>**为统计指定的帧数量的时间，范围是 5 到 300，单位是 200ms。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 5。

**使用指南：**经过指定的检测周期时间后，检测端口错误符号数量，如果错误符号数量大于或等于阈值，则产生相应事件并通过 OAMPDU 来通知对端。

**举例：**配置端口 1/1/4 的错误符号事件的检测周期为 2s。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam errored-symbol-period window 10

## 3.11.20 ethernet-oam link-monitor

**命令：ethernet-oam link-monitor**

**no ethernet-oam link-monitor**

**功能：**使能 OAM 的链路监控功能，本命令的 no 操作为关闭链路监控功能。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**缺省使能本地链路监控功能。

**使用指南：**使能 OAM 监控本地链路错误，一般情况下在开启端口 OAM 功能时，就使能了链路监控；关闭 OAM 链路监控后，虽然不再监控本地的链路错误，但依然正常接收和处理对端发送的链路事件通知（Event information OAMPDU）。

**举例：**开启端口 1/1/4 的链路监控功能。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam link-monitor

## 3.11.21 ethernet-oam mode

**命令：ethernet-oam mode {active | passive}**

**no ethernet-oam mode**

**功能：**配置 OAM 功能的工作模式，本命令的 no 操为恢复配置为默认值。

**参数：active**：主动模式

**passive**：被动模式。

**命令模式：**端口配置模式。

**缺省情况：**缺省为主动模式。

**使用指南：**在两个相连的 OAM 实体中必须有至少一个设置为主动模式。在使能 OAM 功能后，就不能再更改 OAM 的工作模式，如果需要改变工作模式，需要先关闭 OAM 功能。

**举例：**配置端口 ethernet 1/1/4 的 OAM 工作模式为被动模式。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam mode passive

## 3.11.22 ethernet-oam period

**命令：ethernet-oam period <*seconds*>**

**no ethernet-oam mode**

**功能：**配置 Information OAMPDU 的发送周期，本命令的 no 操作为恢复配置为默认值。

**参数：<*seconds*>**：发送周期，取值范围是 1-2s。

**命令模式：**端口配置模式。

**缺省情况：**缺省配置为 1s。

**使用指南：**用来配置正常维持 OAM 连接的 Information OAMPDU 的发送间隔。

**举例：**配置端口 ethernet 1/1/4 的 Information OAMPDU 发送间隔为 2s。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam period 2

## 3.11.23 ethernet-oam remote-failure

**命令：ethernet-oam remote-failure**

**no ethernet-oam remote-failure**

**功能：**使能 OAM 的远端故障指示功能，本命令的 no 操作为关闭远端故障指示功能。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**缺省使能 OAM 的远端故障指示功能。

**使用指南：**使能 OAM 的远端故障指示后，若本地发生 critical-event 或 link fault 事件，将通过发送 Information OAMPDU 来通知对端，并记录该故障信息到日志系统，发送 SNMP trap 告警；关闭 OAM 远端故障指示后，虽然不再监控本地的 critical-event 或 link fault 事件，但依然正常接收和处理对端发送的故障指示信息。

**举例：**使能端口 ethernet 1/1/4 的远端故障指示功能。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam remote-failure

## 3.11.24 ethernet-oam remote-loopback

**命令：ethernet-oam remote-loopback**

**no ethernet-oam remote-loopback**

**功能：** 本地 OAM 实体发出远端环回请求，使能远端进入 OAM 环回模式；本命令的 no 操作为取消远端环回。

**参数：** 无。

**命令模式：** 端口配置模式。

**缺省情况：** 缺省不使能。

**使用指南：** 只有工作在主动模式的 OAM 实体才能发起远端环回请求，工作在被动模式的 OAM 实体不能发起远端环回；当远端 OAM 实体处于环回模式时，除了 OAMPDU 报文以外的所有报文都将按照原路返回本地端口（注意，在 OAM 环回期间将无法正常通信），管理员借助于环回可以检测链路的延时，抖动和吞吐量。必须在 OAM 连接建立后才能执行环回操作，如果环回过程中 OAM 连接断开，环回会被自动取消。本命令与 ethernet-oam remote-loopback supported 命令互斥。

**举例：** 使能端口 ethernet 1/1/4 的远端 OAM 实体进入远端环回模式。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam remote-loopback

Normal forwarding will be suspended during the remote-loopback, are you sure to start remote-loopback? [Y/N]

## 3.11.25 ethernet-oam remote-loopback supported

**命令：ethernet-oam remote-loopback supported**

no **ethernet-oam remote-loopback supported**

**功能：** 使能端口的 OAM 环回支持，本命令的 no 操作为关闭环回支持。

**参数：** 无。

**命令模式：** 端口配置模式。

**缺省情况：** 缺省关闭环回支持功能。

**使用指南：** 只有开启环回支持功能的端口才能接受 OAM 环回请求，进入环回模式。因此在使能远端进入 OAM 环回时，请确保远端已经配置了环回支持。本命令与 ethernet-oam remote-loopback 命令互斥。

举例： 使能端口 ethernet 1/1/4 的 OAM 环回支持功能。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam remote-loopback supported

## 3.11.26 ethernet-oam timeout

**命令：ethernet-oam timeout <*seconds*>**

**no ethernet-oam timeout**

**功能：**配置 OAM 连接的超时时间，本命令的 no 操作为恢复配置为默认值。

**参数：<*seconds*>** 超时时间，取值范围为 5-10s。

**命令模式：**端口配置模式。

**缺省情况：**缺省为 5s。

**使用指南：**如果超过指定的超时时间都没有接收到 OAMPDU，则断开 OAM 连接。

**举例：**配置端口 ethernet 1/1/4 的 OAM 连接超时时间为 6 秒。

Switch(Config-If-Ethernet1/1/4)#ethernet-oam timeout 6

## 3.11.27 show ethernet-oam

**命令：show ethernet-oam [{local | remote} interface { ethernet | } <*IFNAME*>]**

**功能：**显示指定端口或者全部端口的以太网 OAM 连接信息。

**参数：**若不输入任何参数，则显示所有以太网 OAM 连接的概要信息；

**local：**表示显示本地 OAM 连接详细信息；

**remote：**表示显示远端 OAM 连接详细信息；

**<*IFNAME*>：**需要显示 OAM 连接信息的端口。

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**显示以太网 OAM 连接的概要信息。

Switch#show ethernet-oam

Remote-Capability codes: L - Link Monitor, R - Remote Loopback

U - Unidirection, V - Variable Retrieval

---

| Interface | Local-Mode | Local-Capability | Remote-MAC-Addr | Remote-Mode | Remote-Capability |
|---|---|---|---|---|---|
| 1/1/1 | active | L R | 0003.0f02.2e5d | active | L R |
| 1/1/2 | active | L R | 0003.0f19.3a3e | avtive | L R |
| 1/1/4 | active | L R | 0003.0f26.480c | passive | L R |
| 1/1/5 | active | L R | 0003.0f28.020a | active | L R |

| 显示信息 | 解释 |
| --- | --- |
| Interface | 开启了Ethernet OAM功能的端口 |
| Local-Mode | 本端口OAM当前工作模式 |
| Local-Capability | 本端口OAM支持的功能<br>L - Link Monitor, R - Remote Loopback<br>U - Unidirection, V - Variable Retrieval |
| Remote-MAC-Addr | 对端MAC地址 |
| Remote-Mode | 对端OAM当前工作模式 |
| Remote-Capability | 对端OAM支持的功能<br>L - Link Monitor, R - Remote Loopback<br>U - Unidirection, V - Variable Retrieval |

显示端口 ethernet1/1/2 的本地 OAM 实体详细信息：

```
Switch#show ethernet-oam local interface ethernet1/1/2
Ethernet1/1/2 oam local Information：
oam_status=enable
local _mode=active
period=1s
timeout=8s
Loopback Supported=YES
Unidirectional Support=YES
Link Events=YES
Remote Failure=YES
local_pdu=INFO
local_mux_action=FWD
local_par_action=DISCARD
Max_OAMPDU_Size=1518
---------------------------------------------------------------------
OAM_local_flags_field：
Link Fault=0        Dying Gasp=0       Critical Events=0
---------------------------------------------------------------------
Packet statistic：
Packets                 Send                  Receive
OAMPDU                  553                   21
Information             552                   21
Event Notification      1                     0
Loopback Control        0                     0
---------------------------------------------------------------------
```

| 显示信息 | 解释 |
| --- | --- |
| oam_status | 以太网OAM使能状态<br>enable：已经使能OAM功能；<br>disable：没有使能OAM功能。 |
| local _mode | 以太网OAM的工作模式<br>active：该端口配置为主动模式；<br>passive：该端口配置为被动模式。 |
| period | 报文发送周期 |
| timeout | 连接超时时间 |
| local_pdu | 本端对于OAMPDU的发送类型控制<br>RX_INFO：该端口只能接收Information OAMPDU报文，不能发送任何OAMPDU报文；<br>LF_INFO：该端口只能发送Flags置相关比特且不带有Information TLV的Information OAMPDU报文，即只发送故障指示报文；<br>INFO：该端口只接收和发送Information OAMPDU报文；<br>ANY：该端口发送和接收任何OAMPDU报文。 |
| local_mux_action | 本端发送器的工作方式：<br>FWD：该端口允许发送任何报文；<br>DISCARD：该端口只允许发送OAMPDU报文，其他报文丢弃。 |
| local_par_action | 本地接收器的工作方式，分为以下三种：<br>FWD：允许接收任何报文；<br>DISCARD：只允许接收OAMPDU报文，其他丢弃；<br>LB：该端口接收方向处于环回状态，收到的所有非OAMPDU报文都环回回去。 |
| Loopback Supported | 是否支持环回：YES表示支持；NO表示不支持。 |
| Unidirectional Support | 是否支持单向传输：YES表示支持；NO表示不支持。 |
| Link Events | 是否支持一般链路事件：YES表示支持；NO表示不支持。 |
| Remote Failure | 是否支持严重链路事件（远端故障指示）：YES表示支持；NO表示不支持。 |
| Link Fault | 是否发生Link Fault事件：0表示没发生；1表示发生。 |
| Dying Gasp | 是否发生Dying Gasp事件：0表示没发生；1表示发生。 |
| Critical Event | 是否发生Critical Event事件：0表示没发生；1表示发生。 |
| Max_OAMPDU_Size | 支持的OAMPDU的最大长度 |
| OAMPDU | 显示OAMPDU的发送和接收的数量，是三种报文的总数。 |
| Information | 显示Information OAMPDU的发送和接收的数量。 |
| Event Notification | 显示Event Notification OAMPDU的发送和接收的数量。 |

| | |
|---|---|
| Loopback Control | 显示Loopback Control OAMPDU的发送和接收的数量。 |

显示端口 ethernet1/1/2 的远端 OAM 实体详细信息：

Switch# show ethernet-oam remote interface ethernet1/1/2

Ethernet1/1/2 oam remote Information：

Remote_Mac_Address=0003.0f19.3a3e

local _mode=active

---

local_pdu=INFO

local_mux_action=FWD

local_par_action=DISCARD

Loopback Supported=YES

Unidirectional Support=NO

Link Events=YES

Remote Failure=YES

Max_OAMPDU_Size=1518

---

OAM Remote Flags Field：

Link Fault=0 Dying Gasp=0 Critical Event=0

| 显示信息 | 解释 |
|---|---|
| Remote_Mac_Address | 远端OAM实体的桥MAC地址 |
| local _mode | 以太网OAM的工作模式<br>active：该端口配置为主动模式；<br>passive：该端口配置为被动模式。 |
| local_pdu | 本端对于OAMPDU的发送类型控制<br>RX_INFO：该端口只能接收Information OAMPDU报文，不能发送任何OAMPDU报文；<br>LF_INFO：该端口只能发送Flags置相关比特的不带有Information TLV且Information OAMPDU报文，即只发送故障指示报文；<br>INFO：该端口只接收和发送Information OAMPDU报文；<br>ANY：该端口发送和接收任何OAMPDU报文。 |
| local_mux_action | 本端发送器的工作方式：<br>FWD：该端口允许发送任何报文；<br>DISCARD：该端口只允许发送OAMPDU报文，其他报文丢弃。 |
| local_par_action | 本地接收器的工作方式，分为以下三种：<br>FWD：允许接收任何报文； |

| | |
|---|---|
| | DISCARD：只允许接收OAMPDU报文，其他丢弃；<br>LB：该端口接收方向处于环回状态，收到的所有非OAMPDU报文都环回回去。 |
| Loopback Supported | 是否支持环回：YES表示支持；NO表示不支持。 |
| Unidirectional Support | 是否支持单向传输：YES表示支持；NO表示不支持。 |
| Link Events | 是否支持一般链路事件：YES表示支持；NO表示不支持。 |
| Remote Failure | 是否支持严重链路事件：YES表示支持；NO表示不支持。 |
| Max_OAMPDU_Size | 支持的OAMPDU的最大长度 |
| Link Fault | 是否发生Link Fault事件：0表示没发生；1表示发生。 |
| Dying Gasp | 是否发生Dying Gasp事件：0表示没发生；1表示发生。 |
| Critical Event | 是否发生Critical Event事件：0表示没发生；1表示发生。 |

## 3.11.28 show ethernet-oam events

**命令：show ethernet-oam events {local | remote} [interface {ethernet |} <*IFNAME*>]**

**功能：**显示交换机上使能了 OAM 功能的所有或指定端口的链路事件统计信息。包括一般链路事件和严重链路事件。

**参数：local：**表示显示本地详细信息；

**remote：**表示显示远端详细信息；

***<IFNAME>*：**需要显示 OAM 链路事件统计信息的端口，如果不指定该参数，则显示所有端口上 OAM 的链路事件统计信息。

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**显示 ethernet1/1/1 端口上的链路事件的统计信息。

```
Switch# show ethernet-oam events local interface eth 1/1/1
ethernet1/1/1 link-events：
OAM_local_errored-symbol-period-events:
---------------------------------------------------------------------------------------------
event time stamp：3539                    errored symbol window(200ms)：5
errored symbol low threshold：1           errored symbol high threshold：none
errored symbol：1200120                   errored running total：2302512542
event running total：232

OAM_local_errored-frame-period-events:
---------------------------------------------------------------------------------------------
event time stamp：3539                    errored frame window(200ms)：50
errored frame low threshold：1            errored frame high threshold：none
```

errored frame：1200120 errored running total：2302512542
event running total：52

OAM_local_errored-frame-events:
---
event time stamp：3539 errored frame window(200ms)：5
errored frame low threshold：1 errored frame high threshold：none
errored frame：1200120 errored running total：2302512542
event running total：75

OAM_local_errored-frame-seconds-summary-events:
---
event time stamp： 3520 errored frame seconds summary window(200ms)：300
errored frame low threshold：1 errored frame high threshold：none
errored frame：1200120 errored running total：2302512542
event running total：232

OAM_local_link-fault：0
OAM_local_dying gasp：0
OAM_local_critical event：0

| 显示信息 | 解释 |
| --- | --- |
| OAM_local_errored-symbol-period-events | 本地发生的错误符号事件统计信息 |
| OAM_local_errored-frame-period-events | 本地发生的错误帧周期事件统计信息 |
| OAM_local_errored-frame-events | 本地发生的错误帧事件统计信息 |
| OAM_local_errored-frame-seconds-summary-events | 本地发生的错误帧秒总数事件统计信息 |
| event time stamp | 事件时间戳 |
| window | 事件检测周期 |
| low threshold | 事件检测低阈值 |
| high threshold | 事件检测高阈值 |
| errored frame | 错误帧数量 |
| errored symbol | 错误符号数量 |
| errored running total | 从OAM功能重置以来发生的错误数 |
| event running total | 从OAM功能重置以来发生的错误 |

| | 事件数 |
|---|---|
| OAM_local_link-fault | 本地发生的link-fault故障数 |
| OAM_local_dying gasp | 本地发生的 dying-gasp 故障数 |
| OAM_local_critical event | 本地发生的critical-event故障数 |

## 3.11.29 show ethernet-oam link-events-configuration

**命令：show ethernet-oam link-events-configuration [interface {ethernet | } *<IFNAME>* ]**

**功能：**显示交换机上使能了 OAM 功能的所有或指定端口上链路事件的配置信息。包括事件的检测周期，高低阈值等。

**参数：*<IFNAME>*：**指需要显示 OAM 链路事件配置信息的端口，如果不指定该参数，则显示所有端口上 OAM 链路事件的配置信息。

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**显示 ethernet1/1/1 端口上的链路事件的配置信息。

```
Switch#show ethernet-oam link-events-configuration interface ethernet1/1/1
Ethernet1/1/1 link-monitor configuration：
event                          high-threshold      low-threshold     window(200ms)
-------------------------------------------------------------------------------------------
Err-symbol-Period                   none               1                2
Err-frame-Period                    none               1               10
Err-frame                           none               2                5
Err-frame-second-summary            none               2              600
-------------------------------------------------------------------------------------------
```

| 显示信息 | 解释 |
|---|---|
| Event | 事件类型 |
| Err-symbol-Period | 错误符号事件 |
| Err-frame-Period | 错误帧周期事件 |
| Err-frame | 错误帧事件 |
| Err-frame-second-summary | 错误帧秒总数事件 |
| high-threshold | 高阈值 |
| low-threshold | 低阈值 |
| window(200ms) | 检测周期，单位为 200ms |

### 3.11.30 show ethernet-oam loopback-status

**命令：show ethernet-oam loopback-status [interface {ethernet | } <*IFNAME*>]**

**功能：** 显示交换机上所有或指定端口的 OAM 环回状态。

**参数：<*IFNAME*>：** 指需要显示 OAM 环回状态信息的端口，如果不指定该参数，将显示所有端口的 OAM 环回状态。

**命令模式：** 特权模式。

**缺省情况：** 无。

**使用指南：** 无。

**举例：** 显示所有端口的 OAM 环回状态。

Switch(config)#show ethernet-oam loopback-status
OAM Loopback Status：
ethernet1/0/1：disable
ethernet1/0/2：loopback_enable_waiting
ethernet1/0/3：loopback_disable_waiting
ethernet1/0/4：loopback_control
ethernet1/0/5：loopback_underControl

| 显示信息 | 解释 |
|---|---|
| disable | 端口未开启OAM环回支持。 |
| loopback_enable_waiting | 本地是环回控制端，发送了远端环回请求，正在等待远端环回的确认报文。 |
| loopback_disable_waiting | 本地是环回控制端，发送了取消远端环回的请求，正在等待远端取消环回的确认报文。 |
| loopback_control | 正处于环回过程中，且本地是环回控制端。 |
| loopback_undercontrol | 正处于环回过程中，且本地是环回受控端。 |
| no_loopback | 端口开启了OAM环回支持，但未收到环回请求。 |

## 3.12 PORT SECURITY

### 3.12.1 clear port-security

**命令：clear port-security {all | configured | dynamic } [[address <*mac-addr*> | interface <*interface-id*>] [vlan <*vlan-id*> ]]**

**功能：**本命令用来清除端口的安全 MAC 表项。

**参数：all**：端口上所有的安全 MAC 表项

**configured**：配置的安全 MAC

**dynamic**：动态学习的安全 MAC

**mac-addr**：指定安全 MAC

**interface-id**：指定端口的安全 MAC 表项

**vlan-id**：指定 VLAN

**缺省情况**：无。

**命令模式**：特权配置模式

**使用指南**：无。

**举例**：端口清除所有的安全 MAC。

Switch#clear port-security all

## 3.12.2 show port-security

**命令：show port-security [interface <*interface-id*>] [address]**

**功能**：显示 port-security 配置信息。

**参数**：interface-id：显示端口的 port-security 配置

address：显示端口的安全地址

**缺省情况**：无。

**命令模式**：任意模式

**使用指南**：无。

**举例**：显示端口所有的安全 MAC。

Switch#show port-security address interface ethernet 1/0/1

## 3.12.3 switchport port-security

**命令：switchport port-security**

**no switchport port-security**

**功能**：用来配置端口的 port-security 功能；本命令的 no 操作为关闭端口的 port-security 功能。

**参数**：无。

**缺省情况**：端口不使能 port-security 功能。

**命令模式**：端口配置模式

**使用指南**：端口使能 port-security 后，清除端口上所有的动态 mac。此后端口上学习的 mac 都标记为 FDB_TYPE_PORT_SECURITY_DYNAMIC。关闭端口 port-security，将端口上所有的 secure mac 清除或者转换为动态 mac。

**举例**：端口开启 port-security 功能。

Switch(config-if-ethernet1/1/1)#switchport port-security

## 3.12.4 switchport port-security aging

本型号交换机不支持此命令。

## 3.12.5 switchport port-security mac-address

**命令：switchport port-security mac-address <*mac-address*> [vlan <*vlan-id*>]**

**no switchport port-security mac-address <*mac-address*> [vlan <*vlan-id*>]**

**功能**：用来配置端口的静态安全 MAC，本命令的 no 操作为取消端口配置的安全 MAC。

**参数**：**mac-address**：配置指定 MAC 地址为静态安全 MAC

**vlan-id**：MAC 地址指定 VLAN，只在 trunk、hybrid 端口有效

**缺省情况**：端口没有绑定任何安全 MAC。

**命令模式**：端口配置模式

**使用指南**：配置静态安全 MAC 的时候注意最大数量是否已经配置足够大，否则可能因为超过最大允许的 MAC 数量而引起违背操作。

**举例**：端口配置安全 MAC 地址。

Switch (config-if- ethernet1/1/1)# switchport port-security mac-address 00-00-00-00-00-01

## 3.12.6 switchport port-security mac-address sticky

命令：switchport port-security mac-address sticky

no switchport port-security mac-address sticky

功能：端口模式下配置粘性使能，mac 类型为 secure-s，只在 trunk、hybrid 端口有效。本命令的 no 操作为取消端口配置的粘性使能。

参数：无

缺省情况：端口没有使能 sticky 类型安全 MAC，默认学习到的是动态安全 MAC。

命令模式：端口配置模式

使用指南：配置粘性使能，将已经在安全端口下动态学到的 mac 转换为粘性 mac，新学到的动态 mac 也是粘性 mac。粘性 mac 受端口安全数量限制。粘性 mac 与动态安全 mac 差别在于，粘性 mac 不老化。

取消配置粘性使能，安全端口下动态学到的 mac 恢复为安全动态 mac.

举例：端口使能 sticky 类型安全 mac 地址。

Switch (config-if-ethernet1/1/1)#switchport port-security mac-address sticky

## 3.12.7 switchport port-security maximum

**命令：switchport port-security maximum <*value*>**

**no switchport port-security maximum <*value*>**

**功能**：配置端口允许的最大安全 MAC 地址数。本命令的 no 操作为取消端口配置的端口允许的最大安全 MAC 地址数。

**参数**：**value**：配置端口允许的最大安全 MAC 数，取值 1-4096；这个取决于设备的最大 MAC 数量

**缺省情况**：当使能 port-security 后，没有其他配置时，此时端口上最大安全 MAC 数目为 1；

**命令模式**：端口配置模式

**使用指南**：无。

**举例**：端口配置安全 MAC 的最大数量。

Switch (config-if-ethernet1/1/1)#switchport port-security maximum 100

### 3.12.8 switchport port-security violation

**命令：switchport port-security violation {protect | recovery | restrict | shutdown}**

**no switchport port-security violation**

**功能**：当超过设定 MAC 地址数量的最大值，或访问该端口的设备 MAC 地址不是这个 MAC 地址表中该端口的 MAC 地址，或同一个 VLAN 中一个 MAC 地址被配置在几个端口上时，就会引发违反 MAC 地址安全。

**参数**：protect：保护模式，不学习新的 MAC，丢弃数据包，不发警告

recovery：触发端口违背动作后，恢复 mac 学习功能

restrict：限制模式，不学习新的 MAC，丢弃数据包，发 snmp trap，同时在 syslog 日志中记录

shutdown：关闭模式，默认模式。在这种情况下，端口被立即关闭，发 snmp trap，同时在 syslog 日志中记录

**缺省情况**：默认 violation mode 是 shutdown。

**命令模式**：端口配置模式

**使用指南**：无。

**举例**：端口配置 violation 模式为 protect。

Switch(config-if-ethernet1/1/1)#switchport port-security violation protect

## 3.13 VLAN

### 3.13.1 vlan

**命令：vlan WORD**

**no vlan WORD**

**功能**： 创建 VLAN 或者创建并进入 VLAN 配置模式。如果参数表示的为用‘;’和‘-’连接的多个 vlan，则只是创建这些 vlan。如果参数只是一个 vlan，若这个 vlan 存在，则进入 vlan 配置模式；若此 vlan 不存在，则创建此 vlan 并进入 vlan 配置模式。在 VLAN 模式中，用户可以配置 VLAN 名称和为该 VLAN 分配交换机端口。本命令的 no 操作为删除指定的 VLAN，如果参数指定了多个 vlan，则同时删除这些 vlan。

**参数：** **WORD** 为要创建/删除的 VLAN 的 VID，取值范围为 1~4094，用';'和'-'连接。

**命令模式：**全局配置模式。

**缺省情况：**交换机缺省只有 VLAN1。

**使用指南：**VLAN1 为交换机的缺省 VLAN，用户不能配置和删除 VLAN1。允许配置 VLAN 的总共数量为 4094 个。另需要提醒的是不能使用本命令删除通过 GVRP 学习到的动态 VLAN。

**举例：**创建 VLAN100，并且进入 VLAN100 的配置模式。

Switch(config)#vlan 100

Switch(Config-Vlan100)#

## 3.13.2 vlan internal

**命令：vlan <2-4094> internal**

**功能：** 指定内部 VLAN 的 ID 号。当某个 ID 号被指定为内部 VLAN 的 ID 后，就被保留不允许其它 VLAN 使用，即不能再用来创建 VLAN。内部 VLAN 仅用于 LOOPBACK 接口，不能添加物理端口。新设置的内部 VLAN ID 必须保存配置并重启交换机后才能生效。

**参数：** **<2-4094>:**指定为内部 VLAN 的 ID 号，取值范围为 2~4094。

**命令模式：** 全局配置模式。

**缺省情况：** 缺省的内部 VLAN 的 ID 为 1006。

**使用指南：** 交换机缺省采用 1006 为内部 VLAN 的 ID，一般不需要修改；只有在组网需要 1006 作为 VLAN 的 ID 时，才有必要把内部 VLAN ID 设置为其它值。内部 VLAN ID 一定要选择一个不使用的 ID 号，否则会影响其它 VLAN 的使用。该命令设置后，必须保存配置并重启交换机后才能生效。

**举例：** 设置 100 为内部 VLAN 的 ID。

Switch(config)#vlan 100 internal

## 3.13.3 vlan ingress enable

**命令：vlan ingress enable**

**no vlan ingress enable**

**功能：**打开端口的 VLAN 入口过滤功能；本命令的 no 操作为关闭入口过滤功能。

**命令模式：**端口配置模式

**缺省情况：**系统缺省打开端口的 VLAN 入口过滤功能。

**使用指南：**当打开端口的 VLAN 入口过滤功能，系统在接收数据时会检查源端口是否是该 VLAN 的成员端口，如果是则接受数据并转发到目的端口，否则丢弃该数据。

**举例：**关闭端口的 VLAN 入口规则。

Switch(Config-If-Ethernet1/1/1)# no vlan ingress enable

## 3.13.4 switchport trunk native vlan

**命令：switchport trunk native vlan <*vlan-id*>**

**no switchport trunk native vlan**

**功能：**设置 Trunk 端口的 PVID；本命令的 no 操作为恢复缺省值。

**参数：<*vlan-id*>**为 Trunk 端口的 PVID。

**命令模式：**端口配置模式。

**缺省情况：**Trunk 端口默认的 PVID 为 1。

**使用指南：**在 802.1Q 中定义了 PVID 这个概念。Trunk 端口的 PVID 的作用是当一个 untagged 的帧进入 Trunk 端口，端口会对这个 untagged 帧打上带有本命令设置的 native PVID 的 tag 标记，用于 VLAN 的转发。

**举例：**设置某 Trunk 端口的 native vlan 为 100。

```
Switch(config)#interface ethernet1/1/5
Switch(Config-If-Ethernet1/1/5)#switchport mode trunk
Switch(Config-If-Ethernet1/1/5)#switchport trunk native vlan 100
Switch(Config-If-Ethernet1/1/5)#exit
```

## 3.13.5 switchport trunk allowed vlan

**命令：switchport trunk allowed vlan {WORD | all | add WORD | except WORD | remove WORD | none}**

**no switchport trunk allowed vlan**

**功能：**设置 Trunk 端口允许通过 VLAN；本命令的 no 操作为恢复缺省情况。

**参数：WORD**： 指定的 VIDs；

**all**： 所有的 VIDs，即 1－4094；

**add**： 在现有的 allow vlan 后面加入指定的 VIDs；

**except**： 除了指定的 VIDs 外所有的 VID 都加为 allow vlan；

**remove**： 从现有的 allow vlan 列表中删除指定的 allow vlan；

**none**：所有 VLAN 都不允许通过。

**命令模式：**端口配置模式。

**缺省情况：**Trunk 端口缺省允许通过所有 VLAN。

**使用指南：**用户可以通过本命令设置哪些 VLAN 的流量通过 Trunk 端口，没有包含的 VLAN 流量则被禁止。

**举例：**设置 Trunk 端口允许通过 VLAN1，3，5-20 的流量。

```
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#switchport mode trunk
```

Switch(Config-If-Ethernet1/0/5)#switchport trunk allowed vlan 1;3;5-20
Switch(Config-If-Ethernet1/0/5)#exit

## 3.13.6 switchport mode trunk allow-null

**命令：switchport mode trunk allow-null**

**功能：**新增加一个配置端口为 trunk 端口的方式，由于原来把端口配置成 trunk 端口默认加入所有 VLAN，对于这种方式无论如何处理在开启 GVRP 功能时都不合适。所以这里增加了一个配置端口为 trunk 端口的方式，它默认不会加入任何 VLAN，所以在这样的 trunk 端口上开启 GVRP 功能比较合适。因此，推荐用户在开启端口 GVRP 功能时，先用此命令把端口配置成 trunk 端口。该命令在端口已经是 trunk 端口时也可以使用，相当于把 allow-list 置空，离开所有 VLAN。

**参数：**无。

**命令模式：**端口配置模式

**缺省情况：**默认端口为 access 模式。

**使用指南：**把端口模式变为 trunk 模式，并使其离开所有 vlan，allow-list 置空。

**举例：**

Switch(config-if-ethernet1/1/1)#switchport mode trunk allow-null

## 3.13.7 switchport mode

**命令：switchport mode {trunk | access | hybrid}**

**功能：**设置交换机的端口为 access 模式，trunk 模式或 hybrid 模式。

**参数：trunk** 表示端口允许通过多个 VLAN 的流量；**access** 为端口只能属于一个 VLAN；**hybrid** 表示端口可以以 tag 或 untag 方式允许通过多个 VLAN 的流量。

**命令模式：**端口配置模式。

**缺省情况：**端口缺省为 Access 模式。

**使用指南：**工作在 trunk mode 下的端口称为 Trunk 端口，Trunk 端口可以通过多个 VLAN 的流量，通过 Trunk 端口之间的互联，可以实现不同交换机上的相同 VLAN 的互通；工作在 access mode 下的端口称为 Access 端口，Access 端口可以分配给一个 VLAN，并且同时只能分配给一个 VLAN。Hybrid 端口同样可以通过多个 VLAN 的流量，可以接收和发送多个 VLAN 的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。Hybrid 端口和 Trunk 端口在接收数据时，处理方法是一样的，唯一不同之处在于发送数据时：Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不打标签。端口的属性不允许在 Hybrid 和 Trunk 之间直接转换，必须先配置为 Access，再配置为 Hybrid 或 Trunk。取消端口的 Trunk 或 Hybrid 属性时，端口属性恢复到默认的 Access 属性，属于 vlan 1。

**举例：**将端口 5 设置为 trunk 模式，端口 8 设置为 access 模式，端口 10 为 Hybrid 模式。

Switch(config)#interface ethernet 1/1/5
Switch(Config-If-Ethernet1/1/5)#switchport mode trunk
Switch(Config-If-Ethernet1/1/5)#exit
Switch(config)#interface ethernet 1/1/8
Switch(Config-If-Ethernet1/1/8)#switchport mode access
Switch(Config-If-Ethernet1/1/8)#exit
Switch(config)#interface ethernet 1/1/10
Switch(Config-If-Ethernet1/1/10)#switchport mode hybrid
Switch(Config-If-Ethernet1/1/10)#exit

## 3.13.8 switchport interface

**命令：switchport interface [ethernet | portchannel] [<*interface-name* | *interface-list*>]**

**no switchport interface [ethernet | portchannel] [<*interface-name* | *interface-list*>]**

**功能：**给 VLAN 分配以太网端口的命令；本命令的 no 操作为删除指定 VLAN 内的一个或一组端口。

**参数：ethernet** 要添加的为以太网端口；**portchannel** 要添加的为一个链路聚合端口；***<interface-name>*** 端口名称，如 e1/1/1，若选择端口名称则不用选 etherneth 或 portchannel；***<interface-list>*** 要添加或者删除的以太网端口的列表，支持";" "-" ，如：ethernet 1/1/1;3;4-7;8，或者是***<interface-list>***要添加或删除的端口链路聚合，如 port-channel 1。

**命令模式：**VLAN 配置模式。

**缺省情况：**新建立的 VLAN 缺省不包含任何端口。

**使用指南：**Access 端口为普通端口，可以加入 VLAN，但同时只允许加入一个 VLAN。

**举例：**为 VLAN100 分配千兆以太网端口 1，3，4-7，8。

Switch(Config-Vlan100)#switchport interface ethernet 1/1/1;3;4-7;8

## 3.13.9 switchport hybrid native vlan

**命令：switchport hybrid native vlan <*vlan-id*>**

**no switchport hybrid native vlan**

**功能：**设置 Hybrid 端口的 PVID；本命令的 no 操作为恢复缺省值。

**参数：*<vlan-id>***为 Hybrid 端口的 PVID。

**命令模式：**端口配置模式。

**缺省情况：**Hybrid 端口默认的 PVID 为 1。

**使用指南：**Hybrid 端口的 PVID 的作用是当一个 untagged 的帧进入 Hybrid 端口，端口会对这个 untagged 帧打上带有本命令设置的 native PVID 的 tag 标记，用于 VLAN 的转发。

**举例：**设置某 Hybrid 端口的 native vlan 为 100。

Switch(config)#interface ethernet1/1/5

Switch(Config-If-Ethernet1/1/5)#switchport mode hybrid
Switch(Config-If-Ethernet1/1/5)#switchport hybrid native vlan 100
Switch(Config-If-Ethernet1/1/5)#exit

## 3.13.10 switchport hybrid allowed vlan

**命令：switchport hybrid allowed vlan {WORD | all | add WORD | except WORD | remove WORD | none} {tag | untag}**

**no switchport hybrid allowed vlan**

**功能：**设置 Hybrid 端口允许以 tag 或 untag 方式通过的 VLAN；本命令的 no 操作为恢复缺省情况。

**参数：WORD**：将 vlan List 加为 allowed vlan,同时覆盖之前的配置。

**all**：将所有 VLAN 都设置为 allowed vlan。

**add WORD**：在现有的 allowed vlanList 中增加 vlanList。

**except WORD**：将除了 vlan List 外所有的 VLAN 都设置为 allowed vlan。

**remove WORD**：从现有的 allow vlanList 中删除 vlanList 指定的 VLAN。

**none**：所有 VLAN 都不允许通过。

**tag**：以 tag 方式加入指定的 VLAN。

**untag**：以 untag 方式加入指定的 VLAN。

**命令模式：**端口配置模式。

**缺省情况：**不允许任何 VLAN 的流量通过。

**使用指南：**用户可以通过本命令设置哪些 VLAN 的流量通过 Hybrid 端口，没有包含的 VLAN 流量则被禁止。设置 allowed vlan 为 tag 和 untag 方式的区别为：设置 VLAN 为 untag 方式时，通过 Hybrid 口去往该 VLAN 的流量不带 tag；设置 VLAN 为 tag 方式时，通过 Hybrid 口去往该 VLAN 的流量带着相应的 tag。Hybrid 不可以同时以 tag 和 untag 方式 allowed 同一个 VLAN，如果先后配置了 allowed 某个 VLAN 为 tag 和 untag 方式，则后配置的会覆盖前面的配置。

**举例：**设置 Hybrid 端口以 untag 方式 allowed vlan 1;3;5-20，以 tag 方式 allowed vlan 100;300;500-2000。

Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/5)#switchport hybrid allowed vlan 1;3;5-20 untag
Switch(Config-If-Ethernet1/0/5)#switchport hybrid allowed vlan 100;300;500-2000 tag
Switch(Config-If-Ethernet1/0/5)#exit

## 3.13.11 switchport forbidden vlan

**命令：switchport forbidden vlan {WORD | all | add WORD | except WORD | remove WORD}**

**no switchport forbidden vlan**

**功能：**设置端口的 forbidden vlan，注意此命令只能在 trunk 端口或者 hybrid 端口上配置，但是可以在没有开启 GVRP 功能的端口上配置。no 命令为取消端口的 forbidden vlanlist。

**参数：**WORD:将 vlanList 加为 forbidden vlan，同时覆盖之前的配置

all:将所有 vlan 都设置为 forbidden vlan

add WORD:在现有的 forbidden vlanList 中增加 vlanList

except WORD:将除了 vlanList 外所有的 vlan 都设置为 forbidden vlan

remove WORD:从现有的 forbidden vlanList 中删除 vlanList 指定的 vlan

**命令模式：**端口配置模式

**缺省情况：**默认端口的 forbidden vlanList 为空。

**使用指南：**把端口的 forbidden vlanList 相应标识位置位，并清除端口的 allow vlanList 标志位。如果端口静态加入了这些 VLAN，则静态离开这些 VLAN，并且向 GVRP 模块发出消息，使该端口相应 VLAN 的注册状态机进入 forbidden 工作模式。

**举例：**端口离开相应 VLAN，GVRP 相应注册状态机进入 forbidden 模式。

Switch (config-if-ethernet1/1/1)# switchport forbidden vlan all

## 3.13.12 switchport access vlan

**命令：switchport access vlan <*vlan-id*>**

**no switchport access vlan**

**功能：**将当前 Access 端口加入到指定 VLAN；本命令 no 操作为将当前端口从 VLAN 里删除。

**参数：<*vlan-id*>**为当前端口要加入的 vlan VID，取值范围为 1~4094。

**命令模式：**端口配置模式。

**缺省情况：**所有端口默认属于 VLAN1。

**使用指南：**只有属于 Access mode 的端口才能加入到指定的 VLAN 中，并且 Access 端口同时只能加入到一个 VLAN 里去。

**举例：**设置某 Access 端口加入 VLAN100。

Switch(config)#interface ethernet 1/1/8

Switch(Config-If-Ethernet1/1/8)#switchport mode access

Switch(Config-If-Ethernet1/1/8)#switchport access vlan 100

Switch(Config-If-Ethernet1/1/8)#exit

## 3.13.13 show vlan

**命令：show vlan [brief| summary] [id <*vlan-id*>] [name <*vlan-name*>] [internal usage [id <*vlan-id*>| name <*vlan-name*>]] [private-vlan [id <*vlan-id*> | name <*vlan-name*> ]]**

**功能：** 显示所有 VLAN 或者指定 VLAN 的详细状态信息。

**参数：** **brief** 简要信息； ***<summary>*** 显示 VLAN 统计信息；***<vlan-id>***为指定要显示状态信息的 VLAN 的 VLAN ID，取值范围 1~4094；***<vlan-name>***为指定要显示状态信息的 VLAN 的 VLAN 名，长度为 1~11。 **private-vlan** 显示 private-vlan 的 id、name、关联 vlan 和端口等相关信息。

**命令模式：** 特权和配置模式。

**使用指南：** 如果不指定***<vlan-id>***或***<vlan-name>***，则显示交换机所有 VLAN 的状态信息。

**举例：** 显示当前 VLAN 状态信息；显示当前 VLAN 统计信息。

```
Switch#show vlan
VLAN Name              Type         Media      Ports
---- ----------- ---------- --------- ------------------------------------
1    default           Static       ENET       Ethernet1/1/1    Ethernet1/1/2
                                                 Ethernet1/1/3    Ethernet1/1/4
                                                 Ethernet1/1/9    Ethernet1/1/10
                                                 Ethernet1/1/11   Ethernet1/1/12
2    VLAN0002          Static       ENET       Ethernet1/1/5      Ethernet1/1/6
                                                 Ethernet1/1/7      Ethernet1/1/8

Switch#sh vlan summary
The max. vlan entrys: 4094

Existing Vlans:
Universal Vlan:
1    12    13    15    16    22

Total Existing Vlans is:6
```

| 显示内容 | 解释 |
|---|---|
| VLAN | VLAN 号。 |
| Name | VLAN 名。 |
| Type | VLAN 的属性，是静态配置的还是动态学习到的。 |
| Media | VLAN 的二层属性。 |
| Ports | VLAN 内 Access 端口。 |

```
Switch(config)#show vlan private-vlan
VLAN Name        Type    Asso   VLAN    Ports
---- ------------ ---------- --------- ---------------------------------------
100   VLAN0100    Primary   101     102       Ethernet1/1/9        Ethernet1/1/10
                                                Ethernet1/1/11
      Ethernet1/1/12
                                                Ethernet1/1/13
101   VLAN0101    Community 100              Ethernet1/1/9        Ethernet1/1/10
                                                Ethernet1/1/11       Ethernet1/1/12
                                                Ethernet1/1/13
102   VLAN0102    Isolate   100              Ethernet1/1/9
```

## 3.13.14 private-vlan association

**命令：private-vlan association <*secondary-vlan-list*>**

**no private-vlan association**

**功能：** 设置 Private VLAN 的绑定操作，该命令的 no 操作为取消 Private VLAN 绑定。

**参数：** <*secondary-vlan-list*> 为与指定 Primary VLAN 相关联的 Secondary VLAN 列表，Secondary VLAN 包括 Isolated VLAN 和 Community VLAN 两种，支持';'连接多个 Secondary VLAN。

**命令模式：** VLAN 配置模式。

**缺省情况：** 缺省没有 Private VLAN 绑定。

**使用指南：**只有 Primary 类型的 VLAN 才能设置 Private VLAN 关联关系；被关联到 Primary VLAN 上的 Secondary VLANs 内的各个端口可以和关联的 Primary VLAN 内的各个端口进行通信。

在设置 Private VLAN 关联前，三种类型的 Private VLAN 都没有以太网端口的成员端口；存在 Private VLAN 关联关系的 Primary VLAN 不能被删除；被解除关联关系的 Private VLANs 会自动将所属成员端口清空。

**举例：** 将 Isolated VLAN200、Community VLAN300 关联到 Primary VLAN100 上。

```
Switch(Config-Vlan100)#private-vlan association 200;300
```

## 3.13.15 private-vlan

**命令：private-vlan {primary | isolated | community}**

**no private-vlan**

**功能：** 将当前VLAN设置为Private VLAN，该命令的no操作为取消Private VLAN设置。

**参数：** primary 将当前VLAN设置为Primary VLAN，isolated将当前VLAN设置为Isolated VLAN，community将当前VLAN设置为Community VLAN。

**命令模式：** VLAN配置模式。
**缺省情况：** 缺省没有Private VLAN配置。
**使用指南：** Private VLAN分为三种：Primary VLAN，Isolated VLAN和Community VLAN。Primary VLAN内的端口可以和关联到该Primary VLAN的Isolated VLAN和Community VLAN中的端口进行通信；Isolated VLAN内的端口之间是隔绝的，它们只可以和其相关联的Primary VLAN内的端口通信；Community VLAN内的端口相互之间可以通信，也可以和其相关联的Primary VLAN内的端口通信；在Isolated VLAN内的端口和在Community VLAN内的端口之间不能通信。
只有不包含任何以太网端口的VLAN才能被设置为Private VLAN；只有设置了关联关系的Private VLAN才能将Access类型的以太网端口设置为成员端口，Isolate VLAN的成员端口应该关闭ingress功能，否则无法通讯；普通VLAN若被设置成Private VLAN后，会自动将所属以太网端口清空。
另外注意GVRP不传播Private VLAN的信息。
**举例：** 将VLAN100、200、300设置为private vlan，类型分别为primary、Isolated、Community。
Switch(config)#vlan 100
Switch(Config-Vlan100)#private-vlan primary
Note:This will remove all the ports from vlan 100
Switch(Config-Vlan100)#exit
Switch(config)#vlan 200
Switch(Config-Vlan200)#private-vlan isolated
Note:This will remove all the ports from vlan 200
Switch(Config-Vlan200)#exit
Switch(config)#vlan 300
Switch(Config-Vlan300)#private-vlan community
Note:This will remove all the ports from vlan 300
Switch(Config-Vlan300)#exit

## 3.13.16 name

**命令：name *<vlan-name>***
**no name**
**功能：**为 VLAN 指定名称，VLAN 的名称是对该 VLAN 一个描述性字符串；本命令的 no 操作为删除 VLAN 的名称。
**参数：*<vlan-name>***为指定的 vlan 名称字符串。
**命令模式：**VLAN 配置模式。
**缺省情况：**VLAN 缺省名称为 vlanXXX，其中 XXX 为 VID。
**使用指南：**交换机提供为不同的 VLAN 指定名称的功能，有助于用户记忆 VLAN，方便管理。
**举例：**为 VLAN100 指定名称为 TestVlan。
Switch(Config-Vlan100)#name TestVlan

## 3.13.17 Vlan-flow-statistics

**命令：vlan-flow-statistics**

**no vlan-flow-statistics**

**功能：开启流量统计，no 表示关闭此功能。**

**参数：无。**

**命令模式：全局配置模式。**

**缺省情况：缺省不开启。**

**使用指南：无**

**举例：** 设置开启基于全局的流量统计。

Switch(config)#vlan-flow-statistics

# 3.14 GVRP

## 3.14.1 garp timer join

**命令：garp timer join <200-500>**

**功能：**设置 garp join 定时器的时间，注意 join timer 必须小于 leave timer 的 1/2。

**参数：**<200-500>:定时器时间（ms）

**命令模式：**全局配置模式

**缺省情况：**join 定时器的默认值为 200（ms）。

**使用指南：**检查设置值是否满足范围要求，满足则把 garp 定时器时间修改为设置值，否则返回配置错误。

**举例：**将 garp join 定时器的时间设置为 200ms。

Switch(config)#garp timer join 200

## 3.14.2 garp timer leave

**命令：garp timer leave <500-1200>**

**功能：**设置 garp leave 定时器的时间，注意 leave timer 必须大于 join timer 的 2 倍，并且小于 leaveAll timer。

**参数：**<500-1200>:定时器时间（ms）

**命令模式：**全局配置模式

**缺省情况：**leave 定时器的默认值为 600（ms）。

**使用指南：**检查设置值是否满足范围要求，满足则把 garp 定时器时间修改为设置值，否则返回配置错误。

**举例：**将 garp leave 定时器的时间设置为 600ms。

Switch (config)#garp timer leave 600

## 3.14.3 garp timer leaveAll

**命令：garp timer leaveall <5000-60000>**

**功能：**设置 garp leaveAll 定时器的时间，注意 leaveAll timer 必须大于 leave timer。

**参数：**<5000-60000>:定时器时间（ms）

**命令模式：**全局配置模式

**缺省情况：**leaveAll 定时器默认值为 10000（ms）。

**使用指南：**检查设置值是否满足范围要求，满足则把 GARP 的 leaveAll 定时器修改为设置值，否则返回配置错误。

**举例：**将 garp leaveAll 定时器的时间设置为 20000ms。

Switch(config)# garp timer leaveall 20000

## 3.14.4 gvrp（全局）

**命令：gvrp**

**no gvrp**

**功能：**全局开启/关闭 GVRP 功能。

**参数：**无。

**命令模式：**全局配置模式

**缺省情况：**默认关闭 GVRP 全局功能。

**使用指南：**开启全局 GVRP 功能，只有开启全局 GVRP 功能 GVRP 模块才能正常工作。

**举例：**显示开启全局 GVRP 功能。

Switch(config)#gvrp

## 3.14.5 gvrp（端口）

**命令：gvrp**

**no gvrp**

**功能：**开启/关闭端口 GVRP 功能。注意：可以在没有开启全局 GVRP 功能前先开启端口 GVRP 功能，但是不生效，只有当开启全局 GVRP 功能后才生效。

**参数：**无。

**命令模式：**端口配置模式

**缺省情况：**默认关闭 GVRP 端口功能。

**使用指南：**只有在 trunk 端口和 hybrid 端口上才能开启 GVRP 功能，在 access 端口开启 GVRP 功能会返回一个不能在 access 端口开启 GVRP 的错误，在端口上开启 GVRP 功能后会把该端口添加到 GVRP 中（即给该端口在 GVRP 中添加相应状态机等结构）。

**举例：**显示开启端口 GVRP 功能。

Switch(config-if-ethernet1/1/1)#gvrp

## 3.14.6 no garp timer

**命令：no garp timer (join | leave | leaveall)**

**功能：**把 garp join|leave|leaveAll 定时器恢复成默认值。

**参数：** join: join 定时器

leave: leave 定时器

leaveAll: leaveAll 定时器

**命令模式：**全局配置模式

**缺省情况：**join|leave|leaveAll 定时器的默认值为 200|600|10000（ms）。

**使用指南：**检查相应 timer 设置成默认值后是否满足范围要求，满足则把 GARP 的 join|leave|leaveAll 定时器时间还原为默认值，否则返回配置错误。

**举例：**GARP 定时器时间还原到默认值。

Switch(config)#no garp timer leaveal

## 3.14.7 show garp timer

**命令：show garp timer (join | leave | leaveall | )**

**功能：**显示当前各个定时器的时间，注意这个时间不是定时器运行的剩余时间，而是每次开启定时器赋予的定时器初始值。

**参数：** join: join 定时器

leave: leave 定时器

leaveAll: leaveAll 定时器

**命令模式：**特权配置模式

**缺省情况：**join|leave|leaveAll 定时器的默认值为 200|600|10000（ms）。

**使用指南：**根据命令中选择的定时器，输出相应定时器时间。

**举例：**显示出当前各个定时器的时间。

Switch#show garp timer join

Garp join timer’s value is 200(ms)

## 3.14.8 show gvrp fsm information

**命令：show gvrp fsm information interface (ethernet | port-channel ) IFNAME**

**功能：**显示指定端口或所有端口当前所有属性注册状态机和请求状态机的状态。

**参数：**ethernet:物理端口

port-channel:汇聚端口

IFNAME:端口名

**命令模式：**特权配置模式

**缺省情况：**注册状态机默认状态是 MT，请求状态机默认状态是 VO。

**使用指南：**遍历端口的所有注册状态机和请求状态机，并显示出相应状态。

**举例：**显示所有状态机状态。

Switch#show gvrp fsm information interface ethernet 1/1/1

VA：Very anxious Active member，AA：Anxious Active member，QA：Quiet Active member

VP：Very anxious Passive member，AP：Anxious Passive member，QP：Quiet Passive member

VO：Very anxious Observer，AO：Anxious Observer，QO：Quiet Observer

LA：Leaving Acitve member，LO：leaving Observer

Interface ethernet 1/1/1 gvrp fsm information:

| Index | VLANID | Applicant | Registrar |
|---|---|---|---|
| 1 | 100 | VO | LV |
| 2 | 300 | VP | IN |

## 3.14.9 show gvrp leaveAll fsm information

**命令：show gvrp leaveall fsm information interface (ethernet | port-channel ) IFNAME**

**功能：**显示指定端口或所有端口 leaveAll 状态机状态。

**参数：**ethernet:物理端口

port-channel:汇聚端口

IFNAME:端口名

**命令模式：**特权配置模式

**缺省情况：**leaveAll 注册状态机默认状态是 passive。

**使用指南：**查看端口 leaveAll 状态机状态。

**举例：**显示端口 leaveAll 状态机状态。

Switch#show gvrp leaveall fsm information interface ethernet 1/1/1

| Interface | leaveAll fsm |
|---|---|
| Ethernet1/1/1 | passive |

## 3.14.10 show gvrp leavetimer running information

**命令：show gvrp leavetimer running information (vlan <1-4094> |) interface (Ethernet | port-channel |) IFNAME**

**功能：**显示当前端口所有 leavetimer 运行信息。

**参数：**<1-4094>：VLAN 标识

Ethernet：物理端口

port-channel：汇聚端口

IFNAME：端口名

**命令模式：**特权配置模式

**缺省情况：** leavetimer 默认是关闭状态。

**使用指南：**遍历端口的所有注册状态机，显示出每个 leave 定时器的运行状态及到期时间。

**举例：**显示当前端口所有 leave 定时器的运行状态及到期时间。

Switch#show gvrp leavetimer running information interface ethernet 1/1/1

| VLANID | running state | expired time |
|---|---|---|
| 100 | UP | 0.2 s |
| 300 | DOWN | non |

## 3.14.11 show gvrp port-member

**命令：show gvrp (active |) port-member**

**功能：**显示当前所有开启 GVRP 的端口，active 表示开启 GVRP 并且处于活动状态的端口。

**参数：**Active：表示端口处于活动状态

**命令模式：**特权配置模式

**缺省情况：**默认端口关闭 GVRP 协议。

**使用指南：**遍历 GVRP 中保存的开启了 GVRP 协议或者开启协议并处于活动状态的端口，显示出来。

**举例：**显示所有开启 GVRP 协议（或者并处于活动状态）的端口。

Switch#show gvrp port-member

Ports which were enabled gvrp included：

| | |
|---|---|
| Ethernet1/1/3（T） | Ethernet1/1/4（T） |
| Ethernet1/1/5（T） | Ethernet1/1/6（T） |
| Ethernet1/1/7（T） | Ethernet1/1/8（T） |
| Ethernet1/1/9（T） | Ethernet1/1/10（T） |

## 3.14.12 show gvrp port registerd vlan

**命令：show gvrp port (dynamic | static ) registerd vlan interface (Ethernet | port-channel |) IFNAME**

**功能：**显示当前端口所有动态注册或者静态注册的 VLAN。

**参数：**dynamic：动态注册

static：静态注册

Ethernet:物理端口

port-channel:汇聚端口

IFNAME：端口名

**命令模式：**特权配置模式

**缺省情况：**默认情况下端口动态或者静态注册的 VLAN 个数为零。

**使用指南：**遍历端口的注册状态机，把包含动态或者静态注册的注册状态机对应的 VLAN 显示出来。

**举例：**显示当前端口所有的动态注册或者静态注册的 VLAN。

Switch#show gvrp port registerd vlan interface ethernet 1/1/1

Current port dynamic registerd vlan included：

Vlan10 vlan20

Vlan40 vlan60

Current port static registerd vlan included：

Vlan10 vlan30

Vlan40 vlan200

## 3.14.13 show gvrp timer running information

**命令：show gvrp timer (join| leaveall) running information interface (ethernet | port-channel |) IFNAME**

**功能：**显示当前端口所有 join|leaveAll 定时器运行信息。

**参数：**join: join 定时器

leaveAll: leaveAll 定时器

ethernet:物理端口

port-channel:汇聚端口

IFNAME:端口名

**命令模式：**特权配置模式

**缺省情况：**默认状态下 join 定时器是关闭的，leaveAll 定时器是开启的。

**使用指南：**查看端口当前的 join|leaveAll 定时器运行状态。

**举例：**显示各个定时器的运行状态及到期时间。

Switch(config)#show gvrp timer join running information interface ethernet 1/1/1

Current port’s jointimer running state is: UP

Current port’s jointimer expired time is: 0.2 s

## 3.14.14 show gvrp vlan registerd port

**命令：show gvrp vlan <1-4094> registerd port**

**功能：**显示出注册了指定 VLAN 的端口集合。

**参数：**<1-4094>：VLAN 标识

**命令模式：**特权配置模式

**缺省情况：**默认情况下注册了指定 VLAN 的端口集合为空。

**使用指南：**无。

**举例：**显示注册了当前 VLAN 的所有端口。

Switch#show gvrp vlan 100 registerd port

Ethernet1/1/3（T） Ethernet1/1/4（T）

Ethernet1/1/5（T） Ethernet1/1/6（T）

Ethernet1/1/7（T） Ethernet1/1/8（T）

Ethernet1/1/9（T） Ethernet1/1/10（T）

## 3.14.15 debug gvrp event

**命令：debug gvrp event interface (ethernet | port-channel | ) IFNAME**

**no debug gvrp event interface (ethernet | port-channel | ) IFNAME**

**功能：**开启/关闭 GVRP 事件调试信息开关，包括状态机的转移以及定时器到期等信息。

**参数：**ethernet：物理端口

port-channel：汇聚端口

IFNAME：端口名

**命令模式：**特权配置模式

**缺省情况：**默认事件调试信息开关关闭。

**使用指南：**把 GVRP 事件调试信息开关打开。

**举例：**显示 GVRP 事件调试信息。

Switch#debug gvrp event interface ethernet 1/1/1

%Jan 16 02:25:14 2006 GVRP EVENT: LO -> VO ，interface ethernet 1/1/1，vlan 100

%Jan 16 02:35:15 2006 GVRP EVENT: join timer expire，interface ethernet 1/1/1

## 3.14.16 debug gvrp packet

**命令：debug gvrp packet (receive | send) interface (ethernet | port-channel | ) IFNAME**

**no debug gvrp packet (receive | send) interface (ethernet | port-channel | ) IFNAME**

**功能：**开启/关闭 GVRP 报文调试信息开关。

**参数：**receive:打开收到 GVRP 报文调试开关

send:打开发送 GVRP 报文调试开关

ethernet:物理端口

port-channel:汇聚端口

IFNAME:端口名

**命令模式：**特权配置模式

**缺省情况：**默认报文调试信息开关关闭。

**使用指南：**把 GVRP 报文调试信息开关打开。

**举例：**显示 GVRP 报文收发信息。

Switch#debug gvrp packet receive interface ethernet 1/1/1

Receive packet, smac 00-21-27-aa-0f-46, dmac 01-80-C2-00-00-21,
length 90, protocol ID:1, attribute type:0x01,

| Attribute Index | Length | Event | Value |
|---|---|---|---|
| 1 | 10 | joinIn | 100 |
| 2 | 10 | joinEmpty | 140 |
| 3 | 10 | leaveIn | 150 |
| 4 | 10 | leaveEmpty | 180 |

# 3.15 Dot1q-tunnel

## 3.15.1 dot1q-tunnel enable

**命令：dot1q-tunnel enable**

**no dot1q-tunnel enable**

**功能：** 使交换机的 access 端口进入 dot1q-tunnel 模式；本命令的 no 命令为恢复缺省值。

**参数：** 无。

**命令模式：** 端口配置模式。

**缺省情况：** 端口缺省为没有使能 dot1q-tunnel 功能。

**使用指南：** 端口使能 dot1q-tunnel 后，对于从该端口进入的无 VLAN tag（以下简称 tag）的数据包打上一层 tag；对于已经有 tag 的数据包打上外层 tag，tag 中的 TPID 为 8100，VLAN ID 为该端口所属的 VLAN ID。带有双层 tag 的数据包由 MAC 地址与外层 tag 决策转发，直到从 access 端出去时去掉外层 tag。由于打上外层 tag 时可能会使数据包长度超过正常大小，故建议该命令与 Jumbo 功能一同使用。本命令在 access 端口上使用。该命令和 dot1q-tunnel tpid 互斥，并且与 vlan-translation enable 互斥。

**举例：** 将端口 1 加入 VLAN3 并启用 dot1q-tunnel 功能。

```
Switch(config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/1/1
Switch(Config-Vlan3)#exit
Switch(config)#interface ethernet 1/1/1
Switch(Config-If-Ethernet1/1/1)# dot1q-tunnel enable
Switch(Config-If-Ethernet1/1/1)# exit
Switch(config)#
```

## 3.15.2 dot1q-tunnel tpid

**命令：dot1q-tunnel tpid {0x8100 | 0x9100 | 0x9200 | *<1-65535>* }**

**功能：** 设置交换机 trunk 端口的协议类型（TPID）。

**参数：** 无。

**命令模式：** 端口配置模式。

**缺省情况：** 端口缺省 TPID 为 0x8100。

**使用指南：** 该功能是为了方便与其它厂商的设备进行互连。与交换机 trunk 端口连接的设备如果发送 TPID 为 0x9100 的数据包，则将该端口的 TPID 设置为 0x9100，这样交换机就可以正常接收并处理收到的数据包。该命令和 dot1q-tunnel enable 互斥。

**举例：** 将交换机的端口 10 设置为 trunk 端口，并设置其 TPID 为 0x9100。

```
Switch(config)#interface ethernet 1/1/10
Switch(Config-If-Ethernet1/1/10)#switchport mode trunk
Switch(Config-If-Ethernet1/1/10)#dot1q-tunnel tpid 0x9100
Switch(Config-If-Ethernet1/1/10)#exit
Switch(config)
```

## 3.15.3 dot1q-tunnel selective enable

**命令：dot1q-tunnel selective enable**

**no dot1q-tunnel selective enable**

**功能：** 使能 dot1q-tunnel selective 模式,即开启灵活 QINQ 模式；本命令的 no 命令为恢复缺省值。

**参数：** 无。

**命令模式：** 端口配置模式。

**缺省情况：** 端口缺省为没有使能 dot1q-tunnel selective 功能。

**使用指南：** 端口使能 dot1q-tunnel selective 后，那么下面的命令 dot1q-tunnel selective s-vlan 就会生效，端口会根据配置的 cvlan 打上一层 svlan。

**举例：** 端口 1/0/1 开启灵活 qinq。

```
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# dot1q-tunnel selective enable
Switch(Config-If-Ethernet1/0/1)# exit
Switch(config)#
```

## 3.15.4 dot1q-tunnel selective s-vlan

**命令：dot1q-tunnel selective s-vlan <1-4094> c-vlan WORD**

**no dot1q-tunnel selective s-vlan <1-4094> （c-vlan WORD | ）**

**功能：** 配置指定的 cvlan 或者 cvlan 范围，打上 svlan 标签；本命令的 no 为删除配置。

**参数：**<1-4094>：表示 s-vlan 的范围

WORD：为 c-vlan 的 VLAN ID，可以使用“-”和“；”表示更多的 VLAN

**命令模式：** 端口配置模式。

**缺省情况：** 没有配置 qinq 关系。

**使用指南：** 本命令配置灵活 qinq 的对应关系，对匹配上的 cvlan 打上对应的 svlan，建议端口配置成 trunk 或者 hybrid 模式使用，svlan 需要存在。

**举例：** 端口 1/0/1 配置灵活 qinq，将 VLAN100 的报文外面加上一层 VLAN200 的标签出去

```
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# dot1q-tunnel selective enable
Switch(Config-If-Ethernet1/0/1)# dot1q-tunnel selective s-vlan 200 c-vlan 100
Switch(Config-If-Ethernet1/0/1)# exit
Switch(config)#
```

## 3.15.5 dot1q-tunnel selective miss drop

**命令：dot1q-tunnel selective miss drop**

**no dot1q-tunnel selective miss drop**

**功能：** 在 dot1q-tunnel selective 模式下,对于没有进行灵活 qinq 的报文会被丢弃；本命令的 no 命令为恢复缺省值。

**参数：** 无。

**命令模式：** 端口配置模式。

**缺省情况：** 端口缺省为没有使能 dot1q-tunnel selective miss drop 功能。

**使用指南：** 端口使能 dot1q-tunnel selective miss drop 后，对于没有进行灵活 qinq 的报文会被丢弃。对 untag 的报文无效。

**举例：** 端口 1/0/1 配置丢弃没有灵活 QINQ 的报文。

```
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# dot1q-tunnel selective enable
Switch(Config-If-Ethernet1/0/1)# dot1q-tunnel selective miss drop
Switch(Config-If-Ethernet1/0/1)# exit
Switch(config)#
```

## 3.15.6 show dot1q-tunnel

**命令：show dot1q-tunnel**

**功能：** 显示所有处于 dot1q-tunnel 状态的端口信息。

**参数：** 无。

**命令模式：** 特权和配置模式。

**使用指南：** 可使用该命令显示处于 dot1q-tunnel 状态的端口信息。

**举例：** 显示当前 dot1q-tunnel 的状态信息。

Switch#show dot1q-tunnel

Interface Ethernet1/1/1:

dot1q-tunnel is enable

Interface Ethernet1/1/3:

dot1q-tunnel is enable

# 3.16 VLAN-translation

## 3.16.1 vlan-translation

**命令：vlan-translation <old-vlan-id> to <new-vlan-id> {in | out}**

**no vlan-translation <old-vlan-id> {in | out}**

**功能：** 添加 VLAN translation 转换规则，使原 VLAN ID 与现 VLAN ID 产生一条映射；本命令的 no 命令为删除对应映射。

**参数：** old-vlan-id 为原 VLAN ID；new-vlan-id 为翻译后的 VLAN ID；in 为入口翻译；out 为出口翻译。

**命令模式：** 端口配置模式。

**缺省情况：** 缺省没有 VLAN translation 翻译关系。

**使用指南：** 本命令为设置 VLAN translation 的进出翻译关系。数据包将根据设置的翻译关系进行匹配，如果匹配成功，则将 VLAN ID 改变为设置条目中的 VLAN ID，如果匹配不成功，则由 vlan-translation miss drop 命令决定下一步的转发。在出口翻译，vlan-translation miss drop 没有设置 drop 的情况，如果报文匹配不成功，会 untag 出去。

**举例：** 在端口 1 将进入的 VLAN100 的数据经入口翻译后划入 VLAN2，并将流出的 VLAN2 的数据经出口翻译后划入 VLAN100。

Switch#config

Switch(config)#interface ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)#vlan-translation enable

Switch(Config-If-Ethernet1/1/1)#vlan-translation 100 to 2 in

Switch(Config-If-Ethernet1/1/1)#vlan-translation 2 to 100 out

Switch(Config-If-Ethernet1/1/1)#exit

Switch(config)#

## 3.16.2 vlan-translation enable

**命令：vlan-translation enable**

**no vlan-translation enable**

**功能：**开启端口的 vlan-translation 功能；本命令的 no 命令为恢复缺省值。

**参数：** 无。

**命令模式：** 端口配置模式。

**缺省情况：** 端口缺省为没有使能 VLAN translation 功能。

**使用指南：**此命令与 dot1q-tunnel enable 互斥

**举例：** 端口 1 上开启 VLAN translation 功能。

Switch#config

Switch(config)#interface ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)#vlan-translation enable

## 3.16.3 vlan-translation cvid

**命令：vlan-translation cvid < 1-4094> svid <1-4094> {pri < 0-7>}**

**no vlan-translation cvid < 1-4094> svid <1-4094>**

**功能：**同时添加双向的 VLAN 翻译规则，并修改报文的优先级。在 in 方向将 cvid 转换成 svid；在 out 方向将 svid 转换成 cvid。

**参数：**

<1-4094>：翻译后的 VLAN ID。

<0-7>：报文优先级。

**命令模式：** 端口配置模式。

**缺省情况：** 缺省没有翻译关系。

**使用指南：** 本命令为同时设置 in 和 out 方向的 VLAN 翻译关系。数据包将根据设置的翻译关系进行匹配，如果匹配成功，在 in 方向将原 VLAN 改变为设置条目中的 svid，并修改报文的优先级为配置的值；在 out 方向，将原 VLAN 改变为设置条目中的 cvid，并修改报文的优先级为配置的值；如果匹配不成功，则由 vlan-translation miss drop 命令决定下一步的转发。

**举例：** 在端口 1 将 in 方向 VLAN100 的数据经翻译后划入 VLAN200，将 out 方向 VLAN200 的数据经翻译后划入 VLAN100。

Switch#config

Switch(config)#interface ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)#vlan-translation enable

Switch(Config-If-Ethernet1/1/1)# vlan-translation cvid 100 svid 200

Switch(Config-If-Ethernet1/1/1)#exit

Switch(config)#

## 3.16.4 vlan-translation miss drop

**命令：vlan-translation miss drop {in|out|both}**

**no vlan-translation miss drop {in|out|both}**

**功能：**定义翻译失败时丢包；本命令的 no 命令为恢复缺省值。

**参数：**in 为入口；out 为出口；both 为双向。

**命令模式：**端口配置模式。

**缺省情况：**翻译失败不丢包。

**使用指南：**在进行原 VID 与现 VID 的映射关系翻译时，如时没有配置相应翻译关系，缺省为不丢包。当使用本命令后，翻译失败会丢掉 tag 报文，此命令对 untag 报文无效。

举例：设置端口 1 入口翻译失败丢包。

Switch(Config-If-Ethernet1/1/1)#vlan-translation miss drop in

## 3.16.5 show vlan-translation

**命令：show vlan-translation**

**功能：** 显示 vlan-translation 相关配置。

**参数：** 无。

**命令模式：** 特权用户配置模式。

**使用指南：** 显示交换机 vlan-translation 的相关配置

**举例：** 显示 vlan-translation 相关配置。

Switch# show vlan-translation

Interface Ethernet1/1/1:

vlan-translation is enable, miss drop is not set

vlan-translation 5 to 10 in

Interface Ethernet1/1/2:

vlan-translation is enable, miss drop is set both

vlan-translation 6 to 12 out

# 3.17 动态 vlan

## 3.17.1 dynamic-vlan mac-vlan prefer

**命令：dynamic-vlan mac-vlan prefer**

**功能：** 设置 MAC-based VLAN 优先。

**参数：** 无。

**命令模式：** 全局配置模式。

**缺省情况：** MAC-based VLAN 优先。

**使用指南：** 设置交换机动态 VLAN 的优先顺序。缺省优先顺序为 MAC-based VLAN、IP-subnet-based VLAN、Protocol-based VLAN，即多种动态 VLAN 在同时使用时优先匹配的顺序。在设置 IP-subnet-based VLAN 优先后，若恢复 MAC-based VLAN 优先时使用本命令。

**举例：** 设置 MAC-based VLAN 优先。

Switch#config

Switch(config)#dynamic-vlan mac-vlan prefer

## 3.17.2 dynamic-vlan subnet-vlan prefer

**命令：dynamic-vlan subnet-vlan prefer**

**功能：** 设置 IP-subnet-based VLAN 优先。

**参数：** 无。

**命令模式：** 全局配置模式。

**缺省情况：** MAC-based VLAN 优先。

**使用指南：** 设置交换机动态 VLAN 的优先顺序。缺省优先顺序为 MAC-based VLAN、IP-subnet-based VLAN、Protocol-based VLAN，即多种动态 VLAN 在同时使用时优先匹配的顺序。本命令为设置 IP-subnet-based VLAN 优先。

**举例：** 设置 IP-subnet-based VLAN 优先。

Switch#config

Switch(config)#dynamic-vlan subnet-vlan prefer

## 3.17.3 mac-vlan

**命令：mac-vlan mac <mac-addrss> <mac-mask> vlan <vlan-id> priority <priority-id>**
**no mac-vlan {mac <mac-addrss> <mac-mask>|all}**

**功能：**添加 MAC 地址与 VLAN 的对应关系，即指定 MAC 地址加入指定 VLAN；本命令的 no 命令为删除 MAC 地址与 VLAN 的对应关系。

**参数：**mac-address 为 MAC 地址，格式为 XX-XX-XX-XX-XX-XX，mac-mask 为 mac 地址掩码，格式为 XX-XX-XX-XX-XX-XX，vlan-id 为 VLAN 号，取值范围为 1~4094；priority-id 为优先级，用于 VLAN tag 中，取值范围 0~7；all 为所有 MAC 地址。

**命令模式：**全局配置模式。

**缺省情况：**没有 MAC 地址加入 VLAN。

**使用指南：**该命令将指定的MAC地址加入到指定VLAN中。若有指定的MAC地址的无VLAN标签数据包从交换机端口进入，它将匹配到指定的 VLAN 号，从而进入指定的 VLAN，不管该数据包从哪个端口进入，其所属 VLAN 是一致的。该命令设置后不对有 VLAN 标签的数据包进行干涉。

**举例：**将 MAC 地址为 00-03-0f-11-22-33 的网络设备划入 VLAN 100.

Switch#config

Switch(config)#mac-vlan mac 00-03-0f-11-22-33 ff-ff-ff-ff-ff-ff vlan 100 priority 0

## 3.17.4 mac-vlan vlan

**命令：mac-vlan vlan <*vlan-id*>**

**no mac-vlan vlan <*vlan-id*>**

**功能：**设置指定VLAN为MAC VLAN；本命令的no命令为取消该VLAN为MAC VLAN。

**参数：<*vlan-id*>**为指定的VLAN号。

**命令模式：**全局配置模式。

**缺省情况：**没有MAC VLAN。

**使用指南：**设置指定VLAN为MAC VLAN。

**举例：**将VLAN100设置为MAC VLAN。

switch#config

switch(config)#mac-vlan vlan 100

## 3.17.5 protocol-vlan

**命令：protocol-vlan etype <*etype-id*>| vlan <*vlan-id*> priority <*priority-id*>**

**no protocol-vlan *etype* <etype-id>**

**功能：** 添加协议与 VLAN 的对应关系，即指定协议加入指定 VLAN；本命令的 no 命令为删除协议与 VLAN 的对应关系。

**参数：** etype-id 为报文协议类型，取值范围为 1536~65535；vlan-id 为 VLAN 号，取值范围为 1~4094；priority 为优先级，取值范围为 0~7；**命令模式：** 全局配置模式。

**缺省情况：** 没有协议加入 VLAN。

**使用指南：** 该命令将指定的协议加入到指定 VLAN 中。若有指定的协议的无 VLAN 标签数据包从交换机端口进入，它将匹配到指定的 VLAN 号，从而进入指定的 VLAN，不管该数据包从哪个端口进入，其所属 VLAN 是一致的。该命令设置后不对有 VLAN 标签的数据包进行干涉。在配置 IP 协议时建议将 ARP 协议一并配置，否则某些应用会受到影响。

**举例：** 将 IP 协议数据包划入 VLAN 200。

Switch#config

Switch(config)#protocol-vlan etype 2048 vlan 200

## 3.17.6 show dynamic-vlan prefer

**命令：show dynamic-vlan prefer**

**功能：** 显示动态 VLAN 的优先顺序。

**参数：** 无。

**命令模式：** 特权和配置模式。

**使用指南：** 显示动态 VLAN 的优先顺序。

**举例：** 显示当前动态 VLAN 的优先顺序。

Switch#show dynamic-vlan prefer

Mac Vlan/Voice Vlan

IP Subnet Vlan

Protocol Vlan

## 3.17.7 show mac-vlan

**命令：show mac-vlan**

**功能：**显示交换机 MAC-based VLAN 的配置情况。

**参数：**无。

**命令模式：**特权和配置模式。

**使用指南：**显示交换机 MAC-based VLAN 的配置情况。

**举例：**显示当前 MAC-based VLAN 的配置情况。

Switch#show mac-vlan

| MAC-Address | VLAN_ID | Priority |
|---|---|---|
| 00-e0-4c-77-ab-9d | 2 | 2 |
| 00-0a-eb-26-8d-f3 | 2 | 2 |
| 00-03-0f-11-22-33 | 5 | 5 |

## 3.17.8 show mac-vlan interface

**命令：show mac-vlan interface**

**功能：**显示处于 MAC-based VLAN 的端口。

**参数：**无。

**命令模式：**特权和配置模式。

**使用指南：**显示使能了 MAC-based VLAN 的端口，端口后括号内标出了端口的属性，A 表示 Access 口，T 表示 Trunk 口，H 表示 Hybrid 口。

**举例：**显示当前使能了 MAC-based VLAN 的端口。

Switch#show mac-vlan interface

| | |
|---|---|
| Ethernet1/1/1(A) | Ethernet1/1/2(A) |
| Ethernet1/1/3(A) | Ethernet1/1/4(A) |
| Ethernet1/1/5(H) | Ethernet1/1/6(T) |

## 3.17.9 show protocol-vlan

**命令：show portocol-vlan**

**功能：**显示交换机 Protocol-based VLAN 的配置情况。

**参数：**无。

**命令模式：**特权和配置模式。

**使用指南：**显示交换机 Protocol-based VLAN 的配置情况。

**举例：**显示当前 Protocol-based VLAN 的配置情况。

```
switch(config)#show protocol-vlan
Protocol_Type                VLAN_ID          Priority
etype 0xfffd                  3                0
etype 0xffff                  1                0
etype 0x600                     1                  0
```

## 3.17.10 show subnet-vlan

**命令：show subnet-vlan**

**功能：** 显示交换机 IP-subnet-based VLAN 的配置情况。

**参数：** 无。

**命令模式：** 特权和配置模式。

**使用指南：** 显示交换机 IP-subnet-based VLAN 的配置情况。

**举例：** 显示当前 IP-subnet-based VLAN 的配置情况。

```
Switch#show subnet-vlan
IP-Address                Mask                VLAN_ID
------------------        -----------------     -------
192.168.1.165             255.255.255.0       2
202.200.121.21            255.255.0.0           2
10.0.0.1                  255.248.0.0           5
```

## 3.17.11 show subnet-vlan interface

**命令：show subnet-vlan interface**

**功能：** 显示处于 IP-subnet-based VLAN 的端口。

**参数：** 无。

**命令模式：** 特权和配置模式。

**使用指南：** 显示使能了 IP-subnet-based VLAN 的端口，端口后括号内标出了端口的属性，A 表示 Access 口，T 表示 Trunk 口，H 表示 Hybrid 口。

**举例：** 显示当前使能了 IP-subnet-based VLAN 的端口。

```
Switch#show subnet-vlan interface
Ethernet1/1/1(A)          Ethernet1/1/2(A)
Ethernet1/1/3(A)          Ethernet1/1/4(A)
Ethernet1/1/5(H)          Ethernet1/1/6(T)
```

## 3.17.12 subnet-vlan

**命令：subnet-vlan ip-address *<ipv4-addrss>* mask *<subnet-mask>* vlan *<vlan-id>* priority *<priority-id>***

**no subnet-vlan {ip-address *<ipv4-addrss>* mask *<subnet-mask>*|all}**

**功能：** 添加 IP 子网与 VLAN 的对应关系，即指定 IP 子网加入指定 VLAN；本命令的 no 命令为删除该/全部对应关系。

**参数：** ipv4-address 为 IPv4 地址，格式为点分十进制，每段取值范围 0~255；subnet-mask 为子网掩码，格式为点分十进制，每段取值范围 0~255；priority-id 为优先级，用于 VLAN tag 中，取值范围 0~7；vlan-id 为 VLAN 号，取值范围为 1~4094；all 为所有子网。

**命令模式：** 全局配置模式。

**缺省情况：** 没有 IP 子网加入 VLAN。

**使用指南：** 该命令将指定的 IP 子网加入到指定 VLAN 中。若有指定的 IP 子网的无 VLAN 标签数据包从交换机端口进入，它将匹配到指定的 VLAN 号，从而进入指定的 VLAN，不管该数据包从哪个端口进入，其所属 VLAN 是一致的。该命令设置后不对有 VLAN 标签的数据包进行干涉。

**举例：** 将 IP 子网为 192.168.1.0/24 的网络设备划入 VLAN 300。

```
Switch#config
Switch(config)#subnet-vlan ip-address 192.168.1.1 mask 255.255.255.0 vlan 300 priority 0
```

## 3.17.13 switchport mac-vlan enable

**命令：switchport mac-vlan enable**

**no switchport mac-vlan enable**

**功能：**打开端口的 MAC-based VLAN 功能；本命令的 no 命令为关闭端口的 MAC-based VLAN 功能。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**端口打开 MAC-based VLAN 功能。

**使用指南：**当添加 MAC 地址属于指定 VLAN 后，缺省全局使能 MAC-based VLAN 功能，此命令可将在指定端口上关闭 MAC-based VLAN 功能，以适应用户特定的应用。

**举例：**关闭端口 1 的 MAC-based VLAN 功能。

```
Switch#config
Switch(config)#interface ethernet 1/1/1
Switch(Config-If-Ethernet1/1/1)#no switchport mac-vlan enable
```

## 3.17.14 switchport subnet-vlan enable

**命令：switchport subnet-vlan enable**

**no switchport subnet-vlan enable**

**功能：** 打开端口的 IP-subnet-based VLAN 功能；本命令的 no 命令为关闭端口的 IP-subnet-based VLAN 功能。

**参数：** 无。

**命令模式：** 端口配置模式。

**缺省情况：** 端口打开 IP-subnet-based VLAN 功能。

**使用指南：** 当添加 IP 子网属于指定 VLAN 后，缺省全局使能 IP-subnet-based VLAN 功能，此命令可将在指定端口上关闭 IP-subnet-based VLAN 功能，以适应用户特定的应用。

**举例：** 关闭端口 1 的 IP-subnet-based VLAN 功能。

```
Switch#config
Switch(config)#interface ethernet 1/1/1
Switch(Config-If-Ethernet1/1/1)#no switchport subnet-vlan enable
```

# 3.18 Voice VLAN

## 3.18.1 show voice-vlan

**命令：show voice-vlan**

**功能：**显示交换机 Voice VLAN 的配置情况。

**参数：**无。

**命令模式：**特权和配置模式。

**使用指南：**显示交换机 Voice VLAN 的配置情况。

**举例：**显示当前 Voice VLAN 的配置情况。

```
switch#show voice-vlan
Voice VLAN ID:2
Ports:ethernet1/1/1;ethernet1/1/3
Voice name       MAC-Address                Mask       Priority
--------------   -----------------          -------    --------
financePhone        00-e0-4c-77-ab-9d          0xff            5
manager             00-0a-eb-26-8d-f3          0xfe            6
Mr_Lee           00-03-0f-11-22-33          0x80            5
NULL             00-03-0f-11-22-33          0x0             5
```

## 3.18.2 switchport voice-vlan enable

**命令：switchport voice-vlan enable**

**no switchport voice-vlan enable**

**功能：**打开端口的 Voice VLAN 功能；本命令的 no 命令为关闭端口的 Voice VLAN 功能。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**端口打开 Voice VLAN 功能。

**使用指南：**当添加语音设备到 Voice VLAN 后，缺省全局使能 Voice VLAN 功能，此命令可在指定端口上关闭 Voice VLAN 功能，以适应用户特定的应用。

**举例：**关闭端口 3 的 Voice VLAN 功能。

```
switch#config
switch(config)#interface ethernet 1/1/3
switch(Config-If-Ethernet1/1/3)#no switchport voice-vlan enable
```

## 3.18.3 voice-vlan

**命令：voice-vlan mac *<mac-address>* *<mac-address-mask>* priority *<priority-id>* [name *<voice-name>*]**

**no voice-vlan {mac *<mac-address>* *<mac-address-mask>*|name *<voice-name>* |all}**

**功能：**指定范围内的语音设备加入 Voice VLAN；本命令的 no 命令为设备离开 Voice VLAN。

**参数：**mac-address 为语音设备 MAC 地址，格式为 xx-xx-xx-xx-xx-xx； mac-address-mask 为 mac 地址掩码，格式为 XX-XX-XX-XX-XX-XX；priority-id 为语音流的优先级，取值范围 0~7；voice-name 为语音设备的名字，便于管理；all 为所有语音设备 MAC 地址。

**命令模式：**全局配置模式。

**缺省情况：**没有语音设备加入 Voice VLAN。

**使用指南：**该命令将指定范围内的语音设备加入到 Voice VLAN 中。若有指定范围内的语音设备的无 VLAN 标签数据包从交换机端口进入，不管该数据包从哪个端口进入，其均属于 Voice VLAN。该命令设置后不对有 VLAN 标签的数据包进行干涉。

**举例：**将研发部 MAC 地址为 00-03-0f-11-22-00 到 00-03-0f-11-22-ff 的 256 台语音设备加入 Voice VLAN。

```
switch#config
switch(config)#voice-vlan vlan 100
Switch(config)#voice-vlan mac 00-03-0f-11-22-33 FF-FF-FF-FF-FF-00 priority 5 name test
```

## 3.18.4 voice-vlan vlan

**命令：voice-vlan vlan *<vlan-id>***

**no voice-vlan**

**功能：**设置指定 VLAN 为 Voice VLAN；本命令的 no 命令为取消该 VLAN 为 Voice VLAN。

**参数：**vlan-id 为指定的 VLAN 号。

**命令模式：**全局配置模式。

**缺省情况：**没有 Voice VLAN。

**使用指南：**设置指定 VLAN 为 Voice VLAN，同一时刻只能有一个 Voice VLAN。Voice VLAN 与 MAC-based VLAN 不能同时使用。

**举例：**将 VLAN100 置为 Voice VLAN。

switch#config

switch(config)#voice-vlan vlan 100

# 3.19 Multi-to-One VLAN translation

## 3.19.1 vlan-translation n-to-1

**命令：vlan-translation n-to-1 <*WORD*> to <*new-vlan-id*>**

**no vlan-translation n-to-1 <*WORD*>**

**功能：**开启/关闭端口的 Multi-to-One VLAN translation 功能。

**参数：**WORD 为映射前的 VLAN ID，取值范围为 1-4094，用';'和'-'连接。如果在相同端口存在两个 VLAN 范围转化为不同的 VLAN ID，则要求这两个 VLAN 范围不能有重叠部分。

new-vlan-id 为映射后的 VLAN ID，取值范围为 1-4094。

**命令模式：**端口配置模式

**缺省情况：**端口默认没有开启该功能。

**使用指南：**Multi-to-One VLAN translation 功能应用在网络边缘层，用于将边缘网络的多个 VLAN 映射到主干网一个 VLAN，同时当数据流从主干网络返回网络边缘层时，会自动还原数据流边缘层的 VLAN 信息，达到多对一的 VLAN 映射效果，从而节省主干网络的 VLAN 资源。注意：使用该功能时，设备上必须先建立映射前与映射后的 VLAN，同时开启该功能的下联端口和连接骨干网的上联端口必须以 Tagged 的方式加入到映射前与映射后的 VLAN；该功能不能同时和 dot1q-tunnel，VLAN translation 功能同时使用。

**注意：**该功能要在开启 MAC 软件学习后使用。

交换机的 access 口不支持此功能。

**举例：**在端口 Ethernet 1/1/1 将 VLAN 范围为 1-5 的数据流转为 VLAN 100，并将从 VLAN 100 流出的属于 VLAN 范围 1-5 的数据流分别转换为自己对应的 VLAN ID；连接骨干网的上联端口为 Ethernet 1/1/5。

Switch(config)#vlan 1-5;100

Switch(config)#interface ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)#switchport mode trunk

Switch(Config-If-Ethernet1/1/1)#vlan-translation n-to-1 1-5 to 100

Switch(config)#interface ethernet 1/1/5

Switch(Config-If-Ethernet1/1/5)#switchport mode trunk

## 3.19.2 show vlan-translation n-to-1

**命令：show vlan-translation n-to-1 [<*interface-name*>]**

**功能：**显示开启该功能的端口配置。

**参数：**interface-name 指定要显示的端口名称，如不指定该参数，则显示所有开启该功能的端口信息。

**命令模式：**特权配置模式

**缺省情况：**缺省没有该功能信息。

**使用指南：把 GVRP 报文调试信息开关打开。**

**注意：交换机的 access 口不支持此功能。**

**举例：**显示开启该功能的所有端口信息。

Switch# show vlan-translation n-to-1

Interface Ethernet1/1/1:

vlan-translation n-to-1 enable, vlan 1-4 to 100

vlan-translation n-to-1 enable,vlan 5-8;13 to 101

Interface Ethernet1/1/2:

vlan-translation n-to-1 enable,vlan 1-4 to 100

# 3.20 Super VLAN

## 3.20.1 supervlan

**命令：supervlan**

**no supervlan**

**功能：**将 vlan 设置为 super vlan；本命令的 no 操作为恢复缺省情况。

**参数：**无。

**命令模式：**VLAN 配置模式。

**缺省情况：**不配置。

**使用指南：**将 VLAN 设置为 Super vlan，必须是普通 VLAN，此 VLAN 不能是 SUB VLAN，设置 truck 口时自动滤除 Super vlan，不能向 Super vlan 中加入端口。

**举例：**将 vlan 2 设置为 supervlan。

Swithc#config

Switch(config)#vlan 2

Switch (config-vlan2)#supervlan

## 3.20.2 subvlan

**命令：subvlan WORD**

**no subvlan {WORD | all}**

**功能：**将 vlan 设置为 subvlan；本命令的 no 操作为恢复缺省情况。

**参数：**WORD 为 VLAN ID，可以使用“-”和“；”表示更多的 VLAN。

all 表示所有 subvlan。

**命令模式：**VLAN 配置模式。

**缺省情况：**不配置。

**使用指南：**将 VLAN 设置为 Sub vlan，该 VLAN 必须已经存在，必须是普通 VLAN，此 VLAN 不能是其他 SUPER VLAN 的 SUB VLAN，也不能是 SUPER VLAN，每一个 Super VLAN 可以和 127 个 Sub VLAN 建立映射关系。系统最多允许建立 1024 个 Super VLAN。

**举例：**将 vlan 3 设置为 subvlan。

```
Swithc#config
Switch(config)#vlan 2-3
Switch(config)#vlan 2
Switch (config-vlan2)#supervlan
Switch (config-vlan2)#subvlan 3
```

## 3.20.3 arp-proxy subvlan

**命令：arp-proxy subvlan {WORD | all}**

**no arp-proxy subvlan {WORD | all}**

**功能：**使能 subvlan 的 arp proxy 功能，此 VLAN 收到的流量可以被代理到其他 subvlan；本命令的 no 操作为恢复缺省情况。

**参数：**WORD 为 VLAN ID，可以使用“-”和“；”表示更多的 VLAN。

all 表示所有 subvlan。

**命令模式：**接口配置模式。

**缺省情况：**不配置。

**使用指南：**此接口必须是 supervlan 的接口。此 VLAN 收到的流量可以被代理到其他 subvlan——当交换机从这个 VLAN 收到 ARP REQUEST 时，用自己的 MAC 回应 ARP REPLY，以便流量可以通过交换机软转发出去。

**举例：**开启 vlan2 的所有 subvlan 的 arp-proxy 功能。

```
Swithc#config
Switch(config)#interface vlan 2
Switch (config-if-vlan2)#arp-proxy subvlan all
```

## 3.20.4 arp-check-range subvlan

本型号交换机不支持此命令

## 3.20.5 ip-addr-range

**命令：ip-addr-range <*ipv4-addrss*> to <ipv4-addrss>**

**no ip-addr-range**

**功能：**为某个接口指定地址范围，交换机收到流量后，发送 ARP REQUEST 时需要检查数据包的目的 IP 地址是否在地址范围内，如果不在，不发送 ARP REQUEST；本命令的 no 操作为恢复缺省情况。

**参数：** <*ipv4-addrss*>表示 IPv4 地址，格式为点分十进制，每段取值范围 0~255。

**命令模式：**接口配置模式。

**缺省情况：**无地址范围。

**使用指南：**交换机从配置了地址范围的接口收到流量后，发送 ARP REQUEST 时需要检查数据包的目的 IP 地址是否在地址范围内，如果不在，不发送 ARP REQUEST；如果这个接口是 SUPER VLAN 的接口，从这个接口收到的 ARP REQUEST，所请求的 IP 地址不在地址范围内，则不代理这个 ARP REQUEST。

**举例：**设置 interface vlan 2 的地址范围。

```
Swithc#config
Switch(config)#interface vlan 2
Switch (config-if-vlan2)#ip-addr-range 1.1.1.1 to 1.1.1.10
```

## 3.20.6 show supervlan

**命令：show supervlan [<*vlan-id*>]**

**功能：**显示系统的 super vlan。

**参数：**<*vlan-id*>为 VLAN ID，范围 1-4094。

**命令模式：**特权和配置模式。

**使用指南：**如果不指定 VLAN ID，则显示所有的 supervlan 信息。

**举例：**显示当前 supervlan 信息。

```
Swithc#show supervlan
VLAN Name            Type          sub VLAN    Ports
---- ------------ ---------- --------- -------------------------------------
2    VLAN0002       Universal     3         Ethernet1/1/2
                                          4         Ethernet1/1/3
```

# 3.21 MAC 地址表

## 3.21.1 mac-address-table avoid-collision

本型号交换机不支持此命令。

## 3.21.2 clear collision-mac-address-table

**命令：clear collision-mac-address-table**

**功能：**清空 hash 冲突表。

**参数：**无

**命令模式：**特权用户配置模式。

**使用指南：**如果使能了 hash 冲突 mac 下发 ffp 表项功能（mac-address-table avoid-collision），已经下发 ffp 的冲突 mac 将不能清除。

**举例：**清空 hash 冲突 mac 表。

Switch#clear collision-mac-address-table

## 3.21.3 clear mac-address-table dynamic

**命令：clear mac-address-table dynamic [address *<mac-addr>*] [vlan *<vlan-id>*] [interface [ethernet | portchannel] *<interface-name>*]**

**功能：**删除动态地址表项。

**参数：** ***<mac-addr>*** 要删除的 MAC 地址；***<interface-name>*** 转发 MAC 数据包的端口名称；***<vlan-id>*** 为 VLAN 号。

**命令模式：**特权用户配置模式。

**使用指南：**删除交换机 MAC 地址表中存在的所有 DYNAMIC 地址表项，而不能删除 APPLICATION、SYSTEM 类型表项。MAC 地址表项根据来源不同可以分为几类：DYNAMIC、STATIC、APPLICATION、SYSTEM。DYNAMIC 类型是交换机自动学习到的动态 MAC 地址表项，能够被交换机自动老化。

**举例：**删除所有动态 MAC。

Switch#clear mac-address-table dynamic

## 3.21.4 mac-address-learning cpu-control

本型号交换机不支持此命令。

## 3.21.5 mac-address-table aging-time

**命令：mac-address-table aging-time *<0 | aging-time>***

**no mac-address-table aging-time**

**功能：**设置 mac 地址表的老化时间。

**参数：0** 表示动态表项不老化，***<aging-time>***是要设置的老化时间，取值范围<10-1000000>，单位是秒。

**命令模式：**全局配置模式。

**缺省情况：**缺省的老化时间为 300 秒。

**使用指南：**当地址表项在老化时间内没有被命中，该表项将会老化。老化时间要根据具体的网络运行情况来设置，一般采用缺省值即可。

**举例：**设置老化时间为 600 秒。

Switch(config)# mac-address-table aging-time 600

## 3.21.6 mac-address-table bucket size

本型号交换机不支持此命令。

## 3.21.7 mac-address-table hash

**命令：mac-address-table hash <algo0 | algo1>**

**功能：**修改 mac 地址的 hash 算法，来提高设备的随机 mac 的学习能力。

**参数：** algo0 适用的是连续 source MAC address 的递增情形，可以学满 32k，而不会遇到 MAC collision 的问题；Hash algo1 针对一般应用会比较合适，但是如果是要验证连续 source MAC address 的递增情形 ，就有可能会遇到 MAC collision 的现象，无法学满 32K.

**命令模式：**全局配置模式。

**缺省情况：**默认 algo0。

**使用指南：**当地址表项在老化时间内没有被命中，该表项将会老化。老化时间要根据具体的网络运行情况来设置，一般采用缺省值即可。

**举例：**设置 mac 地址的 hash 算法为 algo0。

Switch(config)# mac-address-table hash algo0

## 3.21.8 mac-address-table static | static-multicast | blackhole

**命令：mac-address-table {static | static-multicast | blackhole} address <*mac-addr*> vlan <*vlan-id*> [interface [ethernet | portchannel] <*interface-name*>] | [source|destination|both|]**

**no mac-address-table {static | *static-multicast* | blackhole | dynamic} *[address* <mac-addr>] *[vlan* <vlan-id>] *[interface [*ethernet | portchannel] <*interface-name*>]**

**功能：** 添加或修改静态地址表项、静态组播 MAC 地址、过滤地址表项，此命令的 no 操作为删除静态地址表项、静态组播 MAC 地址、过滤地址表项。

**参数：** static 静态表项；static-multicast 静态组播表项；blackhole 过滤表项，配置过滤表项的目的是丢弃指定 MAC 地址的帧，用于过滤不想让其通过的流量，可以选择过滤源地址、目标地址或同时过滤，可以过滤源地址和目标地址，当选择过滤表项时，blackhole 地址不能基于端口，不对 interface 进行配置；dynamic 动态地址表项；<mac-addr> 要添加或删

除的 MAC 地址；<interface-name> 转发 MAC 数据包的端口名称；<vlan-id> 为 VLAN 号；source 表示基于源地址过滤；destination 表示基于目的地址过滤；both 表示基于源地址和目的地址过滤，默认是 both 选项。

**命令模式：**全局配置模式。

**缺省情况：**当配置 VLAN 接口并且该 VLAN 接口 UP 后，系统会生成一个系统固有 MAC 地址与该 VLAN 号对应的静态地址映射表项。

**使用指南：**在某些特殊用途或者交换机不能动态的学习到 MAC 地址，用户可以使用本命令将 MAC 地址与端口及 VLAN 手工建立映射关系。

命令 **no mac-address-table** 为删除 MAC 地址表项时，可以删除交换机 MAC 地址表中存在的所有 DYNAMIC、STATIC、过滤 MAC 地址表项，而不能删除 APPLICATION、SYSTEM 类型表项。MAC 地址表项根据来源不同可以分为几类：DYNAMIC、STATIC、APPLICATION、SYSTEM。DYNAMIC 类型是交换机自动学习到的动态 MAC 地址表项，能够被交换机自动老化；STATIC 类型是用户添加的静态 MAC 地址表项（包括 blackhole 类型表项）；APPLICATION 类型是交换机上层应用协议（如 dot1x、security port...）添加的静态 MAC 地址表项；SYSTEM 类型是交换机根据 VLAN 接口状态而添加的静态 MAC 地址表项。添加 STATIC 类型表项时，可以覆盖冲突的 DYNAMIC 类型表项，而不能覆盖冲突的 APPLICATION、SYSTEM 类型表项。

本命令可以用来配置静态组播 MAC，配置静态组播 MAC 后，当交换机收到该组播 MAC 的流量后会转发到指定 VLAN 的指定端口。

**举例：** 端口 1/1/1 属于 VLAN200，与 MAC 地址为 00-03-0f-f0-00-18 建立地址映射。

Switch(config)#mac-address-table static address 00-03-0f-f0-00-18 vlan 200 interface ethernet 1/1/1

配置一条静态组播 MAC 01-00-5e-00-00-01，出口为 1/1/1。

Switch(config)#mac-address-table static-multicast address 01-00-5e-00-00-01 vlan 1 interface ethernet1/1/1

## 3.21.9 l2-address-table static-multicast address

本型号交换机不支持此命令。

## 3.21.10 show collision-mac-address-table

**命令：show collision-mac-address-table**

**功能：**打印 hash 冲突 mac 表。

**参数：**无

**命令模式：**全局配置模式。

**使用指南：**如果使能了 hash 冲突 mac 下发 ffp 表项功能（mac-address-table avoid-collision），已经下发 ffp 的冲突 mac 地址前以*标记。

**举例：**打印 hash 冲突 mac 表。

Switch(Config)#show collision-mac-address-table

The max number can be recorded is 200

The max number of collision is 0

The current number recorded is 0

MAC Address VLAN Collision-count

## 3.21.11 show mac-address-table

**命令：show mac-address-table [static | blackhole | multicast | aging-time <*aging-time*> | count] [address <*mac-addr*>] [vlan <*vlan-id*>] [count] [interface <*interface-name*>]**

**功能：** 显示交换机当前的 MAC 地址表的内容。

**参数：** static 静态表项；blackhole 过滤表项；aging-time <aging-time>MAC 地址老化时间；multicast 组播表项；count 显示表项的条目总数；<mac-addr> 要显示的表项包含的 MAC 地址；<vlan-id> 要显示的表项包含的 VLAN 号；<interface-name> 要显示的表项包含的端口名称。

**命令模式：**特权和配置模式。

**缺省情况：**系统缺省不显示 MAC 地址表的内容。

**使用指南：**本命令可以分类显示各种 MAC 地址表项，也可以使用命令 **show mac-address-table** 显示当前交换机内所有的 MAC 地址表项。

**举例：**显示当前 MAC 地址表中的过滤表项。

Switch#show mac-address-table blackhole

## 3.21.12 Show l2-address-table multicast

本型号交换机不支持此命令。

# 3.22 Rmon

## 3.22.1 rmon enable

**命令：rmon enable**

**no rmon enable**

**功能：**打开 RMON；本命令的 no 操作为关闭 RMON。

**命令模式：**全局配置模式

**缺省情况：**开启 snmp-server enable 系统默认开启 RMON。

**使用指南：**无

**举例：**启动RMON

Switch(config)# rmon enable

## 3.22.2 rmon statistic

**命令：rmon statistics *<1-65535>* (ethernet *IFNAME|IFNAME)* (owner *WORD|*)**

**no rmon statistics *<1-65535>***

**功能：**当希望系统持续统计当前接口的使用情况时，通过 rmon statistics 命令配置统计表，为统计表添加一个表项后即可实现 RMON 以太网统计功能。该功能可以设置对监视以太网接口的使用及进行错误统计。统计信息包括冲突、循环冗余校验和错误数、太小或超大包、广播、多播、单播消息等。本命令的 no 操作为删除 RMON 统计表。

**参数：*<1-65535>*** ：统计表索引号。

***IFNAME*** ：以太网接口名称。

***WORD*** ：创建者名称，长度1-255。

**命令模式：**全局配置模式

**缺省情况：**缺省不配置

**使用指南：**无

**举例：**配置接口1/1/12的RMON统计组

Switch(config)# rmon statistics 3 ethernet 1/1/12

## 3.22.3 rmon history

**命令：rmon history *<1-65535>* (ethernet *IFNAME|IFNAME)* (buckets *<1-100>|*)**

**(interval *<5-3600>|*) (owner *WORD|*)**

**no rmon history *<1-65535>***

**功能：**如果希望系统定期对指定接口进行数据采集并保存以备后续查看，可以通过rmon

history命令配置历史控制表，为历史控制表添加一个表项后即可实现RMON历史统计功能。配置该功能后，系统将按周期定时的对接口的各种流量信息进行统计，统计数据包括带宽利用率、错误包数和总包数等。本命令的 no 操作为删除RMON历史表。

**参数：*<1-65535>***：历史表索引号。

***IFNAME*** ：以太网接口名称。

***<1-100>*** ：该历史控制表项对应的历史表容量，取值范围为1～100，默认为50。

***<5-3600>***：统计时间间隔，取值范围为5～3600，单位为秒，默认值为1800。

***WORD*** ：创建者名称，长度1-255。

**命令模式：**全局配置模式

**缺省情况：**缺省不配置

**使用指南：**可保存的统计值个数由buckets number参数决定，当历史表的容量达到最大值时，系统会删除最早的记录来保存新的统计值。统计信息包括接口一个采样周期内收到的报文总数、广播报文总数和组播报文总数等，可以使用show rmon history命令来查看历史采样结果。

**举例：**配置接口1/1/22的RMON历史组

Switch(config)#rmon history 100 ethernet 1/1/22

## 3.22.4 rmon event

**命令：rmon event *<1-65535>* (description *NAME*|) type (*log* | *trap WORD* | *log-trap WORD* | *none*) (owner *WORD*|)**

**no rmon event *<1-65535>***

**功能：**RMON 的事件管理定义事件索引号及事件的处理方式包括：记录日志并生成告警信息发送给设备的 SNMP 模块或者选择其中一种方式或者不做任何事件处理。这样系统就可以对告警表中定义的告警事件进行相应的处理。本命令的 no 操作为删除 RMON 事件表。

**参数：*<1-65535>***：事件表实例索引号

***NAME***：事件的描述信息，长度0～127。

***log***：日志事件。当该事件被触发时，系统会记录日志。

***trap WORD***：trap告警事件。当该事件被触发时，生成告警信息，生成的告警信息将发送到设备的SNMP模块。通过设置SNMP中告警信息的发送参数，来决定告警信息输出的相关属性。WORD表示RMON生成的告警信息中携带的团体名，长度0～127。

***log-trap WORD***：日志和告警事件。当该事件被触发时，系统会同时记录日志和生成告警信息，生成的告警信息将发送到设备的SNMP模块。通过设置SNMP中告警信息的发送参数，来决定告警信息输出的相关属性。WORD表示RMON生成的告警信息中携带的团体名，长度0～127。

***none***：不产生动作的事件。当该事件被触发时，系统不做处理。

***WORD***：创建者名称，长度1-255。

**命令模式：**全局配置模式

**缺省情况：**缺省不配置

**使用指南：**用户配置指定事件的处理方式后，需要通过 rmon alarm 命令配置告警对象。否则，不会有告警触发此事件。可以通过 show rmon event 来查看当前配置的事件表属性，

通过 show rmon event log 来查看对应 alarm 产生的事件 log。trap 功能需要配合命令 snmp-server trap-source，snmp-server host，snmp-server enable traps 才能生效。

**举例：**配置RMON事件组告警类型为log

Switch(config)# rmon event 2 description aaa type log

## 3.22.5 rmon alarm

**命令：rmon alarm *<1-65535>* *OID* interval *<5-3600>* (*absolute*|*delta*) rising-threshold *WORD* *<1-65535>* falling-threshold *WORD* *<1-65535>* startup-alarm (*rising*|*falling*|*risingorfalling*) (owner *NAME*|)**

**no rmon alarm *<1-65535>***

**功能：**本命令用来设置告警项，以便在出现异常时触发告警事件，再由告警事件来定义具体的处理方式。用户定义了告警表项后，系统会按照定义的时间周期去获取被监视的告警变量的值，并将该值和设定的阈值进行比较，去执行相应的处理过程。本命令的 no 操作为删除RMON告警表。

**参数：*<1-65535>*：**告警表实例索引号

***OID*：**指定告警节点OID

**interval *<5-3600>*：**采样间隔时间，取值范围为5～3600，单位为秒。

***absolute*：**采样类型为绝对值采样，即采样时间到达时直接提取变量的值。

***delta*：**采样类型为变化值采样，即采样时间到达时提取的是变量在采样间隔内的变化值。

**rising-threshold *WORD* *<1-65535>*：***WORD*为上限阈值，范围为-2147483648～2147483647；*<1-65535>*表示上限阈值相应的事件索引号，取值范围为1～65535。

**falling-threshold *WORD* *<1-65535>*：***WORD*为下限阈值，范围为-2147483648～2147483647；*<1-65535>*表示上限阈值相应的事件索引号，取值范围为1～65535。

***rising*：**表示初次采样时，如果超出上限阈值，触发的告警类型。

***falling*：**表示初次采样时，如果低于下限阈值，触发的告警类型。

***risingorfalling*：**如果超出上限阈值或低于下限阈值，触发的告警类型。

***NAME*：**创建者名称，长度1-255。

**命令模式：**全局配置模式

**缺省情况：**缺省不配置

**使用指南：**当采样值大于等于设定的上限rising-threshold *WORD*，触发事件表中定义的事件rising-threshold event；采样值小于等于设定的下限falling-threshold *WORD*，触发事件表中定义的事件falling-threshold event。在生成告警事件之前，需要通过rmon event命令定义好告警表项中引用的事件。如果不配置，rmon alarm 命令可以下发，但是不产生log/trap事件。

**举例：**配置每间隔2000秒，监控接口1/1/1上限阈值为500，下限阈值为300的报文接收速率

Switch(config)# rmon alarm 333 1.3.6.1.4.1.6339.100.3.2.1.26.1 interval 2000 delta rising-threshold 500 111 falling-threshold 300 222 startup-alarm rising

## 3.22.6 show rmon statistic

**命令：show rmon statistics (ethernet *IFNAME*|)**

**功能：**使用该命令可以查看 RMON 的统计表采样信息，包括冲突、循环冗余校验和错误数、太小或超大包、广播、多播、单播消息等。

**参数：*IFNAME*：** 以太网接口名称

**缺省情况：**缺省不配置

**命令模式：**特权模式和全局配置模式。

**使用指南：**指定接口显示指定以太网接口的 RMON 以太网信息。如果不使用该参数，则显示所有 RMON 统计组的以太网信息。

**举例：**

```
Switch(config)# snmp-server enable
Switch(config)# rmon statistics 1 Ethernet1/1/1
Switch(config)# show rmon statistics
Statistics entry 1 owner is Invalid.
  Interface : Ethernet1/1/1(index is 1,oid is 1.3.6.1.2.1.2.2.1.1.1)
  7802 packets received, 1610539 octets, 0 packets dorp
  Input packets type statistics:
  broadcast packets      :1284        ,multicast packets :6518
  undersize packets      :0           ,oversize packets   :0
  fragments packets      :0           ,jabbers packets    :0
  CRC alignment errors :0             ,collisions         :0
  Input packets length statistics:
  (64)          packets    :289       ,(65~127)    packets:683
  (128~255)   packets    :6805        ,(256~511)   packets:0
  (512~1023) packets     :0           ,(1024~1518)packets:25
```

## 3.22.7 show rmon history

**命令：show rmon history (ethernet *IFNAME*|)**

**功能：**使用该命令可以查看 RMON 的历史表配置信息以及间隔时间段内历史表的采样信息

**参数：*IFNAME*：** 以太网接口名称

**缺省情况：**缺省不配置

**命令模式：**特权模式和全局配置模式。

**使用指南：**指定接口显示指定以太网接口的 RMON 历史采样信息。如果不使用该参数，则显示所有 RMON 历史组的采样信息。

**举例：**

```
Switch(config)# snmp-server enable
Switch(config)# rmon history 1 ethernet 1/1/1 buckets 100 interval 5 owner aa
Switch(config)# show rmon history
History control entry 1 owner is aa.
  Interface          : Ethernet1/1/1(index is 1,oid is 1.3.6.1.2.1.2.2.1.1.1)
```

```
  Interval timer    : 5
  Buckets numbers : 100

 History statistics entry index 1 input packets:
 Start time :(12600)00:02:06.00
 recived packets          :5797        ,recived Octets       :371008
 broadcast packets        :0           ,multicast packets :0
 undersize packets        :0           ,oversize packets    :0
 fragments packets        :0           ,jabbers packets     :0
 CRC alignment errors :0               ,collisions          :0
 drop packets             :0           ,utilization         :7
```

## 3.22.8 show rmon event

**命令：show rmon event (<*1-65535*>|)**

**功能：**使用该命令可以查看 RMON 事件组的配置信息

**参数：*<1-65535>*：**事件表索引号

**缺省情况：**缺省不配置

**命令模式：**特权模式和全局配置模式。

**使用指南：**指定索引号显示指定事件表行索引号的 RMON 事件组配置信息。如果不指定索引号，则显示所有 RMON 事件组的配置信息。

**举例：**

```
Switch(config)#rmon event 3 description aaa type log-trap bb owner cc
Switch(config)# show rmon event
History control entry 3 owner is cc.
  eventDescription :aaa
  eventType :log && trop
  eventCommunity :bb
```

## 3.22.9 show rmon event-log

**命令：show rmon event-log (<*1-65535*>|) (event <*1-65535*> |)**

**功能：**使用该命令可以查看 RMON 告警组触发生成的日志信息

**参数：event-log *<1-65535>*：**事件日志表索引号

**event *<1-65535>*：**事件表索引号

**缺省情况：**缺省不配置

**命令模式：**特权模式和全局配置模式。

**使用指南：**配置日志表索引显示指定 RMON 事件组日志表的行索引号的日志信息。如果不指定索引号，则显示所有 RMON 事件的日志信息。指定事件表索引号显示当前 RMON 事件组产生的所有日志信息。

**举例：**

```
Switch(config)# show rmon event-log
logIndex 2 in event 1
(33500)00:05:35.00 The 1.3.6.1.4.1.6339.100.3.2.1.26.1 defined in alarm table 1.alarm
sample type is absolute.
log message : : alarm rising event : value = 800, RisingThreshold = 100
```

## 3.22.10 show rmon alarm

**命令：show rmon alarm (<*1-65535*>|)**

**功能：**使用该命令可以查看 RMON 告警组的配置信息

**参数：*<1-65535>*：**告警表索引号

**缺省情况：**缺省不配置

**命令模式：**特权模式和全局配置模式。

**使用指南：**配置索引号显示指定 RMON 告警组的表项索引号的配置信息。如果不指定索引号，则显示所有 RMON 告警组的配置信息。

**举例：**

```
Switch(config)# rmon alarm 1 1.3.6.1.4.1.6339.100.3.2.1.26.1 interval 5 absolute
rising-threshold 100 1 falling-threshold 50 2 startup-alarm risingorfalling
Switch(config)# show rmon alarm 1
event index is 1,owner is Invalid
  Interval timer      :5
  Variable            :1.3.6.1.4.1.6339.100.3.2.1.26.1
  SampleType          :absolute
  Startup Alarm       :risingorfalling
  Rising Threshold    :100
  Rising EventIndex :1
  Falling Threshold :50
  Falling EventIndex:2
```

# 3.23 MAC Notification

## 3.23.1 snmp-server enable traps mac-notification

**命令：snmp-server enable traps mac-notification**

**no snmp-server enable traps mac-notification**

**功能：**全局配置打开 MAC 地址 trap 通知；no 命令全局关闭 MAC 地址 trap 通知。

**参数：**无。

**缺省情况：**全局关闭 MAC 地址 trap 通知。

**命令模式：**全局配置模式。

**使用指南：**该命令和 MAC 地址通知开关一起使用，该开关关闭的情况下，其余配置可见，但是功能失效。

**举例：**在交换机上打开 MAC 地址 trap 通知。

Switch(Config)#snmp-server enable traps mac-notification

## 3.23.2 mac-address-table notification

**命令：mac-address-table notification**

**no mac-address-table notification**

**功能：**全局配置打开 MAC 地址通知；no 命令全局关闭 MAC 地址通知。

**参数：**无。

**缺省情况：**全局关闭 MAC 地址通知。

**命令模式：**全局配置模式。

**使用指南：**该命令和 snmp 部分 trap 开关一起使用，该开关关闭的情况下，其余配置可见，但是功能失效。

**举例：**在交换机上打开 MAC 地址通知。

Switch(Config)#mac-address-table notification

## 3.23.3 mac-address-table notification interval

**命令：mac-address-table notification interval <0-86400>**

**no mac-address-table notification interval**

**功能：**配置发送 MAC 地址通知的时间间隔；no 命令恢复该时间间隔为默认值。

**参数：**interval :发送通知的时间间隔，单位为：秒；范围：0-86400。

**缺省情况：**MAC 地址通知的时间间隔为默认值 30s

**命令模式：**全局配置模式。

**使用指南：**该命令在全局开关关闭后可以继续配置。

**举例：**将交换机发送 MAC 地址通知的时间间隔改为 30s。

Switch(Config)#mac-address-table notification interval 30

## 3.23.4 mac-address-table notification history-size

**命令：mac-address-table notification history-size <0-500>**

**no mac-address-table notification history-size**

**功能：**配置存储 MAC 变化消息的最大条数。

**参数：**history-size:发送通知的数据长度，范围：0-500。

**缺省情况：**MAC 变化消息的最大条数为默认值 10

**命令模式：**全局配置模式。

**使用指南：**该命令在全局开关关闭后可以继续配置。

**举例：**将交换机发送 MAC 变化消息的最大条数改为 256。

Switch(Config)#mac-address-table notification history-size 256

## 3.23.5 mac-notification

**命令：mac-notification {added | all | moved | removed}**

**no mac-notification**

**功能：**配置指定端口 MAC 地址通知功能；no 命令取消该端口 MAC 地址通知功能。

**参数：**added：添加的 MAC 地址；

all：添加和删除的 MAC 地址

moved：移动的 MAC 地址；

removed：删除的 MAC 地址。

**缺省情况：**缺省端口不做 MAC 地址通知功能。

**命令模式：**端口配置模式。

**使用指南：**该命令在全局开关关闭后可以继续配置。

**举例：**将交换机的端口 ethernet 1/1/5 配置对添加的 MAC 地址进行通知。

Switch(Config)#in ethernet 1/1/5

Switch(Config-if-ethernet 1/1/5)#mac-notification added

## 3.23.6 show mac-notification summary

**命令：show mac-notification summary**

**功能：**显示 MAC 通知的配置情况和通知报文数据。

**参数：**无。

**缺省情况：**缺省情况下不显示。

**命令模式：**特权模式。

**使用指南：**可以通过该命令查看 MAC 地址的操作情况和 MAC 通知 trap 的发送情况。

**举例：**

Switch#show mac-notification summary

MAC address notification:enabled

MAC address snmp traps:enabled

MAC address notification interval = 10

MAC address notification history log size = 120

MAC address added = 0

MAC address removed = 0

MAC address snmp traps generated = 0

## 3.23.7 clear mac-notification statistics

**命令：clear mac-notification statistics**

**功能：**清除 MAC 操作和 MAC 通知 trap 的计数值。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**该命令和 show 命令一起使用，执行该命令后可以通过 show 命令查看该命令执行的结果。

**举例：**

Switch# clear mac-notification statistics

# 第 4 章 IP 业务命令

## 4.1 三层接口

### 4.1.1 Bandwidth

**命令：bandwidth <bandwidth>**

**no bandwidth**

**功能：**配置 interface vlan 的带宽。本命令的 no 命令为恢复 interface vlan 的带宽值为默认值。

interface vlan 接口下面的 bandwidth 不会实际控制端口的带宽，而是用于协议计算。例如，OSPF 计算链路的 cost 时，使用的就是接口的 bandwidth（cost=10^8/bandwidth），因此改变 bandwidth 会导致 OSPF 链路 cost 的改变。

**参数：<*bandwidth*>**：interface vlan 带宽值。范围<1-10000000000 bits>。可取的单位有 k，m，g。该值转化 bit 后不能有小数。

**命令模式：**VLAN 接口配置模式。

**缺省情况：**interface vlan 默认带宽值为 100,000,000bit。

**使用指南：**该命令只能应用于 interface vlan 接口。本命令单位换算关系：1g=1,000m=1,000,000k=1,000,000,000bit。

**举例：**配置 vlan 1 的带宽值为 50,000,000bit。

Switch(Config-if-Vlan1)#bandwidth 50m

### 4.1.2 description

**命令：description <text>**

**no description**

**功能：** 配置 VLAN 接口的描述信息；其 no 形式取消该 VLAN 接口的描述信息。

**参数：** <*text*>为 VLAN 接口的描述信息，它的长度不超过 256 的字符串。

**命令模式：** VLAN 接口配置模式

**缺省情况：** 默认不配置。

**使用指南：** description 后面为用户对 VLAN 接口的描述信息，会显示在所配置的 VLAN 下。

**举例：** 配置 VLAN 接口的描述信息为 test vlan。

Switch(config)#interface vlan 2

Switch(config-if-vlan2)#description test vlan

### 4.1.3 description（VRF 配置模式）

**命令：description <text>**

**no description**

**功能：**配置 VRF 的描述信息，可用来记录 VPN 实例与某个 VPN 的关系等信息；其 no 形式取消该 VPN 的描述信息。

**参数：<*text*>**：描述性文本，1-256 个字符。

**缺省情况：**默认不配置。

**命令模式：**VRF 配置模式。

**使用指南：**description 后面为用户对 VRF 的描述信息。会显示在所配置的 VRF 下，以提供相关的指示信息。

**举例：**配置 VRF 的描述信息为'associate with VRF-B VRF-C'

Switch(config)#ip vrf VRF-A

Switch(config-vrf)#description associate with VRF-B VRF-C

## 4.1.4 interface vlan

**命令：interface vlan <vlan-id>**

**no interface vlan <vlan-id>**

**功能：**创建一个 VLAN 接口，即创建一个交换机的三层接口；本命令的 no 操作为删除交换机指定的三层接口。

**参数：<*vlan-id*>** 是已建立的 VLAN 的 VLAN ID，取值范围 1～4094。

**缺省情况：**出厂时没有三层接口。

**命令模式：**全局配置模式。

**使用指南：**在创建 VLAN 接口（三层接口）前，需要先配置 VLAN。使用本命令在创建 VLAN 接口（三层接口）的同时，进入 VLAN 接口（三层接口）配置模式。在 VLAN 接口（三层接口）创建好之后，仍旧可以使用 interface vlan 命令进入三层接口模式。使用命令 **exit** 可以从 VLAN 接口配置模式退回到全局配置模式。

**举例：**在 VLAN 1 上创建一个 VLAN 接口（三层接口）。

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#

## 4.1.5 mac-address

**命令：mac-address <*mac-addr*>**

**no mac-address <*mac-addr*>**

**功能：**在三层接口下配置 mac 地址；本命令的 no 操作为删除三层接口下的 mac 地址。

**参数：**<mac-addr> 是要添加或删除的 MAC 地址。

**缺省情况：**出厂时三层接口没有 mac 地址。

**命令模式：**全局配置模式。

**使用指南：**在创建 VLAN 接口（三层接口）后，可以在三层接口下配置 mac 地址

**举例：**在 VLAN 接口（三层接口）下配置 mac 地址。

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)# mac-address 00-11-22-33-44-55

## 4.1.6 interface loopback

**命令：interface loopback <loopback -id>**

**no interface loopback <loopback -id>**

**功能：** 创建一个 Loopback 接口；本命令的 no 操作为删除指定的 Loopback 接口。

**参数：** ***<loopback-id>*** 是已建立的 Loopback 的 ID。

**缺省情况：** 出厂时没有 Loopback 接口。

**命令模式：** 全局配置模式。

**使用指南：** 配置的 Loopback 接口其实占用了 ID 从 1006 开始的 VLAN。若 Loopback 占用了 VLAN 1006 以后(包括 VLAN 1006)的某个 VLAN，则不能再配置对应的 VLAN；若原先已配置某 VLAN 1006 后的某个 VLAN，比如 VLAN 1006，则配置的 Loopback 接口占用其后第一个未被占用的 VLAN，比如 VLAN 1007。

**举例：** 进入 Loopback 1 接口配置模式。

Switch(config)#interface loopback 1

Switch(Config-if-Loopback1)#

## 4.1.7 ip vrf

**命令：ip vrf <vrf-name>**

**no ip vrf <vrf-name>**

**功能：** 配置相应名称的 VPN 实例；其 no 形式取消该 VPN 实例。

**参数：** ***<vrf-name>***：配置的 VPN 实例名称，取值长度范围 1～64。

**缺省情况：** 默认不配置。

**命令模式：** 全局配置模式。

**使用指南：** 配置相应名称的 VPN 实例。PE 上没有缺省的 VPN 实例，一个 PE 上可以创建多个 VPN 实例。VPN 实例的名字区分大小写。需要注意：VPN 实例只有配置了 RD 后才生效。

**举例：**

Switch(config)#ip vrf VRF-A

Switch(config-vrf)#

## 4.1.8 ip vrf forwarding vrfName

**命令：ip vrf forwarding <vrfName>**

**no ip vrf forwarding <vrfName>**

**功能：** 关联接口到指定 VRF。

**参数：** ***<vrfName>*** 为 VRF 名称，它是一个长度小于 32 的字符串；

**缺省情况：** 系统默认将接口绑定于主 VRF。

**命令模式：** 接口配置模式。

**使用指南：** 如果该接口有访问 Internet 的需求，可以配置此命令。一个接口只能绑定到一个 VRF，一个 VRF 可以绑定多个接口。支持 VPN 的 IGP 记录端口和 VRF 之间的绑定关系，从绑定端口接收到路由，就加入与之绑定的 VRF 路由表。默认情况下，接口不关联任何 VRF，属于公网接口。

**举例：**

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ip vrf forwarding vpn1

## 4.1.9 no interface IFNAME

**命令：no interface IFNAME**

**功能：**删除 interface 接口，只处理 interface vlan 和 interface loopback 两种接口。

**参数：**IFNAME：接口名。

**命令模式：**全局模式。

**使用指南：**该命令用以删除三层接口，是处理接口名是特殊拼写形式的情况。IFNAME 可以匹配多种形式的拼写，如 vlan1、Vlan1、v1、V1 等。

**举例：**删除 interface vlan1 这个接口。

(config)# no interface vlan1

## 4.1.10 rd

**命令：rd <ASN:nn_or_IP-address:nn>**

**功能：**配置 VRF 的 RD（Route Distinguish）。

**参数：ASN**:nn_or_IP-address:nn：路由器标识的 IP 地址格式。

**缺省情况：**默认不配置。

**命令模式：**VRF 配置模式。

**使用指南：**RD 用于对 VPN 路由进行唯一标识，VPN 实例通过 RD 实现地址空间独立，可以实现不同 VPN 之间的地址重叠。通常设置由 AS 号和一个任意数组成。无法直接删除 RD。

**举例：**

Switch (config)#ip vrf VRF-A

Switch (config-vrf)# rd 300:3

Switch (config-vrf)#

## 4.1.11 route-target

**命令：route-target {import | export | both} <rt-value>**

**no route-target {import | export | both} <*rt-value*>**

**功能：** 配置指定 VRF 的 Route-Target；no 命令删除配置。

**参数：** **import：表示对路由进行入口过滤，即判断 VPN 路由是否可以加入本 VRF；**

**export：表示当将本 VRF 的路由作为 VPNv4 路由向外发送时需附加的 Route-Target，用于对端口进行入口过滤；**

**both：表示 import、export 使用相同的 Route-Target 值；**

***<rt-value>***：表示路由目标值。

**缺省情况：** 默认不配置。

**命令模式：** VRF 配置模式。

**使用指南：** 一个 RT 是一个 BGP 扩展团体，用于对 VPN 路由进行过滤，实现对直连 site 的 VPN 成员关系和路由规则的控制。对于配置的 import 规则，遍历所有 BGP 进程收到的路由，对符合条件的路由（路由的 export route-target 与本 VRF 的 import route-target 有交集），添加到该 VRF 下的 BGP 进程中，并向该 VRF 下的 BGP 私网邻居发布路由更新消息。对于配置的 export 规则，遍历该 VRF 关联的 BGP 进程中存储的所有 BGP 路由，对这些路由增加一个 export route-target，之后向所有公网邻居发布路由更新消息，同时，如果有其它 VRF 的 import route-target 与该 export route-target 相匹配，则复制一份路由到匹配 VRF 中，并向这个 VRF 下的 BGP 私网邻居发布路由更新。

**举例：**

```
Switch (config)#ip vrf VRF-A
Switch (config-vrf)# route-target both 100:1
Switch (config-vrf)#
```

## 4.1.12 show ip route

**命令：** **show ip route [ database ]**

**功能：** 显示路由表。

**参数：** *<database>*为数据库信息。

**命令模式：** 特权用户配置模式。

**使用指南：** 显示核心路由表的内容，包括：路由类型、目的网络、掩码、下一跳地址、接口等。

**举例：**

```
Switch#show ip route
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
A - OSPF ASE, B - BGP derived
    Destination Mask Nexthop Interface Pref
    C 2.2.2.0 255.255.255.0 0.0.0.0 vlan2 0
    C 4.4.4.0 255.255.255.0 0.0.0.0 vlan4 0
    S 6.6.6.0 255.255.255.0 9.9.9.9 vlan9 1
```

| 显示信息 | 解释 |
| --- | --- |
| C - connected | 直连路由，即与三层交换机直接相连的网段 |
| S – static | 静态路由，由用户手工配置的路由 |
| R - RIP derived | RIP 路由，三层交换机通过 RIP 协议得到的 |
| O - OSPF derived | OSPF 路由，三层交换机通过 OSPF 协议得到的 |
| A- OSPF ASE | OSPF 引入的路由 |
| B- BGP derived | BGP 路由，路由通过 BGP 协议得到 |
| Destination | 目标网络 |
| Mask | 目标网络的掩码 |
| Nexthop | 下一跳 IP 地址 |
| Interface | 下一跳经过的三层交换机接口 |
| Preference | 路由的优先级，如果到达目标网络还有其它类型的路由，在核心路由表中只显示优先级高的路由信息 |

## 4.1.13 show ip route vrf

**命令：show ip route vrf <vrf-name> [bgp | datebase]**

**参数：** <***vrf-name***>：VRF 名称，通过 if vrf <vrf-name>命令创建；

bgp：表示通过 BGP 引入的路由；

database：IP 路由表数据库。

**缺省情况：** 无。

**命令模式：** 任意配置模式。

**使用指南：** 可以针对指定的路由协议显示。

**举例：**

Switch#show ip route vrf vrf-a bgp

Network Next Hop Metric LocPrf Weight Path

Route Distinguisher: 100:10 (Default for VRF test)

*> 11.1.1.0/24 11.1.1.64 0 0 200 ?

*> 20.1.1.0/24 11.1.1.64 0 0 200 ?

## 4.1.14 show ip vrf

**命令：show ip vrf [<vrf-name>]**

**功能：**本命令显示与该 VPN 路由/转发实例相关的 RIP 实例信息。可显示绑定 VRF 的接口配置 fallback global 选项。

**参数：**<***vrf-name***>指明了 VPN 路由/转发实例的名称。

**缺省情况：**缺省不显示。

**命令模式：**任意模式。

**使用指南：**本命令在其它的路由协议中也存在，使用本命令时，与该 VPN 路由/转发实例相关的其它路由协议进程的信息也会显示出来。

**举例：**显示与 IPI 的 VRF 路由/转发实例相关的 RIP 实例信息。

```
Switch# show ip vrf IPI
  VRF IPI, FIB ID 1
  Router ID: 11.1.1.1 (automatic)
  Interfaces:
  Vlan1
  !
  VRF IPI; (id=1); RIP enabled Interfaces:
  Ethernet1/1/8

  Name                Interfaces
  IPI                  Vlan1

  Name                      Default RD          Interfaces
  IPI                                           Vlan1
```

## 4.1.15 shutdown

**命令：shutdown**

**no shutdown**

**功能：**关闭交换机的指定 VLAN 接口；本命令的 no 操作为打开 VLAN 接口。

**命令模式：**VLAN 接口配置模式。

**缺省情况：**VLAN 接口缺省为打开。

**使用指南：**当关闭交换机的 VLAN 接口，VLAN 接口将不发送数据帧。如果交换机的 VLAN 接口需要通过 BOOTP/DHCP 协议获取 IP 地址时，必须将 VLAN 接口打开。

**举例：**打开交换机的 VLAN1 接口。

```
Switch(Config-if-Vlan1)#no shutdown
```

# 4.2 网管端口

## 4.2.1 duplex

本型号交换机不支持此命令。

## 4.2.2 interface ethernet

**命令：interface ethernet *<interface-name>***

**功能：**从全局配置模式进入到网管端口配置模式。

**参数：*<interface-name>***为端口号，取 0。

**命令模式：**全局配置模式。

**使用指南：**使用命令 exit 可从以网管端口配置模式退回到全局配置模式。

**举例：**进入网管端口。

Switch(config)#interface ethernet 0

Switch(Config-If-Ethernet0)#

## 4.2.3 ip address

**命令：ip address *<ip-address>* *<mask>***

**no ip address [*<ip-address>* *<mask>*]**

**功能：**设置交换机的 IP 地址及掩码；本命令的 no 操作为删除该 IP 地址配置。

**参数：*<ip-address>***为 IP 地址，点分十进制格式；***<mask>***为子网掩码，点分十进制格式。

**命令模式：**网管端口配置模式。

**缺省情况：**系统缺省没有 IP 地址配置。

**使用指南：**本命令为在网管端口配置 IP 地址。

**举例：**网管端口的 IP 地址设置为 192.168.1.10/24。

Switch(Config-If-Ethernet0)#ip address 192.168.1.10 255.255.255.0

## 4.2.4 shutdown

**命令：shutdown**

**no shutdown**

**功能：**关闭网管端口；本命令的 no 操作为打开端口。

**命令模式：**网管端口配置模式。

**缺省情况：**网管端口缺省为打开。

**使用指南：**当关闭网管端口时，网管端口将不发送数据帧，并且在用户输入 show interface 命令时显示端口状态为 down。

**举例：**打开网管端口。

Switch(config)#interface ethernet 0

Switch(Config-If-Ethernet0)#no shutdown

### 4.2.5 speed

本型号交换机不支持此命令。

## 4.3 IP 配置

### 4.3.1 clear ip traffic

**命令：clear ip traffic**

**功能：**清除 IP 协议统计信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权用户配置模式。

**使用指南：**清除 IP 内核协议收发数据包的统计信息，包括 IP 协议，ICMP 协议、TCP 协议和 UDP 协议的收包统计、发包统计、丢包统计以及收发数据包的错误信息等内容。

**举例：**清除 ip 协议统计信息。

Switch#clear ip traffic

### 4.3.2 clear ipv6 neighbor

**命令：clear ipv6 neighbors**

**功能：**清除 IPv6 的邻居缓存。

**参数：**无。

**命令模式：**特权配置模式。

**缺省情况：**无。

**使用指南：**该命令不能清除静态邻居。

**举例：**清除邻居表。

Switch #clear ipv6 neighbors

### 4.3.3 debug ip icmp

**命令：debug ip icmp**

**no debug ip icmp**

**功能：**ICMP 数据包收发调试信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权用户配置模式。

**使用指南：**

**举例：**

Switch#debug ip icmp

IP ICMP: sent, type 8, src 0.0.0.0, dst 20.1.1.1

| 显示内容 | 解释 |
| --- | --- |
| IP ICMP: sent | 发送 ICMP 数据报 |
| type 8 | 类型为 8（PING 请求） |
| src 0.0.0.0 | 源 IPv4 地址 |
| dst 20.1.1.1 | 目的 IPv4 地址 |

## 4.3.4 debug ip packet

**命令：debug ip packet**

**no debug ip packet**

**功能：**打开 IP 报文调试开关；本命令的 no 操作为关闭调试开关。

**参数：**无。

**缺省情况：**缺省 IP 数据包调试功能是关闭的。

**命令模式：**特权用户配置模式。

**使用指南：**显示接收或发送的 IP 数据包的内容，包括：源地址、目的地址、字节数等。

**举例：**打开 IP 报文调试开关。

Switch #debug ip packet

IP PACKET: sent, src 200.1.1.35, dst 224.0.0.9, size 312, proto 17, vrf 0

IP PACKET: rcvd, src 101.1.1.1, dst 224.0.0.9, size 312, proto 17, from Vlan200, vrf 0

## 4.3.5 debug ipv6 packet

**命令：debug ipv6 packet**

**no debug ipv6 packet**

**功能：**IPv6 数据包收发调试信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**

**举例：**

Switch#debug ipv6 packet

IPv6 PACKET: rcvd, src <fe80::203:fff:fe01:2786>, dst <fe80::1>, size <64>, proto <58>, from Vlan1

| 显示内容 | 解释 |
| --- | --- |
| IPv6 PACKET: rcvd | 接收 IPv6 数据报 |

| | |
|---|---|
| src <fe80::203:fff:fe01:2786> | 源 IPv6 地址 |
| dst <fe80::1> | 目的 IPv6 地址 |
| size <64> | 数据报的大小 |
| proto <58> | IPv6 头中协议字段 |
| from Vlan1 | IPv6 数据报是从三层口 vlan 1 收上来 |

## 4.3.6 debug ipv6 icmp

**命令：debug ipv6 icmp**

**no debug ipv6 icmp**

**功能：**ICMP 数据包收发调试信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**

**举例：**

Switch#debug ipv6 icmp

IPv6 ICMP: sent, type <129>, src <2003::1>, dst <2003::20a:ebff:fe26:8a49> from Vlan1

| 显示内容 | 解释 |
|---|---|
| IPv6 ICMP: sent | 发送 ICMP 数据报 |
| type <129> | Ping 协议号 |
| src <2003::1> | 源 IPv6 地址 |
| dst <2003::20a:ebff:fe26:8a49> | 目的 IPv6 地址 |
| from Vlan1 | 发送的三层端口 |

## 4.3.7 debug ipv6 nd

**命令：debug ipv6 nd [ns | na | rs | ra | redirect]**

**no debug ipv6 nd [ns | na | rs | ra | redirect]**

**功能：**打开指定类型的 IPv6 ND 协议报文收发调试开关，其中 ns，na，rs，ra 和 redirect 分别表示邻居请求，邻居公告，路由器请求，路由器公告和路由重定向，如果不指定其中任何一种类型，则表示同时打开所有 5 种类型的 ND 报文收发调试开关。本命令的 no 操作关闭指定类型的 IPv6 ND 协议报文收发调试开关，如果不指定类型，则关闭所有 5 种 ND 报文收发调试开关。

**参数：**无。

**缺省情况：**IPv6 ND 的所有 5 种协议报文收发调试开关默认是关闭的。

**命令模式：**特权模式。

**使用指南：**ND 协议是 IPv6 的一个核心协议，使用本命令可以显示指定类型的 ND 协议报文，达到诊断排错的目的。

**举例：**

Switch#debug ipv6 nd

IPv6 ND: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst <fe80::203:fff:fe01:59ba>

| 显示内容 | 解释 |
|---|---|
| IPv6 ND: rcvd | 接收 ND 数据报 |
| type <136> | ND 类型 |
| src <fe80::203:fff:fe01:2786> | 源 IPv6 地址 |
| dst <fe80::203:fff:fe01:59ba> | 目的 IPv6 地址 |

## 4.3.8 debug ipv6 tunnel packet

**命令：debug ipv6 tunnel packet**

**no debug ipv6 tunnel packet**

**功能：** tunnel 数据包收发调试信息。

**参数：** 无。

**缺省情况：** 无。

**命令模式：** 特权模式。

**使用指南：**

**举例：**

Switch#debug ipv6 tunnel packet

IPv6 tunnel: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst <fe80::203:fff:fe01:59ba>

IPv6 tunnel packet : rcvd src 178.1.1.1 dst 179.2.2.2 size 128 from tunnel1

| 显示内容 | 解释 |
|---|---|
| IPv6 tunnel packet : rcvd | 接收隧道数据报 |
| type <136> | ND 类型 |
| src 178.1.1.1 dst | 隧道源 IPv4 地址 |
| dst 179.2.2.2 | 隧道目的 IPv4 地址 |

## 4.3.9 description

**命令：description <desc>**

**no description**

**功能：** 配置隧道的描述信息，本命令的no操作删除隧道描述信息。

**参数：** ***<desc>***为隧道的描述信息，它是长度不超过256的字符串。

**命令模式：** 隧道配置模式。
**缺省情况：** 隧道缺省没有配置描述信息。
**使用指南：** 在系统中有多条隧道时，配置描述信息有助于用户识别不同隧道的用途。
**举例：** 配置隧道描述为toCernet2。

Switch(Config-if-Tunnel1)#description toCernet2

## 4.3.10 ipv6 proxy enable

本型号交换机不支持此命令。

## 4.3.11 ip address

**命令：ip address *<ipaddress>* *<mask>* [secondary]**
**no ip address [*<ipaddress>* *<mask>*] [secondary]**
**功能：**设置交换机的 IP 地址及掩码；本命令的 no 操作为删除该 IP 地址配置。
**参数：*<ipaddress>***为 IP 地址，点分十进制格式；***<mask>***为子网掩码，点分十进制格式；**[secondary]**为表示配置的 IP 地址为从 IP 地址。
**命令模式：**VLAN 接口配置模式。
**缺省情况：**系统缺省没有 IP 地址配置。
**使用指南：**本命令为在 VLAN 接口手工配置 IP 地址，若没有配置可选参数 secondary，表示配置为 VLAN 接口的主 IP 地址，若配置了可选参数 secondary，则表示该 IP 地址为 VLAN 接口的从 IP 地址。一个 VLAN 接口只能有一个主 IP 地址，可以有多个从 IP 地址。主 IP 和从 IP 均可以用于 SNMP/Web/Telnet 管理。此外，交换机还提供了 BOOTP/DHCP 方式获取 IP 地址。
**举例：**交换机 VLAN1 接口的 IP 地址设置为 192.168.1.10/24。

Switch(Config-If-Vlan1)#ip address 192.168.1.10 255.255.255.0

## 4.3.12 ip default-gateway

本型号交换机不支持此命令。

## 4.3.13 ip route

**命令：ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>*/*<prefix-length>*} {*<gateway-address>* | *<gateway-interface>*} [*<distance>*]**
**no ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>*/*<prefix-length>*} [*<gateway-address>* | *<gateway-interface>*] [*<distance>*]**
**功能：** 配置静态路由；本命令的 no 操作为删除静态路由。

**参数：<*ip-prefix*>**和**<*mask*>**分别为目的 IP 地址和子网掩码，点分十进制格式；**<*ip-prefix*>**和**<*prefix-length*>**分别为目的 IP 地址和前缀长度；**<*gateway-address*>**为下一跳的 IP 地址，点分十进制格式；**<*gateway-interface*>**为下一跳接口，**<*distance*>**为路由管理距离值，取值范围为 1～255。

**缺省情况：** 静态路由缺省管理距离值为 1。

**命令模式：** 全局配置模式。

**使用指南：** 在配置静态路由的下一跳时，可采用指定路由数据包发送下一跳 IP 地址或者出接口方式。二层交换机也能够配置该命令，但配置的路由仅供交换机自身发包用，不会下发到交换芯片中参与报文的三层转发。

**举例：** 添加一条静态路由。

Switch(config)#ip route 1.1.1.0 255.255.255.0 2.1.1.1

## 4.3.14 ip route unreachable-to-cpu enable

**命令：ip route unreachable-to-cpu enable { enable | disable}**

**功能**：允许不可达报文上 CPU 或禁止不可达报文上 CPU。

**参数**：enable 表示允许不可达报文上 CPU；disable 表示禁止不可达报文上 CPU。

**缺省情况**：缺省为禁止不可达报文上 CPU。

**命令模式**：全局配置模式。

使用指南：允许大量不可达报文上 CPU 会显著增加设备的 CPU 负载，特别是在高流量的网络环境中。这可能会导致设备性能下降，影响其他网络功能的正常运行。在极端情况下，过高的 CPU 负载可能会导致设备响应缓慢、丢包率增加甚至设备崩溃。

举例：允许不可达报文上 CPU。

Switch(config)#ip route unreachable-to-cpu enable

## 4.3.15 ip route vrf

**命令：ip route vrf <vrf-name>{<ip-prefix> <mask>|<ip-prefix/prefix-length>}**

**{<*gateway-address*>|null0} [<*1-255*>]**

**no ip route vrf <*vrf-name*>{<*ip-prefix*> <*mask*>|<*ip-prefix/prefix-length*>}**

**{<*gateway-address*>|null0} [<*1-255*>]**

**功能**：为指定 VRF 配置静态路由。使用本命令前必须先配置成功 VPN 路由转发实例；no 命令删除已配置静态路由。

**参数：<*vrf-name*>**：指定的 VRF 名称；

**<*ip-prefix*>**：为目的 IP 地址；

**<*mask*>**：子网掩码，点分十进制格式；

**<*prefix-length*>**：前缀长度；

***<gateway-address>***：下一条地址；

**null0**：黑洞路由；

<***1-255***>：管理距离。

**缺省情况**：默认不配置。

**命令模式**：全局配置模式。

**举例**：配置 VRF-A 的静态路由，目的 IP 为 10.1.1.10，掩码 24 位，下一跳为 10.1.1.1，管理距离默认：

Switch(config)# ip route vrf VRF-A 10.1.1.10 255.255.255.0 10.1.1.1

Switch(config)#

## 4.3.16 ipv6 address

**命令：ipv6 address <*ipv6address/prefix-length*> [eui-64]**

**no ipv6 address <*ipv6address/prefix-length*> [eui-64]**

**功能**：为接口配置可聚合全球单播地址、本地站点地址、本地链路地址。

**参数**：**<*ipv6address*>**参数为 IPv6 地址的前缀，**<*prefix-length*>**参数为 IPv6 地址的前缀长度，前缀长度为 3-128 之间，**eui-64** 表明根据接口的 eui64 接口标识符自动生成 IPv6 地址。

**命令模式**：接口配置模式。

**缺省情况**：无。

**使用指南**：IPv6 地址前缀不能是多播地址，及其它有特定用途的 IPv6 地址，不同的 vlan 三层接口不能配置相同的地址前缀。对于全球单播地址，前缀长度必须大于或等于 3。对于本地站点地址和本地链路地址，前缀长度必须大于或等于 10。对于 interface loopback 接口，前缀长度必须等于 128。

**举例**：在 Vlan1 三层接口上配置一个 IPv6 地址：前缀为 2001:3f:ed8::99，前缀长度为 64。

Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64

## 4.3.17 ipv6 default-gateway

本型号交换机不支持此命令。

## 4.3.18 ipv6 route

**命令：ipv6 route <*ipv6-prefix/prefix-length*> {<*ipv6address*>**

**|<*interface-type interface-number*>|{<*ipv6address*> <*interface-type interface-number*>} | tunnel <*tunnel no*> } [<*precedence*>]**

**no ipv6 route <*ipv6-prefix/prefix-length*> {<*ipv6address*>**

**|<*interface-type interface-number*>|{<*ipv6address*> <*interface-type interface-number*>} | tunnel <*tunnel no*> } [<*precedence*>]**

**功能：** 设置 IPv6 静态路由。

**参数：** ***<ipv6-prefix>***参数为 IPv6 网络静态路由的目的地址，***<prefix-length>***参数为 IPv6 前缀长度，***<ipv6address>***参数为可以到达指定网络的下一跳 IPv6 地址，***<interface-type interface-number>***参数为指向静态路由出口接口名， ***<tunnel no>*** 参数为隧道路由的出口隧道号， ***<precedence>***参数为本路由的权重，范围为 1-255,默认为 1。

**缺省情况：** 没有配置任何的 IPv6 静态路由。

**命令模式：** 全局配置模式。

**使用指南：** 在下一跳 IPv6 地址为本地链路地址时，必须指定出口的接口名。下一跳 IPv6 地址为全球可聚合单播地址和本地站点地址时，当不指定出口的接口名，必须保证该下一跳的 IP 地址和交换机某一接口的地址在同一个网段内。对于隧道路由可以直接指定接口名。

**举例：** 配置静态路由 1，目的地址为 3ffe:589:dfc::88，前缀长度为 64，下一跳为 2001:8fd:c32::99（该路由器已经配置了 2001:8fd:c32::34/64 的 IPv6 地址）。

Switch(config)#ipv6 route 3ffe:589:dfc::88/64 2001:8fd:c32::99

配置静态路由 2，目的地址为 3ffe:ff7:123::55，前缀长度为 64，下一跳为 fe80::203:ff:89fd:46ac,出接口名为 Vlan1。

Switch(config)#ipv6 route 3ffe:ff7:123::55/64 fe80::203:ff:89fd:46ac Vlan1

## 4.3.19 ipv6 redirect

**命令：ipv6 redirect**

**no ipv6 redirect**

**功能：** 使能 IPv6 路由重定向功能，本命令的 no 操作为关闭 IPv6 路由重定向功能。

**参数：** 无。

**命令模式：** 全局配置模式。

**缺省情况：** IPv6 路由重定向功能缺省是关闭的。

**使用指南：** 如果路由器 A，路由器 B 和节点 C 位于同一网络链路，路由器 A 把来自节点 C 的 IPv6 数据包转发到路由器 B，希望路由器 B 继续转发该数据包，则路由器 A 会向数据包源节点 C 发送 IPv6 ICMPv6 路由重定向报文，告知数据包源点 C 发往该目的地址的最优下一跳是路由器 B，这样节省了路由器 A 的转发开销，也缩短了节点 C 的网络传输延迟。

**举例：** 打开 IPv6 路由重定向功能。

Switch(config)# ipv6 redirect

## 4.3.20 ipv6 nd dad attempts

**命令：ipv6 nd dad attempts <*value*>**

**no ipv6 nd dad attempts**

**功能：**设置重复地址检测时接口连续发出的邻居请求消息数目。

**参数：<*value*>**参数为重复地址检测连续发出的邻居请求消息数目，**<*value*>**值必须在 0-10 之间，**no** 命令为恢复到默认值 1。

**命令模式：**接口配置模式。

**缺省情况：**缺省的请求消息数目为 1

**使用指南：**当在接口上配置一个 IPv6 地址时，要执行 IPv6 重复地址检测，该命令用于配置需要发送的重复地址检测的 ND 报文数量，*value* 为 0 则不进行重复地址检测。

**举例：**设置重复地址检测时接口连续发出的邻居请求消息数目为 3。

Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3

## 4.3.21 ipv6 nd ns-interval

**命令：ipv6 nd ns-interval <*seconds*>**

**no ipv6 nd ns-interval**

**功能：**设置接口发送邻居请求消息的时间间隔。

**参数：<*seconds*>**参数为发送邻居请求消息的时间间隔，**<*seconds*>**值必须在 1-3600 秒之间，*no* 命令为恢复到默认值 1 秒。

**命令模式：**接口配置模式。

**缺省情况：**缺省的请求消息时间间隔为 1 秒。

**使用指南：**该设定的值将包含在该接口上所有的路由公告消息中，在一般的情况下不推荐非常短的时间间隔。

**举例：**设置 Vlan1 接口发送邻居请求消息的时间间隔为 8 秒。

Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8

## 4.3.22 ipv6 nd suppress-ra

**命令：ipv6 nd suppress-ra**

**no ipv6 nd suppress-ra**

**功能：**禁止路由器公告。

**参数：**无。

**命令模式：**接口配置模式。

**缺省情况：**没有启动路由公告功能。

**使用指南：**no ipv6 nd suppress-ra 命令开启路由公告功能。

**举例：**打开路由公告功能。

Switch(Config-if-Vlan1)#no ipv6 nd suppress-ra

## 4.3.23 ipv6 nd ra-lifetime

命令：ipv6 **nd ra-lifetime <*seconds*>**

**no ipv6 nd ra-lifetime**

**功能：** 配置路由器公告的生存期。

**参数：** ***<seconds>***参数表示路由器公告生存期的秒数，***<seconds>***值必须为 0-9000 之间。

**命令模式：** 接口配置模式。

**缺省情况：** 路由器缺省公告生存期的秒数为 1800。

**使用指南：** 该命令用于配置三层接口上路由器的生存时间，seconds 为 0 说明此接口不能用于默认路由器，否则该值不应该小于发送路由公告的最大时间间隔。如果不进行配置，该值等于发送路由公告的最大时间间隔的 3 倍。

**举例：** 设置路由公告的生存期为 100 秒。

Switch (Config-if-Vlan1)#ipv6 nd ra-lifetime 100

## 4.3.24 ipv6 nd min-ra-interval

**命令：ipv6 nd min-ra-interval *<seconds>***

**no ipv6 nd min-ra-interval**

**功能：** 设置发送路由公告的最小时间间隔。

**参数：*<seconds>***参数为发送路由公告的最小时间间隔秒数，***<seconds>***值必须为 3-1350 秒之间。

**命令模式：** 接口配置模式。

**缺省情况：** 发送路由公告缺省的最小时间间隔为 200 秒。

**使用指南：** 路由公告的最小时间间隔不超过最大时间间隔的 3/4。

**举例：** 设置发送路由公告的最小时间间隔为 10 秒。

Switch (Config-if-Vlan1)#ipv6 nd min-ra-interval 10

## 4.3.25 ipv6 nd max-ra-interval

**命令：ipv6 nd max-ra-interval <seconds>**

**no ipv6 nd max-ra-interval**

**功能：** 设置发送路由公告的最大时间间隔。

**参数：*<seconds>***参数为发送路由公告的时间间隔秒数，***<seconds>***值必须为 4-1800 秒之间。

**命令模式：** 接口配置模式。

**缺省情况：** 发送路由公告缺省的最大时间间隔为 600 秒。

**使用指南：** 路由公告的最大时间间隔要小于路由公告的生存期的值。

**举例：** 设置发送路由公告的最大时间间隔为 20 秒。

Switch (Config-if-Vlan1)#ipv6 nd max-ra-interval 20

## 4.3.26 ipv6 nd prefix

**命令：ipv6 nd prefix <*ipv6-prefix/prefix-length*> { [<*valid-lifetime*> <*preferred-lifetime*>] [ no-autoconfig | off-link [no-autoconfig] ]}**

**no ipv6 nd prefix <*ipv6-prefix/prefix-length*>**

**功能：** 配置用于路由器公告的地址前缀以及相关参数。

**参数：** **<*ipv6-prefix*>**参数为指定要公告的地址前缀，**<*prefix-length*>**参数为指定要公告的地址前缀的长度，**<*valid-lifetime*>**参数为该前缀的有效生存期，**<*preferred-lifetime*>**参数为该前缀的优先生存期，有效生存期必须不小于优先生存期。no-autoconfig 参数说明在本地链路的主机上不能使用该前缀来自动配置 IPv6 地址，off-link 参数说明路由器公告消息指定的前缀不分配给本地链路，向包含这个指定前缀的地址发送数据的节点认为目的地是本地链路不可达的。

**命令模式：** 接口配置模式。

**缺省情况：** ***valid-lifetime 的默认值是 2592000 秒***(30 天)，preferred-lifetime 的默认值是 604800 秒(7 天)。off-link 默认是关闭的，no-autoconfig 默认是关闭的。

**使用指南：** 该命令允许控制每一个 IPv6 前缀的路由器公告参数，注意有效生存期和优先生存期必须同时配置。

**举例：** 在 Vlan1 配置 IPv6 公告前缀为 2001:410:0:1::/64，该前缀有效生存期为 8640 秒，优先生存期为 4320 秒。

Switch (Config-if-Vlan1)#ipv6 nd prefix 2001:410:0:1::/64 8640 4320

## 4.3.27 ipv6 nd ra-hoplimit

**命令：ipv6 nd ra-hoplimit <value>**

**功能：** 设置发送路由公告的 hoplimit 值。

**参数：** **<value>**参数为发送路由公告的 hoplimit 值，**<value>**值必须为 0-255 之间。

**命令模式：** 接口配置模式。

**缺省情况：** 发送路由公告缺省的 hoplimit 值为 64。

**举例：** 设置 interface vlan 1 内发送的路由公告的 hoplimit 值为 128。

Switch#(config-if-vlan1)#ipv6 nd ra-hoplimit 128

## 4.3.28 ipv6 nd ra-mtu

**命令：ipv6 nd ra-mtu <value>**

**功能：** 设置发送路由公告的 mtu 值。

**参数：** **<value>**参数为发送路由公告的 mtu 值，**<value>**值必须为 0-1500 之间。

**命令模式：** 接口配置模式。

**缺省情况：** 发送路由公告缺省的 mtu 值为 1500。

**举例：** 设置 interface vlan 1 内发送的路由公告的 mtu 值为 500。

Switch#(config-if-vlan1)#ipv6 nd ra-mtu 500

## 4.3.29 ipv6 nd reachable-time

**命令：ipv6 nd reachable-time <seconds>**

**功能：** 设置发送路由公告的 reachable-time 值。

**参数：** **<seconds>**参数为发送路由公告的 reachable-time 值，**<seconds>**值必须为 0-3600000 毫秒之间。

**命令模式：** 接口配置模式。

**缺省情况：** 发送路由公告缺省的 reachable-time 值为 30000 毫秒。

**举例：** 设置 interface vlan 1 内发送的路由公告的 reachable-time 值为 100000 毫秒。

Switch(config-if-vlan1)#ipv6 nd reachable-time 100000

## 4.3.30 ipv6 nd retrans-timer

**命令：ipv6 nd retrans-timer <seconds>**

**功能：** 设置发送路由公告的 retrans-timer 值。

**参数：** **<seconds>**参数为发送路由公告的 retrans-timer 值，**<seconds>**值必须为 0-4294967295 毫秒之间。

**命令模式：** 接口配置模式。

**缺省情况：** 发送路由公告缺省的 retrans-timer 值为 1000 毫秒。

**举例：** 设置 interface vlan 1 内发送的路由公告的 retrans-timer 值为 10000 毫秒。

Switch(config-if-vlan1)#ipv6 nd retrans-timer 10000

## 4.3.31 ipv6 nd other-config-flag

**命令：ipv6 nd other-config-flag**

**no ipv6 nd other-config-flag**

**功能：** 设置发送路由公告的其他状态配置标志为 1。

**参数：** 无。

**命令模式：** 接口配置模式。

**缺省情况：** 路由公告的其他状态配置标志默认为 0。

**使用指南：** 当其他状态配置标志为 1 时，表示收到这个路由公告的主机必须使用有状态地址配置协议(比如 DHCPv6)来获得非地址配置的信息(比如 DNS 地址等)。

**举例：** 设置发送路由公告的其他状态配置标志。

Switch(config-if-vlan1)#ipv6 nd other-config-flag

## 4.3.32 ipv6 nd managed-config-flag

**命令：ipv6 nd managed-config-flag**

**no ipv6 nd managed-config-flag**

**功能：** 设置发送路由公告的管理地址配置标志为 1。

**参数：** 无。

**命令模式：** 接口配置模式。

**缺省情况：** 路由公告的管理地址配置标志默认为 0。

**使用指南：** 当管理地址配置标志为 1 时，表示收到这个路由公告的主机除了可能按照无状态地址自动配置协议获得地址外，还必须使用有状态地址配置协议(比如 DHCPv6)来获得地址；当管理地址配置标志为 0 时，表示收到这个路由公告的主机只使用无状态地址自动配置协议获得地址。

**举例：** 设置发送路由公告的管理地址配置标志。

Switch(config-if-vlan1)#ipv6 nd managed-config-flag

## 4.3.33 ipv6 neighbor

**命令：ipv6 neighbor *<ipv6address>* *<hardware-address>* interface *<interface-type interface-name>***

**no ipv6 neighbor *<ipv6address>***

**功能：**设置静态邻居表项。

**参数：*ipv6address*** 参数为静态邻居 IPv6 地址，与接口前缀相同，***hardware-address*** 参数为静态邻居硬件地址，***interface-type*** 为 ethernet 类型，***interface-name*** 为二层接口名。

**命令模式：**接口配置模式。

**缺省情况：**没有静态邻居表项。

**使用指南：**不能将用于特殊用途的 IPv6 地址和多播地址，及本机地址设置为邻居。

**举例：**在端口 E1/1/1 上设置静态邻居 2001:1:2::4，硬件 MAC 地址为 00-03-0f-89-44-bc。

Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-03-0f-89-44-bc interface Ethernet 1/1/1

## 4.3.34 interface tunnel

命令：interface **tunnel *<tnl-id>***

**no interface tunnel *<tnl-id>***

**功能：** 创建/删除隧道。

**参数：** ***<tnl-id>*** 参数为隧道号。

**命令模式：** 全局配置模式。

**缺省情况：** 无。

**使用指南：** 该命令创建一个虚拟的隧道接口，由于没有指定隧道的模式和隧道源等信息，show ipv6 tunnel 没有显示该隧道，创建后进入隧道模式，在该模式下可以指定隧道的源、目的等信息。no 命令是删除一条隧道。

**举例：** 创建隧道 1。

Switch(Config)#interface tunnel 1

## 4.3.35 show ip interface

**命令：show ip interface [<*ifname*> | vlan <*vlan-id*>] brief**

**功能：**显示配置的三层接口的简要信息。

**参数：<*ifname*>**为接口名称；**<*vlan-id*>**为 VLAN 号。

**缺省情况：**不指定参数时，显示所有配置的三层接口的简要信息。

**命令模式：**所有模式

**使用指南：**无。

**举例：**Restarter#show ip interface vlan1 brief

| Index | Interface | IP-Address | Protocol |
|---|---|---|---|
| 3001 | Vlan1 | 192.168.2.11 | up |

## 4.3.36 show ip traffic

**命令：show ip traffic**

**功能：**显示 IP 数据包统计信息。

**命令模式：**特权用户配置模式。

**使用指南：**显示 IP，ICMP，TCP，UDP 数据包的接收、发送等统计信息。

**举例：**

```
Switch #show ip traffic
IP statistics:
  Rcvd:  3249810 total, 3180 local destination
         0 header errors, 0 address errors
         0 unknown protocol, 0 discards
  Frags: 0 reassembled, 0 timeouts
         0 fragment rcvd, 0 fragment dropped
         0 fragmented, 0 couldn't fragment, 0 fragment sent
  Sent:  0 generated, 3230439 forwarded
         0 dropped, 0 no route
ICMP statistics:
  Rcvd:  0 total 0 errors 0 time exceeded
         0 redirects, 0 unreachable, 0 echo, 0 echo replies
         0 mask requests, 0 mask replies, 0 quench
         0 parameter, 0 timestamp, 0 timestamp replies
  Sent:  0 total 0 errors 0 time exceeded
         0 redirects, 0 unreachable, 0 echo, 0 echo replies
         0 mask requests, 0 mask replies, 0 quench
         0 parameter, 0 timestamp, 0 timestamp replies
TCP statistics:
  TcpActiveOpens            0, TcpAttemptFails          0
  TcpCurrEstab              0, TcpEstabResets           0
```

TcpInErrs 0, TcpInSegs 3180
TcpMaxConn 0, TcpOutRsts 3
TcpOutSegs 3, TcpPassiveOpens 8
TcpRetransSegs 0, TcpRtoAlgorithm 0
TcpRtoMax 0, TcpRtoMin 0
UDP statics:
UdpInDatagrams 0, UdpInErrors 0
UdpNoPorts 0, UdpOutDatagrams 0

| 显示信息 | 解释 |
|---|---|
| IP statistics： | IP 数据包的统计信息： |
| Rcvd： 3249810 total, 3180 local destination<br>0 header errors, 0 address errors<br>0 unknown protocol, 0 discards | 接收总量的统计及其中有多少到达本地、多少数据包的包头有错误、多少地址有错误、多少不明协议的数据包、多少丢包等的统计。 |
| Frags： 0 reassembled, 0 timeouts<br>0 fragment rcvd, 0 fragment dropped<br>0 fragmented, 0 couldn't fragment, 0 fragment sent | 分段统计：重组多少数据包、超时的有多少、接收分段数、丢失分段数、多少不能分段、发送多少分段等。 |
| Sent： 0 generated, 3230439 forwarded<br>0 dropped, 0 no route | 发送总量的统计及其中包括多少从本地产生的、多少是转发的、多少丢失的、多少没有路由的等。 |
| ICMP statistics： | ICMP 数据包的统计信息： |
| Rcvd： 0 total 0 errors 0 time exceeded<br>0 redirects, 0 unreachable, 0 echo, 0 echo replies<br>0 mask requests, 0 mask replies, 0 quench<br>0 parameter, 0 timestamp, 0 timestamp replies | 接收 ICMP 数据包总量的统计及将这些 ICMP 数据包进行分类，分类后的统计数据。 |
| Sent： 0 total 0 errors 0 time exceeded<br>0 redirects, 0 unreachable, 0 echo, 0 echo replies<br>0 mask requests, 0 mask replies, 0 quench<br>0 parameter, 0 timestamp, 0 timestamp replies | 发送 ICMP 数据包总量的统计及将这些 ICMP 数据包进行分类，分类后的统计数据。 |
| TCP statistics: | TCP 数据包统计信息： |
| TcpActiveOpens 0,TcpAttemptFails 0<br>TcpCurrEstab 0, TcpEstabResets 0<br>TcpInErrs 0, TcpInSegs 3180 | 主动打开连接数，失败重试次数。<br>当前建立连接数，连接重置数<br>接收错误数据包，接收的段内数据包数 |

| | |
|---|---|
| TcpMaxConn 0, TcpOutRsts 3<br>TcpOutSegs 3, TcpPassiveOpens 8<br>TcpRetransSegs 0, TcpRtoAlgorithm 0<br>TcpRtoMax 0, TcpRtoMin 0 | 最大连接数，输出重置数<br>输出分段数据包数，被动连接数<br>重传数据包数，重传定时器时间<br>重传定时器允许最大时间，重传定时器允许最小时间 |
| UDP statics: | UDP 数据包统计信息： |
| UdpInDatagrams 0,UdpInErrors 0<br>UdpNoPorts 0, UdpOutDatagrams 0 | 接收的 UDP 数据包，接收的错误数据包。<br>无端口数据包数，发送数据包数 |

## 4.3.37 show ipv6 interface

**命令：show ipv6 interface {brief|{interface-name}}**

**功能：**显示接口 IPv6 参数。

**参数：**brief 参数为 IPv6 状态和配置简要概括, interface-name 参数为三层接口名。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**如果只是指定 brief，则显示所有三层接口的信息，也可以指定具体某一个三层接口。

**举例：**

```
Switch#show ipv6 interface Vlan1
Vlan1 is up, line protocol is up, dev index is 2004
Device flag 0x1203(UP BROADCAST ALLMULTI MULTICAST)
IPv6 is enabled
Link-local address(es):
 fe80::203:fff:fe00:10    PERMANENT
Global unicast address(es):
 3001::1                                    subnet is 3001::1/64    PERMANENT
Joined group address(es):
 ff02::1
 ff02::16
 ff02::2
 ff02::5
 ff02::6
 ff02::9
 ff02::d
 ff02::1:ff00:10
 ff02::1:ff00:1
MTU is 1500 bytes
```

ND DAD is enabled, number of DAD attempts is 1
ND managed_config_flag is unset
ND other_config_flag is unset
ND NS interval is 1 second(s)
ND router advertisements is disabled
ND RA min-interval is 200 second(s)
ND RA max-interval is 600 second(s)
ND RA hoplimit is 64
ND RA lifetime is 1800 second(s)
ND RA MTU is 0
ND advertised reachable time is 0 millisecond(s)
ND advertised retransmit time is 0 millisecond(s)

| 显示内容 | 解释 |
|---|---|
| Vlan1 | 三层接口名 |
| [up/up] | 三层接口状态 |
| dev index | 内部索引号 |
| fe80::203:fff:fe00:10 | 三层接口自动配置的 IPv6 地址 |
| 3001::1 | 三层接口配置的 IPv6 地址 |

## 4.3.38 show ipv6 route

**命令：show ipv6 route [ <**destination**> | <*destination* > | <*length*> | database | fib [local] | nsm [connected | static | rip | ospf | bgp | isis | kernel | database] | statistics]**

**功能：** 显示 IPv6 路由表。

**参数：** **<destination>** 为目标网络地址； ***<destination >/<length>*** 为目标网络地址加上前缀长度； **connected** 为直连路由； **static** 为静态路由； **rip** 为 RIP 路由； **ospf** 为 OSPF 路由； **bgp** 为 BGP 路由； **isis** 为 ISIS 路由； **kernel** 为核心路由； **statistics** 显示路由条数； **database** 为路由数据库。

**缺省情况：** 无。

**命令模式：** 特权和配置模式。

**使用指南：** **show ipv6 route 只显示 IPv6 核心路由表**(tcpip 中的路由表)，database 显示除本地路由中的所有路由，fib local 显示本地路由，statistics 显示路由统计信息。

**举例：**

Switch#show ipv6 route
Codes: C - connected, L - Local, S - static, R - RIP, O - OSPF,
I - IS-IS, B - BGP

```
C       ::/0        via ::,     tunnel3     256
S       2001:2::/32         via fe80::789,      Vlan2       1024
S       2001:2:3:4::/64         via fe80::123,      Vlan2       1024
O       2002:ca60:c801:1::/64         via ::,       Vlan1       1024
C       2002:ca60:c802:1::/64         via ::,       tunnel49      256
C       2003:1::/64         via ::,       Vlan4       256
C       2003:1::5efe:0:0/96         via ::,       tunnel26      256
S       2004:1:2:3::/64         via fe80:1::88,       Vlan2       1024
O       2006:1::/64         via ::,       Vlan1       1024
S       2008:1:2:3::/64         via fe80::250:baff:fef2:a4f4,       Vlan1       1024
C       2008:2005:5:8::/64         via ::,       Ethernet0       256
S       2009:1::/64         via fe80::250:baff:fef2:a4f4,       Vlan1       1024
C       2022:1::/64         via ::,       Ethernet0       256
O       3333:1:2:3::/64         via fe80::20c:ceff:fe13:eac1,       Vlan12      1024
C       3ffe:501:ffff:1::/64         via ::,       Vlan4       256
O       3ffe:501:ffff:100::/64         via ::,       Vlan5       1024
O       3ffe:3240:800d:1::/64         via ::,       Vlan1       1024
O       3ffe:3240:800d:2::/64         via ::,       Vlan2       1024
O       3ffe:3240:800d:10::/64         via ::,       Vlan12      1024
O       3ffe:3240:800d:20::/64         via fe80::20c:ceff:fe13:eac1,       Vlan12      1024
C       fe80::/64         via ::,       Vlan1       256
C       fe80::5efe:0:0/96         via ::,       tunnel26      256
C       ff00::/8         via ::,       Vlan1       256
```

| 显示内容 | 解释 |
| --- | --- |
| IPv6 Routing Table | IPv6 路由表情况 |
| Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,I - IS-IS, B - BGP > - selected route, * - FIB route, p - stale info | 各个项的缩写显示标记 |
| S 2009:1::/64 via fe80::250:baff:fef2:a4f4, Vlan1 1024 | FIB 表中的静态路由，目的网段为 2002::/64 ，via 表示通过 fe80::250:baff:fef2:a4f4 为下一跳，Vlan1 为出接口名，1024 为路由权重 |

## 4.3.39 show ipv6 neighbors

**命 令 ： show ipv6 neighbors [{vlan|ethernet|tunnel } interface-number | interface-name | address *<ipv6address>*]**

**功能：**显示邻居表项信息。

**参数：{vlan|ethernet|tunnel} *interface-number*** 和 ***interface-name*** 参数指定按接口名或者端口名进行查找。**address *<ipv6address>***参数指定按 IPv6 地址进行查找。当没有指定参数时，本命令显示所有的邻居表项。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**

**举例：**

```
Switch#show ipv6 neighbors
IPv6 neighbour unicast items: 14, valid: 11, matched: 11, incomplete: 0, delayed: 0,
        manage items 5
IPv6 Address                              Hardware Addr        Interface       Port
State
2002:ca60:c801:1:250:baff:fef2:a4f4       00-50-ba-f2-a4-f4                    Vlan1
Ethernet1/1/2       reachable
3ffe:3240:800d:1::100                     00-03-0f-01-27-86                    Vlan1
Ethernet1/1/3       reachable
3ffe:3240:800d:1::8888                    00-02-01-00-00-00                    Vlan1
Ethernet1/1/1       permanent
3ffe:3240:800d:1:250:baff:fef2:a4f4       00-50-ba-f2-a4-f4                    Vlan1
Ethernet1/1/4       reachable
3ffe:3240:800d:2::8888                    00-02-01-00-01-01                    Vlan2
Ethernet1/1/16      permanent
3ffe:3240:800d:2:203:fff:fefe:3045        00-03-0f-fe-30-45                    Vlan2
Ethernet1/1/15      reachable
fe80::203:fff:fe01:2786                   00-03-0f-01-27-86                    Vlan1
Ethernet1/1/5       reachable
fe80::203:fff:fefe:3045                   00-03-0f-fe-30-45                    Vlan2
Ethernet1/1/17      reachable
fe80::20c:ceff:fe13:eac1                  00-0c-ce-13-ea-c1                    Vlan12
Ethernet1/1/20      reachable
fe80::250:baff:fef2:a4f4                  00-50-ba-f2-a4-f4                    Vlan1
Ethernet1/1/6       reachable

IPv6 neighbour table: 11 entries
```

| 显示内容 | 解释 |
|---|---|

| | |
|---|---|
| IPv6 Address | 邻居 IPv6 地址 |
| Hardware Addr | 邻居 MAC 地址 |
| Interface | 出接口名 |
| Port | 出端口名 |
| State | 邻居状态(reachable、statle、delay、probe、permanent、incomplete、unkown) |

## 4.3.40 show ipv6 traffic

**命令：show ipv6 traffic**

**功能：**显示 IPv6 转发数据包统计信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**

**举例：**

```
Switch#show ipv6 traffic
IP statistics:
  Rcvd:  90 total, 17 local destination
         0 header errors, 0 address errors
         0 unknown protocol, 13 discards
  Frags: 0 reassembled, 0 timeouts
         0 fragment rcvd, 0 fragment dropped
         0 fragmented, 0 couldn't fragment, 0 fragment sent
  Sent:  110 generated, 0 forwarded
         0 dropped, 0 no route
ICMP statistics:
  Rcvd:  0 total 0 errors 0 time exceeded
         0 redirects, 0 unreachable, 0 echo, 0 echo replies
```

| 显示内容 | 解释 |
|---|---|
| IP statistics | IPv6 数据报统计 |
| Rcvd: 90 total, 17 local destination0 header errors, 0 address errors0 unknown protocol, 13 discards | IPv6 收包统计 |
| Frags: 0 reassembled, 0 timeouts | IPv6 分片统计 |

| | |
|---|---|
| 0 fragment rcvd, 0 fragment dropped0 fragmented, 0 couldn't fragment, 0 fragment sent | |
| Sent: 110 generated, 0 forwarded<br>0 dropped, 0 no route | IPv6 发包统计 |

## 4.3.41 show ipv6 redirect

**命令：show ipv6 redirect**

**功能：** 显示 IPv6 重定向开关状态。

**参数：** 无。

**缺省情况：** 无。

**命令模式：** 特权和配置模式。

**使用指南：** 本命令可用于了解系统中 IPv6 路由重定向功能是否启用。

**举例：**

Switch#show ipv6 redirect

ipv6 redirect is disabled

## 4.3.42 show ipv6 tunnel

**命令：show ipv6 tunnel [<tnl-id>]**

**功能：** 显示隧道信息。

**参数：** ***<tnl-id>*** 参数为隧道号。

**缺省情况：** 无。

**命令模式：** 特权和配置模式。

**使用指南：** 如果不加隧道号，显示所有隧道的信息，如果带有隧道号将显示指定隧道的详细信息。

**举例：**

Switch#show ipv6 tunnel

name mode source destination nexthop

tunnel3 6to4 178.1.1.1

| 显示内容 | 解释 |
|---|---|
| Name | 隧道名 |
| mode | 隧道类型 |
| source | 隧道源 ipv4 地址 |
| destination | 隧道目的 ipv4 地址 |
| nexthop | 隧道下一跳（只适用于 ISATAP 隧道） |

## 4.3.43 tunnel source

**命令：tunnel source {<ipaddress> | <ipv6address> | <interface-name>}**

**no tunnel source**

**功能：** 配置隧道源点的IPv4/IPv6地址。

**参数：** ***<ipaddress>*** 为隧道源点的IPv4地址， ***<ipaddress>*** 必须是单播地址；***<ipv6address>***为隧道源点的IPv6地址； ***<interface-name>*** 表示隧道源地址取自接口***<interface-name>***的主IPv4地址。

**命令模式：** 隧道配置模式。

**缺省情况：** 隧道缺省没有配置源点的IPv4/IPv6地址，也没有配置隧道源接口名。

**使用指南：** 配置任何类型的隧道都必须配置源点的IPv4/IPv6地址或指定一个借用隧道源地址的接口名。

**举例：** 配置隧道源点IPv4地址为202.89.176.6。

Switch(Config-if-Tunnel1)#tunnel source 202.89.176.6

## 4.3.44 tunnel destination

**命令：tunnel destination <ipaddress | ipv6address>**

**no tunnel destination**

**功能：** 配置隧道终点的IPv4/IPv6地址。

**参数：** ***<ipaddress>*** 为隧道终点的IPv4地址， ***<ipv6address>*** 为隧道终点的IPv6地址。

**命令模式：** 隧道配置模式。

**缺省情况：** 隧道缺省没有配置终点的IPv4/IPv6地址。

**使用指南：** 该命令仅适用于手工隧道，用于配置手工隧道的终点IPv4/IPv6地址。

**举例：** 配置隧道终点IPv4地址为203.78.120.5。

Switch(Config-if-Tunnel1)#tunnel destination 203.78.120.5

## 4.3.45 tunnel nexthop

**命令：tunnel nexthop <ipaddress>**

**no tunnel nexthop**

**功能：** 配置隧道下一跳的IPv4地址。

**参数：** ***<ipaddress>*** 为隧道下一跳的IPv4地址。

**命令模式：** 隧道配置模式。

**缺省情况：** 隧道缺省没有配置下一跳IPv4地址。

**使用指南：** 该命令仅适用于ISATAP隧道，其它类型的隧道不会检查nexthop的配置。注意，ISATAP隧道的下一跳IPv4地址必须和隧道源的IPv4地址在同一网段。

**举例：** 配置ISATAP隧道的下一跳ipv4地址为178.99.156.8。

Switch(Config-if-Tunnel1)#tunnel source 178.99.156.7

Switch(Config-if-Tunnel1)#tunnel nexthop 178.99.156.8

Switch(Config-if-Tunnel1)#tunnel mode ipv6ip isatap

### 4.3.46 tunnel 6to4-relay

本型号交换机不支持此命令。

### 4.3.47 tunnel mode

**命令：tunnel mode [[gre] [ip | ipv6]| ipv6ip [6to4 | isatap]]**

**no tunnel mode**

**功能：** 配置隧道模式。

**参数：** gre 为 GRE 隧道。Ip 表示通过 ip 头封装，ipv6 表示通过 ipv6 头封装；ipv6ip 表明是配置隧道。Ipv6ip 6to4 表明是 6to4 隧道，ipv6ip isatap 表明是 ISATAP 隧道。

**命令模式：** 隧道配置模式。

**缺省情况：** 无。

**使用指南：** 在配置隧道模式的时候，只指定 ipv6ip 表明是配置隧道。Ipv6ip 6to4 表明是 6to4 隧道，ipv6ip isatap 表明是 ISATAP 隧道。

**举例：** 配置隧道模式

Switch(Config-if-Tunnel1)#tunnel mode ipv6ip

Switch(Config-if-Tunnel1)#tunnel mode ipv6ip 6to4

Switch(Config-if-Tunnel1)#tunnel mode ipv6ip isatap

## 4.4 IP 转发

### 4.4.1 ip fib optimize

**命令：ip fib optimize**

**no ip fib optimize**

**功能：**配置交换机使用优化 IP 路由聚合算法；本命令的 no 操作为交换机不使用优化 IP 路由聚合算法。

**缺省情况：**出厂时不使用优化 IP 路由聚合算法。

**命令模式：**全局配置模式。

**使用指南：**该命令是为了实现对聚合算法的优化，优化方法为：如果路由表不具备缺省路由，根据被引用最多的下一跳构造一个虚拟缺省路由，以简化聚合的结果。使用该方式的好处是更有效的简化了聚合的结果；缺点是虽然降低了（通过将虚拟缺省路由加入芯片网段路由表项）本交换机 CPU 负载，但是可能会为下一跳交换机引入不必要的数据流（实际上为将部分本交换机 CPU 负载转给了下一跳交换机）。

**举例：**配置交换机不使用优化 IP 路由聚合算法。

Switch(config)#no ip fib optimize

### 4.4.2 l3-miss software forward

本型号交换机不支持此命令。

## 4.5 URPF

### 4.5.1 debug urpf

**命令：debug urpf**

**no debug urpf 功能：** 打开 URPF 调试功能，在 URPF 规则安装失败时提示错误。

**命令模式：** 特权模式。

**参数：** 无。

**使用指南：** 无。

**举例：**

Switch#debug urpf

### 4.5.2 ip urpf enable

**命令：ip urpf enable {loose | strict}**

**no ip urpf enable**

**功能：** 使能端口上的 URPF 功能。

**参数：** loose：松散类型；

strict：严格类型；

**命令模式：** 端口配置模式。

**缺省情况：** 端口不打开 URPF 功能。

**使用指南：** 要指明是严格或者松散模式。

**举例：**

Switch(config)#interface ethernet 1/1/4

Switch(Config-If-Ethernet1/1/4)#ip urpf enable strict

Switch(Config-If-Ethernet1/1/4)#interface ethernet 1/1/5

Switch(Config-If-Ethernet1/1/5)#ip urpf enable loose

### 4.5.3 show urpf rule ipv4 num

本型号交换机不支持此命令。

## 4.5.4 show urpf rule ipv6 num

本型号交换机不支持此命令。

## 4.5.5 show urpf rule ipv4

本型号交换机不支持此命令。

## 4.5.6 show urpf rule ipv6

本型号交换机不支持此命令。

## 4.5.7 show urpf

**命令：show urpf**

**功能：**显示哪些端口启动了 URPF。

**命令模式：**特权和配置模式。

**参数：**无。

**使用指南：**无。

**举例：**

Switch#show urpf

## 4.5.8 urpf enable

**命令：urpf enable**

**no urpf enable**

**功能：**启动全局 URPF 功能。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**系统不启动 URPF 协议模块。

**使用指南：**无。

**举例：**

Switch(config)#urpf enable

## 4.5.9 ip urpf allow-default-route

本型号交换机不支持此命令。

# 4.6 ARP

## 4.6.1 arp

**命令：arp <ip_address> <mac_address> {interface [ethernet] <portName>}**

**no arp <ip_address>**

**功能：**配置静态 ARP 表项；本命令的 no 操作为删除指定 IP 地址的 ARP 表项。

**参数：*<ip_address>***为 IP 地址，与接口在同一字段；***<mac_address>***为 MAC 地址；**ethernet** 为以太网端口；***<portName>***为二层端口名称。

**缺省情况：**缺省没有静态 ARP 表项。

**命令模式：**VLAN 接口配置模式。

**使用指南：**在交换机上可以配置静态 ARP 表项。

**举例：**在接口 vlan 1 配置静态 ARP。

Switch(Config-if-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34 interface eth 1/1/2

## 4.6.2 clear arp-cache

**命令：clear arp-cache**

**功能：**清除交换机学习到的动态 ARP。

**命令模式：**特权用户配置模式。

**举例：**

Switch#clear arp-cache

## 4.6.3 clear arp traffic

**命令：clear arp traffic**

**功能：**清除交换机 ARP 报文统计信息。对于机箱交换机，本命令只清除当前板卡的 ARP 报文统计信息。

**命令模式：**特权用户配置模式

**举例：**

Switch#clear arp traffic

## 4.6.4 clear ip arp dynamic

本型号交换机不支持此命令。

## 4.6.5 clear ipv6 nd dynamic

本型号交换机不支持此命令。

## 4.6.6 debug arp

**命令：debug arp {receive|send|state}**

**no debug arp {receive|send|state}**

**功能：**打开 ARP 调试开关；本命令的 no 操作为关闭该调试功能。

**参数：**receive 交换机接收 ARP 数据包调试开关；send 交换机发送 ARP 数据包调试开关；state 交换机 ARP 状态变化调试开关。

**缺省情况：**缺省 ARP 调试功能是关闭的。

**命令模式：**特权用户配置模式。

**使用指南：**显示接收或发送的 ARP 数据包的内容，包括：类型、源地址、目的地址。

**举例：**打开 ARP RECEIVE 调试开关。

Switch#debug arp receive

%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

e%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

## 4.6.7 ip proxy-arp

**命令：ip proxy-arp**

**no ip proxy-arp**

**功能：** 打开 VLAN 接口代理 ARP 的功能；本命令的 no 操作为关闭代理 ARP 的功能。

**缺省情况：** 缺省代理 ARP 功能是关闭的。

**命令模式：** VLAN 接口配置模式。

**使用指南：** 当交换机的三层接口收到某 ARP 请求，该请求的 IP 地址与三层接口地址在一个 IP 网段，但却不在同一物理网络中，此时该三层接口若启动了代理 ARP 的功能，三层接口会将自己的 MAC 地址作为 ARP 的回应，然后将收到的实际数据报文进行转发。启动该项功能可以使因为物理网络分离但属于同一 IP 网段的机器忽视物理网络分离的事实，经过具有代理 ARP 接口的转发像处在一个物理网络中。代理 ARP 在回应 ARP 请求之前，需要查找路由表，以确定目的网络是否可达，只有目的网络可达的 ARP 请求，才会回应 ARP 请求。

**举例：** 打开 VLAN 接口 1 的代理 ARP 功能。

Switch(Config-if-Vlan1)#ip proxy-ar

## 4.6.8 l3 hashselect

本型号交换机不支持此命令。

## 4.6.9 show arp

**命令：show arp [<ipaddress>][<vlan-id>][<hw-addr>][type {static|dynamic}][count][vrf word]**

**功能：**显示 ARP 映射表。

**参数：*<ipaddress>***为显示指定 IP 地址的表项；***<vlan-id>***为显示指定 VLAN 标识的表项；***<hw-addr>***为显示指定 MAC 地址的表项；**static** 为显示静态 ARP 表项；**dynamic** 为显示动态 ARP 表项；**count** 为显示 ARP 表项数量信息；**word** 为要显示的指定 vrf 的名称。

**命令模式：**特权和配置模式。

**使用指南：**显示当前 ARP 映射表的内容，如：IP 地址，硬件地址，硬件类型，接口名等。

**举例：**

Switch#show arp

ARP Unicast Items: 7, Valid: 7, Matched: 7, Verifying: 0, Incomplete: 0, Failed: 0, None: 0

| Address | Hardware Addr | Interface | Port | Flag |
|---|---|---|---|---|
| 50.1.1.6 | 00-0a-eb-51-51-38 | Vlan50 | Ethernet1/1/11 | Dynamic |
| 50.1.1.9 | 00-00-00-00-00-09 | Vlan50 | Ethernet1/1/1 | Static |
| 150.1.1.2 | 00-00-58-fc-48-9f | Vlan150 | Ethernet1/1/4 | Dynamic |

| 显示信息 | 解释 |
|---|---|
| Total arp items | ARP 表项的总数； |
| Valid | 符合过滤规则的属于合法状态的 Arp 表项数量； |
| Matched | 符合过滤规则的 Arp 表项数量； |
| Verifying | 处于重验证 Arp 合法性状态的 Arp 表项数量； |
| InCompleted | 发了 Arp request，但未接收到 Arp reply 的 Arp 表项数量； |
| Failed | 处于失效状态的 Arp 表项数量； |
| None | 处于初始创建状态的 Arp 表项数量； |
| Address | Arp 表项 IP 地址； |
| Hardware Address | Arp 表项硬件地址； |
| Interface | Arp 表项对应的三层接口； |
| Port | Arp 表项对应的物理（二层）端口； |
| Flag | Arp 表项是动态还是静态说明。 |

## 4.6.10 show arp traffic

**命令：show arp traffic**

**功能：**显示交换机 ARP 报文统计信息。对于机箱交换机，本命令只统计当前板卡的 ARP 报文收发信息。

**命令模式：**特权和配置模式。

**使用指南：**显示 ARP 报文的接收、发送统计信息。

**举例：**

```
Switch#show arp traffic
ARP statistics:
  Rcvd:   10 request, 5 response
  Sent:    5 request, 10 response
```

# 4.7 l3 station movement

## 4.7.1 l3-station-move

本型号交换机不支持此命令。

# 4.8 防 ARP 扫描

## 4.8.1 anti-arpscan enable [ip|port]

**命令：anti-arpscan enable [ip|port]**

**no anti-arpscan enable [ip|port]**

**功能：**全局启动防 ARP 扫描功能；no 命令全局关闭防 ARP 扫描功能。

**参数：**无。

**缺省情况：**缺省时为同时开启或关闭基于 ip 及端口的防 arp 扫描功能。

**命令模式：**全局配置模式。

**使用指南：**通过 telnet 等手段远程管理交换机时，必须在启动防 ARP 扫描功能之前将上联端口设置为超级信任端口，以防止此端口收到较多的 ARP 报文而被关闭。在关闭防 ARP 扫描功能之后此端口的属性会恢复为默认值的非信任端口。

**举例：**在交换机上启动防 ARP 扫描功能。

```
Switch(config)#anti-arpscan enable ip
```

## 4.8.2 anti-arpscan port-based threshold

**命令：anti-arpscan port-based threshold <*threshold-value*>**

**no anti-arpscan port-based threshold**

**功能：**设置基于端口的防 ARP 扫描的接收 ARP 报文的阈值，如果接收的 ARP 报文的速率超过此设定值，则关闭此端口。单位为个/秒。no 命令恢复为默认值，即 10 个/秒。

**参数：**速率阈值，有效范围为 2-200。

**缺省情况：**10 个/秒。

**命令模式：**全局配置模式。

**使用指南：**基于端口的防 ARP 扫描的阈值应该比基于 IP 的防 ARP 扫描的阈值大，否则基于 IP 的防 ARP 扫描将不起作用。

**举例：**在交换机上配置基于端口的防 ARP 扫描速率阈值为 10 个/秒。

Switch(config)#anti-arpscan port-based threshold 10

## 4.8.3 anti-arpscan ip-based level1|level2 threshold

**命令：anti-arpscan ip-based level1|level2 threshold <threshold-value>**

**no anti-arpscan ip-based level1|level2 threshold**

**功能：**设置基于 IP 的防 ARP 扫描的接收 ARP 报文的一级或二级阈值，一级阈值默认为 4p/s，二级默认为 8p/s。二级阈值必须大于一级阈值。

**参数：**速率阈值，有效范围为 1-200。

**缺省情况：**一级阈值默认为 4p/s，二级阈值默认为 8p/s。

**命令模式：**全局配置模式。

**使用指南：**基于端口的防 ARP 扫描的阈值应该比基于 IP 的防 ARP 扫描的阈值大，否则基于 IP 的防 ARP 扫描将不起作用。

**举例：**在交换机上配置基于 IP 的防 ARP 扫描速率阈值为 6 个/秒。

Switch(Config)# anti-arpscan ip-based level1 threshold 6

## 4.8.4 anti-arpscan trust

**命令：anti-arpscan trust { port | supertrust-port | iptrust-port }**

**no anti-arpscan trust {port | supertrust-port | iptrust-port}**

**功能：**配置为信任端口或超级信任端口；no 命令恢复为非信任端口。

**参数：**无。

**缺省情况：**缺省全部为非信任端口。

**命令模式：**端口配置模式。

**使用指南：**如果某端口配置为信任端口，则防 ARP 扫描功能将不对此端口作处理，即使接收到的 ARP 报文速率超过设定的阈值，也不关闭此端口，但对此端口下的非信任 IP 仍然检测。如果配置为超级信任端口，则既不对端口作处理，也不对此端口下的任何 IP 作处理。如果端口已经被防 ARP 扫描关闭，则配置为信任端口后立即打开此端口。如果配置为 IP 信任端口，则不检测此端口下的 IP，紧对端口做处理；如果端口下已有 IP 被禁，则配置为 IP 信任端口后被禁 IP 立即恢复。

通过 telnet 等手段远程管理交换机时，必须在启动防 ARP 扫描功能之前将上联端口设置为超级信任端口，以防止此端口收到较多的 ARP 报文而被关闭。在关闭防 ARP 扫描功能之后此端口的属性会恢复为默认值的非信任端口。

**举例：**将交换机的端口 ethernet 1/1/5 配置为信任端口。

Switch(config)#interface ethernet1/1/5

Switch(Config-if-ethernet 1/1/5)#anti-arpscan trust port

## 4.8.5 anti-arpscan trust ip

**命令：anti-arpscan trust ip <*ip-address*> [<*netmask*>]**

**no anti-arpscan trust ip <*ip-address*> [<*netmask*>]**

**功能：**配置信任 IP；no 命令恢复为非信任 IP。

**参数：<*ip-address*>**：要配置的信任 IP 地址；**<*netmask*>**：IP 的子网掩码。

**缺省情况：**缺省所有 IP 都为非信任 IP。掩码缺省为 255.255.255.255。

**命令模式：**全局配置模式。

**使用指南：**如果某 IP 被配置为信任 IP，则防 ARP 扫描功能将不对此 IP 作处理，即使从其收到的 ARP 报文速率超过了设定的阈值，也不禁掉此 IP。如果此 IP 已经被防 ARP 扫描禁掉，则立即恢复其流量。

**举例：**将 192.168.1.0/24 配置为信任 IP。

Switch(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0

## 4.8.6 anti-arpscan recovery enable

**命令：anti-arpscan recovery enable**

**no anti-arpscan recovery enable**

**功能：**启动自动恢复功能，no 命令取消自动恢复功能。

**参数：**无。

**缺省情况：**关闭自动恢复功能。

**命令模式：**全局配置模式。

**使用指南：**如果希望端口被关闭一段时间后，自动恢复为正常状态，则可配置此功能。

**举例：**

在交换机上启动自动恢复功能。

Switch(config)#anti-arpscan recovery enable

## 4.8.7 anti-arpscan recovery time

**命令：anti-arpscan recovery time <*seconds*>**

**no anti-arpscan recovery time**

**功能：**配置自动恢复时间；no 命令恢复自动恢复时间为默认值。

**参数：**自动恢复时间值，单位为秒。有效范围为 5-86400 秒。

**缺省情况：**300 秒。

**命令模式：**全局配置模式。

**使用指南：**必须先启动自动恢复功能。

**举例：**设置自动恢复时间为 3600 秒。

Switch(config)#anti-arpscan recovery time 3600

## 4.8.8 anti-arpscan log enable

**命令：anti-arpscan log enable**

**no anti-arpscan log enable**

**功能：**启动防 ARP 扫描的日志功能；no 命令关闭防 ARP 扫描的日志功能。

**参数：**无。

**缺省情况：**关闭防 ARP 扫描的日志功能。

**命令模式：**全局配置模式。

**使用指南：**打开防 ARP 扫描的日志功能后，可以通过日志信息查看端口被防 ARP 扫描关闭及自动恢复、IP 被禁掉及被恢复的详细信息。日志的等级为 Warning。

**举例：**在交换机上启动防 ARP 扫描的日志功能。

Switch(config)#anti-arpscan log enable

## 4.8.9 anti-arpscan trap enable [level1|level2 ]

**命令：anti-arpscan trap enable [level1|level2 ]**

**no anti-arpscan trap enable [level1|level2 ]**

**功能：**启动防 ARP 扫描的 SNMP Trap 功能；no 命令关闭防 ARP 扫描的 SNMP Trap 功能。

**参数：**无。

**缺省情况：**缺省时为同时关闭或开启一级限速及二级隔离 trap 功能。

**命令模式：**全局配置模式。

**使用指南：**打开防 ARP 扫描的 SNMP Trap 功能后，在端口被防 ARP 扫描关闭或恢复，IP 被禁掉或恢复时，可通过网管软件收到 Trap 消息。

**举例：**在交换机上启动防 ARP 扫描的 SNMP Trap 功能。

Switch(config)#anti-arpscan trap enable level1

## 4.8.10 anti-arpscan ip-based level2 action {isolate | discard-ARP}

**命令：anti-arpscan ip-based level2 action {isolate | discard-ARP}**

**功能：**超过二级阀值后的处理动作可配置为 IP 业务隔离和丢弃 ARP 报文不送 CPU。

**参数：**isolate—该 IP 的业务被隔离，discard-ARP ---丢弃该 IP 上来的 ARP 报文，但保留其原 ARP 表项。默认动作为 discard-ARP。

**命令模式：**全局配置模式。

**使用指南：**配置超过二级阈值保护动作为 diacard-arp，当某端口收到的以某一 IP 为源的 ARP 报文的速率大于二级阈值时，将此 IP 的 ARP 报文丢弃，IP 数据正常转发;配置超过二级阈值保护动作为 isloate，当某端口收到的以某一 IP 为源的 ARP 报文的速率大于二级阈值时，将此 IP 的 ARP 报文和 IP 数据都被丢弃。

**举例：**Switch(config)#anti-arpscan ip-based level2 action isolate

## 4.8.11 anti-arpscan FFP max-num <num>

**命令：anti-arpscan FFP max-num <num>**

**功能：**防 ARP 扫描功能可占用的 FFP 表项最大数量。

**参数：**<1-1024>,默认 200 个可用表项资源。

**命令模式：**全局配置模式。

**使用指南：**当端口收到的 arp 报文的源大于 max-num，且每个源 ip 的 arp 速率超过一级或者二级阈值，FFP 资源耗尽后，会提示资源不足，可适当将 ffp 表项的最大值调高。

**举例：**Switch(config)#anti-arpscan ffp max-num 1024

## 4.8.12 anti-arpscan ip-based arp-to-cpu speed<pps>

**命令：anti-arpscan ip-based arp-to-cpu speed<pps>**

**no anti-arpscan ip-based arp-to-cpu speed**

**功能：**配置一级阀值超限后 ARP 送 CPU 的速率。

**参数：**<1-20>,默认值为 1p/s。

**命令模式：**全局配置模式。

**使用指南：**用于配置 arp 速率超过一级限速后 arp 报文上 cpu 的速率，可以实时修改。

**举例：**Switch(config)#anti-arpscan ip-based arp-to-cpu speed 2

## 4.8.13 show anti-arpscan

**命令：show anti-arpscan [trust {ip | port | supertrust-port | iptrust-port} |prohibited {ip | port}]**

**功能：**显示防 ARP 扫描功能运行信息。

**参数：**无。

**缺省情况：**显示所有端口是否是信任端口，是否被关闭，如果被关闭了，则还显示被关闭了多长时间。显示所有的信任 IP，所有被禁掉的 IP。

**命令模式：**特权模式、配置模式。

**使用指南：**若只查看配置的信任端口则使用命令 show anti-arpscan trust port，如此类推。

**举例：**在交换机上启动防 ARP 扫描功能后查看运行情况。

Switch(config)#show anti-arpscan

## 4.8.14 show anti-arpscan ip-based attack-list [history]

**命令：show anti-arpscan ip-based attack-list [history]**

**功能：**显示防 ARP 扫描攻击源信息或历史攻击源信息。

**参数：**无。

**缺省情况：**显示防 ARP 扫描攻击源信息。

**命令模式：**特权模式、配置模式。

**使用指南：**

**1)** 显示防 arp 扫描攻击源信息，包括源 ip，对应端口，所属 vlan，速率，及状态。超过一级阈值的 state 为 Speed-Limit，超过二级阈值时，action 为 discard-arp 则 state 为 Discard-Arp，action 为 isolate 则 state 为 Isolate。

**2)** 显示防 arp 扫描历史攻击源信息，包括源 ip，对应端口，所属 vlan，攻击次数，最后一次攻击的状态，及攻击持续时间。超过一级阈值的 state 为 Speed-Limit，超过二级阈值时，action 为 discard-arp 则 state 为 Discard-Arp，action 为 isolate 则 state 为 Isolate。

**举例：**

```
Switch#show anti-arpscan ip-based attack-list
SIP-Addr                Port                VLAN        Speed       ARP-Count
State
30.1.1.6                Ethernet2/48        26          4           57
Speed-Limit
30.1.1.4                Ethernet2/48        26          4           56
Speed-Limit
Switch#show anti-arpscan ip-based attack-list history
SIP-Addr                Port                VLAN        Attack-Times State
Keep-Time
30.1.1.6                Ethernet2/48        26          6           Speed-Limit
0 weeks,0 days,0 hours,8 minutes,46 seconds
30.1.1.4                Ethernet2/48        26          3           Speed-Limit
0 weeks,0 days,0 hours,0 minutes,28 seconds
```

## 4.8.15 show anti-arpscan ip-based running-config

**命令：show anti-arpscan ip-based running-config**

**功能：**显示防 arp 扫描的当前配置。

**参数：**无。

**命令模式：** 特权模式、配置模式。

**使用指南：**显示当前防 arp 扫描的相关配置，如果一级、二级阈值，超过二级阈值后采用的动作，arp 超过一级阈值后上 cpu 的速率，ffp 表项大小等。

**举例：**

```
switch(config)#show anti-arpscan ip-based running-config
level1 thrshould:     4
level2 thrshould:     8
level2 action:        Discard-Arp
arp-to-cpu speed:     1
ffp-max:              1024
ffp-used:             0
ip based thrshould:   8
recovery-time:        300
actIp-num:            0
```

## 4.8.16 clear anti-arpscan speed-limit< IP Address>

**命令：clear anti-arpscan speed-limit< IP Address>**

**功能：**手动清除对特定主机的 ARP 限速。

**参数：**特定主机的 IP 地址。

**命令模式：**特权模式。

**使用指南：**当 arp 报文超过一级限速时，可以通过该命令清除表项，能够通过打开 debug 命令 debug anti-arpscan ip 查看表项被删除。

**举例：**Switch#clear anti-arpscan speed-limit 30.1.1.6

## 4.8.17 clear anti-arpscan ip-isolate <IP Address>

**命令：clear anti-arpscan ip-isolate <IP Address>**

**功能：**手动清除对特定主机的 IP 业务隔离。

**参数：**特定主机的 IP 地址。

**命令模式：**特权模式。

**使用指南：**当 arp 报文超过二级限速时，可以通过该命令清除表项，能够通过打开 debug 命令 debug anti-arpscan ip 查看表项被删除。

**举例：**Switch#clear anti-arpscan ip-isolate 30.1.1.6

## 4.8.18 clear anti-arpscan attack-list {ip <IP Address>| all}

**命令：clear anti-arpscan attack-list {ip <IP Address> | all}**

**功能：**手动清除对特定主机或所有主机的限制。

**参数：*<IP Address>*：**特定主机的 IP 地址。

**命令模式：**特权模式。

**使用指南：**当 arp 报文超过一级或二级限速时，可以通过该命令清除表项，能够通过打开 debug 命令 debug anti-arpscan ip 查看表项被删除。

**举例：**Switch#clear anti-arpscan attack-list ip 30.1.1.6

## 4.8.19 clear anti-arpscan attack-history-list {ip <IP Address>| all}

**命令：clear anti-arpscan attack-history-list {ip <IP Address> | all}**

**功能：**手动清除特定主机或所有主机的攻击历史信息。

**参数：*<IP Address>*：**特定主机的 IP 地址。

**命令模式：**特权模式。

**使用指南：**可以通过该命令清除攻击的历史信息，可以通过命令 show anti-arpscan ip-based attack-list history 查看表项被删除。

**举例：**Switch#clear anti-arpscan attack-history-list ip 30.1.1.6

## 4.8.20 debug anti-arpscan

**命令：debug anti-arpscan [port | ip]**

**no debug anti-arpscan [port | ip]**

**功能：**打开防 ARP 扫描的调试开关；no 命令关闭防 ARP 扫描的调试开关。

**参数：**无。

**缺省情况：**关闭防 ARP 扫描的调试开关。

**命令模式：**特权模式。

**使用指南：**打开防 ARP 扫描的调试开关后，在端口被防 ARP 扫描关闭，或端口自动恢复，IP 被禁掉或恢复时，可查看相应的调试信息。也可单独打开基于端口或基于 IP 的调试开关。

**举例：**在交换机上打开防 ARP 扫描的调试开关。

Switch#debug anti-arpscan

# 4.9 ARP 绑定

## 4.9.1 ip arp-security updateprotect

**命令：ip arp-security updateprotect**

**no ip arp-security updateprotect**

**功能：**禁止 IPv4 版本的 ARP 更新功能，no 命令操作重新启动 ARP 更新功能。

**参数：**无

**缺省情况：**学习 ARP 并正常更新。

**命令模式：**全局配置模式/接口配置。

**使用指南:** 本命令用于防止 ARP 的 request 和 reply 报文对交换机进行 ARP 表的更新操作。不过即使在不转换动态 ARP 的情况下，如果交换机一直收到合法的 ARP 请求/应答报文则此动态表项不会超时，当收到的 ARP 请求或应答包与保存不符才予以丢弃。命令全局优先。此功能与 l3 station move 功能互斥，l3 station move 功能会自动更新 ARP 的 MAC 和端口的对应关系（此功能默认是开启的），所以使能 ARP 安全更新功能的同时需要关闭 l3 station move 功能。

**举例：**

Switch(Config-if-Vlan1)#ip arp-security updateprotect

Switch(config)#ip arp-security updateprotect

## 4.9.2 ip arp-security learnprotect

**命令：ip arp-security learnprotect**

**no ip arp-security learnprotect**

**功能：**禁止 IPv4 版本的 ARP 自动学习功能，no 命令操作重新启动 ARP 自动学习功能。

**参数：**无。

**缺省情况：**学习 ARP 并正常更新。

**命令模式：**全局配置模式/接口配置。

**使用指南:** 本命令用于在防止 ARP 的自动学习与更新。与 ip arp-security updateprotect 不同的是，此命令开启后，无论是否合法的 ARP 表项，即使一直发送请求/应答报文，一样会超时。建议与转换操作搭配使用，命令全局优先。

**举例：**

Switch(Config-if-Vlan1)#ip arp-security learnprotect

Switch(config)#ip arp-security learnprotect

## 4.9.3 ip arp-security convert

**命令：ip arp-security convert**

**功能：**将所有动态 ARP 转变为静态 ARP。

**参数：**无。

**命令模式：**全局配置模式/接口配置。

**使用指南:** 本命令用于将动态 ARP 表项转换为静态的 ARP 表项。配合关闭学习功能达到防止 ARP 绑定的作用。执行之后，该命令就无效了。

**举例：**

Switch(Config-if-Vlan1)#ip arp-security convert

Switch(config)# ip arp-security convert

## 4.9.4 clear ip arp dynamic

**命令：clear ip arp dynamic**

**功能：**清除接口上所有的动态 ARP。

**参数：**无。

**命令模式：**接口配置。

**使用指南：**本命令用于在使用 ARP 绑定功能之前的动态表项清理工作。执行之后，该命令就无效了。

**举例：**

Switch(Config-if-Vlan1)#clear ip arp dynamic

# 4.10 ARP GUARD

## 4.10.1 arp-guard ip

**命令：arp-guard ip <addr>**

**no arp-guard ip <addr>**

**功能：**添加 ARP GUARD 地址，no 命令操作删除 ARP GUARD 地址。

**参数：<addr>**：受到保护的 IP 地址，点分十进制形式。

**缺省情况：**默认没有 ARP GUARD 地址。

**命令模式：**端口配置模式。

**使用指南：** 配置 ARP GUARD 地址之后，从配置了 ARP GUARD 的端口接收到的 ARP 报文将被进行过滤，如果 ARP 报文的源 IP 地址匹配该端口上所配置 ARP GUARD 地址，就认为是 ARP 欺骗攻击报文，这样的 ARP 报文将直接被丢弃，不会送交换机 CPU，也不会被转发，每个端口下最多可以配置 16 个 ARP GUARD 地址。

**举例：**

在端口 Ethernet1/1/1 启动配置 ARP GUARD 地址 100.1.1.1。

switch(config)#interface ethernet1/1/1

switch(Config-If-Ethernet1/1/1)#arp-guard ip 100.1.1.1

在端口 Ethernet1/1/1 删除 ARP GUARD 地址 100.1.1.1。

switch(config)#interface ethernet1/1/1

switch(Config-If-Ethernet1/1/1)#no arp-guard ip 100.1.1.1

# 4.11 Arp local proxy

## 4.11.1 ip local proxy-arp

**命令：ip local proxy-arp**

**no ip local proxy-arp**

**功能：**打开/关闭指定接口的 local arp proxy 功能。

**参数：**无。

**缺省情况：**所有的接口默认不启动此功能。

**命令模式：**VLAN 接口配置模式。

**使用指南：**打开接口的 local arp proxy 功能后，对于从本接口收到的 arp request 报文，如果 arp request 报文中的目的 ip 和源 ip 都与该接口的 ip 处于同一网段，则交换机会回应 arp reply 报文，将交换机的 mac 填充到 arp REPLY 报文中。用这种方式来引导所有的 ip 流量通过交换机进行三层转发。

**举例：**打开 Vlan1 接口的 local arp proxy 功能。

```
Switch(Config-if-Vlan1)#ip local proxy-arp
```

# 4.12 免费 ARP 发送

## 4.12.1 ip gratuitous-arp

**命令：ip gratuitous-arp [<interval-time>]**

**no ip gratuitous-arp**

**功能：**使能免费 ARP 发送功能，并设置发送免费 ARP 报文的间隔时间；本命令的 no 命令为取消使能免费 ARP 发送功能。

**参数：*<interval-time>*** 为发送免费 ARP 报文的间隔时间；范围为 5-1200 秒，默认为 300 秒。

**命令模式：**全局配置模式和接口配置模式。

**缺省情况：**不使能免费 ARP 发送功能。

**使用指南：**在全局配置模式下使能免费 ARP 发送功能时，将使能系统中所有存在的三层接口的免费 ARP 发送功能。在接口配置模式下使能免费 ARP 发送功能时，只是使能当前接口的免费 ARP 发送功能。配置的免费 ARP 发送间隔时间以接口配置模式下配置的间隔时间为准。如果全局配置模式下和接口配置模式下都配置了免费 ARP 发送功能的发送间隔时间时，使用接口配置模式下配置的间隔时间。

**举例：**

1) 全局配置模式下使能免费 ARP 发送功能，并设置免费 ARP 发送间隔时间为 400 秒。

```
Switch>enable
Switch#config
Switch(config)#ip gratuitous-arp 400
```

2) 接口配置模式下使能接口 interface vlan 10 的免费 ARP 发送功能，并设置免费 ARP 发送间隔时间为 350 秒。

Switch(config)#interface vlan 10

Switch(Config-if-Vlan10)#ip gratuitous-arp 350

## 4.12.2 show ip gratuitous-arp

**命令：show ip gratuitous-arp [interface vlan <vlan-id>]**

**功能：**显示免费 ARP 发送功能的配置信息。

**参数：*<vlan-id>*：**为指定的 VLAN 号。***<vlan-id>***的取值范围为 1 ~ 4094。

**命令模式：**各种配置模式。

**使用指南：**在任意命令模式下，输入命令 **show ip gratuitous-arp**，则显示全局配置模式下和接口配置模式下的免费 ARP 发送功能配置信息。如果输入命令 **show ip gratuitous-arp interface vlan *<vlan-id>***，则显示指定接口的免费 ARP 发送功能配置信息。

**举例：**

1) 显示全局配置模式下和接口配置模式下的免费 ARP 发送功能配置信息。

Switch#show ip gratuitous-arp

Gratuitous ARP send is Global enabled, Interval-Time is 300(s)

Gratuitous ARP send enabled interface vlan information:

| Name | Interval-Time(seconds) |
|---|---|
| Vlan1 | 400 |
| Vlan10 | 350 |

2) 显示接口 interface vlan 10 的免费 ARP 发送功能配置信息。

Switch#show ip gratuitous-arp interface vlan 10

Gratuitous ARP send interface Vlan10 information:

| Name | Interval-Time(seconds) |
|---|---|
| Vlan10 | 350 |

# 4.13 Keepalive gateway

## 4.13.1 keepalive gateway

**命令：keepalive gateway <ip-address> [{<interval-seconds> | msec <interval-millisecond>} [retry-count]]**

**no keepalive gateway**

**功能：**启动 keepalive gateway 功能和配置发送 ARP 请求报文的间隔周期和判定探测失败的重试次数，no 命令为关闭该功能。

**参数：** ip-address 为探测的网关 IP 地址。

interval-seconds：发送 ARP 请求报文的间隔周期（秒），取值范围：1-32767。如果不配置，缺省是 10 秒。

interval-millisecond：发送 ARP 请求报文的间隔周期（毫秒），取值范围：160-999。

retry-count：判定探测失败的重试次数。如果不配置，缺省是 5 次。

**缺省情况：** 默认关闭 keepalive gateway 功能。

**命令模式：** 接口配置模式

**使用指南：** 只在三层交换机上才具有该命令，二层交换机上不支持，该种探测方法仅适用于点对点的拓扑模式。

**举例：**

```
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#keealive gateway  1.1.1.1 3 10
```

## 4.13.2 show ip interface

**命令：show ip interface [interface-name]**

**功能：**显示指定接口的 IPv4 运行状态。

**参数：**interface-name 为指定接口名，如果参数为空，则显示所有接口的 IPv4 运行状态。

**缺省情况：**无。

**命令模式：**特权和配置模式

**使用指南：**显示接口 IPv4 运行状态。

**举例：**

```
Switch(config)#show ip interface brief
Index      Interface              IP-Address      Protocol
3001       Vlan1                  1.1.1.2         up
9000       Loopback               127.0.0.1       up
```

## 4.13.3 show keepalive gateway

**命令：show keepalive gateway [interface-name]**

**功能：**显示指定接口的 keepalive 运行情况。

**参数：**interface-name 为指定接口名，如果参数为空，则显示所有接口的 keepalive 运行状态。

**缺省情况：**无。

**命令模式：**特权和配置模式

**使用指南：**显示接口 keepalive 运行状态。

**举例：**

```
Switch(config)#show keepalive gateway
```

interface Vlan1 gateway 1.1.1.1 time 10s retry 1 remain 4 now UP

# 4.14 DHCP

## 4.14.1 DHCP 服务器配置命令

### 4.14.1.1 bootfile

**本型号交换机不支持此命令。**

### 4.14.1.2 clear ip dhcp binding

**命令：clear ip dhcp binding {<address> | all }**

**功能：**删除某指定的 IP 地址与其硬件地址的绑定记录或所有 IP 地址与相应的硬件地址的绑定记录。

**参数：*<address>***为指定的有绑定记录的 IP 地址，点分十进制格式；**all** 通指为有绑定记录的所有的 IP 地址。

**命令模式：**特权用户配置模式。

**使用指南：**通过 **show ip dhcp binding** 命令可以查看 IP 地址与相应的 DHCP 客户机硬件地址的绑定信息，当 DHCP 服务器得知某 DHCP 客户机因为特殊原因没有使用分配的 IP 地址但规定的租期未到，DHCP 服务器不会自动解除该绑定信息，此时系统管理员可以使用本命令手工删除该 IP 地址与客户机硬件地址的自动绑定；如果使用 **all**，将删除所有自动绑定记录，这样 DHCP 地址池中的所有地址将被重新分配。

**举例：**删除所有 IP 地址与硬件地址的绑定记录。

Switch#clear ip dhcp binding all

**相关命令：show ip dhcp binding**

### 4.14.1.3 clear ip dhcp conflict

**命令：clear ip dhcp conflict {<address> | all }**

**功能：**删除在地址冲突日志中有冲突记录的地址。

**参数：*<address>***为某指定的有冲突记录的地址；**all** 通指为有冲突记录的所有地址。

**命令模式：**特权用户配置模式。

**使用指南：**通过 **show ip dhcp conflict** 命令可以查看哪些 IP 地址在使用上有冲突，使用本命令可以删除某一地址的冲突记录，如果使用 **all** 则是删除日志中所有的地址的冲突记录。在日志中删除冲突记录后，这些地址可被 DHCP 服务器重新使用。

**举例：**网络管理员查看冲突日志文件，发现文件中有冲突记录的 10.1.128.160 地址现已无人使用，将该地址的记录从地址冲突文件中删除。

Switch#clear ip dhcp conflict 10.1.128.160

**相关命令：ip dhcp conflict logging，show ip dhcp conflict**

## 4.14.1.4 clear ip dhcp server statistics

**命令：clear ip dhcp server statistics**

**功能：**删除 DHCP 服务器的统计记录，将 DHCP 服务器的计数器清零。

**参数：**无。

**命令模式：**特权用户配置模式。

**使用指南：**通过 **show ip dhcp server statistics** 命令可以查看 DHCP 服务器的计数器的统计信息，所有的统计信息都是一个累计值，使用本命令可以将计数器清零，方便统计信息的查看。

**举例：**将 DHCP 服务器的计数器清零。

Switch#clear ip dhcp server statistics

**相关命令：show ip dhcp server statistics**

## 4.14.1.5 client-identifier

**命令：client-identifier <unique-identifier>**

**no client-identifier**

**功能：**在手工绑定地址时，指定用户的唯一标识；本命令的 no 操作为删除用户标识。

**参数：*<unique-identifier>***为用户的标识，格式为连字符十六进制(xx-xx-xx-xx-xx-xx)。

**命令模式：**DHCP 地址池模式。

**使用指南：**本命令在手工绑定地址时结合命令 **host** 一起使用。当发出请求的客户机的标识恰好和指定的标识相吻合，DHCP 服务器就将 **host** 命令中定义的 IP 地址分配给客户机。

**举例：**手工绑定时，将 IP 地址 10.1.128.160 与用户唯一标识为 00-10-5a-60-af-12 的用户绑定。

Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

**相关命令：host**

## 4.14.1.6 debug ip dhcp client

**命令：debug ip dhcp client {event | packet}**

**no debug ip dhcp server {event | packet}**

**功能：**打开 DHCP 客户端的调试信息；本命令的 no 操作为关闭 DHCP 客户端的调试信息。

**缺省情况：**缺省调试开关是关闭的。

**命令模式：**特权用户配置模式。

## 4.14.1.7 debug ip dhcp relay

**命令：debug ip dhcp server packet**

**no debug ip dhcp server packet**

**功能：**打开 DHCP 中继的调试信息；本命令的 no 操作为关闭 DHCP 中继的调试信息。

**缺省情况：**缺省调试开关是关闭的。

**命令模式：**特权用户配置模式。

## 4.14.1.8 debug ip dhcp server

**命令：debug ip dhcp server { events|linkage|packets }**

**no debug ip dhcp server { events|linkage|packets }**

**功能：**打开 DHCP 服务器的调试信息；本命令的 no 操作为关闭 DHCP 服务器的调试信息。

**缺省情况：**缺省调试开关是关闭的。

**命令模式：**特权用户配置模式。

## 4.14.1.9 default-router

**命令：default-router <address1>[<address2>[…<address8>]]**

**no default-router**

**功能：**为 DHCP 客户机配置缺省网关；本命令的 no 操作为删除缺省网关。

**参数：*address1…address8*** 为 IP 地址，均为点分十进制格式。

**缺省情况：**系统没有给 DHCP 客户机配置缺省网关。

**命令模式：**DHCP 地址池模式。

**使用指南：**缺省网关的 IP 地址应与 DHCP 客户机的 IP 地址在一个子网网段内，交换机最多可支持 8 个网关地址，最先设置的网关地址优先级最高，因此 address1 优先级最高，依次 address2、address3……。

**举例：**设置 DHCP 客户机的缺省网关为 10.1.128.2 和 10.1.128.100。

Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100

## 4.14.1.10 dns-server

**命令：dns-server <address1>[<address2>[…<address8>]]**

**no dns-server**

**功能：**为 DHCP 客户机配置 DNS 服务器；本命令的 no 操作为删除 DNS 服务器。

**参数：*address1…address8*** 为 IP 地址，均为点分十进制格式。

**缺省情况：**系统没有给 DHCP 客户机配置 DNS 服务器。

**命令模式：**DHCP 地址池模式。

**使用指南：**系统最多可支持配置 8 个 DNS 服务器地址，最先设置的 DNS 服务器的地址优先级最高，因此 address1 优先级最高，依次 address2、address3……。

**举例：**设置 DHCP 客户机的 DNS 服务器的地址为 10.1.128.3。

Switch(dhcp-1-config)#dns-server 10.1.128.3

### 4.14.1.11 domain-name

**命令：domain-name <domain>**

**no domain-name**

**功能：**为 DHCP 客户机配置域名；本命令的 no 操作为删除域名。

**参数：*<domain>***为域的名称，最长不超过 255 个字符。

**命令模式：**DHCP 地址池模式。

**缺省情况：**无。

**使用指南：**为客户机指定域名。

**举例：**指定 DHCP 客户机的域名为 digitalchina.com.cn。

Switch(dhcp-1-config)#domain-name digitalchina.com.cn

### 4.14.1.12 hardware-address

**命令：hardware-address <hardware-address> [{Ethernet | IEEE802|<type-number>}]**

**no hardware-address**

**功能：** 在手工分配地址时，指定用户的硬件地址；本命令的 no 操作为删除该项配置。

**参数：*<hardware-address>***为硬件地址，十六进值表示的数值；**Ethernet | IEEE802** 为以太网协议类型，***<type-number>***为 RFC 定义的协议类型的数字表示，取值范围为 1~255，如参数 **Ethernet** 的数字表示为 1，**IEEE802** 的数字表示形式为 6。

**缺省情况：**缺省为协议类型为 Ethernet 协议。

**命令模式：**DHCP 地址池模式。

**使用指南：**本命令在手工绑定地址时结合命令 **host** 一起使用。当发出请求的客户机的硬件地址恰好和指定的硬件地址相吻合，DHCP 服务器就将 **host** 命令中定义的 IP 地址分配给客户机。

**举例：**手工绑定时，将 IP 地址 10.1.128.160 与硬件地址为 00-00-e2-3a-26-04 的用户绑定。

Switch(dhcp-1-config)#hardware-address 00-00-e2-3a-26-04

Switch(dhcp-1-config)#host 10.1.128.160 24

**相关命令：host**

### 4.14.1.13 host

**命令：host <address> [<mask> | <prefix-length> ]**

**no host**

**功能：**在手工绑定地址时，分配给指定客户机的用户的 IP 地址；本命令的 no 操作为删除 IP 地址。

**参数：*<address>***为 IP 地址，点分十进制格式；***<mask>***为掩码，点分十进制格式；***<prefix-length>*** 为用前缀表示法，如掩码为 255.255.255.0 用前缀法表示为“24”，掩码为 255.255.255.252 用前缀法表示为“30”。

**命令模式：**DHCP 地址池模式。

**缺省情况：**无。

**使用指南：**如果在配置 IP 地址时，仅配置了 IP 地址，没有配置掩码和前缀，并且在 IP 地址池中也没有任何有关掩码的信息，缺省系统会按有类地址自动分配掩码。

本命令在手工绑定地址时结合 **hardware-address** 命令或者 **client-identifier** 命令一起使用。当发出请求的客户机的标识或硬件地址恰好和指定的标识或硬件地址相吻合，DHCP 服务器就将 **host** 命令中定义的 IP 地址分配给客户机。

**举例：**手工绑定时，将 IP 地址 10.1.128.160 与硬件地址为 00-10-5a-60-af-12 的用户绑定。

Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

**相关命令：hardware-address、client-identifier**

## 4.14.1.14 ip dhcp conflict logging

**命令：ip dhcp conflict logging**

**no ip dhcp conflict logging**

**功能：**打开 DHCP 服务器检测地址冲突的日志功能；本命令的 no 操作为关闭该日志功能。

**参数：**无。

**缺省情况：**缺省情况下，记录地址冲突的日志功能是打开的。

**命令模式：**全局配置模式。

**使用指南：**当日志功能是打开的，一旦 DHCP 服务器检测到有地址冲突时，就会将该冲突地址记录到日志中。对于在日志中出现的有冲突记录的地址，DHCP 服务器将不再对其进行动态分配，直到把这些冲突记录删除。

**举例：**关闭 DHCP 服务器的日志功能。

Switch(config)#no ip dhcp conflict logging

**相关命令：clear ip dhcp conflict**

## 4.14.1.15 ip dhcp disable

**命令：ip dhcp disbale**

**no ip dhcp disable**

**功能：** 端口关闭 DHCP 相关的服务；本命令的 no 操作为打开 DHCP 相关的服务。

**参数：** 无。

**缺省情况：** 端口的 DHCP 服务缺省打开的。

**命令模式：** 端口配置模式。

**使用指南：** 端口关闭了 DHCP 相关的服务后，端口送上来的所有 DHCP 报文将不做处理，直接丢弃。

**举例：** 端口关闭 DHCP 相关服务。

switch(config-if-ethernet1/1/3)#ip dhcp disable

## 4.14.1.16 ip dhcp excluded-address

**命令：ip dhcp excluded-address <low-address> [<high-address>]**

**no ip dhcp excluded-address <low-address> [<high-address>]**

**功能：**排除地址池中的不用于动态分配的地址；本命令的 no 操作为取消该项配置。

**参数：*<low-address>***为起始的 IP 地址；**[*<high-address>*]**为结束的 IP 地址。

**缺省情况：**缺省为仅排除单个地址。

**命令模式：**全局配置模式。

**使用指南：**使用本命令可以将地址池中的一个地址或连续的几个地址排除，这些地址由系统管理员留作其它用途。

**举例：**将 10.1.128.1 到 10.1.128.10 之间的地址保留，不用于动态分配。

Switch(config)#ip dhcp excluded-address 10.1.128.1 10.1.128.10

## 4.14.1.17 ip dhcp pool

**命令：ip dhcp pool <name>**

**no ip dhcp pool <name>**

**功能：**配置 DHCP 地址池，进入 dhcp 地址池模式；本命令的 no 操作为删除该地址池。

**参数：*<name>***为地址池名，最长不超过 32 个字符。

**命令模式：**全局配置模式。

**使用指南：**在全局模式下定义一个 DHCP 地址池，进入到 DHCP 地址池配置模式。

**举例：**定义一个地址池，取名 1。

Switch(config)#ip dhcp pool 1

Switch(dhcp-1-config)#

## 4.14.1.18 ip dhcp conflict ping-detection enable

**命令：ip dhcp conflict ping-detection enable**

**no ip dhcp conflict ping-detection enable**

**功能：**打开 DHCP 服务器 Ping 方式检测地址冲突的功能；本命令的 no 操作为关闭该检测功能。

**参数：**无。

**缺省情况：**缺省情况下，Ping 方式检测地址冲突的功能是关闭的。

**命令模式：**全局配置模式。

**使用指南：**打开 Ping 方式地址冲突检测功能前需打开记录地址冲突的日志功能；当关闭该日志功能时，Ping 方式地址冲突检测功能同时被关闭。当客户端无法接收 Ping 请求报文时（比如防火墙屏蔽了 Ping 请求报文），本功能根据分配 IP 对本地 ARP 进行检查：若选择的 IP 存在对应的 ARP，则判定为地址冲突；反之，则分配该 IP 给客户端。

**举例：**打开 Ping 方式检测地址冲突的功能。

Switch(config)#ip dhcp conflict ping-detection enable

**相关命令：ip dhcp conflict logging, ip dhcp ping packets, ip dhcp ping timeout**

## 4.14.1.19 ip dhcp ping packets

**命令：ip dhcp ping packets <request-num>**

**no ip dhcp ping packets**

**功能：**设置 DHCP 服务器 Ping 方式检测地址冲突时，尝试发送 Ping 请求报文（Echo Request）的最大个数，默认为 2 个；本命令的 no 操作为恢复默认发送 Ping 请求报文的个数。

**参数：*<request-num>***是 Ping 方式检测地址冲突时尝试发送的 Ping 请求报文个数。

**缺省情况：**缺省情况下，最多发送 2 个 Ping 请求报文。

**命令模式：**全局配置模式。

**举例：**设置 DHCP 服务器 Ping 方式检测地址冲突时发送 Ping 请求报文最大个数为 3。

Switch(config)#ip dhcp ping packets 3

**相关命令：ip dhcp conflict ping-detection enable, ip dhcp ping timeout**

## 4.14.1.20 ip dhcp ping timeout

**命令：ip dhcp ping timeout <timeout-value>**

**no ip dhcp ping timeout**

**功能：**设置 DHCP 服务器 Ping 方式检测地址冲突时，每次发送 Ping 请求报文（Echo Request）后，等待回应报文（Echo Reply）的超时时长（单位为 ms），默认为 500ms；本命令的 no 操作为恢复默认超时时长。

**参数：*<timeout-value>***是 Ping 方式检测地址冲突时每次 Ping 请求等待回应的超时时长。

**缺省情况：**缺省情况下，超时时长为 500ms。

**命令模式：**全局配置模式。

**举例：**设置 DHCP 服务器 Ping 方式检测地址冲突时等待每个回应报文的超时时长为 600ms。

Switch(config)# ip dhcp ping timeout 600

**相关命令：ip dhcp conflict ping-detection enable, ip dhcp ping packets**

## 4.14.1.21 lease

**命令：lease { [<days>] [<hours>][<minutes>] | infinite }**

**no lease**

**功能：**配置地址池中地址的租用期限；本命令的 no 操作为恢复缺省值。

**参数：*<days>***为天数，取值范围为 0~365；***<hours>***为小时数，取值范围为 0~23；***<minutes>***为分数，取值范围为 0~59；**infinite** 为永久的使用。

**缺省情况：**缺省的租期设置为 1 天。

**命令模式：**DHCP 地址池模式。

**使用指南：**DHCP 是动态的分配网络配置参数，并非永久分配，因此有租期的限制。租期设置过长，难以发挥 DHCP 灵活、动态的优势；租期设置过短，有会造成网络通信量的增加，加大网络开销，因此租期的设置可由网络管理员根据自身网络的特点设定。交换机缺省的租期设置为 1 天。

**举例：**DHCP 地址池 1 的租期设置为 3 天 12 个小时 30 分钟。

Switch(dhcp-1-config)#lease 3 12 30

## 4.14.1.22 max-lease-time

**命令：max-lease-time {[<days>] [<hours>][<minutes>] | infinite}**

**no max-lease-time**

**功能：**配置地址池中地址的最大租用期限；本命令的 no 操作为恢复缺省值。

**参数：**<*days*>为天数，取值范围为 0~365；<*hours*>为小时数，取值范围为 0~23；<*minutes*>为分数，取值范围为 0~59；infinite 为永久的使用。

**缺省情况：**缺省的租期设置为 1 天。

**命令模式：**DHCP 地址池模式。

**使用指南：**该配置命令使用于带有 option51 选项的 DHCP 请求报文场景中，如果用户请求地址租期的时间超过配置的最大租用期限，则 DHCP 服务器分配该地址的租期为配置最大租期时间，如果用户请求地址的租期时间小于配置的最大租期时间，则 DHCP 服务器分配该地址的租期为用户请求报文携带的请求租用期限。最大租用期限的设置可由网络管理员根据自身网络的特点进行设定。交换机缺省的最大租用期限设置为 1 天。

**举例：**DHCP 地址池 1 的最大租期设置为 3 天 12 个小时 30 分钟。

Switch(dhcp-1-config)#max-lease-time 3 12 30

## 4.14.1.23 netbios-name-server

**命令：netbios-name-server <address1>[<address2>[…<address8>]]**

**no netbios-name-server**

**功能：**配置 Wins 服务器的地址；本命令的 no 操作为删除 Wins 服务器。

**参数：*address1…address8*** 为 IP 地址，均为点分十进制格式。

**缺省情况：**系统缺省没有配置 Wins 服务器。

**命令模式：**DHCP 地址池模式。

**使用指南：**为客户机指定 Wins 服务器，最多可设置 8 个 Wins 服务器，最先设置的 Wins 服务器的地址优先级最高，因此 address1 优先级最高，依次 address2、address3……。

**举例：**配置地址池 1 的 Wins 服务器的地址为 192.168.1.1。

Switch(dhcp-1-config)#netbios-name-server 192.168.1.1

## 4.14.1.24 netbios-node-type

**命令：netbios-node-type {b-node|h-node|m-node|p-node|<type-number>}**

**no netbios-node-type**

**功能：**配置 DHCP 客户机的节点类型；本命令的 no 操作为取消该项配置。

**参数：b-node** 为广播型；**h-node** 为先点对点后广播的混合型；**m-node** 为先广播后点对点的混合型；**p-node** 为点对点型；***<type-number>***为节点类型的十六进值表示法，取值范围为 0~255。

**缺省情况：**没有为客户机指定节点类型。

**命令模式：**DHCP 地址池模式。

**使用指南：**如果要为客户机指定节点类型，建议把客户机的节点类型配置为先点对点后广播的混合型节点类型。

**举例：**地址池 1 的客户机的节点类型为广播型。

Switch(dhcp-1-config)#netbios-node-type b-node

## 4.14.1.25 network-address

**命令：network-address <network-number> [<mask> | <prefix-length>]**

**no network-address**

**功能：**配置地址池可分配的地址范围；本命令的 no 操作为取消该项配置。

**参数：*<network-number>***为网络号码；***<mask>***为掩码，点分十进制格式；***<prefix-length>***为用前缀表示法，如掩码为 255.255.255.0 用前缀法表示为“24”，掩码为 255.255.255.252 用前缀法表示为“30”。注意：在使用 DHCP-SERVER 的时候，配置地址掩码的时候，应该使地址池中掩码长于或等于交换机上对应网段的三层接口 IP 地址的掩码，DHCP 地址池配置时无法配置掩码为 31 位和 32 位的地址池。

**缺省情况：**如果不带掩码，缺省掩码为按照有类地址自动分配。

**命令模式：**DHCP 地址池模式。

**使用指南：**DHCP 服务器用于动态分配 IP 地址时使用本命令配置可分配的 IP 地址范围，一个地址池只能对应一个网段。本命令与手工绑定地址的命令即 **hardware-address** 命令、**host** 命令互斥。

**举例：**地址池 1 的可分配的地址为 10.1.128.0/24。

Switch(dhcp-1-config)#network-address 10.1.128.0 24

**相关命令：ip dhcp excluded-address**

## 4.14.1.26 next-server

**命令：next-server <address1>[<address2>[…<address8>]]**

**no next-server**

**功能：**配置客户机导入文件存放的服务器地址；本命令的 no 操作为取消该项配置。

**参数：*address1…address8*** 为 IP 地址，均为点分十进制格式。

**命令模式：**DHCP 地址池模式。

**缺省情况：**无。

**使用指南：**为客户机指定导入文件存放的服务器地址。一般用在无盘工作站，系统启动时需要从服务器上下载配置文件，和 **bootfile** 结合使用。

**举例：**文件存放的服务器地址为 10.1.128.4。

Switch(dhcp-config)#next-server 10.1.128.4

**相关命令：bootfile**

## 4.14.1.27 option

**命令：option <code> {ascii <string> | hex <hex> | ipaddress <ipaddress>}**

**no option <code>**

**功能：**配置 option 所指定代码的网络参数的值；本命令的 no 操作为取消对该 option 的配置。

**参数：*<code>***为网络参数的代码值；***<string>***为 ASCⅡ型字符串，最长不超过 255 个字符；***<hex>***为十六进值表示的数值，最长不超过 510，且长度必须为偶数；***<ipaddress>***为 IP 地址，点分十进制格式，最长可以设置 63 个 IP 地址。

**命令模式：**DHCP 地址池模式。

**缺省情况：**无。

**使用指南：**系统不仅提供多项在网络配置中常用的命令，还提供了配置网络参数的通用命令，满足用户的多方面的配置需求。Option 的代码定义在 **RFC2132** 中有详细介绍。

**举例：**配置 WWW 服务器的地址为 10.1.128.240。

Switch(dhcp-1-config)#option 72 ip 10.1.128.240

## 4.14.1.28 service dhcp

**命令：service dhcp**

**no service dhcp**

**功能：**启动 DHCP 服务器功能；本命令的 no 操作为关闭 DHCP 服务。

**参数：**无。

**缺省情况：**DHCP 服务缺省是关闭的。

**命令模式：**全局配置模式。

**使用指南：**DHCP 服务包括 DHCP 服务器功能和 DHCP 中继的功能。当打开 DHCP 服务时，DHCP 服务器功能和 DHCP 中继功能都被打开。只有打开 DHCP 服务器功能，交换机才能给 DHCP 客户机分配 IP 地址及开启 DHCP 的 RELAY 功能。

**举例：**打开 DHCP 服务器。

Switch(config)#service dhcp

## 4.14.1.29 show ip dhcp binding

**命令：show ip dhcp binding [ [<ip-addr>] [type {all | manual | dynamic}] [count] ]**

**功能：**显示 IP 地址与 MAC 地址的绑定情况。

**参数：*<ip-addr>***为某指定的 IP 地址，点分十进制格式；all 表示所有的绑定类型（手工绑定与动态分配）；manual 表示手工绑定类型；dynamic 表示动态分配类型；count 表示显示 DHCP 地址绑定表项数量信息。

**命令模式：**特权和配置模式。

**举例:**

Switch#sh ip dhcp binding

| IP address | Hardware address | Lease expiration | Type |
|---|---|---|---|
| 10.1.1.233 | 00-00-E2-3A-26-04 | Infinite | Manual |
| 10.1.1.254 | 00-00-E2-3A-5C-D3 | 60 | Automatic |

| 显示信息 | 解释 |
|---|---|
| IP address | 分配给 DHCP 客户机的 IP 地址； |
| Hardware address | DHCP 客户机的硬件地址； |
| Lease expiration | DHCP 客户机拥有该 IP 地址的有效时间； |
| Type | 类型，指手工绑定还是动态分配的。 |

## 4.14.1.30 show ip dhcp conflict

**命令：show ip dhcp conflict**

**功能：**显示有冲突记录的地址的日志信息。

**命令模式：**特权和配置模式。

**举例：**

Switch#sh ip dhcp conflict

| IP Address | Detection method | Detection Time |
|---|---|---|
| 10.1.1.1 | Ping | FRI JAN 02 00:07:01 2002 |

| 显示信息 | 解释 |
|---|---|
| IP Address | 有冲突的 IP 地址。 |
| Detection method | 检测到冲突的方式。 |
| Detection Time | 检测到冲突的时间。 |

## 4.14.1.31 show ip dhcp relay information option

**命令：show ip dhcp relay information option**

**功能：**显示 DHCP 中继 option 82 选项相关配置信息。

**命令模式：**特权和配置模式。

**举例:**

Switch#show ip dhcp relay information option

ip dhcp server relay information option(i.e. option 82) is enabled

ip dhcp relay information option(i.e. option 82) is enabled

## 4.14.1.32 show ip dhcp server statistics

**命令：show ip dhcp server statistics**

**功能：**显示 DHCP 服务器的对各种 DHCP 数据包的统计信息。

**命令模式：**特权和配置模式。

**举例：**

```
Switch#show ip dhcp server statistics
Address pools                3
Database agents              0
Automatic bindings           2
Manual bindings              0
Conflict bindings            0
Expiried bindings            0
Malformed message            0

Message                      Recieved
BOOTREQUEST                  3814
DHCPDISCOVER                 1899
DHCPREQUEST                  6
DHCPDECLINE                  0
DHCPRELEASE                  1
DHCPINFORM                   1

Message                      Send
BOOTREPLY                    1911
DHCPOFFER                    6
DHCPACK                      6
DHCPNAK                      0
DHCPRELAY                    1907
DHCPFORWARD                  0
Switch#
```

| 显示信息 | 解释 |
|---|---|
| Address pools | 配置的 DHCP 地址池个数； |
| Database agents | 代理数据库的个数； |
| Automatic bindings | 自动分配地址的个数； |
| Manual bindings | 手工绑定地址的个数； |
| Conflict bindings | 有地址冲突的个数； |
| Expiried bindings | 绑定超期的个数； |

| | |
|---|---|
| Malformed message | 错误信息的个数； |
| Message Recieved | 接收 DHCP 数据包的统计 |
| BOOTREQUEST | 接收的数据包总数； |
| DHCPDISCOVER | 其中 DHCPDISCOVER 包个数； |
| DHCPREQUEST | 其中 DHCPREQUEST 包个数； |
| DHCPDECLINE | 其中 DHCPDECLINE 包个数； |
| DHCPRELEASE | 其中 DHCPRELEASE 包个数； |
| DHCPINFORM | 其中 DHCPINFORM 包个数； |
| Message Send | 发送 DHCP 数据包的统计 |
| BOOTREPLY | 发送的数据包的总数； |
| DHCPOFFER | 其中 DHCPOFFER 包的个数； |
| DHCPACK | 其中 DHCPACK 包的个数； |
| DHCPNAK | 其中 DHCPNAK 包的个数； |
| DHCPRELAY | 其中 DHCPRELAY 包的个数； |
| DHCPFORWARD | 其中 DHCPFORWARD 包的个数。 |

## 4.14.2 DHCP 中继配置命令

### 4.14.2.1 ip dhcp broadcast suppress

**命令：ip dhcp broadcast suppress**

**no ip dhcp broadcast suppress**

**功能：** 开启 DHCP 广播报文抑制功能；no 命令为关闭 DHCP 广播报文抑制功能。

**参数：** 无。

**缺省情况：** 默认不启动 DHCP 广播报文抑制功能。

**命令模式：** 全局配置模式

**使用指南：** 抑制 DHCP 广播报文的转发，以及 DHCP 广播报文丢弃和复制至 CPU。

**举例：** 在交换机上开启 DHCP 广播报文抑制功能。

Switch(config)#ip dhcp broadcast suppress

### 4.14.2.2 ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>

**命令：ip dhcp relay share-vlan *<vlanid>* sub-vlan *<vlanlist>***

**no ip dhcp relay share-vlan**

**功能：** 指定一个 share-vlan 的 sub-vlan；本命令的 no 操作为取消 share-vlan 的 sub-vlan。

**参数：** ***<vlanid>*** 为 share-vlan 的 vlan 号， ***<vlanlist>*** 为 sub-vlan 的列表。

**缺省情况：** 无。

**命令模式：** 全局配置模式。

**使用指南：** share-vlan 可以有许多的 sub-vlan，但一个 sub-vlan 只能对应一个 share-vlan。当 DHCP Relay 二层设备收到 DHCP Request 时，首先判断收到的包中 vlan 是否有三层接口，如果有就用此三层接口进行 DHCP Relay。如果收到包中的 vlan 没有三层接口，但此 vlan 是某个 share-vlan 的 sub-vlan，则用 share-vlan 的三层接口进行 DHCP Relay。

### 4.14.2.3 ip forward-protocol udp bootps

**命令：ip forward-protocol udp bootps**

**no ip forward-protocol udp bootps**

**功能：**配置 DHCP 中继转发指定端口的 UDP 广播报文；本命令的 no 操作为取消该项服务。

**参数：**bootps 标识转发 UDP 端口为 67 DHCP 广播报文。

**缺省情况：**DHCP 中继缺省不转发 DHCP 广播报文。

**命令模式：**全局配置模式。

**使用指南：**该命令的转发目的地址在随后的 ip helper-address 命令里设定。

**举例：**转发 DHCP 包，且目的服务器地址为 192.168.1.5。

```
Switch(config)#ip forward-protocol udp bootps
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)#ip helper-address 192.168.1.5
```

### 4.14.2.4 ip helper-address

**命令：ip helper-address <ipaddress>**

**no ip helper-address <ipaddress>**

**功能：**指定 DHCP 中继转发 UDP 报文的目标地址；本命令的 no 操作为取消该项设置。

**参数：*<ipaddress>***为 DHCP 中继转发 UDP 报文的目标 IP 地址。

**缺省情况：**无。

**命令模式：**接口配置模式。

**使用指南：**DHCP 中继转发的服务器地址是与转发 UDP 的端口相对应的，即 DHCP 中继只转发相应 UDP 协议的报文给相应的服务器，并不是把所有 UDP 报文转发给所有的服务器。当使用 **ip forward-protocol udp *<port>***命令后，再配置本命令时，本命令所配置的转发地址接收到的是端口号为***<port>***的 UDP 报文。

### 4.14.2.5 show ip forward-protocol

**命令：show ip forward-protocol**

**功能：**显示已配置的支持广播报文转发的协议端口号，主要指 DHCP 报文转发的端口号。

**命令模式：**特权和配置模式。

**举例：**

Switch#show ip forward-protocol

Forward protocol(UDP port): 67(active)

### 4.14.2.6 show ip helper-address

**命令：show ip helper-address**

**功能：**显示可转发广播报文的协议端口号、支持转发功能的接口以及转发的目的 IP 的配置关系。

**命令模式：**特权和配置模式。

**举例：**

Switch#show ip helper-address

| Forward protocol | Interface | Forward server |
|---|---|---|
| 67(active) | Vlan1 | 192.168.1.1 |

## 4.15 DHCP option 82

### 4.15.1 debug ip dhcp relay packet

**命令：debug ip dhcp relay packet**

**功能：**使用本命令显示 DHCP 中继代理处理数据包的信息，包括 option 82 选项的添加和剥离动作信息。

**参数：**无

**命令模式：**特权配置模式

**使用指南：**运行时使用本命令显示中继代理处理中继数据包的过程，并显示相应的 option82 动作信息。

**举例：**配置显示 DHCP 中继代理处理数据包的信息。

Switch#debug ip dhcp relay packet

### 4.15.2 ip dhcp relay information option

**命令：ip dhcp relay information option**

**no ip dhcp relay information option**

**功能：**设置本命令启用交换机中继代理的 option82 功能，本命令的 no 操作关闭交换机中继代理的 option82 功能。

**参数：**无

**缺省情况：**系统默认关闭 option82 功能。

**命令模式：**全局配置模式

**使用指南：**只有配置本命令 DHCP 中继代理才能在 DHCP 请求报文中添加 option82 选项交给服务器处理。启用本功能之前确保系统已经使能 DHCP 服务并配置转发目的端口 67 的 udp 广播报文。

**举例：**开启交换机中继代理的 option82 功能

Switch(config)#service dhcp

Switch(config)#ip forward-protocol udp bootps

Switch(config)#ip dhcp relay information option

## 4.15.3 ip dhcp relay information option delimiter

**命令：ip dhcp relay information option delimiter [colon | dot | slash | space]**

**no ip dhcp relay information option delimiter**

**功能：**该命令用来配置用户在全局定义的用来生成 option82 子选项的各参数的分隔符，该命令的 no 形式恢复分隔符为默认值，即 slash。

**参数：**无

**缺省情况：**系统默认分隔符为 slash (“/”)。

**命令模式：**全局配置模式

**使用指南：**当用户在全局自定义了用来生成 option82 子选项（remote-id，circuit-id）的各参数后，该命令配置的分隔符用来分隔这些参数。

**举例：**配置 option82 子选项各参数分隔符为 dot（“.”）。

Switch(config)#ip dhcp relay information option delimiter dot

## 4.15.4 ip dhcp relay information option remote-id

**命令：ip dhcp relay information option remote-id {standard | <remote-id>}**

**no ip dhcp relay information option remote-id**

**功能：**本命令用于设置从接口接收的 DHCP 请求报文添加 option 82 子选项 2(远程 ID 选项)的具体内容。本命令的 no 操作把添加 option 82 子选项 2(远程 ID 选项)的形式设置为 standard。

**参数：**standard 表示默认的交换机 VLAN MAC 格式，*<remote-id>*为用户自己指定的 option 82 的 remote-id 内容，它是一个长度小于等于 64 的字符串。

**命令模式：**全局配置模式

**缺省情况：**系统默认使用 standard 形式设置 option 82 中的 remote-id。

**使用指南：**因为交换机添加的 option 82 信息要配合第三方的 DHCP 服务器使用，在交换机的标准 remote-id 形式不能满足服务器的要求时，提供一种手段由用户依据服务器情况自己指定 remote-id 的内容。

**举例：**设置 DHCP option82 选项的子选项 remote-id 为 street-1-1。

Switch(config)# ip dhcp relay information option remote-id street-1-1

## 4.15.5 ip dhcp relay information option remote-id format

**命令：ip dhcp relay information option remote-id format {default | vs-hp}**

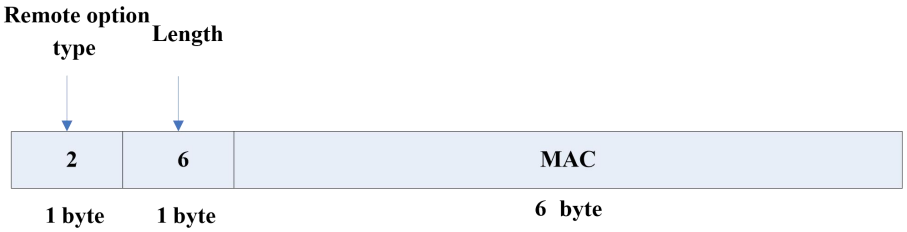
**功能：**本命令设置交换机中继代理的 option82 功能 remote-id 默认格式。

**参数：**default 表示 remote-id 为十六进制格式的交换机 VLAN MAC 地址，vs-hp 表示 remote-id 兼容设备厂商 HP 的 remote-id 格式。

**缺省情况：**系统默认 option82 功能 remote-id 格式为 default。

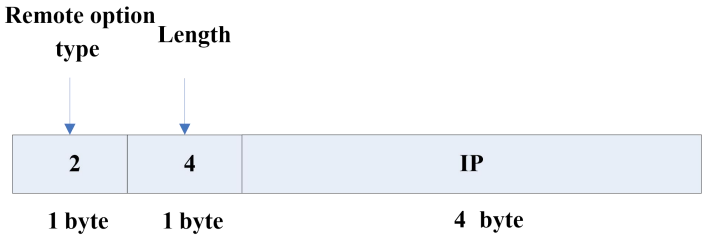
**命令模式：**全局配置模式

**使用指南：**默认 remote-id 格式定义如下：




其中 MAC 为交换机 VLAN MAC 地址。

兼容设备厂商 HP 的 remote-id 格式定义如下：




其中 IP 为 DHCP 报文来自三层接口的主 IP 地址。

**举例：**配置交换机中继代理 option82 功能 remote-id 为兼容设备厂商 HP 格式。

Switch(config)#ip dhcp relay information option remote-id format vs-hp

## 4.15.6 ip dhcp relay information option self-defined remote-id

**命令：ip dhcp relay information option self-defined remote-id {hostname | mac | string WORD}**

**no ip dhcp relay information option self-defined remote-id**

**功能：**该命令用来配置 option82 的生成方式，用户可以自定义用来生成 option82 子选项 remote-id 的参数（集）。

**参数：** WORD 自定义的 remote-id 字符串，最大长度为 64。

**缺省情况：**缺省采用标准生成方式。

**命令模式：**全局配置模式

**使用指南：**配置本命令后，若用户没有在接口上配置 remote-id，则根据本命令的自定义生成方式来生成 option82 子选项 remote-id。对于 mac，如果是用 ascii 的形式填到报文中则采用形如 00-02-d1-2e-3a-0d 的形式。对于 mac，如果是用 ascii 的形式填到报文中则采用形如 00-02-d1-2e-3a-0d 的形式，如果是 hex 形式则占 6 个字节。各个选项按照命令配置的顺序填入报文，中间用分隔符分隔（分隔符为 ip dhcp relay information option delimiter 配置）。

**举例：**配置 option82 子选项 remote-id 的生成方式为 hostname 和字符串“abc”。

Switch(config)#ip dhcp relay information option self-defined remote-id hostname string abc

## 4.15.7 ip dhcp relay information option self-defined remote-id format

**命令：ip dhcp relay information option self-defined remote-id format [ascii | hex]**

**功能：**该命令用来配置 relay option82 中 remote-id 的生成格式。

**参数：**无。

**缺省情况：**系统默认生成格式为 ascii。

**命令模式：**全局配置模式

**使用指南：**本命令的生成格式指定了用命令 ip dhcp relay information option type self-defined remote-id 生成 remote-id 的格式。

**举例：**配置 relay option82 中 remote-id 的生成格式为 hex。

Switch(config)# ip dhcp relay information option self-defined remote-id format hex

## 4.15.8 ip dhcp relay information option self-defined subscriber-id

**命令：ip dhcp relay information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac)| string WORD }**

**no ip dhcp relay information option self-defined subscriber-id**

**功能：**该命令用来配置 option82 的生成方式，用户可以自定义用来生成 option82 子选项 circuit-id 的参数（集）。

**参数：**WORD 自定义的 circuit-id 字符串，最大长度为 64。

**缺省情况：**缺省采用标准生成方式。

**命令模式：**全局配置模式

**使用指南：**配置本命令后，若用户没有在接口上配置 circuit-id，则根据本命令的自定义生成方式来生成 option82 子选项 circuit-id。用该命令生成的 circuit-id 的格式为：若 self-defined format 为 ascii，则填入的 vlan 选项形如“Vlan2”，port 选项形如“Ethernet1/1/1”，mac 选项和 remote-mac 选项形如“00-02-d1-2e-3a-0d”；若 self-defined format 为 hex，则填入的 vlan 选项占两个字节，port 选项占 4 个字节，一个字节表示 slot（对于机架式交换机，表示插槽号；对于盒式交换机，为 1），一个字节表示 Module（默认为 0），两个字节表示端

口号，从 1 开始，mac 选项和 remote-mac 选项占 6 个字节。各个选项按照命令配置的顺序填入报文，中间用分隔符分隔（分隔符为 ip dhcp relay information option delimiter 配置）。

**举例：**配置生成 option82 子选项 circuit-id 的生成方式为 port，mac。

Switch(config)# ip dhcp relay information option self-defined subscriber-id port id switch-id mac

## 4.15.9 ip dhcp relay information option self-defined subscriber-id format

**命令：ip dhcp relay information option self-defined subscriber-id format [ascii | hex]**

**功能：**该命令用来配置 relay option82 中 circuit-id 的生成格式。

**参数：**无。

**缺省情况：**系统默认生成格式为 ascii。

**命令模式：**全局配置模式

**使用指南：**本命令的生成格式指定了用命令 ip dhcp relay information option type self-defined subscriber-id 生成 circuit-id 的格式。

**举例：**配置 relay option82 中 circuit-id 的生成格式为 hex。

Switch(config)# ip dhcp relay information option self-defined subscriber-id format hex

## 4.15.10 ip dhcp relay information option subscriber-id

**命令：ip dhcp relay information option subscriber-id {standard | <circuit-id>}**

**no ip dhcp relay information option subscriber-id**

**功能：**本命令用于设置从接口接收的 DHCP 请求报文添加 option 82 子选项 1(电路 ID 选项)的形式，**standard** 表示标准的 vlan 名加物理端口名形式，如“Vlan2+Ethernet1/1/12”，***<circuit-id>***为用户自己指定的 option 82 的 circuit-id 内容，它是一个长度小于 64 的字符串。本命令的 no 操作把添加 option 82 子选项 1(电路 ID 选项)的形式设置为 standard 形式。

**参数：**无

**命令模式：**接口配置模式

**缺省情况：**系统默认使用 standard 形式设置 option 82 中的 circuit-id。

**使用指南：**因为交换机添加的 option 82 信息要配合第三方的 DHCP 服务器使用，在交换机的标准 circuit-id 形式不能满足服务器的要求时，提供一种手段由用户依据服务器情况自己指定 circuit-id 的内容。

**举例：**设置 DHCP option82 选项的子选项 circuit-id 为 foobar

Switch(config-if-vlan1)#ip dhcp relay information option subscriber-id foobar

## 4.15.11 ip dhcp relay information option subscriber-id format

**命令：ip dhcp relay information option subscriber-id format {hex | acsii | vs-hp}**

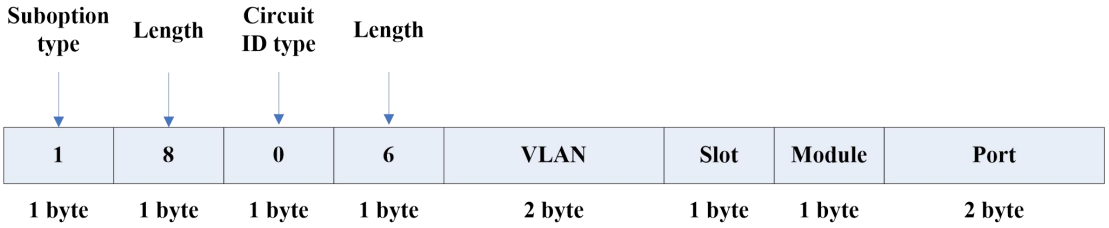
**功能：**本命令设置交换机中继代理的 option82 功能 subscriber-id 默认格式。

**参数：**hex 表示 subscriber-id 为十六进制格式的 VLAN 和端口信息，acsii 表示 subscriber-id 为 ACSII 格式的 VLAN 和端口信息，vs-hp 表示 subscriber-id 兼容设备厂商 HP 的格式。

**缺省情况：**系统默认 option82 功能 subscriber-id 格式为 acsii。

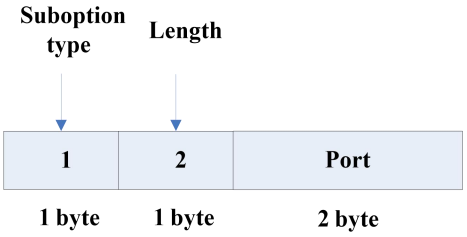
**命令模式：**全局配置模式

**使用指南：**ASCII 格式的 VLAN 和端口信息形如“Vlan1+Ethernet1/1/11”。十六进制格式的 VLAN 和端口信息定义如下：




其中，VLAN 字段填写交换机 VLAN ID。Slot 对于机架式交换机，表示插槽号；对于盒式交换机，为 1。Module 默认为 0。Port 表示端口号，从 1 开始。

兼容设备厂商 HP 的 subscriber-id 格式定义如下：




其中 Port 表示端口号，从 1 开始。

**举例：**配置交换机中继代理 option82 功能 subscriber-id 格式为十六进制格式。

Switch(config)#ip dhcp relay information option subscriber-id format hex

## 4.15.12 ip dhcp relay information policy

**命令：ip dhcp relay information policy {drop | keep | replace}**

**no ip dhcp relay information policy**

**功能：**本命令用于设置系统对于接收到的含有 option82 选项的 DHCP 请求报文的重转发策略，其中 drop 模式表示如果报文中含有 option82 选项，则系统丢弃该 DHCP 报文不作处理；keep 模式表示系统保持现有报文中的 option82 选项不变转发给服务器处理；replace 模式表示系统使用自己的 option82 选项替换现有报文中的 option82 选项，然后转发给服务器处理。本命令的 no 操作设置 option82 选项 DHCP 报文的重转发策略为 replace。

**参数：**无

**命令模式：**接口配置模式

**缺省情况：**系统默认使用 replace 模式使用本系统的 option82 选项替换现有报文中的 option 选项。

**使用指南：**由于 DHCP 客户端报文向 DHCP 服务器传递的过程中可能经过多个 DHCP 中继代理，该路径上后续中继需要设置策略决定如何对先前中继添加的 option82 选项进行处理。Option 82 重转发策略的选择要配合 DHCP 服务器的配置策略而定。

**举例：**设置 DHCP 报文 option82 选项的重转发策略为 keep

Switch(config-if-vlan1)#ip dhcp relay information policy keep

## 4.15.13 ip dhcp server relay information enable

**命令：ip dhcp server relay information enable**

**no ip dhcp server relay information enable**

**功能：**本命令用于设置交换机 DHCP 服务器支持对 option82 选项的识别。本命令的 no 操作使服务器忽略处理 option 82 选项。

**参数：**无

**命令模式：**全局配置模式

**缺省情况：**系统默认不启用 option82 选项识别功能。

**使用指南：**如果希望交换机 DHCP 服务器识别 option82 选项并在应答报文中返回 option 82 信息，需要配置本命令，否则交换机 DHCP 服务器会忽视 option82 选项的存在。

**举例：**设置 DHCP 服务器支持 option82 选项

Switch(config)# ip dhcp server relay information enable

## 4.15.14 show ip dhcp relay information option

**命令：show ip dhcp relay information option**

**功能：**本命令显示系统 DHCP option 82 的状态信息，包括 option82 使能开关，接口重转发策略，接口电路 ID 模式，以及交换机 DHCP 服务器 option82 使能开关。

**参数：**无

**命令模式：**特权和全局配置模式

**使用指南：**运行时使用本命令检查中继代理 option82 状态信息。

**举例：**

```
Switch#show ip dhcp relay information option
ip dhcp server relay information option(i.e. option 82) is disabled
ip dhcp relay information option(i.e. option 82) is enabled

Vlan2:
        ip dhcp relay information policy keep
        ip dhcp relay information option subscriber-id standard

Vlan3:
        ip dhcp relay information policy replace
```

ip dhcp relay information option subscriber-id foobar

# 4.16 DHCP Snooping

## 4.16.1 debug ip dhcp snooping binding

**命令：debug ip dhcp snooping binding**

**no debug ip dhcp snooping binding**

**功能：**该命令用来打开 DHCP snooping 调试开关，调试 DHCP snooping 绑定数据的状态。

**命令模式：**特权用户配置模式。

**使用指南：**主要用于调试 DHCP snooping 任务根据绑定数据添加 ARP 表项，dot1x 用户，信任用户表项的状态。

## 4.16.2 debug ip dhcp snooping event

**命令：debug ip dhcp snooping event**

**no debug ip dhcp snooping event**

**功能：**该命令用来打开 DHCP snooping 调试开关，调试 DHCP snooping 任务的状态。

**命令模式：**特权用户配置模式。

**使用指南：**主要用于调试 DHCP snooping 任务状态，可以输出 DHCP snooping 检查绑定数据，执行端口动作等状态。

## 4.16.3 debug ip dhcp snooping packet interface

**命令：debug ip dhcp snooping packet interface {[ethernet] <InterfaceName>}**

**no debug ip dhcp snooping packet {[ethernet] <InterfaceName>}**

**功能：**该命令用来打开 DHCP snooping 调试开关，调试 DHCP snooping 接收报文的消息。

**参数：*<InterfaceName>***：接口名称。

**命令模式：**特权用户配置模式。

**使用指南：** DHCP snooping 从特定端口接收报文的消息。

## 4.16.4 debug ip dhcp snooping packet

**命令：debug ip dhcp snooping packet**

**no debug ip dhcp snooping packet**

**功能：**该命令用来打开 DHCP snooping 调试开关，调试 DHCP snooping 处理报文的流程。

**命令模式：**特权用户配置模式。

**使用指南：** DHCP snooping 处理 DHCP 报文的调试信息。这些调试信息包括报文处理流程的每个步骤：添加报警信息、添加绑定信息、转发 DHCP 报文、添加/剥离 option 82 等等。

## 4.16.5 debug ip dhcp snooping update

**命令：debug ip dhcp snooping update**

**no debug ip dhcp snooping update**

**功能：**该命令用来打开 DHCP snooping 调试开关，调试 DHCP snooping 和 HELPER SERVER 之间的通讯信息。

**命令模式：**特权配置模式。

**使用指南：** 调试 DHCP snooping 接收、发送与 HELPER SERVER 之际的通讯报文消息。

## 4.16.6 enable trustview key

**命令：enable trustview key {0|7} <password>**

**no enable trustview key**

**功能：**配置私有报文的 DES 加密密钥，本命令同时也是交换机启用私有报文加密/散列功能的开关。

**参数：*<password>***是长度小于 16 的字符串，用作 DES 加密密钥。**0** 表示以明文方式显示密钥，**7** 表示以密文方式显示密钥。

**命令模式：**全局配置模式。

**缺省情况：**交换机默认没有配置 DES 加密密钥，即交换机默认不启用私有报文加密/散列功能。

**使用指南：**交换机与 DCN 内网安全管理后台系统通过私有报文进行私有信息的传输，在默认情况下，私有报文是以明文传递的，为了防止私有报文被窃听破解，可选择对私有报文的内容进行加密，同时，管理员也需要在 DCN 内网安全管理后台配置相同的密钥。

**举例：**使能私有报文的加密/散列功能。

Switch(config)#enable trustview key 0 digitalchina

## 4.16.7 ip dhcp snooping

**命令：ip dhcp snooping enable**

**no ip dhcp snooping enable**

**功能：**开启 DHCP Snooping 功能。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**DHCP snooping 默认关闭。

**使用指南：** 开启后将监听所有非信任端口的 DHCP Server 包。

**举例：**启动 DHCP snooping 功能。

switch(config)#ip dhcp snooping enable

## 4.16.8 ip dhcp snooping action

**命令：ip dhcp snooping action {shutdown|blackhole} [recovery <second>]**

**no ip dhcp snooping action**

**功能：**设置或删除端口上的自动防御动作。

**参数：shutdown:** 端口检测到伪装 DHCP Server 时，将 shutdown 此端口。

**blackhole：**端口检测到伪装 DHCP Server 时，将以伪装数据包的 vid 和源 mac 设置 blackhole 来阻止此 Mac 的流量。

**recovery：**用户可选设置自动防御动作执行后还可以自动恢复（no shut 端口或删除相应的 blackhole）。

***<second>*：**用户指定多长时间后恢复防御动作，单位：秒，范围是 10-3600。

**命令模式：**端口配置模式。

**缺省情况：**没有默认的防御动作。

**使用指南：**必须全局开启 DHCP snooping，才能配置此命令。信任端口不会检测 DHCP Server 伪装，所以永远不会触发相应的防御动作。当端口从非信任端口变更为信任端口时，端口上原来的防御动作将自动去除。

**举例：**设置端口 ethernet1/1/1 的 DHCP snooping 防御动作为设置 blackhole，自动恢复时间为 30 秒。

switch(config)#interface ethernet 1/1/1

switch(Config- Ethernet 1/1/1)#ip dhcp snooping action blackhole recovery 30

## 4.16.9 ip dhcp snooping action MaxNum

**命令：ip dhcp snooping action {<maxNum>|default}**

**功能：** 设置端口上同时生效的防御动作数目。

**参数：***<maxNum>*: 每个端口的防御动作数目，范围是 1-200，默认为 10。

default：恢复默认的防御动作数目。

**命令模式：**全局配置模式。

**缺省情况：**默认数目为 10。

**使用指南：**设置防御动作数目限制，是为了防止交换机被攻击而耗尽系统资源。如果报警信息的数目大于了设置的值，那么最早的防御动作将被强行恢复，并下发新的防御动作。

**举例：**配置端口防御动作数量为 100。

switch(config)#ip dhcp snooping action 100

## 4.16.10 ip dhcp snooping binding

**命令：ip dhcp snooping binding enable**

**no ip dhcp snooping binding enable**

**功能：**开启 DHCP snooping 绑定功能。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**DHCP snooping 绑定默认关闭。

**使用指南：**开启后将记录所有信任端口的 DHCP Server 分配的绑定信息。只有启动 DHCP snooping 功能之后，才能启动绑定功能。

**举例：**启动 DHCP snooping 绑定功能。

switch(config)#ip dhcp snooping binding enable

**相关命令：**ip dhcp snooping enable

## 4.16.11 ip dhcp snooping binding arp

**命令：ip dhcp snooping binding arp**

**no ip dhcp snooping binding arp**

**功能：** 开启 DHCP snooping 绑定 ARP 功能。

**参数：** 无。

**命令模式：** 全局配置模式。

**缺省情况：** DHCP snooping 绑定 ARP 功能默认关闭。

**使用指南：** 开启后 DHCP snooping 将根据绑定信息添加绑定 ARP 表项，只有启动绑定功能之后才能启动绑定 ARP 功能。绑定 ARP 表项为静态表项，但是没有配置保留，直接添加到 NEIGHBOUR 表中。绑定 ARP 表项优先级低于管理员配置的静态 ARP 表项，可以被静态 ARP 表项覆盖；但是当静态 ARP 表项被删除之后，绑定 ARP 表项不能恢复，直到 DHCP snooping 重新捕获到绑定信息。添加绑定 ARP 表项是为了防止这些表项被 ARP 欺骗行为攻击，同时这些静态表项无需重认证，可以避免交换机受到 ARP 扫描攻击时重认证 ARP 失败。

只有启动 DHCP snooping 绑定功能之后，才能配置绑定 ARP 功能。

**举例：** 启动 DHCP snooping 绑定 ARP 功能。

switch(config)#ip dhcp snooping binding arp

**相关命令：ip dhcp snooping binding enable**

## 4.16.12 ip dhcp snooping binding dot1x

**命令：ip dhcp snooping binding dot1x**

**no ip dhcp snooping binding dot1x**

**功能：**开启 DHCP snooping 绑定 DOT1X 功能。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**所有端口默认不启动绑定 DOT1X 功能。

**使用指南：**开启后 DHCP snooping 将把捕获的绑定信息通知到 DOT1X 模块，作为 DOT1X 受控用户。这个命令和 ip dhcp snooping binding user-control 命令互斥。

只有启动 DHCP snooping 绑定功能之后，才能配置绑定 DOT1X 功能。

**举例：**在端口 ethernet1/1/1 启动绑定 DOT1X 功能。

switch(config)#interface ethernet 1/1/1

switch(Config- Ethernet 1/1/1)# ip dhcp snooping binding dot1x

**相关命令：ip dhcp snooping binding enable**

**ip dhcp snooping binding user-control**

## 4.16.13 ip dhcp snooping binding user

**命令：ip dhcp snooping binding user <mac> address <ipaddress> vlan <vid> interface [Ethernet] <ifname>**

**no ip dhcp snooping binding user <mac> interface [Ethernet] <ifname>**

**功能：** 配置静态绑定用户信息。

**参数：**

***<mac>***：静态绑定用户的 MAC 地址，MAC 地址是绑定用户的唯一索引值；

***<ipaddress>***：静态绑定用户的 IP 地址；

***<vid>***： 静态绑定用户的所属 VLAN ID；

***<ifname>***：静态绑定用户的接入端口。

**命令模式：**全局配置模式。

**缺省情况：**DHCP snooping 默认没有静态绑定表项。

**使用指南：**静态绑定用户和 DHCP snooping 捕获的动态绑定用户一样处理，可以通知 DOT1X 作为 DOT1X 的受控用户，可以直接添加信任用户表项，可以添加绑定 ARP 表项。静态绑定用户永远不会被老化，并且优先级大于动态绑定用户。只有启动 DHCP snooping 绑定功能之后，才能配置静态绑定用户。

**举例：**配置静态绑定用户。

switch(config)#ip dhcp snooping binding user 00-03-0f-12-34-56 address 192.168.1.16 vlan 1 interface ethernet 1/1/16

**相关命令：ip dhcp snooping binding enable**

## 4.16.14 ip dhcp snooping binding user-control

**命令：ip dhcp snooping binding user-control**

**no ip dhcp snooping binding user-control**

**功能：**开启 DHCP snooping 绑定用户功能。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**所有端口默认不启动绑定用户功能。

**使用指南：**开启后 DHCP snooping 将把捕获的绑定信息直接作为信任用户允许访问所有资源。这个命令和 ip dhcp snooping binding dot1x 命令互斥。

只有启动 DHCP snooping 绑定功能之后，才能配置绑定用户功能，这个命令不受基于 VLAN 的 ip dhcp snooping 限制，只受全局 ip dhcp snooping enable 限制。

**举例：**在端口 ethernet1/1/1 启动绑定 USER 功能。

switch(config)#interface ethernet 1/1/1

switch(Config- Ethernet 1/1/1)#ip dhcp snooping binding user-control

**相关命令：ip dhcp snooping binding enable**

**ip dhcp snooping binding dot1x**

## 4.16.15 ip dhcp snooping binding user-control max-user

**命令：ip dhcp snooping binding user-control max-user <number>**

**no ip dhcp snooping binding user-control max-user**

**功能：** 设置 DHCP snooping 绑定用户功能时指定端口最多允许接入的用户数；本命令的 no 操作为恢复缺省值。

**参数：*<number>*** 最多允许的接入用户数，取值范围为 0~1024。

**命令模式：**端口配置模式。

**缺省情况：**每个端口缺省最多允许接入的用户数为 1024。

**使用指南：**这个命令限制在端口使能 ip dhcp snooping binding user-contrl 时，根据绑定信息下发成信任用户的最大数目。在默认情况下，允许将绑定信息下发成信任用户的数目为 1024。由于交换机的硬件资源有限，真正下发为信任用户的数据取决于交换机的硬件资源。在交换机存在空闲硬件资源的情况下，如果通过此命令调整最大用户数，如果调整后的最大用户数大于调整前的用户数，则 DHCP snooping 将未能设置成信任用户的绑定信息下发到硬件成为信任用户。如果将最大用户数调小，则 DHCP snooping 根据新的最大用户数值重新调整下发到硬件的绑定信息数。当下发到硬件的绑定信息数达到最大值后，新的 DHCP 用户无法成为信任用户，则无法通过交换机访问其他网络资源。

**举例：**在端口 Ethernet1/1/1 启动绑定 dhcp snooping binding user 功能，设置端口 Ethernet1/1/1 最多允许接入 5 个用户。

Switch(Config-If-Ethernet1/1/1)#ip dhcp snooping binding user-control max-user 5

**相关命令：ip dhcp snooping binding user-control**

## 4.16.16 ip dhcp snooping information enable

**命令：ip dhcp snooping information enable**

**no ip dhcp snooping information enable**

**功能：** 设置本命令启用交换机 DHCP snooping 的 option 82 功能，本命令的 no 操作关闭交换机 DHCP snooping 的 option 82 功能。

**参数：** 无。

**缺省情况：** DHCP snooping 默认关闭 option 82 功能。

**命令模式：** 全局配置模式。

**使用指南：** 只有配置本命令 DHCP snooping 才能在 DHCP 请求报文中添加标准的 option 82 选项并转发。option 82 子选项 1(电路 ID 选项) 的形式为标准的 vlan 名加物理端口名形式，如 vlan1+ethernet1/1/12。option 82 子选项 2(远端 ID 选项) 的形式为交换机 cpu mac，如 00030f023301。如果接收到的含有 option 82 选项的 DHCP 请求报文，DHCP snooping 使用自己的 option 82 选项替换现有报文中的 option 82 选项；如果接收到的含有 option 82 选项的 DHCP 应答报文，则将报文中的 option 82 选项丢弃再转发 DHCP 报文。

**举例：** 开启交换机 dhcp snooping 的 option 82 功能。

```
Switch(config)#ip dhcp snooping enable
Switch(config)#ip dhcp snooping binding enable
Switch(config)#ip dhcp snooping information enable
```

## 4.16.17 ip dhcp snooping information option allow-untrusted

**命令：ip dhcp snooping information option allow-untrusted (replace|)**

**no ip dhcp snooping information option allow-untrusted (replace|)**

**功能：本命令用于设置允许从 DHCP** snooping 的非信任端口接收含有 option82 选项的 DHCP 报文，在设置参数 replace 时，允许替换 option82 选项；关闭此命令时，所有非信任端口将丢弃含有 option82 选项的 DHCP 报文。

**参数：无。**

**命令模式：全局配置模式**

**缺省情况：系统默认丢弃非信任端口接收的含有 option82 选项的 DHCP 报文。**

**使用指南：启用 DHCP** snooping 功能的交换机一般来说直接连接最终用户，为了防止用户私自添加 option82 选项，默认关闭 allow-untrusted 功能。启用 DHCP snooping 功能的交换机级联时，请配置级联端口为信任端口。

**举例：全局打开允许接收含有 option82 选项的 DHCP 报文功能。**

```
Switch(config)#ip dhcp snooping information option allow-untrusted
```

## 4.16.18 ip dhcp snooping information option delimiter

**命令：ip dhcp snooping information option delimiter [colon | dot | slash | space]**

**no ip dhcp snooping information option delimiter**

**功能：**该命令用来配置用户在全局定义的用来生成 option82 子选项的各参数的分隔符，该命令的 no 形式恢复分隔符为默认值，即 slash。

**参数：**无。

**缺省情况：**系统默认分隔符为 slash (“/”)。

**命令模式：**全局配置模式

**使用指南：**当用户在全局自定义了用来生成 option82 子选项（remote-id，circuit-id）的各参数后，该命令配置的分隔符用来分隔这些参数。

**举例：**配置 option82 子选项各参数分隔符为 dot（“.”）。

Switch(config)# ip dhcp snooping information option delimiter dot

## 4.16.19 ip dhcp snooping information option remote-id

**命令：ip dhcp snooping information option remote-id {standard | <remote-id>}**

**no ip dhcp snooping information option remote-id**

**功能：**本命令用于设置从端口接收的 DHCP 请求报文添加 option 82 子选项 2(远程 ID 选项)的具体内容。本命令的 no 操作把添加 option 82 子选项 2(远程 ID 选项)的形式设置为 standard。

**参数：standard** 表示默认的交换机 VLAN MAC 格式，***<remote-id>***为用户自己指定的 option 82 的 remote-id 内容，它是一个长度小于等于 64 的字符串。

**命令模式：**全局配置模式

**缺省情况：**系统默认使用 standard 形式设置 option 82 中的 remote-id。

**使用指南：**因为交换机添加的 option 82 信息要配合第三方的 DHCP 服务器使用，在交换机的标准 remote-id 形式不能满足服务器的要求时，提供一种手段由用户依据服务器情况自己指定 remote-id 的内容。

**举例：**设置 DHCP option82 选项的子选项 remote-id 为 street-1-1。

Switch(config)# ip dhcp snooping information option remote-id street-1-1

## 4.16.20 ip dhcp snooping information option self-defined remote-id

**命令：ip dhcp snooping information option self-defined remote-id {hostname | mac | string WORD}**

**no ip dhcp snooping information option self-defined remote-id**

**功能：**该命令用来配置 option82 的生成方式，用户可以自定义用来生成 option82 子选项 remote-id 的参数（集）。

**参数：** WORD 自定义的 remote-id 字符串，最大长度为 64。

**缺省情况：**缺省采用标准生成方式。

**命令模式：**全局配置模式

**使用指南：**配置本命令后，若用户没有在全局配置命令 ip dhcp snooping information option remote-id 则根据本命令的自定义生成方式来生成 option82 子选项 remote-id。对于 mac，如果是用 ascii 的形式填到报文中则采用形如 00-02-d1-2e-3a-0d 的形式，如果是 hex 形式则占 6 个字节。各个选项按照命令配置的顺序填入报文，中间用分隔符分隔（分隔符为 ip dhcp snooping information option delimiter 配置）。

**举例：**配置 option82 子选项 remote-id 的生成方式为 mac 和自定义的字符串“abc”。

Switch(config)# ip dhcp snooping information option self-defined remote-id mac string abc

## 4.16.21 ip dhcp snooping information option self-defined remote-id format

**命令：ip dhcp snooping information option self-defined remote-id format [ascii | hex]**

**功能：**该命令用来配置 snooping option82 中 remote-id 的生成格式。

**参数：**无。

**缺省情况：**系统默认生成格式为 ascii。

**命令模式：**全局配置模式

**使用指南：**本命令的生成格式指定了用命令 ip dhcp snooping information option type self-defined remote-id 生成 remote-id 的格式。

**举例：**配置 snooping option82 中 remote-id 的生成格式为 hex。

Switch(config)# ip dhcp snooping information option self-defined remote-id format hex

## 4.16.22 ip dhcp snooping information option self-defined subscriber-id

**命令：ip dhcp snooping information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac) | string WORD}**

**no ip dhcp snooping information option type self-defined subscriber-id**

**功能：**该命令用来配置 option82 的生成方式，用户可以自定义用来生成 option82 子选项 circuit-id 的参数（集）。

**参数：** WORD 自定义的 circuit-id 字符串，最大长度为 64。

**缺省情况：**缺省采用标准生成方式。

**命令模式：**全局配置模式

**使用指南：**配置本命令后，若用户没有在端口上配置 circuit-id 则根据本命令的自定义生成方式来生成 option82 子选项 circuit-id。用该命令生成的 circuit-id 的格式为：若 self-defined subscriber-id format 为 ascii，则填入的 vlan 选项形如“Vlan2”，port 选项形如“Ethernet1/1/1”，mac 选项和 remote-mac 选项形如“00-02-d1-2e-3a-0d”；若 self-defined format 为 hex，则填入的 vlan 选项占两个字节，port 选项占 4 个字节，一个字节表示 slot（对于机架式交换机，

表示插槽号；对于盒式交换机，为 1），一个字节表示 Module（默认为 0），两个字节表示端口号，从 1 开始，mac 选项和 remote-mac 选项占 6 个字节。各个选项按照命令配置的顺序填入报文，中间用分隔符分隔（分隔符为 ip dhcp snooping information option delimiter 配置）。

**举例：**配置 option82 子选项 circuit-id 的生成方式为 vlan，port 和 remote-mac。

Switch(config)#ip dhcp snooping information option self-defined subscriber-id vlan port id remote-mac

## 4.16.23 ip dhcp snooping information option self-defined subscriber-id format

**命令：ip dhcp snooping information option self-defined subscriber-id format [ascii | hex]**

**功能：**该命令用来配置 snooping option82 中 circuit-id 的生成格式。

**参数：**无。

**缺省情况：**系统默认生成格式为 ascii。

**命令模式：**全局配置模式

**使用指南：**本命令的生成格式指定了用命令 ip dhcp snooping information option type self-defined subscriber -id 生成 circuit-id 的格式。

**举例：**配置 snooping option82 中 circuit-id 的生成格式为 hex。

Switch(config)#ip dhcp snooping information option self-defined subscriber-id format hex

## 4.16.24 ip dhcp snooping information option subscriber-id

本型号交换机不支持此命令。

## 4.16.25 ip dhcp snooping information option subscriber-id format

**命令：ip dhcp snooping information option subscriber-id format {hex | acsii | vs-hp}**

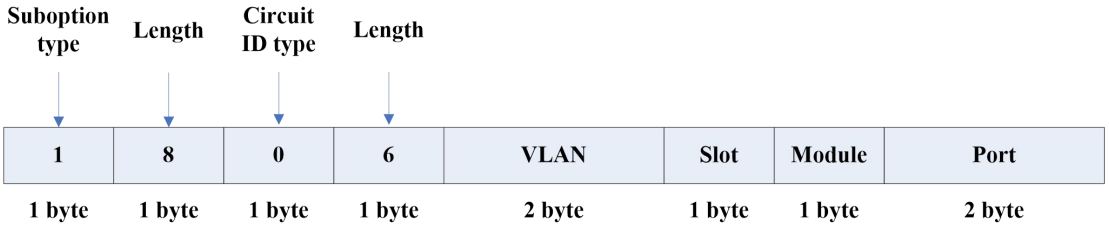
**功能：**本命令设置 DHCP snooping option82 功能 subscriber-id 默认格式。

**参数：hex** 表示 subscriber-id 为十六进制格式的 VLAN 和端口信息，**acsii** 表示 subscriber-id 为 ACSII 格式的 VLAN 和端口信息，**vs-hp** 表示 subscriber-id 兼容设备厂商 HP 的格式。

**缺省情况：**系统默认 option82 功能 subscriber-id 格式为 acsii。

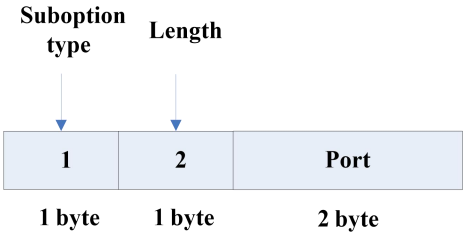
**命令模式：**全局配置模式

**使用指南：**ASCII 格式的 VLAN 和端口信息形如 Vlan1+Ethernet1/1/11。十六进制格式的 VLAN 和端口信息定义如下：




其中，VLAN 字段填写交换机 VLAN ID。Slot 对于机架式交换机，表示插槽号；对于盒式交换机，为 1。Module 默认为 0。Port 表示端口号，从 1 开始。

兼容设备厂商 HP 的 subscriber-id 格式定义如下：




其中 Port 表示端口号，从 1 开始。

**举例：**配置交换机 DHCP snooping option82 功能 subscriber-id 格式为十六进制格式。

Switch(config)#ip dhcp snooping information option subscriber-id format hex

## 4.16.26 ip dhcp snooping limit-rate

本型号交换机不支持此命令。

## 4.16.27 ip dhcp snooping timeout detection

**命令：ip dhcp snooping timeout detection <0-7200>**

**no ip dhcp snooping timeout detection**

**功能：** 设置绑定表项的流量监测超时时间。

**参数：** 可配置的流量监测超时时间范围为 0-7200，默认值为 3。单位为秒。

**命令模式：** 全局配置模式。

**使用指南：** 绑定表项处于保护模式时，每过一段时间，会检查下在该时间段内是否有该源 mac 的流量通过；若有流量通过，会继续处于保护模式；若没有流量通过，会启动静默定时器，并在该静默时间段内仍处于保护模式。若在静默时间段内，仍没有流量经过，则删除表项的保护模式。

**举例：** (Config)#ip dhcp snooping timeout detection 100

## 4.16.28 ip dhcp snooping timeout quiet

**命令：ip dhcp snooping timeout quiet <0-4294967295>**

**no ip dhcp snooping timeout quiet**

**功能：**设置绑定表项的流量监测静默时间。

**参数：**可配置的流量监测静默时间范围为 0-4294967295，默认值为 0。单位为秒。

**命令模式：**全局配置模式。

**使用指南：**绑定表项处于保护模式时，每过一段时间，会检查下在该时间段内是否有该源 mac 的流量通过；若有流量通过，会继续处于保护模式；若没有流量通过，会启动静默定时器，并在该静默时间段内仍处于保护模式。若在静默时间段内，仍没有流量经过，则删除表项的保护模式。

**举例：**(Config)#ip dhcp snooping timeout quiet 1000

## 4.16.29 ip dhcp snooping trust

**命令：ip dhcp snooping trust**

**no ip dhcp snooping trust**

**功能：**设置或删除端口的 DHCP snooping 信任属性。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**所有端口默认为非信任端口。

**使用指南：**必须全局开启 DHCP snooping，才能配置此命令。当端口从非信任端口变更为信任端口时，端口上原来的防御动作将自动去除，所有安全历史记录将清除（不会清除系统日志中的信息）。

**举例：**设置端口 ethernet1/1/1 为 DHCP snooping 信任端口。

switch(config)#interface ethernet 1/1/1

switch(Config- Ethernet 1/1/1)#ip dhcp snooping trust

## 4.16.30 ip dhcp snooping vlan

**命令：ip dhcp snooping vlan (WORD | )**

**no ip dhcp snooping vlan (WORD | )**

**功能：** 在 vlan 中使能 dhcp snooping 功能。

**参数：** 无参数。默认在所有 vlan 上使能 dhcp snooping，否则在参数指定的 vlan 上使能 dhcp snooping。

**命令模式：** 全局配置模式。

**缺省情况：** 默认不在 vlan 中使能 dhcp snooping 功能。

**使用指南：** no ip dhcp snooping vlan <vlan-id>表示在指定 vlan 上禁用 dhcp snooping 功能。

**举例：** 启动 DHCP snooping 功能。

switch(config)#ip dhcp snooping vlan 10

switch(config)#no ip dhcp snooping vlan 10

## 4.16.31 ip user helper-address

**命令：ip user helper-address <svr_addr> [port <udp_port> ] source <src_addr> [secondary]**

**no ip user helper-address [secondary]**

**功能：** 设置 HELPER SERVER 地址和端口号。

**参数：** <svr_addr>：HELPER SERVER 的 IP 地址，点分十进制形式。

udp_port：HELPER SERVER 的 UDP 端口号，范围是 1－65535，默认值是 9119。

src_addr：交换机本地管理 IP 地址，点分十进制形式。

sencondary：是否为第二 SERVER 地址。

**命令模式：** 全局配置模式。

**缺省情况：** 没有 HELPER SERVER 地址。

**使用指南：** DHCP snooping 把监控到的绑定信息发送到 HELPER SERVER 保存，当交换机异常启动之后，可以从 HELPER SERVER 恢复这些绑定数据。HELPER SERVER 功能一般集成到 DCBI 软件包中。DHCP snooping 和 HELPER SERVER 通过 UDP 协议进行通讯，并且通过重传保证数据可靠到达。HELPER SERVER 配置还可以用于从服务器下发 DOT1X 用户数据，具体用法见《dot1x 配置》章节。

可以配置两个 HELPER SERVER 地址，DHCP snooping 尽量和 PRIMARY SERVER 创建连接；只有 PRIMARY SERVER 不可达时，才和 SECONDARY SERVER 建立连接。

**请注意：**source 地址是交换机的有效管理 IP 地址，如果交换机管理 IP 地址更新，应该及时更新此配置。

**举例：** 配置本地管理 IP 地址为 100.1.1.1，主 HELPER SERVER 地址为 100.1.1.100，端口号为默认值。

```
switch(config)#interface vlan 1
switch(Config- If-Vlan1)#ip address 100.1.1.1 255.255.255.0
switch(Config-If-Vlan1)exit
switch(config)#ip user helper-address 100.1.1.100 source 100.1.1.1
```

## 4.16.32 ip user private packet version two

**命令：ip user private packet version two**

**no ip user private packet version two**

**功能：**在交换机和 DCN 内网安全管理系统 trustview 系统之间选择版本 2 私有报文进行通信。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**交换机和 DCN 接入管理系统 DCBI 之间选择使用版本 1 私有报文进行通信。

**使用指南：**如果管理员使用 DCN 接入管理系统 DCBI，则需要在交换机和 DCBI 间使用版本 1 私有报文进行通信；如果使用 DCN 内网安全管理系统 TrustView，则必须使用版本 2 的私有报文。

**举例：**交换机使用版本 2 私有报文与 DCN 内网安全管理后台系统通信。

switch(config)#ip user private packet version two

**相关命令：ip user helper-address**

## 4.16.33 show ip dhcp snooping

**命令：show ip dhcp snooping [interface [ethernet] <interfaceName>]**

**功能：**显示当前 DHCP snooping 的配置信息，或显示指定端口的防御动作记录。

**参数：*<interfaceName>*：**指定端口名称。

**命令模式：**特权和全局配置模式。

**缺省情况：**无。

**使用指南：** 如果不指定端口，那么显示当前 DHCP snooping 的配置信息，如果指定端口，那么显示指定端口的防御动作记录。

**举例：**

switch#show ip dhcp snooping

DHCP Snooping is enabled

DHCP Snooping binding arp: disabled

DHCP Snooping maxnum of action info:10

DHCP Snooping limit rate: 100(pps), switch ID: 0003.0F12.3456

DHCP Snooping droped packets: 0, discarded packets: 0

DHCP Snooping alarm count: 0, binding count: 0,

expired binding: 0, request binding: 0

| interface | trust | action | recovery | alarm num | bind num |
|---|---|---|---|---|---|
| Ethernet1/1/1 | trust | none | 0second | 0 | 0 |
| Ethernet1/1/2 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/3 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/4 | untrust | none | 0second | 0 | 1 |
| Ethernet1/1/5 | untrust | none | 0second | 2 | 0 |
| Ethernet1/1/6 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/7 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/8 | untrust | none | 0second | 0 | 1 |
| Ethernet1/1/9 | untrust | none | 0second | 0 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| Ethernet1/1/10 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/11 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/12 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/13 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/14 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/15 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/16 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/17 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/18 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/19 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/20 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/21 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/22 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/23 | untrust | none | 0second | 0 | 0 |
| Ethernet1/1/24 | untrust | none | 0second | 0 | 0 |

| 显示信息 | 解释 |
|---|---|
| DHCP Snooping is enable | DHCP Snooping 全局开启或关闭状态。 |
| DHCP Snooping binding arp | 是否启动绑定 ARP 功能。 |
| DHCP Snooping maxnum of action info | 端口防御动作数量限制。 |
| DHCP Snooping limit rate | 收包速率限制。 |
| switch ID | 交换机 ID 用户标记交换机，一般直接取 CPU MAC 地址。 |
| DHCP Snooping droped packets | 因为接收到的 DHCP 报文超越限速而丢弃的报文数量。 |
| discarded packets | 因为系统内部任务之间通讯失败而丢弃报文数量，出现这种丢包现象很可能是因为交换机 CPU 太忙碌 DHCP snooping 任务得不到调度而无法处理接收到的 DHCP 报文。 |
| DHCP Snooping alarm count: | 报警信息数量。 |
| binding count | 绑定信息数量。 |
| expired binding | 已经超时暂时还没有被删除的绑定信息数量，没有立即删除超时绑定信息可能是因为交换机需要向 helper server 通告这些信息，而 helper server 暂时还没 |

| | |
|---|---|
| | 有确认收到。 |
| request binding | REQUEST 信息数量。 |
| interface | 端口名称。 |
| trust | 端口的信任属性。 |
| action | 端口的自动防御动作。 |
| recovery | 端口自动防御动作的恢复时间。 |
| alarm num | 端口自动防御动作历史记录数目。 |
| bind num | 端口相关绑定信息数量。 |

switch#show ip dhcp snooping int Ethernet1/1/1

interface Ethernet1/1/1 user config:

trust attribute: untrust

action: none

binding dot1x: disabled

binding user: disabled

recovery interval:0(s)

Alarm info: 0

Binding info: 0

Expired Binding: 0

Request Binding: 0

| 显示信息 | 解释 |
|---|---|
| interface | 端口名称。 |
| trust attribute | 端口的信任属性。 |
| action | 端口的自动防御动作。 |
| recovery interval | 端口自动防御动作的恢复时间。 |
| maxnum of alarm info | 端口可记录的自动防御动作最大数目。 |
| binding dot1x | 端口是否启动绑定 dot1x 功能。 |
| binding user | 端口是否启动绑定 user 功能。 |
| Alarm info | 报警信息。 |
| Binding info | 绑定信息。 |
| Expired Binding | 超时绑定信息。 |
| Request Binding | REQUEST 信息。 |

## 4.16.34 show ip dhcp snooping binding all

**命令：show ip dhcp snooping binding all**

**功能：**显示当前 DHCP snooping 全局绑定信息。

**参数：**无。

**命令模式：**特权和全局配置模式。

**缺省情况：**无。

**使用指南：**该命令可查看 DHCP Snooping 全局绑定信息，每条显示表项包括 DHCP Snooping 绑定对应的 MAC 地址，IP 地址，所属端口名和 Vlan ID，以及绑定状态标识。必须全局开启 DHCP snooping，才能配置此命令。

**举例：**

```
switch#show ip dhcp snooping binding all
ip dhcp snooping static binding count:1169, dynamic binding count:0

MAC                 IP address        Interface        Vlan ID    Flag
------------------------------------------------------------------------------
00-00-00-00-11-11   192.168.40.1      Ethernet1/1/1      1          S
00-00-00-00-00-10   192.168.40.10     Ethernet1/1/2      1          D
00-00-00-00-00-11   192.168.40.11     Ethernet1/1/4      1          D
00-00-00-00-00-12   192.168.40.12     Ethernet1/1/4      1          D
00-00-00-00-00-13   192.168.40.13     Ethernet1/1/4      1          SU
00-00-00-00-00-14   192.168.40.14     Ethernet1/1/4      1          SU
00-00-00-00-00-15   192.168.40.15     Ethernet1/1/5      1          SL
00-00-00-00-00-16   192.168.40.16     Ethernet1/1/5      1          SL
------------------------------------------------------------------------------
绑定状态 flag 解释
S 静态绑定由 shell 命令配置
D 动态绑定类型
U 绑定已上传至服务器
R 静态绑定由服务器配置
O DHCP 应答带有 option82 选项
L 绑定已通知硬件驱动
X 绑定成功通知 dot1x 模块
E 绑定通知 dot1x 模块失败
```

## 4.16.35 show trustview status

**命令：show trustview status**

**功能：**显示交换机收发 DCN 内网安全管理后台系统 TrustView 各种类型私有报文的状态信息。

**参数：**无。

**命令模式：**特权和全局配置模式。

**缺省情况：**无。

**使用指南：**管理员可以使用此命令来显示交换机收发 TrustView 系统各种类型私有报文的状态信息，包括版本通知是否成功，私有报文加密是否协商成功，free resource，web 重定向网页地址，收到的强制下线报文数目，收到的强制计费报文数目。

**举例：**

```
Switch#show trustview status
Primary TrustView Server 200.101.0.9:9119
    TrustView version2 message inform successed
    TrustView inform free resource successed
    TrustView inform web redirect address successed
    TrustView inform user binding data successed
TrustView version2 message encrypt/digest enabled
Key: 08:02:33:34:35:36:37:38
Rcvd 106 encrypted messages, in which MD5-error 0 messages, DES-error 0 messages
Sent 106 encrypted messages
Free resource is 200.101.0.9/255.255.255.255
Web redirect address for unauthencated users is <http://200.101.0.9:8080>
Rcvd 0 force log-off packets
Rcvd 19 force accounting update packets
using version two private packet
```

# 4.17 DHCP option 60 和 option 43

## 4.17.1 option 43 ascii LINE

**命令：option 43 ascii LINE**

**no option 43**

**功能：**在 ip dhcp pool 模式下以 ascii 格式配置 option 43 字符串。本命令的 no 操作为删除配置的 option 43。

**参数：**LINE：以 ascii 格式配置的 option 43 字符串，字符串长度范围为 1-255。

**缺省情况：**默认没有配置 option 43 字符串。

**命令模式：**ip dhcp pool 模式

**使用指南：**无。

**举例：**以 ascii 格式配置 option 43 为"AP 1000"。

```
switch(config)#ip dhcp pool a
```

switch (dhcp-a-config)#option 43 ascii AP 1000

## 4.17.2 option 43 hex WORD

**命令：option 43 hex WORD**

**no option 43**

**功能：**在 ip dhcp pool 模式下以 hex 格式配置 option 43 字符串。本命令的 no 操作为删除配置的 option 43。

**参数：**WORD：以 hex 格式配置的 option 43 字符串，如 a1241b。

**缺省情况：**默认没有配置 option 43。

**命令模式：**ip dhcp pool 模式

**使用指南：**当使用 hex 方式配置 option 43 时，字符串需要按照 TLV（Type-Length-Value）的格式填写。比如通过 option 43 下发 ip 地址 10.1.1.1，则此处的 hex 字符串应该为 01040A010101，其中 Type=0x01，表示 IP 地址；Length=0x04，即 IP 地址的长度为 4 字节；Value=0x0A010101，即 10.1.1.1 的十六进制格式。

**举例：**以 hex 格式配置 option 43 为"01040a010101"。

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 43 hex 01040a010101

## 4.17.3 option 43 ip A.B.C.D

**命令：option 43 ip A.B.C.D**

**no option 43**

**功能：**在 ip dhcp pool 模式下以 IP 格式配置 option 43 字符串。本命令的 no 操作为删除配置的 option 43。

**参数：**A.B.C.D：以 IP 格式配置的 option 43，如 192.168.1.1。

**缺省情况：**默认没有配置 option 43。

**命令模式：**ip dhcp pool 模式

**使用指南：**用该命令配置形如"192.168.1.1"的 option 43，则填入报文中的 option 43 为"C0A80101"。

**举例：**以 IP 格式配置 option 43 为"192.168.1.1"。

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 43 ip 192.168.1.1

## 4.17.4 option 60 ascii LINE

**命令：option 60 ascii LINE**

**no option 60**

**功能：**在 ip dhcp pool 模式下以 ascii 格式配置 option 60 字符串。本命令的 no 操作为删除配置的 option 60。

**参数：**LINE：以 ascii 格式配置的 option 60 字符串，字符串长度范围为 1-255。

**缺省情况：**默认没有配置 option 60 字符串。

**命令模式：**ip dhcp pool 模式

**使用指南：**无。

**举例：**以 ascii 格式配置 option 60 为"AP 1000"。

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 60 ascii AP 1000

## 4.17.5 option 60 hex WORD

**命令：option 60 hex WORD**

**no option 60**

**功能：**在 ip dhcp pool 模式下以 hex 格式配置 option 60 字符串。本命令的 no 操作为删除配置的 option 60。

**参数：**WORD：以 hex 格式配置的 option 60 字符串，如 a1241b。

**缺省情况：**默认没有配置 option 60。

**命令模式：**ip dhcp pool 模式

**使用指南：**无。

**举例：**以 hex 格式配置 option 60 为"41502031303030"。

switch(config)#ip dhcp pool a

switch(dhcp-a-config)#option 60 hex 41502031303030

## 4.17.6 option 60 ip A.B.C.D

**命令：option 60 ip A.B.C.D**

**no option 60**

**功能：**在 ip dhcp pool 模式下以 IP 格式配置 option 60 字符串。本命令的 no 操作为删除配置的 option 60。

**参数：**A.B.C.D：以 IP 格式配置的 option 60，如 192.168.1.1。

**缺省情况：**默认没有配置 option 60。

**命令模式：**ip dhcp pool 模式

**使用指南：**用该命令配置形如"192.168.1.1"的 option 60，则匹配报文中的 option 60 为"C0A80101"。

**举例：**以 IP 格式配置 option 60 为"192.168.1.1"。

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 60 ip 192.168.1.1

# 第 5 章 路由协议相关命令

## 5.1 路由协议概述

### 5.1.1 ip prefix-list description

**命令：ip prefix-list <list_name> description <description>**

**no ip prefix-list <list_name> description**

**功能：**配置前缀列表的描述文字，本命令的 no 操作为删除描述文字。

**参数：*<list _name>***为前缀列表名称，***<description >***为描述文字。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**可以使用本命令为一个prefix-list进行说明、描述，例如prefix-list的用途、注意事项等。

**举例：**

Switch#config terminal

Switch(config)#ip prefix-list 3 description This list is used by BGP

### 5.1.2 ip prefix-list seq

**命令：ip prefix-list <list_name> [seq <sequence_number>] <deny | permit> < any | ip_addr/mask_length [ge <min_prefix_len>] [le <max_prefix_len>]>**

**no ip prefix-list <list_name> [seq <sequence_number>] [<deny | permit> < any | ip_addr/mask_length [ge <min_prefix_len>] [le <max_prefix_len>]>]**

**功能：**配置前缀列表，本命令的 no 操作为删除前缀列表。

**参数：*<list _name>***为前缀列表名称，seq表示后面所接的参数为序列号，***<sequence_number>***为序列号，deny表示拒绝该路由，permit表示接受该路由，any表示适用于所有前缀及掩码长度的报文，***ip_addr/mask_length***表示前缀地址（点分十进制）及掩码长度，ge表示大于、等于，***<min_prefix_len>***为要匹配的最小前缀长度（范围为0～32），le表示小于、等于，***<max_prefix_len>***为要匹配的最大前缀长度（范围为0～32）。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**一个prefix-list由前缀列表名标识，每个前缀列表可以包含多个表项，每个表项可以独立指定一个网络前缀形式的匹配范围，并用一个*sequence-number*来标识，*sequence-number*指明了在prefix-list中进行匹配检查的顺序。在匹配的过程中，交换机按升序依次检查由*sequence -number*标识的各个表项，只要有某一表项满足条件就意味着通过该prefix-list的过滤（不会进入下一个表项的测试）。

需要注意的是，如果定义了一个以上的前缀列表表项，那么至少应该有一个表项的匹配模式是permit模式。deny模式的表项可以先被定义，以快速的过滤掉不符合条件的路由信息。但如果所有表项都是deny模式，则任何路由都不会通过该地址前缀列表的过滤。可以在定义了多条deny模式的表项后定义一条permit 0.0.0.0/0 ge 0 le 32的表项,以允许其它所有路由信息通过。

**举例：**

Switch#config terminal

Switch(config)#ip prefix-list mylist seq 12345 deny 10.0.0.0/8 le 22 ge 14

## 5.1.3 ip prefix-list sequence-number

**命令：ip prefix-list sequence-number**

**no ip prefix-list sequence-number**

**功能：**启动序号自动生成功能，本命令的no操作为关闭前缀列表条目序号。

**参数：**无。

**缺省情况：**启动序号自动生成功能。

**命令模式：**全局配置模式。

**使用指南：**可以使用本命令的no操作来关闭前缀列表条目序号。

**举例：**

switch(config)#no ip prefix-list sequence-number

## 5.1.4 match as-path

**命令：match as-path <list-name>**

**no match as-path [<list-name>]**

**功能：**配置匹配BGP路由信息的AS路径域，本命令的no操作为删除配置。

**参数：*<list-name >***为 access-list 名称。

**命令模式：**route-map 配置模式。

**使用指南：**本命令按 as-path list 中指定的规则对 BGP 路由信息的 AS 路径域进行匹配，如果匹配成功，则执行 route-map 中的 permit 或 deny 操作。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match as-path 60

## 5.1.5 match community

**命令：match community <community-list-name | community-list-num > [exact-match]**

**no match community [<community-list-name | community-list-num > [exact-match]]**

**功能：**配置匹配BGP路由信息的团体属性，本命令的no操作为删除配置。

**参数：<community-list-name >**为community-list名称，**<community-list-num >**为community-list序号，取值范围为1～99（标准ACL）或100～199（扩展ACL），**[exact-match]**表示精确匹配。

**命令模式：**route-map 配置模式。

**使用指南：**本命令按 community list 中指定的规则对 BGP 路由信息的团体属性进行匹配，如果匹配成功，则执行 route-map 中的 permit 或 deny 操作。团体属性通过 match 和 set 可以提供对大量路由应用策略的能力。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match community 100 exact-match

## 5.1.6 match interface

**命令：match interface <interface-name >**

**no match interface [<interface-name >]**

**功能：**配置对接口匹配，本命令的no操作为删除配置。

**参数：<*interface-name* >**为接口名称。

**命令模式：**route-map 配置模式。

**使用指南：**本命令按路由中的下一跳接口信息进行匹配，如果匹配成功，则执行 route-map 中的 permit 或 deny 操作。本命令仅用于 RIP 和 OSPF 协议。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match interface vlan1

## 5.1.7 match ip

**命令：match ip <address | next-hop> <ip-acl-name | ip-acl-num | prefix-list list-name>**

**no match ip <address | next-hop> [<ip-acl-name | ip-acl-num | prefix-list list-name>]**

**功能：**配置匹配路由前缀或下一跳，本命令的no操作为删除配置。

**参数：<address >**表示匹配的是路由前缀，**<next-hop>**表示匹配的是路由下一跳，**<*ip-acl-name* >**为 ip access-list 名称，**<*ip-acl-num* >**为 ip access-list 序号，取值范围为 1～199 或 1300～2699（扩展范围），**prefix-list** 表示要按前缀列表规则进行匹配，***list-name*** 为前缀列表名称。

**命令模式：**route-map 配置模式。

**使用指南：**本命令按路由中的路由前缀或下一跳信息进行匹配，如果匹配成功，则执行 route-map 中的 permit 或 deny 操作。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match ip address prefix-list mylist

## 5.1.8 match ipv6 address

**命令：match ipv6 address *<ipv6-acl-name | prefix-list list-name>***

**no match ipv6 address [*<ipv6-acl-name | prefix-list list-name>*]**

**功能：**配置匹配 ipv6 路由前缀，本命令的 no 操作为删除配置。

**参数：address** 表示匹配的是路由前缀，***<ipv6-acl-name >***为 ipv6 access-list 名称，**prefix-list** 表示要按前缀列表规则进行匹配，**list-name** 为前缀列表名称。

**命令模式：**route-map 配置模式。

**使用指南：**本命令按路由中的路由前缀进行匹配，如果匹配成功，则执行 route-map 中 permit deny 操作。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match ipv6 address prefix-list mylist

## 5.1.9 match ipv6 next-hop

**命令：match ipv6 next-hop <ipv6-address>**

**no match ipv6 next-hop [<ipv6-address>]**

**功能：**配置匹配 ipv6 路由下一跳，本命令的 no 操作为删除配置。

**参数：next-hop** 表示匹配的是路由下一跳，***ipv6-address*** 表示下一跳的接口 ipv6 地址。

**命令模式：**route-map 配置模式。

**使用指南：**本命令按路由中的下一跳信息进行匹配，如果匹配成功，则执行 route-map 中的 permit 或 deny 操作。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)# match ipv6 next-hop 2000::1

## 5.1.10 match metric

**命令：match metric <metric-val>**

**no match metric [<metric-val>]**

**功能：**配置匹配路由信息的度量值，本命令的no操作为删除配置。

**参数：<*metric-val*>**为度量值，范围为 0～4294967295。

**命令模式：**route-map 配置模式。

**使用指南：**本命令按路由中的度量值进行匹配，如果匹配成功，则执行 route-map 中的 permit 或 deny 操作。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match metric 60

## 5.1.11 match origin

**命令：match origin <egp | igp | incomplete>**

**no match origin <egp | igp | incomplete>**

**功能：**配置匹配BGP路由信息的源，本命令的no操作为删除配置。

**参数：egp** 表示路由学习自外部网关协议，**igp** 表示路由学习自内部网关协议，**incomplete** 表示路由源不能确定。

**命令模式：**route-map 配置模式。

**使用指南：**本命令按 BGP 路由中的源信息进行匹配，如果匹配成功，则执行 route-map 中的 permit 或 deny 操作。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match origin egp

## 5.1.12 match route-type

**命令：match route-type external <type-1 | type-2>**

**no match route-type external [<type-1 | type-2>]**

**功能：**配置匹配OSPF路由信息的路由类型，本命令的no操作为删除配置。

**参数：type-1** 表示匹配 OSPF 类型 1 外部路由，**type-2** 表示匹配 OSPF 类型 2 外部路由。

**命令模式：**route-map 配置模式。

**使用指南：**本命令按 OSPF 路由的类型进行匹配（OSPF AS-external LSA 类型为 type 1 或 type 2），如果匹配成功，则执行 route-map 中的 permit 或 deny 操作。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match route-type external type-1

## 5.1.13 match tag

**命令：match tag <tag-val>**

**no match tag [<tag-val>]**

**功能：**配置匹配OSPF路由信息的tag域，本命令的no操作为删除配置。

**参数：<*tag-val*>**为 tag 值，范围为 0～4294967295。

**命令模式：**route-map 配置模式。

**使用指南：**本命令按 OSPF 路由中的 tag 值进行匹配，如果匹配成功，则执行 route-map 中的 permit 或 deny 操作。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match tag 60

## 5.1.14 route-map

**命令：route-map <map_name> {deny | permit} <sequence_num>**

**no route-map <map_name> [{deny | permit} <sequence_num>]**

**功能：**配置 route-map，并且进入 route-map 模式，本命令的 no 操作为删除 route-map。

**参数：<*map_name*>**为route-map名称，**permit**指定所定义的route-map的匹配模式为允许模式，**deny**指定所定义的route-map的匹配模式为拒绝模式（此模式下**set**子句不会被执行），**<*sequence_num*>**为route-map序列号，取值范围为1～65535。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**一个route-map可由多个节点构成，每个节点是进行匹配检查的一个单元，节点间依据顺序号*sequence-number*标识检查顺序。permit表示当路由项满足该节点的所有match子句时，认为通过该节点的过滤，并执行该节点的set子句，不进入下一个节点的测试；如路由项不满足该节点的match子句将进入下一个节点继续测试。deny表示set子句不会被执行，当路由项满足该节点的所有match子句时被拒绝通过该节点，不进入下一个节点的测试；如路由项不满足该节点的match子句，将进入下一个节点继续测试。不同节点间是或的关系，即交换机依次检查route-map的各个节点,通过route-map的某一节点就意味着通过该route-map过滤。

需要注意的是，如果定义了一个以上的route-map节点，route-map的各个节点中至少应该有一个节点的匹配模式是permit。当一个route-map用于路由信息过滤时，如果某路由信息没有通过任一节点，则认为该路由信息没有通过该route-map。当route-map的所有节点都是deny模式时，所有路由信息都不会通过该route-map。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match as-path 60

Switch(config-route-map)#set weight 30

## 5.1.15 set aggregator

**命令：set aggregator as <as-number> <ip_addr>**

**no set aggregator as [<as-number> <ip_addr>]**

**功能：**配置为BGP聚合者分配一个AS号，本命令的no操作为删除配置。

**参数：<*as-number*>**为 AS 号，**<*ip_addr*>**为聚合者的 ip 地址，点分十进制形式。

**命令模式：**route-map 配置模式。

**使用指南：**要使用本命令，需首先定义一条 match 语句。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set aggregator as 200 10.1.1.1

## 5.1.16 set as-path

**命令：set as-path prepend <as-num>**

**no set as-path prepend [<as-num>]**

**功能：**配置在BGP路由信息的AS路径域增加AS号，本命令的no操作为删除配置。

**参数：<*as-num*>**为 AS 号，取值范围为 1-4294967295。可用十进制表示，如 6553700；也可用分隔符方式表示，如 100.100。可连续循环输入多个。

**命令模式：**route-map 配置模式。

**使用指南：**通过在 BGP 的 AS 域增加 AS 号，可以增加 AS 路径长度，从而影响邻居最佳路径的选择。要使用本命令，需首先定义一条 match 语句。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set as-path prepend 200 100.100

## 5.1.17 set atomic-aggregate

**命令：set atomic-aggregate**

**no set atomic-aggregate**

**功能：**配置BGP路由信息的原子聚合属性，本命令的no操作为删除配置。

**参数：**无。

**命令模式：**route-map 配置模式。

**使用指南：**BGP 使用原子聚合属性告知其它 BGP 发言者，本地系统选择了一个次具体的路由，而没有选择包含在其内的更具体的路由。要使用本命令，需首先定义一条 match 语句。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set atomic-aggregate

## 5.1.18 set comm-list

**命令：set comm-list <community-list-name | community-list-num > delete**

**no set comm-list <community-list-name | community-list-num > delete**

**功能：**配置BGP从入站或出站路由信息中删除团体属性，本命令的no操作为删除配置。

**参数：<*community-list-name*>**为团体列表名称，**<*community-list-num*>**为团体列表序号，取值范围为 1～99（标准团体列表）或 100～199（扩展团体列表）。

**命令模式：**route-map 配置模式。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set comm-list 100 delete

## 5.1.19 set community

**命令：set community [AA:NN] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]**

**no set community [AA:NN] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]**

**功能：**配置BGP路由信息的团体属性，本命令的no操作为删除配置。

**参数：[*AA:NN*]**为团体属性值，**[internet]**表示因特网范围，**[local-AS]**表示本路由不发送到 local AS 外（可以在联盟的子 AS 之间发布），**[no-advertise]**表示本路由不发送给任何邻居，**[no-export]**表示本路由不发送给 EBGP 邻居，**[none]**表示从本路由前缀中删除团体属性，**[additive]**表示添加在已有团体属性后。

**命令模式：**route-map 配置模式。

**使用指南：**要使用本命令，需首先定义一条 match 语句。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set community local-as additive

## 5.1.20 set extcommunity

**命令：set extcommunity <rt | soo> <AA:NN>**

**no set extcommunity <rt | soo> [<AA:NN>]**

**功能：**配置BGP路由信息的扩展团体属性，本命令的no操作为删除配置。

**参数：<*rt*>**为路由目标（route target），**<*soo*>**为源站点（site of origin），**<*AA:NN*>**为团体属性值，其中 AA 为 AS 号，取值范围为 1-4294967295。可用十进制表示，如 6553700；也可用分隔符方式表示，如 100.100。NN 为任意两字节数字。

**命令模式：**route-map 配置模式。

**使用指南：**要使用本命令，需首先定义一条 match 语句。

**举例：**设置 rt 为 100:10。

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set extcommunity rt 100:10

设置 soo 为 200.200:10

Switch(config)#route-map r1 permit 10

Switch(config-route-map)#set extcommunity soo 200.200:10

## 5.1.21 set ip next-hop

**命令：set ip next-hop <ip_addr>**

**no set ip next-hop [<ip_addr>]**

**功能：**配置路由的下一跳，本命令的no操作为删除配置。

**参数：<*ip_addr* >**为下一跳的 ip 地址，点分十进制形式。

**命令模式：**route-map 配置模式。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set ip next-hop 10.2.2.2

## 5.1.22 set local-preference

**命令：set local-preference <pre_val>**

**no set local-preference [<pre_val>]**

**功能：**配置BGP路由的本地优先级，本命令的no操作为删除配置。

**参数：<*pre_val* >**为本地优先级值，范围为 0～4294967295。

**命令模式：**route-map 配置模式。

**使用指南：**本地优先级属性是给予一个路由的优先程度，并使其与同一目的地的其它路由比较，较高的本地优先级表示该路由更为优选。本地优先级只在本 AS 内有效，不会传送给 EBGP 邻居。要使用本命令，需首先定义一条 match 语句。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set local-preference 60

## 5.1.23 set metric

**命令：set metric < metric_val>**

**no set metric [<metric_val>]**

**功能：**配置路由的度量值，本命令的no操作为删除配置。

**参数：<*metric_val* >**为度量值，范围为 1～4294967295。

**命令模式：**route-map 配置模式。

**使用指南：**度量值可以影响外部邻居到本 AS 的路径选择。度量值越小，优先程度越高。一般情况下，只比较同一 AS 内的邻居的路径的度量值。要扩展比较不同 AS 邻居路径的度量值，需配置命令 bgp always-compare-med。要使用本命令，需首先定义一条 match 语句。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set metric 60

## 5.1.24 set metric-type

**命令：set metric-type <type-1 | type-2>**

**no set metric-type [<type-1 | type-2>]**

**功能：**配置OSPF路由信息的度量类型，本命令的no操作为删除配置。

**参数：type-1** 表示匹配 OSPF 类型 1 外部路由，**type-2** 表示匹配 OSPF 类型 2 外部路由。

**命令模式：**route-map 配置模式。

**使用指南：**要使用本命令，需首先定义一条 match 语句。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set metric-type type-1

## 5.1.25 set origin

**命令：set origin <egp | igp | incomplete >**

**no set origin [<egp | igp | incomplete >]**

**功能：**配置BGP路由信息的源码，本命令的no操作为删除配置。

**参数：egp** 表示路由学习自外部网关协议，**igp** 表示路由学习自内部网关协议，**incomplete** 表示路由源不能确定。

**命令模式：**route-map 配置模式。

**使用指南：**要使用本命令，需首先定义一条 match 语句。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set origin egp

## 5.1.26 set originator-id

**命令：set originator-id <ip_addr>**

**no set originator-id [<ip_addr>]**

**功能：**配置BGP路由信息的源ip地址，本命令的no操作为删除配置。

**参数：*<ip_addr>***为路由的源 ip 地址，点分十进制形式。

**命令模式：**route-map 配置模式。

**使用指南：**要使用本命令，需首先定义一条 match 语句。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set originator-id 10.1.1.1

## 5.1.27 set tag

**命令：set tag <tag_val>**

**no set tag [<tag_val>]**

**功能：**配置OSPF路由信息的tag域，本命令的no操作为删除配置。

**参数：*<tag-val >***为 tag 值，范围为 0～4294967295。

**命令模式：**route-map 配置模式。

**使用指南：**AS-external-LSA类型的LSA有一个route-tag域，该域一般是由其它路由协议标记的。要使用本命令，需首先定义一条match语句。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set tag 60

## 5.1.28 set vpnv4 next-hop

**命令：set vpnv4 next-hop <ip_addr>**

**no set vpnv4 next-hop [<ip_addr>]**

**功能：**配置BGP VPNv4路由信息的下一跳，本命令的no操作为删除配置。

**参数：*<ip_addr>***为 VPNv4 路由的下一跳 ip 地址，点分十进制形式。

**命令模式：**route-map 配置模式。

**使用指南：**要使用本命令，需首先定义一条 match 语句。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set vpnv4 next-hop 10.1.1.1

## 5.1.29 set weight

**命令：set weight <weight_val>**

**no set weight [<weight_val>]**

**功能：**配置BGP路由信息的权重值，本命令的no操作为删除配置。

**参数：*<weight_val>***为权重值，范围为 0～4294967295。

**命令模式：**route-map 配置模式。

**使用指南：**权重值用于帮助最佳路径的选择，只在本交换机有效。在到同一目的地有多条路由的情况下，权重值越高越优先。要使用本命令，需首先定义一条 match 语句。

**举例：**

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set weight 60

## 5.1.30 show ip prefix-list <list-name>

**命令：show ip prefix-list [<list-name> [<ip_addr/len> [first-match | longer] | seq <sequence-number>]]**

**功能：**按前缀列表名称进行显示。

**参数：*<list-name>***为前缀列表名称，***<ip_addr/len>***为前缀 ip 地址和掩码长度，**first-match** 表示显示对特定 ip 地址而言匹配的第一个路由表，**longer** 表示要查找更长的前缀，**seq** 表示按序列号进行显示，***<sequence-number>***为序列号，范围为 0～4294967295。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**不指定前缀列表的名字时，会显示所有的前缀列表。

**举例：**

Switch#show ip prefix-list

ip prefix-list 1: 1 entries

deny any

ip prefix-list mylist: 1 entries

deny 1.1.1.1/8

Switch#show ip prefix-list mylist 1.1.1.1/8

seq 5 deny 1.1.1.1/8 (hit count: 0, refcount: 0)

| 显示内容 | 解释 |
|---|---|

| | |
|---|---|
| ip prefix-list mylist: 1 entries | 显示名称为 mylist 的前缀列表，该前缀列表包含 1 个实体 |
| seq 5 deny 1.1.1.1/8 (hit count: 0, refcount: 0) | 表示序列号为 5 的前缀列表内容，hit count: 0 表示被命中 0 次，refcount: 0 表示引用 0 次 |

## 5.1.31 show ip prefix-list <detail | summary>

**命令：show ip prefix-list [<detail | summary> [<list-name>] ]**

**功能：**显示前缀列表内容。

**参数：detail** 表示显示详细信息，**summary** 表示显示摘要信息，***<list-name>***为前缀列表名称。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**不指定前缀列表的名字时，会显示所有的前缀列表。

**举例：**

Switch#show ip prefix-list detail mylist

ip prefix-list mylist:

count: 2, range entries: 0, sequences: 5 - 10

seq 5 deny 1.1.1.1/8 (hit count: 0, refcount: 0)

seq 10 permit 2.2.2.2/8 (hit count: 0, refcount: 0)

Switch#show ip prefix-list summary mylist

ip prefix-list mylist:

count: 2, range entries: 0, sequences: 5 - 10

| 显示内容 | 解释 |
|---|---|
| ip prefix-list mylist: | 显示名称为 mylist 的前缀列表 |
| count: 2, range entries: 0, sequences: 5 - 10 | count: 2 表示 2 个前缀列表实体，sequences: 5 – 10 显示序列号，5 为起始序列号，10 为尾序列号 |
| deny 1.1.1.1/8 (hit count: 0, refcount: 0) | deny 1.1.1.1/8 为前缀列表实体具体内容，hit count: 0 表示被命中 0 次，refcount: 0 表示引用 0 次 |

## 5.1.32 show route-map

**命令：show route-map**

**功能：**显示 route-map 内容。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**无。

**举例：**

```
Switch# show route-map
route-map a, deny, sequence 10
  Match clauses:
    as-path 60
  Set clauses:
    metric 10
```

| 显示内容 | 解释 |
| --- | --- |
| route-map a, deny, sequence 10 | route-map a 表示 route-map 的名称为 a，deny 表示模式为 deny，sequence 10 表示序列号为 10 |
| Match clauses: | Match 子句 |
| as-path 60 | Match 子句的具体内容 |
| Set clauses: | Set 子句 |
| metric 10 | Set 子句的具体内容 |

### 5.1.33 show router-id

**命令：show router-id**

**功能：**显示路由器的 router-id 信息。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**举例：**

例 1：

```
Switch#show router-id
Router ID: 20.1.1.1 (automatic)
```

例 2：

```
Switch#show router-id
Router ID: 20.1.1.2 (config)
```

## 5.2 静态路由

### 5.2.1 ip route

**命令：ip route {<ip-prefix> <mask> | <ip-prefix>/<prefix-length>} {<gateway-address> | <gateway-interface>} [<distance>]**

**no ip route {<ip-prefix> <mask> | <ip-prefix>/<prefix-length>} [<gateway-address> | *<gateway-interface>*] [*<distance>*]**

**功能：**配置静态路由；本命令的 no 操作为删除静态路由。

**参数：*<ip-prefix>***和***<mask>***分别为目的 IP 地址和子网掩码，点分十进制格式；***<ip-prefix>***和***<prefix-length>***分别为目的 IP 地址和前缀长度；***<gateway-address>***为下一跳的 IP 地址，点分十进制格式；***<gateway-interface>***为下一跳接口，***< distance >***为路由管理距离值，取值范围为 1～255。

**缺省情况：**静态路由缺省管理距离值为 1。

**命令模式：**全局配置模式。

**使用指南：**在配置静态路由的下一跳时，可采用指定路由数据包发送下一跳 IP 地址或者出接口方式。

神州数码三层交换机的各种路由类型缺省的 distance 值为：

| 路由类型 | Distance 值 |
|---|---|
| 直连路由 | 0 |
| 静态路由 | 1 |
| OSPF | 110 |
| RIP | 120 |
| IBGP | 200 |
| EBGP | 20 |

在不改变各种路由管理距离值的情况下，直连路由优先级最高，依次是静态路由、EBGP、OSPF、RIP、IBGP。

**举例：**

例 1．添加一条静态路由。

Switch(config)#ip route 1.1.1.0 255.255.255.0 2.1.1.1

例 2．添加缺省路由。

Switch(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1

## 5.2.2 ip route vrf

**命令：ip route vrf <vrf-name> {<ip-prefix> <mask>|<ip-prefix/prefix-length>} {<gateway-address>|null0} [<1-255>]**

**no ip route vrf <vrf-name> {<ip-prefix> <mask>|<ip-prefix/prefix-length>} {<gateway-address>|null0} [<1-255>]**

**功能：**为指定 VRF 配置静态路由。使用本命令前必须先配置成功 VPN 路由转发实例；no 命令删除已配置静态路由。

**参数：*<vrf-name>***：指定的 VRF 名称；

***<ip-prefix>***：为目的 IP 地址；

***<mask>***：子网掩码，点分十进制格式；

***<prefix-length>***：前缀长度；

***<gateway-address>***：下一条地址；

**null0**：黑洞路由；

<***1-255***>：管理距离。

**缺省情况**：默认不配置。

**命令模式**：全局配置模式。

**举例**：配置 VRF-A 的静态路由，目的 IP 为 10.1.1.10，掩码 24 位，下一跳为 10.1.1.1，管理距离默认：

Switch(config)# ip route vrf VRF-A 10.1.1.10 255.255.255.0 10.1.1.1

Switch(config)#

## 5.2.3 show ip route

**命令：show ip route [<destination>|<destination >/<length>|connected | static | rip| ospf | bgp | isis| kernel| statistics| database [connected | static | rip| ospf | bgp | isis| kernel] |fib [statistics]]**

**功能**：显示路由表。

**参数**：<***destination***>为目标网络地址；<***destination >/<length***>为目标网络地址加上前缀长度；**connected** 为直连路由；**static** 为静态路由；**rip** 为 RIP 路由；**ospf** 为 OSPF 路由； **bgp** 为 BGP 路由；**isis** 为 ISIS 路由；**kernel** 为核心路由；**statistics** 显示路由条数；**database** 为路由数据库；**fib** 为核心路由表。

**命令模式**： 所有模式

**使用指南**：显示路由表的内容，包括：路由类型、目的网络、掩码、下一跳地址、接口等。

**举例**：switch#show ip route

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default

Gateway of last resort is 210.0.0.3 to network 0.0.0.0

S* 0.0.0.0/0 [1/1] via 210.0.0.3, Vlan1

C 127.0.0.0/8 is directly connected, Loopback

O IA 172.16.11.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47

O IA 172.16.12.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47

O IA 172.16.13.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47

O IA 172.16.14.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47

O IA 172.16.15.0/24 [110/50] via 210.14.0.1, Vlan3014, 00:00:47

O E2 172.16.100.0/24 [110/0] via 210.14.0.1, Vlan3014, 00:00:46

| 显示信息 | 解释 |
| --- | --- |
| C - connected | 直连路由，即与三层交换机直接相连的网段； |
| S – static | 静态路由，由用户手工配置的路由； |
| R - RIP derived | RIP 路由，三层交换机通过 RIP 协议得到的； |
| O - OSPF derived | OSPF 路由，三层交换机通过 OSPF 协议得到的； |
| A- OSPF ASE | OSPF 引入的路由 |
| B- BGP derived | BGP 路由，路由通过 BGP 协议得到 |
| Destination | 目标网络； |
| Mask | 目标网络的掩码； |
| Nexthop | 下一跳 IP 地址； |
| Interface | 下一跳经过的三层交换机接口； |
| Preference | 路由的优先级，如果到达目标网络还有其它类型的路由，在核心路由表中只显示优先级高的路由信息。 |

## 5.2.4 show ip route vrf

**命令：show ip route vrf <name> [connected | static | rip| ospf | bgp | isis| kernel|statistics| database[connected | static | rip| ospf | bgp | isis|kernel] ]**

**show ip route fib vrf <name> [default|main|local]**

**功能：显示路由表。**

**参数：*<name>*** 是 VPN 路由转发实例的名称；***<destination>*** 为目标网络地址；***<destination >/<length>***为目标网络地址加上前缀长度； **connected** 为直连路由；**static** 为静态路由；**rip** 为 RIP 路由；ospf 为 OSPF 路由； **bgp** 为 BGP 路由；isis 为 ISIS 路由；kernel 为核心路由；statistics 显示路由条数；database 为路由数据库；fib 为核心路由表。

**命令模式：**所有模式

**使用指南：**显示 VPN 路由表的内容，包括：路由类型、目的网络、掩码、下一跳地址、接口等。

## 5.2.5 show ip route fib

**命令：show ip route fib**

**功能：** 显示路由表的内容，包括：路由类型、目的网络、掩码、下一跳地址、接口等。

**命令模式：** 特权和配置模式。

**使用指南：** 使用 show ip route fib 命令可以显示路由表中关于静态路由的目的 IP 地址、网络掩码以及下一跳 IP 地址或转发接口等信息。

**举例：**

```
Switch#show ip route fib
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
       A - OSPF ASE, B - BGP derived

   Destination      Mask            Nexthop         Interface       Pref
C  2.2.2.0          255.255.255.0   0.0.0.0         vlan1           0
S  6.6.6.0          255.255.255.0   2.2.2.9         vlan1           1
```

其中，S 表示静态路由，即目的网络地址为 6.6.6.0、网络掩码为 255.255.255.0、下一跳地址为 2.2.2.9 以及转发接口为以太口 vlan1 的一条路由为静态路由，它的优先级为 1。

# 5.3 RIP

## 5.3.1 accept-lifetime

**命令：accept-lifetime <start-time> {<end-time>| duration<seconds>| infinite}**

**no accept-lifetime**

**功能：**使用本命令指明密匙链上的一个密匙接收为合法的时间段。本命令的 no 操作取消此配置。

**参数：*<start-time>***参数指明时间段的起始时间，它的形式如下：

***<start-time>*={*<hh:mm:ss> <month> <day> <year>*|*<hh:mm:ss> <day> <month> <year>*}**

***<hh:mm:ss>***用小时、分钟和秒的指明 **accept-lifetime** 生效的具体时间；

***<day>***指明生效的具体日期，取值范围 1-31；

***<month>***指明生效的具体月份，用月份英文的头三个字母表示，如 Jan；

***<year>***指明开始生效的具体年份，取值范围 1993-2035；

***<end-time>***参数指明时间段的到期时间，它的形式如下：

***<end-time>*={*<hh:mm:ss> <month> <day> <year>*|*<hh:mm:ss> <day> <month> <year>*}**

***<hh:mm:ss>***用小时、分钟和秒的指明 **accept-lifetime** 到期的具体时间；

***<day>***指明到期的具体日期，取值范围 1-31；

***<month>***指明到期的具体月份，用月份英文的头三个字母表示，如 Jan；

***<year>***指明到期的具体年份，取值范围 1993-2035；

***<seconds>***密匙持续有效的时间长短，以秒为单位，取值范围 1-2147483646；

**infinite** 密匙永远不过期。

**缺省情况：**没有缺省配置。

**命令模式：**keychain-key 模式。

**使用指南：**无。

**举例：**下面的例子显示了在名为 mychain 的密匙链上为 key 1 所作的 accept-lifetime 设置。

Switch# config terminal

Switch(config)# key chain mychain

Switch(config-keychain)# key 1

Switch(config-keychain-key)# accept-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006

**相关命令：**

**key**

**key-string**

**key chain**

**send-lifetime**

## 5.3.2 address-family ipv4

**命令：address-family ipv4 vrf <*vrf-name*>**

**no address-family ipv4 vrf <*vrf-name*>**

**功能：配置本命令使能 VRF 间路由信息交换并且进入地址族模式，本命令的 no 操作删除与该 VPN 路由/转发实例相关联的 RIP 实例。**

**参数：<*vrf-name*>**指明了 VPN 路由/转发实例的名称。

**命令模式：路由模式。**

**使用指南：本命令只用于 PE 路由器。在使用本命令前，必须首先使用命令 ip** vrf 生成一个 VPN 路由/转发实例，然后使用本命令可以将该 VPN 路由/转发实例与 RIP 实例关联起来。

**举例：Switch#** config terminal

Switch(config)# router rip

Switch(config-router)# address-family ipv4 vrf VRF1

## 5.3.3 clear ip rip route

**命令：clear ip rip route {<A.B.C.D/M>|kernel|static|connected|rip|ospf|isis|bgp|all}**

**功能：**从 RIP 路由表中清除特定的路由。

**参数：<*A.B.C.D/M*>** 从 RIP 路由表中清除与目的地址相符的路由，A.B.C.D/M 表示目的地址的 IP 地址前缀与前缀长度；

**kernel** 从 RIP 路由表中删去核心路由；

**static** 从 RIP 路由表中删去静态路由；

**connected** 从 RIP 路由表删去直连路由；

**rip** 从 RIP 路由表中仅删去 RIP 路由；

**ospf** 从 RIP 路由表中仅删去 OSPF 路由；

**isis** 从 RIP 路由表中仅删去 ISIS 路由；

**bgp** 从 RIP 路由表中仅删去 BGP 路由；

**all** 删去 RIP 路由表中的所有路由。

**缺省情况：**没有缺省配置。

**命令模式：**特权模式。

**使用指南：**使用带 all 参数的本命令时，将删除 RIP 路由表中的所有路由。删除的路由除了 rip 路由外，其他引入的所有路由都会立即恢复。动态学习到的 RIP 路由只能通过再次学习而恢复。

**举例：**Switch# clear ip rip route 10.0.0.0/8

Switch# clear ip rip route ospf

## 5.3.4 debug rip

**命令：debug rip [events| nsm| packet[recv|send][detail]| all]**

**no debug rip [events| nsm| packet[recv|send][detail]| all]**

**功能：**用来打开RIP的各种调试开关，显示各类调试信息。no操作关闭相应的调试开关。

**参数：**events表示显示RIP events的调试信息；

nsm表示显示RIP与NSM的之间的通讯信息；

packet表示显示RIP数据报的调试信息；

recv表示显示接收到的数据报的信息；

send表示显示发出的数据报的信息；

detail表示显示接收或者发出的数据报的具体信息。

**默认情况：**不打开调试开关。

**命令模式：**特权模式与全局模式。

**举例：**Switch# debug rip packet

Switch#1970/01/11 01:01:43 IMI: SEND[Vlan1]: Send to 224.0.0.9:520

1970/01/11 01:01:43 IMI: SEND[Vlan1]: Send to 224.0.0.9:520

1970/01/11 01:01:47 IMI: RECV[Vlan1]: Receive from 20.1.1.2:520

## 5.3.5 debug rip redistribute message send

**命令：debug rip redistribute message send**

**no debug rip redistribute message send**

**功能：**打开 RIP 进程引入其他 OSPF 不同进程、BGP 等协议的路由的命令下发调试开关。本命令的 no 操作为关闭 RIP 进程引入其他 OSPF 不同进程、BGP 等协议的路由的命令下发调试开关。

**参数：**无。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#debug rip redistribute message send

Switch#no debug rip redistribute message send

## 5.3.6 debug rip redistribute route receive

**命令：debug rip redistribute route receive**

**no debug rip redistribute route receive**

**功能：**打开 RIP 进程收到 nsm 发来的路由信息的调试开关。本命令的 no 操作为关闭 RIP 进程收到 nsm 发来的路由信息的调试开关。

**参数：**无。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#debug rip redistribute route receive

Switch#no debug rip redistribute route receive

## 5.3.7 default-information originate

**命令：default-information originate**

**no default-information originate**

**功能：**允许将网络 0.0.0.0 重新分配到 RIP 中，本命令的 no 操作禁用此功能。

**参数：**无。

**缺省情况：**禁用。

**命令模式：**路由模式与地址族模式。

**使用指南：**本命令告诉路由器将目的地为 0.0.0.0 的默认路由插入到 RIP 路由数据库中，并且与通告其他路由一样来通告该路由。

**举例：**Switch# config terminal

Switch(config)# router rip

Switch(config-router)# default-information originate

## 5.3.8 default-metric

**命令：default-metric <value>**

**no default-metric**

**功能：**设定引入路由的缺省路由权值；本命令的 no 操作恢复缺省值 1。

**参数：*<value>***为所要设定的路由权值，取值范围 1～16。

**缺省情况：**缺省的路由权值为 1。

**命令模式：**路由模式与地址族模式。

**使用指南：default-metric** 命令用于设定将其它路由协议的路由引入到 RIP 路由时使用的缺省路由权值。当使用 **redistribute** 命令引入其它协议的路由时，如果不指定具体的路由权值，则以 **default-metric** 所指定的缺省路由权值引入。

**举例：**设定在 RIP 路由中引入其它路由协议的缺省路由权值为 3。

Switch(config-router)#default-metric 3

**相关命令：redistribute**

## 5.3.9 distance

**命令：distance <number> [<A.B.C.D/M> ] [<access-list-name|access-list-number >]**

**no distance [<A.B.C.D/M> ]**

**功能：**利用本命令设置管理距离。本命令的 no 操作恢复缺省值 120。

**参数：*<number>***指定距离的值，取值范围 1-255。***<A.B.C.D/M>***指定网络前缀和前缀长度。

***<access-list-name|access-list-number >***指定所应用的访问列表号或者名字。

**缺省情况：**缺省情况下 RIP 的管理距离为 120。

**命令模式：**路由模式与地址族模式。

**使用指南：**当到达同一目的地存在来自于两个不同路由协议的路由时，管理距离用来选择路由。路由协议的管理距离值越小，表明由该协议得到的路由越可靠。

**举例：**Switch# config terminal

Switch(config)# router rip

Switch(config-router)# distance 8 10.0.0.0/8 mylist

## 5.3.10 distribute-list

**命令：distribute-list{<access-list-number|**

**access-list-name> |prefix<prefix-list-name>} {in|out} [<ifname>]**

**no distribute-list{<access-list-number|**

**access-list-name> |prefix<prefix-list-name>} {in|out} [<ifname>]**

**功能：**本命令使用访问列表或者前缀列表来过滤发送与接收的路由更新报文。本命令的 no 操作取消路由过滤功能。

**参数：*<access-list-number |access-list-name>***要应用的访问列表号或者名字。

***<prefix-list-name>***是要应用的前缀列表的名字。

***<ifname>***指定应用路由过滤的接口名。

**缺省情况：**缺省情况下 RIP 禁用此功能。

**命令模式：**路由模式与地址族模式。

**使用指南：**如果不指定接口：过滤器将应用于所有接口。

**举例：**Switch# config terminal

Switch(config)# router rip

Switch(config-router)# distribute-list prefix myfilter in vlan 1

## 5.3.11 exit-address-family

**命令：exit-address-family**

**功能：退出地址族模式。**

**命令模式：地址族模式。**

**举例：Switch**(config)# router rip

Switch(config-router)# address-family ipv4 vrf IPI

Switch(config-router-af)# exit-address-family

Switch(config-router)#

## 5.3.12 ip rip aggregate-address

**命令：ip rip aggregate-address A.B.C.D/M**

**no ip rip aggregate-address A.B.C.D/M**

**功能：**配置 RIP 聚合路由。本命令的 no 操作取消配置 RIP 聚合路由。

**参数：**A.B.C.D/M:IPv4 地址及掩码长度。

**命令模式：**路由模式或接口配置模式。

**缺省情况：**默认没有配置聚合路由。

**使用指南：**若是在路由模式下配置聚合路由，则必须先启用 RIP 协议。若是在接口配置模式下，则未启用 RIP 协议也可以配置聚合路由，但是在接口上启用协议后才能生效。

**举例：**配置全局聚合路由 192.168.20.0/22。

Switch(config)#router rip

Switch(config-router)#ip rip agg 192.168.20.0/22

## 5.3.13 ip rip authentication key-chain

**命令：ip rip authentication key-chain <name-of-chain>**

**no ip rip authentication key-chain**

**功能：**使用本命令在一个接口上使能 RIPV2 认证并且配置所使用的密匙链。本命令的 no 操作取消认证。

**参数：*<name-of-chain>***是所使用的密匙链的名字，字符串中可以包括空格，输入以回车结束，字符串长度不超过 256。

**缺省情况：**缺省情况下不配置。

**命令模式：**接口配置模式。

**使用指南：**如果只配置认证模式，不配置接口所使用的密匙链或者密码，认证是完全不起用的。如果配置本命令前没有配置 mode，配置本命令后会将 mode 设置为明文认证。本命令的 no 操作将会取消认证，但是不表示会将 mode 设置为无认证类型，只是发送或接收数据包时不会进行认证处理。可以输入 ip rip authentication key-chain my key，表示密匙链名字是 my key，共 6 个字符。

**举例：**Switch#config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip authentication key-chain my key

**相关命令：key, key chain**

## 5.3.14 ip rip authentication mode

**命令：ip rip authentication mode {text|md5|sm3}**

**no ip rip authentication mode {text|md5|sm3}**

**功能：**设置认证使用的类型；本命令的 no 操作为恢复缺省认证类型即文本认证。

**参数：text** 表示文本认证；**md5** 表示 MD5 认证；**sm3** 表示 SM3 国密认证。

**缺省情况：**文本认证。

**命令模式：**接口配置模式。

**使用指南：**RIP-I 不支持验证，RIP-II 支持三种认证：文本认证（即 Simple 认证）和数据报认证（即 MD5 和 SM3 国密认证）。本命令需要结合 ip rip authentication key-chain 或 ip rip authentication string 来使用，单独配置不会进行认证处理。

**举例：**Switch#config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip authentication mode md5

**相关命令：ip rip authentication key-chain，ip rip authentication string**

## 5.3.15 ip rip authentication string

**命令：ip rip authentication string <text>**

**no ip rip authentication string**

**功能：**设置 RIP 认证使用的密码。本命令的 no 操作取消认证。

**参数：*<text>***是认证所使用的密码，长度为 1-16 个字符。密码中可以包括空格，输入以回车作为结束。

**命令模式：**接口模式。

**使用指南：**配置了本命令，就不能配置 ip rip authentication key chain。在使用 MD5 或 SM3 认证时需要使用 key id 值，如果使用本命令配置命令，key id 值相当于 1。如果配置本命令前没有配置 mode，配置本命令后会将 mode 设置为明文认证。本命令的 no 操作将会取消认证，但是不表示会将 mode 设置为无认证类型，只是发送或接收数据包时不会进行认证处理。可以输入 ip rip authentication string aaa aaa，表示密码是 aaa aaa，供 7 个字符。

**举例：**Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip authentication string guest

**相关命令：ip rip authentication mode**

## 5.3.16 ip rip authentication cisco-compatible

**命令：ip rip authentication cisco-compatible**

**no ip rip authentication cisco-compatible**

**功能：**配置本命令后，在配置了明文认证或者 MD5 认证的情况下，可以接收 cisco 的 RIP 报文，no 命令恢复缺省配置。

**参数：**无。

**缺省情况：**缺省不配置。

**命令模式：**接口模式。

**使用指南：**cisco 路由器在配置了认证后，如果要发送的路由条目超过 25 条，则 RIP 报文的长度超过协议规定的标准长度。配置本命令后，可以接收超过标准长度的 RIP 报文，否则将拒绝此类报文。

**举例：**Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip authentication cisco-compatible

**相关命令：ip rip authentication mode**

## 5.3.17 ip rip receive-packet

**命令：ip rip receive-packet**

**no ip rip receive-packet**

**功能：**设置接口能够接收 RIP 报文；本命令的 no 操作为接口不能接收 RIP 报文。

**缺省情况：**接口缺省接收 RIP 报文。

**命令模式：**接口配置模式。

**举例：**Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip receive-packet

**相关命令：ip rip send-packet**

## 5.3.18 ip rip receive version

**命令：ip rip receive version { 1 | 2|1 2 }**

**no ip rip receive version**

**功能：**设置接口接收 RIP 报文的版本信息。缺省接收 RIP 版本 2；本命令的 no 操作恢复使用 version 命令所设置的值。

**参数：**1 和 2 分别表示 RIP 版本 1 和 RIP 版本 2，1 2 表示 RIP 版本 1、2。

**缺省情况：**Version 2。

**命令模式：**接口配置模式。

**举例：**Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip receive version 1 2

**相关命令：version**

## 5.3.19 ip rip send-packet

**命令：ip rip send-packet**

**no ip rip send-packet**

**功能：**设置接口能够发送 RIP 报文；本命令的 no 操作为接口不能发送 RIP 报文。

**缺省情况：**接口缺省发送 RIP 报文。

**命令模式：**接口配置模式。

**举例：**Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip send-packet

**相关命令：ip rip receive-packet**

## 5.3.20 ip rip send version

**命令：ip rip send version { 1 | 2 | 1-compatible | 1 2}**

**no ip rip send version**

**功能：**设置接口发送 RIP 报文的版本信息。缺省发送 RIP 版本 2；本命令的 no 操作恢复使用 version 命令所设置的值。

**参数：**1 和 2 分别表示 RIP 版本 1 和 RIP 版本 2，1 2 表示 RIP 版本 1、2。

**缺省情况：**Version 2。

**命令模式：**接口配置模式。

**举例：**Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip send version 1

**相关命令：version**

## 5.3.21 ip rip split-horizon

**命令：ip rip split-horizon [poisoned]**

**no ip rip split-horizon**

**功能：**设置允许水平分割，本命令的 no 操作禁用水平分割。

**参数：[poisoned]**表示配置带逆向毒化的水平分割。

**缺省情况：**配置带逆向毒化的水平分割。

**命令模式：**接口配置模式。

**使用指南：**水平分割用于防止路由循环（Routing Loops），即防止三层交换机把从一个接口上所学习到的路由再从这个接口广播出去。

**举例：**Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip split-horizon poisoned

## 5.3.22 key

**命令：key <keyid>**

**no key <keyid>**

**功能：**本命令用于在密匙链中管理、增加密匙。本命令的 no 操作删除一个密匙。

**参数：*<keyid>***是密匙的ID，取值范围0-2147483647。

**命令模式：**keychain模式和keychain-key模式。

**使用指南：**本命令允许进入 keychain-key 模式，并设置密匙所对应的密码。

**举例：**Switch#config terminal

Switch(config)#key chain mychain

Switch(config-keychain)#key 1

Switch(config-keychain-key)#

**相关命令：key chain, key-string, accept-lifetime, send-lifetime**

## 5.3.23 key chain

**命令：key chain <name-of-chain>**

**no key chain < name-of-chain >**

**功能：**本命令用于进入 keychain 管理模式并且配置一个密匙链。本命令的 no 操作删除一个 keychain。

**参数：*<name-of-chain>***是密匙链的名字字符串，长度无具体限制。

**命令模式：**全局模式和 keychain 模式。

**举例：**Switch#config terminal

Switch(config)#key chain mychain

Switch(config-keychain)#

**相关命令：key, key-string, accept-lifetime, send-lifetime**

## 5.3.24 key-string

**命令：key-string <text>**

**no key-string <text>**

**功能：**配置与一个密匙相对应的密码，no 操作删除相应的密码。

**参数：*<text>***是字符串，长度不限制，但是被 RIP 认证引用时，只会取前 16 个字符。

**命令模式：**keychain-key 模式。

**使用指南：**使用本命令为不同ID的密匙配置不同的密码。

**举例：**Switch# config terminal

Switch(config)# key chain mychain

Switch(config-keychain)# key 1

Switch(config-keychain-key)# key-string prime

**相关命令：key, key chain, accept-lifetime, send-lifetime**

## 5.3.25 maximum-prefix

**命令：maximum-prefix <maximum-prefix> [<threshold>]**

**no maximum-prefix**

**功能：**配置路由表中 RIP 路由的最大条数；本命令的 no 操作取消对路由条数的限制。

**参数：*<maximum-prefix>***RIP 路由所能允许的最大条数，取值范围 1-65535；当路由条数占最大条数的百分比超过***<threshold>***时产生一个警告，取值范围 1-100，默认值为 75。

**命令模式：**路由模式。

**使用指南：**RIP 路由的最大条数只限制通过 RIP 学习到的路由，不包括直连路由和引入的路由以及用 route 命令所配置的 RIP 静态路由。比较的依据是 show ip route database 命令中标记为 R 的路由条数。也是 show ip route statistics 命令中所显示的 RIP 路由数量。

**举例：**Switch# config terminal

Switch(config)# router rip

Switch(config-router)# maximum-prefix 150

## 5.3.26 neighbor

**命令：neighbor <A.B.C.D>**

**no neighbor <A.B.C.D>**

**功能：**指定需要定点发送的目的地址；本命令的 no 操作为取消指定的地址，恢复信任所有的网关。

**参数：*<A.B.C.D>***为指定发送的目的 IP 地址，点分十进制格式。

**缺省情况：**RIP 缺省不向任何定点目的地址发送。

**命令模式：**路由模式。

**使用指南：**与 passive-interface 命令配合可以配置只向特定的邻居发送路由信息。

**举例：**Switch# config terminal

Switch(config)# router rip

Switch(config-router)# neighbor 1.1.1.1

**相关命令：passive-interface**

## 5.3.27 network

**命令：network <A.B.C.C/M|ifname>**

**no network <A.B.C.C/M|ifname>**

**功能：**配置运行 RIP 协议的网络。

**参数：*<A.B.C.C/M|>***是网络的 IP 地址前缀以及前缀长度；

***<ifname>***是接口名。

**缺省情况**：网络不运行 RIP 协议。

**命令模式**：路由模式与地址族模式。

**使用指南**：使用本命令配置发送或接收 RIP 更新报文的网络。如果不配置网络，则网络所属的接口都不能发送与接收数据报。

**举例**：Switch# config terminal

Switch(config)# router rip

Switch(config-router)# network 10.0.0.0/8

Switch(config-router)# network vlan 1

**相关命令**：**show ip rip, clear ip rip**

## 5.3.28 offset-list

**命令：offset-list <access-list-number |access-list-name> {in|out }<number >[<ifname>]**

**no offset-list <access-list-number |access-list-name> {in|out }<number >[<ifname>]**

**功能**：对通过 RIP 学习到的路由的度量加上一个偏移量，本命令的 no 操作禁用此功能。

**参数**：***< access-list-number |access-list-name>***要应用的访问列表号或者名字。***<number >***是附加的偏移量，取值范围 0-16；***<ifname>***是具体的接口名。

**缺省情况**：默认的偏移量是系统所规定的接口的度量。

**命令模式**：路由模式与地址族模式。

**举例**：Switch# config terminal

Switch(config)# router rip

Switch(config-router)# offset-list 1 in 5 vlan 1

**相关命令**：**access-list**

## 5.3.29 passive-interface

**命令**：**passive-interface <ifname>**

**no passive-interface <ifname>**

**功能**：指示 RIP 三层交换机在指定的接口上阻塞 RIP 广播，只能向配置了 neighbor 的三层交换机接口发送 RIP 数据包；本命令的 no 操作取消该功能。

**参数**：*<ifname>*是具体的接口名。

**缺省情况**：缺省不配置。

**命令模式**：路由模式。

**举例**：Switch# config terminal

Switch(config)# router rip

Switch(config-router)# passive-interface vlan 1

**相关命令**：**show ip rip**

## 5.3.30 recv-buffer-size

**命令：recv-buffer-size<*size*>**

**no recv-buffer-size**

**功能：**本命令配置 RIP 的 UDP 接收缓冲区大小；no 操作恢复系统缺省值。

**参数：<*size*>**是缓冲区的大小，以字节为单位，取值范围8192-2147483647。

**缺省情况：**8192 字节。

**命令模式：**路由模式。

**举例：**Switch# config terminal

Switch(config)# router rip

Switch(config-router)# recv-buffer-size 23456789

## 5.3.31 redistribute

**命令：redistribute {kernel |connected| static| ospf [<process-id>]| isis|[area tag] bgp} [metric<*value*>] [route-map<*word*>]**

**no redistribute {kernel |connected| static| ospf [<process-id>]| isis| bgp} [metric<*value*>] [route-map<*word*>]**

**功能：**引入从其它路由协议学习到的路由到 RIP 中。

**参数：kernel** 从核心路由中引入；

**connected** 从直连路由中引入；

**static** 从静态路由中引入；

**ospf** 从 OSPF 路由中引入，process-id 是 OSPF 进程 id 号，无该参数表示默认进程，取值范围 1-65535；

**isis** 从 ISIS 路由中引入；

**area tag** 域名；

**bgp** 从 BGP 路由中引入；

**<*value*>**是赋给引入路由的度量，取值范围 0-16；

**<*word*>**指向用于引入路由的路由地图的指针。

**命令模式：路由模式与地址族模式。**

**使用指南：**在地址族模式下，参数 kernel 与 isis 不可用。

**举例：**

Switch#config terminal

Switch(config)#router rip

Switch(config-router)#redistribute kernel route-map ipi

RIP 引入 OSPF 进程 2 的路由。

Switch(config)#router rip

Switch(config-router)#redistribute ospf 2

## 5.3.32 redistribute ospf （vrf 命令）

**命令：redistribute ospf [<*process-id*>] [metric<*value*>] [route-map<*word*>]**

**no redistribute ospf [<*process-id*>]**

**功能：** 本 vrf 中 RIP 进程引入从 OSPF 不同进程学到的路由到本 vrf 的 RIP 进程中。本命令的 no 操作为取消本 vrf 中 RIP 进程引入从 OSPF 指定进程学到的路由到本 vrf 的 RIP 进程中。

**参数：** **process-id** 是 ospfv2 进程 id 号，无该参数表示默认进程，取值范围 1-65535。

**metric <*value*>**是赋给引入路由的度量，取值范围 0-16。

**route-map <*word*>**指向用于引入路由的路由地图的指针。

**缺省情况：** 默认不引入。

**命令模式：** rip vrf 配置模式。

**使用指南：** 无。

**举例：** rip 在 vrf aaa 中的进程要引入 ospf 进程 2 的路由。

```
Switch(config)#router rip
Switch(config-router)#address-family ipv4 vrf aaa
Switch(config-router-af)#redistribute ospf 2
```

## 5.3.33 route

**命令：route <A.B.C.D/M>**

**no route <A.B.C.D/M>**

**功能：**本命令配置一条静态 RIP 路由，no 操作删除此路由。

**参数：**<*A.B.C.D/M*>指明目的 IP 地址前缀及前缀长度。

**命令模式：路由模式。**

**使用指南：本命令增加一条静态 RIP 路由。这条命令主要是用于调试目的。在核心路由表中不会出现该命令配置的路由，但是路由存在于 RIP 路由数据库中。**

**举例：**

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# route 1.0.0.0/8
```

## 5.3.34 router rip

**命令：router rip**

**no router rip**

**功能：**开启 RIP 路由进程并进入 RIP 配置模式；本命令的 no 操作为关闭 RIP 路由协议。

**缺省情况：**不运行 RIP 路由。

**命令模式：**全局配置模式。

**使用指南：**本命令是 RIP 路由协议的启动开关，进行 RIP 协议的其他配置要先打开本命令。

**举例：**启动 RIP 协议配置模式。

Switch(config)#router rip

Switch(config-router)#

## 5.3.35 send-lifetime

**命令：send-lifetime <start-time> {<end-time>| duration<seconds>| infinite}**

**no send-lifetime**

**功能：**使用本命令指明密匙链上的一个密匙为发送密匙的时间段。本命令的 no 操作取消此配置。

**参数：*<start-time>***参数指明时间段的起始时间，它的形式如下：

***<start-time>*={*<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>*}**

***<hh:mm:ss>***用小时、分钟和秒的指明 **send-lifetime** 生效的具体时间；

***<day>***指明生效的具体日期，取值范围 1-31；

***<month>***指明生效的具体月份，用月份英文的头三个字母表示，如 Jan；

***<year>***指明开始生效的具体年份，取值范围 1993-2035；

***<end-time>***参数指明时间段的到期时间，它的形式如下：

***<end-time>*={*<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>*}**

***<hh:mm:ss>***用小时、分钟和秒的指明 **send-lifetime** 到期的具体时间；

***<day>***指明到期的具体日期，取值范围 1-31；

***<month>***指明到期的具体月份，用月份英文的头三个字母表示，如 Jan；

***<year>***指明到期的具体年份，取值范围 1993-2035；

***<seconds>***密匙持续有效的时间长短，以秒为单位，取值范围 1-2147483646；

**infinite** 密匙永远不过期。

**缺省情况：**没有缺省配置。

**命令模式：**keychain-key 模式。

**使用指南：**参考 3.13RIP 认证介绍一节。

**举例：**下面的例子显示了在名为 mychain 的密匙链上为 key 1 所作的 send-lifetime 设置。

Switch# config terminal

Switch(config)# key chain mychain

Switch(config-keychain)# key 1

Switch(config-keychain-key)# send-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006

**相关命令：key，key-string ，key chain，accept-lifetime**

## 5.3.36 show debugging rip

**命令：show debugging rip**

**功能：**显示RIP event debugging、RIP packet debugging和RIP nsm debugging的调试状态。

**命令模式：**任意模式。

**举例：**Switch# show debugging rip

RIP debugging status:

RIP event debugging is on

RIP packet detail debugging is on

RIP NSM debugging is on

## 5.3.37 show ip protocols rip

**命令：show ip protocols rip**

**功能：**显示 RIP 进程参数和统计信息。

**命令模式：**任意模式。

**举例：**

show ip protocols rip

Routing Protocol is "rip"

Sending updates every 30 seconds with +/-50%, next due in 8 seconds

Timeout after 180 seconds, garbage collect after 120 seconds

Outgoing update filter list for all interface is not set

Incoming update filter list for all interface is not set

Default redistribution metric is 1

Redistributing: static

Default version control: send version 2, receive version 2

Interface Send Recv Key-chain

Vlan1 2 2

Routing for Networks:

Vlan1

Vlan2

Routing Information Sources:

Gateway Distance Last Update Bad Packets Bad Routes

20.1.1.1 120 00:00:31 0 0

Distance: (default is 120)

| 显示信息 | 解释 |
|---|---|
| Sending updates every 30 seconds with +/-50%, next due in 8 seconds | 每 30 秒发送一次更新 |
| Timeout after 180 seconds, garbage collect after 120 seconds | 路由超时事件时间为 180 秒，垃圾收集时间为 120 秒 |
| Outgoing update filter list for all interface is not set | 所有接口均未设置发送更新过滤列表 |
| Incoming update filter list for all interface is not set | 所有接口均未设置接收更新过滤列表 |

| | |
|---|---|
| Default redistribution metric is 1 | 引入路由的度量默认是 1 |
| Redistributing: static | 将静态路由引入到 RIP 路由中 |
| Default version control: send version 2, receive version 2<br>Interface Send Recv Key-chain<br>Ethernet1/1/3 2 2 | 接口的接收与发送报文配置，发送与接收版本都是 2，没有配置密匙 l 链 |
| Routing for Networks:<br>Vlan1<br>Vlan2 | 运行 RIP 的网段是接口 Vlan1 与 Vlan2 |
| Routing Information Sources:<br>Gateway Distance Last Update BadPackets Bad Routes<br>20.1.1.1 120 00:00:31 0 0 | 路由信息源：<br>从网关 20.1.1.1 处收到的错误报文与错误路由都是 0，自上次收到路由更新已经过了 31 秒，管理距离是 120 |
| Distance: (default is 120) | 管理距离，默认是 120 |

## 5.3.38 show ip rip

**命令：show ip rip**

**功能：**显示 RIP 路由数据库中的路由。

**命令模式：**任意模式。

**举例：**

show ip rip

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
B - BGP

| | Network | Next Hop | Metric | From | If | Time |
|---|---|---|---|---|---|---|
| R | 12.1.1.0/24 | 20.1.1.1 | 2 | 20.1.1.1 | Vlan1 | 02:51 |
| R | 20.1.1.0/24 | | 1 | | Vlan1 | |

其中，R 表示 RIP 路由，即目的网络地址为 12.1.1.0、网络前缀长度为 24、下一跳地址为 20.1.1.1 一条路由为 RIP 路由，它是从以太网口 E1/1/3 学习而来的，度量为 2，离超时还剩 2 分 51 秒。

## 5.3.39 show ip rip database

**命令：show ip rip database**

**功能：**显示 RIP 路由数据库中的路由。

**命令模式：**任意模式。

**举例：**Switch# show ip rip database

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
B - BGP

| | Network | Next Hop | Metric From | If | Time |
|---|---|---|---|---|---|
| R | 10.1.1.0/24 | | 1 | Vlan1 | |
| R | 20.1.1.0/24 | | 1 | Vlan2 | |

**等价命令：show ip rip**

## 5.3.40 show ip rip database vrf

**命令：show ip rip database vrf *<vrf-name>***

**功能：** 本命令显示 VPN 路由/转发实例相关的 RIP 数据库信息。

**参数：** ***<vrf-name>***指明了 VPN 路由/转发实例的名称。

**命令模式：** 任意模式。

**举例：** Switch# show ip rip database vrf IPI

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
B - BGP

| | Network | Next Hop | Metric From | If | Time |
|---|---|---|---|---|---|
| R | 10.1.1.0/24 | | 1 | Vlan1 | 00:46 |

## 5.3.41 show ip rip interface

**命令：show ip rip interface [<ifname>]**

**功能：**显示 RIP 接口的有关信息。

**参数：*<ifname>***是要显示信息的接口名。

**命令模式：**任意模式。

**举例：**Switch# show ip rip interface vlan 1

Vlan1 is up, line protocol is up
Routing Protocol: RIP
Receive RIP packets
Send RIP packets
Passive interface: Disabled
Split horizon: Enabled with Poisoned Reversed
IP interface address:
10.1.1.1/24

## 5.3.42 show ip rip interface vrf

**命令：show ip rip interface vrf <*vrf-name*>[<*ifname*>]**

**功能：** 本命令显示该 VPN 路由/转发实例相关的 RIP 接口。

**参数：** ***<vrf-name>***指明了 VPN 路由/转发实例的名称；

***<ifname>***是接口名。

**命令模式：** 任意模式。

**举例：** Switch# show ip rip interface vrf IPI Vlan1

Ethernet1/1 is up, line protocol is up

Routing Protocol: RIP

VPN Routing/Forwarding: vpnb

Receive RIP packets

Send RIP packets

Passive interface: Disabled

Split horizon: Enabled with Poisoned Reversed

IP interface address:

11.1.1.1/24

| 显示信息 | 解释 |
|---|---|
| Vlan1 is up, line protocol is up | 接口已经 Up。 |
| Routing Protocol: RIP | 接口运行的路由协议为 RIP。 |
| VPN Routing/Forwarding: vpnb | 接口与 VPN 路由/转发实例 vpnb 相关联。 |
| Receive RIP packets | 接口可以接收 RIP 报文。 |
| Send RIP packets | 接口可以发送 RIP 报文。 |
| Passive interface: Disabled | 不存在 passive-interface。 |
| Split horizon: Enabled with Poisoned Reversed | 接口配置带毒性逆转的水平分割。 |
| IP interface address:<br>11.1.1.1/24 | 接口的 IP 地址。 |

## 5.3.43 show ip rip aggregate

**命令：show ip rip aggregate**

**功能：**本命令显示 ipv4 聚合路由信息。

**参数：**无。

**命令模式：**特权和配置模式。

**缺省情况：**无。

**使用指南：**该命令显示聚合路由在那个接口上配置，Metric 、Count、 Suppress 等，若是在全局上配置，则接口显示“----”。Metric 表示度量。Count 表示该聚合路由聚合的学习到的路由。Suppress 表示该聚合路由被聚合的次数。

**举例：**显示 ipv4 聚合路由信息。

Switch(Config-if-Vlan1)#show ip rip agg

Aggregate information of rip

| Network | Aggregated Ifname | Metric | Count | Suppress |
|---|---|---|---|---|
| 192.168.0.0/16 | Vlan1 | 1 | 2 | 0 |
| 192.168.4.0/22 | ---- | 1 | 2 | 0 |
| 192.168.4.0/24 | ---- | 1 | 1 | 1 |
| | Vlan1 | 1 | 1 | 1 |

| 显示内容 | 解释 |
|---|---|
| Network | 路由前缀和前缀长度。 |
| Aggregated Ifname | 配置该聚合路由的接口名。若是全局聚合路由，则显示“----” 。 |
| Metric | 聚合路由的度量。 |
| Count | 聚合路由聚合的除聚合路由外的路由数目。 |
| Suppress | 聚合路由被聚合的次数。 |

## 5.3.44 show ip rip redistribute

**命令：show ip rip redistribute [vrf <NAME>]**

**功能：** 显示 rip 进程引入其它外部路由的配置信息，可以分 vrf 显示。

**参数：** vrf 名，无参数表示显示所有 vrf 的 RIP 进程重分布路由信息。

**缺省情况：** 不显示信息。

**命令模式：** 特权模式和配置模式。

**使用指南：** 无。

**举例：**

Switch#show ip rip redistribute

## 5.3.45 show ip vrf

**命令：show ip vrf [<vrf-name>]**

**功能：** 本命令显示与该 VPN 路由/转发实例相关的 RIP 实例信息。

**参数：** ***<vrf-name>***指明了 VPN 路由/转发实例的名称。

**命令模式：** 任意模式。

**使用指南：** 本命令在其它的路由协议中也存在，使用本命令实，与该 VPN 路由/转发实例相关的其它路由协议进程的信息也会显示出来。

**举例：** Switch# show ip vrf IPI

VRF IPI, FIB ID 1

Router ID: 11.1.1.1 (automatic)

Interfaces:

Vlan1

!

VRF IPI; (id=1); RIP enabled Interfaces:

Ethernet1/8

| Name | Interfaces |
|---|---|
| IPI | Vlan1 |

| Name | Default RD | Interfaces |
|---|---|---|
| IPI | | Vlan1 |

## 5.3.46 timers basic

**命令：timers basic <update> <invalid> <garbage>**

**no timers basic**

**功能：**调整 RIP 计时器更新、超时、垃圾收集的时间；本命令的 no 操作为恢复各项参数的缺省值。

**参数：*<update>***发送更新报文的时间间隔，单位秒，取值范围5-2147483647；***<invalid>***宣布RIP路由无效的时间段，单位秒，取值范围5-2147483647；***<garbage>***为宣布某路由无效后仍可在路由表中存在的时间段，单位秒，取值范围5-2147483647。

**缺省情况：*<update>***缺省值 30；***<invalid>***缺省值 180；***<garbage>***缺省值 120。

**命令模式：**路由模式。

**使用指南：**缺省情况下，系统每 30 秒会广播 RIP 更新报文；当过了 180 秒不能收到某路由的更新报文，就认为该路由无效；但该路由还能在路由表中存在 120 秒，120 秒后，在路由表删除该路由。

**举例：**设置 RIP 路由表更新时间为 20 秒，超时时间为 80 秒，垃圾收集的时间为 60 秒。

Switch(Config-Router)#timers basic 20 80 60

## 5.3.47 version

**命令：version {1| 2}**

**no version**

**功能：**设置所有路由器接口发送/接收 RIP 数据报的版本；no 操作恢复缺省设置 2。

**参数：1** 为 rip 版本 1；**2** 为 rip 版本 2。

**缺省情况：**发送与接收都为版本 2 的数据报。

**命令模式：**路由模式与地址族模式。

**使用指南：**1 表示三层交换机各接口只发送/接收 RIP-I 数据报，2 表示三层交换机各接口只发送/接收 RIP-II 数据报。缺省情况下，发送 RIP-II 同时接收 RIP-II 数据报。

**举例：**设置该交换机接口发送/接收 RIP 数据报的版本为 2。

Switch(config-router)#version 2

**相关命令：ip rip receive version**

**ip rip send version**

# 5.4 OSPF

## 5.4.1 area authentication

**命令：area <id> authentication [message-digest md5 ]**

**no area <id> authentication**

**功能：**配置 OSPF 区域的认证方式；本命令的 no 操作为恢复缺省值。

**参数：*<id>***为区域号，可以是数字，取值范围 0～4294967295，也可以是一个 IP 地址。**message-digest md5** 如果选择这个参数就证明是 MD5 认证，如果不选择就证明是简单明文认证。

**缺省情况：**无认证。

**命令模式：**OSPF 协议配置模式。

**使用指南：**配置 OSPF 区域的认证方式为简单明文密码认证方式或者 MD5 认证方式。接口模式下同样可以配置认证方式，接口下的认证方式优先级高于区域的认证配置方式。当接口未配置认证方式时，如果区域配置是简单明文密码认证，需要在接口模式下使用 ip ospf authentication-key 设置密码；如果是 MD5 认证，需要在接口模式下使用 ip ospf message-digest-key 配置 MD5 key。当接口配置认证方式后，该接口所在区域的认证方式无法影响该接口的认证行为。

**举例：**设置区域 0 认证方式为 MD5。

Switch(config-router)#area 0 authentication message-digest md5

## 5.4.2 area default-cost

**命令：area <id> default-cost <cost>**

**no area <id> default-cost**

**功能：**配置发送到 stub 或 NSSA 区域的缺省 summary 路由的代价；本命令的 no 操作为恢复缺省值。

**参数：<*id*>**为区域号，可以是数字，取值范围 0～4294967295，也可以是一个 IP 地址；**<*cost*>** 取值范围为<0-16777214>。

**缺省情况：**OSPF 缺省 cost 值为 1。

**命令模式：**OSPF 协议配置模式 。

**使用指南：**该命令只适用于连接到 stub 区域或者 NSSA 区域的 ABR 路由器。

**举例：**设置 area 1 的 default-cost 为 10。

Switch(config-router)#area 1 default-cost 10

## 5.4.3 area filter-list

**命令：[no] area <*id*> filter-list {access|prefix} {in|out}**

**功能：**配置在 ABR 上广播 summary 路由的过滤器；本命令的 no 操作为恢复缺省值。

**参数：<*id*>**为区域号，可以是数字，取值范围 0～4294967295，也可以是一个 IP 地址；access 指定使用 access-list，prefix 指定使用 prefix-list；**<*name*>**为过滤器的名字，长度 1-256；in 指定从其他区域到本区域，out 是本区域到其他区域。

**缺省情况：**缺省不配置任何过滤器。

**命令模式：**OSPF 协议配置模式。

**使用指南：**该命令用于抑制特定的区间路由在本区和其他区域之间的传播。如果没有查找到 access-list 或者 prefix-list，OSPF 协议按照 deny 方式过滤路由。

**举例：**在区域 1 上设置一个过滤器。

Switch(config)#access-list 1 deny 172.22.0.0 0.0.0.255

Switch(config)#access-list 1 permit any-source

Switch(config)#router ospf 100

Switch(config-router)#area 1 filter-list access 1 in

## 5.4.4 area nssa

**命令： area <id> nssa [TRANSLATOR| no-redistribution |DEFAULT-ORIGINATE |no-summary]**

**no area <id> nssa[TRANSLATOR| no-redistribution |DEFAULT-ORIGINATE |no-summary]**

**功能：**设置区域为 Not-So-Stubby-Area（NSSA）区域。

**参数：<*id*>**为区域号，可以是数字，取值范围 0～4294967295，也可以是一个 IP 地址；

**TRANLATOR = translator-role {candidate|never|always}**，指定 router 的 LSA 转换行为：**candidate** 表示如果路由器被选举为 translator，可以转换 Type 7 LSA 为 Type-5 LSA，默认为 **candidate**；

**never** 表示路由器永不进行 Type 7 LSA 到 Type 5 LSA 的转换；

**always** 表示路由器总是进行 Type 7 LSA 到 Type 5 LSA 的转换；

**no-redistribution** 表示不分发 external-LSA 到 NSSA；

**DEFAULT-ORIGINATE=default-information-originate [metric <0-16777214>] [metric-type <*1-2*>]**,生成 Type-7 的 LSA；

**metric <*0-16777214*>**指定度量值；

**metric-type <*1-2*>**指定 external-LSA 的度量值类型，2 为缺省值；

**no-summary** 表示不注入区间路由到 NSSA。

**缺省情况：**缺省没有定义任何 NSSA 区域。

**命令模式：**OSPF 协议配置模式。

**使用指南：** 同一个区域不能既是 NSSA 又是 stub。

**举例：**设置区域 3 为 NSSA 区。

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#area 0.0.0.51 nssa

Switch(config-router)#area 3 nssa default-information-originate metric 34 metric-type 2 translator-role candidate no-redistribution

## 5.4.5 area range

**命令：area <*id*> range <*address*> [advertise| not-advertise| substitute]**

**no area <*id*> range <*address*>**

**功能：**在区域边界上汇聚 OSPF 路由，no 命令取消此功能。

**参数：<*id*>**为区域号，可以是数字，取值范围 0～4294967295，也可以是一个 IP 地址；

**<*address*>=<*A.B.C.D/M*>,**指明区域的网络前缀及前缀长度；

**advertise：**通告这个区域，为缺省值；

**not-advertise ：**不通告这个区域；

**substitute= substitute <*A.B.C.D/M*>：**将此区域作为另一个前缀通告；

**<*A.B.C.D/M*>：**取代区域将要被通告的网络前缀。

**缺省情况：**缺省没有配置此功能。

**命令模式：**OSPF 协议配置模式。

**使用指南：**使用本命令汇聚一个区的区内路由。如果区内的网络号以不连续的方式进行配置，在 ABR 上配置本命令可以通告一条 summary 路由，该路由包含了区内所有属于特定 range 的单个网络。

**举例：**

Switch # config terminal

Switch (config)# router ospf 100

Switch (config-router)# area 1 range 192.16.0.0/24

## 5.4.6 area stub

**命令：area <id> stub [no-summary]**

**no area <id> stub [no-summary]**

**功能：**将一个区域定义为一个存根区域，no 命令取消此功能。

**参数：*<id>***为区域号，可以是数字，取值范围 0～4294967295，也可以是一个 IP 地址；

**no-summary：**区域边界路由器停止向存根区发送汇聚链路通告。

**缺省情况：**不定义存根区。

**命令模式：**OSPF 协议配置模式。

**使用指南：**在存根区的所有路由器上配置 area stub。对于存根区的路由器有两条配置命令：stub 和 default-cost。所有连接到存根区的路由器都要配置 area stub 命令，对于连接到存根区的区域边界路由器，通过 area default-cost 命令来定义引入的 cost 值。

**举例：**

Switch # config terminal

Switch (config)# router ospf 100

Switch (config-router)# area 1 stub

**相关命令：area default-cost**

## 5.4.7 area virtual-link

**命令：area <id> virtual-link A.B.C.D {AUTHENTICATION|AUTH_KEY|INTERVAL}**

**no area <id> virtual-link A.B.C.D [AUTHENTICATION|AUTH_KEY|INTERVAL]**

**功能：**在物理上被非骨干区域分开的两个骨干区域之间配置一条逻辑链路。no 命令移去此虚链路。

**参数：*<id>***为区域号，可以是数字，取值范围 0～4294967295，也可以是一个 IP 地址

AUTHENTICATION = authentication [message-digest md5 [message-digest-key <1-255> <LINE>] |null|AUTH_KEY]；

**authentication ：**在这个虚链路上使能认证；

**message-digest md5：**使用MD-5认证；

**null ：**使用空认证覆盖密码或者报文摘要

AUTH_KEY= authentication-key <*key*>；

**<key>：**是不多于8个字符组成的密码；

INTERVAL= [dead-interval | hello-interval | message-digest-key<1-255>md5<LINE> | retransmit-interval | transmit-delay] <value>

***<value>*：**延迟或间隔的秒数，取值范围1~65535；

***<dead-interval>*：**经过一段时间没有收到分组，路由器认为一个邻居已经离线。缺省是40秒；

***<hello-interval>*：**路由器在发送一个hello分组前所等待的时间，缺省是10秒；

***<message-digest-key***>：MD-5认证密钥；

***<retransmit-interval>***：路由器在重传一个分组前所等待的时间，缺省是5秒；

***<transmit-delay>***：在发送一个分组前路由器的延迟时间，缺省为1秒。

**缺省情况**：没有缺省配置。

**命令模式**：OSPF 协议配置模式。

**使用指南**：在 OSPF 中，所有的非骨干区域都被连接到一个骨干区域。如果到骨干区域的连接丢失了，虚链路将会修复该连接。你可以在任何两个与一个公共非骨干区域有连接的骨干区域路由器之间配置虚链路。协议对待由虚链路连接起来的路由器就如一个点对点网络。

**举例**：

Switch#config terminal

Switch(config) #router ospf 100

Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20

**相关命令**：**area authentication, show ip ospf, show ip ospf virtual-links**

## 5.4.8 auto-cost reference-bandwidth

**命令**：**auto-cost reference-bandwidth <bandwith>**

**no auto-cost reference-bandwidth**

**功能**：本命令控制 OSPF 怎样计算接口的默认度量。no 命令仅依据接口类型给接口配置费用。

**参数**：***<bandwith>***：以兆比特每秒为单位的参考带宽值，取值范围是 1~*4294967*。

**缺省情况**：参考带宽默认为 100Mbps。

**命令模式**：OSPF 协议配置模式。

**使用指南**：用参考带宽除以接口带宽就得到接口的度量值。这个命令主要用来区分高带宽的链路。如果存在几条不同的高带宽链路，配置一个比较大的参考带宽值，可以将这些连路的代价区分开来。

**举例**：

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#auto-cost reference-bandwidth 50

**相关命令**：**ip ospf cost**

## 5.4.9 compatible rfc1583

**命令**：**compatible rfc1583**

**no compatible rfc1583**

**功能**：本命令配置与rfc1583兼容，no命令关闭兼容性。

**缺省情况**：缺省与 rfc 2328 兼容。

**命令模式**：OSPF 协议配置模式。

**使用指南**：

**举例**：

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#compatible rfc1583

## 5.4.10 clear ip ospf process

**命令：clear ip ospf [<process-id>] process**

**功能：**使用本命令清除和重启OSPF路由进程。如果指定OSPF进程ID，则清除一个特定的OSPF进程，否则清除所有的OSPF进程。

**缺省情况：**无缺省配置。

**命令模式：**特权模式。

**使用指南：**

**举例：**

Switch#clear ip ospf process

## 5.4.11 debug ospf events

**命令：debug ospf events [abr|asbr|lsa|nssa|os|router|vlink]**

**no debug ospf events [abr|asbr|lsa|nssa|os|router|vlink]**

**功能：**打开显示 OSPF 的各种事件信息的调试开关；本命令的 no 操作为关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式与全局模式。

**举例：**

Switch#debug ospf events router

## 5.4.12 debug ospf ifsm

**命令：debug ospf ifsm [status|events|timers]**

**no debug ospf ifsm [status|events|timers]**

**功能：**打开显示 OSPF 接口状态机调试开关；本命令的 no 操作为关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式与全局模式。

**举例：**

Switch#debug ospf ifsm events

## 5.4.13 debug ospf lsa

**命令：debug ospf lsa [generate|flooding|install|maxage|refresh]**

**no debug ospf lsa [generate|flooding|install|maxage|refresh]**

**功能：**打开显示链路状态宣告信息的调试开关；本命令的 no 操作为关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式与全局模式。

**举例：**

Switch#debug ospf lsa generate

## 5.4.14 debug ospf nfsm

**命令：debug ospf nfsm [status|events|timers]**

**no debug ospf nfsm [status|events|timers]**

**功能：**打开显示 OSPF 邻居状态机调试开关；本命令的 no 操作为关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式与全局模式。

**举例：**

Switch#debug ospf nfsm events

## 5.4.15 debug ospf nsm

**命令：debug ospf nsm [interface|redistribute]**

**no debug ospf nsm [interface|redistribute]**

**功能：**打开显示 OSPF NSM 调试开关；本命令的 no 操作为关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式与全局模式。

**举例：**

Switch#debug ospf nsm interface

## 5.4.16 debug ospf packet

**命令：debug ospf packet [dd|detail|hello|ls-ack|ls-request|ls-update|recv|detail]**

**no debug ospf packet [dd|detail|hello|ls-ack|ls-request|ls-update|recv|detail]**

**功能：**打开显示 OSPF 报文信息的调试开关；本命令的 no 操作为关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式与全局模式。

**举例：**

Switch#debug ospf packet hello

## 5.4.17 debug ospf route

**命令：debug ospf route [ase|ia|install|spf]**

**no debug ospf route [ase|ia|install|spf]**

**功能：**打开显示 OSPF 有关路由的调试开关；本命令的 no 操作关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式与全局模式。

**举例：**

Switch#debug ospf route spf

## 5.4.18 debug ospf redistribute message send

**命令：debug ospf redistribute message send**

**no debug ospf redistribute message send**

**功能：**打开 OSPF 进程引入其他 OSPF 进程路由的命令下发调试开关。此命令的 no 命令关闭 OSPF 进程引入其他 OSPF 进程路由的命令下发调试开关。

**参数：**无。

**缺省情况：**默认不打开。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**打开 OSPF 进程引入其他 OSPF 进程路由的命令下发调试开关。

Switch#debug ospf redistribute message send

## 5.4.19 debug ospf redistribute route receive

**命令：debug ospf redistribute route receive**

**no debug ospf redistribute route receive**

**功能：**打开/关闭 ospf 进程收到 nsm 发来的路由信息的调试开关。

**参数：**无。

**缺省情况：**默认不打开。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**打开 ospf 进程收到 nsm 发来的路由信息的调试开关。

Switch#debug ospf redistribute route receive

## 5.4.20 default-information originate

**命令：default-information originate [always|METRIC|METRICTYPE|ROUTEMAP]**

**no default-information originate**

**功能：**本命令创造一条默认的外部路由到OSPF路由域，no命令关闭此特性。

**参数：always：**不论软件中是否存在默认路由，总是通告默认路由

**METRIC = metric <*value*>：**设置用于创建默认路由时的度量，**<*value*>**取值范围是0~*16777214*。默认的度量值是10

**METRICTYPE = metric-type {1|2}**设置默认路由的OSPF external link类型

1 设置OSPF外部类型1度量值

2 设置OSPF外部类型2度量值

ROUTEMAP = route-map <*WORD*>

**<WORD>**指明应用的路由地图名

**缺省情况：**度量值默认是 10，OSPF external link 类型默认是 2。

**命令模式：**OSPF 协议配置模式。

**使用指南：** 当你使用本命令将引入路由到OSPF路由域时，系统表现得像一个ASBR。

**举例：**

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#default-information originate always metric 23 metric-type 2 route-map myinfo

**相关命令：route-map**

## 5.4.21 default-metric

**命令：default-metric <value>**

**no default-metric**

**功能：**本命令设置OSPF路由协议的默认度量值，no命令返回到默认状态。

**参数：<*value*>，**度量值，范围是0~*16777214*。

**缺省情况：**内置，自动度量转换。

**命令模式：**OSPF 协议配置模式。

**使用指南：**默认度量使得度量不兼容时，路由引入也能继续进行。如果度量不能转换，默认度量提供了替代选择使得路由引入能够继续进行下去。本命令将导致当前的路由协议对于所有的引入路由使用相同的度量值。本命令应该与命令redistribute结合使用。

**举例：**

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#default-metric 100

## 5.4.22 distance

**命令：distance {<value>|ROUTEPARAMETER}**

**no distance ospf**

**功能：**基于路由种类配置OSPF路由管理距离，no命令恢复默认值。

**参数：<*value*>**，OSPF路由管理距离值，取值范围1~255

**ROUTEPARAMETER= ospf {ROUTE1|ROUTE2|ROUTE3}**

**ROUTE1= external <exernal-distance>,**设置从其他路由域学到的路由的管理距离值，

**<exernal-distance>**管理距离值，取值范围1~255

**ROUTE2= inter-area <inter-distance>，**设置从一个区到另一个区的路由管理距离值

**<inter-distance>**管理距离值，取值范围1~255

**ROUTE3= intra-area <intra-distance>，**设置一个区内所有路由的管理距离值

**<intra-distance>**管理距离值，取值范围1~255

**缺省情况：**OSPF 的管理距离默认值是 110。

**命令模式：**OSPF 协议配置模式。

**使用指南：**管理距离表明了路由信息源的可信度。距离值可以是1~255之间的任意值。更大的管理距离值意味着更低的可信度。

**举例：**

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#distance ospf inter-area 20 intra-area 10 external 40

## 5.4.23 distribute-list

**命令：distribute-list <access-list-name> out {kernel |connected| static| rip| isis| bgp}**

**no distribute-list out {kernel |connected| static| rip| isis| bgp}**

**功能：**在路由更新中过滤网络。no 命令禁止使用本功能。

**参数：*< access-list-name>***要应用的访问列表者名字。

**out:** 过滤发出的路由更新；

**kernel** 核心路由；

**connected**直连路由；

**static** 静态路由；

**rip** RIP 路由；

**isis** ISIS 路由；

**bgp** BGP 路由。

**缺省情况：**没有缺省配置。

**命令模式：**OSPF 协议配置模式。

**使用指南：**当将其它路由协议的路由引入到 OSPF 路由表中时，可以配置本命令。

**举例：**下面的例子基于访问列表list1所作的BGP路由更新的发布。

Switch#config terminal

Switch(config)#access-list l1 permit 172.10.0.0 0.0.255.255

Switch(config)#router ospf 100

Switch(config-router)#redistribute bgp

Switch(config-router)#distribute-list 1 out bgp

## 5.4.24 filter-policy

**命令：filter-policy <*access-list-name*>**

**no filter-policy**

**功能：**使用访问列表对 OSPF 计算得到的路由进行过滤。no 命令取消路由过滤。

**参数：**<*access-list-name*>要应用的访问列表名字。可以使用数字标准 IP 访问列表和命名标准 IP 访问列表进行配置。

**缺省情况：**没有缺省配置。

**命令模式：**OSPF 协议配置模式。

**使用指南：**当需要对 OSPF 计算得到的路由进行过滤时，可以配置本命令。当指定的访问列表不存在时，不会对任何路由条目进行过滤。不匹配访问列表 permit 规则的所有路由都会被过滤。该命令只允许配置一条访问列表，多次配置时只有最后一次的配置生效。

**举例：**下面的例子使用访问列表 1，对 172.10.0.0/16 网段之外的路由进行过滤。

Switch#config terminal

Switch(config)#access-list 1 permit 172.10.0.0 0.0.255.255

Switch(config)#router ospf

Switch(config-router)#filter-policy 1

## 5.4.25 host area

**命令：host <host-address> area <area-id> [cost <cost>]**

**no host <host-address> area <area-id> [cost <cost>]**

**功能：**使用本命令配置一个属于某个特定区的存根主机条目，no命令取消配置。

**参数：**<***host-address***>主机IP地址，点分十进制格式；

<***area-id***>区ID，点分十进制IP地址格式或者取值范围是0~4294967295的整数；

<***cost***>指明条目的cost，范围0~65535的整数，缺省值为0。

**缺省情况：**不配置主机条目。

**命令模式：**OSPF 协议配置模式。

**使用指南：**使用本命令你可以在router-LSA中将某条特定的主机路由作为存根链路通告出去。由于存根host属于特定的路由器，制定cost并不重要。

**举例：**

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#host 172.16.10.100 area 1

Switch(config-router)#host 172.16.10.101 area 2 cost 10

## 5.4.26 ip ospf authentication

**命令：ip ospf [<*ip-address*>] authentication [message-digest|null] [md5|sm3]**

**no ip ospf [<*ip-address*>] authentication**

**功能：**指定接口上发送和接受 OSPF 报文所需要的验证方式；本命令的 no 操作为取消验证。

**参数：**<***ip-address***>为接口的 IP 地址，点分十进制格式。

**message-digest：**使用 message-digest 秘钥串 **null：**不使用认证

Md5: 使用 MD5 认证

Sm3：使用 SM3 认证

**缺省情况：**接口上接受 OSPF 报文缺省不需要验证。

**命令模式：**接口配置模式。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf authentication message-digest md5

## 5.4.27 ip ospf authentication-key

**命令：ip ospf [<*ip-address*>] authentication-key <*0 LINE | 7 WORD | LINE*>**

**no ip ospf [<*ip-address*>] authentication**

**功能：**指定接口上发送和接受 OSPF 报文所需要的验证密钥。本命令的 no 操作为取消验证密钥。

**参数：**<*ip-address*>为接口的 IP 地址，点分十进制格式；<*LINE*>指定认证的密钥，如果密钥选项为 0，则后续指定明文密钥。如果选项为 7，则后续指定为明文密钥加密后的密文字串；不带任何选项，则默认指定为明文密钥。

**缺省情况：**接口上接受 OSPF 报文缺省不需要验证。

**命令模式：**接口配置模式。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf authentication-key 0 password

## 5.4.28 ip ospf cost

**命令：ip ospf [<*ip-address*>] cost <*cost*>**

**no ip ospf [<*ip-address*>] cost**

**功能：**指定接口运行 OSPF 协议所需的代价；本命令的 no 操作为恢复缺省值。

**参数：<*ip-address*>**为接口的 IP 地址，点分十进制格式；

***<cost >***为 OSPF 协议所需花费的值，取值范围 1～65535。

**缺省情况：**接口缺省的 OSPF 协议所需花费根据带宽自动计算。

**命令模式：**接口配置模式。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf cost 3

## 5.4.29 ip ospf database-filter

**命令：ip ospf [<*ip-address*>] database-filter all out**

**no ip ospf [<*ip-address*>] database-filter**

**功能：**本命令在特定接口上打开 LSA 数据库过滤开关；本命令的 no 操作关闭过滤开关。

**参数：<*ip-address*>**为接口的 IP 地址，点分十进制格式；

**all：**所有 LSAs；

**out：**发出的 LSAs。

**缺省情况：**过滤开关关闭。

**命令模式：**接口配置模式。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf database-filter all out

## 5.4.30 ip ospf dead-interval

**命令：ip ospf [<*ip-address*>] dead-interval <*time* >**

**no ip ospf [<*ip-address*>] dead-interval**

**功能：**指定相邻三层交换机路由失效的时间长度；本命令的 no 操作为恢复缺省值。

**参数：<*ip-address*>**为接口的 IP 地址，点分十进制格式；

**<*time* >**为相邻三层交换机失效的时间长度，单位为秒，取值范围 1～65535。

**缺省情况：**三层交换机失效的时间长度缺省为 40 秒（通常是 hello-interval 的 4 倍）。

**命令模式：**接口配置模式。

**使用指南：**当三层交换机在 **dead-interval** 时间间隔内没有接收到来自邻居三层交换机的 Hello 数据包，则认为该三层交换机不可达、失效。本命令可以根据链路的实际情况修改相邻三层交换机路由失效时间的值。设置的 **dead-interval** 的值将写入 Hello 报文中，并随 Hello 报文传送。为使 OSPF 协议的正常运行，必须保证和该接口相邻的三层交换机之间的 **dead-interval** 参数一致，且至少为 **hello-interval** 值的 4 倍。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf dead-interval 80

## 5.4.31 ip ospf disable all

**命令：ip ospf disable all**

**no ip ospf disable all**

**功能：**配置接口上停止 OSPF 分组处理。

**命令模式：**接口配置模式。

**使用指南：**本命令重置了 network area 命令，停止了特定接口上的分组处理。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf disable all

## 5.4.32 ip ospf hello-interval

**命令：ip ospf [<*ip-address*>] hello-interval <*time*>**

**no ip ospf [<*ip-address*>] hello-interval**

**功能：**指定在接口上发送 HELLO 报文的时间间隔；本命令的 no 操作为恢复缺省值。

**参数：<*ip-address*>**为接口的 IP 地址，点分十进制格式；

**<*time*>**为发送 HELLO 报文的时间间隔，单位为秒，取值范围 1～65535。

**缺省情况：**接口缺省发送 HELLO 报文的间隔时间为 10 秒。

**命令模式：**接口配置模式。

**使用指南：**HELLO 数据包是一种最常见的一种数据包，它周期性地被发送至邻接三层交换机，用于发现和维持邻接关系、选举 DR 与 BDR。用户设置的 **hello-interval** 的值将写入 HELLO 报文中，并随 HELLO 报文传送。**hello-interval** 的值越小，则网络拓扑结构的变化将被越快的发现，同时链路开销也增加。为使 OSPF 协议的正常运行，必须保证和该接口相邻的三层交换机之间的 **hello-interval** 参数一致。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf hello-interval 20

**相关命令：ip ospf dead-interval**

## 5.4.33 ip ospf message-digest-key

**命令：ip ospf [<*ip-address*>] message-digest-key <*key_id*> <*0 LINE |7 WORD | LINE*>**

**no ip ospf [<*ip-address*>] message-digest-key <*key_id*>**

**功能：**指定在接口上认证的 key id 和 key 值；本命令的 no 操作为恢复缺省值。 ，该命令配合 ip ospf authentication message-digest 命令使用。

**参数：**<*ip-address*>为接口的 IP 地址，点分十进制格式； <*key_id*>取值范围 1-255； <*LINE*>为 OSPF 密钥，如果密钥选项为 0，则后续指定明文密钥，如果选项为 7，则后续指定为明文密钥加密后的密文字串；不带任何选项，则默认指定为明文密钥。

**缺省情况：**接口不配置 key。

**命令模式：**接口配置模式。

**使用指南：**使用加密认证来达到网络上 OSPF 路由器间的安全。该命令必须在邻居之间配置相同的 key id 和密钥，否则将无法建立起邻接关系。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf message-digest-key 2 0 yourpassword

## 5.4.34 ip ospf mtu

**命令：ip ospf mtu *<mtu>***

**no ip ospf mtu**

**功能：**指定接口的 mtu 值，作为构造 OSPF 分组的依据；本命令的 no 操作为恢复缺省值。

**参数：*<mtu >***为接口 mtu 值，取值范围 576~65535。

**缺省情况：**使用从内核得到的接口 mtu 值。

**命令模式：**接口配置模式。

**使用指南：**本命令所配置的接口值仅为 ospf 协议所使用，并不更新到内核。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf mtu 1480

## 5.4.35 ip ospf mtu-ignore

**命令：ip ospf <*ip-address*> mtu-ignore**

**no ip ospf <*ip-address*> mtu-ignore**

**功能：**本命令使得进行 DD 交换时不检查 mtu 大小；本命令的 no 操作确保在进行 DD 交换时检查 mtu 大小。

**参数：*<ip-address>***为接口的 IP 地址，点分十进制格式。

**缺省情况：**进行 DD 交换时检查 mtu 大小。

**命令模式：**接口配置模式。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf mtu-ignore

## 5.4.36 ip ospf network

**命令：ip ospf network {broadcast|non-broadcast|point-to-point|point-to-multipoint}**

**no ip ospf network**

**功能：**本命令配置接口的 OSPF 网络类型；no 命令恢复缺省值。

**参数：broadcast：**设置 OSPF 网络类型为广播类型；

**non-broadcast：**设置 OSPF 网络类型为 NBMA；

**point-to-point：**设置 OSPF 网络类型为点对点类型；

**point-to-multipoint**：设置 OSPF 网络类型为点对多点类型。

**缺省情况**：接口的 OSPF 网络类型为广播类型。

**命令模式**：接口配置模式。

**举例**：下面的配置设置接口 vlan1 的 OSPF 网络类型为点对点类型。

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf network point-to-point

## 5.4.37 ip ospf priority

**命令**：**ip ospf [<*ip-address*>] priority <*priority*>**

**no ip ospf [<*ip-address*>] priority**

**功能**：配置接口在选举“指定三层交换机”（DR）时的优先级；本命令的 no 操作为恢复缺省值。

**参数**：**<*ip-address*>**为接口的 IP 地址，点分十进制格式；

**<*priority*>**为优先级，合法的取值范围是 0～255。

**缺省情况**：接口在选举指定三层交换机时缺省的优先级值为 1。

**命令模式**：接口配置模式。

**使用指南**：当连在同一网段的两台三层交换机都想成为“指定三层交换机”时，根据优先级的值来决定谁是“指定三层交换机”，通常选择优先级高的作为“指定三层交换机”；如果优先级值相等，则选 router-id 号大的。当一台三层交换机的优先级值为 0 时，这台三层交换机将不会被选举为“指定三层交换机”或“备份指定三层交换机”。

**举例**：配置接口在选举指定三层交换机 DR 中的优先级。将接口 vlan1 配置成没有选举权利，即 priority 值为 0。

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf priority 0

## 5.4.38 ip ospf retransmit-interval

**命令**：**ip ospf [<*ip-address*>] retransmit-interval <*time*>**

**no ip ospf [<*ip-address*>] retransmit-interval**

**功能**：指定接口与邻接三层交换机之间传送链路状态宣告（LSA）时的重传间隔；本命令的 no 操作为恢复缺省值。

**参数**：**<*ip-address*>**为接口的 IP 地址，点分十进制格式；

**<*time*>**为与邻接三层交换机之间传送链路状态宣告时的重传间隔，单位为秒，取值范围 1～65535。

**缺省情况**：缺省重传间隔为 5 秒。

**命令模式**：接口配置模式。

**使用指南：**当一台三层交换机向它的邻居传送链路状态宣告时，它将保持链路状态宣告直至收到对方的确认，若在时间间隔内没有收到确认报文，则三层交换机将重传链路状态宣告。重传间隔的值必须大于两台三层交换机传送报文一个来回的时间。

**举例：**设置接口 vlan1 重传 lsa 的时间为 10 秒。

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf retransmit-interval 10

## 5.4.39 ip ospf transmit-delay

**命令：ip ospf [<*ip-address*>] transmit-delay <*time*>**

**no ip ospf [<*ip-address*>] transmit-delay**

**功能：**设置在接口上传送链路状态宣告（LSA）的时延值；本命令的 no 操作为恢复缺省值。

**参数：<*ip-address*>**为接口的 IP 地址，点分十进制格式；

***<time>***为接口上传送链路状态宣告的时延值，单位为秒，取值范围 1～65535。

**缺省情况：**接口上传送链路状态宣告的缺省时延值为 1 秒。

**命令模式：**接口配置模式。

**使用指南：**链路状态宣告在本三层交换机中会随时间老化，但在网络传输过程中却不会，因此在发送链路状态宣告之前增加 **transit-delay** 的时延，使之能在老化之前将链路状态宣告发送出去。应该根据链路状态合理配置 transmit-delay 的数值，不合理的配置可能导致 OSPF 邻居状态不稳定。

**举例：**设置接口 vlan1 发送 LSA 的时延为 3 秒。

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf transmit-delay 3

## 5.4.40 key

**命令：key <*keyid*>**

**no key <*keyid*>**

**功能：**本命令用于在密匙链中管理、增加密匙。本命令的 no 操作删除一个密匙。

**参数：<*keyid*>**是密匙的ID，取值范围0-2147483647。

**命令模式：**keychain模式和keychain-key模式。

**使用指南：**本命令允许进入 keychain-key 模式，并设置密匙所对应的密码。

**举例：**Switch#config terminal

Switch(config)#key chain mychain

Switch(config-keychain)#key 1

Switch(config-keychain-key)#

**相关命令：key chain, key-string, accept-lifetime, send-lifetime**

## 5.4.41 key chain

**命令：key chain *<name-of-chain>***

**no key chain *< name-of-chain >***

**功能：**本命令用于进入 keychain 管理模式并且配置一个密匙链。本命令的 no 操作删除一个 keychain。

**参数：*<name-of-chain>***是密匙链的名字字符串，长度无具体限制。

**命令模式：**全局模式和 keychain 模式。

**举例：**Switch#config terminal

Switch(config)#key chain mychain

Switch(config-keychain)#

## 5.4.42 log-adjacency-changes detail

**命令：log-adjacency-changes detail**

**no log-adjacency-changes detail**

**功能：**设置是否记录OSPF邻居变化的日志信息。

**参数：**无。

**缺省情况：**不记录OSPF邻居变化的日志信息。

**命令模式：**OSPF协议配置模式。

**使用指南：**当配置该命令时，将OSPF邻居变化的信息记录到日志中。

**举例：**

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)# log-adjacency-changes detail

## 5.4.43 max-concurrent-dd

**命令：max-concurrent-dd *<value>***

**no max-concurrent-dd**

**功能：**本命令配置OSPF进程处理当前dd的最大并发数，no命令恢复默认值。

**参数：*<value>***取值范围为***<1-65535>***，处理最大并发dd数据包的上限。

**缺省情况：**没有缺省配置，不限制并发 dd 的数量。

**命令模式：**OSPF 协议配置模式。

**使用指南：**指定OSPF进程处理当前dd的最大并发数。

**举例：**设置最大并发 dd 为 20。

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#max-concurrent-dd 20

## 5.4.44 neighbor

**命令：neighbor A.B.C.D [*<cost>*| priority *<value>* | poll-interval *<value>*]**

**no neighbor A.B.C.D [*<cost>*| priority *<value>* | poll-interval *<value>*]**

**功能：**本命令配置互联NBMA网络的OSPF路由器，no命令移去配置。

**参数：*<cost>***，OSPF邻居费用值，范围1-65535；

**priority *<value>*** ，邻居优先级，缺省值为0，范围0-255；

**poll-interval *<value>***，缺省值为120s，未形成邻居关系的路由器链路之间的轮询时间，范围1-65535。

**缺省情况：**没有缺省配置。

**命令模式：**OSPF 协议配置模式。

**使用指南：**在NBMA网络上手动配置邻居使用本命令，应该为每一个知道的非广播网络邻居路由器配置一个邻居项。配置的邻居地址应该是接口的主地址。poll-interval的值应该比hello-interval大得多。

**举例：**

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#neighbor 1.2.3.4 priority 1 poll-interval 90

Switch(config-router)#neighbor 1.2.3.4 cost 15

## 5.4.45 network area

**命令：network NETWORKADDRESS area <*area-id*>**

**no network NETWORKADDRESS area <*area-id*>**

**功能：**本命令在具有与网络地址相匹配的IP地址的接口上使能OSPF路由功能。no命令移去配置并且停止在相应接口上运行OSPF。

**参数：NETWORKADDRESS = A.B.C.D/M | A.B.C.D X.Y.Z.W，**网络地址的前缀表示或者掩码表示，如果是掩码表示，则是wildcast掩码；

**<*area-id*>**是IP地址格式或者点分十进制格式的区域号，如果是十进制格式的整数，则取值范围是0~4294967295。

**缺省情况：**没有缺省配置。

**命令模式：**OSPF 协议配置模式。

**使用指南：**当配置某个网段在某个区域后，该网段所在的接口就属于该区域下，与其相连的邻居开始进行hello和数据库交互。

**举例：**配置 10.1.1.0/24 在区域 1 里。

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#network 10.1.1.0/24 area 1

## 5.4.46 ospf abr-type

**命令：ospf abr-type {cisco|ibm|shortcut|standard}**

**no ospf abr-type**

**功能：**使用本命令配置一个OSPF ABR类型，no命令恢复默认值。

**参数：cisco**，使用cisco ABR实现方式；

**ibm**，使用ibm ABR实现方式；

**shortcut**，指定一个shortcut-ABR；

**standard**，使用标准（RFC2328）ABR实现方式。

**缺省情况：**缺省配置为 **cisco**。

**命令模式：**OSPF 协议配置模式。

**使用指南：**指定abr的实现类型。本命令有利于OSPF不同实现之间的互操作。在多宿主的环境下，这个命令特别有用。

**举例：**配置 abr 为 standard。

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#ospf abr-type standard

## 5.4.47 ospf router-id

**命令：ospf router-id *<address>***

**no ospf router-id**

**功能：**为OSPF进程配置一个路由器 ID，no命令取消ID号。

**参数：*<address>***，router-id的IPv4地址格式。

**缺省情况：**没有缺省配置。

**命令模式：**OSPF 协议配置模式。

**使用指南：**新的router-id立即生效。

**举例：**配置 ospf 100 的 router-id 为 2.3.4.5。

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#ospf router-id 2.3.4.5

## 5.4.48 overflow database

**命令：overflow database *<maxdbsize >* [{hard|soft}]**

**no overflow database**

**功能：**本命令配置最大 LSA 条数。no 操作不限制最大条数。

**缺省情况：**缺省不配置。

**参数：< *maxdbsize* >**LSA最大条数，取值范围0~4294967294；

**soft**：软限制，越界给出警告；

**hard**：硬限制，越界则直接关闭ospf实例；

如果不配置soft或者hard，则按照配置hard处理。

**命令模式**：OSPF 协议配置模式。

**举例**：

Switch#config terminal

Switch(config)#router ospf

Switch(config-router)#overflow database 10000 soft

## 5.4.49 overflow database external

**命令**：**overflow database external [<*maxdbsize* > <*maxtime*>]**

**no overflow database external [<*maxdbsize* > <*maxtime*>]**

**功能**：本命令配置外部链路数据库的大小以及路由器在退出 overflow 状态前所必需等待的时间。no 操作恢复缺省值。

**参数**：< ***maxdbsize*** >外部链路数据库的大小，取值范围0~4294967294，缺省值4294967294;

**< *maxtime* >**路由器在试图退出数据库 overflow 状态前必须等待的秒数，取值范围0~65535。

**命令模式**：OSPF 协议配置模式。

**举例**：

Switch#config terminal

Switch(config)#router ospf

Switch(config-router)#overflow database external 5 3

## 5.4.50 passive-interface

**命令**：**passive-interface<*ifname*> [<ip-address>]**

**no passive-interface<*ifname*> [<ip-address>]**

**功能**：配置在特定接口上不发送 hello 分组，本命令的 no 操作取消该功能。

**参数**：<***ifname***>是具体的接口名；

**<*ip-address*>**接口的 IP 地址，点分十进制格式。

**缺省情况**：缺省不配置。

**命令模式**：OSPF 协议配置模式。

**举例**：

Switch#config terminal

Switch(config)#router ospf

Switch(config-router)#passive-interface vlan1

## 5.4.51 redistribute

**命令：** **redistribute {kernel |connected| static| rip| isis| [<area tag>] bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>][tag<*tag-value*>]**

**no redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>][tag<*tag-value*>]**

**功能：**引入从其它路由协议学习到的路由到 OSPF 中。

**参数：****kernel** 从核心路由中引入；

**connected** 从直连路由中引入；

**static** 从静态路由中引入；

**rip** 从 RIP 路由中引入；

**area tag** 域名；

**isis** 从 ISIS 路由中引入；

**bgp** 从 BGP 路由中引入；

**metric <*value*>**是赋给引入路由的度量，取值范围 0-16777214；

**metric-type {1|2}**是引入的外部路由的度量类型，只能取 1 或者 2，缺省为 2；

**route-map <*word*>**指向用于引入路由的路由地图的指针；

**tag<*tag-value*>**是外部路由的标记号，取值范围 0~4294967295，缺省为 0。

**命令模式：OSPF 协议配置模式。**

**使用指南：**将其它路由协议学习引入到 OSPF 区域，生成 AS-external_LSAs。

**举例：**

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#redistribute bgp metric 12
```

## 5.4.52 redistribute ospf

**命令：****redistribute ospf [<*process-id*>] [metric<*value*>] [metric-type {1|2}][route-map<*word*>]**

**no redistribute ospf [<*process-id*>] [metric<*value*>] [metric-type {1|2}] [route-map<*word*>]**

**功能：**引入 process-id 进程的路由引入到本进程中。此命令的 no 操作取消对引入 process-id 进程的路由到本进程中，当输入 metric，metric-type 和 routermap 可选参数时，表示恢复默认引入属性配置。

**参数：****process-id** 是 OSPF 进程 id 号，默认为 0。

**metric <*value*>**是赋给引入路由的度量，取值范围 0-16777214。

**metric-type {1|2}**是引入的路由的度量类型，只能取 1 或者 2，缺省为 2。

**route-map <*word*>**指向用于引入路由的路由地图的指针。

**缺省情况：**默认不引入任何 OSPF 进程的路由。

**命令模式：**router ospf 配置模式。

**使用指南：**当不输入 process-id 时，表示要引入默认 OSPF 进程的路由（process-id 为 0）。

**举例：**

Switch(config-router)#redistribute ospf

## 5.4.53 router ospf

**命令：router ospf <process_id> <vrf-name>**

**no router ospf <process_id> <vrf-name>**

**功能：** 配置本命令使能 OSPF 进程和一个具体的 VPN 关联起来，配置成功之后该 OSPF 进程下的所有配置命令均和该 VPN 相关。本命令的 no 操作删除与该 VPN 路由/转发实例相关联的 OSPF 实例。

**参数：** ***<process_id>***指明了要创建的 OSPF 进程 ID，取值范围应该说明，为<1-65535>。

**<vrf-name>**指明了 VPN 路由/转发实例的名称。

**命令模式：** 全局模式。

**使用指南：** 在使用本命令前，必须首先使用命令ip vrf 生成一个VPN 路由/转发实例，然后使用本命令可以将该VPN 路由/转发实例与OSPF 实例关联起来。

**举例：**

Switch#config terminal

Switch(config)#router ospf 100 VRF1

Switch(config-router)#network 10.1.1.0/24 area 0

## 5.4.54 show ip ospf

**命令：show ip ospf [*<process-id>*]**

**功能：** 显示 OSPF 主要信息。

**参数：** ***<process-id>***是进程 ID，取值范围 0~65535。

**缺省情况：** 不显示。

**命令模式：** 特权和配置模式。

**举例：**

Switch#show ip ospf

Routing Process 'ospf 0' with ID 192.168.1.1

Process bound to VRF default

Process uptime is 2 days 0 hour 30 minutes

Conforms to RFC2328, and RFC1583Compatibility flag is disabled

Supports only single TOS(TOS0) routes

Supports opaque LSA

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

Refresh timer 10 secs

Number of external LSA 0. Checksum Sum 0x000000

Number of opaque AS LSA 0. Checksum Sum 0x000000

Number of non-default external LSA 0

External LSA database is unlimited.
Number of LSA originated 0
Number of LSA received 0
Number of areas attached to this router: 1
Area 0 (BACKBONE) (Inactive)
Number of interfaces in this area is 0(0)
Number of fully adjacent neighbors in this area is 0
Area has message digest authentication
SPF algorithm executed 0 times
Number of LSA 0. Checksum Sum 0x000000

Routing Process 'ospf 10' with ID 0.0.0.0
Process bound to VRF test
Process uptime is 4 days 23 hours 51 minutes
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 0
Number of LSA received 0
Number of areas attached to this router: 1
Area 0 (BACKBONE) (Inactive)
Number of interfaces in this area is 0(0)
Number of fully adjacent neighbors in this area is 0
Area has no authentication
SPF algorithm executed 0 times
Number of LSA 0. Checksum Sum 0x000000

## 5.4.55 show ip ospf border-routers

**命令：show ip ospf [*<process-id>*] border-routers**

**功能：**显示本交换机到达所有实例下的 ABR 和 ASBR 的域内路由条目。

**参数：*<process-id>***是进程 ID，取值范围 0~65535。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**举例：**

Switch#show ip ospf border-routers

OSPF process 0 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 10.15.0.1 [10] via 10.10.0.1, Vlan1, ASBR, Area 0.0.0.0

i 172.16.10.1 [10] via 10.10.11.50, Vlan2, ABR, ASBR, Area 0.0.0.0

## 5.4.56 show ip ospf database

**命令：show ip ospf [*<process-id>*] database[{**

**adv-router [{<*linkstate_id*>|self-originate |adv-router <*advertiser_router*>}]**

**|asbr-summary[{<*linkstate_id*> |self-originate |adv-router <*advertiser_router*>}]**

**|externel [{<*linkstate_id*>| self-originate |adv-router <*advertiser_router*>}]**

**|network [{<*linkstate_id*>|self-originate |adv-router <*advertiser_router*>}]**

**|nssa-external [{<*linkstate_id*>|self-originate |adv-router <*advertiser_router*>}]**

**|opaque-area [{<*linkstate_id*>|self-originate |adv-router <*advertiser_router*>}]**

**|opaque-as [{<*linkstate_id*>|self-originate |adv-router <*advertiser_router*>}]**

**|opaque-link [{<*linkstate_id*>|self-originate |adv-router <*advertiser_router*>}]**

**|router [{<*linkstate_id*>|self-originate |adv-router <*advertiser_router*>}]**

**|summary [{<*linkstate_id*>|self-originate |adv-router <*advertiser_router*>}]**

**|self-originate | max-age }]**

**功能：**显示 OSPF 连接状态数据库信息。

**参数：*<process-id>***是进程 ID，取值范围 0~65535；

***<linkstate_id>*** Link state ID，点分十进制 IP 地址形式；

***<advertiser_router>***是 Advertising 路由器的 ID，点分十进制 IP 地址形式。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**使用指南：**根据本命令的输出信息，可以查看 OSPF 连接状态数据库信息。

**举例：**

Switch#show ip ospf database

Router Link States (Area 0.0.0.2)

| Link ID | ADV Router | Age | Seq# | CkSum | Link count |
|---|---|---|---|---|---|
| 192.168.1.2 | 192.168.1.2 | 254 | 0x80000031 | 0xec21 | 1 |
| 192.168.1.3 | 192.168.1.3 | 236 | 0x80000033 | 0x0521 | 2 |

Net Link States (Area 0.0.0.2)

```
Link ID         ADV Router      Age Seq#       CkSum
20.1.1.2        192.168.1.2       254 0x8000002b  0xece4

                Summary Link States (Area 0.0.0.2)

Link ID         ADV Router      Age Seq#       CkSum  Route
6.1.0.0         192.168.1.2        68 0x8000002b  0x5757  6.1.0.0/22
6.1.1.0         192.168.1.2       879 0x8000002a  0xf8bc   6.1.1.0/24
22.1.1.0        192.168.1.2       308 0x8000000c  0xc8f0   22.1.1.0/24

                ASBR-Summary Link States (Area 0.0.0.2)

Link ID         ADV Router      Age Seq#       CkSum
192.168.1.1     192.168.1.2      1702 0x8000002a  0x89c7

                AS External Link States

Link ID         ADV Router      Age Seq#       CkSum  Route
2.2.2.0         192.168.1.1      1499 0x80000056 0x3a63   E2 2.2.2.0/24 [0x0]
2.2.3.0         192.168.1.1      1103 0x8000002b 0x0ec3   E2 2.2.3.0/24 [0x0]
```

## 5.4.57 show ip ospf interface

**命令：show ip ospf interface *<interface>***

**功能：**显示 OSPF 接口信息。

**参数：*<interface>***为接口名。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**举例：**

```
Switch#show ip ospf interface
Loopback is up, line protocol is up
  OSPF not enabled on this interface
Vlan1 is up, line protocol is up
  Internet Address 10.10.10.50/24, Area 0.0.0.0
    Process ID 0, Router ID 10.10.11.50, Network Type BROADCAST, Cost: 10
    Transmit Delay is 5 sec, State Waiting, Priority 1
    No designated router on this network
    No backup designated router on this network
    Timer intervals configured, Hello 35, Dead 35, Wait 35, Retransmit 5
      Hello due in 00:00:16
    Neighbor Count is 0, Adjacent neighbor count is 0
```

## 5.4.58 show ip ospf neighbor

**命令：show ip ospf [<*process-id*>] neighbor [{<*neighbor_id*> |all |detail [all] |interface<*ifaddress*>}]**

**功能：**显示 OSPF 邻接点信息。

**参数：*<process-id>***是进程 ID，取值范围 0~65535；

***<neighbor_id>***是点分十进制格式的邻居 ID；

**all**：显示所有邻居的信息；

**detail**：显示邻居的详细信息；

***<ifaddress>***接口的 IP 地址。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**使用指南：**根据本命令输出信息，可以查看 OSPF 邻居的情况。

**举例：**

Switch#show ip ospf neighbor

OSPF process 0:

| Neighbor ID | Pri | State | Dead Time | Address | Interface |
|---|---|---|---|---|---|
| 192.168.1.1 | 1 | Full/Backup | 00:00:32 | 6.1.1.1 | Vlan1 |
| 192.168.1.3 | 1 | Full/DR | 00:00:36 | 20.1.1.3 | Vlan2 |
| 192.168.1.3 | 1 | Full/ - | 00:00:30 | 20.1.1.3 | VLINK2 |

| 显示信息 | 解释 |
|---|---|
| Neighbor ID | 邻居 ID |
| priority | 优先级 |
| state | 邻居关系状态 |
| Dead time | 邻居死亡时间 |
| Address | 接口地址 |
| Interface | 接口名 |

## 5.4.59 show ip ospf redistribute

**命令：show ip ospf [<*process-id*>] redistribute**

**功能：**显示 ospf 进程引入其它外部路由的配置信息。

**参数：*<process-id>***是进程 ID，取值范围 0~65535。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**使用指南：**无。

**举例：**

Switch#show ip ospf redistribute

ospf process 1 redistribute information：

ospf process 2

ospf process 3

bgp

ospf process 2 redistribute information：

ospf process 1

bgp

ospf process 3 redistribute information：

ospf process 1

bgp

Switch#show ip ospf 2 redistribute

ospf process 2 redistribute information：

ospf process 1

bgp

## 5.4.60 show ip ospf route

**命令：show ip ospf [*<process-id>*] route**

**功能：**显示 OSPF 路由表信息。

**参数：*<process-id>***是进程 ID，取值范围 0~65535。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**举例：**

Switch#show ip ospf route

O 10.1.1.0/24 [10] is directly connected, Vlan1, Area 0.0.0.0

O 10.1.1.4/32 [10] via 10.1.1.4, Vlan1, Area 0.0.0.0

IA 11.1.1.0/24 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0

IA 11.1.1.2/32 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0

IA 12.1.1.0/24 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0

IA 12.1.1.2/32 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0

O 13.1.1.0/24 [10] is directly connected, Vlan4, Area 0.0.0.3

O 14.1.1.0/24 [10] is directly connected, Vlan5, Area 0.0.0.4

IA 15.1.1.0/24 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3

IA 15.1.1.2/32 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3

E1 100.1.0.0/16 [21] via 10.1.1.1, Vlan1

E1 100.2.0.0/16 [21] via 10.1.1.1, Vlan1

## 5.4.61 show ip ospf virtual-links

**命令：show ip ospf [*<process-id>*] virtual-links**

**功能：**显示 OSPF 虚连接信息。

**参数：*<process-id>***是进程 ID，取值范围 0~65535。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**举例：**

```
Switch#show ip ospf virtual-links
Virtual Link VLINK0 to router 10.10.0.9 is up
   Transit area 0.0.0.1 via interface Vlan1
   Transmit Delay is 1 sec, State Point-To-Point,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:02
      Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is down
   Transit area 0.0.0.1 via interface Vlan1
   Transmit Delay is 1 sec, State Down,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in inactive
      Adjacency state Down
```

## 5.4.62 show ip route process-detail

**命令：show ip route [database] process-detail**

**功能：**显示带有具体的进程标识（进程 id 或 tag）的 ip 路由表。

**参数：**含参数 database 表示显示所有路由，不含参数表示只显示生效路由。

**缺省情况：**默认不引入任何 OSPF 进程的路由。

**命令模式：**特权和配置模式。

**使用指南：**无。

**举例：**

```
Switch#show ip route database process-detail
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          > - selected route, * - FIB route, p - stale info
```

C *> 127.0.0.0/8 is directly connected, Loopback

O 192.168.2.0/24 [110/10] is directly connected, Vlan2, 00:06:13,process 12

C *> 192.168.2.0/24 is directly connected, Vlan2

## 5.4.63 show ip route vrf process-detail

本型号交换机不支持此命令。

## 5.4.64 show ip protocols

**命令：show ip protocols**

**功能：**显示运行的路由协议信息。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**举例：**

Switch#show ip protocols

使用 show ip protocols 命令可以显示当前三层交换机运行路由协议的信息。

例如，显示信息为：

Routing Protocol is "ospf 0"

Invalid after 0 seconds, hold down 0, flushed after 0

Outgoing update filter list for all interfaces is

Incoming update filter list for all interfaces is

Redistributing:

Routing for Networks:

10.1.1.0/24

12.1.1.0/24

Routing Information Sources:

Gateway Distance Last Update

Distance: (default is 110)

Address Mask Distance List

Routing Protocol is "bgp 0"

Outgoing update filter list for all interfaces is

Incoming update filter list for all interfaces is

IGP synchronization is disabled

Automatic route summarization is disabled

Neighbor(s):

Address FiltIn FiltOut DistIn DistOut Weight RouteMap

Incoming Route Filter:

## 5.4.65 summary-address

**命令：summary-address *<A.B.C.D/M>* [{not-advertise|tag*<tag-value>*}]**

**功能：**用特定地址范围来汇总或者抑制外部路由。

**参数：*<A.B.C.D/M>***地址范围，点分十进制格式 IPv4 地址加上掩码长度；

**not-advertised** 抑制外部路由；

**tag*<tag-value>***是外部路由的标记号，取值范围 0~4294967295，默认取 0。

**命令模式：OSPF 协议配置模式。**

**使用指南：**当把路由从其它路由协议引入 OSPF 时，要求在一个 external LSA 中分别通告每一条路由。使用本命令可以为那些被特定网络地址和掩码包含的引入路由只通告一条 summary 路由，这可以极大地减小链路状态数据库的大小。

**举例：**

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#summary-address 172.16.0.0/16 tag 3
```

## 5.4.66 timers spf

**命令：timers spf *<spf-delay> <spf-holdtime>***

**no timers spf**

**功能：**调整路由计算定时器的值。no 命令将相关的值恢复到默认。

**参数：*<spf-delay>*** 默认 5 秒；

***<spf-holdtime>***默认 10 秒。

**命令模式：OSPF 协议配置模式。**

**使用指南：** 本命令配置了收到拓扑变化与 SPF 计算之间的延迟时间，还配置了两次不连续的 SPF 计算之间的 hold 时间。

**举例：**

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#timers spf 5 10
```

# 5.5 BGP

## 5.5.1 address-family

**命令：address-family *<AFI> <SAFI>***

**功能：**进入地址族配置模式。

**参数：*<AFI>*** ：地址族，如 IPv4、IPv6、VPNv4 等；

***<SAFI>***：子地址族，如 unicast 、multicast 、VRF。

**缺省情况：**无。

**命令模式：**BGP 路由配置模式。

**使用指南：**由于 BGP-4 支持多协议，因此有些可以针对每个地址族进行的不同的配置。在没有进入该地址族模式时实际上是针对缺省地址族（通常是 IPv4 unicast）的进行配置，而进入这个地址族模式来配置非缺省模式的配置。

如果支持 MCE，需要启 VRF，将其与对应地址族进行关联；使用该命令针对指定的 VRF 进行配置，它独立于 IPv4 单播地址族。VRF 的配置在全局配置模式下使用 ip vrf <NAME>命令进行，只有配置了 VRF 之后才能进入该地址族进行配置。

如果支持 MPLS VPN，需要在边缘路由器上启动 VRF；为了实现 VPN 功能，在私网上使用 VRF 地址族为 BGP 建立邻居，在公网上使用 VPNv4 地址族建立 BGP 邻居。使用该命令对 VPNv4 地址族进行配置，它可以使用 IPv4 单播地址的连接，其邻居配置可以与 IPv4 单播相同，只需在该邻居上使用 neighbor A.B.C.D activate 使能该地址族即可。

**举例：**

1) 进入 IPv4 单播地址模式。

```
Switch(config-router)# address-family ipv4 unicast
```

2) 创建一个VRF名为test，并进入BGP的地址族进行配置。

```
Switch(config)#ip vrf test
Switch(config-vrf)#exit
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf test
Switch(config-bgp-vrf)#
```

3) 进入BGP VPNv4 地址族配置模式。

```
Switch(config)#router bgp 100
Switch(config-router)#address-family vpnv4
Switch(config-bgp-vpnv4)#
```

**相关命令：exit-address-family**

## 5.5.2 aggregate-address

**命令：aggregate-address *<ip-address/M>* [summary-only] [as-set]**

**no aggregate-address *<ip-address/M>* [summary-only] [as-set]**

**功能：**通过地址聚合可以减少向外大量扩散路由消息；no 命令取消配置。

**参数：*<ip-address/M>***：IP 地址、掩码长度。

**[summary-only]**：指仅发送聚合而忽略具体路由。

**[as-set]**：以列表形式表示路径上的 AS，每个 AS 只出现一次。

**缺省情况：**没有聚合配置。

**命令模式：**地址族配置模式。

**使用指南：**通过地址聚合可以减少向外大量扩散路由消息。使用 summary-only 选项可以只向邻居扩散聚合路由而不扩散具体路由，而 as-set 选项可以把聚合所覆盖的各路由所来源的各 AS 都只列出一次而不会重复列出。

**举例：**

Switch(config-router)# aggregate-address 100.1.0.0/16 summary-only

Switch(config-router)# aggregate-address 100.2.0.0/16 summary-only as-set

Switch(config-router)# aggregate-address 100.3.0.0/16 as-set

**相关命令：bgp aggregate-nexthop-check, no bgp aggregate-nexthop-check**

## 5.5.3 bgp aggregate-nexthop-check

**命令：bgp aggregate-nexthop-check**

**no bgp aggregate-nexthop-check**

**功能：**配置 BGP 在聚合时是否对所有聚合的路由的下一跳进行检查，其 no 形式取消该配置，即不对聚合路由的下一跳是否一致进行检查。

**参数：**无。

**缺省情况：**聚合时不进行下一跳检查。

**命令模式：**全局配置模式。

**使用指南：**进行检查时，若所覆盖路由的下一跳有不统一的情况就不进行聚合。而不进行检查时，只要为聚合地址所覆盖的路由都会聚合到聚合路由里。

**举例：**

Switch(config)#bgp aggregate-nexthop-check

**相关命令：aggregate-address, no aggregate-address**

## 5.5.4 bgp always-compare-med

**命令：bgp always-compare-med**

**no bgp always-compare-med**

**功能：**配置是否总是比较 MED。其 no 形式取消该配置。

**参数：**无。

**缺省情况：**不配置。

**命令模式：**BGP 路由配置模式。

**使用指南：**通常，BGP 仅在 AS 相同时才比较 MED，进行该项设置后，可以在不同 AS 来源的路由也比较 MED。

**举例：**

AS（200）的路由器收到来至两个 AS（100 和 300）同样的路由前缀，携带不同的 MED。配置该路由器总是进行 MED 比较。

Switch(config-router)#bgp always-compare-med

## 5.5.5 bgp asnotation asdot

**命令：bgp asnotation asdot**

**no bgp asnotation asdot**

**功能：**配置以 ASDOT 的方式显示 AS 号和进行正则表达式的匹配。其 no 形式取消以 ASDOT 方式显示和进行正则式匹配。

**参数：**无。

**缺省情况：**系统默认为 ASPLAIN 方式。

**命令模式：**BGP 路由配置模式。

**使用指南：**要改变显示 AS 号和正则表达式的匹配的方式，在配置此命令后还必须配置“clear ip bgp *”来重启所有的 BGP 邻居关系，来使配置生效。

**举例：**

配置以 ASDOT 的方式显示 AS 号和进行正则表达式的匹配

Switch(config)#router bgp 200

Switch(config-router)#bgp asnotation asdot

**相关命令：**无

## 5.5.6 bgp bestpath as-path ignore

**命令：bgp bestpath as-path ignore**

**no bgp bestpath as-path ignore**

**功能：**配置忽略 AS-PATH 的长度。其 no 形式取消该配置。

**参数：**无。

**缺省情况：**不配置。

**命令模式：**BGP 路由配置模式。

**使用指南：**通常 BGP 在选路时会比较 AS-PATH 的长度。进行该项设置后，可以忽略其长度。

**举例：**

配置忽略 AS-PATH 的长度：

Switch(config)#router bgp 200

Switch(config-router)#bgp bestpath as-path ignore

**相关命令：bgp bestpath compare-confed-aspath, bgp bestpath compare-routerid, bgp bestpath med, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-routerid, no bgp bestpath med**

## 5.5.7 bgp bestpath compare-confed-aspath

**命令：bgp bestpath compare-confed-aspath**

**no bgp bestpath compare-confed-aspath**

**功能：**配置关注联盟 AS-PATH 的长度。其 no 形式取消该配置。

**参数：**无。

**缺省情况：**不配置。

**命令模式：**BGP 路由配置模式。

**使用指南：**通常的，BGP 在选路时仅会比较外部 AS-PATH 的长度，进行该项设置后，可以同时比较 AS 内部联盟的 AS-PATH 长度。

**举例：**配置关注联盟 AS-PATH 的长度。

Switch(config-router)#bgp bestpath compare-confed-aspath

**相关命令：bgp bestpath as-path ignore, bgp bestpath compare-routerid, bgp bestpath med, no bgp bestpath as-path ignore, no bgp bestpath compare-routerid, no bgp bestpath med**

## 5.5.8 bgp bestpath compare-routerid

**命令：bgp bestpath compare-routerid**

**no bgp bestpath compare-routerid**

**功能：**配置比较路由器 ID。其 no 形式取消该配置。

**参数：**无。

**缺省情况：**不配置。

**命令模式：**BGP 路由配置模式。

**使用指南：**通常的，来自同一 AS 的路由（其他条件相同）会选择最先到达的作为最优路由，配置该命令后，则会比较来源路由器的 ID。

**举例：** AS200 的一台设备收到了来至同一个 AS（100）的两台设备的同样的路由前缀通告，可以配置该设备进行路由器 ID 比较。

Switch(config-router)#bgp bestpath compare-routerid

**相关命令：bgp bestpath compare-confed-aspath, bgp bestpath compare-confed-aspath, bgp bestpath med, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-confed-aspath, no bgp bestpath med**

## 5.5.9 bgp bestpath med

**命令：bgp bestpath med {[confed] [missing-as-worst]}**

**no bgp bestpath med {[confed] [missing-as-worst]}**

**功能：**配置在联盟路径中比较 MED 的属性，以及缺少 MED 时认为其值为最大。其 no 形式取消该配置。

**参数：[confed]**：在联盟路径中比较 MED；

**[missing-is-worst]**：认为 MED 缺少时 MED 值为最大。

**缺省情况：**不配置。

**命令模式：**BGP 路由配置模式。

**使用指南：**可以通过该命令选择在联盟间是否比较 MED，在 MED 没有时，若配置了 missing-is-worst 则认为 MED 为最大值，否则认为是 0。

**举例：**配置在联盟路径中比较 MED，若 MED 缺少时认为 MED 值为最大。

Switch(config-router)#bgp bestpath med confed missing-as-worst

**相关命令：bgp bestpath compare-confed-aspath, bgp bestpath compare-confed-aspath, bgp bestpath compare-routerid, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-routerid**

## 5.5.10 bgp client-to-client reflection

**命令：bgp client-to-client reflection**

**no bgp client-to-client reflection**

**功能：**配置是否进行路由反射。其 no 形式取消该配置。

**参数：**无。

**缺省情况：**在配置了客户的情况下，缺省进行反射。

**命令模式：**BGP 路由配置模式。

**使用指南：**在使用 neighbor {<ip-address>|<TAG>} route-reflector-client 配置了反射客户后，路由器缺省在 client 间进行路由反射。使用该命令的 no 形式取消 client 间的路由反射（client 与非 client 间的反射不受影响）。

**举例：**配置不进行路由反射。

Switch(config-router)#no bgp client-to-client reflection

**相关命令：neighbor route-reflector-client, no neighbor route-reflector-client**

## 5.5.11 bgp cluster-id

**命令：bgp cluster-id {*<ip-address>*|*<01-4294967295>*}**

**no bgp cluster-id {<[*<ip-address>*]|*<0-4294967295>*}**

**功能：**配置进行路由反射时的路由反射簇 ID。其 no 形式取消该配置。

**参数：*<ip-address>*|*<1-4294967295>*：**cluster-id，分别为用点分十进制或 32 位数表示。

**缺省情况：**不配置。

**命令模式：**BGP 路由配置模式。

**使用指南：** 一个 cluster 包含一个区域内的路由反射器和它的客户，但为了提高冗余度，有时一个区域内会配置超过一台路由反射器。当只有一个路由反射器时，区域可以以路由反射器的 router-id 作为标识，而有两个以上的反射器时，则需要配置 cluster-id 作为区域的标识。

**举例：**配置路由反射簇ID为1.1.1.1。

Switch(config-router)#bgp cluster-id 1.1.1.1

**相关命令：neighbor route-reflector-client**

## 5.5.12 bgp confederation identifier

**命令：bgp confederation identifier *<as-id>***

**no bgp confederation identifier [*<as-id>* | *word*]**

**功能：**创建/删除一个联盟配置。其 no 形式删除一个联盟。

**参数：*<as-id>***：联盟 AS 的 ID 号，取值范围为 1-4294967295。可用十进制表示，如 6553700；也可用分隔符方式表示，如 100.100。

**缺省情况：**没有联盟。

**命令模式：**BGP 路由配置模式。

**使用指南：**使用联盟可以把大的 AS 分为若干小 AS，而对外仍然只识别大的 AS。使用这个命令创建大的 AS 号。

**举例：**

Switch(config-router)# bgp confederation identifier 600

**相关命令：bgp confederation peers，no bgp confederation peers**

## 5.5.13 bgp confederation peers

**命令：bgp confederation peers *<as-id>* [*<as-id>..*]**

**no bgp confederation peers *<as-id>* [*<as-id>..*]**

**功能：**添加/删除一个或多个 AS 到一个联盟。其 no 形式从联盟删除一个或多个 AS。

**参数：*< as-id>***：联盟包含的 AS 的 ID 号，取值范围为 1-4294967295。可用十进制表示，如 6553700；也可用分隔符方式表示，如 100.100。可以是多个。

**缺省情况：**没有成员。

**命令模式：**BGP 路由配置模式。

**使用指南：**使用联盟可以把大的 AS 分为若干小 AS，而对外仍然只识别大的 AS。使用这个命令向联盟里添加/删除联盟的成员。

**举例：**创建 1 个联盟，ID 号为 600，添加成员 100，200，100.300。

Switch(config-router)# bgp confederation identifier 600

Switch(config-router)#bgp confederation peers 100 200 100.300

**相关命令：bgp confederation identifier**

## 5.5.14 bgp dampening

**命令：bgp dampening [*<1-45>*] [*<1-20000> <1-20000> <1-255>*] [*<1-45>*]**

**no bgp dampening**

**功能：**配置路由衰减。其 no 形式取消路由衰减功能。

**参数：*<1-45>***：分别为可达和不可达路由的惩罚半衰期，即惩罚值减小到原来一半的时间，单位为分钟。

***<1-20000>***：分别为惩罚的再使用界限和抑制界限。

***<1-255>***：抑制路由的最大抑制时间，单位为分钟。

**缺省情况：**可达路由的半衰期为 15 分钟，不可达路由的半衰期为 15 分钟。抑制界限为 2000，再使用界限为 750，最大抑制时间为 60 分钟。

**命令模式：BGP** 地址族配置模式。

**使用指南：**使用路由衰减技术可以减少不稳定路由带来的过多的路由更新，路由衰减的算法是当路由波动时对路由进行惩罚，惩罚超过抑制界限时就不再对路由进行广告，路由若不再波动则按时间减小惩罚值，其减小按指定半衰期的指数规律进行，当惩罚值小于再使用界限后路由再次被广告，或者抑制时间超过最大抑制时间也将再次广告该路由。本指令就是启动/取消路由衰减并配置所需的参数。

**举例：**启动路由衰减，并且采用缺省的参数配置。

Switch(config-bgp-ipv4)# bgp dampening

## 5.5.15 bgp default

**命令：bgp default {ipv4-unicast|local-preference *<0-4294967295>*}**

**no bgp default {ipv4-unicast|local-preference [*<0-4294967295>*]}**

**功能：**设置 BGP 的缺省配置。其 no 形式取消该配置。

**参数： ipv4-unicast：**配置缺省采用IPv4单播建立邻居关系。

**local-preference*<0-4294967295>*：**配置缺省的本地优先级。

**缺省情况：**IPv4 单播为在 BGP 启动时缺省启动，缺省的本地优先级为 100。

**命令模式：**BGP 路由配置模式。

**使用指南：**BGP 缺省启动 IPv4 单播地址族，可以使用 no bgp default ipv4-unicast 命令取消该配置，则不再缺省启动该地址族。可以通过 bgp default local-preference 命令配置缺省的本地优先级。

**举例：**配置本地缺省优先级为 500。

在 10.1.1.66 上配置：

Switch(config)#router bgp 200

Switch(config-router)# bgp default local-preference 500

## 5.5.16 bgp deterministic-med

**命令：bgp deterministic-med**

**no bgp deterministic-med**

**功能：**设置 BGP 在 AS 内同样的前缀采用最优的 MED 与其它 AS 进行比较。其 no 形式取消该配置。

**参数：**无。

**缺省情况：**不配置。

**命令模式：**BGP 路由配置模式。

**使用指南：**通常如果同样的前缀路由来自多个路径，各路径将分别进行比较，配置了该属性后，系统会只采用每个 AS 中 MED 最小的（其他主要属性都相等时）路径和其它 AS 进行比较，得到最优的之后，再不管 MED 值在 AS 内部比较进行选路。

**举例：**设置 BGP 在 AS 内同样的前缀采用最优的 MED 与其它 AS 进行比较。

Switch(config-router)#bgp deterministic-med

## 5.5.17 bgp enforce-first-as

**命令：bgp enforce-first-as**

**no bgp enforce-first-as**

**功能：**设置 BGP 在接收外部的路由时，强制路由的 AS-PATH 必须在第一个 AS 的位置包含邻居的 AS 号，否则中断该对等体的连接。其 no 形式取消该配置。

**参数：**无。

**缺省情况：**不配置。

**命令模式：**BGP 路由配置模式。

**使用指南：**这通常是为了避免不安全或未经认证的路由。

**举例：**

Switch(config-router)#bgp enforce-first-as

## 5.5.18 bgp fast-external-failover

**命令：bgp fast-external-failover**

**no bgp fast-external-failover**

**功能：**设置 BGP 邻居连接在接口发生变化时快速重置，而不等待 TCP 超时。其 no 形式取消该配置。

**参数：**无。

**缺省情况：**配置。

**命令模式：**BGP 路由配置模式。

**使用指南：**可以让与邻居的连接在接口 DOWN 时立即中断。

**举例：**

Switch(config-router)# bgp fast-external-failover

## 5.5.19 bgp inbound-route-filter

**命令：bgp inbound-route-filter**

**no bgp inbound-route-filter**

**功能：** 配置 bgp 不安装本地没有的 RD 的路由信息，其 no 形式表示不管本地有没有该 RD，都安装其路由信息到 BGP。

**参数：** 无。

**命令模式：** BGP 模式。

**使用指南：** 通常情况下，交换机作为 PE 出现时，bgp 从 VPN 得到的路由，会根据本 PE 所配置的 VRF 中是否有匹配的信息来决定是否在 BGP 中保存该路由，使用该命令的 no 形式，BGP 将不再判断本 PE 是否包含匹配的信息，而一律保留该路由信息。

**举例：**

Switch(config)#router bgp 100

Switch(config-router)#no bgp inbound-route-filter

## 5.5.20 bgp inbound-max-route-num

**命令：bgp inbound-max-route-num <0-500000>**

**no bgp inbound-max-route-num**

**功能：**限制 bgp 进程从其邻居学到的路由的数量。

**参数：**具体限制的路由数量，取值范围为<0-500000>。

**缺省情况：**缺省限制数量为 50000 条。

**命令模式：**BGP 路由配置模式和地址族配置模式。

**使用指南：**可以通过该命令，限制 bgp 进程从其邻居学到的路由的数量。

**举例：**经过如下配置，bgp 进程最多可以从其邻居接受 20000 条路由。

Switch(config-router)#bgp inbound-max-route-num 20000

**相关命令：**无

## 5.5.21 bgp log-neighbor-changes

**命令：bgp log-neighbor-changes**

**no bgp log-neighbor-changes**

**功能：**设置 BGP 邻居变化时输出 log 信息。其 no 形式取消该配置。

**参数：**无。

**缺省情况：**不配置。

**命令模式：**BGP 路由配置模式。

**使用指南：**配置该命令后，可以在监视器上输出邻居变化信息。

**举例：**

Switch(config-router)# bgp log-neighbor-changes

**相关命令：**无

## 5.5.22 bgp network import-check

**命令：bgp network import-check**

**no bgp network import-check**

**功能：**设置是否检查 BGP 网络路由的 IGP 可达性。其 no 形式设置不检查 IGP 可达性。

**参数：**无。

**缺省情况：**不配置。

**命令模式：**BGP 路由配置模式。

**使用指南：**对于 BGP 通告的路由，是否检查其 IGP 是否可达，也就是检查其下一跳是否存在且 IGP 可达。

**举例：**设置检查 BGP 网络路由的 IGP 可达性。

Switch(config-router)# bgp network import-check

## 5.5.23 bgp rfc1771-path-select

**命令：bgp rfc1771-path-select**

**no bgp rfc1771-path-select**

**功能：**配置了该属性后，在选路比较时按 rfc1771 规定的方式，即在存在不同外部 AS 时不检查 AS 内部的 METRIC；否则，要对该内部的 METRIC 进行比较。

**参数：**无。

**缺省情况：**遵循。

**命令模式：**全局配置模式。

**使用指南：**配置了该属性后，在选路比较时按 rfc1771 规定的方式。即在存在不同外部 AS 时不检查 AS 内部的 METRIC。否则如果没有配置该属性，则要对该值进行比较。

**举例：**配置遵循 rfc1771 的规定进行路径选择。

Switch(config)# bgp rfc1771-path-select

## 5.5.24 bgp rfc1771-strict

**命令：bgp rfc1771-strict**

**no bgp rfc1771-strict**

**功能：**配置是否严格遵循 rfc1771 的限制。其 no 形式表示不严格遵循 rfc1771 的限制。

**参数：**无。

**缺省情况：**不遵循 RFC1771 的限制。

**命令模式：**全局配置模式。

**使用指南：**配置了该属性，对于从 RIP、OSPF、ISIS 等协议得到的路由被认为始发类型为 IGP（来自于内部），若没有配置该属性，上述协议得到的路由会被认为始发类型为 INCOMPLETE（不完整）。

**举例：**配置严格遵循 rfc1771 的限制。

Switch(config)#bgp rfc1771-strict

## 5.5.25 bgp router-id

**命令：bgp router-id *<A.B.C.D>***

**no bgp router-id [*<A.B.C.D>*]**

**功能：**手动设置路由器的 ID。其 no 形式取消该配置。

**参数：*<A.B.C.D>*：**路由器 ID。

**缺省情况：**自动取得路由器 ID。

**命令模式：**BGP 路由配置模式。

**使用指南：**通过该命令手动设定路由器 ID。

**举例：**设置路由器 ID 为 1.1.1.1。

Switch(config-router)#bgp router-id 1.1.1.1

**相关命令：**无。

## 5.5.26 bgp scan-time

**命令：bgp scan-time *<0-60>***

**no bgp scan-time [*<0-60>*]**

**功能：**设置 BGP 定期对路由下一跳是否合法的检查的时间间隔。其 no 形式恢复该值为默认值。

**参数：*<0-60>*：**进行检查的时间间隔。

**缺省情况：**间隔为 60s。

**命令模式：**BGP 路由配置模式。

**使用指南：**对于 BGP 路由的下一跳，定期检查其是否合法，该命令用于配置进行该检查的时间间隔，若不想进行检查，设该参数为 0。

**举例：**设置 BGP 定期对路由下一跳是否合法的检查的时间间隔为 30s。

Switch(config-router)# bgp scan-time 30

**相关命令：**无。

## 5.5.27 clear ip bgp

**命令：clear ip bgp * [vrf <vrf-name>] [in | out | soft [in | out ]]**

**功能：** 重启 vrf-name 对应的 BGP 进程与该进程下所有 peer 之间的连接。

**参数：** **<vrf-name>：** 配置的 VPN 实例名称，取值长度范围 1～64；

**in：** 软重启配置入站更新；

**out：** 软重启配置出站更新；

**soft：** 软重启。

**缺省情况：** 默认不配置。

**命令模式：** 特权模式。

**使用指南：** 当配置 clear ip bgp *命令，重启 BGP 进程；当配置 in 参数，将会向邻居发送请求路由的消息；当配置 out 参数，将自己的路由发送给邻居。配置了 soft，将不会重启 BGP 进程。

**举例：**

Switch#clear ip bgp * vrf VRF-A

Switch#

## 5.5.28 clear ip bgp dampening

**命令：clear ip bgp [*<address-family>*] dampening [<ip-address>|<ip-address/M>]**

**功能：**用于重置 BGP 路由衰减。

**参数：*<address-family>*：**地址族，如“ipv4 unicast”；

***<ip-address>*：**IP 地址；

***<ip-address/M>***：IP 地址及掩码。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**可以针对不同参数（如地址族或 IPv4 地址）清除 BGP 路由衰减的信息和状态。

**举例：**清除 IPv4 unicast 地址簇的 BGP 路由衰减的信息和状态。

Switch# clear ip bgp ipv4 unicast dampening

**相关命令：bgp dampening**

## 5.5.29 clear ip bgp flap-statistics

**命令：clear ip bgp [*<address-family>*] flap-statistics [*<ip-address>*|*<ip-address/M>*]**

**功能：**用于重置 BGP 路由衰减统计信息。

**参数：*<address-family>***：地址族，如“ipv4 unicast”；

***<ip-address>***：IP 地址；

***<ip-address/M>***：IP 地址及掩码。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**可以针对不同参数（如地址族或 IPv4 地址）清除 BGP 路由衰减的统计信息。

**举例：**清除 IPv4 unicast 地址簇的 BGP 路由衰减的统计信息。

Switch#clear ip bgp ipv4 unicast flap-statistics

**相关命令：bgp dampening**

## 5.5.30 debug bgp

**命令：debug bgp [*<MODULE>*|all]**

**no debug bgp [*<MODULE>*|all]**

**功能：**用于调试 BGP。其 no 形式用于关闭 BGP 的调试信息。

**参数：*<MODULE>***：BGP 模块名，包括 dampening、events、filters、fsm、keepalives、nsm、updates 等。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**可以监视 BGP 事件和发生的错误、警告信息等。

**举例：**显示 bgp 所有模块的调式信息。

Switch#debug bgp all

**相关命令：**无

## 5.5.31 debug bgp redistribute message send

**命令：debug bgp redistribute message send**

**no debug bgp redistribute message send**

**功能：**打开 BGP 进程引入其他 OSPF 不同进程、RIP 等协议的路由的命令下发调试开关。本命令的 no 操作关闭 BGP 进程引入其他 OSPF 不同进程、RIP 等协议的路由的命令下发调试开关。

**参数：**无。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#debug bgp redistribute message send

Switch#no debug bgp redistribute message send

## 5.5.32 debug bgp redistribute route receive

**命令：debug bgp redistribute route receive**

**no debug bgp redistribute route receive**

**功能：**打开 BGP 进程收到 nsm 发来的路由信息的调试开关。本命令的 no 操作关闭 BGP 进程收到 nsm 发来的路由信息的调试开关。

**参数：**无。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#debug bgp redistribute route receive

Switch#no debug bgp redistribute route receive

## 5.5.33 distance

**命令：distance *<1-255>* *<ip-address/M>* [*<WORD>*]**

**no distance *<1-255>* *<ip-address/M>* [*<WORD>*]**

**功能：**设置指定路由前缀的管理距离。其 no 形式恢复管理距离为默认值。

**参数：*<1-255>*：**设定的管理距离。

***<ip-address/M>*：**设定的路由前缀。

***<WORD>*：**访问列表名。

**缺省情况：**不配置。

**命令模式：**BGP 路由配置模式。

**使用指南：**对于指定的 BGP 路由，设定管理距离，以作为选路的依据。

**举例：**设定路由 90 10.1.1.64/32 的管理距离为 90。

Switch(config-router)# distance 90 10.1.1.64/32

**相关命令：distance bgp, no distance bgp**

## 5.5.34 distance bgp

**命令：distance bgp *<1-255> <1-255> <1-255>***

**no distance bgp [*<1-255> <1-255> <1-255>*]**

**功能：**设置 BGP 的协议管理距离。其 no 形式恢复管理距离为默认值。

**参数：*<1-255>*：**分别为 BGP 外部（EBGP）、内部（IBGP）路由和本地（LOCAL）路由的管理距离。

**缺省情况：**EBGP 为 20，其它的为 200。

**命令模式：**BGP 路由配置模式。

**使用指南：**对于 BGP 路由，设定管理距离，以作为 NSM 选路的依据。

**举例：**设定 EBGP 路由的管理距离为 15，IBGP 和本地路由的管理距离为 150。

Switch(config-router)# distance bgp 15 150 150

**相关命令：distance, no distance**

## 5.5.35 exit-address-family

**命令：exit-address-family**

**功能：**退出 BGP 地址族配置模式。

**参数：**无。

**缺省情况：**无。

**命令模式：**BGP 地址族配置模式。

**使用指南：**在 BGP 下对地址族配置时，使用该命令退出该模式以结束地址族配置。

**举例：**

Switch(config)#router bgp 100

Switch(config-router)#address-family ipv4 unicast

Switch(config-bgp-ipv4)# exit-address-family

Switch(config-router)#

**相关命令：address-family**

## 5.5.36 import map

**命令：import map <*map-name*>**

**no import map <*map-name*>**

**功能：** 使用该命令配置在 VRF 中引入路由时使用指定的路由图规则。

**参数：** ***<map-name>*** 为使用的路由图的名称。

**缺省情况：** 无。

**命令模式：** vrf 配置模式。

**使用指南：** 使用路由图命令 route-map NAME permit|deny <1-65535>建立路由图并设定规则，使用本命令可以将规则应用到本 VRF 的路由引入中。

**举例：** 本举例配置了一个路由图map1,再配置VRF test使用该路由图。

```
Switch(config)#route-map map1 permit 15
Switch(config-map)#match interface Vlan1
Switch(config-map)#set weight 655
Switch(config-map)#exit
Switch(config)#ip vrf test
Switch(config-vrf)#rd 100:10
Switch(config-vrf)#import map map1
Switch#show ip bgp vpn all neighbors
    Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:10 (Default for VRF test)
*> 11.1.1.0/24      11.1.1.64                0             0 200 ?
*>i15.1.1.0/24      10.1.1.68                0    100      655 300 ?
*> 20.1.1.0/24      11.1.1.64                0             0 200 ?
*>i100.1.1.0/24     10.1.1.68                0    100      655 300 ?
Route Distinguisher: 100:10
*>i15.1.1.0/24      10.1.1.68                0    100      0 300 ?
*>i100.1.1.0/24     10.1.1.68                0    100      0 300 ?
```

可以看到，从 VPN 引入的路由在进入 VRF test 的路由表后，权重变为了 655。

## 5.5.37 ip as-path access-list

**命令：ip as-path access-list *<.LINE>* {*<permit>*|*<deny>*} *<LINE>***

**no ip as-path access-list *<.LINE>* {*<permit>*|*<deny>*} *<LINE>***

**功能：**配置 AS-PATH 的访问列表。其 no 形式删除该访问列表。

**参数：*<.LINE>*：**访问列表名；

***<LINE>*：**AS-PATH 列表中匹配的字符串。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**使用该命令可以配置关于 AS-PATH 的访问列表，以提供通过/过滤的条件。

**举例：**配置名为 ASPF 的访问列表，过滤 AS-PATH 中含有 100 的路由。

```
Switch(config)#ip as-path access-list ASPF deny ^100$
```

## 5.5.38 ip community-list

**命令：ip community-list {*<LISTNAME>*|*<1-199>*|[expanded *<WORD>*]|[standard *<WORD>*]} {deny|permit} *<.COMMUNITY>***

**no ip community-list {*<LISTNAME>*|*<1-199>*|[expanded *<WORD>*]|[standard *<WORD>*]} [{deny|permit} *<.COMMUNITY>*]**

**功能：**配置团体列表。其 no 形式用于删除团体列表。

**参数：*<LISTNAME>*：**团体列表名；

***<1-199>*:** 标准或扩展团体号；

***<WORD>*:**标准或扩展团体号；

***<.COMMUNITY >*：**团体列表成员。可以是aa:nn，或者internet、local-AS、no-advertise、no-export的组合。在扩展情况下，可以是正则表达式表示的。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**使用该命令可以配置团体列表，以提供通过/过滤/查询的条件。

**举例：**配置名 LN 的 ip community-list, 允许 community 属性为 100:10。

Switch(config)# ip community-list LN permit 100:10

## 5.5.39 ip extcommunity-list

**命令：ip extcommunity-list {*<1-199>*|[expanded *<WORD>*]|[standard *<WORD>*]} {deny|permit} *<.COMMUNITY>***

**no ip extcommunity-list {*<LISTNAME>*|*<1-199>*|[expanded *<WORD>*]|[standard *<WORD>*]} {deny|permit} *<.COMMUNITY>***

**功能：**配置扩展团体列表。其 no 形式用于删除扩展团体列表。

**参数：** ***<1-199>*：** 标准或扩展团体号；

***<WORD>*：**标准或扩展团体号；

***<.COMMUNITY >*：**团体列表成员。可以是aa:nn、internet、local-AS、no-advertise、no-export的组合。在扩展情况下，可以是正则表达式表示的。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**使用该命令可以配置团体列表，以提供通过/过滤/查询的条件。

**举例：**配置名团体号为, 允许 community 属性为 100:10。

Switch(config)# ip extcommunity-list 1 permit rt 100:10

## 5.5.40 neighbor activate

**命令：neighbor {*<ip-address>*|*<TAG>*} activate**

**no neighbor {*<ip-address>*|*<TAG>*} activate**

**功能：**在 BGP 邻居上配置是否与 BGP 邻居交换指定地址族的路由。其 no 形式用于设置不交换指定地址族的路由。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

**缺省情况：**使能 IP 单播地址族的路由交换，不使能其它地址族。

**命令模式：**BGP 地址族配置模式。

**使用指南：**在 BGP 路由配置模式下，配置的是 IP 单播。在指定的地址族配置模式下，配置指定地址族是否交换。若本端和对端之中的任何一端不使能该选项，本端的该地址族路由都不能被对端得到，即使原来得到的相应地址族路由，在设置不使能后也会取消。

**举例：**配置和邻居 2002::2 交换单播路由。

```
Switch(config-router)#neighbor 2002::2 activate
Switch(config-router)#address-family ipv4
Switch(config-bgp-ipv4)#no neighbor 2002::2 activate
Switch(config-router-af)#
```

## 5.5.41 neighbor advertisement-interval

**命令：neighbor {*<ip-address>*|*<TAG>*} advertisement-interval *<0-600>***

**no neighbor {*<ip-address>*|*<TAG>*} advertisement-interval [*<0-600>*]**

**功能：**配置对指定邻居路由更新的间隔。其 no 形式恢复该值为默认值。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

***<0-600>*：**是广告时间间隔，单位为秒。

**缺省情况：**IBGP 的缺省值为 5s，EBGP 为 30s。

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式。

**使用指南：**减短该值会提升路由更新的速度，但也会多消耗带宽。

**举例：**设置和邻居 10.1.1.64 的路由更新间隔为 60 秒。

```
Switch(config-router)#neighbor 10.1.1.64 advertisement-interval 20
```

## 5.5.42 neighbor allowas-in

**命令：neighbor {*<ip-address>*|*<TAG>*} allowas-in [*<1-10>*]**

**no neighbor {*<ip-address>*|*<TAG>*} allowas-in**

**功能：**配置指定邻居的路由 AS 列表中同一 AS 允许出现的次数。其 no 形式恢复为不允许同一 AS 重复出现。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

***<1-10>*：**是允许一个 AS 号重复出现的次数。

**缺省情况：**缺省不允许 AS 在同一路由里重复出现。配置允许重复出现时，不带<1-10>参数的缺省允许重复次数为 3。

**命令模式：**BGP 地址族配置模式。

**使用指南：**通常 BGP 认为同一 AS 号是不能在路由中出现多次的，系统在接到自己 AS 号出现在 AS 路径中时会拒绝接受该路由。但为了支持某些特殊的需求，特别是例如对 VPN 的支

持，在扩展 BGP 上是允许经过配置让 AS 号重复出现的。这个命令是配置其可以重复出现的次数。

**举例：**设置邻居 10.1.1.66 的路由 AS 列表中同一 AS 允许出现的次数为 3。

Switch(config-router)#neighbor 10.1.1.66 allowas-in

## 5.5.43 neighbor as-override

**命令：neighbor {<ip-address> | <TAG>} as-override**

**no neighbor {*<ip-address>* | *<TAG>*} as-override**

**功能：** 覆盖 AS 路径(上一个 AS 号)，配置该命令需要先创建邻居；其 no 形式删除该设置。

**参数：*<ip-address>*：** 指定 BGP 邻居地址；

***<TAG>*：** 指定 BGP 邻居组编号。

**缺省情况：** 无。

**命令模式：** VRF 地址族配置模式。

**使用指南：** 配置该命令后，从邻居过来的路由将被覆盖已存在的上一个 AS 号。

**举例：**

Switch (config)#router bgp 100

Switch (config-router)#address-family ipv4 vrf VRF-A

Switch(config-bgp-vrf)#neighbor 3.0.0.1 remote-as 65001

Switch(config-bgp-vrf)# neighbor 3.0.0.1 as-override

Switch(config-bgp-vrf)#

## 5.5.44 neighbor attribute-unchanged

**命令：neighbor {*<ip-address>*|*<TAG>*} attribute-unchanged [as-path][med][next-hop]**

**no neighbor {*<ip-address>*|*<TAG>*} attribute-unchanged [as-path] [med] [next-hop]**

**功能：**配置指定邻居的路由中原样发送的某些属性，即属性透传。其 no 形式表示不进行属性透传。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

**缺省情况：**不配置任何属性不改变。

**命令模式：**BGP 地址族配置模式

**使用指南：**通过该配置可以使相关的路由属性在传送给指定邻居时不被改变。BGP路由配置模式为对IPV4单播地址模式的配置。无参数表示上述三个参数共同设置。

**举例：**设置邻居 10.1.1.64 的路由 as-path、med、next-hop 属性进行原样传递。

Switch(config-bgp-ipv4)#neighbor 10.1.1.64 attribute-unchanged

## 5.5.45 neighbor capability

**命令：neighbor {*<ip-address>*|*<TAG>*} capability {dynamic | route-refresh}**

**no neighbor {*<ip-address>*|*<TAG>*} capability {dynamic | route-refresh}**

**功能：**配置与邻居间的动态更新及路由刷新能力协商，其 no 形式表示不启动指定能力的协商。

**参数：<ip-address>**：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

**缺省情况：**不配置动态更新能力而配置路由刷新能力。

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式。

**使用指南：**这是 BGP 的扩展能力。通过该配置在 OPEN 报文中协商双方支持的能力，若对端支持该能力，则作出回应，否则会发出 NOTIFICATION，发起端会发送不包含该能力的 OPEN 以重新建立连接。动态能力是指在支持的地址族协商发生改变时，不必重新启动连接。路由刷新是指在配置一些可以进行软重置的属性时发出路由刷新请求并由对方把已有路由重新向发起端重新发送。在配置了路由刷新属性后，可以在改变策略时使用 clear ip bgp * soft in 指令进行刷新而不必重建连接。

**举例：**

Switch(config-router)#neighbor 10.1.1.64 capability dynamic

Switch(config-router)# no neighbor 10.1.1.64 capability route-refresh

## 5.5.46 neighbor capability orf prefix-list

**命令：neighbor {*<ip-address>*|*<TAG>*} capability orf prefix-list {*<both>*|*<send>*|*<receive>*}**

**no neighbor {*<ip-address>*|*<TAG>*} capability orf prefix-list {*<both>*|*<send>*|*<receive>*}**

**功能：**配置与邻居间的出路由过滤功能协商。其 no 形式配置不进行出路由过滤能力的协商。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

**缺省情况：** 不配置 ORF 能力。

**命令模式：**BGP 地址族操作模式。

**使用指南：** 这是 BGP 的扩展能力。通过该配置在 OPEN 报文中协商双方支持的能力，若对端支持该能力，则作出回应，否则会发出 NOTIFICATION，发起端会发送不包含该能力的 OPEN 以重新建立连接。该能力配置后，配置了入 prefix-list 过滤规则的一方会在建立连接时把自己的过滤规则发给对等体，其对等体会把其规则变成自己的出规则进行应用，从而避免发送会被对端过滤的路由。

**举例：**设置和邻居 10.1.1.66 进行出路由过滤能力协商。

Switch(config-bgp-ipv4)#neighbor 10.1.1.66 capability orf prefix-list both

**相关命令：neighbor capability, no neighbor capability**

## 5.5.47 neighbor collide-established

**命令：neighbor {*<ip-address>*|*<TAG>*} collide-established**

**no neighbor {*<ip-address>*|*<TAG>*} collide-established**

**功能：**使能在发生 TCP 连接冲突时的冲突检测和解决。其 no 形式不使能 TCP 连接冲突解决。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

**缺省情况：**无效不使能

**命令模式：**BGP 路由配置模式和 VRF 地址簇配置模式。

**使用指南：**这是为解决发生 TCP 连接冲突造成对等体间多连接的问题增加的功能。在这个选项下建立连接时，即使在本端发起的连接已经进入 established 状态时也检查是否有冲突的连接，并在有冲突时检查本端 IP 是否大于对端 IP，如是，则删除原连接。如不配置该选项，只在本端发起的连接为 opensent 和 openconfirm 时才检查。

**举例：**设置和邻居 10.1.1.64 进行 TCP 冲突连接检测和解决。

Switch(config-router)#neighbor 10.1.1.64 collide-established

## 5.5.48 neighbor default-originate

**命令：neighbor {*<ip-address>*|*<TAG>*} default-originate [route-map *<WORD>*]**

**no neighbor {*<ip-address>*|*<TAG>*} default-originate [route-map *<WORD>*]**

**功能：**配置是否使能向指定邻居传送缺省默认路由。其 no 形式配置不向邻居传送缺省默认路由。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

***<WORD>*** ：路由映射名。

**缺省情况：**不发送缺省默认路由。

**命令模式：**BGP 地址族配置模式。

**使用指南：**配置该选项后，本端的缺省默认路由将发送给对端。否则，不发送缺省默认路由给对端。配置该选项后这是为了给由谁来提供默认路由提供选项，若对端有多个邻居提供缺省默认路由，则会根据选路原则选择最合适的路由。根据路由映射，可以选择在何种情况下发送缺省默认路由。

**举例：**设置向邻居 10.1.1.64 发送缺省路由。

Switch(config-bgp-ipv4)#neighbor 10.1.1.64 default-originate

Switch(config-bgp-ipv4)#

此时对端的路由表里会产生来自 BGP 的缺省路由。

**相关命令：route-map。**

## 5.5.49 neighbor description

**命令：neighbor {*<ip-address>*|*<TAG>*} description *<.LINE>***

**no neighbor {*<ip-address>*|*<TAG>*} description**

**功能：**配置对等体或对等体组的描述字符串。其 no 形式删除该字符串的配置。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

***<.LINE>***：不超过 80 个字符的可显示字符组成的描述字符串。

**缺省情况：**描述字符串为空。

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式。

**使用指南：**配置为对等体或对等体组的说明。

**举例：**设置和邻居 10.1.1.64 的描述字符串为 tester。

```
Switch(config-router)#neighbor 10.1.1.64 description tester
Switch(config-router)#
```

## 5.5.50 neighbor distribute-list

**命令：neighbor {*<ip-address>*|*<TAG>*} distribute-list {*<1-199>*|*<1300-2699>*|*<WORD>*} {in|out}**

**no neighbor {*<ip-address>*|*<TAG>*} distribute-list {*<1-199>*|*<1300-2699>*|*<WORD>*} {in|out}**

**功能：**配置对对端收发路由更新所应用的策略。其 no 形式用于取消策略的配置。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

***<1-199>*|*<1300-2699>*|*<WORD>***：为访问列表的号或名字。

**缺省情况：**不使用策略。

**命令模式：**BGP 地址族配置模式。

**使用指南：**通过 access-list 命令配置策略，并使用本命令应用在路由分发和接收上，若使用了 in 方式，则对于对端来的更新路由进行过滤，使用 out 方式，则对本端发往对端的路由进行过滤。

**举例：**设置法发送到邻居 10.1.1.66 的路由中，过滤目的为 100.1.0.0 的路由。

```
Switch(config)#access-list 101 deny ip 100.1.0.0 0.0.1.255 any
Switch(config)#access-list 101 permit ip any any
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch(config-bgp-ipv4)# neighbor 10.1.1.66 distribute-list 101 in
```

**相关命令：ip access-list**

## 5.5.51 neighbor dont-capability-negotiate

**命令：neighbor {*<ip-address>*|*<TAG>*} dont-capability-negotiate**

**no neighbor {*<ip-address>*|*<TAG>*} dont-capability-negotiate**

**功能：**配置在建立连接时不进行能力协商。其 no 形式取消不进行能力协商的配置。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

**缺省情况：**进行能力协商。

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式。

**使用指南：**因为缺省在建立连接时与对端进行能力协商，因此在明知对方为不支持能力协商的老版本 BGP 时，通过此配置可以直接建立连接而不进行能力协商。

**举例：**在进行如下配置后，新增的能力协商将不会体现在连接中。

Switch(config-router)#neighbor 10.1.1.64 dont-capability-negotiate

**相关命令：neighbor capability, no neighbor capability**

## 5.5.52 neighbor ebgp-multihop

**命令：neighbor {*<ip-address>*|*<TAG>*} ebgp-multihop [*<1-255>*]**

**no neighbor {*<ip-address>*|*<TAG>*} ebgp-multihop [*<1-255>*]**

**功能：**配置 EBGP 邻居可以不在同一网段和允许的连接跳数（TTL）。其 no 形式配置 EBGP 邻居必须在同一网段。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

***<1-255>*：**允许的跳数。

**缺省情况：**要求在同一网段。

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式。

**使用指南：**不配置该命令，要求 EBGP 对等体一定要在同一网段，配置该命令后，对等体地址就可以是不在同一网段的，允许的 TTL（跳数）可以进行设定，若该参数省略，则为 255。

**举例：**

三台设备，10.1.1.64(AS100)和 11.1.1.120(AS300)分别与另一设备(未启动 BGP)的 10.1.1.66 及 10.1.1.100 两个接口相连，通过静态配置两侧的路由保证 10.1.1.64 和 11.1.1.120IGP 可达。建立 10.1.1.64 和 11.1.1.120 的邻居关系。若直接配置，两者分别保持在 ACTIVE 状态。在两边分别配置如下命令后，才可以建立邻居关系：

在 10.1.1.64 上配置：

Switch(config-router)#neighbor 11.1.1.120 ebgp-multihop

在 11.1.1.120 上配置：

Switch(config-router)#neighbor 10.1.1.64 ebgp-multihop

在配置后，不在同一网段的交换机可以建立 BGP 邻居关系。

**相关命令：**无

## 5.5.53 neighbor enforce-multihop

**命令：neighbor {*<ip-address>*|*<TAG>*} enforce-multihop**

**no neighbor {*<ip-address>*|*<TAG>*} enforce-multihop**

**功能：**强制到邻居的连接多跳。其 no 形式取消该配置。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

**缺省情况：**不强制。

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式。

**使用指南：**事实上直连路由是不能被强制为多跳的，但有个这个配置后，可以强制系统把该连接当作一个多跳连接进行处理。也就是说，本来只对 IBGP 和非直连路由的 EBGP 进行的检查，在设置该属性后，一律进行检查。而在入口处,，对强制多跳的情况就不再进行下一跳是否直连的检查。

**举例：**强制邻居 10.1.1.66 为多跳的连接。

Switch(config-router)#neighbor 10.1.1.66 enforce-multihop

**相关命令：**无

## 5.5.54 neighbor filter-list

**命令：neighbor {*<ip-address>*|*<TAG>*} filter-list *<.LINE>* {*<in>*|*<out>*}**

**no neighbor {*<ip-address>*|*<TAG>*} filter-list *<.LINE>* {*<in>*|*<out>*}**

**功能：**针对 AS-PATH 进行的访问列表控制。其 no 形式取消针对 AS-PATH 的访问列表控制。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

***<.LINE>*：**通过 ip as-path access-list *<.LINE> <permit|deny> <LINE>*命令配置的 AS-PATH 访问列表名。

**缺省情况：**不配置。

**命令模式：**BGP 地址族配置模式。

**使用指南：** 在首先配置了 IP AS-PATH 的访问列表后，应用在指定的邻居上，可以控制向该邻居发送/接收在 AS 列表里含有指定 AS 号的路由。接受和拒绝取决于访问列表的设置，而发出和接收由本命令设置。

**举例：**

配置 AS-PATH 访问控制列表，“ASPF”为访问列表的名字。则拥有 AS 号为 100 的路由由于过滤表的控制不能更新到对端。

Switch(config)#ip as-path access-list ASPF deny 100

Switch(config)#router bgp 100

Switch(config-router)# redistribute static

Switch(config-router)# address-family ipv4 unicast

Switch(config-bgp-ipv4)# neighbor 10.1.1.66 filter-list aspf out

**相关命令：ip as-path access-list**

## 5.5.55 neighbor interface

**命令：neighbor *<ip-address>* interface *<IFNAM>***

**no neighbor *<ip-address>* interface *<IFNAM>***

**功能：**指定去往邻居的接口。其 no 形式取消该配置。

**参数：*<ip-address>***：邻居的 IP 地址。

***<IFNAME>***：接口名，如“Vlan2”。

**缺省情况：**不配置。

**命令模式：**BGP 路由配置模式和 vrf 地址族配置模式。

**使用指南：**通过该命令指定去往邻居的出接口，应注意要保证从该接口可达目的地。

**举例：**设置通往邻居 10.1.1.64 的接口为 interface vlan 2。

Switch(config-router)# neighbor 10.1.1.64 interface Vlan2

**相关命令：**无。

## 5.5.56 neighbor maximum-prefix

**命令：neighbor {*<ip-address>*|*<TAG>*} maximum-prefix *<1-4294967295>* [*<1-100>* *<warning-only>*]**

**no neighbor {*<ip-address>*|*<TAG>*} maximum-prefix *<1-4294967295>* [*<1-100>* *<warning-only>*]**

**功能：**控制从邻居来的路由前缀的个数。其 no 形式取消该配置。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

***<1-4294967295>***：允许的最大前缀值。

***<1-100>***： 发出警告时达到最大值的百分比。

***<warning-only>***：是否仅发出警告。

**缺省情况：**不进行限制。

**命令模式：**BGP 地址族配置模式。

**使用指南：**由于可能担心从一个邻居有太多的路由更新（例如受到攻击），因此对从一个邻居得到的最大前缀数进行限制，而在达到一定比例的时候就发出警告。如果配置了 warning-only，就仅仅发出警告，若没有配置，将中断该邻居的连接直到用 clear ip bgp 命令清除记录后才重新进行连接。

**举例：**配置从邻居 10.1.1.64 中接收的路由前缀数最多为 12 个，达到 6 个时会开始警告，若达到 13 个将中断连接。

Switch(config-bgp-ipv4)#neighbor 10.1.1.64 maximum-prefix 12 50

**相关命令：**无。

## 5.5.57 neighbor next-hop-self

**命令：neighbor {*<ip-address>*|*<TAG>*} next-hop-self**

**no neighbor {*<ip-address>*|*<TAG>*} next-hop-self**

**功能：**配置要求邻居对于本端发出的路由下一跳指向本端。其 no 形式取消该配置。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

**缺省情况：**不配置。

**命令模式：**BGP 地址族配置模式。

**使用指南：**在 EBGP 环境中，下一跳自动指向来源邻居，但在 IBGP 环境中，如果是同一网段的路由，则原来的下一跳保持不变。但如果不是广播网络，就会出现问题，因此可以用这个命令只要是在 IBGP 下，就强制使用自己作为邻居的下一跳。

**举例：**

Switch(config-bgp-ipv4)#neighbor 10.1.1.66 next-hop-self

**相关命令：**无

## 5.5.58 neighbor override-capability

**命令：neighbor {*<ip-address>*|*<TAG>*} override-capability**

**no neighbor {*<ip-address>*|*<TAG>*} override-capability**

**功能：**是否使能不考虑能力协商结果。其 no 形式恢复进行能力协商。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

**缺省情况：**不使能。

**命令模式：**BGP 路由配置模式和 VRF 地址簇配置模式。

**使用指南：**若配置了该属性，则对邻居要求的本端不支持的能力协商，不会因此发送错误提示（notify）。

**举例：**

Switch(config-router)#neighbor 10.1.1.64 override-capability

**相关命令：neighbor capability**

## 5.5.59 neighbor passive

**命令：neighbor {*<ip-address>*|*<TAG>*} passive**

**no neighbor {*<ip-address>*|*<TAG>*} passive**

**功能：**配置本方在与指定邻居的连接中是否不主动发送连接请求。其 no 形式恢复主动发送连接请求。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

**缺省情况：**主动发起连接。

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式

**使用指南：**若配置了该属性，则配置邻居后，本方不主动发起 TCP 连接请求，而是处于监听状态，等待对端发起。

**举例：**

Switch(config-router)#neighbor 10.1.1.64 passive

在配置该属性并重新建立连接时，本端不企图建立连接而立即处于 ACTIVE 状态，等待响应对端的 TCP 连接请求。

**相关命令：**无

## 5.5.60 neighbor password

**命 令：** **neighbor <*ip-address*> password [key-id <*key-id*>] [algorithm-id <*algorithm-id*>] [algorithm-type <sm3|md5>] [<0 LINE |7 WORD | LINE>] <*password*>**

**no neighbor <*ip-address*> assword**

**功能：**配置 BGP 邻居认证，认证模式可配置为 MD5 和 SM3 国密认证，该命令的 no 形式删除认证。

**参数：**< ***ip-address*** >：为邻居的 ip 地址。

**<*key-id*>：**是所使用的密匙链的 id，取值范围为<0-63> 。

**<*algorithm-id*>：**用来配置 Keychain 支持的 TCP 认证算法所对应的算法 ID。

**<*password*>：**为字符串，长度在 1~80 字符之间。

**缺省情况：**缺省不配置。

**命令模式：**BGP 路由配置模式。

**使用指南：**配置本命令后，发送 BGP 会话报文时会启用认证加密，在接收到 BGP 邻居会话报文将检验加密字段是否认证成功。当未指定认证类型时，默认为明文的 key-id 为 1 的 MD5 认证，密码输入类型 0 时采用明文输入，为 7 时采用密文输入，缺省下为明文输入。

**举例：**

配置BGP邻居1.1.1.1采用明文MD5加密，加密密码DCN。

Switch(config-router)#neighbor 10.1.1.64 password DCN

**相关命令：**

无

## 5.5.61 neighbor peer-group （创建）

**命令：neighbor < *TAG*> peer-group**

**no neighbor < *TAG*> peer-group**

**功能：**创建/删除一个对等体组。其 no 形式删除一个对等体组。

**参数：*<TAG>*：**对等体组的名字，最大长度为 256 个字符。

**缺省情况：**没有对等体组

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式

**使用指南：**通过配置对等体组，可以使属性相同的一组对等体同时配置而减少配置人员的工作量。用 neighbor <ip-address> peer-group <TAG>命令向对等体组中添加成员。

**举例：**

Switch(config-router)#neighbor pg peer-group

Switch(config-router)#neighbor 10.1.1.64 peer-group pg

Switch(config-router)#neighbor pg remote-as 100

**相关命令：neighbor peer-group （配置组成员）**

## 5.5.62 neighbor peer-group （配置组成员）

**命令：neighbor *<ip-address>* peer-group *<TAG>***

**no neighbor *<ip-address>* peer-group *<TAG>***

**功能：**向对等体组里添加/删除对等体。其 no 形式从对等体组里删除对等体。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

**缺省情况：**没有对等体组

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式

**使用指南：**通过配置对等体组，可以使属性相同的一组对等体同时配置而减少配置人员的工作量。用上面的命令创建对等体组，用本命令向对等体组中添加成员。

**举例：**见前例。

**相关命令：neighbor peer-group （创建）**

## 5.5.63 neighbor port

**命令：neighbor *<ip-address>* port *<0-65535>***

**no neighbor *<ip-address>* port [*<0-65535>*]**

**功能：**指定对端与该邻居通信的 TCP 端口号。其 no 形式恢复端口号为默认值。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

***<0-65535>*：**TCP 端口号。

**缺省情况：**端口号为 179。

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式

**使用指南：**这是在对端可能通过并非 BGP 指定端口进行连接时进行的配置。

**举例：**

Switch(config-router)#neighbor 10.1.1.64 port 1023

**相关命令：无**

## 5.5.64 neighbor prefix-list

**命令：neighbor {*<ip-address>*|*<TAG>*} prefix-list *<LISTNAME|number>* {*<in|out>*}**

**no neighbor {*<ip-address>*|*<TAG>*} prefix-list *<LISTNAME|number>* {*<in>*|*<out>*}**

**功能：**配置发送或接收指定邻居的路由时应用的前缀限制规则。其 no 形式取消该配置。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

***<LISTNAME|number>***：prefix-list 的名字或序号。

***<in|out>***：规则应用的方向。

**缺省情况：**不应用任何前缀规则。

**命令模式：**BGP 地址族配置模式

**使用指南：**通过配置 ip prefix-list 指定前缀和其覆盖范围，并确定允许或拒绝该范围。只有被允许通过的前缀覆盖的路由才能被发送或接收。

**举例：**

Switch(config)#ip prefix-list prw permit 100.1.0.0/22 ge 23 le 25

Switch(config)#router bgp 200

Switch(config-router)#address-family ipv4 unicast

Switch(config-bgp-ipv4)neighbor 10.1.1.66 prefix-list prw out

**相关命令：无**

## 5.5.65 neighbor remote-as

**命令：neighbor {*<ip-address>*|*<TAG>*} remote-as *<as-id>***

**no neighbor {*<ip-address>*|*<TAG>*} [remote-as *<as-id>*]**

**功能：**配置 BGP 的邻居。其 no 形式用于删除 BGP 邻居。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

***<as-id>***：邻居的 AS 号，范围为 1-4294967295。可用十进制表示，如 6553700；也可用分隔符方式表示，如 100.100。

**缺省情况：**没有邻居。

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式。

**使用指南：**BGP 的邻居完全通过命令配置产生，双方要互相配置对方才能真正建立邻居关系。配置时要指定对端的 AS 号，若 AS 号不正确也不能建立邻居关系。若是在 AS 内部，对端的 AS 号与本端相同。

**举例：**配置 2 个邻居的 AS 分别为 100 和 100.200。

Switch(config)#router bgp 200

Switch(config-router)# neighbor 10.1.1.64 remote-as 100

Switch(config-router)# neighbor 10.2.1.64 remote-as 100.200

**相关命令：**无

## 5.5.66 neighbor remove-private-AS

**命令：neighbor {*<ip-address>*|*<TAG>*} remove-private-AS**

**no neighbor {*<ip-address>*|*<TAG>*} remove-private-AS**

**功能：**配置送往邻居时是否除去私有 AS 号。其 no 形式取消该配置。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

**缺省情况：**不设置。

**命令模式：**BGP 地址族配置模式。

**使用指南：**配置该属性避免在有内部 AS 时把内部 AS 号向外部 AS 发送。内部 AS 号为 64512-65535，该范围内的 AS 号是不能向 Internet 发送的，不是外部可用的合法 AS 号。这里仅会去除路径上全为私有 AS 的路由的私有 AS 号，对于既有私有 AS 号又有公有 AS 号的，不进行处理。

**举例：**

```
Switch(config-bgp-ipv4)#neighbor 10.1.1.64 remove-private-AS
```

**相关命令：**无

## 5.5.67 neighbor route-map

**命令：neighbor {*<ip-address>*|*<TAG>*} route-map *<NAME>* {*<in*|*out>*}**

**no neighbor {*<ip-address>*|*<TAG>*} route-map *<NAME>* {*<in*|*out>*}**

**功能：**配置发送路由或从邻居接收路由时应用的路由映射策略。其 no 形式取消该配置。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

***<NAME>*：**路由映射的名字。

***<in*|*out>*：**路由映射应用的方向。

**缺省情况：**不设置。

**命令模式：**BGP 地址族配置模式。

**使用指南：**首先要在全局配置模式下配置路由映射，配置的方式是先使用 route-map 命令创建一个路由映射，并设置匹配条件和所做处理，然后才能使用本命令应用它。

**举例：**

```
Switch(config)#route-map test permit 5
Switch(config-route-map)#match interface Vlan1
Switch(config-route-map)#set as-path prepend 65532
Switch(config-route-map)#exit
Switch(config)#router bgp 200
Switch(config-router)#address-family ipv4 unicast
Switch(config-bgp-ipv4)#neighbor 10.1.1.64 route-map test out
```

**相关命令：**无

## 5.5.68 neighbor route-reflector-client

**命令：neighbor {*<ip-address>*|*<TAG>*} route-reflector-client**

**no neighbor {*<ip-address>*|*<TAG>*} route-reflector-client**

**功能：**配置路由反射器客户机。其 no 形式取消该配置。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

**缺省情况：**不设置。

**命令模式：**BGP 地址族配置模式。

**使用指南：**路由反射用于 AS 内部 IBGP 路由器较多时减少对等体个数，其客户机只与路由反射器交换信息，而路由反射器处理各客户机间和与其他 IBGP 和 EBGP 路由器的信息交换。这个命令把自己配置为路由反射器而指定的对等体（组）作为它的客户机。注意：这种配置只能在 AS 内部进行。

**举例：**

```
Switch(config)#router bgp 100
Switch(config-router)#neighbor 10.1.1.66 remote-as 100
Switch(config-router)#neighbor 10.1.1.68 remote-as 100
Switch(config-router)#address-family ipv4 unicast
Switch(config-bgp-ipv4)#neighbor 10.1.1.66 route-reflector-client
Switch(config-bgp-ipv4)#neighbor 10.1.1.68 route-reflector-client
```

**相关命令：bgp client-to-client reflection, no bgp client-to-client reflection, bgp cluster-id**

## 5.5.69 neighbor route-server-client

**命令：neighbor {*<ip-address>*|*<TAG>*} route-server-client**

**no neighbor {*<ip-address>*|*<TAG>*} route-server-client**

**功能：**配置路由服务器客户机。其 no 形式取消该配置。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

**缺省情况：**不设置

**命令模式：**BGP 地址族配置模式。

**使用指南：**路由服务用于 EBGP 环境下 AS 之间路由器较多时减少对等体个数，其客户机通过路由服务器交换信息时，服务器透明的把路由消息传送给其它客户机。

**举例：**

三台路由器，10.1.1.64（AS100）和 10.1.1.68（AS300）分别与 10.1.1.66（AS200）相连并与其建立邻居关系，配置如下：

```
Switch(config)#router bgp 200
Switch(config-router)#neighbor 10.1.1.64 remote-as 100
Switch(config-router)# neighbor 10.1.1.68 remote-as 300
Switch(config-router)# address-family ipv4 unicast
Switch(config-bgp-ipv4)#neighbor 10.1.1.64 route-server-client
```

Switch(config-bgp-ipv4)# neighbor 10.1.1.68 route-server-client

**相关命令：**无

## 5.5.70 neighbor send-community

**命令：neighbor {*<ip-address>*|*<TAG>*} send-community [both|extended|standard]**

**no neighbor {*<ip-address>*|*<TAG>*} send-community [both|extended|standard]**

**功能：**配置是否向该邻居发送团体属性。其 no 形式配置不向邻居发送团体属性。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

**[both|extended|standard]：**表示是只针对标准团体、扩展团体还是都包括。

**缺省情况：**发送团体属性。

**命令模式：**BGP 地址族配置模式。

**使用指南：**团体属性可以向外发送，也可以不向外发送。神州数码的缺省是发送，而标准协议的缺省是不发送。配置该属性可以在向邻居发送路由信息时携带团体属性，否则不携带。省略后面的选择相当于 standard。

**举例：**

Switch(config-bgp-ipv4)#no neighbor 10.1.1.66 send-community

Switch(config-bgp-ipv4)#neighbor 10.1.1.66 send-community

**相关命令：**无

## 5.5.71 neighbor shutdown

**命令：neighbor {*<ip-address>*|*<TAG>*} shutdown**

**no neighbor {*<ip-address>*|*<TAG>*} shutdown**

**功能：**关闭邻居的连接。其 no 形式取消该配置。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

**缺省情况：**不关闭连接

**命令模式：**BGP 路由配置模式。

**使用指南：**可以不必取消邻居的配置而直接关闭/打开一个对等体（组）的连接。

**举例：**

Switch(config-router)#neighbor 10.1.1.64 shutdown

**相关命令：**无

## 5.5.72 neighbor soft-reconfiguration inbound

**命令：neighbor {*<ip-address>*|*<TAG>*} soft-reconfiguration inbound**

**no neighbor {*<ip-address>*|*<TAG>*} soft-reconfiguration inbound**

**功能：**配置是否进行入站软重配置。其 no 形式配置不进行入栈软重配置。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

**缺省情况：**不进行入站软重配置。

**命令模式：**BGP 地址族配置模式。

**使用指南：**配置了软重配置时，系统会先在缓存中保存入站的信息，在重新启动后立即应用在本端，从而减少与其它路由器进行交换的消耗。该指令在不启动路由刷新能力时才有意义。

**举例：**

Switch(config-bgp-ipv4)#neighbor 11.1.1.120 soft-reconfiguration inbound

**相关命令：**无

## 5.5.73 neighbor soo

**命令：neighbor *<ip-address>* soo *<soo-val>***

**no neighbor *<ip-address>* soo *<soo-val>***

**功能：** 配置来自邻居路由的初始源；no 删除配置。

**参数：** ***<ip-addr>***为邻居 IP 地址，点分十进制形式。***<soo-val>***为初始源，格式为***<AA:NN>***，其中 AA 为 AS 号，取值范围为 1-4294967295，可用十进制表示，如 6553700；也可用分隔符方式表示，如 100.100，NN 为任意两字节数字。

**缺省情况：** 无。

**命令模式：** VRF 地址族配置模式

**使用指南：** 如果用户 AS 与多个 ISP 的设备相连，为避免用户路由经过 P 区域又回到用户 AS，可以设置该属性。配置了该属性后，该属性会随路由扩散。携带 SOO 属性的路由，遇到了配置该属性的邻居，路由不向该邻居扩散。

**举例：**

Switch (config)#router bgp 100

Switch(config-router)#address-family ipv4 vrf test

Switch(config-bgp-vrf)# neighbor 11.1.1.64 remote 200

Switch(config-bgp-vrf)# neighbor 11.1.1.64 soo 100.100:10

配置该属性后，交换机不再把远端传来的含有 100.100:10 rt 属性的路由向 11.1.1.64 扩散。（这里应当提到的是，soo 属性是与其它 rt 属性一同判断的，也就是说即使并非真的始发源，只要 rt 配置了同样的属性值，仍被认为是遇到了始发的邻居。事实上，通常的配置中 soo 是单独配置，是与 rt/rd 等不同的值，而且在可到达的范围内唯一配置，这样就可以准确的表达始发的概念）。

## 5.5.74 neighbor strict-capability-match

**命令：neighbor {*<ip-address>*|*<TAG>*} strict-capability-match**

**no neighbor {*<ip-address>*|*<TAG>*} strict-capability-match**

**功能：**配置建立连接时是否要求严格的能力匹配。其 no 形式配置不要求严格的能力匹配。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

**缺省情况：**不配置严格能力匹配

**命令模式：**BGP 路由配置模式。

**使用指南：**该命令只对 BGP 多协议有效，使用了该命令后，当双方的 bgp 多协议能力匹配时才能建立邻居，否则无法建立；其他能力是否匹配不影响邻居建立。

**举例：**

Switch(config-router)#neighbor 10.1.1.64 strict-capability-match

**相关命令：**无

## 5.5.75 neighbor timers

**命令：neighbor {*<ip-address>*|*<TAG>*} timers *<0-65535> <0-65535>***

**no neighbor {*<ip-address>*|*<TAG>*} timers *<0-65535> <0-65535>***

**功能：**配置 KEEPALIVE 时间间隔和保持时间，no 形式恢复为默认值。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

***<0-65535>***：两个分别是 KEEPALIVE 和 HOLD TIME 的时间。

**缺省情况：**KEEPALIVE 时间为 60s， HOLD TIME 为 240s。

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式。

**使用指南：**使用该命令配置与对等体连接中发送 KEEPALIVE 的时间间隔和保持时间的间隔。所谓保持时间，是指没有收到对端的任何消息（如 KEEPALIVE）仍认为连接持续的时间间隔，超过该时间间隔，连接会中断。

**举例：**

Switch(config-router)#neighbor 10.1.1.64 timers 50 200

**相关命令：neighbor timers connect,timers bgp, no timers bgp**

## 5.5.76 neighbor timers connect

**命令：neighbor {*<ip-address>*|*<TAG>*} timers connect *<0-65535>***

**no neighbor {*<ip-address>*|*<TAG>*} timers connect [*<0-65535>*]**

**功能：**配置连接重试时间间隔。其 no 形式恢复为默认值。

**参数：*<ip-address>***：邻居的 IP 地址。

***<TAG>***：是对等体组的名字。

***<0-65535>***：连接重试时间。

**缺省情况：**120s。

**命令模式：**BGP 路由配置模式和 VRF 地址族配置模式

**使用指南：**使用该命令配置与对等体连接中进行连接重试的间隔，no 形式恢复为默认值。

**举例：**

Switch(config-router)#neighbor 10.1.1.64 timers connect 100

**相关命令：neighbor timers**

## 5.5.77 neighbor unsuppress-map

**命令：neighbor {*<ip-address>*|*<TAG>*} unsuppress-map *<WORD>***

**no neighbor {*<ip-address>*|*<TAG>*} unsuppress-map *<WORD>***

**功能：**配置或取消对符合指定路由映射的情况不抑制。其 no 形式取消该配置。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

***<WORD>*：**route-map 名

**缺省情况：**不做该配置。

**命令模式：**BGP 地址簇配置模式。

**使用指南：**这主要是针对被聚合且 summary-only 的情况抑制的具体路由的，符合路由映射条件的路由在这种情况下不被抑制，仍单独发出。

**举例：**

Switch(config-bgp-ipv4)#neighbor 10.1.1.66 unsuppress-map rmp

Switch(config)#access-list 10 permit 10.1.1.100 0.0.0.255

Switch(config)#route-map rmp permit 5

Switch(config-route-map)#match ip next-hop 10

不抑制下一跳为 10.1.1.100 的路由。

**相关命令：route-map**

## 5.5.78 neighbor update-source

**命令：neighbor {*<ip-address>*|*<TAG>*} update-source *<IFNAME>***

**no neighbor {*<ip-address>*|*<TAG>*} update-source *<IFNAME>***

**功能：**配置更新源。其 no 形式取消该配置。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

***<IFNAME>*：**接口名或接口 IP。

**缺省情况：**不做该配置，即使用最近的接口。

**命令模式：**BGP 路由配置模式和 VRF 地址簇配置模式。

**使用指南：**指定的更新源允许使用任何可使用的接口进行连接，通常都会使用环回接口。no 形式恢复为最近的接口更新源。使用不当的更新源可能导致邻居连接不能建立，而且失效的接口也会引起问题，这也是一般使用环回接口的原因。注意：使用环回接口作为更新源时要保持环回接口地址的可达性才能建立连接。

**举例：**

Switch(config-router)#neighbor 10.1.1.66 update-source 192.168.0.1

**相关命令：** 无

## 5.5.79 neighbor version 4

**命令：neighbor {*<ip-address>*|*<TAG>*} version 4**

**功能：**配置对端的 BGP 版本号

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

**4：**允许的 BGP 版本号，只能为 4。

**缺省情况：**4。

**命令模式：**BGP 路由配置模式和 VRF 地址簇配置模式。

**使用指南：**目前只支持版本 4，所以无论如何配置，版本号都为 4。

**举例：**

```
Switch(config-router)#neighbor 10.1.1.66 version 4
Switch(config-router)#
```

**相关命令：**无

## 5.5.80 neighbor weight

**命令：neighbor {*<ip-address>*|*<TAG>*} weight *<0-65535>***

**no neighbor {*<ip-address>*|*<TAG>*} weight [*<0-65535>*]**

**功能：**配置对端发出的路由的权重。其 no 形式恢复为默认值。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**是对等体组的名字。

***<0-65535>*：**权重。

**缺省情况：**从其它路由器得到的路由缺省的权重为 0。本地静态配置的权重缺省为 32768。

**命令模式：**BGP 路由配置模式和 VRF 地址簇配置模式。

**使用指南：**可以通过权重的配置影响选路。权重仅与本路由器相关，不是可以向外发出的属性。

**举例：**

```
Switch(config-router)#neighbor 10.1.1.66   weight 500
```

**相关命令：**无。

## 5.5.81 network (BGP)

**命令：network *<ip-address/M>* [route-map *<WORD>*] [backdoor]**

**no network *<ip-address/M>* [route-map *<WORD>*] [backdoor]**

**功能：**设置 BGP 管理的网络。设置网络应用指定的路由映射，或设置网络采用“后门”。其 no 形式取消该配置。

**参数：*<ip-address/M>*：**网络前缀标识。

***<WORD>***：路由映射名。

**缺省情况：**无。

**命令模式：**BGP 地址簇配置模式。

**使用指南：**对于 BGP 路由，指定通过 BGP 广告的路由。通过该指令定义的网络，即使在本地没有路由（不可达），也会被扩散到邻居的路由表中。 通过路由映射指定网络应用的属性，通过 backdoor 参数指定网络在既有来自 EBGP 也有来自内部的路由时，即使外部的路由距离比较小，也选择内部提供路由作为优选路由。

**举例：**

Switch(config-bgp-ipv4 )# network 172.16.0.0/16

**相关命令：**无

## 5.5.82 redistribute (BGP)

**命令：redistribute *<ROUTES>* [route-map *<WORD>*]**

**no redistribute *<ROUTES>* [route-map *<WORD>*]**

**功能：**设置 BGP 把来源于其它方式的路由重定向分配到 BGP 中。其 no 形式取消该配置。

**参数：*<ROUTES>***：路由来源或协议，包括：connected, isis, kernel, ospf, rip, static 等。

***<WORD>***：路由映射名。

**缺省情况：**无。

**命令模式：**BGP 地址簇配置模式。

**使用指南：**对于来源于其他途径的路由，通过该命令可以导入 BGP 的路由表中并向邻居发送。

**举例：**经过此配置，本机的静态路由被导入 BGP，并广告到邻居。

Switch(config-bgp-ipv4)# redistribute static

**相关命令：**无

## 5.5.83 redistribute ospf

**命令：redistribute ospf [*<process-id>*] [route-map*<word>*]**

**no redistribute ospf [*<process-id>*]**

**功能：** 引入从 OSPF 不同进程学到的路由到 BGP 进程中。本命令的 no 操作取消引入从 OSPF 指定进程学到的路由到 BGP 进程中。

**参数：process-id** 是 OSPF 进程 id 号，无该参数表示默认进程，取值范围 1-65535。

**route-map *<word>***指向用于引入路由的路由地图的指针。

**缺省情况：** 默认不引入。

**命令模式：** BGP 地址簇配置模式。

**使用指南：** 无。

**举例：** BGP（as number 为 1）引入 OSPF 进程 2 的路由。

Switch(config)#router bgp 1

Switch(config-router)#address-family ipv4 unicast

Switch(config-bgp-ipv4)#redistribute ospf 2

## 5.5.84 router bgp

**命令：router bgp *<as-id>***

**no router bgp *<as-id>***

**功能：**启动 BGP 实体，该命令的 no 形式为删除 BGP 实体。

**参数：*<as-id>***：为 AS 号，范围为 1-4294967295。可用十进制表示，如 6553700；也可用分隔符方式表示，如 100.100。

**缺省情况：**BGP 不启动。

**命令模式：**全局配置模式。

**使用指南：**基于指定的 AS 启动 BGP，执行后，进入 config-router 配置状态，可以在该提示符下对该协议进行配置。

**举例：**启动 BGP，AS 号为 4294967295，用十进制表示。

Switch(config)#router bgp 4294967295

Switch(config-router)#exit

启动 BGP，AS 号为 4294967295，用分隔符方式表示。

Switch(config)#router bgp 65535.65535

Switch(config-router)#exit

## 5.5.85 set vpnv4 next-hop

**命令：set vpnv4 next-hop <*ip-addr*>**

**no set vpnv4 next-hop <*ip-addr*>**

**功能：** 配置 VPNv4 路由的下一跳。

**参数：*<ip-addr>*** 为 vpnv4 路由的下一跳。

**缺省情况：** 无。

**命令模式：** vpnv4 地址簇配置模式。

**使用指南：** 使用该命令，配置 VPNv4 路由的下一跳，因为普通的设置下一跳只能针对 IPv4 路由，而此命令专门针对 VPNv4 地址族进行设置。

**举例：**

配置地址族如下：

Switch(config)#route-map map1 permit 15

Switch(config-map)#match interface Vlan1

Switch(config-map)#set weight 655

```
Switch(config-map)#set vpnv4 next-hop 10.1.1.250
Switch(config-map)#exit
Switch(config)#router bgp 100
Switch(config-router)#neighbor 10.1.1.68 remote-as 100
Switch(config-router)#neighbor 10.1.1.68 route-map map1 in
Switch(config-router)#address-family vpnv4 unicast
Switch(config-bgp-vpnv4)#neighbor 10.1.1.68 activate
Switch(config-bgp-vpnv4)#exit-address-family
```

刷新后，查看路由信息：

```
Switch#show ip bgp vpnv4 all
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:10 (Default for VRF test)
*> 11.1.1.0/24      11.1.1.64                0             0 200 ?
*>i15.1.1.0/24      10.1.1.250               0    100      655 200 ?
*> 20.1.1.0/24      11.1.1.64                0             0 200 ?
*>i100.1.1.0/24     10.1.1.250               0    100      655 200 ?
Route Distinguisher: 100:10
*>i15.1.1.0/24      10.1.1.68                0    100      0 200 ?
*>i100.1.1.0/24     10.1.1.68                0    100      0 200 ?
```

可以看到下一跳为 10.1.1.68 的 VPN 路由在应用了路由图后下一跳变为 10.1.1.250。

## 5.5.86 show ip bgp(ipv4)

**命令：** **show ip bgp [*<ADDRESS-FAMILY>*] [*<ip-address>*|*<ip-address/M>* [longer-prefixes]| cidr-only]**

**功能：**用于显示 BGP 维护的路由信息。

**参数：*<ADDRESS-FAMILY>*：**地址族，如“ipv4 unicast”；

***<ip-address>*：**IP 地址；

***<ip-address/M>*：**IP 地址及掩码。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**可以针对不同参数（如地址族或 IPv4 地址）显示 BGP 路由信息，也可以显示一个前缀所覆盖的路由或只显示不符合最早的 IP 地址类的路由信息（即路由不是 A 类、B 类和 C 类地址）。

**举例：**

```
Switch#show ip bgp
BGP table version is 147, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
```

Origin codes: i - IGP, e - EGP, ? - incomplete

| Network | Next Hop | Metric | LocPrf | Weight | Path |
|---|---|---|---|---|---|
| *> 12.0.0.0 | 10.1.1.121 | 0 | | 32768 | ? |
| *> 100.1.1.0/24 | 10.1.1.200 | 0 | | 32768 | ? |
| *> 100.1.2.0/24 | 10.1.1.200 | 0 | | 32768 | ? |
| *> 172.0.0.0/8 | 0.0.0.0 | | | 32768 | i |

Total number of prefixes 4

## 5.5.87 show ip bgp attribute-info

**命令：show ip bgp attribute-info**

**功能：**显示 BGP 属性信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示 BGP 维护的属性信息（如下一跳）。

**举例：**

Switch#show ip bgp attribute-info

attr[1] nexthop 0.0.0.0

attr[1] nexthop 10.1.1.64

attr[3] nexthop 10.1.1.64

attr[1] nexthop 10.1.1.121

attr[2] nexthop 10.1.1.200

## 5.5.88 show ip bgp community

**命令：show ip bgp [*<ADDRESS-FAMILY>*] community *<TYPE>* [exact-match]**

**功能：**用于显示 BGP 维护的含有团体信息的路由。

**参数：*<ADDRESS-FAMILY>*：**地址族，如“ipv4 unicast”；

***<TYPE>*：**由 AA:NN 形式表示的团体属性号或 local-AS、no-advertise、no-export 组成的集合。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**可以同时选择多个团体，exact-match 表示只显示完全匹配的表项。

**举例：**

Switch#show ip bgp community

BGP table version is 10, local router ID is 10.1.1.64

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

| | Network | Next Hop | Metric | LocPrf | Weight | Path |
|---|---|---|---|---|---|---|
| * | 100.1.1.0/24 | 0.0.0.0 | | | 32768 | 700 800 i |
| *> | 172.0.0.0/8 | 0.0.0.0 | | | 32768 | 700 800 i |

Total number of prefixes 2

## 5.5.89 show ip bgp community-info

**命令：show ip bgp community-info**

**功能：**用于显示 BGP 维护的团体信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**可以同时选择显示多个在同一团体内的信息。

**举例：**

Switch#show ip bgp community-info
Address Refcnt Community
[0x3312558] (3) 100:50

**相关命令：**无。

## 5.5.90 show ip bgp community-list

**命令：show ip bgp [*<ADDRESS-FAMILY>*] community-list *<NAME>* [exact-match]**

**功能：**用于显示 BGP 维护的含有指定团体列表信息的路由。

**参数：*<ADDRESS-FAMILY>*：**地址族，如“ipv4 unicast”；

***<NAME>*：**团体列表名。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用 ip community-list 命令配置团体列表并把包含的团体配置进去。使用其名字显示时，相当于包含了所有列表中的团体。

**举例：**

Switch(config)#ip community-list commu per 100:50
Switch#show ip bgp community-list commu
BGP table version is 25, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

| | Network | Next Hop | Metric | LocPrf | Weight | Path |
|---|---|---|---|---|---|---|
| * | 100.1.1.0/24 | 0.0.0.0 | | | 32768 | 700 800 i |
| *> | 172.0.0.0/8 | 0.0.0.0 | | | 32768 | 700 800 i |

**相关命令：ip community-list**

## 5.5.91 show ip bgp dampening

**命令：show ip bgp [<ADDRESS-FAMILY>] dampening {<dampened-paths> | <flap-statistics> | <parameters>}**

**功能：**用于显示 BGP 维护的与路由衰减有关的路由。

**参数：*<ADDRESS-FAMILY>*：**地址族，如“ipv4 unicast”。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：** 只有经过了振荡的路由才会被显示。Parameters 表示显示配置，不显示具体路由。其它两个选项则分别显示被抑制的路由和正进行衰减（近期曾经失效）的路由信息。

**举例：**

Switch#show ip bgp dampening dampened-paths

BGP table version is 12, local router ID is 10.1.1.66

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

| | Network | From | Reuse | Path |
|---|---|---|---|---|
| *d | 100.1.3.0/24 | 10.1.1.64 | 00:27:40 | 100 ? |

Total number of prefixes 1

Switch#show ip bgp dampening flap-statistics

BGP table version is 13, local router ID is 10.1.1.66

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

| | Network | From | Flaps | Duration | Reuse | Path |
|---|---|---|---|---|---|---|
| *d | 100.1.3.0/24 | 10.1.1.64 | 3 | 00:06:05 | 00:27:00 | 100 ? |

Switch#show ip bgp dampening parameters

dampening 15 750 2000 60 15 (route-map rmp)
Reachability Half-Life time : 15 min
Reuse penalty : 750
Suppress penalty : 2000
Max suppress time : 60 min
Un-reachability Half-Life time : 15 min
Max penalty (ceil) : 11999
Min penalty (floor) : 375
Total number of prefixes 1

**相关命令：bgp dampening**

## 5.5.92 show ip bgp filter-list

**命令：show ip bgp [*<ADDRESS-FAMILY>*]filter-list [*<WORD >*]**

**功能：**用于显示 BGP 符合指定 AS 过滤列表的路由。

**参数：*<ADDRESS-FAMILY>*：**地址族，如“ipv4 unicast”；

***< WORD >*：**AS-PATH 访问列表名。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用 ip as-path access-list 命令配置 AS 访问列表。该命令可以显示通过了访问列表的路由。

**举例：**

```
Switch#show ip bgp filter-list FL
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 100.1.1.0/24     10.1.1.64                0             0 100 ?

Total number of prefixes 1
```

**相关命令： neighbor filter-list，ip as-path access-list**

## 5.5.93 show ip bgp inconsistent-as

**命令：show ip bgp [*<ADDRESS-FAMILY>*] inconsistent-as**

**功能：**用于显示 BGP AS 不正常的路由。

**参数：*<ADDRESS-FAMILY>***：地址族，如“ipv4 unicast”。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**同一前缀来自不同的始发 AS，被认为是 AS 不正常的路由，该命令可以把这种路由显示出来。

**举例：**

```
Switch#show ip bgp inconsistent-as
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric LocPrf Weight Path
*    100.1.1.0/24     10.1.1.68                0              0 300 ?
*>                    10.1.1.64                0              0 100 ?

Total number of prefixes 1
```

**相关命令：**无。

## 5.5.94 show ip bgp neighbors

**命令：show ip bgp [*<ADDRESS-FAMILY>*] neighbors [IP-ADDRESS] [advertised-routes | received {prefix-filter | routes} | routes]**

**功能：**用于显示 BGP 邻居的相关信息。

**参数：*<ADDRESS-FAMILY>***：地址族，如“ipv4 unicast”；

***<ip-address>***：邻居的 IP 地址。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用不带参数的命令显示所有邻居的详细信息，指定 IP 地址时则显示指定 IP 地址的邻居的详细信息，带 advertised-routes、received prefix-filter、received routes、routes 参数，分别显示本端广播的路由，收到的前缀过滤，收到的路由（在启动软重配置功能时）和指定邻居传来的路由信息。

**举例：**

```
Switch#show ip bgp neighbor
BGP neighbor is 10.1.1.66, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 11.1.1.100
  BGP state = Established, up for 00:13:43
  Last read 00:13:43, hold time is 240, keepalive interval is 60 seconds
  Neighbor capabilities:
```

Route refresh: advertised and received (old and new)

Address family IPv4 Unicast: advertised and received

Received 17 messages, 0 notifications, 0 in queue

Sent 17 messages, 0 notifications, 0 in queue

Route refresh request: received 0, sent 0

Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast

BGP table version 2, neighbor version 2

Index 1, Offset 0, Mask 0x2

Community attribute sent to this neighbor (both)

0 accepted prefixes

1 announced prefixes

Connections established 7; dropped 6

**相关命令：**无

## 5.5.95 show ip bgp paths

**命令：show ip bgp [*<ADDRESS-FAMILY>*] paths**

**功能：**用于显示 BGP 维护的路径信息。

**参数：*<ADDRESS-FAMILY>*：**地址族，如“ipv4 unicast”。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**显示 BGP 路径信息，包括其路径被利用的情况。

**举例：**

Switch#show ip bgp paths

Address Refcnt Path

[0x331dad0:0] (1)

[0x331d850:93] (1) 600

[0x331d8d8:249] (2) 200 300

**相关命令：**无。

## 5.5.96 show ip bgp prefix-list

**命令：show ip bgp [*<ADDRESS-FAMILY>*] prefix-list [*<NAME>*]**

**功能：**用于显示 BGP 符合指定前缀列表的路由。

**参数：*<ADDRESS-FAMILY>*：**地址族，如“ipv4 unicast”；

***<NAME>*：**前缀列表名。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**可以通过正则表达式选择想要显示的 BGP 路由。

**举例：**

```
Switch(config)#ip prefix-list PL permit any
Switch(config)#
Switch#show ip bgp prefix-list PL
BGP table version is 1, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf Weight Path
*   100.1.1.0/24     10.1.1.66                                0 200 300 ?
*>                   10.1.1.100               0             32768 ?

Total number of prefixes 1
```

**相关命令：**无。

## 5.5.97 show ip bgp quote-regexp

**命令：show ip bgp [*<ADDRESS-FAMILY>*] quote-regexp [*<WORD>*]**

**功能：**用于显示 BGP 符合指定 AS 相关正则表达式的路由。

**参数：*<ADDRESS-FAMILY >*：**地址族，如“ipv4 unicast”；

***<WORD>*：**正则表达式。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**可以通过正则表达式选择想要显示的 BGP 路由。

**举例：**

```
Switch#show ip bgp quote-regexp ^300$
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf Weight Path
*> 100.1.1.0/24     10.1.1.68              0                 0 300 ?

Total number of prefixes 1
```

```
Switch#sh ip bgp quote-regexp 100
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.64                0             0 500 100 600 ?

Total number of prefixes 1
```

**相关命令：**无。

## 5.5.98 show ip bgp redistribute

**命令：show ip bgp redistribute [vrf <*NAME*>]**

**功能：** 显示 BGP 进程引入其它外部路由的配置信息，可以分 vrf 显示。

**参数：** vrf 名，无参数表示显示所有 vrf 的 rip 进程重分布路由信息。

**缺省情况：** 不显示信息。

**命令模式：** 特权模式和配置模式。

**使用指南：** 无。

**举例：**

```
Switch#show ip bgp redistribute
```

## 5.5.99 show ip bgp neighbors

**命令：show ip bgp neighbors [vrf <*NAME*>]**

**功能：** 显示指定或全部 BGP 进程 neighbor 的信息。

**参数：** vrf 名，无参数表示显示所有 vrf 的 BGP 邻居信息。

**缺省情况：** 不显示信息。

**命令模式：** 特权模式和配置模式。

**使用指南：** 无。

**举例：**

```
Switch#show ip bgp neighbors
```

## 5.5.100 show ip bgp regexp

**命令：show ip bgp [*<ADDRESS-FAMILY>*] regexp [*<LINE>*]**

**功能：**用于显示 BGP 符合指定 AS 相关普通表达式的路由。

**参数：*<ADDRESS-FAMILY >*：**地址族，如“ipv4 unicast”；

***<LINE>*：**正则表达式。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**可以通过普通表达式选择想要显示的 AS 的 BGP 路由。

**举例：**

```
Switch#show ip bgp regexp 100
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.64                0             0 500 100 600 ?

Total number of prefixes 1
```

**相关命令：**无.

## 5.5.101 show ip bgp route-map

**命令：show ip bgp [*<ADDRESS-FAMILY>*] route-map [*<NAME>*]**

**功能：**用于显示 BGP 符合指定路由映射的路由。

**参数：*<ADDRESS-FAMILY >*：**地址族，如“ipv4 unicast”；

***<NAME>*：**路由映射名。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用 route-map 命令配置路由映射。该命令可以显示经过路由映射处理路由。本命令可以显示符合指定路由映射的路由。

**举例：**

```
Switch#show ip bgp route-map rmp
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.64                0             0 500 100 600 ?
```

*> 10.1.1.68 0 0 300 ?

Total number of prefixes 1

**相关命令：route-map, neighbor route-map**

## 5.5.102 show ip bgp scan

**命令：show ip bgp scan**

**功能：**用于显示 BGP 扫描信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**BGP 定期对下一跳信息进行扫描，该命令可显示目前的间隔和相关路由。

**举例：**

Switch#show ip bgp scan

BGP Instance: (Default) AS 200, router-id 11.1.1.100

BGP scan interval is 60

Current BGP nexthop cache:

**相关命令：bgp scan-time**

## 5.5.103 show ip bgp summary

**命令：show ip bgp [*<ADDRESS-FAMILY>*] summary**

**功能：**用于显示 BGP 的摘要信息。

**参数：*<ADDRESS-FAMILY>*：**地址族，如“ipv4 unicast”。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**显示 BGP 的一些基本摘要信息。

**举例：**

Switch#show ip bgp summary

BGP router identifier 10.1.1.66, local AS number 200

BGP table version is 1

1 BGP AS-PATH entries

0 BGP community entries

| Neighbor | V | AS | MsgRcvd | MsgSent | TblVer | InQ | OutQ | Up/Down | State/PfxRcd |
|---|---|---|---|---|---|---|---|---|---|
| 10.1.1.68 | 4 | 300 | 0 | 0 | 0 | 0 | 0 | never | Active |

Total number of neighbors 1

| 显示内容 | 解释 |
| --- | --- |
| identifier | 本地标识符 |
| local AS number | 本地路由器 AS 号 |
| table version | BGP 内部数据库版本号 |
| AS-PATH entries | AS-PATH 表项数 |
| community entries | 团体属性数 |
| Neighbor | 邻居地址 |
| V | 邻居运行 BGP 版本 |
| AS | 邻居所属 AS 号 |
| MsgRcvd | 从邻居接收信息数 |
| MsgSent | 向邻居发送信息数 |
| TblVer | 路由表版本 |
| Up/Down | 如与邻居状态曾为 established，邻居会话时间长度，否则显示当前状态 |
| State/PfxRcd | 如与该邻居状态为 established，显示接收的路由前缀数量，否则显示当前邻居状态 |

**相关命令：**无

## 5.5.104 show ip bgp view

**命令：show ip bgp view [*<NAME>*] [*<ip-address>*|*<ip-address/M>*|[*<ADDRESS-FAMILY>*] summary]**

**功能：**用于显示指定 BGP 实体的信息。

**参数：*<NAME>***：BGP 实体名；

***<ip-address>***：IP 地址；

***<ip-address/M>***：IP 地址及掩码；

***<ADDRESS-FAMILY>***：地址族，如“ipv4 unicast”。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**显示指定 BGP 实体的信息。

**举例：**

Switch#show ip bgp view as300 100.1.1.0/24

**相关命令：router bgp**

## 5.5.105 show ip bgp view neighbors

**命令：show ip bgp view [*<NAME>*] neighbors [*<ip-address>*]**

**功能：**用于显示指定 BGP 实体的邻居信息。

**参数：*<NAME>***：BGP 实体名。

***<ip-address>***：邻居 IP 地址。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**显示指定 BGP 实体的邻居信息。

**举例：**

Switch#show ip bgp view as300 neighbors

**相关命令：**无。

## 5.5.106 show ip bgp vrf

**命令：show ip bgp vrf [NAME] {summary | A.B.C.D | A.B.C.D/M}**

**功能：**用于显示 BGP 维护的邻居和路由信息。

**参数：** <NAME>：VRF 实例号

summary：显示 BGP 邻居汇总信息

A.B.C.D：IP 地址

A.B.C.D/M：IP 地址及掩码

**缺省情况：** 无。

**命令模式：** 特权和配置模式。

**使用指南：** 可以针对不同参数（如 IPv4 地址或 IPv4 地址/掩码）显示 BGP 路由信息，也可以显示一个前缀所覆盖的路由或只显示不符合最早的 IP 地址类的路由信息（即路由不是 A 类、B 类和 C 类地址）。

**举例：**

1)显示 bgp neighbor 信息:

S2#show ip bgp vrf 1 summary

BGP router identifier 30.1.1.2, local AS number 200

BGP table version is 8

1 BGP AS-PATH entries

0 BGP community entries

| Neighbor | V | AS | MsgRcvd | MsgSent | TblVer | InQ | OutQ | Up/Down | State/PfxRcd |
|---|---|---|---|---|---|---|---|---|---|
| 30.1.1.1 | 4 | 100 | 57 | 51 | 8 | 0 | 0 | 00:41:44 | 31 |

Total number of neighbors 1

显示内容解释

显示内容 解释

identifier 本地标识符

local AS

table version

AS-PATH entries

community entries

Neighbor 邻居地址

V 邻居运行 BGP

AS 邻居所属 AS
MsgRcvd 从邻居接收信息数
MsgSent 向邻居发送信息数
TblVer 路由表版本
Up/Down 如与邻居状态曾为 established，邻居会话时间长度，
否则显示当前状态
State/PfxRcd 如与该邻居状态为 established，显示接收的路由前
缀数量，否则显示当前邻居状态

2)显示 bgp 路由信息:

```
S2#show ip bgp vrf 1
BGP routing table entry for 44.1.1.0/24
Paths: (1 available, best #1, table vrf 1 ipv4 unicast)
  Not advertised to any peer
  100
    30.1.1.1 from 30.1.1.1 (30.1.1.1)
      Origin incomplete, metric 6, localpref 100, valid, external, best
      Last update: 00:41:47
BGP routing table entry for 44.1.2.0/24
Paths: (1 available, best #1, table vrf 1 ipv4 unicast)
  Not advertised to any peer
  100
    30.1.1.1 from 30.1.1.1 (30.1.1.1)
      Origin incomplete, metric 6, localpref 100, valid, external, best
      Last update: 00:41:47
BGP routing table entry for 44.1.3.0/24
Paths: (1 available, best #1, table vrf 1 ipv4 unicast)
  Not advertised to any peer
  100
    30.1.1.1 from 30.1.1.1 (30.1.1.1)
      Origin incomplete, metric 6, localpref 100, valid, external, best
      Last update: 00:41:47
BGP routing table entry for 44.1.4.0/24
Paths: (1 available, best #1, table vrf 1 ipv4 unicast)
  Not advertised to any peer
  100
    30.1.1.1 from 30.1.1.1 (30.1.1.1)
      Origin incomplete, metric 6, localpref 100, valid, external, best
      Last update: 00:41:47
```

## 5.5.107 show ip bgp vpnv4

**命令：show ip bgp vpnv4 {all | rd <rd-val> }**

**功能：** 本命令用于显示本交换机下所有 VPNv4 对等体或者指定路由区分符的 BGP 邻居连

接的详细信息**参数：all：** 所有 VPNv4 对等体；

**rd-val：** 表示路由区分符，形式通常是（AS 号或 IP 地址）：数字，如 100:10；

**缺省情况：** 无。

**命令模式：** 任意配置模式。

**使用指南：** 可以针对指定的 RD 显示。

**举例：**

```
switch(config)#show ip bgp vpnv4 all neighbors
BGP neighbor is 11.1.1.2, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 0.0.0.0
  Neighbor under common administration
  BGP state = Active
  Last read          , hold time is 240, keepalive interval is 60 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 0; dropped 0
Next connect timer due in 83 seconds
```

## 5.5.108 timers bgp

**命令：timers bgp *<0-65535> <0-65535>***

**no timers bgp [*<0-65535> <0-65535>*]**

**功能：**BGP 对所有邻居的时间进行设置。其 no 形式恢复这些时间为默认值。

**参数：*<0-65535>*：**分别是 KEEPALIVE 的时间间隔和保持时间

**缺省情况：**KEEPALIVE 时间为 60s，HOLD TIME 为 240s。

**命令模式：**特权和配置模式。

**使用指南：**与邻居的时间设置相似，只是这个设置针对所有邻居。

**举例：**

Switch(config-router)# timers bgp 50 200

**相关命令：neighbor timers, no neighbor timers**

# 5.6 IPv4 黑洞路由

## 5.6.1 ip route null0

**命令：ip route {*<ip-prefix> <mask>*|*<ip-prefix>*|*<prefix-length>*} null0 [*<distance>*]**

**no ip route {*<ip-prefix> <mask>*|*<ip-prefix>*|*<prefix-length>*} null0**

**功能：**配置到某一网段的路由，其出接口为 null0。

**参数：***<ip-prefix>*和*<mask>*分别为目的 IP 地址和子网掩码，点分十进制格式；*<ip-prefix>*和*<prefix-length>*分别为目的 IP 地址和前缀长度；null0 为黑洞路由的出接口；*<distance>*为路由管理距离值，取值范围为 1～255。

**缺省：**无。

**命令模式：**全局模式。

**使用指南：**在配置 IPv4 的黑洞路由的时候，出接口为 null0。

**举例：**配置一条到目的网段为 192.168.188.0/24 的黑洞路由。

Switch(config)#ip route 192.168.188.0/24 null0 20

# 5.7 GRE

## 5.7.1 debug gre

**命令：debug gre {packet | events | all}**

**no debug gre {packet | events | all}**

**功能：**打开 GRE 隧道的相应的调试开关。

**参数：**all：打开 GRE 隧道的所有 DEBUG 信息显示功能。

packet：打开 GRE 隧道的收发报文的 DEBUG 信息显示功能。

events：打开 GRE 隧道的事件 DEBUG 信息显示功能。

**缺省情况：**无。

**命令模式：**特权模式。

**举例：**打开 GRE 隧道的相应调试开关，GRE 隧道的相关信息在进行 GRE 隧道的封装转发的时候都会显示处理。

Switch# debug gre all

GRE Tunnel PACKET: sent, src <1.1.1.1>, dst <1.1.1.2>, size <140>, proto <0x0800>, to <tunnel1>

GRE Tunnel PACKET: recv, src <1.1.1.2>, dst <1.1.1.1>, size <140>, proto <0x0800>, from <tunnel1>

## 5.7.2 ip address

**命令：ip address *<ipv4-address>* *<mask>***

**no ip address *<ipv4-address>* *<mask>***

**功能：**配置 GRE 隧道接口的 IPv4 地址。

**参数：***<ipv4-address>*为 IPv4 地址,*<mask>*为子网掩码。

**命令模式：**隧道接口配置模式。

**缺省情况：**无。

**使用指南：**配置 GRE 隧道的接口地址为 IPv4 地址。对于隧道接口配置 IPv4 地址只允许配置一个 Primary 地址，不允许配置 Secondary 地址，该限制同样适用于其它模式的隧道，如配置隧道、6to4、isatap 等。

**注意：**配置 IPv4 地址的时候由于实现的原因必须要求隧道 active，存在配置保留后丢失 ipv4 地址配置的可能，这个和 IPv6 地址的配置逻辑不一致，IPv6 不要求隧道必须 active。

**举例：**配置 GRE 隧道的接口地址为 IPv4 地址。

Switch(config)# interface tunnel 1

Switch(config-if-tunnel1)#ip address 11.0.0.1 255.255.255.0

## 5.7.3 ip route

**命令：ip route *<ipv4-address/mask>* tunnel *<ID>***

**no ip route *<ipv4-address/mask>* tunnel *<ID>***

**功能：**配置 IPv4 静态路由的出接口是 GRE 隧道。

**参数：***<ipv4-address>*为 IPv4 地址,*<mask>*为子网掩码，*<ID>*为 GRE 隧道 ID。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**配置 IPv4 静态路由的出接口是 GRE 隧道。

**举例：**配置 IPv4 静态路由的出接口是 GRE 隧道。

Switch(config)# interface tunnel 1

Switch(config)#ip route 101.0.0.0/24 tunnel 1

## 5.7.4 ipv6 address

**命令：ipv6 address *<ipv6-address/prefix>***

**no ipv6 address *<ipv6-address/prefix>***

**功能：**配置 GRE 隧道接口的 IPv6 地址。

**参数：***<ipv6-address>*为 IPv6 地址, *<prefix>*为路由前缀。

**命令模式：**隧道接口配置模式。

**缺省情况：**无。

**使用指南：**配置 GRE 隧道的接口地址为 IPv6 地址。对于隧道接口配置 IPv6 地址，它和 VLAN 接口配置的 IPv6 地址一样，但是只可以配置一个 IPv6 地址，配置多个也没有什么意义，该限制同样适用于其它模式的隧道，如配置隧道、6to4、isatap 等。

注意：6to4 隧道还会自动生成一个 IPv6 地址。配置 IPv6 地址的时候不要求隧道必须 active，这个和 IPv4 地址的配置逻辑不一致。

**举例：**配置 GRE 隧道的接口地址为 IPv6 地址。

Switch(config)# interface tunnel 1

Switch(config-if-tunnel1)#ipv6 address 2011::1/64

## 5.7.5 ipv6 route

**命令：ipv6 route *<ipv6-address/prefix>* tunnel *<ID>***

**no ipv6 route *<ipv6-address/prefix>* tunnel *<ID>***

**功能：**配置 IPv6 静态路由的出接口是 GRE 隧道。

**参数：***<ipv6-address>*为 IPv6 地址,*<prefix>*为路由前缀，*<ID>*为 GRE 隧道 ID。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**配置 IPv6 静态路由的出接口是 GRE 隧道。

**举例：**配置 IPv6 静态路由的出接口是 GRE 隧道。

Switch(config)# interface tunnel 1

Switch(config)# ipv6 route 2080::/64 tunnel 1

## 5.7.6 loopback-group（全局）

**命令：loopback-group *<id>***

**no loopback-group *<id>***

**功能：**创建业务环回组。

**参数：***<id >*为环回组号，范围为 1-128。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**创建业务环回组。

**举例：**创建业务环回组 1。

Switch(config)# loopback-group 1

## 5.7.7 loopback-group （端口）

**命令：loopback-group *<id>***

**no loopback-group *<id>***

**功能：**将二层以太网口加入到指定的业务环回组。

**参数：***<id >*为环回组号，范围为 1-128。

**命令模式：**端口配置模式。

**缺省情况：**无。

**使用指南：**将特定端口加入到环回组前，应确保该端口是闲置端口且没有任何功能配置。

**举例：**将交换机的 1/1/1 端口加入到环回组 1 中。

Switch (config-if-ethernet1/1/1)#loopback-group 1

## 5.7.8 loopback-group （隧道接口）

**命令：loopback-group *<id>***

**no loopback-group *<id>***

**功能：**指定隧道引用特定的业务环回组。

**参数：***<id>*为环回组号，范围为 1-128。

**命令模式：**隧道接口配置模式。

**缺省情况：**无。

**使用指南：**指定隧道引用一个业务环回组，目前支持这一功能的隧道只有 GRE 隧道和 ISATAP 隧道，另外 ISATAP 隧道引用环回组和配置 nexthop 互斥。

**举例：**指定 tunnel 1 引用业务环回组 1。

Switch (config-if-tunnel1)#loopback-group 1

## 5.7.9 show gre tunnel

**命令：show gre tunnel {<1-50>|}**

**功能：**显示交换机中的 GRE 隧道配置信息。

**参数：**<1-50>-隧道 ID。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**举例：**显示交换机中的 GRE 隧道配置信息。

Switch# show gre tunnel

| name | mode | source | destination |
|---|---|---|---|
| Tunnel1 | gre ip | 192.168.1.1 | 192.168.1.2 |
| Tunnel2 | gre ipv6 | 2001::1 | 2001::2 |

| 显示内容 | 解释 |
|---|---|
| name | 隧道名 |

| | |
|---|---|
| mode | 隧道类型 |
| source | 隧道源地址（IPv4 或者 IPv6） |
| destination | 隧道目的地址（IPv4 或者 IPv6） |

## 5.7.10 show interface tunnel

**命令：show interface tunnel *<1-50>***

**功能：**显示隧道接口相关信息。

**参数：**<1-50>-隧道 ID。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**举例：**显示交换机中的指定隧道接口相关信息，如果是 GRE 隧道则显示指定 GRE 隧道的接口相关信息。

```
Switch# show interface tunnel 1
Tunnel1 is up, line protocol is up, dev index is 8001
  Device flag 0x81(UP NOARP)
  IPv4 address is:
    (NULL)
  VRF Bind: Not Bind
```

## 5.7.11 tunnel destination

**命令：tunnel destination {<ipv6-address> | <ipv4-address>}**

**no** tunnel **destination**

**功能：** 配置 GRE 隧道的目的地址为 IPv6 或者 IPv4 地址。

**参数：** *<ipv6-address>*为 IPv6 地址，*<ipv4-address>*为 IPv4 地址。

**命令模式：** 隧道接口配置模式。

**缺省情况：** 无。

**使用指南：** 配置 GRE 隧道的目的地址为 IPv6 或者 IPv4 地址。

**举例：** 配置 GRE 隧道的目的地址为 IPv4 地址。

```
Switch(config)# interface tunnel 1
Switch(config-if-tunnel1)#tunnel destination 60.0.0.3
```

## 5.7.12 tunnel mode gre ip

**命令：tunnel mode gre ip**

**no tunnel mode**

**功能：**配置隧道模式为 GREv4 隧道，数据报文 GRE 封装后是 IPv4 报文头，穿越 IPv4 网络。

**参数：**无。

**命令模式：**隧道接口配置模式。

**缺省情况：**无。

**使用指南：**配置 GREv4 隧道模式，数据报文进行 GREv4 隧道的封装后转发。

**举例：**数据报文进行 GREv4 隧道的封装转发。

Switch(config)# interface tunnel 1

Switch(config-if-tunnel1)# tunnel mode gre ip

## 5.7.13 tunnel mode gre ipv6

**命令：tunnel mode gre ipv6**

**no tunnel mode**

**功能：** 配置隧道模式为 GREv6 隧道，数据报文 GRE 封装后是 IPv6 报文头，穿越 IPv6 网络。

**参数：** 无。

**命令模式：** 隧道接口配置模式。

**缺省情况：** 无。

**使用指南：** 配置 GREv6 隧道模式，数据报文进行 GREv6 隧道封装后转发。

**举例：** 数据报文进行 GREv6 隧道封装转发。

Switch(config)# interface tunnel 2

Switch(config-if-tunnel1)# tunnel mode gre ipv6

## 5.7.14 tunnel source

**命令：tunnel source {<ipv6-address> | <ipv4-address>}**

**no tunnel source**

**功能：** 配置 GRE 隧道的源地址为 IPv6 或者 IPv4 地址。

**参数：** *<ipv6-address>*为 IPv6 地址，*<ipv4-address>*为 IPv4 地址。

**命令模式：** 隧道接口配置模式。

**缺省情况：** 无。

**使用指南：** 配置 GRE 隧道的源地址为 IPv6 或者 IPv4 地址。

**举例：** 配置 GRE 隧道的源地址为 IPv6 或者 IPv4 地址。

Switch(config)# interface tunnel 1

Switch(config-if-tunnel1)#tunnel source 10.1.1.3

# 5.8 ECMP

## 5.8.1 load-balance

本型号交换机不支持此命令。

## 5.8.2 maximum-paths

**命令：maximum-paths <1-32>**

**no maximum-paths**

**功能：** 本命令用来配置支持等价多路径的最大路径数目限制。本命令的 no 命令为恢复等价多路径的最大路径数目为缺省配置。

**参数：** <1-32>：目前支持用户配置的多路径数目为 1-32。当配置为 1 时等同关闭 ECMP 功能。另外，实际配置的数目为与用户输入值最相近的且大于用户输入值的 2 的幂。

**命令模式：** 全局配置模式。

**缺省情况：** 默认支持等价多路径的数目为 4 条。

**使用指南：** 无。

**举例：** 配置等价多路径的最大路径数目限制为 8。

Switch(config)# maximum-paths 8

## 5.8.3 load-balance hash-shift

**命令：load-balance hash-shift { dstmac| srcmac | srcport | vlan | dstip | srcip | l4-srcport | l4-dstport | flow-label | proto} value < num >**

**功能：** 设置交换机的字段偏移参与负载均衡算法。

**参数：** **dstmac**：使用目的 mac 的偏移参与运算；

**srcmac**：使用源 mac 的偏移参与运算；

**srcport**：使用源端口的偏移参与运算；

**vlan**：使用 vlan 的偏移参与运算；

**dstip**：使用目的 ip 的偏移参与运算；

**srcip**：使用源 ip 的偏移参与运算；

**l4-srcport**：使用 l4 源端口的偏移参与运算；

**l4-dstport**：使用 l4 目的端口的偏移参与运算；

**flow-label**：使用 flow-label 的偏移参与运算；

**proto**：使用协议的偏移参与运算。

**num**：取值范围为 0-5

**命令模式**： 全局配置模式。

**缺省情况**：不设置字段偏移。

**使用指南**：设置字段偏移来使聚合口成员的流量均匀。 此命令目的是辅助调试负载不均衡的场景。

**举例： 设置 dstip 偏移 5**

**Switch(**config)# load-balance hash-shift dstip value 5

# 5.9 BFD

## 5.9.1 bfd authentication key

**命令：bfd authentication key <*1-255*>**

**no bfd authentication key**

**功能**：接口开启 BFD 认证功能和配置使用的密钥。本命令的 no 操作为关闭 BFD 认证功能。

**参数**：<*1-255*>密钥号。

**缺省情况**：接口没有开启 BFD 认证功能。

**命令模式**：接口配置模式。

**使用指南**：配置该 BFD 接口使用的密钥号，不同的接口可以使用不同的加密认证方式。

输出：BFD 指定接口使用加密认证。

**举例**：接口开启 BFD 认证功能，使用的密钥号为 1。

s5(config-if-vlan50)#bfd authentication key 1

## 5.9.2 bfd authentication key md5

**命令：bfd authentication key <*1-255*> md5 <*WORD*>**

**no bfd authentication key <*1-255*>**

**功能**：配置 BFD 使用的 key 和 md5 方式加密的认证字符串。no 命令为删除配置的 key。

**参数**：<*1-255*>密钥号，<*WORD*>认证密钥串，长度为 1-16 个字节。

**缺省情况**：缺省没有配置认证的 key 和认证字符串。

**命令模式**：全局配置模式。

**使用指南**：配置 BFD 认证使用的 md5 模式和认证密钥串，配置该命令后 BFD 会使用报文中的可选字段进行认证，只有 BFD 两端的密钥配置一致时 BFD 才会建立邻居。

**举例**：采用 MD5 方式加密，密钥号为 1，认证字符串为 123456。

s5(config)#bfd authentication key 1 md5 123456

## 5.9.3 bfd authentication key text

**命令：bfd authentication key <*1-255*> text <*WORD*>**

**no bfd authentication key <*1-255*>**

**功能：**配置 BFD 认证使用的 key 和文本方式加密的认证字符串。no 命令为删除配置的 key。

**参数：**<*1-255*>密钥号，<*WORD*>认证字符串，长度为 1-16 个字节。

**缺省情况：**缺省没有配置认证的 key 和认证字符串。

**命令模式：**全局配置模式。

**使用指南：**配置 BFD 认证使用的模式和认证字符串，配置该命令后 BFD 会使用报文中的可选字段进行认证，只有 BFD 两端的认证密码配置一致时 BFD 才会建立邻居。

**举例：**采用文本方式加密，密钥号为 1，认证字符串为 123456。

s5(config)#bfd authentication key 1 text 123456

## 5.9.4 bfd echo

**命令：bfd echo**

**no bfd echo**

**功能：**开启 bfd echo 功能，no 命令为关闭 bfd echo 功能。

**参数：**无。

**缺省情况：**缺省接口上未开启 echo 功能。

**命令模式：**接口配置模式。

**使用指南：**启用 echo 功能，处于 UP 状态的 session 发送 echo 报文，从而降低 control 报文的频率。

**举例：**在接口上开启 echo 功能。

s5(config)#in vlan 50

s5(config-if-vlan50)#bfd echo

## 5.9.5 bfd echo-source-ip

**命令：bfd echo-source-ip <*ipv4-address*>**

**no bfd echo-source-ip**

**功能：**配置的 Echo 报文源地址进行链路故障的探测，no 命令操作为删除配置的 echo 报文源地址。

**参数：**<*ipv4-address*>为 IPv4 地址。配置参数的合法性由用户自己保证，不进行地址的合法性检查。

**缺省情况：**缺省没有配置 echo 报文源地址。

**命令模式：**全局配置模式。

**使用指南：**当 IPv4 链路 BFD 使用回声功能进行链路故障探测时需要配置 Echo 报文的源地址，源地址的配置比较随意，只要避免 ICMP 重定向报文的发送即可。报文的目的地址是本地的某一个接口地址，保证报文能够原路返回。对于报文的 UDP 数据内容则不做特殊要求。

**举例：**配置 bfd echo 报文源地址为 192.168.1.1。

s5(config)#bfd echo-source-ip 192.168.1.1

## 5.9.6 bfd echo-source-ipv6

**命令：bfd echo-source-ipv6 <*ipv6-address*>**

**no bfd echo-source-ipv6**

**功能：**配置的 Echo 报文源地址进行链路故障的探测，no 命令操作为删除配置的 echo 报文源地址。

**参数：**<*ipv6-address*>为 IPv6 地址。配置参数的合法性由用户自己保证，不进行地址的合法性检查。

**缺省情况：**缺省没有配置 echo 报文源地址。

**命令模式：**全局配置模式。

**使用指南：**当 IPv6 链路 BFD 使用回声功能进行链路故障探测时需要配置 Echo 报文的源地址，源地址的配置比较随意，只要避免 ICMPv6 重定向报文的发送即可。报文的目的地址是本地的某一个接口地址，保证报文能够原路返回。对于报文的 UDP 数据内容则不做特殊要求。

**举例：**配置 bfd echo 报文源地址为 2000::1。

s5(config)#bfd echo-source-ipv6 2000::1

## 5.9.7 bfd enable

**命令：bfd enable**

**no bfd enable**

**功能：**启用 VRRP（v3）协议与 BFD 联动功能，在该组上启用 BFD 检测功能，no 命令操作为禁用 VRRP（v3）协议与 BFD 联动功能。

**参数：**无。

**缺省情况：**默认情况没有开启 VRRP（v3）与 BFD 的联动功能。

**命令模式：**VRRP（v3）组配置模式。

**使用指南：**该组上启用 BFD 检测功能后，若该组在 backup 时收到 hello 报文，会通知 BFD 建立相应的 session，local ip 和 remote ip 为两端接口的实 IP。

**举例：**在 VRRP 组 1 上上开启 BFD 功能。

s5(config)#router vrrp 1

s5(config-router)#virtual-ip 50.1.1.10

s5(config-router)#interface vlan 50

s5(config-router)#bfd enable

s5(config-router)#enable

在 VRRPv3 组 1 上开启 BFD 功能。

s5(config)#router ipv6 vrrp 1

s5(config-router)#virtual-ipv6 fe80::1 interface vlan 50

s5(config-router)#bfd enable

s5(config-router)#enable

## 5.9.8 bfd interval

**命令：bfd interval <*value1*> min_rx <*value2*> multiplier <*value3*>**

**no bfd interval**

**功能：**配置 BFD 控制报文的最小发送时间间隔和会话检测系数。本命令的 no 操作为恢复检测系数为默认值。

**参数：**<*value1*>-最小发送时间间隔，单位 ms，范围 1-1000，对于不同的机型最小发送时间可能不同。<*value2*>-最小接收时间间隔，单位 ms，范围 1-1000，对于不同的机型最小接收时间可能不同，<*value3*>会话监测系数，范围 3-15。

**缺省情况：**缺省最小发送间隔为 20ms，最小接收间隔为 20ms，检测系数为 3。

**命令模式：**接口配置模式。

**使用指南：**配置 BFD 控制报文的最小发送时间间隔和会话检测系数，默认最小发送时间间隔为 20ms，会话监测系数为 3。

**举例：**修改接口上 BFD 最小发送间隔和最小接收间隔为 800ms，检测系数为 15。

s5(config)#in vlan 50

s5(config-if-vlan50)#bfd interval 800 min-rx 800 multiplier 15

s5(config-if-vlan50)#

## 5.9.9 bfd min-echo-recv-interval

本型号交换机不支持此命令

## 5.9.10 bfd mode

**命令：bfd mode {active | passive}**

**no bfd mode**

**功能：**配置 BFD 会话建立前的工作模式，默认为 active 模式。本命令的 no 操作为恢复 active 模式。

**参数：**active-主动模式，passive-被动模式。

**缺省情况：**缺省情况为 active 模式。

**命令模式：**全局配置模式。

**使用指南：**配置 BFD 会话建立前的工作模式，默认为 active 模式，不管是否收到对端发来的 BFD 控制报文，都会主动发送 BFD 控制报文。

**举例：**全局设置 BFD 的工作模式为 passive。

s1(config)#bfd mode passive

## 5.9.11 debug bfd

**命令：debug bfd {packet | event | all | fsm | error | timer}**

**功能：**打开 BFD 功能的相应的调试开关。

**参数：**all：打开 BFD 的所有 DEBUG 信息显示功能

packet：打开 BFD 的收发报文的 DEBUG 信息显示功能

event：打开 BFD 的事件 DEBUG 信息显示功能

fsm：打开 BFD 状态机事件的显示功能

error：打开 BFD 错误事件的显示功能

timer：打开 BFD 状态超时事件显示功能

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**打开 BFD 功能的相应调试开关。

**举例：**打开 BFD 功能的调试开关。

s5#debug bfd all

## 5.9.12 ip ospf bfd enable

**命令：ip ospf bfd enable**

**no ip ospf bfd enable**

**功能：**在指定接口上配置 OSPF 协议与 BFD 联动，no 命令操作为禁用已经配置的 OSPF 协议与 BFD 进行联动功能。

**参数：**无。

**缺省情况：**默认情况下没有开启 OSPF 与 BFD 的联动功能。

**命令模式：**接口配置模式。

**使用指南：**在启动 OSPF 协议的指定接口上配置 OSPF 协议与 BFD 进行联动功能，BFD 探测出链路故障后通知 OSPF 协议，OSPF 协议在最短时间内处理链路故障。

**举例：**在接口上开启 OSPF 与 BFD 的联动功能。

s5(config-if-vlan50)#ip ospf bfd enable

## 5.9.13 ip route bfd

**命令：ip route {vrf <*name*> <*ipv4-address*> | <*ipv4-address*>} mask <*nexthop*> bfd**

**no ip route {vrf <*name*> <*ipv4-address*> | <*ipv4-address*>} mask <*nexthop*> bfd**

**功能：**配置静态路由与 BFD 进行联动。no 命令操作为取消配置静态路由与 BFD 进行联动。

**参数：**<*name*>vrf name，<*ipv4-address*>路由目标地址，mask 路由的子网掩码，nexthop 路由的下一跳地址。

**命令模式：**全局配置模式。

**缺省配置：**默认情况下没有配置静态路由与 BFD 联动。

**使用指南：**配置 BFD 与该条路由进行联动，同时指明探测的模式。

**举例：**配置静态路由与 BFD 联动。

s3(config)#ip route 10.1.1.0/24 20.1.1.2 bfd

## 5.9.14 ipv6 ospf bfd enable

**命令：ipv6 ospf bfd enable**

**no ipv6 ospf bfd enable**

**功能：**在指定接口上配置 OSPFv3 协议与 BFD 联动。no 命令操作为禁用已经配置的 OSPFv3 协议与 BFD 进行联动功能。

**参数：**无。

**缺省情况：**默认情况下没有开启 OSPF 与 BFD 的联动功能。

**命令模式：**接口配置模式。

**使用指南：**在启动 OSPFv3 协议的指定接口上配置 OSPFv3 协议与 BFD 进行联动功能，BFD 探测出链路故障后通知 OSPFv3 协议，OSPFv3 协议在最短时间内处理链路故障。

**举例：**在接口上开启 OSPFv3 与 BFD 的联动功能。

s5(config-if-vlan50)#ipv ospf bfd enable

## 5.9.15 ipv6 ospf bfd enable instance-id

**命令：ipv6 ospf bfd enable instance-id *<0-255>***

**no ipv6 ospf bfd enable**

**功能：**在指定接口上配置指定 OSPFv3 实例与 BFD 联动。no 命令操作为禁用已经配置的 OSPFv3 实例与 BFD 进行联动功能。

**参数：**无。

**缺省情况：**默认情况下没有开启 OSPF 实例与 BFD 的联动功能。

**命令模式：**接口配置模式。

**使用指南：**在启动 OSPFv3 协议的指定接口上配置 OSPFv3 指定实例与 BFD 进行联动功能，BFD 探测出链路故障后通知 OSPFv3 协议，OSPFv3 协议在最短时间内处理链路故障。

**举例：**在接口上开启 OSPFv3 与 BFD 的联动功能。

s5(config-if-vlan50)#ipv ospf bfd enable instance-id 254

## 5.9.16 ipv6 rip bfd enable

**命令：ipv6 rip bfd enable**

**no ipv6 rip bfd enable**

**功能：**在指定接口上配置 RIPng 协议与 BFD 联动。no 命令操作为禁用已经配置的 RIPng 协议与 BFD 进行联动功能。

**参数：**无。

**缺省情况：**默认情况接口没有开启 RIPng 与 BFD 的联动。

**命令模式：**接口配置模式。

**使用指南：**启动 RIPng 协议与 BFD 进行联动功能，启用联动功能后，若在该接口上收到 RIPng 报文，RIPng 会通知 BFD 建立 remote ip 为该报文源 IP 的 session，并且检测该 session 的状态，及时通知 RIPng。

**举例：**开启接口上 RIPng 与 BFD 的联动功能。

s5(config-if-vlan50)#ipv6 rip bfd enable

## 5.9.17 ipv6 route bfd

**命令：ipv6 route {vrf <*name*> <*ipv6-address*> | <*ipv6-address*>} prefix <*nexthop*> bfd**

**no ipv6 route {vrf <name> <ipv6-address>|<ipv6-address>} prefix <*nexthop*> bfd**

**功能：**配置 IPv6 静态路由与 BFD 进行联动。no 命令操作为取消配置 IPv6 静态路由与 BFD 进行联动。

**参数：**<*name*>: vrf name，<*ipv6-address*>:路由目标地址，prefix:路由的前缀长度，vlanid:路由出接口，nexthop:路由的下一跳地址。

**缺省情况：**缺省没有配置 IPv6 静态路由与 BFD 联动。

**命令模式：**全局配置模式。

**使用指南：**配置 BFD 与该条路由进行联动，同时指明探测的模式。

**举例：**配置 IPv6 静态路由与 BFD 功能联动。

s3(config)#ipv6 route 3000::/64 2010::1 bfd

## 5.9.18 neighbor

**命令：neighbor {<*ipv6-address*> | <*ipv4-address*>} bfd**

**no neighbor {<*ipv6-address*> | <*ipv4-address*>}bfd**

**功能：**配置 BGP（4+）对等体邻居上使能 BFD 提供的链路检测功能，no 命令操作为取消配置 BGP（4+）对等体邻居上使能 BFD 提供的链路检测功能。

**参数：**<*ipv4-address*>为 IPv4 地址

<*ipv6-address*>为 IPv6 地址

配置参数的合法性由用户自己保证，不进行地址的合法性检查

**缺省配置：**默认情况下没有开启 BGP（4+）与 BFD 的联动功能。

**命令模式：**BGP（4+）路由配置模式

**使用指南：**在配置的 BGP（4+）对等体邻居上使能 BFD 提供的链路检测功能，BFD 探测出该邻居的链路故障后通知 BGP（4+）协议。

**举例：**

配置 BGP 对等体邻居上使能 BFD 提供的链路检测功能。

s5(config)#router bgp 1

s5(config-router)#neighbor 1.1.1.1 bfd

配置 BGP4+对等体邻居上使能 BFD 提供的链路检测功能。

s5(config-router)#router bgp 1

s5(config-router)#neighbor 2001::2 remote-as 200

s5(config-router)#neighbor 2001::2 bfd

## 5.9.19 rip bfd enable

**命令：rip bfd enable**

**no rip bfd enable**

**功能：**在指定接口上配置 RIP 协议与 BFD 联动，no 命令操作为禁用已经配置的 RIP 协议与 BFD 进行联动功能。

**参数：**无。

**缺省情况：**默认情况接口没有开启 RIP 与 BFD 的联动。

**命令模式：**接口配置模式。

**使用指南：**启动 RIP 协议与 BFD 进行联动功能,启用联动功能后，若在该接口上收到 RIP 报文，RIP 会通知 BFD 建立 remote ip 为该报文源 IP 的 session，并且检测该 session 的状态，及时通知 RIP。

**举例：**开启接口上 RIP 与 BFD 的联动功能。

s5(config-if-vlan50)#rip bfd enable

## 5.9.20 show bfd neighbor

**命令：show bfd neighbor [[*<ipv6-address>*|*<ipv4-address>*][details]]**

**功能：**显示交换机中的 BFD neighbor 的信息。

**参数：**<*ipv6-address*>:指定 IPv6 地址显示的 neighbor 信息，<*ipv4-address*>:指定 IPv4 地址显示的 neighbor 信息，这里的 IP 地址是指远端的 IP 地址，details:显示 neighbor 的详细信息。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**使用指南：**显示交换机中的 BFD neighbor 的信息。

**举例：**查看 BFD 邻居的相关信息。

switch#show bfd neighbor details

| OurAddr | NeighAddr | LD/RD | Detec Int(ms) | State | Interface |
|---|---|---|---|---|---|

12.1.1.1 12.1.1.2 1/1 3000 Down Vlan10

Local Diag: 3, Poll bit: 0

MinTx Int: 20(ms), MinRx Int: 20(ms), Multiplier: 3

Local Act Trans Int: 1000(ms), Remote Act Trans Int: 1000(ms)

Local Act Detec Int: 3000(ms)

Registered protocols: IPv4 Static Route

Echo state: Disable, Echo Detec Int(ms): 0

Multi Hop: No, Vrf Id: 0Min tx interval: 400(ms) - Min rx interval: 400(ms)

Min Echo interval: 400(ms)

# 5.10 BGP GR

## 5.10.1 bgp graceful-restart

**命令：bgp graceful-restart**

**no bgp graceful-restart**

**功能：**配置使能 BGP 支持 GR，并设置重启时间 restart-time 和废弃路由保持时间 stale-path-time 为默认值。本命令的 no 命令为不支持 GR 能力。

**参数：**无。

**命令模式：**BGP 路由配置模式

**缺省情况：**不使能 BGP 支持 GR。

**使用指南：**无。

**举例：**配置支持 GR 能力。

Switch(config-router)# bgp graceful-restart

## 5.10.2 bgp graceful-restart restart-time

**命令：bgp graceful-restart restart-time <1-3600>**

**no bgp graceful-restart restart-time <1-3600>**

**功能：**配置 BGP GR 的重启超时时间（Receiving Speaker 为发生重启的邻居启动一个重启超时定时器，使用 restart-time 为超时时间）。重启超时时间指定 Receiving Speaker 从发现邻居重启到收到邻居的 OPEN 消息最长的等待时间，如果超过这个时间 Receiving Speaker 没有收到邻居的 OPEN 消息，Receiving Speaker 可以删除为邻居保留的 SATLE 路由。

本命令 no 操作是恢复 restart-time 为初始值 120 秒。

**参数：**<1-3600>：时间，单位为秒

**命令模式：**BGP 路由配置模式

**缺省情况：**BGP GR 功能的 restart-time 采用默认值 120s。

**使用指南：**无。

**举例：**配置 BGP 的 GR restart-time 为 60 秒。

Switch(config-router)# bgp graceful-restart restart-time 60

## 5.10.3 bgp graceful-restart stale-path-time

**命令：bgp graceful-restart stale-path-time <1-3600>**

**no bgp graceful-restart stale-path-time <1-3600>**

**功能：**配置 BGP GR 保留废弃（STALE）路由超时时间，指定了 Receiving Speaker 从收到重启邻居的 OPEN 消息到收到重启邻居的 EOR 后删除废弃路由的最长的等待时间。

本命令 no 操作是恢复 stale-path-time 为初始值 360 秒。

**参数：**<1-3600>：时间，单位为秒。

**命令模式：**BGP 路由配置模式。

**缺省情况：**BGP GR 功能的 stalepath-time 采用默认值 360。

**使用指南：**无。

**举例：**配置 BGP 的 GR stale-path-time 为 460 秒。

Switch(config-router)# bgp graceful-restart stale-path-time 460

## 5.10.4 bgp selection-deferral-time

**命令：bgp selection-deferral-time <1-3600>**

**no bgp selection-deferral-time <1-3600>**

**功能：**配置 BGP GR 功能的优选延期超时时间，指定了 Restarting Speaker 从收到邻居的 OPEN 消息到收到所有邻居的 EOR 后开始路由优选计算的最长的等待时间，如果超过这个时间 Restarting Speaker 还没有收到所有邻居的 EOR，Restarting Speaker 可以开始路由的优选计算。

本命令 no 操作是恢复 selection-deferral-time 为初始值 120 秒。

**参数：**<1-3600>：时间，单位为秒。

**命令模式：**BGP 路由配置模式。

**缺省情况：**BGP GR 功能的优选延期超时时间采用默认值 120s。

**使用指南：**无。

**举例：**配置 BGP 的 GR selection-deferral-time 为 240 秒。

Switch(config-router)# bgp selection-deferral-time 240

## 5.10.5 neighbor capability graceful-restart

**命令：neighbor (A.B.C.D | X:X::X:X | WORD) capability graceful-restart**

**no neighbor (A.B.C.D | X:X::X:X | WORD) capability graceful-restart**

**功能：**配置邻居是否支持 GR 能力，本命令的 no 命令为不支持 GR 能力。

**参数：**(A.B.C.D | X:X::X:X | WORD)：BGP 邻居地址或者邻居组的名字。

**命令模式：**BGP 协议单播地址族模式、VRF 地址族模式。

**缺省情况：**系统默认为不配置，即不向邻居发送 GR 能力参数。

**使用指南：**无。

**举例：**配置给邻居 1.1.1.1 发送 GR 能力。

Switch(config-router)#neighbor 1.1.1.1 capability graceful-restart

## 5.10.6 neighbor restart-time

**命令：neighbor (A.B.C.D | X:X::X:X | WORD) restart-time <1-3600>**

**no neighbor (A.B.C.D | X:X::X:X | WORD) restart-time <1-3600>**

**功能：**配置邻居的重启超时时间，本命令 no 操作使该定时器恢复默认时间。

**参数：**(A.B.C.D | X:X::X:X | WORD)：BGP 邻居地址或者邻居组的名字。

<1-3600>：时间，单位为秒。

**命令模式：**BGP 协议单播地址族模式、VRF 地址族模式。

**缺省情况：**邻居的重启超时时间为默认值 120s。

**使用指南：**无。

**举例：**配置给邻居 1.1.1.1 的 restart-time 为 60 秒。

Switch(config-router)# neighbor 1.1.1.1 restart-time 60

# 5.11 OSPF GR

## 5.11.1 capability restart graceful

**命令：capability restart graceful**

**no capability restart**

**功能：**开启特定 OSPF 进程的 GR 功能；no 命令为关闭特定 OSPF 进程的 GR 功能。

**参数：**无。

**命令模式：**OSPF 协议配置模式。

**缺省情况：**缺省开启 OSPF GR 功能。

**使用指南：**交换机正在进行 OSPF GR，如果关闭 GR 功能，会使交换机立即退出 GR 过程。

**举例：**打开交换机 OSPF 默认进程的 OSPF GR 功能。

Switch(config)#router ospf

Switch(config-router)#capability restart graceful

## 5.11.2 debug ospf events gr

**命令：debug ospf events gr**

**no debug ospf events gr**

**功能：**开启显示 OSPF GR 相关事件信息的调试开关；no 命令为关闭显示 OSPF GR 相关事件信息的调试开关。

**参数：**无。

**命令模式：**特权模式。

**缺省情况：**缺省关闭显示。

**使用指南：**无。

**举例：**开启显示 OSPF GR 相关事件信息的调试开关。

Switch# debug ospf events gr

## 5.11.3 ospf graceful-restart grace-period

**命令：ospf graceful-restart grace-period <*integer*>**

**no ospf restart grace-period**

**功能：**配置 GR restarter 的 grace period。本命令的 no 操作为恢复 restarter 的 grace period 为缺省值。

**参数：<*integer*>**:配置的 grace period 取值，范围 1-1800，单位为秒。

**命令模式：**全局配置模式。

**缺省情况：**缺省的 grace period 为 60 秒。

**使用指南：**配置 GR restarter（进行主备切换或协议重启的交换机）的 grace period，GR 过程应该在一个 grace period 内完成，如果到期后 restarter 的 GR 过程依然没有完成，则强制退出 GR 过程，进行正常的 OSPF 重启。

**举例：**配置 GR restarter 的 grace period 为 100s。

Switch(config)#ospf graceful-restart grace-period 100

## 5.11.4 ospf graceful-restart helper max-grace-period

**命令：ospf graceful-restart helper max-grace-period <*integer*>**

**no ospf graceful-restart helper**

**功能：**GR helper 策略之一，配置 helper 支持的最大 grace period。本命令的 no 操作为删除所有配置的 helper 策略。

**参数：<*integer*>**:配置的 grace period 取值，范围 1-1800，单位为秒。

**命令模式：**全局配置模式。

**缺省情况：**缺省对 helper 支持的 grace period 无限制。

**使用指南：**如果 GR restarter 设置的 grace period 大于 helper 上所配置的 max-grace period，则 helper 将拒绝帮助 restarter 完成 GR。No 命令会删除所有的 helper 策略。

**举例：**配置 GR helper 允许的最大 grace period 为 100s。

Switch(config)#ospf graceful-restart helper max-grace-period 100

## 5.11.5 ospf graceful-restart helper never

**命令：ospf graceful-restart helper never**

**no ospf graceful-restart helper**

**功能：**GR helper 策略之一，配置交换机不能作为 OSPF GR helper 角色。本命令的 no 操作为删除所有配置的 helper 策略。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**缺省交换机可以作为 GR helper。

**使用指南：**配置该策略后，交换机只能充当 GR restarter（即进行主备切换或协议重启的交换机）角色，但不能充当 GR helper（帮助 restarter 完成 GR 过程的交换机）角色。

**举例：**配置交换机不作为 OSPF helper。

Switch(config)#ospf graceful-restart helper never

## 5.11.6 show ip ospf

**命令：show ip ospf [<process-id>]**

**功能：**显示 OSPF 主要信息，其中包括是否支持 GR，是否可以作为 GR helper，配置的 grace period 等信息。

**参数：<*process-id*>**:进程 ID，取值范围 0-65535。不配置参数时，表示显示所有进程的 OSPF 主要信息。

**命令模式：**特权配置模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**显示所有进程的 OSPF 主要信息。

```
Switch#show ip ospf
Routing Process "ospf 0" with ID 192.168.40.69
  Process bound to VRF default
  Process uptime is 52 minutes
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Graceful Restart
  Supports helper mode for Graceful Restart
  Grace period for Graceful Restart 100 secs
  SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
```

Refresh timer 10 secs

Number of external LSA 0. Checksum Sum 0x000000

Number of opaque AS LSA 0. Checksum Sum 0x000000

Number of non-default external LSA 0

External LSA database is unlimited.

Number of LSA originated 0

Number of LSA received 0

Number of areas attached to this router: 0

| 显示信息 | 解释 |
| --- | --- |
| Supports Graceful Restart | 交换机支持 OSPF GR 功能 |
| Supports helper mode for Graceful Restart | 交换机支持 OSPF GR 的 helper 模式 |
| Grace period for Graceful Restart 100 secs | 交换机配置的 OSPF GR Grace Period 为 100s |

## 5.11.7 show ip ospf graceful-restart

**命令：show ip ospf [<process-id>] graceful-restart**

**功能：**显示 OSPF GR 状态信息，包括是否正在进行 GR，是否处于 helper 模式，GR 剩余时间等信息。

**参数：*<process-id>:***进程 ID，取值范围 0-65535。不配置参数时，表示显示所有进程的 GR 状态信息。

**命令模式：**特权配置模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**

在 GR restarter（即进行主备切换或协议重启的交换机）上显示所有进程的 GR 状态信息：

Switch#show ip ospf graceful-restart

OSPF process 0 graceful-restart information：

GR status :GR in progress

GR remaining time : 50

| 显示信息 | 解释 |
| --- | --- |
| OSPF process 0 graceful-restart information | 进程 0 的 OSPF GR 状态信息 |
| GR status | GR 状态,GR in progress 表示交换机正在进行 GR |
| GR remaining time | GR 剩余时间 |

在 GR helper（即帮助 GR restarter 完成 GR 过程的交换机）上显示所有进程的 GR 状态信息：

Switch#show ip ospf graceful-restart

OSPF process 0 graceful-restart information：

GR status :Helper

| Neighbor ID | Interface | Remaining time |
|---|---|---|
| 1.1.1.1 | Vlan1 | 100 |
| 2.2.2.2 | Vlan1 | 200 |

| 显示信息 | 解释 |
|---|---|
| OSPF process 0 graceful-restart information | 进程 0 的 OSPF GR 状态信息 |
| GR status | GR 状态，Helper 表示交换机处于 helper 模式 |
| Neighbor ID | 正在帮助的 restarter 的 router-id |
| Interface | 与该 restarter 连接的三层接口 |
| Remaining time | GR 剩余时间 |

# 第 6 章 组播协议相关命令

## 6.1 组播

### 6.1.1 show ip mroute

**命令：show ip mroute [<GroupAddr> [<SourceAddr>]]**

**功能：**显示 ipv4 组播的软件转发表。

**参数：GroupAddr:** 显示跟此组播地址相关的转发表项。

**SourceAddr：**显示跟此源相关的转发表项。

**缺省情况：**无。

**命令模式：**特权模式和全局配置模式。

**使用指南：**

**举例：**显示所有组播转发表。

Switch(config)#show ip mroute

Name: Loopback, Index: 2002, State:49

Name: null0, Index: 2003, State:49

Name: sit0, Index: 2004, State:80

Name: Vlan1, Index: 2005, State:1043

Name: Vlan2, Index: 2006, State:1002

Name: pimreg, Index: 2007, State:c1

The total matched ipmr active mfc entries is 1, unresolved ipmr entries is 0

| Group | Origin | Iif | Wrong | Oif:TTL |
|---|---|---|---|---|
| 225.1.1.1 | 192.168.1.136 | vlan1 | 0 | 2006:1 |

| 显示信息 | 解释 |
|---|---|
| Name | 接口名 |
| Index | 接口索引 |
| State | 接口状态 |
| The total matched ipmr active mfc entries | 软件转发条目总数 |
| unresolved ipmr entries | 没有下发的转发条目数 |
| Group | 转发条目组地址 |
| Origin | 转发条目源地址 |
| Iif | 转发条目入接口名 |
| Wrong | 从错误接口收到的组播报文个数 |
| Oif | 转发条目出接口索引 |
| TTL | TTL 值 |

# 6.2 PIM-DM

## 6.2.1 debug pim timer sat

**命令：debug pim timer sat**

**no debug pim timer sat**

**功能：**打开显示 PIM DM 源活动计时器详细信息的调试开关；本命令的 no 操作为关闭本调试开关。

**参数：**无。

**缺省情况：**关闭。

**命令模式：**特权用户配置模式。

**使用指南：**打开此开关，可以显示源活动计时器的详细信息。

**举例：**

Switch # debug pim timer sat

备注：PIM-DM 中其他 debug 开关与 PIM-SM 通用，包括 debug pim event，debug pim packet，debug pim nexthop，debug pim nsm， debug pim mfc，debug pim mib，debug pim timer， debug pim state，请参考 PIM-SM 手册部分

## 6.2.2 debug pim timer srt

**命令：debug pim timer srt**

**no debug pim timer srt**

**功能：**打开显示 PIM DM 状态更新计时器详细信息的调试开关；本命令的 no 操作为关闭本调试开关。

**参数：**无。

**缺省情况：**关闭。

**命令模式：**特权用户配置模式。

**使用指南：**打开此开关，可以显示 PIM DM 状态更新计时器的详细信息。

**举例：**Switch # debug pim timer srt

备注：PIM-DM 中其他 debug 开关与 PIM-SM 通用，包括 debug pim event，debug pim packet，debug pim nexthop，debug pim nsm， debug pim mfc，debug pim mib，debug pim timer， debug pim state，请参考 PIM-SM 手册部分

## 6.2.3 ip mroute

**命令：ip mroute *<A.B.C.D> <A.B.C.D> <ifname> <.ifname>***

**no ip mroute *<A.B.C.D> <A.B.C.D>* [*<ifname> <.ifname>*]**

**功能：**配置静态组播表项。No 操作删除静态组播表项或部分出接口。

**参数：*<A.B.C.D> <A.B.C.D>***分别为组播的源地址和组地址。

***<ifname> <.ifname>***，第一个为入接口，后面的为出接口。

**缺省情况：**若不包含接口参数，则删除该静态组播表项。

**命令模式：**全局配置模式。

**使用指南：**所有配置的接口名必须存在，且必须是 VLAN 接口。出接口只有启动了 PIM 且 UP 的接口才能下发，如入接口没有 UP、未启动 PIM 或 RPF 检查不正确，不会下发该表项。通过 no 命令删除配置的静态组播表项，若删除指令包含所有出接口或未指定接口信息，则删除该静态组播表项，否则删除指定的出接口。

**举例：**

Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30

## 6.2.4 ip pim bsr-border

**命令：ip pim bsr-border**

**no ip pim bsr-border**

**功能：**配置、取消接口为 PIM BSR-BORDER。

**参数：**无。

**缺省情况：**非 BSR-BORDER。

**命令模式：**接口配置模式。

**使用指南：**配置为 BSR-BORDER 的接口，BSR 相关消息不向该接口发送也不从该接口接收，连接的网络被认为都是该接口的直连网络。

**举例：**

Switch(Config-if-Vlan1)#no ip pim bsr-border

## 6.2.5 ip pim dense-mode

**命令：ip pim dense-mode**

**no ip pim dense-mode**

**功能：**在接口上启动 PIM-DM 协议；本命令的 no 操作在接口上关闭 PIM-DM 协议。

**参数：**无。

**缺省情况：**缺省为不启动 PIM-DM 协议。

**命令模式：**接口配置模式。

**使用指南：**此命令需要在全局配置模式下执行 ip pim multicast-routing，才能生效。不支持组播协议互操作，即同一台交换机不能同时开启密集模式和稀疏模式。

**举例：**在接口 VLAN1 上启动 PIM-DM 协议。

Switch(config)#ip pim multicast-routing

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip pim dense-mode

## 6.2.6 ip pim dr-priority

**命令：ip pim dr-priority <*priority*>**

**no ip pim dr-priority**

**功能：**设置、取消以及改变接口的 DR 优先级值。同一网段相邻节点通过 hello 报文选举出本网段的指定路由器 DR，no 操作恢复默认值。

**参数：*<priority>*** 优先级。

**缺省情况：**1。

**命令模式：**接口配置模式。

**使用指南：**取值范围 0-4294967294，值越高，越优先。

**举例：**配置接口 VLAN1 的 DR priority 值为 100

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)#ip pim dr-priority 100

Switch (Config-if-Vlan1)#

## 6.2.7 ip pim exclude-genid

**命令：ip pim exclude-genid**

**no ip pim exclude-genid**

**功能：**此命令使得发出的 Hello 报文不包含 GenId 选项，no 操作恢复默认。

**参数：**无。

**缺省情况：**Hello 报文包含 GenId 选项。

**命令模式：**接口配置模式。

**使用指南：**此命令用于与较老的 Cisco IOS 版本交互。

**举例：**配置交换机发出的 hello 报文中不包含 GenID 选项。

Switch (Config-if-Vlan1)#ip pim exclude-genid

Switch (Config-if-Vlan1)#

## 6.2.8 ip pim hello-holdtime

**命令：ip pim hello-holdtime <*value*>**

**no ip pim hello-holdtime**

**功能：**设置 Hello 消息中 Holdtime 项的值，此值用于描述邻居超时时间，如果在这一时间内，没有收到该邻居的 hello 报文，则将此邻居纪录删除。no 操作取消设置的 holdtime 值而恢复到缺省值。

**参数：*<vaule>*** holdtime 设置时间，取值范围<1-65535>。

**缺省情况：**为 3.5*Hello_interval，hello_interval 的默认值为 30s，因此 hello-holdtime 的默认值为 105s。

**命令模式：**接口配置模式。

**使用指南：**如果不设置，则 hello-holdtime 默认为当前 Hello-interval 的 3.5 倍。如果设置的 hello-holdtime 小于当前的 hello_interval，则这个设置会被拒绝。每次 hello-interval 被更新的

时候，hello-holdtime 也会根据如下规则更新：如果 hello_holdtime 没有被配置，或者如果 hello_holdtime 被配置了但是比当前的 hello_interval 小，则 hello_holdtime 被修改为 3.5*Hello_interval，否则保持被配置的值。

**举例：**配置接口 hello holdtime 的值。

Switch (config)# interface vlan1

Switch (Config -if-Vlan1)#ip pim hello-holdtime 10

Switch (Config -if-Vlan1)#

## 6.2.9 ip pim hello-interval

**命令：ip pim hello-interval <*interval*>**

**no ip pim hello-interval**

**功能：**配置接口 PIM-DM hello 报文间隔时间；本命令的 no 操作恢复为缺省值。

**参数：<*interval*>**为周期发送 PIM-DM hello 报文的时间间隔，取值范围 1～18724s。

**缺省情况：**周期发送 PIM-DM hello 报文的时间间隔缺省为 30s。

**命令模式：**接口配置模式。

**使用指南：**hello 消息使得 PIM-DM 交换机可以互相定位，确定邻居关系。PIM-DM 交换机通过周期向邻居发送 hello 消息来宣告自己的存在，如果在规定的时间内没有收到邻居发送的 hello 消息，则认为该邻居丢失。该时间值的配置不能大于邻居超时时间。

**举例：**在接口 VLAN1 上配置 PIM-DM hello 间隔。

Switch(config)#interface vlan1

Switch(Config-if-Vlan1)#ip pim hello-interval 20

## 6.2.10 ip pim multicast-routing

**命令：ip pim multicast-routing**

**no ip pim multicast-routing**

**功能：**全局启动 PIM 协议；本命令的 no 操作全局关闭 PIM 协议。

**参数：**无。

**缺省情况：**缺省为不启动 PIM 协议。

**命令模式：**全局配置模式。

**使用指南：**本命令全局启动 PIM，但是要让 PIM-DM 工作，还必须在接口上启动 PIM-DM。

**举例：**全局启动 PIM 协议。

Switch (config)#ip pim multicast-routing

Switch (config)#

## 6.2.11 ip pim neighbor-filter

**命令：ip pim neighbor-filter <*list-number*>**

**no ip pim neighbor-filter <*list-number*>**

**功能：**配置邻居访问列表。如果被列表过滤，如果已经同此邻居建立连接，则此连接马上被切断，如果没有建立连接，则这个连接不能建立。

**参数：*<list-number>*:**简单访问列表号，取值 1-99。

**缺省情况：**没有 neighbor filter 设置。

**命令模式：**接口配置模式。

**使用指南：**ACL 的默认行为为 DENY。即如果配置 access-list 1，则 access-list 1 中的默认行为是 deny。在下面的举例中如果不配置 permit any-source，则 deny 10.1.4.10 0.0.0.255 的效果同于 deny any-source。

**举例：**设置接口 VLAN1 上 pim 邻居的过滤规则。

```
Switch #show ip pim neighbor
Neighbor          Interface          Uptime/Expires      Ver   DR
Address                                                        Priority/Mode
10.1.4.10         Vlan1              02:30:30/00:01:41 v2     4294967294 / DR
Switch (Config-if-Vlan1)#ip pim neighbor-filter 2
Switch (config)#access-list 2 deny 10.1.4.10 0.0.0.255
Switch (config)#access-list 2 permit any-source
Switch (config)#show ip pim neighbor
Switch (config)#
```

## 6.2.12 ip pim scope-border

**命令：ip pim scope-border [*<1-99 >*|*<acl_name>*]**

**no ip pim scope-border**

**功能：**配置、取消 PIM 的管理边界。

**参数：*<1-99 >*:** 判断是否属于管理范围组地址的 ACL 号。

***<acl_name>*:** 判断是否属于管理范围组地址的 ACL 名，应当是标准 ACL 名。

**缺省情况：**非管理边界，访问列表不指定表示使用默认的管理组范围。

**命令模式：**接口配置模式。

**使用指南：**配置 IP pim 的管理边界和使用的 ACL。组播数据不向 SCOPE-BORDER 扩散。

**举例：**

```
Switch(Config-if-Vlan2)#ip pim scope-border 3
```

## 6.2.13 ip pim state-refresh origination-interval

**命令：ip pim state-refresh origination-interval *<interval>***

**no ip pim state-refresh origination-interval**

**功能：**在全局模式下配置 state-refresh 报文发送间隔。no 操作恢复默认值。

**参数：**<*interval*> 报文发送间隔值 4-100s。

**缺省情况：**60s。

**命令模式：**全局配置模式。

**使用指南：**第一跳路由器定期发送 state-refresh 报文以维持所有下游路由器的 PIM-DM 表项。通过此命令可以修改 state-refresh 报文的发送间隔，通常不建议您修改相关定时器的时间间隔。

**举例：**将交换机上的 state-refresh 报文发送间隔设为 90 秒。

Switch (config)#ip pim state-refresh origination-interval 90

## 6.2.14 show ip pim interface

**命令：show ip pim interface**

**功能：**显示 PIM 接口信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示 PIM 协议的接口信息。

**举例：**Switch (config)#show ip pim interface

| Address | Interface | VIFindex | Ver/ Mode | Nbr Count | DR Prior | DR |
|---|---|---|---|---|---|---|
| 10.1.4.3 | Vlan1 | 0 | v2/S | 1 | 1 | 10.1.4.3 |
| 10.1.7.1 | Vlan2 | 2 | v2/S | 0 | 1 | 10.1.7.1 |

| 显示信息 | 解释 |
|---|---|
| Address | 接口地址 |
| Interface | 接口名 |
| VIF index | 接口索引号 |
| Ver/Mode | pim 版本和模式，版本一般为 v2，sparse mode 显示 S，dense mode 显示 D |
| Nbr Count | 此接口上的邻居个数 |
| DR Prior | Dr 优先级 |
| DR | 此接口 DR 的地址 |

## 6.2.15 show ip pim mroute dense-mode

**命令：show ip pim mroute dense-mode [group <*A.B.C.D*>] [source <*A.B.C.D*>]**

**功能：**显示 PIM-DM 报文转发项。

**参数：**group <A.B.C.D>：显示跟此组播地址相关的转发表项。

source <A.B.C.D>：显示跟此源相关的转发表项。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**使用指南：**本命令用于显示 PIM-DM 维护的组播路由信息。

**举例：**显示所有 PIM-DM 报文转发项。

Switch(config)#show ip pim mroute dense-mode

IP Multicast Routing Table

(*,G) Entries: 1

(S,G) Entries: 1

(*, 226.0.0.1)

Local ..l.....

(192.168.1.12, 226.0.0.1)

RPF nbr: 0.0.0.0

RPF idx: Vlan2

Upstream State: FORWARDING

Origin State: ORIGINATOR

Local .....

Pruned .....

Asserted .....

Outgoing ..o.....

Switch#

| 显示信息 | 解释 |
|---|---|
| (*,226.0.0.1) | (*,G)转发项 |
| (192.168.1.12, 226.0.0.1) | (S,G)转发项 |
| RPF nbr | 反向路径邻居，DM 中指源方向的上游邻居，0.0.0.0 表示此交换机既为第一跳 |
| RPF idx | RPF 邻居所在的接口 |
| Upstream State | 上游方向状态，有 FORWARDING(可以转发上游的数据)，PRUNED(上游停止转发数据)，ACKPENDING(等待上游响应，转发上游数据) |
| Origin State | 有两个值：ORIGINATOR(处于可发 state-refresh 状态)，NON_ ORIGINATOR(不可发 state-refresh 状态) |
| Local | 本地加入接口，此接口收到 IGMP Join |
| Pruned | PIM 剪枝接口，此接口收到 Prune 消息 |
| Asserted | Asserted 状态 |
| Outgoing | 组播数据最终出接口的 index 号，在此例中出接口的 index 为 2。可以通过命令 show ip pim |

| | |
|---|---|
| | interface 察看接口详细信息 |

## 6.2.16 show ip pim neighbor

**命令：show ip pim neighbor**

**功能：**显示路由器邻居。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示 PIM 协议维护的组播路由器邻居信息。

**举例：**Switch (config)#show ip pim neighbor

| Neighbor Address | Interface | Uptime/Expires | Ver | DR Priority/Mode |
|---|---|---|---|---|
| 10.1.6.1 | Vlan1 | 00:00:10/00:01:35 | v2 | 1 / |
| 10.1.6.2 | Vlan1 | 00:00:13/00:01:32 | v2 | 1 / |
| 10.1.4.2 | Vlan3 | 00:00:18/00:01:30 | v2 | 1 / |
| 10.1.4.3 | Vlan3 | 00:00:17/00:01:29 | v2 | 1 / |

| 显示信息 | 解释 |
|---|---|
| Neighbor Address | 邻居地址 |
| Interface | 邻居所在接口 |
| Uptime/Expires | 运行时间/超时时间 |
| Ver | pim 版本，一般为 v2 |
| DR Priority/Mode | 此邻居发来 Hello 消息中的 DR 优先级以及此邻居是否该接口上的 DR |

## 6.2.17 show ip pim nexthop

**命令：show ip pim nexthop**

**功能：**显示 PIM 缓存的单播路由表中的下一跳路由器

**参数：**无

**缺省情况：**无

**命令模式：**特权和配置模式。

**使用指南：**用于显示 PIM 保存的下一跳路由器信息。

**举例：**

Switch(config)#show ip pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable

Destination Type Nexthop Nexthop Nexthop Nexthop Metric Pref Refcnt

```
                        Num       Addr            Ifindex     Name
____
192.168.1.1       N...  1         0.0.0.0         2006              0       0       1

192.168.1.9       ..S.  1         0.0.0.0         2006              0       0       1
```

| 显示信息 | 解释 |
|---|---|
| Destination | 下一跳的目标地址 |
| Type | N：新创建的下一跳，还没有确定 RP 方向或者 S 方向 R：RP 方向 S：源方向 U：不可到达 |
| Nexthop Num | 下一跳计数 |
| Nexthop Addr | 下一跳地址 |
| Nexthop Ifindex | 下一跳所在接口索引 |
| Nexthop Name | 下一跳名字 |
| Metric | 到下一跳的路径损耗 Metric |
| Pref | 路径 Preference |
| Refcnt | 引用计数 |

# 6.3 PIM-SM

## 6.3.1 clear ip pim bsr rp-set

**命令：clear ip pim bsr rp-set ***

**功能：**清除所有RP集。

**参数：**无。

**命令模式：**特权用户配置模式。

**使用指南：**快速清除所有RP集。

**举例：**清除所有RP集。

Switch# clear ip pim bsr rp-set *

**相关命令：show ip pim bsr-router**

## 6.3.2 debug pim event

**命令：debug pim event**

**no debug pim event**

**功能：**打开/关闭 pim event debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权用户配置模式。

**使用指南：**通过开启此开关，可以监控 PIM 协议运行中发生的事件信息。

**举例：**

Switch# debug pim event

Switch#

## 6.3.3 debug pim mfc

**命令：debug pim mfc**

**no debug pim mfc**

**功能：**打开/关闭 pim 组播转发缓存 debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权用户配置模式。

**使用指南：**打开此开关，显示生成和下发的组播表项的信息。

**举例：**

Switch# debug pim mfc

## 6.3.4 debug pim mib

**命令：debug pim mib**

**no debug pim mib**

**功能：**打开/关闭 PIM MIB debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权用户配置模式。

**使用指南：**可以通过此开关监控关于 PIM MIB 相关的信息。

**举例：**

Switch# debug pim mib

Switch#

## 6.3.5 debug pim nexthop

**命令：debug pim nexthop**

**no debug pim nexthop**

**功能：**打开/关闭 pim 中关于 nexthop 变化的 debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权用户配置模式。

**使用指南：**可以通过此开关监控关于 PIM NEXTHOP 数据变化的相关信息。

**举例：**

Switch# debug pim nexthop

Switch#

## 6.3.6 debug pim nsm

**命令：debug pim nsm**

**no debug pim nsm**

**功能：**打开/关闭 pim Network Services 模块通讯的 debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权用户配置模式。

**使用指南：**使用此调试开关可以用于监控 PIM 模块与网络服务模块交互的信息。

**举例：**

Switch# debug pim nsm

Switch#

## 6.3.7 debug pim packet

**命令：debug pim packet**

**debug pim packet in**

**debug pim packet out**

**no debug pim packet**

**no debug pim packet in**

**no debug pim packet out**

**功能：**打开/关闭 pim 包的 debug 开关。

**参数：**in 只显示收到的 pim 包。

out 只显示发出的 pim 包。

无 以上两者都显示。

**缺省情况：**不打开此开关。

**命令模式：**特权用户配置模式。

**使用指南：**通过开启此开关，可以监控 PIM 协议收到和/或发送的报文。

**举例：**

Switch# debug pim packet in

Switch#

## 6.3.8 debug pim state

**命令：debug pim state**

**no debug pim state**

**功能：**打开/关闭 pim sm 转发状态机的 debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权用户配置模式。

**使用指南：**可以通过此开关监控关于 PIM 状态机变化的相关信息。

**举例：**

Switch# debug pim state

Switch#

## 6.3.9 debug pim timer

**命令：debug pim timer**

**debug pim timer assert**

**debug pim timer assert at**

**debug pim timer bsr bst**

**debug pim timer bsr crp**

**debug pim timer bsr**

**debug pim timer hello ht**

**debug pim timer hello nlt**

**debug pim timer hello tht**

**debug pim timer hello**

**debug pim timer joinprune et**

**debug pim timer joinprune jt**

**debug pim timer joinprune kat**

**debug pim timer joinprune ot**

**debug pim timer joinprune plt**

**debug pim timer joinprune ppt**

**debug pim timer joinprune pt**

**debug pim timer joinprune**

**debug pim timer register rst**

**debug pim timer register**

**no debug pim timer**

**no debug pim timer assert**

**no debug pim timer assert at**

**no debug pim timer bsr bst**

**no debug pim timer bsr crp**

**no debug pim timer bsr**

**no debug pim timer hello ht**

**no debug pim timer hello nlt**

**no debug pim timer hello tht**

**no debug pim timer hello**

**no debug pim timer joinprune et**

**no debug pim timer joinprune jt**

**no debug pim timer joinprune kat**

**no debug pim timer joinprune ot**

**no debug pim timer joinprune plt**

**no debug pim timer joinprune ppt**

**no debug pim timer joinprune pt**

**no debug pim timer joinprune**

**no debug pim timer register rst**

**no debug pim timer register**

**功能：**打开/关闭 pim 各个模块计时器。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权用户配置模式。

**使用指南：**可以根据需求打开指定的计时器的调试信息。

**举例：**

Switch# debug pim timer assert

Switch#

## 6.3.10 ip mroute

**命令：ip mroute *<A.B.C.D> <A.B.C.D> <ifname> <.ifname>***

**no ip mroute *<A.B.C.D> <A.B.C.D>* [*<ifname> <.ifname>*]**

**功能：**配置静态组播表项。No 操作删除静态组播表项或部分出接口。

**参数：*<A.B.C.D> <A.B.C.D>***分别为组播的源地址和组地址。

***<ifname> <.ifname>***，第一个为入接口，后面的为出接口。

**缺省情况：**若不包含接口参数，则删除该静态组播表项。

**命令模式：**全局配置模式。

**使用指南：**所有配置的接口名必须存在，且必须是 VLAN 接口。出接口只有启动了 PIM 且 UP 的接口才能下发，如入接口没有 UP、未启动 PIM 或 RPF 检查不正确，不会下发该表项。通过 no 命令删除配置的静态组播表项，若删除指令包含所有出接口或未指定接口信息，则删除该静态组播表项，否则删除指定的出接口。

**举例：**

Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30

## 6.3.11 ip multicast unresolved-cache aging-time

**命令：ip multicast unresolved-cache aging-time <value>**

**no ip multicast unresolved-cache aging-time**

**功能：** 配置内核组播路由缓存时间；本命令的 no 操作恢复为缺省值。

**参数：** **< value>** 为配置的缓存时间，取值范围 1～20s。

**缺省情况：** 缺省为 10s。

**命令模式：** 全局配置模式。

**使用指南：** 配置组播路由条目在内核的缓存时间。

**举例：**

Switch(config)# ip multicast unresolved-cache aging-time 18

## 6.3.12 ip pim accept-register

**命令：ip pim accept-register list <*list-number*>**

**no ip pim accept-register**

**功能：**用这个命令去过滤指定的组播源和组播地址。

**参数：**<***list-number***>：访问列表号，取值范围 1-99 或 100-199，1-99 为标准访问列表号，100-199 为扩展访问列表号。

**缺省情况：**允许任何源到任何组的组播注册。

**命令模式：**全局配置模式。

**使用指南：**该命令用于设置对 PIM 的 REGISTER 报文进行过滤的访问列表，访问列表中的地址分别指定了过滤的组播源和组播组信息。对于匹配为 DENY 的组源组合，PIM 协议在收到 REGISTER 报文后立即发送 REGISTER-STOP 并且不建立组记录。

**举例：**配置接受 register 报文过滤规则。

Switch(config)#ip pim accept-register list 120

Switch (config)#access-list 120 deny ip 10.1.0.2 0.0.0.255 239.192.1.10 0.0.0.255

Switch (config)#

## 6.3.13 ip pim bsr-border

**命令：ip pim bsr-border**

**no ip pim bsr-border**

**功能：**配置、取消接口为 PIM BSR-BORDER。

**参数：**无。

**缺省情况：**非 BSR-BORDER。

**命令模式：**接口配置模式。

**使用指南：**配置为 BSR-BORDER 的接口，BSR 相关消息不向该接口发送也不从该接口接收，连接的网络被认为都是该接口的直连网络。

**举例：**

Switch(Config-if-Vlan1)#no ip pim bsr-border

## 6.3.14 ip pim bsr-candidate

**命令：ip pim bsr-candidate {vlan <*vlan-id*>| <*ifname*>} [*hash-mask-length*] [priority]**

**no ip pim bsr-candidate**

**功能：**该命令为全局候选 BSR 配置命令，用于配置 PIM-SM 候选 BSR 的信息，以用于同其它候选 BSR 竞争 BSR 路由器；本命令的 no 操作为取消候选 BSR 的配置。

**参数：*vlan-id*：**为 VLAN ID;

***ifname*：**为指定接口名；

**[*hash-mask-length*]：**为指定哈希算法中掩码长度，其用于 RP 自举选择，取值范围为 0-32；

**[*priority*]：**为本候选 BSR 的 BSR 优先级，取值范围为 0-255，若不配置该参数，则本候选 BSR 的 BSR 缺省优先级为 0。

**缺省情况：**本交换机不是 BSR 候选路由器。

**命令模式：**全局配置模式。

**使用指南：**该命令为全局候选 BSR 配置命令，用于配置 PIM-SM 候选 BSR 的信息，以用于同其它候选 BSR 竞争 BSR 路由器，只有配置本命令，本交换机才是 BSR 候选路由器。

**举例：**全局配置接口 VLAN1 为候选 BSR 消息发送接口。

Switch (config)# ip pim bsr-candidate vlan1 30 10

Switch (config)#

## 6.3.15 ip pim cisco-register-checksum

**命令：ip pim cisco-register-checksum [group-list <*simple-acl*>]**

**no ip pim cisco-register-checksum [group-list <*simple-acl*>]**

**功能：**设置在计算被 group-list 指定的组的注册报文的 checksum 时使用整个报文的长度。

**缺省情况：**用注册报文的头部长度来计算 checksum，即 8

**参数：<*simple-acl*>：** <1-99> Simple access list

**命令模式：**全局配置模式

**使用指南：**此命令是用于较老的 Cisco IOS 版本中交互。当不带参数时，表示对整个注册计算校验和(与 cisco 兼容)，带 group-list 参数，表示设置在计算被 group-list 指定的组的注册报文的 checksum 时使用整个报文的长度。

**举例：**配置计算访问列表 23 所指定的组的注册报文的 checksum 使用整个报文的长度

Switch (config)#ip pim cisco-register-checksum group-list 23

Switch (config)#

## 6.3.16 ip pim dr-priority

**命令：ip pim dr-priority <*priority*>**

**no ip pim dr-priority**

**功能：**设置、取消以及改变接口的 DR 优先级值。同一网段相邻节点通过 hello 报文选举出本网段的指定路由器 DR，no 操作恢复默认值

**参数：*<priority>*** 优先级。

**缺省情况：**1

**命令模式：**接口配置模式

**使用指南：**取值范围 0-4294967294，值越高，越优先。

**举例：**配置接口 VLAN1 的 DR priority 值为 100

Switch (config)# interface vlan 1

Switch (Config-if-Vlan1)# ip pim dr-priority 100

## 6.3.17 ip pim exclude-genid

**命令：ip pim exclude-genid**

**no ip pim exclude-genid**

**功能：**此命令使得 PIM SM 发出的 Hello 报文不包含 GenId 选项，no 操作恢复默认

**参数：**无

**缺省情况：**Hello 报文包含 GenId 选项

**命令模式：**接口配置模式

**使用指南：**此命令用于与较老的 Cisco IOS 版本交互

**举例：**配置交换机发出的 hello 报文中不包含 GenID 选项

Switch (Config-if-Vlan1)#ip pim exclude-genid

Switch (Config-if-Vlan1)#

## 6.3.18 ip pim hello-holdtime

**命令：ip pim hello-holdtime <*value*>**

**no ip pim hello-holdtime**

**功能：**设置 Hello 消息中 Holdtime 项的值，此值用于描述邻居超时时间，如果在这一时间内，没有收到该邻居的 hello 报文，则将此邻居纪录删除。no 操作取消设置的 holdtime 值而恢复到缺省值。

**参数：*<vaule>*** holdtime 设置时间，取值范围<1-65535>。

**缺省情况：**为 3.5*Hello_interval，hello_interval 的默认值为 30s，因此 hello-holdtime 的默认值为 105s。

**命令模式：**接口配置模式

**使用指南：**如果不设置，则 hello-holdtime 默认为当前 Hello-interval 的 3.5 倍。如果设置的 hello-holdtime 小于当前的 hello_interval，则这个设置会被拒绝。每次 hello-interval 被更新的时候，hello-holdtime 也会根据如下规则更新：如果 hello_holdtime 没有被配置，或者如果

hello_holdtime 被配置了但是比当前的 hello_interval 小，则 hello_holdtime 被修改为 3.5*Hello_interval，否则保持被配置的值。

**举例：**配置接口 hello holdtime 的值

Switch (config)# interface vlan1

Switch (Config -if-Vlan1)#ip pim hello-holdtime 10

Switch (Config -if-Vlan1)#

## 6.3.19 ip pim hello-interval

**命令：ip pim hello-interval <*interval*>**

**no ip pim hello-interval**

**功能：**配置接口 pim hello 报文间隔时间；本命令的 no 操作恢复为缺省值。

**参数：<*interval*>**为周期发送 pim hello 报文的时间间隔，取值范围 1～18724s。

**缺省情况：**周期发送 pim hello 报文的时间间隔缺省为 30s。

**命令模式：**接口配置模式

**使用指南：**hello 消息使得 pim 交换机可以互相定位，确定邻居关系。pim 交换机通过周期向邻居发送 hello 消息来宣告自己的存在，如果在规定的时间内没有收到邻居发送的 hello 消息，则认为该邻居丢失。该时间值的配置不能大于邻居超时时间。

**举例：**在接口 VLAN1 上配置 PIM-SM hello 间隔。

Switch (config)#interface vlan 1

Switch (Config-If-Vlan1)#ip pim hello-interval 20

Switch (Config-If-Vlan1)#

## 6.3.20 ip pim ignore-rp-set-priority

**命令：ip pim ignore-rp-set-priority**

**no ip pim ignore-rp-set-priority**

**功能：**设置在进行 RP 选举时，仅使用 Hashing 机制而忽略 rp 的优先级。此命令是用于同较老的 Cisco IOS 版本交互。

**缺省情况：**不配置此选项

**参数：无**

**命令模式：**全局配置模式

**使用指南：**通常的，PIM 协议选择 RP 时会根据 RP 优先级进行选择，配置此命令后，PIM 将不根据 RP 优先级进行选择。除非网络中有较老的路由器，否则不建议配置此选项。

**举例：**

Switch (config)#ip pim ignore-rp-set-priority

Switch (config)#

## 6.3.21 ip pim jp-timer

**命令：ip pim jp-timer <*value*>**

**no ip pim jp-timer**

**功能：**设置加入/剪枝计时器值，no 操作恢复默认值

**参数：<*value*>**取值范围 10-65535s

**缺省情况：**60s

**命令模式：**全局配置模式

**使用指南：**该命令用于设置 PIM 协议定期发送的 JOIN-PRUNE 报文的发送间隔，默认为 60 秒，如果没有特别的原因，建议使用默认值。

**举例：**设置 jt 定时器的间隔

Switch (config)#ip pim jp-timer 59

Switch (config)#

## 6.3.22 ip pim multicast-routing

**命令：ip pim multicast-routing**

**no ip pim multicast-routing**

**功能：**全局启动 PIM-SM 协议；本命令的 no 操作全局关闭 PIM-SM 协议。

**参数：**无

**缺省情况：**缺省为不启动 PIM-SM 协议。

**命令模式：**全局配置模式

**使用指南：**本命令全局启动 PIM-SM，但是要让 PIM-SM 工作，还必须在接口上启动 PIM-SM

**举例：**全局启动 PIM-SM 协议。

Switch (config)#ip pim multicast-routing

Switch (config)#

## 6.3.23 ip pim neighbor-filter

**命令：ip pim neighbor-filter <*list-number*>**

**no ip pim neighbor-filter <*list-number*>**

**功能：**配置邻居访问列表。如果被列表过滤，如果已经同此邻居建立连接，则此连接马上被切断，如果没有建立连接，则这个连接不能建立。

**参数：<*list-number*>:**简单访问列表号，取值 1-99

**缺省情况：**没有 neighbor filter 设置

**命令模式：**接口配置模式

**使用指南：**ACL 的默认行为为 DENY。即如果配置 access-list 1，则 access-list 1 中的默认行为是 deny。在下面的举例中如果不配置 permit any-source，则 deny 10.1.4.10 0.0.0.255 的效果同于 deny any-source。

**举例：**设置接口 VLAN1 上 pim 邻居的过滤规则

Switch #show ip pim neighbor

Neighbor Interface Uptime/Expires Ver DR
Address Priority/Mode
10.1.4.10 Vlan1 02:30:30/00:01:41 v2 4294967294 / DR
Switch (Config-if-Vlan1)#ip pim neighbor-filter 2
Switch (config)#access-list 2 deny 10.1.4.10 0.0.0.255
Switch (config)#access-list 2 permit any-source
Switch (config)#show ip pim neighbor
Switch (config)#

## 6.3.24 ip pim register-rate-limit

**命令：ip pim register-rate-limit <*limit*>**
**no ip pim register-rate-limit**
**功能：**这个命令用于配置 DR 发送注册包的速率，单位是包/每秒。No 操作恢复默认值，这个配置的速率是指每一个（S，G）状态的不是整个系统范围内的。
**参数：**<***limit***> 取值范围 1-65535
**缺省情况：**不限制发注册包的速度
**命令模式：**全局配置模式
**使用指南：**该设置主要是为了防止 DR 受到攻击，因此采取限制发送 REGISTER 报文的方式进行保护，避免攻击过分冲击到 RP。
**举例：**设置发送注册报文的速率为 59 包/每秒
Switch (config)#ip pim register-rate-limit 59
Switch (config)#

## 6.3.25 ip pim register-rp-reachability

**命令：ip pim register-rp-reachability**
**no ip pim register-rp-reachability**
**功能：**用这个命令使得 DR 在进行注册过程中进行 RP 能不能到达的检测。
**参数：**无
**缺省情况：**默认情况不检测。
**命令模式：**全局配置模式。
**使用指南：**配置该命令后，DR 将对 RP 是否可达进行检测，如果 RP 不可达，DR 将不会试图发送注册报文。
**举例：**配置 DR 进行 RP 可达性检查。
Switch (config)#ip pim register-rp-reachability
Switch (config)#

## 6.3.26 ip pim register-source

**命令：ip pim register-source {<*A.B.C.D*> | <*ifname*> | vlan <*vlan-id*>}**

**no ip pim register-source**

**功能：**此命令用于配置 DR 发送的注册包的源地址，以覆盖默认的源地址，这个默认的源地址一般是源主机方向的 RPF 邻居

**参数：*<ifname>*：**接口名称；

***<vlan-id>*：**为 VLAN ID；

***<A.B.C.D>*：**设置的源 IP 地址 。

**缺省情况：**默认情况不配置。

**命令模式：**全局配置模式。

**使用指南：**no 操作恢复为默认值。此时语法为 no ip pim register-source，无需加 SOURCEADDRESS 和 IFNAME。配置的地址必须是 RP 发送的 Register-Stop 消息可达的。通常是个环回地址，但也可以是其他物理地址。这个地址必须是通过 DR 上的单播路由协议可广告的。

**举例：**配置 DR 发送的 register 报文的源地址

Switch (config)#ip pim register-source 10.1.1.1

Switch (config)#

## 6.3.27 ip pim register-suppression

**命令：ip pim register-suppression <*value*>**

**no ip pim register-suppression**

**功能：**用这个命令去配置注册抑制计时器的值，单位为秒。no 操作使恢复为默认值。

**参数：*<value>*，**时间值，取值范围 10-65535s。

**缺省情况：**60s。

**命令模式：**全局配置模式

**使用指南：**如果在 DR 上配置这个值，则是注册抑制计时器的值；RP 上的注册保活时间取默认保活时间（210s）和 3 倍注册抑制时间加 5 两个值中的较大者。所以如果在 RP 上配置这个值，而且没配置 ip pim rp-register-kat 命令，则此命令可能修改 RP 注册保活时间。

**举例：**配置注册抑制计时器的值为 10s。

Switch (config)#ip pim register-suppression 10

Switch (config)#

## 6.3.28 ip pim rp-address

**命令：ip pim rp- address <*A.B.C.D*> <*A.B.C.D/M*>**

**no ip pim rp-address <*A.B.C.D*> [<*A.B.C.D/M*>|<*all*>]**

**功能：**该命令为全局或某个组播地址范围的配置静态 RP，本命令的 no 操作为取消静态 RP 的配置。

**参数： *<A.B.C.D>*** RP 地址

***<A.B.C.D/M>***为希望成为某个范围的 RP

***<all>*** 所有范围

**缺省情况：**本交换机不是 RP 静态路由器。

**命令模式：**全局配置模式

**使用指南：**该命令为全局或某个组播地址范围的静态 RP 配置命令，用于配置 PIM-SM 静态 RP 的信息。需要注意的是，在进行 rp 计算时，优先在 BSR RP 集中选择，不成功才在静态 RP 集中选择。

**举例：**全局配置接口 VLAN1 为候选 RP 公告消息发送接口。

Switch (config)# ip pim rp-address 10.1.1.1 238.0.0.0/8

Switch (config)#

## 6.3.29 ip pim rp-candidate

**命令：ip pim rp-candidate {vlan<vlan-id> |loopback<index> |<ifname>} [<A.B.C.D/M>] [<priority>]**

**no ip pim rp-candiate**

**功能：**该命令为全局候选 RP 配置命令，用于配置 PIM-SM 候选 RP 的信息，以用于同其它候选 RP 竞争 RP 路由器；本命令的 no 操作为取消候选 RP 的配置。

**参数：*vlan-id***，为 VLAN ID；

**index**，为 Loopback 接口索引；

***ifname***，为指定接口名；

**A.B.C.D/M** 为 ip 前缀及掩码；

***<priority>***RP 选举的优先级，取值 0-255，默认为 192，数值越低优先级越高。

**缺省情况：**本交换机不是候选 RP 路由器。

**命令模式：**全局配置模式

**使用指南：**该命令为全局候选 RP 配置命令，用于配置 PIM-SM 候选 RP 的信息，以用于同其它候选 RP 竞争 RP 路由器，只有配置本命令，本交换机才是 RP 候选路由器。

**举例：**全局配置接口 VLAN 1 为候选 RP 公告消息发送接口。

Switch (config)# ip pim rp-candidate vlan1 100

Switch (config)#

## 6.3.30 ip pim rp-register-kat

**命令：ip pim rp-register-kat <*vaule*>**

**no ip pim rp-register-kat**

**功能：**用这个命令去配置 RP 上的（S，G）表项的 KAT（KeepAlive Timer）的值，单位为秒，no 操作恢复默认值。

**参数：<*vaule*>**，时间值，取值范围 1-65535s。

**缺省情况：**185s。

**命令模式：**全局配置模式

**使用指南：**用于配置 RP 上（S,G）表项保活时间，在此时间内 RP 上的（S,G）表项不会因为没有继续收到 REGISTER 报文而被删除。若直到保活时间超时也没有收到新的 REGISTER 报文，表项会被老化。

**举例：**配置 RP 上的(S,G)表项的 kat 的值是 180s。

Switch (config)#ip pim rp-register-kat 180

Switch (config)#

## 6.3.31 ip pim scope-border

**命令：ip pim scope-border [*<1-99 >*|*<acl_name>*]**

**no ip pim scope-border**

**功能：**配置、取消 PIM 的管理边界。

**参数：*<1-99 >***: 判断是否属于管理范围组地址的 ACL 号。

***<acl_name>***: 判断是否属于管理范围组地址的 ACL 名，应当是标准 ACL 名。

**缺省情况：**非管理边界，访问列表不指定表示使用默认的管理组范围。

**命令模式：**接口配置模式。

**使用指南：**配置 IP pim 的管理边界和使用的 ACL。组播数据不向 SCOPE-BORDER 扩散。

**举例：**

Switch(Config-if-Vlan2)#ip pim scope-border 3

## 6.3.32 ip pim sparse-mode

**命令：ip pim sparse-mode [passive]**

**no ip pim sparse-mode [passive]**

**功能：**在接口上启动 PIM-SM 协议；本命令的 no 操作在接口上关闭 PIM-SM 协议。

**参数：[passive]**表示不启动 PIM-SM（即 PIM-SM 不收发任何包），仅启动 IGMP（即收发 IGMP 报文）。

**缺省情况：**缺省为不启动 PIM-SM 协议。

**命令模式：**接口配置模式

**使用指南：**通过该命令启动接口的 PIM-SM 协议。

**举例：**在接口 VLAN 1 上启动 PIM-SM 协议。

Switch(config)#interface vlan 1

Switch(Config-If-Vlan1)#ip pim sparse-mode

Switch(Config-If-Vlan1)#

## 6.3.33 show ip pim bsr-router

**命令：show ip pim bsr-router**

**功能：**显示 BSR 地址。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示 PIM 协议维持的网络中的 BSR 路由器情况。

**举例：**show ip pim bsr-router

PIMv2 Bootstrap information

This system is the Bootstrap Router (BSR)

BSR address: 10.1.4.3 (?)

Uptime: 00:06:07, BSR Priority: 0, Hash mask length: 10

Next bootstrap message in 00:00:00

Role: Candidate BSR

State: Elected BSR

Next Cand_RP_advertisement in 00:00:58

RP: 10.1.4.3(Vlan1)

| 显示信息 | 解释 |
|---|---|
| BSR address | Bsr-router 地址 |
| Priority | Bsr-router 优先级 |
| Hash mask length | Bsr-router 哈希掩码长度 |
| State | 该候选 BSR 目前所处状态，Elected BSR 为选中 BSR |

## 6.3.34 show ip pim interface

**命令：show ip pim interface**

**功能：**显示 PIM 接口信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示 PIM 协议的接口信息。

**举例：**testS2(config)#show ip pim interface

| Address | Interface | VIFindex | Ver/ Mode | Nbr Count | DR Prior | DR |
|---|---|---|---|---|---|---|
| 10.1.4.3 | Vlan1 | 0 | v2/S | 1 | 1 | 10.1.4.3 |
| 10.1.7.1 | Vlan2 | 2 | v2/S | 0 | 1 | 10.1.7.1 |

| 显示信息 | 解释 |
|---|---|
| Address | 接口地址 |
| Interface | 接口名 |

| | |
|---|---|
| VIF index | 接口索引号 |
| Ver/Mode | pim 版本和模式，版本一般为 v2，sparse mode 显示 S， dense mode 显示 D |
| Nbr Count | 此接口上的邻居个数 |
| DR Prior | Dr 优先级 |
| DR | 此接口 DR 的地址 |

## 6.3.35 show ip pim mroute sparse-mode

**命令：show ip pim mroute sparse-mode [group <*A.B.C.D*>] [source <*A.B.C.D*>]**

**功能：**显示 pim sm 协议的组播路由表。

**参数：**group <A.B.C.D>：显示跟此组播地址相关的转发表项

source <A.B.C.D>：显示跟此源相关的转发表项

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**使用指南：**用于显示 PIM-SM 维护的组播路由信息。

**举例：**Switch#show ip pim mroute sparse-mode

IP Multicast Routing Table

(*,*,RP) Entries: 0

(*,G) Entries: 1

(S,G) Entries: 0

(S,G,rpt) Entries: 0

(*, 239.192.1.10)

RP: 10.1.6.1

RPF nbr: 10.1.4.10

RPF idx: Vlan1

Upstream State: JOINED

Local ..l.....

Joined .....

Asserted .....

Outgoing ..o.....

| 显示信息 | 解释 |
|---|---|
| Entries | 各种表项的个数 |
| RP | 所在共享树的 RP 地址 |
| RPF nbr | RP 方向或源方向的上游邻居 |
| RPF idx | RPF nbr 所在接口 |

| | |
|---|---|
| Upstream State | 上游方向状态，有 Joined（加入树，希望受到上游转发的数据），Not Joined（退出树，不希望收到上游转发的数据）两种状态，对于（S,G,rpt）表项还有 RPT Not Joined，Pruned，Not Pruned |
| Local | 本地加入接口，此接口收到 IGMP Join |
| Joined | PIM 加入接口，此接口收到 J/P 消息 |
| Asserted | Asserted 状态 |
| Outgoing | 组播数据最终出接口的 index 号，在此例中出接口的 index 为 2。可以通过命令 show ip pim interface 察看接口详细信息 |

## 6.3.36 show ip pim neighbor

**命令：show ip pim neighbor**

**功能：**显示路由器邻居。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示 PIM 协议维护的组播路由器邻居信息。

**举例：**s1(config)#show ip pim neighbor

| Neighbor Address | Interface | Uptime/Expires | Ver | DR Priority/Mode |
|---|---|---|---|---|
| 10.1.6.1 | Vlan1 | 00:00:10/00:01:35 | v2 | 1 / |
| 10.1.6.2 | Vlan1 | 00:00:13/00:01:32 | v2 | 1 / |
| 10.1.4.2 | Vlan3 | 00:00:18/00:01:30 | v2 | 1 / |
| 10.1.4.3 | Vlan3 | 00:00:17/00:01:29 | v2 | 1 / |

| 显示信息 | 解释 |
|---|---|
| Neighbor Address | 邻居地址 |
| Interface | 邻居所在接口 |
| Uptime/Expires | 运行时间/超时时间 |
| Ver | pim 版本，一般为 v2 |
| DR Priority/Mode | 此邻居发来 Hello 消息中的 DR 优先级以及此邻居是否该接口上的 DR |

## 6.3.37 show ip pim nexthop

**命令：show ip pim nexthop**

**功能：**显示 PIM 缓存的单播路有表中的下一跳路由器。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示 PIM 保存的下一跳路由器信息。

**举例：**

Switch(config)#show ip pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable

| Destination | Type | Nexthop Num | Nexthop Addr | Nexthop Ifindex | Nexthop Name | Metric | Pref | Refcnt |
|---|---|---|---|---|---|---|---|---|
| 192.168.1.1 | N... | 1 | 0.0.0.0 | 2006 | | 0 | 0 | 1 |
| 192.168.1.9 | ..S. | 1 | 0.0.0.0 | 2006 | | 0 | 0 | 1 |

| 显示信息 | 解释 |
|---|---|
| Destination | 下一条的目标地址 |
| Type | N：新创建的下一跳，还没有确定 RP 方向或者 S 方向 R：RP 方向 S：源方向 U：不可到达 |
| Nexthop Num | 下一跳计数 |
| Nexthop Addr | 下一跳地址 |
| Nexthop Ifindex | 下一跳所在接口索引 |
| Nexthop Name | 下一跳名字 |
| Metric | 到下一跳的路径损耗 Metric |
| Pref | 路径 Preference |
| Refcnt | 引用计数 |

## 6.3.38 show ip pim rp-hash

**命令：show ip pim rp-hash <*A.B.C.D*>**

**功能：**显示组 A.B.C.D 的汇合点 RP 地址。

**参数：**组地址。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示指定组地址对应的 RP 地址。

**举例：**testS2(Config-if-Vlan1)#show ip pim rp-hash 239.192.1.10

RP: 10.1.6.1

Info source: 10.1.6.1, via bootstrap

| 显示信息 | 解释 |
| --- | --- |
| RP | 被查询组的 RP |
| Info source | Bootstrap 消息的来源 |

### 6.3.39 show ip pim rp mapping

**命令：show ip pim rp mapping**

**功能：**显示组到 RP 影射和 RP 集。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示当前 RP 集及映射关系。

**举例：**testS2(Config-if-Vlan1)#show ip pim rp mapping

PIM Group-to-RP Mappings

Group(s): 224.0.0.0/4

RP: 10.1.6.1

Info source: 10.1.6.1, via bootstrap, priority 6

Uptime: 00:11:04

| 显示信息 | 解释 |
| --- | --- |
| Group(s) | RP 对应的组地址范围 |
| Info source | Bootstrap 消息的来源 |
| priority | Bootstrap 消息中的优先级 |

## 6.4 MSDP

### 6.4.1 cache-sa-holdtime

**命令：cache-sa-holdtime *<150-3600>***

**no cache-sa-holdtime**

**功能：**本命令配置 MSDP 缓存中 SA 表项的最大存活时间。

**参数：***seconds*：以秒为单位，范围为<150-3600>。

**命令模式：**MSDP 配置模式。

**缺省情况：**默认为 150。

**使用指南：**根据用户的需求来设定 MSDP 缓存的（S，G）表项的老化时间。

**举例：**

Switch(config)#router msdp

Switch(router-msdp)#cache-sa-holdtime 350

## 6.4.2 cache-sa-maximum

**命令：cache-sa-maximum <*sa-limit*>**

**no cache-sa-maximum**

**功能：**本命令配置指定 MSDP Peer 缓存 SA 条目的最大值。

**参数：<*sa-limit*>**：缓存 SA 条目的最大值，取值范围（1-75000）。

**命令模式：**MSDP 配置模式和 MSDP Peer 配置模式。

**缺省情况：**缺省情况下，缓存 SA 的最大值是 20000。

**使用指南：**为了防止路由器受到 DoS（Deny of Service）攻击，可以配置路由器缓存 SA 消息的最大数量。设置 MSDP 全局或指定 MSDP Peer 的缓存 SA 条目的最大数量为给定的数值。如果配置的值小于目前缓存中 SA 条目的数量，那么此配置无效。如果 Peer 下配置的数目大于 MSDP 全局下配置的数目，配置无效。如果 MSDP 下配置的条目小于 Peer 下已配置的条目，则 MSDP 下配置无效。

**举例：**

Switch(config)#router msdp

Switch(router-msdp)#cache-sa-maximum 50000

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)#cache-sa-maximum 22000

## 6.4.3 cache-sa-state

**命令：cache-sa-state**

**no cache-sa-state**

**功能：**本命令配置路由器的 SA 缓存状态。

**参数：**无。

**命令模式：**MSDP 配置模式和 MSDP Peer 配置模式。

**缺省情况：**在缺省情况下，SA 缓存处于使能状态。

**使用指南：**在路由器上配置缓存 SA 状态，可以使后续新加入的组不必等待下一次到达的 SA 消息，就可以从 SA 缓存中获得所有的活动源，加入到相应的源树。所有的 MSDP Speaker 上必须使能 SA-cache。no 命令取消配置路由器的 SA 缓存状态。需要注意的是，该命令与 sa-request 命令不能同时配置。

**举例：**

Switch(config)#router msdp

Switch(router-msdp)#no cache-sa-state

## 6.4.4 clear msdp peer

**命令： clear msdp peer {*peer-address*| *}**

**功能：**断开和指定 MSDP 对等体的 TCP 连接，清除该 Peer 的统计信息。

**参数：***peer-address*：对等体的 IP 地址；

* 断开和所有的 Peer 的连接。

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**如果有参数，断开与指定 MSDP 对等体的 TCP 连接，清除 TCP 连接信息，清除该 Peer 的统计信息；没有参数则清除所有 Peer 的连接和统计信息。

**举例：**

Switch#clear msdp peer *

## 6.4.5 clear msdp sa-cache

**命令： clear msdp sa-cache {group A.B.C.D|* }**

**功能：**清除 MSDP 缓存中的 Source-Active 信息：指定组的所有源对应的数据项，或者一个特定的（S，G）对应的所有的数据项。

**参数：***group-address：*组播组的 IP 地址，清除 Cache 中该组的（S，G）表项。

*：清除 cache 中的所有表项。

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**如果有参数，MSDP 缓存中指定组对应数据项中所有的非本地的 SA 数据项，若没有参数，清除 MSDP 缓存中所有的的非本地的 SA 数据项。

**举例：**

Switch#clear msdp sa-cache group 224.1.1.1

## 6.4.6 clear msdp statistics

**命令：clear msdp statistics {*peer-address*| *}**

**功能：**本命令清除 MSDP 统计信息，但不重启 MSDP 对等体的会话。

**参数：***peer-address*：对等体的 IP 地址；

* 断开和所有的 Peer 的连接。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#clear msdp statistics *

## 6.4.7 connect-source

**命令：connect- source < *IFNAME >< loopback>< vlan>***

**no connect- source**

**功能：**为所有的 MSDP Peer 设置使用哪个接口地址和对端 MSDP Peer 建立 MSDP 对等关系。

**参数：*< IFNAME >< loopback>< vlan>*：**接口名称、环回接口和 vlan 接口。

**命令模式：**MSDP 配置模式和 MSDP Peer 配置模式。

**缺省情况：**默认没有指定接口。

**使用指南：**本端路由器使用此接口的 IP 地址和 MSDP Peer 建立 MSDP 对等关系。**注意：**指定的 connect-source 地址必须与对端配置的 Peer 地址一致，否则将无法建立 TCP 连接。MSDP Peer 模式下的配置会覆盖在 MSDP 模式下的配置。no 命令取消配置的接口，重置此路由器上所有使用此接口的 MSDP 连接。

**举例：**

```
Switch(config)#router msdp
Switch(router-msdp)#connect-source vlan 2
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)#connect-source loopback 10
```

## 6.4.8 debug msdp all

**命令：debug msdp all**

**no debug msdp all**

**功能：**打开交换机的 MSDP 的所有调试开关；本命令的 no 操作为关闭该调试开关。

**命令模式：**特权用户配置模式。

**缺省情况：**缺省关闭交换机的 MSDP 的调试开关。

**使用指南：**用来打开交换机 MSDP 调试开关，可以显示交换机 MSDP 对等体的协议报文收发信息——packet，keepalive 报文收发信息——keepalive，事件信息——event，nsm 交互信息——nsm，计时器信息——timer，协议状态机信息——fsm，过滤策略信息——filter。

**举例：**

```
Switch#debug msdp all
```

## 6.4.9 debug msdp events

**命令：debug msdp events**

**no debug msdp events**

**功能：**打开/关闭 msdp events debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权模式。

**使用指南：**通过开启此开关，可以监控 msdp 协议运行中发生的事件信息。

**举例：**

```
Switch#debug msdp events
```

## 6.4.10 debug msdp filter

**命令：debug msdp filter**

**no debug msdp filter**

**功能：**打开/关闭 msdp 过滤策略信息的 debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权模式。

**使用指南：**通过开启此开关，可以监控 msdp 协议接收/发送报文的过滤信息。

**举例：**

Switch#debug msdp filter

## 6.4.11 debug msdp fsm

**命令：debug msdp fsm**

**no debug msdp fsm**

**功能：**打开/关闭 msdp 协议状态机 debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权模式。

**使用指南：**打开此开关，显示 MSDP 对等体的协议状态信息。

**举例：**

Switch#debug msdp fsm

## 6.4.12 debug msdp keepalive

**命令：debug msdp keepalive**

**no debug msdp keepalive**

**功能：**打开/关闭 msdp 协议 keepalive 报文信息的 debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权模式。

**使用指南：**通过开启此开关，可以监控 msdp 协议接收/发送 keepalive 报文的信息。

**举例：**

Switch#debug msdp keepalive

## 6.4.13 debug msdp nsm

**命令：debug msdp nsm**

**no debug msdp nsm**

**功能：**打开/关闭 msdp nsm debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权模式。

**使用指南：**通过开启此开关，可以监控 msdp 协议运行中与 nsm 模块的交互信息。

**举例：**

Switch#debug msdp nsm

## 6.4.14 debug msdp packet

**命令：debug msdp packet {send | receive}**

**no debug msdp packet {send | receive}**

**功能：**打开/关闭 msdp 协议报文发送/接收的 debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权模式。

**使用指南：**通过开启此开关，可以监控 msdp 协议收到和/或发送的报文。

**举例：**

Switch#debug msdp packet send

## 6.4.15 debug msdp peer

**命令：debug msdp peer A.B.C.D**

**no debug msdp peer**

**功能：**打开/关闭 msdp 指定对等体的所有 debug 调试信息开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权模式。

**使用指南：**可以根据需求打开指定 msdp 对等体的所有调试信息，不显示其他对等体的调试信息。该命令只对一个并且是最后指定的 msdp 对等体生效。

**举例：**

Switch#debug msdp peer 10.1.1.1

## 6.4.16 debug msdp timer

**命令：debug msdp timer**

**no debug msdp timer**

**功能：**打开/关闭 msdp 相关计时器 debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权模式。

**使用指南：**可以根据需求打开指定的计时器的调试信息。

**举例：**

Switch#debug msdp timer

## 6.4.17 default-rpf-peer

**命令：default-rpf-peer <peer-address> [ rp-policy <acl-list-number>|<word> ]**

**no default-rpf-peer**

**功能：**设置静态 RPF 对等体。

**参数：peer-address：**MSDP 对等体的 IP 地址。

**access-list-number：**ACL 号，仅支持 1-99 的标准 ACL。

**word：**标准 ACL 列表名称。

**命令模式：**MSDP 配置模式。

**缺省情况：**默认没有静态 RPF Peer。如果 peer 命令只配置了一个 MSDP 对等体，这个 MSDP 对等体将被作为缺省 RPF 对等体。

**使用指南：**当同时配置多个静态RPF对等体时，必须遵守如下两种配置方法：

都使用rp-policy参数：多个缺省RPF对等体同时起作用，并按照所配置的前缀列表对SA消息中的RP进行过滤，只接收RP地址通过过滤的SA消息。

都不使用 rp-policy 参数：按照配置的先后顺序，只有第一个连接状态是 UP 的静态 RPF 对等体是激活的，接收来自该对等体所有的 SA 消息，从其它静态 RPF 对等体接收到的 SA 消息将被丢弃。如果这个激活的静态 RPF 对等体失效（如配置取消或连接断开），仍然按照配置的先后顺序,重新选择第一个连接状态是 UP 的静态 RPF 对等体作为激活的静态 RPF 对等体。

**举例：**

Switch(config)#router msdp

Switch(router-msdp)#default-rpf-peer 10.0.0.1 rp-policy 10

## 6.4.18 description

**命令：description <*text*>**

**no description**

**功能：**本命令为指定的 MSDP Peer 添加描述性信息。

**参数：***text*：描述性文本，1-80 个字节。

**命令模式：**MSDP Peer 配置模式。

**缺省情况：**默认没有指定。

**使用指南：**本命令为指定的 MSDP Peer 添加描述性信息。管理员可以通过 MSDP 对等体的描述信息方便地区分不同的 MSDP 对等体，从而更好地管理 MSDP 对等体。no 命令删除为指定的 MSDP Peer 添加的描述性信息。

**举例：**

Switch(config)#router msdp

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)#description test-20

## 6.4.19 exit-peer-mode

**命令：exit-peer-mode**

**功能：**退出 MSDP Peer 配置模式，进入 MSDP 配置模式。

**命令模式：**MSDP Peer 配置模式。

**缺省情况：**无。

**使用指南：**如果已经对指定的 MSDP 对等体配置结束，需要退回到 MSDP 配置模式，可通过 exit-peer-mode 返回到 MSDP 配置模式。

**举例：**从 MSDP Peer 配置模式返回到 MSDP 配置模式。

Switch(config-msdp-peer)#exit-peer-mode

## 6.4.20 mesh-group

**命令：mesh-group <*name*>**

**no mesh-group <*name*>**

**功能：**本命令配置MSDP对等体为指定全连接组的成员，将同一MSDP对等体配置到多个全连接组时，最后一个有效。

**参数：**name：Mesh-group 名称。

**命令模式：**MSDP Peer 配置模式。

**缺省情况：**默认 MSDP 对等体不属于任何全连接组。

**使用指南：**全连接组可以减少 SA 消息的泛洪并简化 Peer-RPF 检查。

**举例：**

Switch(config)#router msdp

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)# mesh-group test-1

## 6.4.21 originating-rp

**命令：originating-rp <*interface-type*> < *interface-number*>**

**no originating-rp**

**功能：**本命令配置 Originating RP 地址，即配置 MSDP 使用指定接口的 IP 地址作为其 SA 消息中的 RP 地址。

**参数：<*interface-type*><*interface-number*>：**接口类型和接口号。

**命令模式：**MSDP 配置模式和 MSDP Peer 配置模式。

**缺省情况：**默认 SA 消息的 RP 地址为 PIM 配置的 RP 地址。

**使用指南：**创建 SA 消息时，MSDP 使用指定接口的 IP 地址作为其 SA 消息中的 RP 地址。当使用本命令指定的接口没有配置 IP 地址，或者为 down 时，就不再发送 SA 消息，此时如果

设备上配置有多个 RP 时，也不会选取其它的 RP 发送 SA 消息。所以必须保证指定接口的有效性，否则认为是配置问题。

**举例：**

Switch(config)#router msdp

Switch(router-msdp)#originating-rp vlan 20

## 6.4.22 peer

**命令：peer <*A.B.C.D*>**

**no peer <*A.B.C.D*>**

**功能：** 配置 MSDP 对等体，进入 MSDP Peer 模式下；本命令的 no 操作为取消配置的 MSDP 对等体。

**命令模式：**MSDP 配置模式。

**缺省情况：**缺省未配置 MSDP 对等体。

**使用指南：**设置指定地址作为为 MSDP 对等体地址，进入 Peer 模式。此时本地路由器在角色选择后进入与该对等体的 TCP 连接状态。可通过 no 操作取消配置的 MSDP 对等体，并中止与该对等体的连接，如已建立起 TCP 连接，将清除所有连接状态信息。**注意：**指定的 Peer 地址必须是对端的某个接口地址：如果对端配置了 Connect-source，那么 Peer 地址必须为 Connect-source 接口地址；对端没有指定 connect-source，配置的 Peer 地址为路由出接口地址，否则将无法建立 TCP 连接。

**举例：**在 MSDP 配置模式下配置 MSDP 对等体。

Switch(config-msdp)#peer 10.1.1.1

Switch(config-msdp-peer)#

## 6.4.23 redistribute

**命令： redistribute [list <*acl-list-number* | *acl-name*>]**

**no redistribute**

**功能：**本命令用来配置 SA 报文的创建规则。

**参数：***acl-number*：指定高级访问控制列表编号（100-199）。

*acl-name*：指定访问控制列表名称。

**命令模式：**MSDP 配置模式。

**缺省情况：**默认情况下，在创建 SA 报文时，对其通告的（S，G）项不作限制，通告域内的所有源。

**使用指南：**如果带 acl 参数的话，在 SA 报文中通告符合过滤条件的（S，G）项。不带 acl 参数，SA 消息将不通告任何源。

**举例：**

Switch(config)#router msdp

Switch(router-msdp)#redistribute list 130

## 6.4.24 remote-as

**命令：remote-as <*as-num*>**

**no remote-as <*as-num*>**

**功能：**本命令为指定的 MSDP Peer 配置 AS（自治域）号。

**参数：***as -num*：AS 号，取值范围（1 – 65535）。

**命令模式：**MSDP Peer 配置模式。

**缺省情况：**默认没有指定 AS 号被初始化为 0。

**使用指南：**此命令为指定的 Peer 设定 AS 号。no 命令为指定的 MSDP Peer 恢复默认的 AS（自治域）号。

**举例：**

Switch(config)#router msdp

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)# remote-as 20

## 6.4.25 router msdp

**命令：router msdp**

**no router msdp**

**功能：**打开交换机的 MSDP 协议，进入 MSDP 模式；本命令的 no 操作为关闭 MSDP 协议。

**命令模式：**全局配置模式。

**缺省情况：**交换机缺省不启动 MSDP 协议。

**使用指南：**本命令全局启动 MSDP 协议，但是要让 MSDP 协议工作，还必须同时配置 PIM SM 组播协议。

**举例：**在全局模式启动 MSDP 协议。

Switch(config)#router msdp

## 6.4.26 sa-filter

**命令：sa-filter{in | out}[ list <*acl-number* / *acl-name*> / rp-list <rp-acl-number | rp-acl-name>]**

**no sa-filter{in | out}[ list <*acl-number*/ *acl-name*> / rp-list <rp-acl-number | rp-acl-name>]**

**功能：**本命令用来配置接收或转发SA 报文的过滤规则，用来控制接收和转发的源信息。

**参数：**in：表示对来自指定MSDP 对等体的SA 报文进行过滤。

out：表示对转发给指定MSDP 对等体的SA 报文进行过滤。

*acl-number*：指定高级访问控制列表编号（100-199）。

*acl-name*：指定高级访问控制列表名称。

*rp-acl-number*：指定标准访问控制列表编号（1-99）。

*rp-acl-name*：指定标准访问控制列表名称。

如果不指定该参数，将过滤掉所有携带（S，G）项的SA 报文。

**命令模式**：MSDP 配置模式和 MSDP Peer 配置模式。

**缺省情况**：缺省情况下，接收或转发所有SA 报文，不对接收或转发的SA 报文进行过滤。

**使用指南**：在Peer下的配置会覆盖MSDP下的配置，也即如果在MSDP下和Peer下都配置了过滤策略，Peer下的生效。除了可以使用本命令控制SA 报文的接收和转发，还可以使用redistribute命令控制SA报文的创建。

**举例**：

Switch(config)#router msdp

Switch(router-msdp)#sa-filter in

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)#sa-filter in list 120

## 6.4.27 sa-request

**命令**：**sa-request**

**no sa-request**

**功能**：本命令配置路由器在接收到一个新组加入消息时，向其指定的 MSDP 对等体发送 SA 请求消息。

**参数**：无。

**命令模式**：MSDP Peer 配置模式。

**缺省情况**：默认不发送 SA Request 报文。

**使用指南**：本命令配置交换机（RP）向指定的 MSDP 对等体发送 SA 请求消息。当一个新组或新成员加入时，交换机向指定的 MSDP 对等体发送 SA 请求消息，该对等体回应其缓存的本地 SA 消息。RP 向 MSDP 对等体发送 SA 请求消息后，会收到对等体回应的 SA_response 报文，得到该对等体上所有活跃源（不包含对等体上通过 MSDP SA 学习的源信息）。如果 RP 配置了 SA 缓存状态，此配置无效。此命令与 sa-cache-state 命令互斥，如果该 MSDP 配置了 SA 缓存状态，则不能配置 sa-request,交换机会输出提示信息；同时注意，该命令只对 RP 有效。

**举例**：

Switch(config)#router msdp

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)# sa-request

## 6.4.28 sa-request-filter

**命令**：**sa-request-filter [list <*access-list-number* | *access-list-name*>]**

**no sa-request-filter [list <*access-list-number* | *access-list-name*>]**

**功能**：本命令过滤来自 MSDP 对等体的所有 SA request 消息。

**参数：***access-list-number*：ACL 号，仅支持 1-99 的标准 ACL。

*access-list-name*：ACL 列表名称。

**命令模式：**MSDP 配置模式。

**缺省情况：**缺省情况下，路由器接收其 MSDP 对等体发送的所有 SA 请求消息。

**使用指南：**如果没有 list 参数，过滤来自指定 MSDP 对等体的所有 SA request 消息；如果有 list 参数，首先检查 ACL 参数的合法性，过滤来自指定 MSDP 对等体的通过基本访问控制列表的组的 SA request 消息。

**举例：**

Switch(config)#router msdp

Switch(router-msdp)# sa-request-filter list 1

## 6.4.29 show msdp global

**命令：show msdp global**

**功能：**显示 MSDP 模式下的配置信息。

**命令模式：**特权和配置模式。

**使用指南：**显示 MSDP 模式下的配置信息，是否使能 MSDP 协议，是否有 Cache 和 MSDP Peer 缓存 SA 条目的最大值等信息。

**举例：**

Switch#show msdp global

Multicast Source Discovery Protocol (MSDP):

SA-Cached, Originator: Vlan2, Connect-Source: Vlan2

MAX External SA Entry: 200000

MAX Peer External SA Entry: 20000

TTL Threshold: 0

SA Entry Hold Time: 350

Filters:

Redistribute_filter: Not set

SA-filter:

[IN]: RP-list: None, SG-list: None

[OUT]:Not Configured

SA-Request-Filter: Not Configured

Default Peer:

Not Configured

Mesh Group:

test-1

显示项说明：

| 字段 | 说明 |
|---|---|
| SA-Cached | MSDP SA-Cached的状态。 |

| | |
|---|---|
| Originator | MSDP发起RP接口。 |
| MAX External SA Entry | MSDP模式下配置的最大表项数目。 |
| MAX Peer External SA Entry | 单个Peer的最大表项数目。 |
| TTL Threshold | TTL阀值。 |
| SA Entry Hold Time | MSDP缓存中外部组播源表项的存活时间。 |
| Redistribute_filter | 创建SA消息的过滤策略。 |
| SA-filter [IN \| OUT] | 接收转发SA报文的过滤策略。 |
| Default Peer | 静态RPF对等体。 |
| Mesh Group | 全连接组名称及其成员。 |

## 6.4.30 show msdp local-sa-cache

**命令：show msdp local-sa-cache**

**功能：**显示缓存中本地活动源信息。

**参数：**无。

**命令模式：**特权和配置模式。

**使用指南：**显示本地缓存SA信息。

**举例：**

Switch#show msdp local-sa-cache

MSDP Flags:

E - set MRIB E flag, L - domain local source is active,

EA - externally active source, PI - PIM is interested in the group,

DE - SAs have been denied.

Cache SA Entry:

| Source Address | Group Address | RP Address | TTL |
|---|---|---|---|
| 5.5.5.9 | 225.0.0.1 | 11.1.1.1 | 64 |
| 5.5.5.9 | 225.0.0.2 | 11.1.1.1 | 64 |
| 5.5.5.9 | 225.0.0.3 | 11.1.1.1 | 64 |
| 5.5.5.9 | 225.0.0.4 | 11.1.1.1 | 64 |

## 6.4.31 show msdp peer

**命令：show msdp peer {A.B.C.D }**

**功能：**显示 MSDP 模式下的配置信息。

**参数：A.B.C.D：**MSDP 对等体地址。

**命令模式：**特权和配置模式。

**使用指南：**显示 MSDP 模式下的配置信息。

**举例：**

```
Switch#show msdp peer 31.1.1.3
MSDP Peer 31.1.1.3 , AS 0 ,  Description:
Connection status:
  State: Established,      Resets: 0,
  Connection Source:   Not set   , Connect address: 31.1.1.1
  Uptime(Downtime): 00h:07m:53s,   SA messages received:16
  TLV messages sent/received:     8 /24
  SA messages incoming Rejected:     0
  SA messages outgoing Rejected:     0
SA Filtering:
  Input filter Not Configured
  Output filter Not Configured
SA-Requests:
  Input filter Not Configured
  Sending SA-Requests to peer: Disabled
Peer ttl threshold:     0
```

显示项说明：

| 字段 | 说明 |
|---|---|
| MSDP Peer | MSDP对等体IP地址。 |
| AS | MSDP对等体所属自治域标号。 |
| State | MSDP对等体状态。 |
| Connection source | 本地用于TCP连接的接口。 |
| Uptime(Downtime) | MSDP对等体up或者down的持续时长。 |
| Messages sent/received | 向对等体发送和从对等体接收报文数统计。 |
| SA Filtering | 当前配置的与对等体间的过滤策略。 |
| SA-Requests | 对SA请求配置的过滤策略。 |
| SAs learned from this peer | SA缓存中来自该MSDP对等体的SA数量。 |
| SAs limit | 与该MSDP对等体间配置的SA信息限制数目。 |

## 6.4.32 show msdp sa-cache

**命令：show msdp sa-cache { *<source-address>* [*<group-address>*] | as-num *<sas-number>* | peer *<peer-address>*| rpaddr *<rp-address>*}**

**功能：**显示 MSDP 缓存中外部活动源信息。

**参数：***source-address*：源地址；

*group-address*：组地址；

*as-number*：autonomous-system-number 自治域标号；

*peer-address*：Peer 地址；

*rp-address*：RP 地址。

**命令模式：**特权和配置模式。

**使用指南：**显示 MSDP 缓存中外部活动源信息。

**举例：**

Switch#show msdp sa-cache 30.30.30.1

MSDP Flags:

E - set MRIB E flag, L - domain local source is active,

EA - externally active source, PI - PIM is interested in the group,

DE - SAs have been denied.

Cache SA Entry:

(S:30.30.30.1, G: 224.1.1.1, RP: 10.1.1.2), AS: 0, 00h:00m:11s/00h:02m:19s

Learn From Peer:20.1.1.1, RPF Peer: 10.1.1.10

SA Received: 10 Encapsulated data received: 0

grp flags: None source flags: EA, DE

显示项说明：

| 字段 | 说明 |
|---|---|
| (S，G，RP) | 活动信源信息(S，G，RP)。 |
| AS Num | 自治域标号。 |
| update time | SA信息缓存时间。 |
| expire time | SA信息超时时间。 |
| Learn From Peer | 通过此Peer学习到该表项。 |
| RPF Peer | 此表项的RPF Peer。 |
| SA Received | 包含此表项的SA报文。 |
| Encapsulated data received | SA报文中封装的组播报文。 |
| grp flags | 表项中组播组的标志。 |
| source flags | 表项中组播源的标志。 |

## 6.4.33 show msdp sa-cache summary

**命令：show msdp sa-cache summary**

**功能：**显示 MSDP Cache 的概要信息。

**命令模式：**特权和配置模式。

**使用指南：**显示 MSDP Cache 的概要信息。

**举例：**

Switch#show msdp sa-cache summary

MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.

Cache SA Entry:
Total number of SA Entries = 1
Total number of Sources = 1
Total number of Groups = 1
Total number of RPs = 1

Originator-RP SA total RPF peer
10.1.1.2 1 10.1.1.10

AS-num SA total
0 1

显示项说明：

| 字段 | 说明 |
|---|---|
| Total number of SA Entries | Cache中SA表项的总数目。 |
| Total number of Sources | Cache中不同组播源的数目。 |
| Total number of Groups | Cache中不同组播组的数目。 |
| Total number of RPs | Cache中不同RP的数目。 |
| Originator-RP | 发起RP地址。 |
| SA total | 从此RP收到的SA报文的总数目。 |
| RPF peer | 该RP对应的RPF Peer地址。 |
| AS-num | 自治域号。 |

## 6.4.34 show msdp statistics

**命令：show msdp statistics peer [*Peer-address*]**
**功能：**显示指定 Peer 或者所有 Peer 的收发报文统计信息。
**参数：***Peer-address*：显示指定 Peer 收发报文的统计信息。
**命令模式：**特权和配置模式。
**使用指南：**显示指定 Peer 或者所有 Peer 的收发报文统计信息。
**举例：**
Switch#show msdp sta peer 2.2.2.4

MSDP Peer Statistics :

Peer 2.2.2.4 , AS is 0 , State is Inactive

TLV Rcvd : 76 total

39 keepalives, 37 SAs

0 SA Requests, 0 SA responses

TLV Send : 80 total

41 keepalives, 39 SAs

0 SA Requests, 0 SA responses

SA msgs : 37 received, 39 sent

显示项说明：

| 字段 | 说明 |
|---|---|
| Peer | MSDP对等体地址。 |
| AS | 自治域标号。 |
| State | MSDP对等体状态。 |
| TLV Rcvd | Peer接收的TLV类型和数目统计。 |
| TLV Send | Peer发送的TLV类型和数目统计。 |
| SA msgs | Peer接收和发送的SA信息数目统计。 |

## 6.4.35 show msdp summary

**命令：show msdp summary**

**功能：**显示 MSDP 的概要信息。

**命令模式：**特权和配置模式。

**使用指南：**显示 MSDP 的概要信息。

**举例：**

Switch#show msdp summary

Maximum External SA's Global : 20000

MSDP Peer Status Summary

| Peer Address | AS | State | Uptime/ Downtime | Reset Count | Peer Name | Active SA | Cfg.Max Cnt | Ext.SAs | TLV recv/sent |
|---|---|---|---|---|---|---|---|---|---|
| 2.2.2.4 | 0 | Established | THU JAN 01 00:00:00 | | | 10 | 0 | | 121/100 |

显示项说明：

| 字段 | 说明 |
|---|---|
| Peer Address | MSDP对等体IP地址。 |

| | |
|---|---|
| AS | MSDP对等体所属自治域标号。 |
| State | MSDP对等体状态。 |
| Uptime/Downtime | MSDP对等体up或者down的持续时长。 |
| Reset Count | MSDP对等体被重置次数。 |
| Peer Name | MSDP对等体描述。 |
| Active SA | 活动的组播源数目。 |
| TLV sent/received | 向对等体发送和从对等体接收报文数统计。 |

## 6.4.36 shutdown

**命令：shutdown**

**no shutdown**

**功能：**本命令关闭指定的 MSDP 对等体。

**参数：**无。

**命令模式：**MSDP Peer 配置模式。

**缺省情况：**缺省情况下，MSDP 对等体是使能的。

**使用指南：**如果要在一个 MSDP 对等体配置多条 MSDP 命令，并且不希望它开始作用，就可以用本命令来关闭该对等体，完成相应的配置后再去激活。关闭与指定 MSDP 对等体的 TCP 连接，并清除 MSDP 对等体的所有统计信息，但配置信息会保留。

**举例：**

Switch(config)#router msdp

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)#shutdown

## 6.4.37 ttl-threshold

**命令： ttl-threshold <*ttl*>**

**no ttl-threshold**

**功能：**本命令用来配置封装在 SA 报文中组播源的最小 TTL 值。

**参数：***ttl*：最小的 TTL 值，范围 1-255。

**命令模式：**MSDP 配置模式。

**缺省情况：**缺省情况下，TTL 阈值为 0，表示不进行 TTL 阀值过滤。

**使用指南：**组播源信息的扩散可以通过配置 TTL 阈值来控制。只有组播源的 TTL 不小于阈值时才封装在 SA 消息通告。

**举例：**

Switch(config)#router msdp

Switch(router-msdp)#ttl-threshold 10

# 6.5 ANYCAST RP

## 6.5.1 debug pim anycast-rp

**命令：debug pim anycast-rp**

**no debug pim anycast-rp**

**功能：**打开交换机 ANYCAST RP 功能的调试开关；本命令的 no 操作为关闭该调试开关。

**命令模式：**特权用户配置模式。

**缺省情况：**缺省关闭交换机的 ANYCAST RP 的调试开关。

**使用指南：**用来打开交换机 ANYCAST RP 调试开关，可以显示交换机处理 PIM 注册数据包信息——packet，事件信息——event。

**举例：**

Switch#debug pim anycast-rp

## 6.5.2 ip pim anycast-rp

**命令：ip pim anycast-rp**

**no ip pim anycast-rp**

**功能：**打开交换机的 ANYCAST RP 功能；本命令的 no 操作为关闭 ANYCAST RP 功能。

**命令模式：**全局配置模式。

**缺省情况：**交换机缺省不启动 ANYCAST RP。

**使用指南：**本命令全局启动 ANYCAST RP 协议，但是要让 ANYCAST RP 工作，还必须配置 self-rp-address 和 other-rp-address 集。

**举例：**在全局模式启动 ANYCAST RP。

Switch(config)#ip pim anycast-rp

## 6.5.3 ip pim anycast-rp

**命令：ip pim anycast-rp <anycast-rp-addr> <other-rp-addr>**

**no ip pim anycast-rp <anycast-rp-addr> <other-rp-addr>**

**功能：**配置 ANYCAST RP 地址（ARA）和与本路由器（作为 RP）通讯的其他 RP 的单播地址。本命令的 no 操作为取消配置的对应 RP 地址的某一其他 RP 单播地址。

**参数：*anycast-rp-addr***：RP 地址，允许该地址当前对应的候选接口不存在。

***other-rp-addr***：用于与本路由器（作为 RP）通讯的其它 RP 单播地址。

**命令模式：**全局配置模式。

**缺省情况：**缺省不配置。

**使用指南：**

1 在本路由器（作为 RP）上配置的 anycast-rp-addr 地址，实际上就是在网络中多个 RP 上配置的 RP 地址，对应候选 RP 接口(或者 Loopback 接口)的地址。配置上允许该地址当前对应的候选接口不存在。

2 在本路由器（作为 RP）上配置与本路由器通讯的其他 RP 的 other-rp-address。该单播地址标志其他 RP，用于与本地路由器之间的通讯。

3 当本路由器（作为 RP）收到从 DR 单播过来的注册报文，需要将该注册报文向网络中其他 RP 转发，使得网络中所有 RP 获得源（S,G）状态。转发时，本路由器修改注册报文目的地址为 other-rp-address。

4 对应一个 anycast-rp-addr 可以配置多个 other-rp-address，当收到 DR 单播过来的注册报文，依次向这些其他 RP 转发。

**举例：**在全局配置模式下配置 other-rp-address。

Switch(config)#ip pim anycast-rp 1.1.1.1 192.168.3.2

## 6.5.4 ip pim anycast-rp self-rp-address

**命令：ip pim anycast-rp self-rp-address *<self-rp-addr>***

**no ip pim anycast-rp self-rp-address**

**功能：**配置本路由器（作为 RP）的 self-rp-address。该地址唯一标志本路由器，用于与其他 RP 区分并进行通讯。本命令的 no 操作为取消配置的本路由器（作为 RP）用于与其它 RP 区分的单播地址。

**参数：*self-rp-addr***：本路由器与其他 RP 通讯的单播地址。

**命令模式：**全局配置模式。

**缺省情况：**缺省不配置 self-rp-address。

**使用指南：**

1 当本路由器（作为 RP）收到从 DR 单播过来的注册报文，需要将该注册报文向网络中其他 RP 转发，使得网络中所有 RP 获得源（S,G）状态。转发时，本路由器修改注册报文源地址为 self-rp-address。

2 当本路由器（作为 RP）收到从其他 RP 单播转发过来的注册报文，如注册报文目的地址为本路由器 self-rp-address，则建立（S,G）状态并反方向发送注册中止报文，注册中止报文目的地址即注册报文的源地址。

3 self-rp-address 应为本路由器上某个三层接口地址，但配置时我们允许此接口当前不存在。

**举例：**在全局配置模式下配置本路由器的 self-rp-address。

Switch(config)#ip pim anycast-rp self-rp-address 1.1.1.1

## 6.5.5 ip pim rp-candidate

**命令：ip pim rp-candidate {vlan<*vlan-id*> |loopback<*index*> |<*ifname*>} [<*A.B.C.D*>] [<*priority*>]**

**no ip pim rp-candidate**

**功能：**相对于原 PIM-SM 命令新增配置某 Loopback 接口作为候选 RP 接口；本命令的 no 操作为取消该 Loopback 接口作为候选 RP 接口。

**参数：*index*：**Loopback 接口索引，范围<1-1024>。

***vlan-id*:**为 VLAN ID。

***ifname*:**为指定接口名。

**A.B.C.D/M:** 为 ip 前缀及掩码。

***<priority>*:** RP 选举的优先级，取值 0-255，默认为 192，数值越低优先级越高。

**命令模式：**全局配置模式。

**缺省情况：**缺省不配置候选 RP 接口。

**使用指南：**为支持 ANYCAST RP 功能，新增允许配置 Loopback 接口作为候选 RP 接口，作为候选 RP 的接口是当前唯一的，并应当将该接口地址加入路由，使得 PIM 路由器可以找到距离自己最近的 RP。可以通过 no ip pim rp-candidate 命令取消候选 RP。

**举例：**在全局配置模式下配置 Loopback1 接口作为候选 RP 接口。

Switch(config)#ip pim rp-candidate loopback1

## 6.5.6 show debugging pim

**命令：show debugging pim**

**命令模式：**特权用户配置模式。

**使用指南：**anycast rp 当前调试开关状态。

**举例：**

Switch(config)#show debugging pim

Debugging status:

PIM anycast-rp debugging is on

## 6.5.7 show ip pim anycast-rp first-hop

**命令：show ip pim anycast-rp first-hop**

**命令模式：**特权和配置模式。

**使用指南：**显示 anycast rp 的状态信息，显示协议当前维护的在首跳 RP 上生成的 mrt 节点信息。

**举例：**

Switch(config)#show ip pim anycast-rp first-hop

IP Multicast Routing Table

(*,G) Entries: 0

(S,G) Entries: 1

(E,G) Entries: 0

INCLUDE (192.168.1.136, 224.1.1.1)

Local .l.....

| 显示信息 | 解释 |
| --- | --- |
| Entries | 各种表项的个数。 |
| INCLUDE | 首跳 RP 上创建的 mrt 信息。 |

## 6.5.8 show ip pim anycast-rp non-first-hop

**命令：show ip pim anycast-rp non-first-hop**

**命令模式：**特权和配置模式。

**使用指南：**显示 anycast rp 的状态信息，显示协议当前维护的在非首跳 RP 上生成的 mrt 节点信息。即由首跳 RP 收到注册报文后转发到本 RP 上，由此创建的 mrt 节点信息。

**举例：**

Switch(config)#show ip pim anycast-rp non-first-hop

IP Multicast Routing Table

(*,G) Entries: 0

(S,G) Entries: 1

(E,G) Entries: 0

INCLUDE (192.168.10.120, 225.1.1.1)

Local .l.....

| 显示信息 | 解释 |
| --- | --- |
| Entries | 各种表项的个数。 |
| INCLUDE | 首跳 RP 上创建的 mrt 信息。 |

## 6.5.9 show ip pim anycast-rp status

**命令：show ip pim anycast-rp status**

**命令模式：**特权和配置模式。

**使用指南：**显示 ANYCAST RP 的配置信息，是否在全局启动了 ANYCAST RP，是否配置 self-rp-address 和当前配置的 anycast rp 集列表。

**举例：**

Switch(config)#show ip pim anycast-rp status

Anycast RP status:
anycast-rp:Enabled!

self-rp-address:192.168.3.2

anycast-rp address: 1.1.1.1
other rp unicast rp address: 192.168.2.1
other rp unicast rp address: 192.168.5.1

anycast-rp address: 192.168.1.4
other rp unicast rp address: 192.168.2.1

---

| 显示内容 | 解释 |
|---|---|
| anycast-rp: | 全局 anycast rp 开关是否打开。 |
| self-rp-address: | 配置的 self-rp-address。 |
| anycast-rp address: | 配置的 anycast-rp-address。 |
| other rp unicast rp address: | 配置的对应上面 anycast-rp-address 的其他 RP 通讯地址。 |
| other rp unicast rp address: | 配置的对应上面 anycast-rp-address 的其他 RP 通讯地址。 |
| anycast-rp address: | 配置的 anycast-rp-address*。 |
| other rp unicast rp address: | 配置的对应上面 anycast-rp-address 的其他 RP 通讯地址*。 |

# 6.6 PIM-SSM

## 6.6.1 ip multicast ssm

**命令：ip multicast ssm {default|range <*access-list-number* >}**
**no ip multicast ssm**

**功能：**配置 pim ssm 组播组地址范围；本命令的 no 操作删除配置的 pim ssm 组播组。

**参数：** ***default :*** 表示 pim ssm 组播组地址取缺省范围 232/8。
***<access-list-number >***为要应用的访问列表号，取值范围 1-99。

**缺省情况：**缺省不配置 pim ssm 组地址范围。

**命令模式：**全局配置模式。

**使用指南：**

1 只有配置本命令后，pim ssm 才起作用。
2 配置本命令之前，必须确保 ip pim multicasting 配置成功。此命令不能与 DVMRP 一起运用。
3 Access-list 不能使用 ip access-list 命令所建立的访问列表，只使用 access-list 命令所建立的访问列表。
4 用户可以先执行此命令再配置对应的 acl；也可以在绑定情况下，删除对应 acl。绑定后，只有执行 no ip multicast ssm 才能将绑定关系解除。
5 如果要启用 ssm 功能，应该在网络边缘上相关交换机上配置此命令，比如有本地 igmp 加入的交换机（必须），以及在组播数据源端的 DR 或者在 RP 上（两者至少有一个）配置此命令，中间交换机则只需起 PIM-SM 即可。
**举例：**配置交换机启动 PIM-SSM，组地址范围是访问列表 23 指定的范围。

Switch (config)#ip multicast ssm range 23

# 6.7 DVMRP

## 6.7.1 debug dvmrp

**命令：debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]| nsm|mfc|mib|timer [probe [probe-timer|neighbor-expiry-timer] | prune [prune-expiry-timer|prune-retx-timer|graft-retx-timer] |route [report-timer|flash-upd-timer|route-expiry-timer|route-holdown-timer|route-burst-timer]] |packet [[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]] | all]**
**no debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]| nsm|mfc|mib|timer [probe [probe-timer|neighbor-expiry-timer] |prune [prune-expiry-timer|prune-retx-timer|graft-retx-timer] |route [report-timer|flash-upd-timer|route-expiry-timer|route-holdown-timer|route-burst-timer]] |packet [[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]] | all]**
**功能：**显示 DVMRP 协议的调试信息；本命令的 no 操作为关闭本调试开关。
**参数：**无。
**缺省情况：**不打开调试开关。
**命令模式：**特权用户配置模式。
**使用指南：**打开此开关，显示 DVMRP 协议运行的相关信息。
**举例：**

Switch # debug dvmrp packet in

## 6.7.2 ip dvmrp enable

**命令：ip dvmrp enable**

**no ip dvmrp**

**功能：**配置在接口上启动 DVMRP 协议；本命令的 no 操作在接口上关闭 DVMRP 协议。

**参数：**无。

**缺省情况：**不启动 DVMRP 协议。

**命令模式：**接口配置模式

**使用指南：**只有在接口运行 DVMRP 协议，接口才能处理 DVMRP 协议报文。

**举例：**在接口 VLAN 1 上启动 DVMRP 协议。

Switch (config)#interface vlan 1

Switch(Config-If-vlan1)#ip dvmrp enable

## 6.7.3 ip dvmrp metric

**命令：ip dvmrp metric <*metric_val*>**

**no ip dvmrp metric**

**功能：**配置接口 DVMRP report 报文度量值；本命令的 no 操作恢复为缺省值。

**参数：< *metric_val* >**为度量值，取值范围 1～31。

**缺省情况：**缺省值为 1。

**命令模式：**接口配置模式

**使用指南：**DVMRP report 报文包含的路由信息中包括一组源网络的地址和度量(Metric)的列表，配置了接口 DVMRP report 报文度量值后，将在所有从该接口接收到的路由条目上加上配置的接口度量值作为该路由的新度量值。度量值用于计算毒性反转，即确定上下游关系。如果本交换机上某条路由的度量值大于或等于 32，则说明该路由不可达。如果经计算后判断自己是某条路由的下游，则向上游发送包含该路由的 report 消息，该路由的 metric 在原基础上增加了 32，以表明自己是下游。

**举例：**配置接口 DVMRP report 报文度量值为 2。

Switch (config)#interface vlan 1

Switch(Config-If-Vlan1)#ip dvmrp metric 2

## 6.7.4 ip dvmrp multicast-routing

**命令：ip dvmrp multicast-routing**

**no ip dvmrp multicast-routing**

**功能：**全局启动 DVMRP 协议；本命令的 no 操作全局关闭 DVMRP 协议。

**参数：**无。

**缺省情况：**缺省不配置。

**命令模式：**全局配置模式

**使用指南：**必须全局运行该命令后，**dvmrp** 组播协议才能正常启动。

**举例：**

Switch (config)#ip dvmrp multicast-routing

## 6.7.5 ip dvmrp output-report-delay

**命令：ip dvmrp output-report-delay <*delay_val*> [<*burst_size*>]**

**no ip dvmrp output-report-delay**

**功能：**配置接口上发送 DVMRP report 报文的延时以及每次发送所发送的报文数量，本命令的 no 操作恢复默认值。

**参数：<*delay_val*>**为周期发送发送 DVMRP report 报文的延时，取值范围 1～5s。

**<*burst_size*>**为每次发送所发送的报文数量,取值范围 1~65535。

**缺省情况：**发送 DVMRP report 报文的延时隔缺省为 1s，缺省每次发送两个报文。

**命令模式：**接口配置模式

**使用指南：**通过设置适当的延时，可以避免报文的突发。

**举例：**

Switch (Config-If-vlan1)#ip dvmrp output-report-delay 1 1024

## 6.7.6 ip dvmrp reject-non-pruners

**命令：ip dvmrp reject-non-pruners**

**no ip dvmrp reject-non-pruners**

**功能：**配置接口上拒绝与 non pruning/grafting 的 DVMRP 路由器建立邻居关系，本命令的 no 操作恢复为可以建立邻居关系。

**参数：** 无。

**缺省情况：** 缺省不配置。

**命令模式：**接口配置模式

**使用指南：**使用本命令决定是否与不能 pruning/grafting 的 DVMRP 路由器建立邻接关系。

**举例：**

Switch (Config-If-vlan1)#ip dvmrp reject-non-pruners

## 6.7.7 ip dvmrp tunnel

**命令：ip dvmrp tunnel <*index*> <*src-ip*> <*dst-ip*>**

**no ip dvmrp tunnel {<*index*> |<*src-ip*> <*dst-ip*>}**

**功能：**本命令配置一条 DVMRP 隧道；本命令的 no 操作删除一条 DVMRP 隧道。

**参数：<*src-ip*>**是源 IP 地址，

**<*dst-ip*>**为远端邻居 IP 地址，

**<*index*>**为隧道的索引号，取值范围 1~65535。

**缺省情况：**缺省为不配置 DVMRP 隧道。

**命令模式：**全局配置模式

**使用指南：**因为不是所有的交换机都支持组播，DVMRP 支持隧道组播通信，隧道是在被不支持组播路由的交换机隔开的 DVMRP 交换机之间发送组播数据报的一种方法。它充当两个 DVMRP 交换机之间的虚拟网络。组播数据包被封装在单播数据包之内，直接发送到下一个支持组播的交换机。DVMRP 协议平等对待隧道接口与一般的物理接口。配置 no ip dvmrp multicast-routing 后将删除所有的 tunnel 配置。

**举例：**

Switch(config)#ip dvmrp tunnel 1 12.1.1.1 24.1.1.1

## 6.7.8 show ip dvmrp

**命令：show ip dvmrp**

**功能：**显示 DVMRP 协议信息。

**参数：** 无。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**使用指南：**本命令用于显示 DVMRP 协议的一些总的统计信息。

**举例：**

Switch#show ip dvmrp

DVMRP Daemon Start Time: MON JAN 01 00:00:09 2001

DVMRP Daemon Uptime: 17:37:03

DVMRP Number of Route Entries: 2

DVMRP Number of Reachable Route Entries: 2

DVMRP Number of Prune Entries: 1

DVMRP Route Report Timer: Running

DVMRP Route Report Timer Last Update: 00:00:56

DVMRP Route Report Timer Next Update: 00:00:04

DVMRP Flash Route Update Timer: Not Running

## 6.7.9 show ip dvmrp interface

**命令：show ip dvmrp interface [<*ifname*>]**

**功能：**显示 DVMRP 接口信息。

**参数：*<ifname>***为接口名称，即显示指定接口上配置的接口信息。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**举例：**

Switch #show ip dvmrp interface vlan4

| Address | Interface | Vif Index | Ver. | Nbr Cnt | Type | Remote Address |
|---|---|---|---|---|---|---|
| 13.1.1.3 | Vlan1 | 1 | v3.ff | 0 | BCAST | N/A |
| 10.1.35.3 | Vlan2 | 0 | v3.ff | 0 | BCAST | N/A |

| 显示信息 | 解释 |
|---|---|
| Address | 地址 |
| Interface | 接口对应的物理接口名 |
| Vif Index | 虚接口索引 |
| Ver | 接口支持的版本 |
| Nbr Cnt | 邻居数 |
| Type | 接口类型 |
| Remote Address | 远端地址 |

## 6.7.10 show ip dvmrp neighbor

**命令：show ip dvmrp neighbor [{*<ifname>* *<A.B.C.D>* [detail]}|{ *<ifname>*[detail]}|detail]**

**功能：**显示 DVMRP 邻居信息。

**参数：*<ifname>***为接口名称，即显示指定接口上的邻居信息。***<A.B.C.D>***为邻居地址。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**举例：**显示以太网口 VLAN 1 上的邻居信息。

Switch #show ip dvmrp neighbor interface vlan 1

| Neighbor Address | Interface | Uptime/Expires | Maj Ver | Min Ver | Cap Flg |
|---|---|---|---|---|---|
| 10.1.35.5 | Vlan2 | 00:00:16/00:00:29 | 3 | 255 | 2e |

| 显示信息 | 解释 |
|---|---|
| Neighbor Address | 邻居地址 |
| Interface | 发现该邻居的接口 |
| Uptime/Expires | 该邻居已存在的时间/距离超时还剩的时间 |
| Maj Ver | 主版本号 |
| Min Ver | 小版本号 |
| Cap Flg | 能力标记 |

## 6.7.11 show ip dvmrp prune

**命令：show ip dvmrp prune [{group *<A.B.C.D>* [detail]}|{source *<A.B.C.D/M>* group *<A.B.C.D>* [detail]}|{source *<A.B.C.D/M>* [detail] }|detail]**

**功能：**显示 DVMRP 报文转发项。

**参数：*<A.B.C.D>***为组 IP 地址；***<A.B.C.D/M>***为路由地址、掩码。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**使用指南：**本命令用于显示 DVMRP 组播转发项，即 dvmrp 协议所计算出来的组播转发表。

**举例：**

```
Switch#show ip dvmrp prune
Flags: P=Pruned,H=Host,D=Holddown,N=NegMFC,I=Init
Source          Mask Group          State  FCR Exptime  Prune/Graft
Address         Len  Address                Cnt          ReXmit-Time
13.1.1.0        24   239.0.0.1      ..... 1  01:59:56     Off
```

| 显示信息 | 解释 |
|---|---|
| Source Address | 源地址 |
| Mask Len | 掩码长度 |
| Group Address | 组地址 |
| State | 表项状态 |
| FCR Exptime | FCR 距离超时还剩的时间 |
| Prune/Graft ReXmit-Time | Prune 距离超时还剩下的时间以及 Graft 重传时间 |

## 6.7.12 show ip dvmrp route

**命令：show ip dvmrp route [{*<A.B.C.D/M>*[detail]}|{nexthop *<A.B.C.D>*[detail]}|{best-match *<A.B.C.D>* [detail]}|detail]**

**功能：**显示 DVMRP 路由信息。

**参数：*<A.B.C.D>***为下一跳地址以及目的地址；***<A.B.C.D/M>***为路由地址、掩码。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**使用指南：**本命令用于显示 DVMRP 路由表项；DVMRP 维护单独的单播路由表用于 RPF 检查。

**举例：**显示 DVMRP 路由信息。

```
Switch #show ip dvmrp route
Flags: N = New, D = DirectlyConnected, H = Holddown
Network          Flags Nexthop  Nexthop             Metric  Uptime    Exptime
                       Xface    Neighbor
10.1.35.0/24     .D.   Vlan2    Directly Connected    1     00:11:16  00:00:00
13.1.1.0/24      .D.   Vlan1    Directly Connected    1     00:10:22  00:00:00
```

| 显示信息 | 解释 |
|---|---|

| | |
|---|---|
| Network | 目标网段或地址及掩码 |
| Flags | 路由状态标记 |
| Nexthop Xface | 下一跳接口地址 |
| Nexthop Neighbor | 下一跳邻居 |
| Metric | 路由度量值 |
| Uptime | 路由已经存在的时间 |
| Exptime | 路由距离超时还剩下的时间 |

# 6.8 DCSCM

## 6.8.1 access-list(组播源控制)

**命令:** **access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}**
**no access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}**

**功能：**配置源受控组播访问列表，其 no 形式用于删除该访问列表。

**参数：** <5000-5099>：源受控访问列表号。
{deny|permit}：拒绝或允许。
<source>：组播源地址。
<source-wildcard>：组播源地址通配符。
<source-host-ip>：组播源主机地址。
<destination>：组播目的地址。
<destination-wildcard>：组播目的地址通配符。
<destination-host-ip>：组播目的主机地址。

**缺省情况：**无。

**命令模式：**全局配置模式

**使用指南：**组播源受控表项使用的 ACL 通过特定的 ACL 号 5000－5099 来控制，本命令用于配置这样的 ACL。组播源受控的 ACL 只需要配置要控制的源 IP 地址和目的 IP 地址（即组 IP 地址），其配置方式与其它 ACL 基本相同，可以采用通配符配置地址范围，也可以指定一个主机地址或所有地址，值得注意的是，这里的“所有地址”对组 IP 地址而言是指 224.0.0.0/4，而不是其它 access-list 下的 0.0.0.0/0。

**举例：**

Switch (config)#access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

## 6.8.2 access-list(组播目的控制)

**命令:** **access-list <6000-7999> {{{add | delete} profile-id WORD} | {{deny|permit} (ip) {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination}}**

**no access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip> {range <2-65535>|}}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip> {range <2-255>|}}|any-destination}**

**功能：** 配置目的受控组播访问列表，其 no 操作用于删除该访问列表。

**参数：** <6000-7999>：目的受控访问列表号。

{add | delete}：添加或者删除 profile 规则

{deny|permit}：拒绝或允许。

<source/M>：组播源地址和掩码长度。

<source-host-ip>：组播源主机地址。

<2-65535>：组播源主机范围

<destination/M>：组播目的地址和掩码长度。

<destination-host-ip>：组播目的主机地址。

<2-255>：组播目的主机范围。

**缺省情况：**无。

**命令模式：**全局配置模式

**使用指南：**组播目的受控表项使用的 ACL 通过特定的 ACL 号 6000－7999 来控制，本命令用于配置这样的 ACL。ip 组播目的受控的 ACL 只需要配置要控制的源 IP 地址和目的 IP 地址（即组 IP 地址），其配置方式与其它 ACL 基本相同，可以采用掩码长度配置地址范围，也可以指定一个主机地址或所有地址，值得注意的是，这里的“所有地址”对组 IP 地址而言是指 224.0.0.0/4，而不是其它 access-list 下的 0.0.0.0/0。并且可以采用添加删除 profile-id 规则来改变组播目的受控 ACL 访问列表。

**举例：**

Switch (config)#access-list 6000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

Switch (config)#access-list 6000 add profile-id 1

## 6.8.3 ip multicast destination-control

**命令: ip multicast destination-control**

**no ip multicast destination-control**

**功能：**使能组播目的控制访问列表，其 NO 形式为去使能。

**参数：**无

**缺省情况：**去使能。

**命令模式：**全局配置模式。

**使用指南：**该命令为使能组播目的控制访问列表，与 5.8.5 和 5.8.6 配合使用。

**举例：**

Switch (config)#ip multicast destination-control

Switch (config)#

## 6.8.4 ip multicast destination-control access-group

**命令: ip multicast destination-control access-group <6000-7999>**

**no ip multicast destination-control access-group <6000-7999>**

**功能：**配置端口使用的组播目的控制访问列表，其 NO 形式删除该配置。

**参数：**<6000-7999>：目的受控访问列表号。

**缺省情况：**不配置。

**命令模式：**端口配置模式

**使用指南：**该命令只有在启动了全局组播目的控制的情况下才起作用，配置该命令后，如果开启 IGMP-SNOOPING，对于向组播组添加该端口的情况，将按所配置的访问列表进行匹配，如匹配为 permit，该端口才会被添加，否则不能添加。

**举例：**

Switch (config)#interface ethernet 1/1/4

Switch (Config-If-Ethernet1/1/4)#ip multicast destination-control access-group 6000

Switch (Config-If-Ethernet1/1/4)#

## 6.8.5 ip multicast destination-control access-group (sip)

**命令: ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>**

**no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>**

**功能：**配置指定网段使用的组播目的控制访问列表，其 NO 形式删除该配置。

**参数：**<IPADDRESS/M>:IP 地址和掩码长度；

<6000-7999>：目的受控访问列表号。

**缺省情况：**不配置。

**命令模式：**全局配置模式。

**使用指南：**该命令只有在启动了全局组播目的控制的情况下才起作用，配置该命令后，如果开启 IGMP-SNOOPING 或启动了 IGMP，对于向组播组添加成员的情况，如果所发送的 IGMP-REPORT 的源 IP 地址配置了组播目的控制，将按所配置的访问列表进行匹配，如匹配为 permit，该端口才会被添加，否则不能添加。该命令在二层交换机上使用。如果使用此命

令之前，show ip igmp groups detail 中相应的组或者源已经建立，需到特权模式下使用命令 clear ip igmp group 清空相应组。

**举例：**

Switch (config)#ip multicast destination-control 10.1.1.0/24 access-group 6000

Switch (config)#

## 6.8.6 ip multicast destination-control access-group (vmac)

**命令: ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>**

**no ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>**

**功能：**配置指定 VLAN-MAC 使用的组播目的控制访问列表，其 NO 形式删除该配置。

**参数：**<1-4094>：VLAN-ID；

<macaddr>：发送 IGMP-REPORT 的源 MAC 地址，格式为“xx-xx-xx-xx-xx-xx”；

<6000-7999>：目的受控访问列表号。

**缺省情况：**不配置。

**命令模式：**全局配置模式。

**使用指南：**该命令只有在启动了全局组播目的控制的情况下才起作用，配置该命令后，如果开启 IGMP-SNOOPING，对于向组播组添加成员的情况，如果所发送的 IGMP-REPORT 的源 MAC 地址配置了组播目的控制，将按所配置的访问列表进行匹配，如匹配为 permit，该端口才会被添加，否则不能添加。

**举例：**

Switch (config)#ip multicast destination-control 1 00-01-03-05-07-09 access-group 6000

Switch (config)#

## 6.8.7 ip multicast policy

**命令: ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>**

**no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos**

**功能：**配置策略组播，其 NO 形式删除之。

**参数：**<IPADDRESS/M>：分别是组播的源地址、掩码长度和目的地址、掩码长度。

<priority>：设定的优先级，范围为<0-7>。

**缺省情况：**不配置。

**命令模式：**全局配置模式。

**使用指南：**可以通过该配置把通过本交换机的指定范围的组播数据包的优先级更改为指定的值，并且同时指定 TOS 为同样值。这里需要注意的是，对于 UNTAG 方式发出的报文，不会更改其优先级值。

**举例：**Switch (config)#ip multicast policy 10.1.1.0/24 225.1.1.0/24 cos 7

## 6.8.8 ip multicast source-control

**命令: ip multicast source-control**

**no ip multicast source-control**

**功能：**配置全局启动组播源受控，其 NO 形式恢复为不启动全局组播源控制。

**参数：**无。

**缺省情况：**不启动。

**命令模式：**全局配置模式。

**使用指南：**只有在启动全局组播源受控的情况下才能把源受控访问列表应用于端口，且只有在所有端口都不再配置源受控访问列表时才能配置为不启动全局组播源控制。配置该命令后，所有端口收到的组播数据，如果没有匹配的组播源受控表项，将被交换机丢弃，即只有匹配为 PERMIT 的组播数据才会接收和转发。

**举例：**

Switch (config)#ip multicast source-control

## 6.8.9 ip multicast source-control access-group

**命令: ip multicast source-control access-group <5000-5099>**

**no ip multicast source-control access-group <5000-5099>**

**功能：**配置端口使用的组播源控制访问列表，其 NO 形式删除该配置。

**参数：**<5000-5099>：源受控访问列表号。

**缺省情况：**不配置。

**命令模式：**端口配置模式。

**使用指南：**该命令只有在启动了全局组播源控制的情况下才能配置成功，配置该命令后，对于从该端口进入的组播数据报文将按所配置的访问列表进行匹配，如匹配为 PERMIT,该报文才会被接收和转发，否则报文被丢弃。

**举例：**

Switch (config)#interface ethernet1/1/4

Switch (Config-If-Ethernet1/1/4)#ip multicast source-control access-group 5000

## 6.8.10 multicast destination-control

**命令: multicast destination-control**

**no multicast destination-control**

**功能：**配置全局启动 IPv4 和 IPv6 组播目的受控，配置该命令后，IPv4 和 IPv6 组播目的受控全局同时生效。其 NO 形式恢复为不启动 IPv4 和 IPv6 全局组播目的控制。

**参数：**无。

**缺省情况：**不启动。

**命令模式：**全局配置模式。

**使用指南：**只有在启动全局组播目的受控的情况下才能使其它的目的控制配置生效，目的受控访问列表可以应用于端口、VLAN-MAC 和 SIP。配置该命令后，IGMP Snooping 和 IGMP 在收到 IGMP REPORT 后试图添加端口时，会按照上述规则进行匹配。

**举例：**

Switch (config)#multicast destination-control

Switch (config)#

## 6.8.11 profile-id(组播目的受控规则列表)

**命令: profile-id <1-50> {deny|permit} {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination}**

**no profile-id <1-50>**

**功能：**配置目的受控的 proflie 规则。其 no 操作用于删除该 profile 规则。

**参数：**<1-50>：profile-id 号。

{deny|permit}：拒绝或允许。

<source/M>：组播源地址和掩码长度。

<source-host-ip>：组播源主机地址。

<2-65535>：组播源主机范围

<destination/M>：组播目的地址和掩码长度。

<destination-host-ip>：组播目的主机地址。

<2-255>：组播目的主机范围

**缺省情况：**无。

**命令模式：**全局配置模式

**使用指南：**组播目的受控表项使用的 profile-list 通过特定的 profile-id 号 1－50 来控制，本命令用于配置这样的 profile 规则，供添加到 ACL 访问列表中进行使用。目的受控规则只需要配置要控制的源 IP 地址和目的 IP 地址（即组 IP 地址），其配置方式与直接配置 ACL 相同，可以采用掩码长度配置地址范围，也可以指定一个主机地址或所有地址，值得注意的是，这里的“所有地址”对组 IP 地址而言是指 224.0.0.0/4，而不是其它 access-list 下的 0.0.0.0/0。

**举例：**

Switch (config)# profile-id 1 deny ip any-source host-destination 224.1.1.2

## 6.8.12 show ip multicast destination-control

**命令：show ip multicast destination-control [detail]**

**show ip multicast destination-control interface *<interfacename>* [detail]**

**show ip multicast destination-control host-address *<ipaddress>* [detail]**

**show ip multicast destination-control *<vlan-id>* *<mac-address>* [detail]**

**功能：**显示组播目的控制配置。

**参数：**detail: 表示是否显示详细信息。

*<Interfacename>*：端口名或端口聚合名，如 Ethernet1/1/1、port-channel 1 或 ethernet 1/1/1。

*<ipaddress>*：主机IP 地址。

*<vlan-id>*：VLAN ID，取值范围<1-4094>。

*<mac-address>*：MAC地址，形式为“XX-XX-XX-XX-XX-XX”。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**通过该命令显示已经配置的组播目的控制规则，如包含 detail 选项，还包括具体使用的 access-list 的信息。

**举例：**

Switch (config)#show ip multicast destination-control

ip multicast destination-control is enabled

ip multicast destination-control 11.0.0.0/8 access-group 6003

ip multicast destination-control 1 00-03-05-07-09-11 access-group 6001

multicast destination-control access-group 6000 used on interface Ethernet1/1/13

switch(config)#

## 6.8.13 show ip multicast destination-control access-list

**命令：show ip multicast destination-control access-list**

**show ip multicast destination-control access-list <6000-7999>**

**功能：**显示配置的目的受控组播访问列表。

**参数：**<6000-7999>:访问列表号。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**通过该命令显示已经配置的目的受控组播访问列表。

**举例：**

Switch#show ip multicast destination-control access-list

access-list 6000 deny ip any-source any-destination

access-list 6000 deny ip any-source host-destination 224.1.1.1

access-list 6000 deny ip host-source 2.1.1.1 any-destination

access-list 6001 deny ip host-source 2.1.1.1 225.0.0.0 0.255.255.255

access-list 6002 permit ip host-source 2.1.1.1 225.0.0.0 0.255.255.255

access-list 6003 permit ip 2.1.1.0 0.0.0.255 225.0.0.0 0.255.255.255

## 6.8.14 show ip multicast destination-control filter-profile-list

**命令：show ip multicast destination-control filter-profile-list**

**show ip multicast destination-control filter-profile-list <1-50>**

**功能：**显示配置的目的受控 profile 组播规则列表。

**参数：**<1-50>：规则列表号。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**通过该命令显示已经配置的目的受控组播 profile 规则列表。

**举例：**

Switch#show ip multicast destination-control filter-profile-list

profile-id 1 deny ip any-source any-destination

profile-id 2 deny ip any-source host-destination 224.1.1.1

profile-id 3 deny ip host-source 2.1.1.1 any-destination

## 6.8.15 show ip multicast policy

**命令：show ip multicast policy**

**功能：**显示配置的组播策略。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**通过该命令显示已经配置的组播策略。

**举例：**

Switch#show ip multicast policy

ip multicast-policy 10.1.1.0/24 225.0.0.0/8 cos 5

## 6.8.16 show ip multicast source-control

**命令：show ip multicast source-control [detail]**

**show ip multicast source-control interface <Interfacename> [detail]**

**功能：**显示组播源控制配置。

**参数：**detail: 表示是否显示详细信息。

<Interfacename>：端口名，如 Ethernet1/1/1 或 ethernet 1/1/1。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**通过该命令显示已经配置的组播源控制规则，如包含 detail 选项，还包括具体使用的 access-list 的信息。

**举例：**

Switch#show ip multicast source-control detail

ip multicast source-control is enabled

Interface Ethernet1/1/13 use multicast source control access-list 5000

access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255

### 6.8.17 show ip multicast source-control access-list

**命令：show ip multicast source-control access-list**

**show ip multicast source-control access-list <5000-5099>**

**功能：**显示配置的源受控组播访问列表。

**参数：**<5000-5099>:访问列表号。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**通过该命令显示已经配置的源受控组播访问列表。

**举例：**

Switch#show ip multicast source-control access-list

access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255

## 6.9 IGMP

### 6.9.1 clear ip igmp group

**命令：clear ip igmp group [A.B.C.D | IFNAME]**

**功能：**删除指定组或指定接口上的组纪录。

**参数：**A.B.C.D 为指定组地址；IFNAME为指定接口地址。

**命令模式：**特权用户配置模式。

**使用指南：**快速删除组纪录，可以通过show 命令察看组纪录。

**举例：**删除所有组。

Switch#clear ip igmp group

**相关命令：show ip igmp group**

### 6.9.2 debug igmp event

**命令：debug igmp event**

**no debug igmp event**

**功能：**打开显示 IGMP 事件的调试开关；本命令的 no 操作为关闭本调试开关。

**参数：**无。

**缺省情况：**关闭。

**命令模式：**特权用户配置模式

**使用指南：**如果需要查看 IGMP 事件信息，则可以打开本调试开关。

**举例：**

Switch# debug igmp event

igmp event debug is on

Switch# 01:04:30:56: IGMP: Group 224.1.1.1 on interface vlan1 timed out

## 6.9.3 debug igmp packet

**命令：debug igmp packet**

**no debug igmp packet**

**功能：**打开显示 IGMP 报文信息的调试开关；本命令的 no 操作为关闭本调试开关。

**参数：**无。

**缺省情况：**关闭。

**命令模式：**特权用户配置模式

**使用指南：**如果需要查看 IGMP 报文信息，则可以打开本调试开关。

**举例：**

Switch# debug igmp packet

igmp packet debug is on

Switch #02:17:38:58: IGMP: Send membership query on dvmrp2 for 0.0.0.0

02:17:38:58: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0

.0.0

02:17:39:26: IGMP: Send membership query on vlan1 for 0.0.0.0

02:17:39:26: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0

.0.0

## 6.9.4 ip igmp access-group

**命令：ip igmp access-group {<*acl_num* | *acl_name*>}**

**no ip igmp access-group**

**功能：**配置接口对 IGMP 组的过滤条件；本命令的 no 操作取消过滤条件。

**参数：{<*acl_num* | *acl_name*>}**为 access list 的序号或名称，其中 ***acl_num*** 的取值范围为 1～99。

**缺省情况：**缺省为无过滤条件。

**命令模式：**接口配置模式

**使用指南：**可以配置接口对组进行过滤，允许或拒绝某些组的加入。

**举例：**配置接口 VLAN 1 接受组 224.1.1.1，拒绝组 224.1.1.2。

Switch (config)#access-list 1 permit 224.1.1.1 0.0.0.0

Switch (config)#access-list 1 deny 224.1.1.2 0.0.0.0

Switch (config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp access-group 1

## 6.9.5 ip igmp immediate-leave

**命令：ip igmp immediate-leave group-list {<number>|<name>}**

**no ip igmp immediate-leave**

**功能：**配置 IGMP 工作在立即离开模式，即当主机发出等价于离开一个组的成员资格报告时，路由器不发送查询，直接认为子网内没有该组的成员；本命令的 no 操作取消立即离开模式。

**参数：*<number>***为访问列表序号，取值为 1-99。

***<name>***为访问列表的名称。

**缺省情况：**出厂时接口缺省不配置立即离开的组。

**命令模式：**接口配置模式

**使用指南：**该命令仅使用在子网内只有一个主机的情况下。

**举例：**将访问列表 1 设为立即离开模式

Switch (Config-if-Vlan1)#ip igmp immediate-leave group-list 1

Switch (Config-if-Vlan1)#

## 6.9.6 ip igmp join-group

**命令：ip igmp join-group <*A.B.C.D* >**

**no ip igmp join-group <*A.B.C.D* >**

**功能：**配置接口加入某个 IGMP 组；本命令的 no 操作取消加入。

**参数：<*A.B.C.D* >**为组地址。

**缺省情况：**不加入组。

**命令模式：**接口配置模式

**使用指南：**当把交换机当做 HOST 时，本命令配置 HOST 加入某个组；即如果配置本接口加入组 224.1.1.1，则当交换机收到其它交换机发送过来的 IGMP 组查询时，将发送 IGMP 成员报告，报告中包含组 224.1.1.1。请注意本命令和 **ip igmp static-group** 命令的区别。

**举例：**在接口 VLAN 1 上配置加入组 224.1.1.1。

Switch (config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp join-group 224.1.1.1

## 6.9.7 ip igmp last-member-query-interval

**命令：ip igmp last-member-query-interval <interval>**

**no ip igmp last-member-query-interval**

**功能：**配置该接口下特定组查询发送的间隔；本命令的 no 操作取消用户手工配置的值，恢复缺省值。

**参数：** ***<interval>***为特定组查询的间隔，范围在 1000-25500ms；取值为 1000ms 的整数倍，即如果输入值不为 1000ms 的整数倍，则系统会自动将其转换为 1000ms 的整数倍。

**缺省情况：**缺省为 1000ms。

**命令模式：**接口配置模式

**举例：**使接口 VLAN 1 的 IGMP last-member-query-interval 配置为 2000。

Switch (config)#int vlan 1

Switch (Config-if-vlan1)#ip igmp last-member-query-interval 2000

## 6.9.8 ip igmp limit

**命令：ip igmp limit <state-count>**

**no ip igmp limit**

**功能：**配置该接口下允许保留的 IGMP 状态数目；本命令的 no 操作取消用户手工配置的值，恢复缺省值。

**参数：** ***<state-count>***接口最大保留的 IGMP 状态，范围在 1-65000。

**缺省情况：**缺省为 0，不做任何限制。

**命令模式：**接口配置模式

**使用指南：**当设置了最大状态 state-count 后，接口只保存不超过 state-count 个组和源的状态，如果到达 state-count 上限，之后接收到有关新的组的成员资格报告，不予处理。如果配置该命令前已经保存了一些 IGMP 组状态，则先删除所有的状态，然后立即发送 IGMP 普通查询收集不超过 state-count 个组的成员资格报告。静态组和静态源不在限制的范围内。

**举例：**使接口 VLAN 1 的 IGMP limit 配置为 4000。

Switch (config)#int vlan 1

Switch (Config-if-vlan1)#ip igmp limit 4000

## 6.9.9 ip igmp query-interval

**命令：ip igmp query-interval <*time_val*>**

**no ip igmp query-interval**

**功能：**配置周期发送 IGMP 查询消息的时间间隔；本命令的 no 操作恢复缺省值。

**参数：*<time_val>***为周期发送 IGMP 查询消息的时间间隔，取值范围 1～65535s。

**缺省情况：**周期发送 IGMP 查询消息的时间间隔缺省为 125s。

**命令模式：**接口配置模式

**使用指南：**当某个接口启动某种组播协议后，会周期性地在该接口上发送 IGMP 查询消息，本命令用于配置该查询周期时间。

**举例：**配置周期发送 IGMP 查询消息的时间间隔为 10s。

Switch (config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query-interval 10

## 6.9.10 ip igmp query-max-response-time

**命令：ip igmp query-max-response-time <*time_val*>**

**no ip igmp query-max-response-time**

**功能：**配置接口对 IGMP 查询的最大响应时间；本命令的 no 操作恢复缺省值。

**参数：<*time_val*>**为接口对 IGMP 查询的最大响应时间，取值范围 1～25s。

**缺省情况：**缺省为 10s。

**命令模式：**接口配置模式

**使用指南：**从交换机接收到一条查询消息后，主机会为其所属的每个组播组都设置一个计时器，计时器的值在0～最大响应时间中随机选定，当其中任何一个计时器的值减为0 时，主机就会发送该组播组的成员报告消息。合理设置最大响应时间，可以使主机快速响应查询信息，路由器也就能快速地掌握组播组成员的存在状况。

**举例：**配置对 IGMP 查询消息进行响应的最大时间为 20s。

Switch (config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query-max-response-time 20

## 6.9.11 ip igmp query-timeout

**命令：ip igmp query-timeout <*time_val*>**

**no ip igmp query-timeout**

**功能：**配置接口对 IGMP 查询的超时时间；本命令的 no 操作恢复缺省值。

**参数：<*time_val*>**为 IGMP 查询的超时时间，取值范围 60～300s。

**缺省情况：**缺省为 255s。

**命令模式：**接口配置模式

**使用指南：**在共享网络上，当存在多个运行IGMP的交换机时，将选举出其中一台交换机作为该共享网络上的查询器，其它交换机则起一个定时器监控查询器的状态；当经过查询超时时间仍未收到查询器发送的查询报文，则重新选举另一交换机成为新的查询器。

**举例：**配置接口对 IGMP 查询的超时时间 100s。

Switch (config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query-timeout 100

## 6.9.12 ip igmp robust-variable

**命令：ip igmp robust-variable <value>**

**no ip igmp robust-variable**

**功能：**设置鲁棒值，no 操作恢复默认值。

**参数：**value：取值范围<2-7>。

**命令模式：**接口配置模式

**缺省情况：**2

**使用指南：**推荐使用默认值。

**举例：**

Switch (config-if-vlan1)#ip igmp robust-variable 3

## 6.9.13 ip igmp static-group

**命令：ip igmp static-group <*A.B.C.D* > [source <*A.B.C.D* >]**

**no ip igmp static -group <*A.B.C.D* > [source <*A.B.C.D* >]**

**功能：**配置接口加入某个 IGMP 静态组；本命令的 no 操作取消加入。

**参数：<*A.B.C.D* >**为组地址；

**source <*A.B.C.D* >**表示配置 SSM 源地址。

**缺省情况：**不加入静态组。

**命令模式：**接口配置模式

**使用指南：**当配置某接口加入某个静态组后，则无论该接口下是否有实际的接收者，都将接收关于该静态组的组播包；即如果配置本接口加入静态组 224.1.1.1，则本接口一直会接收关于组 224.1.1.1 的组播报文，而不管接口下是否有接收者。请注意本命令和 **ip igmp join-group** 命令的区别。

**举例：**在接口 VLAN 1 上配置加入静态组 224.1.1.1。

Switch (config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp static-group 224.1.1.1

## 6.9.14 ip igmp version

**命令：ip igmp version <*version*>**

**no ip igmp version**

**功能：**配置接口上 IGMP 版本；本命令的 no 操作恢复为缺省值。

**参数：<*version*>**为配置的 IGMP 版本，目前支持版本 1 和版本 2，以及版本 3。

**缺省情况：**缺省为版本 2。

**命令模式：**接口配置模式

**使用指南：**该命令主要用于提供不同版本之间的前向兼容性；需注意的是版本 1 和版本 2 之间是不能互通的，因此在同网络内必须配置成相同版本的 IGMP。当接口相连的子网上还有其它未升级到 IGMPv3 的路由器需要一起参与子网的 IGMP 的成员资格收集时，建议将该接口配置为相应的版本。

**举例：**配置接口运行的 IGMP 为版本 1。

Switch (config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp version 1

## 6.9.15 show ip igmp groups

**命令：show ip igmp groups [<*A.B.C.D*>] [*detail*]**

**功能：**显示 IGMP 组信息。

**参数：< *A.B.C.D* >**为组地址，即查看指定组信息；

**detail** 表示详细方式组信息。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**举例：**

Switch (config)#show ip igmp groups

IGMP Connected Group Membership (2 group(s) joined)

| Group Address | Interface | Uptime | Expires | Last Reporter |
|---|---|---|---|---|
| 226.0.0.1 | Vlan1 | 00:00:01 | 00:04:19 | 1.1.1.1 |
| 239.255.255.250 | Vlan1 | 00:00:10 | 00:04:10 | 10.1.1.1 |

Switch#

| 显示信息 | 解释 |
|---|---|
| Group Address | 组播组 IP 地址 |
| Interface | 组播组所属的接口 |
| Uptime | 组播组已经存在的时间 |
| Expires | 组播组离超时所剩时间 |
| Last Reporter | 最后报告该组播组的主机 |

Switch (config)#show ip igmp groups 234.1.1.1 detail

IGMP Connect Group Membership (2 group(s) joined)

Flags: SG - Static Group, SS - Static Source, SSM - SSM Group, V1 - V1 Host Pres

ent, V2 - V2 Host Present

Interface: Vlan1

Group: 234.1.1.1

Flags:

Uptime: 00:00:19

Group Mode: INCLUDE

Last Reporter: 10.1.1.1

Exptime: stopped

Source list: (2 members S - Static)

| Source Address | Uptime | v3 Exp | Fwd | Flags |
|---|---|---|---|---|
| 1.1.1.1 | 00:00:19 | 00:04:01 | Yes | |
| 2.2.2.2 | 00:00:19 | 00:04:01 | Yes | |

| 显示信息 | 解释 |
|---|---|

| | |
|---|---|
| Group | 组播组 IP 地址 |
| Interface | 组播组所属的接口 |
| Flags | 组属性标记 |
| Uptime | 组播组已经存在的时间 |
| Group Mode | 组模式，包括 INCLUDE 和 EXCLUDE。V3 的组才有意义，V1 和 V2 的组都被认为是 EXCLUDE 模式 |
| Exptime | 组播组离超时所剩时间 |
| Last Reporter | 最后报告该组播组的主机 |
| Source Address | 该组下的源地址 |
| V3 Exp | 源的超时时间 |
| Fwd | 该源的数据是否要转发 |
| Flags | 源属性标记 |

## 6.9.16 show ip igmp interface

**命令：show ip igmp interface {vlan *<vlan_id>*|*<ifname>*}**

**功能：**显示接口上相关 IGMP 信息。

**参数：*<ifname>***为接口名称，即显示指定接口上的 IGMP 信息。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**举例：**显示以太网口 VLAN 1 上的 IGMP 信息。

```
Switch (config)#show ip igmp interface Vlan1
Interface Vlan1(2005)
  Index 2005
  Internet address is 10.1.1.2
  IGMP querier
  IGMP current version is V3, 2 group(s) joined
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 ms
  Group Membership interval is 260 seconds
  IGMP is enabled on interface
```

# 6.10 IGMP Snooping

## 6.10.1 clear ip igmp snooping vlan

**命令：clear ip igmp snooping vlan <1-4094> groups [A.B.C.D]**

**功能：**删除指定VLAN里的组纪录。

**参数：**<1-4094>为指定VLAN ID；A.B.C.D为指定组地址。

**命令模式：**特权用户配置模式。

**使用指南：**快速删除组纪录，可以通过show 命令察看组纪录。

**举例：**删除所有组。

Switch#clear ip igmp snooping vlan 1 groups

**相关命令：show ip igmp snooping vlan <1-4094>**

## 6.10.2 clear ip igmp snooping vlan <1-4094> mrouter-port

**命令：clear ip igmp snooping vlan <1-4094> mrouter-port [ethernet IFNAME | IFNAME]**

**功能：**删除指定VLAN里的mrouter 端口。

**参数：**<1-4094>为指定VLAN ID；ethernet为以太网端口名；IFNAME为端口名。

**命令模式：**特权用户配置模式。

**使用指南：**快速删除指定VLAN里的mrouter 端口，可以通过show 命令察看结果。

**举例：**删除VLAN 1 里的mrouter端口。

Switch# clear ip igmp snooping vlan 1 mrouter-port

**相关命令：**show ip igmp snooping mrouter-port

## 6.10.3 debug igmp snooping all/packet/event/timer/mfc/authentication/ha

**命令：debug igmp snooping all/packet/event/timer/mfc/authentication/ha**

**no debug igmp snooping all/packet/event/timer/authentication/ha**

**功能：**打开交换机的 IGMP Snooping 的调试开关；本命令的 no 操作为关闭该调试开关。

**命令模式：**特权用户配置模式

**缺省情况：**缺省关闭交换机的 IGMP Snooping 的调试开关。

**使用指南：**用来打开交换机 IGMP Snooping 调试开关，可以显示交换机处理 IGMP 数据包信息——packet， 事件信息——event， 计时器信息——timer， 下发硬件表项信息——mfc， 认证信息——authention，高可用信息——ha，所有 debug 信息——all。

## 6.10.4 ip igmp snooping

**命令：ip igmp snooping**

**no ip igmp snooping**

**功能：**打开交换机的 IGMP Snooping 功能；本命令的 no 操作为关闭 IGMP Snooping。

**命令模式：**全局配置模式

**缺省情况：**交换机缺省不启动 IGMP Snooping。

**使用指南：**打开交换机全局 IGMP Snooping 开关，即允许每个 VLAN 设置 IGMP Snooping 功能。No 操作关闭所有 VLAN 的 IGMP Snooping 功能，并关闭全局 IGMP Snooping 开关。

**举例：**在全局模式启动 IGMP Snooping。

Switch (config)#ip igmp snooping

## 6.10.5 ip igmp snooping proxy

**命令：ip igmp snooping proxy**

**no ip igmp snooping proxy**

**功能：** 开启 IGMP Snooping 代理功能，本命令的 no 操作为关闭 IGMP Snooping 代理功能。

**参数：** 无。

**命令模式：** 全局配置模式

**缺省情况：** 默认 IGMP Snooping 开启代理功能。

**举例：**

Switch(config)#no ip igmp snooping proxy

## 6.10.6 ip igmp snooping vlan

**命令：ip igmp snooping vlan *<vlan-id>***

**no ip igmp snooping vlan *<vlan-id>***

**功能：**打开指定 VLAN 的 IGMP Snooping 功能；本命令的 no 操作为关闭指定 VLAN 的 IGMP Snooping 功能。

**参数：*<vlan-id>***为 VLAN 的 ID 号，取值范围<1-4094>。

**命令模式：**全局配置模式

**缺省情况：**VLAN 缺省不打开 IGMP Snooping。

**使用指南：**设置某一个 VLAN 的 IGMP Snooping，要先打开全局 IGMP Snooping 开关。可通过 no ip igmp snooping vlan *<vlan-id>*关闭指定 VLAN 上的 IGMP Snooping 功能。

**举例：**在全局配置模式下启动 VLAN 100 的 IGMP Snooping 功能。

Switch (config)#ip igmp snooping vlan 100

## 6.10.7 ip igmp snooping vlan immediately-leave

**命令：ip igmp snooping vlan *<vlan-id>* immediately-leave**

**no ip igmp snooping vlan *<vlan-id>* immediately-leave**

**功能：**打开指定 VLAN 内 IGMP Snooping 协议的快速离开功能；本命令的 no 操作为关闭 IGMP Snooping 协议的快速离开功能。

**参数：*<vlan-id>***为指定的 VLAN 的 ID 号，取值范围<1-4094>。

**命令模式：**全局配置模式

**缺省情况：**缺省关闭该功能。

**使用指南：**打开 IGMP Snooping 协议的快速离开功能，可以加速对端口离开组播组的处理，不会发该组的指定组查询，直接删除。

**举例：**打开 VLAN 100 的 IGMP Snooping 快速离开功能。

Switch (config)#ip igmp snooping vlan 100 immediately-leave

## 6.10.8 ip igmp snooping vlan <id> immediately-leave mac-based

**命令：ip igmp snooping vlan <id> immediately-leave mac-based**

**no ip igmp snooping vlan <id> immediately-leave mac-based**

**功能：** 在交换机上面配置了此命令，表示当开启 igmp snooping 功能的交换机收到 leave 报文时，是根据 leave 报文中的源 mac 来删除已有的 igmp snooping 表项。即，当只有接收到此 leave 报文的端口、leave 报文的源 mac 和组播组 G，与已有的 igmp snooping 表项中的端口、点播 mac 和组播组项相同时，对应的 snooping 表项才会删除。倘若没有配置此命令，即表示，根据接收到此 leave 报文的端口和 leave 报文的组播组 G，来删除 igmp snooping 表项中的已有项。

**命令模式：** 全局配置模式。

**缺省情况：** 默认为 no。

**使用指南：** 要使此条命令生效，需要同时也配置在同一 vlan 下的 immediately-leave，这个时候才根据端口下的点播 mac 进行离开处理。

**举例：** 需要根据端口下的点播 mac 来删除表项时，使用如下配置：

switch(config)#ip igmp snooping vlan 12 immediately-leave

switch(config)#ip igmp snooping vlan 12 immediately-leave mac-based

## 6.10.9 ip igmp snooping vlan l2-general-querier

**命令：ip igmp snooping vlan < *vlan-id* > l2-general-querier**

**no ip igmp snooping vlan < *vlan-id* > l2-general-querier**

**功能：**将该 VLAN 设为二层普通查询者。

**参数：*vlan-id***:为 VLAN 的 ID 号，取值范围<1-4094>。

**命令模式：**全局配置模式

**缺省情况：**VLAN 缺省不是 IGMP Snooping 二层普通查询者。

**使用指南：**推荐一个网段配置一个二层普通查询者。如果设置此命令之前，该 VLAN 没有打开 IGMP Snooping 功能，应先打开该 VLAN 的 IGMP Snooping 功能。在关闭二层普通查询者功能时，不会关闭 IGMP Snooping 功能。该命令主要功能是定期发送普通查询来帮助此网段内的交换机学习 mrouter 端口。

**备注：**IGMP Snooping 中学习 mrouter 端口的途径有三种：

1 收到 IGMP 查询消息的端口

2 收到 DVMRP，PIM 等组播协议报文的端口

3 静态配置的端口

## 6.10.10 ip igmp snooping vlan l2-general-querier-source

**命令：ip igmp snooping vlan <vlanid> l2-general-querier-source <A.B.C.D>**

**no ip igmp snooping vlan <vlanid> l2-general-querier-source**

**功能：**配置 igmp snooping 二层查询者发送查询的源地址。

**参数：**<vlan-id>：指定 VLAN 的 VLAN ID,范围<1- 4094>

<A.B.C.D>：查询源地址

**命令模式：**全局模式

**缺省情况：**0.0.0.0

**使用指南：** Win2000/XP 不支持源地址为 0.0.0.0 的查询，所以没有配置二层查询的源地址，客户端在发送一个加入报文后，不再发送加入报文，一段时间后不能再接收到组播流量。

**举例：**

Switch(config)#ip igmp snooping vlan 2 l2-general-querier-source 192.168.1.2

## 6.10.11 ip igmp snooping vlan l2-general-querier-version

**命令：ip igmp snooping vlan <vlanid> l2-general-querier-version<version>**

**功能：**配置 igmp snooping 二层查询者发送查询的版本号。

**参数：**vlan-id：为 VLAN 的 ID 号，范围<1- 4094>

version：查询版本号，范围<1-3>

**命令模式：**全局模式

**缺省情况：**版本 3

**使用指南：**当交换机处于只支持 V1 或 V2 的环境中时，配置了二层查询者的 VLAN 只有发送相应的版本的查询才能被识别，该命令用来配置发送二层查询的版本号。

**举例：**

Switch(config)#ip igmp snooping vlan 2 l2-general-querier-version2

## 6.10.12 ip igmp snooping vlan limit

**命令：ip igmp snooping vlan < *vlan-id* > limit {group <*g_limit*> | source <*s_limit*>}**

**no ip igmp snooping vlan < *vlan-id* > limit**

**功能：**设置 IGMP Snooping 可加入组的个数和每个组中源个数的最大值。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>

***g_limit*：**<1-65535>，加入的组个数最大值

***s_limit*：**<1-65535>，每一个组中最多的源表项个数，包括 include 源和 exclude 源

**命令模式：**全局配置模式

**缺省情况：**默认最多 50 个组，每一个组最多可以存放 40 个源表项。

**使用指南：**当加入的组超过 limit，将会拒绝加入。这是为了防止恶意攻击。使用这个命令的前提是该 VLAN 打开了 IGMP Snooping 功能。No 操作恢复默认值，而不是设置为“无限制”。安全起见，此命令不会设置“无限制”。推荐使用默认值，如果三层 IGMP 在运行，请尽量保证此配置与 IGMP 的配置一致。

**举例：**Switch(config)#ip igmp snooping vlan 2 limit group 300

## 6.10.13 ip igmp snooping vlan interface (ethernet | port-channel|) IFNAME limit

**命令：ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit {group <1-65535>| source <1-65535>} strategy (replace | drop)**

**no ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit group source strategy**

**功能：**设置 IGMP Snooping 端口下可允许加入组的个数和每个组中源个数的最大值，及当达到上限值时的处理策略：包括替换和丢弃。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>

***ehternet*：**以太网端口名

***ifname*：**接口名

***port-channel:*** 端口汇聚

***<1-65535>：***允许加入的组个数最大值

***<1-65535>：***每一个组中最多的源表项个数，包括 include 源和 exclude 源

***replace ：***替换组、源信息

***drop：***丢弃新的组、源信息

**命令模式：**全局配置模式

**缺省情况：**默认无限制

**使用指南：**当端口下加入的组个数或该组中源个数超过 limit，将会根据配置的策略进行处理，若为 drop 则丢弃新加入的组、源信息；若为 replace，则从端口下找到一个动态的组、

源进行删除替换，加入新的组、源信息。使用这个命令的前提是该 VLAN 打开了 IGMP Snooping 功能。No 操作设置为“无限制”。

**举例：**

Switch(config)#ip igmp snooping vlan 2 interface ethernet 1/1/11 limit group 300 source 200 strategy replace

## 6.10.14 ip igmp snooping vlan mrouter-port interface

**命令：ip igmp snooping vlan <*vlan-id*> mrouter-port interface [<ehternet> | <port-channel>] <ifname>**

**no ip igmp snooping vlan <*vlan-id*> mrouter-port interface [<ehternet> | <port-channel>] <ifname>**

**功能：**设置 VLAN 的静态 mrouter 端口。no 操作取消设置。

**参数：*vlan-id***: VLAN ID 取值范围<1-4094>

***ehternet***：以太网端口名

***ifname***：接口名

***port-channel***：端口汇聚

**命令模式：**全局配置模式

**缺省情况：**VLAN 缺省没有静态 mrouter 端口。

**使用指南：**当一个端口同时成为静态 mrouter 端口和动态 mrouter 端口时，以静态 mrouter 端口为准。删除静态 mrouter 端口只能通过 no 操作进行。

**举例：**Switch(config)#ip igmp snooping vlan 2 mrouter-port interface ethernet1/1/13

Switch(config)#

## 6.10.15 ip igmp snooping vlan mrouter-port learnpim

**命令：ip igmp snooping vlan <*vlan-id*> mrouter-port learnpim**

**no ip igmp snooping vlan <*vlan-id*> mrouter-port learnpim**

**功能：**打开指定 VLAN 根据 pim 报文学习 mrouter-port 的功能；本命令的 no 操作为关闭指定 VLAN 根据 pim 报文学习 mrouter-port 的功能。

**参数：**<*vlan-id*>为指定的 VLAN 的 ID 号，取值范围<1-4094>。

**命令模式：**全局配置模式

**缺省情况：**默认开启该功能。

**使用指南：**打开指定 VLAN 根据 pim 报文学习 mrouter-port 的功能后，当端口收到 pim 协议报文后，会把该端口设置为 mrouter 端口，达到自动学习 mrouter 端口的目的。

**举例：**关闭 vlan 100 根据 pim 报文学习 mrouter-port 的功能。

Switch(config)#no ip igmp snooping vlan 100 mrouter-port learnpim

## 6.10.16 ip igmp snooping vlan mrouter-port flood

**命令：ip igmp snooping vlan <*vlan-id*> mrouter-port flood**

**no ip igmp snooping vlan <*vlan-id*> mrouter-port flood**

**功能：**打开指定 VLAN 根据 pim 报文学习 mrouter-port 的功能；本命令的 no 操作为关闭指定 VLAN 根据 pim 报文学习 mrouter-port 的功能。

**参数：**<*vlan-id*>为指定的 VLAN 的 ID 号，取值范围<1-4094>。

**命令模式：**全局配置模式

**缺省情况：**默认开启该功能。

**使用指南：**打开指定 VLAN 根据 pim 报文学习 mrouter-port 的功能后，当端口收到 pim 协议报文后，会把该端口设置为 mrouter 端口，达到自动学习 mrouter 端口的目的。

**举例：**关闭 vlan 100 根据 pim 报文学习 mrouter-port 的功能。

Switch(config)#no ip igmp snooping vlan 100 mrouter-port flood

## 6.10.17 ip igmp snooping vlan mrpt

**命令：ip igmp snooping vlan <*vlan-id*> mrpt <*value*>**

**no ip igmp snooping vlan <*vlan-id*> mrpt**

**功能：**设置 mrouter 端口的生存时间。

**参数：*vlan-id***: VLAN ID 取值范围<1-4094>

***value***：mrouter 端口生存时间，取值范围<1-65535>秒

**命令模式：**全局配置模式

**缺省情况：**255s。

**使用指南：**这个设置对动态 mrouter 端口有效，对静态 mrouter 端口无效。使用这个命令的前提是该 VLAN 的 IGMP Snooping 功能打开。

**举例：**Switch(config)#ip igmp snooping vlan 2 mrpt 100

## 6.10.18 ip igmp snooping vlan query-interval

**命令：ip igmp snooping vlan <*vlan-id*> query-interval <*value*>**

**no ip igmp snooping vlan <*vlan-id*> query-interval**

**功能：**设置查询间隔。

**参数：*vlan-id***: VLAN ID 取值范围<1-4094>

***value***：查询间隔，取值范围<1-65535>秒

**命令模式：**全局配置模式

**缺省情况：**125s。

**使用指南：**推荐使用默认值，如果三层 IGMP 在运行，请尽量保证此配置与 IGMP 的配置一致。

**举例：**

Switch(config)#ip igmp snooping vlan 2 query-interval 130

## 6.10.19 ip igmp snooping vlan query-mrsp

**命令：ip igmp snooping vlan <*vlan-id*> query-mrsp <*value*>**

**no ip igmp snooping vlan <*vlan-id*> query-mrsp**

**功能：**设置查询的最大响应时间，no 操作恢复默认值。

**参数：*vlan-id***: VLAN ID 取值范围<1-4094>

***value***：取值范围<1-25>秒

**命令模式：**全局配置模式

**缺省情况：**10s。

**使用指南：**推荐使用默认值，如果三层 IGMP 在运行，请尽量保证此配置与 IGMP 的配置一致。

**举例：**

Switch(config)#ip igmp snooping vlan 2 query-mrsp 18

## 6.10.20 ip igmp snooping vlan query-robustness

**命令：ip igmp snooping vlan <vlan-id> query-robustness <*value*>**

**no ip igmp snooping vlan <vlan-id> query-robustness**

**功能：**设置查询鲁棒值，no 操作恢复默认值。

**参数：*vlan-id***: VLAN ID 取值范围<1-4094>

***value***：取值范围<2-10>

**命令模式：**全局配置模式

**缺省情况：**2。

**使用指南：**推荐使用默认值，如果三层 IGMP 在运行，请尽量保证此配置与 IGMP 的配置一致。

**举例：**

Switch(config)#ip igmp snooping vlan 2 query-robustness 3

## 6.10.21 ip igmp snooping vlan report source-address

**命令：ip igmp snooping vlan *<vlan-id>* report source-address *<A.B.C.D>***

**no ip igmp snooping vlan *<vlan-id>* report source-address**

**功能：** 设置转发 IGMP 报文源地址，no 操作恢复默认值。

**参数：** ***vlan-id***： VLAN ID 取值范围<1-4094>；

***A.B.C.D***： IP 地址，允许为全零地址。

**命令模式：** 全局配置模式。

**缺省情况：** 不配置转发 IGMP 报文源地址。

**使用指南：**推荐使用默认值，如果需要使用 IGMP Snooping 的代理功能，可以配置转发 IGMP 报文源地址为全零地址；如果需要满足上游对 IGMP 报文源地址同网段检测，可以配置转发 IGMP 报文源地址与上游接口为同一网段地址，以通过地址检测。

**举例：**

Switch(config)#ip igmp snooping vlan 2 report source-address 10.1.1.1

## 6.10.22 ip igmp snooping vlan specific-query-mrsp

**命令：ip igmp snooping vlan <vlan-id> specific-query-mrsp <value>**

**no ip igmp snooping vlan <vlan-id> specific-query-mrspt**

**功能：**配置特定组/源查询的最大响应时间值，no 操作恢复默认值。

**参数：**<vlan-id>为指定的 VLAN 的 ID 号，取值范围<1-4094>

<value>为配置的最大响应时间值，单位秒，取值范围<1-25>，默认值为 1

**命令模式：**全局配置模式。

**缺省情况：**默认开启该功能。

**使用指南：**全局配置模式下开启 vlan snooping 后，输入该命令以配置特定组查询的最大响应时间。

**举例：**配置/取消 vlan 3 的特定组/源查询最大响应时间为 2s。

Swith(config)#ip igmp snooping vlan 3 specific-query-mrsp 2

Swith(config)#no ip igmp snooping vlan 3 specific-query-mrspt

## 6.10.23 ip igmp snooping vlan static-group

**命令：ip igmp snooping vlan <*vlan-id*> static-group <A.B.C.D> [source < A.B.C.D >] interface [ethernet | port-channel] <IFNAME>**

**no ip igmp snooping vlan <*vlan-id*> static-group <A.B.C.D> [source < A.B.C.D >] interface [ethernet | port-channel] <IFNAME>**

**功能：**端口上配置静态组，no 操作恢复默认值。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>。

**A.B.C.D：**IP 地址。

**命令模式：**全局配置模式。

**缺省情况：**不配置静态组。

**使用指南：**当添加的组源同时为静态组和动态组时，以静态组和源为准，添加时需要指明对应端口。

**举例：**

Switch(config)#ip igmp snooping vlan 1 static-group 224.1.1.1 source 192.168.1.1 interface ethernet 1/1/1

## 6.10.24 ip igmp snooping vlan passthrough-group

**命令：ip igmp snooping vlan <*vlan-id*> passthrough-group <A.B.C.D>**

**no ip igmp snooping vlan <*vlan-id*> passthrough-group <A.B.C.D>**

**功能：**配置透传组，no 操作恢复默认值。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>。

**A.B.C.D：**IP 地址。

**命令模式：**全局配置模式。

**缺省情况：**不配置透传组。

**使用指南：**配置为透传的组，相应组播流量会向 vlan 内所有端口转发。

**举例：**

Switch(config)#ip igmp snooping vlan 1 passthrough-group 224.1.1.1

## 6.10.25 ip igmp snooping vlan not-forward

**命令：ip igmp snooping vlan <*vlan-id*> not-forward**

**no ip igmp snooping vlan <*vlan-id*> not-forward**

**功能：**配置组播业务流量不向 mroute 口转发，no 操作恢复默认设置。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>。

**命令模式：**全局配置模式。

**缺省情况：**不开启。

**使用指南：**配置开启 not-forward 功能后，所有组播流量都不再向 mroute 端口转发。

**举例：**

Switch(config)#ip igmp snooping vlan 1 not-forward

## 6.10.26 ip igmp snooping vlan suppression-query-time

**命令：ip igmp snooping vlan <*vlan-id*> suppression-query-time <*value*>**

**no ip igmp snooping vlan <*vlan-id*> suppression-query-time**

**功能：**设置抑制查询时间值，no 操作恢复默认值。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>。

***value*：**取值范围<1-65535>。

**命令模式：**全局配置模式。

**缺省情况：**255s。

**使用指南：**此命令只能在 L2 普通查询者上设置。Suppression-query-time 的含义为：普通查询者在收到网段内三层 IGMP 发来的查询时，进入抑制状态维持的时间。此命令需要确保一个网段内的不同交换机 query-interval 配置一致。推荐使用默认值。

**举例：**

Switch(config)#ip igmp snooping vlan 2 suppression-query-time 270

## 6.10.27 show ip igmp snooping

**命令：show ip igmp snooping [vlan <*vlan-id*>]**

**参数：<*vlan-id*>**为指定要显示 IGMP Snooping 信息的 VLAN 号。

**命令模式：**特权和配置模式。

**使用指南：**如果不指定 VLAN 号，则显示全局 IGMP Snooping 开关有没有打开，三层组播协议是否在运行，以及都有哪些 VLAN 打开了 IGMP Snooping 功能，哪一个 VLAN 设置了 l2-general-querier 功能。如果指定 VLAN 号，则显示该 VLAN 的 IGMP Snooping 详细信息。

**举例：**

1.显示交换机的 IGMP Snooping 摘要信息。

Switch(config)#show ip igmp snooping

Global igmp snooping status: Enabled

L3 multicasting: running

Igmp snooping is turned on for vlan 1(querier)

Igmp snooping is turned on for vlan 2

---

| 显示内容 | 解释 |
|---|---|
| Global igmp snooping status | 交换机全局 IGMP Snooping 开关是否打开 |
| L3 multicasting | 交换机本机三层组播协议是否在运行 |
| Igmp snooping is turned on for vlan 1(querier) | 交换机上哪些 VLAN 开启了 IGMP Snooping 功能，是否为 l2-general-querier |

2.显示 VLAN 1 的 IGMP Snooping 详细信息。

Switch#show ip igmp snooping vlan 1

Igmp snooping information for vlan 1

Igmp snooping L2 general querier :Yes(COULD_QUERY)

Igmp snooping query-interval :125(s)

Igmp snooping max reponse time :10(s)

Igmp snooping robustness :2

Igmp snooping mrouter port keep-alive time :255(s)

Igmp snooping query-suppression time :255(s)

IGMP Snooping Connect Group Membership

Note:*-All Source, (S)- Include Source, [S]-Exclude Source

| Groups | Sources | Ports | Exptime | System Level |
|---|---|---|---|---|
| 238.1.1.1 | (192.168.0.1) | Ethernet1/1/8 | 00:04:14 | V2 |
| | (192.168.0.2) | Ethernet1/1/8 | 00:04:14 | V2 |

Igmp snooping vlan 1 mrouter port

Note:"!"-static mrouter port

!Ethernet1/1/2

| 显示内容 | 解释 |
|---|---|
| Igmp snooping L2 general querier | VLAN 是否启动 l2-general-querier 功能,并且显示 querier 的状态是 could-query 还是 suppressed |
| Igmp snooping query-interval | 该 VLAN 的查询间隔时间 |
| Igmp snooping max reponse time | 该 VLAN 的最大响应时间 |
| Igmp snooping robustness | 该 VLAN 设置的鲁棒值 |
| Igmp snooping mrouter port keep-alive time | 该 VLAN 动态 mrouter 的存活期限 |
| Igmp snooping query-suppression time | VLAN 作为 l2-general-querier 在抑制状态下的超时时间 |
| IGMP Snooping Connect Group Membership | 该 VLAN 的组成员关系，即端口和（S,G）的对应关系 |
| Igmp snooping vlan 1 mrouter port | 该 VLAN 的 mrouter 端口，包括静态的和动态的 |

# 6.11 IGMP Proxy

## 6.11.1 clear ip igmp proxy agggroup

**命令：clear ip igmp proxy agggroup**

**功能：**删除所有组纪录。

**参数：**无。

**命令模式：**特权用户配置模式。

**使用指南：**快速删除组纪录，可以通过show 命令察看组纪录。

**举例：**删除所有组。

Switch#clear ip igmp proxy agggroup

**相关命令：show ip igmp proxy upstream group**

## 6.11.2 debug igmp proxy all

**命令：debug igmp proxy all**

**no debug igmp proxy all**

**功能：**打开交换机的 IGMP Proxy 的所有调试开关；本命令的 no 操作为关闭该调试开关。

**命令模式：**特权用户配置模式。

**缺省情况：**缺省关闭交换机的 IGMP Proxy 的调试开关。

**使用指南：**用来打开交换机 IGMP Proxy 调试开关，可以显示交换机处理 IGMP 数据包信息——packet， 事件信息——event， 计时器信息——timer， 下发硬件表项信息——mfc。

**举例：**

Switch#debug igmp proxy all

## 6.11.3 debug igmp proxy event

**命令：debug igmp proxy event**

**no debug igmp proxy event**

**功能：**打开/关闭 igmp proxy event debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权模式和全局模式。

**使用指南：**通过开启此开关，可以监控 igmp proxy 协议运行中发生的事件信息。

**举例：**

Switch#debug igmp proxy event

## 6.11.4 debug igmp proxy mfc

**命令：debug igmp proxy mfc**

**no debug igmp proxy mfc**

**功能：**打开/关闭 igmp proxy 组播转发缓存 debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权模式和全局模式。

**使用指南：**打开此开关，显示生成和下发的组播表项的信息。

**举例：**

Switch#debug igmp proxy mfc

## 6.11.5 debug igmp proxy packet

**命令：debug igmp proxy packet**

**no debug igmp proxy packet**

**功能：**打开/关闭 igmp proxy 包的 debug 开关。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权模式和全局模式。

**使用指南：**通过开启此开关，可以监控 igmp proxy 协议收到和/或发送的报文。

**举例：**

Switch#debug igmp proxy packet

## 6.11.6 debug igmp proxy timer

**命令：debug igmp proxy timer**

**no debug igmp proxy timer**

**功能：**打开/关闭 igmp proxy 各个模块计时器。

**参数：**无。

**缺省情况：**不打开此开关。

**命令模式：**特权模式和全局模式。

**使用指南：**可以根据需求打开指定的计时器的调试信息。

**举例：**

Switch#debug ip igmp proxy timer

## 6.11.7 ip igmp proxy

**命令：ip igmp proxy**

**no ip igmp proxy**

**功能：**打开交换机的 IGMP Proxy 功能；本命令的 no 操作为关闭 IGMP Proxy 功能。

**命令模式：**全局配置模式。

**缺省情况：**交换机缺省不启动 IGMP Proxy。

**使用指南：**本命令全局启动 IGMP Proxy 协议，但是要让 IGMP Proxy 协议工作，还必须在接口模式配置一个上游接口和至少一个下游接口。

**举例：**在全局模式启动 IGMP Proxy。

Switch(config)#ip igmp proxy

## 6.11.8 ip igmp proxy aggregate

**命令：ip igmp proxy aggregate**

**no ip igmp proxy aggregate**

**功能：**设置 IGMP Proxy 非查询者下游接口也可以作为下发表项的出接口。

**命令模式：**全局配置模式。

**缺省情况：**非查询者下游接口不作为下发表项的出接口。

**使用指南：** 默认情况下，非查询者下游接口不作为下发表项的出接口，配置本命令后，所有下游接口都可以作为组播流量的出接口下发表项。

**举例：**

Switch(config)#ip igmp proxy aggregate

## 6.11.9 ip igmp proxy downstream

**命令：ip igmp proxy downstream**

**no ip igmp proxy downstream**

**功能：**打开指定接口的 IGMP Proxy 下游接口功能；本命令的 no 操作为关闭指定接口的 IGMP Proxy 下游接口功能。

**命令模式：**接口配置模式。

**缺省情况：**缺省不打开 IGMP Proxy 下游接口功能。

**使用指南：**设置指定接口的 IGMP Proxy 下游接口功能，但是要让 IGMP Proxy 协议工作，还必须通过 **ip igmp proxy upstream** 在其它接口上配置一个上游接口。可通过 no ip igmp proxy downstream 关闭指定接口上的 IGMP Proxy 下游功能。

**举例：**在接口配置模式下启动 interface vlan 2 的 IGMP Proxy 下游接口功能。

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ip igmp proxy downstream

## 6.11.10 ip igmp proxy limit

**命令：ip igmp proxy limit {group <*g_limit*> | source <*s_limit*>}**

**no ip igmp proxy limit**

**功能：**设置 IGMP Proxy 上游接口可加入组的个数和每个组中源个数的最大值。

**参数：*g_limit***：<1-500>，加入的组个数最大值。

***s_limit***：<1-500>，每一个组中最多的源表项个数。

**命令模式：**全局配置模式。

**缺省情况：**默认最多 50 个组，每一个组最多可以存放 40 个源。

**使用指南：**当加入的组超过 limit，将会拒绝加入。这是为了防止恶意攻击导致无限加入。

**举例：**

Switch(config)#ip igmp proxy limit group 30 source 20

## 6.11.11 ip igmp proxy multicast-source

**命令：ip igmp proxy multicast-source**

**no ip igmp proxy multicast-source**

**功能：**设置指定下游接口作为组播数据源；本命令的 no 操作删除配置的下游组播源接口。

**命令模式：**接口配置模式。

**缺省情况：**下游接口不作为组播数据源接口。

**使用指南：**配置指定下游接口作为组播数据源接口后，组播数据可以从该接口流入，建立表项时默认加入上游接口作为出接口。同时为了配合这一配置，直接与 IGMP PROXY 交换机相

连的组播路由器，应配置对应接口认为所有来源于本接口的源均是直连的，以确定 DR 或 ORIGINATOR 的身份。

**举例：**配置交换机下游接口 VLAN 1 启动 igmp proxy multicast-source。

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp proxy multicast-source

## 6.11.12 ip igmp proxy unsolicited-report interval

**命令：ip igmp proxy unsolicited-report interval <value>**

**no ip igmp proxy unsolicited-report interval**

**功能：**设置 IGMP Proxy 上游接口状态改变报告重传时间间隔。

**参数：*valut*** <1-5>，上游接口状态改变报告重传时间间隔为 1~5 秒。

**命令模式：**全局配置模式。

**缺省情况：**默认上游接口状态改变报告重传时间间隔为 1 秒。

**使用指南：**为了覆盖一个或多个路由器丢失状态变更报告的可能性，上游接口重传状态变更报告[Robustness Variable]次。本命令配置重传间隔。

**举例：**

Switch(config)#ip igmp proxy unsolicited-report interval 3

## 6.11.13 ip igmp proxy unsolicited-report robustness

**命令：ip igmp proxy unsolicited-report robustness <value>**

**no ip igmp proxy unsolicited-report robustness**

**功能：**设置 IGMP Proxy 上游接口状态改变报告重传次数。

**参数：*value*** ：<2~10>，上游接口状态改变报告重传次数为 2~10 次。

**命令模式：**全局配置模式。

**缺省情况：**默认上游接口状态改变报告重传次数为 2 次。

**使用指南：**为了覆盖一个或多个路由器丢失状态变更报告的可能性，上游接口重传状态变更报告[Robustness Variable]次。

**举例：**

Switch(config)#ip igmp proxy unsolicited-report robustness 3

## 6.11.14 ip igmp proxy upstream

**命令：ip igmp proxy upstream**

**no ip igmp proxy upstream**

**功能：**打开指定接口的 IGMP Proxy 上游接口功能；本命令的 no 操作为关闭指定接口的 IGMP Proxy 上游接口功能。

**命令模式：**接口配置模式。

**缺省情况：**缺省不打开 IGMP Proxy 上游接口功能。

**使用指南：**设置指定接口的 IGMP Proxy 上游接口功能，但是要让 IGMP Proxy 协议工作，还必须通过 **ip igmp proxy downstream** 在接口上配置至少一个下游接口。可通过 **no ip igmp proxy upstream** 关闭指定接口上的 IGMP Proxy 上游功能。

**举例：**在接口配置模式下启动 interface vlan 1 的 IGMP Proxy 上游接口功能。

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp proxy upstream

## 6.11.15 ip multicast ssm

**命令：ip multicast ssm {range <access-list-number> | default}**

**no ip multicast ssm**

**功能：**设置 ssm 组播组地址范围；本命令的 no 操作删除配置的 ssm 组播组。

**参数：**default：表示 ssm 组播组地址取缺省范围 232/8。

<access-list-number>：要应用的访问列表号，取值范围 1-99。

**命令模式：**全局配置模式。

**缺省情况：**ssm 组播组地址取缺省范围 232/8。

**使用指南：**该命令设置交换机对指定组地址范围内的(*,g)加入进行过滤，使之收不到申请加入组播组的流量。该命令统一了组播的 SSM 功能命令，同时对 IGMP PROXY 和 PIM 模块生效。需要注意的是，该命令不能与 DVMRP 一起使用。

**举例：**配置交换机启动 **ssm**，组地址范围是访问列表 23 指定的范围。

Switch(config)# access-list 23 permit host-source 224.1.1.1

Switch(config)#ip multicast ssm range 23

## 6.11.16 ip pim bsr-border

**命令：ip pim bsr-border**

**no ip pim bsr-border**

**功能：**设置指定 PIM 接口认为所有来源于本接口的组播数据源都是直连的；本命令的 no 操作取消 PIM 接口的组播数据源直连工作模式。

**命令模式：**接口配置模式。

**缺省情况：**接口不使用组播数据源直连工作模式。

**使用指南：**配置直接与 IGMP PROXY 交换机相连的 PIM 接口认为所有来源于本接口的源均是直连的，以确定 DR 和 ORIGINATOR 的身份。

**举例：**配置交换机 PIM 接口 VLAN 2 为 BSR-BORDER 接口，对于其所连接的网络到来的组播数据，BSR-BORDER 接口可以认为所连接的网络都是自己的直连网络，从而达到与异种组播协议（如 IGMP PROXY）衔接的目的。

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ip pim bsr-border

## 6.11.17 show debugging igmp proxy

**命令：show debugging igmp proxy**

**功能：**显示 IGMP proxy 当前调试开关状态。

**命令模式：**特权用户配置模式。

**使用指南：**IGMP proxy 当前调试开关状态。

**举例：**

Switch(config)#show debugging igmp proxy

IGMP PROXY debugging status:

IGMP PROXY event debugging is on

IGMP PROXY packet debugging is on

IGMP PROXY timer debugging is on

IGMP PROXY mfc debugging is on

## 6.11.18 show ip igmp proxy

**命令：show ip igmp Proxy**

**功能：**显示 igmp proxy 的配置信息。

**命令模式：**特权用户配置模式。

**使用指南：**显示 igmp proxy 的配置信息，是否在全局启动了 igmp proxy，是否配置了上游接口和下游接口。

**举例：**

Switch(config)#show ip igmp Proxy

IGMP PROXY MRT running: Enabled

Total active interface number: 2

Global igmp proxy configured: YES

Total configured interface number: 2

Upstream Interface configured: YES

Upstream Interface Vlan1(2005)

Upstream Interface configured: YES

Downstream Interface Vlan2(2006)

---

| 显示内容 | 解释 |
|---|---|
| IGMP PROXY MRT running | 协议是否运行 |
| Total active interface number | 配置的活动的上游接口和下游接口数目 |
| Global igmp proxy configured | 全局 igmp proxy 开关是否打开 |
| Upstream Interface configured | igmp proxy upstream 开关是否启动 |

| | |
|---|---|
| Upstream Interface Vlan | 上游接口所在接口 |
| Upstream Interface configured | igmp proxy downstream 开关是否启动 |
| Downstream Interface Vlan | 下游接口所在接口 |

## 6.11.19 show ip igmp proxy mroute

**命令：show ip igmp Proxy mroute**

**功能：**显示 igmp proxy mroute 的状态信息。

**命令模式：**特权用户配置模式。

**使用指南：**显示 igmp proxy mroute 的状态信息，显示协议当前维护的 mrt 节点信息。

**举例：**

Switch(config)#show ip igmp proxy mroute

IP Multicast Routing Table

(*,G) Entries: 0

(S,G) Entries: 2

(1.1.1.2, 225.0.0.1)

Local_include_olist ..l.....

Local_exclude_olist .....

Outgoing ..o.....

(1.1.1.3, 225.0.0.1)

Local_include_olist ..l.....

Local_exclude_olist .....

Outgoing ..o.....

| 显示信息 | 解释 |
|---|---|
| Entries | 各种表项的个数 |
| Local_include_olist | 本地 include 加入条目出接口的 index 号 |
| Local_exclude_olist | 本地 exclude 加入条目出接口的 index 号 |
| Outgoing | 对应的(S,G)组播数据出接口的 index 号 |

## 6.11.20 show ip igmp proxy upstream groups

**命令：show ip igmp proxy upstream groups {A.B.C.D}**

**命令模式：**特权用户配置模式。

**使用指南：**显示协议当前维护的上游接口的组播成员关系信息。不指定组显示所有组，指定组则只显示指定的组信息。

**举例：**

Switch(config)#show ip igmp proxy upstream groups

IGMP PROXY Connect Group Membership

| Groups | Filter-mode | source |
|---|---|---|
| 224.1.1.1 | INCLUDE | 192.168.1.136 |
| 226.1.1.1 | * | |

| 显示信息 | 解释 |
|---|---|
| Groups | 组播组地址 |
| Filter-mode | 该组播组的接收模式 |
| source | 该组播组的拥有的源 |

# 6.12 组播 VLAN

## 6.12.1 multicast-vlan

**命令：multicast-vlan**

**no multicast-vlan**

**功能：**启动一个 VLAN 的组播 VLAN 功能；本命令的 no 操作为关闭组播 VLAN 功能。

**参数：**无。

**命令模式：**VLAN 配置模式。

**缺省情况：**默认不启动组播 VLAN 功能。

**使用指南：**Private VLAN 不能启动组播 VLAN 功能。如果要禁止 VLAN 的组播 VLAN 功能，必须先删除组播 VLAN 的关联 VLAN 配置，注意默认 VLAN 不能配置该命令。且只允许在交换机上配置一个组播 VLAN。

**举例：**

Switch(config)#vlan 2

Switch(Config-Vlan2)#multicast vlan

## 6.12.2 multicast-vlan association

**命令：multicast-vlan association *<vlan-list>***

**no multicast-vlan association *<vlan-list>***

**功能：**将一个组播 VLAN 与多个 VLAN 关联；本命令的 no 操作取消关联关系。

**参数：*<vlan-list>***，与组播 VLAN 关联的 VLAN ID 列表，每个 VLAN 只能与一个组播 VLAN 关联。只有在 VLAN ID 列表中所列出的 VLAN 确实存在的情况下，关联才会成功。

**命令模式：**VLAN 配置模式。

**缺省情况：**默认不将组播 VLAN 与任何 VLAN 关联。

**使用指南：**如果一个 VLAN 与组播 VLAN 关联后，该 VLAN 内的端口被添加到组播 VLAN，如果本 VLAN 有端口点播组播 VLAN 的组播源的流量，那么组播数据将从组播 VLAN 发送到这个端口，而不需要将流量的入端口配置为 Trunk 端口，从而达到减少组播复制的目的。与组播 VLAN 关联的 VLAN 不能是 Private VLAN。只有在 VLAN 上启动了组播 VLAN 功能后，才能配置关联 VLAN。一个交换机上只能启动一个组播 VLAN。

**举例：**

Switch(config)#vlan 2

Switch(Config-Vlan2)# multicast-vlan association 3, 4

Switch(Config-Vlan2)#multicast-vlan

## 6.12.3 multicast-vlan association interface

**命令：multicast-vlan association interface (ethernet | port-channel|) IFNAME out-tag<tag id>**

**no multicast-vlan association interface (ethernet | port-channel|) IFNAME**

**功能：**将特定端口关联到组播 VLAN 上，这样关联到组播 VLAN 的端口上都能收到组播流量；no 命令取消关联端口关联关系。

**参数：** IFNAME：以太网端口或汇聚端口名。

tag-id:组播出口报文带上的 cvlan-tag

**命令模式：** VLAN 配置模式。

**缺省情况：** 无。

**使用指南：**

1.组播vlan'关联vlan'和'关联端口'是相互独立的，在出现交叉时互不影响。

2.端口是汇聚成员时不能关联，但关联端口可添加到port-group，此时撤销关联。

3.可配置端口类型：汇聚端口或普通端口，且端口只能是 ACCESS 模式。

4.要关联的端口不能属于组播 VLAN，同样，关联端口也不能划到组播 VLAN 下。

5.关联端口模式修改为非 ACCESS 模式时，不能修改模式。

**举例：** 假设 vlan2 是组播 VLAN。

Switch(config-vlan2)#multicast-vlan association interface ethernet 1/1/2

Switch(config-vlan2)#multicast-vlan association interface ethernet 1/1/2 out-tag 10

Switch(config-vlan2)#multicast-vlan association interface port-channel 2

Switch(config-vlan2)#no multicast-vlan association interface ethernet 1/1/2

Switch(config-vlan2)#no multicast-vlan association interface port-channel 2

## 6.12.4 multicast-vlan mode

**命令：multicast-vlan mode {dynamic| compatible}**

**no multicast-vlan mode {dynamic| compatible}**

**功能：**该命令是配置组播 vlan 的两种模式；本命令的 no 操作为取消组播 VLAN 的模式配置。

**参数：**dynamic：动态模式；

compatible：兼容模式。

**命令模式：**VLAN 配置模式。

**缺省情况：**默认两种模式都不属于。

**使用指南：**当配置 dynamic 模式时，在下发组播表项时，不再自动添加 mrouter 端口；当配置 compatible 模式时，report 报文不再转发到 mrouter 端口，默认不配置的情况下，在下发组播表项时，会添加 mrouter 端口，并且收到 report 报文会向 mrouter 端口转发。

**举例：**

Switch(Config-Vlan2)#multicast vlan mode dynamic

## 6.12.5 switchport association multicast-vlan

**命令：switchport association multicast-vlan <vlan-id> out-tag <tag-id>**

**no switchport association multicast-vlan <vlan-id>**

**功能：** 将一个端口与指定的组播 VLAN 关联；本命令的 no 操作取消关联关系。

**参数：** <vlan-id>，与端口关联的组播 vlan，每个端口只能与一个组播 VLAN 关联。只有组播 VLAN 确实存在的情况下，关联才会成功。

<tag-id>，取值范围<1-4094>，指定了从此关联端口转发的组播数据所带的 vlan tag，只有该关联端口 tag allow 该组播 vlan，此 tag-id 才会生效。

**命令模式：** 端口配置模式。

**缺省情况：** 默认该端口不与任何组播 vlan 关联。

**使用指南：** 如果一个端口关联了组播 vlan 后，该端口便被添加到组播 VLAN，如果此端口点播了组播 VLAN 的组播源的流量，那么组播数据将从组播 VLAN 发送到这个端口，而不需要将流量的入端口配置为 Trunk 端口，从而达到减少组播复制的目的。如果该关联端口是 trunk 端口并且 allow 了该组播 vlan，则组播流量便会带着此命令中指定的 vlan tag 转发出去。这种以 trunk 端口关联组播 vlan 的功能可以支持该下游端口通过二层网络连接下游点播端的需求而不再局限于该下游端口需要直连点播端的限制。只有配置了组播 VLAN 功能后，才能配置关联端口。

**举例：**

Switch(config)#vlan 2

Switch(Config-Vlan2)#multicast-vlan

Switch(config)#interface ethernet 1/1/1

Switch(config-if-ethernet1/1/1)#switchport mode trunk

Switch(config-if-ethernet1/1/1)#switchport association multicast-vlan 2 out-tag 5

# 第 7 章 安全功能命令

## 7.1 ACL

### 7.1.1 absolute-periodic/periodic

**命令：[no] absolute-periodic {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <start_time> to {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <end_time>**

**[no] periodic {{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday} | daily | weekdays | weekend} <start_time> to <end_time>**

**功能：** 定义一周内的各种不同要求的时间范围，每周都循环这个时间。

**参数：**

**Friday** Friday(星期五)

**Monday** Monday (星期一)

**Saturday** Saturday (星期六)

**Sunday** Sunday (星期日)

**Thursday** Thursday （星期四）

**Tuesday** Tuesday (星期二)

**Wednesday** Wednesday (星期三)

**daily** Every day of the week （每天）

**weekdays** Monday thru Friday （星期一到星期五）

**weekend** Saturday and Sunday （星期六到星期日）

**start_time** 开始时间点，HH:MM:SS (小时：分钟：秒)

**end_time** 结束时间点，HH:MM:SS (小时：分钟：秒)

注：time-range轮询时间是 1 分钟一次，所以时间的误差<=1 分钟。

**命令模式：**时间范围模式

**缺省情况：**没有时间范围配置

**使用指南：**周期性的时间和日期，周期是定义每周的 1～6 和周日的具体时间段，可以同时配置多个周期性时段，它们之间是“或”的关系。它的形式是：

day1 hh:mm:ss To day2 hh:mm:ss 或者

{[day1+day2+day3+day4+day5+day6+day7]|weekend|weekdays|daily} hh:mm:ss To hh:mm:ss

**举例：**使能在Tuesday到Saturday内的 9:15:30 到 12:30:00 时间段内配置生效

Switch(config)#time-range admin_timer

Switch(Config-Time-Range-admin_timer)#absolute-periodic tuesday 9:15:30 to saturday 12:30:00

使能在Monday、Wednesday、Friday和Sunday四天内的 14:30:00 到 16:45:00 时间段配置生效
Switch (Config-Time-Range-admin_timer)#periodic monday wednesday friday sunday 14:30:00 to 16:45:00

## 7.1.2 absolute start

**命令：[no]absolute start *<start_time>* *<start_data>* [end *<end_time>* *<end_data>*]**
**功能：**定义一个绝对时间段,这个时间段是根据本设备的时钟运行。
**参数：*start_time*** ：开始时间点，HH:MM:SS (小时：分钟：秒)
***end_time*** ：结束时间点，HH:MM:SS (小时：分钟：秒)
***start_data*** ：开始日期，格式是，YYYY.MM.DD（年.月.日） ***end_data*** ：结束日期，格式是，YYYY.MM.DD（年.月.日）
注：time-range轮询时间是 1 分钟一次，所以时间的误差<=1 分钟。
**命令模式：**时间范围模式
**缺省情况：**没有时间范围配置
**使用指南：**绝对时间及日期，指定具体开始的年，月，日，小时，分钟，不能配置多个绝对时间及日期，重复配置时，后配置的覆盖以前配置的绝对时间及日期。
**举例：**使能在 2004.10.1 到 2005.1.26 内从 6:00:00 到 13:30:00 配置生效
Switch(config)#Time-range admin_timer
Switch(Config-Time-Range-admin_timer)#absolute start 6:00:00 2004.10.1 end 13:30:00 2005.1.26

## 7.1.3 access-list deny-preemption

本型号交换机不支持此命令。

## 7.1.4 access-list(ip extended)

**命令：access-list *<num>* {deny | permit} icmp {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr>* *<dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [*<icmp-type>* [*<icmp-code>*]] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]**

**access-list *<num>* {deny | permit} igmp {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr>* *<dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [*<igmp-type>*] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]**

**access-list *<num>* {deny | permit} tcp {{ *<sIpAddr>* *<sMask>* } | any-source | {host-source *<sIpAddr>* }} [s-port { *<sPort>* | range *<sPortMin>* *<sPortMax>* }] {{ <dIpAddr> *<dMask>* } | any-destination | {host-destination *<dIpAddr>* }} [d-port { *<dPort>* | ran**

**ge <*dPortMin*> <*dPortMax*> }] [ack+ fin+ psh+ rst+ urg+ syn] [precedence <*prec*> ] [tos <*tos*> ][time-range <*time-range-name*> ]**

**access-list <num> {*deny* / permit} udp *{{* <sIpAddr> <*sMask*> *}* | any-source | {host-source <*sIpAddr*> }} [s-port *{* <*sPort*> | range <*sPortMin*> <*sPortMax*> ] {{ <dIpAddr> <*dMask*> *}* | any-destination | *{host-destination* <dIpAddr> *}} [d-port* { <dPort> / range <dPortMin> <*dPortMax*> }] [precedence <*prec*> ] [tos <*tos*> ][time-range<*time-range-name*> ]**

**access-list <*num*> {deny / permit} {eigrp | *gre* / igrp / ipinip | ip | ospf | <*protocol-num*> } {{ <*sIpAddr*> <sMask> } / any-source / *{*host-source <sIpAddr> *}} {{ <dIpAddr>* <dMask> } | *any-destination* / {host-destination <dIpAddr> }} *[precedence* <*prec*> ] *[tos* <tos> ][time-range <*time-range-name*> *]***

**no access-list <*num*>**

**功能：**创建一条匹配特定IP协议或所有IP协议的数字扩展IP访问列表，如果已有此访问列表，则增加一条rule表项；本命令的no操作为删除一条数字扩展IP访问列表。

**参数：*<num>***为访问表标号，100-299；***<protocol>***为ip上层协议号，0-255；***<sIpAddr>***为源IP地址，格式为点分十进制；***<sMask >***为源IP的反掩码，格式为点分十进制；***<dIpAddr>***为目的IP地址，格式为点分十进制；***<dMask>***为目的IP的反掩码，格式为点分十进制，关心的位置 0，忽略的位置 1；***<igmp-type>***，igmp的类型， 0-255；***<icmp-type>***，icmp的类型，0-255 ；***<icmp-code>***，icmp的协议编号， 0-255；***<prec>***，IP优先级，0-7；***<tos>***，tos值，0-15；***<sPort>***， 源端口号，0-65535； ***<sPortMin>***， 源端口范围下边界； ***<sPortMax>***， 源端口范围上边界； ***<dPort>***， 目的端口号，0-65535； ***<dPortMin>***， 目的端口范围下边界； ***<dPortMax>***， 目的端口范围上边界； ***<time-range-name>***， 时间范围名称。

**命令模式：**全局配置模式

**缺省情况：**没有配置任何的访问列表。

**使用指南：**当用户第一次指定特定***<num>***时，创建此编号的ACL，之后在此ACL中添加表项；标号为 200-299 访问列表可以配置非连续IP地址反掩码。

***<igmp-type>***代表IGMP报文的类型，常用的取值可参照以下的说明：

17(0x11)：IGMP QUERY报文

18(0x12)：IGMP V1 REPORT报文

22(0x16)：IGMP V2 REPORT报文

23(0x17)：IGMP V2 LEAVE报文

34(0x22)：IGMP V3 REPORT报文

19(0x13)：DVMRP报文

20(0x14)：PIM V1 报文

特别提示：这里所指的报文类型是指不含有IP OPTION情况下的报文类型，在通常情况下，IGMP报文是包含有OPTION字段的，这样的设置对这种报文没有作用。如果希望对包含OPTION的报文进行配置，请直接使用配置OFFSET的方式进行。

**举例：**创建编号为 110 的数字扩展访问列表。拒绝icmp报文通过，允许目的地址为 192.168.0.1 目的端口为 32 的udp包通过。

Switch(config)#access-list 110 deny icmp any-source any-destination

Switch(config)#access-list 110 permit udp any-source host-destination 192.168.0.1 d-port 32

## 7.1.5 access-list(ip standard)

**命令：access-list *<num>* {deny | permit} {{*<sIpAddr>* *<sMask >*} | any-source | {host-source *<sIpAddr>*}}**

**no access-list *<num>***

**功能：**创建一条数字标准IP访问列表，如果已有此访问列表，则增加一条rule表项；本命令的no操作为删除一条数字标准IP访问列表。

**参数：*<num>***为访问表标号，1-99；***<sIpAddr>***为源IP地址，格式为点分十进制；***<sMask >***为源IP的反掩码，格式为点分十进制。

**命令模式：**全局配置模式

**缺省情况：**没有配置任何的访问列表。

**使用指南：**当用户第一次指定特定***<num>***时，创建此编号的ACL，之后在此ACL中添加表项。

**举例：**创建一条编号为 20 的数字标准IP访问列表，允许源地址为 10.1.1.0/24 的数据包通过，拒绝其余源地址为 10.1.1.0/16 的数据包通过。

Switch(config)#access-list 20 permit 10.1.1.0 0.0.0.255

Switch(config)#access-list 20 deny 10.1.1.0 0.0.255.255

## 7.1.6 access-list(mac extended)

**命令：access-list <num> {deny | permit} {any-source-mac | { host-source-mac < host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} {untagged | tagged}}**

**no access-list <num>**

**功能：** 定义一条扩展数字MAC ACL规则，No命令删除一个扩展数字MAC访问表规则

**参数：** <num>访问表号，这是一个从 1100－1199 的十进制号；deny 如果规则匹配，拒绝访问；permit 如果规则匹配，允许访问；<any-source-mac>任何源地址；<any-destination-mac> 任何目的地址； <host_smac>，<smac>源MAC地址 ；<smac-mask>源MAC地址的掩码(反掩码)； <host_dmac> ，<dmac> 目的MAC地址；<dmac-mask> 目的MAC地址的掩码(反掩码)；

**命令模式：** 全局配置模式

**缺省配置：** 没有配置任何的访问列表

**使用指南：** 当用户第一次指定特定<num>时，创建此编号的ACL，之后在此ACL中添加表项。

**举例：** 允许任意源 MAC 地址任意目的 MAC 地址的 tagged ethertype 65535S

witch(config)# access-list 1100 permit any-source-mac any-destination-mac tagged ethertype 65535

## 7.1.7 access-list(mac-ip extended)

**命令：**

**access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}icmp {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}}[<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]**

**access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}igmp {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]**

**access-list <*num*> {deny|permit}{any-source-mac| {host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }}{any-destination-mac| {host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }}tcp {{ <*source*> <*source-wildcard*> }|any-source| {host-source <*source-host-ip*> }}[s-port{ <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <*destination*> <destination-wildcard> } | any-destination | {host-destination <*destination-host-ip*> }} [d-port { <*port3*> | range <*dPortMin*> <*dPortMax*> }] [ack+fin+psh+rst+urg+syn] [precedence <*precedence*> ] [tos <*tos*> ] [time-range <*time-range-name*> ]**

**access-list <num> *{deny*|permit}{any-source-mac| *{host-source-mac* <host_smac> *}|{* <*smac*> <*smac-mask*> }}{any-destination-mac| {host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }}udp {{ <*source*> <*source-wildcard*> }|any-source| {host-source <*source-host-ip*> }}[s-port{ <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <destination> <*destination-wildcard*> }|any-destination*/ {host-destination* <destination-host-ip> *}}[d-port*{ <port3> *| range* <dPortMin> <*dPortMax*> }] [precedence <*precedence*> ] [tos <*tos*> ][time-range <*time-range-name*> ]**

**access-list <*num*> {deny|permit}{any-source-mac| {host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }} {any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }} {eigrp|gre*/igrp|ip|ipinip|ospf*|{ <protocol-num> *}} {{* <source> <*source-wildcard*> }|any-source|{*host-source <source-host-ip> }}* {{ <destination> <*destination-wildca*

***rd>* }|any-destination| *{host-destination* <destination-host-ip> }} [precedence <precedence> *] [tos* <tos> *][time-range* <time-range-name> ]**

**功能：**定义一条扩展数字MAC-IP ACL规则，No命令删除一个扩展数字MAC-IP ACL访问表规则

**参数：num** 访问表号。这是一个从 3100－3299 的十进制号；**deny** 如果规则匹配，拒绝访问；**permit** 如果规则匹配，允许访问；**any-source-mac**任何源MAC地址；**any-destination-mac**任何目的MAC地址；**host_smac ，smac**源MAC地址；**smac-mask**源MAC地址的掩码(反掩码)；**host_dmac ， dmac** 目的MAC地址；**dmac-mask** 目的MAC地址的掩码(反掩码)；**protocol** 名字或IP协议的号。它可以是关键字 eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, 也可以是表IP协议号的 0 到 255 的一个整数。为了匹配任何Internet协议（包括ICMP，TCP和UDP）使用关键字ip；**source-host-ip, source**包发送的源网络或源主机号。32 位二进制数，点分十进制表示；**host-source** 表示地址是源主机IP地址，否则是网络IP地址；**source-wildcard** 源IP的掩码。用四个点隔开的十进制数表示的 32 位二进制数，反掩码；**destination-host-ip，destination**包发送时要去往的目的网络或主机号。32 位二进制数，点分十进制表示；**host-source** 表示地址是目的主机IP地址，否则是网络IP地址；**destination-wildcard** 目的IP的掩码。用四个点隔开的十进制数表示的 32 位二进制数，反掩码；**s-port** (可选) 表示要匹配TCP/UDP源端口； **port1** (可选) TCP/UDP源端口号值，端口号是一个 0 到 65535 的数字； <sPortMin>， 源端口范围下边界； ***<sPortMax>***， 源端口范围上边界； **d-port** (可选)表示要匹配TCP/UDP目的端口； **port3** (可选)TCP/UDP目的端口号值，端口号是一个 0 到 65535 的数字； ***<dPortMin>***， 目的端口范围下边界； ***<dPortMax>***， 目的端口范围上边界； **[ack] [fin] [psh] [rst] [urg] [syn]**， (可选) 只对TCP协议，可选多个标志位，当TCP数据报**[ack] [fin] [psh] [rst] [urg] [syn]**的相应位设置时，即初始化TCP数据报以形成一个连接时出现匹配；**precedence** (可选) 包可由优先级过滤， 为 0 到 7 的数字；**tos** (可选)包可由服务级类型过滤，为 0 到 15 的数字；**icmp-type** (可选) ICMP包可由ICMP报文类型过滤。类型是数字 0 到 255；**icmp-code** (可选) ICMP包可由ICMP报文码过滤。该代码是数字 0 到 255；**igmp-type** (可选) IGMP包可由IGMP报文类型或报文名过滤。类型是数字 0 到 15；***<time-range-name>*** 时间范围名称。

**命令模式：**全局配置模式

**缺省情况：**没有配置任何的访问列表。

**使用指南：**当用户第一次指定特定***<num>***时，创建此编号的ACL，之后在此ACL中添加表项；标号为 3200-3299 访问列表可以配置非连续IP地址反掩码。

**举例：**允许源MAC为 00-12-34-45-XX-XX，任意目的MAC地址，源IP地址为：100.1.1.0 0.255.255.255，任意目的IP地址，且源端口是 100，目的端口是 40000 的TCP报文通过

```
Switch(config)# access-list 3199 permit 00-12-34-45-67-00 00-00-00-00-FF-FF any-destination-mac tcp 100.1.1.0 0.255.255.255 s-port 100 any-destination d-port 40000
```

## 7.1.8 access-list(mac standard)

**命令：access-list *<num>* {deny|permit} {any-source-mac | {host-source-mac *<host_smac>* } | {*<smac>* *<smac-mask>*} }**

**no access-list <num>**

**功能：**定义一条标准数字MAC ACL规则，No命令删除一个标准数字 MAC访问表规则

**参数：*<num>***访问表号，这是一个从 700 到 799 的十进制号；***deny*** 如果规则匹配，拒绝访问；***permit*** 如果规则匹配，允许访问；***<smac>，<host_smac>*** 源MAC地址；***<smac-mask>*** 源MAC地址的掩码（反掩码）

**命令模式：**全局配置模式

**缺省情况：**没有配置任何的访问列表。

**使用指南：**当用户第一次指定特定***<num>***时，创建此编号的ACL，之后在此ACL中添加表项。

**举例：**允许源MAC地址为 00-00-XX-XX-00-01 的数据包通过，拒绝源地址为 00-00-00-XX-00-ab的数据包通过。

Switch(config)# access-list 700 permit 00-00-00-00-00-01 00-00-FF-FF-00-00

Switch(config)# access-list 700 deny 00-00-00-00-00-ab 00-00-00-FF-00-00

## 7.1.9 access-list(arp mac suppress)

**命令：access-list *<num>* (deny|permit) (any-sender-mac|host-sender-mac *<sendermac>* *<sendermac-mask>*)**

**no access-list <num>**

**功能：**定义一条ARP MAC SUPPRESS ACL规则，No命令删除一个标准数字 MAC访问表规则

**参数：*<num>***访问表号，这是一个从 1000 到 1099 的十进制号；***deny*** 如果规则匹配，拒绝访问；***permit*** 如果规则匹配，允许访问；***<sendermac>*** arp sender mac地址；***<sendermac>*** arp sender mac地址的掩码（反掩码）

**命令模式：**全局配置模式

**缺省情况：**没有配置任何的访问列表。

**使用指南：**当用户第一次指定特定***<num>***时，创建此编号的ACL，之后在此ACL中添加表项。

**举例：**允许arp sender mac地址为 00-00-XX-XX-00-01 的数据包通过，拒绝arp sender mac地址为 00-00-00-XX-00-ab的数据包通过。

Switch(config)# access-list 1000 permit 00-00-00-00-00-01 00-00-FF-FF-00-00

Switch(config)# access-list 1000 deny 00-00-00-00-00-ab 00-00-00-FF-00-00

## 7.1.10 clear access-group

**命令：clear access-group(in | out) statistic interface { *<interface-name>* | ethernet*<interface-name>* }**

**功能：清空指定接口的包过滤统计信息。**

**参数：*<interface-name>*：接口名称。**

**命令模式：特权用户模式。**

**缺省情况：无。**

**举例：清空 1/1/1 接口的包过滤统计信息。**

Switch#clear access-group out statistic interface ethernet 1/1/1

## 7.1.11 firewall

**命令：firewall { enable | disable}**

**功能：**允许防火墙起作用或禁止防火墙起作用。

**参数：enable**表示允许防火墙起作用；**disable**表示禁止防火墙起作用。

**缺省情况：**缺省为防火墙不起作用。

**命令模式：**全局配置模式。

**使用指南：**在允许和禁止防火墙时，都可以设置访问规则。但只有在防火墙起作用时才可以将规则应用至特定端口。使防火墙不起作用后将删除端口上绑定的所有ACL。

**举例：**允许防火墙起作用。

Switch(config)#firewall enable

## 7.1.12 ip access extended

**命令：ip access extended *<name>***

**no ip access extended *<name>***

**功能：**创建一条命名扩展IP访问列表；本命令的no操作为删除此命名扩展IP访问列表（包含所有表项）。

**参数：*<name>***为访问表标名，字符串长度为 1-64，不允许为纯数字序列。

**命令模式：**全局配置模式

**缺省情况：**没有配置任何的访问列表。

**使用指南：**第一次调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

**举例：**创建一条名为tcpFlow的命名扩展IP访问列表。

Switch(config)#ip access-list extended tcpFlow

## 7.1.13 ip access standard

**命令：ip access standard *<name>***

**no ip access standard *<name>***

**功能：**创建一条命名标准IP访问列表；本命令的no操作为删除此命名标准IP访问列表（包含所有表项）。

**参数：*<name>***为访问表标名，字符串长度为 1-64，不允许为纯数字序列。

**命令模式：**全局配置模式

**缺省情况：**没有配置任何的访问列表。

**使用指南：**第一次调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

**举例：**创建一条名为ipFlow的命名标准IP访问列表。

Switch(config)#ip access-list standard ipFlow

## 7.1.14 ipv6 access-list

**命令：ipv6 access-list *<num-std>* {deny | permit} *{<sIPv6Prefix/*sPrefixlen> | any -source | {host-source *<sIPv6Addr>*}}**

**ipv6 access-list *<num-ext>* {deny | permit} icmp {{ *<sIPv6Prefix*/*sPrefixlen>* } | any-source | {host-source *<sIPv6Addr>* }} { *<dIPv6Prefix/dPrefixlen>* | any-destination | {host-destination *<dIPv6Addr>* }} [ *<icmp-type>* [ *<icmp-code>* ]] [dscp *<dscp>* ] [flow-label *<fl>* ] [time-range*<time-range-name>]***

**ipv6 access-list *<num-ext>* {deny | permit} tcp {{ *<sIPv6Prefix/<sPrefixlen>* } | any-source | {host-source *<sIPv6Addr>* }} [s-port { *<sPort>* | range *<sPortMin>* *<sPortMax>* }] {{ *<dIPv6Prefix/<dPrefixlen>* } | any-destination | {host-destination *<dIPv6Addr>* }} [dPort { *<dPort>* | range *<dPortMin>* *<dPortMax>* }] [syn | ack | urg | rst | fin | psh] [dscp *<dscp>* ] [flow-label *<flowlabel>* ] [time-range *<time-range-name>*]**

**ipv6 *access-list* <num-ext> {deny | permit} *udp {{* <sIPv6Prefix/<sPrefixlen> } | any-source | {host-source *<sIPv6Addr>* }} [s-port { *<sPort>* | range *<sPortMin>* *<sPortMax>* }] {{ *<dIPv6Prefix/<dPrefixlen>* } | any-destination | {host-destination *<dIPv6Addr>* }} [dPort { *<dPort>* | range *<dPortMin>* *<dPortMax>* }] [dscp <dscp> ] [flow-label <flowlabel> ] [time-range<time-range-name>]**

**ipv6 *access-list <num-ext>* {deny | *permit}* <next-header> *{* <sIPv6Prefix/ *sPrefixlen>* | any-source | {host-source *<sIPv6Addr>* }} { *<dIPv6Prefix/dPrefixle n>* | any-destination | {host-destination *<dIPv6Addr>* }} [dscp *<dscp>* ] [flow-la bel *<fl>* ] [time-range*<time-range-name>*]**

**no ipv6 access-list { *<num-std>* | <num-ext> *}***

**功能：** 创建一条IPv6 数字标准访问列表，如果已有此访问列表，则增加一条rule表项；本命令的no操作为删除一条数字标准IPv6 访问列表。

**参数：** ***<num-std>*** 为访问表标号，取值范围为 500～599； ***<num-ext>*** 为访问表标号，取值范围为 600～699； ***<sIPv6Prefix>*** 为源IPv6 地址前缀， ***<sPrefixlen >*** 为源IPv6 地址前缀长度，取值范围为 1～128； ***<sIPv6Addr>*** 为源IPv6 地址； ***<dIPv6Prefix>*** 为目的IPv6 地址前缀， ***<dPrefixlen >*** 为目的IPv6 地址前缀长度，取值范围为 1～128； ***<dIPv6Addr>*** 为目的IPv6 地址； ***<icmp-type>*** icmp的类型； ***<icmp-code>*** icmp的协议编号； ***<dscp>*** IPv6 优先级，范围为 0～63； ***<fl>*** 流标签值，范围为 0～1048575； **syn，ack，urg，rst，fin，psh，tcp** 标志位； ***<sPort>*** 源端口号，范围为 0～65535； **<**

***sPortMin>*** 源端口范围下边界； ***<sPortMax>*** 源端口范围上边界； ***<dPort>*** 目的端口号，范围为 0～65535； ***<dPortMin>*** 目的端口范围下边界； ***<dPortMax>*** 目的端口范围上边界； ***<next-header>*** IPv6 下一头，范围为 0~255； ***<time-range-name>*** 时间范围名称。

**命令模式：** 全局配置模式

**缺省情况：** 缺省没有配置任何的访问列表。

**使用指南：** 当用户第一次以特定***<num>***创建此编号的acl，之后则在此acl中添加表项。

**举例：** 创建一条编号为 520 的IPv6 数字标准访问列表，允许源地址为 2003:1:2:3::1/64 网段的数据包通过，拒绝其余源地址为 2003:1:2::1/48 网段的数据包通过。

Switch (config)#ipv6 access-list 520 permit 2003:1:2:3::1/64

Switch (config)#ipv6 access-list 520 deny 2003:1:2::1/48

## 7.1.15 ipv6 access standard

**命令：ipv6 access-list standard *<name>***

**no ipv6 access-list standard *<name>***

**功能：**创建一条IPv6 命名标准访问列表；本命令的no操作为删除此IPv6 命名标准访问列表（包含所有表项）。

**参数：*<name>***为访问表标名，字符串长度为 1-64。

**命令模式：**全局配置模式

**缺省情况：**没有配置任何的访问列表。

**使用指南：**第一次调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

**举例：**创建一条名为ip6Flow的命名标准IPv6 访问列表。

Switch(config)#ipv6 access-list standard ip6Flow

## 7.1.16 ipv6 access extended

**命令：ipv6 access-list extended *<name>***

**no ipv6 access-list extended *<name>***

**功能：** 创建一条IPv6 命名扩展访问列表；本命令的no操作为删除此IPv6 命名扩展访问列表。

**参数：** ***<name>*** 为访问表标名，字符串长度为 1～64。

**命令模式：** 全局配置模式

**缺省情况：** 没有配置任何的访问列表。

**使用指南：** 第一次调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

**举例：** 创建一条名为tcpFlow的IPv6 命名扩展访问列表。

Switch (config)#ipv6 access-list extended tcpFlow

## 7.1.17 {ip|ipv6|mac|mac-ip} access-group

**命令：{ip|ipv6|mac|mac-ip} access-group *<name>* {in | out }[traffic-statistic]**

**no {ip|ipv6|mac|mac-ip} access-group *<name>* {in | out }**

**功能：**在端口的某个方向上应用一条access-list，并且根据可选项决定是否对ACL规则加上统计计数器；本命令的no操作为删除绑定在端口上的access-list。

**参数：**<name>，命名访问表的名字，字符串长度为 1-32。

**命令模式：**端口配置模式

**缺省情况：**端口没有绑定ACL。

**使用指南：**一个端口可以绑定一条入口和出口规则

基于关心的包头字段ACL可以分为四种：MAC ACL，IP ACL, MAC-IP ACL,IPV6 ACL；某种情况下，当一个数据包匹配四条ACL中的多条时，ACL的过滤动作（permit，deny）会发生冲突。基于结果确定性的考虑，为每一种ACL指定了严格的优先级。当过滤动作发生冲突时，可以依据优先级决定包过滤的最终动作。

当绑定ACL到端口时，有如下限制：

1. 每个端口入口可以绑定一条MAC-IP ACL，一条IP ACL，一条MAC ACL和一条IPV6 ACL；

2. 当同时绑定四条ACL且数据包同时匹配其中多条ACL时，优先关系从高到低如下，如果优先级相同，则先配置的优先级高：

入口IPV6 ACL

入口MAC-IP ACL

入口MAC ACL

入口 IP ACL

**举例：**将名为aaa的访问列表绑定到端口的入方向上。

Switch(Config-If-Ethernet1/1/5)#ip access-group aaa in

## 7.1.18 {ip|ipv6|mac|mac-ip} access-group（接口模式）

本型号交换机不支持此命令。

## 7.1.19 mac access extended

**命令：mac-access-list extended *<name>***

**no mac-access-list extended *<name>***

**功能：**定义一个命名方式的MAC ACL表或进入访问表配置模式，no命令删除命名方式的ACL表。

**参数：*<name>*** 访问表的名字，不包括空格或引号，必须用字母字符开头。长度最大为 32。（注：大小写敏感）

**命令模式：**全局配置模式

**缺省配置：**没有配置任何的访问列表。

**使用指南：**第一次以调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

**举例：**创建一个名字为mac_acl的MAC ACL。

Switch(config)# mac-access-list extended mac_acl

Switch(Config-Mac-Ext-Nacl-mac_acl)#

## 7.1.20 mac-ip access extended

**命令：mac-ip-access-list extended *<name>***

**no mac-ip-access-list extended *<name>***

**功能：**定义一个命名方式的MAC-IP ACL表或进入访问表配置模式，no命令删除命名方式的ACL表。

**参数：*name*** 访问表的名字，不包括空格或引号，必须用字母字符开头。长度最大为 32。（注：大小写敏感）

**命令模式：**全局配置模式

**缺省情况：**没有命名的MAC-IP访问表。

**使用指南：**第一次调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

**举例：**创建一个名字为macip_acl的MAC-IP ACL。

Switch(config)# mac-ip-access-list extended macip_acl

Switch(Config-MacIp-Ext-Nacl-macip_acl)#

## 7.1.21 permit | deny(ip extended)

**命令：[no] {deny | permit} icmp {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr> <dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [*<icmp-type>* [*<icmp-code>*]] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]**

**[no] {deny | permit} igmp {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr> <dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [*<igmp-type>*] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]**

**[no] {deny | permit} tcp {{ *<sIpAddr> <sMask>* } | any-source | {host-source *<sIpAddr>* }} [s-port { *<sPort>* | range *<sPortMin> <sPortMax>* }] {{ *<dIpAddr> <dMask>* } | any-destination | {host-destination *<dIpAddr>* }} [d-port { *<dPort>* | range *<dPortMin> <dPortMax>* }] [ack+fin+psh+rst+urg+syn] [precedence *<prec>* ] [tos *<tos>* ][time-range *<time-range-name>* ]**

**[no] {deny *| permit}* udp {{ *<sIpAddr>* <sMask> *} |** any-source **| {host-source *<sIpAddr>* }} [s-port *{ <sPort>* | range *<sPortMin> <sPortMax>* }] {{ <dIpAddr> *<dMask>* } | any-destination *| {host-destination* <dIpAddr> *}} [*d-port { *<dPort> |* range *<dPortMin> <dPortMax>* }] [precedence *<prec>* ] [tos *<tos>* ][time-range*<time-range-name>* ]**

**[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | *<protocol-num>*} {{ *<sIpAddr>* *<sMask>* } | any-source | {host-source *<sIpAddr>* }} {{ *<dIpAddr>* *<dMask>* } | any-destination | {host-destination *<dIpAddr>* }} [precedence *<prec>* ] [tos *<tos>* ][time-range *<time-range-name>* ]**

**功能：**创建一条匹配特定IP协议或所有IP协议的命名扩展IP访问规则；

**参数：*<sIpAddr>***为源IP地址，格式为点分十进制；***<sMask>***为源IP的反掩码，格式为点分十进制；***<dIpAddr>***为目的IP地址，格式为点分十进制；***<dMask>***为目的IP的反掩码，格式为点分十进制，关心的位置 0，忽略的位置 1；***<igmp-type>***，igmp的类型，0－255；***<icmp-type>***，icmp的类型，0－255；***<icmp-code>***，icmp的协议编号，0－255；***<prec>***，IP优先级，0－7；***<tos>***，tos值，0-15；***<sPort>***， 源端口号，0-65535； ***<sPortMin>***， 源端口范围下边界；***<sPortMax>***， 源端口范围上边界；***<dPort>***，目的端口号，0-65535； ***<dPortMin>***， 目的端口范围下边界； ***<dPortMax>***， 目的端口范围上边界； ***<time-range-name>***， 时间范围名称。

**命令模式：**命名扩展IP访问列表配置模式

**缺省情况：**没有配置任何的访问列表。

**使用指南：**无。

**举例：**创建名为udpFlow的扩展访问列表。拒绝igmp报文通过，允许目的地址为 192.168.0.1 目的端口为 32 的udp包通过。

```
Switch(config)#ip access-list extended udpFlow
Switch(Config-Ext-Nacl-udpFlow)# deny igmp any-source any-destination
Switch(Config-Ext-Nacl-udpFlow)# permit udp any-source host-destination 192.168.0.1 d-port 32
```

## 7.1.22 permit | deny(ip standard)

**命令：{deny | permit} {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}}**

**no {deny | permit} {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}}**

**功能：**创建一条命名标准IP访问规则（rule）；本命令的no操作为删除此命名标准IP访问规则（rule）。

**参数： *<sIpAddr>***为源IP地址，格式为点分十进制；***<sMask>***为源IP的反掩码，格式为点分十进制。

**命令模式：**命名标准Ip访问列表配置模式

**缺省情况：**没有配置任何的访问列表。

**使用指南：**无。

**举例：**允许源地址为 10.1.1.0/24 的数据包通过，拒绝其余源地址为 10.1.1.0/16 的数据包通过。

```
Switch(config)# ip access-list standard ipFlow
Switch(Config-Std-Nacl-ipFlow)# permit 10.1.1.0 0.0.0.255
```

Switch(Config-Std-Nacl-ipFlow)# deny 10.1.1.0 0.0.255.255

## 7.1.23 permit | deny(ipv6 extended)

**命令：[no] {deny | permit} icmp {{*<sIPv6Prefix/sPrefixlen>*} | any-source | {host-source *<sIPv6Addr>*}} {*<dIPv6Prefix/dPrefixlen>* | any-destination | {host-destination *<dIPv6Addr>*}} [*<icmp-type>* [*<icmp-code>*]] [dscp *<dscp>*] [flow-label *<fl>*][time-range *<time-range-name>*]**

**[no] {deny | permit} tcp { *<sIPv6Prefix/sPrefixlen>* | any-source | {host-source *<sIPv6Addr>* }} [s-port { *<sPort>* | range *<sPortMin>* *<sPortMax>* }] { *<dIPv6Prefix/dPrefixlen>* | any-destination | {host-destination *<dIPv6Addr>* }} [d-port { *<dPort>* | range *<dPortMin>* *<dPortMax>* }] [syn | ack | urg | rst | fin | psh] [dscp *<dscp>* ] [flow-label *<fl>* ][time-range *<time-range-name>* ]**

**[no] {deny *| permit}* udp { *<sIPv6Prefix/sPrefixlen>* | *any-source |* {host-source *<sIPv6Addr>* }} [s-port *{ <sPort>* | *range <sPortMin>* <sPortMax> }] { *<dIPv6Prefix/dPrefixlen>* | any-destination *| {host-destination* <dIPv6Addr> *}}* [d-port { *<dPort>* | range *<dPortMin>* <dPortMax> }] [dscp *<dscp>* ] [flow-label *<fl>* ][time-range *<time-range-name>* ]**

**[no] {deny *| permit}* <next-header> *{<sIPv6Prefix/*sPrefixlen> | *any-source |* {host-source *<sIPv6Addr>*}} {<dIPv6Prefix*/dPrefixlen>* | any-destination *| {host-destination* <dIPv6Addr>}} [dscp *<dscp>]* [flow-label <fl>*][time-range* <time-range-name>]**

***[no]* {deny | *permit}* {<sIPv6Prefix/*sPrefixlen>* | any-source | {host-source <sIPv6Addr>*}}* {<dIPv6Prefix/dPrefixlen> | any-destination | *{host-destination* <dIPv6Addr>}} [dscp *<dscp>*] [flow-label *<fl>*] [time-range*<time-range-name>*]**

**功能：** 创建一条匹配特定IPv6 协议或所有IPv6 协议的IPv6 命名扩展访问规则。

**参数：** ***<sIPv6Addr>*** 为源IPv6 地址； **<sPrefixlen>** 为源IPv6 地址的前缀长度，范围为 1～128； ***<dIPv6Addr>*** 为目的IPv6 地址； ***<dPrefixlen>*** 为目的IPv6 地址的前缀长度，范围为 1～128； ***<icmp-type>，*** icmp的类型； **<icmp-code>，** icmp的协议编号； **<dscp>，** IPv6 优先级，范围为 0～63； ***<fl>，*** 流标签值，范围为 0～1048575； **syn，ack，urg，rst，fin，psh，** tcp标志位； **<sPort>，** 源端口号，范围为 0～65535； **<sPortMin>，** 源端口范围下边界； ***<sPortMax>，*** 源端口范围上边界； **<dPort>，** 目的端口号，范围为 0～65535； <dPortMin>， 目的端口范围下边界； ***<dPortMax>***， 目的端口范围上边界； ***<next-header>***， IPv6 下一头，范围为 0~255； ***<time-range-name>***， 时间范围名称。

**命令模式：** IPv6 命名扩展访问列表配置模式

**缺省情况：** 没有配置任何的访问列表。

**使用指南：** 无。

**举例：** 创建名为udpFlow的扩展访问列表。拒绝icmp报文通过，允许目的地址为 2001:1:2:3::1 目的端口为 32 的udp包通过。

Switch(config)#ipv6 access-list extended udpFlow

Switch(Config-Ext-Nacl-udpFlow)# )#deny icmp any-source any-destination
Switch(Config-Ext-Nacl-udpFlow)#permit udp any-source host-destination 2001:1:2:3::1 d-Port 32

## 7.1.24 permit | deny(ipv6 standard)

**命令：[no] {deny | permit} {{*<sIPv6Prefix/sPrefixlen>*} | any-source | {host-source *<sIPv6Addr>*}}**

**功能：**创建一条IPv6 命名标准访问规则（rule）；本命令的no操作为删除此IPv6 命名标准访问规则（rule）。

**参数：*<sIPv6Prefix>***为源IPv6 地址前缀，***<sPrefixlen>***为源IPv6 地址前缀长度，取值范围为 1～128。***<sIPv6Addr>***为源IPv6 地址。

**命令模式：**IPv6 命名标准访问列表配置模式

**缺省情况：**没有配置任何的访问列表。

**使用指南：**

**举例：**允许源地址为 2001:1:2:3::1/64 的数据包通过，拒绝其余源地址为 2001:1:2:3::1/48 的数据包通过。

Switch(config)# ipv6 access-list standard ipv6Flow
Switch(Config-Std-Nacl-ipv6Flow)# permit 2001:1:2:3::1/64
Switch(Config-Std-Nacl-ipv6Flow)# deny 2001:1:2:3::1/48

## 7.1.25 permit | deny(mac extended)

**命令：**

**[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [cos <cos-val> [ <cos-bitmask> ][vlanid <vid-value> [ <vid-mask> ][ethertype <protocol> [ <protocol-mask> ]]]]**

**[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [ethertype <protocol> [ <protocol-mask> ]]**

**[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [vlanid <vid-value> [ <vid-mask> ][ethertype <protocol> [ <protocol-mask> ]]]**

**[no]{deny|permit} {any-source-mac|{host-source-mac *<host_smac>* }|{ *<smac>* *<smac-mask>* }} {any-destination-mac|{host-destination-mac *<host_dmac>* }|{ *<dmac>* *<dmac-mask>* }} [untagged-eth2 [ethertype <protocol> [protocol-mask]]]**

**[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [untagged-802-3]**

**[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ *<smac>* <smac-mask> }*}* *{*any-destination-mac|{*host-destination-mac* <host_dmac> }|{ <dmac> <dmac-mask> }} [tagged-eth2 [cos <cos-val> [ <cos-bitmask> ]] [vlanId <vid-value> [ <vid-mask> ]] [ethertype <protocol> [ <protocol-mask> ]]]**

**[no]{deny|permit}{any-source-mac|{host-source-mac *<host_smac>* }|{ *<smac>* *<smac-mask>* }} {any-destination-mac|{host-destination-mac *<host_dmac>* }|{ *<dmac>* *<dmac-mask>* }} [tagged-802-3 [cos <cos-val> [ <cos-bitmask> ]] [vlanId *<vid-value>* [ *<vid-mask>* ]]]**

**功能：**定义一条扩展命名MAC ACL规则，No命令删除一个扩展命名MAC ACL访问表规则。

**参数：any-source-mac**：任何源MAC地址；**any-destination-mac**：任何目的MAC地址；**host_smac ， smac**：源MAC地址；**smac-mask** 源MAC地址的掩码(反掩码)；**host_dmac ， dmac** 目的MAC地址；**dmac-mask** 目的MAC地址的掩码(反掩码)；**untagged-eth2:** 未标记的ethernet II包格式；**tagged-eth2:** 标记的ethernet II包格式；**untagged-802-3:** 未标记的ethernet 802.3 包格式；**tagged-802-3:** 标记的ethernet 802.3 包格式；**cos-val:** cos值，0-7；**cos-bitmask:** cos掩码， 0-7 反掩码且掩码比特连续；**vid-value:** vlan号，1-4094；**vid-bitmask:**vlan掩码， 0-4095，反掩码且掩码比特连续；**protocol:** 特定的以太网协议号，1536－65535；**protocol-bitmask:** 协议掩码，0－65535，反掩码且掩码比特连续

**注意：**掩码比特连续是指，掩码有效位必须从左第一位开始连续有效，不允许中间插入无效位，例如：一个字节的反掩码形式为：00001111b ；正掩码形式为：11110000；不允许 00010011。

**命令模式：**命名扩展MAC访问列表配置模式

**缺省配置：**没有配置任何的访问列表

**使用指南：**

**举例：**不允许转发源MAC地址是00-12-11-23-XX-XX的数据报文。

```
Switch(config)# mac-access-list extended macExt
Switch(Config-Mac-Ext-Nacl-macExt)# deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac ethertype 65535
```

## 7.1.26 permit | deny(mac-ip extended)

**命令：**

**[no] {deny|permit}**
**{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} icmp{{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination <*destination-host-ip*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]**

**[no]{deny|permit}**
**{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} igmp{{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination <*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]**

**[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*> }| { <*smac*> <*smac-mask*> }}{any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }} tcp{{ <*source*> <*source-wildcard*> }|any-source| {host-source <*source-host-ip*> }}[s-port { <*port1*> | range <sPortMin> <sPortMax> }] {{ <destination> <destination-wildcard> } | any-destination| {host-destination <destination-host-ip> }} [d-port { <port3> | range <dPortMin> <*dPortMax*> }] [ack＋fin＋psh＋rst＋urg＋syn] [precedence <*precedence*> ] [tos <*tos*> ][time-range <*time-range-name*> ]**

**[no]{deny|*permit}{any-source-mac*|{host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }}{any-destination-mac|{host-destination-mac <*host_dmac*> }| { <*dmac*> <*dmac-mask*> }}udp{{ <*source*> <*source-wildcard*> }|any-source| {host-source <*source-host-ip*> }}[s-port { <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <destination> <*destination-wildcard*> }|any-destination| *{host-destination* <destination-host-ip> *}} [d-port* { <port3> / range <dPortMin> <*dPortMax*> }] [precedence <*precedence*> ] [tos <*tos*> ][time-range <*time-range-name*> ]**

**[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*> <*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}| {<*dmac*><*dmac-mask*>}}{eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}} {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination <*destination-host-ip*>}} [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]**

**功能：**定义一条扩展命名MAC-IP ACL规则，No命令删除一个扩展数字MAC-IP ACL访问表规则。

**参数：num** 访问表号。这是一个从 3100－3199 的十进制号；**deny** 如果规则匹配，拒绝访问；**permit** 如果规则匹配，允许访问；**any-source-mac**：任何源MAC地址；**any-destination-mac**：任何目的MAC地址；**host_smac ，smac**：源MAC地址；**smac-mask**：源MAC地址的掩码(反掩码)；**host_dmac ，dmas** 目的MAC地址；**dmac-mask** 目的MAC地址的掩码(反掩码)；**protocol** 名字或IP协议的号。它可以是关键字 eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, 也可以是表IP协议号的 0 到 255 的一个整数。为了匹配任何Internet协议（包括ICMP，TCP和UDP）使用关键字ip；**source-host-ip, source**包发送的源网络或源主机号。32 位二进制数，点分十进制表示；**host-source**:表示地址是源主机IP地址，否则是网络IP地址；**source-wildcard**:源IP的掩码。用四个点隔开的十进制数表示的 32 位二进制数，反掩码；**destination-host-ip，destination**包发送时要去往的目的网络或主机号。32 位二进制数，点分十进制表示；**host-source**:表示地址是目的主机IP地址，否则是网络IP地址；**destination-wildcard**：目的IP的掩码。用四个点隔开的十进制数表示的 32 位二进制数，反掩码；**s-port** (可选)：表示要匹配TCP/UDP源端口； **port1** (可选)：TCP/UDP源端口号值，端口号是一个 0 到 65535 的数字； ***<sPortMin>***， 源端口范围下边界； ***<sPortMax>***， 源端口范围上边界； d-port (可选)：表示要匹配TCP/UDP目的端口； **port3** (可选)：TCP/UDP目的端口号值，端口号是一个 0 到 65535 的数字； ***<dPortMin>***， 目的端口范围下边界； ***<dPortMax>***， 目的端口范围上边界； **[ack] [fin] [psh] [rst] [urg] [syn]** (可选) 只对TCP协议，可选多个标志位，当TCP数据报[ack] [fin] [psh] [rst] [urg] [syn]的相应位设置时，即初始化TCP数据报以形成一个连接时出现匹配；**precedence** (可选) 包可由优先级过滤， 为 0 到 7 的数字；**tos** (可选)包可由服务级类型过滤，为 0 到 15 的数字；**icmp-type** (可选) ICMP包可由ICMP报文类型过滤。类型是数字 0 到 255；**icmp-code** (可选) ICMP包可由ICMP报文码过滤。该代码是数字 0 到 255；**igmp-type** (可选) IGMP包可由IGMP报文类型或报文名过滤。类型是数字 0 到 15；***<time-range-name>***，时间范围名称。

**命令模式：**命名扩展MAC-IP访问列表配置模式

**缺省情况：**没有配置任何的访问列表。

**使用指南：**无。

**举例：** 拒绝任意源MAC地址及目的MAC地址，任意源IP地址及目的IP地址，且源端口是 100，目的端口是 40000 的UDP报文通过

```
Switch(config)# mac-ip-access-list extended macIpExt
Switch(Config-MacIp-Ext-Nacl-macIpExt)# deny any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000
```

## 7.1.27 show access-lists

**命令： show access-lists [*<num>*|*<acl-name>*]**

**功能：** 显示配置的访问控制列表。

**参数：** ***<acl-name>***，特定的访问控制列表命名字符串；***<num>***，特定的访问控制列表的编号。

**缺省情况：** 无。

**命令模式：**特权和配置模式

**使用指南：**不指定访问控制列表的名字时，会显示所有的访问控制列表；used x time（s）表明了此ACL被引用的次数。

**举例：**

```
Switch#show access-lists
access-list 10(used 0 time(s))
    access-list 10 deny any-source

access-list 100(used 1 time(s))
    access-list 100 deny ip any-source any-destination
    access-list 100 deny tcp any-source any-destination

access-list 1100(used 0 time(s))
    access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800

 access-list 3100(used 0 time(s))
    access-list 3100 deny any-source-mac any-destination-mac udp any-source s-port 100 a
ny-destination d-port 40000
```

| 显示内容 | 解释 |
|---|---|
| access-list 10(used 1 time(s)) | 数字ACL10，被引用 0 次 |
| access-list 10 deny any-source | 拒绝所有IP数据包通过 |
| access-list 100(used 1 time(s)) | 数字ACL100，被引用 1 次 |
| access-list 100 deny ip any-source any-destination | 拒绝任意源IP地址及目的IP地址的IP包通过 |
| access-list 100 deny tcp any-source any-destination | 拒绝任意源IP地址及目的IP地址的TCP包通过 |
| access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800 | 允许任意源MAC地址任意目的MAC地址的tagged-eth2，且其第 15 16 个字节分别为 0x08 ，0x0 的包通过 |
| access-list 3100 permit any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000 | 拒绝任意源MAC地址及目的MAC地址，任意源IP地址及目的IP地址，且源端口是 100，目的端口是 40000 的UDP报文通过 |

## 7.1.28 show access-group

**命令：show access-group in (interface {Ethernet | Ethernet IFNAME | port-channel <IFNAME>})**

**功能：**显示端口上ACL绑定情况。

**参数：IFNAME**，端口名。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**不指定接口名时，会显示所有端口上绑定的ACL。

**举例：**

```
Switch#show access-group
interface name:Ethernet1/1/1
    IP Ingress access-list used is 100, traffic-statistics Disable.
interface name:Ethernet1/1/2
    IP Ingress access-list used is 1, packet(s) number is 11110.
```

| 显示内容 | 解释 |
| --- | --- |
| interface name:Ethernet1/1/1 | 端口Ethernet1/1/1 的绑定情况 |
| IP Ingress access-list used is 100 | 端口Ethernet1/1/1 入口方向绑定了编号 100 的数字扩展ACL |
| packet(s) number is 11110 | 统计到匹配此ACL规则的数据包数 |

## 7.1.29 show firewall

**命令： show firewall**

**功能：** 显示包过滤功能配置信息。

**参数：** 无。

**缺省情况：** 无。

**命令模式：特权和配置模式。**

**使用指南：无。**

**举例：**

```
Switch#show firewall
  Firewall Status: Enable.
```

| 显示内容 | 解释 |
| --- | --- |
| Firewall Status: Enable | 包过滤功能打开 |

## 7.1.30 show ipv6 access-lists

**命令：show ipv6 access-lists [*<num>*|*<acl-name>*]**

**功能：**显示配置的IPv6 访问控制列表。

**参数：**<num>为特定的访问控制列表的编号，取值范围为 500～699，其中 500～599 为数字标准IPv6 ACL编号，600～699 为数字扩展IPv6 ACL编号；<acl-name>为特定的访问控制列表命名字符串，长度为 1～16。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**不指定访问控制列表的名字时，会显示所有的访问控制列表；used x time（s）表明了此ACL被引用的次数。

**举例：**

```
Switch #show ipv6 access-lists
ipv6 access-list 500(used 1 time(s))
    ipv6 access-list 500 deny any-source

ipv6 access-list 510(used 1 time(s))
    ipv6 access-list 510 deny ip any-source any-destination
    ipv6 access-list 510 deny tcp any-source any-destination

ipv6 access-list 520(used 1 time(s))
    ipv6 access-list 520 permit ip any-source any-destination
```

## 7.1.31 show time-range

**命令： show time-range*<word>***

**功能：** 显示时间范围功能配置信息。

**参数：** ***word***指定要显示的time-range的名字

**缺省情况：** 无。

**命令模式：**特权和配置模式。

**使用指南：** 不指定time-range的名字时，显示所有的time-range。

**举例：**

```
Switch#show time-range
time-range timer1 (inactive, used 0 times)
        absolute-periodic Saturday 0:0:0 to Sunday 23:59:59
time-range timer2 (inactive, used 0 times)
        absolute-periodic Monday 0:0:0 to Friday 23:59:59
```

## 7.1.32 time-range

**命令：[no] time-range *<time_range_name>***

**功能：**创建一个名为**time_range_name**的时间范围名，并同时进入时间范围模式。

**参数：*time_range_name***时间范围名字，必须用字母字符开头，名字最大长度为 16 个字符。

**命令模式：**全局配置模式

**缺省情况：**没有时间范围配置。

**使用指南：**无。

**举例：**创建一个名为admin _timer的时间范围。

Switch(config)#time-range admin_timer

# 7.2 自定义ACL

## 7.2.1 permit | deny

本型号交换机不支持此命令。

## 7.2.2 udf-access-list standard

本型号交换机不支持此命令。

## 7.2.3 userdefined-access-list standard offset

**命令：userdefined-access-list standard offset [window1 <*offset*>] [window2 <*offset*>] [window3 <*offset*>] [window4 <*offset*>][ l2start <*offset*> | l3start <*offset*>| l4start <*offset*>] no userdefined-access-list standard offset [window1] [window2] [window3] [window4]功能：**创建标准自定义访问列表模板，如果已有此模板则修改模板对应的window；本命令的no操作为删除标准自定义访问列表模板对应window，如果未指定任何window则删除整个标准自定义访问列表模板。

**参数：**

**window1-window4** 自定义窗口 1 至 4

***offset*** 配置的偏移量<0-31>（单位为 2 字节）

**l2start** 配置偏移起始位置为报文头

**l3start** 配置偏移起始位置为三层头部

**l4start** 配置偏移起始位置为四层头部

**命令模式：**全局配置模式

**缺省情况：**没有配置模板

**使用指南：**<*offset*>为配置一个window的偏移量，取值范围为<0-31>，单位为 2Bytes，即 0 代表偏移 0Bytes，1 代表偏移 2Bytes，可以配置至多 4 个window的偏移起始位置和偏移量。全局共享一个基本自定义ACL模板，在配置有使用了某个window的自定义ACL规则时该模板中对应的window无法被修改，当没有规则引用某个window时可以用本命令修改这个window的配置。

删除模板命令可以删除模板中的某个或某些窗口的偏移配置或删除整个模板的配置（未指定任何具体的window）。必须当模板对应window没有被自定义ACL规则使用时才能删除成功。

**举例：**创建全局模板，使用window3，分别配置偏移起始位和偏移量：

Switch(config)# userdefined-access-list standard offset window3 l2 0 window4

## 7.2.4 userdefined-access-list extended offset

本型号交换机不支持此命令。

## 7.2.5 userdefined-access-list standard

命令：userdefined-access-list standard <num> {deny | permit} [packet-type {ipv4 | ipv6] [window1 <value> <mask>] [window2 <value> <mask>] [window3 <value> <mask>] [window4 <value> <mask>] no userdefined-access-list <num>

功能： 创建一条数字标准自定义访问列表，如果已有此访问列表，则增加一条规则（rule）表项；本命令的no操作为删除一条标准自定义访问列表。

参数： <num>访问表号，这是一个从 1200－1299 的十进制号；deny 如果规则匹配，拒绝访问；permit 如果规则匹配，允许访问；packet-type的各个类型是针对不同的报文类型匹配；各个window的<value>和<mask>为一个 2 字节长度 16 进制数。

命令模式： 全局配置模式

缺省情况： 没有配置任何的访问列表

**使用指南： 当用户第一次指定特定<num>时，创建此编号的ACL，之后在此ACL中添加表项。**

举例： 允许报文的前两个字节为 0x4501 的包通过。

Switch(config)#userdefined-access-list standard offset window1 l2start 0

Switch(config)#userdefined-access-list standard 1200 permit window1 4501 FFFF

## 7.2.6 userdefined-access-list extended

本型号交换机不支持此命令。

## 7.2.7 userdefined access-group

命令：userdefined access-group {<name>|<num>} {in} [traffic-statistic]

no userdefined access-group {<name>|<num>} {in}

功能：在端口的某个方向上应用一条userdefined-access-list，并且根据可选项决定是否对ACL规则加上统计计数器；本命令的no操作为删除绑定在端口上的userdefined-access-list。

参数： <num>访问表的名字，这是一个从 1200-1299 的十进制号数字名字；

<name>访问表的名字，字符串长度为 1-64，不允许为纯数字序列。

命令模式： 物理端口配置模式

缺省情况： 端口没有绑定userdefined-access-list

使用指南： 一个端口可以在入口方向上绑定一个自定义访问列表，自定义访问列表与其它类型的访问列表可以同时配置在同一个端口入方向上，不同类型的访问列表同时匹配时遵循deny优先原则，即如果有某类访问列表匹配deny规则则一定会执行deny，反之会permit报文。

举例： 已配置的自定义访问列表如下：

Switch(config)#userdefined-access-list standard offset window1 0

Switch(config)#userdefined-access-list standard 1200 permit window1 4501 FFFF

绑定自定义访问列表至端口Ethernet1/1/1：

Switch(config)#interface ethernet1/1/1

Switch(config-if-ethernet1/1/1)#userdefined access-group 1200 in

## 7.2.8 vacl ip access-group

**命令：vacl ip access-group <*num*> in [traffic-statistic] vlan <*vlan-id*>**

**no ip access-group <*num*> in vlan <*vlan-id*>**

**功能：**在vlan的某个方向上应用一条userdefined-access-list，并且根据可选项决定是否对ACL规则加上统计计数器；本命令的no操作为删除绑定在vlan上的userdefined-access-list。

**参数：**<*num*>访问表的名字，这是一个从 1200-1399 的十进制号数字名字。

**命令模式：**全局配置模式

**缺省情况：**vlan没有绑定userdefined-access-list

**使用指南：**一个vlan可以在入口方向上绑定一个自定义访问列表，自定义访问列表与其它类型的访问列表可以同时配置在同一个vlan入方向上，不同类型的访问列表同时匹配时遵循deny优先原则，即如果有某类访问列表匹配deny规则则一定会执行deny，反之会permit报文。

**举例：**已配置的自定义访问列表如下：

Switch(config)#userdefined-access-list standard offset window1 l2start 0

Switch(config)#userdefined-access-list standard 1200 permit window1 4501 FFFF

绑定自定义访问列表至vlan 1：

Switch(config)# vacl ip access-group 1200 in vlan 1

# 7.3 802.1x

## 7.3.1 authentication dot1x radius none

本交换机不支持此命令。

## 7.3.2 debug dot1x detail

**命令：debug dot1x detail {pkt-send | pkt-receive | internal| all | userbased | webbased } interface {[ethernet] <*interface-name*> | port-channel <IFNAME>}**

**no debug dot1x detail {pkt-send | pkt-receive | internal | all | userbased | webbased } interface {[ethernet] <*interface-name*> | port-channel <IFNAME>}**

**功能：**打开dot1x的细节调试信息；本命令的no操作为关闭dot1x的细节调试信息。

**参数：pkt-send:** 打开dot1x的发送包调试信息；

**pkt-receive:** 打开dot1x的接收包调试信息；

**internal:** 打开dot1x的内部细节调试信息；

**all:** 打开dot1x的所有以上细节调试信息；

**userbased：** 基于用户认证方式；

**webbased：** 基于Web认证方式；

**<*interface-name*>:** 端口名称。

**<IFNAME>: port-channel**名称。

**命令模式：**特权配置模式。

**使用指南：**打开dot1x细节调试信息，可以查看dot1x协议运行的细节过程，在遇到故障时有助于监测故障原因。

**举例：**打开端口 1/1/1 下dot1x的所有细节调试信息。

Switch#debug dot1x detail all interface ethernet 1/1/1

## 7.3.3 debug dot1x error

**命令：debug dot1x error**

**no debug dot1x error**

**功能：**打开dot1x的出错调试信息；本命令的no操作为关闭dot1x的出错调试信息。

**参数：**无。

**命令模式：**特权配置模式。

**使用指南：**打开dot1x出错调试信息，可以查看dot1x协议运行过程中的出错信息，在遇到故障时有助于监测故障原因。

**举例：**打开dot1x出错调试信息。

Switch#debug dot1x error

## 7.3.4 debug dot1x fsm

**命令：debug dot1x fsm {all | aksm | asm | basm | ratsm} interface { <IFNAME> | ethernet <interface-name> | port-channel <IFNAME>}**

**no debug dot1x fsm {all | aksm | asm | basm | ratsm} interface { <IFNAME> | ethernet <interface-name> | port-channel <IFNAME>}**

**功能：**打开dot1x的状态机调试信息；本命令的no操作为关闭dot1x的状态机调试信息。

**命令模式：**特权配置模式。

**参数：all：**打开dot1x的所有状态机调试信息；

**aksm：**打开Authenticator Key Transmit状态机调试信息；

**asm：** 打开Authenticator状态机调试信息；

**basm：**打开Backend Authentication状态机调试信息；

**ratsm：**打开Re-Authentication Timer状态机调试信息；

***<interface-name>*：**端口名称。

**<IFNAME>: port-channel**名称。

**使用指南：**打开dot1x调试信息，可以查看dot1x协议的协商过程，在遇到故障时有助于监测故障原因。

**举例：**打开dot1x状态机调试信息。

Switch#debug dot1x fsm asm interface ethernet1/1/1

## 7.3.5 debug dot1x packet

**命令：debug dot1x packet {all | receive | send} interface { <IFNAME> | ethernet <interface-name> | port-channel <IFNAME>}**

**no debug dot1x packet {all | receive | send} interface { <IFNAME> | ethernet < interface-name> | port-channel <IFNAME>}**

**功能：**打开dot1x的报文调试信息；本命令的no操作为关闭dot1x的报文调试信息。

**命令模式：**特权配置模式。

**参数：send：** 打开dot1x的发包调试信息；

**receive：** 打开dot1x的收包调试信息；

**all：** 打开dot1x的收包和发包调试信息；

***<interface-name>*:** 端口名称。

**<IFNAME>: port-channel**名称。

**使用指南：**打开dot1x调试信息，可以查看dot1x协议的协商过程，在遇到故障时有助于监测故障原因。

**举例：**打开dot1x报文调试信息。

Switch#debug dot1x packet all interface ethernet1/1/1

## 7.3.6 dot1x accept-mac

**命令：dot1x accept-mac <*mac-address*> [interface { <IFNAME> | ethernet <interface-name> | port-channel <IFNAME>}]**

**no dot1x accept-mac <*mac-address*> [interface { <IFNAME> | ethernet <interface-name> | port-channel <IFNAME>}]**

**功能：**向dot1x地址过滤表中添加一个MAC地址表项，如果指定端口则添加的表项仅适用于指定端口，不指定端口则添加的表项适用于全部端口；本命令的no操作为删除dot1x的地址过滤表中的表项。

**参数：<*mac-address*>**为MAC地址；**<*interface-name*>**为接口名称及接口号；**<IFNAME>: port-channel**名称。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**交换机的dot1x地址过滤功能是根据MAC地址过滤表实现的，dot1x地址过滤表由用户手工添加或删除。当添加dot1x地址过滤表项时指定了端口，则该地址过滤表项仅适用于该端口；若添加时未指定端口，则该地址过滤表项适用于交换机所有端口。当交换机的dot1x地址过滤功能打开，交换机会对认证者的MAC地址进行过滤，只有在dot1x地址过滤表中存在的客户发起的认证请求才能被接受，否则将被拒绝。

**举例:** 将MAC地址 00-01-34-34-2e-0a添加到Ethernet 1/1/5 的过滤表中。

Switch(config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/1/5

## 7.3.7 dot1x authentication

**命令:** dot1x authentication{local|radius}

**功能：**开启本地认证或者 radius 认证

**命令模式：** 全局配置模式

**缺省情况：** 开启radius认证

**举例:** 开启本地认证

Switch(config)#dot1x authentication local

## 7.3.8 dot1x eapor enable

**命令：dot1x eapor enable**

**no dot1x eapor enable**

**功能：**设置交换机采用EAP中继的方式进行认证；本命令的no操作为设置交换机采用EAP本地终结的方式进行认证。

**命令模式：**全局配置模式

**缺省情况：**交换机采用EAP中继的方式进行认证。

**使用指南：**交换机与Radius认证服务器之间可能采用以太网方式连接或者采用PPP方式连接。如果交换机与Radius认证服务器之间采用以太网连接，那么交换机需要采用EAP中继的方式进行认证（即EAPoR认证）；如果交换机与Radius认证服务器之间采用PPP方式连接，则交换机需要采用EAP本地终结的方式进行认证（即CHAP认证）。根据交换机与认证服务器的连接方式的不同，交换机应该采用不同的认证方式进行认证。

**举例:** 设置交换机采用EAP本地终结的方式进行认证。

Switch(config)#no dot1x eapor enable

## 7.3.9 dot1x enable

**命令：dot1x enable**

**no dot1x enable**

**功能：** 打开交换机全局及端口的 802.1x功能；本命令的no操作为关闭 802.1x功能。

**命令模式：** 全局配置模式及端口配置模式

**缺省情况：** 交换机在全局下不打开 802.1x功能；若交换机在全局下打开 802.1x功能，则端口缺省也不打开 802.1x功能。

**使用指南：** 如果要对端口进行 802.1x认证时，首先要打开全局下的 802.1x功能，再在相应的端口下打开 802.1x功能。如果该端口已经打开了Spanning Tree，或者使能了mac绑定，或者是Trunk端口、端口聚合组的成员，则必须关闭端口下的Spanning Tree功能、或者关闭mac绑定、或者改变端口为Access端口、取消参加端口汇聚组，否则无法打开端口下的 802.1x功能。

**举例：** 启动交换机的 802.1x功能，并且打开 1/1/12 号端口 802.1x功能。

Switch(config)#dot1x enable

Switch(config)#interface ethernet 1/1/12

Switch(Config-If-Ethernet1/1/12)#dot1x enable

## 7.3.10 dot1x ipv6 passthrough

本型号交换机不支持此命令

## 7.3.11 dot1x dhcp passthrough

本型号交换机不支持此命令。

## 7.3.12 dot1x guest-vlan

**命令：dot1x guest-vlan <*vlanid*>**

**no dot1x guest-vlan**

**功能：**设置指定端口的guest-vlan；本命令的no操作为删除guest-vlan。

**参数：*<vlanid>*** 所配置的Vlan id，取值范围为 1-4094。

**命令模式：**端口配置模式。

**缺省情况：**端口上不配置 802.1x guest-vlan功能。

**使用指南：**如果因为没有专用的认证客户端或者客户端版本过低等原因，导致在一定的时间内端口上无客户端认证成功，接入设备会把该端口加入到Guest VLAN。用户在Guest VLAN中可以获取 802.1x客户端软件，升级客户端，或执行其他一些应用升级程序（例如防病毒软件、操作系统补丁程序等）。当Guest VLAN 中端口下的用户发起认证，如果认证失败，该端口将会仍然处在Guest VLAN 内；如果认证成功，分为以下两种情况：

- 认证服务器下发一个Auto VLAN，这时端口离开Guest VLAN，加入下发的Auto VLAN中。用户下线后，端口会被重新划分到所配置的Guest Vlan内。
- 认证服务器不下发VLAN，这时端口离开Guest VLAN，加入配置的VLAN中。用户下线后，端口会被重新划分到所配置的GuestVlan内。

**注意事项：**

- 不同的端口可以配置不同的Guest VLAN，但一个端口只能配置一个Guest VLAN。
- 当端口的接入控制方式为portbased 时，Guest VLAN才能生效；若端口的接入控制为macbased或userbased，Guest VLAN能够配置成功，但不生效。

**举例：**设置端口Ethernet1/1/3 的Guest-Vlan为Vlan 10。

```
Switch(Config-If-Ethernet1/1/3)#dot1x guest-vlan 10
```

## 7.3.13 dot1x macfilter enable

**命令：dot1x macfilter enable**

**no dot1x macfilter enable**

**功能：** 打开交换机的dot1x地址过滤功能；本命令的no操作为关闭dot1x地址过滤功能。

**命令模式：** 全局配置模式

**缺省情况：** 交换机关闭dot1x地址过滤功能。

**使用指南：** 当打开交换机的dot1x地址过滤功能，交换机会对认证者的MAC地址进行过滤，只有在dot1x地址过滤表中存在的客户发起的认证请求才能被接受。

**举例：** 打开交换机的dot1x地址过滤功能。

```
Switch(config)#dot1x macfilter enable
```

## 7.3.14 dot1x macbased guest-vlan

**命令：dot1x macbased guest-vlan <vlanid>**

**no dot1x macbased guest-vlan**

**功能：**设置指定基于mac认证的端口的guest-vlan；本命令的no操作为删除guest-vlan。

**参数：**<vlanid> 所配置的Vlan id，取值范围为 1-4094。

**命令模式：**端口配置模式。

**缺省情况：**端口上不配置 802.1x macbased guest-vlan功能。

**使用指南：**如果因为没有专用的认证客户端或者客户端版本过低等原因，导致在一定的时间内端口上无客户端认证成功，接入设备会把该用户加入到Guest VLAN。用户在Guest VLAN 中可以获取 802.1x客户端软件，升级客户端，或执行其他一些应用升级程序（例如防病毒软件、操作系统补丁程序等）。当Guest VLAN 中端口下的用户发起认证，如果认证失败，该端口将会仍然处在Guest VLAN 内；如果认证成功，分为以下两种情况：

1 认证服务器下发一个Auto VLAN，这时用户离开Guest VLAN，加入下发的Auto VLAN 中。用户下线后，用户会被重新划分到所配置的Guest Vlan内。

2 认证服务器不下发VLAN，这时用户离开Guest VLAN，加入配置的Native VLAN中。用户下线后，用户会被重新划分到所配置的Guest Vlan内。

**注意事项：**

1 只有基于mac认证且为HYBRID模式的端口才能配置dot1x macbased guest-vlan

2 不同的端口可以配置不同的macbased Guest VLAN，但一个端口只能配置一个macbased Guest VLAN。

**举例：**设置端口Ethernet1/1/3 的Guest-Vlan为Vlan 10。

Switch(Config-If-Ethernet1/1/3)#dot1x macbased guest-vlan 10

## 7.3.15 dot1x macbased port-down-flush

**命令：dot1x macbased port-down-flush**

**no dot1x macbased port-down-flush**

**功能：**打开该命令，当基于mac进行dot1x认证的端口down时，删除该端口上已经认证通过的用户；本命令的no操作不对该情况下已认证用户进行下线操作。

**命令模式：**全局配置模式

**缺省情况：**交换机缺省未打开该命令。

**使用指南：**当基于mac进行认证的用户在不同端口中切换时，需要在原来已经认证上的端口上删除才能在新的端口上重新进行认证，这时需要开启该命令来保证原来端口上删除认证通过的用户。

**举例：**基于mac进行dot1x认证的端口down时，删除该端口上已经认证通过的用户。

Switch(config)#dot1x macbased port-down-flush

## 7.3.16 dot1x max-req

**命令：dot1x max-req *<count>***

**no dot1x max-req**

**功能：**设置交换机在没有收到supplicant回应而重新启动认证前，发送EAP-request/MD5 帧的最大次数；本命令的no操作为恢复缺省值。

**参数：<*count*>** 为发送EAP-request/ MD5 帧的次数，取值范围为 1~10。

**命令模式：**全局配置模式

**缺省情况：**最大次数为 2 次。

**使用指南：**用户在配置发送EAP-request/ MD5 帧的最大次数时，建议使用缺省值。

**举例：**更改发送EAP-request/ MD5 帧的最大次数为 5 次。

Switch(config)#dot1x max-req 5

## 7.3.17 dot1x user allow-movement

**命令：dot1x user allow-movement**

**no dot1x user allow-movement**

**功能：** 打开交换机允许用户迁移端口认证功能；本命令的no操作为关闭用户迁移端口认证功能。

**命令模式：** 全局配置模式

**缺省情况：** 交换机关闭用户迁移端口认证功能。

**使用指南：** 当打开交换机允许用户迁移端口认证功能，交换机允许用户迁移端口认证。一个典型的应用是在交换机下接hub的情况下，用户由hub迁移到交换机其他端口认证，此时可以打开此命令。

**举例：** 打开用户迁移端口认证功能。

Switch(config)#dot1x user allow-movement

## 7.3.18 dot1x user free-resource

**命令：dot1x user free-resource <*prefix*> <*mask*>**

**no dot1x user free-resource**

**功能：** 设置交换机的 802.1x有限资源；本命令的no操作为关闭 802.1x有限资源功能。

**参数：** **<*prefix*>** 为有限资源所在的网段，点分十进制格式； **<*mask*>** 为有限资源所在的网络掩码，点分十进制格式。

**命令模式：** 全局配置模式。

**缺省情况：** 交换机没有缺省的有限资源。

**使用指南：** 本命令只有在端口采用基于用户的接入控制方式时才有效。当采用基于用户的接入控制方式时，没有经过认证的用户能够访问本命令配置的有限资源。而当采用基于端口和基于MAC地址的接入控制方式时，没有经过认证的用户不能够访问任何网络资源。

如果交换机与内网安全管理后台系统TrustView配合使用，则管理员可以在TrustView后台配置该交换机的free resource，然后下发给交换机。

**注意：** 对整个系统只能够配置一条有限资源。

**举例：** 设置有限资源所在的网段为 1.1.1.0，网络掩码为 255.255.255.0。

Switch(Config)#dot1x user free-resource 1.1.1.0 255.255.255.0

## 7.3.19 free-resource destination

本型号交换机不支持此命令

## 7.3.20 dot1x max-user macbased

**命令：dot1x max-user macbased *<number>***

**no dot1x max-user macbased**

**功能：** 设置指定端口最多允许接入的基于MAC地址接入控制方式的用户数；本命令的no操作为恢复缺省值。

**参数：** ***<number>*** 最多允许的接入用户数，取值范围为 1~256。

**命令模式：** 端口配置模式。

**缺省情况：** 每个端口缺省最多允许接入的用户数为 1。

**使用指南：** 本命令只有在端口采用基于MAC地址的接入控制方式时才有效，若通过认证的MAC地址数量超过最多允许接入用户数，超出的用户将无法接入网络。

**举例：** 设置端口 1/1/3 最多允许接入 5 个用户。

Switch(Config-If-Ethernet1/1/3)#dot1x max-user macbased 5

## 7.3.21 dot1x max-user userbased

**命令：dot1x max-user userbased *<number>***

**no dot1x max-user userbased**

**功能：** 设置指定端口最多允许接入的基于用户接入控制方式的用户数；本命令的no操作为恢复缺省值。

**参数：** ***<number>*** 最多允许的接入用户数，取值范围为 1~256。

**命令模式：** 端口配置模式。

**缺省情况：** 每个端口缺省最多允许接入的用户数为 10。

**使用指南：** 本命令只有在端口采用基于用户的接入控制方式时才有效，若通过认证的用户数量超过最多允许接入用户数，超出的用户将无法接入网络。

**举例：** 设置端口Ethernet1/1/3 最多允许接入 5 个用户。

Switch(Config-If-Ethernet1/1/3)#dot1x max-user userbased 5

## 7.3.22 dot1x portbased mode single-mode

**命令：dot1x portbased mode single-mode**

**no dot1x portbased mode single-mode**

**功能：** 配置基于portBase认证方式的单一用户模式；本命令的no操作为关闭该功能。

**参数：** 无。

**命令模式：** 端口配置模式

**缺省情况：** 关闭单一用户模式。

**使用指南：** 本命令仅在端口接入方式为portbased时生效。若在配置单一用户模式前，该端口已经开启dot1x port-method portbased命令，并存在在线用户，则交换机将强制该端口所有用户下线，重新认证时该端口只接受一个认证成功用户，认证通过后该用户可以访问指定的网络资源，但同一端口后续认证用户将被拒绝，并且不能访问网络；关闭单一用户模式后，交换机也会强制已认证用户下线。

**举例：**

Switch(Config-If-Ethernet1/1/1)#dot1x portbased mode single-mode

## 7.3.23 dot1x port-control

**命令：dot1x port-control {auto|force-authorized|force-unauthorized }**

**no dot1x port-control**

**功能：** 设置端口的 802.1x授权状态；本命令的no操作为恢复缺省值。

**参数：** auto为启动 802.1x认证，根据交换机和supplicant之间的认证信息来确定端口处于已授权状态或者非授权状态；force-authorized为设置端口为已授权状态，允许没有经过认证的数据通过该端口；force-unauthorized为设置端口为非授权状态，交换机在该端口不提供对supplicant的认证服务，不允许任何数据通过该端口。

**命令模式：** 端口配置模式

**缺省情况：** 当打开端口的 802.1x功能，端口缺省为auto。

**使能指南：** 如果端口需要对用户进行 802.1x认证，必须将端口认证状态设置为auto。

**举例：** 配置端口Ethernet 1/1/1 为需要 802.1x认证状态。

Switch(config)#interface ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)#dot1x port-control auto

## 7.3.24 dot1x port-method

**命令：dot1x port-method {macbased | portbased | userbased advanced}**

**no dot1x port-method**

**功能：**设置指定端口的接入控制方式；本命令的no操作用来恢复缺省的接入控制方式。

**参数：**macbased为基于MAC地址的接入控制方式；portbased为基于端口的接入控制方式；**webbased** 为基于web认证的接入控制方式； **userbased** 为基于用户的接入控制方式，

其中分为两种控制类型： **advanced** 为高级控制类型。本交换机不支持webbased接入控制方式，userbased接入控制方式中不支持standard控制类型。

**命令模式：**端口配置模式。

**缺省情况：**端口缺省使用基于用户的高级控制类型的接入方式。

**使用指南：**本命令是设置在指定端口上基于何种方式来对用户接入进行认证。当采用基于端口的接入控制方式时，该端口下只能有一个用户接受认证，当认证通过后接入网络访问所有资源；当采用基于MAC地址的接入控制方式时，该端口下同时可以有多个用户接受认证，当认证通过后接入网络访问所有资源。当采用前面这两种接入控制方式时，没有经过认证的用户不能够访问任何网络资源。

而采用基于用户的接入控制方式时，没有经过认证的用户能够访问配置的有限资源。对基于用户的接入控制方式，存在标准控制与高级控制两种类型。基于用户的标准控制类型不对有限资源的访问进行限制，该端口下的所有用户在没有经过认证之前都可以访问有限资源，当认证通过后可以访问所有资源；但基于用户的高级控制类型会对有限资源的访问进行限制，在该端口下只有特定用户在没有经过认证之前能够访问有限资源，当这些用户认证通过后可以访问所有资源，（也可以在TrustView后台设定一个网段资源，用户认证通过后只能访问该网段）。

基于Web的接入控制方式记录的是IP地址，主要应用于汇聚层的三层交换机上。启动端口Web认证代理功能之前，必须先启动全局Web认证代理功能，设置HTTP重定向地址，并且启动端口 802.1x认证功能。注意，基于web认证的接入控制方式在端口上与ip dhcp snooping binding user-control命令互斥。

**注意：**对于基于用户的标准控制类型，需要先配置 802.1x有限资源，且需要和命令dot1x privateclient enable一起使用。

**举例：**配置端口Ethernet 1/1/4 采用基于端口的接入控制方式。

Switch(Config-If-Ethernet1/1/4)#dot1x port-method portbased

## 7.3.25 dot1x privateclient enable

**命令：dot1x privateclient enable**

**no dot1x privateclient enable**

**功能：** 使能交换机强制客户端软件使用私有 802.1x认证报文格式；本命令的no操作为关闭该功能，允许客户端软件使用标准 802.1x认证报文格式。

**命令模式：** 全局配置模式

**缺省情况：** 交换机不支持私有 802.1x认证报文。

**使用指南：** 如果要实现整体解决方案，交换机必须使能支持私有 802.1x认证报文，否则很多应用将不能使用，具体参见DCBI整体解决方案。交换机如果配置强制客户端软件使用私有 802.1x认证报文格式，那么标准的 802.1x客户端将不能通过认证。

**举例：** 使能交换机强制客户端软件使用私有 802.1x认证报文格式。

Switch(config)#dot1x privateclient enable

## 7.3.26 dot1x privateclient protect enable

**命令：dot1x privateclient protect enable**

**no dot1x privateclient protect enable**

**功能：** 使能交换机私有认证保护功能；本命令的no操作为关闭该保护功能。

**命令模式：** 全局配置模式

**缺省情况：** 交换机默认不开启私有认证保护功能。

**使用指南：** 支持私有认证协议部分加密，提高私有认证的安全性。

**举例：** 使能交换机私有认证保护功能。

Switch(config)#dot1x privateclient protect enable

## 7.3.27 dot1x re-authenticate

**命令：dot1x re-authenticate [interface { <IFNAME> | ethernet <interface-name> | port-channel <IFNAME>}]**

**功能：**设置即时对所有端口或某个指定端口进行 802.1x重认证，不必等待超时。

**参数：*<interface-name>***为端口号，如果无参数则表示所有端口。

**命令模式：**全局配置模式

**使用指南：**本命令为全局模式下的命令，当配置本命令后，交换机立刻对客户端进行重认证，不需要等待重新认证定时器超时。认证之后，该命令就无效了。

**举例：**对端口Ethernet 1/1/8 进行即时重认证。

Switch(config)#dot1x re-authenticate interface ethernet 1/1/8

## 7.3.28 dot1x re-authentication

**命令：dot1x re-authentication**

**no dot1x re-authentication**

**功能：**设置允许对supplicant进行周期性重认证；本命令的no操作为关闭该功能。

**命令模式：**全局配置模式

**缺省情况：**缺省情况下周期性重认证功能是关闭的。

**使用指南：**当打开对supplicant的周期性重认证功能，交换机会周期性的对supplicant进行重新认证。一般情况下建议不打开周期性重认证功能。

**举例：**打开对认证者进行周期性重认证功能。

Switch(config)#dot1x re-authentication

## 7.3.29 dot1x timeout quiet-period

**命令：dot1x timeout quiet-period *<seconds>***

**no dot1x timeout quiet-period**

**功能：**设置supplicant在认证失败后端口保持静默状态的时间；本命令的no操作为恢复缺省值。

**参数：**<***seconds***>为端口保持静默状态的时间长度值，单位为秒，取值范围为 1~65535。

**命令模式：**全局配置模式

**缺省情况：**缺省为 10 秒。

**使用指南：**建议使用缺省值。

**举例：**设置静默时间为 120 秒。

Switch(config)#dot1x timeout quiet-period 120

## 7.3.30 dot1x timeout re-authperiod

**命令：dot1x timeout re-authperiod** <***seconds***>

**no dot1x timeout re-authperiod**

**功能：**设置交换机对supplicant重认证的时间间隔；本命令的no操作为恢复缺省值。

**参数：**<***seconds***>重认证的时间间隔，单位为秒，取值范围为 1~65535。

**命令模式：**全局配置模式。

**缺省情况：**缺省为 3600 秒。

**使用指南：**在修改交换机对supplicant的重认证时间间隔时，必须首先打开dot1x re-authentication。如果没有配置交换机的重认证功能,那么所设置交换机对supplicant重认证的时间间隔将不起作用。

**举例：**设置重认证时间为 1200 秒。

Switch(config)#dot1x timeout re-authperiod 1200

## 7.3.31 dot1x timeout tx-period

**命令：dot1x timeout tx-period** <***seconds***>

**no dot1x timeout tx-period**

**功能：**设置交换机对supplicant重发EAP-request/identity帧的时间间隔；本命令的no操作为恢复缺省值。

**参数：**<***seconds***>为重新发送EAP请求帧的时间间隔，单位为秒，取值范围为 1~65535。

**命令模式：**全局配置模式。

**缺省情况：**缺省为 30 秒。

**使用指南：**建议使用缺省值。

**举例：**更改重新发送EAP请求帧的时间间隔为 1200 秒。

Switch(config)#dot1x timeout tx-period 1200

## 7.3.32 dot1x unicast enable

**命令：dot1x unicast enable**

**no dot1x unicast enable**

**功能：** 打开交换机全局 802.1x单播透传功能；本命令的no操作关闭 802.1x单播透传功能。

**命令模式：** 全局配置模式。

**缺省情况：** 交换机在全局下不打开 802.1x单播透传功能。

**使用指南：** 如果要对端口进行 802.1x单播透传功能认证时，首先要打开全局下的 802.1x功能，然后打开全局 802.1x单播透传功能，最后再配置相应端口下的 802.1x功能。

**举例：** 启动交换机的 802.1x单播透传功能，并且打开 1/1/1 号端口 802.1x功能。

```
Switch(config)#dot1x  enable
Switch(config)#dot1x  unicast  enable
Switch(config)#interface  ethernet  1/1/1
Switch(Config-If-Ethernet1/1/1)#dot1x  enable
```

## 7.3.33 dot1x username

**命令:** dot1x username <username> password {0|7}<password>[dynamic-vlan]<1-4094>

**功能:**设置 dot1x 本地认证的用户名，密码和 autovlan

**参数:**<username> 为用户名,0 表示明文,7 表示密文,}<password>为密码,[dynamic-vlan]为动态 vlan,<1-4094>为 vlan 的值

**命令模式:** 全局配置模式

**缺省情况:** 缺省时不配置

**举例:**

```
Switch(config)#dot1x  username  admin  password  0  admin  dynamic-vlan  100
```

## 7.3.34 dot1x web authentication enable

本型号交换机不支持此命令。

## 7.3.35 dot1x web authentication ipv6 passthrough

本型号交换机不支持此命令。

## 7.3.36 dot1x web redirect

本型号交换机不支持此命令。

## 7.3.37 dot1x web redirect enable

本型号交换机不支持此命令。

## 7.3.38 free-mac

本型号交换机不支持此命令。

## 7.3.39 show dot1x

**命令：show dot1x [interface *<interface-list>*]**

**功能：**显示有关dot1x参数信息，如果后面增加参数信息，则显示相应端口的dot1x的状态。

**参数：*<interface-list>***为端口列表。如果无参数，则显示所有端口信息

**命令模式：**特权和配置模式

**使用指南：**通过show dot1x命令可以查看端口的dot1x的相关参数以及端口的dot1x的信息。

**举例：**

1.显示交换机的dot1x全局参数信息。

```
Switch#show dot1x
Global 802.1x Parameters
   reauth-enabled          no
   reauth-period           3600
   quiet-period            10
   tx-period               30
   max-req                 2
   authenticator mode      passive

Mac Filter Disable
MacAccessList :
dot1x-EAPoR Enable
dot1x-privateclient Disable
dot1x-unicast Disable
dot1x-web authentication Enable

802.1x is enabled on ethernet Ethernet1/1/1
Authentication Method:Port based
Max User Number:1
   Status                  Authorized
   Port-control            Auto
   Supplicant              00-03-0F-FE-2E-D3

Authenticator State Machine
   State                   Authenticated
```

Backend State Machine
State Idle

Reauthentication State Machine
State Stop

802.1X is enabled on ethernet Ethernet1/1/16
Authentication Method:web based
Status Authorized
Port-control Auto
Supplicant IP 192.168.1.11
VLAN id 2

| 显示内容 | 解释 |
|---|---|
| Global 802.1x Parameters | 全局 802.1x参数信息 |
| reauth-enabled | 交换机是否打开重认证功能 |
| reauth-period | 重认证时间间隔 |
| quiet-period | 静默时间间隔 |
| tx-period | EAP数据包重传时间间隔 |
| max-req | EAP数据包重传次数 |
| authenticator mode | 交换机认证模式 |
| Mac Filter | 交换机是否使能dot1x地址过滤功能 |
| MacAccessList ： | Dot1x地址过滤表 |
| dot1x-EAPoR | 交换机采用的认证方式（EAP中继 、EAP本地终结） |
| dot1x-privateclient | 交换机是否支持神州数码私有客户端方式 |
| dot1x-web authentication | 交换机是否支持web认证功能 |
| 802.1x is enabled on ethernet Ethernet1/1/1 | 显示端口的dot1x是否打开 |
| Authentication Method: | 端口认证方式（基于MAC，基于端口，基于Web） |
| Status | 端口认证状态 |
| Port-control | 端口授权状态 |
| Supplicant | 认证者MAC地址，webbased方式下为认证者IP地址 |
| Authenticator State Machine | Authenticator状态机状态 |
| Backend State Machine | Backend状态机状态 |
| Reauthentication State Machine | Reauthentication状态机状态 |

## 7.3.40 show dot1x user

命令：show dot1x user

**功能：**显示已通过 dot1x 认证的在线用户信息。

**命令模式：**特权和配置模式.

**使用指南：**此命令通常用于查看在线用户的信息，这些信息对于技术支持人员进行故障诊断和排除非常有用。通过查看已认证的在线用户，可以了解当前网络中的用户活动情况，包括用户名、端口、在线时长、MAC 地址、用户 IP 地址和用户 IPv6 地址等。

**举例:** 显示通过 dot1x 认证的在线用户信息。

```
Switch(config)# show dot1x user
------------------------ total authenticated users: 0 -------------------------------
 UserName          Port          OnTime(sec)         MAC          UserIP          UserIPv6
--------------------------------------------------------------------------------
                ---------------- total authenticated users: 0----------------
```

## 7.3.41 clear dot1x all

**命令：**clear dot1x {all | interface <ethernet IFNAME | IFNAME> | mac WORD | user WORD}

**功能：**删除已通过 dot1x 认证的在线用户。

**参数：***<all>*：删除所有 dot1x 在线用户

*<IFNAME>*：删除特定端口上的 dot1x 在线用户

mac *<WORD>*：删除具有特定 MAC 地址的 dot1x 在线用户

user *<WORD>*：删除具有特定用户名的 dot1x 在线用户

**命令模式：**特权模式。

**使用指南：**用户可以使用此命令从交换机中删除具有特定 MAC 地址、端口、用户名或所有 dot1x 在线用户。

举例：删除所有在线的 dot1x 用户。

```
Switch#clear dot1x all
```

## 7.3.42 user-control limit ipv4

本型号交换机不支持此命令。

## 7.3.43 user-control limit ipv6

本型号交换机不支持此命令。

## 7.3.44 vlan-pool

本型号交换机不支持此命令。

# 7.4 端口、VLAN中MAC、IP数量限制

## 7.4.1 debug ip arp count

**命令：debug ip arp count**

**no debug ip arp count**

**功能：**当打开VLAN中arp数量限制功能debug后，VLAN中动态arp的数量、arp数量已经超出最大允许值的时候都会看到debug信息。本命令的no操作为VLAN中arp数量限制功能debug。

**参数：**无。

**命令模式：**特权模式。

**缺省情况：**缺省没有配置。

**使用指南：**通过该命令显示VLAN中动态arp的数量debug信息。

**举例：**

Switch#debug ip arp count

%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in vlan 1!!

%Jun 14 16:04:40 2007Arp learning will be stopped and some arp will be delete !!

## 7.4.2 debug ipv6 nd count

**命令：debug ipv6 nd count**

**no debug ipv6 nd count**

**功能：**当打开VLAN中neighbor数量限制功能debug后，VLAN中动态neighbor的数量、neighbor数量已经超出最大允许值的时候都会看到debug信息。本命令的no操作为VLAN中neighbor数量限制功能debug。

**参数：**无。

**命令模式：**特权模式。

**缺省情况：**缺省没有配置。

**使用指南：**通过该命令显示VLAN中动态neighbor的数量debug信息。

**举例：**

Switch#debug ipv6 nd count

%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in vlan 1!!

## 7.4.3 debug switchport arp count

**命令：debug switchport arp count**

**no debug switchport arp count**

**功能：**当打开端口arp数量限制功能debug后，端口动态arp的数量、arp数量已经超出最大允许值的时候都会看到debug信息。本命令的no操作为关闭端口arp数量限制功能debug。**参数：**无。

**命令模式：**特权模式

**缺省情况：**缺省没有配置。

**使用指南：**通过该命令显示端口动态arp的数量debug信息。

**举例：**

Switch#debug switchport arp count

%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum li mit in port Ethernet1/1/1

!!%Jun 14 16:04:40 2007 Arp learning will be stopped and some mac will be delete !!

## 7.4.4 debug switchport mac count

**命令：debug switchport mac count**

**no debug switchport mac count**

**功能：**当打开端口mac数量限制功能debug后，端口动态mac的数量、MAC数量已经超出最大允许值的时候都会看到debug信息。本命令的no操作为关闭端口mac数量限制功能debug。

**参数：**无。

**命令模式：**特权模式。

**缺省情况：**缺省没有配置。

**使用指南：**通过该命令显示端口动态mac的数量debug信息。

**举例：**

Switch#debug switchport mac count

%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the maxim um limit in port Ethernet1/1/1

!!%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be delet e !!

## 7.4.5 debug switchport nd count

**命令：debug switchport nd count**

**no debug switchport nd count**

**功能：**当打开端口nd数量限制功能debug后，端口动态nd的数量、nd数量已经超出最大允许值的时候都会看到debug信息。本命令的no操作为关闭端口nd数量限制功能debug。

**参数：**无。

**命令模式：**特权模式

**缺省情况：**缺省没有配置。

**使用指南：**通过该命令显示端口动态nd的数量debug信息。

**举例：**

Switch#debug switchport arp count

%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximu m limit in port Ethernet1/1/1

!!%Jun 14 16:04:40 2007 Neighbor learning will be stopped and some mac will be delet e !!

## 7.4.6 debug vlan mac count

**命令：debug vlan mac count**

**no debug vlan mac count**

**功能：**当打开VLAN中mac数量限制功能debug后，VLAN中动态mac的数量、MAC数量已经超出最大允许值的时候都会看到debug信息。本命令的no操作为VLAN中mac数量限制功能**debug。**

**参数：**无。

**命令模式：**特权模式

**缺省情况：**缺省没有配置。

**使用指南：**通过该命令显示VLAN中动态mac的数量debug信息。

**举例：**

Switch#debug vlan mac count

%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the maxim um limit in vlan 1!!

%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be delete !!

## 7.4.7 ip arp dynamic maximum

**命令：ip arp dynamic maximum *<value>***

**no ip arp dynamic maximum**

**功能：**设置VLAN中允许的最大动态ARP数量，同时开启VLAN中动态ARP数量限制功能；本命令的no操作为关闭VLAN中动态ARP数量限制功能。

**参数：**<*value*>VLAN中动态ARP数上限，取值范围 1~4096。

**缺省情况：**关闭VLAN中动态ARP数量限制功能。

**命令模式：**接口配置模式

**使用指南：**配置VLAN中允许的最大动态ARP数量时，如果VLAN中学习的动态ARP数量已经大于将要配置的最大数量，将删除多出来的动态ARP。

**举例：**

VLAN 1 中打开动态ARP数量限制功能，配置最大数量 50 个。

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)# ip arp dynamic maximum 50

VLAN 1 中关闭动态ARP数量限制功能。

Switch(Config-if-Vlan1)#no ip arp dynamic maximum

## 7.4.8 ipv6 nd dynamic maximum

**命令：ipv6 nd dynamic maximum *<value>***

**no ipv6 nd dynamic maximum**

**功能：**设置VLAN中允许的最大动态NEIGHBOR数量，同时开启VLAN中动态NEIGHBOR数量限制功能；本命令的no操作为关闭VLAN中动态NEIGHBOR数量限制功能。

**参数：**<*value*>VLAN中动态NEIGHBOR数上限，取值范围 1~4096。

**缺省情况：**关闭VLAN中动态NEIGHBOR数量限制功能。

**命令模式：**接口配置模式

**使用指南：**配置VLAN中允许的最大动态NEIGHBOR数量时，如果VLAN中学习的动态NEIGHBOR数量已经大于将要配置的最大数量，将删除多出来的动态NEIGHBOR。

**举例：**

VLAN 1 中打开动态NEIGHBOR数量限制功能，配置最大数量 50 个。

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)# ipv6 nd dynamic maximum 50

VLAN 1 中关闭动态NEIGHBOR数量限制功能。

Switch(Config-if-Vlan1)#no ipv6 nd dynamic maximum

## 7.4.9 mac-address query timeout

本型号交换机不支持此命令。

## 7.4.10 show arp-dynamic count

**命令：show arp-dynamic count { (vlan <1-4096>)| interface ethernet *<portName>*}**

**功能：**显示相应端口、VLAN中的动态ARP数量。

**参数：*<vlan-id>***为显示指定vlan标识，***<portName>***为二层端口名称。

**命令模式：**特权和配置模式。

**使用指南：**通过该命令显示出端口、VLAN中动态ARP的数量。

**举例：**显示配置了ARP数量限制功能的端口和VLAN中的动态ARP数量。

```
Switch(config)#show arp-dynamic count interface ethernet 1/1/3
 Port                MaxCount                CurrentCount
-------------------------------------------------------------------------------------------------
 Ethernet1/1/3               5                       1
-------------------------------------------------------------------------------------------------
Switch(config)# show arp-dynamic count vlan 1
 Vlan                MaxCount                CurrentCount
-------------------------------------------------------------------------------------------------
 1                      55                      15
-------------------------------------------------------------------------------------------------
```

## 7.4.11 show mac-address dynamic count

命令：show **mac-address dynamic count { (vlan <1-4096>)| interface ethernet *<portName>*}**

**功能：** 显示相应端口、VLAN中的动态MAC数量。

**参数：** ***<vlan-id>***为显示指定vlan标识，***<portName>***为二层端口名称。

**命令模式：** 特权和配置模式。

**使用指南：** 通过该命令显示出端口、VLAN中动态MAC的数量。

**举例：** 显示配置了MAC数量限制功能的端口、VLAN中的动态MAC数量。

```
Switch(config)#show mac-address dynamic count interface ethernet 1/1/3
 Port                MaxCount                CurrentCount
-------------------------------------------------------------------------------------------------
 Ethernet1/1/3               5                       1
-------------------------------------------------------------------------------------------------
Switch(config)# show mac-address dynamic count vlan 1
 Vlan                MaxCount                CurrentCount
-------------------------------------------------------------------------------------------------
 1                      55                      15
-------------------------------------------------------------------------------------------------
```

## 7.4.12 show nd-dynamic count

**命令：show nd-dynamic count { (vlan <1-4096>)| interface ethernet *<portName>*}**

**功能：**显示相应端口、VLAN中的动态ND数量。

**参数：*<vlan-id>***为显示指定vlan标识，***<portName>***为二层端口名称。

**命令模式：**特权和配置模式。

**使用指南：**通过该命令显示出端口、VLAN中动态ND的数量。

**举例：**显示配置了ND数量限制功能的端口和VLAN中的动态ND数量。

```
Switch(config)#show nd-dynamic count interface ethernet 1/1/3
 Port                MaxCount                CurrentCount
-------------------------------------------------------------------------------------------------
 Ethernet1/1/3              5                       1
-------------------------------------------------------------------------------------------------
Switch(config)# show nd-dynamic count vlan 1
 Vlan                MaxCount                CurrentCount
-------------------------------------------------------------------------------------------------
 1                          55                      15
-------------------------------------------------------------------------------------------------
```

## 7.4.13 switchport arp dynamic maximum

**命令：switchport arp dynamic maximum *<value>***

**no switchport arp dynamic maximum**

**功能：**设置端口允许的最大动态ARP数量，同时开启端口动态ARP数量限制功能；本命令的no操作为关闭端口动态ARP数量限制功能。

**参数：***<value>* 端口动态ARP数量上限，取值范围 1~4096。

**缺省情况：**关闭端口动态ARP数量限制功能。

**命令模式：**端口配置模式

**使用指南：**配置端口允许的最大动态量数量时，如果端口学习的动态量数量已经大于将要配置的最大数量，将删除多出来的动态ARP。汇聚端口不支持该功能。

**举例：**

端口Ethernet 1/1/2 模式上打开动态ARP数量限制功能，配置最大数量 20 个。

```
Switch(config)#interface ethernet 1/1/2
Switch(Config-If-Ethernet1/1/2)#switchport arp dynamic maximum 20
```

端口 1/1/2 模式上关闭动态ARP数量限制功能。

```
Switch(Config-If-Ethernet1/1/2)#no switchport arp dynamic maximum
```

## 7.4.14 switchport mac-address dynamic maximum

**命令：switchport mac-address dynamic maximum *<value>***

**no switchport mac-address dynamic maximum**

**功能：**设置端口允许的最大动态MAC地址数，同时开启端口动态MAC地址数量限制功能；本命令的no操作为关闭端口动态MAC地址数量限制功能。

**参数：*<value>*** 端口动态MAC地址数上限，取值范围 1~4096。

**缺省情况：**关闭端口动态MAC地址数量限制功能。

**命令模式：**端口配置模式

**使用指南：**配置端口允许的最大动态MAC数量时，如果端口学习的动态MAC地址数量已经大于将要配置的最大数量，将删除多出来的动态MAC地址。该功能与dot1x、MAC绑定等功能互斥，如果该端口启动了dot1x、MAC绑定等功能或者汇聚端口，则不会允许配置该功能。

**举例：端口 1/1/2** 模式上打开动态MAC地址数量限制功能，配置最大数量 20 个。

Switch(config)#interface ethernet 1/1/2

Switch(Config-If-Ethernet1/1/2)#switchport mac-address dynamic maximum 20

端口 1/1/2 模式上关闭动态MAC地址数量限制功能。

Switch(Config-If-Ethernet1/1/2)#no switchport mac-address dynamic maximum

## 7.4.15 switchport mac-address violation

**命令：switchport mac-address violation {protect | shutdown} [recovery <5-3600>]**

**no switchport mac-address violation**

**功能：** 设置端口违背模式；本命令的no操作为恢复违背模式为protect。

**命令模式：** 端口配置模式。

**参数：** protect为保护模式

shutdown为关闭模式

recovery：配置边缘端口执行shutdown违背操作后可以自动恢复

<5-3600>：恢复时间，默认不进行恢复。

**缺省情况：** 端口违背模式缺省为protect，即禁止学习功能，有自己的恢复机制。

**使用指南：** 端口必须使能MAC数量限功能之后才能设置端口违背模式。如果端口违背模式设置为protect，那么当端口MAC地址超过设置的端口安全MAC上限的时候，端口仅仅关闭动态MAC地址学习功能；如果端口违背模式设置为shutdown，那么当端口MAC地址数量超过设置的端口MAC上限的时候，端口将被关闭，用户可以通过no shutdown命令手工或者配置自动恢复超时时间打开该端口。

**举例：** 设置端口 1 的违背模式为shutdown恢复时间为 60s。

Switch(config)#interface Ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)#switchport mac-address violation shutdown recovery 60

## 7.4.16 switchport nd dynamic maximum

**命令：switchport nd dynamic maximum *<value>***

**no switchport nd dynamic maximum**

**功能：**设置端口允许的最大动态NEIGHBOR数量，同时开启端口动态NEIGHBOR数量限制功能；本命令的no操作为关闭端口动态NEIGHBOR数量限制功能。

**参数：*<value>*** 端口动态NEIGHBOR数量上限，取值范围 1~4096。

**缺省情况：**关闭端口动态NEIGHBOR数量限制功能。

**命令模式：**端口配置模式

**使用指南：**配置端口允许的最大动态NEIGHBOR数量时，如果端口学习的动态量数量已经大于将要配置的最大数量，将删除多出来的动态NEIGHBOR。汇聚端口不支持该功能。

**举例：**

端口 1/1/2 模式上打开动态NEIGHBOR数量限制功能，配置最大数量 20 个。

Switch(config)#interface ethernet 1/1/2

Switch(Config-If-Ethernet1/1/2)#switchport nd dynamic maximum 20

端口 1/1/2 模式上关闭动态NEIGHBOR数量限制功能。

Switch(Config-If-Ethernet1/1/2)#no switchport nd dynamic maximum

## 7.4.17 mac-address dynamic maximum

**命令：mac-address dynamic maximum <value>**

**no mac-address dynamic maximum**

**功能：**设置全局允许的最大动态MAC地址数；本命令的no操作为关闭全局动态MAC地址数量限制功能。

**参数：<*value*>** 全局动态MAC地址数上限，取值范围 1~4096。

**缺省情况：**关闭全局动态MAC地址数量限制功能。

**命令模式：**全局配置模式

**使用指南：**配置全局允许的最大动态MAC数量。

**举例：全局**模式上打开动态MAC地址数量限制功能，配置最大数量 20 个。

Switch(config)# mac-address dynamic maximum 20

## 7.4.18 vlan mac-address dynamic maximum

**命令：vlan mac-address dynamic maximum <value> [port-group < 1-128 >]**

**no vlan mac-address dynamic maximum**

**功能：** 设置VLAN中允许的最大动态MAC地址数，同时开启VLAN中动态MAC地址数量限制功能；本命令的no操作为关闭VLAN中动态MAC地址数量限制功能。

**参数：** <*value*>VLAN中动态MAC地址数上限，取值范围 1~4096。

port-group <1-128> 设置聚合口的动态MAC地址数量限制

**缺省情况：** 关闭VLAN中动态MAC地址数量限制功能。

**命令模式：** VLAN配置模式

**使用指南：** 配置VLAN中允许的最大动态MAC数量时，如果VLAN中学习的动态MAC地址数量已经大于将要配置的最大数量，将删除多出来的动态MAC地址。在VLAN中启动动态MAC数

量限制功能后，MAC数量限制针对VLAN中的普通ACCESS口和聚合口，TRUNK口和启动了dot 1x和MAC绑定功能等特殊端口不进行MAC数量限制和统计。

**举例：** VLAN 1 中打开动态MAC地址数量限制功能，配置最大数量 50 个

Switch(config)#vlan1

Switch(Config-Vlan1)#vlan mac-address dynamic maximum 50

VLAN 1 中关闭动态MAC地址数量限制功能。

Switch(Config-Vlan1)#no vlan mac-address dynamic maximum

## 7.4.19 vlan mac-address maximum action

**命令:vlan mac-address dynamic maximum{drop|forward}**

**no vlan mac-address dynamic maximum**

**功能:**设置当 VLAN 中 mac 地址数量超过最大时，多余的报文的处理方式

**参数：**{drop|forward}

**缺省情况：** 该功能关闭

**命令模式：** VLAN配置模式

**使用指南：** 交换机收到大量的报文时，会学习这些报文的 mac 地址，当 mac 地址的数量超过了交换机允许的最大数量时，多余的报文的处理方式，包含丢弃和转发

**举例:**

switch(config-vlan11)#vlan mac-address maximum action drop

# 7.5 AM

## 7.5.1 am enable

**命令：am enable**

**no am enable**

**功能：**全局启动/关闭AM功能。

**参数：**无。

**缺省情况：**默认不启动AM功能。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**在交换机上启动AM功能。

Switch(config)#am enable

在交换机上关闭AM功能。

Switch(config)#no am enable

## 7.5.2 am port

**命令：am port**

**no am port**

**功能：**打开/关闭端口上的AM功能。

**参数：**无。

**缺省情况：**所有端口AM功能关闭。

**命令模式：**端口配置模式。

**举例：**在交换机的端口interface Ethernet 1/1/3 上打开AM功能。

Switch(Config-If-Ethernet 1/1/3)#am port

在交换机的端口interface 1/1/3 上关闭AM功能。

Switch(Config-If-Ethernet 1/1/3)#no am port

## 7.5.3 am ip-pool

**命令：am ip-pool *<ip-address> <num>***

**no am ip-pool *<ip-address> <num>***

**功能：**设置端口的访问管理IP地址段，允许/禁止以该IP地址段内的IP地址为源IP地址的IP报文与ARP报文通过该端口进行转发。

**参数：*<ip-address>*** 是IP地址池中某段地址范围的起始地址。***<num>*** 是从ip-address开始的连续的地址数量，其值不大于 32。

**缺省情况：**IP地址池为空。

**命令模式：**端口配置模式。

**使用指南：**无。

**举例：**在交换机的端口interface Ethernet 1/1/3 上配置允许对源ip地址在起始地址为 10.10.10.1 的连续 10 个ip地址范围内的数据包进行转发。

Switch(Config-If-Ethernet 1/1/3)#am ip-pool 10.10.10.1 10

## 7.5.4 am mac-ip-pool

**命令：am mac-ip-pool *<mac-address> <ip-address>***

**no am mac-ip-pool *<mac-address> <ip-address>***

**功能：**设置端口的访问管理MAC-IP地址，允许/禁止以该MAC-IP地址为源地址的IP报文与ARP报文通过该端口进行转发。

**参数：*<mac-address>***为源MAC地址，***<ip-address>***为包发送的源IP地址，32 位二进制数，用四个隔开的十进制数表示。

**缺省情况：**MAC-IP地址池为空。

**命令模式：**端口配置模式。

**使用指南：**无。

**举例：**在交换机的端口interface Ethernet 1/1/3 上配置允许对源mac地址为 11-22-22-11-11-11，且源ip地址为 10.10.10.1 的数据包进行转发。

Switch(Config-If-Ethernet 1/1/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1

## 7.5.5 no am all

**命令：no am all [ip-pool|mac-ip-pool]**

**功能：**删除全部用户配置的MAC-IP地址池或IP地址池或两个地址池都删除。

**参数：ip-pool**为IP地址池，**mac-ip-pool**为MAC-IP地址池，无参数表示对两个地址池都适用。

**缺省情况：**初始情况两个地址池都为空。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**删除全部已经配置的IP地址池。

Switch(config)#no am all ip-pool

## 7.5.6 show am

**命令：show am [interface *<interface-name>*]**

**功能：**显示已经配置的AM入口表项。

**参数：*<interface-name>***为要显示AM配置信息的物理接口名，无参数表示显示所有接口的AM配置信息。

**命令模式：**特权和配置模式。

**举例：**显示当前所有已经配置的AM入口表项。

```
Switch#show am
AM is enabled

Interface Ethernet1/1/3
          am port
          am ip-pool 30.10.10.1   20
Interface Ethernet1/1/5
          am port
          am ip-pool 50.10.10.1   30
          am mac-ip-pool   00-02-04-06-08-09 20.10.10.5
          am ip-pool 50.20.10.1   20
Interface Ethernet1/1/6
          am port
Interface Ethernet1/1/1
```

```
        am  port
        am  ip-pool  10.10.10.1    20
        am  ip-pool  10.20.10.1    20
```

显示交换机端口ethernet1/1/5 的AM配置入口表项。

```
Switch#show  am  interface  ethernet  1/1/5
AM  is  enabled

Interface  Ethernet1/1/5
        am  port
        am  ip-pool  50.10.10.1    30
        am  mac-ip-pool    00-02-04-06-08-09  20.10.10.5
    am  ip-pool  50.20.10.1    20
```

# 7.6 安全特性

## 7.6.1 dosattack-check srcip-equal-dstip enable

**命令：[no] dosattack-check srcip-equal-dstip enable**

**功能：**使能交换机检查源IP地址等于目的IP地址功能；本命令的no操作为关闭检查源IP地址等于目的IP地址功能。

**参数：**无。

**缺省情况：**交换机不打开检查源IP地址等于目的IP地址功能。

**命令模式：**全局配置模式。

**使用指南：**开启该功能可以丢弃源IP地址等于目的IP地址的数据报。

**举例：**丢弃源IP地址等于目的IP地址的数据报。

```
Switch(config)#  dosattack-check  srcip-equal-dstip  enable
```

## 7.6.2 dosattack-check ipv4-first-fragment enable

本型号交换机不支持此命令。

## 7.6.3 dosattack-check tcp-flags enable

**命令：[no] dosattack-check tcp-flags enable**

**功能：**使能交换机的检查非法TCP标志功能；本命令的no操作为关闭检查非法TCP标志功能。

**参数：**无。

**缺省情况：**交换机不打开检查非法TCP标志功能。

**命令模式：**全局配置模式。

**使用指南：**开启该功能后交换机可以丢弃下述 4 种包含非法TCP标志的数据报：SYN=1 且源端口小于 1024；TCP标志位全为 0 且序列号等于 0；FIN=1，URG=1，PSH=1 且TCP序列号=0；SYN=1 且FIN=1。该功能可以与dosattack-check ipv4-first-fragment enable结合使用，可以阻止ipv4 分片的包含非法TCP标志的数据报。

**举例：**丢弃上述 4 种类型报文中的 1 种或若干种。

Switch(config)# dosattack-check tcp-flags enable

## 7.6.4 dosattack-check srcport-equal-dstport enable

**命令：dosattack-check srcport-equal-dstport enable**

**no dosattack-check srcport-equal-dstport enable**

**功能：**使能交换机的检查源端口等于目的端口功能；本命令的no操作为关闭检查源端口等于目的端口功能。

**参数：**无。

**缺省情况：**交换机不打开检查源端口等于目的端口功能。

**命令模式：**全局配置模式。

**使用指南：**开启该功能后，交换机可以丢弃目的端口等于源端口的TCP和UDP数据报。该功能可以与dosattack-check ipv4-first-fragment enable功能结合使用，可以阻止IPv4 分片的源端口等于目的端口的TCP和UDP数据报。

**举例：**丢弃不分片的源端口等于目的端口的TCP/UDP数据报。

Switch(config)# dosattack-check srcport-equal-dstport enable

## 7.6.5 dosattack-check tcp-fragment enable

本型号交换机不支持此命令

## 7.6.6 dosattack-check tcp-segment

本型号交换机不支持此命令

## 7.6.7 dosattack-check icmp-attacking enable

**命令：[no] dosattack-check icmp-attacking enable**

**功能：**使能交换机的检查ICMP碎片攻击功能；本命令的no操作为关闭检查ICMP碎片攻击功能。

**参数：**无。

**缺省情况：**交换机不打开检查ICMP碎片攻击功能。

**命令模式：**全局配置模式。

**使用指南：**开启该功能后，交换机可以防止ICMP碎片攻击，丢弃分片的ICMP报文和ICMP净荷长度大于指定长度的ICMPv4/v6 的数据报。

**举例：**开启检查ICMP碎片攻击功能。

Switch(config)# dosattack-check icmp-attacking enable

### 7.6.8 dosattack-check icmpV4-size

本型号交换机不支持此命令

### 7.6.9 dosattack-check icmpv6-size

本型号交换机不支持此命令

### 7.6.10 invalid-dip-drop

**命令：invalid-dip-drop {enable|disable}**

**功能：** IPv4 非法目的 IP 检查功能，非法 IP 将禁止通过，并送 cpu 记录信息。

**参数：** **enable** 使能功能，**disable** 关闭功能。

**缺省情况：** 缺省值为 **disable**。

**命令模式：** 全局配置模式。

**使用指南：** 非法目的 IP 包括 x.x.x.0，127.x.x.x，240.0.0.0~255.255.255.254。

**举例：** 开启功能。

Switch(config)#invalid-dip-drop enable

## 7.7 TACACS+

### 7.7.1 tacacs-server authentication host

命令：tacacs-server **authentication host {{vrf <vrf-name>| } <ip-address>} [port <port-number>] [timeout *<seconds>*] [key {0 | 7} <string>] [primary]**

**no tacacs-server authentication host <ip-address>**

**功能：** 设置TACACS+服务器IP地址、监听端口号、认证服务器超时时间、密钥字符串；本命令的no操作为删除TACACS+认证服务器。

**参数：<vrf-name>为指定的VRF名称**

***<ip-address>*** 服务器的IP地址；***<port-number>*** 为服务器的监听端口号，取值范围为 0~65535，其中 0 表示不作认证服务器使用；***<seconds>*** 为TACACS+认证超时定时器值，单位为秒，

取值范围为 1~60； **<string>** 为密钥字符串，如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符，如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符；primary 为主用服务器。

**命令模式：**全局配置模式。

**缺省情况：**系统没有设置TACACS+认证服务器。

**使用指南：** 本命令用于指定与交换机进行认证的TACACS+服务器的IP地址、端口号、认证服务器超时时间和密钥字符串，可以配置多条该命令。其中参数port用于指定认证端口号，该端口号必须与指定的TACACS+服务器上的认证端口号相同，缺省为 49，参数key 和timeout，用于设置该服务器自身单独的key和timeout，如果不配置这两个参数，缺省使用**tacacs-server key *<string>***，**tacacs-server timeout *<seconds>*** 全局配置命令；本命令可以反复配置多条以指定多台与交换机建立通讯关系的TACACS+服务器，其中以配置的顺序作为交换机认证服务器的顺序。如果配置**primary**，则将此TACACS+服务器作为主用服务器。

**举例：**配置TACACS+认证服务器地址为 192.168.1.2，且使用全局配置的key。

Switch(config)#tacacs-server authentication host 192.168.1.2

## 7.7.2 tacacs-server key

**命令：tacacs-server key {0 | 7} *<string>***

**no tacacs-server key**

**功能：** 设置TACACS+认证服务器的密钥；本命令的no操作为删除TACACS+服务器的密钥。

**参数：** ***<string>*** 为TACACS+服务器的密钥字符串，如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符，如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符。

**命令模式：** 全局配置模式。

**使用指南：** 该密钥为交换机与TACACS+服务器进行加密的报文通信使用。该设置的密钥必须与TACACS+服务器上的密钥相同，否则将不能进行正确的TACACS+认证。为保证TACACS+认证数据的安全，建议配置认证服务器密钥。

**举例：** 配置TACACS+服务器认证密钥为test。

Switch(config)# tacacs-server key 0 test

## 7.7.3 tacacs-server nas-ipv4

**命令：tacacs-server nas-ipv4 <ip-address>**

**no tacacs-server nas-ipv4**

**功能：**设置交换设备发送TACACS+报文的IP源地址。本命令的no操作用来删除该配置。

**参数：**<ip-address>为指定发送TACACS+报文使用的IP源地址，点分十进制格式，必须为合法的单播地址。

**缺省情况：**没有配置特定的IP源地址，TACACS+报文源地址使用发送接口的IP地址。

**命令模式：**全局配置模式。

**使用指南：**配置的源地址必须为本机的IP地址，否则发送TACACS+报文时会返回无法绑定IP地址的错误提示。推荐使用loopback接口的地址作为源地址，这样可以避免物理接口down时TACACS+服务器返回的报文不可达。

**举例：**配置交换设备发送TACACS+报文使用源地址 192.168.2.254。

Switch#tacacs-server nas-ipv4 192.168.2.254

### 7.7.4 tacacs-server timeout

**命令：tacacs-server timeout *<seconds>***

**no tacacs-server timeout**

**功能：**设置TACACS+服务器认证超时定时器；本命令的no操作为恢复缺省配置。

**参数：*<seconds>***为TACACS+认证超时定时器值，单位为秒，取值范围为 1~60。

**命令模式：**全局配置模式。

**缺省情况：**缺省为 3 秒。

**使用指南：**本命令指定交换机通过TACACS+服务器认证的等待时间。交换机建立到TACACS+的连接，向TACACS+ Server发送请求认证数据包后，等待接收相应的响应数据包。若在规定的等待时间内没有建立连接或者没有接收到TACACS+服务器的回应，则认为这次认证失败。

**举例：**配置tacacs+服务器超时定时器为 30 秒。

Switch(config)#tacacs-server timeout 30

### 7.7.5 debug tacacs-server

**命令：debug tacacs-server**

**no debug tacacs-server**

**功能：**打开TACACS+的调试信息；本命令的no操作为关闭TACACS+的调试信息。

**命令模式：**特权配置模式。

**参数：**无。

**使用指南：**打开TACACS+调试信息，可以查看TACACS+协议的协商过程，在遇到故障时有助于监测故障原因。

**举例：**打开TACACS+协议的调试信息。

Switch#debug tacacs-server

## 7.8 RADIUS

### 7.8.1 aaa enable

**命令：aaa enable**

**no aaa enable**

**功能：**使能交换机AAA认证功能；本命令的no操作为关闭AAA认证功能。

**命令模式：**全局配置模式。

**参数：**无。

**缺省情况：**交换机不打开AAA认证功能。

**使用指南：**如果要实现交换机的 802.1x 认证功能，必须打开交换机的AAA认证功能。

**举例：**打开交换机的AAA功能。

Switch(config)#aaa enable

## 7.8.2 aaa-accounting enable

**命令：aaa-accounting enable**

**no aaa-accounting enable**

**功能：**打开交换机的AAA计费功能；本命令的no 操作为关闭AAA计费功能。

**命令模式：**全局配置模式。

**缺省情况：**交换机不打开AAA计费功能。

**使用指南：**打开交换机的计费功能后，交换机将对认证者所在的端口的流量信息或上网时间进行计费。在计费开始时，交换机向Radius计费服务器发出计费开始的消息；并且每隔 5 秒钟针对在线用户向Radius计费服务器发一次计费包；在计费停止时，又向Radius计费服务器发送计费停止的消息。注意：只有当计费功能打开时，交换机在用户下线时才通知Radius计费服务器，用户的下线消息并不会通知Radius认证服务器。

**举例：**打开交换机的AAA计费功能。

Switch(config)#aaa-accounting enable

## 7.8.3 aaa-accounting update

**命令：aaa-accounting update {enable|disable}**

**功能：**打开或关闭交换机的AAA计费更新功能。

**命令模式：**全局配置模式。

**缺省情况：**交换机打开AAA计费更新功能。

**使用指南：**打开交换机的计费更新功能后，对于每个在线用户，交换机将定时向计费服务器发送计费报文。

**举例：**关闭交换机的AAA计费更新功能。

Switch(config)#aaa-accounting update disable

## 7.8.4 aaa group server radius

**命令：aaa group server radius <WORD>**

**no aaa group server radius <WORD>**

**功能：**使用该命令配置一个 aaa radius 服务器组名称，并进入 aaa radius 服务器组配置模式，该命令的 no 形式删除这个 aaa radius 服务器组。

**参数:**WORD：aaa group server radius 的名字，它是一个长度不大于 32 的字符串, (a-z, A-Z, 0-9, '_', '-'and space are allowed)

**缺省情况：**无。

**命令模式：**全局配置模式

**使用指南：**使用该命令配置一个 aaa radius 服务器组。

**举例：**使用该命令配置一个 aaa radius 服务器组，组名为 group1。

Switch (Config)# aaa group server radius group1

## 7.8.5 debug aaa packet

**命令：debug aaa packet {send|receive|all} interface {ethernet <*interface-number*>| <*interface-name*>}**

**no debug aaa packet {send|receive|all} interface {ethernet <*interface-number*>| <*interface-name*>}**

**功能：**打开aaa的收发包调试信息；本命令的no操作为关闭aaa的收发包调试信息。

**参数：**

| | |
|---|---|
| send： | 打开aaa的发包调试信息。 |
| receive： | 打开aaa的收包调试信息。 |
| all： | 打开aaa的收包和发包调试信息。 |
| <*interface-number*>: | 端口序号。 |
| <*interface-name*>: | 端口名称。 |

**命令模式：**特权配置模式。

**使用指南：**打开aaa收发包调试信息，可以查看Radius协议收到的和发出的报文，在遇到故障时有助于监测故障原因。

**举例：**打开端口 1/1/1 下aaa所有收发包调试信息。

Switch#debug aaa packet all interface Ethernet 1/1/1

## 7.8.6 debug aaa detail attribute

**命令：debug aaa detail attribute interface {ethernet <*interface-number*>| <*interface-name*>}**

**no debug aaa detail attribute interface {ethernet <*interface-number*>| <*interface-name*>}**

**功能：**打开aaa的Radius属性细节调试信息；本命令的no操作为关闭aaa的Radius属性细节调试信息。

**参数：**<*interface-number*>: 端口序号。

<*interface-name*>: 端口名称。

**命令模式：**特权配置模式。

**使用指南：**打开aaa的Radius属性细节调试信息，可以查看Radius报文的Radius属性细节，在遇到故障时有助于监测故障原因。

**举例：**打开端口 1/1/1 下aaa的Radius属性细节调试信息。

Switch#debug aaa detail attribute interface Ethernet 1/1/1

## 7.8.7 debug aaa detail connection

**命令：debug aaa detail connection**

**no debug aaa detail connection**

**功能：**打开aaa的连接细节调试信息；本命令的no操作为关闭aaa的连接细节调试信息。

**参数：**无。

**命令模式：**特权配置模式。

**使用指南：**打开aaa连接细节调试信息，可以查看aaa的连接细节信息，在遇到故障时有助于监测故障原因。

**举例：**打开aaa连接细节调试信息。

Switch#debug aaa detail connection

## 7.8.8 debug aaa detail escape

**命令：debug aaa detail escape**

**功能：**打开 radius server 逃生功能调试信息。本命令的 no 操作为关闭 radius server 逃生功能调试信息。

**命令模式：**特权配置模式。

**使用指南：**打开逃生功能调试信息，可以查看 aaa 模块对 radius server 的周期性探测，在遇到故障时有助于监测故障原因。

**举例：**打开 radius server 逃生功能调试信息。

Switch#debug aaa detail escape

## 7.8.9 debug aaa detail event

**命令：debug aaa detail event**

**no debug detail event**

**功能：**打开aaa的事件调试信息；本命令的no操作为关闭aaa的事件调试信息。

**参数：**无。

**命令模式：**特权配置模式。

**使用指南：**打开aaa事件调试信息，可以查看Radius协议运行过程的产生的各种事件信息，在遇到故障时有助于监测故障原因。

**举例：**打开aaa的事件调试信息。

Switch#debug aaa detail event

## 7.8.10 debug aaa error

**命令：debug aaa error**

**no debug error**

**功能：**打开aaa的出错调试信息；本命令的no操作为关闭aaa的出错调试信息。

**参数：**无。

**命令模式：**特权配置模式。

**使用指南：**打开aaa出错调试信息，可以查看Radius协议运行过程中产生的各种出错信息，在遇到故障时有助于监测故障原因。

**举例：**打开aaa出错调试信息。

Switch#debug aaa error

## 7.8.11 radius-server attributes

**命令：**radius-server attributes{8021p,acl,egress-bandwidth,ingress-bandwidth,vlan} enable

**功能:**设置接收报文的扩展属性

**参数:**8021p 为 802.1p 属性， acl 为 acl 属性， egress-bandwidth 为出方向的带宽属性，ingress-bandwidth 为入方向的带宽属性,vlan 为 vlan 属性

**缺省情况:**缺省时不配置

举例:

switch(config)#lradius-server attributes 8021p enable

## 7.8.12 radius nas-ipv4

**命令：radius nas-ipv4** ***<ip-address>***

**no radius nas-ipv4**

**功能：**设置交换设备发送RADIUS报文的IP源地址。本命令的no操作用来删除该配置。

**参数：*<ip-address>***为指定发送RADIUS报文使用的IP源地址，点分十进制格式，必须为合法的单播地址。

**缺省情况：**没有配置特定的IP源地址，RADIUS报文源地址使用发送接口的IP地址。

**命令模式：**全局配置模式。

**使用指南：**配置的源地址必须为本机的IP地址，否则发送RADIUS报文时会返回无法绑定IP地址的错误提示。推荐使用loopback接口的地址作为源地址，这样可以避免物理接口down时RADIUS服务器返回的报文不可达。

**举例：**配置交换设备发送RADIUS报文使用源地址 192.168.2.254。

radius nas-ipv4 192.168.2.254

## 7.8.13 radius nas-ipv6

**命令：radius nas-ipv6 *<ipv6-address>***

**no radius nas-ipv6**

**功能：** 设置交换设备发送RADIUS报文的IPv6 源地址。本命令的no操作用来删除该配置。

**参数：** ***<ipv6-address>*** 为指定发送RADIUS报文使用的IPv6 源地址，必须为合法的单播地址。

**缺省情况：** 没有配置特定的IPv6 源地址，RADIUS报文源地址使用发送接口的IPv6 地址。

**命令模式：** 全局配置模式

**使用指南：** 配置的源地址必须为本机的IPv6 地址，否则发送RADIUS报文时会返回无法绑定IPv6 地址的错误提示。推荐使用loopback接口的地址作为源地址，这样可以避免物理接口down时RADIUS服务器返回的报文不可达。

**举例：** 配置交换设备发送RADIUS报文使用IPv6 源地址 2001:da8:456::1。

radius nas-ipv6 2001:da8:456::1

## 7.8.14 radius-server accounting host

**命令：radius-server accounting host {{vrf <vrf-name>| } *<ipv4-address>* | *<ipv6-address>*} [port *<port-number>*] [key {0 | 7} *<string>*] [primary]**

**no radius-server accounting host {*<ipv4-address>* | *<ipv6-address>*}**

**功能：** 设置RADIUS 计费服务器IPv4 或者IPv6 地址和监听端口号、是否为主用服务器；本命令的no 操作为删除RADIUS计费服务器。

**参数：<vrf-name>为指定的VRF名称**

**{*<ipv4-address>* | *<ipv6-address>*}** 服务器的IPv4 地址或者IPv6 地址。

***<port-number>*** 为服务器的监听端口号，取值范围为 0~65535。

***<string>*** 为密钥字符串。如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符；如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符。

**[primary]** 是否设为主用服务器，在配置radius server时，可以配置多个，使用顺序如果不配置primary时，按配置顺序查找可以使用的radius server。如果配置的primary，则首先使用这个radius server。

**命令模式：**全局配置模式。

**缺省情况：**系统没有设置RADIUS 计费服务器。

**使用指南：**本命令用于指定与交换机进行计费的RADIUS 服务器的IPv4 地址或者IPv6 地址和端口号，可以配置多条该命令。其中参数***<port-number>***用于指定计费端口号，该端口号必须与指定的RADIUS服务器上的计费端口号相同，缺省为 1813，

若将该端口号配置为 0，端口随机产生，可能导致无效。本命令可以反复配置多条以指定多台与交换机建立通讯关系的RADIUS 服务器，交换机将向所有配置好的计费服务器发送计费报文，所配置的这些RADIUS计费服务器可以相互作为备份服务器。如果配置primary，则将此RADIUS服务器作为主用服务器。只能配置一个RADIUS主服务器，不管该服务器使用IPv4还是IPv6 地址。

**举例：**设置RADIUS 计费服务器的IPv6 地址为 2004:1:2:3::2，端口号为 3000，并作为主用服务器。

Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary

## 7.8.15 radius-server authentication host

**命令：radius-server authentication host {{vrf <vrf-name>| } *<ipv4-address>* | *<ipv6-address>*} [port *<port-number>*] [key *{0* | 7} <string>] [primary] [access-mode {dot1x | telnet}]**

**no radius-server authentication host {*<ipv4-address>* | *<ipv6-address>*}**

**功能：** 设置RADIUS 认证服务器IPv4 地址或者IPv6 地址和监听端口号、加密密钥、是否为主用服务器以及使用模式；本命令的no 操作为删除RADIUS 服务器。

**参数：<vrf-name>为指定的VRF名称**

**{*<ipv4-address>* | *<ipv6-address>*}** 服务器的IPv4 地址或者IPv6 地址。

***<port-number>*** 为服务器的监听端口号，取值范围为：0～65535。

***<string>*** 为密钥字符串。如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符；如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符。

**[primary]**是否设为主用服务器，在配置radius server时，可以配置多个，使用顺序如果不配置primary时，按配置顺序查找可以使用的radius server。如果配置的primary，则首先使用最后配置的这个radius server。

**[access-mode {dot1x | telnet}]** 指明当前RADIUS服务器只为 802.1x认证或telnet远程认证使用，默认所有服务均可使用当前RADIUS服务器。

**命令模式：**全局配置模式。

**缺省情况：**系统没有设置RADIUS 认证服务器。

**使用指南：**本命令用于指定与交换机进行认证的RADIUS服务器的IPv4 地址或者IPv6 地址和端口号以及密钥字符串和访问模式，可以配置多条该命令。其中参数***<port-number>***用于指定认证端口号，该端口号必须与指定的RADIUS服务器上的认证端口号相同，缺省为 1812，若将该端口号配置为 0 端口随机产生，可能导致无效。本命令可以反复配置多条以指定多台与交换机建立通讯关系的RADIUS 服务器，其中以配置的顺序作为交换机认证服务器的顺序，当第一服务器有响应（无论是认证成功或失败）时，交换机不向下一个服务器发送认证请求。如果配置 primary，则将此RADIUS服务器作为主用服务器。当前RADIUS服务器若没有配置key <string>，则使用命令radius-server key <string>全局配置的密钥。另外，还可以通过acces

s-mode选项指定当前RADIUS服务器只为 802.1x认证或 telnet远程认证使用。默认不配置access-mode选项，所有远程认证服务均可使用该RADIUS服务器。

**举例：**配置RADIUS认证服务器的IPv6 地址为 2004:1:2:3::2。

Switch(config)#radius-server authentication host 2004:1:2:3::2

## 7.8.16 radius-server dead-time

**命令：radius-server dead-time *<minutes>***

**no radius-server dead-time**

**功能：**设置RADIUS服务器死机后的恢复时间；本命令的no操作为恢复缺省配置。

**参数：*<minutes>***为RADIUS服务器死机的恢复时间值，单位为分钟，取值范围为 1~255。

**命令模式：**全局配置模式。

**缺省情况：**缺省为 5 分钟。

**使用指南：**本命令指定交换机等待RADIUS服务器由不可访问状态恢复为可以访问状态的时间。交换机查知该服务器不能访问时，交换机将该服务器状态设置成无效状态，超过上述配置间隔时间后，系统将认证服务器状态设置成有效。

**举例：**配置RADIUS服务器死机后的恢复时间为 3 分钟。

Switch(config)#radius-server dead-time 3

## 7.8.17 radius-server key

**命令：radius-server key {0 | 7} *<string>***

**no radius-server key**

**功能：** 设置RADIUS服务器（包括认证和计费）的密钥；本命令的no操作为删除RADIUS服务器的密钥。

**参数：*<string>*** 为RADIUS服务器的密钥字符串。如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符；如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符。

**命令模式：** 全局配置模式。

**使用指南：** 该密钥为交换机与设置的RADIUS服务器进行加密的报文通信使用。该设置的密钥必须与交换机设置的RADIUS服务器上的密钥相同，否则将不能进行正确的RADIUS认证和计费。

**举例：** 配置RADIUS认证密钥为test。

Switch(config)#radius-server key 0 test

## 7.8.18 radius-server retransmit

**命令：radius-server retransmit *<retries>***

**no radius-server retransmit**

**功能：**设置RADIUS认证报文的重传次数；本命令的no操作为恢复缺省配置。

**参数：*<retries>***为RADIUS服务器的重传次数，取值范围为 0~100。

**命令模式：**全局配置模式。

**缺省情况：**缺省为 3 次。

**使用指南：**本命令指定交换机向RADIUS服务器发送数据包后，接收不到RADIUS服务器的回应需要重新发送该数据包的次数。在没有收到认证服务器发送的认证信息时，需向认证服务器重传AAA的认证请求。重传AAA请求计数达到设定的重传次数并仍没有接收到服务器的回应后，认为该服务器已不能正常工作，交换机将该服务器设置为不可访问状态。

**举例：**配置RADIUS认证报文重传次数为 5 次。

Switch(config)#radius-server retransmit 5

## 7.8.19 radius-server timeout

**命令：radius-server timeout *<seconds>***

**no radius-server timeout**

**功能：**设置RADIUS服务器超时定时器；本命令的no操作为恢复缺省配置。

**参数：*<seconds>***为RADIUS服务器超时定时器值，单位为秒，取值范围为 1~1000。

**命令模式：**全局配置模式。

**缺省情况：**缺省为 3 秒。

**使用指南：**本命令指定交换机等待RADIUS服务器响应的时间间隔。交换机发送给RADIUS Server的请求数据包后，等待接收相应的响应数据包。若在规定的等待时间内没有接收到RADIUS服务器的回应，则根据当时的状态重新发送请求数据包或将该服务器状态设置为不可访问。

**举例：**配置RADIUS服务器超时定时器为 30 秒。

Switch(config)#radius-server timeout 30

## 7.8.20 radius-server accounting-interim-update timeout

**命令：radius-server accounting-interim-update timeout *<seconds>***

**no radius-server accounting-interim-update timeout**

**功能：**设置计费更新报文发送的时间间隔；本命令的no操作为恢复缺省配置。

**参数：*<seconds>***为计费更新报文发送的时间间隔，单位为秒，取值范围为 60～3600。

**命令模式：**全局配置模式。

**缺省情况：**缺省的计费更新报文发送的时间间隔为 300 秒。

**使用指南：**本命令指定NAS发送计费更新报文的时间间隔。为了对用户实施实时计费，从用户上线时间开始，每间隔设定的时间，NAS会向RADIUS服务器发送一次该在线用户的计费更新报文。

计费更新报文发送时间间隔的取值与NAS支持的最大用户数有一定的相关性要求——取值越小，NAS支持的最大用户数也就越少；取值越大，NAS支持的最大用户数也就越的多。以下是计费更新报文发送时间间隔与最大用户数之间的推荐比例关系：

表 6-1 计费更新报文发送时间间隔与用户量之间的推荐比例关系

| 最大用户数 | 计费更新报文发送时间间隔（秒） |
|---|---|
| 1~299 | 300（缺省值） |
| 300~599 | 600 |
| 600~1199 | 1200 |
| 1200~1799 | 1800 |
| ≥1800 | 3600 |

**举例：**NAS支持的最大用户数为 700 人，配置计费更新报文发送的时间间隔为 1200 秒。

Switch(config)#radius-server accounting-interim-update timeout 1200

## 7.8.21 Server

**命令：server <*A.B.C.D*>**

**no server <*A.B.C.D*>**

**功能：**使用该命令添加 aaa radius 服务器组的服务器，no 形式删除该服务器。

**参数: <*A.B.C.D*>：**server 的 IP 地址

**缺省情况：**无

**命令模式：**aaa radius 服务器组配置模式

**使用指南：**使用该命令在 aaa radius 服务器组中添加 radius 服务器地址

**举例：**使用该命令在 aaa radius 服务器组 group1 中添加一个 radius 服务器，IP 地址为 192.168.10.1

Switch (Config)# aaa group server radius group1

Switch (config-sg-radius)# server 192.168.10.1

## 7.8.22 show aaa authenticated-user

**命令：show aaa authenticated-user**

**功能：**显示已经通过认证的在线用户。

**命令模式：**特权和配置模式。

**使用指南：**一般只关心在线用户的信息，其它显示信息为技术支持人员用于故障诊断和排错。

**举例：**

Switch#show aaa authenticated-user

---------- authenticated users ----------

UserName Retry RadID Port EapID ChapID OnTime UserIP MAC

---

---------- total: 0 ----------

## 7.8.23 show aaa authenticating-user

**命令：show aaa authenticating-user**

**功能：**显示正在进行认证的用户。

**命令模式：**特权和配置模式。

**使用指南：**一般只关心正在进行认证用户的信息，其它显示信息为技术支持人员用于故障诊断和排错。

**举例：**

Switch#show aaa authenticating-user

---------- authenticating users ----------

User-name Retry-time Radius-ID Port Eap-ID Chap-ID Mem-Addr State

---

---------- total: 0 ----------

## 7.8.24 show aaa config

**命令：show aaa config**

**功能：**显示radius client已经有的配置命令令并包含其中IPv6 有关信息。

**命令模式：**特权和配置模式。

**使用指南：**显示交换机是否打开aaa认证、计费功能，及密钥，认证、计费服务器的信息等。

**举例：**

Switch#show aaa config

显示的内容举例如下（如果是布尔量，1 代表TRUE，0 代表FALSE）：

---------- AAA config data ----------

Is Aaa Enabled = 1 ：1 表示aaa认证使能，0 表示没被使能

Is Account Enabled= 0 ：1 表示aaa计费使能，0 表示没被使能

MD5 Server Key = yanshifeng ：认证密钥

authentication server sum = 2 ：配置的认证服务器的个数

authentication server[0].sock_addr =2:100.100.100.60.1812：第一个认证服务器的地址协议族、IP和端口号

.Is Primary = 1：是为主用服务器

.Is Server live by radius escape function = 1: 开启逃生功能时该服务器是否存活

.Is Server Dead = 0：该服务器是否死掉

.Socket No = 0 ：通向该服务器的本地socket号

authentication server[1].sock_addr =10:2004:1:2::2.1812

.Is Primary = 0

.Is Server live by radius escape function = 1: 开启逃生功能时该服务器是否存活

.Is Server Dead = 0

.Socket No = 0

accounting server sum = 2 ：配置的计费服务器的个数

accounting server[0].sock_addr =2:100.100.100.65.1813：计费服务器的地址协议族、IP和端口号

.Is Primary = 1：是为主用服务器

.Is Server Dead = 0：该服务器是否死掉

.Socket No = 0：通向该服务器的本地socket号

accounting server[1].sock_addr = 10:2004::7.1813

.Is Primary = 1

.Is Server Dead = 0

.Socket No = 0

Time Out = 5s：发送请求包后，等待回应超时时间

Retransmit = 3：超时重传次数

Dead Time = 5min：对死掉服务器开始重试的时间间隔

Account Time Interval = 0min：计费时间间隔

## 7.8.25 show radius authenticated-user count

**命令：show radius authenticated-user count**

**功能：**显示已经通过认证的在线用户数量。

**命令模式：**特权和配置模式。

**举例：**

Switch#show radius authenticated-user count

The authenticated online user num is: 105

## 7.8.26 show radius authenticating-user count

**命令：show radius authenticating-user count**

**功能：**显示正在进行认证的用户数量。

**命令模式：**特权和配置模式。

**举例：**

Switch#show radius authenticating-user count

The authenticating user num is: 10

## 7.8.27 show radius count

**命令：show radius {authenticated-user|authenticating-user} count**

**功能：显示radius认证用户的统计信息。**

**参数：authenticated-user：显示已经通过认证的在线用户；authenticating-user：正在进行认证的用户。**

**命令模式：特权和配置模式。**

**使用指南：通过show** radius count命令可以查看radius认证用户的相关统计信息。

**举例：**

1.显示有关radius认证通过用户的统计信息。

Switch#show radius authenticated-user count

The authenticated online user num is: 0

2.显示radius正在认证用户的统计信息。

Switch#sho radius authenticating-user count

# 7.8.28 radius逃生

## 7.8.28.1 radius-server escape { enable | disable}

**命令：radius-server escape enable**

**radius-server escape disable**

**功能：**使能交换机 AAA 的 radius server 逃生功能。

**参数：**无。

**缺省情况：**默认关闭逃生功能。

**命令模式：**全局配置模式。

**使用指南：**打开 radius server 逃生功能以后，对于 dot1x 或者 portal 认证客户端来说，当 dot1x 或者 portal 认证客户端上所配置的 radius server 不可达时，此时 dot1x 或者 portal 认证客户端的流量放行。当探测到所配置的认证服务器重新可达时，删除对逃生客户端先前下发的流量放行规则表项。

**举例：**使能全局认证功能。

Switch (Config)# radius-server escape enable

## 7.8.28.2 radius-server escape detection-interval

**命令：radius-server escape detection-interval {default| < second >)}**

**功能：**配置对 radius server 进行可达性探测的周期。

**参数：**default:时间间隔恢复成默认的 3 分钟；

second:配置时间间隔值，取值范围为 1-1800 秒。

**缺省情况：**默认时间是 180 秒。

**命令模式：**全局配置模式。

**使用指南：**配置的时间间隔越小，逃生功能越灵敏。但是配置的时间间隔要大于（Retransmit+1）* Time Out。

**举例：**配置对 radius server 探测的周期为 120 秒。

Switch(config)#radius-server escape detection-interval 120

## 7.8.29 radius-server attributes

**命令：**radius-server attributes{8021p,acl,egress-bandwidth,ingress-bandwidth,vlan} enable

**功能:**设置接收报文的扩展属性

**参数:**8021p 为 802.1p 属性， acl 为 acl 属性， egress-bandwidth 为出方向的带宽属性，ingress-bandwidth 为入方向的带宽属性,vlan 为 vlan 属性

**举例:**

switch(config)#lradius-server attributes 8021p enable

# 7.9 SSL

## 7.9.1 ip http secure-server

**命令：ip http secure-server**

**no ip http secure-server**

**功能：**启动/关闭SSL功能。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**本命令用于启动/关闭SSL功能。当启动SSL功能后，用户在客户端通过https访问交换机时，交换机就会和客户端进行SSL握手连接，形成安全的SSL连接通道，在此之后应用层协议所传送的数据都会被加密，从而保证通信的私密性。

**举例：**启动SSL功能

Switch(config)#ip http secure-server

## 7.9.2 ip http secure-port

**命令：ip http secure-port** ***<port-number>***

**no ip http secure-port**

**功能：**配置/删除SSL服务监听的端口号。

**参数：***<port-number>*设置的监听端口号，范围 1025～65535。默认配置为 443。

**命令模式：**全局配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**如果使用了本命令配置了端口号，则使用配置的端口号进行监听。如果改变了https使用的端口号，用户尝试使用https连接的时候必须指定端口号为修改后的，如：https://device:port_number。端口号的修改每次都需要重启SSL功能。

**举例：**配置SSL使用的端口号 1028。

Switch(config)#ip http secure-port 1028

## 7.9.3 ip http secure-ciphersuite

**命令：ip http secure-ciphersuite { aes128-gcm-sha256| aes128-sha| aes128-sha256| aes256-sha| aes256-sha256| des-cbc3-sha| ecdhe-rsa-aes128-gcm-sha256| ecdhe-rsa-aes128-sha| ecdhe-rsa-aes256-sha}**

**no ip http secure-ciphersuite**

**功能：**配置/删除SSL使用的加密套件。

**参数：**

| | |
|---|---|
| **aes128-gcm-sha256** | 算法AES128-GCM-SHA256 |
| **aes128-sha** | 算法AES128-SHA |
| **aes128-sha256** | 算法AES128-SHA256 |
| **aes256-sha** | 算法AES256-SHA |
| **aes256-sha256** | 算法AES256-SHA256 |
| **des-cbc3-sha** | 算法DES-CBC3-SHA |
| **ecdhe-rsa-aes128-gcm-sha256** | 算法ECDHE-RSA-AES128-GCM-SHA256 |
| **ecdhe-rsa-aes128-sha** | 算法ECDHE-RSA-AES128-SHA |
| **ecdhe-rsa-aes256-sha** | 算法ECDHE-RSA-AES256-SHA |

**命令模式：**全局配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**如果使用了本命令配置了加密套件，则使用配置的加密套件进行加密的协商。加密套件的修改每次都需要重启SSL功能。使用des-cbc-sha加密套件时，必须ie7.0 以上的浏览器才能支持。

**举例：**配置SSL使用的加密套件aes128-gcm-sha256。

switch(config)#ip http secure-ciphersuite aes128-gcm-sha256

### 7.9.4 show ip http secure-server status

**命令：show ip http secure-server status**

**功能：**显示配置的SSL信息。

**参数：**无。

**命令模式：**特权和配置模式。

**举例：**

Switch#show ip http secure-server status

HTTP secure server status: Enabled

HTTP secure server port: 1028

HTTP secure server ciphersuite: rc4-128-sha

### 7.9.5 debug ssl

**命令：debug ssl**

**no debug ssl**

**功能：**显示使用SSL功能信息，该命令的no形式关闭DEBUG显示。

**参数：**无。

**命令模式：**特权模式。

**举例：**

Switch#debug ssl

%Jan 01 01:02:05 2006 ssl will to connect to web server 127.0.0.1:9998

%Jan 01 01:02:05 2006 connect to http security server sucess!

## 7.10 VLAN-ACL

### 7.10.1 clear vacl statistic vlan

**命令：clear vacl [in | out] statistic vlan [<*1-4094*>]**

**功能：**此命令可清除VACL的统计信息。

**参数：in | out：**清除入口/出口流量统计。

**vlan <*1-4094*>：**需要清除VACL统计信息的VLAN，如果不输入VLAN ID，则清除所有VLAN的统计信息。

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**

清除Vlan1 的VACL统计信息：

Switch# clear vacl statistic vlan 1

## 7.10.2 show vacl vlan

**命令：show vacl [in | out] vlan [<*1-4094*>] | [begin | include | exclude <*regular-expression*>]**

**功能：**此命令显示VACL的配置及统计信息。

**参数：in | out**：显示入口/出口配置及统计。

**vlan <*1-4094*>**：需要显示VACL配置及统计信息的VLAN，如果不输入VLAN ID，则显示所有VLAN的VACL配置及统计信息。

**begin | include | exclude <*regular-expression*>**：正则表达式

. 匹配除换行符以外的任意字符

^ 匹配行的开始

$ 匹配行的结束

| 匹配竖线左侧或右侧的字符串

[0-9] 匹配数字 0 到 9

[a-z] 匹配小写字母a到z

[aeiou] 匹配aeiou中的任意一个字母

\ 转义字符，用于匹配元字符，例如\$将匹配字符$，而不是匹配字符串的结束

\w 匹配字母或数字或下划线

\b 匹配单词的开始或结束

\W 匹配任意不是字母，数字，下划线的字符

\B 匹配不是单词开头或结束的位置

[^x] 匹配除了x以外的任意字符

[^aeiou] 匹配除了aeiou这几个字母以外的任意字符

* 重复零次或更多次

+ 重复一次或更多次

{n} 重复n次

{n,} 重复n次或更多次

{n,m} 重复n到m次

目前使用的正则表达式不支持以下语法：

\s 匹配任意的空白符

\d 匹配数字

\S 匹配任意不是空白符的字符

\D 匹配任意非数字的字符

? 重复零次或一次

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**

Switch (config)#show vacl in vlan 2

Vlan 2:

IP Ingress access-list used is 100, traffic-statistics Disable.

Switch (config)# show vacl in vlan 3

Vlan 3:

IP Ingress access-list used is myacl, packet(s) number is 5.

| 显示信息 | 解释 |
|---|---|
| Vlan 2 | VLAN名称 |
| 100、myacl | VACL的名字 |
| traffic-statistics Disable | VACL统计功能关闭 |
| packet(s) number is 5 | 匹配此VACL的out-profile数据报文总数 |

## 7.10.3 vacl ip access-group

**命令：vacl ip access-group {<1-299> | WORD} {in | out} [traffic-statistic] vlan WORD**

**no vacl ip access-group {<1-299> | WORD} {in | out} vlan WORD**

**功能：**此命令在指定VLAN上配置IP类型的VACL。

**参数：<1-299> | WORD：**可配置数字IP ACL（包括:标准访问列表规则 <1-99>, 扩展访问列表规则 <100-299>）或命名ACL。

**in | out：**过滤入口\出口流量。

**traffic-statistic**:开启VACL匹配报文数统计功能。

**vlan WORD**:要绑定VACL的VLAN。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**可以用“；”或“-”来输入或多个VLAN，但最多不超过 128 个，并且CLI长度小于 80 个字符。目前在VLAN Egress方向上绑定IP ACL时不支持绑定匹配tcp/udp range的ACL。

**举例：**为Vlan1-5，6，7-9 配置数字IP ACL，并开启统计功能。

Switch(config)#vacl ip access-group 1 in traffic-statistic vlan 1-5;6;7-9

## 7.10.4 vacl ipv6 access-group

命令：vacl **ipv6 access-group (<500-699> | WORD) {in | out} (traffic-statistic|) vlan WORD**

**no ipv6 access-group {<500-699> | WORD} {in | out} vlan WORD**

**功能：** 此命令在指定VLAN上配置IPv6 类型的VACL。

**参数：** <500-699> | WORD：可配置数字IP ACL（包括:IPv6 标准访问列表规则 <500-599>, IPv6 扩展访问列表规则 <600-699>）或命名ACL。

**in | out：**过滤入口/出口流量。

**traffic-statistic：**开启VACL匹配报文数统计功能。

**vlan WORD：**要绑定VACL的VLAN。

**命令模式：** 全局配置模式。

**缺省情况：** 无。

**使用指南：** 可以用';'或'-'来输入或多个VLAN，但最多不超过 128 个，并且CLI长度小于 80 个字符。目前在VLAN Egress方向上绑定IPv6 ACL时不支持绑定匹配flowlabel的ACL。

**举例：** 为Vlan5 配置数字IPv6 ACL。

Switch(config)#vacl ipv6 access-group 600 in traffic-statistic vlan 5

## 7.10.5 vacl mac access-group

命令：vacl **mac access-group {<700-1199> | WORD} {in | out} [traffic-statistic] vlan WORD**

**no vacl mac access-group {<700-1199> | WORD} {in | out} vlan WORD**

**功能：** 此命令在指定VLAN上配置MAC类型的VACL。

**参数：** <700-1199> | WORD：可配置数字IP ACL（包括:<700-799> MAC标准访问列表，<1100-1199> MAC扩展访问列表）或命名ACL。

**in | out：** 过滤入口\出口流量。

**traffic-statistic：** 开启VACL匹配报文数统计功能。

**vlan WORD：** 要绑定VACL的VLAN。

**命令模式：** 全局配置模式。

**缺省情况：** 无。

**使用指南：** 可以用';'或'-'来输入或多个vlan，但最多不超过 128 个，并且CLI长度小于 80 个字符。

**举例：** 为Vlan1-5 配置数字MAC ACL。

Switch(config)#vacl mac access-group 700 in traffic-statistic vlan 1-5

## 7.10.6 vacl mac-ip access-group

命令：vacl **mac-ip access-group {<3100-3299> | WORD} {in | out} [traffic-statistic] vlan WORD**

**no vacl mac-ip access-group {<3100-3299> | WORD} {in | out} vlan WORD**

**功能：** 此命令在指定VLAN上配置MAC-IP类型的VACL。

**参数：** <3100-3299>| WORD：可配置数字IP ACL或命名ACL。

**in | out：**过滤入口/出口流量。

**traffic-statistic**：开启VACL匹配报文数统计功能。

**vlan WORD**：要绑定VACL的VLAN。

**命令模式**： 全局配置模式。

**缺省情况**： 无。

**使用指南**： 可以用';'或'-'来输入或多个VLAN，但最多不超过 128 个，并且CLI长度小于 80 个字符。目前在VLAN Egress方向上绑定MAC-IP ACL时不支持绑定匹配tcp/udp range的ACL。

**举例**： 为Vlan1、2、5 配置数字MAC-IP ACL。

Switch(config)#vacl mac-ip access-group 3100 in traffic-statistic vlan 1;2;5

# 7.11 PPPoE中间代理

## 7.11.1 debug pppoe intermediate agent packet {receive | send} interface ethernet <interface-name>

本型号交换机不支持此命令

## 7.11.2 pppoe intermediate-agent

**命令：pppoe intermediate-agent**

**no pppoe intermediate-agent**

**功能**：开启全局PPPoE intermediate agent功能；本命令的no操作为关闭全局PPPoE intermediate agent功能。

**参数**：无。

**缺省情况**：默认关闭PPPoE intermediate agent全局功能。

**命令模式**：全局配置模式

**使用指南**：全局开启PPPoE IA功能后，对PPPoE发现阶段报文按照相关配置进行处理。

**举例**：开启全局PPPoE intermediate-agent功能。

Switch(config)#pppoe intermediate-agent

## 7.11.3 pppoe intermediate-agent（端口）

本型号交换机不支持此命令

## 7.11.4 pppoe intermediate-agent circuit-id

**命令：pppoe intermediate-agent circuit-id <string>**

**no pppoe intermediate-agent circuit-id <string>**

**功能：**配置端口的circuit id；本命令的no操作为取消该配置。

**参数：** <string>：circuit-id，最大字符数为 63 个字节。

**缺省情况：**端口默认配置为空。

**命令模式：**端口配置模式

**使用指南：**此命令为每个端口单独配置circuit-id，优先级高于命令pppoe intermediate-agent identifier-string的配置。

**举例：**在属于vlan 3 的端口ethernet1/1/3 上配置circuit-id为abcd/efgh。

Switch(config-if-ethernet1/1/3)#pppoe intermediate-agent circuit-id abcd/efgh

端口ethernet1/1/3 接收到PPPoE报文后，添加的vendor tag中circuit-id value为”abcd/efgh”。

## 7.11.5 pppoe intermediate-agent delimiter

**命令：pppoe intermediate-agent delimiter <WORD>**

**no pppoe intermediate-agent delimiter**

**功能：**设置circuit-id和remote-id内各个字段的分隔符，本命令的no操作为取消该分隔符的设置。

**参数：** <WORD>：分隔符，取值范围为(#|.|,|;|:|/|space)。

**缺省情况：**默认情况下各个字段用’\0’分隔。

**命令模式：**全局配置模式

**使用指南：**当设置此分隔符后，添加的circuit-id和remote-id中各个字段便用此分隔符作分隔标记。注意：必须开启全局pppoe intermediate-agent功能。

**举例：**设置分隔符。

Switch(config)#pppoe intermediate-agent delimiter space

## 7.11.6 pppoe intermediate-agent format

**命令：pppoe intermediate-agent format (circuit-id | remote-id) (hex | ascii)**

**no pppoe intermediate-agent format (circuit-id | remote-id)**

**功能：**设置circuit-id和remote-id的表示形式，十六进制或者ASCII码，本命令的no操作为取消相应设置。

**参数：** hex：十六进制表示。

ascii：ASCII码表示。

**缺省情况：**默认此配置为空。

**命令模式：**全局配置模式

**使用指南：**在vendor tag中添加的circuit-id和remote-id会按照此项配置字符串形式进行添加。注意：必须开启全局pppoe intermediate-agent功能。

**举例：**配置在信任端口ethernet1/1/1 开启vendor tag剥离功能。

Switch(config)#pppoe intermediate-agent format remote-id ascii

## 7.11.7 pppoe intermediate-agent remote-id

**命令：pppoe intermediate-agent remote-id <string>**

**no pppoe intermediate-agent remote-id <string>**

**功能：**配置端口的remote id；本命令的no操作为取消该配置。

**参数：** <string>：remote-id，最大字符数为 63 个字节。

**缺省情况：**端口默认配置为空。

**命令模式：**端口配置模式

**使用指南：**配置每个端口remote-id；如果没有配置，则使用交换机Mac作为remote-id value。

**举例：** 在交换机端口ethernet1/1/2 上配置remote-id为abcd。

Switch(config-if-ethernet1/1/2)#pppoe intermediate-agent remote-id abcd

## 7.11.8 pppoe intermediate-agent trust

**命令：pppoe intermediate-agent trust**

**no pppoe intermediate-agent trust**

**功能：**配置端口为信任端口；本命令的no操作为配置端口为非信任端口。

**参数：**无。

**缺省情况：**端口默认为非信任端口。

**命令模式：**端口配置模式

**使用指南：**连接服务器端的端口必须配置为信任端口。注意：至少有一个端口可以连接到PPPoE服务器，并且此端口为trust端口。

**举例：**配置交换机端口ethernet1/1/1 为信任端口。

Switch(config-if-ethernet1/1/1)#pppoe intermediate-agent trust

## 7.11.9 pppoe intermediate-agent type self-defined circuit-id

本型号交换机不支持此命令

## 7.11.10 pppoe intermediate-agent type self-defined remoteid

**命令：pppoe intermediate-agent type self-defined remoteid {mac | vlan-mac | hostname | string WORD}**

**no pppoe intermediate-agent type self-defined remote-id**

**功能：**配置自定义形式的remote-id，本命令的no操作为取消该配置。

**参数：** mac：以太网端口MAC地址。

vlan-mac：IP接口MAC地址。

hostname：交换机主机名。

string WORD：指定的关键字标识。

**缺省情况：**默认此配置为空。

**命令模式：**全局配置模式

**使用指南：**此处配置的各个字段的先后顺序就是remote-id中各个字段的先后顺序。

**举例：**在交换机上配置自定义的remote-id形式为string abcd mac hostname。

Switch(config)#pppoe intermediate-agent type self-defined remoteid string abcd mac hostname

## 7.11.11 pppoe intermediate-agent type tr-101 circuit-id access-node-id

**命令：pppoe intermediate-agent type tr-101 circuit-id access-node-id <string>**

**no pppoe intermediate-agent type tr-101 circuit-id access-node-id**

**功能：**配置添加tr-101 标准的vendor tag中circuit ID的access-node-id域的值。

**参数：**<string>：access-node-id，最大字符数为 47 个字节。

**缺省情况：**默认access-node-id为交换机的MAC地址。

**命令模式：**全局配置模式

**使用指南：**使用此配置生成vendor tag标识中circuit ID的access-node-id。circuit-id value为access-node-id +“ eth ”+ Slot ID + 分隔符 + Port Index + 分隔符 + Vlan ID，其中access-node-id为n个字节(n<48)，“ eth ”为space + e + t + h + space共占 5 个字节，Slot ID占 2 个字节，Port Index占 3 个字节，Vlan ID占 4 个字节，，分隔符占 1 个字节。默认情况下，circuit-id中access-node-id的值为：交换机Mac，占 6 个字节。例如：交换机Mac地址为”0a0b0c0d0e0f”, Slot ID为 12，Port Index为 34，Vlan ID为 567。默认配置下的circuit-id value为”0a0b0c0d0e0f eth 12/034:0567”。

**举例：**配置vendor tag标识中circuit ID的access-node-id值为abcd。

Switch(config)#pppoe intermediate-agent access-node-id abcd

在属于vlan 3 的端口ethernet1/1/3 接收到PPPoE报文后，添加的vendor tag中circuit-id value为”abcd eth 01/103:0003”。

## 7.11.12 pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter

**命令：pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> option {sp | sv | pv | spv} delimiter <WORD> [delimiter <WORD>]**

**no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter**

**功能：** 配置添加tr-101 标准的vendor tag标识中的circuit-id，no 命令为删除此设置。

**参数：**<string>：identifier-string，最大字符数为 47 个字节。

{sp | sv | pv | spv}：此选项是对slot，port，vlan的组合形式的选择;sp代表slot和port，sv代表slot和vlan，pv代表port和vlan，spv代表slot、port和vlan。

<WORD>：slot，port，vlan中间的分隔符，取值范围是( # | . | , | ; | : | / | space)。注意，在spv组合模式下有两个delimiter WORD，第一个是slot和port间的分隔符，第二个是port和vlan间的分隔符。

**缺省情况：**默认此配置为空。

**命令模式：**全局配置模式

**使用指南：**此命令用于配置全局的circuit id，优先级高于命令pppoe intermediate-agent access-node-id的配置。circuit-id value为access-node-id +“ eth ”+ Slot ID + 分隔符 + Port Index + 分隔符 + Vlan ID，其中access-node-id为n个字节(n<48)，“ eth ”为space + e + t + h + space共占 5 个字节，Slot ID占 2 个字节，Port Index占 3 个字节，Vlan ID占 4 个字节，分隔符占 1 个字节。

**举例：**在交换机上配置access-node-id为xyz，使用spv组合模式，Slot ID和Port ID的分隔符为“#”，Port ID和Vlan ID的分隔符为“/”。

Switch(config)#pppoe intermediate-agent identifier-string xyz option spv delimiter # delimiter /

Switch# show pppoe intermediate-agent identifier-string option delimiter

config identifier string is : xyz

config option is : slot , port and vlan

the first delimiter is : "# "

the second delimiter is : "/ "

在属于vlan 3 的端口ethernet1/1/3 接收到PPPoE报文后，添加的vendor tag中circuit-id value为”xyz eth 01#003/0003”。

## 7.11.13 pppoe intermediate-agent vendor-tag strip

**命令：pppoe intermediate-agent vendor-tag strip**

**no pppoe intermediate-agent vendor-tag strip**

**功能：**开启端口的vendor-tag剥离功能，本命令的no操作为取消端口的vendor-tag剥离功能。

**参数：** 无。

**缺省情况：**默认没有开启端口的vendor-tag剥离功能。

**命令模式：**端口配置模式

**使用指南：**如果收到的从服务器发送给客户端的报文中含有vendor tag标识，则剥离该vendor tag。

注意：1．必须开启全局pppoe intermediate-agent trust功能。

2．必须在信任端口上配置。

**举例：**配置在信任端口ethernet1/1/1 开启vendor tag剥离功能。

Switch(config-if-ethernet1/1/1)#pppoe intermediate-agent trust

Switch(config-if-ethernet1/1/1)#pppoe intermediate-agent vendor-tag strip

## 7.11.14 show pppoe intermediate-agent access-node-id

**命令：show pppoe intermediate-agent access-node-id**

**功能：**显示用户配置的access node id。

**参数：**无。

**缺省情况：**默认配置信息为空。

**命令模式：**全局配置模式 **使用指南：**通过该命令显示用户配置的access-node-id。

**举例：**显示access-node-id的配置信息。

switch(config)#pppoe intermediate-agent access-node-id abcd

Switch#show pppoe intermediate-agent access-node-id

pppoe intermediate-agent access-node-id is : abcd

## 7.11.15 show pppoe intermediate-agent identifier-string option delimiter

**命令：show pppoe intermediate-agent identifier-string option delimiter**

**功能：**显示用户配置的identifier-string；slot，port，vlan的组合形式和分隔符。

**参数：**无。

**缺省情况：** 默认配置信息为空。

**命令模式：**特权配置模式

**使用指南：**显示用户配置的identifier-string；slot，port，vlan的组合形式和分隔符。

**举例：**显示pppoe intermediate-agent identifier-string的配置信息。

Switch(config)#pppoe intermediate-agent identifier-string abcd option spv delimiter # delimiter /

Switch# show pppoe intermediate-agent identifier-string option delimiter

config identifier string is : abcd

config option is : slot , port and vlan

the first delimiter is : "# "

the second delimiter is : "/ "

## 7.11.16 show pppoe intermediate-agent info

**命令：show pppoe intermediate-agent info [interface ethernet <interface-name>]**

**功能：**显示所有端口或指定端口的PPPoE IA相关配置信息。

**参数：**ethernet:物理端口

interface-name：端口名

**缺省情况：**默认端口配置信息为空。

**命令模式：**特权配置模式

**使用指南：**查找相应端口的配置信息，显示该端口是否为信任端口，是否开启剥离功能，是否开启限速，显示配置的circuit id和remote id。

**举例：**显示端口ethernet 1/1/2 的pppoe intermediate-agent的配置信息。

```
Switch# show pppoe intermediate-agent info interface ethernet 1/1/2
Interface      IA      Trusted   vendor Strip   Rate limit   circuit id  remote id
----------  ------  ------  -----------  -------  ---------  ----------
Ethernet1/1/2  yes        no         no              no         test1/port1    host1
```

# 7.12 QoS

## 7.12.1 accounting

**命令：accounting**

**no accounting**

**功能：**为分类后的流量设置统计功能。

**参数：**无。

**缺省情况：**缺省不设置统计功能。

**命令模式：**策略分类表配置模式。

**使用指南：**功能开启后，会对策略分类表中的流量增加统计功能，单桶模式，报文经过policy时仅会有绿色和红色两种颜色，打印统计信息时in-profile表示绿色，out-profile表示红色；双桶模式下，会有三种颜色的报文，打印统计信息时in-profile表示绿色，out-profile表示红色和黄色。

**举例：**将满足c1 分类规则的报文进行统计。

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#accounting
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

## 7.12.2 class

**命令：class <*class-map-name*> [insert-before <class-map-name>]**

**no class <*class-map-name*>**

**功能：**对应一个class（分类表），并进入策略分类表模式；本命令的no操作为删除指定策略分类表。

**参数：<*class-map-name*>** 指定策略分类表采用的分类表名称。

**insert-before <*class-map-name*>** 将新配置的class插入到某个已存在的class前面，以此提高新配置class的优先级。

**缺省情况：**缺省不存在策略分类表。

**命令模式：**策略表配置模式。

**使用指南：**建立策略分类表以前，必须先建立一个策略表并且进入策略表模式；在策略分类表模式中，可以对按照分类表分类的包流量进行分类和下一跳配置。

**举例：**在策略表中增加一个策略分类表c1，再新增加一个策略分类表 2 并插入到c1 之前。

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#class c2 insert-before c1
Switch(Config-PolicyMap-p1-Class-c2)#exit
```

## 7.12.3 class-map

**命令：class-map <*class-map-name*>**

**no class-map <*class-map-name*>**

**功能：**建立一个class-map（分类表），并进入class-map模式；本命令的no操作为删除指定的class-map。

**参数：<*class-map-name*>** 分类表的名称。

**缺省情况：**缺省不存在分类表。

**命令模式：**全局配置模式。

**使用指南：**

**举例：**创建和删除一个命名为c1 的class-map。

```
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)# exit
Switch(config)#no class-map c1
```

## 7.12.4 clear mls qos statistics

**命令：clear mls qos statistics [interface <interface-name> | vlan <vlan-id>]**

**功能：**清除特定端口或者vlan Policy Map的Accounting数据，如果不带参数，清除所有的Policy Map的Accounting数据。

**参数：<vlan-id>**：VlAN ID

**<interface-name>**：交换机端口

**缺省情况**：缺省不设置动作。

**命令模式**：特权配置模式。

**使用指南**：清除特定端口或者vlan Policy Map的Accounting数据，如果不带参数，清除所有的Policy Map的Accounting数据。

**举例**：清除Vlan 100 的Policy Map统计。

Switch#clear mls qos statistics vlan 100

## 7.12.5 drop

**命令：drop**

**no drop**

**功能**： 丢掉分类后的数据包；本命令的no操作为取消分配的动作。

**参数**： 无。

**缺省情况**： 缺省不设置动作。

**命令模式**： 策略分类表配置模式

**使用指南**： 配置了该命令以后，丢弃指定的报文。

**举例**：

对满足分类表c1 的报文进行丢弃。

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class c1

Switch(Config-PolicyMap-p1-Class-c1)#drop

Switch(Config-PolicyMap-p1-Class-c1)#exit

Switch(Config-PolicyMap-p1)#exit

## 7.12.6 Match

**命令：match {access-group <acl-index-or-name> | ip dscp <dscp-list>| ip precedence <ip-precedence-list> | ipv6 access-group <acl-index-or-name> | ipv6 dscp <dscp-list> | ipv6 flowlabel <flowlabel-list>| vlan <vlan-list>| cos <cos-list>}**

**no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos}**

**功能**：设置分类表中的匹配标准；本命令的no操作为删除指定的匹配标准。

**参数：access-group <acl-index-or-name>** 匹配指定的IP ACL，MAC ACL或IPV6 标准ACL表，参数为ACL的编号或名称；

**ip dscp <*dscp-list*>** 和 **ipv6 dscp <dscp-list>** 匹配指定的DSCP值，参数为一个DSCP值列表，最多由 8 个DSCP值组成，范围为 0～63；

**ip precedence <ip-precedence-list>** 匹配指定的IP优先级值，参数为一个IP优先级值列表，最多由 8 个IP优先级值组成，范围为 0～7；

**ipv6 access-group <acl-index-or-name>** 匹配指定的IPV6 ACL表，参数为IPV6 ACL的编号或名称；

**ipv6 flowlabel <flowlabel-list>** 匹配指定的IPV6 FL流标签，参数为IPV6 FL的流标签值，范围为 0～1048575；

**vlan <vlan-list>** 匹配指定的VLAN ID值，参数为一个VLAN ID列表，最多 8 个VLAN ID, 范围为 1～4094；

**cos *<cos-list>*** 匹配指定的CoS值，参数为一个CoS列表，最多 8 个CoS。范围为 0～7。

**缺省情况：**缺省不存在匹配标准。

**命令模式：**class-map（分类表）配置模式。

**使用指南：**每个分类表内，只能设置一条匹配标准。当匹配ACL时，permit规则就是匹配项，应用Policy Map action；deny规则就是排除项，不应用Policy Map action。（PBR特性中不支持deny规则的下发，请注意规避。）如果已经配置了其他的match规则，提示无法配置，如果配置相同的match规则，就覆盖处理。

**举例：**创建一个命名为c1 的class-map，设置此class-map的分类规则是匹配IP Precedenc优先级为 0 的报文。

```
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match ip precedence 0
Switch(Config-ClassMap-c1)#exit
```

## 7.12.7 mls qos aggregate-policy

**命令：**

**单桶模式：**

**mls qos aggregate-policy <policer_name> <bits_per_second> <normal_burst_bytes> [{conform-action ACTION | exceed-action ACTION }]**

**双桶模式：**

**mls qos aggregate-policy <policer_name> <bits_per_second> <normal_burst_bytes> (pir <peak_rate_bps> | <maximum_burst_bytes>) ({conform-action ACTION | exceed-action ACTION | violate-action ACTION )**

**ACTION 定义：**

**drop | transmit | set-internal-priority <intp_value> | set-cos-transmit <new-cos> | set-dscp-transmit <new-dscp> | set-prec-transmit <ip-precedence> | set-drop-precedence < new-drop-priority>**

**[no] mls qos aggregate-policy <policer_name>**

**功能： 定义一条聚合 Policy 命令，根据配置参数解析出令牌桶的工作模式，是单速单桶、单速双桶还是双速双桶，并且给不同颜色报文设置相应动作。no 命令删除模式配置。**

**参数：**

**policer_name：聚合 Policy 名字**

**bits_per_second：约定信息速率，即 CIR(Committed Information Rate),单位是千比特/秒，范围是 1～16777200；**

**normal_burst_bytes：约定突发尺寸，即 CBS(Committed Burst Size)**，单位是千字节，范围是 1～16383, 当设置的 CBS 值超过芯片的最大值时，采用芯片支持的最大值设置硬件，CLI 无提示信息；

**maximum**_burst_bytes：峰值突发尺寸，即 PBS**(Peak Burst Size)**，单位是千字节，范围是 1～16383, 当设置的 PBS 值超过芯片的最大值时，采用芯片支持的最大值设置硬件，CLI 无提示信息；注：此配置仅在双桶模式存在；

**pir** peak_rate_bps：峰值信息速率,即 PIR**(Peak Information Rate)**，peak_rate_bps 单位是千比特/秒，范围是 **1～16777200**，当没有配置 PIR 时，Poilce 工作在单速双桶模式，配置了 PIR 时，Police 工作在双速双桶模式；注：此配置仅在双桶模式存在；

**conform-action: 当没有超过 CIR 速率，报文为绿色时，采取的策略**,缺省为 transmit

**exceed-action：当超出 CIR 速率但仍小于 PIR 速率，报文为黄色时采取的策略，缺省为 Drop**

**violate-action：当超出 PIR 速率，报文为红色时采取的策略，缺省为 Drop**

**ACTION 包括：**

**drop/transmit 丢弃/通过报文**

**set-dscp-transmit <new-dscp>** 修改 dscp

**set-prec-transmit< ip-precedence > 修改 TOS**

**命令模式： 全局配置模式。**

**缺省状态：** 缺省不存在策略动作，对于动作的缺省配置，exceed-action 和 violate-action 的缺省动作都为 drop。

使用指南： 命令行可以同时支持单桶配置和双桶配置，根据是否配置 PIR 或者 PBS 来确定是选择单桶还是双桶；在进行命令行配置时，如果配置了 CBS 后，直接配置动作，就是单速单桶双色；CBS 后仅配置 PBS 为单速双桶三色；CBS 后配置 PIR 和 PBS 则为双速双桶三色。Policy Map 中同时选择了 set 和 policy（policy aggregate），并且 set 和 policy（policy aggregate）选择的动作相同，policy（policy aggregate）选择的动作可以覆盖 set 选择的动作。

**举例：**设置双速双桶工作模式，CIR 为 10000，CBS 为 1000，PIR 为 20000，PBS 为 10000，当超出 CIR 速率但仍小于 PIR 速率，报文为黄色时，采取的策略为 transmit：

**Switch(config)#mls qos aggregate-policy color 10000 1000** pir 20000 10000 exceed-action transmit

## 7.12.8 mls qos cos

**命令：mls qos cos {<*default-cos*> }**

**no mls qos cos**

**功能：**配置交换机端口的缺省CoS值；本命令的no操作为恢复缺省情况。

**参数：<*default-cos*>** 交换机端口的缺省CoS值，范围为 0～7。

**缺省情况：**缺省CoS值为 0。

**命令模式：**端口配置模式。

**使用指南：**配置交换机端口的缺省CoS值。在默认配置下，不管报文是否带tag，从该端口进入报文的入口cos都为设定的默认值，如果报文不带tag，则报文打上tag中的cos值为设定的值。

**举例：**在端口ethernet 1/1/1 配置缺省cos值为 7，即从此端口进来的报文如果不带cos值，则分配默认cos值为 7。

Switch(config)#interface ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)#mls qos cos 7

## 7.12.9 mls qos internal-priority

本型号交换机不支持此命令。

## 7.12.10 mls qos map

**命令：mls qos map (cos-dp <dp1…dp8> | cos-intp <IntPrio1…IntPrio8> | dscp-dp <in-dscp list> to <dp> | dscp-dscp <in-dscp list> to <out-dscp> |dscp-intp <in-dscp list> to <intp> | exp-dp <dp1…dp8> | exp-intp <IntPrio1…IntPrio8>)**

**no mls qos map (cos-dp | cos-intp | dscp-dp | dscp-dscp | dscp-intp | exp-dp | exp-intp)**

**功能：** 设置QoS的优先级映射，no命令恢复缺省映射值。

**参数：**

**cos-dp <dp1…dp8>** 定义CoS值到丢弃优先级(drop precedence, dp)值的映射，<dp1..dp8>为 8 个丢弃优先级值分别对应CoS值的 0～7，每个丢弃优先级值之间用空格隔开，丢弃优先级值的范围为 0～2；

**cos-intp <IntPrio1…IntPrio8>** 定义CoS值到内部优先级的值的映射；

**dscp-dp** 定义dscp值到丢弃优先级的映射；

**dscp-dscp** 定义入口dscp值到出口dscp值的映射，<in-dscp list>输入的dscp值，最多 8 个，相互之间使用空格隔开，范围 0-63，<out-dscp>输出的dscp值，范围 0-63；

**dscp-intp** 定义dscp值到内部优先级的值的映射；

**exp-dp <dp1…dp8>** 定义exp值到丢弃优先级的映射；

**exp-intp <IntPrio1…IntPrio8>** 定义exp值到内部优先级的映射；

**缺省情况：** 缺省映射值为：

Ingress COS-TO-Internal-Priority map:

| COS: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| INTP: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

Ingress DSCP-TO-Internal-Priority map:

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

Ingress COS-TO-Drop-Precedence map:

| COS: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| DP: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Ingress DSCP-TO-DSCP map:

| d1 : d2 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1: | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 2: | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 3: | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| 4: | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 |
| 5: | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 |
| 6: | 60 | 61 | 62 | 63 | | | | | | |

Ingress DSCP-TO-Drop-Precedence map:

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

Ingress EXP-TO-Internal-Priority map:

| EXP: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| INTP: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

Ingress EXP-TO-Drop-Precedence map:

| EXP: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| DP: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Egress Internal-Priority-TO-EXP map:

| INTP: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| EXP: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

**命令模式：** 全局配置模式。

**使用指南：** 这里的INTP指的都是交换芯片内部优先级设置，DP指的是丢弃优先级。由于内部dscp值有 64 个，而芯片内部优先级为 8 个，所以dscp-cos映射需要连续的 8 个内部dscp值映射到同一个INTP或DP。

## 7.12.11 mls qos queue algorithm

**命令：mls qos queue algorithm {sp | wrr | wdrr}**

**no mls qos queue algorithm**

**功能：**配置了该命令以后，端口队列调度算法被设定。

**参数：sp:**严格优先级，队列数大的优先级高

**wrr:** 选择wrr算法

**wdrr:** 选择wdrr算法

**缺省情况：**端口缺省队列调度算法为wrr。

**命令模式：**端口配置模式。

**使用指南：**配置了该命令以后，端口队列调度算法被设定。

**举例：**配置端口队列调度算法为sp。

Switch(interface-ethernet1/1/1)#mls qos queue algorithm sp

## 7.12.12 mls qos queue drop-algorithm

本型号交换机不支持此命令。

## 7.12.13 mls qos queue statistics enable

**命令：mls qos queue statistics enable**

**no mls qos queue statistics enable**

**功能：**使能或禁止队列功能统计。

**参数：**无。

**缺省状态：**默认关闭队列统计功能。

**命令模式：**全局模式。

**使用指南：**通过该命令使能统计功能，让计数器对出端口的每个队列分别统计数据包。

**举例：**打开队列统计功能。

switch(config)#mls qos queue statistics enable

## 7.12.14 mls qos queue weight

本型号交换机不支持此命令。

## 7.12.15 mls qos queue wrr weight

**命令：mls qos queue wrr weight <weigh0..weigh7>**

**no mls qos queue wrr weight**

**功能：**配置了该命令以后，端口队列权重被设定。

**参数：<weight0..weight7>**定义队列调度权重，本配置对于WRR有效，SP算法无效。当权重配置为 0 时，这个队列采用SP算法进行调度，WRR算法进化为SP+WRR算法。WRR权重的绝对值是没有意义的，WRR通过八个权重值的比率来分配带宽。不同的芯片支持的选择权重范围不一样，如果设置超过芯片范围，报错并提示正常的范围。对于支持 4 个队列的芯片，参数变成< weight1..weight4>。

**缺省情况：队列权重为** 1 2 3 4 5 6 7 8。

**命令模式：** 端口模式。

**使用指南：** 如果有队列的权重配置为 0，这个队列按照SP算法调度，这时候WRR算法就进化为SWRR算法。在队列调度时，系统会优先保证SP队列调度，当SP队列中没有报文发送时，才会调度WRR队列。SP队列执行严格优先级调度方式，WRR队列执行加权轮询调度方式。

**举例：** 配置端口队列权重为 1 2 3 4 5 6 7 8

Switch(interface-ethernet1/1/1)#mls qos queue wrr weight 1 2 3 4 5 6 7 8

## 7.12.16 mls qos queue wred

本型号交换机不支持此命令。

## 7.12.17 mls qos queue wdrr weight

**命令：mls qos queue wdrr weigh <weigh0..weigh7>**

**no mls qos queue wdrr weight**

**功能：** 配置了该命令以后，端口队列权重被设定。

**参数：** <weight0..weight7>定义队列调度权重，单位是kbytes，本配置对于WDRR算法有效，SP算法无效。当权重配置为 0 时，这个队列采用SP算法进行调度， WDRR算法进化为SP+WDRR算法。WDRR以字节为单位，通过八个权重值的比率来分配带宽。不同的芯片支持的选择权重范围不一样，如果设置超过芯片范围，报错并提示正常的范围。对于支持 4 个队列的芯片，参数变成< weight1..weight4>。

**缺省情况：** 队列权重为 10 20 40 80 160 320 640 1280。

**命令模式：** 端口模式。

**使用指南：** 如果有队列的权重配置为 0，这个队列按照SP算法调度，这时候WDRR算法就进化为SWDRR算法。在队列调度时，系统会优先保证SP队列调度，当SP队列中没有报文发送时，才会调度WDRR队列。SP队列执行严格优先级调度方式，WDRR队列执行加权轮询调度方式。

**举例：** 配置端口队列带宽分别为 10kbytes, 10kbytes, 20kbytes, 20kbytes, 30kbytes, 30 kbytes, 40kbytes, 40kbytes。

Switch(interface-ethernet1/1/1)#mls qos queue wdrr weight 10 10 20 20 40 40 80 8 0

## 7.12.18 mls qos queue bandwidth

**命令：mls qos queue <queue-id> bandwidth <maximum-bandwidth>**

**no mls qos queue <queue-id> bandwidth**

**功能：** 配置了该命令以后，端口队列带宽保证功能被设定。

**参数：** **<queue-id>** 指定当前要配置带宽保证的队列，对于不同芯片支持的队列数不同，其范围也不同，可配置的范围是 1-8；

**<maximum-bandwidth >** 配置的是此队列的最大带宽，范围 0-10000000，当输入 0 时，表示最大带宽功能失效。

**缺省情况：** 端口缺省无队列带宽保证配置.

**命令模式：** 端口模式。

**使用指南：**队列的最小带宽保证和最大带宽限制均是可以单独配置的，而且可以仅在一个队列上配置。出端口队列带宽保证功能与端口的调度模式也是密切相关的，如：某端口为严格优先级队列SP，此时 8 队列的优先级最高，在拥塞发生会优先满足此队列的流量，但如果用户需要给此端口某个低优先级的队列保证一定的带宽时，可以通过此配置命令为队列预留带宽，配置后的效果为此低优先级队列的最小带宽会被优先满足，剩余带宽才按照SP来调度。

**举例：** 配置端口ethernet1/1/2 队列 1 的最大带宽 128kbps。

Switch(config)#interface ethernet 1/1/2

Switch(config-If-Ethernet1/1/2)#mls qos queue 1 bandwidth 128

## 7.12.19 mls qos trust

**命令：mls qos trust {cos | dscp}**

**no mls qos trust {cos | dscp}**

**功能：** 配置交换机端口信任状态；本命令的 no 操作为禁止交换机端口的当前信任状态。

**参数：** **cos** 配置端口信任 CoS 值； **dscp** 配置端口信任 DSCP 值。

**缺省情况：** 端口默认不信任 CoS 值与 DSCP 值。

**命令模式：** 端口配置模式。

**使用指南：** trust cos模式：可以根据cos- to-intp映射设置报文的intp值；

trust dscp模式：可以根据dscp-to-intp映射设置报文的intp值，对IPv4、IPv6报文都能生效；

trust cos和trust dscp可以同时设置，trust dscp优先级高于trust cos的优先级。

**配置举例：**在端口ethernet1/1/1配置信任cos值，即报文按cos值分类。

switch(config-if-ethernet1/1/1)#mls qos trust cos

## 7.12.20 mls qos trust exp

**命令：mls qos trust exp**

**no mls qos trust exp**

**功能：** 配置交换机全局信任 exp；本命令的 no 操作为禁止交换机全局信任 exp。

**参数：** 无。

**缺省情况：** 无。

**命令模式：** Config 配置模式。

**使用指南：** 可以根据exp- to-intp映射设置报文的intp值；

**配置举例：**全局信任exp，即报文按exp值分类。

switch(config)#mls qos trust exp

## 7.12.21 mls qos policer

**命令 : mls qos policer ipg enable**

**no mls qos policer ipg enable**

**功能:** 使能或禁止 policer 限速对帧间隙计数

**参数：**无

**命令模式:**全局模式

**使用指南：**使能帧间隙计数，policer 在限速时会将帧间隙统计到报文总长度中。同样的限速值，统计帧间隙时，报文的实际速率就会降低，不统计帧间隙时，报文的实际速率就会增加。

Centec 设备，入口带宽控制和 Qos Policy 使用 policer 来实现限速。

**举例：** 使能 policer 限速对帧间隙计数。

Switch(config)#mls qos policer ipg enable

## 7.12.22 mls qos policer ipg enable

**命令:mls qos policer ipg enable**

**功能:**入方向控制带宽限速，将限速改为L1 限速

**参数：** 无

**缺省情况：** 缺省不设置动作

**命令模式：** 配置模式

**使用指南:**IPG表示帧间隙

举例:

Switch(config)#mls qos policer ipg enable

## 7.12.23 mls qos shape

**命令 : mls qos shape ipg enable**

**no mls qos shape ipg enable**

**功能:** 使能或禁止 shape 功能对帧间隙计数

**参数：**无

**命令模式:**全局模式

**使用指南：**使能帧间隙计数，shape 在限速时会将帧间隙统计到报文总长度中。同样的限速值，统计帧间隙时，报文的实际速率就会降低，不统计帧间隙时，报文的实际速率就会增加。

Centec 设备，出口带宽控制和队列带宽控制使用 shape 来实现限速。

**举例：** 使能 shape 对帧间隙计数。

Switch(config)#mls qos shape ipg enable

## 7.12.24 mls qos shape ipg enable

**命令:mls qos policer ipg enable**

**功能:**出方向控制带宽限速，将限速改为L1 限速

**参数：** 无

**缺省情况：** 缺省不设置动作

**命令模式：** 配置模式

**使用指南:**IPG表示帧间隙

举例:

Switch(config)#mls qos shape ipg enable

## 7.12.25 pass-through-cos

本型号交换机不支持此命令。

## 7.12.26 pass-through-dscp

本型号交换机不支持此命令。

## 7.12.27 policy burst

本型号交换机不支持此命令。

## 7.12.28 policy

**命令：**

**单桶模式：**

**policy <bits_per_second> <normal_burst_bytes> ({conform-action ACTION | exceed-action ACTION} )**

**双桶模式：**

**policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] | <maximum_burst_bytes> [{conform-action ACTION | exceed-action ACTION | violate-action ACTION }]**

**ACTION定义：**

**drop | transmit | set-internal-priority <inp_value> |**

**no policy**

**功能：** 支持三色color的非聚合Policy命令，根据配置参数解析出令牌桶的工作模式是单速单桶、单速双桶还是双速双桶，并且给不同颜色报文设置相应动作。no命令删除模式配置。

**参数：**

bits_per_second：约定信息速率，即CIR(Committed Information Rate)，单位是千比特/秒，范围是 1～10000000；
normal_burst_bytes：约定突发尺寸，即CBS(Committed Burst Size)，单位是字节，范围是 1～1000000，当设置的CBS值超过芯片的最大值时，采用芯片支持的最大值设置硬件，CLI无提示信息；
maximum_burst_bytes：峰值突发尺寸，即PBS(Peak Burst Size)，单位是字节，范围是 1～1000000，当设置的PBS值超过芯片的最大值时，采用芯片支持的最大值设置硬件，CLI无提示信息；注：此配置仅在双桶模式存在；
pir peak_rate_bps：峰值信息速率，即PIR(Peak Information Rate)，peak_rate_bps单位是千比特/秒，范围是 1～10000000，当没有配置PIR时，Poilce工作在单速双桶模式，配置了PIR时，Police工作在双速双桶模式。注：此配置仅在双桶模式存在；
violate-action：当超出PIR速率，报文为红色时，采取的策略，缺省为drop；
conform-action：当没有超过CIR速率，报文为绿色时，采取的策略，缺省为transmit；
exceed-action：当超出CIR速率但仍小于PIR速率，报文为黄色时，采取的策略，缺省为drop。

ACTION包括：
drop/transmit丢弃/通过报文；

set-internal-priority 修改报文内部优先级；
**命令模式：**策略分类表配置模式。
**缺省状态：**缺省不存在策略动作，对于动作的缺省配置，conform-action缺省动作为transmit，exceed-action和violate-action的缺省动作都为drop。
**使用指南：**命令行可以同时支持单桶配置和双桶配置，根据是否配置PIR或者PBS来确定是选择单桶还是双桶；在进行命令行配置时，如果配置了CBS后，直接配置动作，就是单速单桶双色；CBS后仅配置PBS为单速双桶三色；CBS后配置PIR和PBS则为双速双桶三色。Policy Map中同时选择了set和policy（policy aggregate），并且set和policy（policy aggregate）选择的动作相同，policy（policy aggregate）选择的动作可以覆盖set选择的动作。
**举例：** 在策略分类表配置模式下设置约定信息速率为 1000，约定突发尺寸为 2000，未超cir速率采取的动作为丢弃

```
Switch(config)#class-map cm
Switch(config-classmap-cm)#match cos 0
Switch(config-classmap-cm)#exit
Switch(config)#policy-map 1
Switch(config-policymap-1)#class cm
Switch(config-policymap-1-class-cm)# policy 1000 2000 conform-action drop
```

## 7.12.29 policy aggregate

**命令：policy aggregate <*aggregate-policy-name*>**

**no policy aggregate<*aggregate-policy-name*>**

**功能：** Police Map对聚合policy的引用，为分类后的流量应用一个聚合policy；本命令的no为删除指定的聚合policy。

**参数：** **<aggregate-policy-name>** 集合策略的名称。

**缺省情况：** 缺省没有引用聚合策略。

**命令模式：** 策略分类表配置模式。

**使用指南：** 可以在不同策略分类表内引用同一个聚合策略。

**举例：** 创建class-map，匹配规则为cos值为 0；匹配策略表policy-map为 1，进入策略表匹配模式；设置Policy为聚合策略color。

Switch(config)#class-map cm

Switch(config-classmap-cm)#match cos 0

Switch(config-classmap-cm)#exit

Switch(config)#policy-map 1

Switch(config-policymap-1)#class cm

Switch(config-policymap-1-class-cm)#policy aggregate color

## 7.12.30 policy-map

**命令：policy-map <*policy-map-name*>**

**no policy-map <*policy-map-name*>**

**功能：**建立一个policy-map（策略表），并进入policy-map（策略表）模式；本命令的no操作为删除指定的policy-map。

**参数：<*policy-map-name*>** 策略表名称。

**缺省情况：**缺省不存在策略表。

**命令模式：**全局配置模式

**使用指南：**进入策略表配置模式后，可以进行一系列 PBR 的分类匹配和下一跳设置等操作。

**举例：创建和删除一个命名为p1 的policy-map。**

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#exit

Switch(config)#no policy-map p1

## 7.12.31 service-policy input

**命令：service-policy input <*policy-map-name*>**

**no service-policy input {<*policy-map-name*>}**

**功能：**在交换机端口上应用一个策略表；本命令的no操作为删除应用到交换机端口的某个指定策略表或删除该端口入方向应用的所有策略表。

**参数：input <*policy-map-name*>** 将指定名称的策略表应用到交换机端口的入方向。

no操作时若不指定策略表名称，则删除该端口入方向所有策略表。

**缺省情况：**缺省端口没有捆绑策略表。

**命令模式：**端口配置模式.

**使用指南：**每个端口或vlan接口在每个方向上只能应用一个策略表。建议不要在vlan和属于该vlan的端口上同时使用policy map。

**举例：**在端口ethernet1/1/1 的入口上绑定策略p1。

Switch(config)#interface ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)# service-policy input p1

## 7.12.32 service-policy input vlan

**命令：service-policy input <*policy-map-name*> vlan <*vlan-list*>**

**no service-policy input{<*policy-map-name*>} vlan <*vlan-list*>**

**功能：**在交换机vlan接口上应用一个策略表；本命令的no操作为删除应用到交换机vlan接口的某个指定策略表或删除该vlan接口入方向应用的所有策略表。

**参数：input <*policy-map-name*>** 将指定名称的策略表应用到交换机vlan接口的入方向。

**vlan <vlan-list>**绑定策略表的vlan列表。

no操作时若不指定策略表名称，则删除该vlan接口入方向所有策略表。

**缺省情况：**缺省vlan接口没有捆绑策略表。

**命令模式：**全局配置模式.

**使用指南：**每个端口或vlan接口在每个方向上只能应用一个策略表。建议不要在vlan和属于该vlan的端口上同时使用policy map。

**举例：**在vlan接口v2，v3, v4, v6 的入方向上绑定策略p1。

Switch(config)# service-policy input p1 vlan 2-4;6

## 7.12.33 set

**命令：set {ip dscp <new-dscp> | ip precedence <new-precedence> | internal priority <new-inp> | drop precedence <new-dp> | ip [default] nexthop [vrf <vrf>] <ip-address> | ipv6 [default] nexthop [vrf <vrf>] <*nexthop-ip*> | cos <new-cos>}**

**no set {ip dscp | ip precedence | internal priority | drop precedence | ip *next hop* | ipv6 nexthop | cos | s-tpid}**

**功能：** 为分类后的流量分配一个新的DSCP和IP Precedence值等；本命令的no操作为取消分配新的值。

**参数：** ip dscp <*new-dscp*> 新的DSCP值，不区分v4 还是v6；

**ip precedence <new-precedence>** 新的IP优先级值；

**ipv6 flowlabel <new-flowlabel>** 新的IPv6 的流标签值；

**ip default nexthop [vrf <vrf>] <ip-address>** 下一跳的ip地址，用于PBR设置下一跳的路由，default参数表示添加的是一条垫底路由，查找优先级低于路由表和arp表；

**vrf是虚拟路由转发，取值范围 0**~252；

**ipv6 default nexthop [vrf <vrf>] <ip-address>** 下一跳的ipv6 地址，用于ipv6 PBR设置下一跳的路由，default参数表示添加的是一条垫底路由，查找优先级低于路由表和neighbor表；vrf是虚拟路由转发，取值范围 0~252；

**cos <new-cos>** 新的CoS值。

**缺省情况：** 缺省不进行分配。

**命令模式：** 策略分类表配置模式.

**使用指南：** 只有符合匹配标准被分类出来的流量才会被重新分配新的值。

**举例：**将满足c1 分类规则的报文里的IP Precedence值都设为 3。

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 3
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

## 7.12.34 show class-map

**命令：show class-map [<*class-map-name*>]**

**功能：**显示QoS的分类表信息。

**参数：<*class-map-name*>** 显示分类表名称。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**显示所有配置的class-map或指定的class-map的信息。

**举例：**

```
Switch # show class-map
Class map name:c1, used by 0 times
  match acl name:1
```

| 显示内容 | 解释 |
|---|---|
| Class map name:c1 | ClassMap的名字 |
| used by 0 times | 被使用的次数 |
| match acl name:1 | ClassMap的分类规则 |

## 7.12.35 show policy-map

**命令：show policy-map [<*policy-map-name*>]**

**功能：** 显示QoS的策略表信息。

**参数：** **<*policy-map-name*>** 策略表名称。

**缺省情况：** 无。

**命令模式：** 特权和配置模式。

**使用指南：** 显示所有配置的policy-map或指定的policy-map的信息。

**举例：**

```
Switch#show policy -map
Policy Map p1, used by 0 port
  Class Map name: c1
    policy CIR: 1000 CBS: 1000  PIR: 200 PBS: 3000
    conform-action:
     transmit
    exceed-action:
     drop
    violate-action:
     drop
```

| 显示内容 | 解释 |
|---|---|
| Policy Map p1 | policy-map的名字 |
| Class map name:c1 | 引用的ClassMap的名字 |
| policy CIR: 1000 CBS: 1000 PIR: 2000 PBS: 3000<br>conform-action:<br>transmit<br>exceed-action:<br>drop<br>violate-action:<br>drop | 采用的策略 |

## 7.12.36 show mls qos interface

**命令：show mls qos {interface { <IFNAME> | ethernet <interface-name> | port-channel <IFNAME>} [policy | queuing] | vlan <vlan-id>} | [ begin | include | exclude <regular-expression> ]**

**功能：** 显示QoS在交换机端口上的配置信息。

**参数：** **<interface-name>** 交换机端口ID；

**<IFNAME>** 交换机port-channel名称；

**<vlan-id>**： VLAN ID；

**policy** 为端口的策略设置；

**queuing** 为端口的队列设置。

**缺省情况：** 无。

**命令模式：** 特权和配置模式。

**使用指南：** 单速单桶模式下，报文经过police时仅会有绿色和红色两种颜色，打印统计信息时in-profile表示绿色，out-profile表示红色；在修改为双桶模式后，会有三种颜色的报文，但由于计数器counter仅能统计两类报文，所有把黄色和红色报文均做为out-profile统计在一起。只有配置入口策略时，才有统计信息。

**举例：**

```
Switch#show mls qos interface ethernet 1/1/2
Ethernet1/1/2：
Default COS：0
Trust：COS DSCP EXP
Attached Policy Map for Ingress: p1
Classmap      classified      in-profile      out-profile (in packets)
     c1             20               10               10
  c2            NA              NA              NA
（如果Class Map没有配置Accounting，显示NA）

Internal-Priority-TO-Queue map:
INTP        0      1      2      3      4      5      6      7
--------------------------------------------------------------------------------
Queue       0      1      2      3      4      5      6      7

Queue Algorithm：WRR
Queue weights：
Queue       0      1      2      3      4      5      6      7
-----------------------------------------------------------------------------------------------------
weight         1      2      3      4      5      6      7      8

Bandwidth Guarantee Configuration:
Queue       0      1      2      3      4      5      6      7
  ----------------------------------------------------------------------------------------------------
  MinBW(K)  128          0           0      0      0      0      0      0
    MaxBW(K)  256    0  0      0      0      0      0      0
```

| 显示内容 | 解释 |
| --- | --- |
| Ethernet1/1/2 | 端口名 |
| default cos:0 | 端口的默认cos值 |
| Trust：COS DSCP EXP | 端口的信任情况 |
| Attached Policy Map for Ingress: p1 | 端口绑定的策略名 |
| ClassMap | ClassMap的名字 |
| classified | 匹配此ClassMap的数据报文总数，如果Class Map没有配置Accounting，显示NA |
| in-profile | 匹配此ClassMap的in-profile数据报文总数，如果Class Map没有配置Accounting，显示NA |
| out-profile | 匹配此ClassMap的out-profile数据报文总数，如果Class Map没有配置Accounting，显示NA |
| Internal-Priority-TO-Queue map:: | 内部优先级到队列的映射关系 |
| Queue Algorithm： | WRR或者PQ出队方式 |
| Queue weights | 队列权重配置 |
| Bandwidth Guarantee Configuration | 带宽保证配置 |

```
Switch(config)#show mls qos interface ethernet1/1/2 queuing
Ethernet1/1/2:
  Internal-Priority-TO-Queue map:
  INTP  0      1      2      3      4      5      6      7
  ---------------------------------------------------------------------------
  Queue    0      1      2      3      4      5      6      7

  Queue Algorithm：WRR
  Queue weights：
  Queue        0      1      2      3      4      5      6      7
  ---------------------------------------------------------------------------------------------------
  weight       1      2      3      4      5      6      7      8

  Bandwidth Guarantee Configuration:
  Queue        0      1      2      3      4      5      6      7
  ---------------------------------------------------------------------------------------------------
  MinBW(K)  128          0          0      0      0      0      0      0
    MaxBW(K)  256    0  0      0      0      0      0      0
```

| 显示内容 | 解释 |
| --- | --- |
| Internal-Priority-TO-Queue map:: | 内部优先级到队列的映射关系 |
| Queue Algorithm： | WRR或者PQ出队方式 |
| Queue weights | 队列权重配置 |
| Bandwidth Guarantee Configuration | 带宽保证配置 |

Switch#show mls qos interface ethernet 1/1/2 policy
Ethernet1/1/2：
Attached Policy Map for Ingress: p1
Accounting：ON
Classmap classified in-profile out-profile (in packets)
c1 0 0 0

| 显示内容 | 解释 |
| --- | --- |
| Ethernet1/1/2 | 端口名 |
| Attached Policy Map for Ingress: p1 | 端口绑定的policy-map |
| ClassMap | ClassMap的名字 |
| classified | 匹配此ClassMap的数据报文总数 |
| in-profile | 匹配此ClassMap的in-profile数据报文总数 |
| out-profile | 匹配此ClassMap的out-profile数据报文总数 |

Switch#show mls qos vlan 100
Vlan 100：
Attached Policy Map for Ingress: p1
Classmap classified in-profile out-profile (in packets)
c1 20 10 10
c2 NA NA NA

## 7.12.37 show mls qos in {interface <interface-name> policy | vlan <vlan-id>

**命令：show mls qos in {interface <interface-name> policy | vlan <vlan-id>**
**功能：** 显示端口或vlan入方向策略配置信息。
**参数：** <interface-name> ：端口名称

**缺省情况：** 无。

**配置模式：** 特权和配置模式。

**使用指南：** 显示端口入方向策略配置信息。

**举例：** 显示端口入方向策略配置信息,举例如下：

Switch#show mls qos in interface ethernet1/1/1 policy

Ethernet1/1/1:

Attached Policy Map for Ingress: p

## 7.12.38 show mls qos interface wred

本型号交换机不支持此命令。

## 7.12.39 show mls qos maps

**命令：show mls qos maps (cos-dp | cos-intp | dscp-dp | dscp-dscp | dscp-intp | exp-dp | exp-intp )**

**功能：** 显示QOS全局映射相关配置内容。

**参数：** **cos-dp：** 入口L2 COS到丢弃优先级映射

**cos-intp：** 入口L2 COS到内部优先级映射

**dscp-dp：** 入口DSCP到丢弃优先级映射

**dscp-dscp：** 入口DSCP到DSCP映射

**dscp-intp：** 入口DSCP到内部优先级映射

**exp-dp：** 入口exp到丢弃优先级映射

**exp-intp：** 入口exp到内部优先级映射

**缺省情况：** 无。

**配置模式：** 特权和配置模式。

**使用指南：** 显示QoS的映射配置信息。

**举例：** 显示映射表配置信息,举例如下：

switch#show mls qos maps

Ingress COS-TO-Internal-Priority map:

COS: 0 1 2 3 4 5 6 7

---

INTP: 0 1 2 3 4 5 6 7

Ingress DSCP-TO-Internal-Priority map:

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

Ingress COS-TO-Drop-Precedence map:

| COS: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| DP: | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Ingress DSCP-TO-DSCP map:

| d1 : d2 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1: | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 2: | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 3: | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| 4: | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 |
| 5: | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 |
| 6: | 60 | 61 | 62 | 63 | | | | | | |

Ingress DSCP-TO-Drop-Precedence map:

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

Ingress EXP-TO-Internal-Priority map:

EXP: 0 1 2 3 4 5 6 7

---

INTP: 0 1 2 3 4 5 6 7

Ingress EXP-TO-Drop-Precedence map:

EXP: 0 1 2 3 4 5 6 7

---

DP: 0 0 0 0 0 0 0 0

Egress Internal-Priority-TO-EXP map:

INTP: 0 1 2 3 4 5 6 7

---

EXP: 0 1 2 3 4 5 6 7

## 7.12.40 show mls qos vlan

**命令：show mls qos vlan <v-id>**

**参数：<v-id>**：VLAN ID，取值为 1-4094

**命令模式：**特权和配置模式。

**缺省情况：**无。

**使用指南：**显示VLAN接口上的qos信息。

**举例：**

Switch#show mls qos vlan 1

## 7.12.41 show mls qos aggregate-policy

**命令：show mls qos aggregate-policy [policy-name]**

**参数：[policy-name ]：策略名称**

**命令模式：特权和配置模式。**

**缺省情况：无。**

**使用指南：显示 aggregate-policy 策略的配置信息。**

**举例：**

Switch#show mls qos aggregate-policy

**aggregate** policy p

**CIR:** 1 CBS: 1 PBS: 1

**conform-action**:

**transmit**

exceed-action:

drop

violate-action:

drop

Not used by any policy map

## 7.12.42 transmit

**命令：transmit**

**no transmit**

**功能：** 传送分类后的数据包；本命令的no操作为取消分配的动作。

**参数：** 无。

**缺省情况：** 缺省不设置动作。

**命令模式：** 策略分类表配置模式

**使用指南：** 配置了该命令以后，直接发送报文。

**举例：**

对满足分类表c1 的报文进行发送。

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#transmit
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

# 7.13 基于流的重定向

## 7.13.1 access-group redirect to interface ethernet

**命令：access-group <aclname> redirect to interface [ethernet *<IFNAME>*|*<IFNAME>*]**

**no access-group <aclname> redirect**

**功能：**指定基于流的重定向；本命令的no操作为删除基于流的重定向。

**参数：**

**<aclname>** 流的名称，目前仅支持数字标准IP访问列表、数字扩展IP访问列表、命名标准IP访问列表、命名扩展IP访问列表、数字标准IPv6 访问列表和命名标准IPv6 访问列表，并且access-list中不能配置Timerange和Portrange参数，类型必须为permit；***<IFNAME>*** 重定向目的端口。

**命令模式：**物理端口配置模式

**使用指南：**本命令的no操作为删除基于流的重定向。基于流的重定向是把端口接收到的、符合特定条件的数据帧转发到另一个指定的端口。

**举例：**将 1 端口收到的源IP为 192.168.1.111 的帧重定向到 6 端口。

Switch(config)#access-list 1 permit host 192.168.1.111

Switch(config)#interface ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)#access-group 1 redirect to interface ethernet 1/1/6

## 7.13.2 match vlan <1-4096> redirect interface (ethernet|) IFNAME

本型号交换机不支持此命令。

## 7.13.3 port-redirect match vlan <1-4094> source-port interface (ethernet|) IFNAME destination-port interface (ethernet|) IFNAME

**本型号交换机不支持此命令。**

## 7.13.4 show flow-based-redirect

**命令：show flow-based-redirect {interface [ethernet *<IFNAME>*|*<IFNAME>*]}**

**功能：**显示当前系统/端口中配置的基于流的重定向信息。

**参数：**1.不指定端口，将显示系统中配置的所有基于流的重定向信息。

2.指定端口***<IFNAME>***，将显示端口列表中指定的端口中配置的基于流的重定向信息。

**命令模式：**特权和配置模式

**使用指南：**通过本命令可以显示当前系统/端口中配置的基于流的重定向信息。

**举例：**

Switch(config)#show flow-based-redirect

Flow-based-redirect config on interface Ethernet1/1/1:

RX flow (access-list 1) is redirected to interface Ethernet1/1/6

## 7.13.5 vlan-port-redirect vlan maximum <1-1000>

**命令：vlan-port-redirect vlan maximum <1-1000>**

**no vlan-port-redirect vlan maximum**

**命令模式：**全局模式

**功能：**设置每个端口 redirect 的 vlan 数最大值。

**缺省值：**500

**参数：**maximum <1-1000> vlan 个数最大值。

**使用指南：**设置每个端口 redirect 的 vlan 数最大值。

**举例：**设置 1/1/1 端口redirect的vlan数最大值为 600

switch(config)#vlan-port-redirect vlan maximum 600

# 7.14 Egress QoS

## 7.14.1 mls qos egress green remark

本型号交换机不支持此命令。

## 7.14.2 service-policy output

**命令：service-policy output <*policy-map-name*>**

**no service-policy output {<*policy-map-name*>}**

**功能：**在交换机端口上应用一个策略表；本命令的no操作为删除应用到交换机端口的某个指定策略表或删除该端口出方向应用的所有策略表。

**参数：output <*policy-map-name*>** 将指定名称的策略表应用到交换机端口的出方向。

no操作时若不指定策略表名称，则删除该端口出方向所有策略表。

**缺省情况：**缺省端口没有捆绑策略表。

**命令模式：**端口配置模式.

**使用指南：**每个端口或vlan接口在每个方向上只能应用一个策略表。建议不要在vlan和属于该vlan的端口上同时使用policy map。

**举例：**在端口ethernet1/1/1 的入口上绑定策略p1。

Switch(config)#interface ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)# service-policy output p1

## 7.14.3 service-policy output vlan

**命令：service-policy output <*policy-map-name*> vlan <*vlan-list*>**

**no service-policy output {<*policy-map-name*>} vlan <*vlan-list*>**

**功能：**在交换机vlan接口上应用一个策略表；本命令的no操作为删除应用到交换机vlan接口的某个指定策略表或删除该vlan接口出方向应用的所有策略表。

**参数：input <*policy-map-name*>** 将指定名称的策略表应用到交换机vlan接口的出方向。

**vlan <vlan-list>**绑定策略表的vlan列表。

no操作时若不指定策略表名称，则删除该vlan接口出方向所有策略表。

**缺省情况：**缺省vlan接口没有捆绑策略表。

**命令模式：**全局配置模式.

**使用指南：**每个端口或vlan接口在每个方向上只能应用一个策略表。建议不要在vlan和属于该vlan的端口上同时使用policy map。

**举例：**在vlan接口v2，v3, v4, v6 的入方向上绑定策略p1。

Switch(config)# service-policy output p1 vlan 2-4;6

## 7.14.4 set

**命令：set {ip precedence <new-precedence> | internal priority <new-inp> | drop precedence <new-dp> | cos <new-cos> | s-tpid (0x8100|0x88a8|0x9100) }**

**no set {ip precedence | internal priority | drop precedence | cos | s-tpid}**

**功能：** 为分类后的流量分配一个新的IP Precedence值等；本命令的no操作为取消分配新的值。

**参数：**

**ip precedence <new-precedence>** 新的IP优先级值；

**cos <new-cos>** 新的CoS值。

**s-tpid (0x8100|0x88a8|0x9100)** 新的tpid值（只能绑定在出口方向）。

**缺省情况：** 缺省不进行分配。

**命令模式：** 策略分类表配置模式.

**使用指南：** 只有符合匹配标准被分类出来的流量才会被重新分配新的值。

**举例：**将满足c1 分类规则的报文里的IP Precedence值都设为 3。

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class c1

Switch(Config-PolicyMap-p1-Class-c1)#set *ip* precedence 3

Switch(Config-PolicyMap-p1-Class-c1)#exit

Switch(Config-PolicyMap-p1)#exit

# 7.15 灵活QinQ

## 7.15.1 add

**命令：add {s-vid <new-vid> | c-vid <new-vid>}**

**no add {s-vid | c-vid}**

**功能：** 对匹配分类表的数据包增加指定的外层 tag 或者内层 tag，no 命令为取消操作。

**参数：** s-vid <new-vid>指定外层 VLAN Tag 中的 VID；

c-vid <new-vid>指定内层 VLAN Tag 中的 VID。

**缺省情况：** 缺省不进行增加 tag 动作。

**命令模式：** 策略分类表配置模式

**使用指南：** 配置了该命令以后，对匹配分类表的报文进行增加指定的外层 tag 或内层 tag。使用灵活 QinQ 功能时，当发送数据包为只有内层 VLAN Tag 或无 Tag，需要用 add s-vid 命令添加指定的外层 VLAN Tag，否则数据因在交换机内部没有外层 VLAN。

**举例：** 对满足 c1 分类规则的报文增加一个 VID 为 2 的外层 VLAN Tag。

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class c1

Switch(Config-PolicyMap-p1-Class-c1)#add s-vid 2

## 7.15.2 delete

**命令：delete {c-vid}**

**no delete c-vid**

**功能：** 对匹配分类表的数据包删除内层 VLAN Tag，no 命令为取消操作。

**参数：** 无。

**缺省情况：** 缺省不进行删除内层 VLAN Tag 操作。

**命令模式：** 策略分类表配置模式

**使用指南：** 配置该命令以后，对匹配分类表的报文进行删除内层 VLAN Tag 操作。使用灵活 QinQ 功能时，当发送数据包为只有内层 VLAN Tag 或无 Tag，需要用 add s-vid 命令添加指定的外层 VLAN Tag，否则数据因在交换机内部没有外层 VLAN。

**举例：** 对满足 c1 分类规则的报文删除内层 VLAN Tag。

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class c1

Switch(Config-PolicyMap-p1-Class-c1)#delete c-vid

## 7.15.3 Match

**命令：match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*>| ip precedence <*ip-precedence-list*>| ipv6 access-group <*acl-index-or-name*> | ipv6 dscp <*dscp-list*> | ipv6 flowlabel <flowlabel-list> | vlan <vlan-list> | cos <*cos-list*>}**

**no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos}**

**功能：设置分类表中的匹配标准；本命令的no操作为删除指定的匹配标准。**

**参数：access-group <*acl-index-or-name*>**匹配指定的IP ACL，MAC ACL表，参数为ACL的编号或名称；

**ip dscp <*dscp-list*>** 和 **ipv6 dscp <dscp-list>**匹配指定的DSCP值，参数为一个DSCP值列表，最多由 8 个DSCP值组成，范围为 0～63；

**ip precedence <*ip-precedence-list*>**匹配指定的IP优先级值，参数为一个IP优先级值列表，最多由 8 个IP优先级值组成，范围为 0～7；

**ipv6 access-group <*acl-index-or-name*>**匹配指定的IPv6 ACL表，参数为IPv6 ACL的编号或名称；

**ipv6 flowlabel <flowlabel-list>** 匹配指定的IPV6 FL流标签，参数为IPV6 FL的流标签值，范围为 0～1048575；

**vlan <*vlan-list*>** 匹配指定的外层VLAN Tag中的VLAN ID值，参数为一个VLAN ID列表，最多 8 个VLAN ID，范围为 1～4094；

**cos <*cos-list*>** 匹配指定的CoS值，参数为一个CoS列表，最多 8 个CoS。范围为 0～7。

**缺省情况：缺省不存在匹配标准**

**命令模式：class-map（分类表）配置模式。**

**使用指南：每个分类表内，只能设置一条匹配标准。当匹配ACL时，permit规则就是匹配项，应用Policy** Map action；deny规则就是排除项，不应用Policy Map action。如果已经配置了其他的match规则，提示无法配置，如果配置相同的match规则，就覆盖处理。

**举例：创建一个名为c1 的class** map，设置此class-map的分类规则是匹配IP precdence为 0 的报文。

```
Switch(config)#class-map c1
Switch(config-classmap-c1)#match ip precedence 0
Switch(config-classmap-c1)#exit
```

## 7.15.4 service-policy

**命令：service-policy input <policy-map-name>**

**no service-policy input {<policy-map-name>}**

**功能：** 将指定名称的灵活QinQ策略绑定到端口入方向，no命令为取消端口的绑定。

**参数： service-policy <*policy-map-name*>**指定名称的灵活QinQ策略表名称。

**缺省情况：** 缺省端口没有绑定策略表。

**命令模式：** 端口配置模式

使用指南： 每个端口上只能绑定一个策略表，将策略表绑定端口后功能才会生效。

**举例：** 在端口Ethernet1/1/1 上为灵活QinQ应用策略表p1。

Switch(Config-If-Ethernet1/1/1)#service-policy input p1

### 7.15.5 set

**命令：set s-vid <vid>**

**no set s-vid功能：**对匹配分类表的数据包增加指定的外层tag，no命令为取消操作。

**参数：** <vid> 指定外层VLAN Tag中的VID。

**缺省情况：** 缺省不进行增加tag动作。

**命令模式：** 策略分类表配置模式

**使用指南：** 配置了该命令以后，对匹配分类表的报文进行增加指定的外层tag。

**举例：** 对满足c1 分类规则的报文增加一个VID为 2 的外层VLAN Tag。

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class c1

Switch(Config-PolicyMap-p1-Class-c1)#set s-vid 2

## 7.16 Captive Portal 认证

### 7.16.1 认证功能命令

#### 7.16.1.1 ac-name

**命令：ac-name <word>**

**no ac-name**

**功能：**配置重定向 url 中的参数 acname 的值。本命令的 no 形式为删除重定向 url 中的参数 acname 值的配置。

**参数：**<word>，为 acname 的值。最多 16 个字符。

**命令模式：** Captive Portal Instance 模式。

**缺省情况：**无。

**使用指南：**本命令用于配置重定向 url 中的参数 acname 的值。某些 portal server 要求重定向时带上特定的 ac-name 值才能够通过认证，所以需要根据 portal server 的要求来配置此命令。

**举例：**根据移动 portal server 的标准配置重定向 url 中的 ac-name 值为 0100.0010.010.00，命名格式为 ACN.CTY.PRO.OPE。

Switch(config-cp-instance)#ac-name 0100.0010.010.00

#### 7.16.1.2 authentication roam enable

**命令：authentication roam enable <vlan WORD>**

**no authentication roam enable <vlan WORD>**

**功能：**使能用户漫游功能。该命令的 no 操作为关闭用户漫游功能。

**参数：**vlan WORD：指定的 VLAN 允许漫游。

**命令模式：**captive portal 配置模式。

**缺省情况：**默认不开启。

**使用指南：**使能该功能后，则允许用户漫游。当一个用户从一个端口漫游到另外一个端口时（同一个 VLAN），就可以触发漫游，用户不需要重新认证就可以访问网络资源；关闭用户漫游功能，不允许用户漫游。当一个用户从一个端口漫游到另外一个端口时，需要重新认证才可以访问网络资源。

**举例：**vlan10 开启用户漫游。

Switch (config-cp)#authentication roam enable vlan 10

## 7.16.1.3 captive-portal

**命令：captive-portal**

**功能：**使用该命令进入 Captive Portal 配置模式。

**参数：**无。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**使用该命令进入 Captive Portal 配置模式。

**举例：**进入全局配置模式进行相应配置。

Switch (config)#captive-portal

## 7.16.1.4 captive-portal client deauthenticate

**命令：captive-portal client deauthenticate {*<1-10>* / *<FF-FF-FF-FF-FF-FF>* { ipv4 | ipv6} *<ip-addr>*}**

**功能：**该命令解关联特定的 Captive Portal 客户端。

**参数：***<1-10>* Captive Portal 的 ID；

*<FF-FF-FF-FF-FF-FF>*客户端的 MAC 地址；

ipv4 用户地址为 ipv4 地址；

ipv6 用户地址为 ipv6 地址；

*<ip-addr>*用户地址，ipv4 地址是以点分十进制格式，ipv6 地址是 X:X::X:X 的格式。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**使用此命令可以解关联指定 MAC 地址的客户端；也可解除指定 captive portal configuration 下的所用用户或单独用户；当没有参数时，将解除所有用户。

**举例：**解关联特定的 Captive Portal 客户端。

Switch #captive-portal client deauthenticate （强制该控制器上所有的 portal 用户下线）

The specified clients will be deauthenticated. Are you sure you want to deauthenticated clients? [Y/N]

Switch #captive-portal client deauthenticate 1（强制例程 1 上所有的用户下线）

Switch #captive-portal client deauthenticate 34-08-04-30-07-ca ipv4 100.1.1.1（强制某个用户下线）

## 7.16.1.5 captive-portal client re-auth log { enable | disable }

**命令：captive-portal client re-auth log enable**

**captive-portal client re-auth log disable**

**功能：**当用户上来的端口，vlan，mac 发生改变，需要重新认证时，show logging buffer 里会记录日志。该命令的 no 操作为重新认证时，不记录日志。

**参数：**无。

**缺省情况：**默认不开启。

**命令模式：**captive portal 模式。

**使用指南：**当在线用户认证的端口,或者 vlan，或者 mac 发生改变，需重新认证时，记录日志。

**举例：**Switch (config-cp)# captive-portal client re-auth log enable

## 7.16.1.6 captive-portal client keep-alive flow-detection enable

**命令：captive-portal client keep-alive flow-detection enable**

**no captive-portal client keep-alive flow-detection enable**

**功能：**使能用户保活功能。该命令的 no 操作为关闭用户保活功能。

**参数：**无。

**缺省情况：**默认不开启。

**命令模式：**captive portal 模式。

**使用指南：**使能该功能后，当用户上线后，对用户进行保活。

**举例：**进入 captive portal 配置模式进行相应配置。

Switch (config-cp)#captive-portal client keep-alive flow-detection enable

## 7.16.1.7 captive-portal client keep-alive flow-detection interval

**命令：captive-portal client keep-alive flow-detection interval <3-120>**

**no captive-portal client keep-alive flow-detection interval**

**功能：**设定用户保活查询间隔。该命令的 no 操作，为设置保活查询间隔为默认值。

**参数：**<3-120>参数范围为 3 分钟到 120 分钟。

**缺省情况：**默认为 5 分钟。

**命令模式：**captive portal 模式。

**使用指南：**配置该命令后，保活定时器每隔设定时间查询一次用户在线状态。

举例：进入 captive portal 配置模式进行相应配置。

Switch (config-cp)# captive-portal client keep-alive flow-detection interval 3

## 7.16.1.8 captive-portal client keep-alive flow-detection number

**命令：captive-portal client keep-alive flow-detection number <1-10>**

**no captive-portal client keep-alive flow-detection number**

**功能：**设置允许保活定时器连续查询失败次数。该命令的 no 操作为设置允许保活定时器连续查询失败次数为默认值。

**参数：**<1-10>:范围 1 次到 10 次。

**缺省情况：**默认是 3 次。

**命令模式：**captive portal 模式。

**使用指南：**配置该命令后，保活定时器连续查询指定次数用户在线状态，如都不在线，则认为用户下线，否则，只要在允许失败次数内有 1 次查到用户在线，认为用户还在线，重置已经查询失败计数。

**举例：**进入 captive portal 配置模式进行相应配置。

Switch (config-cp)# captive-portal client keep-alive flow-detection interval 3

## 7.16.1.9 configuration

**命令：configuration *<cp-id>***

**no configuration *<cp-id>***

**功能：**使用该命令进入 Captive Portal 例程模式。该命令的 no 操作为删除 Captive Portal 例程配置。

**参数：***<cp-id>*为 Captive Portal 例程数量，取值范围为 1-10。

**缺省情况：**无。

**命令模式：**Captive Portal 全局配置模式。

**使用指南：**该配置用于配置 Captive Portal 的例程，每一个例程代表一类场景，处于同一例程下的用户其流量、速率等配置相同，反之亦然。该命令的 no 模式删除一个 captive portal 配置。如果有接口关联在某个例程上，则对该例程使用 no 命令无效。

**举例：**配置 ID 参数为 4。

Switch (config-cp)#configuration 4

## 7.16.1.10 debug captive-portal packet

**命令：debug captive-portal packet {send|receive|all}**

**no debug captive-portal packet {send|receive|all}**

**功能：**打开 captive portal 认证功能的报文调试开关。本命令的 no 形式为关闭 captive portal 认证功能的报文调试开关。

**参数：**send，为打开 captive portal 的发包调试信息；

receive，为打开 captive portal 的收包调试信息；

all，为打开 captive portal 的收发包和解析包调试信息。

**命令模式：**特权模式。

**缺省情况：**缺省情况下 captive portal 认证功能的报文调试信息是关闭的。

**使用指南：**本命令用于打开 captive portal 认证功能的报文调试开关。

**举例：**打开 captive portal 认证功能的收发包和解析包调试信息。

Switch #debug captive-portal packet all

## 7.16.1.11 debug captive-portal trace

**命令：debug captive-portal trace**

**no debug captive-portal trace**

**功能：**打开 captive portal 认证功能的跟踪情况调试。本命令的 no 形式为关闭 captive portal 认证功能的跟踪情况调试。

**参数：**无。

**命令模式：**特权模式。

**缺省情况：**缺省情况下 captive portal 认证功能的跟踪调试是关闭的。

**使用指南：**本命令用于打开 captive portal 认证功能的跟踪情况调试。

**举例：**打开 captive portal 认证功能的跟踪情况调试。

Switch #debug captive-portal trace

## 7.16.1.12 debug captive-portal alive-detail

**命令：debug captive-portal alive-detail**

**no debug captive-portal alive-detail**

**功能：**portal 认证保活处理详细调试信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权用户配置模式。

**举例：**Switch#debug captive-portal alive-detail

## 7.16.1.13 debug captive-portal alive-status

**命令：debug captive-portal alive-status**

**no debug captive-portal alive-status**

**功能：**portal 认证保活处理状态调试信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权用户配置模式。

**举例：**Switch#debug captive-portal alive-status

## 7.16.1.14 debug captive-portal alive-time

**命令：debug captive-portal alive-time**

**no debug captive-portal alive-time**

**功能：**portal 认证保活处理时间调试信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权用户配置模式。

**举例：**Switch#debug captive-portal alive-time

## 7.16.1.15 debug captive-portal error

**命令：debug captive-portal error**

**no debug captive-portal error**

**功能：**打开 captive portal 认证功能的错误调试信息。本命令的 no 形式为关闭 captive portal 认证功能的错误调试信息。

**参数：**无。

**命令模式：**特权模式。

**缺省情况：**缺省情况下 captive portal 认证功能的错误调试信息是关闭的。

**使用指南：**本命命令用于打开 captive portal 认证功能的错误调试信息。

**举例：**打开 captive portal 认证功能的错误调试信息。

Switch #debug captive-portal error

## 7.16.1.16 enable (全局)

**命令：enable**

**disable**

**功能：**使用 enable 命令全局使能控制器上的 Captive Portal 功能，使用 disable 功能全局关闭控制器上的 Captive Portal 功能。

**参数：**无。

**缺省情况：**全局关闭控制器上的 Captive Portal 功能。

**命令模式：**Captive Portal 全局配置模式

**使用指南：**使用该命令全局使能 Captive Portal 在控制器上的特征。

**举例：**打开 Captive Portal 在控制器上的全局功能。

Switch (config-cp)#enable

## 7.16.1.17 enable (例程)

**命令：enable**

**disable**

**功能：**该命令使能 Captive Portal 配置。

**参数：**无。

**缺省情况：**使能 Captive Portal 配置。

**命令模式：**Captive Portal Instance 配置模式

**使用指南：**默认为 enable 模式，关闭 captive-portal 功能的命令为 disable，关闭 portal 功能后在线的 portal 用户被强制下线。

**举例：**打开 captive-portal 功能。

Switch (config-cp-instance)#enable

## 7.16.1.18 external portal-server server-name

**命令：external portal-server server-name <*name*> {ipv4 | ipv6} <*ipaddr*> [port <*0-65535*>]**

**no external portal-server {ipv4 | ipv6}server-name <*name*>**

**功能：**该命令配置外置 portal 服务器，通过该服务器推出重定向页面，客户端输入正确的用户名和密码后，认证成功，该客户端能够访问外网。

**参数：**<*name*> 外置 portal 服务器的名字

<*ipaddr*> 外置 portal 服务器的 ip 地址

ipv4 配置的 Portal 服务器地址是 ipv4 地址

ipv6 配置的 Portal 服务器地址是 ipv6 地址

<*0-65535*> portal server 的端口号

**缺省情况：**无。

**命令模式：**Captive Portal 全局配置模式

**使用指南：**配置外置 portal 服务器，最多可以配置 10 台。每个 cp configuration 可以绑定一台 portal 服务器。

**举例：**配置一个外置 portal 服务器。

Switch (config-cp)# external portal-server server-name x1 ipv4 1.0.0.1 port 11111

## 7.16.1.19 http-redirect-filter <1-32> {ip A.B.C.D| domain WORD}

**命令：http-redirect-filter <1-32> {ip A.B.C.D| domain WORD}**

**no http-redirect-filter (<1-32>|all)**

**功能：**为 portal 认证的 HTTP 重定向指定 IP 或域名，只有匹配了这个 IP 或域名的 HTTP 报文才做重定向处理。no 操作为删除配置认证域名或 ip 地址后，按照之前的流程认证，所有未认证的 mac，认证前 http 报文均重定向到 portal server。

**参数：**<1-32> ：规则 ID 号（索引）；

ip A.B.C.D：HTTP 重定向指定 IP 地址；

domain WORD：HTTP 重定向指定域名，最大长度为 256。

**缺省情况：**默认不配置此命令，所有未认证的 mac，认证前 http 报文均重定向到 portal server。

**命令模式：**Captive Portal 配置模式。

**使用指南：**增加一条配置认证域名或者 ip 地址的命令。

**举例：**配置一条指定 ip 地址为 1.1.1.1 的命令。

Switch (config-cp)# http-redirect-filter 1 ip 1.1.1.1

配置一条指定域名为 www.dcn.com 的命令。

Switch (config-cp)# http-redirect-filter 1 domain www.dcn.com

## 7.16.1.20 http-redirect-filter <1-32>

**命令：http-redirect-filter <1-32>**

**no http-redirect-filter <1-32>**

**功能：**captive portal 的一个实例绑定一个规则。该命令的 no 操作是删除一个 redirect 绑定。

**参数：<1-32> ：**规则 ID 号（索引）。

**缺省情况：**默认不配置此命令。

**命令模式：**Captive Portal Instance 模式。

**使用指南：**captive portal 的一个实例进行一个 redirect 绑定。

**举例：**实例绑定规则。

Switch (config-cp-instance)# http-redirect-filter 1

## 7.16.1.21 name

**命令：name *<cp-name>***

**no name**

**功能：**该命令定义 Captive Portal 配置的名称。

**参数：***<cp-name>*，Captive Portal配置的名称，其最多可以包含32个字符的字母或数字。

**缺省情况：**无。

**命令模式：**Captive Portal Instance 配置模式

**使用指南：**定义 Captive Portal Instance 配置的名称。

**举例：**定义 Captive Portal 配置的名称为 abc123。

Switch (config-cp-instance)#name abc123

## 7.16.1.22 nas-ipv4

**命令：nas-ipv4 < *A.B.C.D*>**

**no nas-ipv4 < *A.B.C.D*>**

**功能：**该命令定义 Captive Portal nas-ip 地址。

**参数：< *A.B.C.D* >**，IPv4 address of NAS。

**缺省情况：**无。

**命令模式：**Captive Portal 配置模式。

**使用指南：定义** Captive Portal nas-ip 地址。

**举例：**配置 Captive Portal nas-ip 地址是 10.1.1.1。

Switch (config-cp)#nas-ipv4 10.1.1.1

## 7.16.1.23 portal enable configuration <id>

**命令：**portal enable configuration <id>

no portal enable

**功能：**端口下使能 portal 功能，指定端口绑定的实例号，并且可以指定哪些 VLAN 使能 portal。一个端口只能绑定一个实例

**参数：**<id> ：指定实例号。

**缺省情况：**无。

**命令模式：**端口配置模式。

**使用指南：**端口下使能 portal 功能，并且将端口绑定到某个实例，绑定后，实例下的规则可以应用到这个端口。端口下所有的流量都要进行认证，端口下关闭 portal 功能，流量恢复正常；

**举例：**配置端口 1/1/1 下绑定 configuration 1 的实例

Switch (config-if-ethernet1/1/1)#portal enable configuration 1

## 7.16.1.24 portal-server

**命令：portal-server {ipv4 | ipv6} <*name*>**

**no portal-server {ipv4 | ipv6}**

**功能：**该命令为 CP configuration 配置绑定特定的外置 portal 服务器。绑定到此 CP configuration 下的端口都通过这个 portal 服务器进行重定向认证。

**参数：**<*name*> 绑定的 Portal 服务器的名字

ipv4 绑定的 Portal 服务器地址是 ipv4 地址

ipv6 绑定的 Portal 服务器地址是 ipv6 地址

**缺省情况：**无。

**命令模式：**Captive Portal Instance 配置模式

**使用指南：**使用此命令可以为 CP configuration 配置绑定特定的外置 portal 服务器；也可为 configuration 解除绑定特定的外置 portal 服务器。

**举例：**为 CP configuration 配置绑定特定的外置 portal 服务器。

Switch (config-cp -instance)#portal-server ipv4 x1

## 7.16.1.25 radius accounting

**命令：radius accounting**

**no radius accounting**

**功能：**使用该命令打开 Captive Portal 例程的计费功能。该命令的 no 操作为关闭 Captive Portal 例程的计费功能

**参数：**无。

**缺省情况：**Captive Portal 例程的计费功能关闭。

**命令模式：**Captive Portal Instance 配置模式

**使用指南：**配置 Captive Portal 的计费功能。

**举例：**打开 Captive Portal 某例程的计费功能。

Switch (config-cp-instance)#radius accounting

## 7.16.1.26 radius-accounting update interval

**命令：radius-accounting update interval <*60-3600*>**

**no radius-accounting update interval**

**功能：**配置交换机向 radius 发送的 portal 用户的计费更新间隔时间。该命令的 no 操作为恢复配置的默认值。

**参数：**<*60-3600*>为时间间隔，单位为秒。

**缺省情况：**300 秒

**命令模式：**Captive Portal Instance 配置模式

**使用指南：**配置 Captive Portal 的计费更新间隔时间。

**举例：**配置交换机向 radius 发送的 portal 用户的计费更新间隔时间为 60 秒。

Switch (config-cp-instance)# radius-accounting update interval 60

## 7.16.1.27 radius-acct-server

**命令：radius-acct-server <*server-name*>**

**no radius-acct-server**

**功能：**使用该命令定义 Captive Portal 配置的 RADIUS 计费服务器名称。该命令的 no 操作为删除此次配置。

**参数：**<*server-name*>，RADIUS计费服务器名称

**缺省情况：**无。

**命令模式：**Captive Portal Instance 配置模式

**使用指南：**定义 Captive Portal 配置的 RADIUS 计费服务器。

**举例：**定义 Captive Portal 配置的 RADIUS 计费服务器为 radius_aaa_1。

Switch (config-cp-instance)#radius-acct-server radius_aaa_1

## 7.16.1.28 radius-auth-server

**命令：radius-auth-server <*server-name*>**

**no radius-auth-server**

**功能：**使用该命令定义 Captive Portal 配置的 RADIUS 认证服务器。该命令的 no 操作为删除此次配置。

**参数：** *<server-name>*，Captive Portal配置的RADIUS认证服务器名称

**缺省情况：**无。

**命令模式：**Captive Portal Instance 配置模式

**使用指南：**定义 Captive Portal 配置的 RADIUS 认证服务器。

**举例：**定义 Captive Portal 配置的 RADIUS 认证服务器为 radius_aaa_1。

Switch (config-cp-instance)#radius-auth-server radius_aaa_1

## 7.16.1.29 redirect url-head <word>

**命令：redirect url-head <word>**

**no redirect url-head**

**功能：**配置重定向 url 头部分，包括传输协议、主机名、端口和 path 等几个部分。本命令的 no 形式为删除重定向 url 头部分的配置。

**参数：**<word>，重定向 url 头部分。如 https://200.101.13.4:8080/index.jsp。也可以为 http://www.portal.com/index.jsp。最多可输入 128 个字符.

**命令模式：**captive portal instance 配置模式。

**缺省情况：**无。

**使用指南：**本命令用于配置重定向 url 头部分，包括传输协议、主机名、端口和 path 等几个部分。需要根据 portal server 上重定向页面的 url 来配置，传输协议、主机名、端口和 path 需要完全相同才能进行重定向。

**举例：**配置重定向 url 头部分为 http://17.16.1.26/control

Switch (config-cp-instance)#redirect url-head http://17.16.1.26/control

## 7.16.1.30 redirect attribute ssid enable

**命令：redirect attribute ssid enable**

**no redirect attribute ssid enable**

**功能：**使能重定向 url 中携带 ssid 参数功能。本命令的 no 形式为关闭重定向 url 中携带 ssid 参数的功能。

**参数：**无。

**命令模式：**captive portal instance 配置模式。

**缺省情况：**缺省情况下重定向 url 中携带 ssid 参数的功能是关闭的。

使用指南：本命令用于使能重定向 url 中携带 ssid 参数功能。使能此功能后，客户端进行重定向时，重定向的 url 中会携带客户端关联的 ssid。

**举例：**使能重定向 url 中携带 ssid 参数功能。

Switch (config-cp-instance)#redirect attribute ssid enable

## 7.16.1.31 redirect attribute ssid name

**命令：redirect attribute ssid name <word>**

**no redirect attribute ssid name**

**功能：**配置在重定向 url 中携带的 ssid 参数名称。本命令的 no 形式为恢复冲向 url 中携带的 ssid 参数名称为默认值。

**参数：**<word>，为 ssid 参数名称。最多 32 个字符

**命令模式：**captive portal instance 配置模式。

**缺省情况：**缺省情况下重定向 url 中携带的 ssid 参数名称为 ssid。

使用指南：本命令用于配置在重定向 url 中携带的 ssid 参数名称。

**举例：**配置重定向 url 中携带的 ssid 参数名称为 ssid。

Switch (config-cp-instance)#redirect attribute ssid name ssid

## 7.16.1.32 redirect attribute nas-ip enable

**命令：redirect attribute nas-ip enable**

**no redirect attribute nas-ip enable**

**功能：**使能重定向 url 中携带 nas-ip 参数功能。本命令的 no 形式为关闭重定向 url 中携带 nas-ip 参数的功能。

**参数：**无。

**命令模式：**captive portal instance 配置模式

**缺省情况：**缺省情况下重定向 url 中携带的 nas-ip 参数的功能是关闭的。

**使用指南：**本命令用户使能重定向 url 中携带 nas-ip 参数功能。使能此功能后，客户端进行重定向时，重定向的 url 中会携带客户端所关联的交换机的 IP 地址。

**举例：**使能重定向 url 中携带 nas-ip 参数功能。

Switch (config-cp-instance)#redirect attribute nas-ip enable

## 7.16.1.33 redirect attribute nas-ip name

**命令：redirect attribute nas-ip name <word>**

**no redirect attribute nas-ip name**

**功能：**配置在重定向 url 中携带的 nas-ip 参数的名称。本命令的 no 形式为恢复重定向 url 中携带的 nas-ip 参数的名称为默认值。

**参数：**<word>，为 nas-ip 参数名称。最多 32 个字节。

**命令模式：**captive portal instance 配置模式。

**缺省情况：**缺省情况下重定向 url 中携带的 nas-ip 参数的名称为 acname。

**使用指南：**本命令用于配置在重定向 url 中携带的 nas-ip 参数的名称。

**举例：**配置在重定向 url 中携带的 nas-ip 参数的名称为 nasip

Switch (config-cp-instance)#redirect attribute nas-ip name nasip

## 7.16.1.34 session-timeout

**命令：session-timeout *<0-86400>***

**no session-timeout**

**功能：**定义 Captive Portal 配置的会话超时。该命令的 no 操作为关闭此功能。

**参数：**<*0-86400*>，会话超时时间，单位为秒，如果是 0 则表示超时功能未生效。

**缺省情况：**86400。

**命令模式：**Captive Portal Instance 配置模式。

**使用指南：**定义 Captive Portal 配置的会话超时。

**举例：**定义 Captive Portal 配置的会话超时时间为 100 秒。

Switch (config-cp-instance)# session-timeout 100

## 7.16.1.35 show captive-portal

**命令：show captive-portal**

**功能：**使用该命令显示 Captive Portal 的特征状态。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式

**使用指南：**该命令显示本交换机上的 captive portal 功能的相关状态参数。

**举例：**显示 Captive Portal 的开启和关闭状态。

captive portal 开启的情况：

Switch #show captive-portal

Administrative Mode..... Enable

Operational Status..... Enabled

CP IP Address..... 101.1.1.3

captive portal 关闭的情况：

switch#show captive-portal

Administrative Mode..... Disable

Operational Status..... Disabled

Disable Reason..... Administrator Disabled

CP IP Address..... 0.0.0.0

## 7.16.1.36 show captive-portal status

**命令：show captive-portal status**

**功能：**该命令显示系统中所有的 Captive Portal 例程的状态。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式

**使用指南：**该命令显示本交换机上的 captive portal 的配置和所支持属性参数。

**举例：**显示控制器上的 Captive Portal 的状态。

Switch #show captive-portal status

Peer Switch Statistics Reporting Interval..... 120

Authentication Timeout..... 300

Authentication Type..... External

Supported Captive Portals..... 10

Configured Captive Portals..... 9

Active Captive Portals..... 0

Local Supported Users..... 128

Configured Local Users..... 0

System Supported Users..... 1024

Authenticated Users..... 0

## 7.16.1.37 show captive-portal configuration

**命令：show captive-portal configuration *<cp-id>***

**功能：**该命令显示了 Captive Portal 配置的状态。

**参数：***<cp-id>*是 captive portal 的 ID 号，范围是 1-10。

**缺省情况：**无。

**命令模式：**特权模式

**使用指南：**该命令显示 portal 的例程配置参数。

**举例：**显示 captive portal1 的配置情况。

Switch #show captive-portal configuration 1

CP ID..... 1

CP Name..... Default

Operational Status..... Enabled

Block Status..... Not Blocked

Configured Locales..... 1

Authenticated Users..... 0

Permit-all Status..... Disabled

## 7.16.1.38 show captive-portal configuration interface

**命令：show captive-portal configuration *<cp-id>* interface <IFNAME or ethernet or port-channel>**

**功能：**该命令显示所有分配到 captive portal 配置的接口的信息。

**参数：***<cp-id>*，cp 的 ID 号；

IFNAME ,Interface Name or number

Ethernet, Ethernet port

Port-channel,Port-channel

**缺省情况：**无。

**命令模式：**特权模式

**使用指南：**该命令显示某个 portal 例程的接口状态。

**举例：**显示 Captive Portal 配置的接口信息。

Switch # show captive-portal configuration 1 interface e1/1/1

CP ID..... 1

CP Name..... Default

Interface..... 1

Interface Description..... Ethernet1/1

Operational Status..... Enabled

Block Status..... Not Blocked

Authenticated Users..... 0

## 7.16.1.39 show captive-portal configuration status

**命令：show captive-portal configuration [<*cp-id*>] status**

**功能：**该命令显示所有的或特定的 Captive Portal 的配置信息。

**参数：**<*cp-id*>，cp 的 ID 号，此处带有参数<cp-id>表示显示某个例程的内容，不带该参数显示当前所有配置的例程相关参数。

**缺省情况：**无。

**命令模式：**特权模式

**使用指南：**该命令显示详细的 portal 例程配置参数。

**举例：**显示所有 Captive Portal 配置信息。

显示所有例程的状态：

Switch # show captive-portal configuration status

| CP ID | CP Name | Mode | Protocol | Verification |
|---|---|---|---|---|
| 1 | Default | Enable | HTTP | RADIUS |
| 2 | Default | Enable | HTTP | RADIUS |

## 7.16.1.40 show captive-portal client status

**命令：show captive-portal client [<*FF-FF-FF-FF-FF-FF*> { ipv4 | ipv6} <*ip-addr*>] status**

**功能：**该命令显示了连接到 captive portal 的用户的详细连接信息或概述。

**参数：**<*FF-FF-FF-FF-FF-FF*>为用户的 MAC 地址

ipv4 用户地址为 ipv4 地址

ipv6 用户地址为 ipv6 地址

<*ip-addr*>用户地址，ipv4 地址是以点分十进制格式，ipv6 地址是 X:X::X:X 的格式

**缺省情况：**无。

**命令模式：**特权模式

**使用指南：**该命令显示所有或某个 portal 用户的状态。

**举例：**显示连接到 captive portal 的用户 user1 的详细信息。

```
Switch # show captive-portal client status
MAC Address       IP Address          User Name   Protocol   Mode     Session Time
20-6a-8a-65-0d-17 66.1.1.2             user1         HTTP      RADIUS 0d:00:00:47
```

## 7.16.1.41 show captive-portal configuration client

**命令：show captive-portal configuration [<*cp-id*>] client status**

**功能：**该命令显示了某个接口下经过 portal 认证的客户端信息。

**参数：**<*cp-id*>，Captive Portal 的 ID 号。

**缺省情况：**无。

**命令模式：**特权模式

**使用指南：**该命令显示某个 portal 例程上的用户参数。

**举例：**显示经过认证的客户端的所有 captive portal 配置信息。

```
Switch #show captive-portal configuration 1 client status
CP ID..................................... 1
CP Name................................... Default
   Client MAC Address     Client IP Address   Interface      Interface Description

    00-24-8c-00-99-27      10.1.1.51             1922         Port-Channel2
```

## 7.16.1.42 show captive-portal ext-portal-server status

**命令：show captive-portal ext-portal-server status**

**功能：**使用该命令查看配置的外置 portal 服务器的信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**查看配置的外置 portal 服务器的信息。

**举例：**查看配置的外置 portal 服务器的信息。

```
Switch #show captive-portal ext-portal-server status
Server Name                Server IP Address                port        SocketNo
-------------------- ---------------------------------------- -------- --------
x1                         100.1.1.2                          7749              0
```

x2 100.1.1.1 7749 0

### 7.16.1.43 show captive-portal interface configuration status

**命令：show captive-portal interface configuration [<*cp-id*>] status**

**功能：**该命令显示为所有的 captive portal 配置或特定的配置的接口信息。

**参数：**<*cp-id*>，captive portal 的ID号。

**缺省情况：**无。

**命令模式：**特权模式

**使用指南：**该命令显示所有或某个portal例程与接口的绑定关系。

**举例：**显示为所有的 captive portal 配置的接口信息。

Switch #show captive-portal interface configuration status

| CP ID | CP Name | Interface | Interface Description | Type |
|---|---|---|---|---|
| 1 | Default | 1 | Ethernet1/1 | Physical |

## 7.16.2 Free-resource

### 7.16.2.1 free-resource（全局）

**命令：free-resource destination { ipv4 | ipv6} <*ip-addr*><*netmask*> }**

**no free-resource destination { ipv4 | ipv6} <*ip-addr*><*netmask*> }**

**功能：**该命令配置 free-resource 规则，符合规则中源 IP 地址段的客户端访问规则中目的 IP 地址段的资源，交换机不进行重定向，客户端不需要通过 Portal 认证可以直接访问。

**参数：**

ipv4 配置的 free resource 地址是 ipv4 地址

ipv6 配置的 free resource 地址是 ipv6 地址

<ip-addr> free-resource 规则中被访问/访问者的 IP 地址段

<netmask> free-resource 规则中被访问/访问者的 IP 地址段

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**配置可以免费访问资源的客户端地址段（访问者）和免费提供该资源的地址段（被访问者）。

**举例：**配置 free-resource 规则。

Switch (config)# free-resource destination ipv4 1.1.1.1/24

## 7.16.3 Portal 无感知

### 7.16.3.1 fast-mac-auth

**命令：fast-mac-auth**

**no fast-mac-auth**

**功能：**该命令配置开启 mac 快速认证功能。no 操作为关闭 mac 快速认证。

**参数说明：**无。

**命令模式：**Captive Portal Instance 模式。

**默认配置：**默认关闭。

**使用指南：**使能该功能后，如果 mac 认证成功，则不需要进行 portal 认证。

**举例：**开启 mac 快速认证功能。

Switch (config-cp-instance)#fast-mac-auth

## 7.16.4 认证成功后页面自动推送命令

### 7.16.4.1 redirect attribute url-after-login enable

**命令：redirect attribute url-after-login enable**

**no redirect attribute url-after-login enable**

**功能：**使能重定向 url 中携带认证成功后推送 url 地址的功能。本命令的 no 形式为关闭重定向 url 中携带认证成功后推送 url 地址的功能。

**参数：**无。

**命令模式：**captive portal instance 配置模式

**缺省情况：**缺省情况下重定向 url 中携带认证成功后推送 url 地址的功能是关闭的。

**使用指南：**本命令用于使能重定向 url 中携带认证成功后推送 url 地址的功能。使能改功能后，交换机推出的重定向 url 中会携带认证成功后需要推送的 url 地址，同时当 redirect attribute url-after-login value 配置的<url-value>为空时，携带的 url 地址为用户认证前访问的页面地址，若不为空，则携带的 url 地址为<url-value>所配置的地址。

**举例：**使能重定向 url 中携带认证成功后推送 url 地址的功能。

Switch (config-cp-instance)#redirect attribute url-after-login enable

### 7.16.4.2 redirect attribute url-after-login name

**命令：redirect attribute url-after-login name <name>**

**no redirect attribute url-after-login name**

**功能：**配置在重定向 url 中携带认证成功后推送 url 地址的属性值名称。本命令的 no 形式为恢复重定向 url 中携带认证成功后推送 url 地址的属性值名称为默认值。

**参数：**<name>，为配置的属性值名称。最多 32 个字符。

**命令模式：**captive portal instance 配置模式。

**缺省情况：**缺省情况下重定向 url 中携带认证通过后推送 url 地址的属性值名称为 srcurl。

**使用指南：**本命令用于配置在重定向 url 中携带认证成功后推送 url 地址的属性值名称。

**举例：**配置在重定向 url 中携带认证成功后推送 url 地址的属性值名称为 redirect

Switch (config-cp-instance)#redirect attribute url-after-login name redirect

### 7.16.4.3 redirect attribute url-after-login encode

**命令：redirect attribute url-after-login encode {plain-text|base64}**

**功能：**配置对重定向 url 中携带的认证成功后推送 url 地址的编码方式。

**参数：**plain-text，为明文方式；

base64，为 base64 编码方式。

**命令模式：**captive portal instance 配置模式。

**缺省情况：**缺省情况下重定向 url 中携带的认证成功后推送 url 地址的编码方式为 plain-text 明文方式。

**使用指南：**本命令用于配置对重定向 url 中携带的认证成功后推送 url 地址的编码方式。可以根据 portal server 所支持的编码方式来配置。

**举例：**配置对重定向 url 中携带的认证成功后推送 url 地址的编码方式为 base64 编码方式。

Switch (config-cp-instance)#redirect attribute url-after-login encode base64

### 7.16.4.4 redirect attribute url-after-login value

**命令：redirect attribute url-after-login value <url-value>**

**no redirect attribute url-after-login value**

**功能：**配置用户认证成功后弹出的指定页面的 url 地址。本命令的 no 形式为删除用户认证成功后弹出的指定页面的 url 地址。

**参数：**<url-value>，为配置的指定页面的 url 地址。最多 512 个字符。

**命令模式：**captive portal instance 配置模式。

**缺省情况：**无。

**使用指南：**本命令用户配置用户认证成功后弹出的指定页面的 url 地址。如果开启重定向 url 中携带认证成功后推送的 URL 地址的功能，这样在重定向 url 中会携带值为<url-value>的指定页面的 URL 地址。

**举例：**配置用户认证成功后弹出的指定页面的 url 地址为 http://www.test.com。

Switch (config-cp-instance)#redirect attribute url-after-login value http://www.test.com

## 7.16.5 Portal 逃生

### 7.16.5.1 portal-server-detect server-name <name>

**命令：portal-server-detect server-name <name> [interval <interval>] [retry <retries>][action {log | permit-all | trap }]**

**no portal-server-detect server-name <name>**

**功能：**开启 Portal server 的逃生功能，并配置相关的检测参数和服务器状态变化时的操作。

**参数：**<name>为 Portal 服务器名称，为 1～32 个字符的字符串，区分大小写。该 Portal 服务器必须已经存在。<interval>：进行探测尝试的时间间隔，取值范围为 20～600，单位为秒，缺省值为 20。<retries>：连续探测失败的最大次数，取值范围为 1～5，缺省值为 3。若连续探测失败数目达到此值，则认为服务器不可达。 { log | permit-all | trap }：Portal 服务器可达状态发生变化时，可触发执行的操作。包括以下三种，且同时可选择多种。

- log：Portal 服务器状态发生改变时，发送日志信息。日志信息中记录了 Portal 服务器名称以及该服务器状态改变前后的状态信息。
- trap：Portal 服务器状态发生改变时，向网管服务器发送 Trap 信息。Trap 信息中记录了 Portal 服务器名称以及该服务器状态改变前后的状态信息。
- permit-all：也称为 Portal 逃生，表示在 Portal 服务器不可达（down）时，暂时取消 Portal 认证，允许所有 Portal 用户访问网络资源。之后，若服务器状态变为可达（up）时，恢复其 Portal 认证功能。

**缺省情况：**逃生功能关闭。interval 缺省为 20，retries 缺省为 3，action 缺省为 permit-all。

**命令模式：**Captive Portal 全局配置模式。

**使用指南：**为了保证 Portal server 发生故障时，可以用该命令打开 Portal 逃生功能。打开 Portal 逃生功能后，如果交换机和 Portal server 连接正常，对于用户 Portal 认证没有任何影响；只有当交换机和 Portal server 连接中断时，才会允许用户不通过认证就可以访问网络。运营商也可以打开逃生功能，但是触发的操作只选择 log 或 trap。

**举例：**打开名称为 test 的 Portal server 的逃生功能,探测周期为 30 秒，最大失败次数为 2，服务器状态变化时触发的操作为发送日志和允许用户接入网络。

Switch (config-cp)# portal-server-detect server-name test interval 600 retry 2 action log permit-all trap

## 7.16.5.2 portal-server-detect client-deauth

**命令：portal-server-detect client-deauth**

**no portal-server-detect client-deauth**

**功能：**开启此命令，则服务器状态从 down 转变为 up 后，所有用户强制下线。no 操作为关闭此命令，则配置 Portal 服务器探测状态从 down 转变为 up 后，不强制已经在线的用户下线。

**参数：**无。

**缺省情况：**默认开启。

**命令模式：**captive portal 模式。

**使用指南：**该命令默认开启，即默认配置为所有用户在服务器状态该变时强制下线。隐藏命令，show run 不能看到。

Switch (config-cp)# portal-server-detect client-deauth

# 7.17 MAB

## 7.17.1 authentication mab

**命令：authentication mab {radius|local} (none|)**

**no authentication mab**

**功能：**配置 MAC 地址认证对登录用户的验证方式和验证选择优先级；该命令的 no 命令恢复缺省验证方式。

**参数：**radius 表示 RADIUS 验证方式，local 表示本地认证，none 表示不需要认证。

**缺省情况：**缺省仅使用 RADIUS 验证方式。

**命令模式：**全局配置模式。

**使用指南：**none 选项用于 MAC 地址认证的逃生功能。当配置的所有 RADIUS 服务器没有应答时，交换机可以采用 none 验证方式，直接放行 MAC 地址认证用户。local 选项用于 MAC 地址的本地认证，通过本地用户名密码进行认证。如果配置成 authentication mab radius local none 的方式，当 radius 服务器无响应时，判断本地是否配置了 mab 认证所使用的用户名和密码，如果配置，则使用 local 进行认证，如果没有配置，则使用后面备用的 none 认证方式。

**举例：**配置 MAC 地址认证支持本地认证及逃生功能。

Switch(config)#authentication mab radius local none

## 7.17.2 clear mac-authentication-bypass binding

**命令：clear mac-authentication-bypass binding {mac WORD | interface (ethernet IFNAME | IFNAME) | all}**

**功能：**删除 MAB 绑定信息。

**参数：MAC:** 删除指定 MAC 地址的 MAB 绑定

**IFNAME:** 删除指定端口上的 MAB 绑定

**all:**删除所有 MAB 的绑定

**命令模式：**特权配置模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**删除所有的 MAB 绑定。

Switch#clear mac-authentication-bypass binding all

## 7.17.3 debug mac-authentication-bypass

**命令：debug mac-authentication-bypass {packet | event | binding}**

**功能：**打开调试 MAB 认证的报文信息或事件信息或绑定信息的开关。

**参数：packet：**打开 MAB 认证功能的报文信息的调试开关。

**event：**打开 MAB 认证功能的事件信息的调试开关。

**binding**：打开 MAB 认证功能的绑定信息的调试开关。

**命令模式**：特权配置模式。

**缺省情况**：无。

**使用指南**：无。

**举例**：打开 MAB 认证功能的报文信息调试开关。

Switch#debug mac-authentication-bypass packet

## 7.17.4 mac-authentication-bypass binding-limit

**命令**：**mac-authentication-bypass binding-limit <*1-100*>**

**no mac-authentication-bypass binding-limit**

**功能**：设置端口上允许建立的最大 MAB 绑定数目；本命令的 no 操作为恢复默认最大动态绑定数目 3。

**参数**：**<*1-100*>**端口 MAB 最大绑定数目，范围为 1-100。

**命令模式**：端口配置模式

**缺省情况**：默认最大 MAB 绑定数目为 3。

**使用指南**：限制端口最大 MAB 绑定数目，当绑定数目达到最大 MAB 绑定数目时，端口将不能再进行绑定，如果设置的最大绑定数目小于目前端口的绑定数目，设置将不成功。

**举例**：配置端口最大绑定数目为 10。

Switch(Config)#interface ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)#mac-authentication-bypass binding-limit 10

## 7.17.5 mac-authentication-bypass enable

**命令**：**mac-authentication-bypass enable**

**no mac-authentication-bypass enable**

**功能**：打开交换机全局及端口的 MAB 功能；本命令的 no 操作为关闭 MAB 功能。

**参数**：无。

**命令模式**：全局配置模式及端口配置模式

**缺省情况**：默认不启动 MAB 认证全局及端口功能。

**使用指南**：如果要对端口进行 MAB 认证时，首先要打开全局下的 MAB 功能，再在相应的端口下打开 MAB 功能。

**举例**：打开全局及端口 Eth1/1/1 的 MAB 认证功能。

Switch(Config)# mac-authentication-bypass enable

Switch(Config)#interface ethernet 1/1/1

Switch(Config-If-Ethernet1/1/1)# mac-authentication-bypass enable

## 7.17.6 mac-authentication-bypass guest-vlan

**命令**：**mac-authentication-bypass guest-vlan <*1-4094*>**

**no mac-authentication-bypass guest-vlan**

**功能：** 设置 MAB 认证的 guest vlan；此命令的 no 操作为清除 MAB 认证的 guest vlan。

**参数：** ***<1-4094>***： guest vlan id，范围为 1-4094。

**命令模式：** 端口配置模式

**缺省情况：** 无。

**使用指南：** 设置 MAB 认证的 guest vlan，此命令只能在 hybrid 端口上使用，在 access 端口上使用无效。在 MAB 认证失败后，如果端口上配置了 guest vlan 并且 guest vlan 存在，MAB 用户接入端口属于 guest vlan，则 MAB 用户加入 guest vlan，允许 MAB 用户访问 guest vlan 中的资源。

**举例：** 配置端口 1/1/1MAB 认证的 guest vlan。

Switch(Config)#interface ethernet 1/1/1

Switch(config-If-Ethernet1/1/1)#mac-authentication-bypass guest-vlan 10

## 7.17.7 mac-authentication-bypass spoofing-garp-check

本型号交换机不支持此命令。

## 7.17.8 mac-authentication-bypass timeout linkup-period

**命令：mac-authentication-bypass timeout linkup-period *<0-30>***

**no mac-authentication-bypass timeout linkup-period**

**功能：** 设置当 MAB 端口 VLAN 绑定转变（认证失败或成功）时，为重新获取 IP，down/up 端口的时间间隔。

**参数：** ***<0-30>***： 端口自动 shutdown 后，重新 up 的时间间隔，单位是秒（s）；0 表示不进行 down/up 操作。

**命令模式：** 全局配置模式

**缺省情况：** 默认的 down/up 的时间间隔为 0，即不进行 down/up 操作。

**使用指南：** 当 MAB 认证成功时，会根据 auto-vlan 的设置下发 VLAN；而 MAB 认证失败后，则根据 guest-vlan 的设置下发 VLAN。在设置 linkup-period 后，MAB 端口 VLAN 绑定改变时，会自动 shutdown，经过 linkup-period 时间自动重新 up，以自动获取客户端 IP。

**举例：** 配置 down/up 时间为 12s。

Switch(Config)# mac-authentication-bypass timeout linkup-period 12

## 7.17.9 mac-authentication-bypass timeout offline-detect

**命令：mac-authentication-bypass timeout offline-detect (0 | <60-7200>)**

**no mac-authentication-bypass timeout offline-detect**

**功能：**配置下线检测时间；此命令的 no 操作是恢复下线检测时间为默认值。

**参数：(*0* | *<60-7200>*):**下线检测时间，范围为 0 或者 60 秒到 7200 秒之间。

**命令模式：**全局配置模式

**缺省情况：**默认下线检测时间为 180 秒。

**使用指南：**当设置的下线检测时间为 0 时，交换机不对 MAB 绑定做下线检测，当设置的下线检测时间为 60 秒到 7200 秒之间时，交换机定时检查 MAB 绑定是否有流量通过，当发现一定时间内没有流量通过时，将删除这个绑定，禁止此源 MAC 流量通过。

**举例：**配置下线检测时间为 200 秒.

Switch(Config)# mac-authentication-bypass timeout offline-detect 200

## 7.17.10 mac-authentication-bypass timeout quiet-period

**命令：mac-authentication-bypass timeout quiet-period <1-60>**

**no mac-authentication-bypass timeout quiet-period**

**功能：**设置 MAB 认证的静默时间；此命令的 no 操作恢复 MAB 功能的静默时间为默认值。

**参数：*<1-60>*：**静默时间，范围为 1 到 60s。

**命令模式：**全局配置模式。

**缺省情况：**默认静默时间为 30s。

**使用指南：**端口 MAB 认证失败后在静默时间内，不响应此 MAC 的认证请求，在静默时间后，重新响应。

**举例：**配置 MAB 认证静默时间为 60s。

Switch(Config)#mac-authentication-bypass timeout quiet-period 60

## 7.17.11 mac-authentication-bypass timeout reauth-period

**命令：mac-authentication-bypass timeout reauth-period *<1-3600>***

**no mac-authentication-bypass timeout reauth-period**

**功能：** 设置处于认证失败状态的用户重认证的时间间隔；此命令的 no 操作恢复 MAB 功能重认证时间为默认值。

**参数： *<1-3600>*：** 重认证的时间间隔，范围为 1-3600s。

**命令模式：** 全局配置模式

**缺省情况：** 默认重认证的时间间隔为 30s。

**使用指南：** 处于认证失败状态的用户，每隔一段的时间进行重认证，如果认证成功则转化为认证通过状态，允许访问网络资源。

**举例：** 配置 MAB 重认证时间为 20s。

Switch(Config)# mac-authentication-bypass timeout reauth-period 20

## 7.17.12 mac-authentication-bypass timeout stale-period

**命令：mac-authentication-bypass timeout stale-period *<0-60>***

**no mac-authentication-bypass timeout stale-period**

**功能：**设置在 MAB 端口 down 后，删除绑定用户的时间；此命令的 no 操作为恢复 MAB 功能延时删除绑定时间为默认值。

**参数：*<0-60>*：**延时删除绑定的时间，范围为 0-60s。

**命令模式：**全局配置模式

**缺省情况：**默认端口 down 后延时删除绑定的时间为 30s。

**使用指南：**当配置延时删除绑定时间为 0 时，MAB 端口 down 后，会立即删除端口下的所有用户绑定。当配置延时删除绑定的时间大于 0 时，MAB 端口 down 后，等待该延时值后再删除用户绑定。

**举例：**配置 MAB 延时删除时间为 40s。

Switch(Config)# mac-authentication-bypass timeout stale-period 40

## 7.17.13 mac-authentication-bypass username-format

**命令：mac-authentication-bypass username-format {**

**mac-address (groupsize (1|2|4|12) |) (separator WORD |) (lowercase | uppercase |)**

**| {fixed username WORD password WORD}}**

**功能：**设置 MAB 认证功能的认证方式。

**参数：mac-address:**使用 MAB 用户的 MAC 地址作为用户名和密码进行认证。

**groupsize (1|2|4|12)**:使用 MAB 用户的 MAC 地址的一个间隔的大小，缺省为 2。

**separator WORD**:使用 MAB 用户的 MAC 地址的分隔符，separator 支持'-' ':' '.'，缺省间隔为'-'。

**lowercase | uppercase**:使用 MAB 用户的 MAC 地址的大小写，缺省为小写。

**fixed username *WORD* password *WORD***：使用 MAB 网络管理员指定的用户名和密码进行认证，用户名和密码的长度范围为 1 到 32 个字符。

**命令模式：**全局配置模式

**缺省情况：**使用 MAB 用户的 MAC 地址作为用户名和密码进行认证。

**使用指南：**MAB 认证功能有两种认证方式，一种是采用 MAC 地址作为 MAB 用户的用户名和密码进行认证，另一种是 MAB 用户使用指定的用户名和密码进行认证，如果没有指定用户名和密码，设备默认采用 MAC 地址作为用户名和密码进行认证。

**举例：**配置所有 MAB 用户使用用户名 mab-user 和密码 mab-pwd 进行认证。

Switch(Config)# mac-authentication-bypass username-format fixed username mab-user password mab-pwd

## 7.17.14 show mac-authentication-bypass

**命令：show mac-authentication-bypass {interface {ethernet IFNAME | IFNAME) |}**

**功能：**显示 MAB 认证的绑定信息。

**参数：interface {ethernet IFNAME | IFNAME}：**端口名称

**命令模式：**特权配置模式

**缺省情况：**无。

**使用指南：**无。

**举例：**显示所有 MAB 用户绑定信息。

Switch#show mac-authentication-bypass

The Number of all binding is 5

| MAC | Interface | Vlan ID | State |
|---|---|---|---|
| 05-0a-eb-6a-7f-88 | Ethernet1/1/1 | 1 | MAB_QUIET |
| 04-0a-eb-6a-7f-88 | Ethernet1/1/1 | 1 | MAB_QUIET |
| 03-0a-eb-6a-7f-88 | Ethernet1/1/1 | 1 | MAB_QUIET |
| 02-0a-eb-6a-7f-88 | Ethernet1/1/1 | 1 | MAB_AUTHENTICATED |
| 00-0a-eb-6a-7f-8e | Ethernet1/1/1 | 1 | MAB_AUTHENTICATED |

| 显示信息 | 解释 |
|---|---|
| The Number of all binding | 所有的 MAB 用户绑定数目，包括认证成功及认证失败而处于静默状态的用户 |
| MAC | MAB 用户的 MAC 地址 |
| Interface | MAB 用户绑定的端口 |
| Vlan | MAB 用户所属 VLAN |
| State | MAB 用户认证状态 |

Switch(config)#show mac-authentication-bypass int e1/1/1

Interface Ethernet1/1/1 user config:

MAB enable: Enable

Binding info: 1

---

MAB Binding built at SUN JAN 01 01:14:48 2006

VID 1, Port: Ethernet1/1/1

Client MAC: 00-0a-eb-6a-7f-8e

Binding State: MAB_AUTHENTICATED

Binding State Lease: 164 seconds left

| 显示信息 | 解释 |
| --- | --- |
| MAB enable | 端口 MAB 功能的开关显示 |
| Binding info | 指定端口上 MAB 绑定用户的数量 |
| MAB Binding built at | 创建 MAB 绑定用户的时间 |
| VID | MAB 用户所属 VLAN |
| Port | MAB 用户绑定的端口 |
| Client MAC | MAB 用户的 MAC 地址 |
| Binding State | MAB 用户认证状态 |
| Binding State Lease | MAB 用户绑定的释放剩余时间 |

# 第 8 章 可靠性命令

## 8.1 MSTP

### 8.1.1 MSTP

#### 8.1.1.1 abort

**命令：abort**

**功能：**放弃本次对 MSTP 域的配置，并且退出 MST 配置模式回到全局配置模式。

**命令模式：**MSTP 域配置模式。

**使用指南：**当使用本命令退出 MST 配置模式时，本次对 MSTP 域做的配置不生效，生效的仍然是前一次保留 MSTP 域配置。

**举例：**退出 MST 配置模式，并且不保留本次配置。

Switch(Config-Mstp-Region)#abort

Switch(config)#

#### 8.1.1.2 exit

**命令：exit**

**功能：**保存本次对 MSTP 域的配置，并且退出 MSTP 域配置模式回到全局配置模式。

**命令模式：**MSTP 域配置模式。

**使用指南：**当使用本命令退出 MST 配置模式时，本次对 MSTP 域做的配置即时生效。

**举例：**退出 MST 配置模式，并且保留本次配置。

Switch(Config-Mstp-Region)#exit

Switch(config)#

#### 8.1.1.3 instance vlan

**命令：instance *<instance-id>* vlan *<vlan-list>***

**no instance *<instance-id>* [vlan *<vlan-list>*]**

**功能：**在 MSTP 域配置模式下，创建 Instance 及配置 VLAN 与 Instance 的映射关系或添加 VLAN 表项与指定 Instance 映射关系；本命令的 no 操作为删除指定的 Instance 或删除某些 VLAN 表项与指定 Instance 的映射关系。

**参数：**对于非 no 命令，***<instance-id>***为 Instance 号，取值范围为 0~64；对于 no 命令，***<instance-id>***为 Instance 号，取值范围为 0~64。***<vlan-list>***为连续的或不连续的 VLAN 号，支持表示连续的“-”符号和不连续的“;”符号。

**命令模式：**MSTP 域配置模式。

**缺省情况：**在没有创建任何 Instance 时，交换机只有 Instance 0，且 VLAN1~4094 均属于 Instance 0。

**使用指南：**本命令用于设置 VLAN 与 Instance 的映射关系，只有所有的映射关系都相同且其他 MSTP 域的参数也相同，交换机才能认为彼此是在相同的 MSTP 域中。在没有配置任何 Instance 时，所有的 VLAN 都属于 Instance 0。MSTP 最多支持 64 个 MSTI（除了 CIST 之外）。可以把 CIST 理解为 MSTI0，其余实例为 MSTI1～64。具体个数依照产品规格而定，64 只是最大的规格值。

**举例：**配置 VLAN1-10;100-110 与 Instance 1 的映射关系。

Switch(config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#instance 1 vlan 1-10;100-110

## 8.1.1.4 name

**命令：name *<name>***

**no name**

**功能：**在 MSTP 域配置模式下，配置 MSTP 域的名字；本命令的 no 操作为删除 MSTP 域的名字。

**参数：*<name>***为 MSTP 域名字，取值范围不超过 32 字节的字符串。

**命令模式：**MSTP 域配置模式。

**缺省情况：**缺省 MSTP 域的名字为该交换机网桥 MAC。

**使用指南：**本命令用于设置 MSTP 域的名字，只有 MSTP 域的名字相同且其他 MSTP 域的参数也相同，交换机才能认为彼此是在相同的 MSTP 域中。

**举例：**配置 MSTP 域的名字为 mstp-test。

Switch(config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#name mstp-test

## 8.1.1.5 no

**命令：no *<instance-id>* | *<name>* | *<revision-level>***

**功能：** 取消一条命令或设置为初始值。

**参数：** *<instance-id>* instance 号，*<name>* mstp 域名，*<revision-level>* 用于计算 MST 配置标识的修正数值。

**命令模式：** MSTP 域配置模式。

**使用指南：**本命令可以删除指定的 instance,删除 MSTP 域的 name,恢复修正数值的缺省值为 0。

**举例：** 删除 instance 1。

Switch(Config-Mstp_Region)#no instance 1

## 8.1.1.6 revision-level

**命令：revision-level *<level>***

**no revision-level**

**功能：**在 MST 配置模式下，配置用于计算 MST 配置标识的修正数值；本命令的 no 操作为恢复修正数值的缺省值 0。

**参数：*<level>***为修正数值，取值范围为 0~65535。

**命令模式：**MSTP 域配置模式。

**缺省情况：**缺省修正数值为 0。

**使用指南：**本命令用于设置计算 MST 配置标识时用到的修正数值，只有修正数值相同且其他 MSTP 域的参数也相同，交换机才能认为彼此是在相同的 MSTP 域中。

**举例：**配置修正数值为 2000。

Switch(config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)# revision-level 2000

## 8.1.1.7 show

**命令：show**

**功能：** 显示当前运行系统的信息。

**命令模式：** MSTP 域配置模式。

**使用指南：** 使用本命令，可以详细的查看当前系统的信息。

**举例：** 显示当前运行系统的信息。

Switch(Config-Mstp-Region)#show

## 8.1.1.8 spanning-tree

**命令：spanning-tree**

**no spanning-tree**

**功能：**在交换机的全局配置模式和端口配置模式下分别启动 MSTP 协议的命令；本命令的 no 操作为关闭 MSTP 协议。

**命令模式：**全局配置模式和端口配置模式。

**缺省情况：**系统缺省不运行 MSTP 协议。

**使用指南：**如果在全局配置模式下启动了 MSTP 协议，除了在端口上打开与 MSTP 应用互斥的端口外，所有的端口缺省都打开 MSTP 协议。

**举例：**在全局模式打开 MSTP，并且在端口 1/1/2 模式上关闭 MSTP。

Switch(config)#spanning-tree

Switch(config)#interface ethernet 1/1/2

Switch(Config-If-Ethernet1/1/2)#no spanning-tree

## 8.1.1.9 spanning- tree cost

**命令：spanning-tree cost *<cost>***

**no spanning-tree cost**

**功能：** 设置当前以太网端口的路径代价；本命令的 no 操作为恢复缺省值。

**参数：** ***<cost>*** 为路径代价值，取值范围为 1~200,000,000。

**命令模式：** 端口配置模式。

**缺省情况：** 缺省情况下，端口的路径代价与端口的带宽相关。

| 端口类型 | 缺省路径开销 | 建议取值范围 |
|---|---|---|
| 10Mbps | 2000000 | 2000000~20000000 |
| 100Mbps | 200000 | 200000~2000000 |
| 1Gbps | 20000 | 20000~200000 |
| 10Gbps | 2000 | 2000~20000 |

对汇聚端口，端口缺省路径代价如下：

| 端口类型 | 汇聚端口个数（在允许汇聚的个数范围内） | 缺省路径开销 |
|---|---|---|
| 10Mbps | N | 2000000/N |
| 100Mbps | N | 200000/N |
| 1Gbps | N | 20000/N |
| 10Gbps | N | 2000/N |

**使用指南：** 通过配置端口路径代价可以控制端口到根网桥的根路径代价，从而控制该端口、指定端口等的选举。

**举例：** 在端口 1/1/2 上设置端口路径代价为 3000000。

Switch(Config-If-Ethernet1/1/2)#spanning-tree cost 3000000

## 8.1.1.10 spanning-tree cost-format

**命令：spanning-tree cost-format {dot1d | dot1t}**

**功能：在交换机的全局配置模式下可修改路径开销值的表示方式，有 dot1d 和 dot1t 格式可选用，默认使用 dot1t 格式。**

**命令模式：全局配置模式。**

**缺省情况：系统缺省使用 dot1t 格式计算路径开销值。**

**使用指南：cost 值的表示方法有两种，分别是 IEEE802.1d-2008 上标示的 dot1d 方式，和 IEEE802.1t 上标示的 dot1t 方式。两种方法定义的路径开销值的取值范围不同，dot1d 的取值范围是 1-65535，dot1t 的取值范围是 1-200000000。**

若用户已使用 spanning-tree cost 命令手动配置过链路上的 cost 值，则使用 cost-format 命令修改 cost 表示方法的配置不能成功，除非用户将手动配置清除。

**举例：在全局模式修改 cost 格式**

Switch(config)#spanning-tree cost-format dot1d

## 8.1.1.11 spanning-tree digest-snooping

**命令：spanning-tree digest-snooping**

**no spanning-tree digest-snooping**

**功能：**配置端口使用对端的认证字，本命令的 no 形式配置端口不使用对端认证字。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**不使用对端认证字。

**使用指南：**MSTP 协议使用指定的密钥，对 INSTANCE 和 VLAN 的对应关系使用 MD5 算法生成区域的认证字，由于个别厂商没有遵守协议的要求使用指定的密钥，而使用了私有的密钥，导致其设备与其它厂商设备无法通过配置实现域内互通，通过该命令可以在指定的端口上使用对方的认证字以实现与其的域间互通。注意：这种配置可能导致 INSTANCE 与 VLAN 对应关系不同的相邻设备认为对端是同一区域，因此使用该功能时要由管理员保证其对应关系一致。并且要保证设备间所有的端口都进行该配置，以避免不希望的后果。

**举例：**配置端口使用对端的认证字。

```
Switch(config)#interface ethernet 1/1/2
Switch(Config-If-Ethernet1/1/2)#spanning-tree digest-snooping
Switch(Config-If-Ethernet1/1/2)#
```

## 8.1.1.12 spanning-tree format

**命令：spanning-tree format {standard | privacy | auto}**

**no spanning-tree format**

**功能：**配置端口报文格式，以便于与其它厂商产品互通。本命令的 no 操作恢复格式为默认的格式。

**参数：standard**：IEEE 规定的报文格式；

**privacy**：私有报文格式，与 CISCO 设备兼容的格式；

**auto**：自动识别报文格式，即通过查看收到的报文的格式决定自己的报文格式。

**命令模式：**端口配置模式。

**缺省情况：**自动识别报文格式。

**使用指南：**由于 CISCO 使用了与 IEEE 规定的报文格式不同的格式，而很多厂家为了与 CISCO 兼容也采用了与 CISCO 相同的格式，因此我们要同时支持这两种格式。其中标准格式（standard）是完全按照 IEEE 规定的格式，私有报文格式（privacy）是与 CISCO 兼容的格式，另外，如果我们不清楚对端是何种格式，可以配置为 AUTO，我们可以根据对方发出的报文识别对方支持何种格式。为了与过往产品和主流厂家的更好的兼容，我们默认的形式是自动识别报文，在配置为 AUTO 时，在收到对方发出的报文前也认为是私有报文格式。

如果我们配置的格式不是 AUTO，而对端与我们规定的格式不匹配，我们在收到对端的报文后，会设置收到报文的端口状态为 DISCARDING 以避免双方都认为自己是根而造成环路。

如果我们配置的格式是 AUTO，而端口外连接了互不兼容的超过 1 个设备（例如通过 HUB 或透传 BPDU 的设备连接了多个运行 MSTP 的设备），我们会统计一段时间内端口格式改变的次数，超过该次数（250 秒内改变 10 次）后，端口将被关闭，只有管理员的干预才能再把端口打开。

**举例：**配置端口报文格式为 IEEE 规定的报文格式。

Switch(config)#interface ethernet 1/1/2

Switch(Config-If-Ethernet1/1/2)#spanning-tree format standard

Switch(Config-If-Ethernet1/1/2)#

## 8.1.1.13 spanning-tree forward-time

**命令：spanning-tree forward-time *<time>***

**no spanning-tree forward-time**

**功能：**设置交换机转发延时的时间值；本命令的 no 操作为恢复缺省值。

**参数：*<time>***为转发延时的时间值，单位为秒，取值范围为 4~30。

**命令模式：**全局配置模式。

**缺省情况：**转发延时缺省为 15 秒。

**使用指南：**当网络拓扑发生变换时，端口状态从阻塞状态转变到监听状态的这段延时称为转发延时。转发延时和 Hello 时间值、最大老化时间之间是有关联的，用户在配置 MSTP 时间参数时必须满足如下条件，否则会影响 MSTP 的正确工作：

2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)

**举例：**在全局模式配置 MSTP 转发延时时间为 20 秒。

Switch(config)#spanning-tree forward-time 20

## 8.1.1.14 spanning-tree hello-time

**命令：spanning-tree hello-time *<time>***

**no spanning-tree hello-time**

**功能：**设置交换机 Hello 时间值；本命令的 no 操作为恢复缺省值。

**参数：*<time>***为 Hello time 的时间值，单位为秒，取值范围为 1~10。

**命令模式：**全局配置模式。

**缺省情况：**Hello 时间缺省为 2 秒。

**使用指南：**交换机发送 BPDU 的时间间隔称为 Hello 时间。Hello 时间和转发延时、最大老化时间之间是有关联的，用户在配置 MSTP 时间参数时必须满足如下条件，否则会影响 MSTP 的正确工作：

2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)

**举例：**在全局模式配置 MSTP Hello 时间为 5 秒。

Switch(config)#spanning-tree hello-time 5

## 8.1.1.15 spanning-tree link-type p2p

**命令：spanning-tree link-type p2p {auto | force-true | force-false}**

**no spanning-tree link-type**

**功能：**设置与当前端口相连的链路类型；本命令的 no 操作恢复当前端口的链路类型为自动检测。

**参数：auto** 表示由系统自动检测链路类型，**force-true** 表示强制为点对点类型，**force-false** 表示强制为非点对点类型。

**命令模式：**端口配置模式。

**缺省情况：**缺省情况下为 auto，MSTP 协议会自动检测端口相连的链路类型。

**使用指南：**当端口工作在全双工模式下，MSTP 协议会自动认为与该端口相连的链路类型为点对点类型；当端口工作在半双工模式下，MSTP 协议会自动认为与该端口相连的链路类型为共享型。

**举例：**强制交换机的端口 1/1/7-8 为点到点连接。

Switch(config)#interface ethernet 1/1/7-8

Switch(Config-If-Port-Range)#spanning-tree link-type p2p force-true

## 8.1.1.16 spanning-tree maxage

**命令：spanning-tree maxage *<time>***

**no spanning-tree maxage**

**功能：**设置交换机 BPDU 信息的最大老化时间值；本命令的 no 操作为恢复缺省值。

**参数：*<time>***为最大老化时间值，单位为秒，取值范围为 6~40。

**命令模式：**全局配置模式。

**缺省情况：**最大老化时间缺省为 20 秒。

**使用指南：**BPDU 的生命周期称为最大老化时间。最大老化时间和转发延时、Hello 时间之间是有关联的，用户在配置 MSTP 时间参数时必须满足如下条件，否则会影响 MSTP 的正确工作：

2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)

**举例：**在全局模式配置 maxage 时间为 25 秒。

Switch(config)#spanning-tree maxage 25

## 8.1.1.17 spanning-tree max-hop

**命令：spanning-tree max-hop *<hop-count>***

**no spanning-tree max-hop**

**功能：**设置 BPDU 支持在 MSTP 域中传输的最大跳数；本命令的 no 操作为恢复缺省值。

**参数：*<hop-count>***为最大跳数，取值范围为 1~40。

**命令模式：**全局配置模式。

**缺省情况：**最大跳数缺省为 20。

**使用指南：**在 MSTP 协议中不仅保留 Max-age 表示 BPDU 的生命周期，在 MSTP 域中还增加了 Max-hop 表示 BPDU 的生命周期，Max-hop 在网络中的传输呈递减状态。从 MSTI 的根网桥发出时 Max-hop 为最大值，BPDU 每被接收一次，该 BPDU 的 Max-hop 值就减少一跳，当交换机端口接收到 Max-hop 为 0 的 BPDU 时，该端口就会丢弃该 BPDU，并且将本端口作为指定端口发送 BPDU。

**举例：**设置最大跳数为 32。

```
Switch(config)#spanning-tree max-hop 32
```

## 8.1.1.18 spanning-tree mcheck

**命令：spanning-tree mcheck**

**功能：**迫使交换机端口迁移到 MSTP 模式下运行。

**命令模式：**端口配置模式。

**缺省情况：**端口运行在 MSTP 模式下。

**使用指南：**如果在与当前以太网端口相连的网段内存在运行 IEEE 802.1D STP 协议的网桥，该端口会迁移到 STP 兼容模式下运行。在网络比较稳定的情况下，虽然网段内运行 STP 协议的网桥被拆离，但与之相连的运行 MSTP 协议的交换机的端口仍然会运行在 STP 兼容模式下，此时可以通过该命令迫使其迁移到 MSTP 模式下运行。端口迁移到 MSTP 模式下运行后，如果再次收到新的 STP 报文，端口又会回到 STP 兼容模式下。

该命令必须在交换机运行在 IEEE802.1s MSTP 模式下时进行配置，如果交换机的协议运行模式被配置为 IEEE802.1D STP 模式，则该命令无效。

**举例：**强制端口 1/1/2 迁移到 MSTP 模式下运行。

```
Switch(Config-If-Ethernet1/1/2)#spanning-tree mcheck
```

## 8.1.1.19 spanning-tree mode

**命令：spanning-tree mode {mstp | stp | rstp}**

**no spanning-tree mode**

**功能：**设置交换机运行 Spanning Tree 的模式；本命令的 no 操作为恢复交换机缺省的模式。

**参数：mstp** 为设置交换机运行 IEEE802.1s 的 MSTP 模式；**stp** 为设置交换机运行 IEEE802.1D STP 模式; **rstp** 为设置交换机运行 IEEE802.1w RSTP 模式。

**命令模式：**全局配置模式。

**缺省情况：**交换机缺省运行 MSTP 模式。

**使用指南：**当交换机运行 IEEE802.1D STP 模式时，只能发送标准的 802.1D BPDU 帧和 TCN BPDU，对接收到的任何 MSTP BPDU 都将丢弃。

**举例：**设置交换机运行 STP 模式。

Switch(config)#spanning-tree mode stp

## 8.1.1.20 spanning-tree mst configuration

**命令：spanning-tree mst configuration**

**no spanning-tree mst configuration**

**功能：**进入交换机的 MST 配置模式，在交换机的 MST 配置模式下，可配置交换机有关 MSTP 域的参数；本命令的 no 操作为恢复交换机的 MSTP 域参数的缺省值。

**命令模式：**全局配置模式。

**缺省情况：**用户在没有进入 MST 配置模式之前，MSTP 域的参数缺省如下：

| MSTP 域参数 | 参数缺省值 |
|---|---|
| Instance | 只有实例 0 存在，且 VLAN1~4094 均映射在实例 0 |
| Name | 取本交换机网桥 MAC |
| Revision | 0 |

**使用指南：**无论交换机是否启动了 MSTP 协议，都可以进入 MSTP 域配置模式，并在配置后保存当前配置。当交换机运行 MSTP 模式时，系统会根据配置的 MSTP 域参数计算出本交换机的 MST 配置标识（MST Configuration Identifier），只有 MSTP 域配置标识相同的交换机才会认为是在同一个 MSTP 域中，且能进行 MSTI 的计算。

**举例：**进入交换机的 MST 配置模式。

Switch(config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#

## 8.1.1.21 spanning-tree mst cost

**命令：spanning-tree mst *<instance-id>* cost *<cost>***

**no spanning-tree mst <instance-id> cost**

**功能：设置当前以太网端口在指定实例的端口路径代价；本命令的 no 操作为恢复缺省值。**

**参数：*<instance-id>***为指定实例的实例 ID，取值范围为 0~64；***<cost>***为路径代价值，取值范围为 1~200,000,000。

**命令模式：端口配置模式。**

**缺省情况：缺省情况下，端口的路径代价与端口的带宽相关。**

| 端口类型 | 缺省路径开销 | 建议取值范围 |
|---|---|---|
| 10Mbps | 2000000 | 2000000~20000000 |
| 100Mbps | 200000 | 200000~2000000 |
| 1Gbps | 20000 | 20000~200000 |
| 10Gbps | 2000 | 2000~20000 |

对汇聚端口，端口缺省路径代价如下：

| 端口类型 | 汇聚端口个数（在允许汇聚的个数范围内） | 缺省路径开销 |
|---|---|---|
| 10Mbps | N | 2000000/N |
| 100Mbps | N | 200000/N |
| 1Gbps | N | 20000/N |
| 10Gbps | N | 2000/N |

**使用指南：通过配置端口路径代价可以控制该实例端口到根网桥的根路径代价，从而控制该实例根端口、指定端口等的选举。**

**举例：在端口 1/1/2** 上设置实例 2 对应的 MSTP 端口路径代价为 3000000。

Switch(Config-If-Ethernet1/1/2)#spanning-tree mst 2 cost 3000000

## 8.1.1.22 spanning-tree cost-format

本型号交换机不支持此命令。

## 8.1.1.23 spanning-tree mst loopguard

**命令：spanning-tree [mst <instance-id>] loopguard**

**no spanning-tree [mst <instance-id>] loopguard**

**功能：**配置 spanning-tree 的指定实例上启动 loopguard 功能，本命令的 no 操作恢复为不在该实例下启动该功能。

**参数：**<instance-id>：MSTP 实例 ID。

**缺省：**不启动 loopguard 功能。

**命令模式：**端口模式

**使用指南：**通过配置该命令，可以避免单向链路失效导致 root 端口或 alternate 端口变成 designated 端口；在端口收包定时器到时时将配置了 loopguard 的端口置为 Block 状态。

**举例：**配置实例 0 的端口 1/1/2 为 loopguard 模式。

Switch(Config)#interface ethernet 1/1/2

Switch(Config-Ethernet-1/1/2)#spanning-tree mst 0 loopguard

Switch(Config-Ethernet-1/1/2)#

## 8.1.1.24 spanning-tree mst port-priority

**命令：spanning-tree mst *<instance-id>* port-priority *<port-priority>***

**no spanning-tree mst *<instance-id>* port-priority**

**功能：**设置当前端口在指定实例的优先级值；本命令的 no 操作为恢复缺省端口的优先级值。

**参数：*<instance-id>***为指定实例的实例 ID，取值范围为 0~64；***<port-priority>***为端口优先级值，取值范围为 0~240 之间的 16 倍数，即取值范围为 0、16、32、48…240。

**命令模式：**端口配置模式。

**缺省情况：**端口缺省优先级值为 128。

**使用指南：**通过配置端口优先级可以控制指定实例的端口 ID，进而影响该实例的根端口、指定端口等选举。端口优先级值越小，优先级越高。

**举例：**在端口 1/1/2 设置实例 1 的端口优先级为 32。

Switch(config)#interface ethernet 1/1/2

Switch(Config-If-Ethernet1/1/2)#spanning-tree mst 1 port-priority 32

## 8.1.1.25 spanning-tree mst priority

**命令：spanning-tree mst *<instance-id>* priority *<bridge-priority>***

**no spanning-tree mst *<instance-id>* priority**

**功能：**设置交换机在指定实例的网桥优先级；本命令的 no 操作为恢复交换机在指定实例的缺省优先级值。

**参数：*<instance-id>***为指定实例的实例 ID，取值范围为 0~64；***<bridge-priority>***为交换机的优先级，取值范围为 0~61440 之间的 4096 的倍数，即取值范围为 0、4096、8192…61440。

**命令模式：**全局配置模式。

**缺省情况：**交换机缺省的优先级为 32768。

**使用指南：**通过配置交换机网桥优先级可以改变指定实例的网桥 ID，进而用于该实例的根网桥、指定端口等选举。交换机网桥优先级值越小，优先级越高。

**举例：**配置交换机实例 2 的优先级为 4096。

Switch(config)#spanning-tree mst 2 priority 4096

## 8.1.1.26 spanning-tree mst rootguard

**命令： spanning-tree mst <instance-id> rootguard**

**no spanning-tree mst <instance-id> rootguard**

**功能：**配置 spanning-tree 的指定实例上启动 rootguard 功能，本命令的 no 操作恢复为不在该实例下启动该功能。

**参数：**<instance-id>：MSTP 实例 ID。

**命令模式：**端口模式。

**缺省情况：**不启动 rootguard 功能。

**使用指南：**根保护功能是基于端口配置的，不允许端口成为 mstp 的根端口，也就是说端口要始终保持在指定端口状态。如果在配置了 root guard 的端口接收到了更优的 bpdu 报文，根保护功能会把该端口设置为 root_inconsistent(blocked)状态，而不是根据该 bpdu 重新计算，选择出一个新的根端口。当交换机不再接收更优的 bpdu 报文，该端口就不会再阻塞，根据生成树协议，端口状态从 discarding，learning，最后转变到 forwarding 状态。恢复是自动的，不需要人为干预。通过 root guard 功能，能够很好的保护二层网络的拓扑结构，不会因为其它设备的加入而改变根网桥，从而不会改变现有网络用户数据所走的链路。

**举例：**配置 spanning-tree 的实例 0 启动 rootguard 功能。

Switch(config)#interface ethernet 1/1/2

Switch(Config-If-Ethernet1/1/2)#spanning-tree mst 0 rootguard

Switch(Config-If-Ethernet1/1/2)#

## 8.1.1.27 spanning-tree portfast

**命令：spanning-tree portfast [bpdufilter | bpduguard] [recovery <30-3600>]**

**no spanning-tree portfast**

**功能：**配置端口为边缘端口，并指定模式 BPDU filter、BPDU guard 或缺省模式（协议规定的模式，即收到 BPDU 报文后转为非边缘端口）。本命令的 no 操作配置端口为非边缘端口。

**参数：bpdufilter**：配置边缘端口模式为 BPDU filter

**bpduguard**：配置边缘端口模式为 BPDU guard

**recovery**：配置边缘端口执行**bpduguard**违背操作后可以自动恢复

**<30-3600>**：恢复时间，默认不进行恢复

**命令模式：**端口模式。

**缺省情况：**非边缘端口。

**使用指南：**对于边缘端口可以在变为指定端口时直接进入转发态，而对于边缘端口可以有三种模式，缺省模式下边缘端口收到 BPDU 后会转为非边缘端口。BPDU filter 模式下收到 BPDU 会丢弃该报文不处理，BPDU guard 模式下收到 BPDU 会丢弃报文并关闭端口。同时只能有一种模式。no 命令将端口恢复为非边缘端口。

**举例：**配置边缘端口模式为 BPDU guard，恢复时间为 60s。

Switch(config)#interface ethernet 1/1/2

Switch(Config-If-Ethernet1/1/2)#spanning-tree portfast bpduguard recovery 60

Switch(Config-If-Ethernet1/1/2)#

## 8.1.1.28 spanning-tree port-priority

**命令：spanning-tree port-priority *<port-priority>***

**no spanning-tree port-priority**

**功能：** 配置端口的优先级。本命令的 no 操作为恢复缺省端口的优先级值。

**参数：** ***<port-priority>*** 为端口优先级值，取值范围为 0~240 之间的 16 倍数，即取值范围为 0、16、32、48…240。

**命令模式：** 端口模式。

**缺省情况：** 交换机缺省的优先级为 32768。

**使用指南：** 配置端口的优先级，可以用于端口的选举。优先级值越小，优先级越高。

**举例：** 配置端口 1 的优先级为 240。

Switch(config-If-Ethernet1/1/1)#spanning-tree port-priority 240

## 8.1.1.29 spanning-tree priority

**命令：spanning-tree priority *<bridge-priority>***

**no spanning-tree priority**

**功能：**设置交换机的网桥优先级；本命令的 no 操作为恢复交换机的缺省优先级值。

**参数：*<bridge-priority>***为交换机的优先级，取值范围为 0~61440 之间的 4096 的倍数，即取值范围为 0、4096、8192…61440。

**命令模式：**全局配置模式。

**缺省情况：**交换机缺省的优先级为 32768。

**使用指南：**通过配置交换机网桥优先级可以改变网桥 ID，进而用于根网桥、指定端口等选举。交换机网桥优先级值越小，优先级越高。

**举例：**配置交换机的优先级为 4096。

Switch(config)#spanning-tree priority 4096

## 8.1.1.30 spanning-tree rootguard

**命令：spanning-tree rootguard**

**no spanning-tree rootguard**

**功能：** 设置端口为根端口。本命令的 no 操作为设置端口为非根端口。

**参数：** 无。

**命令模式：** 端口模式。

**缺省情况：** 端口为非根端口。

**使用指南：** 根保护功能是基于端口配置的，不允许端口成为 mstp 的根端口，也就是说端口要始终保持在指定端口状态。如果在配置了 root guard 的端口接收到了更优的 bpdu 报文，根保护功能会把该端口设置为 root_inconsistent(blocked)状态，而不是根据该 bpdu 重新计算，选择出一个新的根端口。当交换机不再接收更优的 bpdu 报文，该端口就不会再阻塞，根据生成树协议，端口状态从 discarding，learning，最后转变到 forwarding 状态。恢复是自动的，不需要人为干预。通过 root guard 功能，能够很好的保护二层网络的拓扑结构，不会因为其它设备的加入而改变根网桥，从而不会改变现有网络用户数据所走的链路。

**举例：** 配置端口 1 为根端口。

Switch(config-If-Ethernet1/1/1)#spanning-tree rootguard

## 8.1.1.31 spanning-tree tcflush (全局模式)

**命令：spanning-tree tcflush {enable | disable | protect}**

**no spanning-tree tcflush**

**功能：**配置全局处理拓扑改变导致的 FLUSH 的方式，其 no 形式恢复为默认的模式。

**参数：**enable：表示标准的每次 TC 都 FLUSH 的模式。

disable：表示对 TC 不做 FLUSH 处理。

protect：表示限制 TC 进行 FLUSH 的次数。

**命令模式：**全局配置模式。

**缺省情况：**enable。

**使用指南：**按协议要求，拓扑改变传播时，传播的端口应当清除 MAC/ARP 表（FLUSH），但在实际环境中，有时用户的网络比较单纯，不需要也不希望每次拓扑改变都清除 MAC/ARP 表，同时要考虑可能有拓扑改变攻击的情况，因此，我们允许用户通过配置决定拓扑改变传播时的行为。默认使用遵守协议的行为，可以配置为不 FLUSH 或每 10 秒最多一次 FLUSH。注意：如果网络环境比较复杂，特别是用户可能从生成树的一个支路快速转移到另一支路的情况，不要使用 DISABLE 的方式。全局的配置对所有没有单独配置的端口生效。

**举例：**配置全局处理拓扑改变导致的 FLUSH 的方式为对 TC 不做 FLUSH 处理。

```
Switch(config)#spanning-tree tcflush disable
Switch(config)#
```

## 8.1.1.32 spanning-tree tcflush (端口模式)

**命令：spanning-tree tcflush {enable | disable | protect}**

**no spanning-tree tcflush**

**功能：**配置端口处理拓扑改变导致的 FLUSH 的方式，其 no 形式恢复为默认的模式。

**参数：**enable：表示标准的每次 TC 都 FLUSH 的模式。

disable：表示对 TC 不做 FLUSH 处理。

protect：表示限制 TC 进行 FLUSH 的次数。

**命令模式：**端口配置模式。

**缺省情况：**使用全局的模式。

**使用指南：**按协议要求，拓扑改变传播时，传播的端口应当清除 MAC/ARP 表（FLUSH），但在实际环境中，有时用户的网络比较单纯，不需要也不希望每次拓扑改变都清除 MAC/ARP 表，同时要考虑可能有拓扑改变攻击的情况，因此，我们允许用户通过配置决定拓扑改变传播时的行为。默认使用遵守协议的行为，可以配置为不 FLUSH 或每 10 秒最多一次 FLUSH。注意：如果网络环境比较复杂，特别是用户可能从生成树的一个支路快速转移到另一支路的情况，不要使用 DISABLE 的方式。

**举例：**配置端口处理拓扑改变导致的 FLUSH 的方式为对 TC 不做 FLUSH 处理。

```
Switch(config)#interface ethernet 1/1/2
Switch(Config-If-Ethernet1/1/2)#spanning-tree tcflush disable
Switch(Config-If-Ethernet1/1/2)#
```

## 8.1.1.33 spanning-tree transmit-hold-count

**命令：spanning-tree transmit-hold-count <tx-hold-count-value>**

**no spanning-tree transmit-hold-count**

**功能：**设置端口的最大发送速率。

**参数：**tx-hold-count-value：取值范围是 1-20，默认值是 10。

**命令模式：**全局配置模式。

**缺省情况：**默认值是 10。

**使用指南：**在每一个 Hello Time 时间间隔内可以发送的最大 BPDU 数，用于控制 BPDU 的流量。该变量值应用于整个 MST 网桥。

**举例：**设置最大发送速率为 20。

Switch(config)#spanning-tree transmit-hold-count 20

## 8.1.2 监测和调试

### 8.1.2.1 debug spanning-tree

**命令：debug spanning-tree**

**no debug spanning-tree**

**功能：**打开 MSTP 的调试信息；本命令的 no 操作为关闭 MSTP 调试信息。

**命令模式：**特权模式。

**使用指南：**该命令是 MSTP 庞大复杂 debug 功能的总开关，逐级打开需要 debug 的相应信息开关后再打开此总开关就能够输出 debug 打印信息了。各级 debug 开关的功能包括：查看 MSTP 协议运行中 bpdu 报文的发送接收、事件的处理、状态机、计时器等等。一般情况下，这些调试信息是给技术人员调试使用，用户不需要关注。

**举例：**打开端口 1/1/1 接收 BPDU 报文的 debug 信息。

Switch#debug spanning-tree

Switch#debug spanning-tree bpdu rx interface e1/1/1

### 8.1.2.2 show mst-pending

**命令：show mst-pending**

**功能：**在 MSTP 域配置模式下显示当前配置的 MSTP 域的参数配置情况。

**命令模式：**特权和配置模式。

**使用指南：**在 MSTP 域配置模式下，输入本命令可以查看 MSTP 域当前的配置参数，如 MSTP 域名字、修正数值、VLAN 和 Instance 的映射情况。

注意：在退出 MSTP 域配置模式之前，该命令显示的参数配置情况可能尚未生效。

**举例：**显示交换机的 MSTP 域当前的参数配置情况。

Switch(config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#show mst-pending

Name switch

Revision 0

Instance Vlans Mapped

---

00 1-29, 31-39, 41-4093

03 30

04 40

05 4094

---

Switch(Config-Mstp-Region)#

## 8.1.2.3 show spanning-tree

**命令：show spanning-tree [mst [*<instance-id>*]] [interface *<interface-list>*] [detail]**

**功能：**显示 MSTP 协议及各实例信息。

**参数：*<interface-list>***为端口列表；***<instance-id>***为实例的值，范围为 0-64； ***<interface-list>*** 为端口列表；**detail** 为显示详细的 spanning-tree 信息。

**命令模式：**特权和配置模式。

**使用指南：**通过 show spanning-tree 命令可以查看该网桥及各实例的 MSTP 信息，域配置信息以及端口的 MSTP 信息等。

**举例：**显示网桥 MSTP 信息，显示信息内容如下表所示。

Switch#sh spanning-tree

-- MSTP Bridge Config Info --

Standard : IEEE 802.1s

Bridge MAC : 00:03:0f:01:0e:30

Bridge Times : Max Age 20, Hello Time 2, Forward Delay 15

Force Version: 3

############################## Instance 0 ##############################

Self Bridge Id : 32768 - 00:03:0f:01:0e:30

Root Id : 16384.00:03:0f:01:0f:52

Ext.RootPathCost : 200000

Region Root Id : this switch

Int.RootPathCost : 0

Root Port ID : 128.1

Current port list in Instance 0:

Ethernet1/1/1 Ethernet1/1/2 (Total 2)

| PortName | ID | ExtRPC | IntRPC | State | Role | DsgBridge | DsgPort |
|---|---|---|---|---|---|---|---|

```
-------------- ------- --------- --------- --- ---- ------------------ -------
 Ethernet1/1/1    128.001              0             0 FWD ROOT 16384.00030f010f52 128.007
 Ethernet1/1/2    128.002              0             0 BLK ALTR 16384.00030f010f52 128.011

############################## Instance 3 ##############################
Self Bridge Id      : 0.00:03:0f:01:0e:30
Region Root Id      : this switch
Int.RootPathCost : 0
Root Port ID        : 0
Current port list in Instance 3:
Ethernet1/1/1 Ethernet1/1/2 (Total 2)

   PortName          ID       IntRPC     State Role        DsgBridge        DsgPort
-------------- ------- --------- --- ---- ------------------ -------
 Ethernet1/1/1    128.001              0 FWD MSTR        0.00030f010e30 128.001
 Ethernet1/1/2    128.002              0 BLK ALTR        0.00030f010e30 128.002

############################## Instance 4 ##############################
Self Bridge Id      : 32768.00:03:0f:01:0e:30
Region Root Id      : this switch
Int.RootPathCost : 0
Root Port ID        : 0
Current port list in Instance 4:
Ethernet1/1/1 Ethernet1/1/2 (Total 2)

   PortName          ID       IntRPC     State Role        DsgBridge        DsgPort
-------------- ------- --------- --- ---- ------------------ -------
 Ethernet1/1/1 128.001              0 FWD MSTR 32768.00030f010e30 128.001
 Ethernet1/1/2 128.002              0 BLK ALTR 32768.00030f010e30 128.002
```

| 显示内容 | 解释 |
|---|---|
| **网桥信息** | |
| Standard | STP 版本 |
| Bridge MAC | 代表本网桥的 MAC |
| Bridge Times | 本网桥 Max Age，Hello Time 及 Forward Delay 的配置值 |
| Force Version | 当前运行 stp 协议的 Version 值 |
| **实例信息** | |
| Self Bridge Id | 该实例对应的本网桥优先级及 MAC |

| | |
|---|---|
| Root Id | 该实例对应的根网桥优先级及 MAC |
| Ext.RootPathCost | 网桥到整个网络总根的路径代价 |
| Int.RootPathCost | 网桥到该实例域根的路径代价 |
| Root Port ID | 网桥上该实例的根端口 |
| **该实例上 MSTP 协议生效的端口列表** | |
| PortName | 端口名字 |
| ID | 端口优先级及端口 index 索引值 |
| ExtRPC | 端口到整个网络总根的路径代价 |
| IntRPC | 端口到该实例域根的路径代价 |
| State | 该实例对应的端口状态 |
| Role | 该实例对应的端口角色 |
| DsgBridge | 该实例端口对应的上游指定网桥 |
| DsgPort | 该实例端口对应的上游指定端口 |

### 8.1.2.4 show spanning-tree mst config

**命令：show spanning-tree mst config**

**功能：**在特权模式下显示生效的 MSTP 域的参数配置情况。

**命令模式：**特权和配置模式。

**使用指南：**在特权配置模式下，输入本命令可以查看 MSTP 域生效的当前参数，如 MSTP 域名、修正数值、VLAN 和 Instance 的映射情况。

**举例：**显示交换机的 MSTP 域的配置情况。

```
Switch#show spanning-tree mst config

Name        switch
Revision    0
Instance    Vlans Mapped
-----------------------------------
00          1-29, 31-39, 41-4094
03          30
04          40
-----------------------------------
```

## 8.1.3 MSTP 多线程

### 8.1.3.1 spanning-tree process

**命令：spanning-tree process <process-id>**

**no spanning-tree process <process-id>**

**功能：**创建新的 mstp 线程。

**参数：**process-id：取值范围是 1-31。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**创建新的 mstp 线程，一台设备可配置多个 mstp 线程，各线程相互独立，互不影响；默认设备只存在线程 0。

**举例：**创建 mstp 线程 1。

Switch(config)#spanning-tree process 1

## 8.1.3.2 spanning-tree tc-notify process0

**命令：spanning-tree tc-notify process0**

**no spanning-tree tc-notify process0**

**功能：**线程 N 将 tc 通告给 mstp 线程 0 中的实例。

**参数：**无。

**命令模式：**mstp 线程配置模式。

**缺省情况：**无。

**使用指南：**mstp 线程 N 中有拓扑变化时，设备会收到 tc 报文，同时，在共享链路上，线程 N 需将 tc 通告给 mstp 线程 0 中的实例，使得线程 0 也刷新相关表项，以保证数据流量不中断。

**举例：**配置线程 1 的 TC 通告通知线程 0。

Switch(Config-Mstp-Process-1)#spanning-tree tc-notify process0

## 8.1.3.3 spanning-tree binding-process

**命令：spanning-tree binding-process <process-id>**

**no spanning-tree binding-process <process-id>**

**功能：**把端口加入到线程 N。

**参数：**process-id：取值范围是 1-31。

**命令模式：**端口配置模式。

**缺省情况：**所有端口都属于线程 0。

**使用指南：**配置端口加入指定 mstp 线程 N，此时端口从原来的线程 0 进入线程 N。本命令与设置共享端口命令（link-share）互斥。

**举例：**将端口 1/1/2 加入线程 1。

switch(config-if-ethernet1/1/2)#spanning-tree binding-process 1

#### 8.1.3.4 spanning-tree binding-process link-share

**命令：spanning-tree binding-process < process-id > link-share**

**no spanning-tree binding-process < process-id > link-share**

**功能：**设置端口属于线程 N 的共享端口。

**参数：**process-id：取值范围是 1-31。

**命令模式：**端口配置模式。

**缺省情况：**端口只参与线程 0 的 mstp 计算。

**使用指南：**设置端口属于线程 N 的共享端口。除线程 0 外，配置端口还可以参与多个 mstp 线程的计算，但端口状态只由线程 0 设置。本命令可多次配置。

**举例：**将端口 1/1/2 设置为线程 1 和 0 的共享端口

switch(config-if-ethernet1/1/2)#spanning-tree binding-process 1 link-share

## 8.2 VRRP

### 8.2.1 advertisement-interval

**命令：advertisement-interval *<adver_interval>***

**功能：**配置 VRRP 定时器时间值。

**参数：*<adver_interval>***发送 VRRP 报文的间隔时间，单位为秒，取值范围为 1~10。

**缺省情况：*<adver_interval>***缺省值为 1 秒。

**命令模式：**VRRP 协议配置模式。

**使用指南：**每隔一段时间，VRRP 备份组中的 Master 都会发送 VRRP 报文来向组内的路由器（或三层以太网交换机）通知自己工作正常，这个间隔时间就是 *adver_interval*。如果 Backup 超过一定时间（时长为 *master_down_interval*）没有收到 Master 发送来的 VRRP 报文，则认为它已经无法正常工作，并将自己的状态转变为 Master。

用户可以使用此命令来调整 Master 发送 VRRP 报文的间隔时间。对于同一备份组的成员，该属性应该设置为相同的数值。对于 Backup 来说，其 *master_down_interval* 的取值是 *adver_interva*l 的 3 倍。如果网络流量过大或者不同的路由器（或三层以太网交换机）上的定时器差异等因素，会导致 *master_down_interval* 超时并随即引发状态转换。对于这种情况，可以通过将 *adver_interval* 的间隔时间延长和设置较长抢占延迟时间的办法来解决。

**举例：**配置 VRRP 定时器时间值为 3 秒。

Switch(config-router)# advertisement-interval 3

### 8.2.2 circuit-failover

**命令：circuit-failover {IFNAME | Vlan <ID>} <value_reduced>**

**no circuit-failover**

**功能：**配置 VRRP 监控接口。

**参数：< *IFNAME* >**被监视的三层接口名。

**<*value_reduced*>**优先级降低的数额，取值范围为 1~253。

**缺省情况：** 缺省为不配置。

**命令模式：** VRRP 协议配置模式。

**使用指南：** 对接口的监视功能是对备份功能的一个很好的扩展，该扩展功能不仅在路由器（或三层以太网交换机）出现故障时，VRRP 能够提供备份功能；而且在某网络接口的状态为 **down** 时，也能够实现通过降低当前路由器（或三层以太网交换机）的优先级以保证备份功能的顺利实施。

使用此命令后，如果被监视接口的状态由 **up** 转为 **down**，则当前路由器（或三层以太网交换机）接口在所属备份组内的优先级就会降低所配置的优先级值，以防止当 Master 出现故障时，Backup 端口由于优先级低于 Master 而无法实现转换。如果 value_reduced 大于接口配置的 priority，则当相应的接口 down 后，接口在所属备份组内的优先级会降低为 0。

**举例：**配置 VRRP 监控接口为 vlan 2，优先级降低的数额为 10。

Switch(config-router)# circuit-failover vlan 2 10

## 8.2.3 debug vrrp

**命令：debug vrrp [ all | events | packet [recv| send] ]**

**no debug vrrp [ all | events | packet [recv| send] ]**

**功能：**显示 VRRP 备份组的状态变化和收发报文的情况，该命令的 no 形式关闭 DEBUG 显示。

**缺省情况：**缺省调试开关是关闭的。

**命令模式：**特权用户配置模式。

**举例：**

Switch#debug vrrp

2001/11/11 00:50:28 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]

2001/11/11 00:50:30 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]

2001/11/11 00:50:31 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]

2001/11/11 00:50:32 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]

2001/11/11 00:50:33 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[10.1.1.1]

## 8.2.4 disable

**命令：disable**

**功能：**关闭 VRRP 协议。

**参数：**无。

**缺省情况：**缺省为不配置。

**命令模式：**VRRP 协议配置模式。

**使用指南：**关闭相应的虚拟路由器，只有在关闭 VRRP 之后才能修改 VRRP 的配置。

**举例：**关闭配置序号为 10 的虚拟路由器。

Switch(config)#router vrrp 10

Switch(config-router)#disable

## 8.2.5 enable

**命令：enable**

**功能：**启动 VRRP 协议。

**参数：**无。

**缺省情况：**缺省为不配置。

**命令模式：**VRRP 协议配置模式。

**使用指南：**启动相应的虚拟路由器，只有通过 enable 启动的路由器（或三层以太网交换机）接口才真正加入备份组中，在启动虚拟路由器之前必须配置 VRRP 虚拟 IP 和接口，且相应的接口上也配置有 IP 地址。

**举例：**启动配置序号为 10 的虚拟路由器。

Switch(config)#router vrrp 10

Switch(config-router)#enable

## 8.2.6 interface

**命令：interface {*IFNAME* | Vlan <*ID*>}**

**no interface**

**功能：**配置 VRRP 的接口。

**参数：*IFNAME*：**接口名称，如“VLAN1”。

**Vlan <*ID*>：**VLAN 的 ID 号 。

**缺省情况：**缺省为不配置。

**命令模式：**VRRP 协议配置模式。

**使用指南：**本命令用向一个已存在的备份组中添加三层接口，本命令的 **no** 形式用来删除指定的备份组的三层接口。

**举例：**将接口 interface vlan 1 添加到 10 号备份组中。

Switch(config)# router vrrp 10

Switch(config-router)#interface vlan 1

## 8.2.7 preempt-mode

**命令：preempt-mode {true | false}**

**功能：**配置 VRRP 的抢占模式。

**参数：**无。

**命令模式：**VRRP 协议配置模式。

**缺省情况：**缺省为抢占模式。

**使用指南：**如果需要高优先级的路由器（或三层以太网交换机）能主动抢占成为活动路由器（或三层以太网交换机），则要设置抢占模式。

**举例：**配置 VRRP 为非抢占模式。

Switch(config-router)#preempt-mode false

## 8.2.8 priority

**命令：priority <*value*>**

**功能：**配置 VRRP 优先级。

**参数：<*value*>**为优先级，取值范围为 1～254。

**缺省情况：backup** 路由器（或三层以太网交换机）在所有备份组内的优先级均为 100。

**命令模式：**VRRP 协议配置模式。

**使用指南：**优先级决定路由器（或三层以太网交换机）在备份组中的地位，优先级越高就越有可能成为 Master。当某备份组内有两台及两台以上路由器（或三层以太网交换机）的优先级取值相同时，VLAN 接口 IP 地址最大的路由器（或三层以太网交换机）将成为 Master。优先级的值越大，优先级越高。

**举例：**配置 VRRP 优先级为 150。

Switch(config-router)#priority 150

## 8.2.9 router vrrp

**命令：router vrrp <*vrid*>**

**no router vrrp <*vrid*>**

**功能：**创建/删除虚拟路由器。

**参数：< *vrid* >**为虚拟路由器序号，取值范围为 1～255。

**缺省情况：**缺省为不配置。

**命令模式：**全局配置模式。

**使用指南：**该命令用于创建或删除虚拟路由器，虚拟路由器通过虚拟路由器序号唯一确定，只有创建了特定的虚拟路由器后，才能对该虚拟路由器进行相关配置。出于稳定性考虑，可配置的虚拟路由器个数最多为 192 个。

**举例：**配置序号为 10 的虚拟路由器。

Switch(config)#router vrrp 10

## 8.2.10 show vrrp

**命令：show vrrp [<*vrid*>]**

**功能：**显示 VRRP 备份组的状态和配置信息。

**参数：*< vrid >***为虚拟路由器序号，取值范围为 1～255。

**命令模式：**特权和配置模式。

**使用指南：**该命令用于显示虚拟路由器的配置和当前的状态。如果没有指定虚拟路由器序号，则显示所有的虚拟路由器的信息。

**举例：**

```
Switch#show vrrp
VrId <1>
  State is Master
  Virtual IP is 10.1.1.1 (Not IP owner)
  Interface is Vlan1
  Priority not configured, Current priority is 254
  Advertisement interval is 1 sec
  Preempt mode is TRUE
  Circuit failover interface Vlan1, Priority Delta 1, Status UP
VrId <10>
  State is Initialize
  Virtual IP is 1.1.1.1 (Not IP owner)
  Interface is unset
  Priority is unset
  Advertisement interval is unset
  Preempt mode is TRUE
Switch#
```

| 显示信息 | 解释 |
|---|---|
| State | 状态。 |
| Virtual IP | 虚拟 IP 地址。 |
| Interface | 接口名称。 |
| priority | 优先级。 |
| Advertisement interval | 定时器的周期时间。 |
| Preempt | 抢占模式。 |
| Circuit failover interface | 监控接口信息。 |

## 8.2.11 virtual-ip

**命令：virtual-ip <*A.B.C.D*>**

**no virtual-ip**

**功能：**配置 VRRP 的虚拟 IP。

**参数：*<A.B.C.D>***虚拟 IP 地址，为点分十进制格式。

**缺省情况：**缺省为不配置。

**命令模式：**VRRP 协议配置模式。

**使用指南：**本命令向一个已存在的备份组中添加虚拟 IP 地址，本命令的 **no** 形式用来删除指定备份组的虚拟 IP 地址。同一备份组只有一个虚拟 IP。 VRRP 优先级为 255(不用配置)，虚拟 IP 应当与接口 IP 在同一网段内。

**特别提示：**当从 5.2.0.0(含)以前的版本升级到新版本，如果原来配置有 VRRP 命令，其配置恢复将不能成功。首先通过 no router vrrp <vrid>来删除相关 VRRP，然后重新配置。否则将出现任务挂起等异常现象。

**举例：**配置虚拟 IP 地址为 10.1.1.1。

Switch(config-router)#virtual-ip 10.1.1.1

## 8.2.12 vrrp track

**命令：vrrp track interface {ethernet IFNAME|IFNAME} priority <priority_value>**

**no vrrp track interface {ethernet IFNAME|IFNAME}**

**功能：**配置 VRRP 会话监控端口的状态。

**参数：**interface {ethernet IFNAME|IFNAME}：端口名字。

<priority_value>：优先级，可配置范围是 1~254。

**命令模式：**VRRP 协议配置模式。

**缺省模式：**不监控端口的状态。

**使用指南：**VRRP 会话监控端口的状态，当端口的状态为 DOWN 时，改变本地 VRRP 的优先级为配置的值，以达到改变 VRRP 会话状态的目的，例如当本地 VRRP 的优先级小于对端的优先级时，本地 VRRP 的状态应该为 BACKUP。

**举例：**

Switch(config)#router vrrp 1

switch(config-router)#vrrp track interface ethernet 1/1/2 priority 1

# 8.3 MRPP

## 8.3.1 control-vlan

**命令：control-vlan *<vid>***

**no control-vlan**

**功能：**设置 MRPP 环的控制 VLAN 的 ID，本命令的 no 操作删除配置的控制 VLAN 的 ID。

**参数：*<vid>***为控制 VLAN 的 ID，取值范围为 1~4094。

**命令模式：**MRPP 环配 j 置模式

**缺省情况：**缺省没有配置。

**使用指南：**本命令指定 MRPP 环的虚拟 VLAN 的 ID，目前可以为 1-4094 内的任何值。但是为了不引起混淆，该 ID 最好为没有配置过的 V LAN ID，而且最好同 MRPP 环的 ID 一致。在属于同一个 MRPP 环的交换机的 MRPP 环的配置中，控制 VLAN 的 ID 必须相同，否则整个 MRPP 环路可能会无法正常工作或者形成广播风暴。

在使用该命令之前，mrpp enable 命令必须启动。此命令后，若 primary port、secondary port、node-mode 和 enable 命令都已配置，则 mrpp 环功能启用。

**举例：**配置 mrpp ring 4000 的控制 VLAN 为 4000。

```
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
```

## 8.3.2 clear mrpp statistics

**命令：clear mrpp statistics [*<ring-id>*]**

**功能：**清除 MRPP 环的接收和发送 MRPP 数据包的统计信息。

**参数：*<ring-id>***为 MRPP 环 ID，取值范围为<1-4096>，如果不指定 ID,则清除所有的 MRPP 环的统计信息。

**命令模式：**特权模式

**缺省情况：**无。

**使用指南：**无。

**举例：**清除交换机上的 MRPP 环 4000 的统计信息。

```
Switch#clear mrpp statistics 4000
```

## 8.3.3 debug mrpp

**命令：debug mrpp**

**no debug mrpp**

**功能：**打开 MRPP 的调试信息；本命令的 no 操作为关闭 MRPP 的调试信息。

**命令模式：**特权配置模式

**参数：**无。

**使用指南：**打开 MRPP 调试信息，可以查看 MRPP 协议的消息处理以及接收数据包过程，在遇到故障时有助于监测故障原因。

**举例：**打开 MRPP 协议的调试信息。

```
Switch#debug mrpp
```

## 8.3.4 enable

**命令：enable**

**no enable**

**功能：**使能配置的 MRPP 环，本命令的 no 操作关闭该使能的 MRPP 环。

**参数：**无。

**命令模式：**MRPP 环配置模式

**缺省情况：**缺省不使能 MRPP 环。

**使用指南：**在执行该命令时，必须已经启动 MRPP 协议。此命令执行后，若其它配置命令都已完成，则 mrpp 环使能。

**举例：**配置交换机上的 MRPP 环 4000 为主节点，并使能该 MRPP 环。

Switch(config)#mrpp enable

Switch(config)#mrpp ring 4000

Switch(mrpp-ring-4000)#control-vlan 4000

Switch(mrpp-ring-4000)# node-mode master

Switch(mrpp-ring-4000)#fail-timer 18

Switch(mrpp-ring-4000)#hello-timer 6

Switch(mrpp-ring-4000)#enable

Switch(mrpp-ring-4000)#exit

Switch(config)#in ethernet 1/1/1

Switch(config-If-Ethernet1/1/1)#mrpp ring 4000 primary-port

Switch(config)#in ethernet 1/1/3

Switch(config-If-Ethernet1/1/3)#mrpp ring 4000 secondary-port

## 8.3.5 errp domain

**命令：errp domain <*domain-id*>**

**no errp domain <*domain-id*>**

**功能：** 创建 ERRP 域，本命令的 no 操作删除已经配置的 ERRP 域。

**参数：<*domain-id*>** 为 ERRP 域 ID，取值范围为<1-15>。

**缺省情况：** 不创建 ERRP 域。

**命令模式：** 全局配置模式

**使用指南：** 如果需要配置 ERRP 域 ID，需要先使能 ERRP 的兼容模式。在执行该命令时，如果没有创建过该 ERRP 域，则创建新的 ERRP 域。在执行本命令的 no 操作时，则删除相应的 ERRP 域 ID。

**举例：** 全局配置 ERRP 的域 ID。

Switch(Config)#errp domain 1

## 8.3.6 fail-timer

**命令：fail-timer *<timer>***

**no fail-timer**

**功能：**设置 MRPP 环的主节点判断是否接收到 Hello 报文的定时器间隔，本命令的 no 操作恢复缺省的定时器间隔。

**参数：*<timer>***取值范围为 1~300 秒。

**命令模式：**MRPP 环配置模式

**缺省情况：**缺省设置定时器间隔为 3 秒。

**使用指南：**如果 MRPP 环的主节点在配置的 fail 定时器值的范围内没有接收到主节点主端口发送的 Hello 报文，则说明整个环路出现故障。MRPP 环的传输节点不需要该定时器，可以不用配置。为防止传输节点转发 Hello 报文的延迟，fail 定时器的值必须大于或等于 Hello 定时器值的 3 倍。在延迟大的环路上，为了防止由于延迟导致主节点无法在 fail 定时器值的范围内接收到 Hello 报文，需要修改该缺省配置，适当增大该值。

**举例：**配置 MRPP 环 4000 的 fail-timer 为 10 秒。

```
Switch(config)#mrpp ring 4000
Switch(mrpp-ring-4000)#fail-timer 10
```

## 8.3.7 hello-timer

**命令：hello-timer *<timer>***

**no hello-timer**

**功能：**设置 MRPP 环的主节点的发送 Hello 报文的定时器间隔，本命令的 no 操作恢复缺省的定时器间隔。

**参数：*<timer>***取值范围为 1~100 秒。

**命令模式：**MRPP 环配置模式

**缺省情况：**缺省设置定时器间隔为 1 秒。

**使用指南：**MRPP 环的主节点在配置的 Hello 定时器的间隔内不断发送 Hello 报文，如果主节点的副端口能够在配置的周期内接收到该报文，则说明整个环路正常，否则表明环路出现故障。MRPP 环的传输节点不需要该定时器，可以不用配置。

**举例：**配置 MRPP 环 4000 的 hello-timer 为 3 秒。

```
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#hello-timer 3
```

## 8.3.8 mrpp eaps compatible

**命令：mrpp eaps compatible**

**no mrpp eaps compatible**

**功能：** 使能 EAPS 的兼容模式，本命令的 no 操作关闭 EAPS 的兼容模式。

**参数：** 无。

**命令模式：** 全局配置模式

**缺省情况：** 系统不启动兼容 EAPS 的功能。

**使用指南：** 如果需要配置 EAPS 的兼容功能，需要先使能 MRPP 协议。在执行 no mrpp eaps compatible 命令时，需要确认该交换机已经使能 MRPP 协议。

**举例：** 全局启动 EAPS 的兼容功能。

Switch(Config)#mrpp enable

Switch(Config)#mrpp eaps compatible

## 8.3.9 mrpp enable

**命令：mrpp enable**

**no mrpp enable**

**功能：**使能 MRPP 协议模块，本命令的 no 操作关闭 MRPP 协议。

**参数：**无。

**命令模式：**全局配置模式

**缺省情况：**系统不启动 MRPP 协议模块。

**使用指南：**如果需要配置 MRPP 环，需要先使能 MRPP 协议。在执行 no mrpp enable 命令时，需要确认已经关闭该交换机使能的 MRPP 环。

**举例：**全局启动 MRPP

Switch(config)#mrpp enable

## 8.3.10 mrpp errp compatible

**命令：mrpp errp compatible**

**no mrpp errp compatible**

**功能：** 使能 ERRP 的兼容模式，本命令的 no 操作关闭 ERRP 的兼容模式。

**参数：** 无。

**命令模式：** 全局配置模式

**缺省情况：** 系统不启动兼容 ERRP 的功能。

**使用指南：** 如果需要配置 ERRP 的兼容功能，需要先使能 MRPP 协议。且需要把配置了 ERRP 兼容模式的端口配置成 hybrid 或者 trunk 模式，允许报文带上 Control Vlan 信息。

**举例：** 全局启动 ERRP 的兼容功能。

Switch(Config)#mrpp enable

Switch(Config)#mrpp errp compatible

Switch(Config)#mrpp ring 2

Switch(mrpp-ring-2)#control-vlan 4000

Switch(config-if-ethernet1/1/51)#switchport mode hybrid

Switch(config-if-ethernet1/1/51)#switchport hybrid allowed vlan 4000 tag

Switch(config-if-ethernet1/1/52)#switchport mode hybrid

Switch(config-if-ethernet1/1/52)#switchport hybrid allowed vlan 4000 tag

## 8.3.11 mrpp poll-time

**命令：mrpp poll-time <20-2000>**

**功能：**配置mrpp端口状态查询时间间隔。

**命令模式：**全局配置模式。

**使用指南：**配置查询时间可以调整MRPP端口状态查询间隔，默认间隔为100ms。

**举例：**设置查询时间为200ms。

Switch(Config)# mrpp poll-time 200

## 8.3.12 mrpp ring

**命令：mrpp ring *<ring-id>***

**no mrpp ring *<ring-id>***

**功能：**创建 MRPP 环，并进入 MRPP 环配置模式，本命令的 no 操作删除已经配置的 MRPP 环。

**参数：*<ring-id>***为 MRPP 环 ID，取值范围为<1-4096>。

**命令模式：**全局配置模式。

**使用指南：**在执行该命令时，如果没有创建过该 MRPP 环，则创建新的 MRPP 环，然后进入 MRPP 环配置模式。在执行本命令的 no 操作时，需要确认已经关闭该 MRPP 环。

**举例：**

Switch(config)# mrpp ring 100

## 8.3.13 mrpp ring primary-port

**命令：mrpp ring <*ring-id*> primary-port**

**no mrpp *ring* <ring-id> primary-port**

**功能：** 指定 MRPP 环的主端口。

**参数：** ***<ring-id>*** 为 MRPP 环 ID，取值范围为<1-4096>。

**命令模式：** 端口配置模式

**缺省情况：** 缺省没有配置。

**使用指南：** 本命令指定 MRPP 环的主端口。主节点利用主端口发送 Hello 健康检查报文，副端口用来接收主节点发出的 Hello 报文。副节点的主端口和副端口在功能上没有区别。

在使用该命令之前，mrpp enable 命令必须启动。此命令后，若 control vlan、secondary port、node-mode 和 enable 命令都已配置，则 mrpp 环功能启用。

**举例：** 配置 MRPP 环 4000 的主端口为 Ethernet1/1/1。

Switch(Config)# int ethernet 1/1/1

Switch(config-If-Ethernet1/1/1)#mrpp ring 4000 primary-port

## 8.3.14 mrpp ring secondary-port

**命令：mrpp ring < *ring-id* > secondary-port**

**no mrpp *ring* < ring-id > secondary-port**

**功能： 指定 MRPP 环的副端口。**

**参数：<ring-id>** 为 MRPP 环 ID，取值范围为<1-4096>。

**命令模式： 端口配置模式。**

**缺省情况： 缺省没有配置。**

***使用指南：* 本命令指定 MRPP 环的副端口。主节点利用副端口接收主节点发出的 Hello 报文。副节点的主端口和副端口在功能上没有区别。**

**在使用该命令之前，mrpp** enable 命令必须启动。此命令后，若 control vlan、primary port、node-mode 和 enable 命令都已配置，则 mrpp 环功能启用。

**举例：** 配置 MRPP 环 4000 的副端口为 1/1/3。

**Switch*(Config)*#**in ethernet 1/1/3

**Switch(config-lf-Ethernet1/1/**3)#mrpp ring 4000 secondary-port

## 8.3.15 node-mode

**命令：node-mode {master|transit}**

**功能：**配置交换机在 MRPP 环的类型是主节点还是副节点。

**参数：**无。

**命令模式：**MRPP 环配置模式

**缺省情况：**缺省设置交换机为该 MRPP 环副节点。

**使用指南：**无。

**举例：**配置交换机为 MRPP 环 4000 的主节点。

Switch(config)# mrpp ring 4000

Switch(mrpp-ring-4000)#node-mode master

## 8.3.16 show mrpp

**命令：show mrpp [*<ring-id>*]**

**功能：**显示 MRPP 环的配置信息。

**参数：*<ring-id>***为 MRPP 环 ID，取值范围为<1-4096>，如果不指定 ID，则显示所有的 MRPP 环的配置信息。

**命令模式：**特权和配置模式

**缺省情况：**无。

**使用指南：**无。

**举例：**显示交换机上的 MRPP 环 4000 的配置信息。

Switch# show mrpp 4000

### 8.3.17 show mrpp statistics

**命令：show mrpp statistics [*<ring-id>*]**

**功能：**显示 MRPP 环的接收和发送 MRPP 数据包的统计信息。

**参数：*<ring-id>***为 MRPP 环 ID，取值范围为<1-4096>，如果不指定 ID,则显示所有的 MRPP 环的统计信息。

**命令模式：**特权和配置模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**显示交换机上的 MRPP 环 4000 的统计信息。

Switch# show mrpp statistic 4000

## 8.4 ULPP

### 8.4.1 clear ulpp flush counter interface

**命令：clear ulpp flush counter interface *<name>***

**功能：**清除flush报文统计信息。

**参数：*<name>***为端口名。

**缺省情况：**无。

**命令模式：**特权配置模式。

**使用指南：**无。

**举例：**清除端口 1/1/1 的 flush 报文统计信息。

Switch# clear ulpp flush counter interface e1/1/1

ULPP flush counter has been reset.

### 8.4.2 control vlan

**命令：control vlan *<integer>***

**no control vlan**

**功能：**配置 ULPP 组的控制 VLAN，no 命令恢复默认值。

**参数：*<integer>***为发送 flush 报文的控制 VLAN 的 ID，取值范围为 1~4094。

**缺省情况：**默认为 VLAN 1。

**命令模式：**ULPP 组配置模式。

**使用指南：**配置 ULPP 组的控制 VLAN。该 VLAN 必须对应存在的 VLAN，配置后不允许删除该 VLAN。该 VLAN 必须属于 ULPP 组所保护的 VLAN，否则会导致 flush 报文环路。

**举例：**配置 ULPP 组发送控制 VLAN 为 10。

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# control vlan 10

## 8.4.3 debug ulpp error

**命令：debug ulpp error**

**no debug ulpp error**

**功能：**显示ULPP错误信息。no操作为关闭显示ULPP错误信息。

**参数：**无。

**缺省情况：**不显示。

**命令模式：**特权配置模式。

**使用指南：**无。

**举例：**显示 ULPP 的错误信息。

Switch# debug ulpp error

Unrecognized Flush packet received.

## 8.4.4 debug ulpp event

**命令：debug ulpp event**

**no debug ulpp event**

**功能：**显示ULPP事件信息，no操作为关闭显示ULPP的事件信息。

**参数：**无。

**缺省情况：**不显示。

**命令模式：**特权配置模式。

**使用指南：**无。

**举例：**显示 ULPP 的事件信息。

Switch# debug ulpp event

ULPP group 1 state changes：

Master port ethernet 1/1/1 in ULPP group 1 changed state to Forwading.

Slave port ethernet 1/1/2 in ULPP group 1 changed state to Standby.

## 8.4.5 debug ulpp flush content {send | receive} interface

**命令：debug ulpp flush content {send | receive} interface *<name>***

**no debug ulpp flush content {send | receive} interface *<name>***

**功能：**显示接收到的flush报文内容。no操作为关闭显示flush报文内容。

**参数：*<name>*：**端口名。

**缺省情况：**不显示。

**命令模式：**特权配置模式。

**使用指南：**无。

**举例：**显示端口 1/1/1 接收到的 flush 报文的内容。

Switch# debug ulpp flush content receive interface ethernet 1/1/1

Flush packet content:

Destination MAC: 01-03-0f-cc-cc-cc

Source MAC: 00-a0-cc-d7-5c-ea

Type: 8100

Vlan ID: 1

Length: 518

Control Type: 2

Control Vlan: 10

MAC number:0

Vlan Bitmap:

## 8.4.6 debug ulpp flush {send | receive} interface

**命令：debug ulpp flush {send | receive} interface *<name>***

**no debug ulpp flush {send | receive} interface *<name>***

**功能：**显示收发flush报文信息，只显示收到报文，不显示报文的具体内容。no操作为关闭显示收发flush报文包信息。

**参数：*<name>***为端口名。

**缺省情况：**不显示。

**命令模式：**特权配置模式。

**使用指南：**无。

**举例：**显示端口 1/1/1 的发送 flush 报文的信息。

Swtich# debug ulpp flush send interface e1/1/1

Flush packet send on port Ethernet 1/1/1。

## 8.4.7 description

**命令：description *<string>***

**no description**

**功能：**配置ULPP组的描述字符串。No命令删除描述。

**参数：*<string>***为ULPP组名称，最大字符数为128。

**缺省情况：**默认没有配置ULPP名称。

**命令模式：**ULPP组配置模式。

**使用指南：**无。

**举例：**配置 ULPP 组的描述为 dcn。

Switch(config)#ulpp group 20

Switch(ulpp-group-20)# description dcn

## 8.4.8 flush disable arp

**命令：flush disable arp**

**功能：**关闭 ARP 删除的 flush 报文发送功能。

**参数：**无。

**缺省情况：**默认使能 ARP 删除的 flush 报文发送功能。

**命令模式：**ULPP 组配置模式。

**使用指南：**若配置该命令，则在链路切换时，不会主动发送 flush 报文通知上游设备删除 ARP 表项。

**举例：**关闭 ULPP 组的 ARP 删除的 flush 报文发送功能。

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# flush disable arp

## 8.4.9 flush disable mac

**命令：flush disable mac**

**功能：**关闭 MAC 地址更新的 flush 报文发送功能。

**参数：**无。

**缺省情况：**默认使能 MAC 地址更新的 flush 报文发送功能。

**命令模式：**ULPP 组配置模式。

**使用指南：**若配置该命令，则在链路切换时，不会主动发送 flush 报文通知上游设备更新 MAC 地址表项。

**举例：**关闭 ULPP 组的 MAC 地址更新的 flush 报文发送功能。

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# flush disable mac

## 8.4.10 flush disable mac-vlan

**命令：flush disable mac-vlan**

**功能：**关闭根据 vlan 删除动态单播 mac 的 flush 报文发送功能

**参数：**无

**缺省情况：**默认不使能 mac-vlan 删除的 flush 报文发送功能

**命令模式：**ULPP 组配置模式

**使用指南：**若配置该功能，则在链路发生切换时，不会主动发出 flush 报文通知上游设备根据 vlan 删除动态单播 mac。

**举例：**关闭 ulpp 组的 mac-vlan 删除的 flush 报文发送功能

Switch(config)#ulpp group 1

Switch(ulpp-group-1)#flush disable mac-vlan

## 8.4.11 flush enable arp

**命令：flush enable arp**

**功能：**使能 ARP 删除的 flush 报文发送功能。

**参数：**无。

**缺省情况：**默认使能 ARP 删除的 flush 报文发送功能。

**命令模式：**ULPP 组配置模式。

**使用指南：**若使能该功能，则在链路切换时，会主动发送 flush 报文通知上游设备删除 ARP 表项。

**举例：**使能 ULPP 组的 ARP 删除的 flush 报文发送功能。

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# flush enable arp

## 8.4.12 flush enable mac

**命令：flush enable mac**

**功能：**使能 MAC 地址更新的 flush 报文发送功能。

**参数：**无。

**缺省情况：**默认使能 MAC 地址更新的 flush 报文发送功能。

**命令模式：**ULPP 组配置模式。

**使用指南：**若使能该功能，则在链路切换时，会主动发送 flush 报文通知上游设备更新 MAC 地址表项。

**举例：**使能 ULPP 组的 MAC 地址更新的 flush 报文发送功能。

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# flush enable mac

## 8.4.13 flush enable mac-vlan

**命令：flush enable mac-vlan**

**功能：**使能根据 vlan 删除动态单播 mac 的 flush 报文发送功能

**参数：**无

**缺省情况：**默认不使能 mac-vlan 删除的 flush 报文发送功能

**命令模式：**ULPP 组配置模式

**使用指南：**若使能该功能，则在链路发生切换时，会主动发出 flush 报文通知上游设备根据 vlan 删除动态单播 mac。

**举例：**使能 ulpp 组的 mac-vlan 删除的 flush 报文发送功能

Switch(config)#ulpp group 1

Switch(ulpp-group-1)#flush enable mac-vlan

## 8.4.14 preemption delay

**命令：preemption delay *<integer>***

**no preemption delay**

**功能：**配置抢占时延，no 命令配置抢占时延为默认值。

**参数：*<integer>*：**抢占时延，范围 1－600。单位为秒。

**缺省情况：**默认抢占时延为 30。

**命令模式：**ULPP 组配置模式。

**使用指南：**抢占时延为主端口抢占为 forwarding 状态前，延迟的一段时间，以防止链路短时间内振荡。抢占时延在启用抢占模式后生效。

**举例：**配置 ULPP 组的抢占时延为 50s。

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# preemption delay 50

## 8.4.15 preemption mode

**命令：preemption mode**

**no preemption mode**

**功能：**打开/关闭 ULPP 组配置抢占模式。

**参数：**无。

**缺省情况：**不抢占。

**命令模式：**ULPP 组配置模式。

**使用指南：**若配置了 ULPP 组的抢占模式，则当副端口为 forwarding 状态，主端口为 standby 状态时，在抢占时延超时后，主端口会转换为 forwarding 状态，将副端口转换为 standby 状态。

**举例：**配置 ULPP 组的抢占模式。

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# preemption mode

## 8.4.16 protect vlan-reference-instance

**命令：protect vlan-reference-instance *<instance-list>***

**no protect vlan-reference-instance *<instance-list>***

**功能：**配置 ULPP 组的保护 VLAN；本命令的 no 操作取消保护 vlan。

**参数：*<instance-list>*为** MSTP 实例列表，形势如：i；j-k；。列表中实例的数量不限制。

**缺省情况：**默认不保护任何 VLAN，即不引用任何实例。

**命令模式：**ULPP 组配置模式。

**使用指南：**保护 VLAN 是通过引用 MSTP 的实例来实现的。该实例对应的 VLAN 在该组一个端口上处于 forwarding 状态，在另一端口上处于 blocked 状态。每个 ULPP 组可以引用所有

的 MSTP 实例。可以引用不存在的 MSTP 实例，此时相当于不保护任何 VLAN，不同的 ULPP 组不能引用相同的实例。

**举例：**配置 ULPP 组保护 VLAN 为实例 1。

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# protect vlan-reference-instance 1

## 8.4.17 show ulpp flush counter interface

**命令：show ulpp flush counter interface {ethernet <IFNAME> | <IFNAME>}**

**功能：**显示flush报文统计信息。

**参数：<IFNAME>**为端口名。

**缺省情况：**无。

**命令模式：**特权配置模式。

**使用指南：**显示flush报文统计信息。如：已接收到的flush报文数量，最后接收flush报文的时间等信息。

**举例：**显示 ULPP 组 1 的 flush 报文统计信息。

Switch# show ulpp flush counter interface e1/1/1

Received flush packets: 10

## 8.4.18 show ulpp flush-receive-port

**命令：show ulpp flush-receive-port**

**功能：**显示哪些端口配置了接收flush报文，以及端口接收flush类型和control vlan。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权配置模式。

**使用指南：**无。

**举例：**显示配置了端口接收 flush 报文的信息。

Switch# show ulpp flush-receive-port

ULPP flush-receive portlist:

Portname Type Control Vlan

---

Ethernet1/1/1 ARP 1

Ethernet1/1/3 MAC 1;3;5-10

---

## 8.4.19 show ulpp group

**命令：show ulpp group [group-id]**

**功能：**显示已配置的ULPP组的配置信息。

**参数：[group-id]**为显示指定ULPP组信息。

**缺省情况：**缺省显示所有已配置的ULPP组信息。

**命令模式：**特权配置模式。

**使用指南：**显示已配置的ULPP组的配置信息。如：主端口，副端口的状态，抢占模式，抢占时延等。

**举例：**显示 ULPP 组 1 的配置信息。

```
Switch# show ulpp group 1
ULPP group 1 information:
Description: abc
Preemption mode: on
Preemption delay: 30s
Control VLAN:1
Protected VLAN: Reference Instance 1
Member                Role            State
--------------------------------------------------------------
Ethernet1/1/1         MASTER          FORWARDING
Ethernet1/1/2         SLAVE           STANDBY
```

## 8.4.20 ulpp control vlan

**命令：ulpp control vlan *<vlan-list>***

**no ulpp control vlan *<vlan-list>***

**功能：**配置端口的接收控制 VLAN；本命令的 no 操作恢复缺省值。

**参数：*<vlan-list>***指定接受 flush 报文的控制 VLAN 列表，形如：i；j-k。每一个字符串中包含的 VLAN 数目不超过 100。端口的接收控制 VLAN 可以追加。

**缺省情况：**默认为 VLAN 1。

**命令模式：**端口配置模式。

**使用指南：**配置端口的接收控制 VLAN。该 VLAN 必须对应存在的 VLAN，配置后不允许删除该 VLAN。

**举例：**配置接收控制 VLAN 为 10。

```
Switch(config)# interface ethernet 1/1/1
Switch(config-If-Ethernet1/1/1)# ulpp control vlan 10
```

## 8.4.21 ulpp flush disable arp

**命令：ulpp flush disable arp**

**功能：**关闭 ARP 删除的 flush 报文接收功能。

**参数：**无。

**缺省情况：**默认关闭 ARP 删除的 flush 报文接收功能。

**命令模式：**端口配置模式。

**使用指南：**若配置该命令，则不会接收 ARP 删除的 flush 报文。

**举例：**关闭 ARP 删除的 flush 报文接收功能。

Switch(config)# interface ethernet 1/1/1

Switch(config-If-Ethernet1/1/1)# ulpp flush disable arp

## 8.4.22 ulpp flush disable mac

**命令：ulpp flush disable mac**

**功能：**关闭 MAC 地址更新的 flush 报文接收功能。

**参数：**无。

**缺省情况：**默认关闭 MAC 地址更新的 flush 报文接收功能。

**命令模式：**端口配置模式。

**使用指南：**若配置该命令，则不会接收 MAC 地址更新的 flush 报文。

**举例：**关闭 MAC 地址更新的 flush 报文接收功能。

Switch(config)# interface ethernet 1/1/1

Switch(config-If-Ethernet1/1/1)# ulpp flush disable mac

## 8.4.23 ulpp flush disable mac-vlan

**命令：ulpp flush disable mac-vlan**

**功能：**关闭 mac-vlan 类型的 flush 报文接收功能

**参数：**无

**缺省情况：**默认不接收 mac-vlan 类型 flush 报文接收功能

**命令模式：**端口配置模式

**使用指南：**若配置该功能，则对于配置端口接收到的 mac-vlan 类型 flush 报文，只进行硬件转发，不进行解析处理。

**举例：**关闭端口的 mac-vlan 类型的 flush 报文接收功能

Switch(config)#interface e1/1/2

Switch(config-if-ethernet1/1/2)#ulpp flush disable mac-vlan

## 8.4.24 ulpp flush enable arp

**命令：ulpp flush enable arp**

**功能：**使能 ARP 删除的 flush 报文接收功能。

**参数：**无。

**缺省情况：**默认关闭 ARP 删除的 flush 报文接收功能。

**命令模式：**端口配置模式。

**使用指南：**若使能该功能，则会接收 ARP 删除的 flush 报文。

**举例：**使能 ARP 删除的 flush 报文接收功能。

Switch(config)# interface ethernet 1/1/1

Switch(config-If-Ethernet1/1/1)# ulpp flush enable arp

## 8.4.25 ulpp flush enable mac

**命令：ulpp flush enable mac**

**功能：**使能 MAC 地址更新的 flush 报文接收功能。

**参数：**无。

**缺省情况：**默认关闭 MAC 地址更新的 flush 报文接收功能。

**命令模式：**端口配置模式。

**使用指南：**若使能该功能，则会接收 MAC 地址更新的 flush 报文。

**举例：**使能 MAC 地址更新的 flush 报文接收功能。

Switch(config)# interface ethernet 1/1/1

Switch(config-If-Ethernet1/1/1)# ulpp flush enable mac

## 8.4.26 ulpp flush enable mac-vlan

**命令：ulpp flush enable mac-vlan**

**功能：**使能 mac-vlan 类型的 flush 报文接收功能

**参数：**无

**缺省情况：**默认不接收 mac-vlan 类型 flush 报文接收功能

**命令模式：**端口配置模式

**使用指南：**若使能该功能，则配置端口接收处理 mac-vlan 类型的 flush 报文，根据报文中携带 vlan 信息删除动态单播 mac。

**举例：**使能端口的 mac-vlan 类型的 flush 报文接收功能

Switch(config)#interface e1/1/2

Switch(config-if-ethernet1/1/2)#ulpp flush enable mac-vlan

## 8.4.27 ulpp group

**命令：ulpp group *<integer>***

**no ulpp group *<integer>***

**功能：**创建一个 ULPP 组。如果该组已经存在，则进入 ULPP 组配置模式。本命令的 no 命令为删除一个 ULPP 组。

**参数：*<integer>***为 ULPP 组 ID。范围为 1－48。

**命令模式：**全局配置模式。

**缺省情况：**没有配置任何 ULPP 组。

**使用指南：**无。

**举例：**配置 ulpp group 20 或者进入 ULPP 组 20 的模式。

Switch(config)# ulpp group 20

Switch(ulpp-group-20)#

## 8.4.28 ulpp group master

**命令：ulpp group *<integer>* master**

**no ulpp group *<integer>* master**

**功能：**配置ULPP组的主端口；no命令删除该主端口。

**参数：*<integer>***为ULPP组ID。范围为1－48。

**缺省情况：**默认没有配置主端口。

**命令模式：**端口配置模式。

**使用指南：**组内的主副端口无先后配置顺序，但配置成员端口之前必须配置保护VLAN。每个组只有一个主端口，如果主端口已经存在，则配置失败。

**举例：**配置 ULPP 组的主端口。

Switch(config)# interface ethernet 1/1/1

Switch(config-If-Ethernet1/1/1)# ulpp group 20 master

## 8.4.29 ulpp group slave

**命令：ulpp group *<integer>* slave**

**no ulpp group *<integer>* slave**

**功能：**配置ULPP组的副端口；no命令删除该副端口。

**参数：*<integer>***为ULPP组ID。范围为1－48。

**缺省情况：**默认没有配置副端口。

**命令模式：**端口配置模式。

**使用指南：**组内的主副端口无先后配置顺序，但配置成员端口之前必须配置保护VLAN。每个组只有一个副端口，如果副端口已经存在，则配置失败。

**举例：**配置 ULPP 组的副端口。

Switch(config)# interface ethernet 1/1/2

Switch(config-If-Ethernet1/1/2)# ulpp group 20 slave

# 8.5 ULSM

## 8.5.1 debug ulsm event

**命令：debug ulsm event**

**no debug ulsm event**

**功能：**显示ULSM事件信息，no操作为关闭显示ULSM事件信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权配置模式。

**使用指南：**无。

**举例：**显示 ULSM 的事件信息。

Switch# debug ulsm event

Downlink synchoronized with ULSM group, change state to Down.

## 8.5.2 show ulsm group

**命令：show ulsm group [group-id]**

**功能：**显示ULSM组的配置信息。

**参数：[group-id]**为ULSM组ID。

**缺省情况：**缺省显示所有已配置的ULSM组信息。

**命令模式：**特权配置模式。

**使用指南：**无。

**举例：**显示 ULSM 组 1 的配置信息。

Switch# show ulsm group 1

ULSM group 1 information:

ULSM group state：Down

| Member | Role | State | Down by ULSM |
|---|---|---|---|
| ethernet1/1/1 | UpLINK | Down | |
| ethernet1/1/2 | DownLINK | Down | Yes |

## 8.5.3 ulsm group

**命令：ulsm group *<group-id>***

**no ulsm group *<group-id>***

**功能：**创建ULSM组。No命令删除ULSM组。

**参数：*<group-id>***为ULSM组号，取值范围为1－32。

**缺省情况：**默认没有配置ULSM组。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**创建 ULSM 组 10。

Switch(config)# ulsm group 10

## 8.5.4 ulsm group {uplink | downlink}

**命令：ulsm group *<group-id>* {uplink | downlink}**

**no ulsm group *<group-id>***

**功能：**配置ULSM组的上行/下行端口。No命令删除上行/下行端口。

**参数：*<group-id>*：**ULSM组号，取值范围为1－32。

**uplink：**配置为上行端口。

**downlink：**配置为下行端口。

**缺省情况：**端口不属于任何ULSM组。

**命令模式：**端口配置模式。

**使用指南：**配置ULSM组的上行/下行端口。每个ULSM组可以配置最多8个上行端口和16个下行端口。

**举例：**配置端口 1/1/3 为 ULSM 组 10 的上行端口。

```
Switch(config)# interface ethernet 1/1/3
Switch(config-If-Ethernet1/1/3)# ulsm group 10 uplink
```

# 8.6 ERPS

## 8.6.1 ethernet tcn-propagation erps to {erps | stp}

**命令：ethernet tcn-propagation erps to {erps | stp}**

**no ethernet tcn-propagation erps to**

**功能：**配置拓扑变化传播通知方式。目前支持 ERPS 环间的 R-APS event 通知，主要用于子环拓扑变化后向交叉环发送 R-APS event 报文通知邻居环。默认拓扑变化只在本环内产生影响，不传播到环以外范围，即不影响与之连接的邻居拓扑。本命令的 no 操作为删除拓扑变化传播通知方式。

**参数：**erps：拓扑变化发送 R-APS event 报文通知本设备上的连接环；stp：拓扑变化发送 stp 报文通知本设备上连接的 stp 拓扑。

**缺省状态：**ERPS 环拓扑变化只在本环内产生影响，不发送通知报文。

**命令模式：**全局模式。

**使用指南：**配置本设备支持的拓扑变化传播通知方式为指定方式；本设备上 ERPS 环实例检测到 ERPS 环拓扑变化，根据配置发送通知报文：如果配置了 erps 方式，则向本设备上的其它 ERPS 环发送 R-APS event 报文；如果配置了 stp 方式，则向外发送 stp 报文。

**举例：**

配置拓扑发生变化后向相交环发送 R-APS event 通知。

```
Switch(config)#ethernet tcn-propagation erps to erps
```

配置拓扑发生变化后向相交环发送 STP 通知。

```
Switch(config)#ethernet tcn-propagation erps to stp
```

删除拓扑变化传播通知方式。

```
Switch(config)#no ethernet tcn-propagation erps to
```

## 8.6.2 erps-ring <ring-name>

**命令：erps-ring < *ring-name* >**

**no erps-ring < *ring-name* >**

**功能：**创建 ERPS 环，并进入 ERPS 环配置模式。如果该 ERPS 环已经存在，则进入 ERPS 环配置模式。本命令的 no 操作为删除 ERPS 环。

**参数：**<*ring-name*>：要创建的 ERPS 环名称，最大字符数为 64，由字母、数字、下划线组成，首尾字符不能为下划线。

**命令模式：**全局配置模式。

**缺省状态：**没有配置任何 ERPS 环。

**使用指南：**如果输入 ring name 字符串长度超过 64 字节，提示错误“Valid ERPS ring name should be no more than 64 bytes!”；如果输入 ring name 字符串格式不合法，提示错误“Invalid ERPS ring name!”；如果该设备配置 ERPS ring 总数已达到最多值，提示错误“Support ERPS ring max number: 32!”；如果存在该 ERPS 环则进入 ERPS 环配置模式，否则创建并进入 ERPS 环配置模式。

**举例：**

创建 ERPS 环 ring1。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#

删除 EPRS 环 ring1。

Switch(config)#no erps-ring ring1

## 8.6.3 version {v1 | v2}

**命令：version {v1 | v2}**

**no version**

**功能：**配置 ERPS 环的支持版本，本次实现为最新的 v2 版本，能与 v1 版本兼容，v1 版本不支持 MS、FS 等管理命令，不支持多实例，并且只支持可逆倒换机制。如果 ERPS 环上没有配置实例，可以多次配置支持版本，以最后一次配置为准。如果环上已配置 ERPS 环实例，则不能修改支持版本。本命令的 no 操作为 ERPS 环恢复成缺省状态，默认支持 V2 版本。

**参数：**{v1 | v2}：参数选择，v1 表示支持 2008-06 发布的 v1 版本及修正案（2009-04）。v2 表示支持 2010-03 发布的 v2 版本及其修正案（2010-06）。

**命令模式：**ERPS 环配置模式。

**缺省状态：**默认支持 v2 版本。

**使用指南：**

1.如果该 ERPS 环上已配置了 ERPS 环实例，提示错误“Cann't config version on ERPS ring whitch has ERPS instance, please delete ERPS instance firstly!”，否则进入下一步处理；

2.设置 ERPS 环支持指定的协议版本；

3.如果配置 ERPS 环支持 v1 版本，则该环不支持多实例，ERPS 环实例不支持 MS、FS 等管理命令，并且不可逆配置无效，强制只支持可逆切换机制。

4.如果配置 ERPS 环支持 v1 版本，则该环上实例处理 ERPS 报文按照 v1 格式要求，即按照 v1 版本格式封装 R-APS 报文和解析处理各字段，v2 定义字段忽略不处理。

**举例：**

配置 ERPS 环 ring1 支持 v1 版本协议。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#version v1

配置 ERPS 环 ring1 支持 v2 版本协议。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#version v2

删除 ERPS 环 ring1 支持的 V1 版本协议

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#no version

## 8.6.4 open-ring

**命令：open-ring**

**no open-ring**

**功能：**配置 ERPS 环为子环开放类型。如果环上已经配置 ERPS 环实例，则不能修改 ERPS 环类型，必须先删除 ERPS 环实例。环中所有节点必须配置一致，该类型 ERPS 可以与其它 ERPS 环相连接，用于环交叉拓扑。本命令的 no 操作为删除 ERPS 环为子环开放类型，恢复为默认的主环封闭类型。

**参数：**无。

**命令模式：**ERPS 环配置模式。

**缺省状态：**默认 ERPS 环为主环封闭类型。

**使用指南：**如果环上已经配置 ERPS 环实例，提示错误“Cann't config open-ring on ERPS ring whitch has ERPS instance, please delete ERPS instance firstly!”，否则进入下一步处理；配置该 ERPS 环类型为子环类型。

**举例：**

配置 ERPS 环 ring1 为子环开放类型。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#open-ring

删除 ERPS 环 ring1 为子环开放类型。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#no open-ring

## 8.6.5 raps-virtual-channel {with | without}

**命令：raps-virtual-channel {with | without}**

**功能**：配置 ERPS 环是否存在 R-APS 虚通道。只在子环中所有节点上配置，配置必须一致。

**参数**：{with | without}：参数选择，若选择 with 表示该 ERPS 环存在 R-APS 虚通道，若选择 without 表示该 ERPS 环不存在 R-APS 虚通道。

**命令模式**：ERPS 环配置模式。

**缺省状态**：ERPS 环不存在 R-APS 虚通道。

**使用指南**：

a）如果是主环，提示错误“Cann't config R-APS virtual channel on ERPS major ring!”；

b）按照配置设置该 ERPS 环是否存在 R-APS 虚通道。

输出：配置成功或提示错误。如果该 ERPS 环不存在 R-APS 虚通道，则该 ERPS 环上所有实例的 R-APS 通道永远畅通，只 block 数据通道；否则 R-APS 通道和数据通道一同被 block。

**举例**：

配置 ERPS 子环 ring1 存在 R-APS 虚通道。

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#raps-virtual-channel with
```

## 8.6.6 erps-ring <ring-name> port0 [port1-none]

**命令：erps-ring <ring-name> port0 [port1-none]**

**no erps-ring <ring-name> port0**

**功能**：配置 ERPS 环节点的 port0。每个环节点只有一个 port0，如果 port0 已经存在，则不会覆盖此前的配置，只是提示错误。若配置了 port1-none 表示该环没有 port1，为交叉节点。本命令的 no 操作为删除 ERPS 配置的 port0。

**参数**：<ring-name> ：ERPS 环名称，最大字符数为 64，由字母、数字、下划线组成，首尾字符不能为下划线。

[port1-none]：表示该 ERPS 环节点只有 port0，没有 port1，为交叉节点。

**命令模式**：端口配置模式。

**缺省状态**：ERPS 环未配置 port0。

**使用指南**：

如果输入 ring name 字符串长度超过 64 字节，提示错误“Valid ERPS ring name should be no more than 64 bytes！”；

如果输入 ring name 字符串格式不合法，提示错误“Invalid ERPS ring name!”；

如果该端口开启 stp 互斥功能，提示错误“Port %s has enable stp or other mutex module!”，%s 为端口名；

如果该端口为汇聚口的成员端口，提示错误“Port %s is LAG member port!”，%s 为端口名；

如果该 ERPS 环不存在，提示错误“The ERPS ring doesn't exist!”；

如果该 ERPS 环已存在 port0，提示错误“Port0 exists on the ERPS ring already!”；

如果该端口已配置为该ERPS环的port1，提示错误“Port %s is already configed as port1 on the ERPS ring!”，%s 为端口名；

如果该 ERPS 环不是 open-ring 类型，则不能配置 port1-none，提示错误“Can not config port1-none on ERPS major ring!”；

配置该端口为指定 ERPS 环的 port0；

检查配置 ERPS 环配置是否完整，若完整则检查其上 ERPS 实例配置是否完整，若完整则激活实例为 active，运行协议。

**举例：**

配置 e 1/1/1 为 ERPS 环 ring1 的 port0。

Switch(config)#interface ethernet 1/1/1

Switch(config-if-ethernet1/1/1)#erps-ring ring1 port0

删除 e1/1/1 为 ERPS 环 ring1 的 port0。

Switch(config)#interface ethernet 1/1/1

Switch(config-if-ethernet1/1/1)#no erps-ring ring1 port0

## 8.6.7 erps-ring <ring-name> port1

**命令：erps-ring <ring-name> port1**

**no erps-ring <ring-name> port1**

**功能：**配置 ERPS 环节点的 port1。每个环节点只有一个 port1，如果 port1 已经存在，则不会覆盖此前的配置，只是提示错误。若配置了 port1-none，则配置 port1 不成功。本命令的 no 操作为删除 ERPS 环配置 port1。

**参数：**<ring-name>：ERPS 环名称，最大字符数为 64，由字母、数字、下划线组成，首尾字符不能为下划线。

**命令模式：**端口配置模式。

**缺省状态：**ERPS 环未配置 port1。

**使用指南：**

如果输入ring name字符串长度超过64字节，提示错误“Valid ERPS ring name should be no more than 64 bytes！”；

如果输入 ring name 字符串格式不合法，提示错误“Invalid ERPS ring name!”；

如果该端口开启 stp 互斥功能，提示错误“Port %s has enable stp or other mutex module!”，%s 为端口名；

如果该端口为汇聚口的成员端口，提示错误“Port %s is LAG member port!”，%s 为端口名；

如果该 ERPS 环不存在，提示错误“The ERPS ring doesn't exist!”；

如果该 ERPS 环已存在 port1，提示错误“Port1 exists on the ERPS ring already!”；

如果该端口已配置为该ERPS环的port0，提示错误“Port %s is already configed as port0 on the ERPS ring!”，%s 为端口名；

如果该 ERPS 环配置了 port1-none，提示错误“Has configed port1-none on the ERPS open ring!”；

配置该端口为指定 ERPS 环的 port1；

检查该 ERPS 环是否配置完整，若完整则检查 ERPS 环上所有实例是否配置完整，若完整则激活 ERPS 实例为 active，运行协议。

**举例：**

配置 e1/1/1 为 ERPS 环 ring1 的 port1。

Switch(config)#interface ethernet 1/1/1

Switch(config-if-ethernet1/1/1)#erps-ring ring1 port1

删除 e1/1/1 为 ERPS 环 ring1 的 port1。

Switch(config)#interface ethernet 1/1/1

Switch(config-if-ethernet1/1/1)#no erps-ring ring1 port1

## 8.6.8 failure-detect {cc | physical-link-or-cc} domain <domain-name> service {< ma-name > | number < ma-num > | pvlan < vlan-id >} mep <mep-id> rmep<rmep-id>

**命令：{port0 | port1} failure-detect {cc | physical-link-or-cc} domain <domain-name> service {< ma-name > | number < ma-num > | pvlan < vlan-id >} mep <mep-id> rmep<rmep-id>**

**no {port0 | port1} failure-detect**

**功能：**配置 ERPS 环端口的故障检测类型。如果检测的为 cc 类型，则需要指明 cc 所属维护域，所属维护集，以及监控的链路（由（mep-id，rmep-id）确定）。配置故障检测类型前提是已把相应环端口加入了 ERPS 环。本命令的 no 操作为删除环端口故障检测类型。

**参数：**{port0 | port1}：参数选择，port0 表示要配置 port0 的故障检测类型。port1 表示要配置 port1 的故障检测类型。

{cc | physical-link-or-cc}：参数选择，cc 表示 ERPS 环端口检测的为 cc 上报故障。physical-link-or-cc 表示 ERPS 环端口检测的为 cc 上报故障和物理链路故障。

<domain-name>：表示 ERPS 环端口检测的 cfm 所属域名字。

<ma-name>：ERPS 环端口检测的 cfm 所属 service 名字。

<mep-id>：ERPS 环端口检测的 cfm 监控的本地 mep id。

<rmep-id>：ERPS 环端口检测的 cfm 监控的远端 mep id。

**命令模式：**ERPS 环配置模式。

**缺省状态：**默认 ERPS 环端口只检测物理链路故障。

**使用指南：**如果输入 domain name 字符串长度超过 43 字节，提示错误“Valid domain name should be no more than 43 bytes！”；

如果输入 domain name 字符串格式错误，提示错误“Invalid domain name!”；

如果输入 service name 字符串长度超过 45 字节，提示错误“Valid service name should be no more than 45 bytes！”；

如果输入 service name 字符串格式错误，提示错误“Invalid service name!”；

如果 local mep 和 remote mep 相同，提示错误“The local mep can not be the same as the remote mep!”，否则进入下一步处理；

配置该 ERPS 环端口的故障检测类型为指定类型，如果检测类型为 cc，保存配置的 md、ma、mep 和 rmep 信息，用于接收到 cfm 故障通知后进行匹配。

**举例：**

配置 ERPS 环 ring1 的 port0 故障检测类型为 cc。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#port0 failure-detect cc domain domain1 service serivice1 mep 1 rmep 2

删除 ERPS 环 ring1 的 port0 故障检测类型为 cc。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#no port0 failure-defect

## 8.6.9 erps-instance <instance-id>

**命令：erps-instance <instance-id>**

**no erps-instance <instance-id>**

**功能：**创建 ERPS 环上实例，并进入 ERPS 环实例配置模式。如果该 ERPS 环实例已经存在，则进入 ERPS 实例配置模式。若 ERPS 环支持 v2 版本，则可配置多个 ERPS 环实例。本命令的 no 操作为删除 ERPS 环实例。

**参数：**<instance-id>：ERPS 环实例 id，范围：1～48。

**命令模式：**ERPS 环配置模式。

**缺省状态：**没有配置任何 ERPS 环实例。

**使用指南：**如果所在 ERPS 环支持版本 1，当配置多于一个 ERPS instance 时，提示错误“Doesn't support multiple ERPS instance capability on the ring running version 1!”；

如果该 ERPS 环上配置多于最大可支持的 ERPS instance 时，提示错误“Support ERPS instance max number: 32 per ERPS ring!”；

如果 ERPS 环上存在该 ERPS 环实例，则进入 ERPS 环实例配置模式；

否则创建相应 ERPS 环实例并进入 ERPS 实例配置模式；

**举例：**

在 ERPS 环 ring1 上配置 ERPS 环实例 1。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#

删除 ERPS 环 ring1 上配置 ERPS 环实例 1。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#no erps-instance 1

Switch(config-erps-ring-inst-1)#

## 8.6.10 description

**命令：description <instance-name>**

**no description <instance-name>**

**功能：**配置 ERPS 实例的描述字符串。

**参数：**<instance-name>：ERPS 实例名称，最大字符数为 64，由字母、数字、下划线组成，首尾字符不能为下划线。本命令的 no 操作为删除 ERPS 环实例名称。

**命令模式：**ERPS 实例配置模式。

**缺省状态：**默认没有配置 ERPS 实例名称。

**使用指南：**判断字符串长度，如果超过 64，则提示错误“Valid ERPS instance name should be no more than 64 bytes！”；如果输入字符串格式非法，提示错误“Invalid ERPS instance name!”；否则设置 ERPS 实例名称为指定字符串。

**举例：**

配置 ERPS 环 ring1 上的实例 1 的名称为 instance1。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)# description instance1

删除 ERPS 环 ring1 上的实例 1 的名称为 instance1。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)# no description

## 8.6.11 ring-id <ring-id>

**命令：ring-id <ring-id>**

**no ring-id <ring-id>**

**功能：**配置 ERPS 环节点发出的 R-APS 报文中目的 MAC 地址最后一个字节携带 ring-id，如果 ERPS 环支持 v1 版本，ring-id 只能配置为 1。本命令的 no 操作为配置 ERPS 环节点发出的 R-APS 报文中目的 MAC 地址不携带 ring-id，即目的 MAC 为 01-19-A7-00-00-01。

**参数：**<ring-id>：ERPS 环 id，范围：1～64。

**命令模式：**ERPS 环实例配置模式。

**缺省状态：**默认发出的 R-APS 报文中目的 MAC 地址为 01-19-A7-00-00-01。

**使用指南：**如果 ERPS 环支持 v1 版本，ring-id 只能配置为 1，因为 v1 版本只支持目的 MAC 地址‘01-19-A7-00-00-01’，否则提示错误“Cann't config ringid other than 1 on the ERPS ring running version 1!”；

如果 ERPS 环支持 v2 版本，配置该 ERPS 环上实例发出的 R-APS 报文中目的 MAC 地址的最后一个字节携带值为指定 ring-id。

**举例：**

配置 ERPS 环 ring1 上实例 2 发送的 R-APS 报文中目的 mac 最后一个字节为 ring-id 2。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 2

Switch(config-erps-ring-inst-2)#ring-id 2

配置 ERPS 环 ring1 上实例 2 发送的 R-APS 报文中目的 MAC 地址不携带 ring-id，即目的 MAC 为 01-19-A7-00-00-01

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 2

Switch(config-erps-ring-inst-2)#no ring-id

## 8.6.12 rpl {port0 | port1} {owner | neighbour}

**命令：rpl {port0 | port1} {owner | neighbour}**

**no rpl {port0 | port1}**

**功能：**配置 ERPS 环实例的成员端口为 RPL owner 或 RPL neighbour，同一 ERPS 环上不同实例的 RPL 节点角色不能配置在同一成员端口上。本命令的 no 操作为配置 ERPS 环实例的成员端口为普通传输端口角色。

**参数：**{port0 | port1}：参数选择，port0 表示要配置 port0 在 ERPS 环实例中的 RPL 角色，port1 表示要配置 port1 在 ERPS 环实例中的 RPL 角色。

{owner | neighbour }：参数选择，owner 表示配置指定成员端口为 rpl owner 角色；neighbour 表示配置指定成员端口为 rpl neighbour 角色。

**命令模式：**ERPS 环实例配置模式。

**缺省状态：**无，即普通传输节点类型。

**使用指南：**如果配置了 port1-none，则不能配置 port1 的节点角色，提示错误“Has configed port1-none on the ERPS open ring!”；

如果该实例节点已经是 rpl owner 或 rpl neighbour，则不能再对任何成员端口执行该命令，提示错误“Has configed port rpl role: %s on the ERPS instance!”，%s 为已配置的 rpl 角色；如果该实例所在 ERPS 环上其它实例已设置了指定 rpl 角色，提示错误“Has configed port rpl role: %s in this or other ERPS instance on the ERPS ring!”；设置该实例所在 ERPS 环上的指定成员端口为该实例上的指定节点角色。

**举例：**

配置 ERPS 环 ring1 上的实例 1 中 port0 为 RPL 拥有节点。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)# rpl port0 owner

配置 ERPS 环 ring1 实例 1 的端口 port0 为普通传输端口角色

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)# no rpl port0

## 8.6.13 non-revertive

**命令：non-revertive**

**no non-revertive**

**功能：**配置 ERPS 环实例为不可逆切换机制，如果该 ERPS 环支持 v1 版本，则该命令无效，不能配置。本命令的 no 操作为配置 ERPS 环实例为可逆切换机制，如果该 ERPS 环支持 v1 版本，则该命令无效。该命令只在子环的 RPL 拥有节点上配置即可。

**参数：**无。

**命令模式：**ERPS 环实例配置模式。

**缺省状态：**默认 ERPS 环实例支持可逆切换机制。

**使用指南：**如果 ERPS 环支持 v1 版本，提示错误“Cann't config non-revertive on the ERPS ring running version 1!”；

如果 ERPS 环支持 v2 版本，配置该 ERPS 环实例支持不可逆切换机制。

**举例：**

配置 ERPS 环 ring1 上的实例 1 支持不可逆切换机制。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#non-revertive

删除 ERPS 环 ring1 上的实例 1 支持不可逆切换机制。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no non-revertive

## 8.6.14 guard-timer <guard-times>

**命令：guard-timer <guard-times>**

**no guard-timer**

**功能：**配置 Guard 定时器。Guard 定时器用于以太网环节点避免依据过时的 R-APS 报文作出错误处理，避免形成封闭环路。在定时器开启时间内，接收到的任何 R-APS 报文（Request/State=“1110”的 R-APS 报文除外）都被丢掉不处理。本命令 no 操作为配置 Guard 定时器为默认值。

**参数：**<guard-times>：时间间隔为 10ms，范围为 10ms～2s。

**命令模式：**ERPS 环实例配置模式。

**缺省状态：**500ms。

**使用指南：**如果定时器没开启，则设置 ERPS 环实例的 Guard 定时器为指定时间；

如果定时器已开启，则立即将 ERPS 环实例的 Guard 定时器设置为配置值，定时器不清零，仍按照最近最后一次配置时间运行，本次配置下一次生效。

**举例：**

配置 ERPS 环 ring1 上实例 1 的 guard timer 为 1s。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)guard-timer 100

配置 ERPS 环 ring1 上实例 1 的 guard 定时器为默认值

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1) no guard-timer

## 8.6.15 holdoff-timer < holdoff-times>

**命令：holdoff –timer <holdoff-times>**

**no holdoff -timer**

**功能：**配置 Holdoff 定时器。Holdoff 定时器用于以太网环节点阻塞故障上报时间。当发生一个新故障或更严重故障时，如果可用的 holdoff timer 不为 0，该故障并不立刻上报给保护切换处理，而是开启 holdoff timer。当定时器超时后，检查开启定时器的链路确认故障是否仍存在，如果仍有故障存在，则上报故障进行保护切换处理，该故障不一定是开启定时器的故障。本命令 no 操作为配置 ERPS 环 Holdoff 定时器为默认值。

**参数：**<holdoff-times>：时间间隔为 1s，取值范围为 0～10s。

**命令模式：**ERPS 环实例配置模式。

**缺省状态：**0s。

**使用指南：**如果定时器没开启，则设置 ERPS 环实例的 Holdoff 定时器为指定时间；

如果定时器已开启，则立即将 ERPS 环实例的 Holdoff 定时器设置为配置值，定时器不清零，仍按照最近最后一次配置时间运行，本次配置下一次生效。

**举例：**

配置 ERPS 环 ring1 上实例 1 的 Holdoff 定时器为 5s。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#holdoff-timer 5

配置 ERPS 环 ring1 上实例 1 的 Holdoff 定时器为默认值。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no holdoff-timer

## 8.6.16 wtr-timer <wtr-times>

**命令：wtr-timer <wtr-times>**

**no wtr-timer**

**功能：**配置 WTR 定时器。WTR 定时器用来避免 RPL 拥有节点由于周期性（间断性）故障引起的频繁保护切换操作。当 RPL Owner 端口收到故障恢复报文后，等待一段时间，以检查链路上其它节点是否仍然存在故障，防止立即阻塞 RPL Owner 端口而引起阻塞点震荡。本命名 no 操作为配置 ERPS 环 WTR 定时器为默认值。

**参数：**<wtr-times>：间隔为 1min，范围为 1～12min。

**命令模式：**ERPS 环实例配置模式。

**缺省状态：**5min。

**使用指南：**如果定时器没开启，则设置 ERPS 环实例的 WTR 定时器为指定时间；

如果定时器已开启，则立即将 ERPS 环实例的 WTR 定时器设置为配置值，定时器不清零，仍按照最近最后一次配置时间运行，本次配置下一次生效。

**举例：**

配置 ERPS 环 ring1 上实例 1 的 WTR 定时器为 10min。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#wtr-timer 10

配置 ERPS 环 ring1 上实例 1 的 WTR 定时器为默认值。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no wtr-timer

## 8.6.17 protected-instance

**命令：protected-instance <instance-list>**

**no protected-instance <instance-list>**

**功能：**配置 ERPS 环实例的保护实例。ERPS 环实例可以保护所有的 MSTP 实例。同一个实例不能被同一个拓扑下的多个 ERPS 环实例引用。在同一 ERPS 环实例下多次执行该命令配置保护实例，结果按多次执行命令的累加生效。本命令 no 操作删除 ERPS 环实例的保护实例。

**参数：**<instance-list>：表示 ERPS 环实例保护的 MSTP 实例列表，形势如：i；j-k。列表中实例的数量不限制。

**命令模式：**ERPS 环实例配置模式。

**缺省状态：**ERPS 环实例不保护任何 MSTP 实例。

**使用指南：**如果输入实例已被其它 ERPS 实例保护，则提示错误“Instance: %d is protected by erps instance: %d on ring: %s!”，第一个%d 为 mstp instance id，第二个%d 为 erps instance id，%s 为 ERPS 环名；

配置 ERPS 环实例的保护实例为指定 MSTP 实例；

检查 ERPS 实例配置是否完整，若完整则激活实例为 active，运行协议。

**举例：**

配置 ERPS 环 ring1 上实例 1 的保护实例为 instance 2。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#protected-instance 2

删除 ERPS 环 ring1 上实例 1 的保护实例 instance 2。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no protected-instance 2

## 8.6.18 raps-mel <level-value>

**命令：raps-mel <level-value>**

**no raps-mel**

**功能：**配置 R-APS channel 的 level。

**参数：**<level-value>：表示 APS 报文的 level 值，范围为：0～7。

**命令模式：**ERPS 环实例配置模式。

**缺省状态：**level 为 7。

**使用指南：**设置 ERPS 环实例的 R-APS channel 的 level 为指定级别。配置成功，则该 ERPS 环实例发出的 R-APS 报文中 mel 字段填充为指定级别，并只允许大于或等于该 level 的 R-APS 报文通过，或提示配置错误。本命令 no 操作为配置 R-APS channel 的 level 为默认值 7。协议报文中的 MEL 字段用于检测当前报文是否能通过。如果 ERPS 环中配置的 MEL 值比故障检测协议中的 MEL 值小，则表明报文等级低而无法通过。实例上所有节点的 level 配置必须一致。

**举例：**

配置 ERPS 环 ring1 上实例 1 的 R-APS channel 允许 level 为 5。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#raps-mel 5

配置 ERPS 环 ring1 上实例 1 的 R-APS channel 允许 level 为 7。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no raps-mel

## 8.6.19 control-vlan <vlan-id>

**命令：control-vlan <vlan-id>**

**no control-vlan**

**功能：**配置 R-APS channel 传输 R-APS 报文的控制 VLAN。在 ERPS 环实例中，该 VLAN 只用来传递 ERPS 协议报文，不用来转发用户业务报文，从而提高了 ERPS 协议的安全性。由用户保证配置唯一性。该 VLAN 在发送 R-APS 报文时作为 vlan tag。实例中所有节点的保护 VLAN 配置必须一致。本命令 no 操作为删除 R-APS channel 传输 RAPS 报文的控制 VLAN。

**参数：**<vlan-id>：表示 R-APS 报文的 vlan id，范围为：2～4094。

**命令模式：**ERPS 环实例配置模式。

**缺省状态：**未配置任何控制 VLAN。

**使用指南：**由用户配置保证满足以下条件：实例中所有节点的保护 VLAN 配置必须一致；控制 vlan 的唯一性；如果实例所在环类型为主环类型，则控制 vlan 和保护 vlan 在同一个实例内；如果实例所在环类型为子环开放类型（open-ring）且是无 R-APS 虚通道方式，则控制 vlan 单独属于一个实例；成员端口属于控制 vlan 和保护 vlan。同时对于配置 control vlan 的处理如下：

a）如果输入 VLAN 不存在，提示错误“Error, VLAN %d does not exist!”，%d 为输入值；

b) 如果该 ERPS 环实例已配置控制 VLAN，提示错误“Control vlan has existed already!”；

c）设置 ERPS 环实例的控制 VLAN 为指定 VLAN；

d）检查 ERPS 实例配置是否完整，若完整则激活实例为 active，运行协议。

**注意：**普通数据 vlan、不同 erps instance 的 control vlan 均不能关联到同一个 MSTI.

**举例：**

配置 ERPS 环 ring1 上实例 1 的控制 vlan 为 vlan10。

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)control-vlan 10
```

删除 ERPS 环 ring1 上实例 1 的控制 vlan。

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)no control-vlan
```

## 8.6.20 forced-switch {port0 | port1}

**命令：forced-switch {port0 | port1}**

**功能：**在 ERPS 环节点的端口上执行强制切换。一个 ERPS 环实例中允许同时存在两个或多个强制切换，但一个环节点上只能存在一个强制切换命令。用户应避免在 ERPS 环实例内使用多个强制切换引发 ERPS 环实例分裂。

**参数：**{port0 | port1}：参数选择，port0 表示强制切换操作要在环节点的 port0 上执行。port1 表示强制切换操作要在环节点的 port1 上执行。

**命令模式：**ERPS 环实例配置模式。

**缺省状态：**ERPS 环实例内无强制切换。

**使用指南：**如果该环支持 version1，提示错误“Doesn't support the command on the ring running version 1!”，否则进入下一步处理；
如果该实例配置不完整，处于 unactive 状态，提示错误“The request is rejected because the ERP instance in unactive state!”，否则进入下一步处理；
如果该环实例的该节点已存在本地强制切换（同一时刻，port0 和 port1 只能有一个处于 local FS 状态），提示错误“The FS request is rejected because an local FS request is present!”，否则进入下一步处理；
如果强制切换命令处于当前最高优先级，block 掉该 ERPS 环指定成员端口（port0 或 port1）上的该 ERPS 环实例的数据通道和 R-APS 通道，并 unblock 该环节点的另一个成员端口；
在强制切换命令处于最高优先级命令期间，在两个环端口（port0 和 port1）上稳定持续发送携带 FS 信息的 R-APS（FS）报文；
接收到 R-APS（FS）报文的环节点，如果本地没有更高优先级请求，应 unblock 所有的 blocked 环端口；
接收到 R-APS（FS）报文的环节点应按照相应的需求执行 flush FDB 操作。
**举例：**
在 ERPS 环 ring1 上的实例 1 的 port0 上进行强制切换操作
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#forced-switch port0

## 8.6.21 manual-switch {port0 | port1}

**命令：manual-switch {port0 | port1}**
**功能：**在 ERPS 环节点的端口上执行手工切换。一个 ERPS 环实例中只允许同时存在一个手工切换，并且前提是 ERPS 环实例内不存在 SF 故障或 FS 命令。
**参数：**{port0 | port1}：参数选择，port0 表示手工切换操作要在环节点的 port0 上执行。port1 表示手工切换操作要在环节点的 port1 上执行。
**命令模式：**ERPS 环实例配置模式。
**缺省状态：**ERPS 环实例内无手动切换。
**使用指南：**如果该环支持 version1，提示错误“Doesn't support the command on the ring running version 1!”，否则进入下一步处理；
如果该实例配置不完整，处于 unactive 状态，提示错误“The request is rejected because the ERP instance in unactive state!”，否则进入下一步处理；
如果该 ERPS 环节点已存在 MS 状态，提示错误“The MS request is rejected because an existing MS request is present!”；
如果该 ERPS 环实例内已存在手工切换，提示错误“The MS request is rejected because an existing FS request is present!”，否则进入下一步处理；
如果该 ERPS 环实例内已存在故障，提示错误“The MS request is rejected because an existing SF is present!”，否则进入下一步处理；

如果手工切换命令处于当前最高优先级，block 掉 ERPS 环指定成员端口（port0 或 port1）上该 ERPS 环实例的数据通道和 R-APS 通道，并 unblock 该环节点的另一个成员端口；
在手工切换命令处于最高优先级命令期间，在两个环端口（port0 和 port1）上稳定持续发送携带 MS 信息的 R-APS（MS）报文；
接收到 R-APS（MS）报文的环节点，如果本地没有更高优先级请求，应 unblock 所有的 blocked 环端口；
接收到 R-APS（MS）报文的环节点应按照相应的需求执行 flush FDB 操作。

**举例：**

在 ERPS 环 ring1 上的实例 1 的 port0 上进行手工切换操作

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#manual-switch port0
```

## 8.6.22 clear command

**命令：clear command**

**功能：**对 ERPS 环节点的成员端口执行清除命令，可以清除本地活动的管理命令：强制切换命令和手工切换命令；也可用于可逆模式下在 WTR 或 WTB 超时之前触发链路切换；还可用于不可逆模式下故障恢复后触发链路从备用链路 RPL 切换回原有链路。后两种情况一般在 rpl owner 节点上执行该命令。

**参数：**无。

**命令模式：**ERPS 环实例配置模式。

**缺省状态：**ERPS 环实例内无清除命令。

**使用指南：**如果该环支持 version1，提示错误“Doesn't support the command on the ring running version 1!”，否则进入下一步处理；
如果该实例配置不完整，处于 unactive 状态，提示错误“The request is rejected because the ERP instance in unactive state!”，否则进入下一步处理；
如果该 ERPS 环实例中存在本地强制切换命令或手工切换命令，则清除切换命令，保持 blocked 成员端口上数据通道和 R-APS 通道的阻塞状态，并在两个成员端口上持续稳定发送 R-APS（NR）报文，直到接收到 R-APS（NR，RB）报文获知 RPL 被 block，或环上发生更高级别的请求（例如 SF）；
如果该 ERPS 环实例中存在本地强制切换命令或手工切换命令，则清除命令后接收到比本地节点 node ID 大的 R-APS（NR）报文，则 unblock 所有无 SF 故障的环端口，停止在两个成员端口上发送 R-APS（NR）报文；
如果 RPL 拥有节点所在 ERPS 环实例为可逆切换模式，并且开启了 WTR 或 WTB 超时，则删除定时器，block 掉 RPL 端口，在两个环端口上发送 R-APS（NR，RB）报文，并执行 flush FDB 操作，提前触发链路切换，否则进入下一步处理；

如果 RPL 拥有节点所在 ERPS 环实例处于不可逆模式下，则 block 掉 RPL 端口，在两个环端口上发送 R-APS（NR，RB）报文，并执行 flush FDB 操作，触发链路从备用链路 RPL 切换回原有链路。

**举例：**

在 ERPS 环 ring1 上的实例 1 上执行 clear 操作。

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#clear command

## 8.6.23 show erps ring {<ring-name> | brief}

**命令：show erps ring {<ring-name> | brief}**

**功能：**读取 ERPS 环信息。

**参数：**<*ring-name*> ：ERPS 环名称，最大字符数为 64，由字母、数字、下划线组成，首尾字符不能为下划线。若不指定，则显示本设备上所有的 ERPS 环。

brief：显示 ERPS 环主要信息。

**命令模式：**特权模式。

**缺省情况：**无。

**举例：**显示所有 ERPS 环的信息。

Switch#show erps ring brief

| Ring-Name | Ring-topo | Port0 | Port1 | Version | Inst-Count |
|---|---|---|---|---|---|
| ring1 | maijor-ring | 1/1/1 | 1/1/2 | V2 | 1 |
| ring2 | open-ring | 1/1/5 | 1/1/6 | V2 | 1 |

| 字段 | 描述 |
|---|---|
| Ring-Name | ERPS环名字，最大字符数为64，由字母、数字、下划线组成，首尾字符不能为下划线。 |
| Ring-topo | ERPS环拓扑模式：major-ring、open-bring |
| Port0 | ERPS环的port0信息 |
| Port1 | ERPS环的port1信息 |
| Version | ERPS环支持的协议版本：V1、V2 |
| Inst-Count | ERPS环上配置的实例总数，范围：1～64 |

显示 ERPS 环 ring1 的信息

Switch#show erps ring ring1

R: RPL Owner

N: RPL Neighbour

C: Common Node

```
---------------------------------------------------------------------------------------------------
R-APS ring topology: open-ring
R-APS Virtual-Channel: with
Port0: Ethernet1/1/1                    Failure-detect type: physical-link-or-cc
Port1: Ethernet1/1/2                    Failure-detect type: physical-link
Instance  Contral  Protected  WTR_Timer  Guard_Timer  Holdoff_Timer  Port0  Port1
ID        Vlan     Instance   (min)      (csec)       (second)
---------------------------------------------------------------------------------------------------
1         10       3          6          100          0              RC
2         20       4          5          500          0              CC
```

| 字段 | 描述 |
|---|---|
| Instance ID | ERPS环实例的id号，范围为1～64 |
| Contral Vlan | 即R-APS通道vlan，封装入R-APS报文tag |
| Protected Instance | ERPS环实例保护的MSTP实例 |
| WTR_Timer | Wait to Restore定时器，范围为1～12min |
| Guard_Timer | Guard定时器，范围为10ms～2s |
| Holdoff_Timer | Holdoff定时器，范围为0～10s |
| Port0 | ERPS环的port0信息 |
| Port1 | ERPS环的port1信息 |
| R-APS ring topology | ERPS环拓扑模式：major-ring、open-bring |
| R-APS Virtual-Channel | 如果为ERPS子环，是否存在R-APS虚通道：with、without |

## 8.6.24 show erps instance [ring <ring-name> [instance <instance-id>]]

**命令：show erps instance [ring <ring-name> [instance <instance-id>]]**

**功能：**显示 ERPS 环实例信息。

**参数：**<*ring-name*>：ERPS 环名称，最大字符数为 64，由字母、数字、下划线组成，首尾字符不能为下划线。若不指定，则显示本设备上所有的 ERPS 环中实例信息。

<instance-id>：ERPS 环实例 ID，范围 1～48。若不指定，则显示指定 ERPS 环上的所有 ERPS 环实例的信息。

**命令模式：**特权模式。

**缺省情况：**无。

**举例：**

显示所有 ERPS 环实例的信息。

```
Switch#show erps instance
ERPS Ring ring1
  Instance 1
  Description: instance1
  Protected Instance: 1
  Revertive mode: non-revertive
  R-APS MEL: 7
  R-APS Virtual-Channel: with
  Control Vlan: 10
  Ring ID:
  Guard Timer (csec): 100
  Holdoff Timer (seconds): 0
  WTR Timer (min): 6
  ----------------------------------------------------------------
  Port          Role              Port-Status
  ----------------------------------------------------------------
  port0         RPL Owner         Blocked
  port1         Common            Forwarding
```

| 字段 | 描述 |
|---|---|
| Description | ERPS环实例的名字 |
| Protected Instance | ERPS环实例保护的MSTP实例 |
| Revertive mode | ERPS环的链路模式：revertive、non-revertive |
| R-APS MEL | R-APS通道的level，封装入R-APS报文 |
| R-APS Virtual-Channel | 如果实例所在ERPS环为子环类型，继承环的R-APS虚通道情况：with、without |
| Ring ID | ERPS环实例发送报文携带的ring-id号，范围为1～64 |
| Contral Vlan | 即R-APS通道vlan，封装入R-APS报文tag |
| WTR_Timer | Wait to Restore定时器，范围为1～12min |
| Guard_Timer | Guard定时器，范围为10ms～2s |
| Holdoff_Timer | Holdoff定时器，范围为0～10s |
| Port | ERPS环的端口信息：port0、port1 |
| Role | ERPS环节点角色：RPL Owner、RPL neighbour、Common |
| Port Status | blocked：端口处于block状态<br>forwarding：端口处于forwarding状态 |

## 8.6.25 show erps status [ring <ring-name> [instance <instance-id>]]

**命令：show erps status [ring <ring-name> [instance <instance-id>]]**

**功能：**显示 ERPS 环实例的状态信息。

**参数：**<*ring-name*> ：ERPS 环名称，最大字符数为 64，由字母、数字、下划线组成，首尾字符不能为下划线。若不指定，则显示本设备上所有的 ERPS 环。

<instance-id>：ERPS 环实例 ID，范围 1～48。若不指定，则显示本设备上的 ERPS 环上所有 ERPS 环实例的状态信息。

**命令模式：**特权模式。

**缺省情况：**无。

**举例：**

显示所有 ERPS 环实例的状态信息。

```
Switch#show erps status
ERPS ring ring1 instance 1 status：
Active：1
Node State：Idle
Time last topology change : Jan 01 00:17:25 2012
---------------------------------------------------------------------------------------------
Port      Interface     Port-Status       Signal-Status     R-RAPS-NodeId       BPR
---------------------------------------------------------------------------------------------
Port0     1/1/1           blocked          Non-failed    00-00-00-00-00-00     0
Port1     1/1/2           forwarding       Non-failed        00-00-00-00-00-00     0
```

| | |
|---|---|
| Active | ERPS环实例的当前所处活动状态：1、0 |
| Node State | ERPS 环实例的当前状态： Idle 、 Protection 、 Forced-switch、Manual-switch、Pending |
| Port Status | blocked：端口处于block状态<br>forwarding：端口处于forwarding状态 |
| Signal Status | ERPS环端口的故障状态：<br>Non-failed：无故障发生<br>Failed：发生故障 |
| Remote R-APS NodeId | ERPS环端口保存的接收到最后一个R-APS中携带的NodeId信息，即mac信息 |
| BPR | ERPS环端口保存的接收到最后一个R-APS中携带的block链路信息，即port0还是port1是blocked的 |
| Time last topology | 表示环拓扑最后一次发生切换的时间 |

| | |
|---|---|
| change | |

## 8.6.26 show erps statistics [ring <ring-name> [instance <instance-id>]]

**命令：show erps statistics [ring <ring-name> [instance <instance-id>]]**

**功能：**显示 ERPS 环实例的统计信息。

**参数：**<ring-name> ：ERPS 环名称，最大字符数为 64，由字母、数字、下划线组成，首尾字符不能为下划线。若不指定，则显示本设备上所有的 ERPS 环的统计信息。

<instance-id>：ERPS 环实例 ID，范围 1～48。若不指定，则显示本设备上的 ERPS 环上所有 ERPS 环实例的统计信息。

**命令模式：**特权模式。

**缺省情况：**无。

**举例：**

显示 ERPS 环实例的统计信息。

```
Switch#show erps statistics ring 1 instance 1
Statistics for ERPS ring ring1 instance 1：
R-APS          Port0(Tx/Rx)          Port1(Tx/Rx)
--------------------------------------------------------------------------
NR                  3/0                  3/0
NR,RB               0/0                  0/0
SF              19129/0              19129/0
MS                  0/0                  0/0
FS                  0/0                  0/0
EVENT               0/0                  0/0
--------------------------------------------------------------------------
TOTOL          19132/0              19132/0
```

## 8.6.27 clear erps statistics [ring <ring-name> [instance <instance-id>]]

**命令：clear erps statistics [ring <ring-name> [instance <instance-id>]]**

**功能：**清除 ERPS 的统计信息。

**参数：**<ring-name> ：ERPS 环名称，最大字符数为 64，由字母、数字、下划线组成，首尾字符不能为下划线。若不指定，则清除本设备上所有的 ERPS 环的统计信息。

<instance-id>：ERPS 环实例 ID，范围 1～48。若不指定，则清除本设备上的 ERPS 环上所有 ERPS 环实例的统计信息。

**命令模式：**特权模式。

**缺省情况：**无。

**举例：**清除 ERPS 环 ring1 上实例 1 的的统计信息。

Switch#clear erps statistics ring 1 instance 1

## 8.6.28 debug erps

**命令：debug erps packet [detail] {send | receive] {[ring <ring-name> [instance <instance-id>]] | [port]}**

**debug erps fsm [ring <ring-name> [instance <instance-id>]]**

**debug erps timer [ring <ring-name> [instance <instance-id>]]**

**no debug eprs**

**功能：**打开 ERPS 的调试信息，本命令的 no 操作为关闭 erps 调试信息。

**参数：**packet：表示打开报文调试信息。

detail：打开报文具体调试信息。

send：打开发送报文调试信息。

received：打开接收报文调试信息。

fsm：表示打开状态机调试信息。

timer：表示打开定时器调试信息。

<ring-name>：ERPS 环名称，最大字符数为 64，由字母、数字、下划线组成，首尾字符不能为下划线。

<instance-id>：配置的 ERPS 环实例 ID。范围 1～48。

**命令模式：**特权用户模式。

**缺省情况：**不显示。

## 8.6.29 debug erps error

**命令：debug erps error**

**no debug erps error**

**功能：**显示 ERPS 的故障信息，本命令 no 操作为关闭显示 erps 故障信息。

**参数：**无。

**命令模式：**特权用户模式。

**缺省情况：**不显示。

## 8.6.30 debug erps event

**命令：debug erps event**

**no debug erps event**

**功能：**显示 ERPS 的事件信息，本命令的 no 操作为关闭显示 erps 事件信息。

**参数：**无。

**命令模式：**特权用户模式。

**缺省情况：**不显示。

## 8.6.31 no debug all

**命令：no debug all**

**功能：**关闭本模块的所有 debug 的信息

**参数：**无。

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**当使用 no debug all 关闭交换机的所有 debug 信息时，该命令对 ERPS 的 debug 信息同样有效，ERPS 的 debug 信息同样关闭。

## 8.6.32 show debugging

**命令：show debugging**

**功能：**打开本模块的所有 debug 信息。

**参数：**无。

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**当使用 show debugging erps 时候显示 debug 信息时本模块支持该命令

# 第 9 章 维护及调试命令

## 9.1 维护及调试

### 9.1.1 clear history all-users

**命令：clear history all-users**

**功能：**清除交换机保存的所有用户命令历史记录。

**命令模式：**特权模式。

**使用指南：**使用该命令可以清除所有用户执行命令的历史纪录。

**举例：**

Switch#clear history all-users

### 9.1.2 history all-users max-length

**命令：history all-users max-length <count>**

**功能：**设置交换机保存的所有用户命令历史记录的最大值。

**命令模式：**全局配置模式。

**参数：**<count>能够保存的命令历史记录数量，取值范围 100-1000

**使用指南：**系统默认最多保存最近 100 条所有用户的命令历史记录，使用该命令可以设置最多记录的命令数量。

**举例：**

Switch(config)#history all-users max-length 500

### 9.1.3 logging executed-commands

**命令：logging executed-commands {enable | disable}**

**功能：**打开或关闭记录用户执行命令的日志开关

**参数：**无。

**命令模式：**全局模式。

**缺省情况：**disable 关闭状态。

**使用指南：**打开开关后，用户在 console，telnet 或 ssh 终端执行的命令会记录日志，所以要配合日志主机命令（logging LOGHOST）一起使用。

**举例：**打开开关，将用户执行的命令发往日志主机（10.1.1.1）

Switch(Config)#logging 10.1.1.1

Switch(Config)#logging executed-commands enable

### 9.1.4 ping

**命令：ping [[src <source-address>] { <*destination-address*> | host <*hostname*> }]**

**功能：**交换机向远端设备发 ICMP 请求包，检测交换机与远端设备之间是否可达。

**参数：*<source-address>*** 为指定 ping 发出的主机源 IP 地址，点分十进制格式；***<destination-address>***为要 ping 的目的主机的 IP 地址，点分十进制格式；***<hostname>***为要 ping 的目的主机名称，最长不超过 64 个字符。

**缺省情况：**发 5 个 ICMP 请求包；包大小为 56 bytes；超时时间为 2 秒。

**命令模式：**特权用户配置模式。

**使用指南：**当用户输入 ping 命令后，直接回车，系统提供给用户一种交互式的配置方式，用户可以自己定义 ping 的各项参数值。

**举例：**

例 1：使用 ping 程序的缺省参数。

Switch#ping 10.1.128.160

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds.

...!!

Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms

上面的例子表示，交换机 ping 某一 IP 地址为 10.1.128.160 的设备，前三个 ICMP 请求包在缺省超时时间 2 秒内没有收到相应的 ICMP 回应包，即没有 ping 通，而后两个包 ping 通了，成功率为 40%。交换机用“.”表示 ping 失败，链路不可达；用“！”表示 ping 成功，链路可达。

例 2：使用 ping 程序的源地址设置参数，其他参数均为缺省。

Switch#ping src 10.1.128.161 10.1.128.160

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 10.1.128.160, using source address 10.1.128.161, timeout is 2 seconds.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

上面的例子表示，交换机 ping 使用 10.1.128.161 作为 ping 发出 ICMP 请求报文的源地址，ping 的目的设备 IP 地址为 10.1.128.160，五个 ICMP 请求包均收到相应的 ICMP 回应包，ping 成功率为 100%。交换机用“.”表示 ping 失败，链路不可达；用“！”表示 ping 成功，链路可达。

例 3：使用 ping 程序提供的手段修改 ping 参数。

Switch#ping

VRF name：

Target IP address：10.1.128.160

Use source address option[n]: y

Source IP address: 10.1.128.161

Repeat count [5]：100

Datagram size in byte [56]：1000

Timeout in milli-seconds [2000]：500

Extended commands [n]：n

| 显示信息 | 解释 |
|---|---|
| VRF name | 选择 VRF，如果没有启动 MPLS 协议，该项为空 |
| Target IP address： | 目标设备的 IP 地址； |
| Use source address option[n] | 是否使用源地址设置选项； |
| Source IP address | 指定 ping 使用的源 IP 地址； |
| Repeat count [5] | 发包的数目，默认为 5； |
| Datagram size in byte [56] | ICMP 包的大小，默认为 56； |
| Timeout in milli-seconds [2000]： | 超时时间，单位为毫秒，默认为 2 秒； |
| Extended commands [n]： | 是否需要改变其他的选项； |

## 9.1.5 ping6

**命 令：** **ping6 [*<dst-ipv6-address>* | host *<hostname>* | src *< src-ipv6-address >* {*<dst-ipv6-address >* | host *<hostname>*} ]**

**功能：**验证网络的可达性。

**参数：** ***<dst- ipv6-address >***参数为目的 IPv6 地址，***< src-ipv6-address >***为源 IPv6 地址，***<hostname>***是为远端主机的主机名，最长不超过 64 个字符。

**缺省情况：**发 5 个 ICMP6 请求包；包大小为 56 bytes；超时时间为 2 秒。

**命令模式：**一般用户模式。

**使用指南：** ping6 后直接跟 IPv6 地址为默认情况，ping6 功能可以根据用户的选择对 ping 包的参数进行设置，当 ipv6-address 为本地链路地址时，需要指定 vlan 接口名。当指定源 IPv6 地址时，发出的 icmp6 请求包将使用指定的源 IPv6 地址作为 ping 包的源地址。

**举例：**

(1) 使用 ping6 程序的缺省参数。

Switch>ping6 2001:1:2::4

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 2001:1:2::4, timeout is 2 seconds.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/320/1600 ms

(2) 使用 ping6 时，指定源 IPv6 地址

switch>ping6 src 2001:1:2::3 2001:1:2::4

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 2001:1:2::4, using src address 2001:1:2::3, timeout is 2 seconds.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

(3) 使用 ping6 程序提供的手段修改 ping6 参数。

switch>ping6

Target IPv6 address:fe80::2d0:59ff:feb8:3b27

Output Interface: vlan1

Use source address option[n]:y

Source IPv6 address: fe80::203:fff:fe0b:16e3

Repeat count [5]:

Datagram size in byte [56]:

Timeout in milli-seconds [2000]:

Extended commands [n]:

Type ^c to abort.

Sending 5 56-byte ICMP Echos to fe80::2d0:59ff:feb8:3b27, using src address fe80::203:fff:fe0b:16e3, timeout is 2 seconds.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms

| 显示内容 | 解释 |
|---|---|
| ping6 | 执行 ping6 功能 |
| Target IPv6 address | 目的 IPv6 地址 |
| Output Interface | Vlan 接口名，当目的地址为本地链路地址时需指定 |
| Use source IPv6 address [n]: | 使用源 IPv6 地址，默认不使用 |
| Source IPv6 address | 源 IPv6 地址 |
| Repeat count[5] | 发送的 ping 包个数，默认值为 5 |
| Datagram size in byte[56] | Ping 包的大小，默认值为 56 |
| Timeout in milli-seconds[2000] | 允许的时间延迟，默认值为 2 秒 |
| Extended commands[n] | 扩展参数的设置，默认不使用 |
| ! | 表明网络可达 |
| . | 表明网络不可达 |
| Success rate is 100 percent (8/8), round-trip min/avg/max = 1/1/1 ms | 统计信息，说明 ping 包成功到达的比率为 100%，无丢包 |

## 9.1.6 show boot-files

**命令：show boot-files**

**功能：** 显示交换机启动的第一、第二 IMG 文件和 CFG 文件。

**命令模式：** 特权和配置模式。

**使用指南：** 执行此命令后，会显示相应存储设备中保存的 IMG 文件启动顺序以及当前是利用哪个 IMG 文件启动、存储设备中保存的 CFG 文件的配置信息和当前启动的 CFG 文件。

**举例：** 显示交换机启动的第一、第二 IMG 文件和 CFG 文件。

```
Switch# show boot-files
Booted files on switch
The primary img file at the next boot time:      flash:/nos.img
The backup img file at the next boot time:       flash:/nos.img
Current booted img file:                         flash:/nos.img

The startup-config file at the next boot time:   flash:/startup.cfg
Current booted startup-config file:              flash:/startup.cfg
```

如果配置的下一次启动的 CFG 文件为 NULL，则上述 CFG 部分显示如下：

```
The startup-config file at the next boot time：NULL
Current booted startup-config file：flash:/startup.cfg
```

## 9.1.7 show debugging

**命令：show debugging {bgp | dvmrp | igmp | ipv6 | mld | nsm | ospf | other | pim | rip | spanning-tree | vrrp}**

**功能：**显示调试开关的状态。

**使用指南：**如果用户需要查看调试开关的状态，可以执行 **show debugging** 命令。

**命令模式：**特权和配置模式。

**举例：**查看 ospf 调试开关当前的状态。

```
Switch#show debugging ospf
OSPF debugging status:
  OSPF all IFSM debugging is on
  OSPF packet Hello detail debugging is on
  OSPF packet Database Description detail debugging is on
  OSPF packet Link State Request detail debugging is on
  OSPF packet Link State Update detail debugging is on
  OSPF packet Link State Acknowledgment detail debugging is on
  OSPF all LSA debugging is on
  OSPF all NSM debugging is on
  OSPF all events debugging is on
  OSPF all route calculation debugging is on
Switch#
```

**相关命令：debug**

## 9.1.8 show fan

**命令：show fan**

**功能：** 显示交换机风扇情况。

**参数：** 无。

**命令模式：** 各种配置模式

**使用指南：** 该命令用于监测交换机风扇情况。

**举例：** 显示交换机当前风扇情况。

```
Switch(Config)#show fan
Fan board information:
Fan No      Status          Speed
1             Normal          High
2             Normal          High
3             Normal          High
4             Normal          High
```

## 9.1.9 show flash

**命令：show flash**

**功能：**显示保存在 flash 中的文件及大小。

**命令模式：**特权和配置模式。

**举例：**查看 flash 中文件及大小。

```
Switch#show flash
boot.rom                                329,828 1900-01-01 00:00:00 --SH
boot.conf                                    94 1900-01-01 00:00:00 --SH
nos.img                               2,449,496 1980-01-01 00:01:06 ----
startup-config                            2,064 1980-01-01 00:30:12 ----
```

## 9.1.10 show history

**命令：show history**

**功能：**显示用户最近输入的历史命令。

**命令模式：**特权和配置模式。

**使用指南：**系统最多保存 20 条用户最近输入的历史命令，用户在输入命令时可以用上下光标键或其等价键（ctrl+p 和 ctrl+n）来访问历史命令。

**举例：**

```
Switch#show history
```

enable

config

interface ethernet 1/1/3

enable

show flash

show ftp

## 9.1.11 show history all-users

**命令：show history all-users [detail]**

**功能：**显示所有用户最近输入的历史命令。

**命令模式：**特权和配置模式。

**参数：**[detail]显示执行命令的用户名称，当用户通过 telnet 或者 ssh 登录执行命令时，显示用户登录的 IP 地址信息。

**使用指南：**该命令用于显示所有用户最近输入的历史命令，包括执行该命令的时间、用户的登录类型、执行的命令等信息。

注意：执行该命令的用户只能看到权限不高于自己的用户的历史命令。

**举例：**

Switch(config)#show history all-users detail

| Time | Type | User | Command |
|---|---|---|---|
| 0w 0d 0h 2m | Telnet/SSH | admin | show history all-users detail 192.168.1.2:1419 |
| 0w 0d 0h 1m | Telnet/SSH | admin | show history all-users 192.168.1.2:1419 |
| 0w 0d 0h 1m | Console | Null | show history all-users |
| 0w 0d 0h 1m | Console | Null | end |
| 0w 0d 0h 1m | Console | Null | ip address 192.168.1.1 255.255.255.0 |
| 0w 0d 0h 0m | Console | Null | in v 1 |
| 0w 0d 0h 0m | Console | Null | telnet-server enable |

## 9.1.12 show memory usage

**命令：show memory usage**

**功能：**显示内存使用情况。

**参数：**无。

**命令模式：**特权和配置模式。

**使用指南：**本命令用于调试交换机。查看交换机当前内存使用情况。

**举例：**

Switch#show memory usage

The memory total 2014 MB, free 1939800064 bytes, usage is 8.15%

## 9.1.13 show running-config

**命令：show running-config**

**功能：**显示当前运行状态下生效的交换机参数配置。

**缺省情况：**对于正在生效的配置参数，如果与缺省工作参数相同，则不显示。

**命令模式：**特权和配置模式。

**使用指南：**当用户完成一组配置后，需要验证是否配置正确，则可以执行 show running-config 命令来查看当前生效的参数。

**举例：**

Switch#show running-config

## 9.1.14 show running-config current-mode

**命令：show running-config current-mode**

**功能：**显示当前模式下的配置。

**命令模式：**所有配置模式。

**缺省情况：**无。

**使用指南：**进入任何一种配置模式，在该模式下输入本命令，能够显示当前模式下的所有配置。

**举例：**

Switch(config-if-ethernet1/1/1)#show run c

!

Interface Ethernet1/1/1

switchport access vlan 2

!

## 9.1.15 show startup-config

**命令： show startup-config**

**功能：**显示当前运行状态下写在 Flash Memory 中的交换机参数配置，通常也是交换机下次上电启动时所用的配置文件。

**缺省情况：** 从 Flash 中读出的配置参数，如果与缺省工作参数相同，则不显示。

**命令模式：**特权和配置模式。

**使用指南：show running-config** 和 **show startup-config** 命令的区别在于，当用户完成一组配置之后，通过 **show running-config** 可以看到配置增加了，而通过 **show startup-config** 却看不出任何的配置。但若用户通过 **write** 命令，将当前生效的配置保存到 Flash Memory 中时，**show running-config** 的显示与 **show startup-config** 的显示结果一致。

## 9.1.16 show switchport interface

**命令：show switchport interface [ethernet *<IFNAME>*]**

**功能：**显示交换机端口的 VLAN 端口模式和所属 VLAN 号及交换机的 Trunk 端口信息。

**参数：*<IFNAME>***为端口号。

**命令模式：**特权和配置模式。

**举例：**显示端口 ethernet 1/1/1 的 VLAN 信息。

Switch#show switchport interface ethernet 1/1/1

Ethernet1/1/1

Type :Universal

Mac addr num :No Limit

Mode :Trunk

Port VID :1

Trunk allowed Vlan :ALL

| 显示内容 | 描述 |
|---|---|
| Ethernet1/1/1 | 对应的以太网接口号； |
| Type | 当前接口的类型； |
| Mac addr num | 当前接口具备学习 MAC 地址的数量； |
| Mode :Trunk | 当前接口的 VLAN 模式； |
| Port VID :1 | 当前接口从属的 VLAN 号； |
| Trunk allowed Vlan :ALL | Trunk 允许通过的 VLAN。 |

## 9.1.17 show tcp

**命令：show tcp**

**功能：**显示当前与交换机建立的 TCP 连接情况。

**命令模式：**特权和配置模式。

**举例：**

Switch#show tcp

| LocalAddress | LocalPort | ForeignAddress | ForeignPort | State |
|---|---|---|---|---|
| 0.0.0.0 | 23 | 0.0.0.0 | 0 | LISTEN |
| 0.0.0.0 | 80 | 0.0.0.0 | 0 | LISTEN |

| 显示内容 | 描述 |
|---|---|
| LocalAddress | tcp 连接的本地地址 |
| LocalPort | tcp 连接的本地端口号 |
| ForeignAddress | tcp 连接的对端的地址 |
| ForeignPort | tcp 连接的对端的端口号 |
| State | tcp 连接所处的当前的状态 |

## 9.1.18 show tcp ipv6

**命令：show tcp *ipv6***

**功能：**显示当前与交换机建立的 TCP 连接情况。

**命令模式：**特权和配置模式

**举例：**

Switch#show tcp ipv6

LocalAddress LocalPort RemoteAddress RemotePort State IF VRF

:: *80* :: 0 LISTEN 0 0

:: 23 :: 0 LISTEN 0 0

| 显示内容 | 描述 |
|---|---|
| LocalAddress | TCP 连接的本地 IPv6 地址 |
| LocalPort | TCP 连接的本地端口号 |
| RemoteAddress | TCP 连接的对端 IPv6 地址 |
| RemotePort | TCP 连接的对端端口号 |
| State | TCP 连接所处的当前状态 |
| IF | TCP 连接的本地端口索引 |
| VRF | 虚拟路由转发实例 |

## 9.1.19 show telnet login

**命令：show telnet login**

**功能：**显示当前与交换机建立起 Telnet 连接的 Telnet 客户端的信息。

**命令模式：**特权和配置模式。

**使用指南：**本命令用以查看当前登录到系统的远程用户的信息。

**举例：**

Switch#show telnet login

Authenticate login by local.

Login user:

aa

## 9.1.20 show temperature

**命令：show temperature**

**功能：** 显示交换机 CPU 当前温度。

**参数：** 无。

**命令模式：** 各种配置模式

**使用指南：** 该命令用于监测交换机 CPU 的温度。

**举例：** 显示交换机 CPU 当前温度。

Switch(Config)#show temperature

Temperature: 47.0625 ℃

## 9.1.21 show tech-support

**命令：show tech-support**

**功能：**显示交换机运行的信息和各任务的状态，技术支持人员利用该命令，诊断交换机的运行是否正常。

**命令模式：**特权和配置模式。

**使用指南：**在交换机出现运行故障时，可以利用该命令获取相关信息，诊断故障原因。

**举例：**

Switch#show tech-support

## 9.1.22 show udp

**命令：show udp**

**功能：**显示当前与交换机建立的 UDP 连接情况。

**命令模式：**特权和配置模式。

**举例：**

Switch#show udp

| LocalAddress | LocalPort | ForeignAddress | ForeignPort | State |
|---|---|---|---|---|
| 0.0.0.0 | 161 | 0.0.0.0 | 0 | CLOSED |
| 0.0.0.0 | 123 | 0.0.0.0 | 0 | CLOSED |
| 0.0.0.0 | 1985 | 0.0.0.0 | 0 | CLOSED |

| 显示内容 | 描述 |
|---|---|
| LocalAddress | udp 连接的本地地址 |
| LocalPort | udp 连接的本地段口号 |
| ForeignAddress | udp 连接的对端的地址 |
| ForeignPort | udp 连接的对端的端口号 |
| State | udp 连接所处的当前的状态 |

## 9.1.23 show udp ipv6

**命令：show udp *ipv6***

**功能：**显示当前与交换机建立的UDP连接情况。

**命令模式：**特权和配置模式

**举例：**

| LocalAddress | LocalPort | RemoteAddress | RemotePort | State |
|---|---|---|---|---|
| :: | 69 | :: | 0 | CLOSED |
| :: | 1208 | :: | 0 | CLOSED |

| 显示内容 | 描述 |
|---|---|
| LocalAddress | UDP 连接的本地 IPv6 地址 |
| LocalPort | UDP 连接的本地端口号 |
| RemoteAddress | UDP 连接的对端 IPv6 地址 |
| RemotePort | UDP 连接的对端端口号 |
| State | UDP 连接所处的当前状态 |

## 9.1.24 show version

**命令：show version**

**功能：**显示交换机版本信息。

**命令模式：**特权和配置模式。

**使用指南：**通过使用此命令来查看交换机的版本信息，包括硬件版本和软件版本信息。

**举例：**

Switch#show version

## 9.1.25 traceroute

**命令：traceroute [source <*ipv4-addr*> ] vrf <vrfname> { <*ip-addr*> | host <*hostname*> |[ethernet target-mac <mac-address>| target-mep <1-4094> domain WORD server (WORD) (number <0-65535>) |(pvlan <1-4094 >) fdb-only|source|ttl] } [hops <*hops*> ] [timeout <*timeout*> ]**

**功能：**本命令用于测试数据包从发送设备到目的地设备所经过的网关，检测网络是否可达，定位网络故障所在。

**参数：*<ipv4-addr>***是指定的 IPv4 源地址，点分十进制格式；***<ip-addr>***是目的主机的 IP 地址，点分十进制格式；***<hostname>***是为远端主机的主机名；***<hops>***为 traceroute 的最大经过的网关数目，取值范围 1-255；***<timeout>***为数据包超时时间，单位为毫秒，取值范围 100~10000,<vrfname> 为 vrf 实例名。

**缺省情况：**数据包最多经过的网关数目缺省为 30，超时时间为 2000 毫秒。

**命令模式：**特权用户配置模式。

**使用指南：**traceroute 一般用于定位目的网络不可达时的故障所在。

**相关命令：ip host**

## 9.1.26 traceroute6

**命令：traceroute6 [source <*addr*>] {<*ipv6-addr*> | host <*hostname*> } [hops <*hops*>] [timeout <*timeout*> ]**

**功能：**本命令用于测试数据包从发送设备到目的地设备所经过的网关，检测网络是否可达，定位网络故障所在。

**参数：*<addr>***是指定的 IPv6 源地址，冒号分割十六进制格式；***<ipv6-addr>***是目的主机的 IPv6 地址，冒号分割十六进制格式；***<hostname>***是为远端主机的主机名；***<hops>***为 traceroute6 的最大经过的网关数目，取值范围 1-255；***<timeout>***为数据包超时时间，单位为毫秒，取值范围 100~10000。

**缺省情况：**数据包最多经过的网关数目缺省为 30，超时时间为 2000 毫秒。

**命令模式：**特权用户配置模式。

**使用指南：**traceroute6 一般用于定位目的网络不可达时的故障所在。

**举例：**

Switch#traceroute6 2004:1:2:3::4

**相关命令：ipv6 host**

# 9.2 Logging

## 9.2.1 logging executed-commands

**命令： logging executed-commands {enable | disable}**

**功能：** 打开或关闭记录用户执行命令的日志开关

**参数：** 无。

**命令模式：** 全局模式。

**缺省情况：** disable 关闭状态。

**使用指南：** 打开开关后，用户在 console，telnet 或 ssh 终端执行的命令会记录日志。所以它应该与 logging loghost 命令一起使用。

**举例：** 启用命令并将用户执行的命令发送到日志主机（10.1.1.1）

Switch(Config)#logging 10.1.1.1

Switch(Config)#logging executed-commands enable

## 9.2.2 show logging executed-commands state

**命令： show logging executed-commands state**

**功能：**显示用于记录用户执行命令的日志开关状态

**参数：**无。

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**使用此 show 命令可以显示开关是 enable 或 disable。

**举例：**

Switch#show logging executed-commands state

Logging executed command state is enable

# 9.3 定时重启交换机

## 9.3.1 reload after

**命令：reload after {[*<HH:MM:SS>*] [days <*days*>]}**

**功能：**定时热启动交换机。

**参数：***<HH:MM:SS >*为配置时间，HH（小时）取值范围为 0~23，MM（分钟）和 SS（秒）取值范围为 0~59。

<*days*> 配置的天数，单位为天，取值范围 1-30。

时间和天数可以同时配置，也可仅配置时间或仅配置天数。

**命令模式：**特权用户配置模式。

**使用指南：**用户可以通过本命令，在不关闭电源的情况下，经过指定的时间以后，重新启动交换机。本命令一般用于版本升级。当升级完版本以后，可以不立刻重启交换机，而是指定经过一段时间以后再重启交换机。本命令没有配置保留，只能一次性起作用。配置该命令后，当用户通过 telnet 登录交换机时，会向该用户提示交换机重启信息。

**举例：**设置交换机在 2 天 10 小时 0 分 1 秒以后自动重启。

Switch#reload after 10:00:01 days 2

Process with reboot after? [Y/N] y

**相关命令：reload，reload cancel，show reload**

## 9.3.2 reload cancel

**命令：reload cancel**

**功能：**取消定时热启动交换机。

**参数：**无。

**命令模式：**特权用户配置模式。

**使用指南：**用户可以通过本命令，取消配置指定时间以后重新启动交换机，即取消 reload after 命令配置。本命令没有配置保留。

**举例：**设置取消交换机在指定时间以后自动重启。

Switch#reload cancel

Reload cancel successful.

**相关命令：reload，reload after，show reload**

### 9.3.3 show reload

**命令：show reload**

**功能：**显示用户 reload after 命令的配置情况。

**参数：**无。

**命令模式：**特权和配置模式。

**使用指南：**用户可以通过本命令，查看 reload after 命令的情况配置，同时可以查看距离交换机重启还剩多少时间。

**举例：**查看 reload after 命令配置情况。下例中，用户配置交换机在 10 小时 0 分 1 秒以后重启，目前距离交换机重启还剩 9 小时 59 分 48 秒。

```
Switch#show reload
 The original reload after configuration is 10:00:01.
 System will be rebooted after 09:59:48 from now.
```

**相关命令：reload，reload after，reload cancel**

## 9.4 CPU 收发报文调试

### 9.4.1 clear cpu-rx-stat protocol

**命令：clear cpu-rx-stat protocol [ <protocol-type> ]**

**功能：**将某类型协议报文的收包统计清 0。

**参数：*<protocol-type>*** 为协议报文类型，**包括 dot1x，stp，snmp，arp，telnet，http，dhcp，igmp，ssh，bgp，bgp4plus，rip，ripng，ospf，ospfv3，pim，pimv6， unknown-mcast，unknow-mcast6，mld**

**命令模式：**特权用户配置模式。

**使用指南：**本命令会清空协议收包的统计信息，使接收到的协议报文重新统计，主要是在调试诊断时使用，建议在厂商技术人员指导下使用。

**举例：**将 ARP 报文的收包统计清 0。

```
Switch#clear cpu-rx-stat protocol arp
```

### 9.4.2 cpu-rx-limitnotify enable interval

**命令： cpu-rx-limitnotify enable interval <interval>**

**功能：**启用 **cpu-rx-limitnotify** 功能，并指定触发的时间间隔。no 命令禁用 **cpu-rx-limitnotify** 功能

**参数：** **<interval>** 为提示间隔，取值范围<180-86400>秒

**命令模式：**配置模式。

**使用指南：**此命令用于诊断交换机接收到的协议信息。请在制造商技术人员的指导下使用。

**举例：**配置 cpu 收报限速 300s 定期提示。

Switch(config)#cpu-rx-limitnotify enable interval 300

## 9.4.3 cpu-rx-limitnotify protocol (all|WORD)(enable|disable)

本型号交换机不支持此命令。

## 9.4.4 cpu-rx-ratelimit channel

本型号交换机不支持该命令。

## 9.4.5 cpu-rx-ratelimit enhanced

本型号交换机不支持该命令。

## 9.4.6 cpu-rx-ratelimit protocol

**命令：** **cpu-rx-ratelimit protocol *<protocol-type> <packets>***

**no cpu-rx-ratelimit *protocol* <protocol-type>**

**功能：**设置协议报文每秒钟允许送 CPU 的个数，本命令的 no 操作为恢复协议报文每秒允许送 CPU 的个数为默认值。

**参数：** **<protocol-type>** 协议报文类型，包括 dot1x，stp，snmp，arp，telnet，http，dhcp，igmp，ssh，bgp，bgp4plus，rip，ripng，ospf，ospfv3，pim，pimv6， unknown-mcast，unknow-mcast6，mld；***<packets>***为每秒钟允许送 CPU 的数量，参数为 32, 128, 256, 512, 768 and 2000 pps。

**命令模式：**全局配置模式。

**缺省情况：**缺省情况下各类型协议都设置有默认值。

**使用指南：**本命令设置的协议限速值会影响交换机 CPU 接收报文的情况，建议在厂商技术人员指导下使用。

**举例：**设置 ARP 协议报文的限速值为 256pps。

Switch(config)#cpu-rx-ratelimit protocol arp 256

## 9.4.7 cpu-rx-ratelimit queue-length

本型号交换机不支持该命令。

## 9.4.8 cpu-rx-ratelimit total

**命令： cpu-rx-ratelimit total *<packets>***

**no cpu-rx-ratelimit total**

**功能：** 设置 cpu 接收报文的总限速，本命令的 no 操作为将 cpu 接收报文的限速值恢复为默认值。

**参数：** ***<packets>*** 为每秒钟允许送 cpu 的数据包个数。

**命令模式：** 全局配置模式。

**缺省情况：**默认情况下，CPU 的限速值为 1200pps。

**使用指南：** 本命令设置的限速值会影响交换机 CPU 接收报文的情况，建议在厂商技术人员指导下使用。

**举例：** 设置 cpu 接收报文的总限速为 1500pps。

Switch(config)#cpu-rx-ratelimit total 1500

## 9.4.9 debug driver

**命令： debug driver {receive | send} [interface {*<interface-name>* | all}] [protocol {*<protocol-type>* | discard | all}] [detail]**

**no debug driver {receive | send}**

**功能：**打开指定端口指定类型报文驱动接收或发送信息的显示，本命令的 no 操作为关闭驱动收发包信息的显示。

**参数：receive | send**：显示收包、发包信息；

**interface {*<interface-list>*| all}**：interface-list 是以太网端口号，只能输入一个端口，all 表示所有端口，如果不输入参数，则后面的参数也不输入，表示显示所有端口所有类型的协议报文的简要信息。

**protocol {<protocol-type> | discard | all}**：protocol-type表示协议类型，可设置为snmp、telnet、http、dhcp、igmp、hsrp、arp、bgp、rip、ospf、pim、ssh、vrrp、ripng、ospfv3、pimv6、icmpv6、bgp4plus、unknown-mcast、unknown-mcast6、ttl0-2cpu、isis、dot1x、gvrp、stp、lacp、cluster、mld、vrrpv3、ra、uldp、lldp、eapou，all代表所有类型的协议，discard表示所有在驱动收包处理中丢掉的报文,如果不输入参数，则后面的参数也不输入，显示所有类型报文的简要信息；

**detail**：显示详细信息，不输入参数，显示简要信息，简要信息包括报文类型，所属 vlan，进来的端口，收包原因，报文长度，源 mac，目的 mac；详细信息包括简要信息，并将报文的前 64 个字节显示出来。

**命令模式：**特权用户配置模式。

**使用指南：**本命令打开交换机 CPU 的收包调试，用于交换机的调试诊断，建议在厂商技术人员指导下使用。

**举例：**打开驱动接收报文调试开关。

Switch#debug driver receive

## 9.4.10 protocol filter

**命令：protocol filter {protocol-type}**

**no Protocol filter {protocol-type}**

**功能：** 开启/关闭相应的具名协议报文的处理。

**参数：** ***<protocol-type>***代表协议类型，可以设置为

{arp|bgp|dhcp|dhcpv6|hsrp|http|igmp|ip|ldp|mpls|ospf|pim|rip|snmp|telnet|vrrp}

**命令模式：** 特权用户配置模式

**使用指南：** 本命令打开或关闭相应的具名协议的处理，用于交换机的调试诊断，建议在厂商技术人员指导下使用。

**举例：** 打开 arp 协议报文的处理

Switch#protocol filter arp

### 9.4.11 show cpu-rx protocol

**命令：show cpu-rx protocol [ *<protocol-type>* ]**

**功能：**显示本机指定类型报文的接收信息。

**参数：*<protocol-type>***数据报文的类型，不输入参数则显示所有的报文统计。

**命令模式：**特权和配置模式。

**使用指南：**本命令用于诊断交换机接收到的各协议情况，建议在厂商技术人员指导下使用。

**举例：** 显示 arp 报文的接收统计信息。

**Switch#**show cpu-rx protocol arp

| Type | Rate-limit | TotPkts | CurState |
|---|---|---|---|
| arp | 500 | 3 | allowed |

## 9.5 info-center

### 9.5.1 info-center enable

**命令：info-center enable**

**no info-center enable**

**功能：**该命令负责开启信息中心输出的功能。无论是否开启输出功能，信息中心仍然可以正常配置。也就是说，该命令是信息中心控制的信息输出的一个开关。去使能可以关闭正在输出的信息，使能后原有的配置仍然生效。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**缺省开启。

**使用指南：**该命令负责开启信息中心输出的功能，默认开启状态。

**举例：**

Switch(config)#info-center enable

Switch(config)#no info-center enable

## 9.5.2 info-center prefix

**命令：info-center (console | logbuffer | monitor | trapbuffer) prefix (on|off)**

**info-center (logfile <1-4> | loghost <1-8>) prefix (on|off) (member <1-4> |)**

**功能：**打开或者关闭某个方向的 log 记录前缀， 默认所有方向的 prefix 都是 on 的。

**参数：**

| 参数 | 描述 |
|---|---|
| console \| logbuffer \| monitor \| logfile <1-4> \| loghost <1-8> \| trapbuffer | 表示需要配置的输出方向 |
| on\|off | 携带 log 记录前缀开关 |
| member <1-4> | member 成员号 |

**命令模式：**全局配置模式。

**缺省情况：**缺省开启。

**使用指南：**无

**举例：**

Switch(config)# info-center console prefix on

## 9.5.3 info-center match

**命令：info-center (console | logbuffer | monitor | trapbuffer) match level (emergencies | alerts | critical | errors | warnings | notifications | informational | debugging) (exact |) (keyword WORD |)**

**info-center (logfile <1-4> | loghost <1-8>) match level (emergencies | alerts | critical | errors | warnings | notifications | informational | debugging) (exact |) (keyword WORD |) (member <1-4> |)**

**no info-center (console | logbuffer | monitor | trapbuffer) match**

**no info-center (logfile <1-4> | loghost <1-8>) match (member <1-4> |)**

**功能：**配置输出方向 log 匹配条件。

**参数：**

| 参数 | 描述 |
|---|---|
| console \| logbuffer \| monitor | 表示需要配置的输出方向 |

| | |
|---|---|
| \| logfile <1-4> \| loghost <1-8> \| trapbuffer | |
| emergencies \| alerts \| critical \| errors \| warnings \| notifications \| informational \| debugging | 配置匹配的信息等级 |
| exact | 严格等级匹配 |
| keyword WORD | 使用正则表达式作为刷选条件 |
| member <1-4> | member 成员号 |

**命令模式：**全局配置模式。

**缺省情况：**默认匹配缺省等级。

**使用指南：**

这个命令设置各个方向上的 log 匹配条件，match 后面可以直接配置允许哪些等级的 log 进入，也可以配置 exact 严格等级匹配。所谓的严格匹配，就是设置什么等级，就只匹配哪个等级，如果不带 exact，按 emergencies < alerts < critical < errors < warnings < notifications < informational < debugging 的方式进行匹配，也可以用 keyword 后面带正则表达式进行匹配。

no 命令取消对应输出方向的匹配条件。

**举例：**

Sysname(config)#info-center console match level warnings exact

Sysname(config)#info-center logfile 1 match level errors member 1

## 9.5.4 info-center output-enable

**命令：info-center (console | logbuffer | monitor | trapbuffer) output-enable**

**info-center (logfile <1-4> | loghost <1-8>) output-enable (member <1-4> |)**

**no info-center (console | logbuffer | monitor | trapbuffer) output-enable**

**no info-center (logfile <1-4> | loghost <1-8>) output-enable (member <1-4> |)**

**功能：**配置输出方向使能。

**参数：**

| 参数 | 描述 |
|---|---|
| console \| logbuffer \| monitor \| logfile <1-4> \| loghost <1-8> \| trapbuffer | 表示需要配置的输出方向 |
| member <1-4> | member 成员号 |

**命令模式：**全局配置模式

**缺省情况：**缺省未配置

**使用指南：**

该命令配置某个输出方向的使能，注意该命令只是使能/去使能，并不会影响匹配条件或者其它配置，当该方向重新使能之后，先前设置的匹配仍然有效。

注意，console、monitor 、logbuffer、trapbuffer 和 logfile 4 默认都是使能，其他默认是去使能的。这里 logfile 4 作为缺省日志文件的输出方向，所以其输出默认也是使能的。

**举例：**

Sysname(config)#info-center monitor output-enable

Sysname(config)#info-center logfile 1 output-enable member 1

## 9.5.5 info-center record-cmd

**命令：info-center (logbuffer | logfile <1-4> | loghost <1-8>) record-cmd**

**no info-center (logbuffer | logfile <1-4> | loghost <1-8>) record-cmd**

**功能：**配置记录用户操作命令。

**参数：**

| 参数 | 描述 |
|---|---|
| logbuffer \| logfile <1-4> \| loghost <1-8> | 表示需要配置的输出方向 |

**命令模式：**全局配置模式

**缺省情况：**缺省未配置

**使用指南：**

在该方向上记录用户操作命令。注意记录命令行操作不受该方向上 match 条件的约束，只要使能该命令，就能够记录。默认情况下不记录用户操作命令。

**举例：**

Sysname(config)#info-center logbuffer record-cmd

## 9.5.6 info-center loghost

**命令：info-center loghost <1-8> config (vrf <vrfname>A.B.C.D | X:X::X:X) facility (local0|local1|local2|local3|local4|local5|local6|local7) (member <1-16> |)**

**no info-center loghost <1-8> config (member <1-16> |)**

**功能：**配置日志主机的 ip 和等级。

**参数：**

| 参数 | 描述 |
|---|---|
| loghost <1-8> | 表示配置 loghost 输出方向 |
| A.B.C.D \| X:X::X:X | 日志主机 IP 地址 |

| | |
|---|---|
| local0\|local1\|local2\|local3\|local4\|local5\|local6\|local7 | 可选的等级 local0~7 |
| member <1-16> | member 成员号 |
| **<vrfname>** | vrf 实例名 |

**命令模式：**全局配置模式

**缺省情况：**缺省未配置

**使用指南：**

该命令配置 loghost 的 ip 地址和等级。

no 命令取消对应 loghost 的 ip 地址和等级配置。

若堆叠环境下使用，后面需要带上 member。

**举例：**

Sysname(config)#info-center loghost 1 config 192.168.1.1 facility local0 member 1

## 9.5.7 info-center logfile

**命令：**

**info-center logfile <1-4> config count <1-40960> (flash|usb) WORD (member <1-4> |)**

**no info-center logfile <1-4> config (member <1-4> |)**

**功能：**配置日志文件的条数和存取路径。

**参数：**

| 参数 | 描述 |
|---|---|
| logfile <1-4> | 表示配置 logfile 输出方向 |
| count <1-40960> | 日志文件的条数 |
| flash\|usb | 可选的存取路径 |
| WORD | 存取日志文件名 |
| member <1-4> | member 成员号 |

**命令模式：**全局配置模式

**缺省情况：**缺省未配置

**使用指南：**

该命令配置日志文件的条数和存取路径。需要注意 logfile 有缺省的配置，对于缺省日志文件，系统使用 logfile 4 作为默认的输出方向，默认存储路径为 flash，缺省文件名为 logfile.log，默认匹配级别为 warning，默认日志文件最大条数为 40960。这样在默认配置下单板掉电重启后仍然可以从主控上使用 show info-center logfile 命令查看到单板掉电前的日志信息。

no 命令取消对应 logfile 的条数和存取路径配置。

**举例：**

Sysname(config)#info-center logfile 1 config count 40960 flash logfile.log member 1

## 9.5.8 info-center clear

**命令：**

**info-center clear trapbuffer**

**info-center clear logbuffer (member <1-4> |)**

**功能：**删除信息中心 logbuffer 或 trapbuffer 记录的所有日志。

**参数：**

| 参数 | 描述 |
|---|---|
| **logbuffer\|trapbuffer** | **可选的清除日志输出方向名称** |
| member <1-4> | **member 成员号** |

**命令模式：**全局配置模式

**缺省情况：**缺省未配置

**使用指南：**

该命令删除信息中心 logbuffer 或 trapbuffer 记录的所有日志。

**举例：**

**Sysname(config)#info-center clear logbuffer member 1**

Sysname(config)#info-center clear trapbuffer

## 9.5.9 show info-center config

**命令：show info-center config**

**功能：**显示信息中心当前配置。

**参数：无**

**命令模式：**所有模式

**缺省情况：**无

**使用指南：**

该命令显示信息中心当前所有配置。

**举例：**

SW1(config)#show info-center config

info-center enable

info-center sync enable

info-center console output-enable

info-center monitor output-enable

info-center trapbuffer output-enable

info-center logbuffer output-enable

info-center logfile 4 config count 40960 nandflash logfile.log
info-center logfile 4 output-enable
info-center console match level warnings
info-center console prefix on
info-center monitor match level debugging
info-center monitor prefix on
info-center trapbuffer prefix on
info-center logbuffer match level warnings
info-center logbuffer prefix on
info-center loghost 1 prefix on
info-center loghost 2 prefix on
info-center loghost 3 prefix on
info-center loghost 4 prefix on
info-center loghost 5 prefix on
info-center loghost 6 prefix on
info-center loghost 7 prefix on
info-center loghost 8 prefix on
info-center logfile 1 prefix on
info-center logfile 2 prefix on
info-center logfile 3 prefix on
info-center logfile 4 match level warnings
info-center logfile 4 prefix on

## 9.5.10 show info-center logbuffer

**命令：**

**show info-center logbuffer (keyword WORD) (member <1-4>)**

**功能：**显示 logbuffer 输出方向的内容。

**参数：**

| 参数 | 描述 |
|---|---|
| keyword WORD | 使用正则表达式作为刷选条件 |
| member <1-4> | member 成员号 |

**命令模式：**所有模式

**缺省情况：**无

**使用指南：**

该命令显示 logbuffer 输出方向内容，并且可以用正则表达式做内容筛选。

注意，并没有单独的一条命令做显示记录操作命令，所有的操作命令在字符串中都额外加了 CMD:这几个字符，可以用这个做关键字进行筛选。

**举例：**

**Sysname(config)#show info-center logbuffer member 1**

## 9.5.11 show info-center trapbuffer

**命令：**

**show info-center trapbuffer (keyword WORD)**

**功能：**显示 trapbuffer 输出方向的内容。

**参数：**

| 参数 | 描述 |
|---|---|
| keyword WORD | 使用正则表达式作为刷选条件 |

**命令模式：**所有模式

**缺省情况：**无

**使用指南：**

该命令显示 trapbuffer 输出方向内容，并且可以用正则表达式做内容筛选。

**举例：**

**Sysname(config)#show info-center trapbuffer**
**severity: 1-emergencies 2-alerts 3-critical 4-errors 5-warnings 6-notifications 7-informational 8-debugging**
**Allowed max messages:2000,Current messages:44**
**44 Jan 25 11:43:21:000 2019 SNR-S2995G-12FX DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to UP**
**43 Jan 25 11:43:20:000 2019 SNR-S2995G-12FX MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1/1, changed state to UP**
**42 Jan 25 11:43:07:000 2019 SNR-S2995G-12FX DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to DOWN**
**41 Jan 25 11:43:06:000 2019 SNR-S2995G-12FX MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1/1, changed state to DOWN**
**40 Jan 25 11:38:22:000 2019 SNR-S2995G-12FX DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to UP**

**39 Jan 25 11:38:21:000 2019 SNR-S2995G-12FX**
**MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1/1, changed state to UP**
**38 Jan 25 11:38:08:000 2019 SNR-S2995G-12FX**
**DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to DOWN**
**37 Jan 25 11:38:07:000 2019 SNR-S2995G-12FX**
**MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1/1, changed state to DOWN**
**36 Jan 25 11:29:33:000 2019 SNR-S2995G-12FX DEFAULT/2/:System cold restart...**
**35 Jan 25 11:28:36:000 2019 SNR-S2995G-12FX**
**DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to UP**
**.....**
----finish show trap buffer----

## 9.5.12 show info-center logfile

命令：

**show info-center logfile <1-4> (keyword WORD) (member <1-4> )**

功能：显示 logfile 输出方向的内容。

参数：

| 参数 | 描述 |
|---|---|
| logfile <1-4> | 可选的 logfile 输出方向 |
| keyword WORD | 使用正则表达式作为刷选条件 |
| member <1-4> | member 成员号 |

**命令模式：**所有模式

**缺省情况：**无

**使用指南：**

该命令显示 logfile 输出方向内容，并且可以用正则表达式做内容筛选。

注意，并没有单独的一条命令做显示记录操作命令，所有的操作命令在字符串中都额外加了 CMD:这几个字符，可以用这个做关键字进行筛选。

**举例：**

**Sysname(config)#show info-center logfile 1 member 1**
**severity: 1-emergencies 2-alerts 3-critical 4-errors 5-warnings 6-notifications 7-informational 8-debugging**

**55 Dec 18 14:47:22:000 2018 switch MODULE_UTILS_FILESYSTEM/2/:fs_write_file 2167: FS_DEV_UNLOCK Slot: 1 dev_name:flash: file_name:flash:/board_web_language**
**54 Dec 18 14:47:22:000 2018 switch MODULE_UTILS_FILESYSTEM/2/:fs_write_file 2149: FS_DEV_LOCK_NO_WAIT Slot: 1 dev_name:flash: file_name:flash:/board_web_language**
**53 Dec 18 14:47:16:000 2018 switch MODULE_MANAGEINTF/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to DOWN**
**52 Dec 18 14:47:16:000 2018 switch MODULE_MANAGEINTF/5/:%LINK-5-CHANGED: Interface Ethernet0, changed state to UP**
**51 Dec 18 14:47:16:000 2018 switch DEFAULT/3/:Clock between master and slave has been synchronized!**
**50 Dec 18 14:47:15:000 2018 sysname MODULE_VSF_PROTO/2/:topo success! vsf done 1 state ALIVE master 00-03-0f-aa-aa-ab seq 0 local seq 0**
**49 Dec 18 14:47:15:000 2018 sysname MODULE_VSF_PROTO/2/:disc success! cpu num 1 vsf done 0 state TOPO master 00-03-0f-aa-aa-ab seq 0 pri 0x4000207f local seq 0 pri 0x4000207f**
**48 Dec 18 14:47:15:000 2018 sysname MODULE_VSF_PROTO/2/:Master 00-03-0f-aa-aa-ab mid 1 pri 0x4000207f seq 0**
**47 Dec 18 14:47:15:000 2018 sysname MODULE_VSF_PROTO/2/:vsf_proto_handle_start 2448: vsf done 0 local seq 0 pri 0x207f**
**.....**
----finish show log file----

## 9.5.13 info-center list all disk

**命令：info-center list all disk**
**功能：**查看信息中心支持存放文件的区域。
**参数：**无
**命令模式：**全局配置模式
**缺省情况：**无
**使用指南：**

该命令主要用于查看信息中心支持存放文件的区域。支持的区域包括 flash、usb 和 nandflash。

**举例：**

**Sysname(config)# info-center list all disk**
**flash:**

**usb:**

nandflash:

## 9.5.14 info-center save all

**命令：**

**info-center save all ((flash|usb) WORD)**

**功能：**信息中心一键收集功能。

**参数：**

| 参数 | 描述 |
|---|---|
| flash\|usb | 可选的存放文件区域 |
| WORD | 存放文件名称 |

**命令模式：**全局配置模式

**缺省情况：**未配置

**使用指南：**

该命令主要用于信息中心一键收集。收集的内容为信息中心各项配置，以及 logbuffer，trapbuffer 等记录的日志信息。不配置文件路径及名称时将在缺省区域以缺省文件名存放收集的信息。默认存储路径为 flash，默认文件名为 icsaveall.txt。

**举例：**

Sysname(config)# info-center save all flash saveall.log

*****Now saving Master card(member 1)*****

Now saving infocenter all configuration, please wait..

Now saving infocenter logbuffer content, please wait..

Now saving infocenter trapbuffer content, please wait..

*****Master card(member 1) saving finished!*****

# 9.6 镜像

## 9.6.1 monitor session source interface

**命令：monitor session <session> source {interface <interface-list> | cpu [member <memberId> ]}{rx| tx| both}**

**no monitor session <session> source {interface *<interface-list>* / cpu [member *<memberId>* ]}**

**功能：**指定镜像源端口；本命令的 no 操作为删除镜像源端口。

**参数：*<session>***为镜像 session 值，端口镜像目前支持 1-4；***<interface-list>***为镜像源端口列表，支持'-'、';'等特殊字符； **cpu member <memberId>** 表示以某个插槽上板卡 CPU 作为镜像源，可以镜像该 CPU 收到或者发出的流量（调试用），CPU 镜像会自带 20 字节的 tag；rx 为镜像源端口接收的流量；tx 为镜像从源端口发出的流量；both 为镜像源端口入和出的流量。

**命令模式：**全局配置模式。

**使用指南：**本命令设置镜像的源端口，交换机对镜像源端口没有限制，可以是一个端口，也可以是多个端口，不仅能镜像源端口的发出和接收双向的流量，还能单独镜像源端口的发出流量及接收流量。如果不指定[rx|tx|both]关键字，缺省为 both。 当镜像多个端口时，多个源端口的方向可以不一致，但要分几次配置。

**举例：**设置镜像源端口为 1/1/1-4 的发出流量和 1/1/5 的接收流量。

Switch(config)#monitor session 1 source interface ethernet 1/1/1-4 tx

Switch(config)#monitor session 1 source interface ethernet1/1/5 rx

## 9.6.2 monitor session source interface access-list

**命 令 ： monitor session *<session>* source {interface *<interface-list>*} access-list *<num>* {rx|tx|both}**

**no monitor session *<session>* source {interface *<interface-list>*} access-list *<num>***

**功能：** 指定流镜像源端口及应用规则；本命令的 no 操作为删除流镜像源端口。

**参数：** ***<session>*** 为镜像 session 值，目前支持 1-4； ***<interface-list>*** 为镜像源端口列表，支持 '-'、';'等特殊字符； ***<num>*** 为访问表标号； **rx** 为镜像源端口接收的流量； **tx** 为镜像源端口发出的流量； **both** 为镜像源端口入和出的流量。

**命令模式：** 全局配置模式。

**使用指南：** 本命令设置流镜像的源端口，交换机对流镜像源端口没有限制，可以是一个端口，也可以是多个端口，流镜像只能镜像源端口接收的流量，参数可以为 rx, tx, both。使用本命令之前必须保证已经创建相应的访问表，有关访问表创建请参见 ACL 配置。流镜像必须在创建该 session 目的端口之后创建。

**举例：** 在 session 2 设置镜像端口 1/1/6 符合规则 120 的入口数据。

Switch(config)#monitor session 2 source interface eth 1/1/6 access-list 120 rx

## 9.6.3 monitor session destination interface

**命令：monitor session *<session>* destination interface *<interface-number>***

**no monitor session *<session>* destination interface *<interface-number>***

**功能：**指定镜像目的端口；本命令的 no 操作为删除镜像目的端口。

**参数：*<session>***为镜像 session 值，目前支持 1-4；***<interface-number>***为镜像目的端口。

**缺省情况：无。**

**命令模式：**全局配置模式。

**使用指南：**交换机支持 4 个镜像目的端口。需要注意的是，作为镜像目的端口不能是端口聚合组的成员，并且端口吞吐量最好大于或等于它所镜像的所有源端口的吞吐量的总和。取消某个 session 的镜像目的端口，该 session 之前设置的所有镜像通路将不存在，重新设置该 session 的镜像目的，端口、CPU 镜像通路将恢复，需要注意的是流镜像须要在设置目的端口之后重新设置才能恢复。

**举例：**设置镜像目的端口为 1/1/7。

Switch(config)#monitor session 1 destination interface ethernet 1/1/7

## 9.6.4 show monitor

**命令：show monitor**

**功能：** 分别显示所有镜像 session 的镜像源、目的端口的信息。

**命令模式：**特权和配置模式。

**使用指南：**通过本命令可以显示当前设置的所有 session 的镜像源端口及目的端口，对于端口镜像，CPU 镜像和流镜像并且能显示镜像源的镜像模式，对于 Mac 镜像，只在支持的板卡上显示所设置的镜像 Mac。

**举例：**

Switch#show monitor

## 9.6.5 mirror sample rate

**命令： monitor session *<session>* sample rate *<0-65535>***

**功能：**针对镜像流进行采样，将采样率设置为 N 意味着从 N 个镜像包中随机选取一个包进行采样。

**参数：*<session>***为镜像 session 值，目前支持 1-4；***<0-65535>***为采样率

**命令模式：**全局配置模式。

**缺省情况：**未开启采样。

**使用指南：**通过本命令可以对镜像流进行采样，避免镜像出来的流量太多了。

**举例：** 在镜像组 1 里面，将采样率设置为 100，即每 100 个包里面采样一个

Switch(config)# monitor session 1 sample rate 100

# 9.7 RSPAN

## 9.7.1 remote-span

**命令：remote-span**

**no remote-span**

**功能：**将 vlan 设置成 RSPAN vlan，此命令的 no 命令为删除 RSPAN vlan。

**参数：**无。

**命令模式：**vlan 配置模式。

**缺省情况：**缺省不配置。

**使用指南：**本命令用于将存在的 vlan 设置为 rspan vlan。在使用 RSPAN 功能之前，要先创建专属的 RSPAN vlan，专用于转发 RSPAN 数据报文。由于默认情况下所有的端口都属于缺省 vlan，在标记 RSPAN vlan 时禁止将缺省 vlan、动态 vlan、私有 vlan、组播 vlan、配置了三层接口的 vlan 等特殊 vlan 配置为 rspan vlan。如果该 vlan 在取消了 RSPAN 特性后仍有 session 在使用，则 session 仍然可以正常工作，但是如果在取消了该 vlan 的 RSPAN 特性后又给该 vlan 配置三层接口，则有可能导致 RSPAN session 工作失效。

**举例：**

```
Switch(Config-Vlan5)#remote-span
```

## 9.7.2 monitor session remote vlan

**命令：monitor session *<session>* remote vlan *<vid>***

**no monitor session *<session>* remote vlan**

**功能：**将本地 mirror 的 session 设置成 RSPAN，此命令的 no 命令为将 RSPAN 还原为本地 mirror。

**参数：*<session>***：session ID 号，有效范围为 1~4。<vid>：RSPAN vlan 的 id 号。

**命令模式：**全局配置模式。

**缺省情况：**缺省不配置。

**使用指南：**通过本命令将本地 mirror 的 session 设置成 rspan，此处的 vlan id 即为 rspan vlan。在被镜像的数据打上 RSPAN tag。

**举例：**

```
Switch(config)#monitor session 1 remote vlan 5
```

## 9.7.3 monitor session reflector-port

**命令：monitor session *<session>* reflector-port *<interface-number>***

**no monitor session *<session>* reflector-port *<interface-number>***

**功能：**配置反射端口，此命令的 no 命令为删除反射端口。

**参数：*<session>***：session ID 号，有效范围为 1~4。***<interface-number>***：端口号。

**命令模式：**全局配置模式。

**缺省情况：**缺省不配置。

**使用指南：**通过本命令将端口设置为反射端口作为 mirror 的目的端口。并将该端口的 MAC 学习功能关闭。反射端口的设置实际上就是把该 session 的本地目的端口设置为反射方式，所以反射端口的设置与目的端口的设置是两个互斥的命令。通过 no 命令将反射端口被还原为普通端口，该 session 不再有目的端口。在源交换机采用反射端口的镜像方式时，不能把镜像的源端口以 access 或者是 trunk 的方式配置为 RSPAN VLAN 的成员端口。采用反射端口做跨板的 cpu tx 方向镜像时，反射端口必须配置为 trunk 端口允许 RSPAN VLAN 的数据通过，并且其 native vlan 不能配置为 RSPAN VLAN。配置 RSPAN 功能后，出口镜像的报文会加上 vlan tag，导致反射端口上出现 abort 错误帧，此时需要修改交换机默认 MTU 值。

**举例：**

Switch(config)#monitor session 1 reflector-port int ethernet1/1/3

# 9.8 ERSPAN

## 9.8.1 monitor session destination tunnel

本型号交换机不支持此命令

# 9.9 sFlow

## 9.9.1 sflow agent-address

**命令：sflow agent-address *<agent-address>***

**no sflow agent-address**

**功能：**配置 sFlow 采样代理地址。no 命令删除采样代理地址。

**参数：*<agent-address >***为采样代理 IP 地址，点分十进制格式。

**命令模式：**全局配置模式。

**缺省情况：**没有缺省值。

**使用指南：**代理地址用来标志采样代理，类似于 OSPF 或者 BGP 中的 Router ID，但是并不是 sFlow 采样代理正常工作所必需配置的。

**举例：**在全局模式采样代理地址。

Switch(config)#sflow agent-address 192.168.1.200

## 9.9.2 sflow analyzer

**命令：sflow analyzer sflowtrend**

**no sflow analyzer sflowtrend**

**功能：**配置 sFlow 使用的分析器。no 命令删除 sflow 的分析器。

**参数：**sflowtrend 为 Inmon 的 Sflowtrend 分析器。

**命令模式：**全局配置模式。

**缺省情况：**不配置。

**使用指南：**使用 sflow 时，当使用 sFlowTrend 分析软件时，要配置这个命令。

**举例：**

Switch(config)#sflow analyzer sflowtrend

## 9.9.3 sflow counter-interval

**命令：sflow counter-interval *<interval-value>***

**no sflow counter-interval**

**功能：**配置 sFlow 进行统计采样的最大间隔。no 命令删除统计采样间隔值。

**参数：*<interval-value>***为间隔值，取值范围 20~120，单位为秒。

**命令模式：**端口配置模式。

**缺省情况：**无缺省值。

**使用指南：**如果没有配置统计采样间隔，那么就不会在接口上进行统计采样。

**举例：**配置接口 e1/1/1 的统计采样间隔为 20 秒。

Switch(Config-If-Ethernet1/1/1)#sflow counter-interval 20

## 9.9.4 sflow data-len

**命令：sflow data-len *<length-value>***

**no sflow data-len**

**功能：**配置 sFlow 报文中允许的最大数据长度，no 命令恢复为默认值。

**参数：*<length-value>***为长度值，取值范围 500~1470。

**命令模式：**端口配置模式。

**缺省情况：**缺省为 1400。

**使用指南：**多个采样组成一个 sFlow 分组发送出去，sFlow 分组除去 mac 头和 IP 头的部分长度不能超过所配置的值。

**举例：**配置 sFlow 报文中允许的最大数据长度为 1000。

Switch(Config-If-Ethernet1/1/2)#sflow data-len 1000

## 9.9.5 sflow destination

**命令：sflow destination *<collector-address>* [*<collector-port>*]**

**no sflow destination**

**功能：**配置 sFlow 分析软件所在主机的 IP 地址和端口号。对于端口来说，如果端口上有配置 IP 地址，则使用端口的配置，否则使用全局的配置。no 命令恢复为默认端口，删除 IP 地址。

**参数：*<collector-address>***为分析器 IP 地址，点分十进制格式。***<collector-port>***为发送的 sFlow 报文的目的端口。

**命令模式：**全局配置模式和端口配置模式。

**缺省情况：**sFlow 报文目的端口缺省为 6343，分析器无默认地址。

**使用指南：**如果接口下配置了分析器地址，那么该接口的采样报文发送时使用接口下配置的 IP 地址和端口，否则就使用全局模式下配置的地址和端口。sFlow 采样代理要正常工作，必须配置分析器地址。

**举例：**在全局模式配置分析器地址和端口。

Switch(config)#sflow destination 192.168.1.200 1025

## 9.9.6 sflow header-len

**命令：sflow header-len *<length-value>***

**no sflow header-len**

**功能：**配置 sFlow 在数据采样中复制的报文数据头的长度，no 命令恢复为默认值。

**参数：*<length-value>***为长度值，取值范围 32~256。

**命令模式：**端口配置模式。

**缺省情况：**缺省为 128。

**使用指南：**当被采样的报文被送往 CPU 时，分析出不是 IPv4 和 IPv6 报文，那么要将分组的一定长度的头部拷贝到 sFlow 报文中发送出去，拷贝内容的内容长度由本命令配置。

**举例：**配置 sFlow 在数据采样中复制的报文数据头的长度为 50。

Switch(Config-If-Ethernet1/1/2)#sflow header-len 50

## 9.9.7 sflow priority

**命令：sflow priority *<priority-value>***

**no sflow priority**

**功能：**配置 sFlow 从硬件收报文时的优先级。no 命令恢复为默认值。

**参数：*<priority-value>***为优先级值，取值范围 0~3。

**命令模式：**全局配置模式。

**缺省情况：**缺省为 0。

**使用指南：**当被采样的报文被送往 CPU 时，其优先级不应该配得太高，以免影响其它协议报文的正常接收。优先级的值越大，优先级越高。

**举例：**在全局模式配置 sFlow 从硬件收报文时的优先级。

Switch(config)#sflow priority 1

## 9.9.8 sflow rate

**命令：sflow rate { input *<input-rate>* | output *<output-rate >*}**

**no sflow rate [input | output]**

**功能：**配置 sFlow 在硬件采样时的采样速率。No 命令删除采样速率值。

**参数：*<input-rate>***为 ingress 分组采样速率值，取值范围 1000~16383500；

***<output-rate>***为 egress 分组采样速率值，取值范围 1000~16383500。

**命令模式：**端口配置模式。

**缺省情况：**无缺省值。

**使用指南：**如果没有配置端口的采样速率，那么就不会在接口上进行流采样。如果配置采样 ingress 分组采样速率为 10000，表示 10000 个 ingress 分组中会采样一个分组。

**举例：**配置接口 e1/1/1 的 ingress 采样速率为 10000, egress 采样速率为 20000。

Switch(Config-If-Ethernet1/1/1)#sflow rate input 10000

Switch(Config-If-Ethernet1/1/1)#sflow rate output 20000

## 9.9.9 sflow version

sflow version

命令：sflow version<version>

no sflow version

功能：配置全局 sflow 版本，本命令的 no 操作恢复为缺省值。

参数：<version>: 为配置的 sflow 版本号，目前支持版本 4 和版本 5。

缺省情况：缺省为版本 4。

命令模式：全局配置模式。

使用指南：该命令主要用于配置 sflow 的版本，目前支持版本 4 和版本 5。

举例：配置全局的 sflow 版本为 5。

Switch (config)#sflow version 5

## 9.9.10 show sflow

**命令：show sflow**

**功能：**显示 sFlow 的配置状态。

**参数：**无。

**命令模式：**所有模式。

**使用指南：**用于了解 sFlow 的运行状态。

Switch #show sflow

Sflow version 1.2

Agent address is 172.16.1.100

Collector address have not configured

Collector port is 6343

Sampler priority is 2

Sflow DataSource: type 2, index 194(Ethernet1/1/2)

Collector address is 192.168.1.200

Collector port is 6343

Counter interval is 0

Sample rate is input 0, output 0

Sample packet max len is 1400

Sample header max len is 50

Sample version is 4

| 显示内容 | 解释 |
| --- | --- |
| Sflow version 1.2 | 表示 sFlow 的 version 为 1.2 |
| Agent address is 172.16.1.100 | sFlow 采样代理地址是 172.16.1.100 |
| Collector address have not configured | sFlow 全局的分析器地址没有配置 |
| Collector port is 6343 | sFlow 全局的目的端口是默认值 6343 |
| Sampler priority is 2 | sFlow 从硬件收报文时的优先级为 2 |
| Sflow DataSource: type 2, index 194(Ethernet1/1/1) | sFlow 一个采样代理的数据源为接口 E1/1/1，类型为 2（以太网），接口的 index 为 194 |
| Collector address is 192.168.1.200 | E1/1/1 接口上采样代理的分析器地址是 192.168.1.200 |
| Collector port is 6343 | E1/1/1 接口采样代理的端口是默认值 6343 |
| Counter interval is 20 | E1/1/1 接口上的统计采样间隔是 20 秒 |
| Sample rate is input 10000, output 0 | E1/1/1 接口采样代理的 ingress 流采样速率为 10000，不进行 egress 流采样 |
| Sample packet max len is 1400 | E1/1/1 接口采样代理发出的 sFlow 分组最大数据长度不得超过 1400 个字节 |
| Sample header max len is 50 | E1/1/1 接口采样代理在数据采样中复制的报文数据头的长度为 50 |
| Sample version is 4 | E1/1/1 接口采样代理发出的 sFlow 分组的 datagram version 为 4 |

# 9.10 NQA

## 9.10.1 nqa agent

**命令：nqa agent**

**no nqa agent**

**功能：**配置本命令使能 nqa 客户端功能，本命令的 no 操作为关掉 nqa 客户端功能。

**参数：**无。

**缺省情况：**默认不开启 NQA 客户端。

**命令模式：**全局配置模式。

**使用指南：**当需要使用nqa客户端功能时，配置该条命令。

**举例：**使能 nqa 客户端功能

Switch#config terminal

Switch(config)#nqa agent

## 9.10.2 nqa entry type icmp-echo

**命令：nqa entry <1-64> type icmp-echo dest-ip *A.B.C.D* (src-ip *A.B.C.D* |)**

**(nexthop-ip *A.B.C.D* |) (vrf *WORD* |)**

**no nqa entry <1-64>**

**功能：**配置 nqa 探测组探测类型为 icmp-echo，本命令的 no 操作为删除 nqa 探测组。

**参数：<1-64>：**nqa探测组id；

**dest-ip *A.B.C.D*：**探测目的地址；

**src-ip *A.B.C.D*：**探测源地址；

**nexthop-ip *A.B.C.D*：**探测下一跳地址；

**vrf *WORD*：**探测vrf实例。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**若是需要进行icmp-echo探测，即可配置该命令行。

**举例：**配置 nqa 探测组探测类型为 icmp-echo 的探测表项

Switch#config terminal

Switch(config)#nqa entry 1 type icmp-echo dest-ip 1.1.1.1 src-ip 2.2.2.2 nexthop-ip 3.3.3.3 vrf 1

## 9.10.3 nqa entry type icmp-jitter

**命令：nqa entry <1-64> type icmp-jitter dest-ip *A.B.C.D* (src-ip *A.B.C.D* |)**

**(nexthop-ip *A.B.C.D* |) (vrf *WORD* |)**

**no nqa entry <1-64>**

**功能：**配置 nqa 探测组探测类型为 icmp-jitter，本命令的 no 操作为删除 nqa 探测组。

**参数：<1-64>：**nqa探测组id；

**dest-ip *A.B.C.D*：**探测目的地址；

**src-ip *A.B.C.D*：**探测源地址；

**nexthop-ip *A.B.C.D*：**探测下一跳地址；

**vrf *WORD*：**探测vrf实例。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**若是需要进行icmp-jitter探测，即可配置该命令行。

**举例：**配置 nqa 探测组探测类型为 icmp-jitter 的探测表项

Switch#config terminal

Switch(config)#nqa entry 1 type icmp-jitter dest-ip 1.1.1.1 src-ip 2.2.2.2 nexthop-ip 3.3.3.3 vrf 1

## 9.10.4 nqa entry type udp-echo

**命令：nqa entry <1-64> type udp-echo dest-ip *A.B.C.D* dest-port <1-65535>**

**(src-ip *A.B.C.D* |) (nexthop-ip *A.B.C.D* |) (vrf *WORD* |)**

**no nqa entry <1-64>**

**功能：**配置 nqa 探测组探测类型为 udp-echo，本命令的 no 操作为删除 nqa 探测组。

**参数：<1-64>：**nqa探测组id；

**dest-ip *A.B.C.D*：**探测目的地址；

**dest-port <1-65535>：**探测目的端口号；

**src-ip *A.B.C.D*：**探测源地址；

**nexthop-ip *A.B.C.D*：**探测下一跳地址；

**vrf *WORD*：**探测vrf实例。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**若是需要进行udp-echo探测，即可配置该命令行。

**举例：**配置 nqa 探测组探测类型为 udp-echo 的探测表项

Switch#config terminal

Switch(config)#nqa entry 1 type udp-echo dest-ip 1.1.1.1 dest-port 1500 src-ip 2.2.2.2 nexthop-ip 3.3.3.3 vrf 1

## 9.10.5 nqa entry type udp-jitter

**命令：nqa entry <1-64> type udp-jitter dest-ip *A.B.C.D* dest-port <1-65535>**

**(src-ip *A.B.C.D* |) (nexthop-ip *A.B.C.D* |) (vrf *WORD* |)**

**no nqa entry <1-64>**

**功能：**配置 nqa 探测组探测类型为 udp-jitter，本命令的 no 操作为删除 nqa 探测组。

**参数：<1-64>：**nqa探测组id；

**dest-ip *A.B.C.D***：探测目的地址；

**dest-port <1-65535>**：探测目的端口号；

**src-ip *A.B.C.D***：探测源地址；

**nexthop-ip *A.B.C.D***：探测下一跳地址；

**vrf *WORD***：探测vrf实例。

**缺省情况**：无。

**命令模式**：全局配置模式。

**使用指南**：若是需要udp-jitter探测，即可配置该命令行。

**举例**：配置 nqa 探测组探测类型为 udp-jitter 的探测表项

Switch#config terminal

Switch(config)#nqa entry 1 type udp-jitter dest-ip 1.1.1.1 dest-port 1500 src-ip 2.2.2.2 nexthop-ip 3.3.3.3 vrf 1

## 9.10.6 nqa entry type tcp

**命令：nqa entry <1-64> type tcp dest-ip *A.B.C.D* dest-port <1-65535>**

**(src-ip *A.B.C.D* |) (nexthop-ip *A.B.C.D* |) (vrf *WORD* |)**

**no nqa entry <1-64>**

**功能**：配置 nqa 探测组探测类型为 tcp，本命令的 no 操作为删除 nqa 探测组。

**参数：<1-64>**：nqa探测组id；

**dest-ip *A.B.C.D***：探测目的地址；

**dest-port <1-65535>**：探测目的端口号；

**src-ip *A.B.C.D***：探测源地址；

**nexthop-ip *A.B.C.D***：探测下一跳地址；

**vrf *WORD***：探测vrf实例。

**缺省情况**：无。

**命令模式**：全局配置模式。

**使用指南**：若是需要tcp探测，即可配置该命令行。

**举例**：配置 nqa 探测组探测类型为 tcp 的探测表项

Switch#config terminal

Switch(config)#nqa entry 1 type tcp dest-ip 1.1.1.1 dest-port 1500 src-ip 2.2.2.2 nexthop-ip 3.3.3.3 vrf 1

## 9.10.7 nqa entry type dhcp

**命令：nqa entry <1-64> type dhcp interface vlan <1-4094>**

**no nqa entry <1-64>**

**功能**：配置 nqa 探测组探测类型为 dhcp，本命令的 no 操作为删除 nqa 探测组。

**参数：<1-64>**：nqa探测组id；

**vlan <1-4094>**：探测vlan口。

**缺省情况**：无。

**命令模式**：全局配置模式。

**使用指南**：若是需要dhcp探测，即可配置该命令行。

**举例**：配置 nqa 探测组探测类型为 dhcp 的探测表项

Switch#config terminal

Switch(config)#nqa entry 1 type dhcp interface vlan 1

## 9.10.8 nqa entry description

**命令**：**nqa entry <1-64> description *TEXT***

**no nqa entry <1-64> description**

**功能**：配置 nqa 探测组描述符，本命令的 no 操作为删除 nqa 探测组描述符。

**参数**：**<1-64>**：nqa探测组id；

**description *TEXT***：描述符。

**缺省情况**：无。

**命令模式**：全局配置模式。

**使用指南**：若是需要配置nqa探测组描述符，即可配置该命令行。

**举例**：配置 nqa 探测组描述符为 icmp-test

Switch#config terminal

Switch(config)#nqa entry 1 description icmp-test

## 9.10.9 nqa entry frequency

**命令**：**nqa entry <1-64> frequency <3-60>**

**no nqa entry <1-64> frequency**

**功能**：配置 nqa 探测组探测周期，本命令的 no 操作为恢复探测周期为缺省值。

**参数**：**<1-64>**：nqa探测组id；

**frequency <3-60>**：探测周期间隔时间，单位为秒。

**缺省情况**：**nqa** 探测组探测周期间隔时间 icmp-jitter、udp-jitter 探测默认为 40s，其他探测默认为 3s。

**命令模式**：全局配置模式。

**使用指南**：若是需要修改nqa探测周期间隔时间，即可配置该命令行。

**举例**：配置 nqa 探测组探测周期间隔时间为 10s

Switch#config terminal

Switch(config)#nqa entry 1 frequency 10

## 9.10.10 nqa entry probe-count

**命令**：**nqa entry <1-64> probe-count <1-5>**

**no nqa entry <1-64> probe-count**

**功能：**配置 nqa 探测组探测周期内探测次数，本命令的 no 操作为恢复探测次数为缺省值。

**参数：<1-64>：**nqa探测组id；

**probe-count <1-5>：**探测周期内探测次数。

**缺省情况：nqa** 探测组探测周期内 icmp-jitter、udp-jitter 探测次数默认为 20 次，其他探测次数默认为 1 次。

**命令模式：**全局配置模式。

**使用指南：**若是需要修改nqa探测周期内探测次数，即可配置该命令行。

**举例：**配置 nqa 探测组探测周期内探测次数为 3 次

Switch#config terminal

Switch(config)#nqa entry 1 probe-count 3

## 9.10.11 nqa entry probe-timeout

**命令：nqa entry <1-64> probe-timeout <1-5>**

**no nqa entry <1-64> probe-timeout**

**功能：**配置 nqa 探测组探测超时时间，本命令的 no 操作为恢复探测超时时间为缺省值。

**参数：<1-64>：**nqa探测组id；

**probe-timeout <1-5>：**探测超时时间，单位为秒。

**缺省情况：nqa** 探测组探测超时时间默认为 2s。

**命令模式：**全局配置模式。

**使用指南：**若是需要修改nqa探测超时时间，即可配置该命令行。

**举例：**配置 nqa 探测组探测超时时间为 3s

Switch#config terminal

Switch(config)#nqa entry 1 probe-timeout 3

## 9.10.12 nqa entry datasize

**命令：nqa entry <1-64> datasize <1-8100>**

**no nqa entry <1-64> datasize**

**功能：**配置 nqa 探测组探测报文长度，本命令的 no 操作为恢复探测报文长度为缺省值。

**参数：<1-64>：**nqa探测组id；

**datasize <1-8100>：**探测报文长度，单位为字节。

**缺省情况：nqa** 探测组探测报文长度默认为 56 字节。

**命令模式：**全局配置模式。

**使用指南：**若是需要修改nqa探测报文长度，即可配置该命令行。

**举例：**配置 nqa 探测组探测报文长度为 1500 字节

Switch#config terminal

Switch(config)#nqa entry 1 datasize 1500

## 9.10.13 nqa entry ttl

**命令：nqa entry <1-64> ttl <1-255>**

**no nqa entry <1-64> ttl**

**功能：**配置 nqa 探测组探测报文 ttl 值，本命令的 no 操作为恢复探测报文 ttl 值为缺省值。

**参数：<1-64>：**nqa探测组id；

**ttl <1-255>：**探测报文ttl值。

**缺省情况：nqa** 探测组探测报文 ttl 值默认为 30。

**命令模式：**全局配置模式。

**使用指南：**若是需要修改nqa探测报文ttl值，即可配置该命令行。

**举例：**配置 nqa 探测组探测报文 ttl 值为 100

Switch#config terminal

Switch(config)#nqa entry 1 ttl 100

## 9.10.14 nqa entry tos

**命令：nqa entry <1-64> tos <0-255>**

**no nqa entry <1-64> tos**

**功能：**配置 nqa 探测组探测报文 tos 值，本命令的 no 操作为恢复探测报文 tos 值为缺省值。

**参数：<1-64>：**nqa探测组id；

**tos <0-255>：**探测报文tos值。

**缺省情况：nqa** 探测组探测报文 tos 值默认为 0。

**命令模式：**全局配置模式。

**使用指南：**若是需要修改nqa探测报文tos值，即可配置该命令行。

**举例：**配置 nqa 探测组探测报文 tos 值为 100

Switch#config terminal

Switch(config)#nqa entry 1 tos 100

## 9.10.15 nqa entry fail-percent

**命令：nqa entry <1-64> fail-percent <1-100>**

**no nqa entry <1-64> fail-percent**

**功能：**配置 nqa 探测组探测失败百分比，本命令的 no 操作为恢复探测失败百分比为缺省值。

**参数：<1-64>：**nqa探测组id；

**fail-percent <1-100>：**探测失败百分比。

**缺省情况：nqa** 探测组探测失败百分比默认为 100%，即只有全部探测失败，本次测试才视为失败。

**命令模式：**全局配置模式。

**使用指南：**若是需要修改nqa探测失败百分比，即可配置该命令行。

**举例：**配置 nqa 探测组探测失败百分比为 10%

Switch#config terminal

Switch(config)#nqa entry 1 fail-percent 10

## 9.10.16 nqa entry records-result

**命令：nqa entry <1-64> records-result <1-10>**

**no nqa entry <1-64> records-result**

**功能：**配置 nqa 探测组探测结果历史记录最大条目数，本命令的 no 操作为恢复探测结果历史记录最大条目数为缺省值。

**参数：<1-64>：**nqa探测组id；

**records-result <1-10>：**探测结果历史记录最大条目数。

**缺省情况：nqa** 探测组探测结果历史记录最大条目数为 5 条。

**命令模式：**全局配置模式。

**使用指南：**若是需要修改nqa探测结果历史记录最大条目数，即可配置该命令行。

**举例：**配置 nqa 探测组探测结果历史记录最大条目数为 10 条

Switch#config terminal

Switch(config)#nqa entry 1 records-result 10

## 9.10.17 nqa entry probe-threshold

**命令：nqa entry <1-64> probe-threshold <50-5000>**

**no nqa entry <1-64> probe-threshold**

**功能：**配置 nqa 探测组探测阈值，本命令的 no 操作为恢复探测组探测阈值为缺省值。

**参数：<1-64>：**nqa探测组id；

**probe-threshold <50-5000>：**探测阈值，单位为ms。

**缺省情况：nqa** 探测组探测阈值为 2000ms。

**命令模式：**全局配置模式。

**使用指南：**若是需要修改nqa探测阈值，即可配置该命令行。

**举例：**配置 nqa 探测组探测阈值为 3000ms

Switch#config terminal

Switch(config)#nqa entry 1 probe-threshold 3000

## 9.10.18 nqa entry start

**命令：nqa entry <1-64> start (|forever|time-range *WORD*)**

**no nqa entry <1-64> start**

**功能：**配置 nqa 探测组开始探测，本命令的 no 操作为 nqa 探测组停止探测。

**参数：<1-64>：**nqa探测组id；

**forever：**探测组一直探测；

**time-range *WORD***：探测组的运行时间。

**缺省情况：nqa** 探测组不开启探测。

**命令模式：**全局配置模式。

**使用指南：**若是不配置探测时间，则默认探测一个周期后结束。

**举例：**配置 nqa 探测组开始探测并且一直探测

Switch#config terminal

Switch(config)#nqa entry 1 start forever

## 9.10.19 nqa alarm enable

**命令：nqa alarm enable**

**no nqa alarm enable**

**功能：**开启 nqa 全局告警功能，本命令的 no 操作为关闭 nqa 全局告警功能。

**参数：无**

**缺省情况：**nqa 关闭全局告警功能。

**命令模式：**全局配置模式。

**使用指南：**若是需要使用nqa告警功能，则配置该命令行。

**举例：**开启 nqa 全局告警功能

Switch#config terminal

Switch(config)#nqa alarm enable

## 9.10.20 nqa traps enable

**命令：nqa traps enable**

**no nqa traps enable**

**功能：**开启 nqa 全局 traps 功能，本命令的 no 操作为关闭 nqa 全局 traps 功能。

**参数：无**

**缺省情况：**nqa 关闭全局 traps 功能。

**命令模式：**全局配置模式。

**使用指南：**若是需要使用nqa traps功能，则配置该命令行。

**举例：**开启 nqa 全局 traps 功能

Switch#config terminal

Switch(config)#nqa traps enable

## 9.10.21 nqa entry alarm enable

**命令：nqa entry <1-64> alarm enable**

**no nqa entry <1-64> alarm enable**

**功能：开启** nqa 探测组告警功能，本命令的 no 操作为关闭 nqa 探测组告警功能。

**参数：<1-64>：**nqa探测组id。

**缺省情况：**nqa 探测组关闭告警功能。

**命令模式：**全局配置模式。

**使用指南：**若是需要使用nqa探测组告警功能，则配置该命令行。

**举例：**配置 nqa 探测组开启告警功能

Switch#config terminal

Switch(config)#nqa entry 1 alarm enable

## 9.10.22 nqa entry traps enable

**命令：nqa entry <1-64> traps enable**

**no nqa entry <1-64> traps enable**

**功能：开启** nqa 探测组 traps 功能，本命令的 no 操作为关闭 nqa 探测组 traps 功能。

**参数：<1-64>：**nqa探测组id。

**缺省情况：**nqa 探测组关闭 traps 功能。

**命令模式：**全局配置模式。

**使用指南：**若是需要使用nqa探测组traps功能，则配置该命令行。

**举例：**配置 nqa 探测组开启 traps 功能

Switch#config terminal

Switch(config)#nqa entry 1 traps enable

## 9.10.23 nqa server

**命令：nqa server**

**no nqa server**

**功能：**开启 nqa 服务端功能，本命令的 no 操作为关闭 nqa 服务端功能。

**参数：无**

**缺省情况：nqa** 关闭服务端功能。

**命令模式：**全局配置模式。

**使用指南：**若是需要使用nqa服务端功能，则配置该命令行。

**举例：**开启 nqa 服务端功能

Switch#config terminal

Switch(config)#nqa server

## 9.10.24 nqa server tcp-port

**命令：nqa server tcp-port <1-65535> (vrf *WORD* |)**

**no nqa server tcp-port (vrf *WORD* |)**

**功能：**配置 nqa 服务端 tcp 监听端口号，本命令的 no 操作为关闭服务端 tcp 监听。

**参数：tcp-port <1-65535>：**tcp监听端口号；

**vrf *WORD*：**vrf实例。

**缺省情况：**默认监听 tcp 端口号 2000，vrf 为 0。

**命令模式：**全局配置模式。

**使用指南：**若是需要nqa服务器监听tcp端口，则配置该命令行。

**举例：**配置 nqa 服务端监听 tcp 端口号 3000，vrf 为 a

Switch#config terminal

Switch(config)#nqa server tcp-port 3000 vrf a

## 9.10.25 nqa server udp-port

**命令：nqa server udp-port <1-65535> (vrf *WORD* |)**

**no nqa server udp-port (vrf *WORD* |)**

**功能：**配置 nqa 服务端 udp 监听端口号，本命令的 no 操作为关闭服务端 udp 监听。

**参数：udp-port <1-65535>：**udp监听端口号；

**vrf *WORD*：**vrf实例。

**缺省情况：**默认监听 udp 端口号 2000，vrf 为 0。

**命令模式：**全局配置模式。

**使用指南：**若是需要nqa服务器监听udp端口，则配置该命令行。

**举例：**配置 nqa 服务端监听 udp 端口号 3000，vrf 为 a

Switch#config terminal

Switch(config)#nqa server udp-port 3000 vrf a

## 9.10.26 track nqa

**命令：track <1-32> nqa <1-64>**

**no track <1-32> (nqa <1-64>|)**

**功能：**配置 track 关联 nqa 探测组，本命令 no 操作为解除关联 nqa 探测组。

**参数：track <1-32>：**track id；

**nqa <1-64>：**nqa探测组id。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**若是需要nqa探测组关联上track，则需要配置该命令行。

**举例：**配置 nqa 探测组关联上 track

Switch#config terminal

Switch(config)#track 1 nqa 1

## 9.10.27 track list boolean

**命令：track <1-32> list boolean (and|or)**

**no track <1-32> list boolean**

**功能：**配置 track 关联多个 nqa 探测组后的布尔关系，本命令 no 操作为取消关联多个 nqa 探测组后的布尔关系。

**参数：track <1-32>：**track id；

**boolean (and|or)：**多个nqa探测组布尔关系为and或者or。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**若是需要多个nqa探测组关联上track，则需要配置该命令行；and为有一个探测失败即算失败，or为有一个探测成功即算成功。

**举例：**配置 track 关联多个 nqa 探测组布尔关系为 and

Switch#config terminal

Switch(config)#track 1 list boolean and

## 9.10.28 ip route track

**命令：ip route (*A.B.C.D A.B.C.D* | *A.B.C.D/M*) *A.B.C.D* track <1-32>**

**no ip route (*A.B.C.D A.B.C.D* | *A.B.C.D/M*) (*A.B.C.D*|) (track <1-32>|)**

**功能：**配置 track 与静态路由联动，本命令 no 操作为取消 track 与静态路由联动。

**参数：*A.B.C.D*：**ip地址；

***A.B.C.D*：**ip地址掩码；

***A.B.C.D/M*：**ip地址加掩码；

***A.B.C.D*：**下一跳ip地址；

**<1-32>：**track id。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**若是需要track关联上静态路由，则需要配置该命令行。

**举例：**配置 track 关联静态路由

Switch#config terminal

Switch(config)#ip route 1.1.1.1/32 2.2.2.2 track 1

## 9.10.29 rip track

**命令：rip track <1-32>**

**no rip track <1-32>**

**功能：**配置 track 与 rip 联动，本命令 no 操作为取消 track 与 rip 联动。

**参数：<1-32>：**track id。

**缺省情况：**无。

**命令模式：**接口配置模式。

**使用指南：**若是需要track关联上rip，则需要配置该命令行。

**举例：**配置 track 关联 rip

Switch#config terminal

Switch(config)#interface vlan 1

Switch(config-if-vlan1)#rip track 1

## 9.10.30 ospf track

**命令：ip ospf track <1-32>**

**no ip ospf track <1-32>**

**功能：**配置 track 与 ospf 联动，本命令 no 操作为取消 track 与 ospf 联动。

**参数：<1-32>：**track id。

**缺省情况：**无。

**命令模式：**接口配置模式。

**使用指南：**若是需要track关联上ospf，则需要配置该命令行。

**举例：**配置 track 关联 ospf

Switch#config terminal

Switch(config)#interface vlan 1

Switch(config-if-vlan1)#ip ospf track 1

## 9.10.31 bgp track

**命令：neighbor {*<ip-address>*|*<TAG>*} track <1-32>**

**no neighbor {*<ip-address>*|*<TAG>*} track <1-32>**

**功能：**配置 track 与 bgp 联动，本命令 no 操作为取消 track 与 bgp 联动。

**参数：*<ip-address>*：**邻居的 IP 地址。

***<TAG>*：**对等体组的名字；

**<1-32>：**track id。

**缺省情况：**无。

**命令模式：**BGP 路由配置模式。

**使用指南：**若是需要track关联上bgp，则需要配置该命令行。

**举例：**配置 track 关联 bgp neighbor 1.1.1.1

Switch#config terminal

Switch(config)#router bgp 1

Switch(config-router)#neighbor 1.1.1.1 track 1

## 9.10.32 show nqa results

**命令：show nqa (entry <1-64>|) results**

**功能：**显示 nqa 探测组探测结果。

**参数：<1-64>：**nqa 探测组 id。

**缺省情况：**无。

**命令模式：**所有模式。

**使用指南：**当 nqa 探测组探测完成后，通过该命令行显示出探测结果；若是不带探测组 id，则是显示所有探测组探测结果。

**举例：** switch#show nqa entry 1 results

---

NQA entry(test probe-type, icmp-echo)

1, Test 17 result The test is finished.

Send operation times: 1 Receive response times: 1

Min/Max/Avg/Sum RTT: 0/0/0/0

RTT Square Sum: 0

Start probe Time: 2023-11-10 11:26:55

Lost packet ratio: 0%

| 显示内容 | 解释 |
|---|---|
| probe-type | 探测类型 |
| Send operation times | 发送探测次数 |
| Receive response times | 接受响应次数 |
| Min/Max/Avg/Sum RTT | 最小/最大/平均/和 往返时延 |
| RTT Square Sum | 往返时延平方和 |
| Start probe Time | 开始探测时间 |
| Lost packet ratio | 丢包率 |

## 9.10.33 show track status

**命令：show track (all|<1-32>) status**

**功能：**显示 track 状态。

**参数：all：**显示所有 track 状态；

**<1-64>：**track id。

**缺省情况：**无。

**命令模式：**所有模式。

**使用指南：**当 track 创建出来后，可通过该命令行看 track 状态。

**举例：** switch#show track 1 status

Track ID: 1

Notification delay: Positive 0, Negative 0 (in milliseconds)

Logical mode: Default

Remote-ip: * probe-status: positive

protocal: NQA 1 status: succes

# 第 10 章 网络时间及域名管理命令

## 10.1 NTP

### 10.1.1 clock timezone

**命令：clock timezone WORD {add | subtract} <0-23> [<0-59>]**

**no clock timezone WORD**

**功能：**此命令在全局配置时区，no 操作命令为删除设置的时区。

**参数：WORD**：时区名，长度最大为 16；

**add | subtract**：时区的操作；

**<0-23>**：小时数；

**<0-59>**：分钟数。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**时区名不能有空格，小时数和分钟数必须在指定范围。

**举例：**全局配置 8 时区，动作为 add。

Switch(config)#clock timezone aaa add 8

### 10.1.2 debug ntp adjust

**命令：debug ntp adjust**

**no debug ntp adjust**

**功能：**打开/关闭显示本地时钟调整信息的调试开关。

**参数：**无。

**缺省情况：**显示本地时钟调整信息的调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**打开显示本地时钟调整信息的调试开关。

Switch#debug ntp adjust

### 10.1.3 debug ntp authentication

**命令：debug ntp authentication**

**no debug ntp authentication**

**功能：**显示 NTP 认证信息，no 命令关闭显示 NTP 认证信息开关。

**参数：**无。

**缺省情况：**显示 NTP 认证信息开关关闭。

**命令模式：**特权模式。

**使用指南：**显示 NTP 认证信息，如果该开关打开，则在收发报文过程中，如果报文携带了认证信息，则会将报文中的 key identifier 字段打印出来。

**举例：**打开显示 NTP 认证信息的开关。

Switch# debug ntp authentication

## 10.1.4 debug ntp events

**命令：debug ntp events**

**no debug ntp events**

**功能：**打开/关闭 NTP 事件的 debug 调试开关。

**参数：**无。

**缺省情况：**显示 NTP 事件的调试开关关闭。

**命令模式：**特权模式。

**使用指南：**该开关打开后，如果有某 server 由可达变为不可达或从不可达变为可达事件，收到非法报文事件会打印出提示信息。

**举例：**打开显示 NTP 事件信息的调试开关。

Switch#debug ntp events

## 10.1.5 debug ntp packet

**命令：debug ntp packet [send | receive]**

**no debug ntp packet [send | receive]**

**功能：**打开/关闭显示 NTP 收发数据包信息的调试开关。

**参数：**send：发送 NTP 报文的调试开关。

receive：接收 NTP 报文的调试开关。

无参数表示同时打开 NTP 报文的发送与接收开关。

**缺省情况：**显示 NTP 数据包信息的调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**打开显示 NTP 收发数据包信息的调试开关。

Switch#debug ntp packet

## 10.1.6 debug ntp sync

**命令：debug ntp sync**

**no debug ntp sync**

**功能：**打开/关闭显示本地时钟同步信息的调试开关。

**参数：**无。

**缺省情况：**显示本地时钟同步信息的调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**打开显示本地时钟同步信息的调试开关。

Switch#debug ntp sync

## 10.1.7 ntp access-group

**命令：ntp access-group server *<acl>***

**no ntp access-group server *<acl>***

**功能：**设置/取消 NTP 服务的访问控制列表。

**参数：*<acl>*：**ACL 的编号，范围为 1-99。

**缺省情况：**没有配置 NTP 服务访问控制。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**创建 NTP 的访问列表 2。

Switch(config)#ntp access-group server 2

## 10.1.8 ntp authenticate

**命令：ntp authenticate**

**no ntp authenticate**

**功能：**启用/取消 NTP 身份验证功能。

**参数：**无。

**缺省情况：**全局不启用 NTP 身份验证。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**启用 NTP 身份验证功能：

Switch(config)#ntp authenticate

## 10.1.9 ntp authentication-key

**命令：ntp authentication-key *<key-id>* md5 *<value>***

**no ntp authentication-key *<key-id>***

**功能：**启动/取消 NTP 身份验证功能，定义 NTP 身份验证的验证密钥。

**参数：**key-id：密钥编号，范围为 1-4294967295。

value：密钥值，1-16 个 ascii 码字符。

**缺省情况：**不配置 NTP 身份验证的验证密钥。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**定义 NTP 身份验证的验证密钥，key-id 为 20，md5 为 abc。

Switch(config)#ntp authentication-key 20 md5 abc

## 10.1.10 ntp broadcast client

**命令：ntp broadcast client**

**no ntp broadcast client**

**功能：** 配置/取消指定接口来接收 NTP 广播包。

**参数：** 无。

**缺省情况：** 接口不接收 NTP 广播包。

**命令模式：** vlan 配置模式。

**使用指南：** 无。

**举例：** 打开 vlan1 接口接受 NTP 广播包的功能。

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ntp broadcast client

## 10.1.11 ntp broadcast server count

**命令：ntp broadcast server count *<number>***

**no ntp broadcast server count**

**功能：**设置 NTP 客户端所能接受的广播或组播 server 最大个数。no 操作取消设置的广播或组播 server 最大个数，恢复缺省值。

**参数：**number：1-100，为广播 server 最大个数。

**缺省情况：**广播 server 最大个数为 50。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**在交换机上配置广播 server 最大个数。

Switch(config)#ntp broadcast server count 70

## 10.1.12 ntp disable

**命令：ntp disable**

**no ntp disable**

**功能：**关闭/开启接口上的 NTP 功能。

**参数：**无。

**缺省情况：**所有接口 NTP 功能打开。

**命令模式：**vlan 配置模式。

**使用指南：**无。

**举例：**关闭 vlan1 接口上的 NTP 功能。

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ntp disable

## 10.1.13 ntp enable

**命令：ntp enable**

**ntp disable**

**功能：**全局打开/关闭 NTP 功能。

**参数：**无。

**缺省情况：**默认不启动 NTP 功能。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**在交换机上启动 NTP 功能。

Switch(config)#ntp enable

## 10.1.14 ntp ipv6 multicast client

**命令：ntp ipv6 multicast client**

**no ntp ipv6 multicast client**

**功能：**配置指定接口来接收 IPv6 的 NTP 组播包，本命令的 no 操作为取消指定接口接收 IPv6 的 NTP 组播包。

**参数：**无。

**缺省情况：**接口不接收 IPv6 的 NTP 组播包。

**命令模式：**vlan 配置模式。

**使用指南：**无。

**举例：**打开 vlan1 接口接受 IPv6 的 NTP 组播包的功能。

Switch(Config)# interface vlan 1

Switch(Config-if-Vlan1)#ntp ipv6 multicast client

## 10.1.15 ntp multicast client

**命令：ntp multicast client**

**no ntp multicast client**

**功能：**配置指定接口来接收 NTP 组播包，本命令的 no 操作为取消指定接口接收 NTP 组播包。

**参数：**无。

**缺省情况：**接口不接收 NTP 组播包。

**命令模式：**vlan 配置模式。

**使用指南：**无。

**举例：**打开 vlan1 接口接受 NTP 组播包的功能。

Switch(Config)# interface vlan 1

Switch(Config-if-Vlan1)#ntp multicast client

## 10.1.16 ntp server

**命 令：** **ntp server {vrf <vrfname>|host <hostname>*<ip-address>*|*<ipv6-address>*} [version *<version_no>*] [key *<key-id>*]**

**no ntp server {vrf <vrfname>|host <hostname>*<ip-address>*|*<ipv6-address>*}**

**功能：**启用作为时钟源的指定时间服务器，no 命令取消作为时钟源的指定时间服务器。

**参数：**ip-address：时间服务器 IPv4 地址。

ipv6-address：时间服务器 IPv6 地址。

version：为该 server 配置版本信息。

version_no：server 的版本号，取值<1-4>，默认为 4。

key：为该 server 配置密钥。

key-id：密钥编号。

<vrfname>:vrf 实例名

<hostname>:服务器主机域名

**缺省情况：**没有配置时间服务器。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**在交换机上配置时间服务器地址 1.1.1.1。

Switch(config)#ntp server 1.1.1.1

## 10.1.17 ntp peer

**命令：** **ntp peer {*<ip-address>*|*<ipv6-address>*} [version *<version_no>*] [key *<key-id>*]**

**no ntp peer {*<ip-address>*|*<ipv6-address>*}**

**功能：**启用作为对等体的指定时间服务器，no 命令取消作为对等体的指定时间服务器。

**参数：**ip-address：时间服务器 IPv4 地址。

ipv6-address：时间服务器 IPv6 地址。

version：为该 server 配置版本信息。

version_no：server 的版本号，取值<1-4>，默认为 4。

key：为该 server 配置密钥。

key-id：密钥编号。

**缺省情况：**没有配置对等体时间服务器。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**在交换机上配置对等体时间服务器地址 1.1.1.1。

Switch(config)#ntp peer 1.1.1.1

## 10.1.18 ntp syn-interval

**命令：ntp syn-interval <1-3600>**

**no ntp syn-interval**

**功能：**设置 ntp client 请求报文发包间隔 1s-3600s。no 命令恢复默认值 64s。

**缺省情况：**64s。

**命令模式：**全局配置模式。

**使用指南：**为了应对高延迟网络下 ntp 调整系统时间的风险，ntp client 会在发送 8 次 ntp 时间请求后，选择延迟最小的一次时间信息来进行系统时间同步。所以默认配置下，ntp client 每 64 秒发送一次请求报文，发送 8 次后再进行时间调整，即 8 分钟调整一次系统时间。所以用户想要设置调整时间的间隔，例如一小时调整一次，则需要调整发包间隔为 450(3600/8)s。

**举例：**设置每隔一小时调整一次系统时间，则调整发包间隔为 450s。

Switch(config)#ntp syn-interval 450

## 10.1.19 ntp trusted-key

**命令：ntp trusted-key *<key-id>***

**no ntp trusted-key *<key-id>***

**功能：**指定密钥是可信赖的，no 命令取消指定的可信赖密钥。

**参数：**key-id：密钥编号，范围为 1-4294967295。

**缺省情况：**不指定可信赖的密钥。

**命令模式：**全局配置模式。

**使用指南：**无。

**举例：**将指定密钥 20 配置为可信赖状态。

Switch(config)#ntp trusted-key 20

## 10.1.20 show ntp session

**命令：show ntp session [*<ip-address>*|*<ipv6-address>*]**

**功能：**显示当前所有的或某个具体的 NTP 会话具体信息，包括有 server ID、server 的层数、本地相对于 server 的 offset 等信息。（带*表示该 server 为优选出的本地时钟源）

**参数**：ip-address：某个具体配置的时间服务器 IPv4 地址。

ipv6-address：某个具体配置的时间服务器 IPv6 地址。

无参数显示所有 server 的会话相关信息（包括广播/组播 server）。

**缺省情况**：无。

**命令模式**：特权和配置模式。

**使用指南**：无。

**举例**：

Switch#show ntp session

| | server | stream | type | rootdelay | rootdispersion | trustlevel |
|---|---|---|---|---|---|---|
| * | 1.1.1.2 | 2 | unicast | 0.010s | 0.002s | 10 |
| | 2.2.2.2 | 3 | unicast | 0.005s | 0.000s | 10 |

## 10.1.21 show ntp status

**命令：show ntp status**

**功能**：显示时间同步的具体状况，包括目前是否同步、层数、时钟源的地址等信息。

**参数**：无。

**缺省情况**：无。

**命令模式**：特权和配置模式。

**使用指南**：无。

**举例**：

Switch#show ntp status

Clock status: synchronized

Clock stratum: 3

Reference clock server: 1.1.1.2

Clock offset: 0.010 s

Root delay: 0.012 ms

Root dispersion: 0.000 ms

Reference time: TUE JAN 03 01:27:24 2006

# 10.2 SNTP

## 10.2.1 clock timezone

**命令：clock timezone WORD {add | subtract} <0-23> [<0-59>]**

**no clock timezone WORD**

**功能：**此命令在全局配置时区，no 操作命令为删除设置的时区。

**参数：WORD**：时区名，长度最大为 16；

**add | subtract**：时区的操作；

**<0-23>**：小时数；

**<0-59>**：分钟数。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**时区名不能有空格，小时数和分钟数必须在指定范围。

**举例：**全局配置 8 时区，动作为 add。

Switch(config)#clock timezone aaa add 8

## 10.2.2 debug sntp

**命令：debug sntp {adjust | packet | select |config}**

**no debug sntp {adjust | packet | select | config}**

**功能：**显示或关闭 SNTP 调试信息。

**参数：adjust** – SNTP 时钟调节信息；**packet** – SNTP 报文；**select** – SNTP 时钟选择; config - SNTP 配置信息。

**命令模式：**特权用户配置模式。

**举例：**显示 SNTP 协议报文的调试信息。

Switch#debug sntp packet

## 10.2.3 sntp polltime

**命令：sntp polltime *<interval>***

**no sntp polltime**

**功能：**设置 SNTP 客户端向 NTP/SNTP 服务器发送请求的间隔；本命令的 no 操作取消设置的 polltime，恢复缺省值 64s。

**参数：*<interval>*** 为要设置的间隔，范围从 16~16284。

**缺省情况：**polltime 缺省为 64s。

**命令模式：**全局配置模式。

**举例：**设客户端每隔 128 秒向服务器请求一次。

Switch#config

Switch(config)#sntp polltime 128

## 10.2.4 sntp server

**命令：sntp server {vrf <vrfname>|host <hostname>|<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]**

**no sntp server {vrf <vrfname>|host <hostname>|<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]**

**功能：**启用作为时钟源的指定时间服务器；本命令的no操作为删除作为时钟源的指定时间服务器。

**参数：**ip-address：时间服务器IPv4地址。

ipv6-address：时间服务器IPv6地址。

source：为该sever指定的源地址接口。

vlan：为该server配置虚拟局域网。

vlan no：虚拟局域网号，取值<1-4094>。

loopback：为该server配置环回接口。

loopback no：Loopback标示符，取值<1-1024>。

version：为该server配置版本信息。

version_no：server的版本号，取值<1-4>，默认为4

<vrfname>:vrf 实例名

<hostname>:服务器主机域名

**缺省情况：**没有配置时间服务器。

**命令模式：**全局配置模式。

**使用指南：**

**举例：**

在交换机上配置时间服务器地址1.1.1.1，指定源地址接口为vlan 1：

Switch(config)#sntp server 1.1.1.1 source vlan 1

在交换机上删除地址为1.1.1.1，指定源地址接口为vlan 1的时间服务器：

Switch(config)#no sntp server 1.1.1.1 source vlan 1

## 10.2.5 show sntp

**命令：show sntp**

**功能：**显示 SNTP 客户端目前的配置及服务器状态。

**参数：**无。

**命令模式：**特权和配置模式。

**举例：**显示 SNTP 当前配置。

Switch#show sntp

server address version last receive

2.1.0.2 1 6

# 10.3 DNSv4v6

## 10.3.1 clear dynamic-host

**命令：clear dynamic-host {*<ip-address>*|*<ipv6-address>*|*all* }**

**功能：**删除动态缓存中指定地址的或者所有的域名表项。

**参数：*<ip-address>***为 IP 地址，点分十进制格式，***<ipv6-address>***为 IPv6 地址。all 是删除所有的域名地址映射关系。

**命令模式：**特权模式。

**缺省情况：**缺省为不配置。

**使用指南：**本命令用于手动删除动态域名缓存中的域名和地址表项, 当域名在缓存中存活的时间太长时，此命令显得非常有用。

**举例：**删除地址为 202.108.22.5 的域名表项。

Switch#clear dynamic-host 202.108.22.5

## 10.3.2 debug dns

**命令：debug dns {all | packet [send | recv]| events|relay}**

**no debug dns {all | packet [send | recv]| events|relay}**

**功能：**显示进行 DNS 域名解析时的应用调试信息，该命令的 **no** 形式关闭 DEBUG 显示。

**参数：**无。

**命令模式：**特权模式。

**举例：**

Switch#debug dns all

Switch#ping host www.sina.com.cn

%Jan 01 00:03:13 2006 domain name www.sina.com.cn is to be parsed!

%Jan 01 00:03:13 2006 Dns query type is A!

%Jan 01 00:03:13 2006 Connect dns server 10.1.120.241 ......

ping www.sina.com.cn [202.108.33.32]

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 202.108.33.32, timeout is 2 seconds.

%Jan 01 00:03:15 2006 Host:www.sina.com.cn Address:202.108.33.32

.....

Success rate is 0 percent (0/5), round-trip min/avg/max = 0/0/0 ms

## 10.3.3 dns-server

**命令：dns-server {*<ip-address>*|*<ipv6-address>*} [priority *<value>*]**

**no dns-server {*<ip-address>*|*<ipv6-address>*}**

**功能：**配置/删除 DNS 服务器。

**参数：*<ip-address>***为 IP 地址，点分十进制格式，***<ipv6-address>***为 IPv6 地址，

***<value>***为 DNS 服务器的优先级，范围 0～255，默认为 0。

**命令模式：**全局配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**本命令用于配置/删除 DNS 服务器，当需要进行动态域名解析时，交换机向配置的 DNS 服务器发出域名查询请求，DNS 服务器最多配置 6 个。其中优先级为可选参数，如果配置了优先级，则按照优先级从大到小的顺序来组织 DNS 服务器，即交换机首先向优先级最大的服务器发送域名查询请求，因此可以把一些查询速度较快、经常使用的 DNS 服务器配置成较高的优先级，以方便查询。如果不配置优先级，则按照配置的先后顺序来查询 DNS 服务器。交换机做为 DNS SERVER 功能时，对 DNS SERVER 的查询不按照上面的优先级原则，而是统一向所有配置的服务器发送请求。

**举例：**配置优先级为 200 的 DNS 服务器 10.1.120.241。

Switch(config)#dns-server 10.1.120.241 priority 200

## 10.3.4 dns lookup

**命令：dns lookup {ipv4|ipv6} *<hostname>***

**功能：**执行 DNS 动态域名解析。

**参数：{ipv4|ipv6}**表示 IPv4 或者 IPv6 地址查询，***<hostname>***为要解析的动态主机名，最大 63 个字符。

**命令模式：**全局配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**本命令根据输入的主机名进行相应地址的查询，可以进行 IPv4 或者 IPv6 地址的查询，查询到的域名和对应地址存储在动态缓存中。本命令只是单独为了进行域名解析，没有什么应用功能，命令使用过程中不能进行中断，如果配置多个服务器和域名后缀，在进行域名解析的时候可能要很长时间。

**举例：**查询 www.sina.com 的 IPv4 地址。

Switch(config)#dns lookup ipv4 www.sina.com

## 10.3.5 show dns name-server

**命令：show dns name-server**

**功能：**显示配置的 DNS 服务器信息。

**参数：**无。

**命令模式：**特权和配置模式。

**举例：**

Switch#show dns name-server

DNS NAME SERVER:

| Address | Priority |
|---|---|
| 10.1.120.231 | 100 |
| 10.1.180.85 | 80 |
| 2001::1 | 20 |

## 10.3.6 show dns domain-list

**命令：show dns domain-list**

**功能：**显示配置的 DNS 域名后缀信息。

**参数：**无。

**命令模式：**特权和配置模式。

**举例：**

Switch#show dns domain-list

DNS DOMAIN LIST:

com.cn

edu.cn

## 10.3.7 show dns hosts

**命令：show dns hosts**

**功能：**显示交换机中解析到的动态域名信息。

**参数：**无。

**命令模式：**特权和配置模式。

**举例：**

Switch# show dns hosts

Total number of dynamic host is 2

DNS HOST LIST：

| Hostname | Address | Time to live | Type |
|---|---|---|---|
| www.sina.com.cn | 202.108.33.32 | 168000 | dynamic |
| www.ipv6.org | 2001:6b0:1: | 168060 | dynamic |

## 10.3.8 show dns config

**命令：show dns config**

**功能：**显示交换机中配置的 DNS 全局信息。

**参数：**无。

**命令模式：**特权和配置模式。

**举例：**

Switch(config)#show dns config

ip dns server enable

ip domain-lookup enable

the maximum of dns client in cache is 3000, timeout is 5

dns client number in cache is 0

dns dynamic host in cache is 0

dns name server number is 1

dns domain-list number is 0

## 10.3.9 show dns client

**命令：show dns client**

**功能：**显示交换机中维护的 DNS Client 信息。

**参数：**无。

**命令模式：**特权和配置模式。

**举例：**

Switch(config)#show dns client

DNS REQUEST LIST:

Total number of dns request is 2

| Address | Request Id |
|---|---|
| 192.168.11.141 | 1 |
| 192.168.11.138 | 2 |

## 10.3.10 ip domain-lookup

**命令：ip domain-lookup**

**no ip domain-lookup**

**功能：**启动/关闭 DNS 功能，交换机是否会向真正的 DNS 服务器进行动态的 DNS 域名查询。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**本命令用于启动/关闭交换机 DNS 动态查询功能。当启动 DNS 动态查询功能后，应用工具(如 ping 等)或者交换机作 DNS SERVER 时遇到域名处理时会向配置的 DNS 服务器发送域名解析请求，得到该域名对应的 IPv4/IPv6 地址。关闭该功能后，遇到域名处理时则不再发送域名解析请求，而只在静态配置的域名中查找，即不再执行动态域名解析，如果此时动态域名缓存中存在以前解析到的域名，也不会去删除，也不会去查找，在时间老化后会被自动删除。

**举例：**启动 DNS 功能，能够动态解析域名。

Switch(config)#ip domain-lookup

## 10.3.11 ip domain-list

**命令：ip domain-list *<WORD>***

**no ip domain-list *<WORD>***

**功能：**配置/删除域名后缀。

**参数：*<WORD>***为域名后缀字符串，最大 63 个字符。

**命令模式：**全局配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**本命令用于配置/删除域名后缀，当输入不完整的域名(如 sina)时，交换机自动添加域名后缀以后再进行域名解析，域名后缀最多配置 6 个。其中先配置的域名后缀则先被添加。

**举例：**配置域名后缀 com。

Switch(config)#ip domain-list com

## 10.3.12 ip dns server

**命令：ip dns server**

**no ip dns server**

**功能：**启动/关闭 DNS SERVER 功能。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**当启动了 DNS SERVER 功能后，能够接收处理客户端的 DNS Request，或者本地查找结果或者向真正 DNS 服务器请求。

**举例：**配置交换机启动 dns server 的功能。

Switch(config)#ip dns server

## 10.3.13 ip dns server queue maximum

**命令：ip dns server queue maximum <1-5000>**

**no ip dns server queue maximum**

**功能：**配置交换机缓存客户信息的最大数量。

**参数：**<1-5000>可以配置 1－5000 个。

**命令模式：**全局配置模式。

**缺省情况：**默认是允许 3000 个用户。

**使用指南：**当接收客户端的 DNS Request 后，交换机会缓存该客户的信息，但是维护的客户信息数量不能超过配置的最大值，超过该值后，该客户的请求不能被处理。

**举例：**配置交换机缓存客户信息的最大数量为 2000。

Switch(config)#ip dns server queue maximum 2000

### 10.3.14 ip dns server queue timeout

**命令：ip dns server queue timeout <1-100>**

**no ip dns server queue timeout**

**功能：**配置交换机缓存客户信息的最大超时时间。

**参数：**<1-100> 可以配置 1－100s 的超时时间。

**命令模式：**全局配置模式。

**缺省情况：**默认是 5s 的超时时间。

**使用指南：**当接收客户端的 DNS Request 后，交换机会缓存该客户的信息，但是维护的客户信息时间不能超过配置的最大超时时间，超时后该客户的信息被清除。

**举例：**配置交换机缓存客户信息的最大超时时间为 10s。

Switch(config)#ip dns server queue timeout 10

## 10.4 夏令时

### 10.4.1 clock summer-time absolute

**命令：clock summer-time <*word*> absolute <*HH:MM*> <*YYYY.MM.DD*> <*HH:MM*> <*YYYY.MM.DD*> [<*offset*>]**

**no clock summer-time**

**功能：**配置夏令时时间范围的具体值，在该范围的时间为夏令时时间，其余为非夏令时时间。本命令的 no 操作为删除夏令时配置。

**参数：*<word>***为夏令时时区名；***<HH:MM>***为起始时间，具体格式 小时（范围 0-23）：分钟（范围 0-59）；***<YYYY.MM.DD>***为起始日期，具体格式 年（范围 2001-2037）.月（范围 1-12）.日（范围 1-31）；***<HH:MM>***为结束时间，具体格式小时（范围 0-23）：分钟（范围 0-59）；***<YYYY.MM.DD>***为结束日期，具体格式年（范围 2001-2037）.月（范围 1-12）.日（范围 1-31）；***<offset>***为时间偏移量，范围是 1-1440，单位：分，缺省值为 60 分。

**缺省情况：**系统缺省为没有配置夏令时时间范围。

**命令模式：**全局配置模式。

**使用指南：**本命令设置夏令时起始和结束的绝对时间点，当系统时间到达夏令时开始时间点时，时钟进行跳变，增加***<offset>***值，系统进入夏令时。当系统时间到达夏令时结束时间点时，时钟再次跳变，减去***<offset>***值，系统结束夏令时。进行配置时，夏令时结束时间应大于夏令时开始时间。

**举例：**配置夏令时时间范围为 2010 年 4 月 6 日 12 点 10 分到 2010 年 8 月 6 日 12 点 10 分，偏移值为 70 分钟，且命名为 aaa。

Switch(config)# clock summer-time aaa absolute 12:10 2010.4.6 12:10 2010.8.6 70

## 10.4.2 clock summer-time recurring

**命 令： clock summer-time <*word*> recurring <*HH:MM*> <*MM.DD*> <*HH:MM*> <*MM.DD*> [<*offset*>]**

**no clock summer-time**

**功能：**配置循环的夏令时时间范围值，在该范围的时间为夏令时时间，其余为非夏令时。

**参数：*<word>***为夏令时时区名；***<HH:MM>***为起始时间，具体格式小时（范围 0-23）：分钟（范围 0-59）；***<MM.DD>***为起始日期，具体格式月（范围 1-12）.日（范围 1-31）；***<HH:MM>***为结束时间，具体格式小时（范围 0-23）：分钟（范围 0-59）；***<MM.DD>***为结束日期，具体格式月（范围 1-12）.日（范围 1-31）；***<offset>***为时间偏移量，范围是 1-1440，单位：分，缺省值为 60 分。

**缺省情况：**系统缺省为没有配置夏令时时间范围。

**命令模式：**全局配置模式。

**使用指南：**本命令设置循环夏令时起始和结束的时间点，当系统时间到达夏令时开始时间点，则系统时钟进行跳变，增加***<offset>***值，系统进入夏令时。当系统时间到达夏令时结束时间点时，时钟再次跳变，减去***<offset>***值，系统结束夏令时。循环夏令时与年份无关，每一年当系统时钟运行到夏令时开始和结束时间点时，都会出现夏令时跳变。本命令支持南半球夏令时。

**举例：**配置夏令时时间为每年的 4 月 6 日 12 点 10 分到 8 月 6 日 12 点 10 分，偏移值为 70 分钟，且命名为 aaa。

Switch(config)# clock summer-time aaa recurring 12:10 4.6 12:10 8.6 70

## 10.4.3 clock summer-time recurring

**命 令： clock summer-time <*word*> recurring <*HH:MM*> <*week*> <*day*> <*month*> < *HH:MM* > <*week*> <*day*> <*month*> [<*offset*>]**

**no clock summer-time**

**功能：**配置循环的夏令时时间范围值，在该范围的时间为夏令时时间，其余为非夏令时。

**参数：*<word>***为夏令时时区名；***<HH:MM>***为起始时间，具体格式小时（范围 0-23）：分钟（范围 0-59）；***<week>***为第几周，配置值为：1-4，first 或 last；***<day>***为星期值，配置值为：“Sun”, “Mon”, “Tue”, “Wed”, “Thu”, “Fri”, “Sat”；***<month>***为月份值，配置值为：“Jan”, “Feb”, “Mar”, “Apr”, “May”,“Jun”,“Jul”, “Aug”, “Sep”, “Oct”, “Nov”, “Dec”；***<HH:MM>***为结束时间，具体格式小时（范围 0-23）：分钟（范围 0-59）；***<week>***为第几周，配置值为：1-4，first 或 last；***<day>***为星期值，配置值为：“Sun”, “Mon”, “Tue”, “Wed”, “Thu”, “Fri”, “Sat”；<month>为月份值，配置值为：“Jan”, “Feb”, “Mar”, “Apr”, “May”, “Jun”,“Jul”, “Aug”, “Sep”, “Oct”, “Nov”, “Dec”；***<offset>***为时间偏移量，范围是 1-1440，单位：分，缺省值为 60 分。

**缺省情况：**系统缺省为没有配置夏令时时间范围。

**命令模式：**全局配置模式。

**使用指南：**本命令可灵活设置循环夏令时起始和结束的时间点，既可以设置某月的第几个星期几进入或退出夏令时，也可设置某月的第一个或最后一个星期几进入或退出夏令时。当系统时间到达夏令时开始时间点，则系统时钟进行跳变，增加***<offset>***值，系统进入夏令时。当系统时间到达夏令时结束时间点时，时钟再次跳变，减去***<offset>***值，系统结束夏令时。循环夏令时与年份无关，每一年当系统时钟运行到夏令时开始和结束时间点时，都会出现夏令时跳变。本命令支持南半球夏令时。

**举例：**配置夏令时时间为每年 4 月第一个星期一 12 点 10 分开始到 8 月最后一个星期六 12 点 10 分结束，偏移值为 70 分钟，且命名为 aaa。

Switch(config)# clock summer-time aaa recurring 12:10 1 mon apr 12:10 last sat aug 70

# 第 11 章 POE 命令

## 11.1 POE

### 11.1.1 PoE

#### 11.1.1.1 power inline enable(全局)

**命令：power inline enable**

**no power inline enable**

**功能：**打开/关闭全局 PoE 供电。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**全局供电状态为关闭。

**使用指南：**全局关闭后，不论端口的供电状态是打开还是关闭，均不会对外供电。

**举例：**关闭全局供电。

Switch(config)#no power inline enable

#### 11.1.1.2 power inline enable(端口)

**命令：power inline enable**

**no power inline enable**

**功能**：打开/关闭端口 PoE 供电。

**参数**：无。

**命令模式**：端口配置模式。

**缺省情况**：端口供电状态为打开。

**使用指南**：使能时：自动检测。处于该状态时，PSE 自动检测 PD，并自动进行分类，然后根据分类进行供电。当 PSE 检测到有 PD 连接时，如果此时有足够的剩余功率，则给该 PD 指定的输出功率，并更新 LED 的指示；如果没有足够的功率，则由功率分配机制决定是否供电。当在该状态正常供电过程中，PD 有额外申请功率并超过最高设定阈值，则断开对该 PD 的供电，并更新 LED 的指示。当正常断开 PD 与 PSE 的连接时，则 PSE 停止对外供电，并更新 LED 的指示。

关闭时：禁止供电。关闭 PSE 供电功能，无论是否有 PD 连接都不对其进行供电。此时端口为普通以太网的数据端口，不影响数据的转发。

全局关闭后，不论端口的供电状态是打开还是关闭，均不会对外供电。

**举例**：关闭端口 1、3、4、5、6 的供电。

Switch(config)#interface ethernet 1/0/1;3-6

Switch(Config-If-Port-Range)#no power inline enable

## 11.1.1.3 power inline power-up mode

**命令**：**power inline power-up mode (af|high-inrush|pre-at|at|pre-bt|bt-type3|bt-type4)**

**no power inline power-up mode**

**功能**：修改 POE 端口上电模式。

**参数**：af：IEEE 802.3af 模式，一般为支持 IEEE 802.3af 模式的 PD 供电；

high-inrush：浪涌电流 700 毫安~1 安，一般为非标 PD 供电；

pre-at：Pre-IEEE 802.3at 模式，浪涌电流 400 毫安~450 毫安，在端口上电后 75 毫秒内切换到更高的电流（700 毫安~1.0 安），一般为支持 Pre-IEEE 802.3at 模式的 PD 供电；

at：IEEE 802.3at 模式，浪涌电流 700 毫安~1.0 安, 一般为支持 IEEE 802.3at 模式的 PD 供电。

Pre-bt: Pre-IEEE 802.3bt type3 模式，冲击电流限制在 850mA，上电电流限制在 850mA

Bt-type3：IEEE 802.3bt type3 模式，冲击电流限制在 425mA，上电电流限制在 850mA，PD 一般最低输入功率在 51W 至 60W，可以支持到 class6

Bt-type4：IEEE 802.3bt type4 模式，冲击电流限制在 850mA，上电电流限制在 850mA，PD 一般最低输入功率在 71W 至 90W，可以支持到 class8

**命令模式**：端口配置模式。

**缺省情况**：bt-byte4 模式。

**使用指南**：需要根据 PD 支持情况来选择端口的上电模式。

**举例**：将端口的 POE 上电模式修改为 IEEE 802.3at 模式。

Switch(config)#interface ethernet 1/0/1;3-6

Switch(Config-If-Port-Range)#power inline power-up mode at

## 11.1.1.4 power inline high-inrush（全局命令）

本型号交换机不支持此命令。

## 11.1.1.5 power inline legacy

**命令：power inline legacy enable**

**no power inline legacy enable**

**功能**：设定是否对非 IEEE 标准 PD 进行供电。

**参数**：无。

**命令模式**：全局配置模式。

**缺省情况**：不对非 IEEE 标准 PD 供电。

**使用指南**：打开该功能时，交换机可以兼容非 IEEE 标准的 PD，并对其进行正常供电。

**举例**：设置交换机可对非标准 PD 供电。

Switch(config)#power inline legacy enable

## 11.1.1.6 power inline max(全局)

**命令：power inline max *<max-wattage>***

**no power inline max**

**功能**：设定 PoE 电源的全局最大输出功率。

**参数：max-wattage**: 最大功率值。单位为 W，粒度为 1W，全局可设置范围 37~370W。

**命令模式：** 全局配置模式。

**缺省情况：** 全局最大输出功率为 370W。no 命令将恢复到缺省配置。

**使用指南**：设定 PoE 电源的全局最大输出功率，以保证电源供电安全，也可用于有效控制下联设备的消耗功率。

**举例**：设置全局最大可输出功率为 50W。

Switch(config)#power inline max 50

## 11.1.1.7 power inline max(端口)

**命令：power inline max *<max-wattage>***

**no power inline max**

**功能**：设定端口最大输出功率。

**参数：** max-wattage：最大功率值。单位为 mW，粒度为 100mW，端口可设置范围为 1~15400mW (802.3af)/1~3000mW (802.3at)。不足 100mW 以 100mW 计，即 1~100 均为 100，15301~15400 均为 15400，同时保持用户配置的值不变，不进行归整处理。

**命令模式：** 端口配置模式。

**缺省情况：** 端口最大输出功率为 9W。

**使用指南：**在与全局最大功率的配合下，有效控制各个端口的输出功率。

**举例：**设定端口 1 的最大输出功率为 0.8W。

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#power inline max 800

## 11.1.1.8 power inline max-power-type (端口)

**命令：power inline max-power-type <*class*|*user-defined*>**

**no power inline max-power-type**

**功能：**设定端口最大输出功率类型是根据 PD class 分类还是根据用户自定义

**参数：** class：端口最大输出功率类型以 PD class 分类的级别为准

user-defined：端口最大输出功率类型以用户自定义的为准，此时可以通过 power inline max 命令来配置端口的最大输出功率

**命令模式：** 端口配置模式。

**缺省情况：** class 模式

**使用指南：**user-defined 模式在与端口最大功率的配合下，有效控制各个端口的输出功率；Class 模式下则 power inline max 命令无效

**举例：**设定端口 1 的最大输出功率类型以用户自定义为准

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#power inline max-power-type user-defined

## 11.1.1.9 power inline police

**命令：power inline police enable**

**no power inline police enable**

**功能：**打开/关闭功率优先级管理策略模式。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**功率优先级管理策略模式关闭。

**使用指南：**功率管理策略是否使用优先级策略。使能命令使用优先级策略，no 命令恢复先到先得策略。当打开优先级策略时，可对端口的优先级进行单独配置。

在优先级模式下，当 PSE 剩余功率不足时，将自动关闭低优先级的端口，保证高优先级端口的正常供电，而与 PD 接入的时间无关。若端口的优先级相同，则序号小的端口的优先级较高。

在先到先得模式下，当 PSE 剩余功率不足时，不能对新接入的 PD 进行供电。

**举例**：打开功率优先级策略模式。

Switch(config)#power inline police enable

### 11.1.1.10 power inline priority

**命令**：**power inline priority {critical | high | low}**

**功能**：设置端口供电优先级。

**参数**：**critical**：极高优先级；**high**：高优先级；**low**：低优先级。

**命令模式**：端口配置模式。

**缺省情况**：端口优先级为 low。

**使用指南**：在 **power inline police enable** 状态下生效，在剩余功率不足以对新接入的 PD 供电时，对高优先级的端口优先供电。

**举例**：调整端口 1 的优先级为 high，2 的优先级为 critical。

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#power inline priority high

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#power inline priority critical

### 11.1.1.11 power inline power-off time-range

**命令**：**power inline power-off time-range *<time-range-name>***

**no power inline power-off time-range**

**功能**：设置/取消 POE 端口下电时间段。

**参数**：***time-range-name***：时间策略名称。

**命令模式**：端口配置模式。

**缺省情况**：无下电时间段配置。

**使用指南**：需要先通过 ***time-range*** 配置时间策略名称 ***time-range-name***，再对 POE 端口配置该命令关联 ***time-range-name***，起始时间对 POE 端口下电，结束时间恢复 POE 端口供电。

**举例**：配置 1/0/2 端口每天 8:30:00 下电，17:30:00 恢复供电。

Switch(config)# time-range abc

Switch(config-time-range-abc)#periodic daily 8:30:00 to 17:30:00

Switch(config-time-range-abc)#quit

Switch(config)#interface ethernet 1/0/2

Switch(config-if-ethernet1/0/2)#power inline power-off time-range abc

## 11.1.2 PoE 监控和调试

### 11.1.2.1 监控和调试信息

## 11.1.2.1.1 show power inline

**命令：show power inline**

**功能：**显示全局 PoE 设置与状态。

**参数：**无。

**命令模式：**特权用户模式。

**缺省情况：**无。

**使用指南：**各显示字段含义如下表

| 字段 | 描述 |
| --- | --- |
| Power Inline Status | 全局功能开关状态 |
| Power Avaliable | 全局可用功率上限值 |
| Power Used | 全局功率已使用值 |
| Power Remaining | 全局剩余可用功率 |
| Police | 功率优先策略开关状态 |
| Legacy | 检测非标准 PD 开关状态 |
| Disconnect | 断开 PD 的方式 |
| HW Version | PoE 模块硬件版本号 |
| SW Version | PoE 模块软件版本号 |
| Mode | 供电模式<br>signal：信号线供电（Alternative A）<br>spare：空闲线供电（Alternative B） |

**举例：** 显示当前 PoE 的全局状态，功率上限值单电源 500W，双电源 1000W。

```
switch#show power inline

Power Inline Status: On
Power Available: 500 W
Power Used: 0 W
Power Remaining: 500 W
Min Voltage: 44 V
Max Voltage: 57 V
Police: Off
Legacy: Off
Disconnect: Dc
Mode: Signal
Pse Type: RTL
```

HW Version:

SW Version: 1.0.0.8

## 11.1.2.1.2 show power inline interface ethernet

**命令：show power inline interface [ethernet <*interface-number*> | <*interface-name*>]**

**功能：**显示端口 PoE 的配置与状态。

**参数：**interface-list：端口列表。若缺省该参数则显示所有端口。

**命令模式：**特权用户模式。

**缺省情况：**无。

**使用指南：**各字段含义如下表

| 字段 | 描述 |
|---|---|
| Interface | 以太网端口号 |
| Status | 供电状态<br>enable：使能<br>disable：关闭供电功能 |
| Oper | 工作状态<br>on：PD 连接并正常受电<br>off：PD 未连接<br>faulty：PD 检测出错<br>deny：可用功率不够或 PD 申请功率过大 |
| Power | 端口当前使用的功率 |
| Max-type | 端口当前最大输出功率类型 |
| Max | 端口最大分配的功率 |
| Current | 端口当前的电流 |
| Volt | 端口当前的电压 |
| Priority | 供电优先级<br>critical：极高优先级<br>high：高优先级<br>low：低优先级 |
| Class | 分类 用途 PD 输入功率（W）<br>0 缺省 0.44~12.95<br>1 可选 0.44~3.84<br>2 可选 3.84~6.49<br>3 可选 6.49~12.95<br>4 可选 12.95~25.5<br>5 可选 25.5~40<br>6 可选 40~51 |

| | |
|---|---|
| | 7 可选 51~62<br>8 可选 62~71 |

**举例：**显示当前 PoE 设备 1 到 6 端口的状态。

switch#show power inline interface

Interface Status Oper Power(mW) Max-type Max(mW) Current(mA) Volt(V) Priority Class

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

Ethernet1/0/1 enable off 0 class 90000 0 0 low 0

Ethernet1/0/2 enable off 0 class 90000 0 0 low 0

Ethernet1/0/3 enable off 0 class 90000 0 0 low 0

Ethernet1/0/4 enable off 0 class 90000 0 0 low 0

Ethernet1/0/5 enable off 0 class 90000 0 0 low 0

Ethernet1/0/6 enable off 0 class 90000 0 0 low 0

## 11.1.2.1.3 debug power inline

**命令：debug power inline**

**no debug power inline**

**功能：**PoE 功能排错开关。

**参数：**无。

**命令模式：**特权用户模式。

**缺省情况：**无。

**使用指南：**当打开该排错开关后，命令执行时的关键过程都会有相关打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

**举例：**打开 PoE 的排错功能。

Switch#debug power inline

# 第 12 章 虚拟化命令

## 12.1 VSF

### 12.1.1 Basic VSF

#### 12.1.1.1 switch convert mode

**命令：switch convert mode ( stand-alone | vsf )**

**功能：**令设备由独立运行模式转换到 VSF 模式，或由 VSF 模式转到独立运行模式。

**参数：** ***<stand-alone>***：独立运行模式，***<vsf>***：VSF 模式。

**缺省情况：**启动时根据 VSF 配置文件 vsf.cfg 判断设备应进入的模式。

**命令模式：**全局配置模式。

**运行模式：**独立运行模式，VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**设备支持两种运行模式：独立运行模式、VSF 模式。处于独立运行模式下的设备只能单机运行，处于 VSF 模式下的设备可以与其他设备形成 VSF。两种模式通过命令行进行切换。

**举例：**设备处于独立运行模式时，配置设备进入 VSF 模式。

Switch#config

Switch(config)#switch convert mode vsf

#### 12.1.1.2 write

**命令：write**

**功能：**设备处于独立运行模式时，write 命令除具有保存当前 running-config 的功能外，还将当前 VSF 相关配置写入 vsf.cfg；若设备处于 VSF 模式，则 write 操作会将当前 running-config 保存在 vsf_startup.cfg 中，并将当前 VSF 相关配置保存到 vsf.cfg 中。

**参数：**无。

**缺省情况：**running-config 和 vsf 相关配置未保存。

**命令模式：**特权模式。

**运行模式：**独立运行模式，VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**具备 VSF 功能的设备，进行配置保存时，将当前配置信息分别写入 startup.cfg 和 vsf.cfg。

**举例：**保存配置。

Switch#write

## 12.1.1.3 vsf port-group

**命令：vsf port-group <*port-number*>**

**no vsf port-group <*port-number*>**

**功能：**配置逻辑 VSF 口。no 命令为删除 VSF 口。

**参数： <*port-number*>：**逻辑 VSF 口编号，取值 1-2。

**缺省情况：**未配置。

**命令模式：**全局配置模式。

**运行模式：**独立运行模式，VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**配置逻辑 VSF 口，同一台设备只能配置两个 vsf port-group，vsf port-group1 和 vsf port-group2。

**举例：**配置逻辑 VSF 口。

Switch(config)#vsf port-group 1

## 12.1.1.4 vsf port-group interface ethernet

**命令：vsf port-group interface Ethernet <*interface-list*>**

**no vsf port-group interface Ethernet <*interface-list*>**

**功能：**建立逻辑 VSF 口后，在 VSF 口模式下，绑定实际物理端口。No 命令是去除物理端口与逻辑 VSF 口的绑定。

**参数：< *interface-list* >：**物理端口号。

**缺省情况：**缺省未绑定物理端口。

**命令模式：**VSF 口模式。

**运行模式：**独立运行模式，VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**一个 vsf port-group 最多绑定 8 个物理端口，端口加入 vsf port-group 模式为 on。当多于 8 个端口进行绑定的时候，提示用户不能绑定。支持跨板绑定物理端口。目前只支持万兆口与逻辑 VSF 口进行绑定。

**举例：**建立逻辑 VSF 口，并进入 VSF 口配置模式，将物理端口 1/1/1 与逻辑 VSF 口绑定。

Switch(config)# vsf port-group 1

Switch(config)# vsf port-group interface ethernet 1/1/1

## 12.1.1.5 vsf domain

**命令：vsf domain <*domain-id*>**

**no vsf domain**

**功能：**配置 VSF 所在逻辑域，no 命令为恢复默认域号，默认域号为 1。设备处于独立运行模式时，vsf 域的配置立即生效，设备处于 VSF 模式时，配置 vsf domain 后，running-config 中显示为最新的配置，但该配置在保存并重启后生效。

**参数：** ***<domain-id>***：域号，取值范围 1-32。

**缺省情况：**设备处于 domain 1 中。

**命令模式：**全局配置模式。

**运行模式：**独立运行模式，VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**域是一个逻辑概念，设备通过 VSF 链路连接在一起就组成一个 VSF，这些成员设备的集合就是一个 VSF 域。为了适应各种组网应用，同一个网络里可以部署多个 VSF，VSF 之间使用域编号来以示区别。同一域内的设备可以形成 VSF，不同域的设备或 VSF 组不能形成 VSF，在形成 VSF 前要进行域号的冲突判断。域号的默认值为 1。

## 12.1.1.6 vsf member

**命令：vsf member <*member-id*>**

**no vsf member <*member-id*>**

**功能：**设置 VSF 成员编号，no 命令为删除设备 VSF 成员编号。

**参数：** ***<member-id>***：成员编号，取值范围是<1-8>

**缺省情况：**设备没有成员编号。

**命令模式：**全局配置模式。

**运行模式：**独立运行模式。

**使用指南：**成员编号标识每台设备，VSF 组中，每台设备都拥有唯一的成员编号。配置该编号后才能进入 VSF 模式，配置多次该命令，最后一次生效。初始化状态，没有成员编号。设备进入 VSF 模式后，端口格式根据成员编号进行修改。成员编号的冲突，不能形成 VSF。

## 12.1.1.7 vsf non-wait port-inactive

**命令：vsf non-wait port-inactive**

**no vsf non-wait port-inactive**

**功能：**快速检测 VSF 链路状态变化，用于需要快速发现 vsf 分裂的场景。该命令的 no 命令将恢复检测 VSF 链路状态为默认方式。

**参数：**无。

**缺省情况：**未配置快速检测 VSF 链路状态功能。

**命令模式：**全局配置模式。

**运行模式：**VSF 运行模式。

**使用指南：**配置该命令后，如果 VSF 链路状态发生变化，系统会立刻收到并确认 VSF 链路状态，快速检测 VSF 拓扑变化。该命令配置后立即生效，建议在 VSF 物理链路稳定的情况下使用。

## 12.1.1.8 vsf priority

**命令：vsf priority <*priority*>**

**no vsf priority**

**功能：**配置 VSF 成员在 VSF 组中的优先级，该命令的 no 命令为恢复为默认优先级，默认优先级为 1。设备处于独立运行模式时，vsf 成员优先级的配置立即生效，设备处于 VSF 模式时，配置 vsf 成员优先级后，running-config 中显示为最新的配置，但该配置在保存并重启后生效。

**参数：** **< *priority* >**：VSF 成员优先级值，取值范围 1~32。

**缺省情况：**设备默认优先级为 1。

**命令模式：**全局配置模式。

**运行模式：**独立运行模式，VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**独立运行模式下，配置成员优先级。成员优先级用于角色选举，成员优先级值越大表示优先级越高，优先级高的设备竞选时，成为 Master 的可能性越大。通过给不同的设备配置不同的优先级，可以指定某一设备作为 VSF 的 Master。

## 12.1.1.9 vsf auto-merge enable

**命令：vsf auto-merge enable**

**no vsf auto-merge enable**

**功能：**使能 VSF 组自动合并功能，该命令的 no 命令去除自动合并功能。

**参数：** 无

**缺省情况：**默认没有开启自动合并功能。

**命令模式：**全局配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**当两 VSF 组由于某种原因具备了正确的物理连接，且连接方式为使用各自的 VSF 口进行连接，并且未出现 vsf domain、vsf member id 冲突，则连接过程中，端口的 up、VSF 口的建立和绑定等操作，会触发两 VSF 组进行自动合并。合并过程中，通过优先级和 member id 的比较，竞选失败的 VSF 组将会进行重启，重启后加入到竞选胜利的 VSF 组中。

## 12.1.1.10 vsf member description

**命令：vsf member <*member-id*> description <*text*>**

**no vsf member <*member-id*> description**

**功能：**对 VSF 成员进行描述，此描述信息只写入 VSF 主控配置文件中。该命令的 no 命令为删除对应 VSF 成员的描述信息。

**参数： <*member-id*>：**VSF 成员编号，**<*text*>：**用户自定义描述信息。

**缺省情况：**VSF 成员没有任何描述信息。

**命令模式：**全局配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**在 VSF 模式下，添加对设备的描述信息。方便对设备进行管理，比如，一个网络中存在多个 VSF，或者一个 VSF 的成员物理位置比较分散时，则可通过添加描述的方法来明确网络拓扑中各设备角色以及其他用户自定义信息。

## 12.1.1.11 vsf link delay

**命令：vsf link delay<*interval*>**

**no vsf link delay**

**功能：**配置 VSF 链路 down 延迟上报功能，用于避免因端口链路层状态在短时间内频繁改变，导致 VSF 分裂、合并的频繁发生。该命令的 no 命令为将延迟上报时间值恢复为默认值。

**参数： <*interval*>：**VSF 链路 down 延迟上报时间值，默认值为 0，即立即上报。

**缺省情况：**缺省未配置延迟上报时间值，该值为 0。

**命令模式：**全局配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**配置 vsf link delay 后，如果 VSF 链路状态从 up 变为 down，端口不会立即向系统报告链路状态变化。经过配置的时间间隔后，如果 VSF 链路仍然处于 down 状态，端口才向系统报告链路状态的变化，系统再作出相应的处理。如果 VSF 链路状态从 down 变为 up，链路层会立即向系统报告。该命令配置后立即生效。

## 12.1.1.12 vsf mac-address persistent

**命令：vsf mac-address persistent <*timer* | *always*>**

**no vsf mac-address persistent**

**功能：**。配置 VSF 分裂后 VSF 组 MAC 地址保留时间。该命令的 no 命令为删除 VSF 组 MAC 地址保留时间的配置，即不保留。

**参数：** ***<timer>***：配置 VSF 桥 MAC 保留时间为 6 分钟，即当 Master 离开 VSF 时，VSF 桥 MAC 地址 6 分钟内保持不变，如果 6 分钟后 Master 没有回到 VSF，则使用新选举的 Master 的桥 MAC 作为 VSF 桥 MAC；*<always>*：always 配置桥 MAC 地址保留时间为永久，则不管 Master 设备是否离开 VSF，VSF 桥 MAC 始终保持不变。

**缺省情况：**默认没有配置桥 MAC 保留时间。

**命令模式：**全局配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**VSF 作为一台虚拟设备与外界通信，也具有唯一的桥 MAC，成为 VSF 桥 MAC。通常情况下使用 Master 设备的桥 MAC 作为 VSF 桥 MAC。桥 MAC 冲突会导致通信故障，桥 MAC 切换也会导致流量中断，因此需要配置桥 MAC 的保留时间，以便在 VSF 组发生分裂后，不包含原 VSF 主控的那部分，按照用户配置来决定是否保留原 VSF 组桥 MAC，以及保留时间。配置了 timer，VSF 主控离开了 VSF，6 分钟后 VSF 原主控没有回到 VSF 组，VSF 重启，VSF 桥 MAC 使用新选举出来的 VSF 主控的 CPU-MAC 作为 VSF 桥 MAC；6 分钟之内 VSF 原主控回到 VSF 组，继续使用 VSF 原主控的 CPU-MAC 作为 VSF 的桥 MAC。配置了 always，VSF 主控离开了 VSF，VSF 不重启，一直使用原有 VSF 主控的 CPU-MAC 作为 VSF 的桥 MAC，若 VSF 重启，则使用新选举出来的 VSF 主控的 CPU-MAC 作为 VSF 桥 MAC。设备重启后，该命令不在生效，需重新配置。

## 12.1.2 VSF 冲突检测配置与调试

### 12.1.2.1 vsf mad lacp enable

**命令：vsf mad lacp enable**

**no vsf mad lacp enable**

**功能：**打开指定 port-channel 端口支持 LACP MAD 检测功能。该命令的 no 命令为关闭 port-channel 口上的 LACP MAD 检测功能。

**参数：**无。

**缺省情况：**LACP MAD 检测功能关闭。。

**命令模式：**port-channel 端口配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**处于 VSF 模式的设备才能配置该命令，配置指定的 port-channel 为 LACP MAD 冲突检测组，组成员发送带 MAD 的 TLV 报文。

**举例：在 port-channel1 端口开启 lacp** mad 检测功能。

```
Switch(config)#interface port-channel 1
Switch(config-if-port-channel1)# vsf mad lacp enable
```

## 12.1.2.2 vsf mad bfd enable

**命令：vsf mad bfd enable**

**no vsf mad bfd enable**

**功能：**打开指定接口支持 BFD MAD 检测功能。该命令的 no 命令为关闭指定接口的 BFD MAD 检测功能。

**参数：**无。

**缺省情况：**BFD MAD 检测功能关闭。

**命令模式：**接口配置模式和网管端口配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**处于 VSF 模式的设备才能配置该命令，配置指定的接口支持 BFD MAD 检测功能。

**举例：在 interface** vlan 2 开启 BFD MAD 检测功能。

Switch(config)# interface vlan 2

Switch(config-if-vlan2)# vsf mad bfd enable

## 12.1.2.3 vsf mad ip address

**命令：vsf mad ip address *<ip-address>* *<ip-mask>* member *<member-number>***

**no vsf mad ip address *<ip-address>* *<ip-mask>* member *<member-number>***

**功能：**指定接口创建成员设备对应的 BFD 会话。

**参数：*<ip-address>***：IP 地址。***<ip-mask>***：ip 地址掩码。***<member-number>***：成员设备编号，范围为：1-8.

**缺省情况：**接口未配置 MAD 地址。

**命令模式：**接口配置模式和网管端口配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**处于 VSF 模式的设备才能配置该命令，配置该命令的同时创建以配置地址为远端地址的会话。

**举例：在 interface** vlan 2 创建成员设备对应的 BFD 会话。

Switch(config)# interface vlan 2

Switch(config-if-vlan2)# vsf mad ip address 2.1.1.1 255.255.255.0 member 1

Switch(config-if-vlan2)# vsf mad ip address 2.1.1.2 255.255.255.0 member 2

## 12.1.2.4 vsf mad exclude

**命令：vsf mad exclude**

**no vsf mad exclude**

**功能：**当设备进入 recovery 状态后，配置该命令的端口可以不被关闭，继续正常转发。该命令的 no 命令为取消 MAD 保留端口配置。

**参数：**无。

**缺省情况：**设备没有配置 MAD 保留端口。

**命令模式：**端口配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**VSF 链路断开后，网络中会存在两台全局配置完全相同的设备，这些设备连接到网络时可能会引起网络故障。为了防止这种情况发生，系统会进行多 Active 检测，最终只保留一台 Active 设备，其它设备都进入 Recovery 状态，并且关闭 Recovery 状态设备上的所有业务接口。使用该命令可以让指定的端口不被关闭，具体哪些接口需要保留由用户决定。

**举例：在端口 2/1/4 配置 MAD 保留端口。**

```
Switch(config)# inte e 2/1/4
Switch (config-if-ethernet2/1/4)#vsf mad exclude
```

## 12.1.2.5 vsf mad restore

**命令：vsf mad restore**

**功能：**本命令将处于 Recovery 状态的 VSF 恢复到正常工作状态。

**参数：**无。

**缺省情况：**VSF 没有配置 restore。

**命令模式：**全局配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**VSF 链路断裂发生多 Active 冲突，原 VSF 分裂为两个状态为 Active 的 VSF，为了防止网络中配置冲突，VSF 系统会通过多 Active 检测机制，将其中一个 VSF 的状态保持为 Active（让它继续正常工作），其它 VSF 的状态修改为 Recovery（处于该状态的 VSF 不能处理业务报文）。如果处于 Active 状态的 VSF 发生故障不能工作，此时可以通过本命令将处于 Recovery 状态的 VSF 恢复到正常工作状态。

**举例：将处于 Recovery 状态的 VSF 恢复到正常工作状态。**

```
Switch(config)#vsf mad restore
```

## 12.1.3 VSF 调试

### 12.1.3.1 show running-config

**命令：show running-config**

**功能：**查看当前所有配置信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**运行模式：**独立运行模式，VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**实现 VSF 功能后，该命令把 VSF 相关的配置信息，集中在所有配置信息的最前端显示。

**举例：**

Switch# show running-config

### 12.1.3.2 show vsf

**命令：show vsf**

**功能：**显示 VSF 中所有成员设备的的相关信息，包括 VSF 的主控、备份主控，VSF 组的 CPU-MAC、VSF 的桥 MAC、对设备的描述、成员优先级。是否使能检测版本同步、桥 MAC 地址保留功能的配置信息、VSF 合并自动重启功能是否使能、VSF 域，等等。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**该命令只在 VSF 模式下可用，通过 VSF 协议获得角色选举信息，通过读每台设备的 VSF 配置文件 vsf.cfg 获得 VSF 配置信息，获得桥 MAC、CPU-MAC 等信息并显示。

**举例：**

```
Switch# sho vsf
Switch    SlotID    Role    Priority    CPU-Mac              Description
------------------------------------------------------------------------------
2         M1        M       1           00-03-0f-0f-66-b4    (null)
2         7         S       1           00-03-0f-0f-66-b4    (null)
The Bridge Mac of the VSF is: 00-03-0f-0f-66-b4
```

Auto Merge: yes

Mac Persistent: off

Domain ID: 1

## 12.1.3.3 show vsf topology

**命令：show vsf topology**

**功能：**显示当前 vsf 拓扑信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**VSF 合并或者有成员离开 VSF，都会触发 VSF 协议运行，计算新的拓扑结构，通过该命令及时获得当前的拓扑信息。

**举例：**

Switch# show vsf topology

| Switch | VSF-Port1 | Neighbor | VSF-Port2 | Neighbor |
|---|---|---|---|---|
| 2 | Ethernet2/7/3(inactive) | -- | -- | -- |

## 12.1.3.4 show vsf-config

**命令：show vsf-config**

**功能：**按设备的顺序显示 VSF 的配置信息，成员编号、成员优先级、成员 VSF 口的信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**当 VSF 组由单台设备构成，则收集本台机器 VSF 配置；若 VSF 组包含多台设备，则向其他设备发送收集配置请求，收集整个 VSF 组配置信息。

**举例：**

Switch# show vsf config

| MemberID | Priority | VSF-Port1 | VSF-Port2 |
|---|---|---|---|
| 2 | 1 | Ethernet2/7/3 | -- |

## 12.1.3.5 show mad config

**命令：show mad config**

**功能：** 查当前 VSF 的 mad 检测配置。

**参数：** 。

**缺省情况：** 。

**命令模式：** 权模式和配置模式。

**运行模式：** SF 运行模式。

**VSF 角色：** SF 主控。

**使用指南：** 命令只在 VSF 模式下可用。显示 LACP、BFD 是否开启，并获取哪些端口开启了这些功能。

**举例：**

```
Switch# show mad config
Current lacp MAD status: Disable
Current bfd MAD status: Detecting
Reserved ports:
Reserved ports(defaults):
 interface Ethernet2/7/3
MAD lacp enabled aggregation port:
MAD BFD enabled interface:
 Interface Vlan10
 vsf mad ip address 10.1.1.1 255.255.255.0 member 1
 vsf mad ip address 10.1.1.2 255.255.255.0 member 2
```

| 显示信息 | 解释 |
|---|---|
| Current lacp MAD status | 显示lacp MAD当前的状态 |
| Current bfd MAD status | 显示BFD MAD当前的状态 |
| Reserved ports | 用户配置的保留接口 |
| Reserved ports(defaults) | 统默认保留的接口（不需要用户配置，自动保留） |
| MAD lacp enabled aggregation port | 使能LACP MAD 的聚合口 |
| MAD BFD enabled interface | 使能BFD MAD 的接口 |

## 12.1.3.6 show vsf cpu-database all-member brief-information

**命令：show vsf cpu-database all-member brief-information**

**功能：**显示 CPU 数据库中所有成员简要信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**显示 CPU 数据库中全部 VSF 成员的简要信息。

**举例：**

Switch# show vsf cpu-database all-member brief-information

Vsf cpu database include 1 member:

Member 2 : cpu key:00-03-0f-0f-66-b4, PRI:1

Master is : 2, Standby is : 0

## 12.1.3.7 show vsf cpu-database member basic-information

**命令：show vsf cpu-database [member <1-8*1-8* >| basic information]**

**功能：**显示整个 vsf 或某个成员 CPU 数据库基本信息。

**参数：< *member* >：**VSF 成员，1-8**1-8:**VSF 成员 member id。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**该命令可显示 CPU 数据库中全部或者指定 VSF 成员的基本信息。

**举例：**

Switch# show vsf cpu-database member 2 basic-information

Vsf cpu database member 2 basic information:

Key: 00-03-0f-0f-66-b4

CPU-MAC: 00-03-0f-0f-66-b4

Member ID: 2

Domain ID: 1

Sequence Num: 4

Master Prioriy: 1

Units Num: 1

Dest unit: 1

Dest port: 0

Unit prefer module id: 2

Unit require module id num: 1

Vsf port num: 1

Flags: 131072

Vsf port index 1:

Unit: 0

port: 1

Weight: 0

Bflag: 1

## 12.1.3.8 show vsf cpu-database member running-information

**命令：show vsf cpu-database [member <*1-8* >| running-information]**

**功能：**显示 CPU 数据库中的运行信息。

**参数：< *member* >：**VSF 成员，**<1-8 >:**VSF 成员 member id。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**显示 CPU 数据库中全部或者指定 VSF 成员的运行信息。

**举例：**

Switch# show vsf cpu-database member 1 running-information

%Member 1 not exist in the cpu-database!

Switch# show vsf cpu-database member 2 running-information

Vsf cpu database member 2 running information:

Flags: 1

Tx unit: 0

Tx port: 0

Dest module: 2

Dest port: 0

Module ID: 2

Topo index: 0

Vsf port index 1 link info:

Flags: 0

Tx cpu key:

Tx port-group: 0

Rx cpu key:

Rx port-group: 0

## 12.1.3.9 show vsf cpu-database member port-information

**命令：show vsf cpu-database [member <*1-8* >| port-information]**

**功能：**显示 CPU 数据库中的 VSF 口基本信息。

**参数：< *member* >**：VSF 成员，**<1-8 >:**VSF 成员 member id。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**显示 CPU 数据库中全部或者指定 VSF 成员的 VSF 口基本信息。

**举例：**

```
Switch# show vsf cpu-database member 2 port-information
Vsf cpu database member 2 port information:
Vsf port index 1:
    Unit: 0
    port: 1
    Weight: 0
    Bflag: 1
```

## 12.1.3.10 show vsf cpu-database member port-link-information

**命令：show vsf cpu-database [member <*1-8* >| port-link-information]**

**功能：**显示 CPU 数据库中的 VSF 口连接信息。

**参数：< *member* >**：VSF 成员，**<1-8 >:**VSF 成员 member id。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**运行模式：**VSF 运行模式。

**VSF 角色：**VSF 主控。

**使用指南：**无。

**举例：**

```
Switch# show vsf cpu-database port-link-information
Vsf cpu database member 1 include 2 vsf port:
Vsf port index 1 link info:
    Flags:1
    Tx cpu key:00-01-05-11-11-11
    Tx stk idx:1
    Rx cpu key: 00-01-05-11-11-11
    Rx cpu key:1
Vsf port index 2 link info:
```

Flags:1

Tx cpu key:00-01-05-11-11-12

Tx stk idx:2

Rx cpu key: 00-01-05-11-11-12

Rx cpu key:2

## 12.1.3.11 show slot

**show slot**

**功能：**独立模式或者堆叠模式下查看板卡状态。

**缺省情况：**无。

**命令模式：**特权模式。

**VSF 角色：**VSF 主控。

**使用指南：** show slot 用在堆叠模式下，查看当前 vsf 主控所在的机架上的板卡状态。

**举例：**Switch#show slot

## 12.1.3.12 debug vsf packet detail <alive | all | config | member-infor | probe | routing | topo>

**命令：debug vsf packet detail <alive | all | config | member-infor | probe | routing | topo>**

**no debug vsf packet detail <alive | all | config | member-infor | probe | r routing | topo>**

**功能：**开启各种 VSF 协议报文查看开关。该命令的 no 命令为关闭相应报文的查看。

**参数：*<alive>***：保活报文；***<all>***：打开所有 VSF 协议报文；***<config>***：配置信息报文，该参数指的是查看在 config 阶段中，VSF 成员间的报文交互。这一阶段主要是 VSF 成员间通过报文交互，获取 master 选举的必要信息，进行 master、standby master 的选举；***<member-infor>***：成员信息报文；***<probe>***：VSF 成员探测报文，其作用是探测到所有 VSF 口的连接信息；***<routing>***：VSF 成员信息传播报文，这些信息包括：本地 VSF 口信息，需要的 modid 信息，芯片个数信息，Master 选举优先级，CPUDB 的状态信息以及到达此 CPU 的目的芯片号和端口号信息；***<topo>***：拓扑分析报文，拓扑分析阶段的任务是 Master 根据收集到拓扑信息计算出无环的网络，并且 Master 为所有成员分配 Module ID，计算出每个成员 VSF 口和目的 Module ID 的对应关系，然后 Master 把这些结果分发给每个成员。

**缺省情况：**默认情况下未开启。

**命令模式：**特权模式。

**VSF 角色：**VSF 主控、成员及线卡。

**使用指南：**VSF 组在形成过程中会经历 discovery、topology analysis 等阶段，在不同阶段，设备会分别处于不同的状态，比如在 discovery 阶段，设备分别经历 probe、routing 和 config 三个子阶段，通过本 debug 开关，可以有选择的查看在不同阶段的相应协议报文的细节情况。

## 12.1.3.13 debug vsf packet

**命令：debug vsf packet <all | receive | send> vsf-port <vsf-port-number>**

**no debug vsf packet <all | receive | send> vsf-port <vsf-port-number>**

**功能：**开启 VSF 报文调试信息开关。该命令的 no 命令为关闭此 debug 功能。

**参数：*<receive>***：打开收到 VSF 报文调试开关，***<send>***:打开发送 VSF 报文调试开关，***<all>***：接收和发送开同时打开，***<vsf-port-id>***：VSF 口号。

**缺省情况：**默认情况下未开启。

**命令模式：**特权模式。

**VSF 角色：**VSF 主控、成员及线卡。

**使用指南：**开启 VSF 报文调试信息开关后，可以看到 VSF 协议报文的收发。

## 12.1.3.14 debug vsf event

**命令：debug vsf event**

**no debug vsf event**

**功能：**开启 VSF 事件调试信息开关。该命令的 no 命令为关闭此 debug 功能。

**参数：**无。

**缺省情况：**默认情况下未开启。

**命令模式：**特权模式。

**VSF 角色：**VSF 主控、成员及线卡。

**使用指南：**开启 VSF 事件调试信息开关后，当 VSF 形运行各阶段中所定义的 event 事件发生后，可反馈给用户相应的输出。

## 12.1.3.15 debug vsf error

**命令：debug vsf error**

**no debug vsf error**

**功能：**开启 VSF 错误调试信息开关。该命令的 no 命令为关闭此 debug 功能。

**参数：**无。

**缺省情况：**默认情况下未开启。

**命令模式：**特权模式。

**VSF 角色：**VSF 主控、成员及线卡。

**使用指南：**开启此 debug 后，可显示 VSF 形运行各阶段中各种出错信息。

# 第 13 章 数据中心命令

## 13.1 MC-LAG 命令

### 13.1.1 evpn nve mac-address

本型号交换机不支持此命令

### 13.1.2 mac-address

**命令：mac-address XX-XX-XX-XX-XX-XX**

**no mac-address**

**功能：**配置网关接口的 mac 地址。

**参数：** XX-XX-XX-XX-XX-XX 网关接口的 mac 地址。

**命令模式：**VLAN 接口模式、NVI 接口模式。

**缺省情况：**无。

**使用指南：**MC-LAG 设备作三层网关时，两台设备相同网段的网关接口都需要配置相同的 MAC 地址；no 命令删除配置的 mac 地址。

**举例：** 配置网关接口 vlan 10 的 mac 地址为 02-02-02-02-02-02

switch(config)#interface vlan 10

switch(config-if-vlan10)#mac-address 02-02-02-02-02-02

### 13.1.3 mclag

**命令：[no] mclag**

**功能：**进入 MC-LAG 配置模式。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**执行 mclag 后进入 MC-LAG 配置模式；no 命令删除 mclag 下的配置并退出 MC-LAG 配置模式。

**举例：** 进入 MC-LAG 配置模式

switch(config)#mclag

switch(config-mclag)#

## 13.1.4 mclag domain-id

**命令：mclag domain-id <1-128>**

**no mclag domain-id**

**功能：**配置 MC-LAG 域 id。

**参数：**域 id 范围：1-128

**命令模式：**MC-LAG 模式。

**缺省情况：**无。

**使用指南：**组成 MC-LAG 的两台设备的域 id 必须保证一致；no 命令用于删除域 id 配置。

**举例：** 配置 MC-LAG 域 id 为 10

Switch(config-mclag)#mclag domain-id 10

## 13.1.5 mclag priority

**命令：mclag priority <1-256>**

**no mclag priority**

**功能：**配置 MC-LAG 域优先级。

**参数：**域优先级 范围：1-256

**命令模式：**MC-LAG 模式。

**缺省情况：**128。

**使用指南：**配置 MC-LAG 域优先级，数值越小优先级越高，优先级高的设备成为 MC-LAG 主设备；no 命令用于恢复默认的域优先级。

**举例：** 配置 MC-LAG 域优先级为 100

switch(config-mclag)#mclag priority 100

## 13.1.6 mclag enable

**命令：[no] mclag enable**

**功能：**使能 MC-LAG 功能。

**参数：**无。

**命令模式：**MC-LAG 模式。

**缺省情况：**无。

**使用指南：**使能 MC-LAG 功能；no 命令用于去使能 MC-LAG 功能。

**举例：** 配置使能 MC-LAG 功能

switch(config-mclag)#mclag enable

## 13.1.7 mclag group

**命令：[no] mclag group**

**功能：**配置 port-group 加入 MC-LAG 组。

**参数：**无。

**命令模式：**汇聚端口配置模式。

**缺省情况：**无。

**使用指南：**配置 port-group 加入 MC-LAG 组；no 命令用于配置离开 MC-LAG 组。

**举例：** 配置 port-group 10 加入 MC-LAG 组

switch(config-if-port-channel10)#mclag group

## 13.1.8 mclag local-ip

**命令：mclag local-ip A.B.C.D**

**no mclag local-ip**

**功能：**配置本机 MC-LAG 控制链路三层接口 ip 地址。

**参数：**A.B.C.D ip 地址

**命令模式：**MC-LAG 模式。

**缺省情况：**无。

**使用指南：**配置本机 MC-LAG 控制链路三层接口 ip 地址；no 命令用于取消本机 ip 地址配置。

**举例：** 配置本机 MC-LAG 控制链路三层接口 ip 地址为 20.4.4.4

switch(config-mclag)#mclag local-ip 20.4.4.4

## 13.1.9 mclag peer-ip

**命令：mclag peer-ip A.B.C.D**

**no mclag peer-ip**

**功能：**配置对端 MC-LAG 控制链路三层接口 ip 地址。

**参数：**A.B.C.D ip 地址

**命令模式：**MC-LAG 模式。

**缺省情况：**无。

**使用指南：**配置对端 MC-LAG 控制链路三层接口 ip 地址；no 命令用于取消对端 ip 地址配置。

**举例：** 配置对端 MC-LAG 控制链路三层接口 ip 地址为 20.2.2.2

switch(config-mclag)#mclag peer-ip 20.2.2.2

## 13.1.10 ip address

**命令：ip address <ipaddress> <mask> [secondary] [mc-lag]**

**no ip address <ipaddress> <mask> [secondary] [mc-lag]**

**功能：**配置 MC-LAG 三层网关独立的对外 IPv4 地址。

**参数：<ipaddress>**为 IP 地址，点分十进制格式；**<mask>**为 IP 地址掩码，点分十进制格式；**[secondary]**表示配置的 IP 地址为从 IP 地址； **[mc-lag]**表示该从地址为 MC-LAG 三层网关独立的对外 IPv4 地址。

**命令模式：**VLAN 接口配置模式。

**缺省情况：无。**

**使用指南：**一个 VLAN 接口下只能有一条 ip address mc-lag 配置，mc-lag 的独立 ip 必须同主 ip 在同一网段。no 命令用于取消该配置。

**举例：** 配置 VLAN10 接口下 MC-LAG 独立的对外 IPv4 地址为 10.10.1.3

switch(config-if-vlan10)#ip address 10.10.1.3 255.255.255.0 secondary mclag

## 13.1.11 ipv6 address

**命令：ipv6 address <ipv6address | prefix-length> [eui-64] [mc-lag]**

**no ipv6 address <ipv6address | prefix-length> [eui-64] [mc-lag]**

**功能：**配置 MC-LAG 三层网关独立的对外 IPv6 地址。

**参数：<ipv6address>**为 IPv6 地址的前缀，**<prefix-length>**参数为 IPv6 地址的前缀长度，前缀长度为 3-128 之间；**[eui-64]**表明根据接口的 eui64 接口标识符自动生成 IPv6 地址；**[mc-lag]**表示该地址为 MC-LAG 三层网关独立的对外 IPv6 地址。

**命令模式：**VLAN 接口配置模式。

**缺省情况：无。**

**使用指南：**一个 VLAN 接口下只能有一条 ipv6 address mc-lag 全球单播的配置，一个 VLAN 接口下只能有一条 ipv6 address mc-lag 本地链路的配置，mc-lag 的独立 ipv6 地址应该与同一 VLAN 接口下其他某个 ipv6 地址在同一网段。no 命令用于取消该配置。

**举例：** 配置 VLAN10 接口下 MC-LAG 独立的对外 IPv6 地址为 2022::3

switch(config-if-vlan10)#ipv6 address 2022::3/64 mclag

配置 VLAN10 接口下 MC-LAG 独立的 linklocal 地址为 fe80::3

switch(config-if-vlan10)#ipv6 address fe80::3/64 mclag

## 13.1.12 mclag dad link

**命令：mclag dad link local <X.X.X.X> peer < X.X.X.X >**

**no mclag dad link local <X.X.X.X> peer < X.X.X.X >**

**功能：**配置本机双主检测链路本地的三层接口 ip 地址和对端设备的 ip 地址。

**参数：**local <X.X.X.X> 本地 ip 地址

peer < X.X.X.X >对端 ip 地址

**命令模式：**MC-LAG 配置模式。

**缺省情况：无。**

**使用指南：**双主检测功能生效需要三层可达。

**举例：**配置 MC-LAG 双主检测本地 ip 地址为 24.24.1.1，对端 ip 地址为 24.24.1.2

switch(config-mclag)#mclag dad link local 24.24.1.1 peer 24.24.1.2

## 13.1.13 error-down exclude

**命令：error-down exclude**

**no error-down exclude**

**功能：**配置本机业务口和 port-group 口不被 error-down。

**参数：无**

**命令模式：**端口和 port-channel 模式。

**缺省情况：无。**

**使用指南：**在检测到双主时，备设备配置了 error-down exclude 的端口不会被系统执行 error-down 操作。

**举例：**配置端口 ethernet1/0/1 不被 error-down

switch(config-if-ethernet1/0/1)#error-down exclude

## 13.1.14 mclag up-delay

**命令：mclag up-delay <interval>**

**no mc-lag up-delay <interval>**

**功能：**配置 MC-LAG 端口延迟 UP 时间。

**参数：**<interval> 0~600 秒，0 表示不延迟。

**命令模式：**MC-LAG 配置模式。

**缺省情况：**120 秒。

**使用指南：**针对控制链路故障恢复的场景，可以配置延迟 MC-LAG 端口 UP 的时间，保障回切性能。

**举例：**配置 MC-LAG 端口延迟 UP 时间为 60 秒

switch(config-mclag)#mclag up-delay 60

## 13.1.15 mclag probe-interval

**命令：mclag probe-interval <interval>**

**no mclag probe-interval <interval>**

**功能：**配置 MC-LAG 探测时间间隔。

**参数：**<interval> 2~90 秒。

**命令模式：**MC-LAG 配置模式。

**缺省情况：**60 秒。

**使用指南：**配置 MC-LAG 探测时间间隔，超过 2 个 probe-interval 的时间未收到 echo 报文或控制报文，MC-LAG 转为 inactive 状态。

**举例：**配置 MC-LAG 探测时间间隔为 30 秒

switch(config-mclag)#mclag probe-interval 30

## 13.1.16 show mclag

**命令：show mclag**

**功能：**显示 MC-LAG 配置状态信息。

**参数：**无。

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**显示 MC-LAG 配置状态信息

Switch#show mclag

mclag domain_id : 10

mclag priority : 128

mclag local system_id : 90-3c-b3-95-0e-d7

mclag peer system_id : 90-3c-b3-95-10-eb

mclag domain state : MDS_READY

mclag ctrlink state : MCLAG_CTL_ACTIVE

mclag tunlink state : MCLAG_TUN_UP

mclag master : LOCAL

## 13.1.17 show mclag group

**命令：show mclag group (<1-128> | )**

**功能：**显示 MC-LAG 组配置状态信息。

**参数：**组 id 范围：1-128

**命令模式：**特权模式。

**缺省情况：**无。

**使用指南：**无。

**举例：**显示 MC-LAG 组配置状态信息

Switch#show mclag group

*********mclag group info :*********

group id:1

group state:ACTIVE

local link num:1

portname status

Ethernet1/0/21 aggregate

peer link num:1

peer-portname status

Ethernet1/0/21 aggregate

## 13.1.18 switchport mclag data link

**命令：[no] switchport mclag data link**

**功能：**配置本机 MC-LAG 数据链路端口。

**参数：**无。

**命令模式：**端口配置模式、汇聚端口配置模式

**缺省情况：**无。

**使用指南：**配置本机 MC-LAG 数据链路端口；no 命令用于取消本机数据链路端口配置。

**举例：**配置 Ethernet1/6/1 为本机 MC-LAG 数据链路端口

Switch(config-if-ethernet1/6/1)#switchport mclag data link

## 13.1.19 virtual-equipment-group ID

**命令：[no] virtual-equipment-group <ID>**

**功能：**配置 VEG 组。

**参数：**ID 指定虚拟交换组的 ID，范围：1-1

**命令模式：**全局模式。

**缺省情况：**无。

**使用指南：** 配置 VEG 组。MC-LAG 需要关联 VEG 组同步 mac/arp/nd 表项。no 命令用于取消配置的 VEG 组。

**举例：**配置 VEG 1

Switch(config)#virtual-equipment-group 1

## 13.1.20 virtual-equipment-group ID

**命令：[no] virtual-equipment-group <ID>**

**功能：**配置 VEG 组关联 MC-LAG。

**参数：**ID 指定虚拟交换组的 ID，范围：1-1

**命令模式：**MC-LAG 模式。

**缺省情况：**无。

**使用指南：** 配置 VEG 组关联 MC-LAG，通过 VEG 功能实现 MC-LAG 两台设备间 mac/arp/nd 表项的同步，同时会删除 VEG 下配置的 source ip 和 remote ip，并自动关联上 MC-LAG 配置的 local ip 和 peer ip；no 命令用于取消 VEG 组关联 MC-LAG。

**举例：**配置 VEG 1 关联 MC-LAG

Switch(config-mclag)#virtual-equipment-group 1

### 13.1.21 virtual-equipment-group ID

**命令：[no] virtual-equipment-group <ID>**

**功能：**配置网关接口绑定 VEG 组。

**参数：**ID 指定虚拟交换组的 ID，范围：1-1

**命令模式：**VLAN 接口模式、NVI 接口模式。

**缺省情况：**无。

**使用指南：** 配置网关接口绑定 VEG 组；no 命令用于取消网关接口绑定 VEG 组。

**举例：**配置接口 Vlan4 绑定 VEG 1

Switch(config)#interface vlan 4

Switch(config-if-vlan4)#virtual-equipment-group 1

# 第 14 章 IPV6 业务命令

## 14.1 DHCPv6

### 14.1.1 clear ipv6 dhcp binding

**命令：clear ipv6 dhcp binding [*<ipv6-address>*] [pd *<ipv6-prefix|prefix-length>*]**

**功能：**删除某指定 DHCPv6 分配地址或前缀的绑定记录或所有 IPv6 地址和前缀的绑定记录。

**参数：*<ipv6-address>***为指定的有绑定记录的 IPv6 地址；***<ipv6-prefix|prefix-length>***为指定的有绑定记录的 IPv6 前缀；没有指定参数时认为清除所有 IPv6 地址和前缀的绑定记录。

**命令模式：**特权用户配置模式。

**使用指南：**通过 **show ipv6 dhcp binding** 命令可以查看 IPv6 地址和前缀与相应的 DHCPv6 绑定信息，当 DHCPv6 服务器得知某 DHCPv6 客户机因为特殊原因没有使用分配的 IPv6 地址或前缀但规定的租期未到，DHCPv6 服务器不会自动解除该绑定信息，此时系统管理员可以使用本命令手工删除该 IP 地址或前缀与客户机硬件地址的自动绑定；如果没有任何参数，本命令将删除所有自动绑定记录，这样 DHCPv6 地址池中的所有地址和前缀将被重新分配。

**举例：**删除所有 IPv6 地址和前缀的绑定记录。

Switch#clear ipv6 dhcp binding

**相关命令：show ipv6 dhcp binding**

### 14.1.2 clear ipv6 dhcp conflict

**命令：clear ipv6 dhcp conflict [*<address>* ]**

**功能：**删除在地址冲突日志中有冲突记录的地址。

**参数：*<address>***为某指定的有冲突记录的地址；不指定地址则清除所有冲突记录。

**命令模式：**特权用户配置模式。

**使用指南：**通过 **show ipv6 dhcp conflict** 命令可以查看哪些 IP 地址在使用上有冲突，使用本命令可以删除某一地址的冲突记录，如果不指定具体地址则是删除日志中所有地址的冲突记录。在日志中删除冲突记录后，这些地址可被 DHCPv6 服务器重新使用。

**举例：**网络管理员查看冲突日志，发现有冲突记录的 2001::1 地址现已无人使用，将该地址的记录从地址冲突文件中删除。

Switch#clear ipv6 dhcp conflict 2001::1

## 14.1.3 clear ipv6 dhcp statistics

**命令：clear ipv6 dhcp statistics**

**功能：**删除 DHCPv6 报文统计记录，将 DHCPv6 报文统计计数器清零。

**参数：**无。

**命令模式：**特权用户配置模式。

**使用指南：**通过 **show ipv6 dhcp statistics** 命令可以查看 DHCPv6 报文计数器的统计信息，所有的统计信息都是一个累计值，使用本命令可以将计数器清零，方便调试查看。

**举例：**将 DHCPv6 报文计数器清零。

Switch#clear ipv6 dhcp statistics

**相关命令：show ipv6 dhcp statistics**

## 14.1.4 debug ipv6 dhcp client packet

**命令：debug ipv6 dhcp client { event | packet }**

**no debug ipv6 dhcp client { event | packet }**

**功能：** 显示 DHCPv6 前缀请求客户端收发报文的 debug 显示，本命令的 no 操作关闭 DHCPv6 前缀请求客户端的 debug 显示信息。

**缺省情况：**缺省调试开关是关闭的。

**命令模式：**特权用户配置模式。

**举例：**

Switch# debug ipv6 dhcp client packet

## 14.1.5 debug ipv6 dhcp detail

**命令：debug ipv6 dhcp detail**

**no debug ipv6 dhcp detail**

**功能：** 显示 DHCPv6 收发各类报文详细内容的 debug 显示，本命令的 no 操作关闭 DHCPv6 收发报文内容的 debug 显示信息。

**缺省情况：**缺省调试开关是关闭的。

**命令模式：**特权用户配置模式。

**举例：**

Switch# debug ipv6 dhcp detail

## 14.1.6 debug ipv6 dhcp relay packet

**命令：debug ipv6 dhcp relay packet**

**no debug ipv6 dhcp relay packet**

**功能：**显示 DHCPv6 中继代理收发报文的 debug 显示，本命令的 no 操作关闭 DHCPv6 中继代理的 debug 显示信息。

**缺省情况：**缺省调试开关是关闭的。

**命令模式：**特权用户配置模式。

**举例：**

Switch# debug ipv6 dhcp relay packet

## 14.1.7 debug ipv6 dhcp server

**命令：debug ipv6 dhcp server {event | packet}**

**no debug ipv6 dhcp server {event | packet}**

**功能：**显示 DHCPv6 服务器的事件和收发报文的情况，本命令的 no 操作关闭 DHCPv6 服务器的 debug 显示信息。

**参数：**event 表示开启/关闭 DHCPv6 服务器事件的 debug 显示，如地址分配情况；packet 表示开启/关闭 DHCPv6 服务器收发报文的 debug 显示。

**缺省情况：**缺省调试开关是关闭的。

**命令模式：**特权用户配置模式。

**举例：**

Switch#debug ipv6 dhcp server packet

## 14.1.8 dns-server

**命令：dns-server *<ipv6-address>***

**no dns-server *<ipv6-address>***

**功能：**为 DHCPv6 客户机配置 DNS 服务器 IPv6 地址；本命令的 no 操作为删除 DNS 服务器 IPv6 地址。

**参数：*<ipv6-address>***为 DNS 服务器的 IPv6 地址。

**缺省情况：**系统默认没有配置地址池的 DNS 服务器地址。

**命令模式：**DHCPv6 地址池模式。

**使用指南：**本命令最多可配置 3 次，即每个地址池最多允许 3 个 DNS 服务器地址，而且服务器地址只能是 IPv6 地址。

**举例：**设置 DHCPv6 客户机的 DNS 服务器的地址为 2001:da8::1。

Switch(dhcp-1-config)#dns-server 2001:da8::1

## 14.1.9 domain-name

**命令：domain-name *<domain-name>***

**no domain-name *<domain-name>***

**功能：**为 DHCPv6 客户机配置域名；本命令的 no 操作为删除域名。

**参数：*<domain-name>***为域的名称，最长不超过 32 字符。

**命令模式：**DHCPv6 地址池模式。

**缺省情况：**系统默认没有配置地址池的域名参数。

**使用指南：**本命令最多可配置 3 次，即每个地址池最多允许 3 个域名参数。

**举例：**指定 DHCPv6 客户机的域名为 test.com.cn

Switch(dhcp-1-config)#domain-name test.com.cn

## 14.1.10 excluded-address

**命令：excluded-address *<ipv6-address> <ipv6-address>***

**no excluded-address *<ipv6-address> <ipv6-address>***

**功能：**配置地址池中不用于动态分配的 IPv6 地址，以避免某些专用地址不被分配；本命令的 no 操作为取消该项配置。

**参数：*<ipv6-address>***为不用于动态分配的地址池中的某个 IPv6 地址。

**缺省情况：**地址池缺省没有配置不用于动态分配的 IPv6 地址。

**命令模式：**DHCPv6 地址池模式。

**使用指南：**使用本命令可以将地址池中的一个或多个地址排除不做 DHCPv6 分配，这些地址由系统管理员留作其它用途。本命令在一个地址池中可以配置多次。

**举例：**将 2001:da8:123::1 和 2001:da8:123::2 地址保留，不用于动态分配。

Switch(dhcp-1-config) #excluded-address 2001:da8:123::1 2001:da8:123::2

## 14.1.11 ipv6 address

**命令：ipv6 address *<prefix-name> <ipv6-prefix/prefix-length>***

**no ipv6 address *<prefix-name> <ipv6-prefix/prefix-length>***

**功能：**在指定接口上配置使用代理前缀生成的 IPv6 地址。本命令的 no 操作在指定接口上删除使用代理前缀生成的 IPv6 地址。

**参数：*<prefix-name>***是一个长度小于 32 的字符串，表示前缀请求客户端获得前缀或手动配置而保存在通用前缀池中的前缀名。***<ipv6-prefix/prefix-length>***表示 IPv6 地址中排除***<prefix-name>***前缀部分的后续地址位。

**命令模式：**接口配置模式。

**缺省情况：**系统默认不在接口配置全局地址。

**使用指南：**接口 IPv6 地址将由***<prefix-name>***和***<ipv6-prefix/prefix-length>***组合而成，最终 IPv6 地址的前缀长度将由***<prefix-length>***指定。如果开启了路由器公告，将公告前 64 位前缀。系统在接口上删除由***<prefix-name>***和***<ipv6-prefix/prefix-length>***组合而成的 IPv6 地址，并停止公告该前缀。一个接口的一个前缀名只能配置唯一的***<ipv6-prefix/prefix-length>***.

**举例：**如果前缀名 my-prefix 表示 2001:da8:221::/48，本命令将在 Vlan1 接口生成 2001:da8:221:2008::2008。

Switch(Config-if-Vlan1)# ipv6 address my-prefix 0:0:0:2008::2008/64

## 14.1.12 ipv6 dhcp client pd

**命令：ipv6 dhcp client pd *<prefix-name>* [rapid-commit]**

**no ipv6 dhcp client pd**

**功能：**在指定接口上启动客户端前缀代理请求功能。本命令的 no 操作在指定接口上关闭客户端前缀代理请求功能，并删除获得的前缀。

**参数：*<prefix-name>***是一个长度小于 32 的字符串，表示成功获得代理前缀后，使用该名称保存在通用前缀池中。如果指定了 **rapid-commit** 选项，且前缀代理服务器端也使能了 rapid-commmit 功能，则前缀代理服务器将向前缀请求客户端直接发出 REPLY 报文，通过一次消息交换完成前缀代理请求过程。

**命令模式：**接口配置模式。

**缺省情况：**系统默认不启动客户端前缀代理请求功能。

**使用指南：**系统在接口上启动客户端前缀代理请求功能，发出 SOLICIT 报文，希望从服务器获得代理前缀。一旦获得了前缀，就可以通过其他命令（比如 ipv6 address 命令）引用通用前缀池中的这个前缀。本命令与 ipv6 dhcp server 和 ipv6 dhcp relay destination 命令互斥。如果系统在接口上关闭客户端前缀代理请求功能，则从通用前缀池中删除获得的前缀，同时删除使用该前缀生成的接口地址，不再使用该前缀进行路由公告。如果已经通过 ipv6 general-prefix 命令配置了同一通用前缀名，则不能注册此通用前缀名。

**举例：**

Switch(Config-if-Vlan1)#ipv6 dhcp client pd ClientA rapid-commit

## 14.1.13 ipv6 dhcp client pd hint

**命令：ipv6 dhcp client pd hint *<prefix|prefix-length>***

**no ipv6 dhcp client pd hint *<prefix|prefix-length>***

**功能：**在指定接口上指定客户端希望获取的前缀和前缀长度的功能。本命令的 no 操作在指定接口上删除客户端希望获取的前缀和前缀长度。

**参数：**<prefix|prefix-length>表示客户端希望获取的前缀和前缀长度。

**命令模式：**接口配置模式。

**缺省情况：**系统默认不指定客户端希望获取的前缀和前缀长度的功能。

**使用指南：**系统在接口上为客户端指定了其希望获取的前缀和前缀长度，如果在接口上启动了客户端前缀代理请求功能且前缀服务器使能了 hint 功能，则服务器端优先把客户端希望获取得前缀和前缀长度分配给客户端。系统目前只允许配置一个 hint 前缀。

**举例：**

Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001::/48

## 14.1.14 ipv6 dhcp pool

**命令：ipv6 dhcp pool *<poolname>***

**no ipv6 dhcp pool *<poolname>***

**功能：**配置 DHCPv6 地址池，进入 DHCPv6 地址池模式，在此模式下配置可分配给客户端的地址前缀、DNS 服务器、域名等信息；本命令的 no 操作为删除该地址池。

**参数：*< poolname>***为 DHCPv6 地址池名，最长不超过 32 个字符。

**缺省情况：**系统默认不配置任何 DHCPv6 地址池。

**命令模式：**全局配置模式。

**使用指南：**在全局模式下定义一个 DHCPv6 地址池，进入到 DHCPv6 地址池配置模式。如果想要删除一个地址池，则需要先解除与该地址相关的接口绑定，并且清除所有相关的地址绑定。

**举例：**定义一个地址池，取名 1。

Switch(config)#ipv6 dhcp pool 1

## 14.1.15 ipv6 dhcp relay destination

**命令：ipv6 dhcp relay destination { [*<ipv6-address>*] [ interface { *<interface-name>* | vlan *<1-4096>* } ] }**

**no ipv6 dhcp relay destination { [*<ipv6-address>*] [ interface { *<interface-name>* | vlan *<1-4096>* } ] }**

**功能：**配置 DHCPv6 接口中继代理为客户端递交中继报文的目的 IPv6 地址，可以是另外的 DHCPv6 中继代理的地址也可以是 DHCPv6 服务器的地址。本命令的 no 操作取消该项配置。

**参数：*<ipv6-address>***为 DHCPv6 中继代理转发中继报文的目的 IPv6 地址；***<interface-name>*** 或 vlan 参数是转发出报文的交换机接口名或接口号，***<interface-name>***只能为三层接口 vlan 名称，vlan 接口号的取值范围为 1～4096。当***<ipv6-address>***为全球单播地址时，不配置转发的接口参数；当***<ipv6-address>***为本地链路地址时，必须配置转发的接口名称；当只配置报文转发出的接口名称时，此时默认转发目的地址为所有 DHCPv6 服务器的本地站点多播地址 **All_DHCP_Servers (FF05::1:3)**。

**命令模式：**接口配置模式。

**缺省情况：**系统默认没有配置 DHCPv6 中继代理的目的 IPv6 地址。

**使用指南：**配置本命令指示本接口启用 DHCPv6 中继代理功能，以后把配置的地址作为 RELAY-FORWARD 报文的目的地址，该地址可以是另外的 DHCPv6 中继代理的地址也可以是

DHCPv6 服务器的地址。系统最多允许配置 3 个中继代理的目的地址。注意只有该接口所有 DHCPv6 中继代理的目的地址都被删除，该接口的 DHCPv6 中继代理功能才不可用。本命令与 ipv6 dhcp server 和 ipv6 dhcp client pd 命令互斥。

**举例：**

Switch(Config-if-Vlan1)#ipv6 dhcp relay destination 2001:da8::1

## 14.1.16 ipv6 dhcp server

**命令：ipv6 dhcp server *<poolname>* [preference *<value>*] [rapid-commit] [allow-hint]**

**no ipv6 dhcp server *<poolname>***

**功能：**配置本命令绑定了 DHCPv6 服务器在接口使用的 DHCPv6 地址池。本命令的 no 操作删除指定接口上的 DHCPv6 地址池，停止本接口的 DHCPv6 服务。

**参数：*<poolname>***是一个长度小于 32 的字符串，表示与本接口关联的 DHCPv6 地址池名称。如果指定了 **rapid-commit** 选项，则 DHCPv6 服务器收到客户端的 SOLICIT 报文后，向客户端直接发出 REPLY 报文，通过一次消息交换完成地址或前缀请求过程。如果指定了 **preference** 选项，则***<value>***表示本服务器的优先值，取值范围是 0～255，默认值是 0，值越大服务器优先级越高。如果指定了 **allow-hint** 选项，表示优先满足客户端期望分配的配置参数，这些期望参数在客户端发出的请求报文中给出。

**命令模式：**接口配置模式。

**缺省情况：**系统默认没有配置接口的 DHCPv6 地址池。

**使用指南：**配置本命令记录了 DHCPv6 服务器在接口使用的 DHCPv6 地址池，及在该接口提供 DHCPv6 服务的相关参数。一个接口上可以绑定多个 DHCPv6 地址池，可以同时为直连链路的 DHCPv6 请求以及来自中继代理的 DHCPv6 请求报文分配地址。

**举例：**

Switch(Config-if-Vlan1)#ipv6 dhcp server PoolA preference 80 rapid-commit allow-hint

## 14.1.17 ipv6 general-prefix

**命令：ipv6 general-prefix *<prefix-name> <ipv6-prefix/prefix-length>***

**no ipv6 general-prefix *<prefix-name>***

**功能：**定义一个 IPv6 通用前缀。本命令的 no 操作取消该项配置。

**参数：*<prefix-name>*** 是一个长度小于 32 的字符串，表示 IPv6 通用前缀名称。***<ipv6-prefix/prefix-length>***表示定义的 IPv6 通用前缀。

**命令模式：**全局配置模式。

**缺省情况：**系统默认没有配置 IPv6 通用前缀。

使用指南：定义了 IPv6 通用前缀后，在接口上可以引用该通用前缀生成接口 IPv6 地址。在使用上通用前缀一般表示企业级的 IPv6 前缀，这样在接口上输入地址时只需要给出通用前缀名加上接口前缀后续部分，简化了用户书写。定义的通用前缀将保存在通用前缀池中。系

统最多可配置 8 个通用前缀。当删除指定的通用前缀名称时，如果有接口引用了这个通用前缀，本命令执行不成功。一个通用前缀名只能配置一个通用前缀。如果有接口使能 IPv6 dhcp 前缀代理客户端占用了通用前缀名，则不能使用此命令配置相同的通用前缀名。

**举例：**把 2001:da8:221::/48 前缀分配给通用前缀名 my-prefix。

Switch(config)# ipv6 general-prefix my-prefix 2001:da8:221::/48

## 14.1.18 ipv6 local pool

**命令：ipv6 local pool *<poolname>* *<prefix/prefix-length>* *<assigned-length>***

**no ipv6 local pool *<poolname>***

**功能：**配置 IPv6 代理前缀池。本命令的 no 操作删除 IPv6 代理前缀池。

**参数：*<poolname>***表示 IPv6 代理前缀池的名字，它是长度小于 32 的字符串。***<prefix/prefix-length>***表示分配给这个代理前缀池的前缀和前缀长度。***<assigned-length>***表示分配给使用这个代理前缀池的前缀请求客户端的前缀长度，它不能小于***<prefix-length>***。

**命令模式：**全局配置模式。

**缺省情况：**系统默认没有配置 IPv6 代理前缀池。

**使用指南：**本命令将与 prefix-degation pool 命令配合使用，向前缀请求客户端分配前缀。删除 IPv6 代理前缀池后，地址池中与之关联的 prefix-delegation 命令将无效。

## 14.1.19 lifetime

**命令：lifetime {*<valid-time>* | infinity} {*<preferred-time>* | infinity}**

**no lifetime**

**功能：**配置 DHCPv6 地址池动态分配地址或前缀的生存期。本命令的 no 操作恢复默认配置。

**参数：*<valid-time>*** 和***<preferred-time>***分别为本地址池分配 IPv6 地址的有效生存期和优选生存期，单位为秒，取值范围是 1-31536000，但***<preferred-time>***必须不大于***<valid-time>***。参数 **infinity** 表示生存期为无限值。

**命令模式：**DHCPv6 地址池模式。

**缺省情况：**地址池有效生存期和优选生存期默认为 2592000 秒(30 天)和 604800 秒(7 天)。

**举例：**配置有效生存期为 1000 秒，优选生存期为 600 秒。

Switch(dhcp-1-config) #lifetime 1000 600

## 14.1.20 network-address

**命令：network-address *<ipv6-pool-start-address>* {*<ipv6-pool-end-address>* | *<prefix-length>*} [eui-64]**

**no network-address**

**功能：**配置 DHCPv6 地址池可分配的 IPv6 地址范围；本命令的 no 操作为取消该项配置。

**参数：*<ipv6-pool-start-address>***为地址池 IPv6 起始地址；***<ipv6-pool-end-address>***为地址池 IPv6 终止地址；***<prefix-length>***为前缀长度，取值范围为 3-128，建议配置为 64，依据

***<prefix-length>***计算出地址池 IPv6 终止地址。***<ipv6-pool-end-address>*** 和***<prefix-length>***二者取其一。如果配置的***<prefix-length>***为 64，同时配置了 eui-64 选项，则 DHCPv6 服务器向客户端分配基于 EUI-64 规范的 IPv6 地址，否则将按自然顺序为客户端分配地址。

**缺省情况：**DHCPv6 地址池默认没有配置可分配的 IPv6 地址范围。

**命令模式：**DHCPv6 地址池模式。

**使用指南：**DHCPv6 服务器使用本命令配置可分配的 IPv6 地址范围，一个地址池只能分配一个地址范围。注意在使用 DHCPv6 服务器并配置前缀长度的时候，应该使地址池中前缀长度大于或等于交换机上对应网段的三层接口 IPv6 地址的前缀长度。如果***<ipv6-pool-end-address>***比***<ipv6-pool-start-address>***大，本命令立即返回。

**举例：**地址池 1 的可分配的地址范围为 2001:da8:123::100-2001:da8:123::200。

```
Switch(dhcp-1-config)#network-address 2001:da8:123::100 2001:da8:123::200
```

**相关命令：excluded-address**

## 14.1.21 prefix-delegation

命令：prefix-delegation ***<ipv6-prefix/prefix-length>*** ***<client-DUID>*** **[iaid *<iaid>*] [lifetime {<valid-time> | infinity} {*<preferred-time>* | infinity}]**

**no *prefix-delegation* <ipv6-prefix/prefix-length> <client-DUID> [*iaid* <iaid>]**

**功能：配置分配给特定前缀请求客户端的代理前缀。本命令的 no 操作删除分配给特定前缀请求客户端的代理前缀。**

**参数：<ipv6-prefix/prefix-length>为分配给特定前缀请求客户端的代理前缀。*<client-DUID>***为指定前缀请求客户端的 DUID，本文支持 DUID-LLT 类型的 DUID，它是长度为 14 的字符串，同时支持 DUID-LL 类型的 DUID。***<iaid>***是客户端请求报文中 IA_PD 选项中指定的 IAID 值。***<valid-time>*** 和***<preferred-time>***分别为客户分配 IPv6 前缀的有效生存期和优选生存期，单位为秒，取值范围是 1-31536000，但***<preferred-time>***必须不大于***<valid-time>***，如果不配置，默认的值***<valid-time>***为 2592000，***<preferred-time>***为 604800。参数 infinity 表示生存期为无限值。

**命令模式：DHCPv6 地址池配置模式。**

**缺省情况：系统默认没有配置分配给特定前缀请求客户端的代理前缀。**

**使用指南：**本命令指定 IPv6 前缀与某个前缀请求客户端静态绑定。如果没有配置 IAID 则客户端的任何 IA 都可以获取此前缀。一个地址池最多可以配置 8 个静态绑定的代理前缀。在前缀代理服务中，静态绑定前缀优先于前缀池被使用。

**举例：**以下命令把 2001:da8::/48 分配给 DUID 为 000100060000000500OBBFAA2408，IAID 为 12 的前缀请求客户端。

```
Switch(dhcp-1-config)#prefix-delegation 2001:da8::/48 000100060000000500OBBFAA2408 iaid
12
```

## 14.1.22 prefix-delegation add static route

本型号交换机不支持此命令。

## 14.1.23 prefix-delegation pool

**命令：prefix-delegation pool *<poolname>* [lifetime *{<valid-time>* | infinity} {*<preferred-time>* | infinity}]no prefix-delegation pool *<poolname>***

**功能：**配置 DHCPv6 地址池使用的代理前缀池名称。本命令的 no 操作删除 DHCPv6 地址池使用的代理前缀池名称。

**参数：*<poolname>***为代理前缀池的名称，它是长度小于 32 的字符串。***<valid-time>*** 和***<preferred-time>***分别为从该前缀池分配 IPv6 前缀的有效生存期和优选生存期，单位为秒，取值范围是 1-31536000，但***<preferred-time>***必须不大于***<valid-time>***，如果不配置，默认的值***<valid-time>***为 2592000，***<preferred-time>***为 604800。参数 infinity 表示生存期为无限值。

**命令模式：**DHCPv6 地址池配置模式。

**缺省情况：**系统默认没有配置 DHCPv6 地址池使用的代理前缀池名称。

**使用指南：**本命令指定 DHCPv6 地址池使用的代理前缀池名称，服务器提供代理前缀服务时将从该前缀池中分配可用的前缀给客户端。本命令与 ipv6 local pool 命令配合使用。一个地址池最多可以绑定 1 个代理前缀池。在删除 DHCPv6 地址池使用的代理前缀池名称时，如果地址池已不关联代理前缀池，也没有配置静态绑定代理前缀，则服务器的前缀代理服务将不可用。

**举例：**

```
Switch(dhcp-1-config)#prefix-delegation pool abc
```

## 14.1.24 service dhcpv6

**命令：service dhcpv6**

**no service dhcpv6**

**功能：**启动 DHCPv6 服务器功能；本命令的 no 操作为关闭 DHCPv6 服务。

**参数：**无。

**缺省情况：**DHCPv6 服务缺省是关闭的。

**命令模式：**全局配置模式。

**使用指南：**DHCPv6 服务包括 DHCPv6 服务器功能、DHCPv6 中继的功能和 DHCPv6 前缀代理功能。DHCPv6 服务器功能、DHCPv6 中继功能和 DHCPv6 前缀代理功能配置在接口上。只有打开 DHCPv6 服务器功能，交换机才能在接口上给 DHCPv6 客户机分配 IP 地址、开启 DHCPv6 的 RELAY 功能以及开启 DHCPv6 前缀代理功能。

**举例：**打开 DHCPv6 服务器。

```
Switch(config)#service dhcpv6
```

## 14.1.25 show ipv6 dhcp

**命令：show ipv6 dhcp**

**功能：**显示交换机 DHCPv6 服务的使能开关以及 DUID。

**命令模式：**特权和配置模式。

**使用指南：**显示交换机 DHCPv6 服务的使能开关以及 DUID，服务器标识符选项只会使用 DUID-LLT 类型的 DUID。

**举例：**

Switch#show ipv6 dhcp

DHCPv6 is enabled

LLT DUID is <00:01:00:01:43:b7:1b:81:00:03:0f:01:5f:9d>

LL DUID is <00:03:00:01:00:03:0f:01:5f:9d>

## 14.1.26 show ipv6 dhcp binding

**命令：show ipv6 dhcp binding [*<ipv6-address>* | pd *<ipv6-prefix*|*prefix-length>* | count]**

**功能：**显示 DHCPv6 所有的地址或前缀绑定信息。

**参数：*<ipv6-address>***为某指定的 IPv6 地址；count 表示显示 DHCPv6 地址绑定表项数量信息。

**命令模式：**特权和配置模式。

**使用指南：**显示 DHCPv6 所有的地址或前缀绑定信息，包括类型、DUID、IAID、前缀、超时时间等。

**举例:**

Switch#show ipv6 dhcp binding

Client: iatype IANA, iaid 0x0e001d92

DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83

IANA leased address: 2001:da8::10

Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds

Lease obtained at %Jan 01 01:34:44 1970

Lease expires at %Jan 31 01:34:44 1970 (2592000 seconds left)

The number of DHCPv6 bindings is 1

## 14.1.27 show ipv6 dhcp conflict

**命令：show ipv6 dhcp conflict**

**功能：**显示有冲突记录的地址的日志信息。

**命令模式：**特权和配置模式。

**举例：**

Switch#show ipv6 dhcp conflict

## 14.1.28 show ipv6 dhcp interface

**命令：show ipv6 dhcp interface [*<interface-name>*]**

**功能：**显示交换机 DHCPv6 接口的信息。

**参数：*<interface-name>***为交换机接口名称及接口号，如果没有提供***<interface-name>***参数，则系统显示当前所有 DHCPv6 接口的信息。

**命令模式：**特权和配置模式。

**使用指南：**显示交换机 DHCPv6 接口的信息，包括接口工作模式（Prefix delegation client、DHCPv6 server、DHCPv6 relay），以及各种模式下的相关配置信息。

**举例：**

Switch#show ipv6 dhcp interface vlan10

Vlan10 is in server mode

Using pool: poolv6

Preference value: 20

Rapid-Commit is disabled

## 14.1.29 show ipv6 dhcp pool

**命令：show ipv6 dhcp pool [*<poolname>*]**

**功能：**显示 DHCPv6 地址池的信息。

**参数：*<poolname>***为系统当前已配置 DHCPv6 地址池名称，长度小于 32 个字符。如果不提供***<poolname>***参数，则系统显示所有 DHCPv6 地址池的信息。

**命令模式：**特权和配置模式。

**使用指南：**显示交换机 DHCPv6 地址池的配置信息以及动态分配信息，包括 DHCPv6 地址池的名称，DHCPv6 地址池的前缀信息，排除地址，DNS server 等配置信息，以及关联的前缀池信息。对于用作地址分配服务器模式的地址池，显示已经分配的地址绑定个数。对于用作前缀代理服务器模式的地址池，显示已分配的前缀个数。

**举例：**

Switch#show ipv6 dhcp pool poolv6

## 14.1.30 show ipv6 dhcp statistics

**命令：show ipv6 dhcp statistics**

**功能：**显示 DHCPv6 服务器的对各种 DHCPv6 数据包的统计信息。

**命令模式：**特权和配置模式。

**举例：**

Switch#show ipv6 dhcp statistics

Address pools 1

Active bindings 0

Expiried bindings 0

Malformed message 0

Message Recieved

DHCP6SOLICIT 0
DHCP6ADVERTISE 0
DHCP6REQUEST 0
DHCP6REPLY 0
DHCP6RENEW 0
DHCP6REBIND 0
DHCP6RELEASE 0
DHCP6DECLINE 0
DHCP6CONFIRM 0
DHCP6RECONFIGURE 0
DHCP6INFORMREQ 0
DHCP6RELAYFORW 0
DHCP6RELAYREPLY 0

Message Send
DHCP6SOLICIT 0
DHCP6ADVERTISE 0
DHCP6REQUEST 0
DHCP6REPLY 0
DHCP6RENEW 0
DHCP6REBIND 0
DHCP6RELEASE 0
DHCP6DECLINE 0
DHCP6CONFIRM 0
DHCP6RECONFIGURE 0
DHCP6INFORMREQ 0
DHCP6RELAYFORW 0
DHCP6RELAYREPLY 0

| 显示信息 | 解释 |
|---|---|
| Address pools | 配置的 DHCPv6 地址池个数； |
| Active bindings | 自动分配地址的个数； |
| Expiried bindings | 绑定超期的个数； |
| Malformed message | 错误信息的个数； |
| Message Recieved | 接收 DHCPv6 数据包的统计 |
| DHCP6SOLICIT | 其中 DHCPv6 SOLICIT 报文个数 |
| DHCP6ADVERTISE | 其中 DHCPv6 ADVERTISE 报文个数 |

| | |
|---|---|
| DHCPv6REQUEST | 其中 DHCPv6 REQUEST 报文个数 |
| DHCP6REPLY | 其中 DHCPv6 REPLY 报文个数 |
| DHCP6RENEW | 其中 DHCPv6 RENEW 报文个数 |
| DHCP6REBIND | 其中 DHCPv6 REBIND 报文个数 |
| DHCP6RELEASE | 其中 DHCPv6 RELEASE 报文个数 |
| DHCP6DECLINE | 其中 DHCPv6 DECLINE 报文个数 |
| DHCP6CONFIRM | 其中 DHCPv6 CONFIRM 报文个数 |
| DHCP6RECONFIGURE | 其中 DHCPv6 RECONFIGURE 报文个数 |
| DHCP6INFORMREQ | 其中 DHCPv6 INFORMREQ 报文个数 |
| DHCP6RELAYFORW | 其中 DHCPv6 RELAYFORW 报文个数 |
| DHCP6RELAYREPLY | 其中 DHCPv6 RELAYREPLY 报文个数 |
| Message Send | 发送 DHCPv6 数据包的统计 |
| DHCP6SOLICIT | 其中 DHCPv6 SOLICIT 报文个数 |
| DHCP6ADVERTISE | 其中 DHCPv6 ADVERTISE 报文个数 |
| DHCPv6REQUEST | 其中 DHCPv6 REQUEST 报文个数 |
| DHCP6REPLY | 其中 DHCPv6 REPLY 报文个数 |
| DHCP6RENEW | 其中 DHCPv6 RENEW 报文个数 |
| DHCP6REBIND | 其中 DHCPv6 REBIND 报文个数 |
| DHCP6RELEASE | 其中 DHCPv6 RELEASE 报文个数 |
| DHCP6DECLINE | 其中 DHCPv6 DECLINE 报文个数 |
| DHCP6CONFIRM | 其中 DHCPv6 CONFIRM 报文个数 |
| DHCP6RECONFIGURE | 其中 DHCPv6 RECONFIGURE 报文个数 |
| DHCP6INFORMREQ | 其中 DHCPv6 INFORMREQ 报文个数 |
| DHCP6RELAYFORW | 其中 DHCPv6 RELAYFORW 报文个数 |

## 14.1.31 show ipv6 general-prefix

**命令：show ipv6 general-prefix**

**功能：**显示 IPv6 通用前缀池的信息。

**命令模式：**特权和配置模式。

**使用指南：**显示 IPv6 通用前缀池的信息，包括通用前缀池中的前缀数目，每个前缀的名称，获取该前缀的接口，具体的前缀值。

**举例：**

Switch#show ipv6 general-prefix

## 14.1.32 show ipv6 local pool

**命令：show ipv6 local pool**

**功能：**显示 DHCPv6 前缀池的信息和统计。

**命令模式：**特权和配置模式。

**使用指南：**显示 DHCPv6 前缀池的信息和统计，包括前缀池的名称，DHCPv6 池中的前缀、前缀长度、分配的前缀长度，可以自由分配前缀的个数，已经分配的前缀的个数和前缀信息。

**举例：**

Switch#show ipv6 local pool

| Pool | Prefix | Free | In use |
|---|---|---|---|
| a | 2010::1/48 | 65536 | 0 |

# 14.2 DHCPv6 option37，38

## 14.2.1 DHCPv6 option37，38

### 14.2.1.1 address range

**命令：address range <*start-ip*> <*end-ip*>**

**no address range <*start-ip*> <*end-ip*>**

**功能：**本命令在 DHCPv6 地址池配置模式下用来为 DHCPv6 服务器地址池中的一个 DHCPv6 class 设置一个地址范围，no 命令用来移除这个地址范围。不支持 prefix/plen 形式。

**参数：**start-ip：定义地址池中地址范围的起始地址。

end-ip：定义地址池中地址范围的结束地址。

**缺省情况：**无。

**命令模式：**DHCPv6 地址池 class 配置模式

**使用指南：**使用该命令为 class 分配的地址范围应做地址检查，保证分配到的地址范围不超出所在地址池的地址范围。一个 class 仅分配一段地址范围，在同一地址池中的多个 class 所分配的地址范围是可以有重叠的。如果不用该命令为一个 DHCPv6 class 在 DHCPv6 服务器地址池中分配地址范围，那么默认这个 class 的地址范围是地址池中的整个子网。

**举例：**将名为 CLASS1 的 DHCPv6 class 关联到 dhcpv6 pool 1 中，为 CLASS1 分配地址范围为 2001:da8:100:1::2 到 2001:da8:100:1::30。

Switch(Config)#ipv6 dhcp pool 1

Switch(dhcp-1-config)#class CLASS1

Switch(dhcp-1-class-CLASS1-config)#address range 2001:da8:100:1::2 2001:da8:100:1::30

### 14.2.1.2 class

**命令：class <*class-name*>**

**no class <*class-name*>**

**功能：**本命令在 DHCPv6 地址池配置模式下将 class 关联到地址池中，并进入地址池中 class 的配置模式，用 no 命令删除这种关联。

**参数：**class-name：DHCPv6 class 的名字。

**缺省情况：**无。

**命令模式：**DHCPv6 地址池配置模式

**使用指南：**应该首先用 IPv6 DHCP Class 全局配置命令定义好这个 class。如果用 class 命令输入了一个尚不存在的 class 名，那么将不创建该 class。

**举例：**将名为 CLASS1 的 DHCPv6 class 关联到 dhcpv6 pool 1 中。

```
Switch(Config)#ipv6 dhcp pool 1
Switch(dhcp-1-config)#class CLASS1
```

## 14.2.1.3 ipv6 dhcp class

**命令：ipv6 dhcp class <*class-name*>**

**no ipv6 dhcp class <*class-name*>**

**功能：**本命令用于定义一个 DHCPv6 class 并进入 DHCPv6 class 配置模式，no 命令用于删除这个 DHCPv6 class。

**参数：**class-name：DHCPv6 class 的名字，它是一个长度小于 32 的字符串。

**缺省情况：**无。

**命令模式：**全局配置模式

**使用指南：**在一个 DHCPv6 class 中可以配置一组 option 37 或者 option 38 选项内容，或者同时配置 option 37 和 option 38 选项内容。该命令当服务器端支持 DHCPv6 class 的时候才能使用。

**举例：**定义一个名为 CLASS1 的 DHCPv6 class。

```
Switch(Config)# ipv6 dhcp class CLASS1
```

## 14.2.1.4 ipv6 dhcp relay remote-id

**命令：ipv6 dhcp relay remote-id <*remote-id*>**

**no ipv6 dhcp relay remote-id**

**功能：**本命令用于设置从接口接收的 DHCPv6 请求报文添加 option 37 选项的形式，<remote-id>为用户自定义的 option 37 的 remote-id 内容，它是一个长度小于 128 的字符串。本命令的 no 操作恢复 option 37 的 remote-id 选项的形式为默认的 enterprise-number 和 vlan MAC 地址。

**参数：**remote-id：用户自定义的 option 37 的内容。

**缺省情况：**系统默认使用 vlan MAC 地址作为 remote-id 的内容，vlan MAC 形式如“00-01-ac-12-23”，中间的连字符为‘-’。

**命令模式：**接口配置模式

**使用指南：**因为交换机添加的 option 37 信息有可能配合第三方的 DHCPv6 服务器使用，在交换机的默认 remote-id 形式不能满足服务器的要求时，提供一种手段由用户依据服务器情况自己指定 remote-id 的内容。系统默认使用 enterprise-number 和 vlan MAC 地址作为 remote-id 的内容。

**举例：**设置 DHCPv6 option 37 选项的 remote-id 为 abc。

Switch(Config-if-vlan1)# ipv6 dhcp relay remote-id abc

## 14.2.1.5 ipv6 dhcp relay remote-id option

**命令：ipv6 dhcp relay remote-id option**

**no ipv6 dhcp relay remote-id option**

**功能：**设置本命令允许交换机中继支持 option 37 选项功能，本命令的 no 操作关闭交换机中继的 option 37 选项功能。

**参数：**无。

**缺省情况：**系统默认关闭交换机中继的 option 37 选项功能。

**命令模式：**全局配置模式

**使用指南：**只有配置本命令 DHCPv6 中继代理才能在 DHCPv6 请求报文中添加 option 37 选项交给服务器或下一级中继代理处理。执行本命令之前确保系统已经使能 DHCPv6 服务。

**举例：**开启交换机中继支持 option 37 选项功能。

Switch(Config)#service dhcpv6

Switch(Config)#ipv6 dhcp relay remote-id option

## 14.2.1.6 ipv6 dhcp relay subscriber-id

**命令：ipv6 dhcp relay subscriber-id <subscriber-id>**

**no ipv6 dhcp relay subscriber-id**

**功能：**本命令用于设置从接口接收的 DHCPv6 请求报文添加 option 38 选项的形式，<subscriber-id>为用户自定义的 option 38 的 subscriber-id 内容，它是一个长度小于 128 的字符串。本命令的 no 操作恢复 option 38 的 subscriber-id 选项的形式为默认的 VLAN 名加物理端口名形式，如“Vlan2+Ethernet1/1/2”。

**参数：**subscriber-id：用户自定义的 option 38 的内容。

**缺省情况：**系统默认使用 VLAN 名加物理端口名形式的形式设置 option 38 中的 subscriber-id。

**命令模式：**接口配置模式

**使用指南：**因为交换机添加的 option 38 信息有可能配合第三方的 DHCPv6 服务器使用，在交换机的标准 subscriber-id 形式不能满足服务器的要求时，提供一种手段由用户依据服务器情况自己指定 subscriber-id 的内容。系统默认使用 VLAN 名加物理端口名形式的形式设置 option 38 中的 subscriber-id。

**举例：**设置 DHCPv6 option 38 选项的 subscriber-id 为 abc。

Switch(Config-if-vlan1)# ipv6 dhcp relay subscriber-id abc

## 14.2.1.7 ipv6 dhcp relay subscriber-id option

**命令：ipv6 dhcp relay subscriber-id option**

**no ipv6 dhcp relay subscriber-id option**

**功能：**设置本命令允许交换机中继支持 option 38 选项功能，本命令的 no 操作关闭交换机中继的 option 38 选项功能。

**参数：**无。

**缺省情况：**系统默认关闭交换机中继的 option 38 选项功能。

**命令模式：**全局配置模式

**使用指南：**只有配置本命令 DHCPv6 中继代理才能在 DHCPv6 请求报文中添加 option 38 选项交给服务器或下一级中继代理处理。执行本命令之前确保系统已经使能 DHCPv6 服务。系统默认关闭交换机中继的 option 38 选项功能。

**举例：**开启交换机中继支持 option 38 选项功能。

Switch(Config)#service dhcpv6

Switch(Config)#ipv6 dhcp relay subscriber-id option

## 14.2.1.8 ipv6 dhcp relay subscriber-id select delimiter

**命令：ipv6 dhcp relay subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD | )**

**no ipv6 dhcp relay subscriber-id select delimiter**

**功能：**配置用户配置选项来生成 subscriber-id，no 命令恢复为最初的默认配置即 VLAN 名加端口名的形式。

**参数：**(sp | sv | pv | spv)：此选项是对 slot，port，vlan 的组合形式的选择，sp 代表 slot 和 port，sv 代表 slot 和 vlan，pv 代表 port 和 vlan，spv 代表 slot、port 和 vlan。

WORD：slot，port，vlan 分隔符，取值范围是(#|.|,|;|:|/|space)，注意，这里有两个 delimiter WORD，第一个是 slot 和 port 间的分隔符，第二个是 port 和 vlan 间的分隔符。

**缺省情况：**默认此配置为空。

**命令模式：**全局配置模式

**使用指南：**该命令对已经自定义 subscriber-id 的端口不起作用，如果配置该命令后，用户又自定义端口的 subscriber-id，则以用户自定义为准。默认此配置为空。

**举例：**

Swithc(config)# ipv6 dhcp relay subscriber-id select sp delimiter #

## 14.2.1.9 ipv6 dhcp server remote-id option

**命令：ipv6 dhcp server remote-id option**

**no ipv6 dhcp server remote-id option**

**功能：**本命令用于设置 DHCPv6 服务器支持对 option 37 选项的识别。本命令的 no 操作使系统不支持 option 37 选项。

**参数：**无。

**缺省情况：**系统默认不支持 option 37 选项功能。

**命令模式：**全局配置模式

**使用指南：**如果希望交换机 DHCPv6 服务器识别 option 37 选项并做处理，需要配置本命令，否则交换机 DHCPv6 服务器会忽视 option 37 选项的存在。系统默认不支持 option 37 选项功能。

**举例：**设置 DHCPv6 服务器支持 option 37 选项。

Switch(Config)# ipv6 dhcp server remote-id option

## 14.2.1.10 ipv6 dhcp server select relay-forw

**命令：ipv6 dhcp server select relay-forw**

**no ipv6 dhcp server select relay-forw**

**功能：**本命令用于设置 DHCPv6 服务器支持对报文中存在多个 option 37 选项或者 option38 选项时对其进行选择，选择最里层 relay-forw 中的 option 37 选项和 option38 选项。本命令的 no 操作恢复默认设置，即选择原始报文中的 option 37 选项和 option38 选项。

**参数：**无。

**缺省情况：**系统默认选择原始报文中的 option 37 选项和 option38 选项。

**命令模式：**接口配置模式

**使用指南：**使用该命令前确定服务器端已开启对 option 37 选项和 option38 选项的支持。系统默认选择原始报文中的 option 37 选项和 option38 选项。

**举例：**设置 DHCPv6 服务器 vlan1 接口选择最里层 relay-forw 中的 option 37 和 option38 选项选项。

Switch(Config-if-vlan1)# ipv6 dhcp server select relay-forw

## 14.2.1.11 ipv6 dhcp server subscriber-id option

**命令：ipv6 dhcp server subscriber-id option**

**no ipv6 dhcp server subscriber-id option**

**功能：**本命令用于设置 DHCPv6 服务器支持对 option 38 选项的识别。本命令的 no 操作使系统不支持 option 38 选项。

**参数：**无。

**缺省情况：**系统默认不支持 option 38 选项功能。

**命令模式：**全局配置模式

**使用指南：**如果希望交换机 DHCPv6 服务器识别 option 38 选项并做处理，需要配置本命令，否则交换机 DHCPv6 服务器会忽视 option 38 选项的存在。系统默认不支持 option 38 选项功能。

**举例：**设置 DHCPv6 服务器支持 option 38 选项。

Switch(Config)# ipv6 dhcp server subscriber-id option

## 14.2.1.12 ipv6 dhcp snooping information option remote-id format

**命令：ipv6 dhcp snooping information option remote-id format {hex | acsii }**

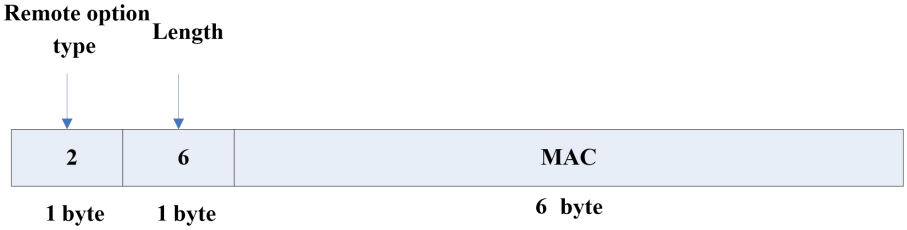
**功能：**本命令设置交换机中继代理的 DHCPV6 option37 功能 remote-id 格式。

**参数：**hex 表示 remote-id 为十六进制格式的交换机 VLAN MAC 地址，acsii 表示 remote-id 为为 ACSII 格式的交换机 VLAN MAC 地址。

**缺省情况：**系统默认 option37 功能 remote-id 格式为 acsii。

**命令模式：**全局配置模式

**使用指南：**十六进制的 remote-id 格式定义如下：




其中 MAC 为交换机 VLAN MAC 地址。

**举例：**配置交换机 DHCP snooping option37 功能 remote-id 为默认格式。

Switch(config)#ipv6 dhcp snooping information option remote-id format ascii

## 14.2.1.13 ipv6 dhcp snooping information option subscriber-id format

**命令：ipv6 dhcp snooping information option subscriber-id format {hex | acsii }**

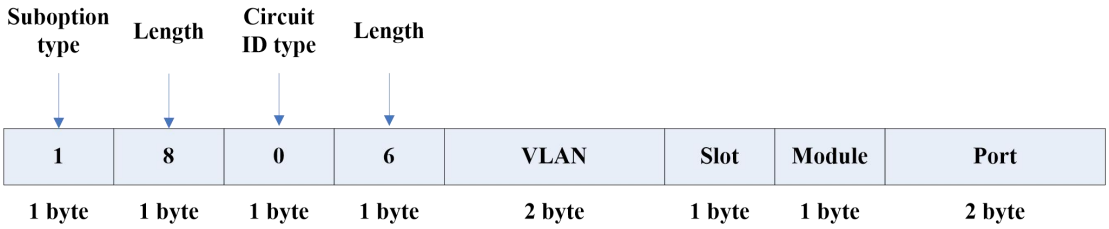
**功能：**本命令设置 DHCPv6 snooping option38 功能 subscriber-id 默认格式。

**参数：**hex 表示 subscriber-id 为十六进制格式的 VLAN 和端口信息，acsii 表示 subscriber-id 为 ACSII 格式的 VLAN 和端口信息。

**缺省情况：**系统默认 option38 功能 subscriber-id 格式为 acsii。

**命令模式：**全局配置模式

**使用指南：**ASCII 格式的 VLAN 和端口信息形如 Vlan1+Ethernet1/11。十六进制格式的 VLAN 和端口信息定义如下：




其中，VLAN 字段填写交换机 VLAN ID。Slot 对于机架式交换机，表示插槽号；对于盒式交换机，为 1。Module 默认为 0。Port 表示端口号，从 1 开始。

**举例：**配置交换机 DHCP snooping option38 功能 subscriber-id 格式为十六进制格式。

Switch(config)#ipv6 dhcp snooping information option subscriber-id format hex

## 14.2.1.14 ipv6 dhcp snooping remote-id

**命令：ipv6 dhcp snooping remote-id <*remote-id*>**

**no ipv6 dhcp snooping remote-id**

**功能：**本命令用于设置在接收的 DHCPv6 请求报文中添加 option 37 选项的形式，<remote-id>为用户自定义的 option 37 中 remote-id 的内容，它是一个长度小于 128 的字符串。本命令的 no 操作恢复 option 37 中 remote-id 的内容为默认的 enterprise-number 和 vlan MAC 地址。

**参数：**remote-id：用户自定义的 option 37 的内容。

**缺省情况：**系统默认使用 vlan MAC 地址作为 remote-id 的内容，vlan MAC 形式如“00-01-ac-12-23”，中间的连字符为‘-’。

**命令模式：**端口配置模式

**使用指南：**因为交换机添加的 option 37 信息有可能配合第三方的 DHCPv6 服务器使用，在交换机的标准 remote-id 形式不能满足服务器的要求时，提供一种手段由用户依据服务器情况自己指定 remote-id 的内容。系统默认使用 enterprise-number 和 vlan MAC 地址作为 remote-id 的内容。

**举例：**设置 DHCPv6 option 37 选项的 remote-id 为 abc。

Switch(Config-if-Ethernet1/1/1)#ipv6 dhcp snooping remote-id abc

## 14.2.1.15 ipv6 dhcp snooping remote-id option

**命令：ipv6 dhcp snooping remote-id option**

**no ipv6 dhcp snooping remote-id option**

**功能：**设置本命令允许 DHCPv6 SNOOPING 支持 option 37 选项功能，本命令的 no 操作关闭 DHCPv6 SNOOPING 的 option 37 选项功能。

**参数：**无。

**缺省情况：**系统默认关闭 DHCPv6 SNOOPING 中的 option 37 选项功能。

**命令模式：**全局配置模式

**使用指南：**只有配置本命令 DHCPv6 SNOOPING 才能在 DHCPv6 报文中添加 option 37 选项交给中继代理或服务器。执行本命令之前确保系统已经使能 DHCPv6 SNOOPING。系统默认关闭 DHCPv6 SNOOPING 中的 option 37 选项功能。

**举例：**开启 DHCPv6 SNOOPING 的 option 37 选项功能。

Switch(Config)#ipv6 dhcp snooping enable

Switch(Config)#ipv6 dhcp snooping remote-id option

## 14.2.1.16 ipv6 dhcp snooping remote-id policy

**命令：ipv6 dhcp snooping remote-id policy {drop | keep | replace}**

**no ipv6 dhcp snooping remote-id policy**

**功能：**本命令用于设置系统对于接收到的含有 option 37 选项的 DHCPv6 报文的重转发策略，其中 drop 模式表示如果报文中含有 option 37 选项，则系统丢弃该 DHCPv6 报文不作处理；keep 模式表示系统保持现有报文中的 option 37 选项不变转发给服务器处理；replace 模式表示系统使用自己的 option 37 选项替换现有报文中的 option 37 选项，然后转发给服务器处理。本命令的 no 操作设置 option 37 选项 DHCPv6 报文的重转发策略为 replace。

**参数：**无。

**缺省情况：**系统默认使用 replace 模式使用本系统的 option 37 选项替换现有报文中的 option 选项。

**命令模式：**全局配置模式

**使用指南：**由于 DHCPv6 客户端报文可能已经含有 option 37 选项信息，所以须制定 DHCPv6 SNOOPING 对该信息的处理策略。如果重转发策略设置为 replace，系统预先必须开启 option 37 选项功能。系统默认使用 replace 模式使用本系统的 option 37 选项替换现有报文中的 option 选项。

**举例：**设置 DHCPv6 SNOOPING 对 DHCPv6 报文的 option 37 选项的重转发策略为 keep。

Switch(Config)# ipv6 dhcp snooping remote-id policy keep

## 14.2.1.17 ipv6 dhcp snooping subscriber-id

**命令：ipv6 dhcp snooping subscriber-id <subscriber-id>**

**no ipv6 dhcp snooping subscriber-id**

**功能：**本命令用于设置在接收的 DHCPv6 请求报文中添加 option 38 选项的形式，<subscriber-id>为用户自定义的 option 38 中 subscriber-id 的内容，它是一个长度小于 128 的字符串。本命令的 no 操作恢复 option 38 中 subscriber-id 的内容为默认的 VLAN 名加物理端口名形式，如“Vlan2+Ethernet1/1/2”。

**参数：**subscriber-id：用户自定义的 option 38 的内容。

**缺省情况：**系统默认使用 VLAN 名加物理端口名形式的形式设置 option 38 中的 subscriber-id。

**命令模式：**端口配置模式

**使用指南：**因为交换机添加的 option 38 信息有可能配合第三方的 DHCPv6 服务器使用，在交换机的标准 subscriber-id 形式不能满足服务器的要求时，提供一种手段由用户依据服务器情况自己指定 subscriber-id 的内容。系统默认使用 VLAN 名加物理端口名形式的形式设置 option 38 中的 subscriber-id。

**举例：**设置 DHCPv6 option 38 选项的 subscriber-id 为 abc。

Switch(Config-if-Ethernet1/1/1)#ipv6 dhcp snooping subscriber-id abc

## 14.2.1.18 ipv6 dhcp snooping subscriber-id option

**命令：ipv6 dhcp snooping subscriber-id option**

**no ipv6 dhcp snooping subscriber-id option**

**功能：**设置本命令允许 DHCPv6 SNOOPING 支持 option 38 选项功能，本命令的 no 操作关闭 DHCPv6 SNOOPING 的 option 38 选项功能。

**参数：**无。

**缺省情况：**系统默认关闭 DHCPv6 SNOOPING 中的 option 38 选项功能。

**命令模式：**全局配置模式

**使用指南：**只有配置本命令 DHCPv6 SNOOPING 才能在 DHCPv6 报文中添加 option 38 选项交给中继代理或服务器。执行本命令之前确保系统已经使能 DHCPv6 SNOOPING。系统默认关闭 DHCPv6 SNOOPING 中的 option 38 选项功能。

**举例：**开启 DHCPv6 SNOOPING 的 option 38 选项功能。

Switch(Config)#ipv6 dhcp snooping enable

Switch(Config)#ipv6 dhcp snooping subscriber-id option

## 14.2.1.19 ipv6 dhcp snooping subscriber-id policy

**命令：ipv6 dhcp snooping subscriber-id policy {drop | keep | replace}**

**no ipv6 dhcp snooping subscriber-id policy**

**功能：**本命令用于设置系统对于接收到的含有 option 38 选项的 DHCPv6 报文的重转发策略，其中 drop 模式表示如果报文中含有 option 38 选项，则系统丢弃该 DHCPv6 报文不作处理；keep 模式表示系统保持现有报文中的 option 38 选项不变转发给服务器处理；replace 模式表示系统使用自己的 option 38 选项替换现有报文中的 option 38 选项，然后转发给服务器处理。本命令的 no 操作设置 option 38 选项 DHCPv6 报文的重转发策略为 replace。

**参数：**无。

**缺省情况：**系统默认使用 replace 模式使用本系统的 option 38 选项替换现有报文中的 option 38 选项。

**命令模式：**全局配置模式

**使用指南：**由于 DHCPv6 客户端报文可能已经含有 option 38 选项信息，所以须制定 DHCPv6 SNOOPING 对该信息的处理策略。如果重转发策略设置为 replace，系统预先必须开启 option

38 选项功能。系统默认使用 replace 模式使用本系统的 option 38 选项替换现有报文中的 option 38 选项。

**举例：**设置 DHCPv6 SNOOPING 对 DHCPv6 报文的 option 38 选项的重转发策略为 keep。

Switch(Config)# ipv6 dhcp snooping subscriber-id policy keep

## 14.2.1.20 ipv6 dhcp snooping subscriber-id select delimiter

**命令：ipv6 dhcp snooping subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD | )**

**no ipv6 dhcp snooping subscriber-id select delimiter**

**功能：**配置用户配置选项来生成 subscriber-id，no 命令恢复为最初的默认配置即 VLAN 名加端口名的形式。

**参数：**(sp | sv | pv | spv)：此选项是对 slot，port，vlan 的组合形式的选择，sp 代表 slot 和 port，sv 代表 slot 和 vlan，pv 代表 port 和 vlan，spv 代表 slot、port 和 vlan。

WORD：slot，port，vlan 分隔符，取值范围是(#|.|,|;|:|/|space)，注意，这里有两个 delimiter WORD，第一个是 slot 和 port 间的分隔符，第二个是 port 和 vlan 间的分隔符。

**缺省情况：**默认此配置为空。

**命令模式：**全局配置模式

**使用指南：**该命令对已经自定义 subscriber-id 的端口不起作用，如果配置该命令后，用户又自定义端口的 subscriber-id，则以用户自定义为准。默认此配置为空。

**举例：**

Swithc(config)# ipv6 dhcp snooping subscriber-id select sv delimiter #

## 14.2.1.21 ipv6 dhcp use class

**命令：ipv6 dhcp use class**

**no ipv6 dhcp use class**

**功能：**本命令用于设置 DHCPv6 服务器在进行地址分配时支持使用 DHCPv6 class，本命令的 no 操作使服务器在进行地址分配时不支持使用 DHCPv6 class，但是却并不删除已经配置的有关 DHCPv6 class 的信息。

**参数：**无。

**缺省情况：**系统默认 DHCPv6 服务器在进行地址分配时支持使用 DHCPv6 class。

**命令模式：**全局配置模式

**使用指南：**默认 DHCPv6 服务器在进行地址分配时支持使用 DHCPv6 class，进行 no 命令操作时并不删除已配置的 DHCPv6 class 信息。执行本命令之前确保系统已经使能 DHCPv6 服务。系统默认 DHCPv6 服务器在进行地址分配时支持使用 DHCPv6 class。

**举例：**设置 DHCPv6 服务器在进行地址分配时支持使用 DHCPv6 class。

Switch(Config)# ipv6 dhcp use class

### 14.2.1.22 remote-id subscriber-id

**命令：{remote-id [*] <remote-id> [*] | subscriber-id [*] <subscriber-id> [*]}**

**no {remote-id [*] <remote-id> [*] | subscriber-id [*] < subscriber-id> [*]}**

**功能：**本命令在 IPv6 DHCP Class 配置模式下配置匹配该 class 的 option37 选项和 option38 选项。

**参数：**<remote-id>: 字符串，用来匹配 37 选项中 remote-id 的内容，范围在 1-128 字节。

<subscriber-id>:字符串，用来匹配 38 选项中 subscriber-id 的内容，范围在 1-128 字节。

[*]:可匹配 0 个或多个字符。

**缺省情况：**无。

**命令模式：**IPv6 DHCP Class 配置模式

**使用指南：**该命令用来设置一个与已经定义的 DHCPv6 class 相匹配的模式。可以在一个 DHCPv6 class 配置多条命令。如果忽略该命令，在 IPv6 DHCP Class 模式下不配置任何模式，那么就认为任何一个 remote-id 或者 subscriber-id 都与这个 DHCPv6 class 相匹配，但是这个 remote-id 或者 subscriber-id 必须是在 DHCPv6 packet 中存在的。

**举例：**在名为 CLASS1 的 DHCPv6 class 中配置若干属于该 class 的 remote-id 或者 subscriber-id 内容。

```
Switch(Config)# ipv6 dhcp class CLASS1
Switch(Dhcpv6-class)#remote-id abc* subscriber-id bcd*
Switch(Dhcpv6-class)#remote-id edf*
Switch(Dhcpv6-class)#subscriber *mmn
```

## 14.2.2 监测和调试

### 14.2.2.1 debug ipv6 dhcp detail

**命令：debug ipv6 dhcp detail**

**功能：**显示 DHCPv6 收发各类报文详细内容的 debug 显示，如果报文中携带 option 37、option 38，其内容也会显示出来。这个命令在 server 端和 relay 端均适用。

**参数：**无。

**命令模式：**特权用户配置模式

**使用指南：**开启/关闭 DHCPv6 收发报文详细内容的 debug 显示。

**举例：**

```
Switch# debug ipv6 dhcp detail
%Jan 01 01:38:45 2006 DHCPv6 DETAILS: contents of SOLICIT packet
%Jan 01 01:38:45 2006        transaction-ID: 0x00b2d47c
%Jan 01 01:38:45 2006     elapsed time option(8), option-len 2
%Jan 01 01:38:45 2006        elapsed time: 0
%Jan 01 01:38:45 2006     client ID option(1), option-len 14
```

%Jan 01 01:38:45 2006 DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83
%Jan 01 01:38:45 2006 identity association option(3), option-len 12
%Jan 01 01:38:45 2006 IANA: 0x0e001d92, T1 0, T2 0
%Jan 01 01:38:45 2006 vendor class option(16), option-len 14
%Jan 01 01:38:45 2006 enterprise number : 311
%Jan 01 01:38:45 2006 option request option(6), option-len 6
%Jan 01 01:38:45 2006 requested-option: domain search list
%Jan 01 01:38:45 2006 requested-option: DNS server list
%Jan 01 01:38:45 2006 requested-option: vendor specific info
%Jan 01 01:38:45 2006 remote-id option(37), option-len 14
%Jan 01 01:38:45 2006 remote-id : 0x0a0b0c
%Jan 01 01:38:45 2006 subscriber-id option(38), option-len 16
%Jan 01 01:38:45 2006 subscriber-id : 0x0a0b0c0d

## 14.2.2.2 debug ipv6 dhcp relay packet

**命令：debug ip dhcp relay packet**

**功能：**使用本命令显示系统处理中继数据包的信息。

**参数：**无。

**命令模式：**特权配置模式

**使用指南：**运行时使用本命令显示中继代理处理中继数据包的过程，并显示相应的 option 37 和 option 38 的动作信息。

**举例：**

Switch# debug ipv6 dhcp relay packet

%May 19 16:45:34 2010 DHCPv6 RELAY PACKET: received msg0 from <fe80::211:22ff:fe33:4455> on <Vlan8>

%May 19 16:45:34 2010 DHCPv6 RELAY PACKET: add subscriber-id option “Vlan8+Ethernet1/1/12”

## 14.2.2.3 debug ipv6 dhcp snooping packet

**命令：debug ipv6 dhcp snooping packet**

**功能：**调试 DHCPv6 SNOOPING 报文信息，如果添加、删除 option37 与 option38，相应信息也会显示。

**参数：**无。

**命令模式：**特权用户配置模式

**使用指南：**开启/关闭 DHCPv6 snooping 处理 dhcpv6 报文的信息，包括接收报文类型，报文源 MAC，目的 MAC，客户端标识 client DUID，IA 地址，优先生存期（preferred lifetime），有效生存期（valid lifetime），报文丢弃等。

**举例：**

switch#debug ipv6 dhcp snooping packet

dhcpv6 snooping packet debug is on

switch#%Jan 05 00:26:40 2006 DHCP6SNP EVENT: Parse packet SOLICIT from fe80::200:ff:fe00:1

src MAC 00-00-00-00-00-01 interface Ethernet1/1/23 vlan 24

%Jan 05 00:26:40 2006 DHCP6SNP PACKET: Receive DHCPv6 packet SOLICIT from fe80::200:ff:fe00:1

src MAC 00-00-00-00-00-01, dst MAC 33-33-00-01-00-02,

interface Ethernet1/1/23 vlan 24,

transaction-ID 6137412, smac host flag 0, dmac host flag 0

%Jan 05 00:26:40 2006 DHCP6SNP PACKET: Forward packet SOLICIT (protocol 0x37)

%Jan 05 00:26:40 2006 DHCP6SNP PACKET: to vlan 24 except port Ethernet1/1/23 (designPort flag 0)

%Jan 05 00:26:40 2006 DHCP6SNP PACKET: and return packet to network stack

switch#

## 14.2.2.4 show ipv6 dhcp relay option

**命令：show ipv6 dhcp relay option**

**功能：**本命令显示系统中继代理的配置信息，包括中继代理 option 37 和 option 38 使能开关。

**参数：**无。

**命令模式：**特权配置模式

**使用指南：**运行时使用本命令检查中继代理对 option 37 和 option 38 选项的配置状态。

**举例：**

Switch#show ipv6 dhcp relay option

remote-id option enable

subscriber-id option enable

Interface Vlan 1: remote-id option configure “abc”

## 14.2.2.5 show ipv6 dhcp snooping option

**命令：show ipv6 dhcp snooping option**

**功能：**本命令显示系统 snooping 的配置信息，包括其中的 option 37 和 option 38 使能开关。

**参数：**无。

**命令模式：**特权配置模式

**使用指南：**运行时使用本命令检查中 snooping 对 option 37 和 option 38 选项的配置状态。

**举例：**

Switch#show ipv6 dhcp snooping option

remote-id option enable

subscriber-id option enable

The slot port vlan select option is : port and vlan

The delimiter is : #

# 14.3 ND 绑定

## 14.3.1 ipv6 nd-security updateprotect

**命令：ipv6 nd-security updateprotect**

**no ipv6 nd-security updateprotect**

**功能：** 禁止 IPv6 版本的 ND 更新功能，no 命令操作重新启动 ND 更新功能。

**参数：** 无。

**缺省情况：** 学习 ND 并正常更新。

**命令模式：** 全局配置模式/接口配置。

**使用指南:** 本命令用于防止 ND 的 request 和 reply 报文对交换机进行 ND 表的更新操作。不过即使在不转换动态 ND 的情况下，如果交换机一直收到合法的 ND 请求/应答报文则此动态表项不会超时，当收到的 ND 请求或应答包与保存不符才予以丢弃。命令全局优先。

**举例：**

Switch(Config-if-Vlan1)#ipv6 nd-security updateprotect

Switch(config)#ipv6 nd-security updateprotect

## 14.3.2 ipv6 nd-security learnprotect

**命令：ipv6 nd-security learnprotect**

**no ipv6 nd-security learnprotect**

**功能：** 禁止 IPv6 版本的 ND 自动学习功能，no 命令操作重新启动 ND 自动学习功能。

**参数：** 无。

**缺省情况：** 学习 ND 并正常更新。

**命令模式：** 全局配置模式/接口配置。

**使用指南:** 本命令用于在防止 ND 的自动学习与更新。与 ip nd-security updateprotect 不同的是，此命令开启后，无论是否合法的 ND 表项，即使一直发送请求/应答报文，一样会超时。建议与转换操作搭配使用，命令全局优先。

**举例：**

Switch(Config-if-Vlan1)#ipv6 nd-security learnprotect

Switch(config)#ipv6 nd-security learnprotect

## 14.3.3 ipv6 nd-security convert

**命令：ipv6 nd-security convert**

**功能：** 将所有动态 ND 转变为静态 ND。

**参数：** 无。

**命令模式：** 全局配置模式/接口配置。

**使用指南:** 本命令用于将动态 ND 表项转换为静态的 ND 表项。配合关闭学习功能达到防止 ND 绑定的作用。执行之后，该命令就无效了。

**举例：**

Switch(Config-if-Vlan1)#ipv6 nd-security convert

Switch(config)#ipv6 nd-security convert

### 14.3.4 clear ipv6 nd dynamic

命令：clear **ipv6 nd dynamic**

**功能：** 清除接口上所有的动态 ND。

**参数：** 无。

**命令模式：** 接口配置。

**使用指南:** 本命令用于在使用防 ND 绑定功能之前的动态表项清理工作。执行之后，该命令就无效了。

**举例：**

Switch(Config-if-Vlan1)#clear ipv6 nd dynamic

## 14.4 RIPng

### 14.4.1 clear ipv6 route

**命令：clear ipv6 rip route { *<ipv6-address >* | kernel |static | connected |rip |ospf |isis | bgp |all }**

**功能：**从 RIPng 路由表中清除特定的路由。

**参数：*<ipv6-address >*** 从 RIP 路由表中清除与目的地址恰好符合的路由，***<ipv6-address >***表示目的地址，是十六进制表示法，带有前缀长度；

**kernel** 从 RIPng 路由表中删去核心路由；

**static** 从 RIPng 路由表中删去静态路由；

**connected** 从 RIPng 路由表删去直连路由；

**rip** 从 RIPng 路由表中仅删去 RIPng 路由；

**ospf** 从 RIPng 路由表中仅删去 IPv6 OSPF 路由；

**bgp** 从 RIPng 路由表中仅删去 IPv6 BGP 路由；

**ISIS** 从 RIPng 路由表中删去 ipv6 isis 路由；

**all** 删去 RIPng 路由表中的所有路由。

**缺省情况：**没有缺省配置。

**命令模式：**特权模式。

**使用指南：**使用带 all 参数的本命令时，将删除 RIPng 路由表中的所有路由。

**举例：**Switch#clear ipv6 rip route 2001:1:1::/64

Switch#clear ipv6 rip route ospf

## 14.4.2 default-information originate

**命令：default-information originate**

**no default-information originate**

**功能：**允许将网络 0::重新分配到 RIPng 中，本命令的 no 操作禁用此功能。

**参数：**无。

**缺省情况：**禁用。

**命令模式：**路由模式。

**举例：**Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#default-information originate

## 14.4.3 default-metric

**命令：default-metric <*value*>**

**no default-metric**

**功能：**设定引入路由的缺省路由权值；本命令的 no 操作恢复缺省值 1。

**参数：<*value*>**为所要设定的路由权值，取值范围 1～16。

**缺省情况：**缺省的路由权值为 1。

**命令模式：**路由模式。

**使用指南：default-metric** 命令用于设定将其它路由协议的路由引入到 RIPng 路由时使用的缺省路由权值。当使用 **redistribute** 命令引入其它协议的路由时，如果不指定具体的路由权值，则以 **default-metric** 所指定的缺省路由权值引入。

**举例：**设定在 RIPng 路由中引入其它路由协议的缺省路由权值为 3。

Switch(config-router)#default-metric 3

**相关命令：redistribute**

## 14.4.4 distance

**命令：distance <*number*> [<*ipv6-address* >] [<*access-list-name*|*access-list-number* >]**

**no distance [<ipv6-address >]**

**功能：**利用本命令设置管理距离。本命令的 no 操作恢复缺省值 120。

**参数：**<number>指定距离的值，取值范围 1-255。<ipv6-address>指定本地链路地址或其前缀。

<access-list-name|access-list-number >指定所应用的访问列表号或者名字。

**缺省情况：**缺省情况下 RIP 的管理距离为 120。

**命令模式：**路由模式与地址族模式。

**使用指南：**当到达同一目的地存在来自于两个不同路由协议的路由时，管理距离用来选择路由。路由协议的管理距离值越小，表明由该协议得到的路由越可靠。

**举例：**

Switch# config terminal

Switch(config)# router rip

Switch(config-router)# distance 8 fe80:1111::4200:21ff:fe00:11 mylist

## 14.4.5 distribute-list

**命令：distribute-list{*access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>|vlan <*vlan-id*>]**

**no distribute-list{*access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>|vlan <*vlan-id*>]**

**功能：**本命令使用访问列表或者前缀列表来过滤发送与接收的路由更新报文。本命令的 no 操作取消路由过滤功能。

**参数：*< access-list-name>***要应用的访问列表号或者名字。***<prefix-list-name>***是要应用的前缀列表的名字。***<ifname>***指定应用路由过滤的接口名。

**缺省情况：**缺省情况下 RIPng 禁用此功能。

**命令模式：**路由模式。

**使用指南：**如果不指定接口：过滤器将应用于所有接口。

**举例：**Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#distribute-list prefix myfilter in Vlan1

## 14.4.6 debug ipv6 rip

**命令：debug ipv6 rip [events| nsm| packet[recv|send][detail]| all]**

**no debug ipv6 rip [events| nsm| packet[recv|send][detail]| all]**

**功能：**用来打开RIPng的各种调试开关，显示各类调试信息。no操作关闭相应的调试开关。

**参数**: events表示显示RIPng events的调试信息；

nsm表示显示RIPng 与NSM的之间的通讯信息；

packet表示显示RIPng数据报的调试信息；

recv表示显示接收到的数据报的信息；

send表示显示发出的数据报的信息；

detail表示显示接收或者发出的数据报的具体信息。

**默认情况：**不打开调试开关。

**命令模式：**特权模式。

**举例：**Switch#debug ipv6 rip packet

Switch#1970/01/11 21:15:08 IMI: SEND[Ethernet1/1/4]: Send to [ff02::9]:521

1970/01/11 21:15:08 IMI: SEND[Ethernet1/1/2]: Send to [ff02::9]:521

1970/01/11 21:15:09 IMI: RECV[Ethernet1/1/4]: Receive from [fe80::20b:46ff:fe57:8e60]:521

1970/01/11 21:15:09 IMI: RECV[Ethernet1/1/4]: 3000:1:1::/64 is filtered by access-list dclist

1970/01/11 21:15:09 IMI: RECV[Ethernet1/1/4]: 3ffe:1:1::/64 is filtered by access-list dclist

1970/01/11 21:15:15 IMI: RECV[Ethernet1/1/2]: Receive from [fe80::203:fff:fe01:257c]:521

## 14.4.7 debug ipv6 rip redistribute message send

**命令：debug ipv6 rip redistribute message send**

**no debug ipv6 rip redistribute message send**

**功能：**打开 RIPng 进程引入其他 OSPFv3 进程路由或者其它路由协议路由的命令下发调试开关。本命令的 no 操作为关闭 RIPng 进程引入其他路由的命令下发调试开关。

**参数：**无。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#debug ipv6 rip redistribute message send

Switch#no debug ipv6 rip redistribute message send

## 14.4.8 debug ipv6 rip redistribute route receive

**命令：debug ipv6 rip redistribute route receive**

**no debug ipv6 rip redistribute route receive**

**功能：**打开 RIPng 进程收到 nsm 发来的路由信息的调试开关。本命令的 no 操作为关闭 RIPng 进程收到 nsm 发来的路由信息的调试开关。

**参数：**无。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#debug ipv6 rip redistribute route receive

## 14.4.9 ipv6 rip aggregate-address

**命令：ipv6 rip aggregate-address X:X::X:X/M**

**no ipv6 rip aggregate-address X:X::X:X/M**

**功能：**配置 IPV6 聚合路由。本命令的 no 操作取消配置 IPV6 聚合路由。

**参数：X:X::X:X/M**：ipv6 地址及前缀长度。

**命令模式：**路由模式或接口配置模式。

**缺省情况：**默认没有配置聚合路由。

**使用指南：**若是在路由模式下配置聚合路由，则必须先启用 RIPng 协议。若是在接口配置模式下，则未启用 RIPng 协议也可以配置聚合路由，但是在接口上启用协议后才能生效。

**举例：**配置全局聚合路由 2001:3f:ed8::99/64。

Switch(config)#router ipv6 rip

Switch(config-router)#ipv6 rip agg 2001:3f:ed8::99/64

## 14.4.10 ipv6 rip split-horizon

**命令：ipv6 rip split-horizon [poisoned]**

**no ipv6 rip split-horizon**

**功能：**设置允许水平分割，本命令的 no 操作禁用水平分割。

**参数：[poisoned]**表示配置带逆向毒化的水平分割。

**缺省情况：**配置带逆向毒化的水平分割。

**命令模式：**接口配置模式。

**使用指南：**水平分割用于防止路由循环（Routing Loops），即防止三层交换机把从一个接口上所学习到的路由再从这个接口广播出去。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**Switch#config terminal

Switch(config)#interface Vlan1

Switch(Config-if-Vlan1)#ipv6 rip split-horizon poisoned

## 14.4.11 ipv6 router rip

**命令：ipv6 router rip**

**no ipv6 router rip**

**功能：**在接口上使能 RIPng，本命令的 no 操作在接口上关闭 RIPng。

**缺省情况：**缺省不配置。

**命令模式：**接口配置模式。

**使用指南：**本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**Switch#config terminal

Switch(config)#interface Vlan1

Switch(Config-if-Vlan1)#ipv6 router rip

## 14.4.12 neighbor

**命令：neighbor <*ipv6-address*> {<*ifname*> | vlan <*vlan-id*>}**

**no neighbor <*ipv6-address*> {<*ifname*> | vlan <*vlan-id*>}**

**功能：**指定需要定点发送的目的地址；本命令的 no 操作为取消指定的地址，恢复信任所有的网关。

**参数：<*ipv6-address*>**为指定发送的目的 IPv6 Link-local 地址，冒号十六进制格式，不带前缀长度。**<*ifname*>**是接口名。

**缺省情况：**RIPng 缺省不向任何定点目的地址发送。

**命令模式：**路由模式。

**使用指南：**与 passive-interface 命令配合可以配置只向特定的邻居发送路由信息。

**举例：**Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#neighbor FE80:506::2 Vlan1

**相关命令：**passive-interface

## 14.4.13 offset-list

**命令： offset-list <*access-list-number |access-list-name*> {in|out }<*number* >[<*ifname*>| vlan <*vlan-id*>]**

**no offset-list <*access-list-number |access-list-name*> {in|out }<*number* >[<*ifname*>| vlan <*vlan-id*>]**

**功能：**对通过 RIPng 学习到的路由的度量加上一个偏移量，本命令的 no 操作禁用此功能。

**参数：< *access-list-number |access-list-name*>**要应用的访问列表号或者名字。**<*number* >**是附加的偏移量，取值范围 0-16；**<*ifname*>**是具体的接口名。

**缺省情况：**默认的偏移量是系统所规定的接口的度量。

**命令模式：**路由模式。

**举例：**Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#offset-list 1 in 5 Vlan1

**相关命令：access-list**

## 14.4.14 passive-interface

**命令：passive-interface[<*ifname*>| vlan <*vlan-id*>]**

**no passive-interface[<*ifname*>| vlan <*vlan-id*>]**

**功能：**指示 RIP 三层交换机在指定的接口上阻塞 RIP 广播，只能向配置了 neighbor 的三层交换机接口发送 RIP 数据包。本命令的 no 操作取消该功能。

**参数：**<*ifname*>是具体的接口名。

**缺省情况：**缺省不配置。

**命令模式：**路由模式。

**举例：**Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#passive-interface Vlan1

**相关命令：show ipv6 rip**

## 14.4.15 redistribute

**命 令 ： redistribute {kernel | connected | static | ospf | isis | bgp} [metric<*value*>] [route-map<*word*>]**

**no redistribute {kernel | connected | static | ospf | isis | bgp} [metric<*value*>] [route-map<*word*>]**

**功能：**引入从其它路由协议学习到的路由到 RIP 中。

**参数：kernel** 从核心路由中引入；

**connected** 从直连路由中引入；

**static** 从静态路由中引入；

**ospf** 从 IPv6 OSPF 路由中引入；

**isis** 从 IPv6 ISIS 路由中引入；

**bgp** 从 IPv6 BGP 路由中引入；

***<value>***是赋给引入路由的度量，取值范围 0-16；

***<word>***指向用于引入路由的路由地图的指针。

**命令模式：**路由模式。

**举例：**Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#redistribute kernel route-map ipi

## 14.4.16 redistribute ospf

**命令：redistribute ospf [*<process-tag>*] [metric*<value>*] [route-map*<word>*]**

**no redistribute ospf [*<process-tag>*]**

**功能：**引入从 OSPFv3 不同进程学到的路由到本 RIPng 进程中。本命令的 no 操作为取消引入从 OSPFv3 指定进程学到的路由到 RIPng 进程中。

**参数：process-tag** 是 OSPFv3 进程标记字符串，最大长度 15，无该参数表示默认进程。

**metric *<value>***是赋给引入路由的度量，取值范围 0-16。

**route-map *<word>***指向用于引入路由的路由地图的指针。

**缺省情况：**默认不引入。

**命令模式：**RIPng 协议配置模式。

**使用指南：**无。

**举例：**RIPng 引入 OSPFv3 进程 abc 的路由。

Switch(config)#router ipv6 rip

Switch(config-router)#redistribute ospf abc

## 14.4.17 route

**命令：route <*ipv6-address*>**

**no route <*ipv6-address*>**

**功能：**本命令配置一条静态 RIPng 路由，no 操作删除此路由。

**参数：<*ipv6-address*>**指明目的 IPv6 地址前缀及前缀长度，冒号十六进制格式。

**使用指南：**本命令增加一条静态 RIPng 路由。这条命令主要是用于调试目的。在核心路由表中不会出现该命令配置的路由，但是用 show ipv6 rip 命令可以查到该命令配置的路由。

**命令模式：**路由模式。

**举例：**Switch#config terminal

Switch(config)#router ipv6 rip

Switch(config-router)#route 3ffe:1234:5678::1/64

## 14.4.18 router ipv6 rip

**命令：router ipv6 rip**

**no router ipv6 rip**

**功能：**开启 RIPng 路由进程并进入 RIPng 配置模式；本命令的 no 操作为关闭 RIPng 路由协议。

**缺省情况：**不运行 RIPng 路由。

**命令模式：**全局配置模式。

**使用指南：**本命令是 RIPng 路由协议的启动开关，进行 RIPng 协议的其他全局配置要先打开本命令。

**举例：**启动 RIP 协议配置模式。

Switch(config)#router ipv6 rip

## 14.4.19 show debugging ipv6 rip

**命令：show debugging ipv6 rip**

**功能：**为以下的调试选项：nsm debugging, RIPng event debugging, RIPng packet debugging和RIPng nsm debugging显示RIPng调试状态。

**命令模式：**特权和配置模式。

**举例：**

Switch#show debugging ipv6 rip

RIPng debugging status:

RIPng event debugging is on

RIPng packet send detail debugging is on

RIPng NSM debugging is on

## 14.4.20 show ipv6 rip interface

**命令：show ipv6 rip interface**

**功能：**确定接口和线协议是已经启动的（UP）。

**命令模式：**特权和配置模式。

**举例：**Switch(config)#show ipv6 rip interface

Loopback is up, line protocol is up

RIPng is not enabled on this interface

Vlan1 is up, line protocol is up

Routing Protocol: RIPng

Passive interface: Disabled

Split horizon: Enabled with Poisoned Reversed

IPv6 interface address:

3000:1:1::1/64

fe80::203:fff:fe0c:cda/64

| 显示信息 | 解释 |
|---|---|
| Vlan1 is up, line protocol is up | 接口已经 Up |
| Routing Protocol: RIP | 接口运行的路由协议为 RIPng |
| Passive interface: Disabled | 不存在 passive-interface |
| Split horizon: Enabled with Poisoned Reversed | 接口配置带毒性逆转的水平分割 |
| IP interface address:<br>3000:1:1::1/64<br>fe80::203:fff:fe01:429e/64 | 接口的 IPv6 地址 |

## 14.4.21 show ipv6 rip redistribute

**命令：show ipv6 rip redistribute**

**功能：**显示 ripng 进程引入其它外部路由的配置信息。

**参数：**无。

**缺省情况：**不显示信息。

**命令模式：**特权和配置模式。

**使用指南：**无。

**举例：**

Switch#show ipv6 rip redistribute

## 14.4.22 show ipv6 protocols rip

**命令：show ipv6 protocols rip**

**功能：**显示 RIPng 进程参数和统计信息。

**命令模式：**特权和配置模式。

**举例：**Switch(config)#show ipv6 protocols rip

Routing Protocol is "ripng"

Sending updates every 30 seconds with +/-50%, next due in 1 seconds

Timeout after 180 seconds, garbage collect after 120 seconds

Outgoing update filter list for all interface is not set

Incoming update filter list for all interface is not set

Ethernet1/1/4 filtered by dclist

Default redistribute metric is 1

Redistributing: static

Interface

Vlan10

Vlan2

Routing for Networks:

| 显示信息 | 解释 |
|---|---|
| Sending updates every 30 seconds with +/-50%, next due in 1 seconds | 每 30 秒发送一次更新 |
| Timeout after 180 seconds, garbage collect after 120 seconds | 路由超时时间为 180 秒，垃圾收集时间为 120 秒 |
| Outgoing update filter list for all interface is not set | 所有接口均未设置发送更新过滤列表 |
| Incoming update filter list for all interface is not set | 所有接口均未设置接收更新过滤列表 |
| Default redistribution metric is 1 | 引入路由的度量默认是 1 |
| Redistributing: static | 将静态路由引入到 RIP 路由中 |
| Interface<br>Vlan10<br>Vlan2 | 运行 RIP 的接口是 Vlan10 与 Vlan2 |

## 14.4.23 show ipv6 rip

**命令：show ipv6 rip**

**功能：**显示 RIPng 路由。

**命令模式：**特权和配置模式。

**举例：**Switch#show ipv6 rip

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,

B - BGP, a - aggregate, s - suppressed

| | Network | Next Hop | If | Met | Tag | Time |
|---|---|---|---|---|---|---|
| R | 2000:1:1::/64 | :: | Vlan2 | 1 | 0 | |
| R | 2001:1:1::/64 | fe80::203:fff:fe01:257c | Vlan2 | 2 | 0 | 02:40 |
| R | 3000:1:1::/64 | :: | Vlan10 | 1 | 0 | |
| R | 3010:1:1::/64 | :: | -- | 1 | 0 | |

其中，R表示RIPng路由，即目的网络地址为2001:1:1::/64、下一跳地址为fe80::203:fff:fe01:257c的一条路由为RIPng路由，它是从以太网口VLAN2学习而来的，度量为2，离超时还剩2分40秒。

**等价命令：show ipv6 rip database**

## 14.4.24 show ipv6 rip database

**命令：show ipv6 rip database**

**功能：**显示 RIPng 数据库的有关信息。

**命令模式：**特权和配置模式。

**举例：**Switch#show ipv6 rip database

**等价命令：show ipv6 rip**

## 14.4.25 show ipv6 rip aggregate

**命令：show ipv6 rip aggregate**

**功能：**本命令显示 ipv6 聚合路由信息。

**参数：**无。

**命令模式：**特权和配置模式。

**缺省情况：**无。

**使用指南：**该命令显示聚合路由在那个接口上配置，Metric、Count、Suppress 等，若是在全局上配置，则接口显示----。Metric 表示度量。Count 表示该聚合路由聚合的学习到的路由。Suppress 表示该聚合路由被聚合的次数。

**举例：**显示 ipv6 聚合路由信息。

Switch(config-router)#show ipv rip agg

Aggregate information of ripng

| Network | Aggregated Ifname | Metric | Count | Suppress |
|---|---|---|---|---|
| 2001::/16 | Vlan1 | 1 | 2 | 0 |

| | | | | |
|---|---|---|---|---|
| 2001:1::/32 | ---- | 1 | 2 | 0 |
| 2001:1:2::/60 | Vlan1 | 1 | 1 | 1 |
| | ---- | 1 | 1 | 1 |

| 显示内容 | 解释 |
|---|---|
| Network | 路由前缀和前缀长度。 |
| Aggregated Ifname | 配置该聚合路由的接口名。若是全局聚合路由，则显示“----” 。 |
| Metric | 聚合路由的度量。 |
| Count | 聚合路由聚合除聚合路由外的路由数目。 |
| Suppress | 聚合路由被聚合的次数。 |

## 14.4.26 show ipv6 rip redistribute

**命令：show ipv6 rip redistribute**

**功能：**显示 RIPng 进程引入其它外部路由的配置信息。

**参数：**无。

**缺省情况：**不显示信息。

**命令模式：**特权模式和配置模式。

**使用指南：**无。

**举例：**

Switch#show ipv6 rip redistribute

## 14.4.27 timers basic

**命令：timers basic *<update> <invalid> <garbage>***

**no timers basic**

**功能：**调整 RIPng 计时器更新、超时、垃圾收集的时间；本命令的 no 操作为恢复各项参数的缺省值。

**参数：*<update>***发送更新报文的时间间隔，单位秒，取值范围5-2147483647；***<invalid>***宣布 RIPng路由无效的时间段，单位秒，取值范围5-2147483647；***<garbage>***为宣布某路由无效后仍可在路由表中存在的时间段，单位秒，取值范围5-2147483647。

**缺省情况：*<update>***缺省值 30；***<invalid>***缺省值 180；***<garbage>***缺省值 120。

**命令模式：**路由模式。

**使用指南：**缺省情况下，系统每 30 秒会广播 RIPng 更新报文；当过了 180 秒不能收到某路由的更新报文，就认为该路由无效；但该路由还能在路由表中存在 120 秒，120 秒后，在路由表删除该路由。

**举例：**设置 RIPng 路由表更新时间为 20 秒，超时时间为 80 秒，垃圾收集的时间为 60 秒。

Switch(config-router)#timers basic 20 80 60

# 14.5 OSPFv3

## 14.5.1 area authentication-mode

**命令：** area (A.B.C.D|<0-4294967295>) authentication-mode (hmac-sha-256) key-id <0-65535> (0 WORD |7 WORD)

no area (A.B.C.D|<0-4294967295>) authentication-mode

**功能：**配置 OSPFv3 区域使用 RFC7166 认证。本命令的 no 操作为取消验证。

**参数：*<id>***为区域号，可以是数字，取值范围 0～4294967295，也可以是一个 IP 地址。

(hmac-sha-256):加密方式，目前只支持 hmac-sha-256 方式。

<0-65535>:key-id 值。

(0 WORD |7 WORD)：指定认证的密钥 ，如果密钥选项为 0，则后续指定明文密钥。如果选项为 7，则后续指定为明文密钥加密后的密文字串。密钥长度范围为 1~128。

**缺省情况：**无认证。

**命令模式：**OSPFv3 协议配置模式。

**使用指南：**配置 OSPFv3 区域使用 RFC7166 认证。接口模式下同样可以配置认证方式，接口下的认证方式优先级高于区域的认证配置方式。当接口配置认证方式后，该接口所在区域的认证方式无法影响该接口的认证行为。一个区域只允许有一个此配置。

**举例：**

Switch(config-router)# area 0 authentication-mode hmac-sha-256 key-id 1 0 qwerty

## 14.5.2 area default cost

**命令：area <*id*> default-cost <*cost*>**

**no area <*id*> default-cost**

**功能：**配置发送到 stub 区域的缺省 summary 路由的代价；本命令的 no 操作为恢复缺省值。

**参数：*<id>***为区域号，可以是数字，取值范围 0～4294967295，也可以是一个 IPv4 地址；***<cost>*** 取值范围为<0-16777214>。

**缺省情况：**OSPFv3 缺省 cost 值为 1。

**命令模式：**OSPFv3 协议配置模式。

**使用指南：**该命令只适用于连接到 stub 区域的 ABR 路由器。

**举例：**设置 area 1 的 default-cost 为 10

Switch(config-router)#area 1 default-cost 10

## 14.5.3 area range

**命令：area <*id*> range <ipv6*address*> [advertise| not-advertise|]**

**no area <*id*> range <ipv6*address*>**

**功能：**在区域边界上汇聚 OSPF 路由，no 命令取消此功能。

**参数：<*id*>**为区域号，可以是数字，取值范围 0～4294967295，也可以是一个 IP 地址；

**<ipv6*address*>=<*X:X::X:X/M*>,**指明区域的 ipv6 网络前缀及前缀长度。

**advertise：**通告这个区域。

**not-advertise ：**不通告这个区域。

如果这两个参数都不配置，则默认是通告这个区域。

**缺省情况：**缺省没有配置此功能。

**命令模式：**OSPFv3 协议配置模式。

**使用指南：**使用本命令汇聚一个区的区内路由。如果区内的网络号以不连续的方式进行配置，在 ABR 上配置本命令可以通告一条 summary 路由，该路由包含了区内所有属于特定 range 的单个网络。

**举例：**

Switch #config terminal

Switch (config)# router ipv6 ospf

Switch (config-router)# area 1 range 2000::/3

## 14.5.4 area stub

**命令：area <*id*> stub [no-summary]**

**no area <*id*> stub [no-summary]**

**功能：**将一个区域定义为一个存根区域，no 命令取消此功能。

**参数：<*id*>**为区域号，可以是数字，取值范围 1～4294967295，也可以是一个 IPv4 地址；

**no-summary：**区域边界路由器停止向存根区发送汇聚链路通告。

**缺省情况：**不定义存根区。

**命令模式：**OSPFv3 协议配置模式。

**使用指南：**在存根区的所有路由器上配置 area stub。对于存根区的路由器有两条配置命令：stub 和 default-cost。所有连接到存根区的路由器都要配置 area stub 命令，对于连接到存根区的区域边界路由器，通过 area default-cost 命令来定义引入的 cost 值。

**举例：**

Switch # config terminal

Switch (config)# router ipv6 ospf

Switch (config-router)# area 1 stub

**相关命令：area default-cost**

## 14.5.5 area virtual-link

**命令：area <*id*> virtual-link A.B.C.D [instance-id <*instance-id*> | INTERVAL <*value*>]**

**no area <*id*> virtual-link A.B.C.D [instance-id <*instance-id*> | |INTERVAL]**

**功能：**在物理上被非骨干区域分开的两个骨干区域之间配置一条逻辑链路。no 命令移去此虚链路。

**参数：<*id*>**为区域号，可以是数字，取值范围 0～4294967295，也可以是一个 IPv4 地址

<***instance-id***>是接口实例 ID，取值范围 0~255，缺省为 0。

***INTERVAL*= [dead-interval|hello-interval|retransmit-interval|transmit-delay]**

**<*value*>:**延迟或间隔的秒数，取值范围1~65535。

**<*dead-interval*>：**经过一段时间没有收到分组，路由器认为一个邻居已经离线。缺省是40秒。

**<*hello-interval*>：**路由器在发送一个hello分组前所等待的时间，缺省是10秒。

**<*retransmit-interval*>：**路由器在重传一个分组前所等待的时间，缺省是5秒。

**<*transmit-delay*>：**在发送一个分组前路由器的延迟时间，缺省为1秒。

**缺省情况：**没有缺省配置。

**命令模式：**OSPFv3 协议配置模式。

**使用指南：**在 OSPFv3 中，所有的非骨干区域都被连接到一个骨干区域。如果到骨干区域的连接丢失了，虚链路将会修复该连接。你可以在任何两个与一个公共非骨干区域有连接的两个骨干区域路由器之间配置虚链路。协议对待由虚链路连接起来的路由器就如一个点对点网络。

**举例：**

Switch#config terminal

Switch(config) #router ipv6 ospf

Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20

Switch(config-router) #area 1 virtual-link 10.10.11.50 instance-id 1

**相关命令：show ipv6 ospf, show ipv6 ospf virtual-links**

## 14.5.6 abr-type

**命令：abr-type {cisco|ibm| standard}**

**no abr-type [cisco|ibm| standard]**

**功能：**使用本命令配置一个OSPF ABR类型，no命令恢复默认值。

**参数：cisco**，使用cisco ABR实现方式；**ibm**，使用ibm ABR实现方式；**shortcut**，指定一个shortcut-ABR；**standard**，使用标准（RFC2328）ABR实现方式。

**缺省情况：**缺省配置为 **cisco**。

**命令模式：**OSPFv3 协议配置模式。

**使用指南：**指定abr的实现类型。本命令有利于OSPF不同实现之间的互操作。在多宿主的环境下，这个命令特别有用。

**举例：**配置 abr 为 standard

Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#abr-type standard

## 14.5.7 default-metric

**命令：default-metric <*value*>**

**no default-metric**

**功能：**本命令设置OSPF路由协议的默认度量值，no命令返回到默认状态。

**参数：<*value*>**，度量值，范围是1~16777214。

**缺省情况：**内置，自动度量转换。

**命令模式：**OSPF 协议配置模式。

**使用指南：**默认度量使得度量不兼容时，路由引入也能继续进行。如果度量不能转换，默认度量提供了替代选择使得路由引入能够继续进行下去。本命令将导致当前的路由协议对于所有的引入路由使用相同的度量值。本命令应该与命令redistribute结合使用。

**举例：**

Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#default-metric 100

## 14.5.8 debug ipv6 ospf events

**命令：[no]debug ipv6 ospf events [abr|asbr|os|router|vlink]**

**功能：**打开显示 OSPF 的各种事件信息的调试开关；本命令是 no 操作为关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

**举例：**

Switch#debug ipv6 ospf events

1970/01/11 01:10:35 IMI: ROUTER[Process:(null)]: GC timer expire

## 14.5.9 debug ipv6 ospf ifsm

**命令：[no]debug ipv6 ospf ifsm [status|events|timers]**

**功能：**打开显示 OSPF 接口状态机调试开关；本命令是 no 操作为关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

**举例：**

Switch#debug ipv6 ospf ifsm

1970/01/11 01:11:44 IMI: IFSM[Vlan1]: Hello timer expire

1970/01/11 01:11:44 IMI: IFSM[Vlan2]: Hello timer expire

## 14.5.10 debug ipv6 ospf lsa

**命令：[no]debug ipv6 ospf lsa [generate|flooding|install|maxage|refresh]**

**功能：**打开显示链路状态宣告信息的调试开关；本命令的 no 操作为关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

## 14.5.11 debug ipv6 ospf nfsm

**命令：[no]debug ipv6 ospf nfsm [status|events|timers]**

**功能：**打开显示 OSPF 邻居状态机调试开关；本命令是 no 操作为关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

Switch#debug ipv6 ospf nfsm

1970/01/11 01:14:07 IMI: NFSM[192.168.2.3-000007d4]: LS update timer expire

1970/01/11 01:14:07 IMI: NFSM[192.168.2.1-000007d3]: LS update timer expire

1970/01/11 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: Full (HelloReceived)

1970/01/11 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: nfsm_ignore called

1970/01/11 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: Full (2-WayReceived)

## 14.5.12 debug ipv6 ospf nsm

**命令：[no]debug ipv6 ospf nsm [interface|redistribute]**

**功能：**打开显示 OSPF NSM 调试开关；本命令是 no 操作为关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

## 14.5.13 debug ipv6 ospf packet

**命令：[no]debug ipv6 ospf packet [dd|detail|hello|ls-ack|ls-request|ls-update|recv|send]**

**功能：**打开显示 OSPF 报文信息的调试开关；本命令的 no 操作为关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

## 14.5.14 debug ipv6 ospf redistribute message send

**命令：debug ipv6 ospf redistribute message send**

**no debug ipv6 ospf redistribute message send**

**功能：**打开/关闭 IPv6 OSPF 进程引入其他 IPv6 OSPF 进程路由的命令下发调试开关。

**参数：**无。

**缺省情况：**默认不打开。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#debug ipv6 ospf redistribute message send

## 14.5.15 debug ipv6 ospf redistribute route receive

**命令：debug ipv6 ospf redistribute route receive**

**no debug ipv6 ospf redistribute route receive**

**功能：**打开/关闭 IPv6 OSPF 进程收到 nsm 发来的路由信息的调试开关。

**参数：**无。

**缺省情况：**默认不打开。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#debug ipv6 ospf redistribute route receive

## 14.5.16 debug ipv6 ospf route

**命令：[no]debug ipv6 ospf route [ase|ia|install|spf]**

**功能：**打开显示 OSPF 有关路由的调试开关；本命令的 no 操作关闭本调试开关。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

## 14.5.17 ipv6 ospf authentication-mode

**命令：** ipv6 ospf authentication-mode (null|(hmac-sha-256) key-id <0-65535> (0 WORD |7 WORD) (instance-id <0-255> | ))

no ipv6 ospf authentication-mode

**功能：**指定接口 OSPFv3 报文使用 RFC7166 认证；本命令的 no 操作为取消验证。

**参数：** NULL:接口为不认证模式。

hmac-sha-256：目前只支持 hmac-sha-256 方式，但后期会扩展。

<0-65535>：key-id 值。

(0 WORD |7 WORD)：指定认证的密钥 ，如果密钥选项为 0，则后续指定明文密钥。如果选项为 7，则后续指定为明文密钥加密后的密文字串。密钥长度范围为 1~128。

instance-id：instance id,范围<0-255>，缺省为 0。

**缺省情况：**跟随区域的认证方式。

**命令模式：**接口配置模式。

**使用指南：**指定接口 OSPFv3 报文使用 RFC7166 认证。注意该接口的认证默认是跟随区域的配置，如区域配置了认证，但该接口不需要认证则需要配置 null。如区域未配置认证，接口配置 null 也是为不认证。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 10

Switch(Config-if-Vlan10)#ipv6 ospf authentication-mode hmac-sha-256 key-id 100 0 asdfg

## 14.5.18 ipv6 ospf cost

**命令：ipv6 ospf cost *<cost>* [instance-id *<id>*]**

**no ipv6 ospf cost [instance-id *<id>*]**

**功能：**指定接口运行 OSPF 协议所需的代价；本命令的 no 操作为恢复缺省值。

**参数：*<id>***是接口实例 ID，取值范围 0~255，缺省为 0。

***<cost >***为 OSPF 协议所需花费的值，取值范围 1～65535。

**缺省情况：**接口缺省的 OSPF 协议所需花费的值为 10。

**命令模式：**接口配置模式。

**使用指南：**本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf cost 3

## 14.5.19 ipv6 ospf dead-interval

**命令：ipv6 ospf dead-interval *<time >* [instance-id *<id>*]**

**no ipv6 ospf dead-interval [instance-id *<id>*]**

**功能：**指定相邻三层交换机路由失效的时间长度；本命令的 no 操作为恢复缺省值。

**参数：*<id>***是接口实例 ID，取值范围 0~255，缺省为 0。

***<time >***为相邻三层交换机失效的时间长度，单位为秒，取值范围 1～65535。

**缺省情况：**三层交换机失效的时间长度缺省为 40 秒（通常是 hello-interval 的 4 倍）。

**命令模式：**接口配置模式。

**使用指南：**当三层交换机在 **dead-interval** 时间间隔内没有接收到来自邻居三层交换机的 HELLO 数据包，则认为该三层交换机不可达、失效。本命令可以根据链路的实际情况修改相邻三层交换机路由失效时间的值。设置的 **dead-interval** 的值将写入 Hello 报文中，并随 Hello 报文传送。为使 OSPF 协议的正常运行，必须保证和该接口相邻的三层交换机之间的

**dead-interval** 参数一致，且至少为 **hello-interval** 值的 4 倍。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf dead-interval 80

## 14.5.20 ipv6 ospf display route single-line

**命令：[no] ipv6 ospf display route single-line**

**功能：**使用本命令改变 show ipv6 ospf route 命令显示结果。no 命令恢复到缺省显示方式。

**缺省情况：**缺省不配置。

**命令模式：**全局模式。

**使用指南：**在缺省情况下，show ipv6 ospf route 命令在多行显示同一条路由。本命令使得在一行显示一条路由。

**举例：**

Switch#config terminal

Switch(config)#ipv6 ospf display route single-line

## 14.5.21 ipv6 ospf hello-interval

**命令：ipv6 ospf hello-interval *<time>* [instance-id *<id>*]**

**no ipv6 ospf hello-interval [instance-id *<id>*]**

**功能：**指定在接口上发送 HELLO 报文的时间间隔；本命令的 no 操作为恢复缺省值。

**参数：*<id>***是接口实例 ID，取值范围 0~255，缺省为 0。

***<time>***为发送 HELLO 报文的时间间隔，单位为秒，取值范围 1～65535。

**缺省情况：**接口缺省发送 HELLO 报文的间隔时间为 10 秒。

**命令模式：**接口配置模式。

**使用指南：**HELLO 数据包是一种最常见的一种数据包，它周期性地被发送至邻接三层交换机，用于发现和维持邻接关系、选举 DR 与 BDR。用户设置的 **hello-interval** 的值将写入 HELLO 报文中，并随 HELLO 报文传送。**hello-interval** 的值越小，则网络拓扑结构的变化将被越快的发现，同时链路开销也增加。为使 OSPF 协议的正常运行，必须保证和该接口相邻的三层交换机之间的 **hello-interval** 参数一致。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf hello-interval 20

**相关命令：ipv6 ospf dead-interval**

## 14.5.22 ipv6 ospf priority

**命令：ipv6 ospf priority *<priority>* [instance-id *<id>*]**

**no ipv6 ospf priority[instance-id *<id>*]**

**功能：**配置接口在选举“指定三层交换机”（DR）时的优先级；本命令的 no 操作为恢复缺省值。

**参数：*<id>***是接口实例 ID，取值范围 0~255，缺省为 0。

***<priority>***为优先级，合法的取值范围是 0～255。

**缺省情况：**接口在选举指定三层交换机时缺省的优先级值为 1。

**命令模式：**接口配置模式。

**使用指南：**当连在同一网段的两台三层交换机都想成为“指定三层交换机”时，根据优先级的值来决定谁是“指定三层交换机”，通常选择优先级高的作为“指定三层交换机”；如果优先级值相等，则选 router-id 号大的。当一台三层交换机的优先级值为 0 时，这台三层交换机将不会被选举为“指定三层交换机”或“备份指定三层交换机”。 本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**配置接口在选举指定三层交换机 DR 中的优先级。将接口 vlan1 配置成没有选举权利，即 priority 值为 0。

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf priority 0
```

## 14.5.23 ipv6 ospf retransmit-interval

**命令：ipv6 ospf retransmit-interval *<time>* [instance-id *<id>*]**

**no ipv6 ospf retransmit-interval [instance-id *<id>*]**

**功能：**指定接口与邻接三层交换机之间传送链路状态宣告（LSA）时的重传间隔；本命令的 no 操作为恢复缺省值。

**参数：*<id>***是接口实例 ID，取值范围 0~255，缺省为 0。

***<time>***为与邻接三层交换机之间传送链路状态宣告时的重传间隔，单位为秒，取值范围 1～65535。

**缺省情况：**缺省重传间隔为 5 秒。

**命令模式：**接口配置模式。

**使用指南：**当一台三层交换机向它的邻居传送链路状态宣告时，它将保持链路状态宣告直至收到对方的确认，若在时间间隔内没有收到确认报文，则三层交换机将重传链路状态宣告。重传间隔的值必须大于两台三层交换机传送报文一个来回的时间。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**设置接口 vlan1 重传 lsa 的时间为 10 秒。

```
Switch#config terminal
```

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf retransmit-interval 10

## 14.5.24 ipv6 ospf transmit-delay

**命令：ipv6 ospf transmit-delay *<time>* [instance-id *<id>*]**

**no ipv6 ospf transmit-delay [instance-id *<id>*]**

**功能：**设置在接口上传送链路状态宣告（LSA）的时延值；本命令的 no 操作为恢复缺省值。

**参数：*<id>***是接口实例 ID，取值范围 0~255，缺省为 0。

***<time>***为接口上传送链路状态宣告的时延值，单位为秒，取值范围 1～65535。

**缺省情况：**接口上传送链路状态宣告的缺省时延值为 1 秒。

**命令模式：**接口配置模式。

**使用指南：**链路状态宣告在本三层交换机中会随时间老化，但在网络传输过程中却不会，因此在发送链路状态宣告之前增加 **transmit-delay** 的时延，使之能在老化之前将链路状态宣告发送出去。应该根据链路状态合理配置 transmit-delay 的数值，不合理的配置可能导致 OSPF 邻居状态不稳定。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**设置接口 vlan1 发送 LSA 的时延为 3 秒。

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf transmit-delay 3

## 14.5.25 ipv6 router ospf

**命令：[no] ipv6 router ospf {area *<area-id>* [instance-id *<instance-id>*|tag *<tag>* [instance-id *<instance-id>*]]| tag *<tag>* aea *<area-id>* [instance-id *<instance-id>*]}**

**功能：**在接口上使能 ospf 路由；本命令的 no 操作取消此配置。

**参数：*<area-id>***是区域 ID，可以是数字，取值范围 0～4294967295，也可以是一个 IPv4 地址。

***<instance-id>***是接口实例 ID，取值范围 0~255，缺省为 0。

***<tag>*** ospfv3 进程标记。

**缺省情况：**缺省不配置。

**命令模式：**接口配置模式。

**使用指南：**当在接口上使能本命令时，area id 和实例 tag 是必须配置的。而实例 ID 是可选的。ospfv3 进程对每个实例 ID 允许一个路由实例。可以在一个接口上用一个实例 ID 使能路由。如果实例 ID 不同，那么可以在一个接口上运行多个 OSPF 进程。但是不同的 OSPF 进程不能使用相同的实例 ID。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 router ospf area 1 tag IPI instance-id 1

## 14.5.26 max-concurrent-dd

**命令：max-concurrent-dd *<value>***

**no max-concurrent-dd**

**功能：**本命令配置OSPF进程处理当前dd的最大并发数，no命令恢复默认值。

**参数：*<value>***取值范围为***<1-65535>***，处理最大并发dd数据包的上限。

**缺省情况：**没有缺省配置，不限制并发 dd 的数量。

**命令模式：**OSPFv3 协议配置模式。

**使用指南：**指定OSPF进程处理当前dd的最大并发数。

**举例：** 设置最大并发 dd 为 20。

Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#max-concurrent-dd 20

## 14.5.27 passive-interface

**命令：[no] passive-interface*<ifname>*|vlan *<vlan-id>***

**功能：**配置在特定接口上不发送 hello 分组，本命令的 no 操作取消该功能。

**参数：*<ifname>***是具体的接口名。

**缺省情况：**缺省不配置。

**命令模式：**OSPFv3 协议配置模式。

**举例：**Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#passive-interface vlan1

## 14.5.28 redistribute

**命令：[no]redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>]**

**功能：**引入从其它路由协议学习到的路由到 OSPF 中。

**参数：kernel** 从核心路由中引入。

**connected** 从直连路由中引入。

**static** 从静态路由中引入。

**rip** 从 RIP 路由中引入。

**isis** 从 ISIS 路由中引入。

**bgp** 从 BGP 路由中引入。

**metric *<value>***是赋给引入路由的度量，取值范围 0~ 16777214。

**metric-type {1|2}**是引入的外部路由的度量类型，只能取 1 或者 2。默认值是 2

**route-map <*word*>**指向用于引入路由的路由地图的指针。

**命令模式：OSPFv3 协议配置模式。**

**使用指南**：将其它路由协议学习引入到 OSPF 区域，生成 AS-external_LSAs。

**举例**：Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#redistribute bgp metric 12 metric-type 1

## 14.5.29 redistribute ospf

**命令：redistribute ospf [<*process-tag*>] [metric<*value*>] [metric-type{1|2}] [route-map<*word*>]**

**no redistribute ospf [<*process-tag*>] [metric<*value*>] [metric-type{1|2}] [route-map<*word*>]**

**功能：** 引入 **process-tag** 进程的路由引入到本进程中。本命令的 no 操作取消对引入 process-tag 进程的路由到本进程中，当输入 metric，metric-type 和 routermap 可选参数时，表示恢复默认引入属性配置。

**参数：process-tag** 是 IPv6 OSPF 进程标记，默认为 NULL。

**metric <*value*>**是赋给引入路由的度量，取值范围 0-16777214。

**metric-type {1|2}**是引入的路由的度量类型，只能取 1 或者 2，缺省为 2。

**route-map <*word*>**指向用于引入路由的路由地图的指针。

**缺省情况：**默认不引入任何 OSPFv3 进程的路由。

**命令模式：**router IPv6 ospf 配置模式。

**使用指南：**当不输入 process-id 时，表示要引入默认 OSPFv3 进程的路由（process-tag 为 NULL）。此命令的 no 操作中，当输入 metric，metric-type 和 routermap 可选参数时，表示恢复默认引入属性配置，当不输入任何的可选参数时表示取消引入该进程的路由。

**举例：**

Switch(config)#router ipv6 ospf 200

Switch(config-router)#redistribute ospf

## 14.5.30 router-id

**命令：router-id<*router-id*>**

**no router-id**

**功能：**为 ospfv3 进程配置路由器 ID。no 操作恢复 ID 到 0.0.0.0。

**参数：<*router-id*>>**是路由器 ID，IPv4 地址格式。

**缺省情况：**缺省是 0.0.0.0。

**使用指南：**如果 router-id 为 0.0.0.0，则 ospfv3 进程无法正常使能。为 ospfv3 配置一个 router-id 是必须的。

**命令模式：**OSPFv3 协议配置模式。

**举例：**Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#router-id 192.168.2.1

## 14.5.31 router ipv6 ospf

**命令：[no] router ipv6 ospf [*<tag>*]**

**功能：**本命令初始化 ospfv3 路由进程并且进入 ospfv3 模式配置 ospfv3 路由进程。no 操作终止相应的进程。

**参数：*<tag>*** ospfv3 进程标记，可以是任意的字母、数字等组成的字符串。

**命令模式：全局模式。**

**使用指南：**为了让 ospfv3 路由进程能够工作，必须配置本命令并且在至少一个接口上使能 ospfv3。当在接口模式下 ipv6 router ospf area 命令所配置的 tag 与 ospf 进程的 tag 相匹配时，ospfv3 进程在该接口上使能。

**举例：**Switch#config terminal

Switch(config)#router ipv6 ospf IPI

## 14.5.32 show ipv6 ospf

**命令：show ipv6 ospf [*<tag>*]**

**功能：**显示 OSPF 全局和区域信息。

**参数：*<tag>***是进程 tag，字符串。

**缺省情况：**不显示。

**命令模式：**所有模式均可。

**举例：**

```
Switch#show ipv6 ospf
Routing Process "OSPFv3 (*null*)" with ID 192.168.2.2
  SPF schedule delay 5 secs, Hold time between SPFs 10 secs
  Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
  Number of external LSA 0. Checksum Sum 0x0000
  Number of AS-Scoped Unknown LSA 0
  Number of LSA originated 6
  Number of LSA received 14
  Number of areas in this router is 1
      Area BACKBONE(0)
          Number of interfaces in this area is 2
          SPF algorithm executed 6 times
          Number of LSA 8.    Checksum Sum 0x43D52
          Number of Unknown LSA 0
```

# 14.5.33 show ipv6 ospf database

**命令：show ipv6 ospf [*<tag>*] database**

**[ router [adv-router <*advertiser_router*>]**

**|network [adv-router <*advertiser_router*>]**

**| intra-prefix [adv-router <*advertiser_router*>]**

**| link [adv-router <*advertiser_router*>]**

**| external [adv-router <*advertiser_router*>]**

**| inter-prefix [adv-router <*advertiser_router*>]**

**| inter-router [adv-router <*advertiser_router*>]]**

**功能：**显示 OSPF 链路状态数据库信息。

**参数：*<tag>***是进程 tag，字符串。

**<*advertiser_router*>**是 Advertising 路由器的 ID，IPv4 地址格式。

**缺省情况：**不显示。

**命令模式：**所有模式均可。

**使用指南：**根据本命令的输出信息，可以查看 OSPF 链路状态数据库信息。

**举例：**

使用 show ipv6 ospf database 命令可以显示关于 OSPF 路由协议的链路状态数据库信息。

例如，显示信息为：

OSPFv3 Router with ID (192.168.2.2) (Process *null*)

Link-LSA (Interface Vlan1)

| Link State ID | ADV Router | Age | Seq# | CkSum | Prefix |
|---|---|---|---|---|---|
| 0.0.7.211 | 192.168.2.2 | 1409 | 0x80000001 | 0x6dda | 1 |
| 0.0.7.212 | 192.168.2.3 | 1357 | 0x80000001 | 0x248e | 1 |

Link-LSA (Interface Vlan2)

| Link State ID | ADV Router | Age | Seq# | CkSum | Prefix |
|---|---|---|---|---|---|
| 0.0.7.211 | 192.168.2.1 | 1450 | 0x80000001 | 0xa565 | 1 |
| 0.0.7.212 | 192.168.2.2 | 1399 | 0x80000001 | 0x4305 | 1 |

Router-LSA (Area 0.0.0.0)

| Link State ID | ADV Router | Age | Seq# | CkSum | Link |
|---|---|---|---|---|---|
| 0.0.0.0 | 192.168.2.1 | 1390 | 0x80000006 | 0x9fe2 | 1 |
| 0.0.0.0 | 192.168.2.2 | 1354 | 0x80000007 | 0x4af5 | 2 |

0.0.0.0 192.168.2.3 1308 0x80000004 0xbbc4 1

Network-LSA (Area 0.0.0.0)

| Link State ID | ADV Router | Age | Seq# | CkSum |
|---|---|---|---|---|
| 0.0.7.211 | 192.168.2.1 | 1390 | 0x80000001 | 0x897e |
| 0.0.7.211 | 192.168.2.2 | 1354 | 0x80000001 | 0x9b69 |

Intra-Area-Prefix-LSA (Area 0.0.0.0)

| Link State ID | ADV Router | Age | Seq# | CkSum | Prefix | Reference |
|---|---|---|---|---|---|---|
| 0.0.0.1 | 192.168.2.1 | 1389 | 0x80000005 | 0x7e2e | 1 | Router-LSA |
| 0.0.0.2 | 192.168.2.1 | 1389 | 0x80000001 | 0x22cb | 1 | Network-LSA |
| 0.0.0.1 | 192.168.2.3 | 1306 | 0x80000002 | 0xd0d7 | 1 | Router-LSA |

| 显示信息 | 解释 |
|---|---|
| Link-LSA (Interface Vlan1) | 表示接口 Vlan1 的 Link LSA 消息 |
| Router-LSA (Area 0.0.0.0) | 表示区域 0 Router LSA 信息； |
| Network-LSA (Area 0.0.0.0) | 表示区域 0 网络 LSA； |
| Intra-Area-Prefix-LSA (Area 0.0.0.0) | 表示区域 0 域内前缀 LSA； |

## 14.5.34 show ipv6 ospf interface

**命令：show ipv6 ospf interface *<ifname>*|vlan *<vlan-id>***

**功能：**显示 OSPF 接口信息。

**参数：*< ifname >***为具体接口名。

**缺省情况：**不显示。

**命令模式：**所有模式均可。

**举例：**

```
Switch#show ipv6 ospf interface
Loopback is up, line protocol is up
  OSPFv3 not enabled on this interface
Vlan1 is up, line protocol is up
  Interface ID 2003
  IPv6 Prefixes
    fe80::203:fff:fe01:257c/64 (Link-Local Address)
    2001:1:1::1/64
  OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0
    Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10
```

```
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 192.168.2.2
      Interface Address fe80::203:fff:fe01:257c
    Backup Designated Router (ID) 192.168.2.3
      Interface Address fe80::203:fff:fe01:d28
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:10
    Neighbor Count is 1, Adjacent neighbor count is 1
Vlan2 is up, line protocol is up
  Interface ID 2004
  IPv6 Prefixes
    fe80::203:fff:fe01:257c/64 (Link-Local Address)
    2000:1:1::1/64
  OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0
    Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State Backup, Priority 1
    Designated Router (ID) 192.168.2.1
      Interface Address fe80::203:fff:fe01:429e
    Backup Designated Router (ID) 192.168.2.2
      Interface Address fe80::203:fff:fe01:257c
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:10
    Neighbor Count is 1, Adjacent neighbor count is 1
    Cryptographic authentication: hmac-sha-256,Key ID:11
```

| 显示信息 | 解释 |
| --- | --- |
| Vlan1 is up, line protocol is up | 接口物理上和逻辑上都 up 起来 |
| IPv6 Prefixes<br>fe80::203:fff:fe01:257c/64 (Link-Local Address)<br>2001:1:1::1/64 | 接口的 IPv6 地址，以及前缀长度； |
| OSPFv3 Process (*null*) | 接口所属的 ospfv3 进程 |
| Area 0.0.0.1 | 接口所属区域； |
| Instance ID 0 | 实例 ID 为 0 |
| Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10 | 进程 ID；路由器 ID；网络类型；代价值 |
| Transmit Delay is 1 sec, State DR, Priority 1 | 接口传送 LAS 的延时值；状态；在选举指定三层交换机中的优先级； |

| | |
|---|---|
| Designated Router (ID) 192.168.2.2<br>Interface Address fe80::203:fff:fe01:257c | 指定三层交换机； |
| Backup Designated Router (ID) 192.168.2.3<br>Interface Address fe80::203:fff:fe01:d28 | 备份指定三层交换机； |
| Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5<br>Hello due in 00:00:10 | OSPF 协议计时器：包括 hello 报文、pollinterval 报文、路由失效、路由重发等的时间值； |
| Neighbor Count is 1, Adjacent neighbor count is 1 | 相邻三层交换机的个数；建立邻接关系三层三层交换机的个数； |
| Cryptographic authentication: hmac-sha-256,Key ID:11 | 此三层接口进行 RFC7166 认证，加密算法为 hmac-sha-256，key id 为 11 |

## 14.5.35 show ipv6 ospf neighbor

**命令：show ipv6 ospf [*<tag>*] neighbor [*<neighbor_id>* | <ifname> detail | detail]**

**功能：**显示 OSPF 邻接点信息。

**参数：*<tag>***是进程 tag，字符串。

***<neighbor_id>***是 IPv4 地址格式的邻居 ID。

**detail：**显示邻居的详细信息。

***<ifname>***接口名。

**缺省情况：**不显示。

**命令模式：**所有模式均可。

**使用指南：**根据本命令输出信息，可以查看 OSPF 邻居的情况。

**举例：**

```
Switch#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
192.168.2.3       1   Full/Backup     00:00:29    Vlan1      0
192.168.2.1       1   Full/DR         00:00:38    Vlan2      0              Vlan1
```

| 显示信息 | 解释 |
|---|---|
| Neighbor ID | 本邻居的 ID |
| Instance ID | 实例 ID |
| Address | 相邻三层交换机的 IP 地址； |
| Interface | 该邻居所属的接口 |
| state | 邻居关系状态； |
| pri | 优先级； |

## 14.5.36 show ipv6 ospf route

**命令：show ipv6 ospf [*<tag>*] route**

**功能：**显示 OSPF 路由表信息。

**参数：*<tag>***是进程 tag，字符串。

**缺省情况：**不显示。

**命令模式：**所有模式均可。

**举例：**

```
Switch#show ipv6 ospf route
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                  Metric
     Next-hop
O  2000:1:1::/64                                10
     directly connected, Vlan2
O  2001:1:1::/64                                10
     directly connected, Vlan1
O  3000:1:1::/64                                20
     via fe80::203:fff:fe01:429e, Vlan2
O  3003:1:1::/64                                20
     via fe80::203:fff:fe01:d28, Vlan1
```

## 14.5.37 show ipv6 ospf redistribute

**命令：show ipv6 ospf [*<process-tag>*] redistribute**

**功能：**显示 OSPF 进程引入其它外部路由的配置信息。

**参数：**IPv6 OSPF 进程 tag 标识，无参数表示显示所有 IPv6 OSPF 进程引入其它外部路由的配置信息。

**缺省情况：**无。

**命令模式：**特权模式和配置模式。

**使用指南：**无。

**举例：**

```
Switch#show ipv6 ospf redistribute
        ospf process abc redistribute information：
          ospf process def
          bgp
        ospf process def redistribute information：
          ospf process abc
```

```
Switch#show ipv6 ospf abc redistribute
        ospf process abc redistribute information：
          ospf process def
          bgp
```

## 14.5.38 show ipv6 ospf topology

**命令：show ipv6 ospf [*<tag>*] topology [area *<area-id>*]**

**功能：**显示 OSPF 拓扑信息。

**参数：*<tag>***是进程 tag，字符串。

***<area-id>***区域 ID，可以是数字，取值范围 0～4294967295，也可以是一个 IPv4 地址。

**缺省情况：**不显示。

**命令模式：**所有模式均可。

**举例：**

```
Switch#show ipv6 ospf topology
OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID           Bits    Metric      Next-Hop              Interface
192.168.2.1                 10          192.168.2.1           Vlan2
192.168.2.2                 --
192.168.2.3                 10          192.168.2.3           Vlan1
```

## 14.5.39 show ipv6 ospf virtual-links

**命令：show ipv6 ospf [*<tag>*] virtual-links**

**功能：**显示 OSPF 虚连接信息。

**参数：*<tag>***是进程 tag，字符串。

**缺省情况：**不显示。

**命令模式：**所有模式均可。

**举例：**

```
Switch#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 5.6.7.8 is up
Transit area 0.0.0.1 via interface Vlan1, instance ID 0
Local address 3ffe:1234:1::1/128
Remote address 3ffe:5678:3::1/128
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Adjacency state Up
```

## 14.5.40 show ipv6 route process-detail

**命令：show ipv6 route [database] process-detail**

**功能：**显示带有具体的进程标识（进程 id 或 tag）的 ip 路由表。

**参数：**含参数 database 表示显示所有路由，不含参数表示只显示生效路由。

**命令模式：**特权和配置模式。

**使用指南：**无。

**举例：**

Switch#show ipv6 route database process-detail

IPv6 Routing Table

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,

I - IS-IS, B - BGP

> - selected route, * - FIB route, p - stale info

Timers: Uptime

C*> ::1/128 via ::, Loopback, 00:29:53

O 2001::/64 [110/10] via ::, Vlan1, 00:01:07 ,process aaa

C*> 2001::/64 via ::, Vlan1, 00:02:54

O*> 2006::/64 [110/10] via ::, Vlan1, 00:01:07, process aaa

O*> 2008::/64 [110/20] via fe80::203:fff:fe01:2542, Vlan1, 00:00:54, process bbb

## 14.5.41 timers spf

**命令：timers spf *<spf-delay> <spf-holdtime>***

**no timers spf**

**功能：**调整路由计算定时器的值。no 命令将相关的值恢复到默认。

**参数：*<spf-delay>*** 默认 5 秒。

***<spf-holdtime>***默认 10 秒。

**命令模式：OSPFv3 协议配置模式。**

**使用指南：**本命令配置了收到拓扑变化与 SPF 计算之间的延迟时间，还配置了两次不连续的 SPF 计算之间的 hold 时间。

**举例：**Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#timers spf 5 10

# 14.6 MBGP4+

## 14.6.1 debug ipv6 bgp redistribute message send

**命令：debug ipv6 bgp redistribute message send**

**no debug ipv6 bgp redistribute message send**

**功能：**打开 MBGP4+进程引入其他 OSPFv3 进程路由或者其它路由协议路由的命令下发调试开关。本命令的 no 操作关闭 MBGP4+进程引入其他路由的命令下发调试开关。

**参数：**无。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#debug ipv6 bgp redistribute message send

## 14.6.2 debug ipv6 bgp redistribute route receive

**命令：debug ipv6 bgp redistribute route receive**

**no debug ipv6 bgp redistribute route receive**

**功能：**打开 MBGP4+进程收到 nsm 发来的路由信息的调试开关。本命令的 no 操作关闭 MBGP4+进程收到 nsm 发来的路由信息的调试开关。

**参数：**无。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#debug ipv6 bgp redistribute route receive

Switch#no debug ipv6 bgp redistribute route receive

## 14.6.3 redistribute ospf (MBGP4+)

**命令：redistribute ospf [<*process-tag*>] [route-map<*word*>]**

**no redistribute ospf [<*process-tag*>]**

**功能：**引入从 OSPFv3 不同进程学到的路由到本 MBGP4+进程中。本命令的 no 操作取消引入从 OSPFv3 指定进程学到的路由到 MBGP4+进程中。

**参数：process-tag** 是 OSPFv3 进程标记字符串，最大长度 15，无该参数表示默认进程。

**route-map <*word*>**指向用于引入路由的路由地图的指针。

**缺省情况：**默认不引入。

**命令模式：**BGP IPv6 协议配置模式。

**使用指南：**无。

**举例：**MBGP4+(as number 为 1)引入 OSPFv3 进程 abc 的路由。

Switch(config)#router bgp 1

Switch(config-router)#address-family ipv6 unicast

Switch (config-router-af)#redistribute ospf abc

作关闭 MBGP4+进程引入其他路由的命令下发调试开关。

**参数：**无。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#debug ipv6 bgp redistribute message send

## 14.6.4 debug ipv6 bgp redistribute route receive

**命令：debug ipv6 bgp redistribute route receive**

**no debug ipv6 bgp redistribute route receive**

**功能：**打开 MBGP4+进程收到 nsm 发来的路由信息的调试开关。本命令的 no 操作关闭 MBGP4+进程收到 nsm 发来的路由信息的调试开关。

**参数：**无。

**缺省情况：**调试开关关闭。

**命令模式：**特权模式。

**使用指南：**无。

**举例：**

Switch#debug ipv6 bgp redistribute route receive

Switch#no debug ipv6 bgp redistribute route receive

## 14.6.5 redistribute ospf (MBGP4+)

**命令：redistribute ospf [<*process-tag*>] [route-map<*word*>]**

**no redistribute ospf [<*process-tag*>]**

**功能：**引入从 OSPFv3 不同进程学到的路由到本 MBGP4+进程中。本命令的 no 操作取消引入从 OSPFv3 指定进程学到的路由到 MBGP4+进程中。

**参数：process-tag** 是 OSPFv3 进程标记字符串，最大长度 15，无该参数表示默认进程。

**route-map *<word>***指向用于引入路由的路由地图的指针。

**缺省情况：**默认不引入。

**命令模式：**BGP IPv6 协议配置模式。

**使用指南：**无。

**举例：**MBGP4+(as number 为 1)引入 OSPFv3 进程 abc 的路由。

Switch(config)#router bgp 1

Switch(config-router)#address-family ipv6 unicast

Switch (config-router-af)#redistribute ospf abc

## 14.6.6 show ipv6 bgp redistribute

**命令：show ipv6 bgp redistribute**

**功能：**显示 MBGP4+进程引入其它外部路由的配置信息。

**参数：**无。

**缺省情况：**不显示信息。

**命令模式：**特权和配置模式。

**使用指南：**无。

**举例：**

Switch#show ipv6 bgp redistribute

5.5.108 show ipv6 bgp

命令：show ipv6 bgp <X:X::X:X/M> longer-prefixes

功能：用于显示 BGP 维护的路由信息。

参数：<X:X::X:X/M>：IPv6 地址及掩码。

缺省情况：无。

命令模式：特权和配置模式。

使用指南：可以针对 IPv6 地址显示 BGP 路由信息。

举例：

Switch#show ipv6 bgp

## 14.6.7 show ipv6 bgp dampening

命令：show ipv6 bgp dampening {<dampened-paths> | <flap-statistics> | <parameters>}

功能：用于显示 BGP 维护的与路由衰减有关的路由。

参数：无。

缺省情况：无。

命令模式：特权和配置模式。

使用指南： 只有经过了振荡的路由才会被显示。Parameters 表示显示配置，不显示具体路由。其它两个选项则分别显示被抑制的路由和正进行衰减（近期曾经失效）的路由信息。

举例：

Switch#show ipv6 bgp dampening dampened-paths

Switch#show ipv6 bgp dampening flap-statistics

Switch#show ipv6 bgp dampening parameters

## 14.6.1 show ipv6 bgp

**命令：show ipv6 bgp *<X:X::X:X/M>* longer-prefixes**

**功能：**用于显示 BGP 维护的路由信息。

**参数：*<X:X::X:X/M>*：**IPv6 地址及掩码。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**可以针对 IPv6 地址显示 BGP 路由信息。

**举例：**

Switch#show ipv6 bgp

## 14.6.2 show ipv6 bgp community

**命令：show ipv6 bgp community *<TYPE>* [exact-match]**

**功能：**用于显示 BGP 维护的含有团体信息的路由。

**参数：*<TYPE>*：**由 AA:NN 形式表示的团体属性号或 local-AS、no-advertise、no-export 组成的集合。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**可以同时选择多个团体，exact-match 表示只显示完全匹配的表项。

**举例：**

Switch#show ipv6 bgp community

## 14.6.3 show ipv6 bgp dampening

**命令：show ipv6 bgp dampening {<dampened-paths> | <flap-statistics> | <parameters>}**

**功能：**用于显示 BGP 维护的与路由衰减有关的路由。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：** 只有经过了振荡的路由才会被显示。Parameters 表示显示配置，不显示具体路由。其它两个选项则分别显示被抑制的路由和正进行衰减（近期曾经失效）的路由信息。

**举例：**

Switch#show ipv6 bgp dampening dampened-paths

Switch#show ipv6 bgp dampening flap-statistics

Switch#show ipv6 bgp dampening parameters

## 14.6.4 show ipv6 bgp filter-list

**命令：show ipv6 bgp filter-list [*<WORD >*]**

**功能：**用于显示 BGP 符合指定 AS 过滤列表的路由。

**参数：*< WORD >*：**AS-PATH 访问列表名。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用 ip as-path access-list 命令配置 AS 访问列表。该命令可以显示通过了访问列表的路由。

**举例：**

Switch#show ip bgp filter-list FL

**相关命令： neighbor filter-list，ip as-path access-list**

## 14.6.5 show ipv6 bgp inconsistent-as

**命令：show ipv6 bgp inconsistent-as**

**功能：**用于显示 BGP AS 不正常的路由。

**参数：*无*。**

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**同一前缀来自不同的始发 AS，被认为是 AS 不正常的路由，该命令可以把这种路由显示出来。

**举例：**

Switch#show ip bgp inconsistent-as

**相关命令：**无。

## 14.6.6 show ipv6 bgp neighbors

**命令：show ipv6 bgp neighbors [IP-ADDRESS] [advertised-routes | received {prefix-filter | routes} | routes]**

**功能：**用于显示 BGP 邻居的相关信息。

**参数：***无*;

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用不带参数的命令显示所有邻居的详细信息，指定 IP 地址时则显示指定 IP 地址的邻居的详细信息，带 advertised-routes、received prefix-filter、received routes、routes 参数，分别显示本端广播的路由，收到的前缀过滤，收到的路由（在启动软重配置功能时）和指定邻居传来的路由信息。

**举例：**

Switch#show ipv6 bgp neighbor

**相关命令：**无

## 14.6.7 show ipv6 bgp paths

**命令：show ipv6 bgp paths**

**功能：**用于显示 BGP 维护的路径信息。

**参数：***无*。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**显示 BGP 路径信息，包括其路径被利用的情况。

**举例：**

Switch#show ipv6 bgp paths

**相关命令：**无。

## 14.6.8 show ipv6 bgp redistribute

**命令：show ipv6 bgp redistribute**

**功能：** 显示 BGP 进程引入其它外部路由的配置信息。

**参数：** 无。

**缺省情况：** 不显示信息。

**命令模式：** 特权模式和配置模式。

**使用指南：** 无。

**举例：**

Switch#show ipv6 bgp redistribute

## 14.6.9 show ipv6 bgp regexp

**命令：show ipv6 bgp regexp [*<LINE>*]**

**功能：**用于显示 BGP 符合指定 AS 相关普通表达式的路由。

**参数：*<LINE>*：**正则表达式。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**可以通过普通表达式选择想要显示的 AS 的 BGP 路由。

**举例：**

Switch#show ipv6 bgp regexp 100

**相关命令：**无.

## 14.6.10 show ipv6 bgp route-map

**命令：show ipv6 bgp route-map [*<NAME>*]**

**功能：**用于显示 BGP 符合指定路由映射的路由。

**参数：*<NAME>*：**路由映射名。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用 route-map 命令配置路由映射。该命令可以显示经过路由映射处理路由。本命令可以显示符合指定路由映射的路由。

**举例：**

Switch#show ipv6 bgp route-map rmp

**相关命令：route-map, neighbor route-map**

## 14.6.11 show ipv6 bgp vrf

**命令：show ipv6 bgp vrf [NAME] {summary | X:X::X:X |X:X::X:X/M}**

**功能：**用于显示 BGP 维护的邻居和路由信息。

**参数：** <NAME>：VRF 实例号

summary：显示 BGP 邻居汇总信息

X:X::X:X：IPv6 网段

X:X::X:X/M：IPv6 地址及前缀长度

**缺省情况：** 无。
**命令模式：** 特权和配置模式。
**使用指南：** 可以针对不同参数（如 IPv4 地址或 IPv4 地址/掩码）显示 BGP 路由信息，也可以显示一个前缀所覆盖的路由或只显示不符合最早的 IP 地址类的路由信息（即路由不是 A 类、B 类和 C 类地址）。
**举例：**
1)显示 bgp ipv6 vrf neighbor 信息:
S2#show ipv6 bgp vrf 1 summary

2)显示 bgp ipv6 vrf 路由信息:

# 14.7 IPv6 黑洞路由

## 14.7.1 ipv6 route null0

**命令：ipv6 route *<ipv6-prefix|prefix-length>* null0 [*<precedence>*]**
**no ipv6 route *<ipv6-prefix|prefix-length>* null0**
**功能：**配置到某一网段的路由，其出接口为 null0。
**参数：***<ipv6-prefix>*参数为 IPv6 网络静态路由的目的地址，*<prefix-length>*参数为 IPv6 前缀长度，null0 为黑洞路由的出口接口名，*<precedence>*参数为本路由的权重，范围为 1-255，默认为 1。
**缺省：**无。
**命令模式：**全局模式。
**使用指南：**在配置 IPv6 的黑洞路由的时候，与普通的静态路由基本一致，只是把出接口置为 null0。
**举例：**增加一条到 2001:2:3:4::/64 网段的黑洞路由。
Switch(config)#ipv6 route 2001:2:3:4::/64 null0

# 14.8 IPv6 组播协议

## 14.8.1 组播

### 14.8.1.1 show ipv6 mroute

**命令：show ipv6 mroute [<GroupAddr> [<SourceAddr>]]**

**功能：**显示 ipv6 组播的软件转发表。

**参数：GroupAddr:** 显示跟此组播地址相关的转发表项。

**SourceAddr：**显示跟此源相关的转发表项。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**无。

**举例：**显示所有组播转发表。

Switch(config)# show ipv6 mroute

Name: Loopback, Index: 2002, State:49

Name: Vlan1, Index: 2006, State:1043

Name: Vlan11, Index: 2007, State:1043

Name: Vlan12, Index: 2008, State:1043

Name: Tunnel1, Index: 2009, State:d1

Name: pim6reg, Index: 2010, State:c1

Name: pimreg, Index: 2011, State:c1

The total matched ip6mr active mfc entries is 1, unresolved ip6mr entries is 1

| Group | Origin | Iif | Wrong | Oif:TTL |
|---|---|---|---|---|
| ff2f::1 | 2014:1:2:3::2 | Tunnel1 | 0 | 2008:1 |
| ff3f::1 | 2012:1:2:3::2 | NULL | 4 | 0:0 |

| 显示信息 | 解释 |
|---|---|
| Name | 接口名 |
| Index | 接口索引 |
| State | 接口状态 |
| The total matched ipmr active mfc entries | 软件转发条目总数 |
| unresolved ipmr entries | 没有下发的转发条目数 |
| Group | 转发条目组地址 |
| Origin | 转发条目源地址 |
| Iif | 转发条目入接口名 |
| Wrong | 从错误接口收到的组播报文个数 |
| Oif | 转发条目出接口索引 |
| TTL | TTL 值 |

## 14.8.2 PIM-DM6

说明：部分 SHOW 和 DEBUG 命令和 PIM-SM 相同，请参考后面 PIM-SM 的配置命令。

### 14.8.2.1 debug ipv6 pim timer sat

**命令：debug ipv6 pim timer sat**

**no debug ipv6 pim timer sat**

**功能：**打开显示 PIM DM 源活动计时器详细信息的调试开关；本命令的 no 操作为关闭本调试开关。

**参数：**无。

**缺省情况：**关闭。

**命令模式：**特权用户配置模式。

**使用指南：**打开此开关，可以显示源活动计时器的详细信息。

**举例：**

Switch # debug ipv6 pim timer sat

备注：PIM-DM 中其他 debug 开关与 PIM-SM 通用。

### 14.8.2.2 debug ipv6 pim timer srt

**命令：debug ipv6 pim timer srt**

**no debug ipv6 pim timer srt**

**功能：**打开显示 PIM DM 状态更新计时器详细信息的调试开关；本命令的 no 操作为关闭本调试开关。

**参数：**无。

**缺省情况：**关闭。

**命令模式：**特权用户配置模式。

**使用指南：**打开此开关，可以显示 PIM DM 状态更新计时器详细信息。

**举例：**

Switch # debug ipv6 pim timer srt

备注：PIM-DM 中其他 debug 开关与 PIM-SM 通用。

### 14.8.2.3 ipv6 mroute

**命令：ipv6 mroute *<X:X::X:X> <X:X::X:X> <ifname> <.ifname>***

**no ipv6 mroute *<X:X::X:X> <X:X::X:X>* [*<ifname> <.ifname>*]**

**功能：**配置静态组播表项。此命令的 no 命令删除静态组播表项或部分出接口。

**参数：*<X:X::X:X> <X:X::X:X>*** 分别为组播的源地址和组地址。

***<ifname> <.ifname>***，第一个为入接口，后面的为出接口。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**所有配置的接口名必须存在，且必须是 VLAN 接口。出接口只有启动了 PIM 且 UP 的接口才能下发，如入接口没有 UP、未启动 PIM 或 RPF 检查不正确，不会下发该表项。通过此命令的 no 命令删除配置的静态组播表项，若删除指令包含所有出接口或未指定接口信息，则删除该静态组播表项，否则删除指定的出接口。

**举例：**

Switch(config)#ipv6 mroute 2001::1 ff1e::1 v10 v20 v30

## 14.8.2.4 ipv6 pim bsr-border

**命令：ipv6 pim bsr-border**

**no ipv6 pim bsr-border**

**功能：**配置、取消接口为 PIM6 BSR-BORDER。

**参数：**无。

**缺省情况：**非 BSR-BORDER。

**命令模式：**接口配置模式。

**使用指南：**配置为 BSR-BORDER 的接口，BSR 相关消息不向该接口发送也不从该接口接收，连接的网络被认为都是该接口的直连网络。

**举例：**

Switch(Config-if-Vlan1)#ipv6 pim bsr-border

## 14.8.2.5 ipv6 pim dense-mode

**命令：ipv6 pim dense-mode**

**no ipv6 pim dense-mode**

**功能：**在接口上启动 PIM-DM 协议；本命令的 no 操作在接口上关闭 PIM-DM 协议。

**参数：**无。

**缺省情况：**缺省为不启动 PIM-DM 协议。

**命令模式：**接口配置模式。

**使用指南：**此命令需要在全局配置模式下执行 ipv6 pim multicast-routing，才能生效。不支持组播协议互操作，即同一台交换机不能同时开启密集模式和稀疏模式。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**在接口 VLAN 1 上启动 PIM-DM 协议。

Switch (config)#ipv6 pim multicast-routing

Switch (config)#interface vlan 1

Switch (Config-if-Vlan1)#ipv6 pim dense-mode

## 14.8.2.6 ipv6 pim dr-priority

**命令：ipv6 pim dr-priority *<priority>***

**no ipv6 pim dr-priority**

**功能：**设置、取消以及改变接口的 DR 优先级值。同一网段相邻节点通过 hello 报文选举出本网段的指定路由器 DR，no 操作恢复默认值。

**参数：*<priority>***优先级，取值范围 0-4294967294。

**缺省情况：**1

**命令模式：**接口配置模式

**使用指南：**取值范围 0-4294967294，值越大，越优先。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**Switch (config)# interface vlan 1

Switch(Config-if-Vlan1)ipv6 pim dr-priority 100

## 14.8.2.7 ipv6 pim exclude-genid

**命令：ipv6 pim exclude-genid**

**no ipv6 pim exclude-genid**

**功能：**此命令使得 PIM DM 发出的 Hello 报文不包含 GenId 选项，no 操作恢复默认。

**参数：**无。

**缺省情况：**Hello 报文包含 GenId 选项。

**命令模式：**接口配置模式

**使用指南：**此命令用于与较老的 Cisco IOS 版本交互。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**配置交换机发出的 hello 报文中不包含 GenID 选项。

Switch(Config-if-Vlan1)#ipv6 pim exclude-genid

## 14.8.2.8 ipv6 pim hello-holdtime

**命令：ipv6 pim hello-holdtime <*value*>**

**no ipv6 pim hello-holdtime**

**功能：**设置 Hello 消息中 Holdtime 项的值，此值用于描述邻居超时时间，如果在这这一时间内，没有收到该邻居的 hello 报文，则将此邻居纪录删除。

**参数：*<value>***是 holdtime 设置时间，取值范围<1-65535>。

**缺省情况：**为 3.5*Hello_interval，hello_interval 的默认值为 30s，因此 hello-holdtime 的默认值为 105s。

**命令模式：**接口配置模式

**使用指南：**如果不设置，则 hellotime 默认为当前 Hello-interval 的 3.5 倍。如果设置的 hellotime 小于当前的 hello_interval，则这个设置会被拒绝。每次 hello-interval 被更新的时候，hello-holdtime 也会根据如下规则更新：如果 hello_holdtime 没有被配置，或者如果 hello_holdtime 被配置了但是比当前的 hello_interval 小，则 hello_holdtime 被修改为

3.5*Hello_interval，否则保持被配置的值。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**配置接 VLAN 1 上的 hello holdtime 设置为 10s。

Switch (config)# interface vlan1

Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10

## 14.8.2.9 ipv6 pim hello-interval

**命令：ipv6 pim hello-interval < *interval*>**

**no ipv6 pim hello-interval**

**功能：**配置接口 PIM-DM hello 报文间隔时间；本命令的 no 操作恢复为缺省值。

**参数：< *interval*>**为周期发送 PIM-DM hello 报文的时间间隔，取值范围 1～18724s。

**缺省情况：**周期发送 PIM-DM hello 报文的时间间隔缺省为 30s。

**命令模式：**接口配置模式

**使用指南：**hello 消息使得 PIM-DM 交换机可以互相定位，确定邻居关系。PIM-DM 交换机通过周期向邻居发送 hello 消息来宣告自己的存在，如果在规定的时间内没有收到邻居发送的 hello 消息，则认为该邻居丢失。该时间值的配置不能大于邻居超时时间。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**在接口 VLAN 1 上配置 PIM-DM hello 间隔。

Switch (config)#interface vlan1

Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20

## 14.8.2.10 ipv6 pim multicast-routing

**命令：ipv6 pim multicast-routing**

**no ipv6 pim multicast-routing**

**功能：**全局启动 PIM 协议；本命令的 no 操作全局关闭 PIM 协议。

**参数：**无。

**缺省情况：**缺省为不启动 PIM 协议。

**命令模式：**全局配置模式

**使用指南：**只有全局运行该命令后，ipv6 pim 才能启动。

**举例：**全局启动 PIM 协议。

Switch (config)#ipv6 pim multicast-routing

## 14.8.2.11 ipv6 pim neighbor-filter

**命令：ipv6 pim neighbor-filter <a*cess-list-name*>**

**no ipv6 pim neighbor-filter <a*cess-list-name*>**

**功能：**配置邻居访问列表。如果被列表过滤，如果已经同此邻居建立连接，则此连接马上被切断，如果没有建立连接，则这个连接不能建立。

**参数：<*acess-list-name*>**是要应用的访问列表名。

**缺省情况：**没有 neighbor filter 设置。

**命令模式：**接口配置模式

**使用指南：**如果不需要与对端建立邻居关系，通过此命令把对端的 pim 信息过滤。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：** 在接口 VLAN 1 上配置 pim 邻居的访问列表。

Switch(Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter

Switch(config)#ipv6 access-list standard myfilter

Switch(config_IPv6_Std-Nacl-myfilter)#deny fe80:20e:cff:fe01::/32

Switch(config_IPv6_Std-Nacl-myfilter)#permit any

## 14.8.2.12 ipv6 pim scope-border

**命令：ipv6 pim scope-border [*<500-599>*|*<acl_name>*]**

**no ipv6 pim scope-border**

**功能：**配置、取消 PIM6 的管理边界。

**参数：*<500-599>*：**判断是否属于管理范围组地址的 ACL 号。

***<acl_name>*：**判断是否属于管理范围组地址的 ACL 名，应当是标准 ACL 名。

**缺省情况：**非管理边界，访问列表不指定表示使用默认的管理组范围。

**命令模式：**接口配置模式。

**使用指南：**配置 IPV6 pim 的管理边界和使用的 ACL。组播数据表项 SCOPE-BORDER 扩散。

**举例：**

Switch(Config-if-Vlan2)#ipv6 pim scope-border 503

## 14.8.2.13 ipv6 pim state-refresh origination-interval

**命令：ipv6 pim state-refresh origination-interval <interval>**

**no ipv6 pim state-refresh origination-interval**

**功能：**配置该接口上 state-refresh 报文发送间隔。no 操作恢复默认值。

**参数：**<*interval*> 报文发送间隔值 4-100s。

**缺省情况：**60s。

**命令模式：**接口配置模式

**使用指南：**第一跳路由器定期发送 state-refresh 报文以维持所有下游路由器的 PIM-DM 表项。通过此命令可以修改 state-refresh 报文的发送间隔，通常不建议您修改相关定时器的时间间隔。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**将 VLAN 1 上的 state-refresh 报文发送间隔设为 90 秒。

Switch (Config-if-Vlan1)#ipv6 pim state-refresh origination-interval 90

Switch (Config-if-Vlan1)#

## 14.8.2.14 show ipv6 pim interface

**命令：show ipv6 pim interface [detail|]**

**功能：**显示 PIM 接口信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**

**举例：**

```
Switch#show ipv6 pim interface
Interface VIFindex Ver/      Nbr       DR
                            Mode      Count    Prior
Vlan2        0              v2/S      0          1
      Address             : fe80::203:fff:fee3:1244
      Global Address: 2000:1:111::100
      DR                  : this system
Vlan3        2              v2/S      0          1
      Address             : fe80::203:fff:fee3:1244
      Global Address: 2000:10:1:13::1
      DR                  : this system
```

| 显示信息 | 解释 |
|---|---|
| Address | 接口地址 |
| Interface | 接口名 |
| VIF index | 接口索引号 |
| Ver/Mode | pim 版本和模式，版本一般为 v2，sparse mode 显示 S， dense mode 显示 D |
| Nbr Count | 此接口上的邻居个数 |
| DR Prior | Dr 优先级 |
| DR | 此接口 DR 的地址 |

## 14.8.2.15 show ipv6 pim mroute dense-mode

**命令：show ipv6 pim mroute dense-mode [group <*X:X::X:X*>] [source <*X:X::X:X*>]**

**功能：**显示 PIM-DM 报文转发项。

**参数：**group <X:X::X:X>：显示跟此组播地址相关的转发表项。

source <X:X::X:X>：显示跟此源相关的转发表项。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**使用指南：**本命令用于显示 PIM-DM 维护的组播路由信息。

**举例：**显示所有 PIM-DM 报文转发项。

```
Switch(config)#show ipv6 pim mroute dense-mode
IP Multicast Routing Table

(*,G) Entries: 1
(S,G) Entries: 1

(*, ff1e::15)
  Local         ..l.....................

(2000:10:1:12::11, ff1e::15)
RPF nbr: ::
RPF idx: Vlan12
Upstream State: FORWARDING
Origin State: ORIGINATOR
  Local         .....................
  Pruned        .....................
  Asserted      .....................
  Outgoing      ..o.....................

Switch#
```

| 显示信息 | 解释 |
|---|---|
| (*, ff1e::15) | (*,G)转发项 |
| (2000:10:1:12::11, ff1e::15) | (S,G)转发项 |
| RPF nbr | 反向路径邻居，DM 中指源方向的上游邻居，::表示此交换机既为第一跳 |
| RPF idx | RPF 邻居所在的接口 |
| Upstream State | 上游方向状态，有 FORWARDING(可以转发上游的数据)，PRUNED(上游停止转发数据)，ACKPENDING(等待上游响应，转发上游数据) |
| Origin State | 有两个值：ORIGINATOR(处于可发 state-refresh 状态)，NON_ ORIGINATOR(不可发 state-refresh 状态) |
| Local | 本地加入接口，此接口收到 MLD Join |
| Pruned | PIM 剪枝接口，此接口收到 Prune 消息 |
| Asserted | Asserted 状态 |

| | |
|---|---|
| Outgoing | 组播数据最终出接口的 index 号，在此例中出接口的 index 为 2。可以通过命令 show ip pim interface 察看接口详细信息 |

## 14.8.2.16 show ipv6 pim neighbor

**命令：show ipv6 pim neighbor [detail|]**

**功能：**显示路由器邻居。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示 PIM 协议维护的组播路由器邻居信息。

**举例：**

Switch(config)#show ipv6 pim neighbor

| Neighbor Address | Interface | Uptime/Expires | Ver | DR Priority/Mode |
|---|---|---|---|---|
| Fe80::203:fff:fee3:1244 | Vlan1 | 00:00:10/00:01:35 | v2 | 1 /DR |
| fe80::20e:cff:fe01:facc | Vlan1 | 00:00:13/00:01:32 | v2 | 1 / |

| 显示信息 | 解释 |
|---|---|
| Neighbor Address | 邻居地址 |
| Interface | 邻居所在接口 |
| Uptime/Expires | 运行时间/超时时间 |
| Ver | pim 版本，一般为 v2 |
| DR Priority/Mode | 此邻居发来 Hello 消息中的 DR 优先级以及此邻居是否该接口上的 DR |

## 14.8.2.17 show ipv6 pim nexthop

**命令：show ipv6 pim nexthop**

**功能：**显示 PIM 缓存的单播路由表中的下一跳路由器。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示 PIM 保存的下一跳路由器信息。

**举例：**

Switch#show ipv6 pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable ….

| Destination | Type | Nexthop Num | Nexthop Addr | ..Nexthop Ifindex | Nexthop Name | Metric | Pref | Refcnt |
|---|---|---|---|---|---|---|---|---|
| 2000:1:111::11 | ..S. | 1 | | 2004 | | 0 | 0 | 2 |
| 2000:1:111::100 | .RS. | 1 | | 2004 | | 0 | 0 | 2 |

| 显示信息 | 解释 |
|---|---|
| Destination | 下一跳的目标地址 |
| Type | N：新创建的下一跳，还没有确定 RP 方向或者 S 方向 R：RP 方向 S：源方向 U：不可到达 |
| Nexthop Num | 下一跳计数 |
| Nexthop Addr | 下一跳地址 |
| Nexthop Ifindex | 下一跳所在接口索引 |
| Nexthop Name | 下一跳名字 |
| Metric | 到下一跳的路径损耗 Metric |
| Pref | 路径 Preference |
| Refcnt | 引用计数 |

## 14.8.3 PIM-DM6

说明：部分 SHOW 和 DEBUG 命令和 PIM-SM 相同，请参考后面 PIM-SM 的配置命令。

### 14.8.3.1 debug ipv6 pim timer sat

**命令：debug ipv6 pim timer sat**

**no debug ipv6 pim timer sat**

**功能：**打开显示 PIM DM 源活动计时器详细信息的调试开关；本命令的 no 操作为关闭本调试开关。

**参数：**无。

**缺省情况：**关闭。

**命令模式：**特权用户配置模式。

**使用指南：**打开此开关，可以显示源活动计时器的详细信息。

**举例：**

Switch # debug ipv6 pim timer sat

备注：PIM-DM 中其他 debug 开关与 PIM-SM 通用。

## 14.8.3.2 debug ipv6 pim timer srt

**命令：debug ipv6 pim timer srt**

**no debug ipv6 pim timer srt**

**功能：**打开显示 PIM DM 状态更新计时器详细信息的调试开关；本命令的 no 操作为关闭本调试开关。

**参数：**无。

**缺省情况：**关闭。

**命令模式：**特权用户配置模式。

**使用指南：**打开此开关，可以显示 PIM DM 状态更新计时器详细信息。

**举例：**

Switch # debug ipv6 pim timer srt

备注：PIM-DM 中其他 debug 开关与 PIM-SM 通用。

## 14.8.3.3 ipv6 mroute

**命令：ipv6 mroute *<X:X::X:X> <X:X::X:X> <ifname> <.ifname>***

**no ipv6 mroute *<X:X::X:X> <X:X::X:X>* [*<ifname> <.ifname>*]**

**功能：**配置静态组播表项。此命令的 no 命令删除静态组播表项或部分出接口。

**参数：*<X:X::X:X> <X:X::X:X>*** 分别为组播的源地址和组地址。

***<ifname> <.ifname>***，第一个为入接口，后面的为出接口。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**所有配置的接口名必须存在，且必须是 VLAN 接口。出接口只有启动了 PIM 且 UP 的接口才能下发，如入接口没有 UP、未启动 PIM 或 RPF 检查不正确，不会下发该表项。通过此命令的 no 命令删除配置的静态组播表项，若删除指令包含所有出接口或未指定接口信息，则删除该静态组播表项，否则删除指定的出接口。

**举例：**

Switch(config)#ipv6 mroute 2001::1 ff1e::1 v10 v20 v30

## 14.8.3.4 ipv6 pim bsr-border

**命令：ipv6 pim bsr-border**

**no ipv6 pim bsr-border**

**功能：**配置、取消接口为 PIM6 BSR-BORDER。

**参数：**无。

**缺省情况：**非 BSR-BORDER。

**命令模式：**接口配置模式。

**使用指南：**配置为 BSR-BORDER 的接口，BSR 相关消息不向该接口发送也不从该接口接收，连接的网络被认为都是该接口的直连网络。

**举例：**

Switch(Config-if-Vlan1)#ipv6 pim bsr-border

## 14.8.3.5 ipv6 pim dense-mode

**命令：ipv6 pim dense-mode**

**no ipv6 pim dense-mode**

**功能：**在接口上启动 PIM-DM 协议；本命令的 no 操作在接口上关闭 PIM-DM 协议。

**参数：**无。

**缺省情况：**缺省为不启动 PIM-DM 协议。

**命令模式：**接口配置模式。

**使用指南：**此命令需要在全局配置模式下执行 ipv6 pim multicast-routing，才能生效。不支持组播协议互操作，即同一台交换机不能同时开启密集模式和稀疏模式。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**在接口 VLAN 1 上启动 PIM-DM 协议。

Switch (config)#ipv6 pim multicast-routing

Switch (config)#interface vlan 1

Switch (Config-if-Vlan1)#ipv6 pim dense-mode

## 14.8.3.6 ipv6 pim dr-priority

**命令：ipv6 pim dr-priority *<priority>***

**no ipv6 pim dr-priority**

**功能：**设置、取消以及改变接口的 DR 优先级值。同一网段相邻节点通过 hello 报文选举出本网段的指定路由器 DR，no 操作恢复默认值。

**参数：*<priority>***优先级，取值范围 0-4294967294。

**缺省情况：**1

**命令模式：**接口配置模式

**使用指南：**取值范围 0-4294967294，值越大，越优先。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**Switch (config)# interface vlan 1

Switch(Config-if-Vlan1)ipv6 pim dr-priority 100

## 14.8.3.7 ipv6 pim exclude-genid

**命令：ipv6 pim exclude-genid**

**no ipv6 pim exclude-genid**

**功能：**此命令使得 PIM DM 发出的 Hello 报文不包含 GenId 选项，no 操作恢复默认。

**参数：**无。

**缺省情况：**Hello 报文包含 GenId 选项。

**命令模式：**接口配置模式

**使用指南：**此命令用于与较老的 Cisco IOS 版本交互。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**配置交换机发出的 hello 报文中不包含 GenID 选项。

Switch(Config-if-Vlan1)#ipv6 pim exclude-genid

## 14.8.3.8 ipv6 pim hello-holdtime

**命令：ipv6 pim hello-holdtime <*value*>**

**no ipv6 pim hello-holdtime**

**功能：**设置 Hello 消息中 Holdtime 项的值，此值用于描述邻居超时时间，如果在这这一时间内，没有收到该邻居的 hello 报文，则将此邻居纪录删除。

**参数：<*value*>**是 holdtime 设置时间，取值范围<1-65535>。

**缺省情况：**为 3.5*Hello_interval，hello_interval 的默认值为 30s，因此 hello-holdtime 的默认值为 105s。

**命令模式：**接口配置模式

**使用指南：**如果不设置，则 hellotime 默认为当前 Hello-interval 的 3.5 倍。如果设置的 hellotime 小于当前的 hello_interval，则这个设置会被拒绝。每次 hello-interval 被更新的时候，hello-holdtime 也会根据如下规则更新：如果 hello_holdtime 没有被配置，或者如果 hello_holdtime 被配置了但是比当前的 hello_interval 小，则 hello_holdtime 被修改为 3.5*Hello_interval，否则保持被配置的值。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**配置接 VLAN 1 上的 hello holdtime 设置为 10s。

Switch (config)# interface vlan1

Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10

## 14.8.3.9 ipv6 pim hello-interval

**命令：ipv6 pim hello-interval < *interval*>**

**no ipv6 pim hello-interval**

**功能：**配置接口 PIM-DM hello 报文间隔时间；本命令的 no 操作恢复为缺省值。

**参数：< *interval*>**为周期发送 PIM-DM hello 报文的时间间隔，取值范围 1～18724s。

**缺省情况：**周期发送 PIM-DM hello 报文的时间间隔缺省为 30s。

**命令模式：**接口配置模式

**使用指南：**hello 消息使得 PIM-DM 交换机可以互相定位，确定邻居关系。PIM-DM 交换机通过周期向邻居发送 hello 消息来宣告自己的存在，如果在规定的时间内没有收到邻居发送的

hello 消息，则认为该邻居丢失。该时间值的配置不能大于邻居超时时间。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**在接口 VLAN 1 上配置 PIM-DM hello 间隔。

Switch (config)#interface vlan1

Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20

## 14.8.3.10 ipv6 pim multicast-routing

**命令：ipv6 pim multicast-routing**

**no ipv6 pim multicast-routing**

**功能：**全局启动 PIM 协议；本命令的 no 操作全局关闭 PIM 协议。

**参数：**无。

**缺省情况：**缺省为不启动 PIM 协议。

**命令模式：**全局配置模式

**使用指南：**只有全局运行该命令后，ipv6 pim 才能启动。

**举例：**全局启动 PIM 协议。

Switch (config)#ipv6 pim multicast-routing

## 14.8.3.11 ipv6 pim neighbor-filter

**命令：ipv6 pim neighbor-filter <a*cess-list-name*>**

**no ipv6 pim neighbor-filter <a*cess-list-name*>**

**功能：**配置邻居访问列表。如果被列表过滤，如果已经同此邻居建立连接，则此连接马上被切断，如果没有建立连接，则这个连接不能建立。

**参数：<a*cess-list-name*>**是要应用的访问列表名。

**缺省情况：**没有 neighbor filter 设置。

**命令模式：**接口配置模式

**使用指南：**如果不需要与对端建立邻居关系，通过此命令把对端的 pim 信息过滤。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：** 在接口 VLAN 1 上配置 pim 邻居的访问列表。

Switch(Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter

Switch(config)#ipv6 access-list standard myfilter

Switch(config_IPv6_Std-Nacl-myfilter)#deny fe80:20e:cff:fe01::/32

Switch(config_IPv6_Std-Nacl-myfilter)#permit any

## 14.8.3.12 ipv6 pim scope-border

**命令：ipv6 pim scope-border [*<500-599>*|*<acl_name>*]**

**no ipv6 pim scope-border**

**功能：**配置、取消 PIM6 的管理边界。

**参数：*<500-599>***：判断是否属于管理范围组地址的 ACL 号。

***<acl_name>***：判断是否属于管理范围组地址的 ACL 名，应当是标准 ACL 名。

**缺省情况：**非管理边界，访问列表不指定表示使用默认的管理组范围。

**命令模式：**接口配置模式。

**使用指南：**配置 IPV6 pim 的管理边界和使用的 ACL。组播数据表项 SCOPE-BORDER 扩散。

**举例：**

```
Switch(Config-if-Vlan2)#ipv6 pim scope-border 503
```

## 14.8.3.13 ipv6 pim state-refresh origination-interval

**命令：ipv6 pim state-refresh origination-interval <interval>**

**no ipv6 pim state-refresh origination-interval**

**功能：**配置该接口上 state-refresh 报文发送间隔。no 操作恢复默认值。

**参数：**<*interval*> 报文发送间隔值 4-100s。

**缺省情况：**60s。

**命令模式：**接口配置模式

**使用指南：**第一跳路由器定期发送 state-refresh 报文以维持所有下游路由器的 PIM-DM 表项。通过此命令可以修改 state-refresh 报文的发送间隔，通常不建议您修改相关定时器的时间间隔。本命令可以在 IPv6 隧道接口上配置，但注意只有配置隧道才能配置成功。

**举例：**将 VLAN 1 上的 state-refresh 报文发送间隔设为 90 秒。

```
Switch (Config-if-Vlan1)#ipv6 pim state-refresh origination-interval  90
Switch (Config-if-Vlan1)#
```

## 14.8.3.14 show ipv6 pim interface

**命令：show ipv6 pim interface [detail|]**

**功能：**显示 PIM 接口信息。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**

**举例：**

```
Switch#show ipv6 pim interface
Interface VIFindex Ver/     Nbr       DR
                            Mode      Count    Prior
Vlan2        0              v2/S      0          1
     Address            : fe80::203:fff:fee3:1244
     Global Address: 2000:1:111::100
     DR                 : this system
```

Vlan3 2 v2/S 0 1

Address : fe80::203:fff:fee3:1244

Global Address: 2000:10:1:13::1

DR : this system

| 显示信息 | 解释 |
|---|---|
| Address | 接口地址 |
| Interface | 接口名 |
| VIF index | 接口索引号 |
| Ver/Mode | pim 版本和模式，版本一般为 v2，sparse mode 显示 S， dense mode 显示 D |
| Nbr Count | 此接口上的邻居个数 |
| DR Prior | Dr 优先级 |
| DR | 此接口 DR 的地址 |

## 14.8.3.15 show ipv6 pim mroute dense-mode

**命令：show ipv6 pim mroute dense-mode [group <*X:X::X:X*>] [source <*X:X::X:X*>]**

**功能：**显示 PIM-DM 报文转发项。

**参数：**group <X:X::X:X>：显示跟此组播地址相关的转发表项。

source <X:X::X:X>：显示跟此源相关的转发表项。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**使用指南：**本命令用于显示 PIM-DM 维护的组播路由信息。

**举例：**显示所有 PIM-DM 报文转发项。

Switch(config)#show ipv6 pim mroute dense-mode

IP Multicast Routing Table

(*,G) Entries: 1

(S,G) Entries: 1

(*, ff1e::15)

Local ..l.....

(2000:10:1:12::11, ff1e::15)

RPF nbr: ::

RPF idx: Vlan12

Upstream State: FORWARDING

Origin State: ORIGINATOR

Local .....
Pruned .....
Asserted .....
Outgoing ..o.....

Switch#

| 显示信息 | 解释 |
|---|---|
| (*, ff1e::15) | (*,G)转发项 |
| (2000:10:1:12::11, ff1e::15) | (S,G)转发项 |
| RPF nbr | 反向路径邻居，DM 中指源方向的上游邻居，::表示此交换机既为第一跳 |
| RPF idx | RPF 邻居所在的接口 |
| Upstream State | 上游方向状态，有 FORWARDING(可以转发上游的数据)，PRUNED(上游停止转发数据)，ACKPENDING(等待上游响应，转发上游数据) |
| Origin State | 有两个值：ORIGINATOR(处于可发 state-refresh 状态)，NON_ ORIGINATOR(不可发 state-refresh 状态) |
| Local | 本地加入接口，此接口收到 MLD Join |
| Pruned | PIM 剪枝接口，此接口收到 Prune 消息 |
| Asserted | Asserted 状态 |
| Outgoing | 组播数据最终出接口的 index 号，在此例中出接口的 index 为 2。可以通过命令 show ip pim interface 察看接口详细信息 |

## 14.8.3.16 show ipv6 pim neighbor

**命令：show ipv6 pim neighbor [detail|]**

**功能：**显示路由器邻居。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示 PIM 协议维护的组播路由器邻居信息。

**举例：**

Switch(config)#show ipv6 pim neighbor

Neighbor Address Interface Uptime/Expires Ver DR Priority/Mode

Fe80::203:fff:fee3:1244 Vlan1 00:00:10/00:01:35 v2 1 /DR

fe80::20e:cff:fe01:facc Vlan1 00:00:13/00:01:32 v2 1 /

| 显示信息 | 解释 |
|---|---|
| Neighbor Address | 邻居地址 |
| Interface | 邻居所在接口 |
| Uptime/Expires | 运行时间/超时时间 |
| Ver | pim 版本，一般为 v2 |
| DR Priority/Mode | 此邻居发来 Hello 消息中的 DR 优先级以及此邻居是否该接口上的 DR |

## 14.8.3.17 show ipv6 pim nexthop

**命令：show ipv6 pim nexthop**

**功能：**显示 PIM 缓存的单播路由表中的下一跳路由器。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权和配置模式。

**使用指南：**用于显示 PIM 保存的下一跳路由器信息。

**举例：**

Switch#show ipv6 pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable ….

| Destination | Type | Nexthop Num | Nexthop Addr | ..Nexthop Ifindex | Nexthop Name | Metric | Pref | Refcnt |
|---|---|---|---|---|---|---|---|---|
| 2000:1:111::11 | ..S. | 1 | | 2004 | | 0 | 0 | 2 |
| 2000:1:111::100 | .RS. | 1 | | 2004 | | 0 | 0 | 2 |

| 显示信息 | 解释 |
|---|---|
| Destination | 下一跳的目标地址 |
| Type | N：新创建的下一跳，还没有确定 RP 方向或者 S 方向 R：RP 方向 S：源方向 U：不可到达 |
| Nexthop Num | 下一跳计数 |
| Nexthop Addr | 下一跳地址 |
| Nexthop Ifindex | 下一跳所在接口索引 |
| Nexthop Name | 下一跳名字 |
| Metric | 到下一跳的路径损耗 Metric |

| | |
|---|---|
| Pref | 路径 Preference |
| Refcnt | 引用计数 |

# 14.8.4 ANYCAST RP v6

## 14.8.4.1 debug ipv6 pim anycast-rp

**命令：debug ipv6 pim anycast-rp**

**no debug ipv6 pim anycast-rp**

**功能：**打开交换机 ANYCAST RP 功能的调试开关；本命令的 no 操作为关闭该调试开关。

**命令模式：**特权用户配置模式。

**缺省情况：**缺省关闭交换机的 ANYCAST RP 的调试开关。

**使用指南：**用来打开交换机 ANYCAST RP 调试开关，可以显示交换机处理 PIM 注册数据包信息——packet，事件信息——event。

**举例：**

Switch# debug ipv6 pim anycast-rp

## 14.8.4.2 ipv6 pim anycast-rp

**命令：ipv6 pim anycast-rp**

**no ipv6 pim anycast-rp**

**功能：**打开交换机的 ANYCAST RP 功能；本命令的 no 操作为关闭 ANYCAST RP 功能。

**命令模式：**全局配置模式。

**缺省情况：**交换机缺省不启动 ANYCAST RP。

**使用指南：**本命令全局启动 ANYCAST RP 协议，但是要让 ANYCAST RP 工作，还必须配置 self-rp-address 和 other-rp-address 集。

**举例：**在全局模式启动 ANYCAST RP。

Switch(config)#ipv6 pim anycast-rp

## 14.8.4.3 ipv6 pim anycast-rp

**命令：ipv6 pim anycast-rp *<anycast-rp-addr> <other-rp-addr>***

**no ipv6 pim anycast-rp *<anycast-rp-addr> <other-rp-addr>***

**功能：**配置 ANYCAST RP 地址（ARA）和与本路由器（作为 RP）通讯的其他 RP 的单播地址。本命令的 no 操作为取消配置的对应 RP 地址的某一其他 RP 单播地址。

**参数：*anycast-rp-addr***：RP 地址，允许该地址当前对应的候选接口不存在。

***other-rp-addr***：用于与本路由器（作为 RP）通讯的其它 RP 单播地址。

**命令模式：**全局配置模式。

**缺省情况：**缺省不配置。

**使用指南：**

1 在本路由器（作为 RP）上配置的 anycast-rp-addr 地址，实际上就是在网络中多个 RP 上配置的 RP 地址，对应候选 RP 接口(或者 Loopback 接口)的地址。配置上允许该地址当前对应的候选接口不存在。

2 在本路由器（作为 RP）上配置与本路由器通讯的其他 RP 的 other-rp-address。该单播地址标志其他 RP，用于与本地路由器之间的通讯。

3 当本路由器（作为 RP）收到从 DR 单播过来的注册报文，需要将该注册报文向网络中其他 RP 转发，使得网络中所有 RP 获得源（S,G）状态。转发时，本路由器修改注册报文目的地址为 other-rp-address。

4 对应一个 anycast-rp-addr 可以配置多个 other-rp-address，当收到 DR 单播过来的注册报文，依次向这些其他 RP 转发。

**举例：**在全局配置模式下配置 other-rp-address。

```
Switch(config)#ipv6 pim anycast-rp 2000::1 2004::2
```

## 14.8.4.4 ipv6 pim anycast-rp self-rp-address

**命令：ipv6 pim anycast-rp self-rp-address *<self-rp-addr>***

**no ipv6 pim anycast-rp self-rp-address**

**功能：**配置本路由器（作为 RP）的 self-rp-address。该地址唯一标志本路由器，用于与其他 RP 区分并进行通讯。本命令的 no 操作为取消配置的本路由器（作为 RP）用于与其它 RP 区分的单播地址。

**参数：*self-rp-addr***：本路由器与其他 RP 通讯的单播地址。

**命令模式：**全局配置模式。

**缺省情况：**缺省不配置 self-rp-address。

**使用指南：**

1 当本路由器（作为 RP）收到从 DR 单播过来的注册报文，需要将该注册报文向网络中其他 RP 转发，使得网络中所有 RP 获得源（S,G）状态。转发时，本路由器修改注册报文源地址为 self-rp-address。

2 当本路由器（作为 RP）收到从其他 RP 单播转发过来的注册报文，如注册报文目的地址为本路由器 self-rp-address，则建立（S,G）状态并反方向发送注册中止报文，注册中止报文目的地址即注册报文的源地址。

3 self-rp-address 应为本路由器上某个三层接口地址，但配置时我们允许此接口当前不存在。

**举例：**在全局配置模式下配置本路由器的 self-rp-address。

```
Switch(config)#ipv6 pim anycast-rp self-rp-address 2000::1
```

## 14.8.4.5 ipv6 pim rp-candidate

**命令：ipv6 pim rp-candidate {vlan<*vlan-id*> |loopback<*index*> |<*ifname*>} [<*A:B::C:D*>] [<*priority*>]**

**no ipv6 pim rp-candidate**

**功能：**相对于原 PIM6-SM 命令新增配置某 Loopback 接口作为候选 RP 接口；本命令的 no 操作为取消该 Loopback 接口作为候选 RP 接口。

**参数：*index*：**Loopback 接口索引，范围<1-1024>。

***vlan-id*:**为 VLAN ID。

***ifname*:**为指定接口名。

**A:B::C:D/M:** 为 ip 前缀及掩码。

***<priority>*:** RP 选举的优先级，取值 0-255，默认为 192，数值越低优先级越高。

**命令模式：**全局配置模式。

**缺省情况：**缺省不配置候选 RP 接口。

**使用指南：**为支持 ANYCAST RP 功能，新增允许配置 Loopback 接口作为候选 RP 接口，作为候选 RP 的接口是当前唯一的，并应当将该接口地址加入路由，使得 PIM 路由器可以找到距离自己最近的 RP。可以通过 no ipv6 pim rp-candidate 命令取消候选 RP。

**举例：**在全局配置模式下配置 Loopback1 接口作为候选 RP 接口。

```
Switch(config)#ipv6 pim rp-candidate loopback1
```

## 14.8.4.6 show debugging ipv6 pim

**命令：show debugging ipv6 pim**

**命令模式：**特权和配置模式。

**使用指南：**anycast rp 当前调试开关状态。

**举例：**

```
Switch(config)#show debugging ipv6 pim

Debugging status:
  PIM anycast-rp debugging is on
```

## 14.8.4.7 show ipv6 pim anycast-rp first-hop

**命令：show ipv6 pim anycast-rp first-hop**

**命令模式：**特权和配置模式。

**使用指南：**显示 anycast rp 的状态信息，显示协议当前维护的在首跳 RP 上生成的 mrt 节点信息。

**举例：**

```
Switch(config)#show ipv6 pim anycast-rp first-hop
```

IP Multicast Routing Table

(*,G) Entries: 0

(S,G) Entries: 1

(E,G) Entries: 0

INCLUDE (2000:1:111::2, ff1e::1)

Local .l.....

| 显示信息 | 解释 |
| --- | --- |
| Entries | 各种表项的个数。 |
| INCLUDE | 首跳 RP 上创建的 mrt 信息。 |

## 14.8.4.8 show ipv6 pim anycast-rp non-first-hop

**命令：show ipv6 pim anycast-rp non-first-hop**

**命令模式：**特权和配置模式。

**使用指南：**显示 anycast rp 的状态信息，显示协议当前维护的在非首跳 RP 上生成的 mrt 节点信息。即由首跳 RP 收到注册报文后转发到本 RP 上，由此创建的 mrt 节点信息。

**举例：**

Switch(config)#show ip pim anycast-rp non-first-hop

IP Multicast Routing Table

(*,G) Entries: 0

(S,G) Entries: 1

(E,G) Entries: 0

INCLUDE (2002:1:111::2, ff1e::2)

Local .l.....

| 显示信息 | 解释 |
| --- | --- |
| Entries | 各种表项的个数。 |
| INCLUDE | 首跳 RP 上创建的 mrt 信息。 |

## 14.8.4.9 show ipv6 pim anycast-rp status

**命令：show ipv6 pim anycast-rp status**

**命令模式：**特权和配置模式。

**使用指南：**显示 ANYCAST RP 的配置信息，是否在全局启动了 ANYCAST RP，是否配置 self-rp-address 和当前配置的 anycast rp 集列表。

**举例：**

Switch(config)#show ipv6 pim anycast-rp status

Anycast RP status:

anycast-rp:Enabled!

self-rp-address:2004::2

anycast-rp address: 2000:1:111::2

other rp unicast rp address: 2002::1

other rp unicast rp address: 2005::1

anycast-rp address: 2003::1

other rp unicast rp address: 2002::2

---

| 显示内容 | 解释 |
|---|---|
| anycast-rp: | 全局 anycast rp 开关是否打开。 |
| self-rp-address: | 配置的 self-rp-address。 |
| anycast-rp address: | 配置的 anycast-rp-address。 |
| other rp unicast rp address: | 配置的对应上面 anycast-rp-address 的其他 RP 通讯地址。 |
| other rp unicast rp address: | 配置的对应上面 anycast-rp-address 的其他 RP 通讯地址。 |
| anycast-rp address: | 配置的 anycast-rp-address*。 |
| other rp unicast rp address: | 配置的对应上面 anycast-rp-address 的其他 RP 通讯地址*。 |

# 14.8.5 PIM-SSM6

## 14.8.5.1 ipv6 pim ssm

**命令：ipv6 pim ssm {default|range <*access-list-name* >}**

**no ipv6 pim ssm**

**功能：**配置 pim ssm 组播组地址范围；本命令的 no 操作删除配置的 pim ssm 组播组。

**参数：** ***default :*** 表示 pim ssm 组播组地址取缺省范围 ff3x::/32。**<*access-list-name* >**为要应用的 IPv6 访问列表名。

**缺省情况：**缺省不配置 pim ssm 组地址范围。

**命令模式：**全局配置模式

**使用指南：**

1 只有配置本命令后，pim ssm 才起作用。

2 配置本命令之前，必须确保 ipv6 pim multicasting 配置成功。

3 Access-list 只使用 ipv6 access-list 命令所建立的访问列表。

4 用户可以先执行此命令再配置对应的 acl；也可以在绑定情况下，删除对应 acl。绑定后，只有执行 no ipv6 pim ssm 才能将绑定关系解除。

5 如果要启用 ssm 功能，应该在网络边缘上相关交换机上配置此命令，比如有本地 mld 加入的交换机（必须），以及在组播数据源端的 DR 或者在 RP 上（两者至少有一个）配置此命令，中间交换机则只需起 PIM-SM 即可。

**举例：**配置交换机启动 PIM-SSM，组地址范围是访问列表 test 指定的范围。

Switch (config)#ipv6 pim ssm range test

Switch(config)#ipv6 access-list standard test

Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::/48

# 14.8.6 IPv6 DCSCM

## 14.8.6.1 ipv6 access-list(ipv6 组播源控制)

**命令：ipv6 access-list *<8000-8099>* {deny|permit} {{*<source/M>* }|{host-source *<source-host-ip>*}|any-source} {{*<destination/M>* }|{host-destination *<destination-host-ip>*}|any-destination}**

**no ipv6 access-list *<8000-8099>* {deny|permit} {{*<source/M>* }|{host-source *<source-host-ip>*}|any-source} {{*<destination/M>* }|{host-destination <destination-host-ip>}|any-destination}**

**功能：** 配置 ipv6 源受控组播访问列表，其 NO 形式用于删除该访问列表。

**参数：** <8000-8099>：源受控访问列表号。

{deny|permit}：拒绝或允许。

<source/M>：组播源地址和掩码长度。

<source-host-ip>：组播源主机地址。

<destination/M>：组播目的地址和掩码长度。

<destination-host-ip>：组播目的主机地址。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**IPV6 组播源受控表项使用的 ACL 通过特定的 ACL 号 8000－8099 来控制，本命令用于配置这样的 ACL。IPV6 组播源受控的 ACL 只需要配置要控制的源 IPV6 地址和目的 IPV6

地址（即组 IPV6 地址），其配置方式与其它 ACL 基本相同，可以采用掩码长度配置地址范围，也可以指定一个主机地址或所有地址，值得注意的是，这里的“所有地址”对组 IPV6 地址而言是指 ff::/8。

**举例：**

Switch(config)#ipv6 access-list 8000 permit fe80::203:228a/64 ff1e::1/64

## 14.8.6.2 ipv6 access-list(组播目的控制)

**命令：ipv6 access-list *<9000-10999>* {deny|permit} {{*<source/M>* }|{host-source *<source-host-ip>*}|any-source} {{*<destination/M>* }|{host-destination <destination-host-ip>}|any-destination}**

**no ipv6 access-list *<9000-10999>* {deny|permit} {{*<source/M>* }|{host-source *<source-host-ip>*}|any-source} {{*<destination/M>* }|{host-destination *<destination-host-ip>*}|any-destination}**

**功能：** 配置 IPV6 目的受控组播访问列表，其 NO 形式用于删除该访问列表。

**参数：** <9000-10999>：源受控访问列表号。

{deny|permit}：拒绝或允许。

<source/M>：组播源地址和掩码长度。

<source-host-ip>：组播源主机地址。

<destination/M>：组播目的地址和掩码长度。

<destination-host-ip>：组播目的主机地址。

**缺省情况：**无。

**命令模式：**全局配置模式。

**使用指南：**IPV6 组播目的受控表项使用的 ACL 通过特定的 ACL 号 9000-10999 来控制，本命令用于配置这样的 ACL。组播目的受控的 ACL 只需要配置要控制的源 IPV6 地址和目的 IPV6 地址（即组 IPV6 地址），其配置方式与其它 ACL 基本相同，可以采用掩码长度配置地址范围，也可以指定一个主机地址或所有地址，值得注意的是，这里的“所有地址”对组 IPV6 地址而言是指 ff::/8。

**举例：**

Switch(config)#ipv6 access-list 9000 permit fe80::203:228a/64 ff1e::1/64

## 14.8.6.3 ipv6 multicast destination-control access-group

**命令：ipv6 multicast destination-control access-group *<9000-10999>***

**no ipv6 multicast destination-control access-group *<9000-10999>***

**功能：** 配置端口使用的 IPV6 组播目的控制访问列表，其 NO 形式删除该配置。

**参数：** <9000-10999>：目的受控访问列表号。

**缺省情况：**不配置。

**命令模式：**端口配置模式。

**使用指南：**该命令只有在启动了全局 IPV6 组播目的控制的情况下才起作用，配置该命令后，如果开启 MLD-SNOOPING，对于向组播组添加该端口的情况，将按所配置的访问列表进行匹配，如匹配为 permit，该端口才会被添加，否则不能添加。

**举例：**

switch(config)#inter ethernet 1/1/4

switch(Config-If-Ethernet1/1/4)#ipv6 multicast destination-control access-group 9000

switch(Config-If-Ethernet1/1/4)#

## 14.8.6.4 ipv6 multicast destination-control access-group (sip)

**命令：** **ipv6 multicast destination-control *<IPADDRESS/M>* access-group *<9000-10999>***

**no ipv6 multicast destination-control *<IPADDRESS/M>* access-group *<9000-10999>***

**功能：** 配置指定网段使用的 IPV6 组播目的控制访问列表，其 NO 形式删除该配置。

**参数：** <IPADDRESS/M>:IP 地址和掩码长度；

<9000-10999>：目的受控访问列表号。

**缺省情况：**不配置。

**命令模式：**全局配置模式。

**使用指南：**该命令只有在启动了全局 IPV6 组播目的控制的情况下才起作用，配置该命令后，如果开启 MLD-SNOOPING 或启动了 MLD，对于向组播组添加成员的情况，如果所发送的 MLD-REPORT 的源 IPV6 地址配置了组播目的控制，将按所配置的访问列表进行匹配，如匹配为 permit，该端口才会被添加，否则不能添加。如果使用此命令之前，show ipv6 mld groups detail 中相应的组或者源已经建立，需到特权模式下使用命令 clear ipv6 mld group 清空相应组。

**举例：**

switch(config)#ipv6 multicast destination-control 2008::8/64 access-group 9000

## 14.8.6.5 ipv6 multicast destination-control access-group (vmac)

**命令：** **ipv6 multicast destination-control *<1-4094>* *<macaddr>* access-group *<9000-10999>***

**no ipv6 multicast destination-control *<1-4094>* *<macaddr>* access-group *<9000-10999>***

**功能：** 配置指定 VLAN-MAC 使用的 IPV6 组播目的控制访问列表，其 NO 形式删除该配置。

**参数：** <1-4094>：VLAN-ID；

<macaddr>：发送 MLD-REPORT 的源 MAC 地址，格式为“xx-xx-xx-xx-xx-xx”。

<9000-10999>：目的受控访问列表号。

**缺省情况：**不配置。

**命令模式：**全局配置模式。

**使用指南：**该命令只有在启动了全局 IPV6 组播目的控制的情况下才起作用，配置该命令后，如果开启 MLD-SNOOPING，对于向组播组添加成员的情况，如果所发送的 MLD-REPORT 的源 MAC 地址配置了组播目的控制，将按所配置的访问列表进行匹配，如匹配为 permit，该端口才会被添加，否则不能添加。

**举例：**

switch(config)#ipv6 multicast destination-control 1 00-01-03-05-07-09 access-group 9000

## 14.8.6.6 ipv6 multicast policy

**命令：** **ipv6 multicast policy *<IPADDRSRC/M> <IPADDRGRP/M>* cos *<priority>***

**no ipv6 multicast policy *<IPADDRSRC/M> <IPADDRGRP/M>* cos**

**功能：** 配置 IPV6 策略组播，其 NO 形式取消 IPV6 的策略组播。

**参数：** <IPADDRSRC/M>：IPV6 组播的源地址、源地址掩码长度。

<IPADDRGRP/M>：IPV6 组播的组播地址，组播地址掩码长度。

<priority>：设定的优先级，范围为<0-7>。

**缺省情况：**不配置。

**命令模式：**全局配置模式。

**使用指南：**可以通过该命令配置把通过本交换机的匹配指定范围的组播数据包的优先级更改为指定的值，并且同时指定 TOS 为同样值。这里需要注意的是，对于 UNTAG 方式发出的报文，不会更改其优先级值。

**举例：**

switch(config)#ipv6 multicast policy 2008::1/64 ff1e::3/64 cos 4

## 14.8.6.7 ipv6 multicast source-control

**命令：** **ipv6 multicast source-control**

**no ipv6 multicast source-control**

**功能：** 配置全局启动 IPV6 组播源受控，其 NO 形式恢复为不启动全局 IPV6 组播源控制。

**参数：** 无。

**缺省情况：**不启动。

**命令模式：**全局配置模式。

**使用指南：**只有在启动全局 IPV6 组播源受控的情况下才能把源受控访问列表应用于端口。配置该命令后，所有端口收到的 IPV6 组播数据，如果没有匹配的组播源受控表项，将被交换机丢弃，即只有匹配为 PERMIT 的组播数据才会接收和转发。

**举例：**

Switch(config)#ipv6 multicast source-control

## 14.8.6.8 ipv6 multicast source-control access-group

**命令：** **ipv6 multicast source-control access-group <8000-8099>**

**no ipv6 multicast source-control access-group <8000-8099>**

**功能：** 配置端口使用的组播源控制访问列表，其 NO 形式删除该配置。

**参数：** <8000-8099>：源受控访问列表号。

**缺省情况：**不配置。

**命令模式：**端口配置模式。

**使用指南：**该命令只有在启动了全局 IPV6 组播源控制的情况下才能配置成功，配置该命令后，对于从该端口进入的 IPV6 组播数据报文将按所配置的访问列表进行匹配，如匹配为 permit,该报文才会被接收和转发，否则报文被丢弃。

**举例：**

switch(config)#inter ethernet 1/1/4

switch(Config-If-Ethernet1/1/4)#ipv6 multicast source-control access-group 8000

## 14.8.6.9 multicast destination-control

**命令：** **multicast destination-control**

**no multicast destination-control**

**功能：** 配置全局启动 IPV4 和 IPV6 组播目的受控，配置该命令后，IPV4 和 IPV6 组播目的受控全局同时生效。其 NO 形式恢复为不启动 IPV4 和 IPV6 全局组播目的控制。

**参数：** 无。

**缺省情况：**不启动。

**命令模式：**全局配置模式。

**使用指南：**只有在启动全局组播目的受控的情况下才能使其它的目的控制配置生效，目的受控访问列表可以应用于端口、VLAN-MAC 和 SIP。配置该命令后，IGMP-SNOOPING,MLD-SNOOPING 和 IGMP，MLD 在收到 IGMP-REPORT 和 MLD-REPORT 后试图添加端口时，会按照的上述规则进行匹配。

**举例：**

switch(config)# multicast destination-control

## 14.8.6.10 show ipv6 multicast destination-control

**命令：** **show ipv6 multicast destination-control [detail]**

**show ipv6 multicast destination-control interface <Interfacename> [detail]**

**show ipv6 multicast destination-control host-address <ipv6addr> [detail]**

**show ipv6 multicast destination-control <vlan-id> <mac> [detail]**

**功能：**显示 IPV6 组播目的控制配置。

**参数：**detail：表示是否显示详细信息。

<Interfacename>：端口名或端口聚合名。

<ipv6addr>：IPV6 地址。

<vlan-id> ：VLAN ID。

<mac>：MAC 地址。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**通过该命令显示已经配置的组播目的控制规则，如包含 detail 选项，还包括具体使用的 access-list 的信息。

**举例：**

switch(config)#show ipv6 multicast destination-control

ipv6 multicast destination-control is enabled

ipv6 multicast destination-control 2003::1/64 access-group 9003

ipv6 multicast destination-control 1 00-03-05-07-09-11 access-group 9001

multicast destination-control access-group 6000 used on interface Ethernet1/1/13

switch(config)#

## 14.8.6.11 show ipv6 multicast destination-control access-list

**命令: show ip multicast destination-control access-list**

**show ip multicast destination-control access-list *<9000-10999>***

**功能：** 显示配置的目的受控组播访问列表。

**参数：** <9000-10999>：访问列表号。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**通过该命令显示已经配置的 IPV6 目的受控组播访问列表。

**举例：**

switch# sh ipv6 multicast destination-control acc

ipv6 access-list 9000 permit 2003::2/64 ff1e::3/64

ipv6 access-list 9000 deny 2008::1/64 ff1e::1/64

ipv6 access-list 9000 permit any-source any-destination

ipv6 access-list 9001 deny any-source host-destination ff1a::1

ipv6 access-list 9001 permit any-source any-destination

## 14.8.6.12 show ipv6 multicast policy

**命令：show ipv6 multicast policy**

**功能：**显示配置的 IPV6 组播策略。

**参数：**无。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**通过该命令显示已经配置的组播策略。

**举例：**

switch#show ipv6 multicast policy

ipv6 multicast-policy 2003::2/64 ff1e::3/64 cos 5

## 14.8.6.13 show ipv6 multicast source-control

**命令：show ipv6 multicast source-control [detail]**

**show ipv6 multicast source-control interface *<Interfacename>* [detail]**

**功能：**显示 IPV6 组播源控制配置。

**参数：**detail：表示是否显示详细信息。

<Interfacename>：端口名。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**通过该命令显示已经配置的组播源控制规则，如包含 detail 选项，还包括具体使用的 access-list 的信息。

**举例：**

Switch#show ipv6 multicast source-control detail

Ipv6 multicast source-control is enabled

Interface Ethernet 1/1/1 use multicast source control access-list 8000

ipv6 access-list 8000 permit 2003::2/64 ff1e::3/64

ipv6 access-list 8000 deny 2008::1/64 ff1e::1/64

ipv6 access-list 8000 permit any-source any-destination

## 14.8.6.14 show ipv6 multicast source-control access-list

**命令: show ipv6 multicast source-control access-list**

**show ipv6 multicast source-control access-list *<8000-8099>***

**功能：** 显示配置的 IPV6 源受控组播访问列表。

**参数：** <8000-8099>：访问列表号。

**缺省情况：**无。

**命令模式：**特权模式。

**使用指南：**通过该命令显示已经配置的源受控组播访问列表。

**举例：**

switch#sh ipv6 multicast source-control access-list

ipv6 access-list 8000 permit 2003::2/64 ff1e::3/64

ipv6 access-list 8000 deny 2008::1/64 ff1e::1/64

# 14.8.7 MLD

## 14.8.7.1 clear ipv6 mld group

**命令：clear ipv6 mld group [ X:X::X:X | IFNAME ]**

**功能：**删除指定组或指定接口上的组纪录。

**参数：**X:X::X:X 为指定组地址；IFNAME为指定接口地址。

**命令模式：**特权用户配置模式。

**使用指南：**快速删除组纪录，可以通过show 命令察看组纪录。

**举例：**删除所有组。

Switch#clear ipv6 mld group

**相关命令：show ipv6 mld group**

## 14.8.7.2 debug ipv6 mld events

**命令：debug ipv6 mld events**

**no debug ipv6 mld events**

**功能：**打开显示 MLD 事件的调试开关；本命令的 no 操作为关闭本调试开关。

**参数：**无。

**缺省情况：**关闭。

**命令模式：**特权用户配置模式。

**使用指南：**如果需要查看 MLD 事件信息，则可以打开本调试开关。

**举例：**

Switch# debug ipv6 mld events

Switch#1970/01/11 07:30:13 IMI: MLD Report recv: src fe80::203:fff:fe12:3457 for ff1e::1:3

1970/01/11 07:30:13 IMI: Processing Report comes from Vlan1, ifindex 2003

1970/01/11 07:30:13 IMI: MLD(Querier) ff1e::1:3 (Vlan1): No Listeners --> Listeners Present

## 14.8.7.3 debug ipv6 mld packet

**命令：debug ipv6 mld packet**

**no debug ipv6 mld packet**

**功能：**打开显示 MLD 报文信息的调试开关；本命令的 no 操作为关闭本调试开关。

**参数：**无。

**缺省情况：**关闭。

**命令模式：**特权用户配置模式

**使用指南：**如果需要查看 MLD 报文信息，则可以打开本调试开关。

**举例：**

Switch# deb ipv6 mld packet

Switch#1970/01/11 07:33:12 IMI: Recv MLD packet

1970/01/11 07:33:12 IMI:  Type: Listener Report (131)

1970/01/11 07:33:12 IMI: Code: 0

1970/01/11 07:33:12 IMI: Checksum: 3b7a

1970/01/11 07:33:12 IMI: Max Resp Delay: 0

1970/01/11 07:33:12 IMI: Reserved: 0

1970/01/11 07:33:12 IMI: Multicast Address: ff1e::1:3

1970/01/11 07:33:12 IMI: MLD Report recv: src fe80::203:fff:fe12:3457 for ff1e::1:3

1970/01/11 07:33:12 IMI: Processing Report comes from Vlan1, ifindex 2003

1970/01/11 07:33:12 IMI: MLD(Querier) ff1e::1:3 (Vlan1): Listeners Present --> Listeners Present

## 14.8.7.4 ipv6 mld access-group

**命令：ipv6 mld access-group {<*acl_name*>}**

**no ipv6 mld access-group**

**功能：**配置接口对 MLD 组的过滤条件；本命令的 no 操作取消过滤条件。

**参数：*<acl-name>***为 IPv6 访问列表的名称。

**缺省情况：**缺省为无过滤条件。

**命令模式：**接口配置模式

**使用指南：**可以配置接口对组进行过滤，允许或拒绝某些组的加入。

**举例：**配置接口 VLAN 1 接受组 FF1E::1:0/112，拒绝其它。

Switch (config)# ipv6 access-list aclv6 permit FF1E::1:0/112

Switch (config)# ipv6 access-list aclv6 deny any

Switch (config)#interface vlan 1

Switch(Config-If-Vlan1)#ipv6 mld access-group aclv6

## 14.8.7.5 ipv6 mld immediate-leave

**命令：ipv6 mld immediate-leave group-list {<*acl-name*>}**

**no ipv6 mld immediate-leave**

**功能：**配置 MLD 工作在立即离开模式，即当主机发出等价于离开一个组的成员资格报告时，路由器不发送查询，直接认为子网内没有该组的成员；本命令的 no 操作取消立即离开模式。

**参数：*<acl-name>***为 IPv6 访问列表的名称。

**缺省情况：**出厂时接口缺省不配置立即离开的组。

**命令模式：**接口配置模式

**使用指南：**该命令仅使用在子网内只有一个主机的情况下。

**举例：**将访问列表“aclv6”设为立即离开模式。

Switch(Config-if-Vlan1)#ipv6 mld immediate-leave group-list aclv6

## 14.8.7.6 ipv6 mld join-group

**命令：ipv6 mld join-group *<address>***

**no ipv6 mld join-group <address>**

**功能：**配置该接口加入某个组播组；本命令的 no 操作取消加入某个组播组。

**参数：** ***<address>***为一个合法的 IPv6 组播地址。

**缺省情况：**出厂时接口缺省不加入任何组播组。

**命令模式：**接口配置模式

**使用指南：**IPv6 组播的地址范围为 FFxy::/8，但对于(FF02::/16)的情况属于永久地址，不能加入。

**举例：**使接口 VLAN 2 加入组播地址为分发 ff1e::1:3 的组播组。

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ipv6 mld join-group ff1e::1:3

## 14.8.7.7 ipv6 mld join-group mode source

**命令：ipv6 mld join-group *<X:X::X:X>* mode *<include|exclude>* source *<.X:X::X:X>***

**no ipv6 mld join-group <X:X::X:X> source <.X:X::X:X>**

**功能：**配置该接口加入某个组播组的某个源，注意，由于客户端的组只能有 INCLUDE 和 EXCLUDE 两种模式，因此一旦配置了与当前模式不符的源，组的模式就会改变，原来配置的其它模式的源将会被永久删除；本命令的 no 操作取消加入某个组播组。

**参数：** ***<X:X::X:X>***为一个合法的 IPv6 组播地址。

***<include|exclude>：***加入的模式

***<.X:X::X:X>：***源列表，可以允许配置多个源。

**缺省情况：**出厂时接口缺省不加入任何组播组。

**命令模式：**接口配置模式

**使用指南：**IPv6 组播的地址范围为 FFxy::/8，但对于(FF02::/16)的情况属于永久地址，不能加入。对于模式与原模式相同的情况，源采用增加的方式。如果模式与原模式不同，会清除原来的源。

**举例：**使接口 VLAN 2 加入组播地址为分发 ff1e::1:3 的组播组，源为 2003::1 和 2003::2,模式为 INCLUDE。

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ipv6 mld join-group ff1e::1:3 mode include source 2003::1 2003::2

## 14.8.7.8 ipv6 mld last-member-query-interval

**命令：ipv6 mld last-member-query-interval *<interval>***

**no ipv6 mld last-member-query-interval**

**功能：**配置该接口下特定组查询发送的间隔；本命令的 no 操作取消用户手工配置的值，恢复缺省值。

**参数：*<interval>***为特定组查询的间隔，范围在 1000-25500ms；取值为 1000ms 的整数倍，即如果输入值不为 1000ms 的整数倍，则系统会自动将其转换为 1000ms 的整数倍。

**缺省情况：**缺省为 1000ms。

**命令模式：**接口配置模式

**举例：**使接口 VLAN 1 的 MLD last-member-query-interval 配置为 2000。

Router(config)#int vlan 1

Router(Config-if-vlan1)#ipv6 mld last-member-query-interval 2000

## 14.8.7.9 ipv6 mld limit

**命令：ipv6 mld limit <*state-count*>**

**no ipv6 mld limit**

**功能：**配置该接口下允许保留的 MLD 状态数目；本命令的 no 操作取消用户手工配置的值，恢复缺省值。

**参数：<*state-count*>**:接口最大保留的 MLD 状态，范围在 1-5000。

**缺省情况：**缺省为 400。

**命令模式：**接口配置模式

**使用指南：**当设置了最大状态state-count后，接口只保存不超过state-count个组的状态，如果到达state-count上限，之后接收到有关新的组的成员资格报告，不予处理。如果配置该命令前已经保存了一些MLD组状态，则先删除所有的状态，然后立即发送MLD普通查询收集不超过state-count个组的成员资格报告。

**举例：**使接口 VLAN 2 的 MLD limit 配置为 4000。

Switch(config)#interface vlan2

Switch(Config-if-Vlan2)#ipv6 mld limit 4000

## 14.8.7.10 ipv6 mld query-interval

**命令：ipv6 mld query-interval <*time_val*>**

**no ipv6 mld query-interval**

**功能：**配置周期发送 MLD 查询消息的时间间隔；本命令的 no 操作恢复缺省值。

**参数：<*time_val*>**为周期发送 MLD 查询消息的时间间隔，取值范围 1～65535s。

**缺省情况：**周期发送 MLD 查询消息的时间间隔缺省为 125s。

**命令模式：**接口配置模式

**使用指南：**当某个接口启动某种组播协议后，会周期性地在该接口上发送 MLD 查询消息，本命令用于配置该查询周期时间。

**举例：**配置周期发送 MLD 查询消息的时间间隔为 10s

Switch (config)#interface vlan 1

Switch(Config-If-Vlan1)#ipv6 mld query-interval 10

## 14.8.7.11 ipv6 mld query-max-response-time

**命令：ipv6 mld query-max-response-time <*time_val*>**

**no ipv6 mld query- max-response-time**

**功能：**配置接口对 MLD 查询的最大响应时间；本命令的 no 操作恢复缺省值。

**参数：<*time_val*>**为接口对 MLD 查询的最大响应时间，取值范围 1～8000s。

**缺省情况：**缺省为 10s。

**命令模式：**接口配置模式

**使用指南：**从交换机接收到一条查询消息后，主机会为其所属的每个组播组都设置一个计时器，计时器的值在0～最大响应时间中随机选定，当其中任何一个计时器的值减为0 时，主机就会发送该组播组的成员报告消息。合理设置最大响应时间，可以使主机快速响应查询信息，路由器也就能快速地掌握组播组成员的存在状况。

**举例：**配置对 MLD 查询消息进行响应的最大时间为 20s

Switch (config)#interface vlan 1

Switch(Config-If-Vlan1)#ipv6 mld query- max-response-time 20

## 14.8.7.12 ipv6 mld query-timeout

**命令：ipv6 mld query-timeout <*time_val*>**

**no ipv6 mld query-timeout**

**功能：**配置接口对 MLD 查询的超时时间；本命令的 no 操作恢复缺省值。

**参数：<*time_val*>**为 MLD 查询的超时时间，取值范围 60～300s。

**缺省情况：**缺省为 255s。

**命令模式：**接口配置模式

**使用指南：**在共享网络上，当存在多个运行MLD的交换机时，将选举出其中一台交换机作为该共享网络上的查询器，其它交换机则起一个定时器监控查询器的状态；当经过查询超时时间仍未收到查询器发送的查询报文，则重新选举另一交换机成为新的查询器。

**举例：**配置接口对 MLD 查询的超时时间 100s。

Switch (config)#interface vlan 1

Switch(Config-If-Vlan1)#ipv6 mld query-timeout 100

## 14.8.7.13 ipv6 mld static-group

**命令：ipv6 mld static-group <*group_address*> [*source <source_address>*]**

**no ipv6 mld static-group <group_address> [source <source_address>]**

**功能：在**该接口上配置某个静态组或静态源；本命令的 no 操作取消某个之前配置的静态组或静态源。

**参数：** <group_address>为合法的 IPv6 组播地址；<source_address>为合法的 IPv6 单播地址。

**缺省情况：**出厂时接口缺省不配置任何静态组和静态源。

**命令模式：**接口配置模式

**使用指南：**接口配置的静态组组播地址的合法范围是 IPv6 协议指定的动态组播地址。一旦接口为一个组播地址配置了静态组或静态源，则不管子网内有无该组或该源的成员资格报告，MLD 都认为存在这个组或这个源。注意：配置的静态源为希望转发的源。

**举例：**在接口 VLAN 2 上配置一个 MLD static-group ff1e::1:3。

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3

在接口 VLAN 2 上配置组 ff1e::1:3 的一个静态源 2001::1

Switch(config)#int vlan2

Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3 source 2001::1

## 14.8.7.14 ipv6 mld version

**命令：ipv6 mld version *<version_no>***

**no ipv6 mld version**

**功能：**配置接口上 MLD 工作的版本；本命令的 no 操作取消手工配置的版本，恢复缺省版本。

**参数：**。 ***<version_no>***为 MLD 版本号，取值范围是 1-2。

**缺省情况：**缺省为 2。

**命令模式：**接口配置模式

**使用指南：**当接口相连的子网上还有其它未升级到MLDv2的路由器需要一起参与子网的MLD的成员资格收集时，应当将该接口配置为相应的版本。

**举例：**配置 MLD 的版本为 2。

Swith(config)#interface vlan 1

Swith(config-if-vlan1)#ipv6 mld version 2

## 14.8.7.15 show ipv6 mld groups

**命令：show ipv6 mld groups [{<IFNAME | X:X::X:X | detail | summary | vlan >}]**

**功能：**显示 MLD 组信息。

**参数：*<ifname>***为接口名，即查看指定接口上的组信息；**<*X:X::X:X*>**为组地址，即查看指定组信息；< ***detail*** >显示独立源信息；< ***summary*** >显示组加入统计信息。

**命令模式：**特权和配置模式。

**举例：**

Switch#sh ipv6 mld group

MLD Connected Group Membership

| Group Address | Interface | Uptime | Expires |
|---|---|---|---|
| ff1e::1:3 | Vlan1 | 00:00:16 | 00:03:14 |

Switch#

| 显示信息 | 解释 |
|---|---|
| Group Address | 组播组 IP 地址 |

| | |
|---|---|
| Interface | 组播组所属的接口 |
| Uptime | 组播组已经存在的时间 |
| Expires | 组播组离超时所剩时间 |

## 14.8.7.16 show ipv6 mld interface

**命令：show ipv6 mld interface {vlan *<vlan_id>*|*<ifname>*}**

**功能：**显示接口上相关 MLD 信息。

**参数：*<ifname>***为接口名称，即显示指定接口上的 MLD 信息。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**举例：**显示以太网口 VLAN 1 上的 MLD 信息。

```
Switch#show ipv6 mld interface Vlan1
Interface Vlan1(2003)
 Index 2003
 Internet address is fe80::203:fff:fe01:e4a
 MLD querier
 MLD query interval is 100 seconds
 MLD querier timeout is 205 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 ms
 Group membership interval is 210 seconds
 MLD is enabled on interface
```

## 14.8.7.17 show ipv6 mld join-group

**命令：show ipv6 mld join-group**

**show ipv6 mld join-group interface {vlan *<vlan_id>*|*<ifname>*}**

**功能：**显示接口上 MLD 组加入信息。

**参数：*<ifname>***为接口名称，即显示指定接口上的 MLD 信息。

**缺省情况：**不显示。

**命令模式：**特权和配置模式。

**举例：**显示以太网口 VLAN 2 上的 MLD 信息。

```
Switch#show ipv6 mld join-groups interface Vlan2
Mld join group information:
INTERFACE            : Vlan2
HOST VERSION         : 2
MULTICAST ADDRESS: ff1e::1:3
GROUP STATE          : EXCLUDE
```

SOURCE ADDRESS: 2003::1 mode: EXCLUDE

SOURCE ADDRESS: 2003::2 mode: EXCLUDE

SOURCE ADDRESS: 2003::6 mode: EXCLUDE

## 14.8.8 MLD Snooping

### 14.8.8.1 clear ipv6 mld snooping vlan

**命令：clear ipv6 mld snooping vlan <1-4094> groups [X:X::X:X]**

**功能：**删除指定VLAN里的组纪录。

**参数：**<1-4094>为指定VLAN ID；X:X::X:X 为指定组地址。

**命令模式：**特权用户配置模式。

**使用指南：**快速删除组纪录，可以通过show 命令察看组纪录。

**举例：**删除所有组。

Switch#clear ipv6 mld snooping vlan 1 groups

**相关命令：show ipv6 mld snooping vlan <1-4094>**

### 14.8.8.2 clear ipv6 mld snooping vlan <1-4094> mrouter-port

**命令：clear ipv6 mld snooping vlan <1-4094> mrouter-port [ethernet IFNAME|IFNAME]**

**功能：**删除指定VLAN里的mrouter 端口。

**参数：**<1-4094>为指定VLAN ID；ethernet为以太网端口名；IFNAME为端口名。

**命令模式：**特权用户配置模式。

**使用指南：**快速删除组纪录，可以通过show 命令察看结果。

**举例：**删除VLAN 1里的mrouter端口。

Switch# clear ipv6 mld snooping vlan 1 mrouter-port

**相关命令：show ipv6 mld snooping mrouter-port**

### 14.8.8.3 debug mld snooping all/packet/event/timer/mfc

**命令：debug mld snooping all/packet/event/timer/mfc**

**no debug mld snooping all/packet/event/timer/mfc**

**功能：**打开交换机的MLD Snooping的调试开关；本命令的no操作为关闭该调试开关。

**命令模式：**特权用户配置模式

**缺省情况：**缺省关闭交换机的MLD Snooping的调试开关。

**使用指南：**用来打开交换机MLD Snooping调试开关，可以显示交换机处理MLD数据包信息——packet， 事件信息——event， 计时器信息——timer， 下发硬件表项信息——mfc， 所有debug信息——all。

## 14.8.8.4 ipv6 mld snooping

**命令：ipv6 mld snooping**

**no ipv6 mld snooping**

**功能：**打开交换机的MLD Snooping功能；本命令的no操作为关闭MLD Snooping。

**命令模式：**全局配置模式

**缺省情况：**交换机缺省不启动MLD Snooping。

**使用指南：**打开交换机全局MLD Snooping 开关，即允许每个VLAN设置MLD Snooping功能。no 操作关闭所有VLAN的MLD Snooping功能，并关闭全局MLD Snooping开关。

**举例：**在全局模式启动MLD Snooping。

Switch (config)#ipv6 mld snooping

## 14.8.8.5 ipv6 mld snooping vlan

**命令：ipv6 mld snooping vlan *<vlan-id>***

**no ipv6 mld snooping vlan *<vlan-id>***

**功能：**打开指定 VLAN 的 MLD Snooping 功能；本命令的 no 操作为关闭指定 VLAN 的 MLD Snooping 功能。

**参数：*<vlan-id>***为 VLAN 的 ID 号，取值范围<1-4094>。

**命令模式：**全局配置模式

**缺省情况：**VLAN 缺省不打开 MLD Snooping。

**使用指南：**设置某一个 VLAN 的 MLD Snooping，要先打开全局 MLD Snooping 开关。可通过 no ipv6 mld snooping vlan vid 关闭指定 VLAN 上的 MLD Snooping 功能。

**举例：**在全局配置模式下启动 VLAN 100 的 MLD Snooping 功能。

Switch (config)#ipv6 mld snooping vlan 100

## 14.8.8.6 ipv6 mld snooping vlan immediate-leave

**命令：ipv6 mld snooping vlan *<vlan-id>* immediate-leave**

**no ipv6 mld snooping vlan *<vlan-id>* immediate-leave**

**功能：**打开指定 VLAN 内 MLD 协议的快速离开功能；本命令的 no 操作为关闭 MLD 协议的快速离开功能。

**参数：*<vlan-id>***为指定的 VLAN 的 ID 号，取值范围<1-4094>。

**命令模式：**全局配置模式

**缺省情况：**缺省关闭该功能。

**使用指南：**打开 MLD 协议的快速离开功能，可以加速对端口离开组播组的处理，不会发该组的指定组查询，直接删除。

**举例：**打开 VLAN 100 的 MLD 快速离开功能。

Switch (config)#ipv6 mld snooping vlan 100 immediate-leave

## 14.8.8.7 ipv6 mld snooping vlan l2-general-querier

**命令：ipv6 mld snooping vlan < *vlan-id* > l2-general-querier**

**no ipv6 mld snooping vlan < *vlan-id* > l2-general-querier**

**功能：**将该 VLAN 设为二层普通查询者。

**参数：*vlan-id***:为 VLAN 的 ID 号 取值范围<1-4094>

**命令模式：**全局配置模式

**缺省情况：**VLAN 缺省不是 MLD Snooping 二层普通查询者。

**使用指南：**推荐一个网段配置一个二层普通查询者。如果设置此命令之前，该 VLAN 没有打开 MLD Snooping 功能，应先打开该 VLAN 的 MLD Snooping 功能。在关闭二层普通查询者功能时，不会关闭 MLD Snooping 功能。该命令主要功能是定期发送普通查询来帮助此网段内的交换机学习 mrouter 端口。

**备注：**MLD Snooping 中学习 mrouter 端口的途径有三种：

1 收到 MLD 查询消息的端口

2 收到组播协议报文，支持 PIM 的端口

3 静态配置的端口

**举例：**设置 VLAN 100 为二层普通查询者。

Switch (config)# ipv6 mld snooping vlan 100

Switch (config)# ipv6 mld snooping vlan 100 l2-general-querier

## 14.8.8.8 ipv6 mld snooping vlan limit

**命令：ipv6 mld snooping vlan < *vlan-id* > limit {group <*g_limit*> | source <*s_limit*>}**

**no ipv6 mld snooping vlan < *vlan-id* > limit**

**功能：**设置 MLD snooping 可加入组的个数和每个组中源个数的最大值。

**参数：*vlan-id***: VLAN ID 取值范围<1-4094>

***g_limit***：<1-65535>，加入的组个数最大值

***s_limit***：<1-65535>，每一个组中最多的源表项个数，包括 include 源和 exclude 源

**命令模式：**全局配置模式

**缺省情况：**默认最多 50 个组，每一个组最多可以存放 40 个源表项。

**使用指南：**当加入的组超过 limit，将会拒绝加入。这是为了防止恶意攻击。使用这个命令的前提是该 VLAN 打开了 MLD snooping 功能。No 操作恢复默认值，而不是设置为“无限制”。安全起见，此命令不会设置“无限制”。推荐使用默认值，如果三层 MLD 在运行，请尽量保证此配置与 MLD 的配置一致。

**举例：**Switch(config)#ipv6 mld snooping vlan 2 limit group 300

## 14.8.8.9 ipv6 mld snooping vlan mrouter-port interface

**命令：ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface (<*ehternet*>|<*port-channel*>)<*ifname*>**

**no ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface (<*ehternet*>|<*port-channel*>)<*ifname*>**

**功能：**设置 VLAN 的静态 mrouter 端口。no 操作取消设置。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>

***ehternet*：**以太网端口名

***ifname*：**接口名

***port-channel*:** 端口汇聚

**命令模式：**全局配置模式

**缺省情况：**VLAN 缺省没有静态 mrouter 端口。

**使用指南：**当一个端口同时成为静态 mrouter 端口和动态 mrouter 端口时，以静态 mrouter 端口为准。删除静态 mrouter 端口只能通过 no 操作进行。

**举例：**Switch(config)#ipv6 mld snooping vlan 2 mrouter-port interface ethernet1/1/13

## 14.8.8.10 ipv6 mld snooping vlan mrouter-port flood

**命令：ipv6 mld snooping vlan <*vlan-id*> mrouter-port flood**

**no ipv6 mld snooping vlan <*vlan-id*> mrouter-port flood**

**功能：**使未知组播流量向 mrouter 口泛洪。

**参数：**<*vlan-id*>为指定的 VLAN 的 ID 号，取值范围<1-4094>。

**命令模式：**全局配置模式

**缺省情况：**默认关闭该功能。

**使用指南：**未知组播流量默认不向 mrouter 口泛洪，该命令可以使能泛洪。

**举例：**使能泛洪。

Switch(config)#ipv6 mld snooping vlan 100 mrouter-port flood

## 14.8.8.11 ipv6 mld snooping vlan mrouter-port learnpim6

**命令：ipv6 mld snooping vlan <*vlan-id*> mrouter-port learnpim6**

**no ipv6 mld snooping vlan <*vlan-id*> mrouter-port learnpim6**

**功能：**打开指定 VLAN 根据 pimv6 报文学习 mrouter-port 的功能；本命令的 no 操作为关闭指定 VLAN 根据 pimv6 报文学习 mrouter-port 的功能。

**参数：**<*vlan-id*>为指定的 VLAN 的 ID 号，取值范围<1-4094>。

**命令模式：**全局配置模式

**缺省情况：**默认开启该功能。

**使用指南：**打开指定 VLAN 根据 pimv6 报文学习 mrouter-port 的功能后，当端口收到 pimv6 协议报文后，会把该端口设置为 mrouter 端口，达到自动学习 mrouter 端口的目的。

**举例：**关闭 vlan 100 根据 pimv6 报文学习 mrouter-port 的功能。

Switch(config)#no ipv6 mld snooping vlan 100 mrouter-port learnpim6

## 14.8.8.12 ipv6 mld snooping vlan mrpt

**命令：ipv6 mld snooping vlan <*vlan-id*> mrpt <*value*>**

**no ipv6 mld snooping vlan <*vlan-id*> mrpt**

**功能：**设置 mrouter 端口的生存时间。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>

***value*：**mrouter 端口生存时间，取值范围<1-65535>秒

**命令模式：**全局配置模式

**缺省情况：**255s。

**使用指南：**这个设置对动态 mrouter 端口有效，对静态 mrouter 端口无效。使用这个命令的前提是该 VLAN 的 MLD Snooping 功能打开。

**举例：**Switch(config)#ipv6 mld snooping vlan 2 mrpt 100

## 14.8.8.13 ipv6 mld snooping vlan query-interval

**命令：ipv6 mld snooping vlan <*vlan-id*> query-interval <*value*>**

**no ipv6 mld snooping vlan <*vlan-id*> query-interval**

**功能：**设置查询间隔。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>

***value*：**查询间隔，取值范围<1-65535>秒

**命令模式：**全局配置模式

**缺省情况：**125s。

**使用指南：**推荐使用默认值，如果三层 MLD 在运行，请尽量保证此配置与 MLD 的配置一致。

**举例：**

Switch(config)#ipv6 mld snooping vlan 2 query-interval 130

## 14.8.8.14 ipv6 mld snooping vlan query-mrsp

**命令：ipv6 mld snooping vlan <*vlan-id*> query-mrsp <*value*>**

**no ipv6 mld snooping vlan <*vlan-id*> query-mrsp**

**功能：**设置查询的最大响应时间，no 操作恢复默认值。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>

***value*：**取值范围<1-25>秒

**命令模式：**全局配置模式

**缺省情况：**10s。

**使用指南：**推荐使用默认值，如果三层 MLD 在运行，请尽量保证此配置与 MLD 的配置一致。

**举例：**

Switch(config)#ipv6 mld snooping vlan 2 query-mrsp 18

## 14.8.8.15 ipv6 mld snooping vlan query-robustness

**命令：ipv6 mld snooping vlan <vlan-id> query-robustness <*value*>**

**no ipv6 mld snooping vlan <vlan-id> query-robustness**

**功能：**设置查询鲁棒值，no 操作恢复默认值。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>

***value*：**取值范围<2-10>

**命令模式：**全局配置模式

**缺省情况：**2。

**使用指南：**推荐使用默认值，如果三层 MLD 在运行，请尽量保证此配置与 MLD 的配置一致。

**举例：**

Switch(config)#ipv6 mld snooping vlan 2 query-robustness 3

## 14.8.8.16 ipv6 mld snooping vlan static-group

**命令： ipv6 mld snooping vlan <*vlan-id*> static-group <X:X::X:X> [source < X:X::X:X >] interface [ethernet | port-channel] <IFNAME>**

**no ipv6 mld snooping vlan <*vlan-id*> static-group <X:X::X:X> [source < X:X::X:X >] interface [ethernet | port-channel] <IFNAME>**

**功能：**端口上配置静态组，no 操作恢复默认值。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>

***X:X::X:X*：**ipv6 地址

**命令模式：**全局配置模式

**缺省情况：**不配置静态组。

**使用指南：**当添加的组源同时为静态组和动态组时，以静态组和源为准，添加时需要指明对应端口。

**举例：**

Switch(config)#ipv6 mld snooping vlan 1 static-group ff1e::1 source 2000::1 interface ethernet 1/1/1

## 14.8.8.17 ipv6 mld snooping vlan suppression-query-time

**命令：ipv6 mld snooping vlan <*vlan-id*> suppression-query-time <*value*>**

**no ipv6 mld snooping vlan <*vlan-id*> suppression-query-time**

**功能：**设置抑制查询时间值，no 操作恢复默认值。

**参数：*vlan-id*:** VLAN ID 取值范围<1-4094>

***value*：**取值范围<1-65535>

**命令模式：**全局配置模式

**缺省情况：**255s。

**使用指南：**此命令只能在 L2 普通查询者上设置。Suppression-query-time 的含义为：普通查询者在收到网段内三层 MLD 发来的查询时，进入抑制状态维持的时间。此命令需要确保一个网段内的不同交换机 query-interval 配置一致。推荐使用默认值。

**举例：**

Switch(config)#ipv6 mld snooping vlan 2 suppression-query-time 270

## 14.8.8.18 show ipv6 mld snooping

**命令：show ipv6 mld snooping [vlan <*vlan-id*>]**

**参数：<*vlan-id*>**为指定要显示 MLD Snooping 信息的 VLAN 号。

**命令模式：**特权和配置模式。

**使用指南：**如果不指定 VLAN 号，则显示全局 MLD Snooping 开关有没有打开，三层组播协议是否在运行，以及都有哪些 VLAN 打开了 MLD Snooping 功能，哪一个 VLAN 设置了 l2-general-querier 功能。如果指定 VLAN 号，则显示该 VLAN 的 MLD Snooping 详细信息。

**举例：**

1.显示交换机的 MLD Snooping 摘要信息。

Switch(config)#show ipv6 mld snooping

Global mld snooping status: Enabled

L3 multicasting: running

Mld snooping is turned on for vlan 1(querier)

Mld snooping is turned on for vlan 2

---

| 显示内容 | 解释 |
|---|---|
| Global mld snooping status | 交换机全局 MLD Snooping 开关是否打开 |
| L3 multicasting | 交换机本机三层组播协议是否在运行 |
| Mld snooping is turned on for vlan 1(querier) | 交换机上哪些 VLAN 开启了 MLD Snooping 功能，是否为 l2-general-querier |

2.显示 VLAN 1 的 MLD Snooping 详细信息。

Switch#show ipv6 mld snooping vlan 1

Mld snooping information for vlan 1

Mld snooping L2 general querier :Yes(COULD_QUERY)
Mld snooping query-interval :125(s)
Mld snooping max reponse time :10(s)
Mld snooping robustness :2
Mld snooping mrouter port keep-alive time :255(s)
Mld snooping query-suppression time :255(s)

MLD Snooping Connect Group Membership
Note:*-All Source, (S)- Include Source, [S]-Exclude Source

| Groups | Sources | Ports | Exptime | System Level |
|---|---|---|---|---|
| Ff1e::15 | (2000::1) | Ethernet1/1/8 | 00:04:14 | V2 |
| | (2000::2) | Ethernet1/1/8 | 00:04:14 | V2 |

Mld snooping vlan 1 mrouter port
Note:"!"-static mrouter port
!Ethernet1/1/2

| 显示内容 | 解释 |
|---|---|
| Mld snooping L2 general querier | VLAN 是否启动 l2-general-querier 功能,并且显示 querier 的状态是 could-query 还是 suppressed |
| Mld snooping query-interval | 该 VLAN 的查询间隔时间 |
| Mld snooping max reponse time | 该 VLAN 的最大响应时间 |
| Mld snooping robustness | 该 VLAN 设置的鲁棒值 |
| Mld snooping mrouter port keep-alive time | 该 VLAN 动态 mrouter 的存活期限 |
| Mld snooping query-suppression time | VLAN 作为 l2-general-querier 在抑制状态下的超时时间 |
| MLD Snooping Connect Group Membership | 该 VLAN 的组成员关系，即端口和（S,G）的对应关系 |
| Mld snooping vlan 1 mrouter port | 该 VLAN 的 mrouter 端口，包括静态的和动态的 |

# 14.9 IPv6 安全 RA

## 14.9.1 ipv6 security-ra enable

**命令：ipv6 security-ra enable**

**no ipv6 security-ra enable**

**功能：**全局使能 IPv6 安全 RA 功能，所有的 RA 公告报文不通过硬件转发而是只送 CPU 处理。本命令的 no 操作关闭全局 IPv6 安全 RA 功能。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**默认不启动 IPv6 安全 RA 功能。

**使用指南：**必须全局启动安全 RA 功能后，在端口上的安全 RA 才能启动。关闭全局安全 RA 后，同时清除掉所有已配置的安全 RA 端口。全局安全 RA 功能与全局 IPv6 SAVI 功能互斥，两者不能同时开启。

**举例：**全局启动 IPv6 安全 RA。

Switch(config)#ipv6 security-ra enable

## 14.9.2 ipv6 security-ra enable

**命令：ipv6 security-ra enable**

**no ipv6 security-ra enable**

**功能：**端口上使能 IPv6 安全 RA 功能，该端口收到的 RA 报文不进行转发处理。本命令的 no 操作关闭端口的 IPv6 安全 RA 功能。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**默认不启动 IPv6 安全 RA 功能。

**使用指南：**必须全局启动安全 RA 功能后，在端口上的安全 RA 才能启动。关闭全局安全 RA 后，清除掉所有已配置的安全 RA 端口。

**举例：**端口上启动 ipv6 安全 RA。

Switch(Config-If-Ethernet1/1/2)#ipv6 security-ra enable

## 14.9.3 show ipv6 security-ra

**命令：show ipv6 security-ra [interface *<interface-list>*]**

**功能：**显示那些接口启动了 ipv6 安全 RA 功能。

**参数：**不输入参数则显示所有的非信任端口，输入参数则显示相应的非信任端口。

**命令模式：**特权和配置模式。

**举例：**

Switch#show ipv6 security-ra

IPv6 security ra config and state information in the switch

Globle IPv6 Security RA State:Enable

Ethernet1/1/1

IPv6 Security RA State: Yes

Ethernet1/1/3

IPv6 Security RA State: Yes

### 14.9.4 debug ipv6 security-ra

**命令：debug ipv6 security-ra**

**no debug ipv6 security-ra**

**功能：**打开 IPv6 安全 RA 的调试信息；本命令的 no 操作为关闭 IPv6 安全 RA 的调试信息。

**命令模式：**特权配置模式。

**参数：**无。

**使用指南：**可以查看 IPv6 安全 RA 的报文接收转发处理，在遇到故障时有助于监测故障原因。

**举例：**打开 IPv6 安全 RA 的调试信息。

Switch#debug ipv security-ra

## 14.10 SAVI

### 14.10.1 SAVI

#### 14.10.1.1 ipv6 cps prefix

**命令：ipv6 cps prefix <*ipv6-address*> vlan <*vid*>**

**no ipv6 cps prefix <*ipv6-address*>**

**功能：**手工配置链路 IPv6 地址前缀，本命令的 no 操作为删除链路 IPv6 地址前缀。

**参数：**ipv6-address: 为链路前缀地址，如 2001::/64；

vid: 当前链路所属 vlan ID。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**若用户启用匹配链路地址前缀功能，请首先配置链路本地地址前缀：fe80::/64，以放行所有源地址为链路本地地址的报文。

**举例：**配置 2001::/64 的链路前缀地址。

Switch(config)#ipv6 cps prefix 2001::/64 vlan 1

## 14.10.1.2 ipv6 cps prefix check enable

**命令：ipv6 cps prefix check enable**

**no ipv6 cps prefix check enable**

**功能：**使能 SAVI 地址前缀检查功能；本命令的 no 操作为关闭 SAVI 地址前缀检查功能。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**关闭 SAVI 地址前缀检查功能。

**使用指南：**使能前缀检查功能后，对嗅探报文的 IPv6 地址进行前缀匹配检查，若不符合当前链路前缀，则不建立对应的 IPv6 地址绑定；若用户启用匹配链路地址前缀功能，请首先配置链路本地地址前缀：fe80::/64，以放行所有源地址为链路本地地址的报文。默认关闭地址前缀检查功能。

**举例：**使能 SAVI 地址前缀检查功能。

Switch(config)#ipv6 cps prefix check enable

## 14.10.1.3 ipv6 dhcp snooping trust

**命令：ipv6 dhcp snooping trust**

**no ipv6 dhcp snooping trust**

**功能：**配置该端口为 dhcpv6 trust 端口功能，该端口不再建立 DHCPv6 类型的动态绑定，放行所有 DHCPv6 协议报文；no 命令为删除端口 trust 功能。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**默认关闭端口信任功能。

**使用指南：**设置该端口为 dhcpv6 trust 属性，一般开启 SAVI 功能交换机的连接 dhcpv6 server 或 dhcpv6 relay 的上联端口。

**举例：**设置端口 ethernet1/1/1 为 DHCP 信任端口。

Switch(config)#interface ethernet1/1/1

Switch(config-if-ethernet1/1/1)#ipv6 dhcp snooping trust

## 14.10.1.4 ipv6 nd snooping trust

**命令：ipv6 nd snooping trust**

**no ipv6 nd snooping trust**

**功能：**配置该端口为 slaac trust 和 RA trust 端口，该端口不再建立 slaac 类型的动态绑定，并且转发 RA 报文；no 命令为删除端口 trust 功能。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**默认关闭端口信任功能。

**使用指南：**如果端口没有启用 ipv6 nd snooping trust 功能，则该端口被认为非信任 RA 报文端口，丢弃收到的所有 RA 报文，设置该端口为 trust 属性，一般为开启 SAVI 交换机功能的上联路由器端口，或开启 SAVI 交换机之间的互联端口。

**举例：**设置端口 ethernet1/1/1 为 nd 信任端口。

Switch(config)#interface ethernet1/1/1

Switch(config-if-ethernet1/1/1)#ipv6 nd snooping trust

## 14.10.1.5 savi check binding

**命令：savi check binding *<simple | probe>* mode**

**no savi check binding mode**

**功能：**配置冲突绑定的检查模式；本命令的 no 操作为删除冲突绑定的检查模式。

**参数：**simple 模式：只检查冲突绑定端口所处的状态，若冲突绑定所在端口为 up 状态，则维持冲突绑定，不建立新绑定；若冲突绑定所在端口为 down 状态，则删除冲突绑定，建立新绑定；

probe 模式：除检查冲突绑定的所在端口状态外，若冲突绑定所在端口为 up 状态，还要发出 NS 报文去探测冲突绑定对应用户的可用性，若收到用户端回应的 NA 报文，则维持原冲突绑定，不建立新绑定，否则删除原冲突绑定，建立新绑定。

**命令模式：**全局配置模式。

**缺省情况：**默认为关闭冲突绑定检查模式，采取直接删除冲突绑定，创建新绑定的方式。

**使用指南：**建议用户配置 probe 模式，防止伪造的地址绑定冲突删除合法用户绑定的攻击。

**举例：**设置冲突绑定的检查模式为 probe 模式。

Switch(config)#savi check binding probe mode

## 14.10.1.6 savi enable

**命令：savi enable**

**no savi enable**

**功能：**打开全局 SAVI 功能；本命令的 no 操作为关闭全局 SAVI 功能。

**参数：**无。

**命令模式：**全局配置模式。

**缺省情况：**默认关闭 SAVI 全局功能。

**使用指南：**使能 SAVI 全局功能后，才能进行 SAVI 功能的命令配置，SAVI 功能已经包含了安全 RA 功能，在全局配置上，SAVI 全局功能与安全 RA 全局功能互斥。

**举例：**使能 SAVI 功能。

Switch(config)#savi enable

## 14.10.1.7 savi ipv6 binding num

**命令：savi ipv6 binding num *<limit-num>***

**no savi ipv6 binding num**

**功能：**配置端口对应的绑定数目，no 命令为还原默认值。

**参数：limit-num：设置范围为 0-100 个，端口绑定数目默认值为 100 个。**

**命令模式：端口配置模式。**

**缺省情况：100。**

**使用指南：**该绑定配置数目仅包括 slaac，dhcp 类型的动态绑定，若绑定总数超过该配置数目，则该端口不再创建任何新的动态绑定，若配置数目为 0，则该端口不建立任何动态绑定。

**举例：**设置端口 ethernet1/0/1 的绑定数目为 100。

Switch(config)#interface ethernet1/0/1

Switch(config-if-ethernet1/0/1)#savi ipv6 binding num 100

## 14.10.1.8 savi ipv6 check source binding

**命令：savi ipv6 check source binding ip <*ip-address*> mac <*mac-address*> interface <*if-name*> {type [slaac | dhcp] lifetime <*lifetime*> | type static}**

**no savi ipv6 check source binding ip <*ip-address*> interface <*if-name*>**

**功能：**手工配置动态或静态绑定功能；本命令的 no 操作为删除手工配置的动态或静态绑定功能。

**参数：**ip-address：为 IPv6 单播地址，包括本地链路和全球单播地址；

mac-address：为以太网 mac 地址；

if-name：为端口名，如 interface ethernet 1/1/1；

slaac | dhcp：slaac 表示创建 slaac 类型动态绑定，dhcp 表示创建 dhcp 类型动态绑定；

lifetime：配置动态绑定的生存周期，单位为秒；

static：创建静态类型绑定。

**命令模式：**全局配置模式。

**缺省情况：**无。

**使用指南：**手工配置的动态绑定超时后，会删除该配置对应的绑定，但配置仍保留，因此显示绑定信息时仍会显示该绑定信息；若让该配置对应的绑定重新生效，则需先删除，然后进行重新配置。

绑定类型为 static 类型，则无需配置绑定生存周期，生存周期为 infinite。

**举例：**

手工配置 SAVI slaac 类型动态绑定。

Switch(config)#savi ipv6 check source binding ip 2001::10 mac 00-25-64-BB-8F-04

Interface ethernet1/1/1 type slaac lifetime 2010

手工配置 SAVI 静态类型绑定。

Switch(config)#savi ipv6 check source binding ip 2001::20 mac 00-25-64-BB-8F-04

Interface ethernet1/1/1 type static

## 14.10.1.9 savi ipv6 check source ip-address mac-address

**命令：savi ipv6 check source [ip-address mac-address | ip-address | mac-address]**

**no savi ipv6 check source**

**功能：**使能端口报文控制验证功能；no 命令为关闭端口报文控制验证功能。

**参数：**无。

**命令模式：**端口配置模式。

**缺省情况：**默认关闭报文控制过滤功能。

**使用指南：**必须使能 SAVI 全局功能后，才能配置该命令。

**举例：**在端口 ethernet1/1/1 时，使能报文控制过滤功能。

Switch(config)#interface ethernet1/1/1

Switch(config-if-ethernet1/1/1)#savi ipv6 check source ip-address mac-address

## 14.10.1.10 savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

**命令：savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable**

**no savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable**

**功能：**使能 SAVI 应用场景功能；本命令的 no 操作为关闭 SAVI 应用场景功能。

**参数：**dhcp-only: dhcp-only 应用场景

slaac-only: slaac-only 应用场景

dhcp-slaac: dhcp-only 与 slaac-only 组合应用场景

**命令模式：**全局配置模式。

**缺省情况：**关闭 SAVI 应用场景。

**使用指南：**dhcp-only 应用场景仅嗅探 DHCPv6 报文和 target 字段 IPv6 地址为 link-local ipv6 地址的 DAD NS 报文，对非 link-local 地址 DAD NS 报文不进行嗅探；而 slaac-only 应用场景则嗅探所有类型的 DAD NS 报文；dhcp-slaac 组合应用场景则嗅探所有的 DHCPv6 和 DAD NS 报文；默认为关闭 SAVI 各种应用场景嗅探功能。

**举例：**使能 SAVI dhcp-only 特定应用场景。

Switch(config)#savi ipv6 dhcp-only enable

## 14.10.1.11 savi ipv6 mac-binding-limit

**命令：savi ipv6 mac-binding-limit <*limit-num*>**

**no savi ipv6 mac-binding-limit**

**功能：**配置同一 MAC 地址对应的动态绑定数目；no 命令为恢复默认值。

**参数：**limit-num：设置范围 1-10，同一 MAC 地址对应的默认动态绑定数目为 32 个。

**命令模式：**全局配置模式。

**缺省情况：**默认值为 32 个。

**使用指南：**该命令主要用于防止 SAVI 动态绑定表项的耗尽攻击。

**举例：**设置同一 MAC 地址对应的动态绑定数为 5。

Switch(config)#savi ipv6 mac-binding-limit 5

## 14.10.1.12 savi max-dad-delay

**命令：savi max-dad-delay <*max-dad-delay*>**

**no savi max-dad-delay**

**功能：**配置动态绑定处于 DETECTION 状态，发出 DAD NS 报文探测的生存周期，no 命令为恢复默认值。

**参数：**max-dad-delay：设置范围为 1-65535 秒，max-dad-delay 默认值为 1 秒。

**命令模式：**端口配置模式。

**缺省情况：**采用默认值 1 秒。

**使用指南：**建议用户采用默认值 1 秒。

**举例：**设置探测生存期为 2 秒。

Switch(config)#savi max-dad-delay 2

## 14.10.1.13 savi max-dad-prepare-delay

**命令：savi max-dad-prepare-delay <*max-dad-prepare-delay*>**

**no savi max-dad-prepare-delay**

**功能：**配置动态绑定重新探测的生存周期，no 命令为恢复默认值。

**参数：**max-dad-prepare-delay: 设置范围为 1-65535 秒，max-dad-prepare-delay 默认值为 1 秒。

**命令模式：**全局配置模式。

**缺省情况：**默认值为 1 秒。

**使用指南：**建议用户采用默认值 1 秒。

**举例：**设置重新探测生存期为 2 秒。

Switch(config)#savi max-dad-prepare-delay 2

## 14.10.1.14 savi max-slaac-life

**命令：savi max-slaac-life <*max-slaac-life*>**

**no savi max-slaac-life**

**功能：**配置 slaac 动态绑定处于 BOUND 状态的生存周期，no 命令为恢复默认值。

**参数：**max-slaac-life：设置范围 1-31536000 秒，max-slaac-life 默认为 4 小时。

**命令模式：**全局配置模式。

**缺省情况：**默认值为 4 小时。

**使用指南：**无。

**举例：**设置 slaac 类型绑定的 BOUND 状态的生存周期为 2010 秒。

Switch(config)#savi max-slaac-life 2010

### 14.10.1.15 savi timeout bind-protect

**命令：savi timeout bind-protect <*protect-time*>**

**no savi timeout bind-protect**

**功能：**配置端口由 up 状态变成 down 状态后，对该端口绑定进行保护的生存周期；no 命令为恢复默认值。

**参数：**protect-time：设置范围 1-300 秒，protect-time 默认为 30 秒。

**命令模式：**全局配置模式。

**缺省情况：**默认值为 30 秒。

**使用指南：**若配置生存周期超时后，端口仍处于 down 状态，则将删除该端口上的绑定；若在配置生存周期内，端口由 down 状态转为 up 状态，则该端口上的绑定将重新设置其生存周期为 BOUND 状态的生存周期。若配置参数为 0 秒，则立即删除端口上的所有绑定。

**举例：**设置保护绑定的生存周期为 20 秒。

Switch(config)#savi timeout bind-protect 20

## 14.10.2 SAVI 监控和调试

### 14.10.2.1 监控和调试信息

### 14.10.2.1.1 debug ipv6 dhcp snooping binding

**命令：debug ipv6 dhcp snooping binding**

**no debug ipv6 dhcp snooping binding**

**功能：**打开 SAVI dhcp 类型绑定调试信息开关；本命令的 no 操作为关闭 SAVI dhcp 类型绑定调试信息开关。

**参数：**无。

**命令模式：**特权用户模式。

**缺省情况：**无。

**使用指南：**当打开该调试开关后，将会有相关 SAVI dhcp 类型以及静态类型绑定创建删除打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

**举例：**打开 dhcp 类型绑定调试信息开关。

Switch#debug ipv6 dhcp snooping binding

### 14.10.2.1.2 debug ipv6 dhcp snooping event

**命令：debug ipv6 dhcp snooping event**

**no debug ipv6 dhcp snooping event**

**功能：**打开 SAVI dhcp 类型事件调试信息开关；本命令的 no 操作为关闭 SAVI dhcp 类型事件调试信息开关。

**参数：**无。

**命令模式：**特权用户模式。

**缺省情况：**无。

**使用指南：**当打开该事件开关后，将会有相关 dhcp 类型事件打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

**举例：**打开 DHCP 类型绑定事件调试信息开关。

Switch#debug ipv6 dhcp snooping event

## 14.10.2.1.3 debug ipv6 dhcp snooping packet

**命令：debug ipv6 dhcp snooping packet**

**no debug ipv6 dhcp snooping packet**

**功能：**打开 DHCPv6 报文调试信息开关；本命令的 no 操作为关闭 DHCPv6 报文调试信息开关。

**参数：**无。

**命令模式：**特权用户模式。

**缺省情况：**无。

**使用指南：**当打开该报文调试开关后，将会有相关 DHCPv6 报文打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

**举例：**打开 DHCPv6 报文调试信息开关。

Switch#debug ipv6 dhcp snooping packet

## 14.10.2.1.4 debug ipv6 nd snooping binding

**命令：debug ipv6 nd snooping binding**

**no debug ipv6 nd snooping binding**

**功能：**打开 SAVI slaac 类型绑定调试信息开关；本命令的 no 操作为关闭 SAVI slaac 类型绑定调试信息开关。

**参数：**无。

**命令模式：**特权用户模式。

**缺省情况：**无。

**使用指南：**当打开该调试开关后，将会有相关 SAVI slaac 类型绑定创建删除打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

**举例：**打开 slaac 类型绑定调试信息开关。

Switch#debug ipv6 nd snooping binding

## 14.10.2.1.5 debug ipv6 nd snooping event

**命令：debug ipv6 nd snooping event**

**no debug ipv6 nd snooping event**

**功能：**打开 SAVI slaac 类型事件调试信息开关；本命令的 no 操作关闭 SAVI slaac 类型事件调试信息开关。

**参数：**无。

**命令模式：**特权用户模式。

**缺省情况：**无。

**使用指南：**当打开该事件开关后，将会有相关 slaac 类型事件打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

**举例：**打开 slaac 类型事件调试信息开关。

Switch#debug ipv6 nd snooping event

## 14.10.2.1.6 debug ipv6 nd snooping packet

**命令：debug ipv6 nd snooping packet**

**no debug ipv6 nd snooping packet**

**功能：**打开 ND 报文调试信息开关；本命令的 no 操作为关闭 ND 报文调试信息开关。

**参数：**无。

**命令模式：**特权用户模式。

**缺省情况：**无。

**使用指南：**当打开该报文调试开关后，将会有相关 ND 报文打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

**举例：**打开 ND 报文调试信息开关。

Switch#debug ipv6 nd snooping packet

## 14.10.2.1.7 show savi ipv6 check source binding

**命令：show savi ipv6 check source binding [interface <if-name>]**

**功能：**显示全局 SAVI 绑定表项。

**参数：**if-name: 为端口名，如 interface ethernet 1/1/1。

**命令模式：**特权用户模式。

**缺省情况：**无。

**使用指南：**各显示字段含义如下表

| 字段 | 描述 |
|---|---|
| MAC | 绑定的 MAC 地址 |
| IP | 绑定的 IP 地址 |
| Vlan | 绑定所属 Vlan |
| Port | 绑定所属端口 |
| Type | 绑定类型 |

| State | 绑定状态 |
| --- | --- |
| Expires | 绑定的生存周期 |

**举例：**显示 SAVI 全局绑定状态。

Switch(config)#show savi ipv6 check source binding

Static binding count: 0

Dynamic binding count: 3

Binding count: 3

| MAC | IP | VLAN | Port | Type | State | Expires |
| --- | --- | --- | --- | --- | --- | --- |
| 00-25-64-bb-8f-04 | fe80::225:64ff:febb:8f04 | 1 | Ethernet1/1/5 | slaac | BOUND | 14370 |
| 00-25-64-bb-8f-04 | 2001::13 | 1 | Ethernet1/1/5 | slaac | BOUND | 14370 |
| 00-25-64-bb-8f-04 | 2001::10 | 1 | Ethernet1/1/5 | slaac | BOUND | 14370 |

# 14.11 IPv6 VRRPv3

## 14.11.1 advertisement-interval

**命令：advertisement-interval *<adver_interval>***

**功能：**配置 VRRPv3 通告时间间隔。

**参数：*<adver_interval>***为发送 VRRPv3 通告报文的间隔时间，单位为厘秒(centiseconds)，取值范围为 1~10，**命令模式：**VRRPv3 协议配置模式。

**缺省情况：*<adver_interval>***缺省值为 1 秒

**使用指南：**每隔一段时间，VRRPv3 备份组中的 Master 都会发送 VRRPv3 报文来向组内的路由器（或三层以太网交换机）通知自己工作正常，这个间隔时间就是 *adver_interval*。如果 Backup 超过一定时间（时长为 *master_down_interval*）没有收到 Master 发送来的 VRRPv3 报文，则认为它已经无法正常工作，并将自己的状态转变为 Master。

用户可以使用此命令来调整 Master 发送 VRRPv3 报文的间隔时间。对于同一备份组的成员，该属性应该设置为相同的数值。对于 Backup 来说，其 *master_down_interval* 的取值是 *adver_interval* 的 3 倍。如果网络流量过大或者不同的路由器（或三层以太网交换机）上的定时器差异等因素，会导致 *master_down_interval* 超时并随即引发状态转换。对于这种情况，可以通过将 *adver_interval* 的间隔时间延长和设置较长抢占延迟时间的办法来解决。

**举例：**配置 VRRPv3 通告时间间隔为 3 秒。

Switch(config-router)#advertisement-interval 3

## 14.11.2 circuit-failover

**命令：circuit-failover {vlan <*ID*>| *IFNAME*} <*value_reduced*>**

**no circuit-failover**

**功能：**配置 VRRPv3 监控接口。

**参数：{vlan <*ID*>| *IFNAME*}**为被监视的三层接口名。

**<*value_reduced*>**为优先级降低的数额，取值范围为 1~253。

**命令模式：**VRRPv3 协议配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**对接口的监视功能是对备份功能的一个很好的扩展，该扩展功能不仅在备份组所在的路由器（或三层以太网交换机）接口出现故障时，VRRPv3 能够提供备份功能；而且在其他接口的状态 **down** 掉时，也能够实现通过降低当前路由器（或三层以太网交换机）的优先级以保证备份功能的顺利实施。

使用此命令后，如果被监控接口的状态由 **up** 转为 **down**，则当前路由器（或三层以太网交换机）接口在所属备份组内的优先级就会降低所配置的优先级数额(如果 value_reduced 大于接口配置的 priority，则当相应的接口 down 后，接口在所属备份组内的优先级会降低为 0)，以防止当 Master 出现故障时，Backup 接口由于优先级低于 Master 而无法实现转换；**down** 掉的被监控接口重新 **up** 之后，对应的路由器（或三层以太网交换机）接口在所属备份组内的优先级会自动恢复。

**举例：**配置 VRRPv3 的监控接口为 vlan 2，优先级降低的数额为 10。

```
Switch(config-router)#circuit-failover vlan 2 10
```

## 14.11.3 debug ipv6 vrrp

**命令：debug ipv6 vrrp [all | events | packet [recv | send] ]**

**no debug ipv6 vrrp [all | events | packet [recv | send] ]**

**功能：**显示 VRRPv3 备份组的状态变化和收发报文的情况，该命令的 **no** 形式关闭 DEBUG 显示。

**参数：**无。

**命令模式：**特权用户配置模式。

**举例：**

```
Switch#debug ipv6 vrrp
Jan 01 01:03:13 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1],
virtual-ip=[fe80::2]

Jan 01 01:03:14 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1],
virtual-ip=[fe80::2]
```

Jan 01 01:03:15 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[fe80::2]

## 14.11.4 disable

**命令：disable**

**功能：**关闭 VRRPv3 虚拟路由器。

**参数：**无。

**命令模式：**VRRPv3 协议配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**关闭相应的虚拟路由器会话。在关闭虚拟路由器之后才能修改相关的配置参数。

**举例：**关闭 ID 为 10 的 VRRPv3 虚拟路由器。

Switch(config)#router ipv6 vrrp 10

Switch(config-router)#disable

## 14.11.5 enable

**命令：enable**

**功能：**启动 VRRPv3 虚拟路由器。

**参数：**无。

**命令模式：**VRRPv3 协议配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**启动相应的虚拟路由器会话。只有启动的路由器（或三层以太网交换机）接口才真正加入备份组中。在启动虚拟路由器之前必须配置 VRRPv3 的虚拟 IPv6 地址和接口。

**举例：**启动 ID 为 10 的 VRRPv3 虚拟路由器。

Switch(config)#router ipv6 vrrp 10

Switch(config-router)#enable

## 14.11.6 preempt-mode

**命令：preempt-mode {true| false}**

**功能：**配置 VRRPv3 的抢占模式。

**参数：**无。

**命令模式：**VRRPv3 协议配置模式。

**缺省情况：**缺省为抢占模式。

**使用指南：**如果需要高优先级的路由器（或三层以太网交换机）能主动抢占成为主控路由器（或三层以太网交换机），则要设置抢占模式。

**举例：**配置 VRRPv3 为非抢占模式。

Switch(config-router)#preempt-mode false

## 14.11.7 priority

**命令：priority <*value*>**

**功能：**配置 VRRPv3 的优先级。

**参数：<*value*>**为优先级，取值范围为 1～254。

**命令模式：**VRRPv3 协议配置模式。

**缺省情况：**Backup 路由器（或三层以太网交换机）在所属备份组内的优先级均为 100，IP 地址拥有者在所属备份组内的优先级均为 255。

**使用指南：**优先级决定路由器（或三层以太网交换机）在备份组中的地位，优先级越高就越有可能成为 Master。可配置的优先级数值为 1～254，优先级 255 保留给 IP 地址所有者使用，优先级 0 则具有特殊用途，即当关闭 VRRP 会话时，Master 会发出优先级为 0 的通告报文，Backup 收到这种通告报文后会启动新一轮的 Master 选举。当某备份组内有两台及两台以上路由器（或三层以太网交换机）的优先级取值相同时，则接口链路本地 IPv6 地址最大的路由器（或三层以太网交换机）具有较高的优先级。

**举例：**配置 VRRPv3 的优先级为 150。

```
Switch(config-router)#priority 150
```

## 14.11.8 router ipv6 vrrp

**命令：router ipv6 vrrp <*vrid*>**

**no router ipv6 vrrp <*vrid*>**

**功能：**创建/删除 VRRPv3 虚拟路由器。

**参数：<*vrid*>**为虚拟路由器序号，取值范围为 1～255。

**命令模式：**全局配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**本命令用于创建/删除 VRRPv3 虚拟路由器。虚拟路由器通过虚拟路由器 ID 和关联的虚拟 IPv6 地址唯一确定，只有创建了特定的虚拟路由器后，才能对该虚拟路由器进行相关配置。出于稳定性考虑，可配置的虚拟路由器个数最多为 64 个。

**举例：**配置 ID 为 10 的 VRRPv3 虚拟路由器。

```
Switch(config)#router ipv6 vrrp 10
```

## 14.11.9 show ipv6 vrrp

**命令：show ipv6 vrrp [<*vrid*>]**

**功能：**显示 VRRPv3 备份组的状态和配置信息。

**参数：<*vrid*>**为虚拟路由器序号，取值范围为 1～255，无参数表示显示所有备份组的状态和配置信息。

**命令模式：**特权和配置模式。

**举例：**

```
Switch#show ipv6 vrrp
VrId 1
  State is Master
  Virtual IPv6 is fe80::2 (Not IPv6 owner)
  Interface is Vlan1
  Configured priority is 150, Current priority is 150
  Advertisement interval is 100 centisec
  Preempt mode is TRUE
  Circuit failover interface Vlan1, Priority Delta 3, Status UP
VrId 10
  State is Initialize
  Virtual IPv6 is fe80::3 (Not IPv6 owner)
  Interface is Vlan2
  Priority is 100
  Advertisement interval is 300 centisec
  Preempt mode is TRUE
  Circuit failover interface Vlan2, Priority Delta 10, Status UP
```

| 显示信息 | 解释 |
|---|---|
| State | 状态。 |
| Virtual IPv6 | 虚拟 IPv6 地址。 |
| Interface | 接口名称。 |
| Priority | 优先级。 |
| Advertisement interval | 发送 VRRPv3 通告报文的时间间隔。 |
| Preempt | 抢占模式。 |
| Circuit failover interface | 监控接口信息。 |

## 14.11.10 virtual-ipv6 interface

**命令：virtual-ipv6 <*ipv6-address*> interface {Vlan <*ID*>| *IFNAM*E}**

**no virtual-ipv6 interface**

**功能：**配置 VRRPv3 的虚拟 IPv6 地址和接口。

**参数：<*ipv6-address*>**为虚拟 IPv6 地址，必须为 IPv6 链路本地地址。

**{Vlan <*ID*>| *IFNAM*E}**为接口名称。

**命令模式：**VRRPv3 协议配置模式。

**缺省情况：**缺省为不配置。

**使用指南：**本命令用于向一个已存在的备份组添加虚拟 IPv6 地址和接口，本命令的 **no** 形式用来删除指定备份组的虚拟 IPv6 地址和接口。这里的虚拟 IPv6 地址为链路本地单播地址。同一备份组内只有一个虚拟 IPv6 地址，为了避免 Ping 虚拟 IPv6 地址时返回物理 MAC 地址

的错误，这里规定虚拟 IPv6 地址不能为接口的真实 IPv6 地址。这样，所有 VRRPv3 备份组的接口默认都是 Backup，需要在备份组内选举 Master。

**举例：**配置备份组的虚拟 IPv6 地址为 fe80::2，接口为 vlan1。

```
Switch(config-router)#virtual-ipv6 fe80::2 interface vlan 1
```